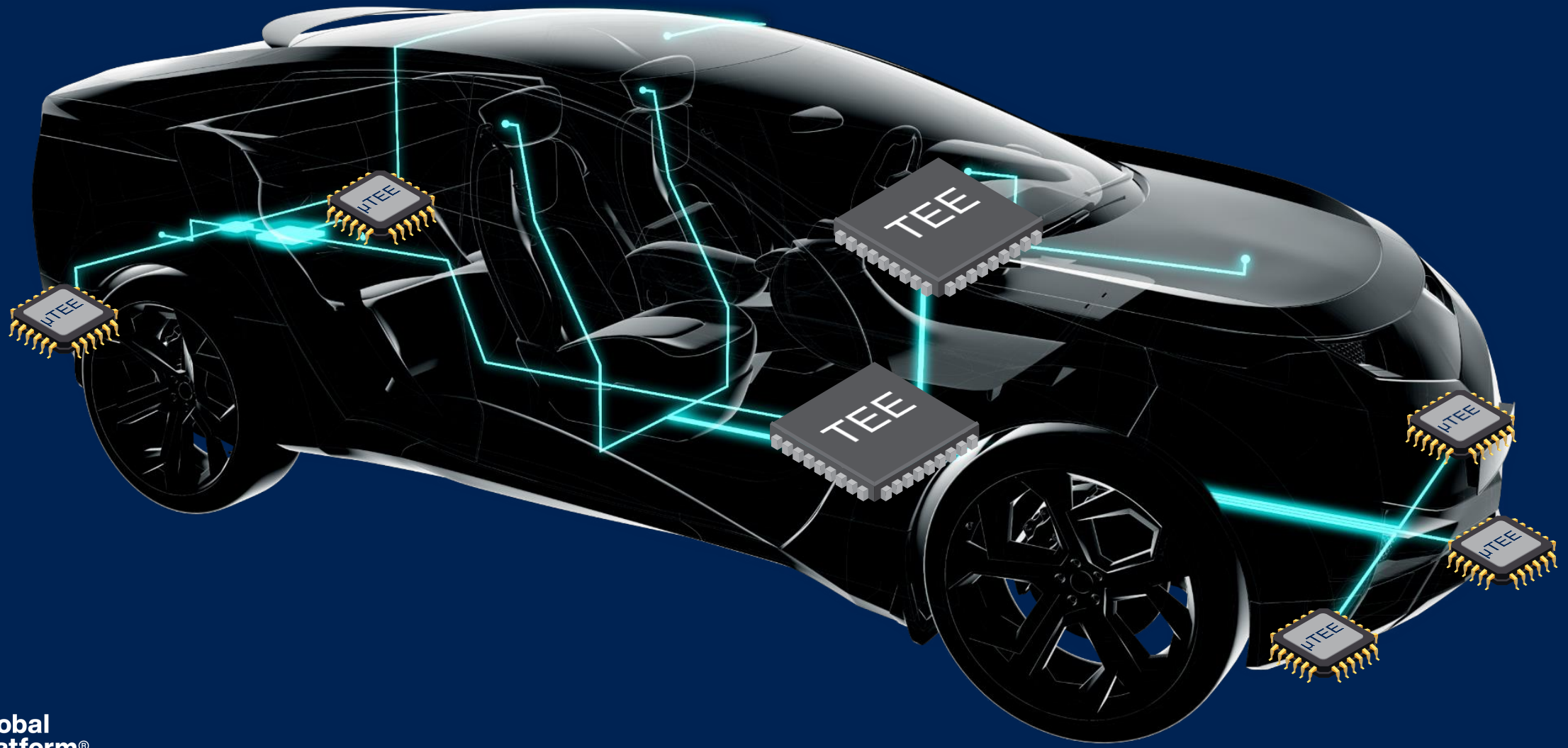
Global Platform®

GP Micro-TEE
Evolving FFM and PSA APIs

Richard Hayton (rhayton@qti.qualcomm.com)
TES Committee Chair

Micro TEEs – TEEs for smaller ECUs



Global Platform®

The idea behind a Micro TEE

Rational is the same as a full-sized TEE:

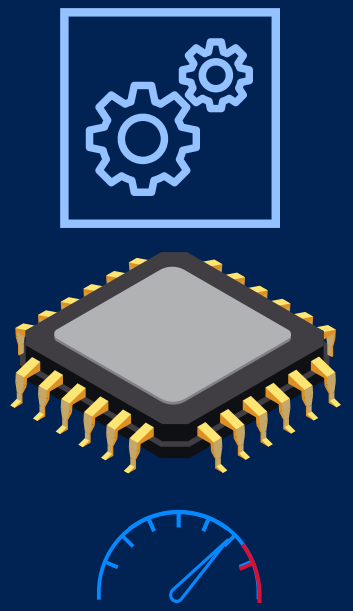
Isolate security critical **code** and **secrets**

GlobalPlatform Micro-TEE will standardize the whole environment

- What it needs to be secure
- Features such as crypto & storage
- How to write code – Programmer APIs.

However there are core differences

- More constraints – but simpler apps
- Focus on leveraging hardware crypto



Software Flexibility

Hardware Speed (Cryptography)

MCU Security: One size does not fit all

Trusted Apps

Firmware Update

Remote Attestation

Secure Storage (Keys/Data)

Crypto Functions

Secure Boot

Secure CAN (SecOC)

SHE++
EVITA
…

MCU+
SHE

TPM

MCU
+
HSM

Micro TEE

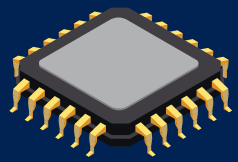
? Multiple Profiles
(=sizes)

?

"Full Sized"
TEE

?

Size/cost of microprocessor

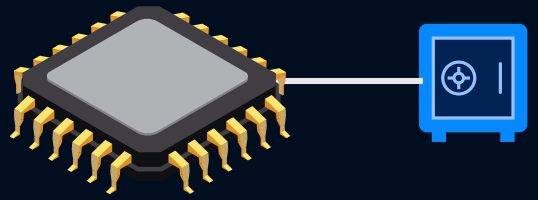


>= 16 bit

>= 32 bit

Micro-TEE: isolated security code

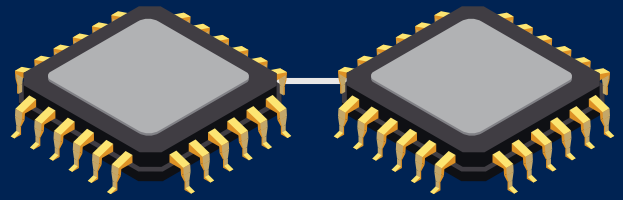
Non-Secure Secure



Fixed function Security or proprietary extensions (e.g. SHE, HSM)

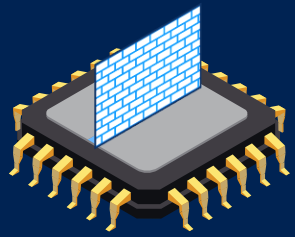
Not considered a Micro-TEE because there is no standardized way of adding OEM security code

Non-Secure Secure



2x Micro-Processor without internal HW partitioning (e.g. Arm Cortex-M v7)

Non-Secure Secure



Micro-Processor with internal HW partitioning (e.g. Arm Cortex-M v8)

Two code ‘zones’
one for regular code, one for security code

Supports OEM security code in secure zone

~~Arm~~ Platform Security Architecture (PSA) APIs

GlobalPlatform

Trusted Apps

Firmware Update

Remote Attestation

Secure Storage

Crypto Functions

Secure Boot

Secure CAN (SecOC)

Arm has standardized APIs for these areas. Called “PSA APIs”

PSA API Example use cases

- Adopted as a crypto library
  - mbedTLS
- As an interoperability layer
  - To provide access to HW acceleration in micro controllers.
- “Under discussion”
  - AUTOSAR CSP internal APIs
- Security APIs within a micro-TEE

~~Arm~~ GlobalPlatform Trusted Firmware Foundation for MCUs

Trusted Apps

Firmware Update

Remote Attestation

Secure Storage

Crypto Functions

Secure Boot

Secure CAN (SecOC)

Arm has standardized an architecture for running secure code. This has evolved to support trusted apps.

FF-M is implemented in TF-M (Trusted Firmware for Mobile)

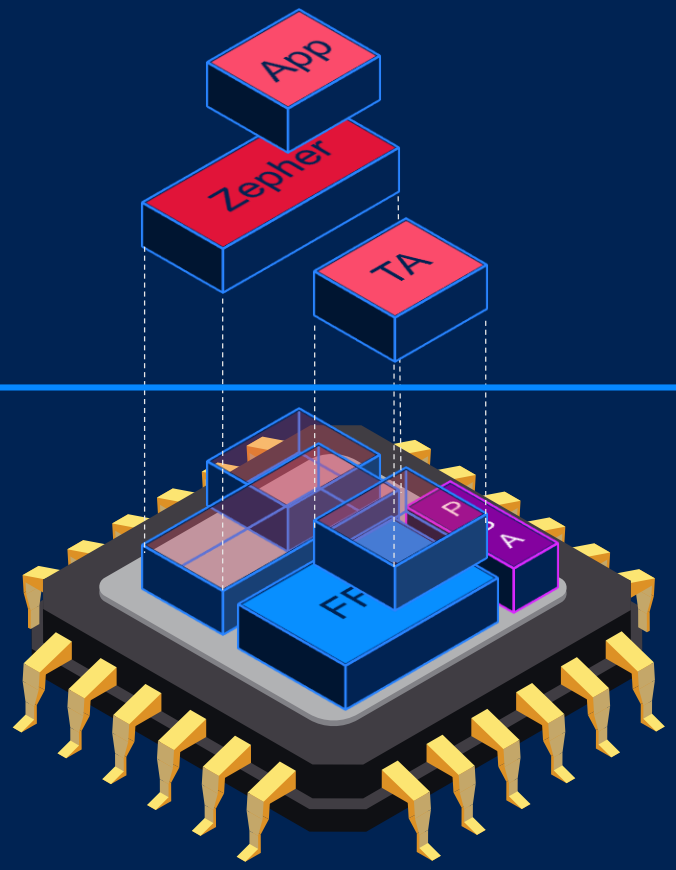
TF-M is an open-source project supported by Arm. It is mature and widely used in IOT

FF-M (the specs) have been donated to GlobalPlatform

TF-M (the implementation) has not.

GlobalPlatform aims to create a Micro-TEE specification based on FF-M without overly disrupting the active TF-M ecosystem

FF-M Stack



OEM apps can access security APIs from a regular OS

Or security functions can be written as Trusted apps and run within the security zone

PSA APIs provide a standardized API for chip features

FF-M ensures secure boot & provides a software platform

SIP creates hardware including any crypto accelerators

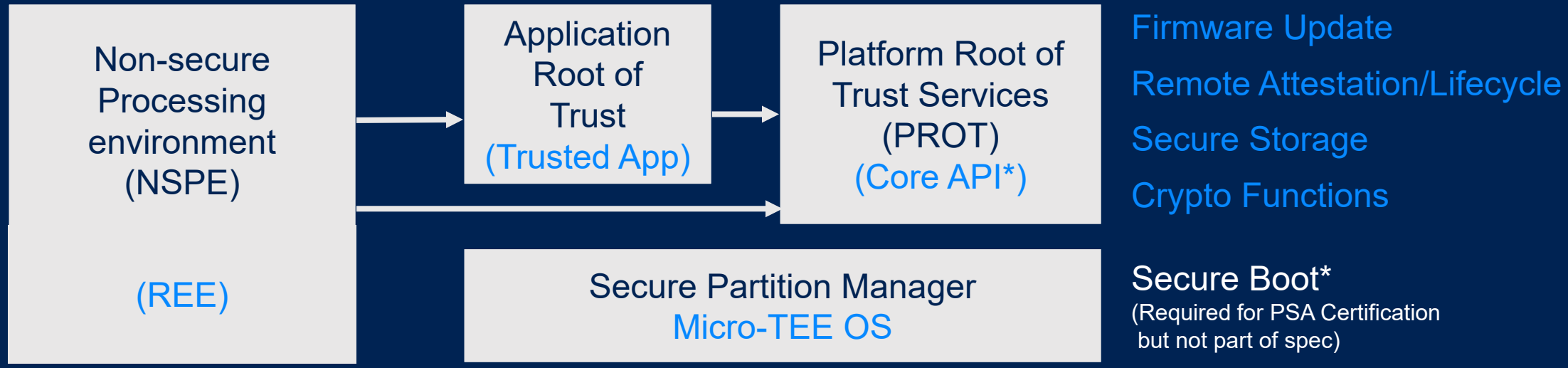
Certifiable Secure MCU

FF-M high level

This is a reimagining of GlobalPlatform TEEs for micro-controllers

It has some differences in intent and many detailed differences in implementation – but it is “broadly similar”

The names are all different [equivalents in blue]

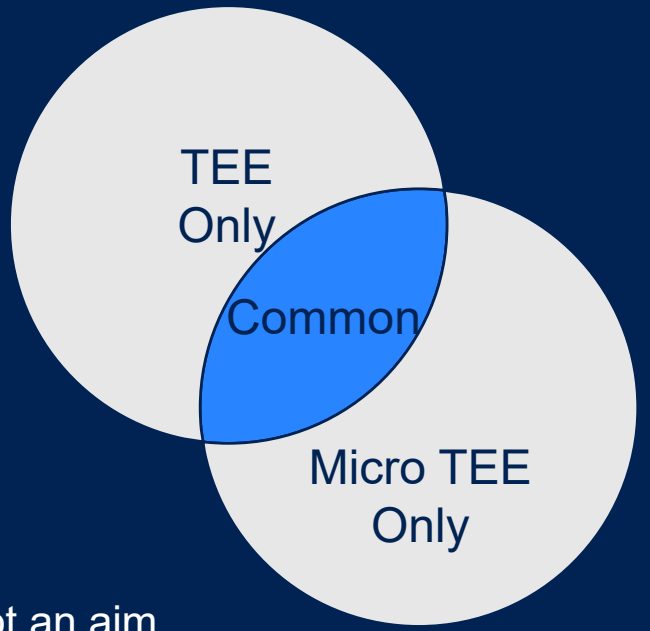


Concepts / Capabilities / APIs

The concepts behind FF-M and GlobalPlatform TEEs are very similar

The capabilities are mainly aligned, but there are gaps we hope to address in Core 2.0 / Micro TEE specs.

- TF-M supports session-less access, GP TEEs do not.
- TF-M allows platform services to be called from NWD. GP TEEs do not
- TF-M support memory handles, GP TEEs do not
- TF-M has strictly controlled access to shared parameters. GP TEEs do not



The APIs are different

- TF-M uses PSA APIs for Crypto
- Etc.

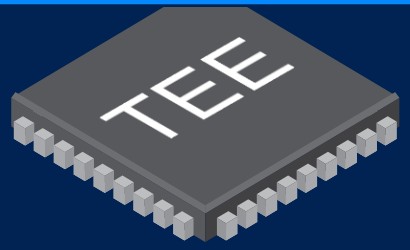
- We hope to make it easier to port code between TEEs – but full compatibility is not an aim

By aligning concepts, porting becomes easier…

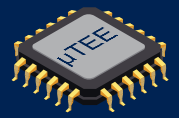
TA

API Adaption layer (TBD)

TEE 2.0 APIs



Micro-TEE APIs / PSA



Current Status

We have started work comparing and contrasting the specifications

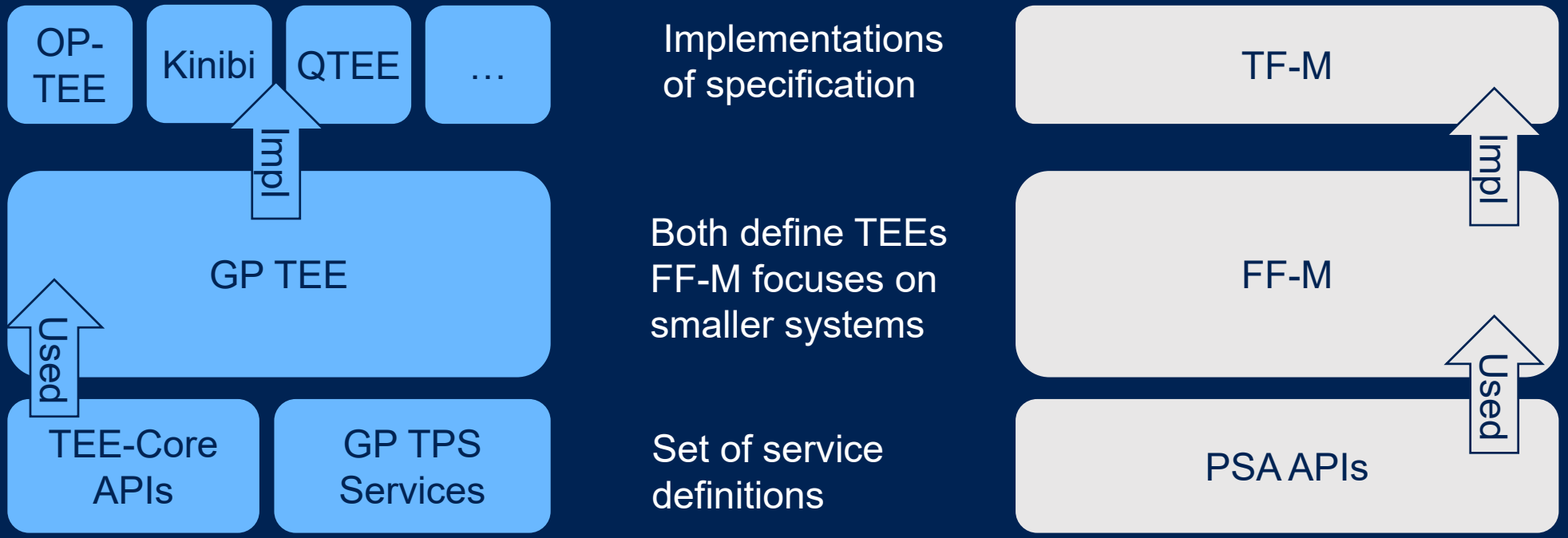
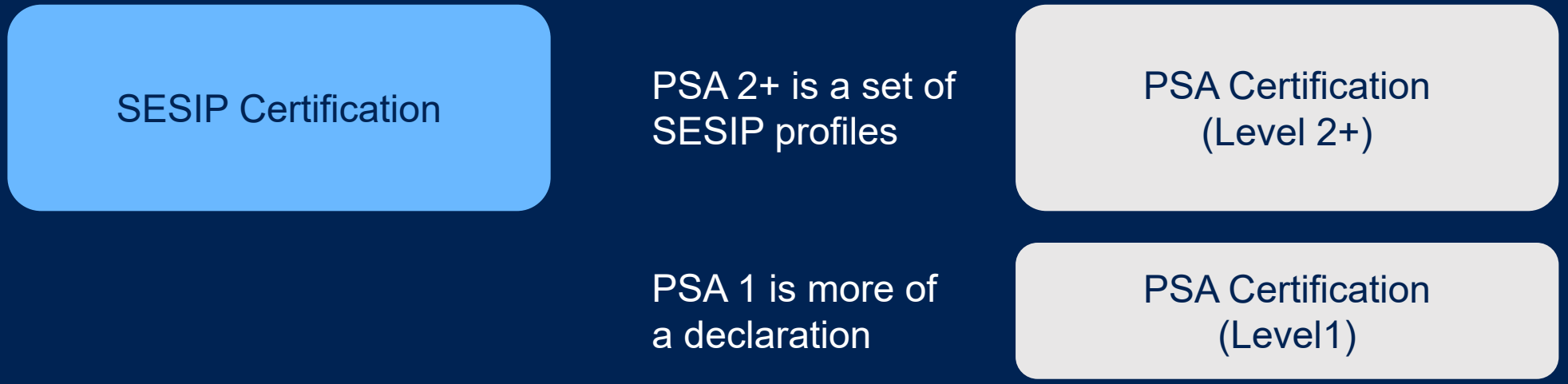
Arm members of the TES Committee are starting work to create an initial Micro TEE specification based on FF-M

FF-M viewpoints are being considered in Core 2.0, with an aim to align concepts

API alignment is not being attempted at this stage – as we don’t wish to disrupt either ecosystem

Global Platform®

Securing the digital future

→globalplatform.org

TEE-Micro TEE comparison