Intro to CEC1736 Trust Shield

A Leading Provider of Smart, Connected and Secure Embedded Control Solutions

Computing Product Group

Sep, 2022

Platform Root of Trust (PRoT) Portfolio

CEC1302
ARM M4 @ 48MHz
Secure Boot w/ HW RoT
144-WFBGA

CEC1702
ARM M4F w/MPU @ 48MHz
Secure Boot w/ HW RoT
84-WFBGA

CEC1712
ARM M4 @ 48 MHz
CNSA Suite Secure Boot
Key Revocation
Code Rollback Protection
84-WFBGA

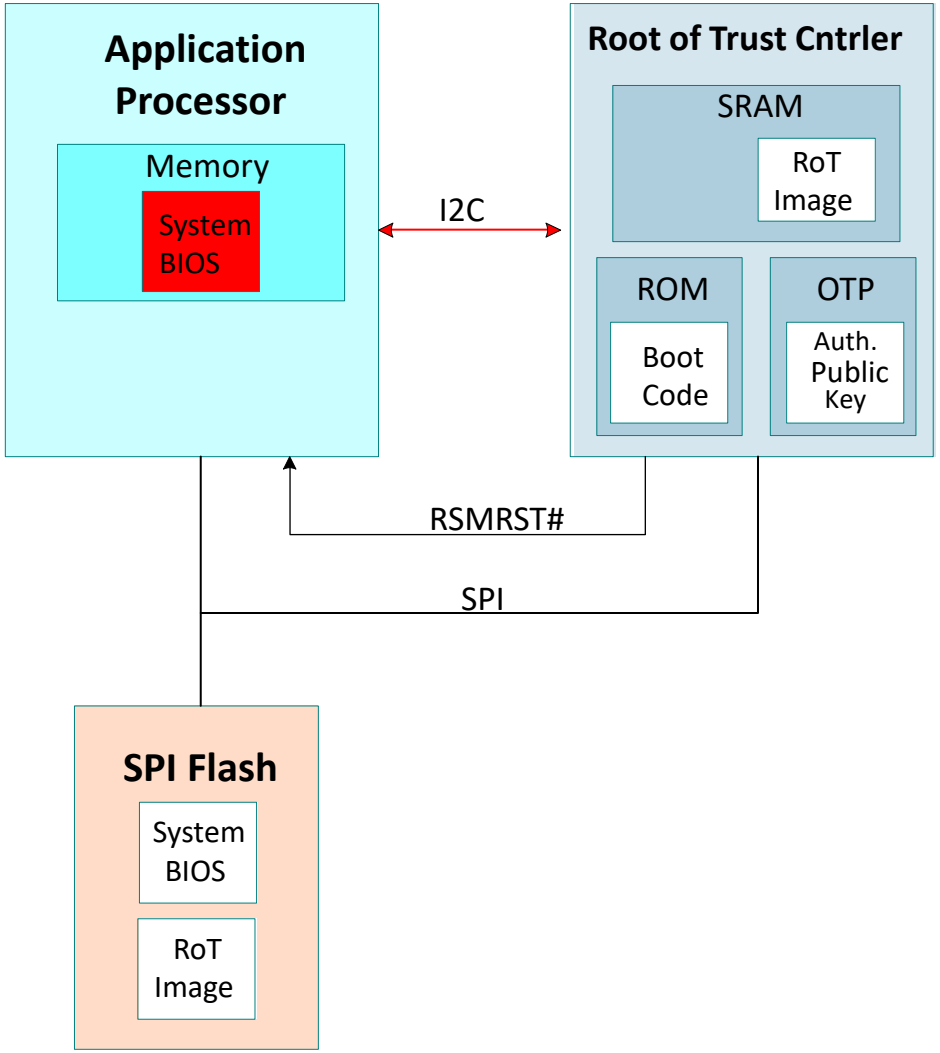
NEW

CEC1736 Trust Shield
ARM M4 @ 96M MHz
Real-time system bus protection
Attestation
Physical Attack Countermeasures
64-/84-WFBGA

May-17, 2022 Announcement

3rd generation Root of Trust of CEC17xx series for Datacenters, Telecom, Networking, Embedded Computing & Industrial

Recap - Secure Boot (Basic Root of Trust)



- **The Root of Trust (RoT) Controller contains the Immutable Boot Code and OTP**
- **At power-on, the RoT Controller:**
  - Holds Application Processor in reset
  - Loads and authenticates RoT Image with the public key in the OTP
- **The authenticated RoT Image begins execution, authenticates the Processor System BIOS code**
- **Releases the Host Processor from reset**

Why CEC1736 Trust Shield?

- **Best in-class Platform Root of Trust Controllers**
  - Hardware Cryptographic Cipher Suite (AES-256, SHA-512, RSA-4096, ECC and ECDSA P-384)
  - Boot ROM, 8Kbit OTP
  - Real-time system bus protection (SPI, I2C/SMBus)
  - Device Identity Authentication
  - Physical Unclonable Function (PUF) technology
- **Reduced system cost**
  - In-package 2MByte/4MByte Flash
  - Integrated QSPI Analog Switches
- **Quick time-to-market**
  - Development board, Trust Platform Design Suite (GUI), MPLAB Harmony
  - Sample Code, User Guides, Design Collateral, Webinars
- **Standards / Compliance**
  - NIST 800-193 PFR, Open Compute Project (OCP) Security, TCG DICE
  - Printer Working Group HCD-CPP, FIPS 140-2, CAVP, 3rd party penetration tests

CEC1736 *vs* CEC1712?

Applications

Runtime / Operating System

Firmware / Boot loader

Hardware (Components)

Trusted hardware & boot code

CEC173x (Real-time PRoT)

Real-time system Bus Protection

Device Identity Authentication

Ownership Transfer

Lifecycle Management

Data Exfiltration Countermeasures

Advanced Key Generation

CEC1712 (RoT)

Recovery

Firmware Authentication

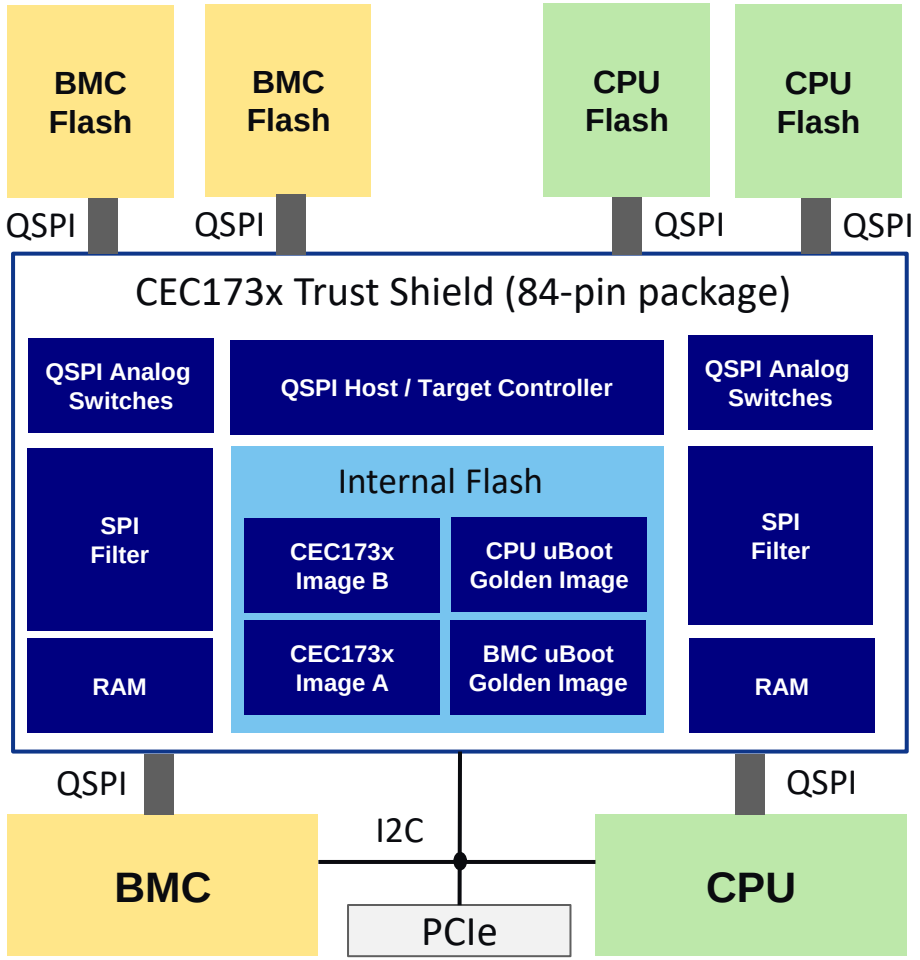
Secure Boot / Update

Provisioned Keys/Certs

CEC1736 Brings Next Gen Root of Trust Subsystem

Application Example

Real-time root of trust in server's baseboard management system



NOTE: 64-pin package option to support one (1) application processor system

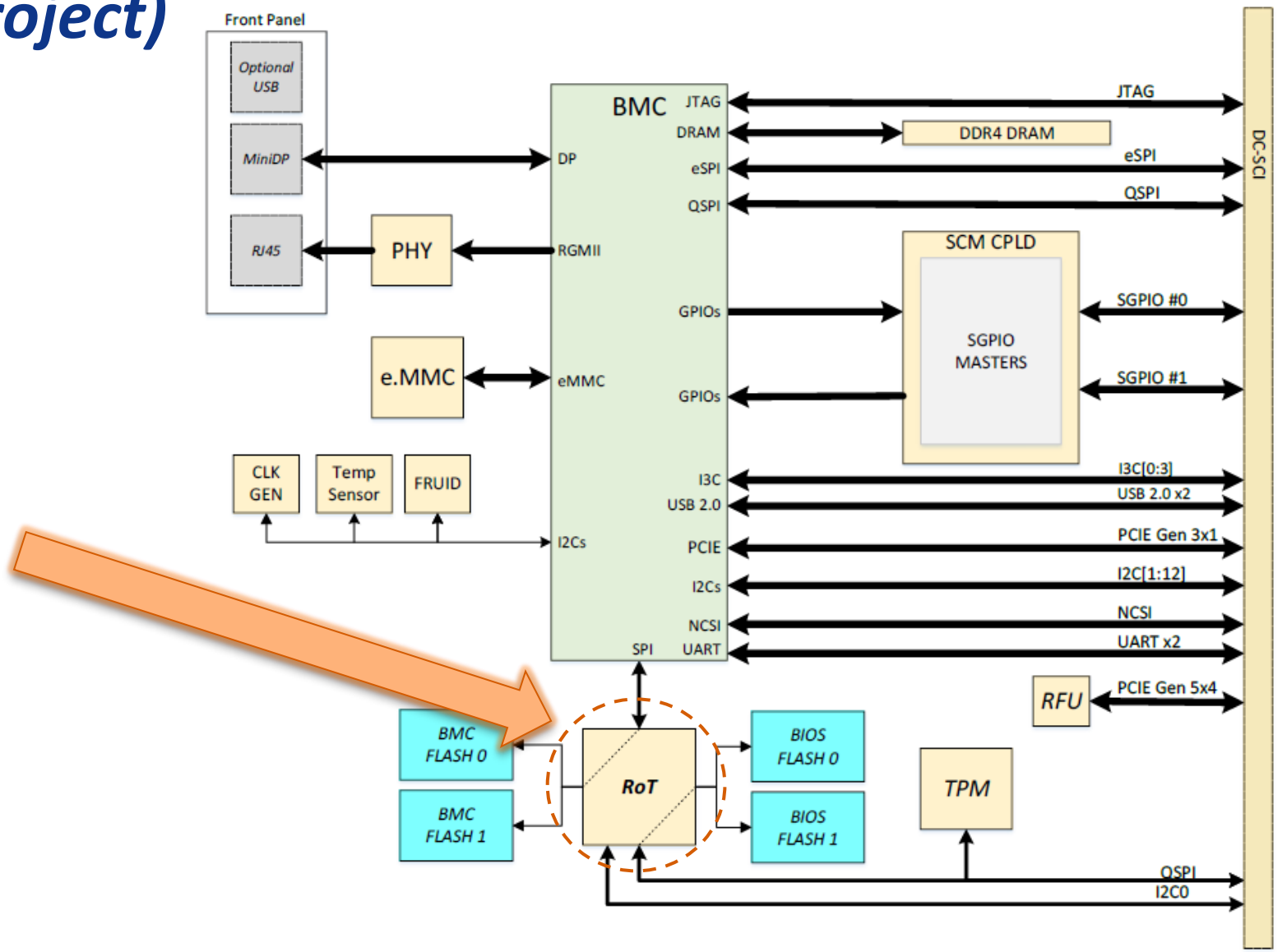
Target Markets

- **Data Centers**
  - Edge
  - Backplane
- **Embedded Computing**
  - Multi-function printers
- **Telecommunications**
  - Distributed/Central units
  - Small cells
- **Networking/Internet of Things**
  - Routers
  - Gateways
- **Industrial**
  - Control systems
  - Robotics/Automation

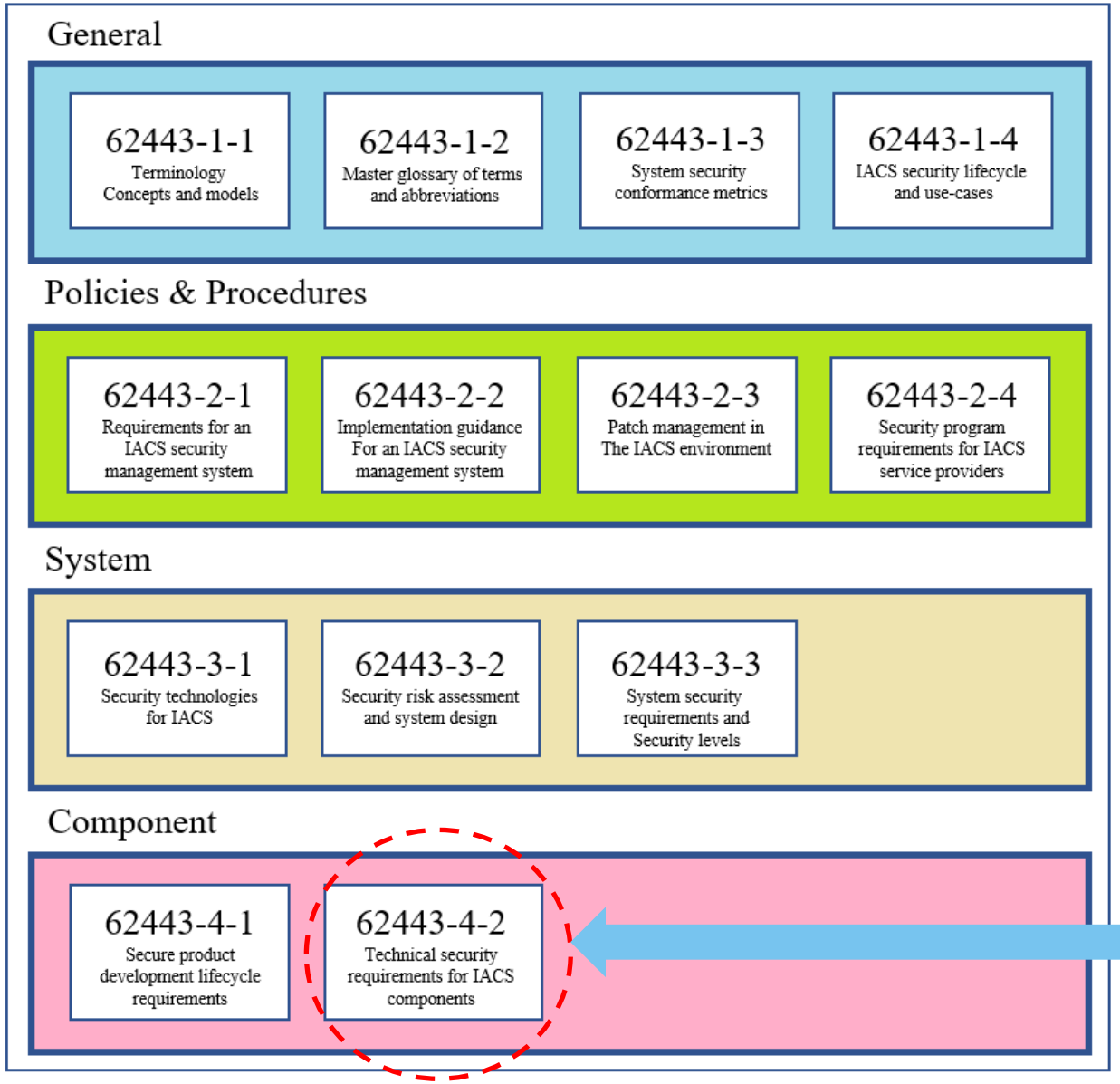
DC-SCM Example Block Diagram

(Open Compute Project)

CEC1736 Trust Shield



Industrial Network and System Security – IEC62443



TUV NORD協助研華取得IEC 62443-4-2認證

2022 / 01 / 14 - 編輯部

MOXA 產品 解決方案 支援 購買

首頁 > 關於我們 > 新聞與活動 > 新聞發布 > Moxa 通過 IEC 62443-4-1 認證，致力確保工業網路安全的承諾

Moxa 通過 IEC 62443-4-1 認證，致力確保工業網路安全的承諾

2021年3月11日
企業快訊

工業通訊及網路設備領導廠商 Moxa 宣布，該公司已通過並取得與網路安全標準相關的 IEC 62443-4-1 認證。該認證由 LCIE Bureau Veritas 負責進行測試和審核，最後由 IECEE 認證機構頒發認證。Moxa 長期在網路安全產業耕耘，經過全球知名相符性評估和認證服務供應商審核後，成為全球最早取得 IEC 62443-4-1 認證的公司之一。

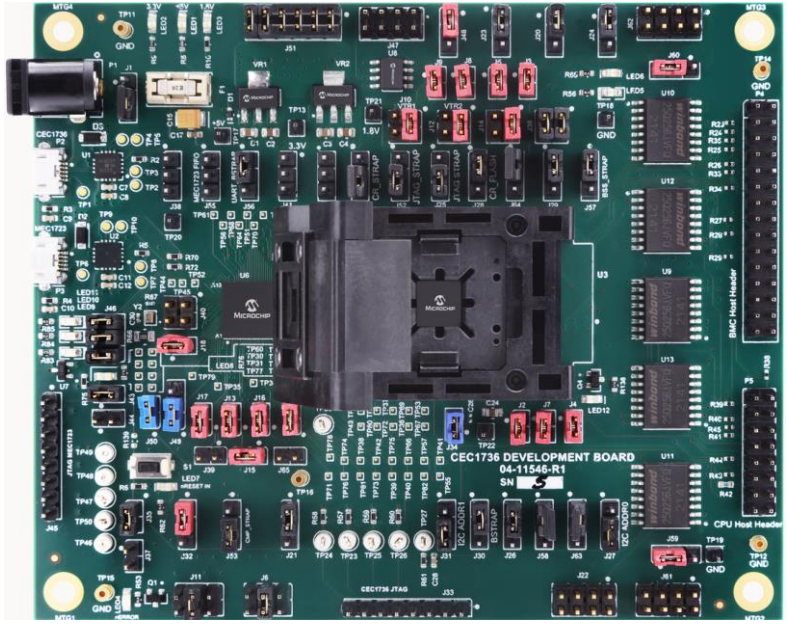
MICROCHIP

CEC1736 Development Board

CPN EV19K07A - $399

- Out-of-box demo with a pre-provisioned CEC1736
- Application processor emulation
- On-board 4x flash devices (128MByte)
- Standalone demo, or Daughter card to the system

- CEC1736 socket
- BMC host header – I2C, QSPI, GPIOs
- CPU host header – QSPI, GPIOs
- Programming/debugging interface



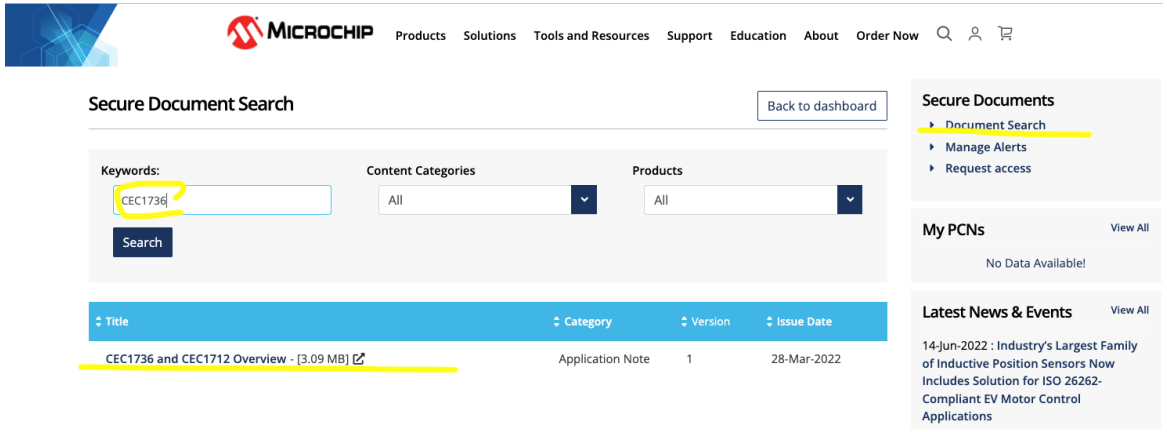
CEC1736 Development Board (CPN EV19K07A – $399)

CEC1736 Supporting Collateral

Why register for myMicrochip?

Join myMicrochip and gain access to member-only benefits with new features added constantly. Take advantage of these great perks by joining today!

We are excited to announce that the FPGA software, design files will be available on **Microchip.com** which will redirect you to **myMicrochip** and user licenses are will be available on **microchipDIRECT!**.
Review **Transferring FPGA software, design files and licenses from Microsemi to Microchip document** to determine the next steps to access FPGA software, design files and licenses on Microchip website.
Please use **Forgot Password?** to reset your account if you are logging in for first time on this Portal.



Keywords: CEC173x

Content Categories: All

Products: All

Search

Title	Category	Version	Issue Date
CEC173x Soteria-G3 OTP Spreadsheet - [102 KB]	Application Note	1	11-Apr-2022
CEC173x Boot Timing - [103 KB]	Application Note	1	08-Mar-2022
CEC173x I2C Crisis Port for Secure Boot Applications - [283 KB]	Application Note	21	15-Dec-2021
CEC173x PUF User Guide - [320 KB]	Application Note	2	15-Dec-2021
CEC173x Crypto ROM API - [289 KB]	Application Note	2	15-Dec-2021
CEC173x SPI Mon Description - [433 KB]	Application Note	1	15-Dec-2021
CEC173x Internal SPI Flash Usage - [22 KB]	Application Note	2	15-Dec-2021
SPDM Support in CEC173x - [252 KB]	Application Note	1	15-Dec-2021
CEC173x EC Firmware Overview - [676 KB]	Application Note	4	15-Dec-2021
CEC173x Development Board Documentation - [38.19 MB]	Board Product	1	27-Apr-2022
CEC173x BSDL File - [27 KB]	BSDL Files	1	24-Feb-2022
CEC173x Data Sheet - [3.20 MB]	Data Sheet	1	15-Nov-2021
CEC173x Data Brief (NDA) - [660 KB]	Data Sheet		20-Oct-2021
CEC173x IBIS Files - [915 KB]	Models	1	24-Feb-2022
CEC173x Soteria-G3 Secure Boot App (binary) - [272.73 MB]	Software	11	27-May-2022