Global Platform®

CSFV Detroit May 2026

TEE Use Cases Today and Tomorrow

Dr Richard Hayton
Board Member, Chair Automotive Task Force & TES Committee, GlobalPlatform®
Chief Strategy and Innovation Officer, Trustonic Ltd.

Global Platform®

TEE - Background

Problem

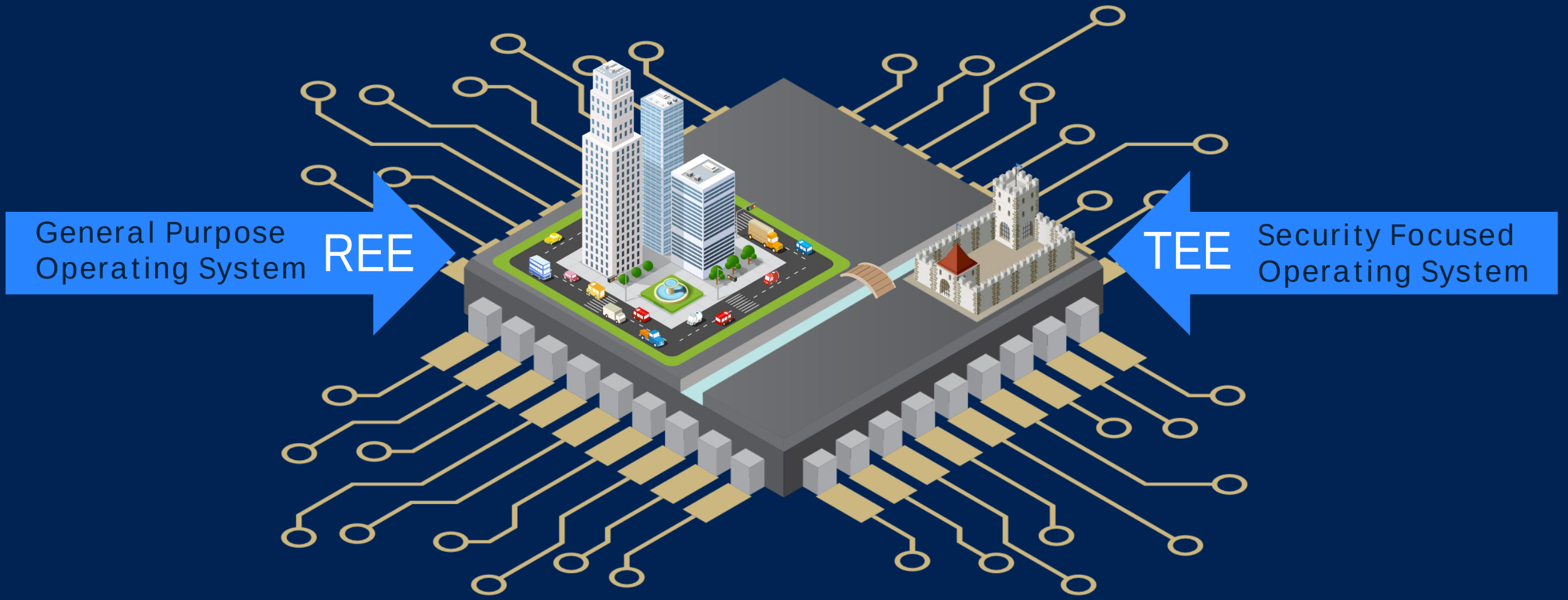
Modern operating systems are large and powerful

Making them secure is hard

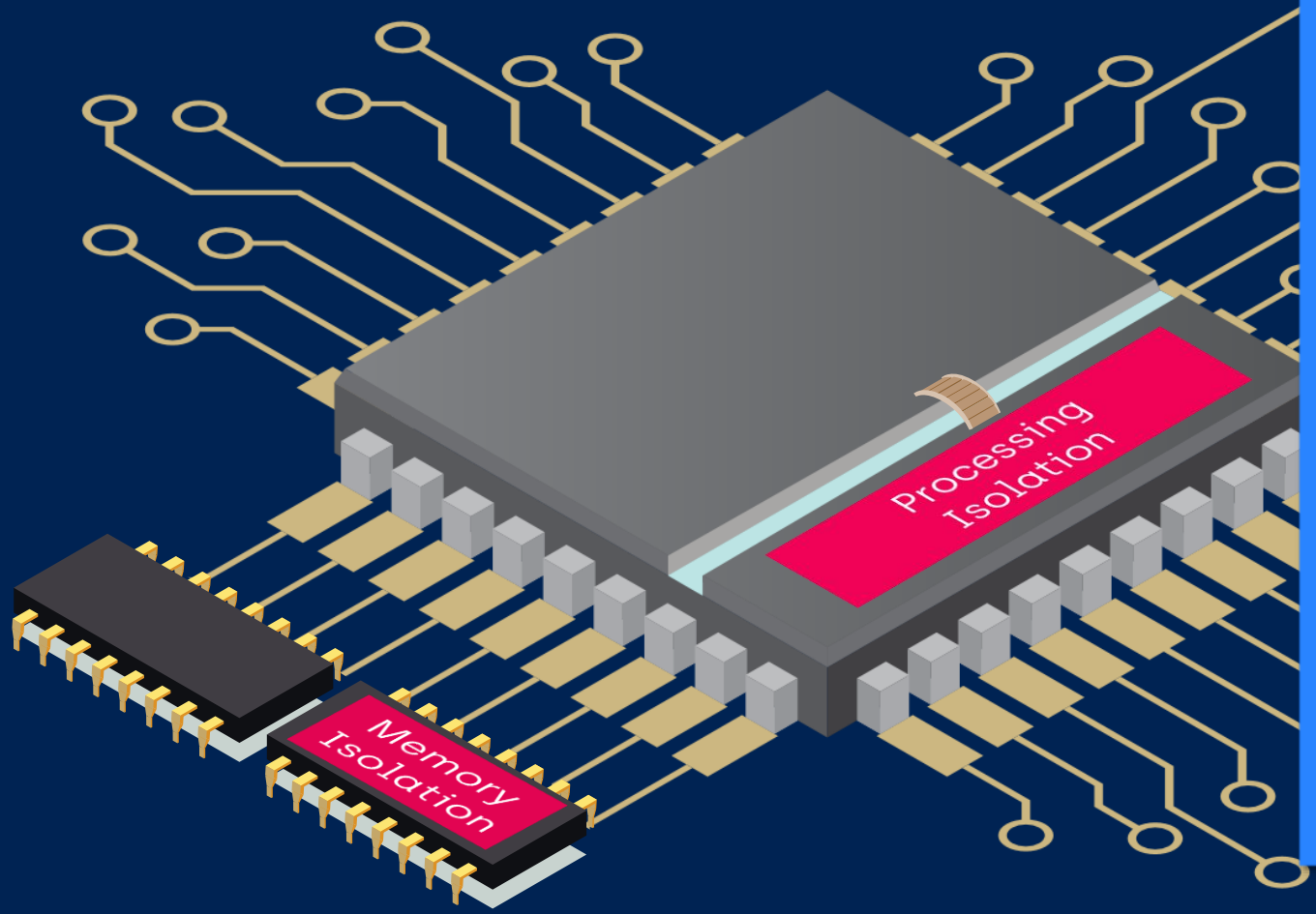
The TEE is an architectural approach to separate security critical code from regular code

It runs outside of the operating system with a minimal trusted computing base

Typical TEE configuration



Hardware Security?

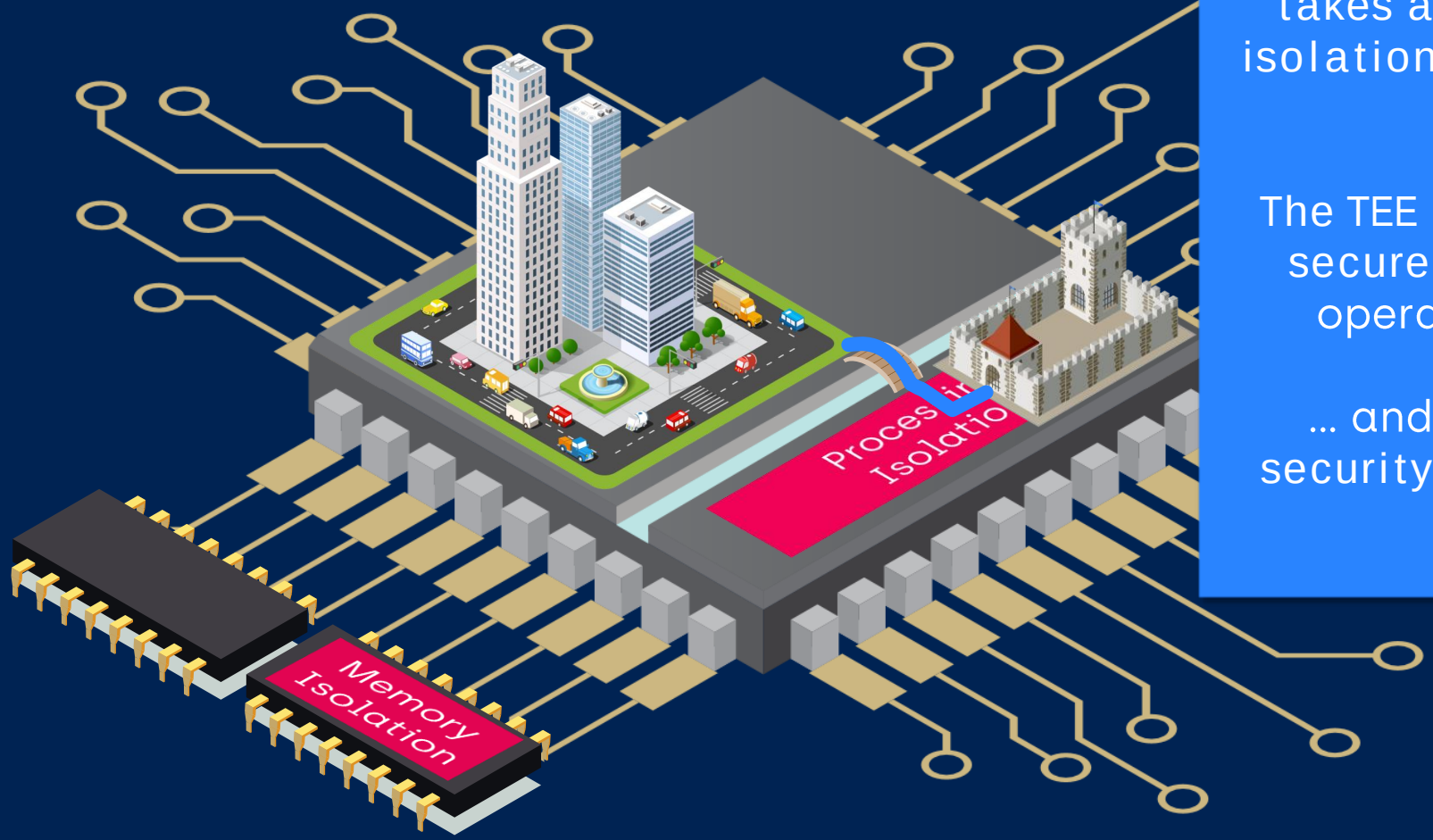


TrustZone™ is a feature of all Arm application processors which provides hardware isolation and privileged access to security features.

Similar features have been added to Arm 'machine class' chips (Cortex-M)

RISC-V processors can also provide similar isolation when paired with a system Memory Protection Unit

Hardware Security?



The TEE Operating System takes advantage of this isolation to provide secure services

The TEE is responsible for securely booting other operating systems...

... and then providing security focused services for them

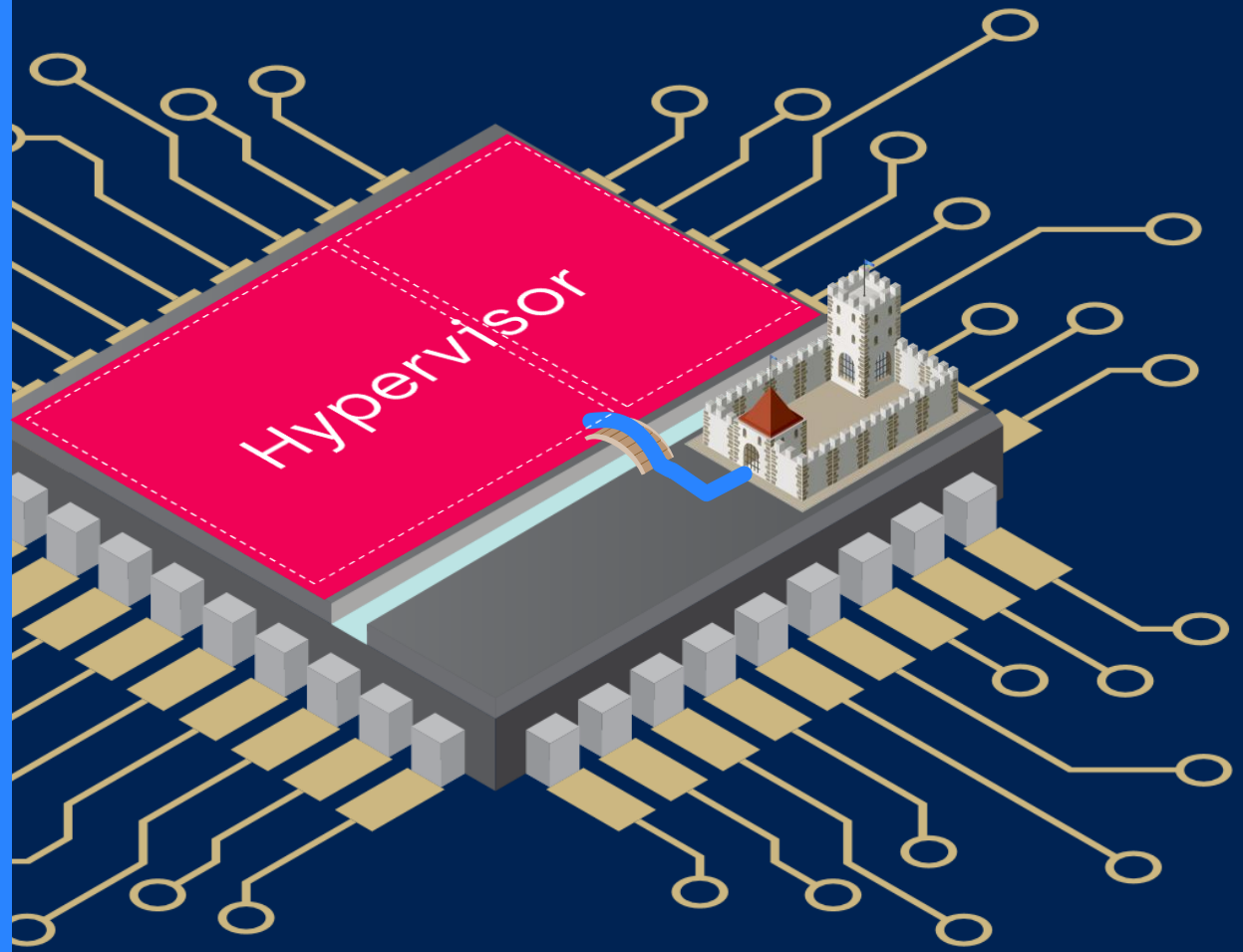
TEEs and Hypervisors

Hypervisors enable multiple operating systems to run along side each other

On Arm CPUs, hypervisor support is an additional mechanism alongside TrustZone

In Arm v9 it is also possible to run a hypervisor in secure world to enable multiple TEEs

(RiscV uses a hypervisor + System MMU to isolate TEE)



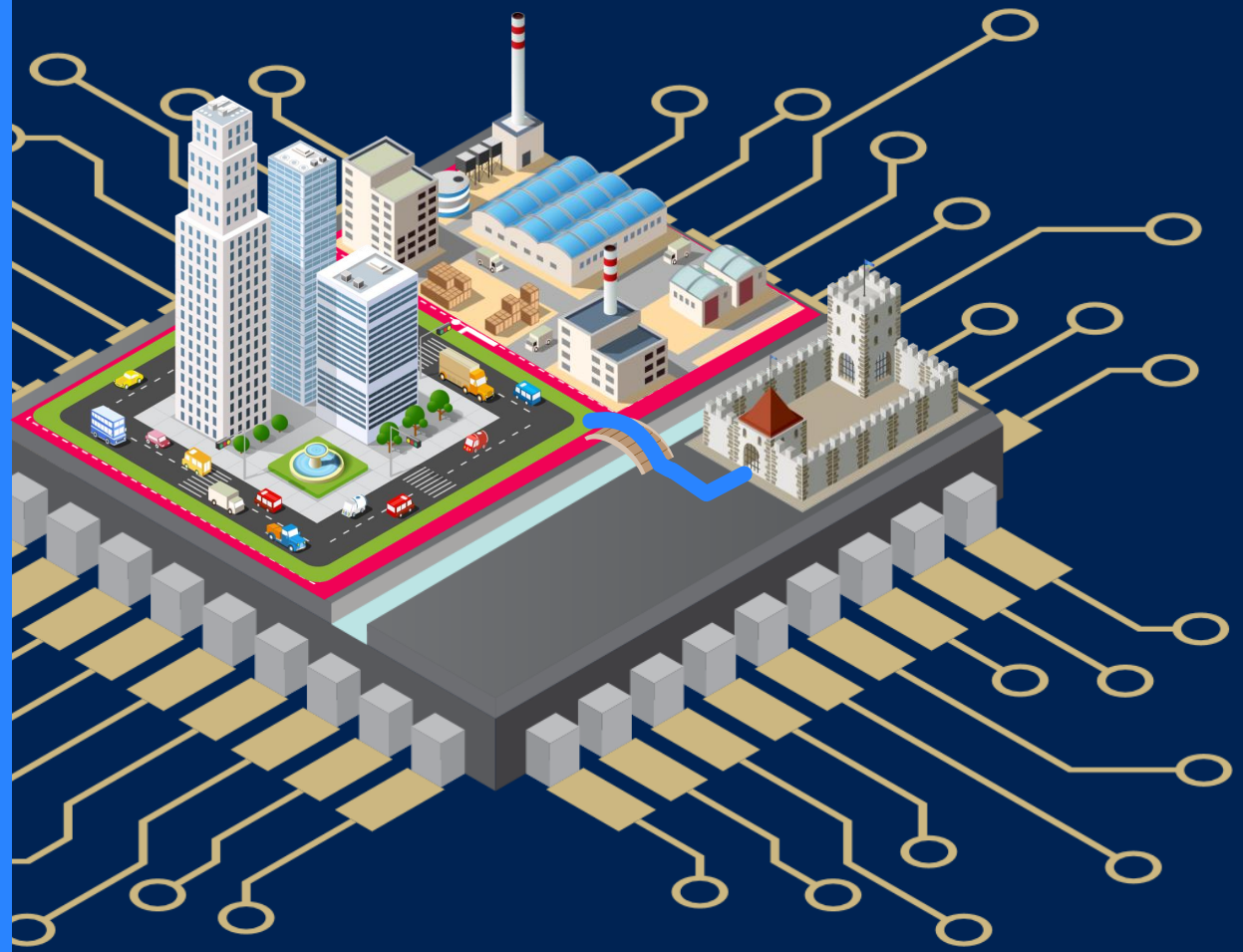
TEEs and Hypervisors

Hypervisors enable multiple operating systems to run along side each other

On Arm CPUs, hypervisor support is an additional mechanism alongside TrustZone

In Arm v9 it is also possible to run a hypervisor in secure world to enable multiple TEEs

(RiscV uses a hypervisor + System MMU to isolate TEE)



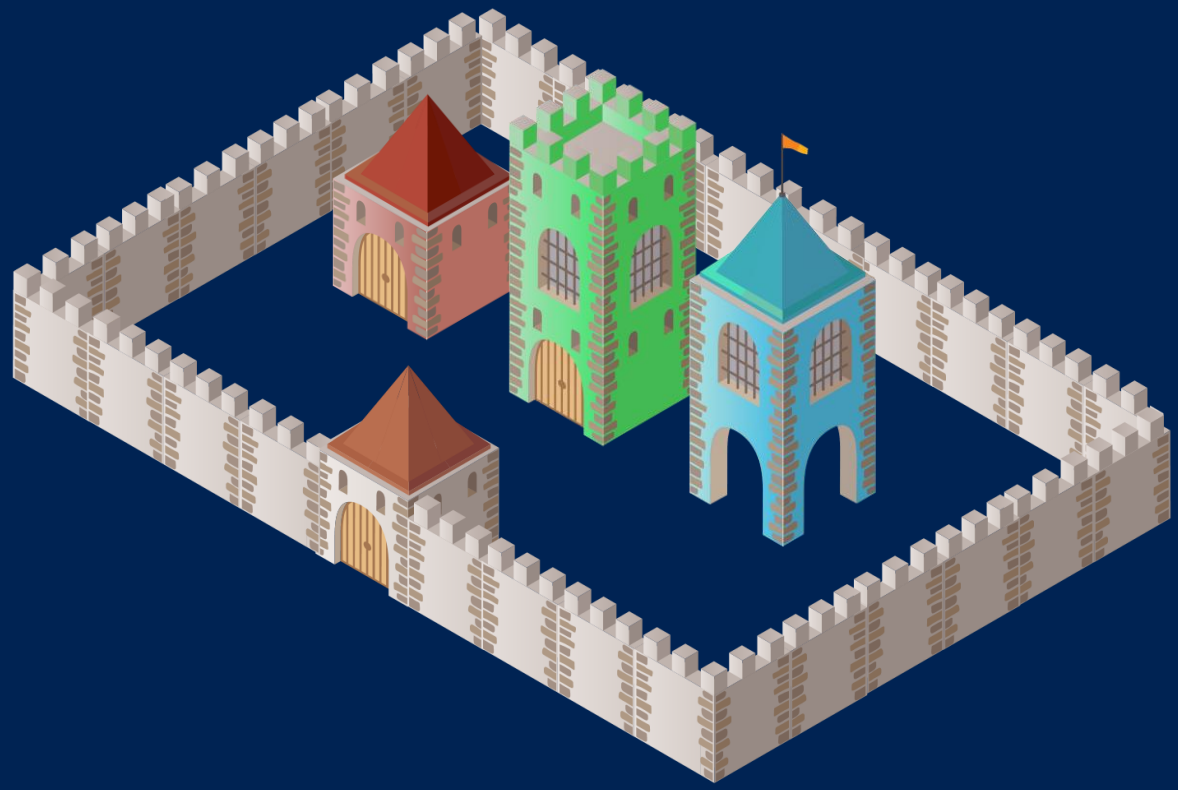
Inside a TEE

TEEs can run many trusted applications (TAs)

Each is isolated from each other and has its own private storage

Trusted apps can also communicate in a controlled way

This makes TEE-based solutions modular and reusable



Global Platform®

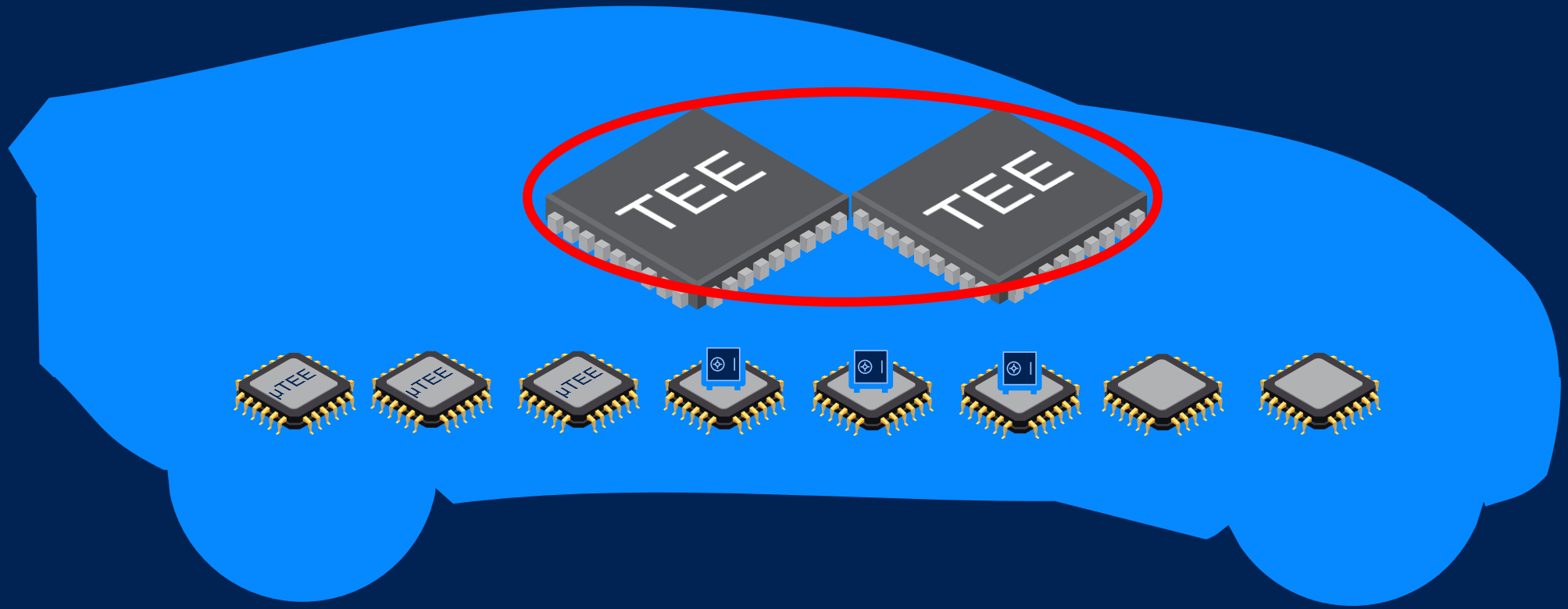
TEE Capabilities

- Focused on supporting the main operating system
- Initially relatively simple and focused on mobile use cases
- Today many TEEs provide fully featured security operating systems, and are used in many industries
- I will talk about some of the evolution from the perspective of automotive

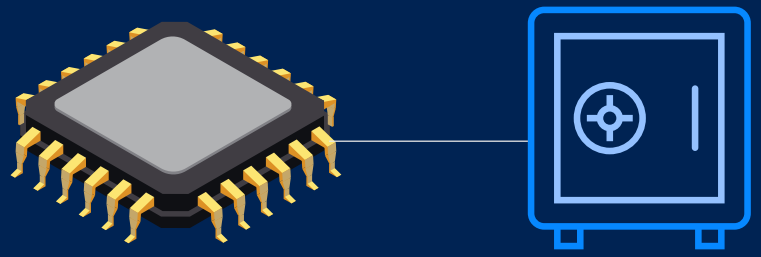
Global Platform®

TEEs in Automotive

TEEs are a great fit for larger ECUs
They underpin security for software defined vehicles



Automotive – Historic view of hardware security



Apps run on Micro-Controller (often AutoSAR)

Hardware Element providing crypto (SHE, SHE+, EVITA…)

Safety is the priority. Security comes second.

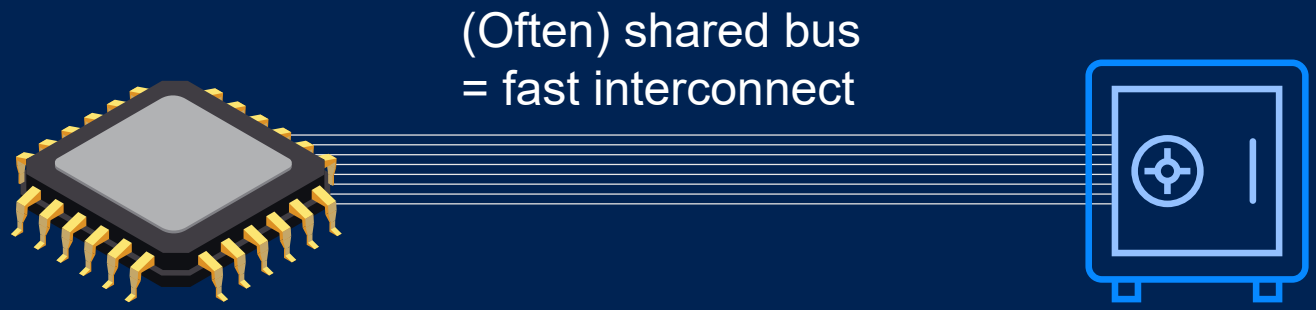
SHE provides a standard solution, but it is very low level

- Focus is on ‘key slots’ which can hold different types of keys / key material

Lots of variation on how it is used (per project)

- CAN limitations lead to a lot of variation
- Different approaches for establishing secure boot
  - SHE stores expected MAC for boot image + secret material to regenerate HMAC
  - Provisioning MAC/Secret is “hard”
- SHE does not protect the broader application.
  - Just a keystore / crypto engine

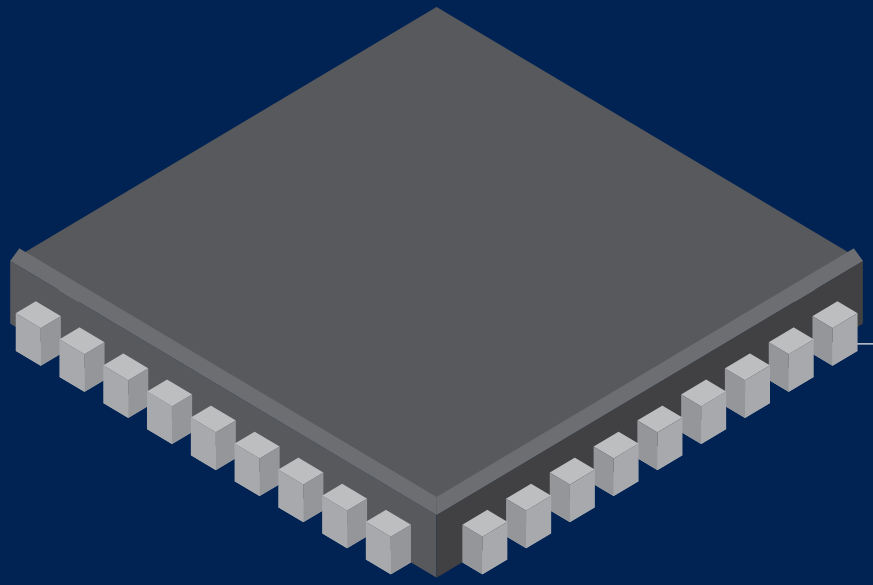
MCUs *need* hardware for crypto performance



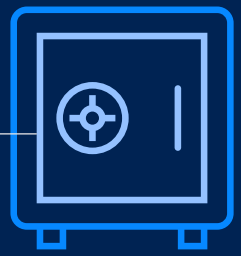
MicroController
= Low Power
= Slow
= Software Crypto is poor

Hardware Crypto provides performance

CPUs *don't* have the same needs



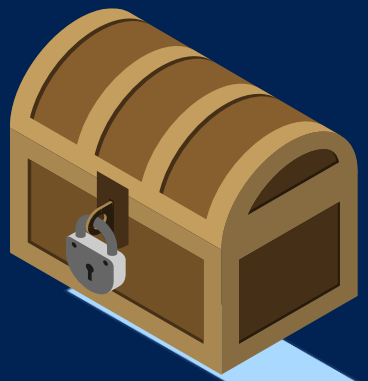
Typically, slow
SPI bus



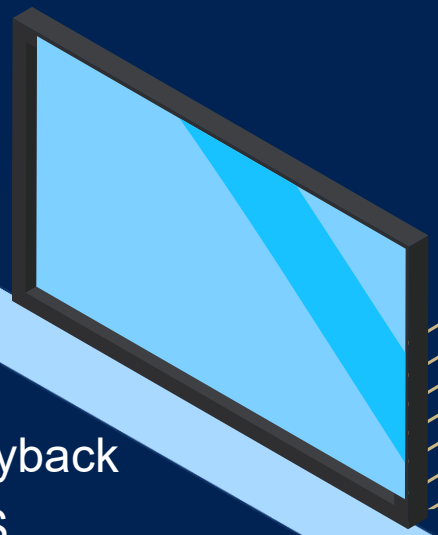
Application Processor
= High Power
= Blindingly fast
= Software Crypto is great!

Hardware crypto elements are orders of magnitude slower than CPU

Use Case Evolution in Automotive



Key Store
(TEE-HSM)



Secure Video Playback
Android CTS

IVI / Cluster

Telematics
/ Gateway

ADAS

Secure
Communications

Security & Monitoring

Global Platform®

Growth Areas

- Multi-Threading
- Performance & Scale

- Ever Broader Cryptography
- Post Quantum Focus

- Attestation & Secure Manufacture
- Data storage / management

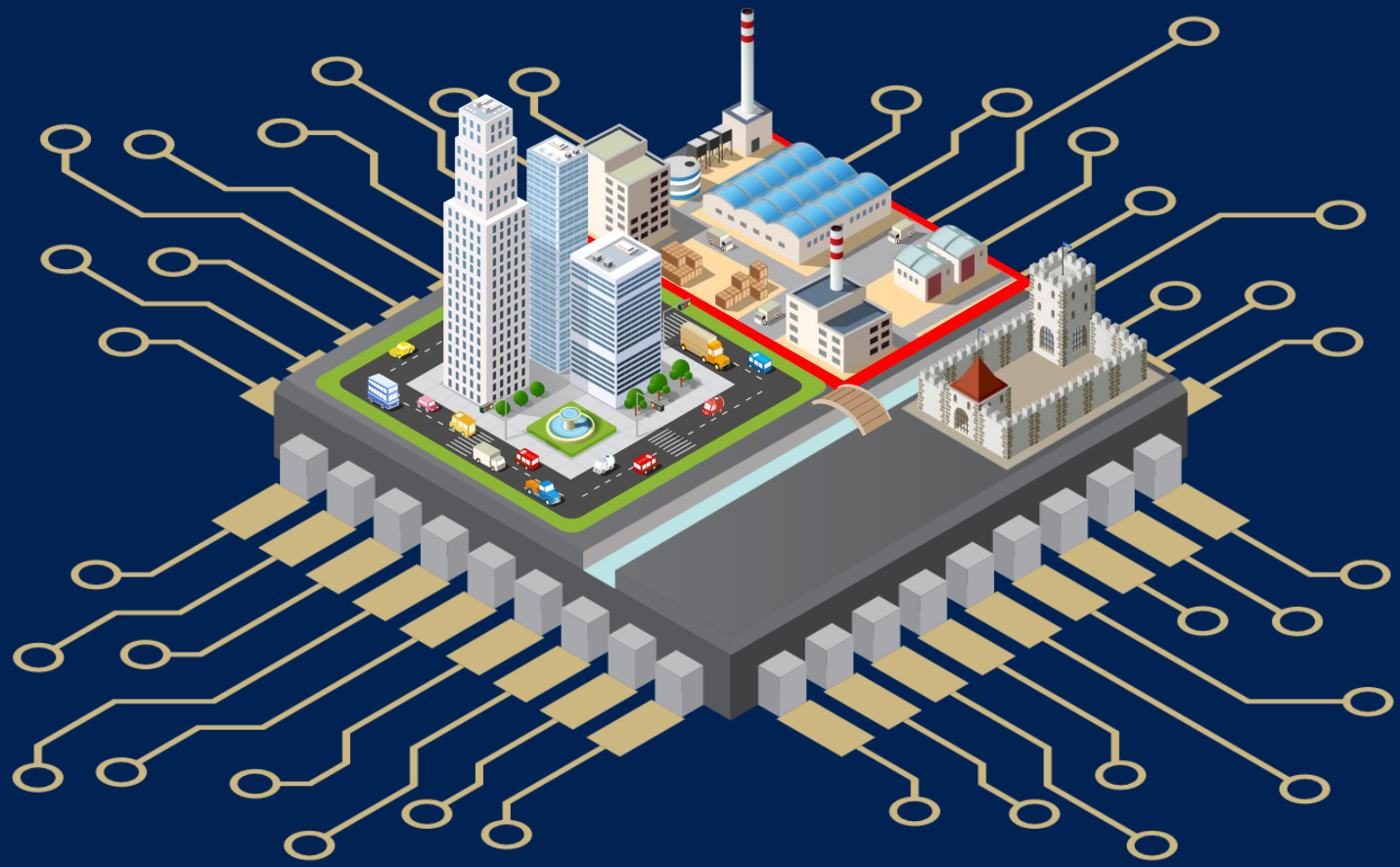
- Safety Critical TEEs (?)
- Freedom from Interference

Supporting Safety Critical Applications

TEEs have strong security isolation, but do not necessarily provide broader freedom from interference needs

One common approach in SDVs is to add a second or third operating system which are more focused on safety critical applications

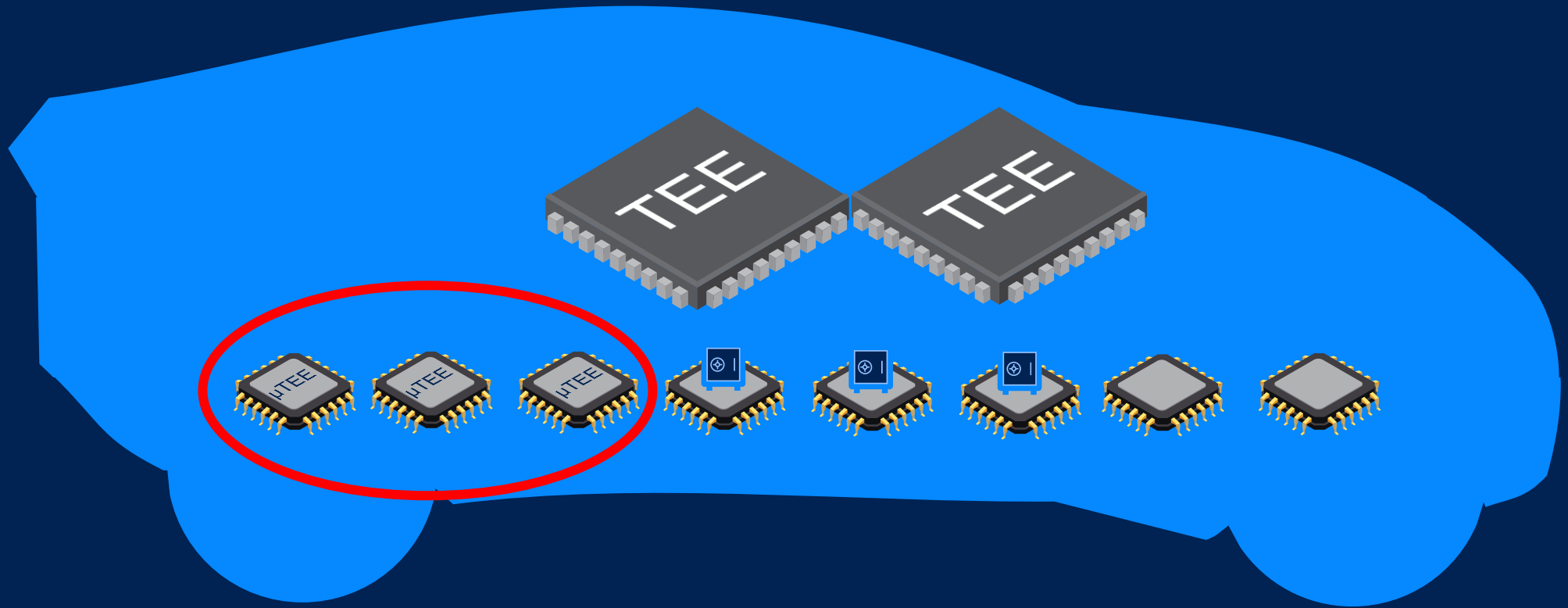
An open dscussion is how (or if) the TEE should support mixed-criticality clients



Global Platform®

Micro-TEEs

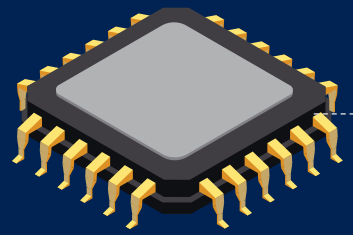
TEEs in smaller ECUs..



The idea behind a Micro TEE

Benefit from software flexibility & secure more than just crypto (as TEE)

Abstract hardware engines for performance (where necessary)



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

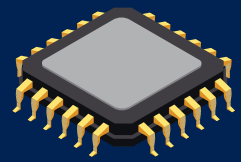
? Micro TEE
? Multiple Profiles
(=sizes)
?

"Full Sized"
TEE
?

Size/cost of microprocessor

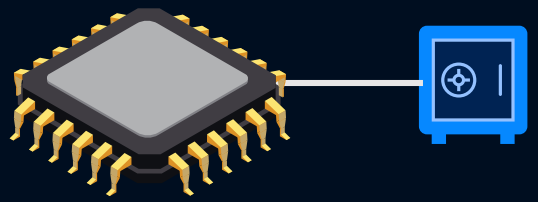
>= 16 bit

>= 32 bit



Micro TEE Architecture

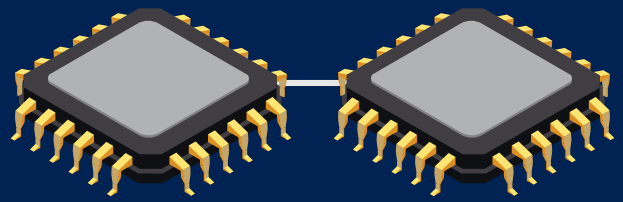
Non-Secure Secure



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

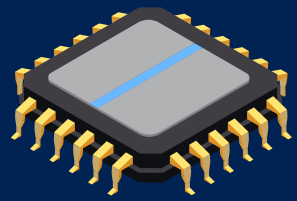


2x Micro-Processor without internal HW partitioning (e.g. Arm Cortex-M v7)

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

Supports OEM security code in secure zone

Non-Secure Secure



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

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

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

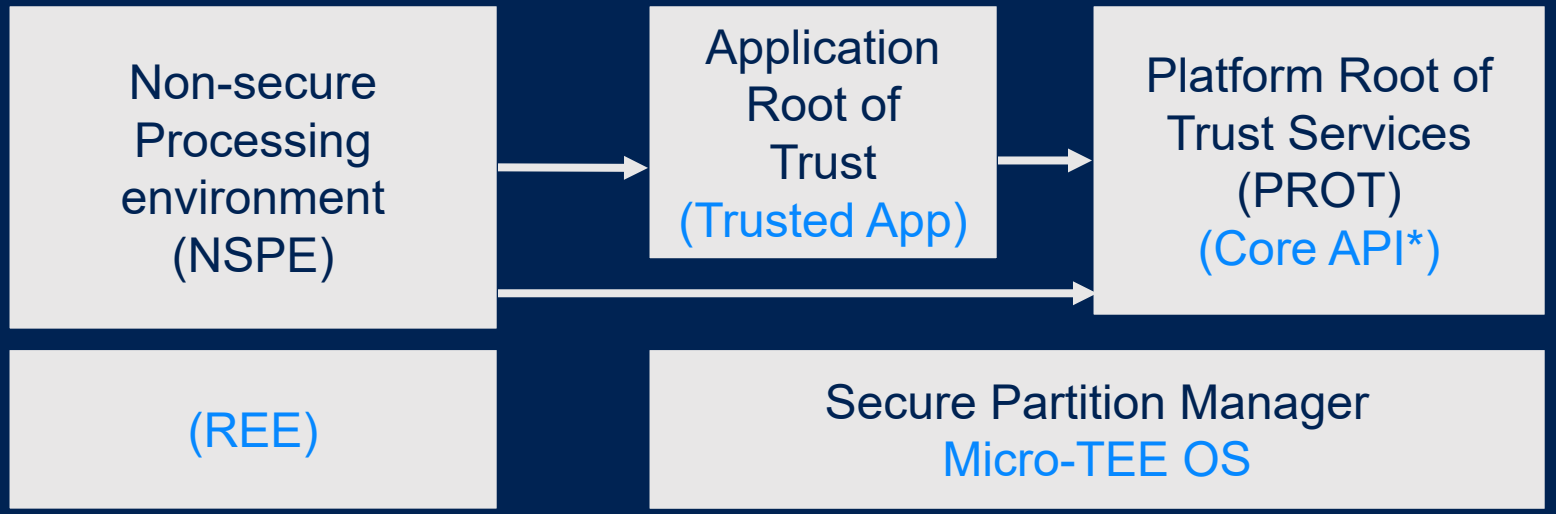
- Adopted as a crypto library
  - mbedTLS
- As an interoperability layer
  - To provide access to HW acceleration in micro controllers.
- “Under discussion”
  - AUTOSAR CSP internal APIs
- PSA APIs also make sense in micro-TEEs
  - Service APIs from “non secure world”
  - Service APIs from “secure world” (Trusted Apps)

FF-M (Firmware foundation for Micro-Controllers)

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]



Firmware Update

Remote Attestation/Lifecycle

Secure Storage

Crypto Functions

Secure Boot*
(Required for PSA Certification but not part of spec)

Current Status

GlobalPlatform traditional TEE APIs are “a bit big” for micro-TEEs

- This does not mean they could not be squeezed to fit
- But no commercial products [that I’m aware of] on smaller micro-controllers

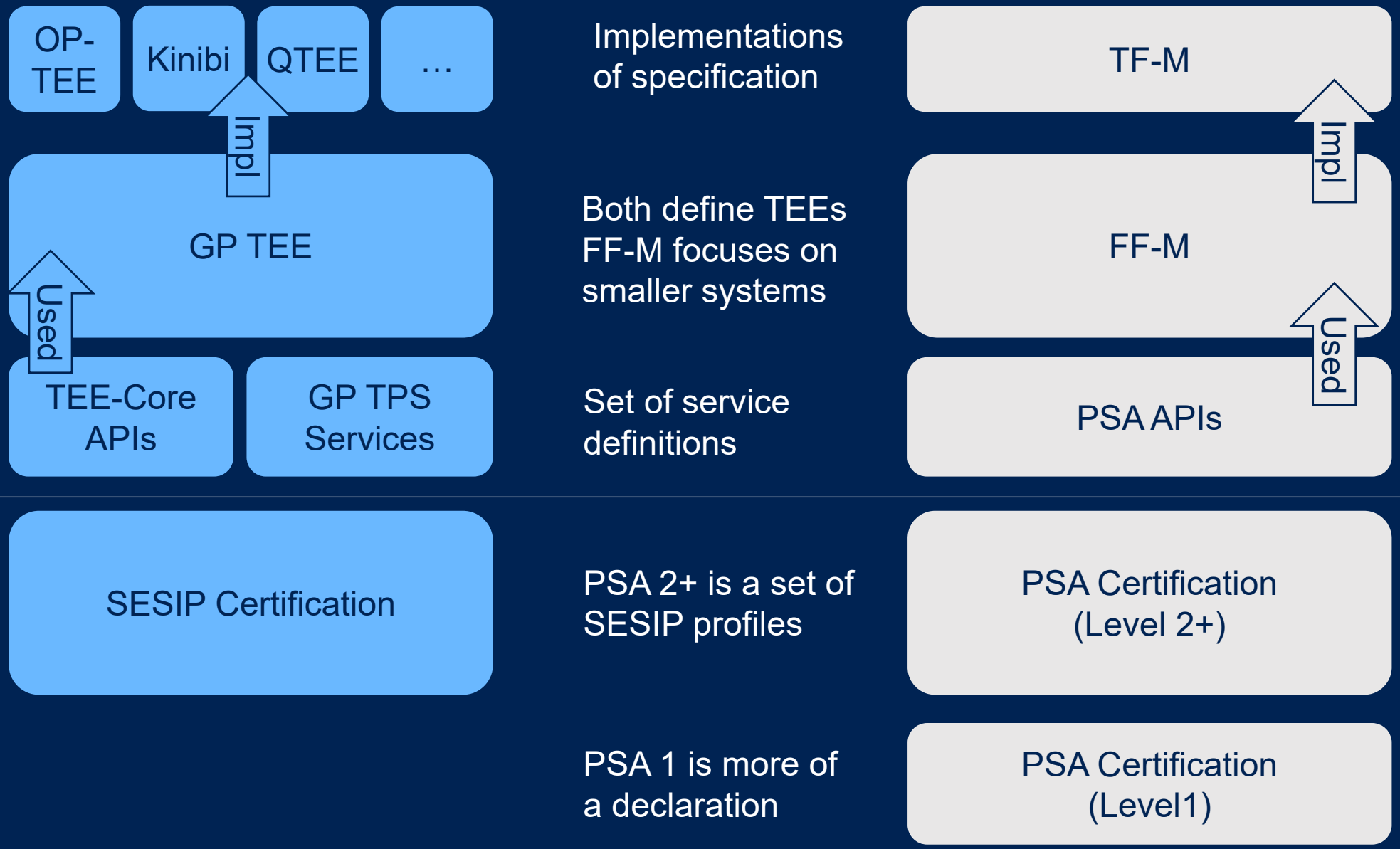
FF-M is a specification that is arguably a better fix

- There is one commercial-grade implementation (Arm TF-M) but it is ported to many chipsets with an active community

Arm has recently donated the PSA and FF-M specifications to GlobalPlatform

- Details of future development and governance [etc] are all TBD
- Note that Arm has already donated the PSA Certification scheme [but that is broader than both PSA APIs and FF-M]

TEE-Micro TEE comparison



Global Platform®

Securing the digital future

→globalplatform.org