Security for IoT Endpoint Devices

How standards and the Arm ecosystem can help accelerate IoT development

Reinhard Keil, Sr. Director Embedded Technology
Electronic Design – Engineering Academy

Agenda

- The Importance of IoT Security
- Potential Security Threats

Enable secure IoT with hardware isolation and software frameworks

- Arm TrustZone Hardware Isolation
- PSA Certified IoT Security Framework www.psacertified.org
- Trusted Firmware www.trustedfirmware.org

Arm Total Solutions for IoT

- Project Centauri - bringing security and compatibility to IoT
- Workshops in collaboration with AWS FreeRTOS

The Importance of IoT Security

Excerpt from the “Top 12 IoT Exploits 2021”

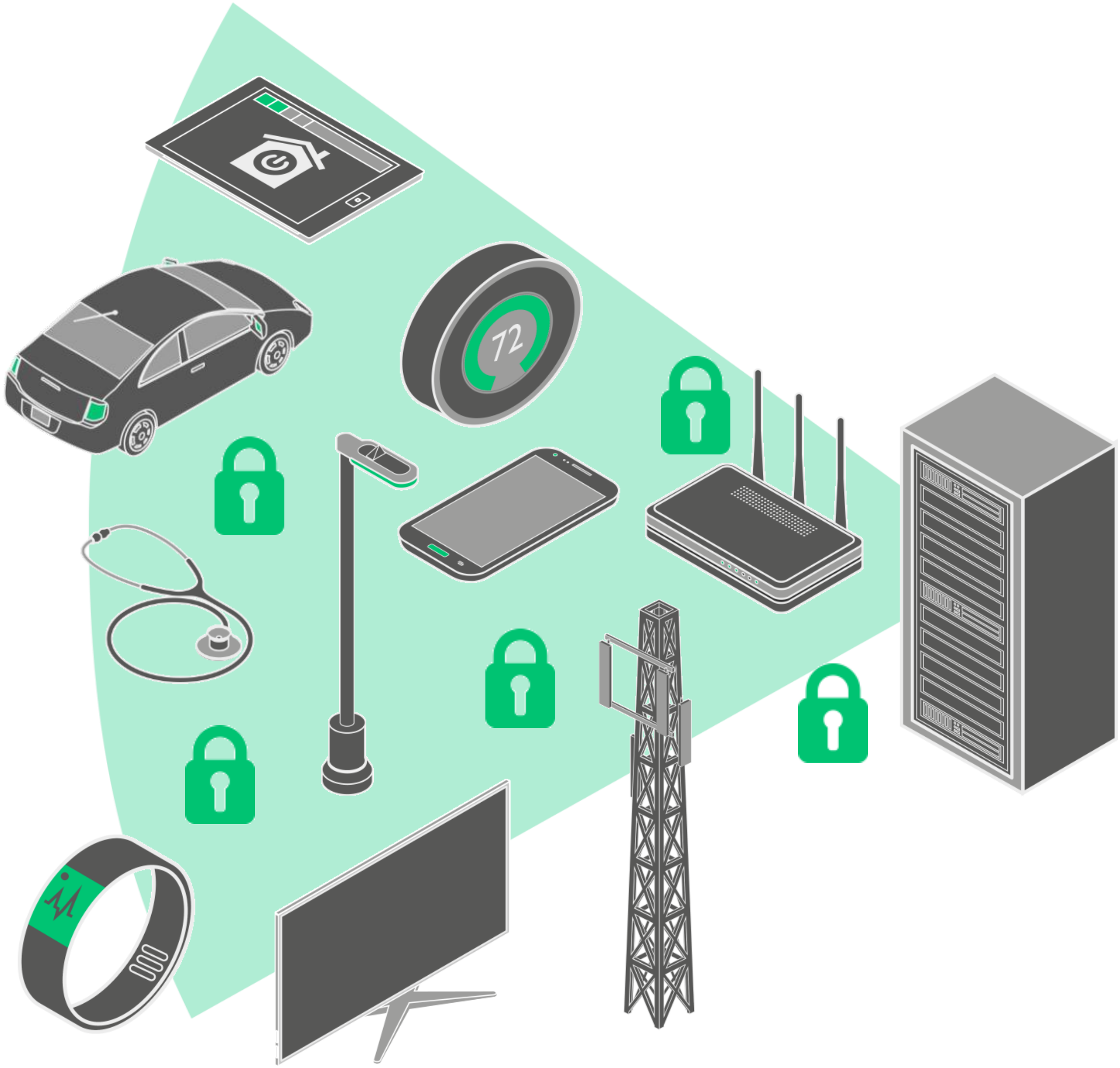
Source: https://finitestate.io/blog/top-12-iot-exploits-of-2021-p1

- **The Big One: The Apache Log4j Vulnerability -** hundreds of millions of devices are likely to be affected
- **Hard-Coded Keys: Device Vulnerabilities -** allow access to patient data and denial of service (DoS) attacks
- **Dangerous DNS: NAME:WRECK Vulnerabilities -** allow remote code execution (RCE) or DoS
- **Remote Takeover: WiFi Module Vulnerabilities -** take over without knowing the Wi-Fi network password (PSK)

Recent report from “Bundesamt für Sicherheit in der Informationstechnik” - 12. Oct. 2022

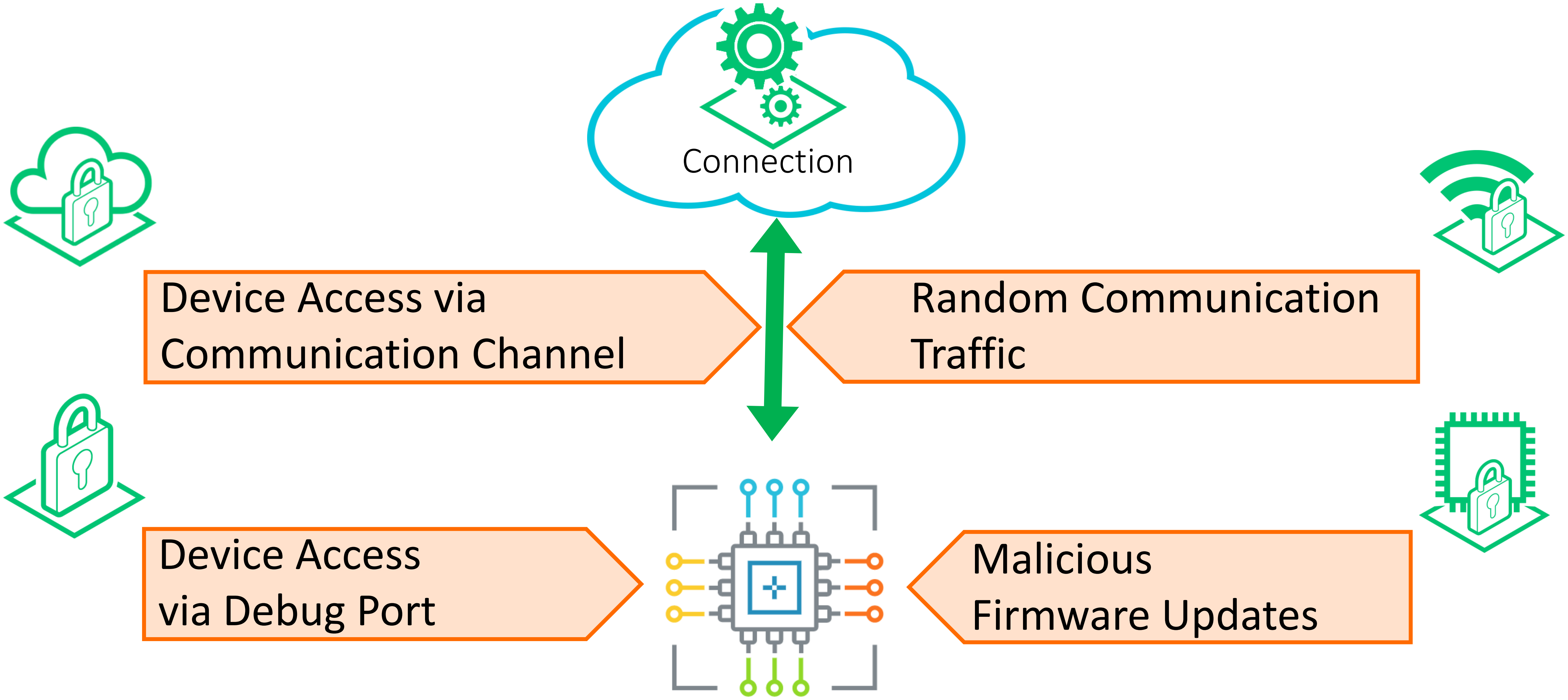
- **Critical Flaw in SIMATIC CPU Family -** outdated crypto technology gives access to control units

The Importance of IoT Security



- Communication protection
  - Cryptography, authentication
- Data protection
  - Secret data (keys, personal information)
- Firmware protection
  - IP theft, reverse engineering
- Operation protection
  - Maintaining service and revenue
- Anti-tamper protection
  - Related to all other protections

Potential Security Threats



Connection

Device Access via Communication Channel

Random Communication Traffic

Device Access via Debug Port

Malicious Firmware Updates

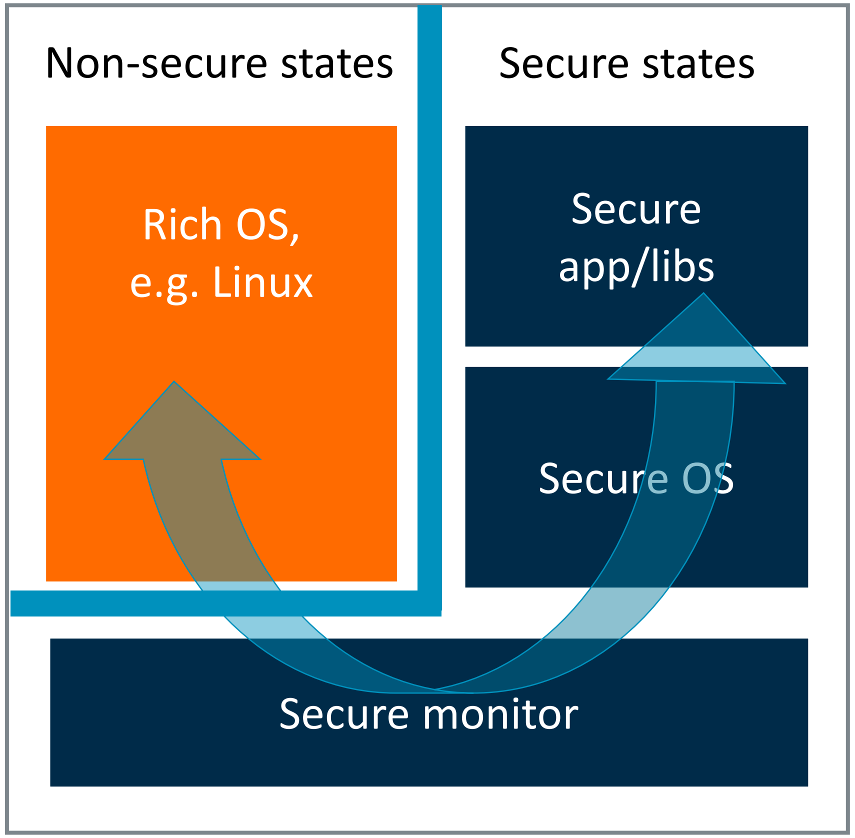
Enable secure IoT with hardware isolation and software frameworks

- Arm TrustZone Hardware Isolation
- PSA Certified IoT Security Framework
- Trusted Firmware

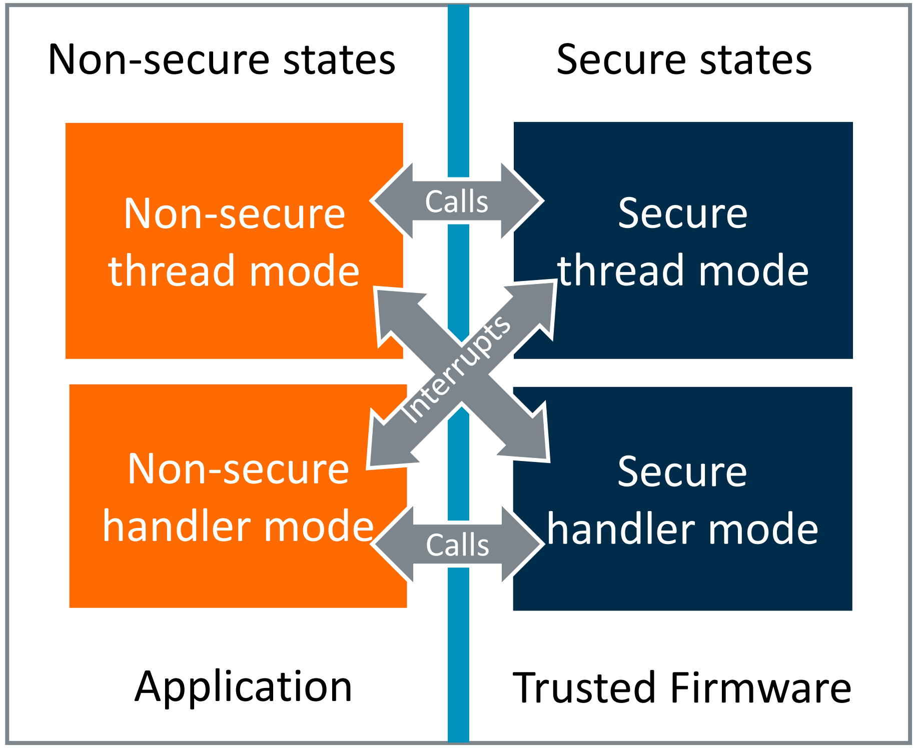
TrustZone Technology: System-Wide Security for IoT Devices

Isolation of critical security firmware, assets and private information from the application

TrustZone for Cortex-A



TrustZone for Cortex-M



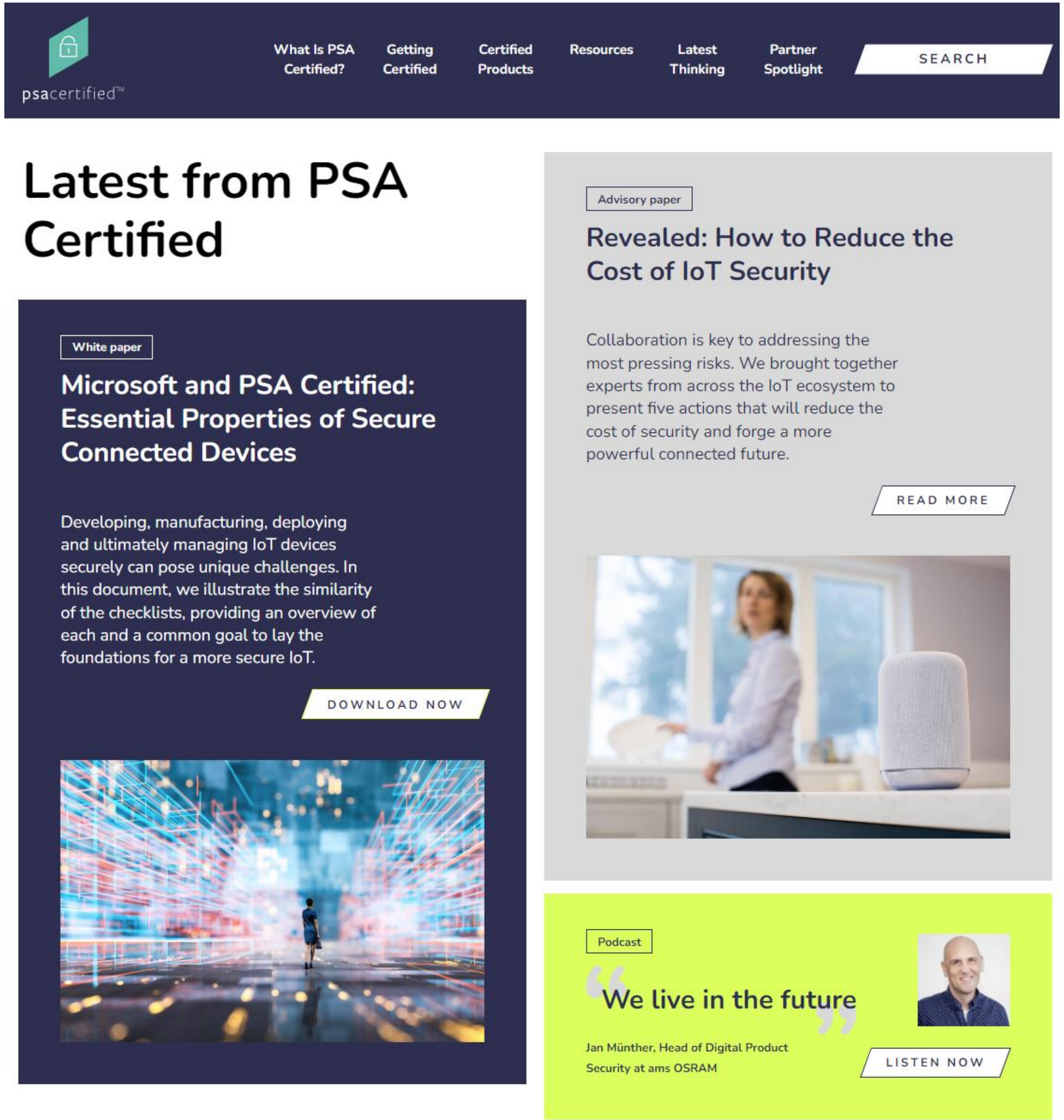
Secure transitions handled by the processor to maintain embedded class latency

PSA Certified

psacertified.org

Created in collaboration with leading industry partners

- Framework for securing connected devices
- Provides guidelines for threat model and security analysis
- Defines and standardizes PSA security APIs to reduce fragmentation
- Certification program to provide evidence



Latest from PSA Certified

White paper

Microsoft and PSA Certified: Essential Properties of Secure Connected Devices

Developing, manufacturing, deploying and ultimately managing IoT devices securely can pose unique challenges. In this document, we illustrate the similarity of the checklists, providing an overview of each and a common goal to lay the foundations for a more secure IoT.

Advisory paper

Revealed: How to Reduce the Cost of IoT Security

Collaboration is key to addressing the most pressing risks. We brought together experts from across the IoT ecosystem to present five actions that will reduce the cost of security and forge a more powerful connected future.

Podcast

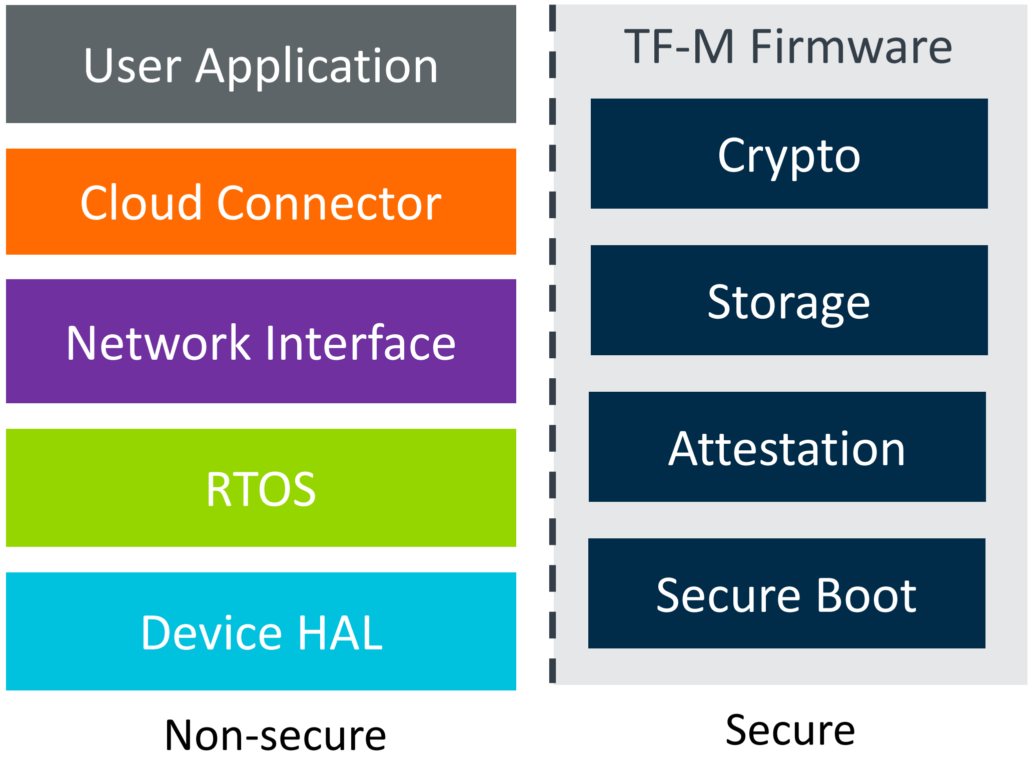
"We live in the future"

Jan Münther, Head of Digital Product Security at ams OSRAM

TrustedFirmware.org

PSA Reference Implementations

TF-M implements the Secure Processing Environment (SPE) utilizing TrustZone for Cortex-M



User Application

Cloud Connector

Network Interface

RTOS

Device HAL

Non-secure

TF-M Firmware

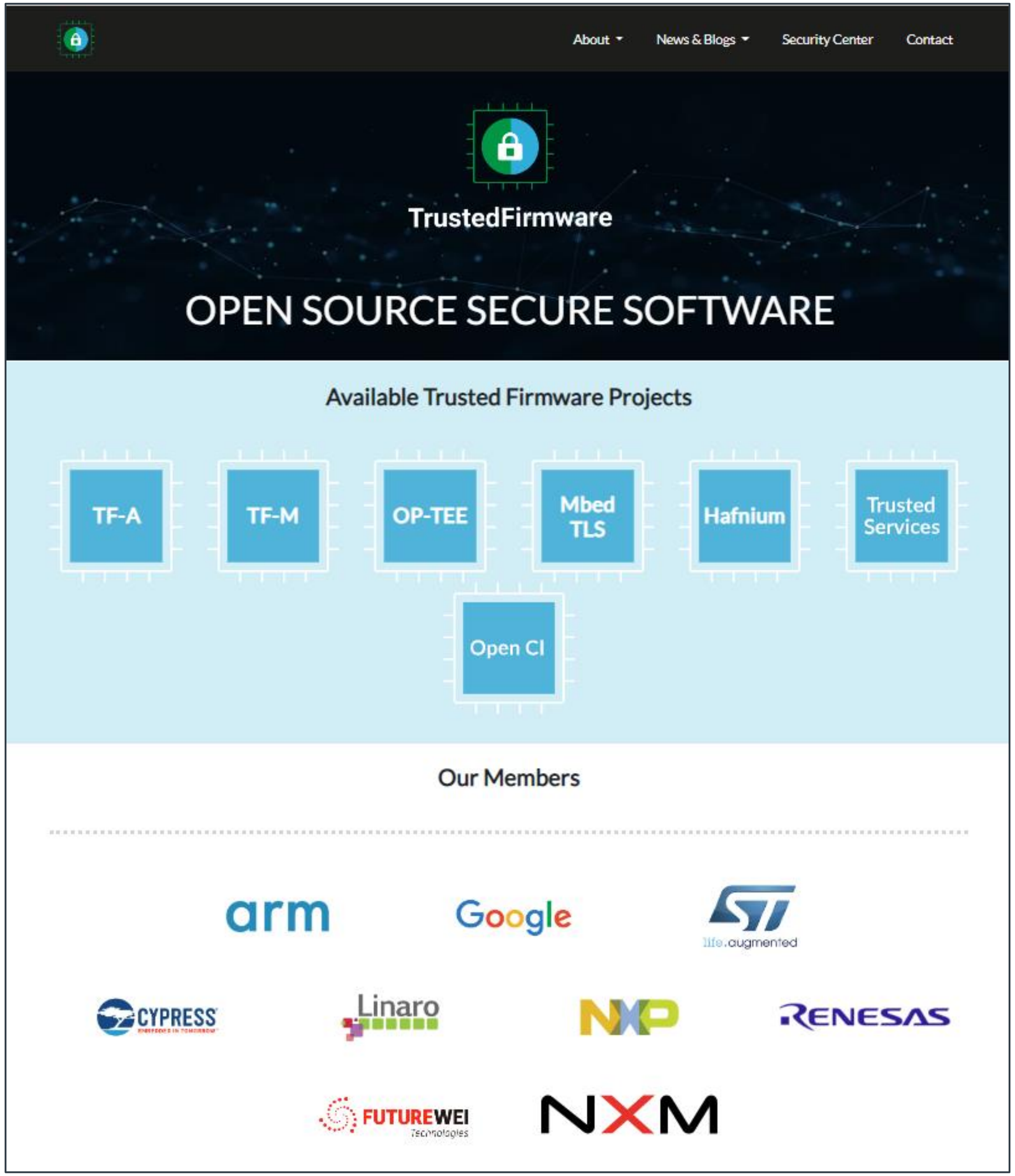
Crypto

Storage

Attestation

Secure Boot

Secure



About · News & Blogs · Security Center · Contact

TrustedFirmware

OPEN SOURCE SECURE SOFTWARE

Available Trusted Firmware Projects

TF-A · TF-M · OP-TEE · Mbed TLS · Hafnium · Trusted Services · Open CI

Our Members

Arm Total Solutions for IoT

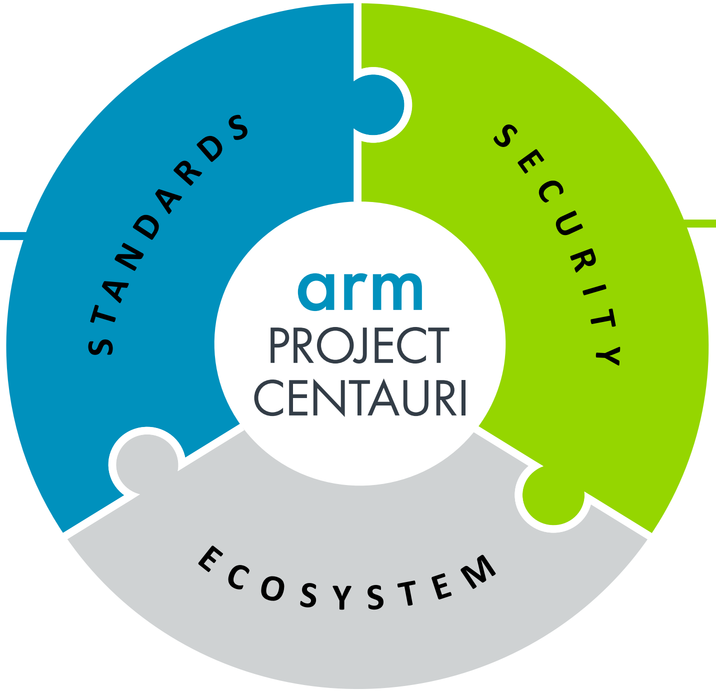
- Project Centauri for Cortex-M
- Workshops with AWS FreeRTOS

Project Centauri – IoT Software Framework for Cortex-M

Open-CMSIS CDI   Open-CMSIS Pack

Foundational Standards

- Promoting one set of device standards: based on CMSIS
- Simplifying choice of RTOS / IoT stack
- Making it easier to connect to the cloud
- Offering the ability to run on different HW
- Based on software component reuse



psacertified™

Device Security

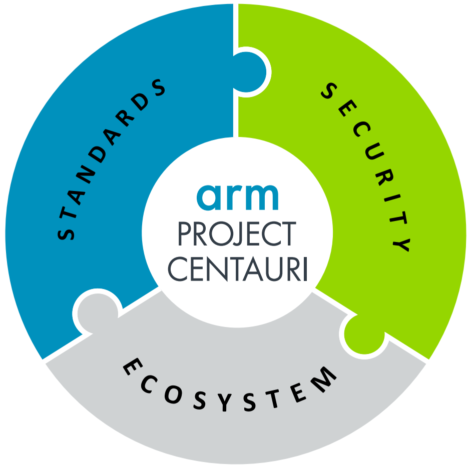
- Providing the ability for devices to be updated in the field, securely
- Based on a well-defined root of trust
- Incorporating PSA Functional APIs
- Implemented: TF-M, Mbed TLS, MCU Boot

Ecosystem Engagement

- Deployable Reference Implementations (IoT-SDK)
- Rich catalog of third-party software packs
- Support for a range of different development tools

Project Centauri: Specific activities

Secure firmware update, for any IoT software stack running on Cortex-M devices



Delivering software to developers in a consistent way, whatever development environment they work with – **Open-CMSIS-Pack**

Open-CMSIS Pack

Collaborating in the open to evolve the PSA Firmware Update API, and other PSA APIs, to allow widespread support for **Secure Firmware Update**

psacertified™

Working with partners to identify a set of existing APIs which can form a common device interface (CDI) for cloud services to use – **Open-CMSIS-CDI**

Open-CMSIS CDI

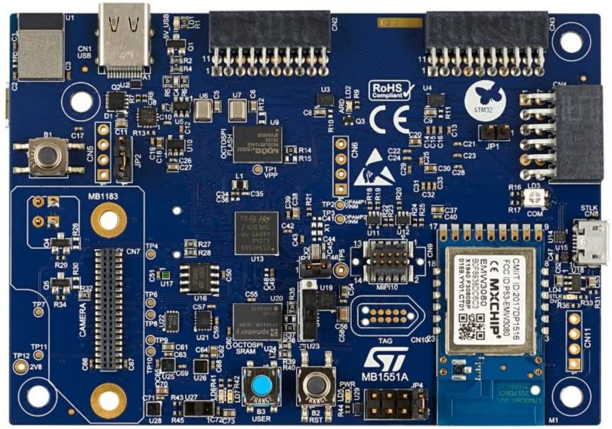
Building a reference implementation which can be used directly by developers and can be consumed by our partners – **Open IoT SDK**

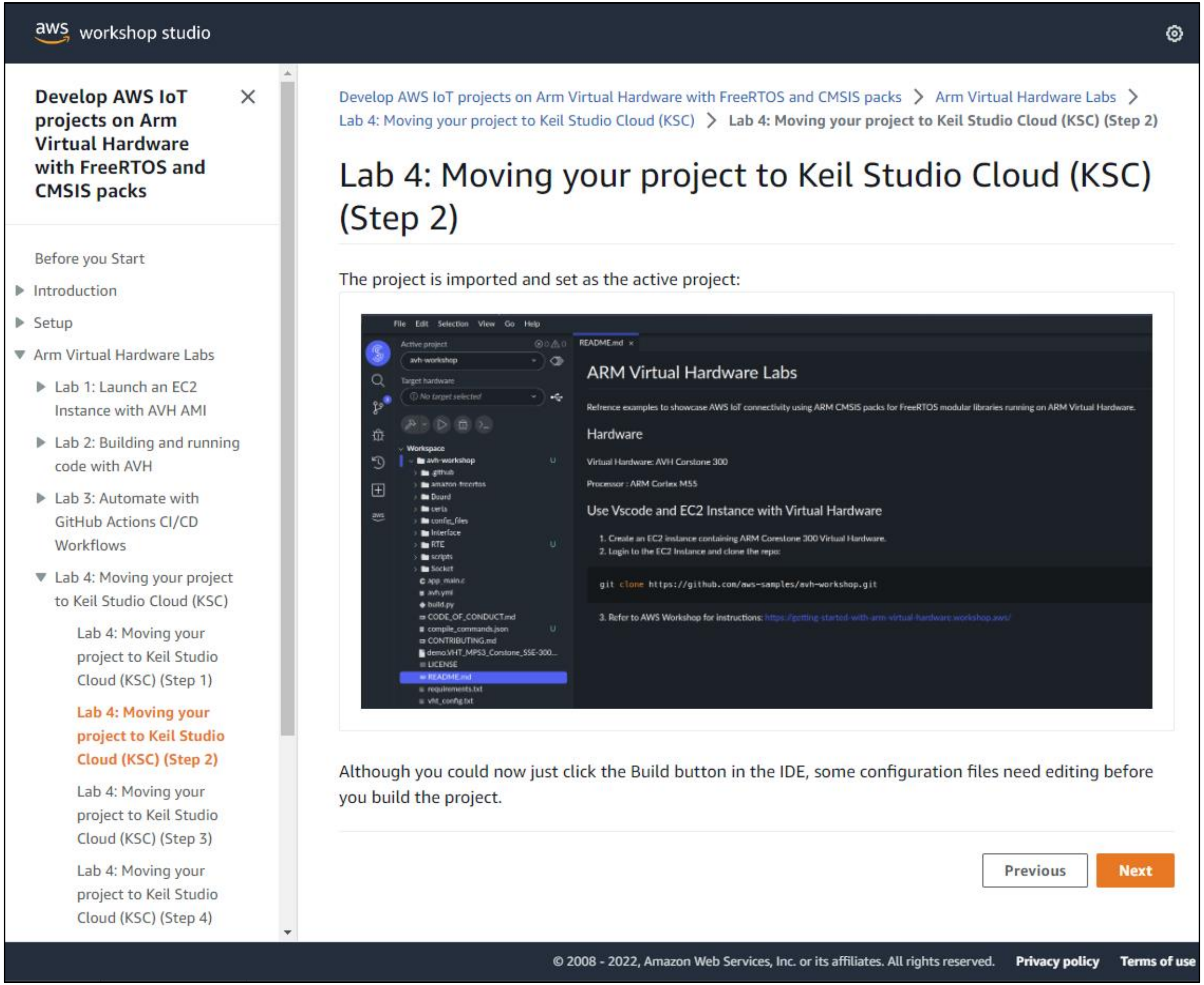
Online Workshop

AWS Cloud Connectivity

Practical examples that get you started and runs on:

- Arm Virtual Hardware removes the need for physical devices
- STM32U5 IoT Eval Board




aws workshop studio
Develop AWS IoT projects on Arm Virtual Hardware with FreeRTOS and CMSIS packs
Before you Start
Introduction
Setup
Arm Virtual Hardware Labs
Lab 1: Launch an EC2 Instance with AVH AMI
Lab 2: Building and running code with AVH
Lab 3: Automate with GitHub Actions CI/CD Workflows
Lab 4: Moving your project to Keil Studio Cloud (KSC)
Lab 4: Moving your project to Keil Studio Cloud (KSC) (Step 1)
Lab 4: Moving your project to Keil Studio Cloud (KSC) (Step 2)
Lab 4: Moving your project to Keil Studio Cloud (KSC) (Step 3)
Lab 4: Moving your project to Keil Studio Cloud (KSC) (Step 4)
Develop AWS IoT projects on Arm Virtual Hardware with FreeRTOS and CMSIS packs > Arm Virtual Hardware Labs > Lab 4: Moving your project to Keil Studio Cloud (KSC) > Lab 4: Moving your project to Keil Studio Cloud (KSC) (Step 2)
File Edit Selection View Go Help
Active project
avh-workshop
Target hardware
No target selected
Workspace
avh-workshop
.github
amazon-freertos
Board
certs
config_files
Interface
RTE
scripts
Socket
app_main.c
avh.yml
build.py
CODE_OF_CONDUCT.md
compile_commands.json
CONTRIBUTING.md
demo.VHT_MPS3_Corstone_SSE-300...
LICENSE
README.md
requirements.txt
vht_config.txt
README.md ×
Previous
Next
Privacy policy
Terms of use

Lab 4: Moving your project to Keil Studio Cloud (KSC) (Step 2)

The project is imported and set as the active project:

ARM Virtual Hardware Labs

Refrence examples to showcase AWS IoT connectivity using ARM CMSIS packs for FreeRTOS modular libraries running on ARM Virtual Hardware.

Hardware

Virtual Hardware: AVH Corstone 300

Processor : ARM Cortex M55

Use Vscode and EC2 Instance with Virtual Hardware

1. Create an EC2 instance containing ARM Corestone 300 Virtual Hardware.
2. Login to the EC2 Instance and clone the repo:

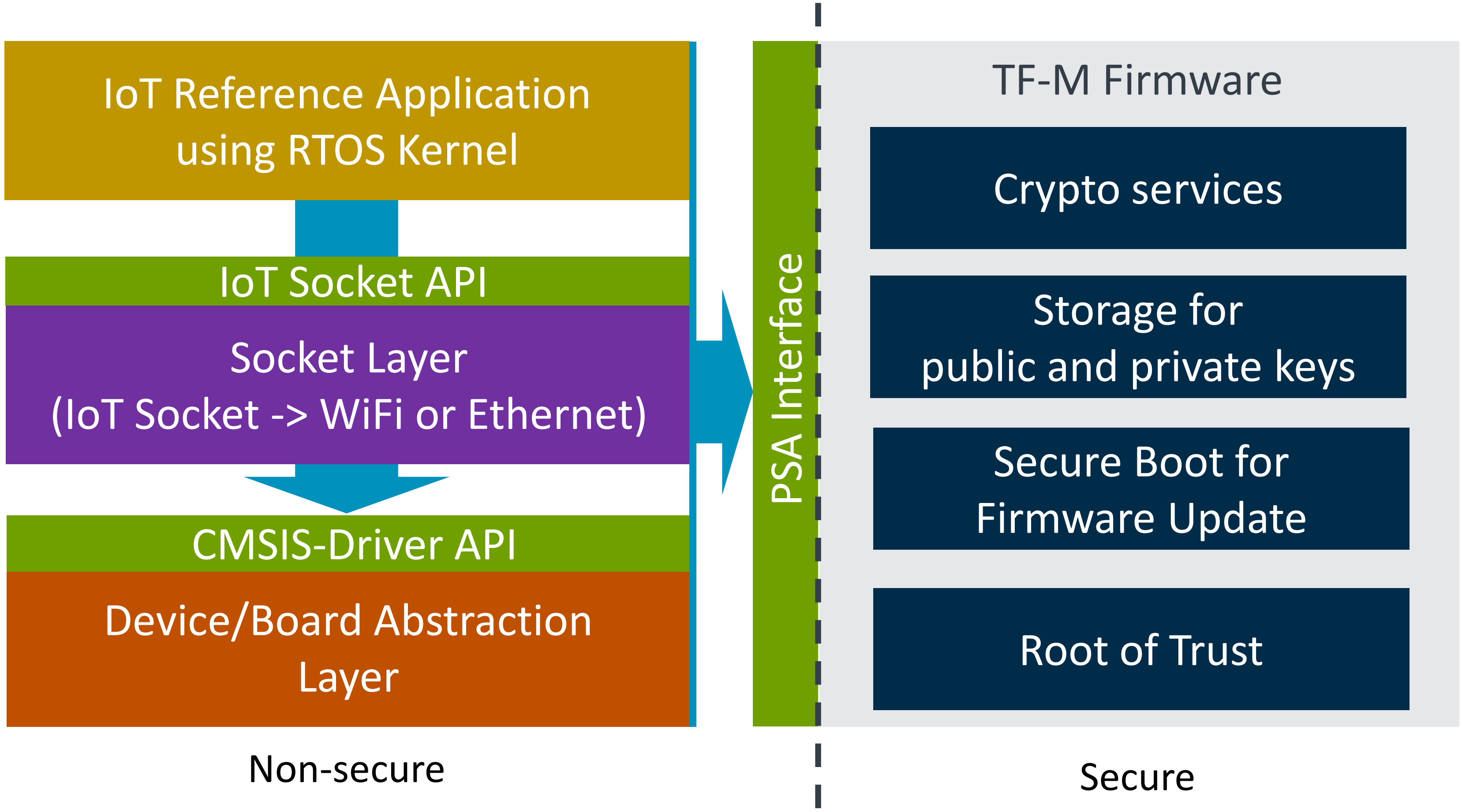
```
git clone https://github.com/aws-samples/avh-workshop.git
```

3. Refer to AWS Workshop for instructions: https://getting-started-with-arm-virtual-hardware.workshop.aws/

Although you could now just click the Build button in the IDE, some configuration files need editing before you build the project.

IoT Workshop Example – Structure

Reference Application Framework with reusable software components



IoT Reference Application using RTOS Kernel

IoT Socket API

Socket Layer (IoT Socket -> WiFi or Ethernet)

CMSIS-Driver API

Device/Board Abstraction Layer

PSA Interface

TF-M Firmware

Crypto services

Storage for public and private keys

Secure Boot for Firmware Update

Root of Trust

Non-secure

Secure

Improve Development Workflows for Embedded and IoT

Benefits of cloud native for embedded and IoT software development

Version Control

Cloud Storage

Repository hosting service that typically includes access control and a number of collaboration features.

Software Development

Software as a Service (SaaS)

Instead of installing the IDE and software tools on your local device, you access the setup of the cloud provider.

Continuous Testing

Virtual Machine (VM)

A “server” running in the cloud contains a tool environment with simulation models and settings specific to your project.

Software Deployment

Geographic Distribution

Over-the-air (OTA) programming offers methods to provision and update software of devices that are already in the field.

Machine Learning (ML)

Data Analytics

Monitor devices to spot anomalies and collect training data for ML algorithms that can be deployed to IoT endpoints.

White Paper: Get More Productivity with Cloud Services

Summary

Summary

Arm is taking a holistic approach to IoT security

- **Flexible and secure IP at the chip level**

- **Software developer enablement through tools and ecosystem collaboration**
  - PSA Certified that provides IoT Security Framework and certification
  - Open-source reference applications and software building blocks
  - With in-field firmware update technologies

- **Providing a clear path to end-to-end security in systems and networks**

Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה