Soteria-G1

Secure Boot and Hardware Root of Trust for a General Purpose Application Processor Using the CEC1702

Introduction

Soteria-G1 is a firmware design executed on the CEC1702 device. It can be used in conjunction with any application processor (AP) that boots out of an external SPI flash device to extend the Root of Trust and enforce a secure boot process in the system.

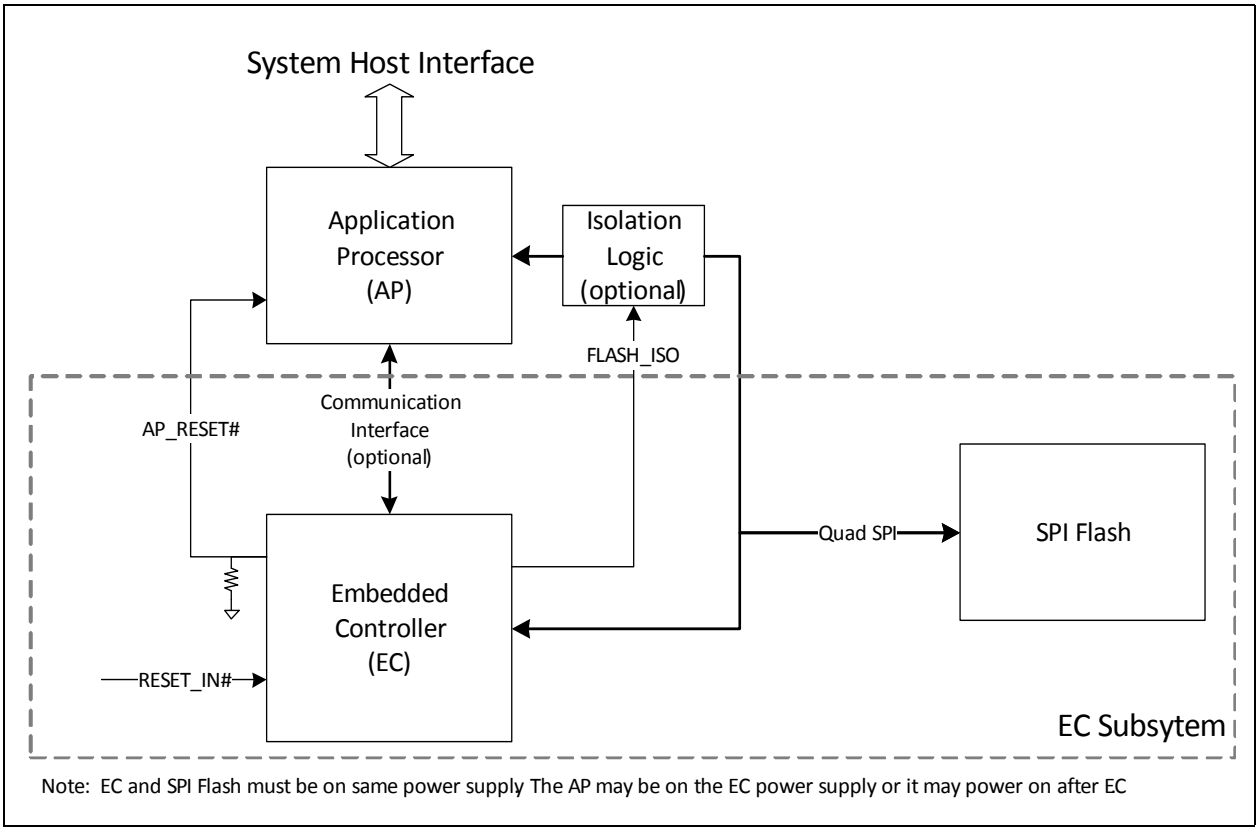
Soteria-G1 uses the CEC1702 immutable secure bootloader, implemented in ROM, as the system Root-of-Trust (RoT). The CEC1702 secure bootloader loads, decrypts and authenticates the embedded controller firmware (EC_FW) from the external SPI Flash. The validated EC_FW that runs on the CEC1702 is designed to subsequently authenticate the application processor firmware (AP_FW) located in the same SPI Flash component and up to three additional SPI Flash components.

Soteria-G1 prevents the system from booting unless the AP_FW stored in the external SPI Flash is authentic code signed by the OEM. It offers security features to authenticate the SPI Flash image in the external SPI flash device.

The validated AP_FW that runs on the application processor can utilize crypto resources in the CEC1702 to authenticate other code in the system, thereby extending the Chain-of-Trust (CoT) to ensure that all code running in the system is authorized.

Soteria-G1 also supports secure firmware updates. EC_FW can authenticate updates to both AP_FW and EC_FW in the system.

FIGURE 1: HIGH-LEVEL BLOCK DIAGRAM



Features

CEC1702 Hardware and Boot ROM Features

Features	Soteria-G1
Immutable Trusted Boot ROM (i.e., Trust Anchor)	Yes
Hardware Security Accelerators support AES-256, SHA-256, ECDSA	Yes
Quad SPI Flash Interface	Yes
Dedicated SPI Flash Access while AP_RESET# is low	Yes
Secure Bootloader Authenticates EC Firmware loaded by Boot ROM	Yes
AES-256 Encrypted EC Firmware	Yes
Read/Write Protected Secure Memory Locations	Yes
Customer usable one-time programmable (OTP) for storing configuration or encrypted secrets	Yes
I2C Host Interface	Yes
GPIOs for Side-band communication	Yes
EC_FW Authentication Key Stored in OTP	Yes
84-Ball WFBGA RoHS Compliant Package, 7mm x 7mm Footprint	Yes

Soteria-G1 Firmware (EC_FW) Features

Features	Soteria-G1
Secure Boot Features	
CEC1702 immutable Boot ROM decrypts and authenticates EC firmware (EC_FW) image while application processor (AP) in reset	Yes
EC_FW authenticates up to 4application firmware (AP_FW) images while AP in reset	Yes
EC_FW authenticates up to 4 golden images while AP in reset	Yes
EC_FW validates AP_FW Public Key Storage used for authenticating AP_FW images	Yes
EC_FW authenticates and parses the application configuration table to customize secure boot solution	Yes
EC_FW releases AP from reset when AP_FW images are authenticated	Yes
AP_FW Public Key Storage	
Validated via SHA-256 hash stored in EC OTP	Yes
Contains DSA public keys used for authenticating AP_FW images	Yes
Number of keys stored in Key Storage	1-4
AP_FW Public Key Types	
RSA PKCS#1, v1.5 with 2k key	Yes
ECDSA P-256; SHA-256	Yes
Application Processor Options	
Supports one Application processor (AP0) or two Application Processors (AP0 and AP1)	Yes
Supports up to two SPI flash components per Application Processor	Yes
SPI flash Isolation (APx_FLASH_ISO)	Yes
Supports AP0 SPI Flash mux select signal (AP0_FLASH_SEL)	Optional

Features	Soteria-G1
Application Configuration (AP_CFG)	
Authenticated using a public key stored in OTP	Yes
Provides system configuration (reset detection, boot types supported and I2C Commands supported)	Yes
Provides location of AP_FW Public Key Storage	Yes
Provides location of AP_FW Image Map	Yes
Reset Generation	
EXTRST#	Optional
AP0_RESET#	Yes
AP1_RESET#	Optional
Reset Detection	
ASYNC_RST_DET# - system reset event	Optional
EXTRST_IN# - AP0 reset event	Optional
AP0_RESET_DET# - AP0 WDT event	Optional
WDTRST1 - AP0 WDT event	Optional
WDTRST2 - AP0 WDT event	Optional
AP0_HBLED# - AP0 heartbeat	Optional
AP1_RESET_IN# - AP1 reset event	Optional
Boot Types Supported	
Primary/Fallback Boot Images	Yes
Primary/Golden Boot Images	Yes
SPI Flash Components Enabled for Boot: • All authenticated components • One authenticated component (either primary or fall-back) • One authenticated component (primary only)	Yes
Runtime SPI Flash Access (AP not in Reset)	
AP0 SPI Flash Access Permitted	Optional
AP1 SPI Flash Access Permitted	Optional
SPI Flash Capabilities	
Normal and Fast SPI Flash Read	Yes
Dual SPI Flash Read	Yes
Quad SPI Flash Read	Yes
4 KB Sector Erase	Yes
Page Program	Yes
SPI Flash Release Power-down / Device ID command	Yes
SPI Flash Enable Reset and Reset Device	Yes
4-byte Addressing Mode	Yes

Features	Soteria-G1
Host I2C Interface	
I2C02_ADDR - slave address strap pin	Yes
Host I2C Commands	
Status Commands (e.g.,Authentication Status)	Yes
Release Flash Isolation	Optional
FLASH_SEL Toggle	Optional
Set Flash Default	Optional
Masked Copy	Optional
Update EC_FW and Reboot (uses Staged and Restore images)	Optional
Restore AP_FW Image (uses Golden Image)	Optional
LED Control	Optional
In-System SPI Flash Updates	
Supports TAG0/TAG1 EC Firmware Image Updates using I2C Command or direct SPI access by AP	Yes
Supports AP_CFG Table Updates using I2C Command or direct SPI access by AP	Yes
Supports AP Firmware updates using direct SPI access by AP	Yes
Supports AP Firmware Recovery (i.e. Golden Image) using I2C Command or direct SPI access by AP	Yes
LED Status	
CEC1702 Activity LED (EC_STS#)	Optional
AP0 Secure Boot Status (LED0)	Optional
AP1 Secure Boot Status (LED1)	Optional
FATAL_ERROR Recovery	
Remote SPI Flash Recovery (FATAL_ERROR# & REMOTE_ACCESS pins)	Yes
Test Modes	
TEST pin (TEST_BYPASS) to bypass Authentication for development (Engineering samples only)	Yes

1.0 OVERVIEW

According to leaders in the industry, the pre-boot firmware environment has come under attack via rootkits and bootkits. These types of attacks are insidious and not detectable by higher level operating systems (OS) or anti-virus software. These attacks can be launched either remotely, by exploiting software bugs and/or software accessible hardware ports, or locally via open hardware ports (i.e., debug ports). Secure boot is a security standard developed to prevent against attacks to the pre-boot firmware environment.

Soteria-G1 provides a complete hardware/software solution for supporting secure boot in the Pre-OS environment that is applicable for a variety of applications (e.g., computing platforms, server, embedded, industrial, automotive, telecommunications, etc.). It provides a method of adding secure boot to system designs that are equipped with an application processor that loads and executes code stored in an external SPI Flash device. Secure Boot ensures the firmware boot code is valid, authentic code signed by the original equipment manufacturer (OEM).

Secure boot refers to a methodology that requires all system firmware to be authenticated before it is executed. Each firmware image must be signed using a known, trusted Digital Signature Algorithm (DSA). The firmware image that authenticates the system firmware signature must either be firmware from an immutable root-of-trust or firmware that has been deemed trusted by the root-of-trust. Once a component is trusted, it can then authenticate the next level firmware in the system.

The Embedded Controller (EC), when used in PC, server, and embedded applications, is designed to authenticate the system BIOS stored in system flash. The EC hardware includes an embedded ARM M4 processor, Boot ROM, Quad SPI Controller, optional I2C host interface, and security acceleration hardware. The hardware accelerators include a TRNG and support for SHA-256, AES-256, RSA, CBC, and ECDSA security features.

Following a power-on-reset (POR) or chip reset the application processor (AP) is held in reset, while the EC executes the Boot ROM firmware. EC Boot ROM firmware, which is used as the root-of-trust or trust anchor in the system, is immutable trusted code implemented in a mask ROM. The Boot ROM secure bootloader acts as a first-stage bootloader (FSBL), which loads, authenticates, and optionally decrypts the EC firmware (EC_FW) stored in SPI Flash. The EC Boot ROM uses elliptic curve signatures (ECDSA) for authenticating the EC_FW stored on SPI Flash.

The EC_FW is used to authenticate the application firmware (AP_FW) stored in SPI Flash. The EC_FW may use either RSA or ECC digital signature algorithms (DSA) for authenticating the AP_FW images. The EC_FW holds the application processor in reset until it validates the firmware integrity of the AP_FW images and validates that they have been signed by the Original Equipment Manufacturer (OEM). Once the EC_FW validates the AP_FW's integrity and authenticity, the EC_FW releases the reset to the application processor (AP).

The AP_FW is custom application specific firmware that ultimately configures and boots the system and loads the runtime OS. The AP_FW, implemented by the system designer, is trusted because it is authenticated by the EC_FW, which was authenticated by the Boot ROM secure bootloader. This process of authenticating each image before it is executed is known as a Chain-of-Trust (CoT).

By design, the Soteria-G1 EC_FW can be either a simple black-box secure boot solution or a customizable EC that provides secure boot, extended security features, and runtime secure commands via a host interface. The EC_FW can be customized to support industry standards like key generation, key wrapping, and DICE+RIOT standards. The EC_FW can support encrypting and storing data on SPI Flash. It can be customized to utilize SPI Flash RPMC feature to prevent against replay attacks.

1.1 References

1. CEC1702 Data Sheet

1.2 System Diagrams

Soteria-G1 supports a number of different system designs.

The following application block diagrams are for illustration purposes only. Specific applications may have additional signals depending on the feature set supported.

FIGURE 1-1: BLOCK DIAGRAM OF ONE AP WITH ONE SPI COMPONENT

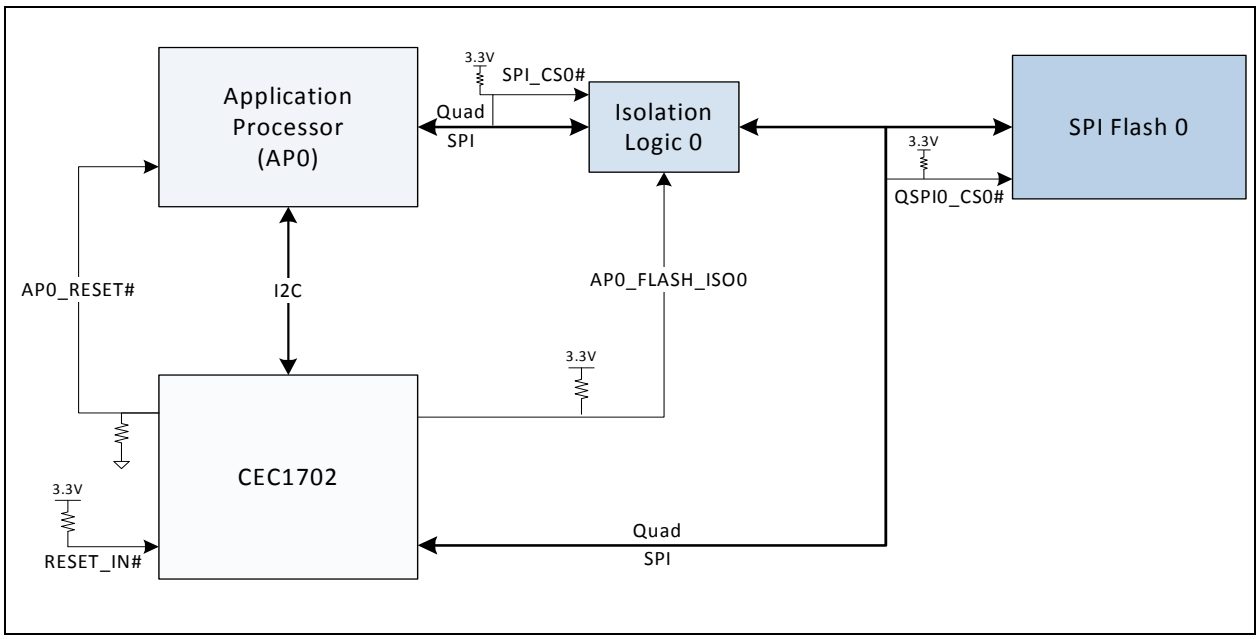
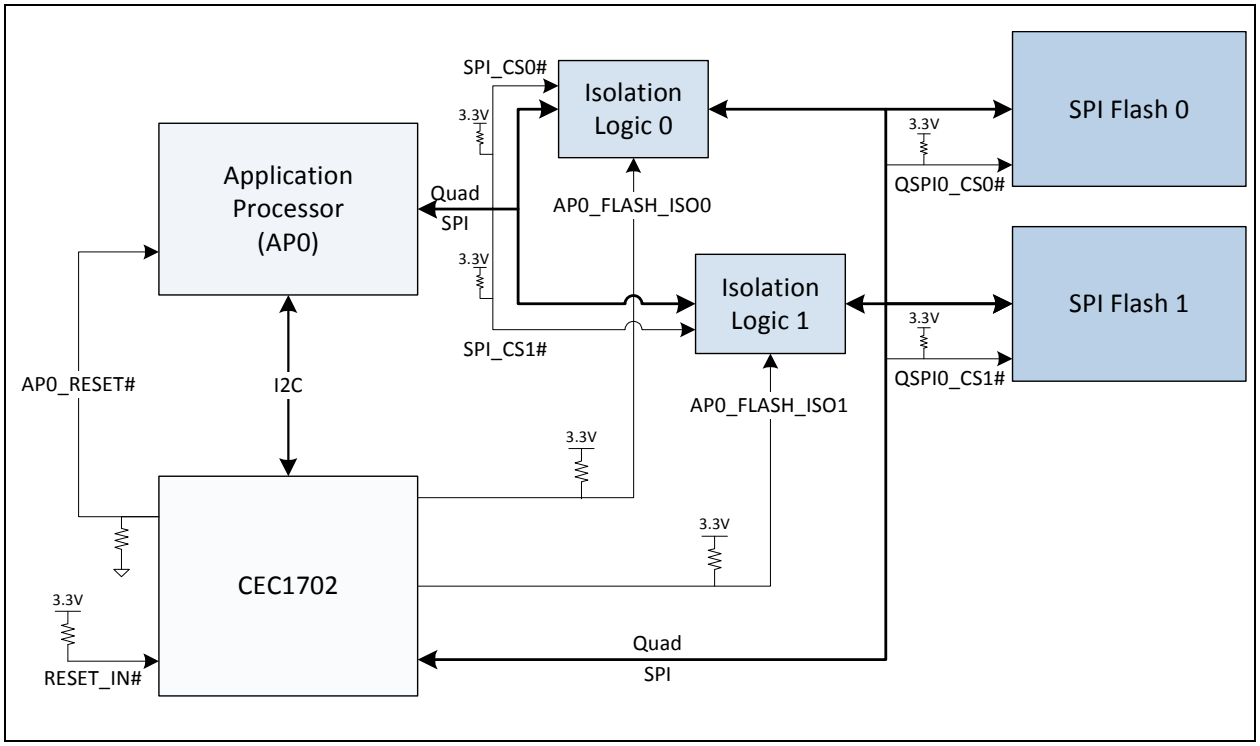


FIGURE 1-2: BLOCK DIAGRAM OF ONE AP WITH TWO SPI COMPONENTS



1.2.1 HIGH-LEVEL BOOT SEQUENCE

In Figure 1-1, "Block Diagram of One AP with One SPI Component", the CEC1702 and the application processor (AP) share access to one flash component. On power-on, the CEC1702 will hold the AP in reset and isolate it from the flash.

The CEC1702 then loads, decrypts and authenticates the EC_FW that runs on the CEC1702 from the flash device. This EC_FW will then authenticate at least one AP_FW image (e.g., Uboot code) in the flash device, before allowing the AP to access the flash and releasing reset to the AP.

If the AP_FW image in the flash component is corrupted, there is an option for the EC_FW to copy a golden image from one location in the flash to the proper location flash component and then once that image is validated, allow the AP to boot from the authentic image.

In Figure 1-2, "Block Diagram of One AP with Two SPI Components", the CEC1702 and the application processor (AP) share access to two flash components. On power-on, the CEC1702 will hold the AP in reset and isolate it from both of the flash components. The EC_FW will then authenticate AP_FW images in both flash components.

If the images in both flash components are validated, then the CEC1702 may allow the AP to boot out of either flash component by allowing AP access to both flash components and releasing reset to the AP. Another option is that the CEC1702 can steer the AP to boot out of one flash component or the other by keeping one component isolated.

If only one of the flash components contain images that pass authentication, then CEC1702 will allow the AP to boot out of the flash component containing authentic images and block access to the flash component with corrupted images. Alternatively, the EC_FW can copy an authenticated image from one component to the other to recover a corrupted image and then allow the AP to boot out of either component.

If both components contain corrupted images, there is an option for the EC_FW to copy a golden image to the proper location in one of the flash components and then once that image is validated, allow the AP to boot from the flash component containing the authentic image.

Figure 1-3, "Block Diagram of Two APs with Two SPI Components" shows support for a second application processor in a system and four SPI flash components.

FIGURE 1-3: BLOCK DIAGRAM OF TWO APS WITH TWO SPI COMPONENTS

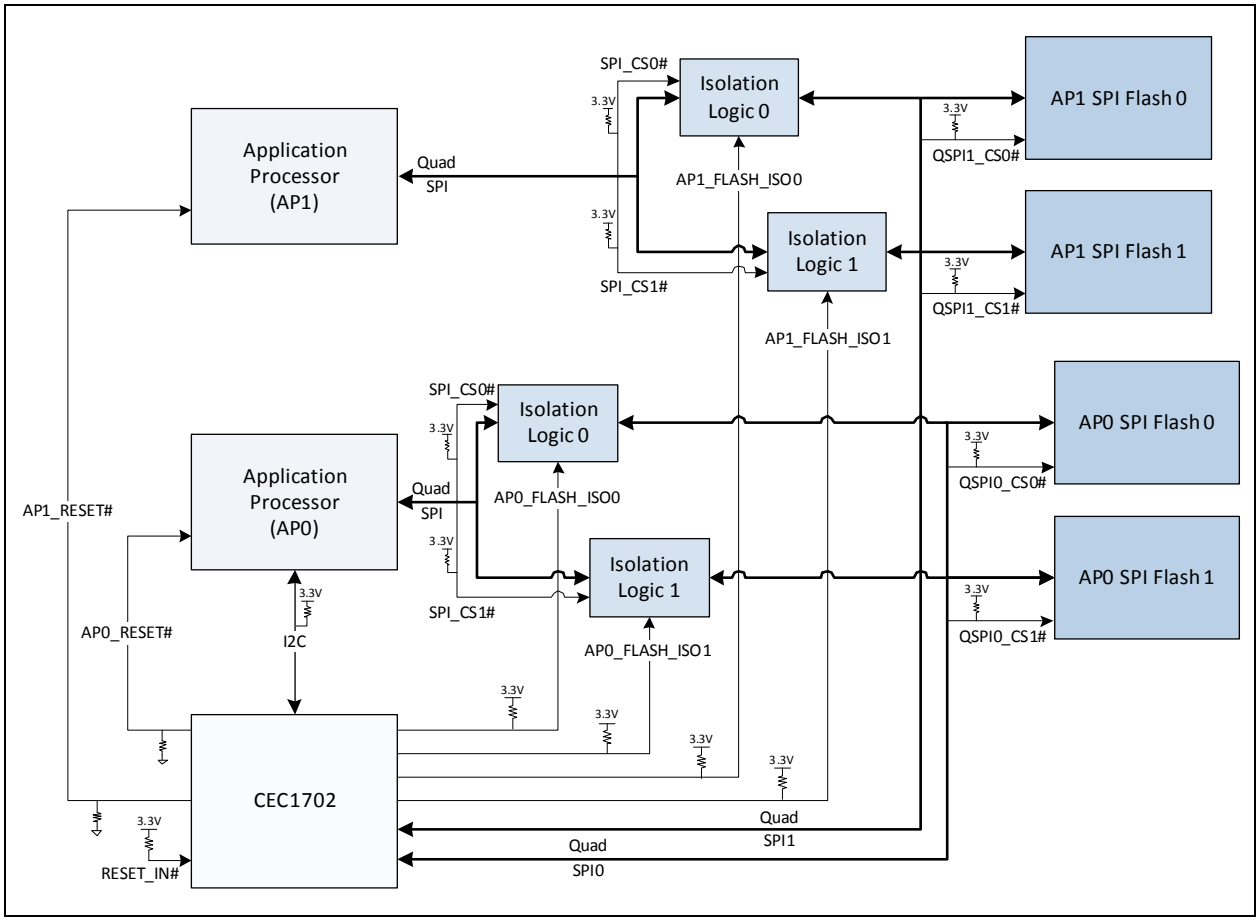


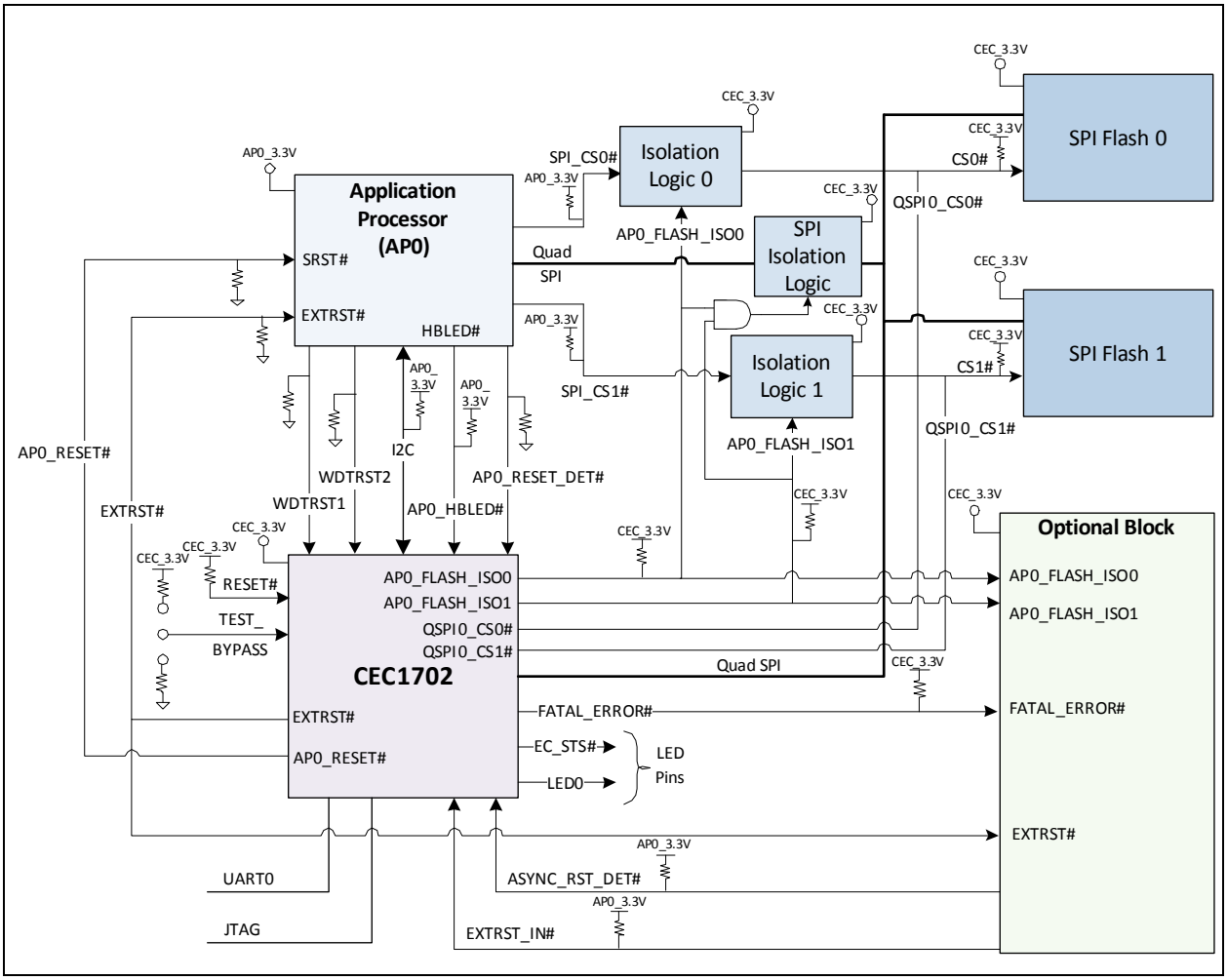
Figure 1-4, "Block Diagram of One AP with Two SPI Components (Detailed)" shows more details of an application of the device.

The optional block can monitor signals to determine authentication status as follows:

TABLE 1-1: AUTHENTICATION STATUS BASED ON SIGNALS

Status	FATAL_ERROR#	EXTRST#	AP0_FLASH_ISO0	AP0_FLASH_ISO1
Fatal error: critical state that prevents the system from booting (i.e., no flash devices contain authentic images)	0	0	1	1
Authentication not complete	1	0	1	1
Authentication complete, both flash devices contain authentic images	1	1	0	0
Authentication complete, flash 0 contains authentic images, flash 1 image(s) failed authentication	1	1	0	1
Authentication complete, flash 1 contains authentic images, flash 0 image(s) failed authentication	1	1	1	0

FIGURE 1-4: BLOCK DIAGRAM OF ONE AP WITH TWO SPI COMPONENTS (DETAILED)



2.0 PIN REQUIREMENTS

This product utilizes the CEC1702 in the 84 pin WFBGA package. See CEC1702 data sheet for the pinout information.

2.1 PINOUT OVERVIEW

2.1.1 PIN MAP

The Power column:

- All power supplies are connected to the same 3.3V power source.

Pin Function(s) Naming Convention:

- The '#' character appended to the end of the name indicates active-low signal

TABLE 2-1: SOTERIA-G1 PIN MAP

CEC1702 Pin Name	Power	Pin Options	Soteria-G1 Pin Function(s)
BGPO0	VBAT	NC	No Connect
GPIO001/PWM4	VTR2	OPT	EXTRST_IN#
GPIO002/PWM5	VTR2	OPT	AP0_FLASH_ISO1 (Note 3)
GPIO003/I2C00_DATA/SPI0_CS#	VTR1	OPT	ASYNC_RST_DET#
GPIO004/I2C00_CLK/SPI0_MOSI	VTR1	REQ	AP0_FLASH_ISO0 (Note 3)
GPIO007/I2C03_DATA	VTR1	REQ	FATAL_ERROR#
GPIO010/I2C03_CLK	VTR1	OPT	I2C02_ALERT0#
GPIO012/I2C07_DATA/TOUT3	VTR2	OPT	EXTRST# (Note 7)
GPIO013/I2C07_CLK/TOUT2	VTR2	OPT	WDTRST2/AP0_RESET_DET#
GPIO016/GPTP-IN7/QSPI0_IO3/ICT3	VTR2	OPT	QSPI0_IO3 (Note 4, Note 8)
GPIO017/GPTP-IN5/KSI0	VTR2	OPT	QSPI0_CS1#
GPIO020/KSI1	VTR2	OPT	Connect to ground (Note 1)
GPIO021/KSI2	VTR2	OPT	Connect to ground (Note 1)
GPIO026/TIN1/KSI3	VTR2		Connect to ground (Note 1)
GPIO027/TIN2/KSI4	VTR2	OPT	AP0_FLASH_SEL
GPIO030/TIN3/KSI5	VTR2	OPT	I2C02_ADDR (strap option)
GPIO031/GPTP-OUT1/KSI6	VTR2	OPT	AP1_FLASH_ISO0 (Note 3)
GPIO032/GPTP-OUT0/KSI7	VTR2	OPT	AP1_FLASH_ISO1 (Note 3)
GPIO034/RC_ID1/SPI0_CLK	VTR1		Connect to ground (Note 1)
GPIO036/RC_ID2/SPI0_MISO	VTR1		Connect to ground (Note 1)
GPIO040/GPTP-OUT2/KSO00	VTR2		Connect to ground (Note 1)
GPIO045/KSO01	VTR1		Connect to ground (Note 1)
GPIO046/BCM1_DAT/KSO02	VTR1		Connect to ground (Note 1)
GPIO047/BCM1_CLK/KSO03	VTR1	OPT	AP0_RESET_DET#
GPIO050/FAN_TACH0/GTACH0	VTR1		Connect to ground (Note 1)
GPIO051/FAN_TACH1/GTACH1	VTR1	REQ	AP0_RESET# (Note 6)

TABLE 2-1: SOTERIA-G1 PIN MAP (CONTINUED)

CEC1702 Pin Name	Power	Pin Options	Soteria-G1 Pin Function(s)
GPIO053/PWM0/GPWM0	VTR2	OPT	EC_STS#
GPIO054/PWM1/GPWM1	VTR2	OPT	AP1_RESET# (Note 6)
GPIO055/PWM2/QSPI0_CS#	VTR2	REQ	QSPI0_CS0# (Note 4)
GPIO056/PWM3/QSPI0_CLK	VTR2	REQ	QSPI0_CLK
GPIO104/UART0_TX	VTR1	OPT	UART0_TX
GPIO105/UART0_RX	VTR1	OPT	UART0_RX
GPIO107/KSO04	VTR2	OPT	Connect to ground (Note 1)
GPIO112/KSO05	VTR2	OPT	Connect to ground (Note 1)
GPIO113/KSO06	VTR2	OPT	AP1_RESET_IN#
GPIO120/KSO7	VTR2	OPT	QSPI1_CS1# (Note 5)
GPIO121/QSPI1_IO0/KSO8	VTR1	OPT	QSPI1_IO0 (Note 5)
GPIO122/QSPI1_IO1/KSO09	VTR1	OPT	QSPI1_IO1 (Note 5)
GPIO124/QSPI1_CS0#/KSO11	VTR1	OPT	QSPI1_CS0# (Note 5)
GPIO125/GPTP-OUT5/QSPI1_CLK/KSO12	VTR1	OPT	QSPI1_CLK (Note 5)
GPIO127/UART0_CTS	VTR1	OPT	WDTRST1
GPIO134/PWM10/UART1_RTS#	VTR1	OPT	TEST_BYPASS
GPIO135/UART1_CTS	VTR1		Connect to ground (Note 1)
GPIO140/ICT5	VTR2	OPT	AP0_HBLED#
GPIO145/I2C09_DATA/JTAG_TDI	VTR1	OPT	JTAG TDI (Note 8)
GPIO146/I2C09_CLK/JTAG_TDO	VTR1	OPT	JTAG TDO (Note 8)
GPIO147/I2C08_DATA/JTAG_CLK	VTR1	REQ	JTAG CLK (SWD Debug)
GPIO150/I2C08_CLK/JTAG_TMS	VTR1	REQ	JTAG TMS (SWD Debug)
GPIO154/I2C02_DATA	VTR1	OPT	I2C02 Data (Note 8)
GPIO155/I2C02_CLK	VTR1	OPT	I2C02 Clock (Note 8)
GPIO156/LED0	VTR1	OPT	LED0
GPIO157/LED1	VTR1	OPT	LED1
GPIO162/VCI_IN1#	VBAT		Connect to ground (Note 1)
GPIO163/VCI_IN0#	VBAT		Connect to ground (Note 1)
GPIO165/32KHZ_IN/CTOUT0	VTR1		Connect to ground (Note 1)
GPIO170/MSCLK/UART1_TX	VTR1		Connect to ground (Note 1)
GPIO171/MSDATA/UART1_RX(JTAG_STRAP)	VTR1	REQ	Connect directly to ground. No external pulls.
GPIO200/ADC00	VTR1	OPT	XNOR test output. Pull to ground.
GPIO201/ADC01	VTR1	OPT	AP0_RESET_DET#
GPIO202/ADC02	VTR1		Connect to ground (Note 1)
GPIO203/ADC03	VTR1		Connect to ground (Note 1)
GPIO204/ADC04	VTR1		Connect to ground (Note 1)

TABLE 2-1: SOTERIA-G1 PIN MAP (CONTINUED)

CEC1702 Pin Name	Power	Pin Options	Soteria-G1 Pin Function(s)
GPIO223/QSPI0_IO0	VTR2	REQ	QSPI0_IO0 (Note 4)
GPIO224/QSPI0_IO1	VTR2	REQ	QSPI0_IO1 (Note 4)
GPIO225/UART0_RTS	VTR1	REQ	REMOTE_ACCESS
GPIO227/QSPI0_IO2	VTR2	OPT	QSPI0_IO2 (Note 4, Note 8)
JTAG_RST#	VTR1	REQ	JTAG (SWD Debug)
RESETI#	VTR1	REQ	EC_RESET# (Note 2)
VCI_OUT	VBAT	NC	No Connect
VBAT	3.3V	PWR	3.3V Power Supply
VR_CAP	CAP	PWR	Voltage Regulator Capacitor (1 uF)
VREF_ADC	3.3V	PWR	VSS
VSS1	GND	PWR	VSS
VSS2	GND	PWR	VSS
VSS_ADC	GND	PWR	VSS
VSS_ANALOG	GND	PWR	VSS
VFLT_PLL	CAP	PWR	External cap
VTR1	3.3V	PWR	3.3V Power Supply
VTR2	3.3V	PWR	3.3V Power Supply
VTR_ANALOG	3.3V	PWR	3.3V Power Supply
VTR_PLL	3.3V	PWR	3.3V Power Supply
VTR_REG	3.3V	PWR	3.3V Power Supply
XTAL1	VBAT	CLOCK	No Connect
XTAL2	VBAT	CLOCK	Connect to ground

Note 1: GPIO pins default to GPIO input unless otherwise noted. GPIO pins must be connected to either power or ground externally to prevent crowbar currents. Once EC firmware is loaded, it will disable all unused GPIO pins where pin function = “Connect to ground,” disabling the buffer internally. Once the buffer is disabled, the leakage currents will go to approx. zero.

2: RESETI# timing requirements are defined in the CEC1702 Data Sheet.

3: The EC_FW tristates the SPI Flash interface before driving AP0_FLASH_ISO0 or AP0_FLASH_ISO1 signals low.

4: QSPI0 is the Shared SPI Flash Interface (i.e., SHD_SPI). This is the port connected to the AP0 SPI Flash components, for example. MCHP recommends the following external logic: SPI bus pull-up values for QSPI_IO[0:3] are 4.7K and QSPI0_CS# value is 2.2K.

5: QSPI1 is referred to as the Private SPI Flash Interface (i.e., PVT_SPI) in some documentation. This port may be connected to SPI Flash components for a second application processor in the system. QSPI1 is a quad-SPI controller, however, only two I/O pins are available for this interface.

6: This pin is a glitch-free tristate pin:

7: EXTRST# is required for certain BMCs and is optional for other application processors. There is an OTP bit that determines if the EXTRST# pin is to be used in the system.

8: This signal is optional. If it is not used, it must be terminated properly on the board. If it is an EC_FW features, it must be terminated to the inactive state on the board. There is no configuration bit to disable this feature. An optional pin without this note has an OTP bit associated with it that is used to determine if the pin is to be used in the system.

9: The I2C02_ALERT0# pin must never be driven high. Systems that do not require this signal will connect directly to ground.

2.1.2 SIGNAL DESCRIPTION TABLE

Note: Application Processor (AP0) refers to an application processor that has its boot images stored in Flash components on the QSPI0 interface.

Note: Application Processor (AP1) refers to an application processor that has its boot images stored in Flash components on the QSPI1 interface.

TABLE 2-2: SOTERIA-G1 SIGNAL DESCRIPTION TABLE

Interface	Pin Function(s)	Direction	Description
AP Reset Signals	AP0_RESET#	Output	AP0_RESET# is signal used to hold AP0 in reset until boot images are authenticated. Requires a pull-down resistor on the board.
	AP1_RESET#	Output	AP1_RESET# is signal used to hold AP1 in reset until boot images are authenticated. Requires a pull-down resistor on the board. **Note:** AP1_RESET# can never be driven high if AP0_RESET# is low.
	EXTRST#	Output	EXTRST# is a runtime reset signal used to put AP0 in reset. This signal is held active until all boot images are authenticated (same as AP0_RESET#). Requires a pull-down resistor on the board.
Reset Detection	ASYNC_RST_DET#	Input	ASYNC_RST_DET# is used to monitor the system reset signal. Requires a pull-up to VTR.
	AP0_RESET_DET#	Input	AP0 Reset Detection signal. Requires a pull-down resistor on the board. • This edge-triggered reset is only valid when AP0_RESET# is high. It is used by EC_FW to detect an unexpected AP0 Reset event. • AP0 firmware must drive this pin high when it boots.
	EXTRST_IN#	Input	EXTRST_IN# is used to monitor the runtime board-level reset signal. Requires a pull-up to VTR.
	AP0_HBLED#	Input	WDT used to detect if AP0 firmware stops executing code. Requires a pull-up to VTR.
	AP1_RESET_IN#	Input	Used to detect AP1 reset not generated by EC. Requires a pull-up to VTR.
	WDTRST1	Input	WDT Reset 1 from AP0 (active-high edge triggered event). Requires a pull-down resistor on the board.
	WDTRST2	Input	WDT Reset 2 from AP0 (active-high edge triggered event). Requires a pull-down resistor on the board.
Error Handling	FATAL_ERROR#	Output	If EC_FW fails to set AP0_RESET# high, this signal is asserted to indicate critical failure. Requires a pull-up to VTR.
	REMOTE_ACCESS	Output	If FATAL_ERROR# is driven low, then this signal is driven high. May be used for external recovery circuit. Requires a pull-down resistor on the board. If not used, pull this pin to ground through a resistor.

TABLE 2-2: SOTERIA-G1 SIGNAL DESCRIPTION TABLE (CONTINUED)

Interface	Pin Function(s)	Direction	Description
I2C	I2C02 Data	I/O	I2C02 Data. Requires a pull-up to VTR.
	I2C02 Clock	Input	I2C02 Clock. Requires a pull-up to VTR.
	I2C02_ADDR	Input	I2C Slave Address strap pin
Flash Isolation	AP0_FLASH_ISO0 (Note 3)	Output	Signal used to isolate Shared SPI Flash Component 0. Requires a pull-up to VTR. This signal is high to isolate AP0 from the flash device.
	AP0_FLASH_ISO1 (Note 3)	Output	Signal used to isolate Shared SPI Flash Component 1. Requires a pull-up to VTR. This signal is high to isolate AP0 from the flash device.
	AP1_FLASH_ISO0 (Note 3)	Output	Signal used to isolate Private SPI Flash Component 0. Requires a pull-up to VTR. This signal is high to isolate AP1 from the flash device.
	AP1_FLASH_ISO1 (Note 3)	Output	Signal used to isolate Private SPI Flash Component 1. Requires a pull-up to VTR. This signal is high to isolate AP1 from the flash device.
LED interface	LED0	Output	LED output, active-high. Provides status of AP0 authentication.
	LED1	Output	LED output, active-high. Provides status of AP1 authentication.
	EC_STS#	Output	LED output, active-low. Provides status of boot process and authentication status.
QSPI0 Interface (Note 4)	QSPI0_CS0#	Output	QSPI0 Flash Component 0 chip select. Requires a pull-up to VTR.
	QSPI0_CS1#	Output	QSPI0 Flash Component 1 chip select. Requires a pull-up to VTR.
	QSPI0_CLK	Output	SPI clock signal
	QSPI0_IO0	I/O	SPI I/O signal
	QSPI0_IO1	I/O	SPI I/O signal
	QSPI0_IO2	I/O	SPI I/O signal
	QSPI0_IO3	I/O	SPI I/O signal
QSPI1 Interface (Note 5)	QSPI1_CS0#	Output	QSPI1 Flash Component 0 chip select. Requires a pull-up to VTR.
	QSPI1_CS1#	Output	QSPI1 Flash Component 1 chip select. Requires a pull-up to VTR.
	QSPI1_IO0	I/O	SPI I/O signal
	QSPI1_IO1	I/O	SPI I/O signal
	QSPI1_CLK	Output	SPI clock signal
Test Bypass	TEST_BYPASS (Bypass authentication)	Input	Test Mode used to bypass authentication during development only. Function disabled in OTP for production parts. Requires options for a pull-down and pull-up to VTR. This pin operates as follows: 1=Bypass; 0=Normal mode
UART0 Interface	UART0_TX	Output	UART transmit pin. May be used for debug.
	UART0_RX	Input	UART receive pin. May be used for debug.

TABLE 2-2: SOTERIA-G1 SIGNAL DESCRIPTION TABLE (CONTINUED)

Interface	Pin Function(s)	Direction	Description
JTAG Interface	JTAG TDI	Input	JTAG Test Data In pin. May be used for debug.
	JTAG TDO	Output	JTAG Test Data Out pin. May be used for debug.
	JTAG CLK (SWD Debug)	Input	JTAG Test Data Out. Also ARM SWO pin. May be used for debug.
	JTAG TMS (SWD Debug)	Input	JTAG Test Mode Select. Also ARM SWDIO pin. May be used for debug.
	JTAG_RST#	Reset	JTAG Reset pin.

Implementation Notes:

1. Any optional pins that are unused should be connected to ground.
2. The power supply for the CEC1702 and flash devices is 3.3V. The CEC1702 and flash devices must be on the same power well.
3. Quad SPI signal pins are shared between the CEC1702 and AP0. Therefore, AP0 must be in reset to tristate these pins in order for the CEC1702 to access the flash. If AP0 is not powered, it must tristate its SPI pins to allow the CEC1702 to access the flash devices, unless isolation logic is added.
4. AP0_RESET_DET# can be connected to any unused GPIO on AP0 for the CEC1702 to detect if the AP is unexpectedly reset. The GPIO on AP0 must tristate when AP0 is reset. Requires a pull-down resistor on the board. A transition low indicates that the AP has been reset. AP0 firmware must drive this pin high when it boots.
5. ASYNC_RST_DET# input to the CEC1702 is a system level reset that can be used to reset the system at any time. Its operation is completely asynchronous to the system boot sequence and runtime operation. When this pin transitions low, the CEC1702 resets the application processor and re-authenticates all AP_FW images.
6. EXTRST_IN# input to the CEC1702 is an external reset event. When this pin transitions low during runtime, the CEC asserts EXTRST# and the AP0 images will be re-authenticated before EXTRST# is asserted high.
7. AP0_HBLED# monitors HBLED# after CEC1702 releases AP0_RESET#. Detects ASPEED unexpectedly executing out of flash after AP0 bootloader runs; CEC1702 treats this event as WDT event. Also reports status of slow/stuck condition.
8. TEST_BYPASS: 1=Bypass; 0=Normal mode. For production boards, tie to ground.
9. I2C pins are recommended to be connected to the application processor in order to use the I2C commands to read authentication status as well as to utilize the other functionality that is provided.
10. For debug, it is recommended to bring UART0_RX and UART0_TX pins to a header.
11. For debug, it is recommended to bring JTAG pins to a header.
12. Programming OTP in system is not supported. For security purposes, it is not recommended to build OTP programming circuit on system board. It is possible this could be used in a firmware attack to alter the unlocked regions of OTP.

APPENDIX A: PRODUCT BRIEF REVISION HISTORY

TABLE A-1: REVISION HISTORY

Revision	Section/Figure/Entry	Correction
DS00003287A (10-23-19)	Initial document release	

THE MICROCHIP WEB SITE

Microchip provides online support via our WWW site at www.microchip.com. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

CUSTOMER CHANGE NOTIFICATION SERVICE

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at www.microchip.com. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

CUSTOMER SUPPORT

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or field application engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: http://www.microchip.com/support

PRODUCT IDENTIFICATION SYSTEM

Not all of the possible combinations of Device, Temperature Range and Package may be offered for sale. To order or obtain information, e.g., on pricing or delivery, refer to the factory or the listed sales office.

PART NO.[1]	-	X	-	XX	-	X[4]/XXX[2]	-	[X][3]
Device		Total SRAM		Version/ Revision		Temp Range/ Package		Tape and Reel Option

Device:	CEC1702[1]	Cryptographic Embedded Controller
Total SRAM:	Q	480KB
Version/Revision:	S1	Soteria-G1
Temperature Range:	Blank	= 0°C to +70°C (Commercial)
	I/	= -40°C to +85°C (Industrial)
Package:	SX	84 pin WFBGA[2], 7mm x 7mm body, 0.65mm pitch
Tape and Reel Option:	Blank	= Tray packaging
	TR	= Tape and Reel[3]

Example:

a) CEC1702Q-S1-I/SX = CEC1702, 480KB total SRAM, Soteria-G1, Industrial Temp, 84-WFBGA, Tray packaging.

Note 1: These products meet the halogen maximum concentration values per IEC61249-2-21.

2: All package options are RoHS compliant. For RoHS compliance and environmental information, please visit http://www.microchip.com/pagehandler/en-us/aboutus/ehs.html

3: Tape and Reel identifier only appears in the catalog part number description. This identifier is used for ordering purposes and is not printed on the device package. Check with your Microchip Sales Office for package availability with the Tape and Reel option.

4: Industrial Temperature is supported by CEC1702.

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

ISBN: 9781522451709

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS

Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
http://www.microchip.com/support
Web Address:
www.microchip.com

Atlanta
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

Austin, TX
Tel: 512-257-3370

Boston
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

Chicago
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

Dallas
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

Detroit
Novi, MI
Tel: 248-848-4000

Houston, TX
Tel: 281-894-5983

Indianapolis
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453
Tel: 317-536-2380

Los Angeles
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608
Tel: 951-273-7800

Raleigh, NC
Tel: 919-844-7510

New York, NY
Tel: 631-435-6000

San Jose, CA
Tel: 408-735-9110
Tel: 408-436-4270

Canada - Toronto
Tel: 905-695-1980
Fax: 905-695-2078

ASIA/PACIFIC

Australia - Sydney
Tel: 61-2-9868-6733

China - Beijing
Tel: 86-10-8569-7000

China - Chengdu
Tel: 86-28-8665-5511

China - Chongqing
Tel: 86-23-8980-9588

China - Dongguan
Tel: 86-769-8702-9880

China - Guangzhou
Tel: 86-20-8755-8029

China - Hangzhou
Tel: 86-571-8792-8115

China - Hong Kong SAR
Tel: 852-2943-5100

China - Nanjing
Tel: 86-25-8473-2460

China - Qingdao
Tel: 86-532-8502-7355

China - Shanghai
Tel: 86-21-3326-8000

China - Shenyang
Tel: 86-24-2334-2829

China - Shenzhen
Tel: 86-755-8864-2200

China - Suzhou
Tel: 86-186-6233-1526

China - Wuhan
Tel: 86-27-5980-5300

China - Xian
Tel: 86-29-8833-7252

China - Xiamen
Tel: 86-592-2388138

China - Zhuhai
Tel: 86-756-3210040

ASIA/PACIFIC

India - Bangalore
Tel: 91-80-3090-4444

India - New Delhi
Tel: 91-11-4160-8631

India - Pune
Tel: 91-20-4121-0141

Japan - Osaka
Tel: 81-6-6152-7160

Japan - Tokyo
Tel: 81-3-6880- 3770

Korea - Daegu
Tel: 82-53-744-4301

Korea - Seoul
Tel: 82-2-554-7200

Malaysia - Kuala Lumpur
Tel: 60-3-7651-7906

Malaysia - Penang
Tel: 60-4-227-8870

Philippines - Manila
Tel: 63-2-634-9065

Singapore
Tel: 65-6334-8870

Taiwan - Hsin Chu
Tel: 886-3-577-8366

Taiwan - Kaohsiung
Tel: 886-7-213-7830

Taiwan - Taipei
Tel: 886-2-2508-8600

Thailand - Bangkok
Tel: 66-2-694-1351

Vietnam - Ho Chi Minh
Tel: 84-28-5448-2100

EUROPE

Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

Finland - Espoo
Tel: 358-9-4520-820

France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

Germany - Garching
Tel: 49-8931-9700

Germany - Haan
Tel: 49-2129-3766400

Germany - Heilbronn
Tel: 49-7131-72400

Germany - Karlsruhe
Tel: 49-721-625370

Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

Germany - Rosenheim
Tel: 49-8031-354-560

Israel - Ra'anana
Tel: 972-9-744-7705

Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

Italy - Padova
Tel: 39-049-7625286

Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

Norway - Trondheim
Tel: 47-7288-4388

Poland - Warsaw
Tel: 48-22-3325737

Romania - Bucharest
Tel: 40-21-407-87-50

Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

Sweden - Gothenberg
Tel: 46-31-704-60-40

Sweden - Stockholm
Tel: 46-8-5090-4654

UK - Wokingham
Tel: 44-118-921-5800
Fax: 44-118-921-5820