CEC173X-TFLX

Real Time Platform Root of Trust Controller

Hardware Features

- Hardware CNSA Based Secure Boot (P-384)
- AES256
- SHA-384
- ECDSA
- True Random Number Generator (SP800-90B)
- SPI Boot Flash Monitoring and Intervention (1.8V or 3.3V)
- Key Management Engine
- Hardware-Based Physically Unclonable Function (PUF)
- Differential Power Analysis Countermeasures
- User Configurable 3.3V or 1.8V Power Spec
- Internal Q-Switches
- Lifecycle Management
- 84-pin and 64-pin Package Sizes (7x7x0.8 mm and 5.5x5.5x0.92 mm)

Soteria-G3 Software Features

- NIST 800-193 and Open Compute Project Compliant
- Soteria-G3 code is cleared by MISRA, checked by Coverity® and CERT® C code analysis and certified by third-party penetration tests
- Secure Boot of up to two Application Processors and up to 16 AP FW images
- SPDM-Compliant Component Attestation
- Secure I^2C Crisis Recovery
- Secure Firmware Updates using PLDM and Crisis Recovery
- Transfer of Ownership
- Authentication Key Revocation
- Firmware Rollback Protection
- Run-time Status Reporting over I^2C
- Life Cycle Management

© 2024 Microchip Technology Inc. and its subsidiaries

TO OUR VALUED CUSTOMERS

It is our intention to provide our valued customers with the best documentation possible to ensure successful use of your Microchip products. To this end, we will continue to improve our publications to better suit your needs. Our publications will be refined and enhanced as new volumes and updates are introduced.

If you have any questions or comments regarding this publication, please contact the Marketing Communications Department via E-mail at **docerrors@microchip.com**. We welcome your feedback.

Most Current Data Sheet

To obtain the most up-to-date version of this data sheet, please register at our Worldwide Web site at:

http://www.microchip.com

You can determine the version of a data sheet by examining its literature number found on the bottom outside corner of any page. The last character of the literature number is the version number, (e.g., DS30000000A is version A of document DS30000000).

Errata

An errata sheet, describing minor operational differences from the data sheet and recommended workarounds, may exist for current devices. As device/documentation issues become known to us, we will publish an errata sheet. The errata will specify the revision of silicon and revision of document to which it applies.

To determine if an errata sheet exists for a particular device, please check with one of the following:

- Microchip's Worldwide Web site; http://www.microchip.com
- Your local Microchip sales office (see last page)

When contacting a sales office, please specify which device, revision of silicon and data sheet (include -literature number) you are using.

Customer Notification System

Register on our web site at **www.microchip.com** to receive the most current information on all of our products.

© 2024 Microchip Technology Inc. and its subsidiaries

Table of Contents

1.0 “General Description” 5

2.0 “System Configuration” 6

3.0 “Memory Zones” 7

- **3.1 “OTP Memory”** 7
- **3.2 “SRAM”** 7
- **3.3 “Internal Flash”** 7

4.0 “Soteria-G3 Overview” 8

5.0 “Pin Configuration” 10

- **5.1 “Packaging Options”** 10
- **5.2 “Pin List”** 10
- **5.3 “Package Information”** 13
  - **5.3.1 “64 Pin VFBGA Package”** 13
  - **5.3.2 “84 Pin WFBGA Package”** 16

6.0 “Detailed Soteria-G3 Description” 19

- **6.1 “Secure Boot”** 19
  - **6.1.1 “Required Secure Boot Components”** 19
  - **6.1.2 “Secure Boot Flow”** 19
  - **6.1.3 “Run Time Authentication”** 20
  - **6.1.4 “Image Configuration Parameters”** 20
- **6.2 “SPI Monitor”** 20
  - **6.2.1 “Pre-Boot and Post-Boot Mode”** 20
  - **6.2.2 “Memory Protection Regions”** 20
  - **6.2.3 “Monitor Violation Settings”** 21
  - **6.2.4 “User Configurable Options”** 21
- **6.3 “Secure Update”** 21
  - **6.3.1 “Supported PLDM Commands”** 22
  - **6.3.2 “User Configurable Options”** 23
- **6.4 “Attestation”** 24
  - **6.4.1 “Device Certificates”** 24
  - **6.4.2 “Supported SPDM Commands”** 24
  - **6.4.3 “User Configurable Options”** 25
- **6.5 “Transfer of Ownership”** 25
  - **6.5.1 “Ownership Transfer Methods”** 25
- **6.6 “Crisis Recovery”** 25
  - **6.6.1 “Soteria-G3 Image Recovery”** 25
  - **6.6.2 “AP Image Recovery”** 25
  - **6.6.3 “User Configurable Parameters”** 26
- **6.7 “Key Revocation”** 26
  - **6.7.1 “User Configurable Options”** 26
  - **6.7.2 “Manual Key Revocation”** 26
  - **6.7.3 “Automatic Key Revocation”** 26

© 2024 Microchip Technology Inc. and its subsidiaries

6.8 “Rollback Protection” 26
6.8.1 “User Configurable Options” 26
6.8.2 “Manual Rollback Protection” 26
6.8.3 “Automatic Rollback Protection” 27
7.0 “I^{2}C Commands” 29
8.0 “Development Tools” 31
8.1 “Software Tools” 31
8.2 “Hardware Tools” 31
9.0 “Electrical Characteristics” 32
Appendix A: “Data Sheet Revision History” 33
“Product Identification System” 34
“The Microchip Web Site” 35
“Customer Change Notification Service” 35
“Customer Support” 35
“Worldwide Sales and Service” 37

© 2024 Microchip Technology Inc. and its subsidiaries

1.0 GENERAL DESCRIPTION

The CEC173x-TFLX Trust Shield Family is the Real Time Platform Root of Trust Controller for Servers, Telecommunications, Networking, Industrials, and Embedded Computing applications.

The CEC173x-TFLX is a partially configured and provisioned variant of the CEC173x Trust Shield family of Real Time Platform Root of Trust Controllers. The devices come pre-provisioned with Soteria-G3 firmware, and the configuration enables customers to use unique credentials for Application Processor images.

The device configuration is designed to make CEC173x-TFLX support most common use cases, while minimizing the learning and development time to enable product quick time to market.

The CEC173x-TFLX is a highly configurable, mixed-signal, advanced I/O controller. It contains a 32-bit 96 MHz ARM® Cortex-M4F processor core with closely coupled memory for optimal code execution and data access.

The CEC173x-TFLX was designed to meet the NIST 800-193 Platform Resiliency Guidelines, as well as the Open Compute Project (OCP) Security Project requirements.

The immutable secure bootloader implemented in the CEC173x TrustFLEX ROM (Boot ROM) loads and authenticates the embedded controller firmware (EC_FW/Soteria-G3) from the internal SPI Flash. The Authenticated EC_FW (Soteria-G3) will then authenticate and validate Application Processor image stored in external SPI Flash.

The validated EC_FW (Soteria-G3) along with the Boot ROM code supports many additional security features of the device, including Key revocation, Code Rollback Protection and Transfer of Ownership. In addition, the Boot ROM implements Life Cycle Management and SPDM for Attestation. The SPDM implementation in EC_FW (Soteria-G3) supports commands that return certificates and measurement information for attestation.

Both the Boot ROM and the EC_FW (Soteria-G3) support more than one public key for image authentication and key revocation. A public key may be revoked, i.e., taken out of service, if the private key becomes compromised.

The Boot ROM and the EC_FW also support Rollback Protection, which prevents certain firmware images from being permitted to run in a system. This feature is used if an older image version may compromise the system security.

The CEC173x TrustFLEX SPI Flash Monitor blocks, one instance per Host, maintain Host firmware integrity both during Host Boot and Host Runtime. At Host Boot, it calculates and verifies signatures of the loaded code blocks in real time, while also verifying that the Host's firmware is executing the correct opcodes from Flash. At Host Runtime, it verifies that only legal Flash accesses are performed, using regional access permission settings, and that no illegal or questionable opcodes (such as Chip Erase) are attempted. Upon seeing an attempted violation of SPI integrity or access rules, it will intervene in real time, in such a way as to cancel a Read, Write, Program or Erase before it can be performed. The Intervention technique works with even the most economical 8-pin standard NOR Flash devices.

The CEC173x TrustFLEX also contains a core Crypto hardware accelerator engine supporting SHA-384, 256-bit AES encryption, ECDSA signing algorithms, Elliptic asymmetric public key algorithms, and a Deterministic Random Number Generator (DRNG). Runtime APIs are provided in the ROM for customer application code to use the cryptographic hardware. PUF ID generation resources and algorithms are included, as well as lockable OTP storage for keys and IDs. Fused Life Cycle security gives access to these resources only when appropriate for development, test, or production phases.

The CEC173x TrustFLEX is designed to be incorporated into low power designs. During normal operation, the hardware always operates in the lowest power state for a given configuration. The chip power management logic offers two low power states: light sleep and heavy sleep. When the chip is sleeping, it has many wake events that can be configured to return the device to normal operation, for example any GPIO pin.

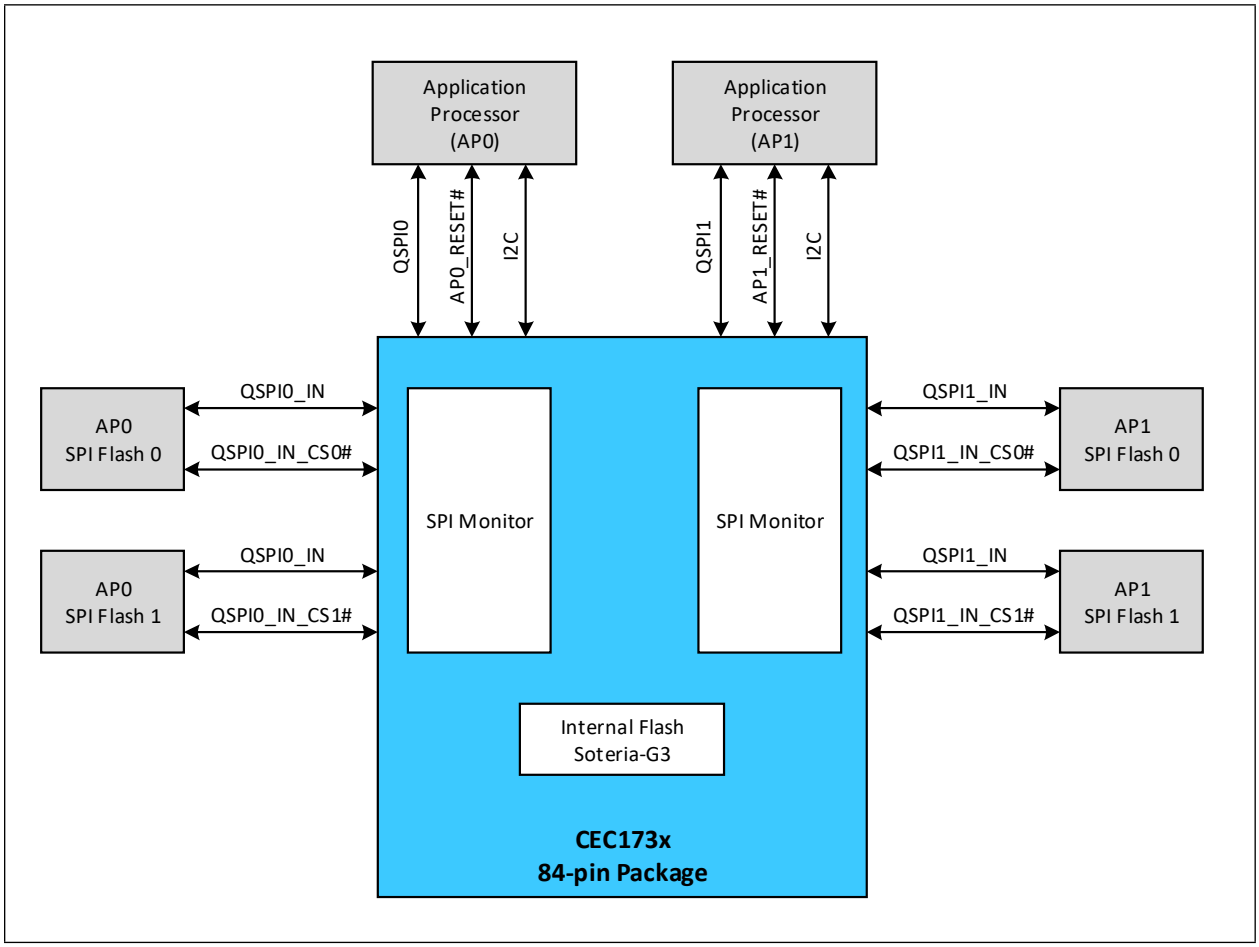
The CEC173x TrustFLEX offers a software development system interface that includes a serial debug port (UART) and a 2-pin Serial Wire Debug (SWD) interface. Also included is a full 4-wire JTAG interface for Boundary Scan testing (disabled for production).

© 2024 Microchip Technology Inc. and its subsidiaries

2.0 SYSTEM CONFIGURATION

Figure 2-1 shows an example usage of the CEC173x-TFLX device. In this configuration, there are two Application Processors, each on their own QSPI port connected to two SPI flash devices. Each Application Processor has their own I^2C port to request status information from the CEC173x-TFLX.

FIGURE 2-1: SYSTEM BLOCK DIAGRAM



© 2024 Microchip Technology Inc. and its subsidiaries

3.0 MEMORY ZONES

The CEC173x-TFLX can be split up into three memory zones: the One-Time Programmable (OTP) memory, SRAM, and Internal Flash memory. Each zone has application-specific uses, configuration information and data, which can be set up and managed using the CEC173x-TFLX Configurator available from Microchip.

3.1 OTP Memory

OTP Memory provides one portion of the configuration and data required for CEC173x-TFLX + Soteria-G3 functionality. Much of the OTP zone will be pre-configured by Microchip to enable rapid prototyping and system integration for the customer. The remaining customer configurable zones can be easily customized when using the Microchip Trust Platform Design Suite to fit specific application requirements.

3.2 SRAM

The SRAM of the CEC173x-TFLX is shared by the Soteria-G3 firmware and data memory for the device during run-time.

3.3 Internal Flash

The internal flash memory of the CEC173x-TLFX is used to store the signed and encrypted Soteria-G3 images, any customer certificate chains, as well as other data blocks used by the device during normal operation. The CEC173x-TFLX offers both 2MB and 4MB options for the internal flash.

© 2024 Microchip Technology Inc. and its subsidiaries

4.0 SOTERIA-G3 OVERVIEW

The Soteria-G3 Firmware is an all-in-one solution developed by Microchip to exercise all the available security features of the CEC173x-TFLX. Soteria-G3 provides an enhanced feature set, including the Secure Boot of Application Firmware images, Secure Firmware Updates, Platform Attestation compliant with SPDM, and much more.

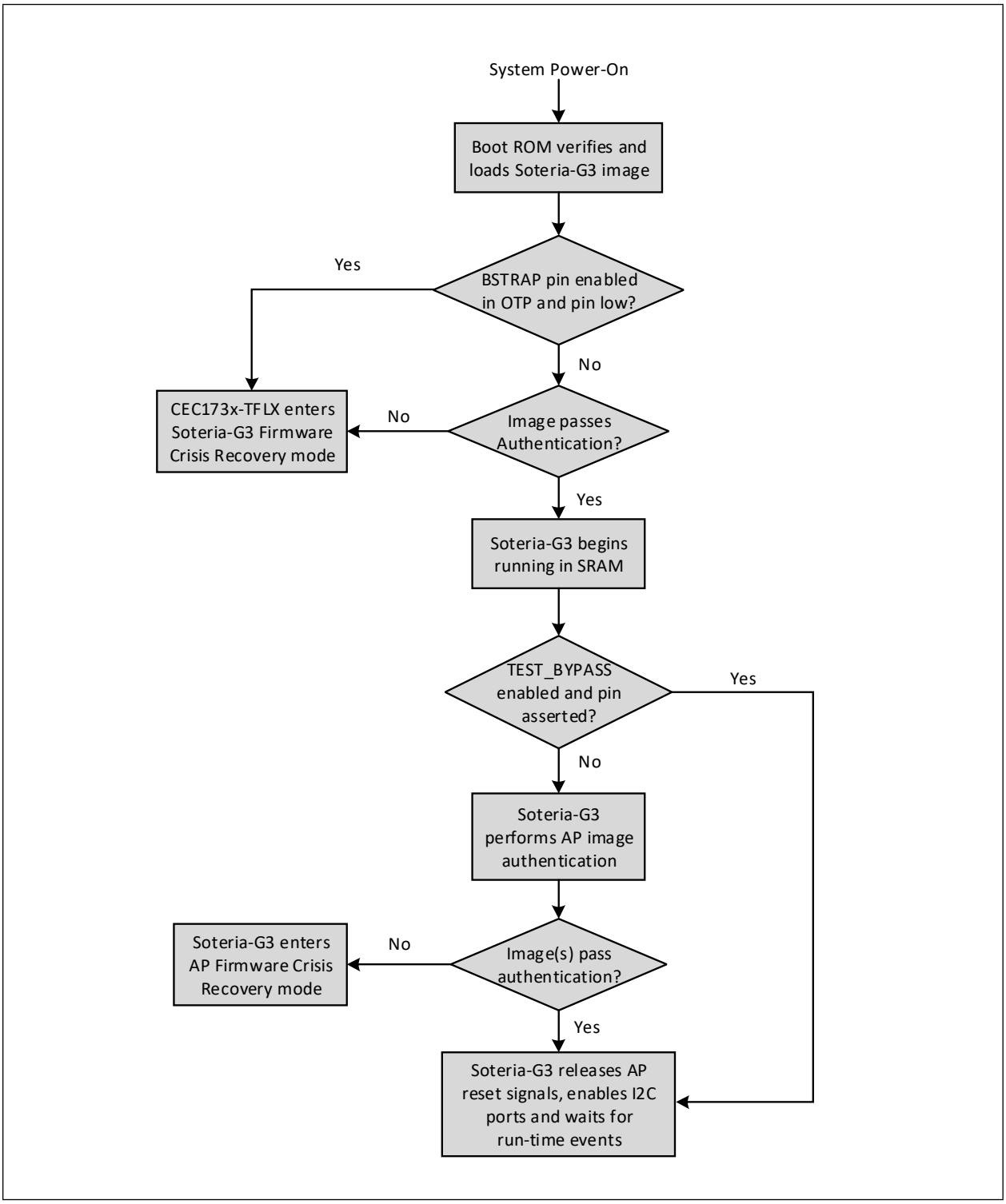
At power-up, the CEC173x-TFLX will hold the Application Processor(s) (AP) in reset and isolate the external flash components. The authenticated Soteria-G3 Firmware running in the CEC173x-TFLX will use the AP Configuration (AP_CFG) Table, which provides all configuration information about the system, to perform any hardware initialization and firmware set-up required before Secure Boot. The Soteria-G3 Firmware will also read the Hash Table(s), which contain the hash values of all AP firmware images present in the external SPI flash components, as well as which images require authentication. Soteria-G3 then performs the Secure Boot process to authenticate the AP firmware images, if they are configured to be, before releasing the AP reset signal. Figure 4-1 below shows a flowchart outlining the boot process.

After AP reset is released, Soteria-G3 will reauthenticate the AP firmware images as they are being read by the AP. This image authentication status is made available through the AP I^2C port for additional validation. At this point, Soteria-G3 is ready to handle requests made for any of the additional software features available that have been enabled and configured by the customer.

Soteria-G3 code is cleared by MISRA, checked by Coverity® and CERT® C code analysis and certified by third-party penetration tests.

© 2024 Microchip Technology Inc. and its subsidiaries

FIGURE 4-1: BOOT PROCESS



5.0 PIN CONFIGURATION

5.1 Packaging Options

The CEC173x-TFLX Family comes in both 64-pin and 84-pin packaging options. The 84-pin package (2ZW) has two QSPI ports with SPI monitoring to support up to two Application Processors with two SPI flash components each. The 64-pin package (2HW) supports only one QSPI port for one Application processor with up to two SPI flash components.

5.2 Pin List

The table below gives the pinout of the available CEC173x-TFLX packages.

FIGURE 5-1: CEC1736 PINOUT

CEC173x-S0-I/2ZW-TFLX	CEC1736-S0-I/2HW-TFLX	CEC173x Signal Name
A4	E2	GPIO000/SPI0_KILL/SPI0_RESET#
J2	F9	GPIO002/QSPI0_CS1#/SPIMON_QSPI0_CS1#
C6	J2	GPIO003/I2C00_SDA(FATAL_ERROR#)
C1	G2	GPIO004/I2C00_SCL
D6	J3	GPIO012(EXTRST#)
F2	K7	GPIO013/SP1_ALT_IO3(WDTRST2)
B3	F2	GPIO015/ICT10[BSTRAP]
K4	D10	GPIO016/QSPI0_IO3/QSPI0_IO3_CLAMP
K1	G9	GPIO020/QSPI0_IN_CS0#
J3	D9	GPIO021/QSPI0_IN_CS1#
J7	A7	GPIO022/QSPI0_IN_IO1
E9	A8	GPIO023/QSPI0_IN_IO0
F7		GPIO024/SPI1PER_CS#
A10	A4	GPIO026/SP0_AP_INTR[I2C_ADDR0]
D5	K2	GPIO027/TFDP_CLK_ALT(SPI0_BLEED#)
B6	D1	GPIO030/I2C10_SDA
A3	G1	GPIO031/SP1_ALT_IO0
K10		GPIO032/QSPI1_IN_IO1
B4		GPIO033(SPI1_BLEED#)
A5	F1	GPIO034/SP1_AP_INTR[I2C_ADDR1]
H9		GPIO045/QSPI1_IN_CS1#
A7	C2	GPIO046/SP1_ALT_CS#(WDTRST1)
C2	K3	GPIO047/SP1_ALT_IO1
B2	H2	GPIO050/ICT0(ASYNC_RST_DET#)
E1	J5	GPIO053/PWM0(EC_STS#)
K2	E9	GPIO055/QSPI0_CS0#/SPIMON_QSPI0_CS0#(QSPI0_PWRGD)
K7	B9	GPIO056/QSPI0_CLK/QSPI0_CLK_CLAMP
D4	J4	GPIO057/VCC_PWRGD
A1	H1	GPIO063/SP1_ALT_CLK(EXTRST_IN#)
D10		GPIO070/QSPI1_IN_IO0
J9		GPIO071/QSPI1_IN_CS0#

© 2024 Microchip Technology Inc. and its subsidiaries

FIGURE 5-1: CEC1736 PINOUT

CEC173x-S0-I/2ZW-TFLX	CEC1736-S0-I/2HW-TFLX	CEC173x Signal Name
E4	K5	GPIO104/UART0_TX/TFDP_CLK
E2	J6	GPIO105/UART0_RX/TFDP_DATA
E3	K6	GPIO106/AP0_RESET#(AP0_RESET#)
A6	E1	GPIO107/I2C10_SCL/ALT_VIOL_0
F4	K8	GPIO112/ALT_VIOL_1/TFDP_DATA_ALT
A2		GPIO113/ICT9(AP1_RESET_IN#)
H10		GPIO120/QSPI1_CS1#/SPIMON_QSPI1_CS1#
F9		GPIO121/QSPI1_IO0/QSPI1_IO0_CLAMP
K9		GPIO122/QSPI1_IO1/QSPI1_IO1_CLAMP
F10		GPIO123/QSPI1_IO2/QSPI1_IO2_CLAMP
J8		GPIO124/QSPI1_CS0#/SPIMON_QSPI1_CS0#(QSPI1_PWRGD)
J10		GPIO125/QSPI1_CLK/QSPI1_CLK_CLAMP
G10		GPIO126/QSPI1_IO3/QSPI1_IO3_CLAMP
F3	J7	GPIO127/SP1_ALT_IO2(WDTRST1)
B1	J1	GPIO130/32KHZ_IN
D2		GPIO131/AP1_RESET# (AP1_RESET#)
C9	D2	GPIO132/I2C06_SDA
B7	C1	GPIO140/I2C06_SCL
A9	A2	GPIO143/I2C04_SDA
B9	A3	GPIO144/I2C04_SCL(REMOTE_ACCESS)
B10	B4	GPIO145/I2C09_SDA/JTAG_TDI
C10	B2	GPIO146/I2C09_SCL/ITM/JTAG_TDO(SWV)
B8	B1	GPIO147/I2C15_SDA/JTAG_CLK (SWDCLK)
A8	B3	GPIO150/I2C15_SCL/JTAG_TMS (SWDIO)
H2	J10	GPIO156/LED0
H1	G10	GPIO157/LED1
B5		GPIO163/SPI1_KILL/SPI1_RESET#
E10		GPIO165/QSPI1_IN_IO2
G5	J8	GPIO170[JTAG_STRAP]
G9		GPIO171/QSPI1_IN_IO3
K8		GPIO200/QSPI1_IN_CLK
G2	J9	GPIO201/32KHZ_OUT[CR_FLASH]
K5	C9	GPIO202/QSPI0_IN_IO2
K3	E10	GPIO203/QSPI0_IN_IO3
K6	B10	GPIO204/QSPI0_IN_CLK
F8	A6	GPIO223/QSPI0_IO0/QSPI0_IO0_CLAMP
J6	A9	GPIO224/QSPI0_IO1/QSPI0_IO1_CLAMP
J4	B7	GPIO227/QSPI0_IO2/QSPI0_IO2_CLAMP
J5	C10	GPIO250/SPI0PER_CS#
E8	B6	GPIO253/TST_CLK_OUT

© 2024 Microchip Technology Inc. and its subsidiaries

FIGURE 5-1: CEC1736 PINOUT

CEC173x-S0-I/2ZW-TFLX	CEC1736-S0-I/2HW-TFLX	CEC173x Signal Name
G1	H9	JTAG_RST#
G4	H10	nRESET_IN
G6	G4	VSS_ANALOG
F1	K9	VTR_PLL
D9	D7	VSS
D7	G7	VTR_REG
H5	B8	VTR1
C5	D4	VTR_ANALOG
D1	K4	VR_CAP
E7	A5	VSS
H6		VTR2
J1	F10	VSS
G7	B5	VSS

© 2024 Microchip Technology Inc. and its subsidiaries

5.3 Package Information

5.3.1 64 PIN VFBGA PACKAGE

FIGURE 5-2: 2HW Package Dimensions, Sheet 1

64-Ball Very Thin Fine-Pitch Ball Grid Array (2HW) - 5.5x5.5x0.92 mm Body [VFBGA]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging

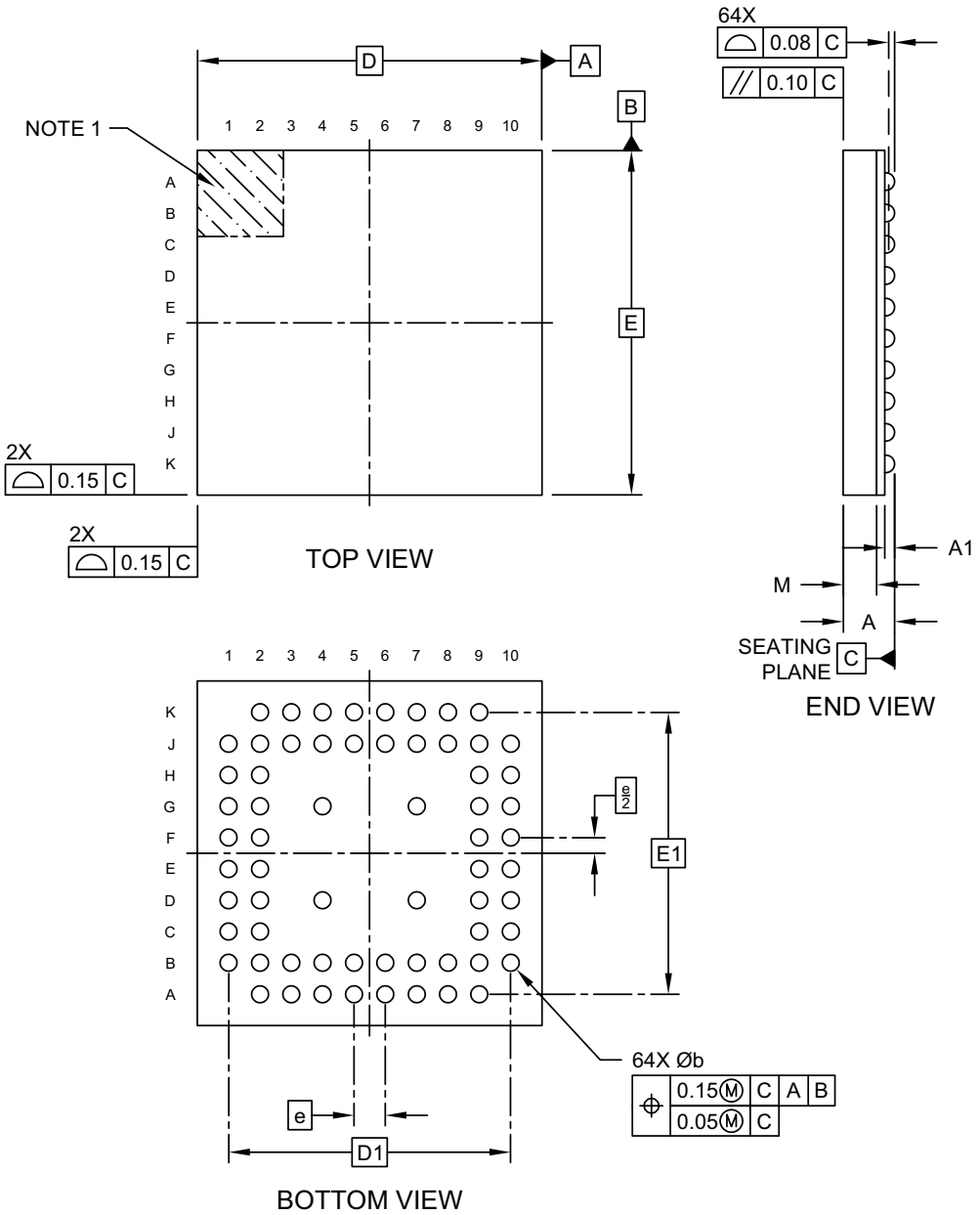
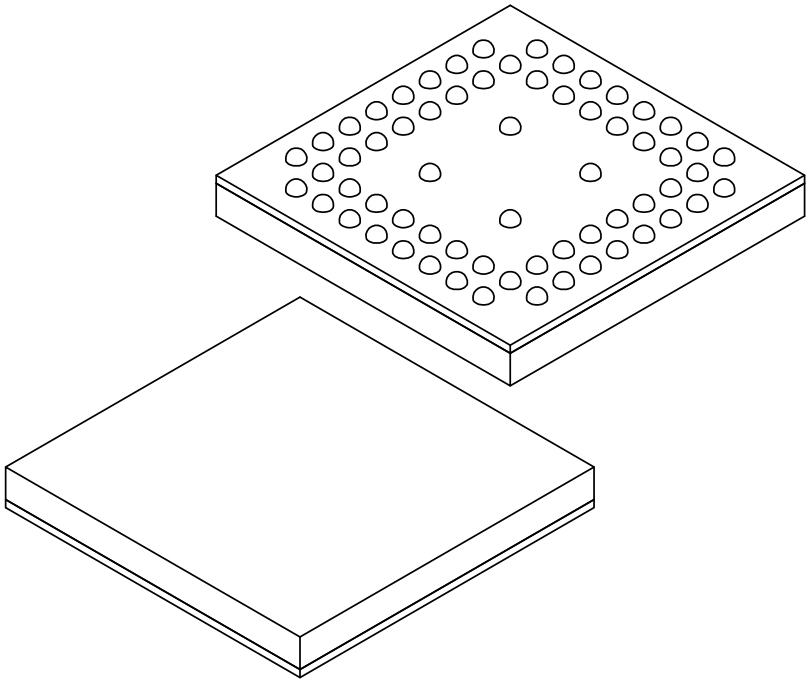


FIGURE 5-3: 2HW Package Dimensions, Sheet 2

64-Ball Very Thin Fine-Pitch Ball Grid Array (2HW) - 5.5x5.5x0.92 mm Body [VFBGA]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Terminals	N	64		
Pitch	e	0.50 BSC		
Overall Height	A	–	–	0.92
Ball Height	A1	0.12	0.16	–
Mold Thickness	M	0.48	0.53	0.58
Overall Length	D	5.50 BSC		
Ball Array Length	D1	4.50 BSC		
Overall Width	E	5.50 BSC		
Ball Array Width	E1	4.50 BSC		
Ball Diameter	b	0.23	0.28	0.33

Notes:

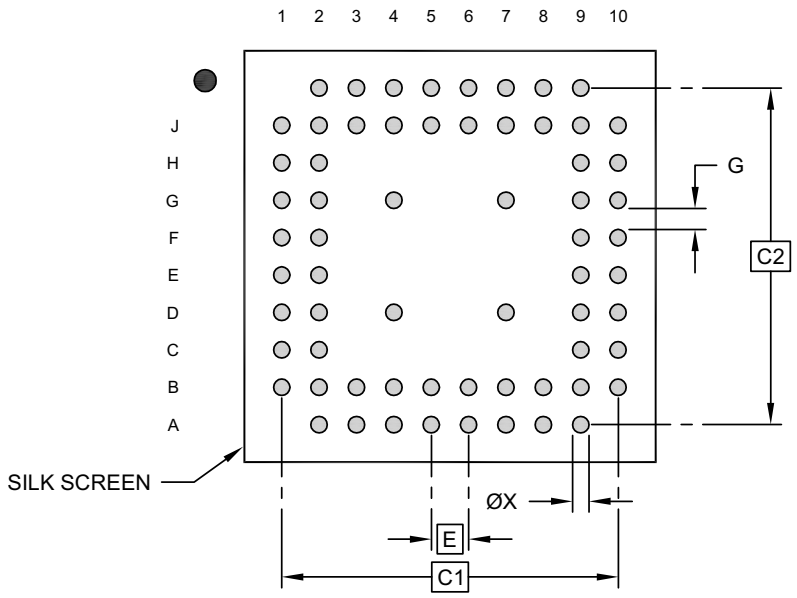
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
   REF: Reference Dimension, usually without tolerance, for information purposes only.

© 2024 Microchip Technology Inc. and its subsidiaries

FIGURE 5-4: 2HW Package Dimensions, Sheet 3

64-Ball Very Thin Fine-Pitch Ball Grid Array (2HW) - 5.5x5.5x0.92 mm Body [VFBGA]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E	0.50 BSC		
Contact Pad Spacing	C1	4.50 BSC		
Contact Pad Spacing	C2	4.50 BSC		
Contact Pad Diameter (X64)	X1			X.XX
Contact Pad to Contact Pad (Xnn)	G	0.28		

Notes:

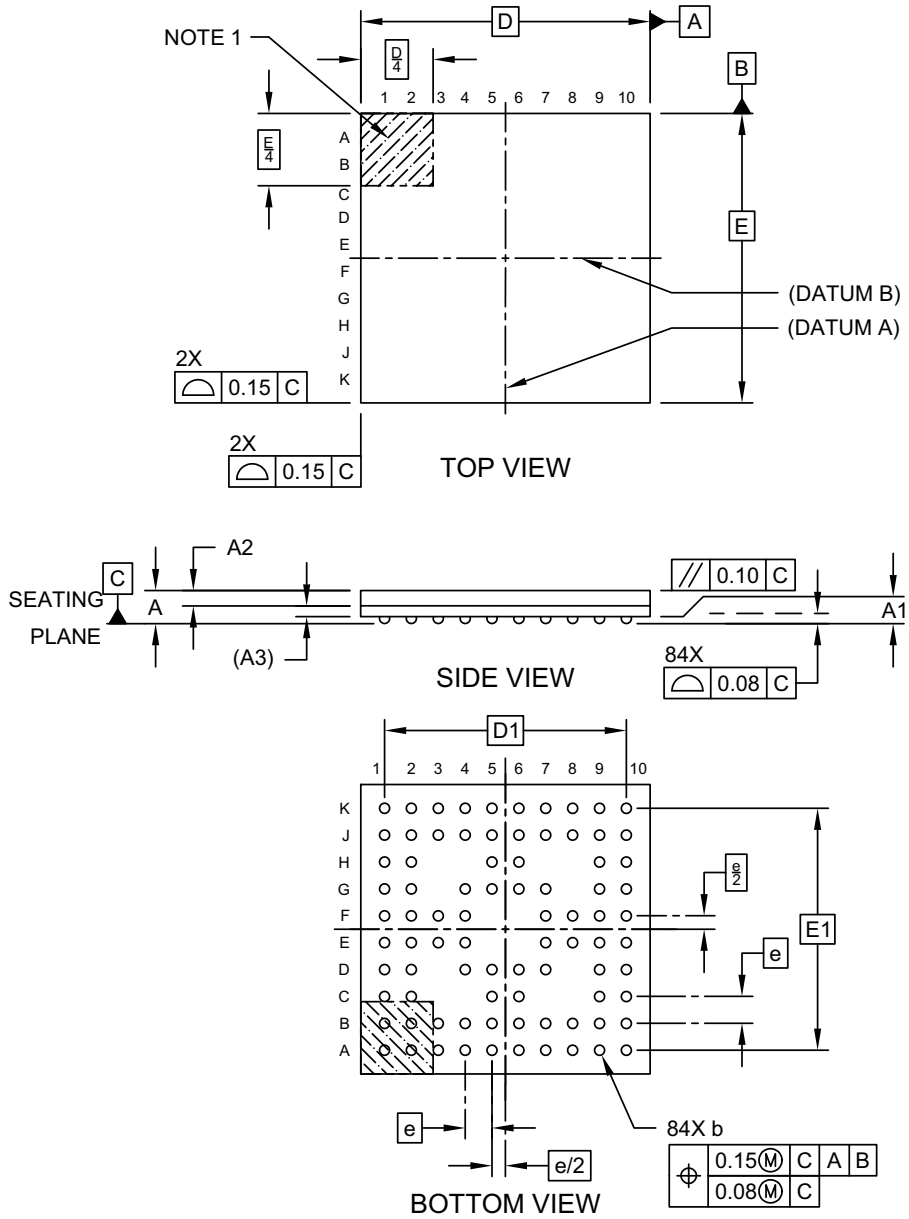
1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

5.3.2 84 PIN WFBGA PACKAGE

FIGURE 5-5: 2ZW Package Dimensions, Sheet 1

84-Ball Very, Very Thin fine Pitch Ball Grid Array (2ZW) - 7x7x0.8 mm Body [WFBGA]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing C04-390-2ZW Rev C Sheet 1 of 2

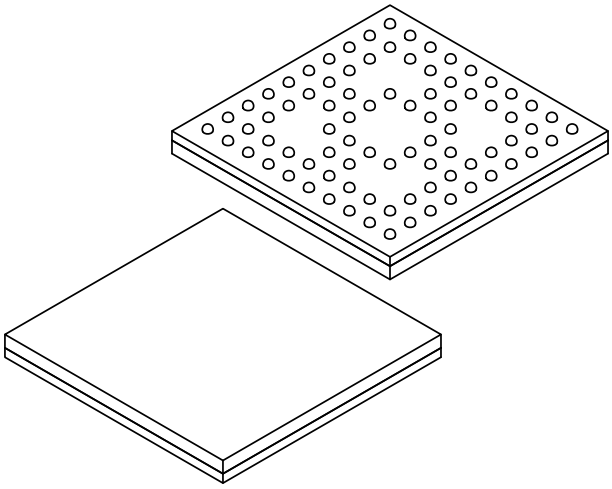
© 2021 Microchip Technology Inc.

© 2024 Microchip Technology Inc. and its subsidiaries

FIGURE 5-6: 2ZW Package Dimensions, Sheet 2

84-Ball Very, Very Thin fine Pitch Ball Grid Array (2ZW) - 7x7x0.8 mm Body [WFBGA]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Terminals	N	84		
Pitch	e	0.65 BSC		
Overall Height	A	-	-	0.80
Standoff	A1	0.12	0.17	-
Mold Cap Thickness	A2	0.35	0.40	0.45
Substrate Thickness	A3	0.13 REF		
Overall Length	D	7.00 BSC		
Overall Termnal Spacing	D1	5.85 BSC		
Overall Width	E	7.00 BSC		
Overall Termnal Spacing	E1	5.85 BSC		
Ball Diameter	b	0.20	0.25	0.30

Notes:

1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
   REF: Reference Dimension, usually without tolerance, for information purposes only.

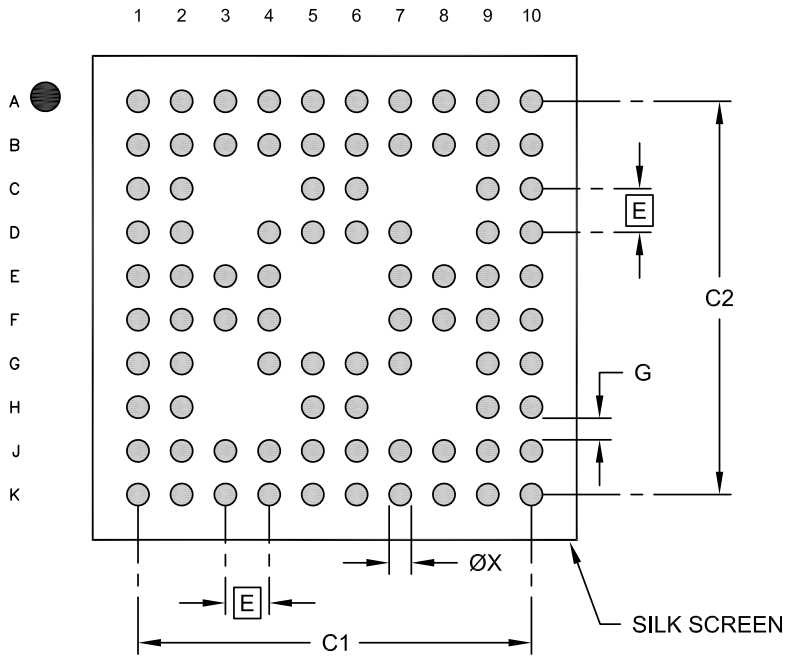
Microchip Technology Drawing C04-390-2ZW Rev C Sheet 2 of 2

© 2021 Microchip Technology Inc.

FIGURE 5-7: 2ZW Package Dimensions, Sheet 3

84-Ball Very, Very Thin Fine Pitch Ball Grid Array (2ZW) - 7x7x0.8 mm Body [WFBGA]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E		0.65 BSC	
Overall Contact Pad Spacing	C1		5.85	
Overall Contact Pad Spacing	C2		5.85	
Contact Pad Width (X84)	X1			0.33
Contact Pad to Contact Pad	G	0.25		

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-2390-2WX Rev C

© 2021 Microchip Technology Inc.

© 2024 Microchip Technology Inc. and its subsidiaries

6.0 DETAILED SOTERIA-G3 DESCRIPTION

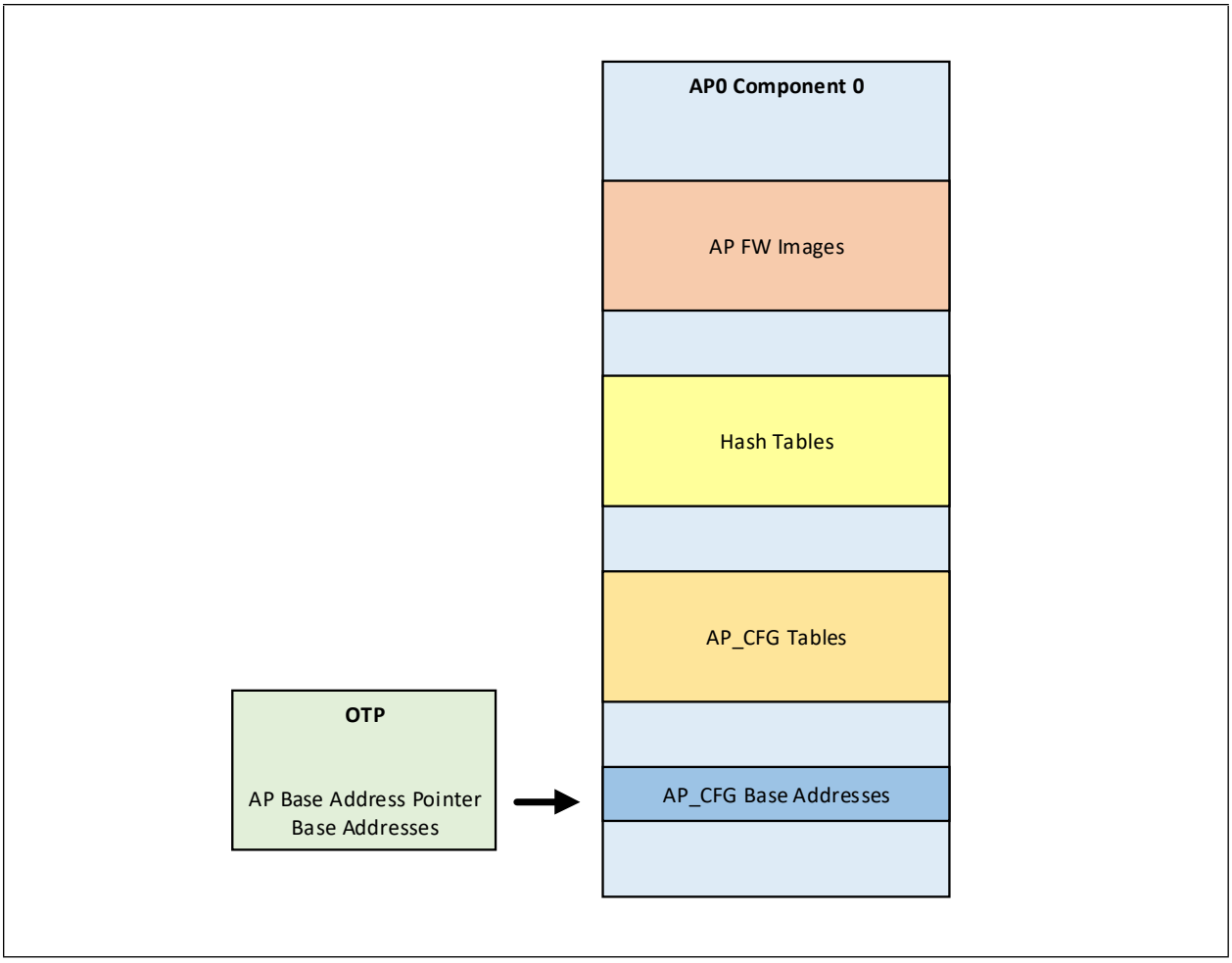
6.1 Secure Boot

The CEC173x-TFLX implements a Secure Boot sequence starting from the Immutable Secure Bootloader, the Boot ROM, to establish the Root of Trust. The Boot ROM authenticates and loads the Soteria-G3 Firmware stored in the internal flash memory. Soteria-G3 extends the Root of Trust by enforcing a secure boot process on the AP(s) by controlling the AP reset signal(s) with release conditioned on the authentication of the AP Firmware stored in the external flash components.

6.1.1 REQUIRED SECURE BOOT COMPONENTS

Soteria-G3 requires several blocks of application-specific data in the external flash components, shown in Figure 6-1 below.

FIGURE 6-1: EXTERNAL FLASH COMPONENTS



6.1.2 SECURE BOOT FLOW

FIGURE 4-1: Boot Process on page 9 shows the flow of the Secure Boot process used by Soteria-G3. At start-up, the CEC173x-TFLX will hold the AP(s) in reset while performing authentication of the images and will isolate the AP(s) from the external flash components. Soteria-G3 will read the AP_CFG Table from the external flash, authenticate the table's signature, and parse the table for the software configuration information. Next, any hash tables will be read from the external flash, their signatures will be validated, and Soteria-G3 will capture the information and hash of each image from the respective table.

Soteria-G3 then authenticates the AP firmware images stored in the external flash.To perform this authentication, each image is read from start to end address, while the internal SPI Monitor peripheral calculates the hash of the image in real time. Once the image read is complete, the calculated hash value is compared against the hash stored in the authenticated hash table. If these hash values match, then the image is deemed authentic. In this phase, only images which are marked as needing authentication will be checked, and all images marked as critical must be authenticated. Release of the AP reset signal will only occur if all critical images pass the authentication sequence.

6.1.3 RUN TIME AUTHENTICATION

After releasing the reset signals, the AP will be allowed to access the SPI flash components and boot. While the AP reads images from the SPI flash, the CEC173x-TFLX will then reauthenticate the image during the AP read, with the result of this authentication available from the AP I^2C port.

6.1.4 IMAGE CONFIGURATION PARAMETERS

Each image can be configured to tell Soteria-G3 how to treat it during the boot process. The image base address must be provided to show Soteria-G3 where the image is in the external SPI flash components.Additionally, an image may be marked as a Primary, Fallback, or Golden image. A Primary image is the go-to image the AP will look for when it is allowed to boot. The Fallback image is a backup image that the AP will know the address of and look for in case there is an issue with the Primary image. The Golden image is a backup of the Primary image that Soteria-G3 can copy to the Primary image location in case of authentication failure. Fallback and Golden images are both linked to a Primary image and are not a requirement for Secure Boot.

Any image that must pass authentication before the AP reset is released should be marked as a Critical image. Fallback images of Critical Primary images are also Critical by default and should not be marked as Critical. If an image should be authenticated before the AP boots but does not need to block the AP reset signal, it can be marked as Authentication Required. The status of these images can be acquired via the AP I^2C port.

Lastly, an image may be configured as either a uBoot or a Run-Time image. During AP read of the image for reauthentication, uBoot images will be compared byte-by-byte with a local copy stored in the CEC173x-TFLX to ensure image integrity. This is to support images which are executed in place and may not be read in order by the AP. Run-Time images are reauthenticated in the same manner as described in Section 6.1.2, Secure Boot Flow. Both images are authenticated the same way before the AP reset signal is released.

6.2 SPI Monitor

The SPI Monitor is used to ensure the integrity and validity of SPI traffic to one or two Flash devices from a Host device. The SPI Monitor operates in a passive mode, where it simply observes the SPI traffic, and an active mode, where it can intervene in the S PI traffic. The peripheral performs an Intervention if a Violation is detected, such as when a specific command is sent over the SPI bus. A Violation is a detection of illegal activity on the SPI bus as defined by the rules programmed. An Intervention is the interruption of SPI traffic by hardware, taking control of signals going to the Flash devices. There are two kinds of Interventions:

- Full Intervention: will have the immediate HW effects like forcing Chip Selects, isolating external Host SPI Bus, Resetting Flash device and Resetting external Host etc.
- Reduced Intervention: available only for SPI Read accesses. It will have the effect of removing Chip Select early. It only allows the Violation interrupt to firmware and updating the AP I^2C registers.

The flash opcodes that may trigger a violation and the intervention response to violations are configurable for the CEC173x-TFLX and can have different configurations for before and after the AP is allowed to boot. Additionally, the SPI monitor is used to calculate the hash value of any data read through the SPI port on the fly.

6.2.1 PRE-BOOT AND POST-BOOT MODE

The SPI Monitor can be configured with two different sets of violation settings for pre-boot mode and post-boot mode. Pre-boot mode is the default state of the SPI Monitor after power on. The AP may switch to post-boot settings at any time after it is released from reset using an I^2C command on the AP I^2C port.

6.2.2 MEMORY PROTECTION REGIONS

Specific memory regions of the device can be configured to have general protection over them during device operation. These regions can be used to protect all, or parts of the AP images and data stored in the external flash. These memory regions can block all reads, writes, or erase operations. The user must provide the base address and size of each region. There must be at least one Memory Protection Region for Soteria-G3 to allow the AP to boot, and a maximum of 16 regions are supported. These regions support pre-boot and post-boot configurations.

© 2024 Microchip Technology Inc. and its subsidiaries

6.2.3 MONITOR VIOLATION SETTINGS

The SPI Monitor Violation Settings allow for the complete customization of what permissions any device accessing the external SPI flash will have. The violation settings can be used to prohibit specific flash opcodes from being sent to the SPI flash device. Additionally, the forbidden opcodes can also be configured to trigger a SPI Monitor violation if required. These violation settings support pre-boot and post-boot configurations.

6.2.4 USER CONFIGURABLE OPTIONS

The CEC173x-TFLX SPI Monitor can be configured to run in Quad or Half Bus mode. Note that selecting Half Bus mode will not allow for any Quad Mode operations. The method of intervention may also be selected; the SPI Monitor can use the HW Kill signal to cut power from the SPI flash device (if the design hardware supports this) or reset the device, issue an AP reset, or simply block the command and allow operation to continue. Specific memory regions that are marked for hash-match may also incur a violation if there is a hash mismatch after the AP performs a read.

The SPI Monitor has timing settings to enhance the security and robustness of the system. The user can set the maximum amount of time between the release of the AP reset signal and the first data fetch from the SPI flash. If this is not met, an AP reset can be issued to reset the device. There may also be no time limit. Additionally, there is a configurable timer for the maximum allowed time between complete fetch of the main AP image and the release of the AP reset signal. There may also be no time limit. The QSPI peripheral Delay Taps may also be modified as per the needs of the customer’s hardware.

6.3 Secure Update

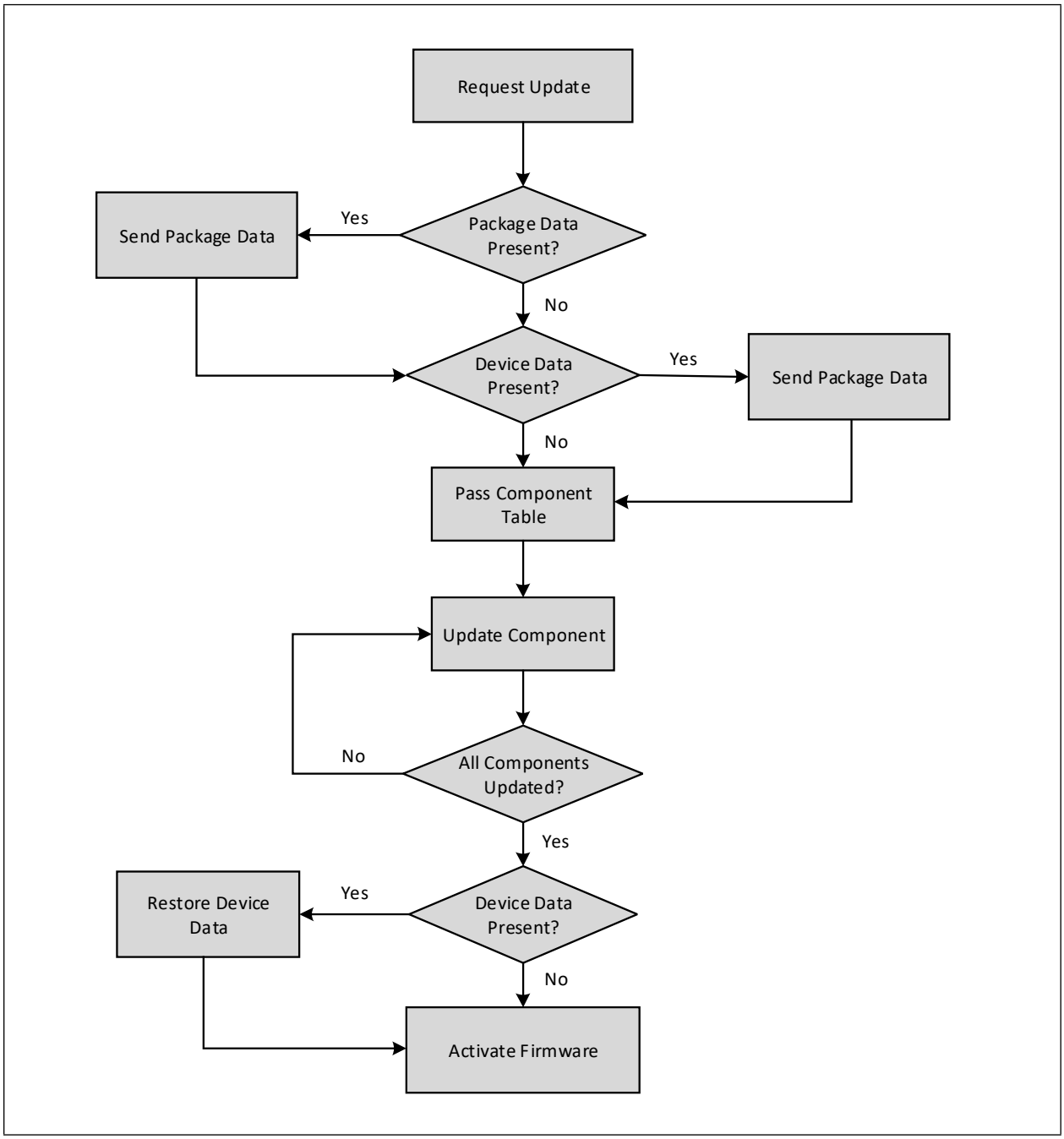
Soteria-G3 supports secure firmware updates for new Soteria-G3 firmware, AP firmware images, AP CFG Tables and Hash Tables. The CEC173x acting as the Firmware Device (FD) uses Platform Level Data Model (PLDM) specification as the base for exchanging the update details with Update Agent (UA).

The firmware update package provides the necessary information to be used with the PLDM Firmware Update commands. To assist in performing an update over PLDM, the firmware update package shall contain a vendor header describing the contents of the firmware update package. Prior to transferring the component images, the header can be parsed by the UA to identify if the firmware update package is applicable for updating a specific FD by comparing Device Identifier records in the package header to those obtained from the FD via the QueryDeviceIdentifiers command. The TPDS CEC173x Configurator will generate this package and header for you after filling in the required fields.

A firmware update package may contain one or more component images applicable to a single FD. The UA must advertise each component image individually and attempt to transfer each of the component images to the FD. The firmware update package header provides the information to be able to identify a component by comparing its identifier value, along with additional information such as the component classification.

Figure 6-2 below describes the high-level process of how the UA updates a FD. This flow occurs after the UA has determined which FD(s) the firmware update package is intended for.

FIGURE 6-2: PLDM UPDATE FLOW



Note: CEC173x-TFLX supports only mandatory PLDM commands.

6.3.1 SUPPORTED PLDM COMMANDS

The tables below show the PLDM commands supported by Soteria-G3.

© 2024 Microchip Technology Inc. and its subsidiaries

TABLE 6-1: PLDM MESSAGING AND CONTROL COMMAND LIST

PLDM Command	Code Values	FD Implementation Requirement	Command Requestor	Supported in CEC173x
GetTID	0x02	Mandatory	UA	Yes
GetPLDMVersion	0x03	Mandatory	UA	Yes
GetPLDMTypes	0x04	Mandatory	UA	Yes
GetPLDMCommands	0x05	Mandatory	UA	Yes

TABLE 6-2: PLDM FOR FIRMWARE UPDATE COMMAND LIST

PLDM Command	Code Values	FD Implementation Requirement	Command Requestor	Supported in CEC173x
Inventory Commands				
QueryDeviceIdentifiers	0x01	Mandatory	UA	Yes
GetFirmwareParameters	0x02	Mandatory	UA	Yes
Update Commands				
RequestUpdate	0x10	Mandatory	UA	Yes
SendPackageData	0x11	Optional	UA	No
RetrieveDeviceData	0x12	Optional	UA	No
PassComponentTable	0x13	Mandatory	UA	Yes
UpdateComponent	0x14	Mandatory	UA	Yes
RequestFirmwareData	0x15	Mandatory	FD	Yes
TransferComplete	0x16	Mandatory	FD	Yes
VerifyComplete	0x17	Mandatory	FD	Yes
ApplyComplete	0x18	Mandatory	FD	Yes
RestoreDeviceData	0x19	Optional	UA	No
ActivateFirmware	0x1A	Mandatory	UA	Yes
GetStatus	0x1B	Mandatory	UA	Yes
CancelUpdateComponent	0x1C	Mandatory	UA	Yes
CancelUpdate	0x1D	Mandatory	UA	Yes

6.3.2 USER CONFIGURABLE OPTIONS

The CEC173x-TFLX allows for configuration of the supported device capabilities during the upgrade process:

- Whether or not to revert to the previous image if an update fails.
- If a component update fails, exit update mode, or continue updating components.
- Reduction of host functionality during updates.
- Support for partial updates.
- Restriction of host environment for updates.
- Enabling downgrade restrictions.

Additionally, up to 30 PLDM device descriptors are supported by the CEC173x-TFLX, making it flexible for use across a wide variety of applications.

© 2024 Microchip Technology Inc. and its subsidiaries

The Stage and Restore Addresses, located in the external SPI flash components, are also configurable by the user to ensure their AP firmware images are not overwritten during the update process. The Staged Address is where the new image will be written before application. The Restore Address is where the old image will be copied to, in case the write of the new image fails and needs to be reverted.

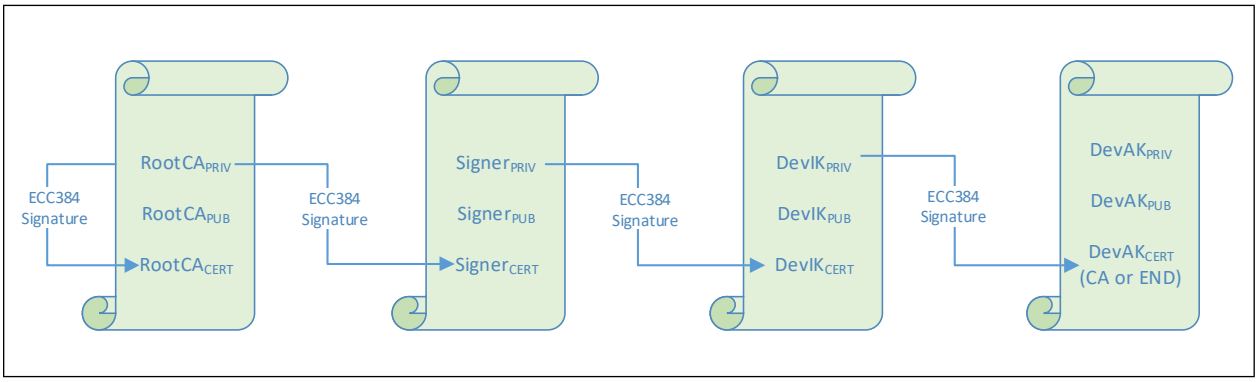
6.4 Attestation

The CEC173x-TFLX can perform platform attestation compliant with the SPDM standard over MCTP using an I^2C bus as the physical interface, and acts as the Responder to a Requester device. The device contains the seeds, keys and certificates required to maintain compatibility with the SPDM specification from DMTF.

6.4.1 DEVICE CERTIFICATES

The CEC173x-TFLX can store a customer certificate chain inside the internal flash memory of the device, with up to eight certificates in the chain. There are two certificates generated by the CEC173x-TFLX that must always be present in the chain for attestation, the Device Attestation (DevAK) certificate and the Device Identity (DevIK) certificate. The DevAK certificate is the leaf certificate in the customer chain, and its associated private key is used by Soteria-G3 to sign any attestation requests. The DevIK private key, generated from the device PUF, is used to sign the DevAK certificate. The DevIK certificate will be read from the CEC173x-TFLX and signed by Microchip during the device provisioning process. Certificates higher than these in the chain are configurable to the customer's needs. An example certificate chain for this device is shown in Figure 6-3 below

FIGURE 6-3: CERTIFICATE CHAIN



Note: CEC173x-TFLX supports only mandatory PLDM commands

6.4.2 SUPPORTED SPDM COMMANDS

The following table shows the SPDM commands supported in the CEC173x-TFLX for device Attestation.

TABLE 6-3: PLDM MESSAGING AND CONTROL COMMAND LIST

SPDM Request / Response	Code Values (Request / Response)	Implementation Requirement	Supported in CEC173x
Get_DIGESTS / DIGESTS	0x81 / 0x01	Optional	Yes
GET_CERTIFICATES / CERTIFICATE	0x82 / 0x02	Optional	Yes
CHALLENGE / CHALLENGE_AUTH	0x83 / 0x03	Optional	Yes
GET_VERSION / VERSION	0x84 / 0x04	Optional	Yes
GET_MEASUREMENTS / MEASUREMENTS	0xE0 / 0x60	Optional	Yes
GET_CAPABILITIES / CAPABILITIES	0xE1 / 0x61	Required	Yes
NEGOTIATE_ALGORITHMS / ALGORITHMS	0xE3 / 0x63	Required	Yes
RESPOND_IF_READY	0xFF / -	Required	Yes

© 2024 Microchip Technology Inc. and its subsidiaries

Please see the SPDM specification from DMTF for more information about SPDM.

6.4.3 USER CONFIGURABLE OPTIONS

The I^2C port used by Soteria-G3 can be configured to be on Ports 4, 6, 9, 10, or 15 of the CEC173x-TFLX (OTP option), allowing for flexibility of options depending on the customer's design. The address of the attestation port is also user configurable.

6.5 Transfer of Ownership

The CEC173x-TFLX supports transferring ownership of a device in the case that a system using a CEC173x-TFLX as the Platform Root of Trust needs to be given to a new party with their own configuration and keys. CEC173x-TFLX devices configured to support Transfer of Ownership will be equipped with a Replay Protected Monotonic Counter (RPMC) container, which contains any information specific to one customer. This container can be securely changed or updated over I^2C.

6.5.1 OWNERSHIP TRANSFER METHODS

The CEC173x-TFLX supports two methods of ownership transfer. In the first case, the new owner of the device can provide their ownership details to the original owner, who will then securely update the CEC173x-TFLX with the new owner's information before giving the system to the new owner.

Alternatively, the original owner may enable the device for ownership transfer, authorizing only the new owner to take ownership through a public key provided by the new owner. The original owner may then give the system to the new owner, who will take ownership of the CEC173x-TFLX securely by updating the device with their own information.

6.6 Crisis Recovery

The CEC173x-TFLX supports two modes of Crisis Recovery to restore a system to working condition after the failure or corruption of an image occurs. The Boot ROM of the CEC173x-TFLX features a crisis mode to recover failing Soteria-G3 images. Additionally, the CEC173x-TFLX supports crisis recovery of the images stored in the external SPI flashes. Both forms of recovery can be enabled and configured through the CEC173x-TFLX Configurator.

6.6.1 SOTERIA-G3 IMAGE RECOVERY

The EC FW Crisis Recovery can be triggered in two ways: using the BSTRAP pin of the device or after a Load Failure of the EC FW. Upon entering the recovery state, the Boot ROM will wait for I^2C commands. At this point, code may be sent to the CEC173x to be loaded into the SRAM to perform the recovery. This code must be signed by one of the EC FW authentication keys, as upon exiting from Crisis Mode, the Boot ROM will perform authentication of this image. Microchip provides a signed PLDM application to easily update the internal flash with a new Soteria-G3 application image.

6.6.2 AP IMAGE RECOVERY

The AP Image Crisis Recovery is a feature of Soteria-G3 and enables the restoration of images in the external SPI flashes. When enabled, this recovery sequence is triggered when there are no images in the flash, or all the images are corrupted. The EC FW will drive the FATAL_ERROR# pin low as an indicator of this failure. Once the crisis mode is entered, the EC FW supports using PLDM over I^2C to securely update only one each of the following entities in the external flash:

- AP Base Address Pointer
- KHB
- AP_CFG Table
- Hash Table
- AP FW Image

Updating these components will allow the system to boot, and from here the Application Owner can use PLDM to securely update the remaining failing entities in the external flash, and the entities overwritten during the Crisis Recovery process.

6.6.3 USER CONFIGURABLE PARAMETERS

To support Crisis Recovery on the CEC173x-TFLX device, few configurations are required. The method of entering the Soteria-G3 firmware recovery sequence can be configured to occur on both load failure and via the BSTRAP pin, only one of the options, or it can be disabled completely. This is an OTP option, and once written to the device cannot be changed. Requires no additional changes to Soteria-G3, and just must be enabled when configuring the device.

6.7 Key Revocation

The CEC173x-TFLX allows for the revocation of any AP signing keys in case any of the customer's private keys are compromised and must be removed from service. Soteria-G3 supports two methods of key revocation: manual and automatic. These two methods are mutually exclusive and cannot both be enabled. In both cases, the key currently in use to authenticate the AP_CFG and Hash Tables may not be revoked. Additionally, all AP resets must be asserted to revoke a key.

6.7.1 USER CONFIGURABLE OPTIONS

To use AP key revocation, it must be enabled in the CEC173x-TFLX and is an OTP setting. Manual or automatic revocation selection is also an OTP setting, with the default as manual revocation. Therefore, switching to automatic revocation is irreversible.

Both manual and automatic key revocation require setting the appropriate permission bits in the AP_CFG Table, that specify which keys are allowed to be revoked. This is simply a 32-bit field, where each bit corresponds to one of the 32 supported AP keys. Both the OTP and permissions settings can be easily managed using the TPDS CEC173x-TFLX Configurator.

6.7.2 MANUAL KEY REVOCATION

Manual key revocation requires the host to perform an I^2C command to the AP I^2C port. Keys may only be revoked if their corresponding permission bit is set in the AP_CFG and Hash Table, which are signed and authenticated, ensuring that only allowed keys can be revoked over I^2C. See Section 6 for specific details about the required I^2C commands. Key revocation permissions can be updated at any time by performing a PLDM update of the AP_CFG Table.

6.7.3 AUTOMATIC KEY REVOCATION

Automatic key revocation requires only that the desired key permission bits in the AP_CFG and Hash Tables are set. Upon boot, Soteria-G3 will validate the tables and, if auto-revocation is enabled in OTP, revoke the keys specified in the permission bits. This method requires an update of the AP_CFG Table, which can be done over PLDM.

6.8 Rollback Protection

The CEC173x-TFLX provides protection against the use of previous and potentially vulnerable previous versions of firmware for the AP. When enabled, Soteria-G3 will check the version information of the AP_CFG and Hash Tables and prevent their use if their versions are revoked, even if they're signed with valid AP keys. AP_CFG and Hash Tables each have independent Rollback Protection settings. There are two methods of Rollback Protection for the CEC173x-TFLX: manual and automatic protection.

6.8.1 USER CONFIGURABLE OPTIONS

To use the Rollback Protection feature it must be enabled in the CEC173x-TFLX and is an OTP setting. Manual or automatic protection selection is also an OTP setting, with the default as manual revocation. Therefore, switching to automatic protection is irreversible.

Both manual and automatic Rollback Protection require setting the appropriate permission bits in the AP_CFG or Hash Table, which specify firmware revisions are to be revoked. Each bit in the permission field corresponds to a revision number for the table. For example, bit 0 is table revision 0 and bit 16 is table revision 16. Both the OTP and permissions settings can be easily managed using the TPDS CEC173x-TFLX Configurator.

6.8.2 MANUAL ROLLBACK PROTECTION

Manual Rollback Protection requires the host to perform an I^2C command to the AP I^2C port. Revision versions may only be revoked if their corresponding permission bit is set in the AP_CFG and/or Hash Table, which are signed and authenticated, ensuring that only allowed version permissions can be revoked over I^2C. See Section 6 for specific details about the required I^2C commands. Rollback Protection permissions can be updated at any time by performing a PLDM update of the AP_CFG and/or Hash Table.

© 2024 Microchip Technology Inc. and its subsidiaries

6.8.3 AUTOMATIC ROLLBACK PROTECTION

Automatic Rollback Protection requires only that the desired revision permission bits in the AP_CFG and Hash Tables are set. Upon boot, Soteria-G3 will validate the tables and, if auto-revocation is enabled in OTP, revoke the specified versions provided in the permission bits. This method requires an update of the AP_CFG and/or Hash Tables, which can be done over PLDM.

© 2024 Microchip Technology Inc. and its subsidiaries

NOTES:

© 2024 Microchip Technology Inc. and its subsidiaries

7.0 I²C COMMANDS

The Soteria-G3 Firmware provides an I²C interface for the external host to gather system information once the Secure Boot process completes successfully. This interface provides information regarding the authentication status and other device details the host may need during run-time. This I²C interface runs at 400kHz on I²C Port 6 (for AP0) and I²C Port 10 (for AP1) of the CEC173x-TFLX and is SMBus 2.0 compliant.

TABLE 7-1: GENERAL DEVICE COMMANDS

Command	Offset	# Bytes	Description
Soteria-G3 Boot Status	03h	1	Provides status of Soteria-G3 image authentication.
Firmware Build Number (MSB)	34h	1	MSB of Soteria-G3 Firmware Build Number.
Firmware Build Number (LSB)	35h	1	LSB of Soteria-G3 Firmware Build Number.
Get SN Command Initiate	36h	1	Starts hash calculation of serial number for read. Bit 0 of the command data byte should be 1.
Get SN Command Status	37h	1	Provides status of serial number hash calculation (Bit 0 = 1 indicates completion).
Get SN Data	38h	1	Once hash calculation is complete, returns the result of the calculation. First return is byte 0, repeated reads provide the next bytes up to byte 47.
EC Reset Initiate	39h	1	Resets the CEC173x-TFLX.

TABLE 7-2: SECURE BOOT COMMANDS

Command	Offset	# Bytes	Description
Flash Component Boot Validation Status	01h	1	Provides status of external flash component authentication. Upper byte indicates if images are present in a component (Present = 1), lower byte indicates the pass status (Pass = 1).
Flash Image Validation Status AP0	68h	4	The lower two bytes provide authentication status of the images in AP0 C0 (Pass = 1). The upper two bytes provide authentication status of the images in AP0 C1 (Pass = 1). Images not authenticated before AP reset release will be marked as failed.
Flash Image Validation Status AP1	6Ch	4	The lower two bytes provide authentication status of the images in AP1 C0 (Pass = 1). The upper two bytes provide authentication status of the images in AP1 C1 (Pass = 1). Images not authenticated before AP reset release will be marked as failed.

TABLE 7-3: SPI MONITOR COMMANDS

Command	Offset	# Bytes	Description
Violation Log Status AP0	4Ch	2	Provides a copy of the SPI Monitor Violation log for AP0 QSPI port.
Violation Log Status AP1	4Eh	2	Provides a copy of the SPI Monitor Violation log for AP1 QSPI port.
Violation Address AP0	50h	4	Provides the address of a violation on AP0 QSPI port.
Violation Address AP0	54h	4	Provides the address of a violation on AP1 QSPI port.

© 2024 Microchip Technology Inc. and its subsidiaries

TABLE 7-3: SPI MONITOR COMMANDS

Command	Offset	# Bytes	Description
Flash Permission Update Initiate	9Eh	2	Updates the opcode and runtime region permissions. Lower byte updates to post-boot settings, upper byte sets pre-boot settings. Writing a 1 to a bit enables the update.

TABLE 7-4: KEY REVOCATION COMMANDS

Command	Offset	# Bytes	Description
Key Revocation Command Initiate	3Ah	1	Starts key revocation process in Soteria-G3. Bits 5:1 provide the key index, Bit 0 = 1 enables execution.
Key Revocation Command Status	3Bh	1	Provides the status of the revocation command. Bit 0 = 1 means command is finished executing and must be cleared by writing a 1. If revocation was successful, Bit 1 will return as 1 after command completion.
Get Key Revocation Status	3Ch	4	Provides revocation status of all AP public keys.

TABLE 7-5: ROLLBACK PROTECTION COMMANDS

Command	Offset	# Bytes	Description
Rollback Protection Command Initiate	40h	1	Starts rollback protection process in Soteria-G3. Bits 7:1 provide the Revision ID, Bit 0 = 1 enables execution.
Rollback Protection Command Status	41h	1	Provides the status of the rollback protection command. Bit 0 = 1 means command is finished executing and must be cleared by writing a 1. If revocation was successful, Bit 1 will return as 1 after command completion.
Rollback Protection Image Select	42h	1	Selects type of table to set protections, APCFG (Bit 4 = 0) or Hash Table (Bit 4 = 1). Bit 0 selects the AP port and Bit 1 selects the flash component.
Get Rollback Protection Status	44h	4	Provides revocation status of all AP public keys.

© 2024 Microchip Technology Inc. and its subsidiaries

8.0 DEVELOPMENT TOOLS

8.1 Software Tools

The CEC173x-TFLX goes hand in hand with the Microchip Trust Platform Design Suite (TPDS), which is available for download on Windows, Linux, and Mac from the Microchip website. The CEC173x-TFLX Configurator on TPDS provides a streamlined graphical interface for enabling and configuring the CEC173x-TFLX device. The configurator provides the ability to generate packages for both prototyping and production flows and allows you to program your CEC173x-TFLX-PROTO parts for testing (requires Microchip MPLAB X installation).

8.2 Hardware Tools

The CEC173x-TFLX can be programmed using the Microchip MPLAB ICD5 or PICkit5 devices. Legacy PICkit4 and ICD4 tools are also supported for the CEC173x-TFLX.

9.0 ELECTRICAL CHARACTERISTICS

Please go to the MyMicrochip website to get the CEC173x-TFLX Electrical Characteristics Addendum, available for download from the Secure Document Exchange (SDE) page.

© 2024 Microchip Technology Inc. and its subsidiaries

APPENDIX A: DATA SHEET REVISION HISTORY

Revision	Section/Figure/Entry	Description
DS00005397A (04-05-24)	Initial Release	

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)	-	XX	-	X/XXX(2)	-	[X]	-	[X](3)
Device		Version/ Revision		Temp Range/ Package		Device Option		Tape and Reel Option

Device:	CEC1736		Cryptographic Embedded Controller, Temperature and Voltage Countermeasures
Version/ Revision:	S#		S = Soteria Version # = Revision Version Number
Temperature Range	I/	=	-40°C to +85°C (Industrial)
Package:	2ZW		84 ball WFBGA, 7x7x0.8 mm body, 0.65 pitch, 4MB Flash, Dual SPI Monitor
	2HW		64 ball VFBGA, 5.5x5.5x0.92 mm body, 0.5 pitch, 2MB Flash, Single SPI Monitor
Device Option	TFLX	=	TrustFLEX Device
Tape and Reel Option:	Blank	=	Tray packaging
	TR	=	Tape and Reel(3)

Example:

a) CEC1736-S0-I/2ZW-TFLX = CEC1736, TrustFLEX Variant, Revision Version 0, 84 ball WFBGA, 7mm x 7mm body, 4MB Flash, Dual SPI Monitor, Industrial grade, Tray packaging

b) CEC1736-S0-I/2HW-TFLX-TR = CEC1736, TrustFLEX Variant, Revision Version 0, 64 ball VFBGA, 5.5mm x 5.5mm body, 2MB Flash, Single SPI Monitor, Industrial grade, Tape and Reel 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.micro-chip.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

© 2024 Microchip Technology Inc. and its subsidiaries

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://microchip.com/support

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

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable" Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at https://www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP "AS IS". MICROCHIP MAKES NO REPRESENTATIONS OR WAR- RANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUD- ING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON- INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICU- LAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAM- AGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, CryptoMemory, CryptoRF, dsPIC, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AgileSwitch, APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet-Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, TrueTime, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, Augmented Switching, BlueSky, BodyCom, Clockstudio, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, GridTime, IdealBridge, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, IntelliMOS, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, KoD, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQI, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, Trusted Time, TSHARC, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, and Symmcom are registered trademarks of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2024, Microchip Technology Incorporated and its subsidiaries.

All Rights Reserved.

ISBN: 9781668343005

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

© 2024 Microchip Technology Inc.

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: 45-4485-5910
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

<Redtext>
© 2024 Microchip Technology Inc. and its subsidiaries
09/14/21