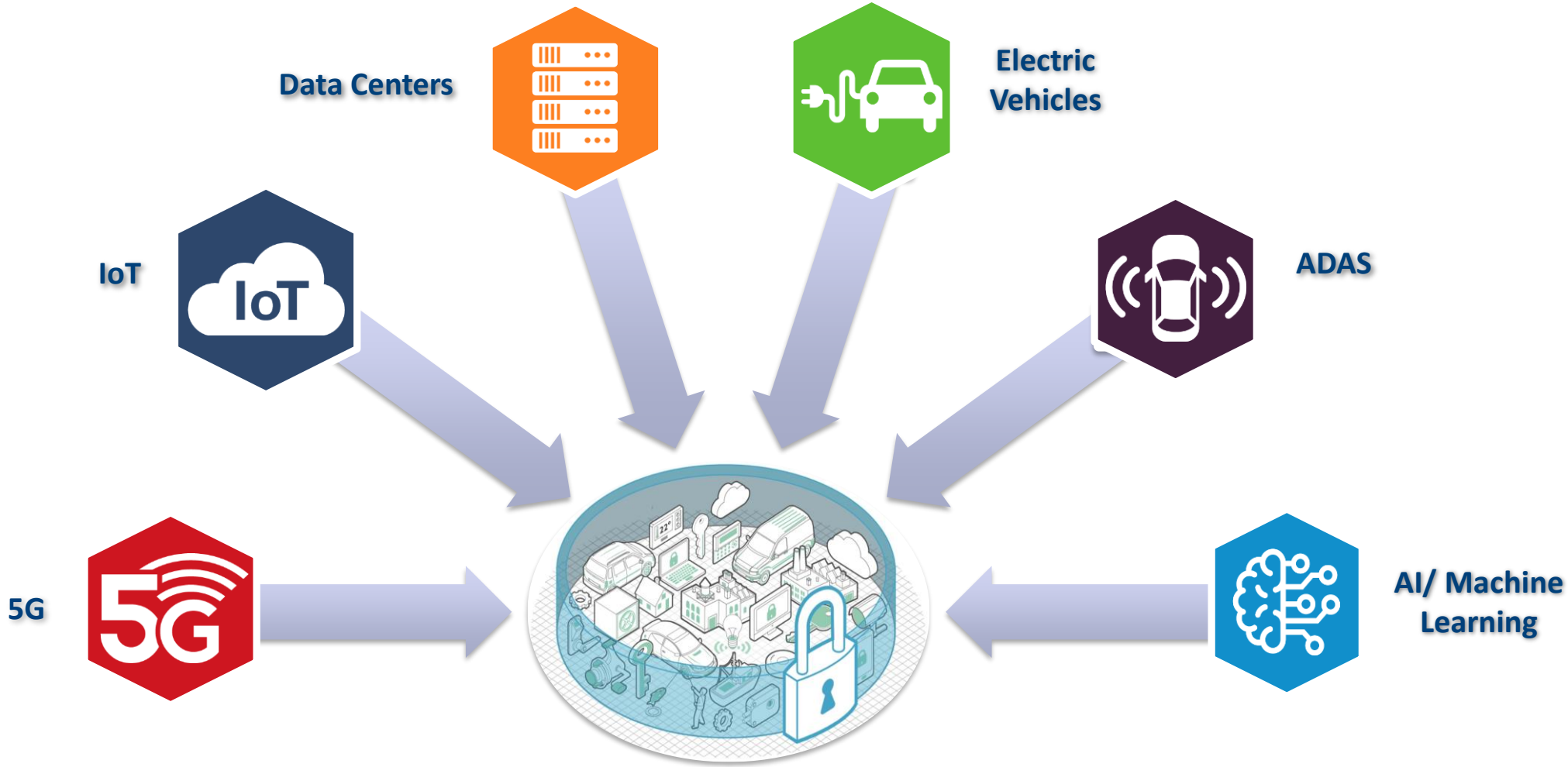
Platform Root of Trust
Platform Firmware Resiliency

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

Secure Computing Group (SCG)
May, 2024

Connected Systems - Everywhere

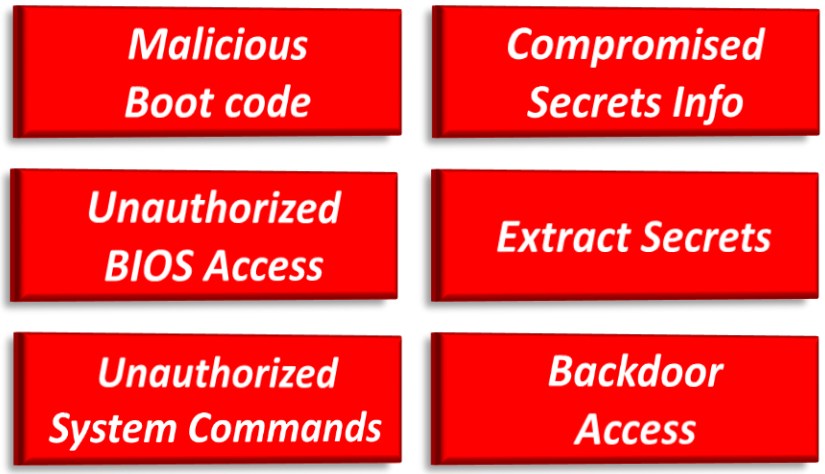


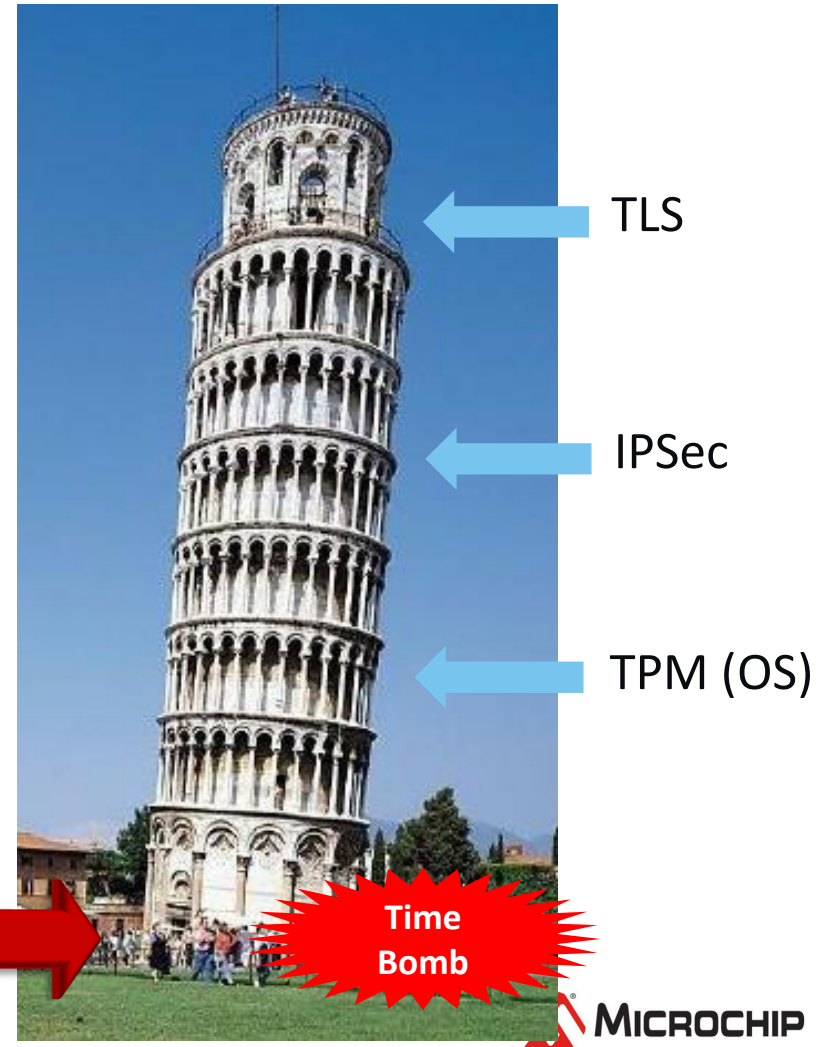
And more …

MICROCHIP

Cyberattacks at the Root

- **Cyberattacks moving beyond attacking the OS & applications**
- **Increased attacks at the root - hardware & boot code / firmware**
  - Bad hardware & boot code/firmware to perform malicious attacks, or lie dormant until days, weeks or years later





MICROCHIP

Outcome from Root Level Attacks

Personal data was stolen from Computers, Mobile Devices

Ransomware Cyber attack caused Colonial Pipeline to shut down

Stuxnet reprogrammed PLCs, destroyed 20% of Iran's centrifuges

Hackers reprogram printers, play Doom, start fires

NIST 800-193

Platform Firmware Resiliency Guidelines

- **Protection:** Mechanisms for ensuring that Platform Firmware code and critical data remain in a state of integrity and are protected from corruption, such as the process for ensuring the authenticity and integrity of firmware updates.

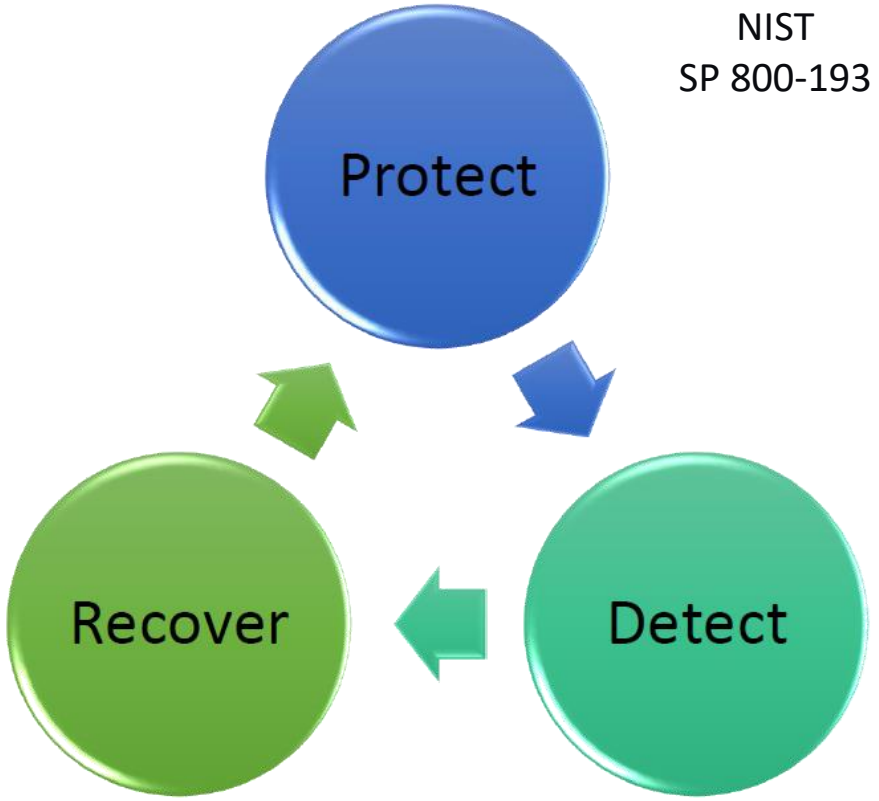
- **Detection:** Mechanisms for detecting when Platform Firmware code and critical data have been corrupted or otherwise changed from an authorized state.

- **Recovery:** Mechanisms for restoring Platform Firmware code and critical data to a state of integrity in the event that any such firmware code or critical data are detected to have been corrupted, or when forced to recover through an authorized mechanism. Recovery is limited to the ability to recover firmware code and critical data.

Firmware Resiliency

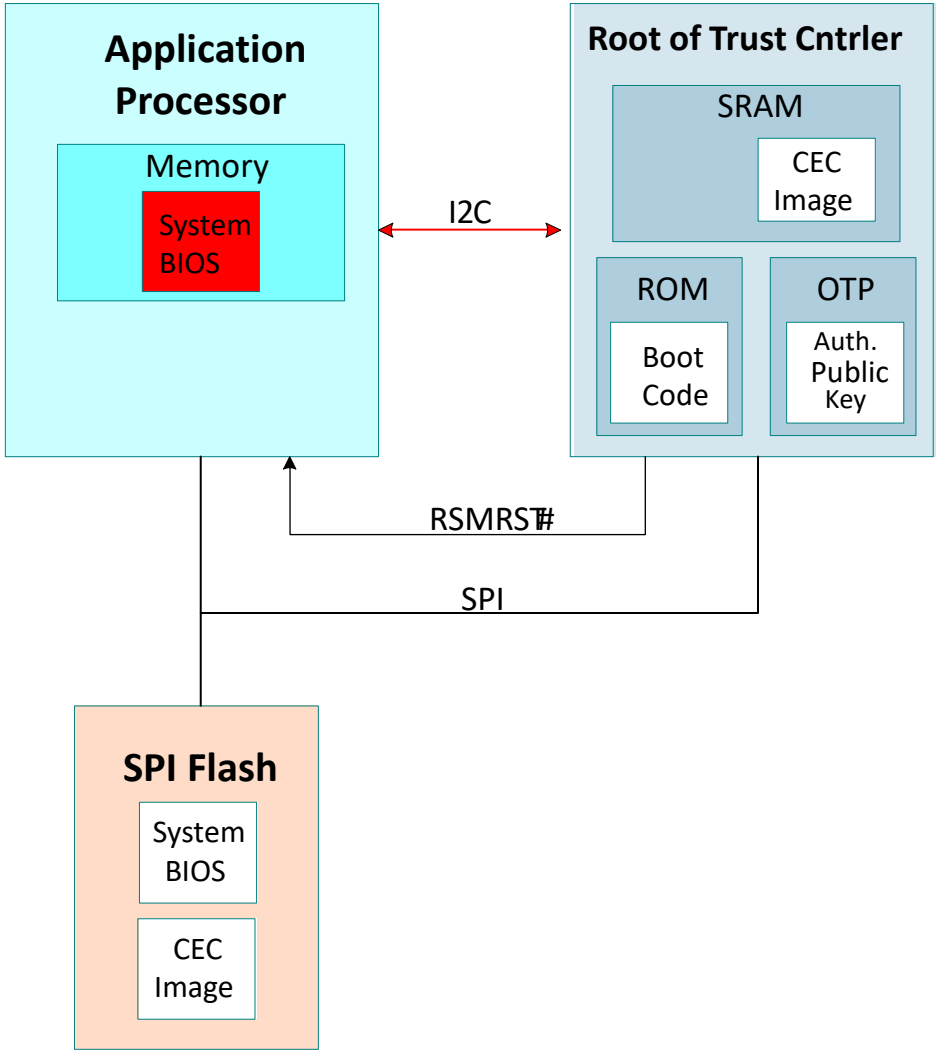
Platform Firmware Resiliency Guidelines

- **Protect**
  - Maintain state of integrity
  - Prevent unauthorized access and corruption
  - Authenticate the integrity of firmware updates
- **Detect**
  - Detect unauthorized access or corruption
- **Recover**
  - Restore FW to a state of integrity



NIST
SP 800-193

Recap - Basic Root of Trust (Secure Boot)



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

Root of Trust Solution

Datacenter | Computing |AI ML |Industrial |Medical

MICROCHIP

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

SMART | CONNECTED | SECURE

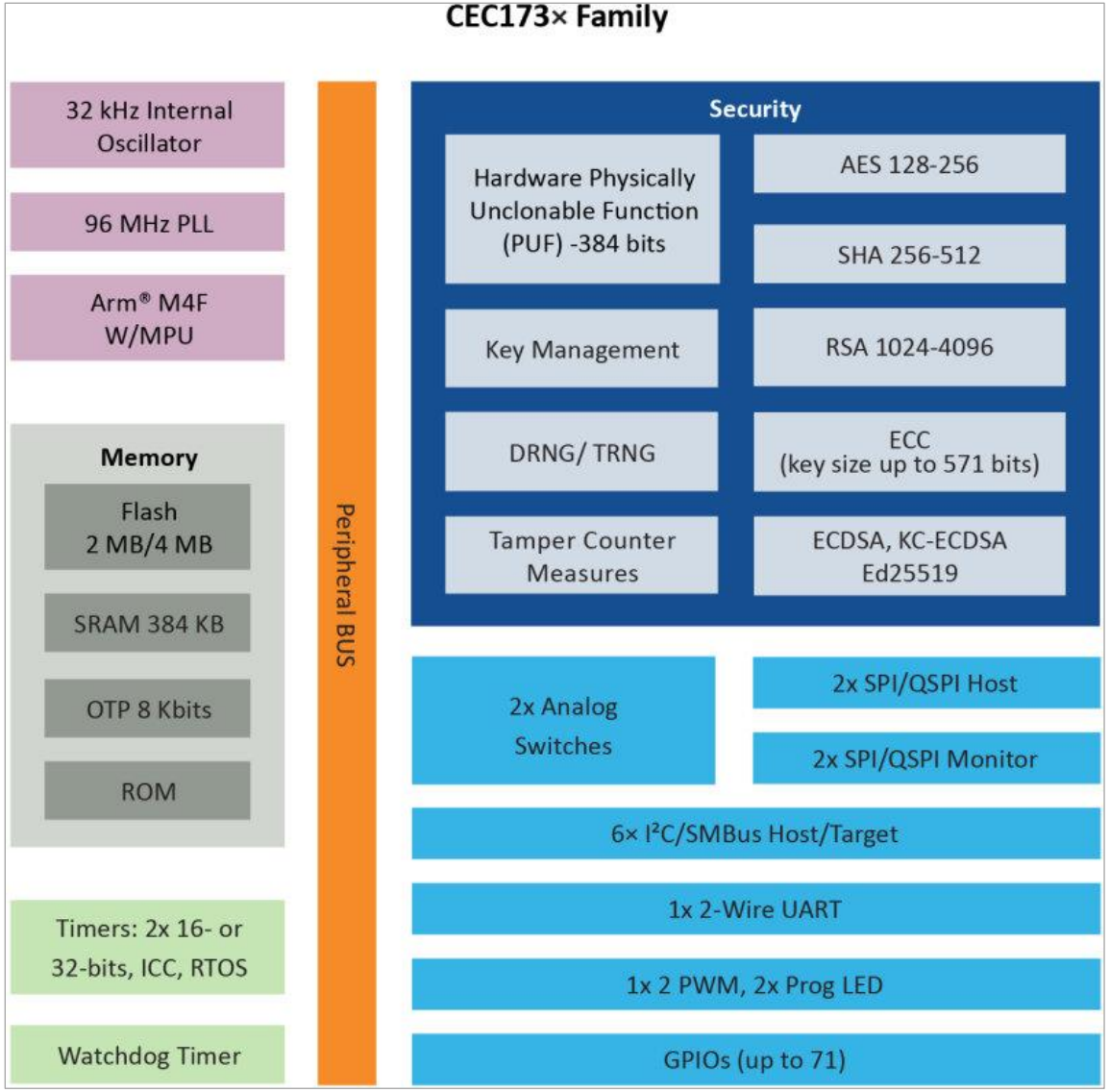
CEC173x Trust Shield Family

Product Features

- 96MHz ARM® Cortex-M4F-based MPU
- 384KB SRAM: code + data
- 2MB/4MB flash, Boot ROM
- 8Kb OTP with anti-fuse technology
- FIPS CAVP hardware crypto engine
- SP800-90B TRNG
- HW Physical Unclonable Function (PUF)

Advanced Security Features

- Real-Time SPI bus monitoring
- I2C/SMBus filtering
- Device attestation



MICROCHIP

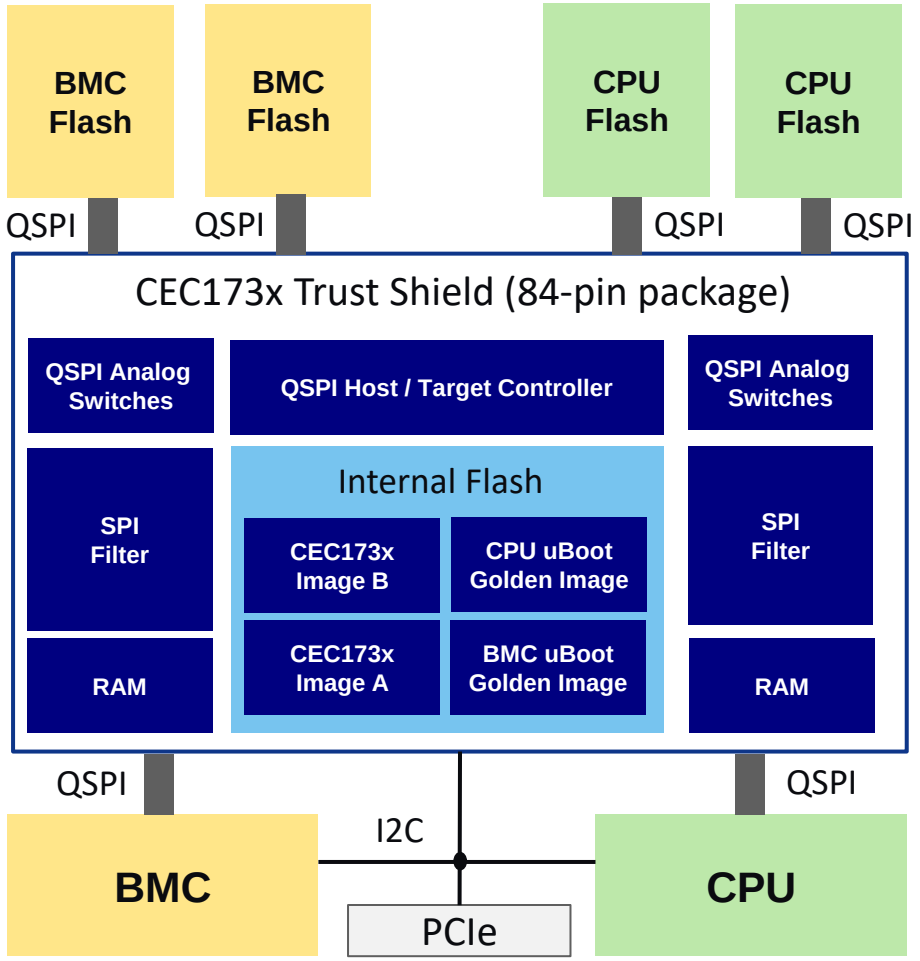
PUF (Physical Unclonable Function)

- **Impossible to:**
  - Duplicate, Clone or Predict
- **Generate:**
  - Device-Unique ID
  - Device-Unique Random Number Generation
  - Device-Unique Key Derivation
    - Wrap and Unwrap:
      - Keys/Secrets Stored in SPI Flash

CEC173x Brings Next Gen Root of Trust Subsystem

Application Example

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



MICROCHIP

Microchip Root Of Trust Solution Overview

Attacks at Root level –Hardware and Boot Code are on the rise…
NIST and **Open Compute Project** recommends Protect, Detect and Recover mechanisms using
Hardware Root Of Trust on EVERY Platforms, Devices and Peripherals

NIST OPEN Compute Project®

NIST 800-193
Platform Firmware Resiliency Guidelines

Hardware Root of Trust Controller

Immutable Boot Loader | CNSA Cryptography

Protection | Detection | Recovery

Root Of Trust | Chain Of Trust

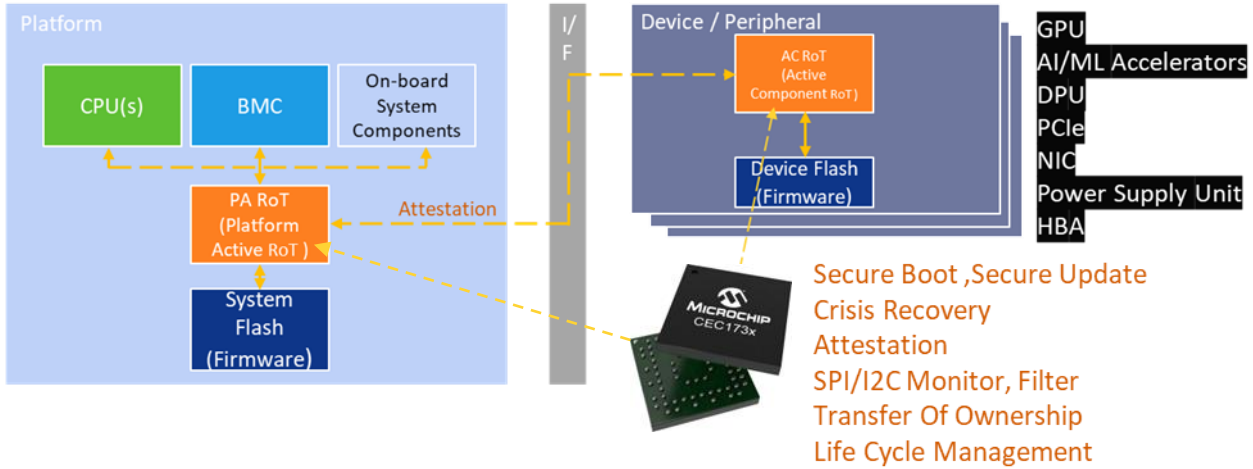
Open Compute Security Project

Secure Boot | Attestation | Secure Update

Bus Monitor | Ownership Transfer | Life Cycle Management

Secure Supply Chain and Manufacturing

Platform Active Root Of Trust | Active Component Root Of Trust



Complete Turnkey Solution – Meets NIST and OCP Guidelines

- **Real-Time Platform Root Of Trust Controllers – CEC173x Family**
  - ✓ Cortex-M4F w/Immutable ROM Boot loader
  - ✓ CNSA, FIPS Compliant and CAVP Certified Hardware Crypto Engine
  - ✓ Reduced System Cost with Integrated SPI Flash and Analog Switches
- **Easily Configurable and Customizable Soteria Firmware and Tools**
  - ✓ NIST and OCP Compliant Soteria FW
  - ✓ TPDS Configurator for Rapid Prototyping and Development
- **Common Criteria Certified Secure Provisioning**

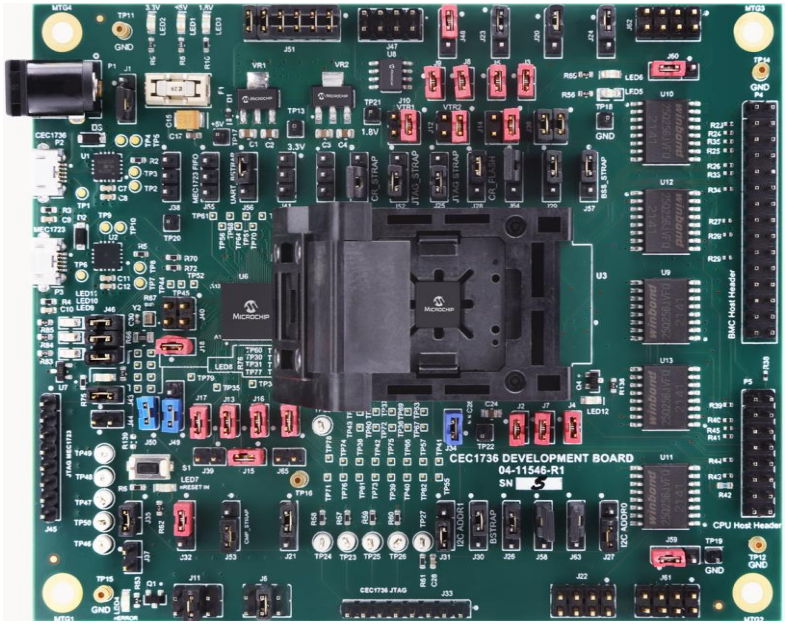
MICROCHIP

CEC1736 Development Board

CPN EV19K07A

- 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

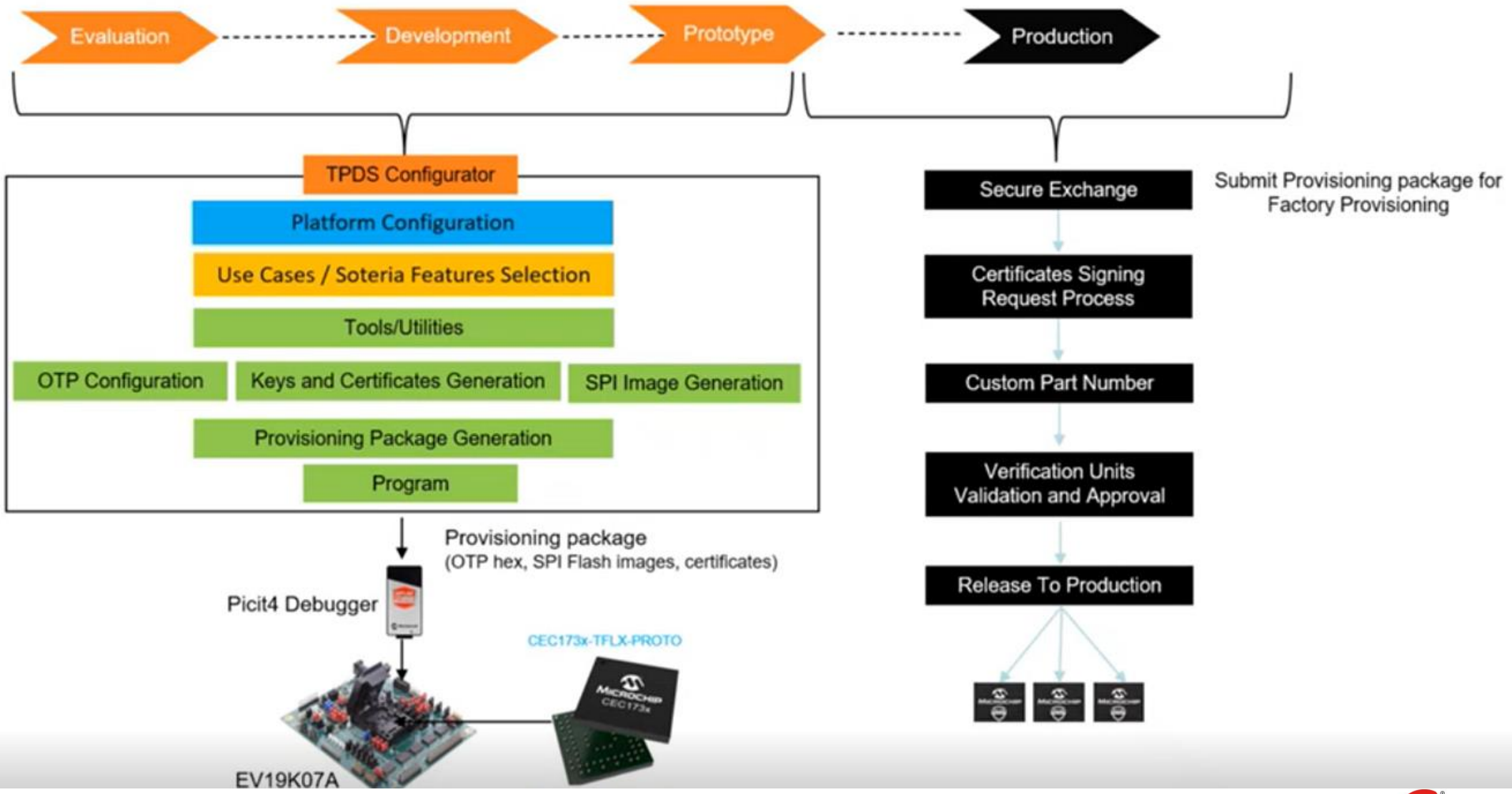
- CEC1736 socket
- BMC host header – I2C, QSPI, GPIOs
- CPU host header – QSPI, GPIOs
- Programming/debugging interface



CEC1736 Development Board (CPN EV19K07A)

MICROCHIP

CEC173x TPDS Configurator



Trust Platform Design Suite

File Packages Help

Tools

Webviews

Trust Platform Design Suite

CEC173x Configurator

Usecases

CEC1736 TrustFLEX

System Configuration

Device Configuration

Secure Boot

SPI Monitor

Rollback Protection

Key Revocation

Attestation

Secure Update

Crisis Recovery

Assets

Tools

Update INI Files

Import Settings

Export Settings

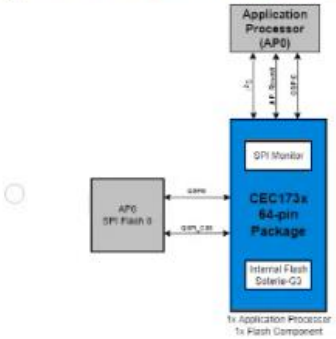
Reset All to Tool defaults

Generate Proto Provisioning Package

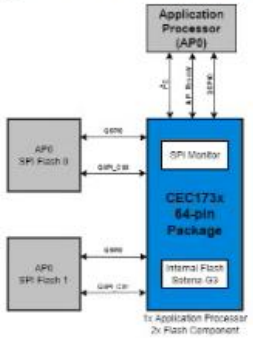
System Configuration

— System Architecture Selection

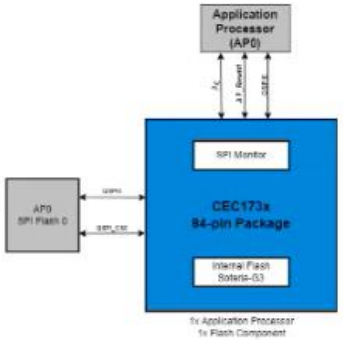
Application Processor(s) and Flash Component(s) Select System Architecture based on Application Processors and Flash Components



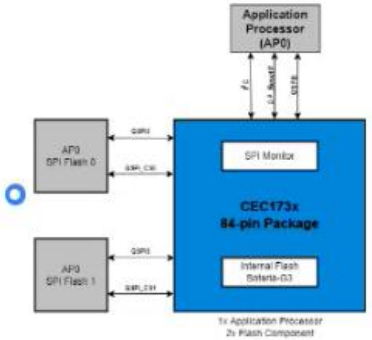
1AP-1C (2HW)



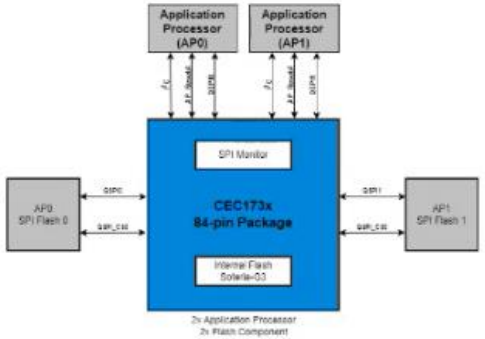
1AP-2C (2HW)



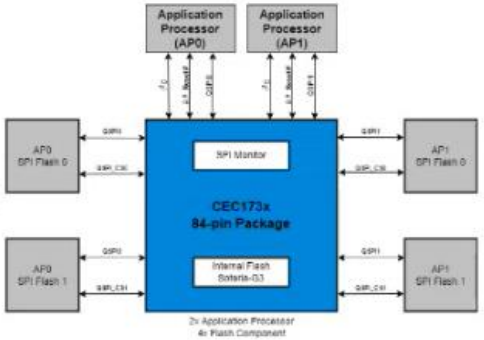
1AP-1C (2ZW)



1AP-2C (2ZW)



2AP-2C (2ZW)



2AP-4C (2ZW)

AP0 External Flash Size Provide AP0 External Flash size in Megabits.

128 128

Select Device OTP Select Real-Time Platform Root of Trust Controller device

MICROCHIP

AP0 External Flash Size Provide AP0 External Flash size in Megabits.

128 | 128

Select Device OTP Select Real-Time Platform Root of Trust Controller device

(•) CEC1736 ( ) CEC1734

Feature(s) Selection Select Soteria-G3 Firmware Features

Select Provisioning Flow

(•) TrustFLEX ( ) TrustCUSTOM

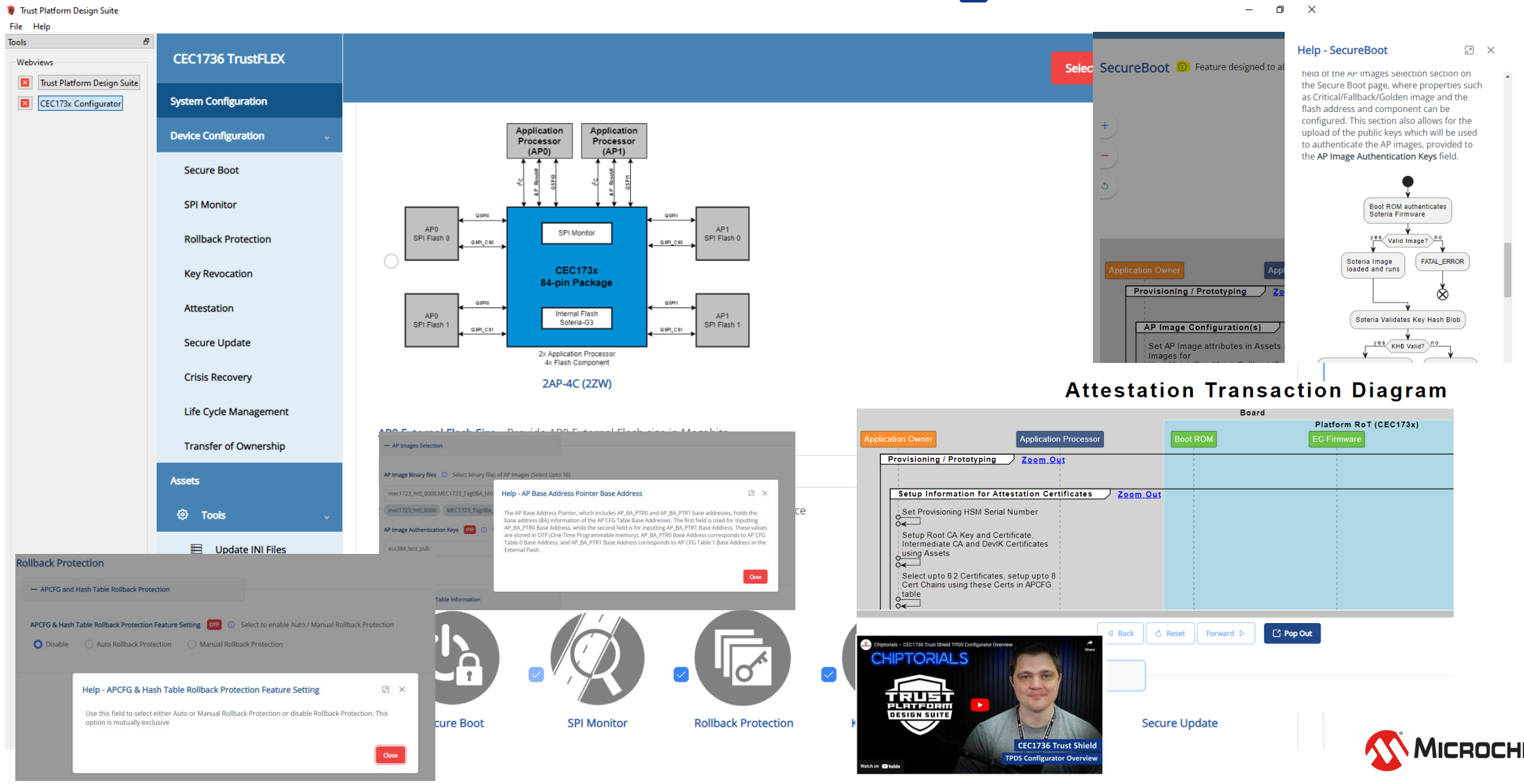
Packages to Generate and Program Select the packages to generate and program on request

[x] OTP Package [x] Internal SPI Package [x] External SPI Package

Bypass Pin Polarity Selection OTP Test Bypass and JTAG Debug are enabled for generating proto package, and disabled for production package. Select bypass pin polarity.

( ) Bypass on Active High (•) Bypass on Active Low

CEC173x TrustFLEX TPDS Configurator



HOW TO START IT !!

Download & install Trust Platform Design Suite (TPDS)

MICROCHIP Developer Help

Search This Site | Search

Site updated 12 days ago
4946 active pages

- Home
- Training
- Development Tools
- Functions
  - Embedded Software Integration
  - Wi-Fi® and Ethernet
  - Universal Serial Bus
  - Wired Communications
  - Wireless Communications
  - Touch Sensing
  - Displays
  - Motor Control
  - Power Conversion
  - Signal Conditioning
  - Digital Signal Processing
  - Authentication
    - *Get Started Here*
    - Trust Platform Design Suite
      - **Installing the Trust Platform Design Suite**
      - Secure Provisioning of TrustFLEX
      - CryptoAuth Trust Platform Factory Reset
    - Trust Platform Getting Started Labs
    - Asymmetric Authentication - Use Case Example
    - Symmetric Authentication - Use Case Example
    - Symmetric Authentication with Non-Secure MCU - Use Case Example
    - Secure Firmware Download - Use Case Example
  - Hardware-Software Integration
- Projects

Installing the Trust Platform Design Suite

This page shows you how to install and set up Microchip's Trust Platform Design Suite for CryptoAuthentication™. The design suite dramatically reduces the time you'll spend provisioning and using Microchip's secure elements.

Click image to enlarge.

1 Installing the Design Suite

1. Installing the Trust Platform Design Suite Graphical User Interface
   - Includes the Trust Platform GUI, Python and Jupyter Notebook.
2. Cloning the Trust Platform Repository
   - The Trust Platform repository is hosted on GitHub and must be downloaded separately.
   - Includes Python packages, C projects, and use case user guides.
3. Setting the Path to the MPLAB X IDE Installation Folder
   - Enables the GUI to re-program the CryptoAuth Trust Platform board.

2 After Installation

1. Choosing the Right Trust Platform Family
2. Starting Jupyter Notebook
   - Start Jupyter Notebook to provision the secure element.

Installing the Trust Platform Design Suite Graphical User Interface

MICROCHIP

Order Development Kit EVK19K07A

MICROCHIP Purchasing & Client Services

evk19k07a

$0.00

Products | Request Large-Quantity Pricing | Design Services | Purchasing Tools | Support | 888-624-7435

Home / Development Tools

View Product Details

Part Number: EV19K07A - CEC1736 Development Board

The CEC1736 Development Board is an evaluation board that can be used for development, customer evaluation and demos.

The CEC1736 "Trust Shield" solution acts as an external root of trust for data center, telecom/5G, embedded computing, networking and industrial platforms. It's rich feature set ensures that a device not only boots and updates its firmware securely, but also provides protection during run-time and throughout its life cycle.

The board comes equipped with a socket that houses a CEC1736 Trust Shield Controller. The CEC1736 can be replaced, allowing customers to experiment and develop with its internal One Time Programmable (OTP) block.

The board comes with an optionally pre-provisioned CEC1736 that partners with a Graphic User Interface to demo several of the part's features.

Standard Pricing:

Order Quantity	USD per Unit
1+	$458.85

Are You Looking For Large-Quantity Pricing?

Request Special Pricing for Annual Volume

In Stock Now: 53

Order now, up to 53 estimated to ship on 25-Mar-2024

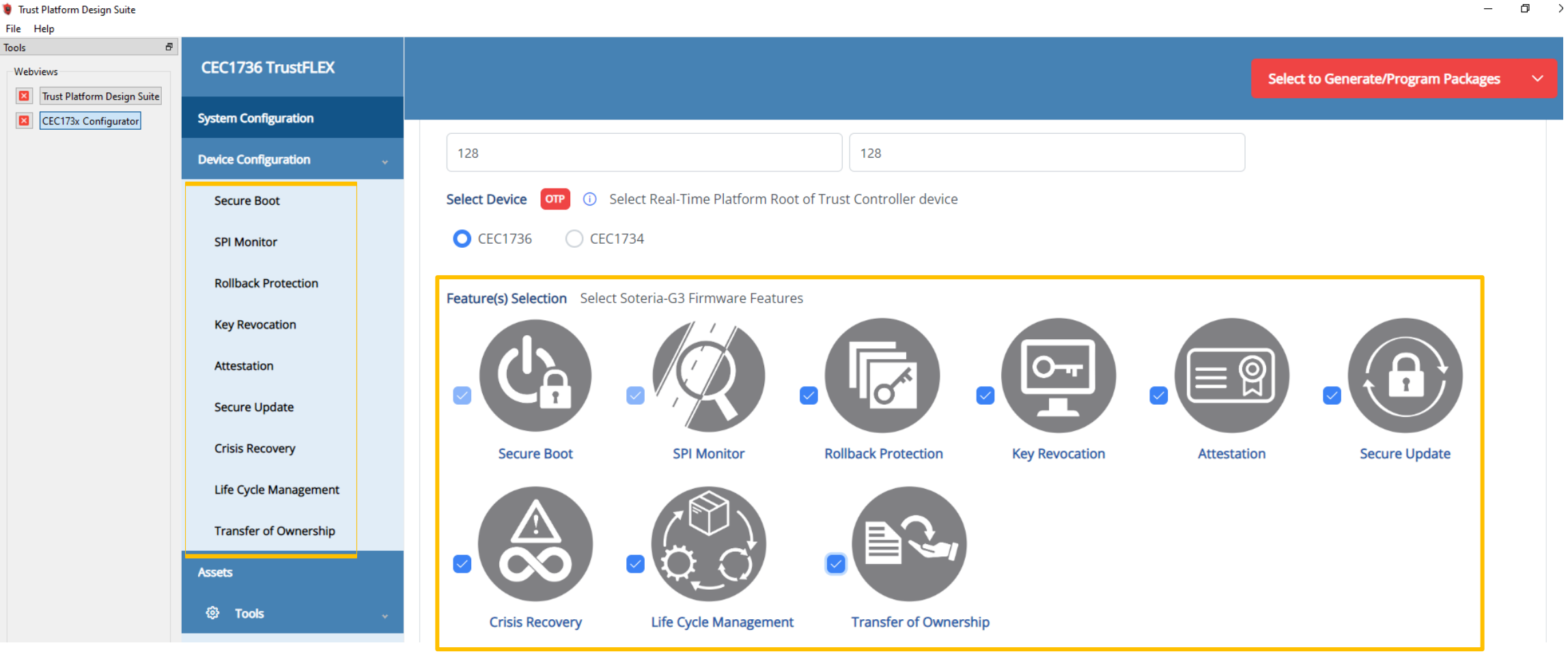
Lead Time For Additional Quantities. Order Now to Secure
Additional quantities estimated to ship by 17-Jun-2024

Delivery and scheduling options available in the cart

Quantity | Add to Cart

MICROCHIP

Evaluate select Use Case(s)



Thank You-