

ARM KNOWLEDGE LAB 2026 DESIGNING THE FUTURE

DAY 1

Secure Your Edge Devices with PSOC™ Edge Protect Software
Trevor Martin, Hitex UK

Arm Knowledge Lab: Three short and compact sessions



Day 1

Secure by Design – From
Threats to Trusted Devices



Day 2

AI at the Edge – Building
Smarter Embedded Systems

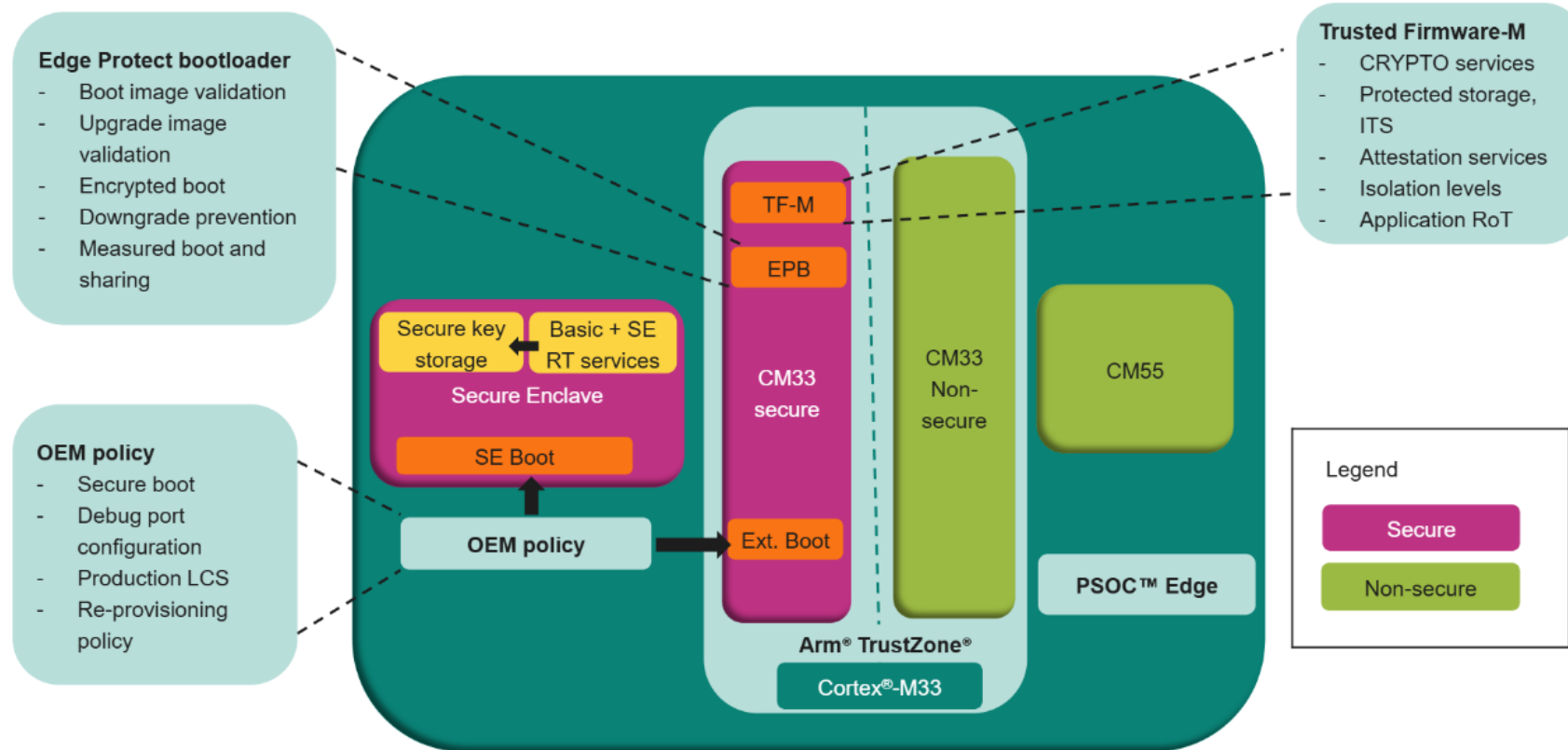


Day 3

Safety-Critical Systems –
Engineering Reliability

Find more presentations from our Arm Knowledge Lab:
<https://www2.hitex.com/arm-knowledge-lab-2026-download>

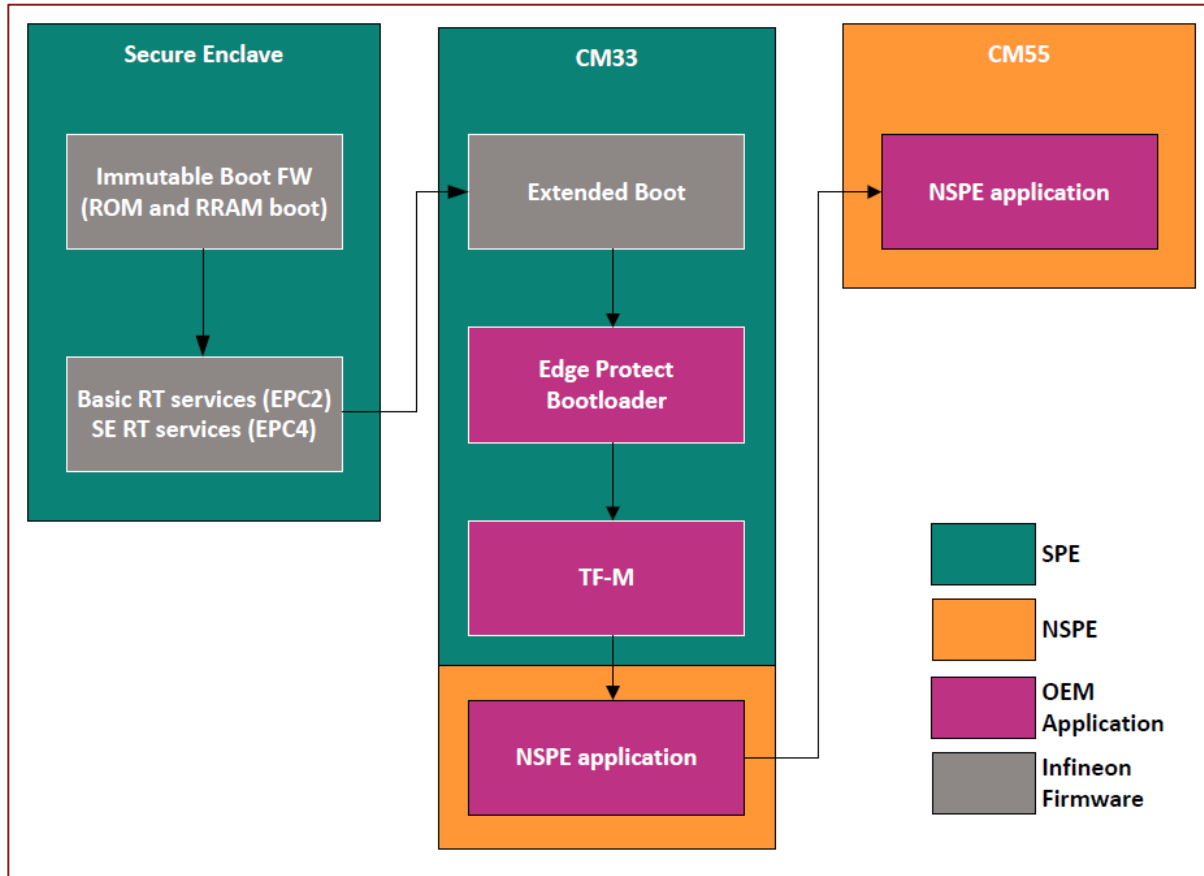
PSOC Security Architecture



- Infineon Edge Protect
 - Tools
 - Firmware
 - Examples

For complete device security

Boot Sequence



– Secure Enclave

- Starts Cortex-M33 and Extended Bootloader

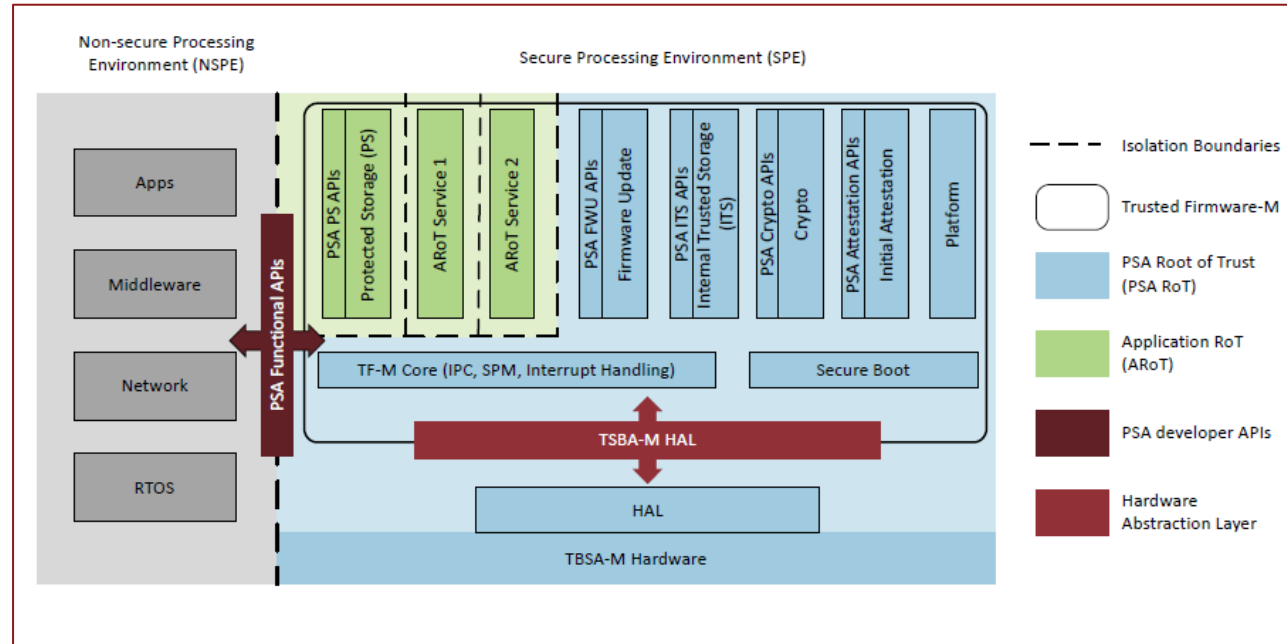
– Cortex-M33

- Extended boot validates one image
- Edge Protect Bootloader

– Edge protect bootloader

- Validates remaining images
 - Cortex-M33 SPE
 - Cortex-M33 NSPE
 - Cortex-M55
- Starts Cortex-M33 NSPE application
 - Which in turn starts
- Starts Cortex-M55 NSPE application

PSA Trusted Firmware



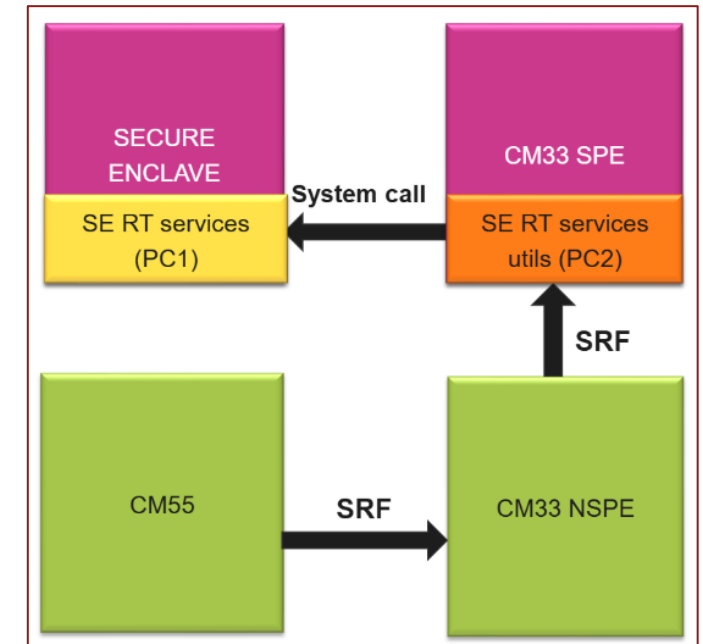
Runs on Cortex-M33 in Secure processing Environment SPE

- Provides Security Services to the NSPE
 - Cryptography
 - Secure Storage
 - Attestation
 - Keystore
- Integrated with Crypto Accelerator

Secure Enclave Run Time Services

Edge Protect Category (EPC) 4 devices provide an additional set of services called secure enclave runtime services

- (SE RT_Services), which include
 - CRYPTO service
 - Key management service
 - Protection service
 - Attestation service
 - System management service
- SE RT services utilities library is a set of utility code that
- provides an interface to SE RT services
 - SE RT services utilities can be accessed from the CM33 SPE application



Configuration tools

Modus Toolbox

- Compiler
- IDE
- Debugger

Configuration apps

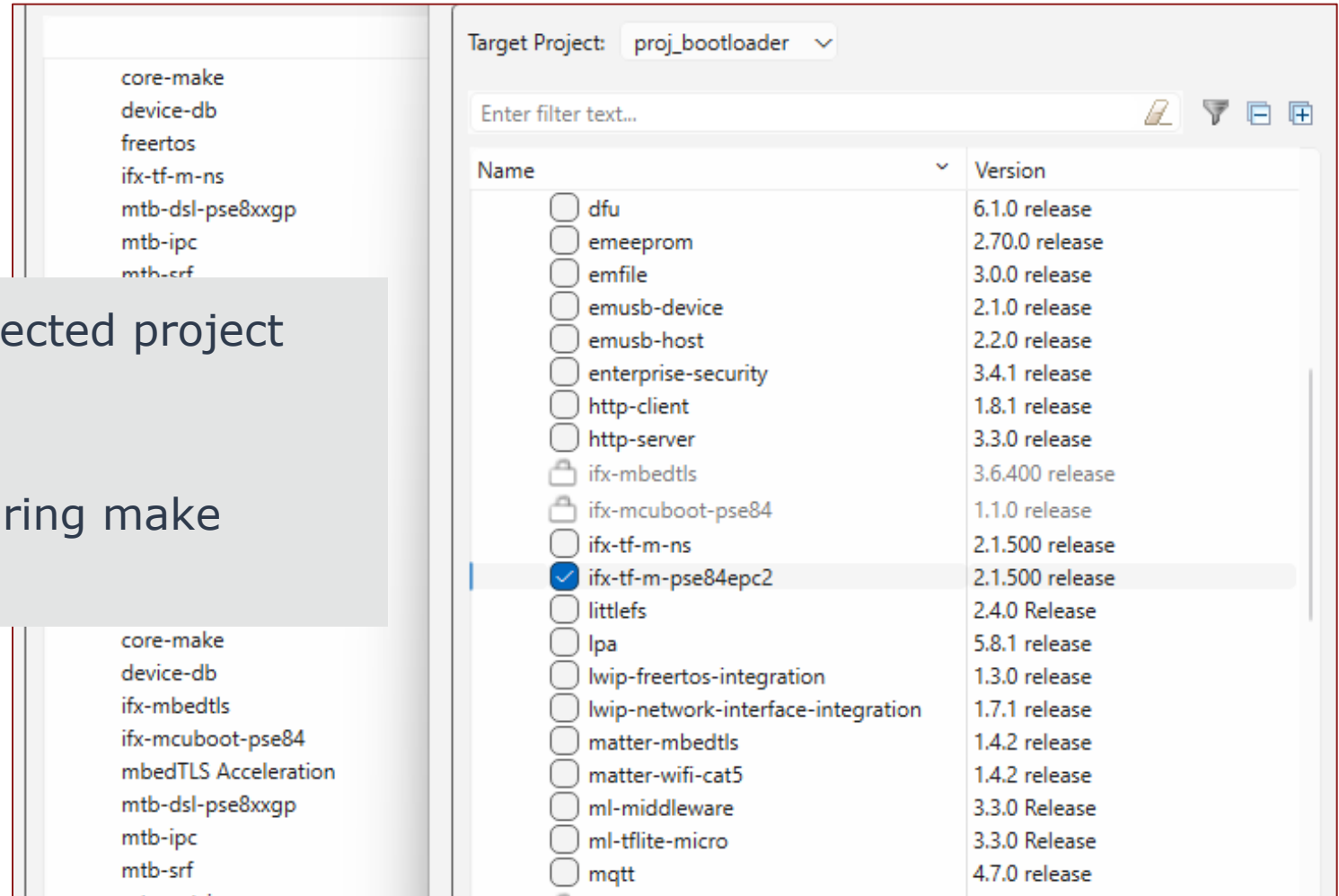
- Device
- Security
- Machine Learning

- Library manager (Software components)
- Edge protect Security Suite

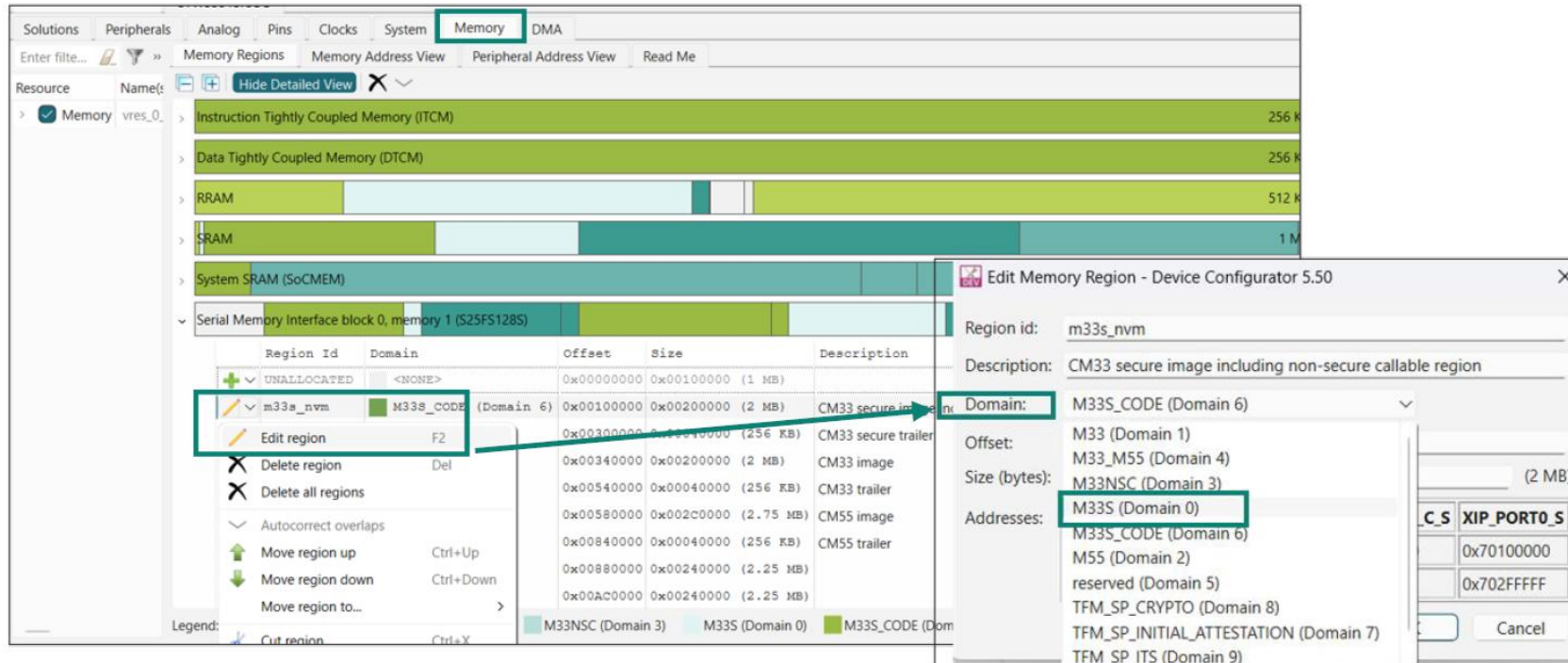
Library Manager



- Add software components to selected project
- Adds URL to a github repo
- Downloads and builds source during make process



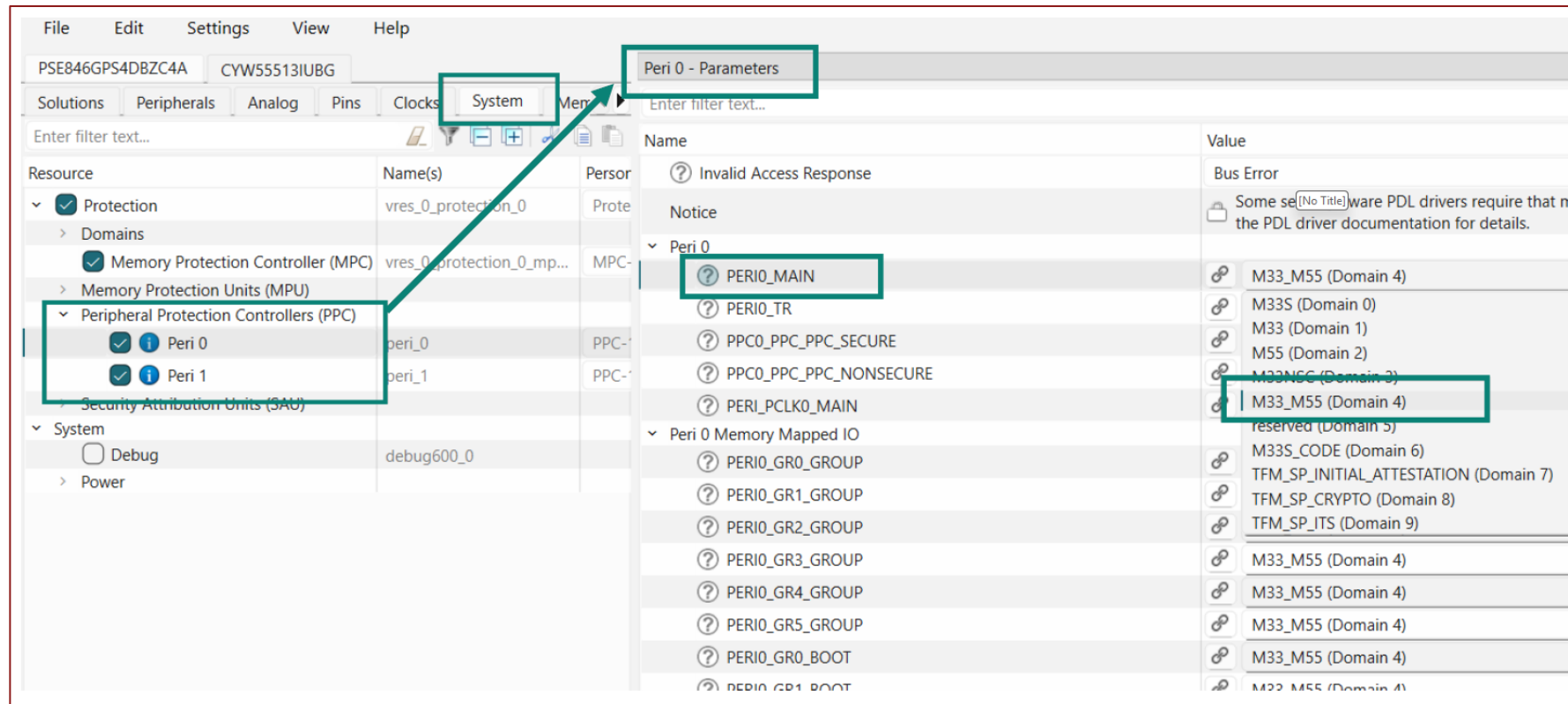
Device Configurator



Memory configuration

- Defines security domains
- Create memory regions and allocate them to a domain

Peripheral Protection Units



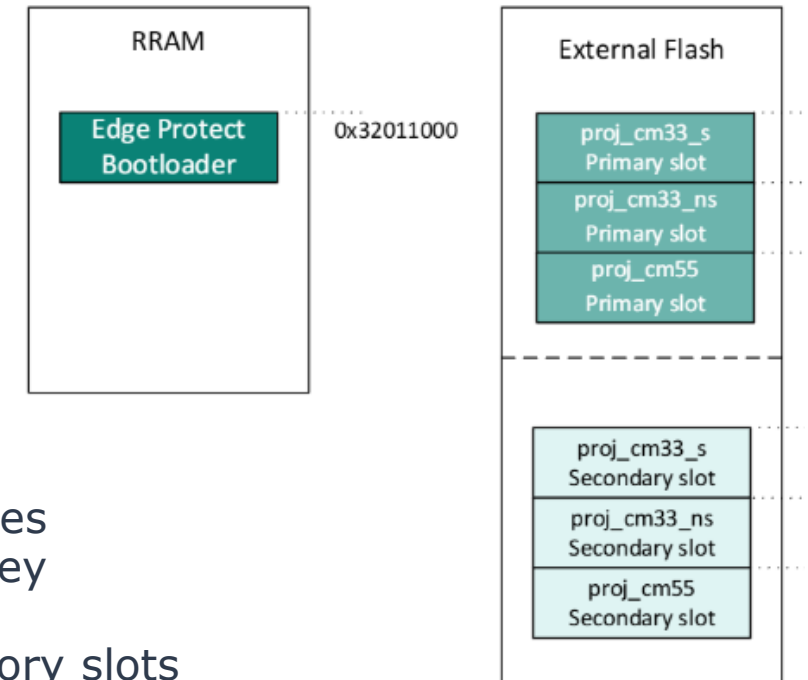
PPU allocates a peripheral to a Security Domain

- Peripheral register access

Edge Protect Bootloader (MCU boot)



Edge Protect Bootloader Solution - Parameters - Device Configurator 5.70		
Enter filter text...		
Name	Value	Notes >>
Documentation		
Edge Protect Bootloader documentation	Edge Protect Bootloader Solution Personality Overview	
MCUBoot config		
Upgrade mode	overwrite	
Logging level	dbg	
FIH level	off	
Image count	3	
Validate boot slot	☒	
Validate upgrade slot	☒	
Measured boot	☒	
Measured Boot		
Max boot record size	0x200	
MCUBoot shared data region	m33s_shared (Memory Region 10)	
HW rollback protection	☒	
Dependency check	☒	
SW downgrade prevention	☒	
Encryption		
Image encryption	XIP encryption single AES key (+ ECIES P256)	
Public Key Encryption Key(KEK) path	../keys/enc-ec256-pub.pem	
AES128 Data Encryption Key(DEK) path	../keys/aes128_key.bin	
NONCE output file path	../keys/nonce.bin	
Stage SE RAM App	☐	
Watchdog	☐	
Bootloader Configuration		
Bootloader project name	proj_bootloader	
Input hex file path	../build/project_hex/proj_bootloader.hex	
Output hex file path	../build/project_hex/proj_bootloader_signed.hex	
OEM private key path	../keys/oem_private_key_0.pem	
Bootloader image version	1.0.0	
Bootloader image boot record	proj_bldr	
Bootloader NVM Region	☒	
Bootloader SRAM load	☐	
Enable Bootloader Signing	☐	



Defines

- MCU Boot features
- Authentication key
- Encryption keys
- Secondary memory slots

OTA Update Library

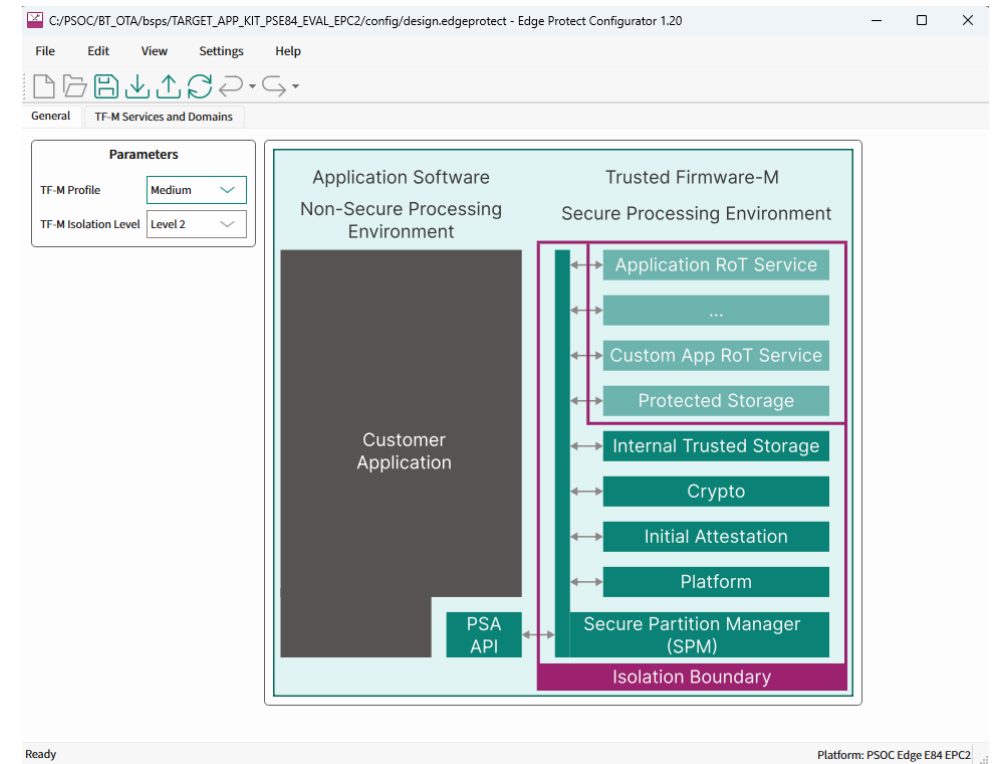
Support library and utilities for OTA Updates

- Examples for Bluetooth HTTP, MQTT and UART
 - Download Python scripts
- Supports Push and Pull models

Edge Protect Configurator



- Security Configuration
 - Configures
 - TrustZone SAU
 - Trusted Firmware
- Supports addition of custom SPE service



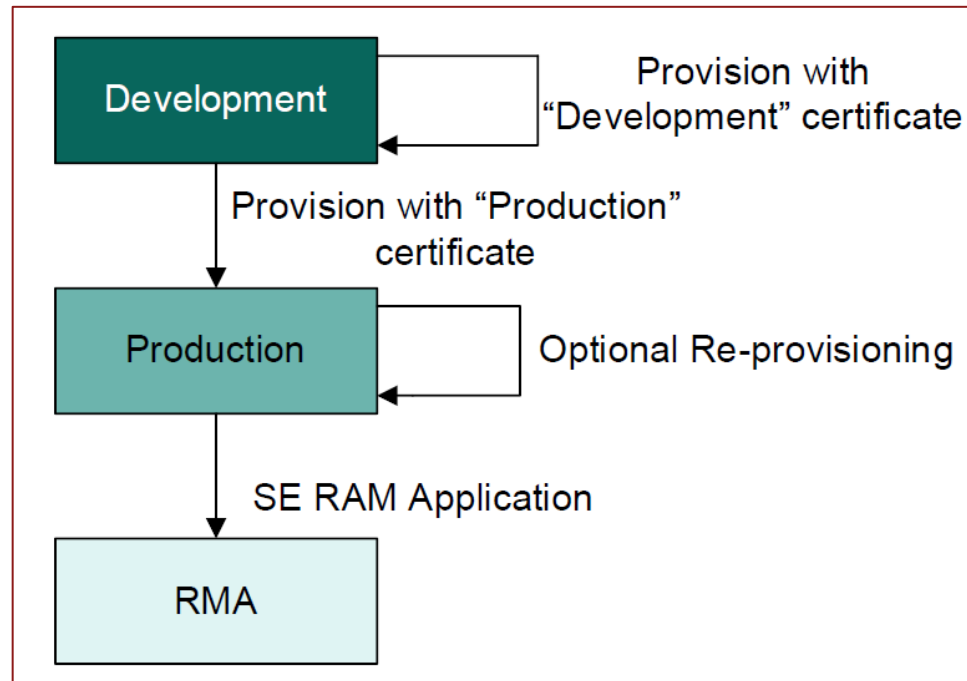
Edge Protect Tools

- ModusToolbox™ Edge Protect Security Suite
- Command Line Utility
- Capabilities
 - ROT Key generation
 - Image signing and encryption
 - Provisioning the device
 - Factory reset
 - Device integrity check
- Communicates with the target device over serial or SWD interfaces

Debug

- Authenticated Debug
 - Can grant different access levels
 - By processor
 - By security level
 - Invasive and non-invasive debug
 - Configured in the device policy file
- System Access port
 - Serial wire channel in addition to the debug channel
 - Allows you to modify policy file and recover the device

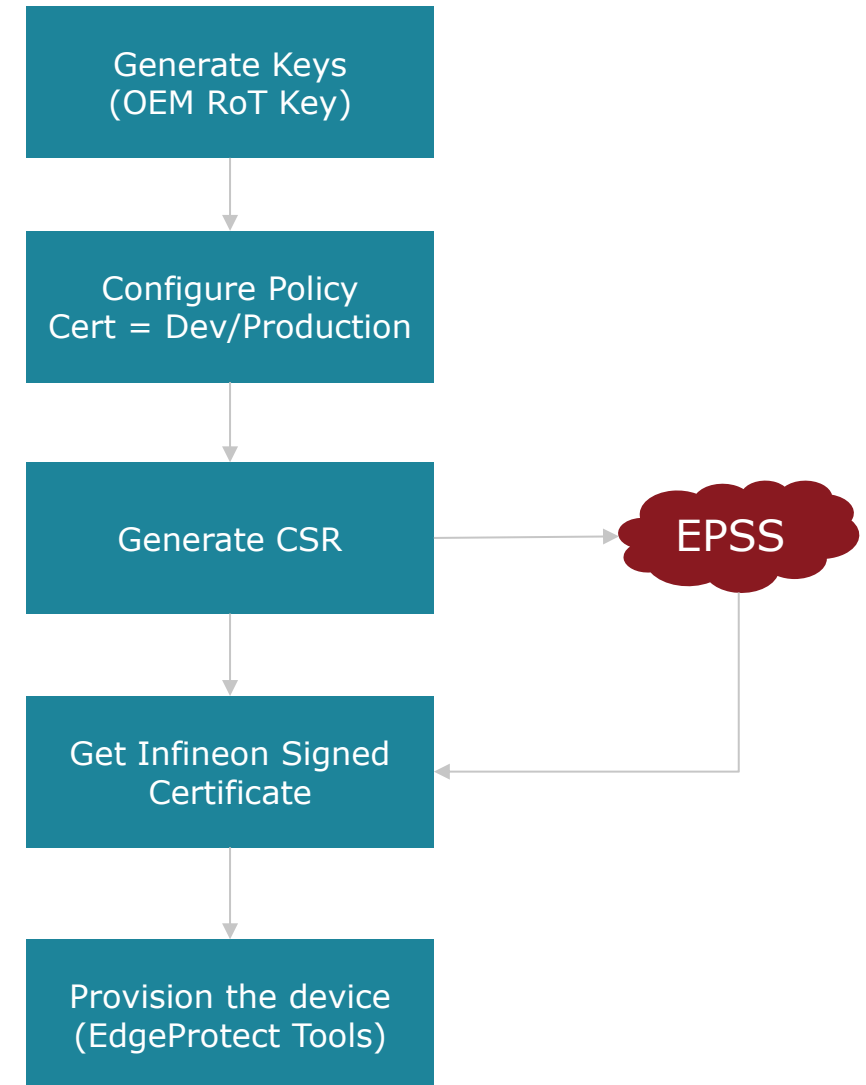
Device Lifecycle



- Supports development and production phases
 - Device cannot be bricked while in development state
- Shifts ownership from Infineon to OEM
 - Provisions OEM certificates

Device Policy file

- Defines a set of config options
 - Life Cycle Status
 - Secure boot
 - OEM_ROT_KEY
 - Debug config
 - SMIF config
 - TRNG enable
- JSON Format File
- OEM Certificate
 - Signed using Edge Protect Signing Service EPSS (online service)



Conclusion



- Full Security Model in Modus Toolbox
- Integrated with Hardware accelerators
- Multi processor design allows you to concentrate on application code
- PSA certification
 - Level 3 and Level 4

Hitex offerings ...



Ask alexander.hess@hitex.de – he looks forward to receiving your inquiries regarding Hitex offerings, including:

- Arm encryption libraries
- Security stack for Hardware Security Modules
- Support for your ISO 21434 Threat Analysis and Risk Assessment (TARA)
- Training courses for embedded systems with Arm
- SO-DIMM compute modules for PSOC™, TRAVEO™ and more for an easy entry into the Infineon MCs.

THANK YOU.
SEE YOU NEXT TIME!

Stay informed: webinars, training sessions, knowledge labs
Find all the information at www.hitex.de