MICROCHIP CEC1736 Trust Shield Root of Trust Controller User Guide

Contents

MICROCHIP CEC1736 Trust Shield Root of Trust Controller

Product Information

The CEC1736 is a device that requires provisioning in order to be configured. Provisioning is the process of setting up the device with the necessary configurations and settings. This guide provides instructions on how to provision the CEC1736 using two different
methods: using the web URL and using the TPDS application.

The CEC1736 is a secure boot solution developed by Microchip. It is designed to enhance the security of embedded systems by providing secure boot functionality.

Product Usage Instructions

Provisioning Using the Web URL

1. Open a web browser and go to the following URL: https://www.microchip.com/en-us/products/security/secure-boot-solutions/cec1736configurator
2. On the webpage, you will find complete instructions on how to provision the CEC1736. Follow the instructions provided.

Provisioning Using the TPDS Application

1. Open a web browser and go to the following URL: https://microchipdeveloper.com/authentication:trust-platform-v2

2. On the webpage, you will find the TPDS application. Install the application by following the provided instructions.
3. Once the TPDS application is installed, launch it from the Start menu.
4. In the TPDS application, select the “Configurators” tab located at the top.
5. Scroll down to the bottom and select “CEC1736”.
6. This will open a web page with instructions on how to configure the CEC1736.
7. Click on the “Download Now” button to download the necessary files. Once the download is complete, unzip the contents into a folder.
8. Locate the file named “CEC173x configurator.html” within the unzipped folder. Open it with a web browser.
9. The instructions for provisioning the CEC1736 will be displayed within the opened web page.

INTRODUCTION

The purpose of this guide is to provide instructions on how to provision the CEC1736. There are two ways to access the instructions to provision the CEC1736, using the web URL and using the TPDS application. Each will be described in this document.

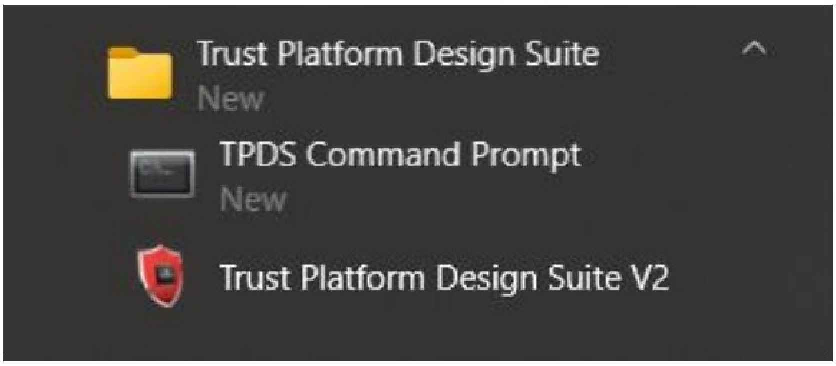
Using the Web URL

The following URL details complete instructions on how to provision the CEC1736.
https://www.microchip.com/en-us/products/security/secure-boot-solutions/cec1736-configurator

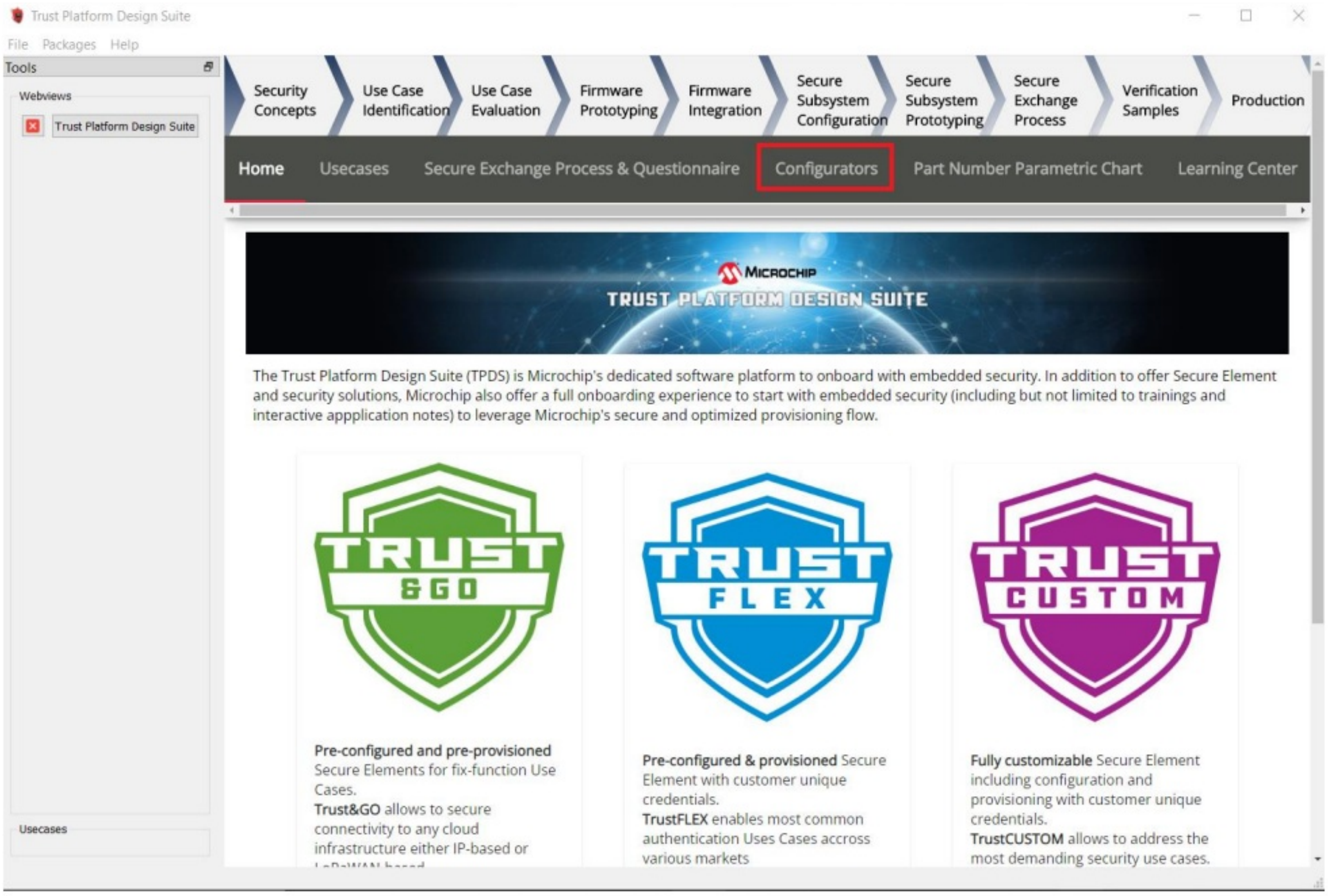
Using the TPDS Application

Step 1
To provision the TPDS using the TPDS application, use the following URL to install the application.
https://microchipdeveloper.com/authentication:trust-platform-v2

Step 2
Launch the TPDS application from the Start menu.



Step 3
On the top, select the Configurators tab.



The Trust Platform Design Suite (TPDS) is Microchip's dedicated software platform to onboard with embedded security. In addition to offer Secure Element and security solutions, Microchip also offer a full onboarding experience to start with embedded security (including but not limited to trainings and interactive application notes) to leverage Microchip's secure and optimized provisioning flow.

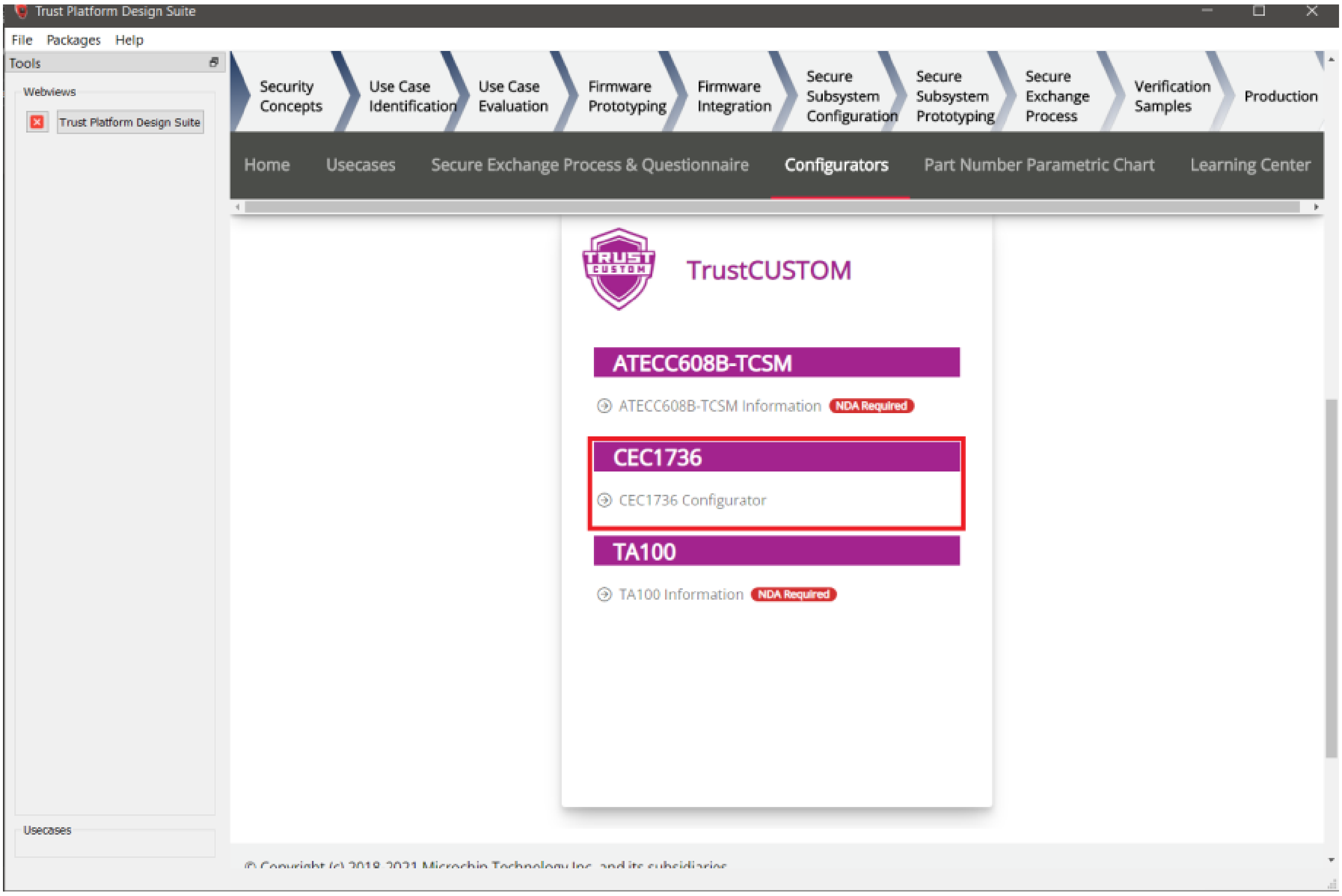
Pre-configured and pre-provisioned Secure Elements for fix-function Use Cases.
Trust&GO allows to secure connectivity to any cloud infrastructure either IP-based or LoRaWAN based

Pre-configured & provisioned Secure Element with customer unique credentials.
TrustFLEX enables most common authentication Uses Cases accross various markets

Fully customizable Secure Element including configuration and provisioning with customer unique credentials.
TrustCUSTOM allows to address the most demanding security use cases.

Step 4

Scroll down to the bottom and select CEC1736



TrustCUSTOM

ATECC608B-TCSM

ATECC608B-TCSM Information NDA Required

CEC1736

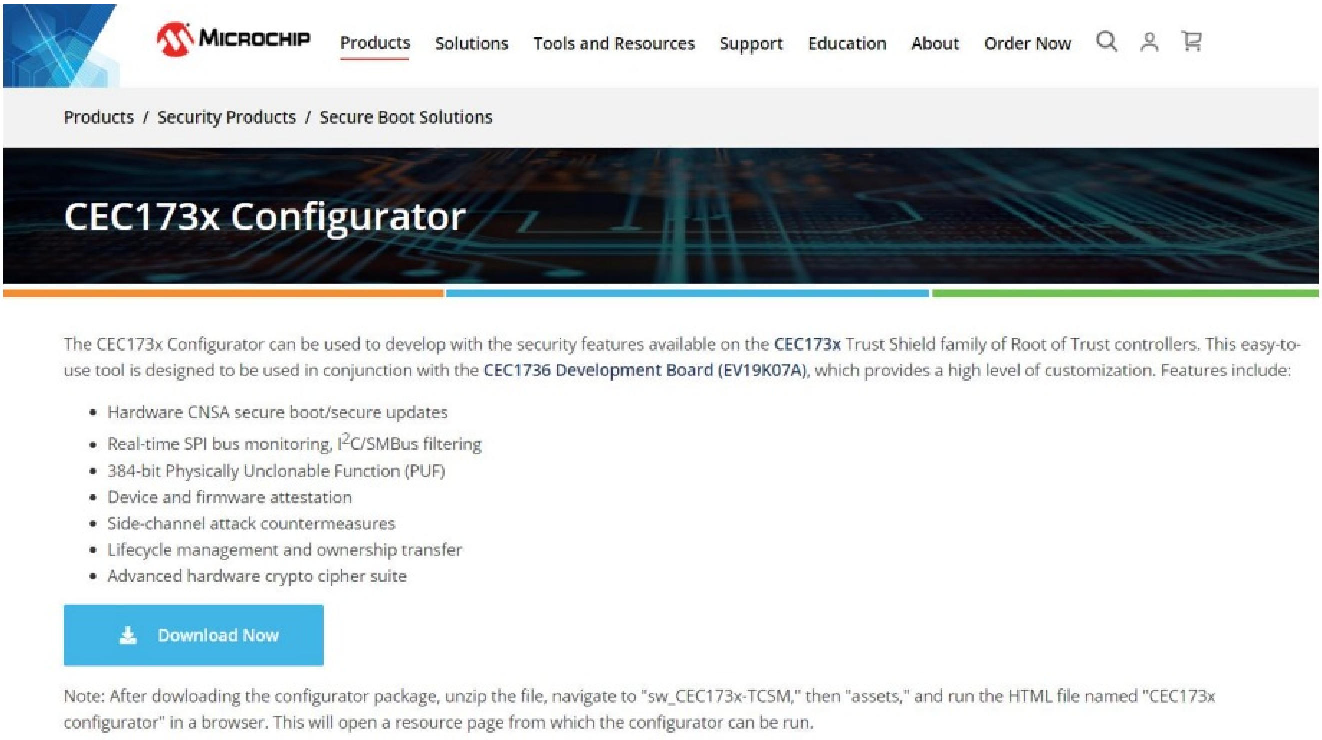
CEC1736 Configurator

TA100

TA100 Information NDA Required

© Copyright (c) 2018-2021 Microchip Technology Inc. and its subsidiaries

This should open a web page with instructions on how to configure the CEC1736.



Products / Security Products / Secure Boot Solutions

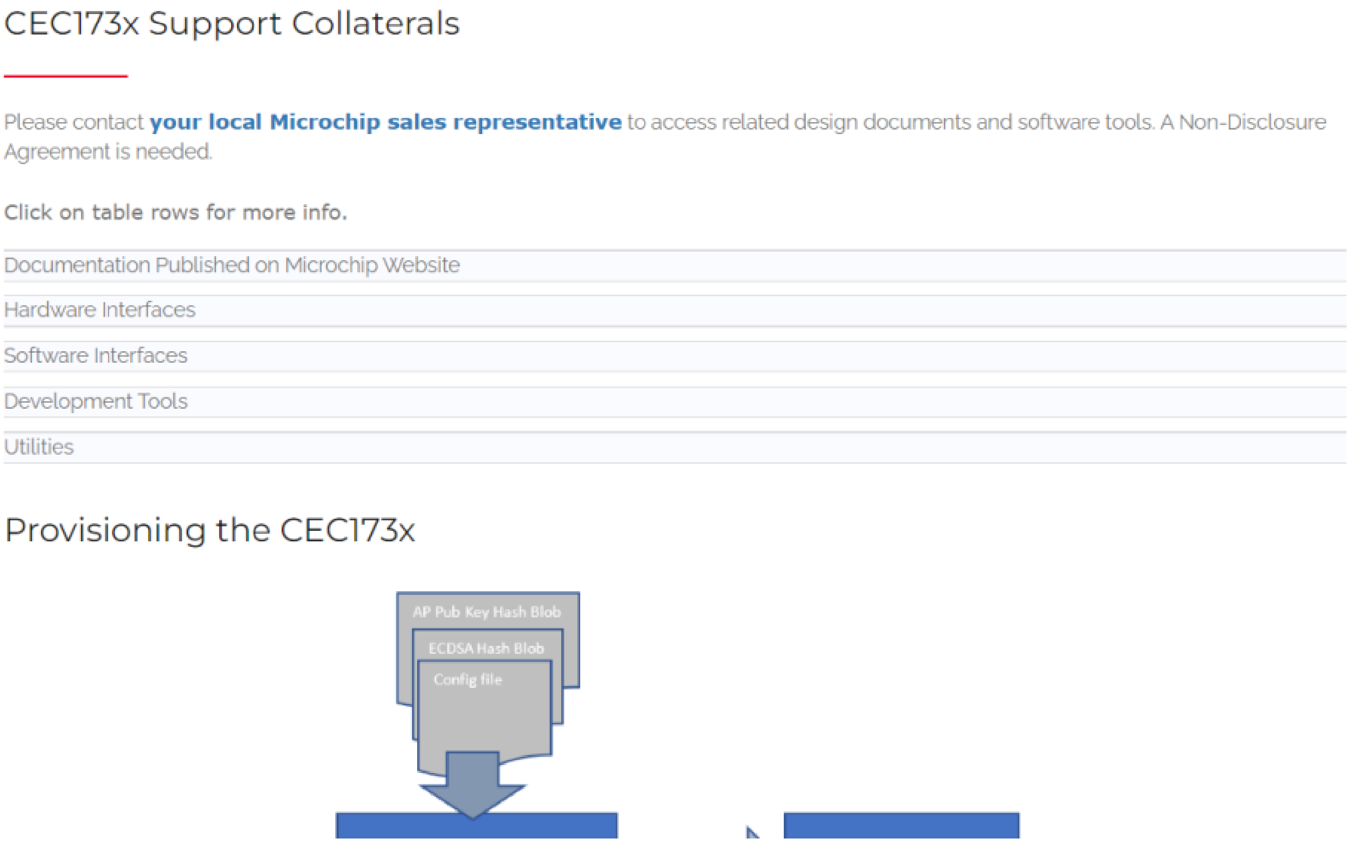
CEC173x Configurator

The CEC173x Configurator can be used to develop with the security features available on the **CEC173x** Trust Shield family of Root of Trust controllers. This easy-to-use tool is designed to be used in conjunction with the **CEC1736 Development Board (EV19K07A)**, which provides a high level of customization. Features include:

- Hardware CNSA secure boot/secure updates
- Real-time SPI bus monitoring, I^{2}C/SMBus filtering
- 384-bit Physically Unclonable Function (PUF)
- Device and firmware attestation
- Side-channel attack countermeasures
- Lifecycle management and ownership transfer
- Advanced hardware crypto cipher suite

Note: After dowloading the configurator package, unzip the file, navigate to "sw_CEC173x-TCSM," then "assets," and run the HTML file named "CEC173x configurator" in a browser. This will open a resource page from which the configurator can be run.

Press ‘Download Now’. Once complete, unzip the contents into a folder.
Open .\CEC173xConfigurator\sw_CEC173x-TCSM\assets\CEC173x configurator.html and the instructions for provisioning the CEC1736 will be displayed.



CEC173x Support Collaterals

Please contact **your local Microchip sales representative** to access related design documents and software tools. A Non-Disclosure Agreement is needed.

Click on table rows for more info.

Documentation Published on Microchip Website
Hardware Interfaces
Software Interfaces
Development Tools
Utilities

Provisioning the CEC173x

Documents / Resources

 Provisioning The CEC1736 Quick Start Guide **INTRODUCTION** The purpose of this guide is to provide instructions on how to provision the CEC1736. There are two ways to access the instructions to provision the CEC1736, using the web URL and using the TPDS application. Each will be described in this document. **Using the Web URL** The following URL details complete instructions on how to provision the CEC1736. https://www.microchip.com/en-us/products/security/secure-boot-solutions/cec1736-configurator **Using the TPDS Application** **Step 1** To provision the TPDS using the TPDS application, use the following URL to install the application. https://microchipdeveloper.com/authentication:trust-platform-v2 **Step 2** Launch the TPDS application from the Start menu. Trust Platform Design Suite New TPDS Command Prompt New Trust Platform Design Suite V2 © 2022 Microchip Technology Inc. **Preliminary** January XX, 2010	MICROCHIP CEC1736 Trust Shield Root of Trust Controller [pdf] User Guide CEC1736, CEC1736 Trust Shield Root of Trust Controller, Trust Shield Root of Trust Controller, Root of Trust Controller, Trust Controller

References

- Installing the Trust Platform Design Suite v2 - Developer Help
- CEC1736 Configurator | Microchip Technology

Manuals+,