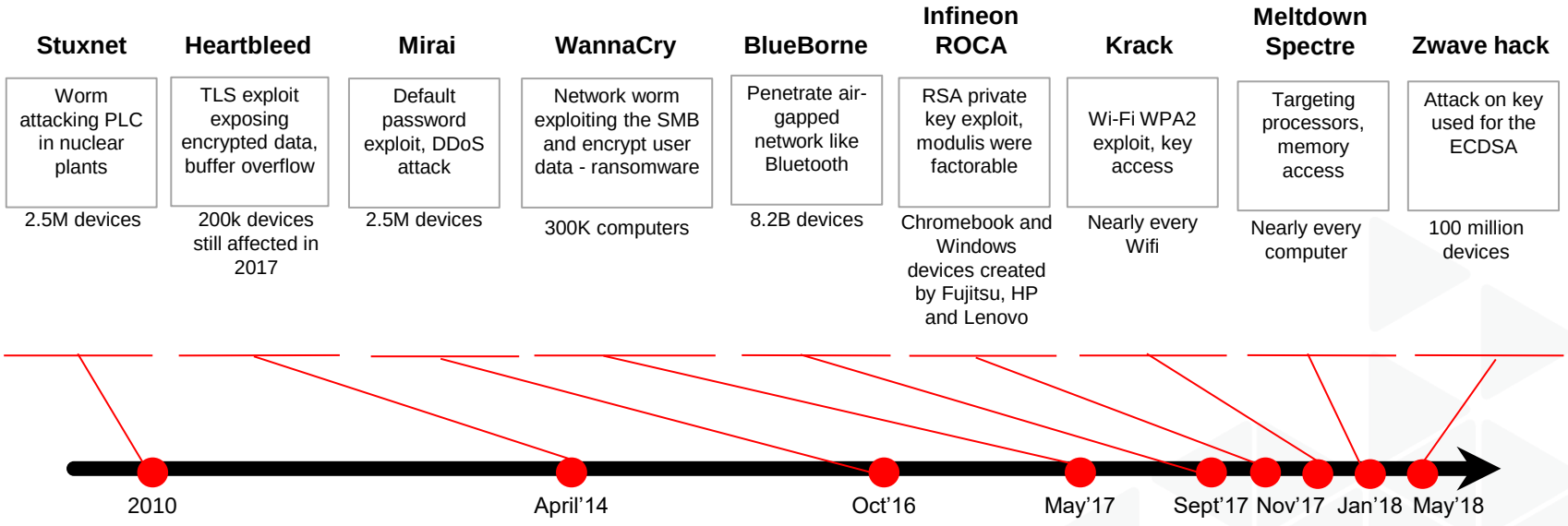
Trust Your Firmware: Secure Boot for Application Processors

Presenter: MJ Kwon, Senior Embedded Solutions Engineer

MICROCHIP

Acceleration in Attacks:



The increase in connected devices accelerates hackers' interests

MICROCHIP

The Impact

Your brand

Your Company

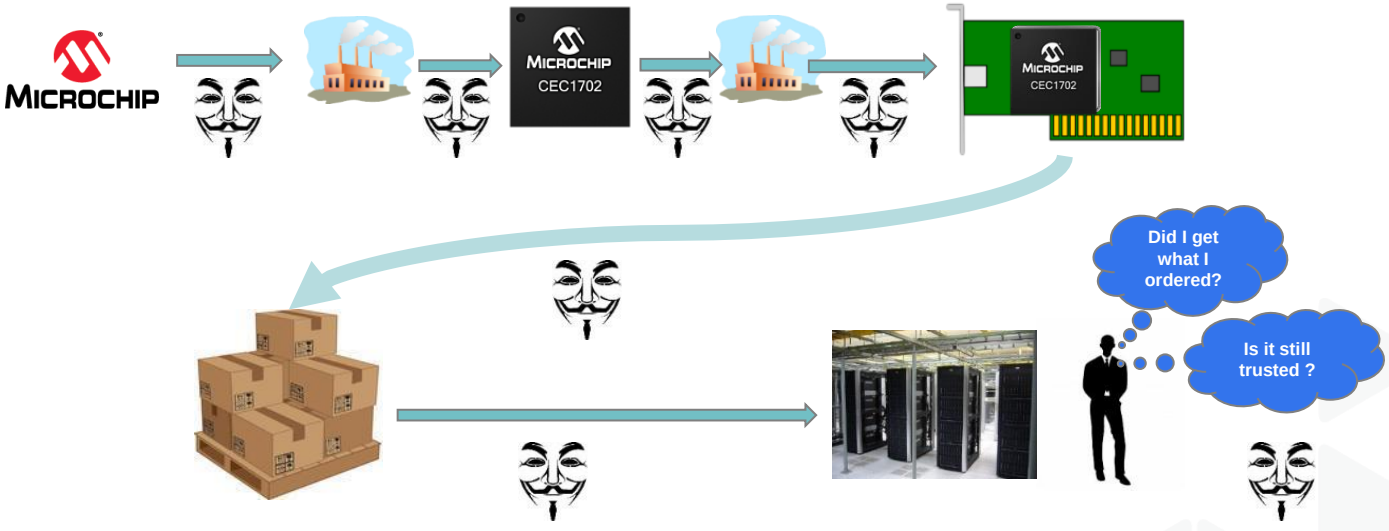
Your Revenue

Your IP

Your Customers

MICROCHIP

Trusted Platforms – Why the need?



- Various Points of entry
- Where has the product been ?
- Is it really the expected product?
- Was it intercepted in flight ?

- Is it running altered firmware / hardware ?
- Does it contain the intended components ?
- Will it stay that way ?
- Is the product genuine ?

Security Threats Along the Way of Manufacturing & Deploying

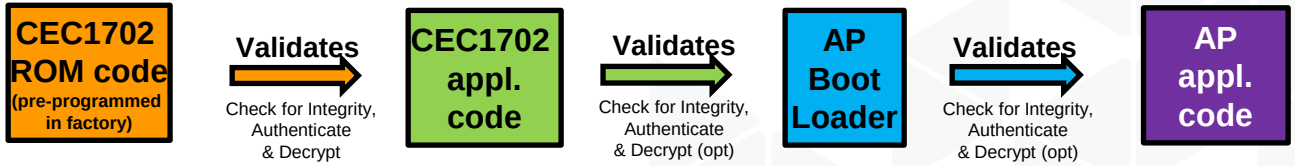
MICROCHIP

What is Secure Boot?

- Silicon HW Root of Trust
- Security begins with the Root of Trust
  - Embedded Signing Keys
  - Strong Hashing Functions
  - Immutable Authenticating Boot logic in Silicon Boot ROM
- Board Components enablement and Security
  - Trust is extended by verifying the authenticity and integrity of FLASH content prior to executing it
  - Digital signatures are supplied with all Firmware and Configuration Binaries
  - Validated with Embedded ASIC signing keys
  - ASIC Calculated hashes are computed against the stored images and compared with stored signatures.

- Why is Secure Boot Important?
  - Protects a system against threats before they can attack or infect it
  - System boots using only software trusted by the manufacturer
  - Prevents malicious software (i.e Root Kits) from loading during system start-up process

Root of Trust



MICROCHIP

CEC1702 Crypto Embedded Controller

Product Features

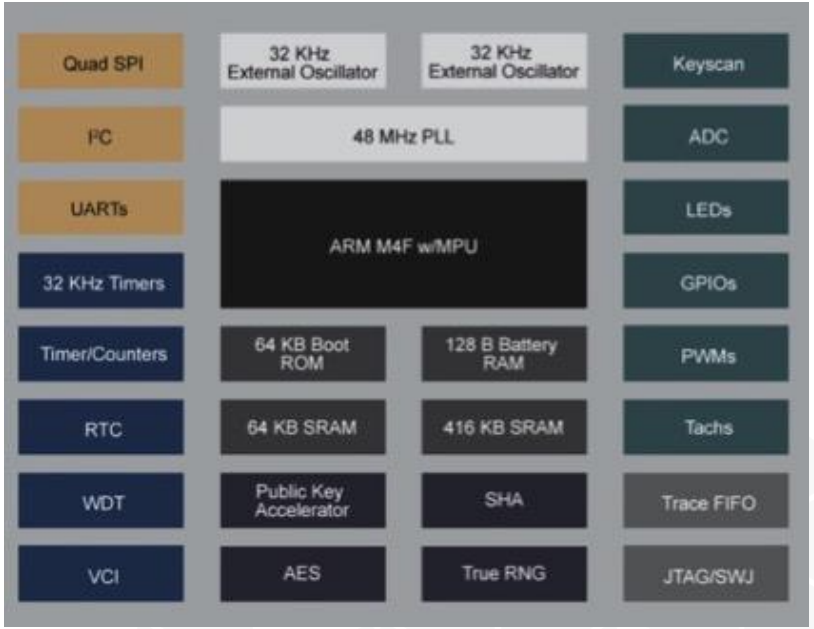
- ARM® Cortex®-M4F microcontroller
- 480KB SRAM: Code + Data
- 64KB Boot ROM
- Fast, hardware based cryptography cipher suite
- Robust HW Crypto Cypher Suite
- ECDSA, EC-KCDSA, Ed25519
- 2.5K bits User Programmable OTP

Typical Applications

- Secure Boot of Application Processors
- Industrial IoT Connected Devices

Differentiators

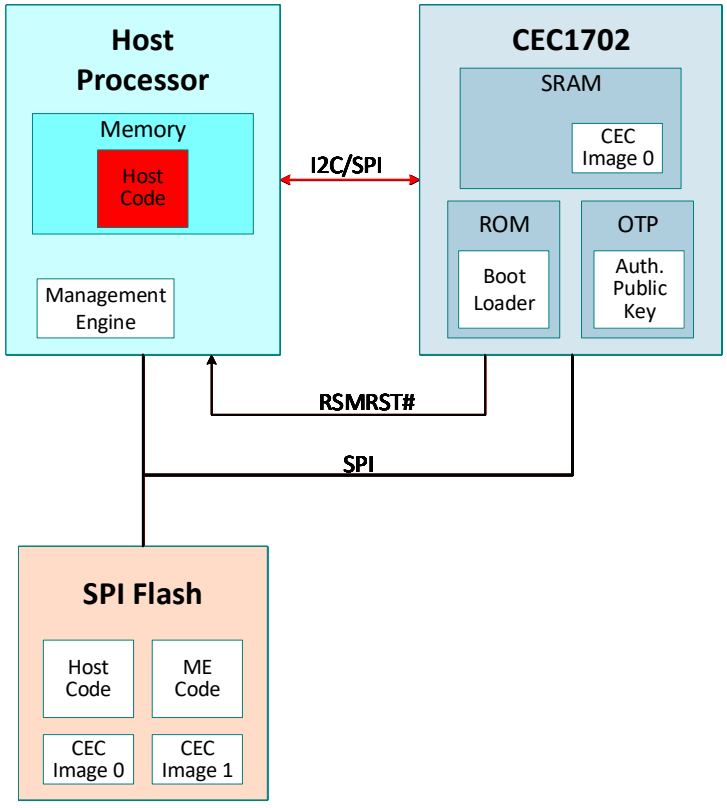
- Secure boot provides a immutable chain of trust



CEC1702 can be used for secure boot and to authenticate subsequent code loaded/running on CEC1702 or other devices in the system (field upgrades)

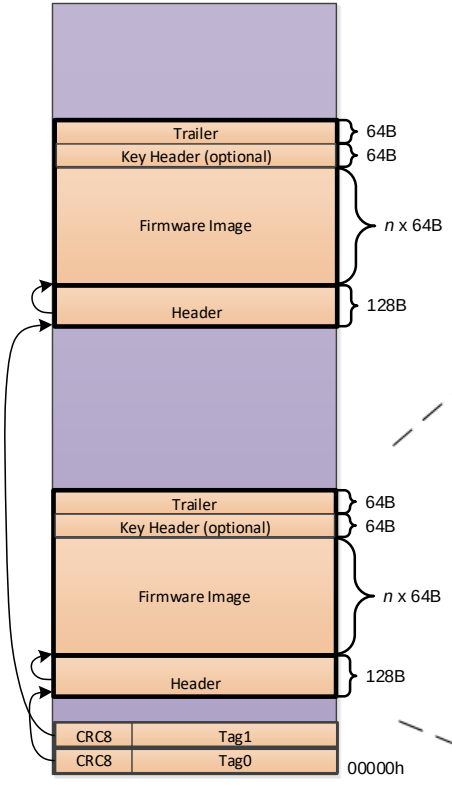
MICROCHIP

Hardware Root of Trust



- Code execution starts with the ROM
  - Hardware based: Trusted immutable code (Boot Loader)
  - Cannot be modified remotely
  - Creates a Root of Trust
- SPI Flash
  - Application code, signed by OEM's private key, is stored in SPI Flash (CEC Image 0 & 1)
  - Host code, signed by a private key, is also stored in the SPI Flash
- At power-on, the Boot Loader
  - Holds Host Processor in reset
  - Loads CEC1702 Application Code from SPI Flash into SRAM and
  - Authenticates CEC1702 Application Code using public key stored in CEC1702 OTP
- The authenticated CEC1702 Code
  - Starts execution
  - Authenticates the system Host code in SPI Flash with a public key in CEC1702 code
  - Releases the Host Processor from reset
- The Host Processor then loads and executes its authenticated code from SPI Flash
- Chain of Trust is now extended to
  - CEC1702 Application Code
  - Host code
- The Host Processor can also use the CEC1702 as a crypto-coprocessor

SPI Flash Image Structure

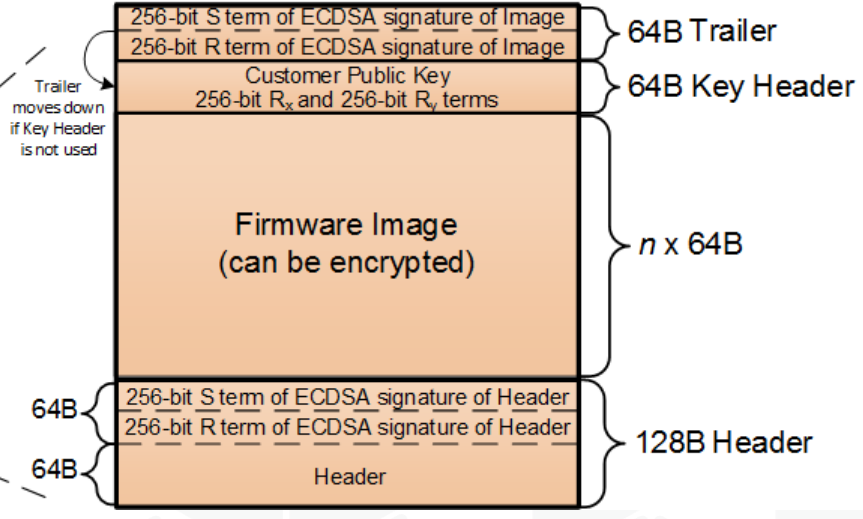


Note – SPI Flash contains two images of CEC1702 code:

Tag0

Tag1

Expanded view of FW image

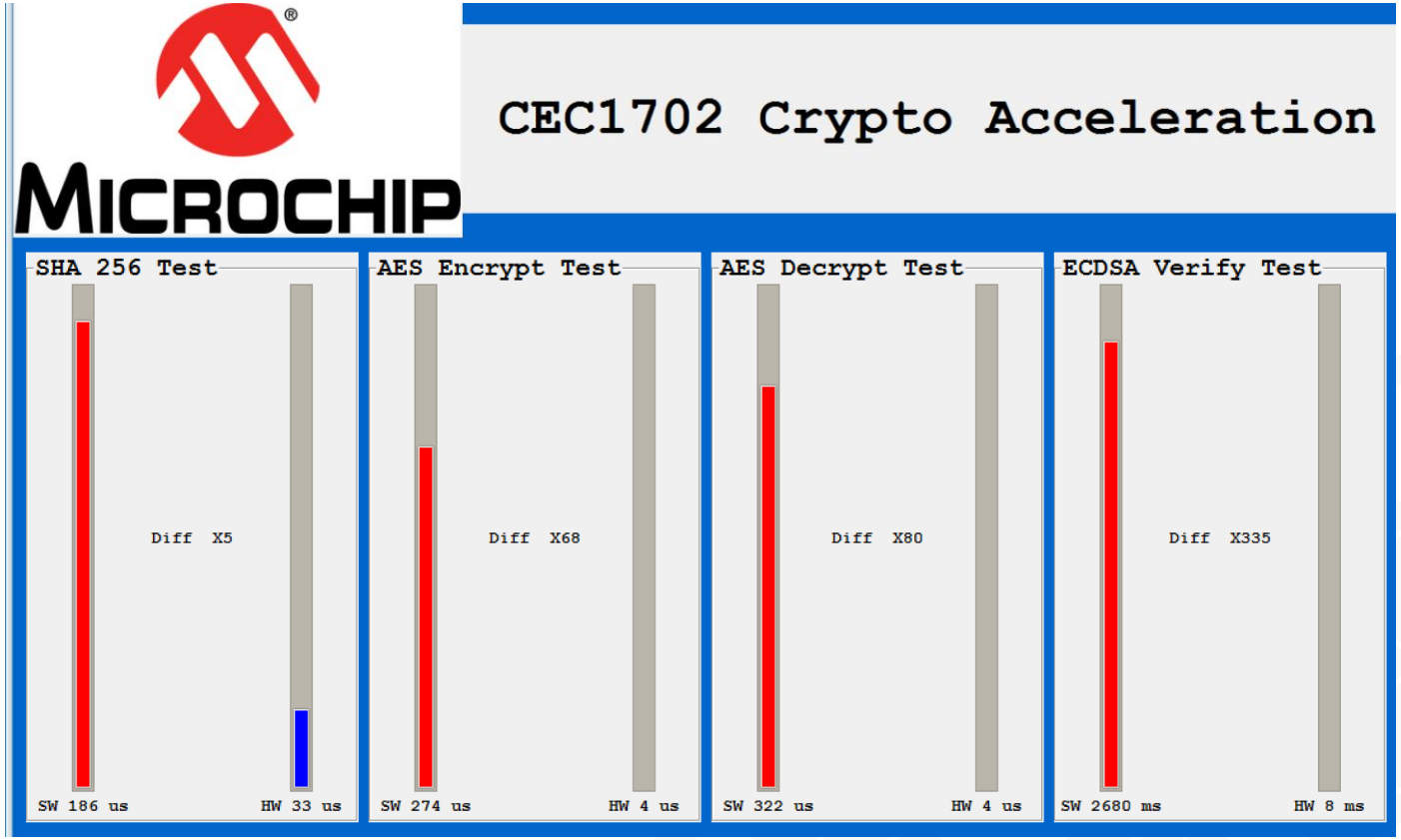


CEC1702 HW Crypto Cipher Suite

	CEC1702
Symmetric Encryption – runs @ 48MHz	AES128, AES192 and AES256
	Modes: ECB, CBC, OFB, CFB, CTR
	One cycle per byte
	100x faster than FW
	Saves up to 8KB-15KB code
Hashing – runs @ 48MHz	SHA-1, SHA-256, SHA-512 (programmable 224 and 384)
	One cycle per byte
	100x faster than FW
	Saves up to 2KB code
Public Key Engine (PKE) – runs @ 96MHz	20x-50x faster than FW
RSA	RSA-1024 to RSA-4096
ECC	Keys with 192 to 640 bits in GF(p) – programmable Keys with 160 to 640 bits in GF(2m) – programmable Curve25519 (ECDSA support) – example, also support BP, etc.
DSA	ECDSA, EC-KCDSA, Ed25519
Other	Secure Remote Password (SRP) Modular Arithmetic Primitives Miller-Rabin Primality Testing
Random Number Generator	True RNG
	1K FIFO for pre-calculation
Monotonic Counter	Yes
User Programmable OTP (in addition to key space)	2.5K bits
Memory Protection Unit	Yes

MICROCHIP

Benefit of HW Crypto



CEC1702 CAVP Validations

Cryptographic Algorithm Validation Program (CAVP)

- In July 1995, NIST and the Communications Security Establishment Canada (CSEC) established the Cryptographic Algorithm Validation Program (CAVP)
- This program focuses on validation testing for NIST recommended, and FIPS 140-2 approved cryptographic algorithms

CEC1702 has received CAVP Validation #s:

- C592: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=10951
- SHS3823: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/Details?validation=2091

Algorithm Capabilities Validated:

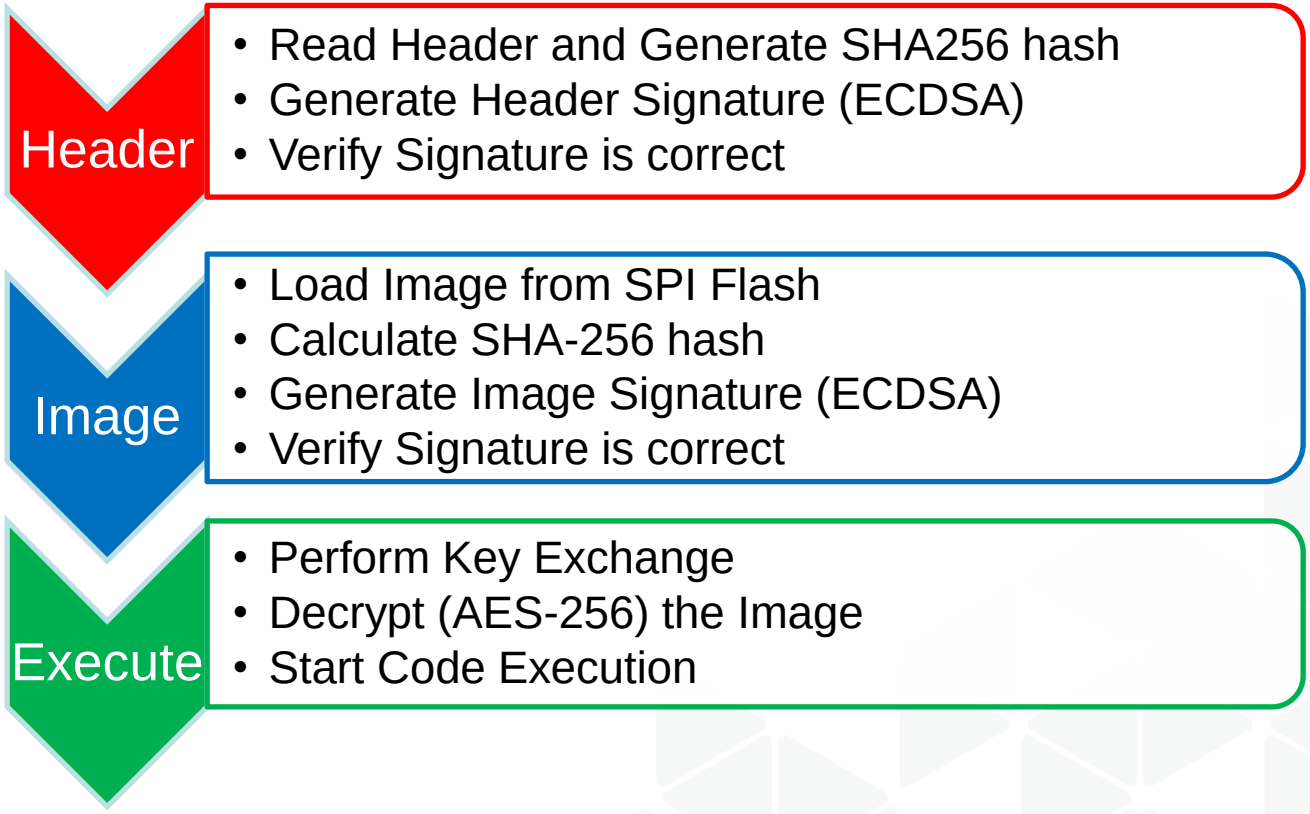
AES-CBC	Counter DRBG	KAS-ECC CDH-Component	SHA-1
AES-CFB128	ECDSA KeyGen (186-4)	RSA KeyGen (186-4)	SHA-224
AES-CFB8	ECDSA KeyVer (186-4)	RSA SigGen (186-2)	SHA-256
AES-CTR	ECDSA SigGen (186-4)	RSA SigGen (186-4)	SHA-384
AES-ECB	ECDSA SigGen (186-4)	RSA SigVer (186-4)	SHA-512
AES-OFB	ECDSA SigVer (186-4)		

Fast Secure Boot

Read Header	
Read Header and generate SHA-256 hash	0.4ms
Verify Header Signature (ECDSA)	11.7ms
Load Image	
Load from SPI, 300K	12.7ms
Calculate SHA-256 hash	8.4ms
Verify Image Signature (ECDSA)	10.5ms
Decrypt Image	
Key Exchange	5.9ms
AES-256 Decrypt	11.9ms
TOTAL	**61.5ms**

Secure boot using firmware cryptographic functions will take ~2.5s

Image Authentication



CEC1702 & NIST 800-193

Protect

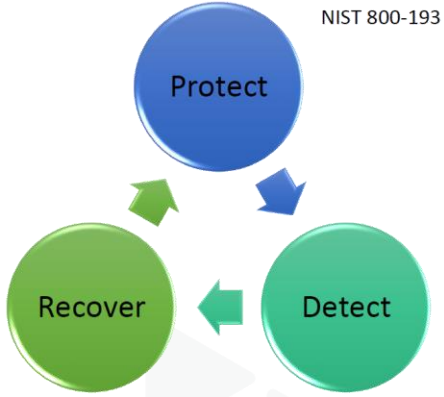
- CEC1702 will only execute Authenticated Code
- Code Update
  - Image is signed (ECDSA) by owner prior to transmittal
  - Image is written to SPI Flash – Staging Area
  - CEC1702 will authenticate the signed image update
  - After Authentication, Updated Code is written to Active Area

Detect

- All code is verified using SHA256 and Authenticated with ECDSA using P-256

Recover

- CEC1702 Firmware
  - Two code images implemented (Tag0 & Tag1)
  - Initial Boot is from Tag0
  - If Tag0 is corrupted switch and use Tag1
  - Automatically handled by Boot Loader
- Application Processor Code
  - Can support using a backup or Golden image to restore the system to a known good state if the Host code is corrupted



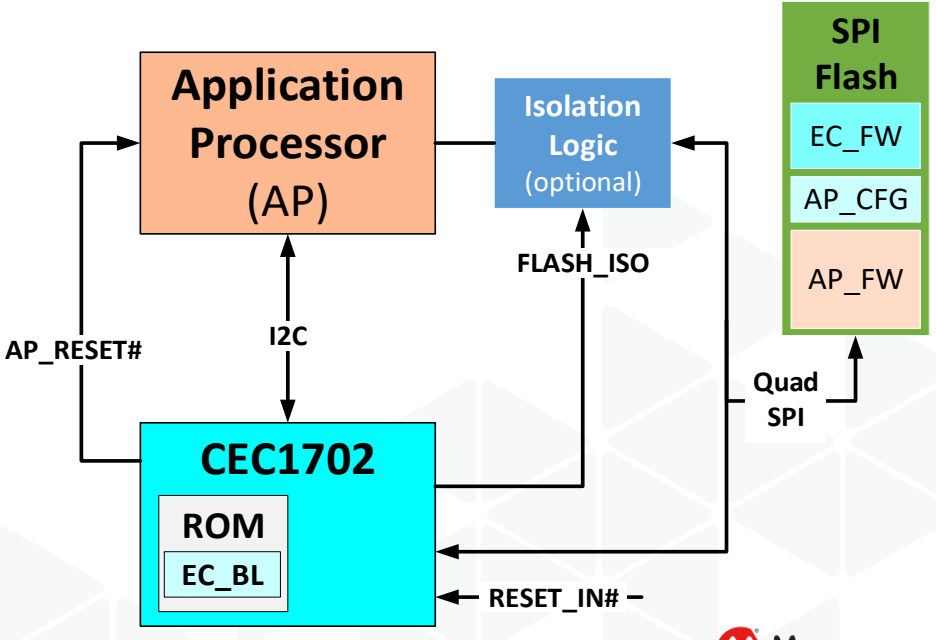
Microchip Soteria

A Microchip FW solution for Microchip CEC1702

Key Features

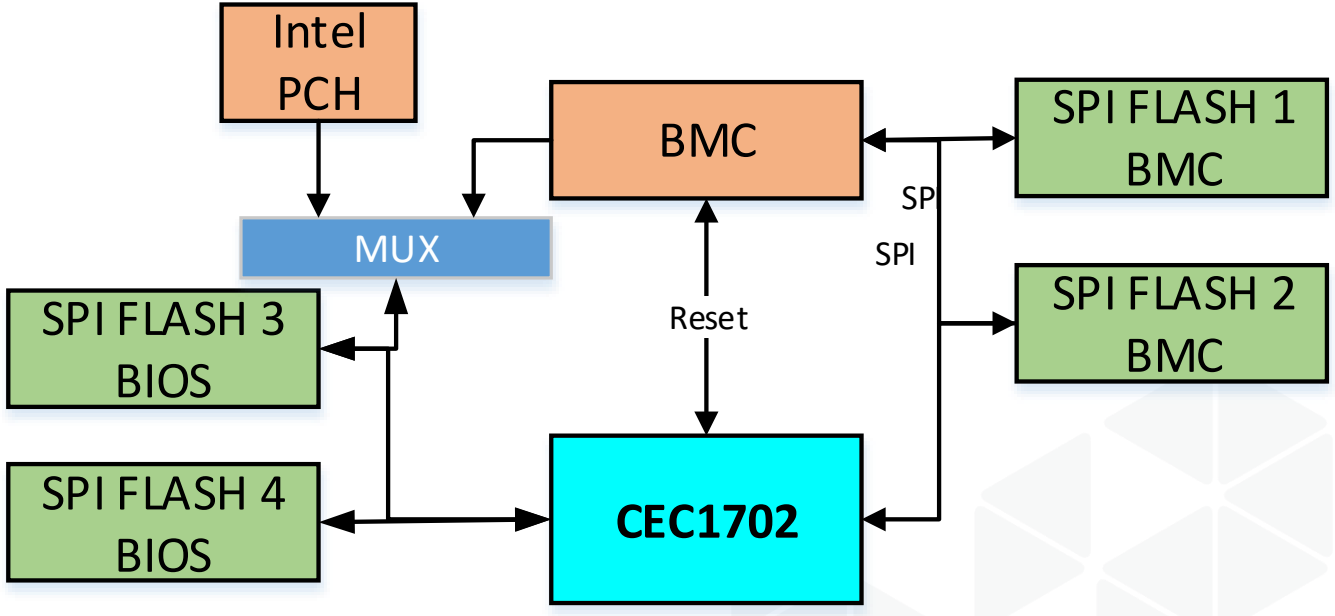
- Secure Boot / Platform-RoT
- Pre-boot Authentication of AP FW
- Authentication of FW Updates

User Configurable and Customizable



Soteria Scalability

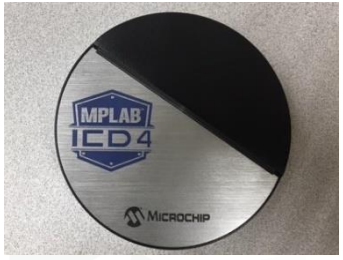
Soteria scales to multiple APs with multiple SPI-flash



Development Tool Support

CEC1702 is supported by Microchip's award winning MPLAB development tools

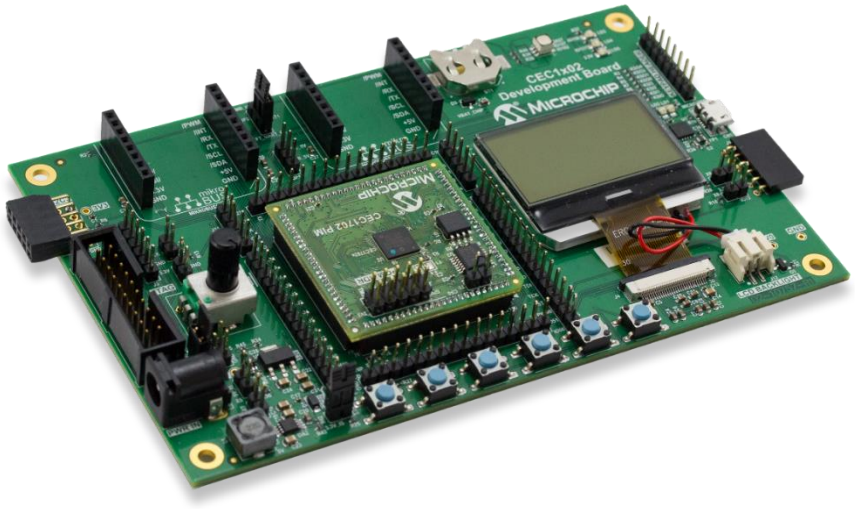
- MPLAB X32 Compiler
- MPLAB REAL ICE in-circuit emulator
- ICD 4 in-circuit debugger



Also supported: Keil, IAR, ARM GCC and Seggar IDE

MICROCHIP

CEC1702 Development Board



- The CEC1702 Development Board is an evaluation board that can be used for development, customer evaluation and demos.
- Customers can evaluate and program keys used for authentication into the CEC1702 devices.
- The packaged CEC1702 Development Board includes the base board and a CEC1702PIM.

Available on MicrochipDirect

Part Number: DM990013
Price: $125 USD

MICROCHIP

CEC1702 Support Collateral

Datasheets / Errata

- CEC1702 Datasheet & ROM Description Addendum
- I2C / SMBus Interface Core Specification
- CEC1702 Silicon Errata and Data Sheet Clarification

Application Notes

- PCB Layout Guide for CEC1702
- BSDL Models for CEC1702
- Peripheral and Crypto Library API Release Package (Users Guide)
- Secure Provisioning Release Package (Utility and Users Guide)

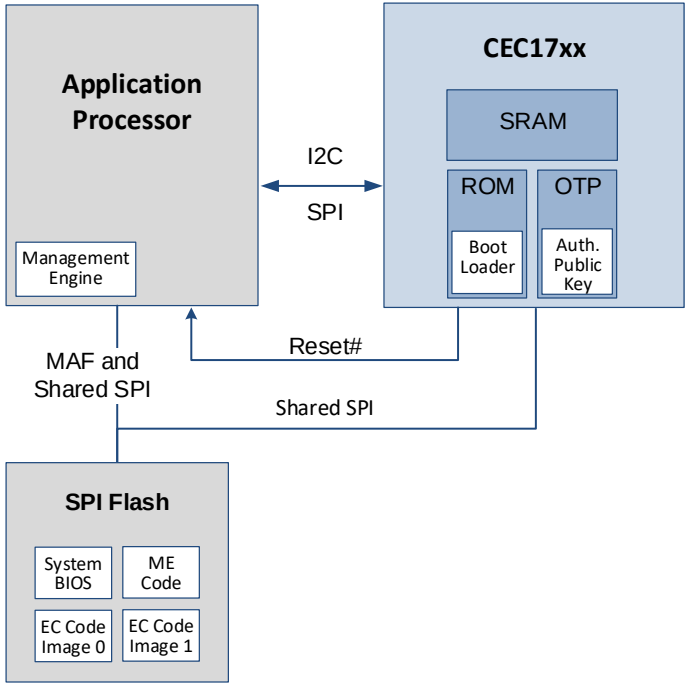
Software and Sample Code

- Blinking LEDs Sample Code by mikroE sample project
- CEC1702 CLIB/PLIB Release
- CEC1702 mikroE SDK (update April 2019)
- AWS IoT SDK for CEC1702
- Azure DICE IoT SDK for CEC1702
- Masters Hand-On Training Class Package
- ECC508 Sample Code and App Note

Utilities

- SPI Image Generators
- eFuse Generator Utility for CEC1702
- Secure Firmware update Utility for CEC1702

Summary



- Hardware Root of Trust – Secure Boot Solution
- Secure any processor using SPI flash
- Boot Rom Authenticates CEC17xx code in SPI Flash
- CEC17xx code authenticates Application processor code in SPI flash
- All authentication prior to code running
- Authentication at every power cycle
- CEC1702 Meets NIST Guidelines

www.microchip.com/CEC1702