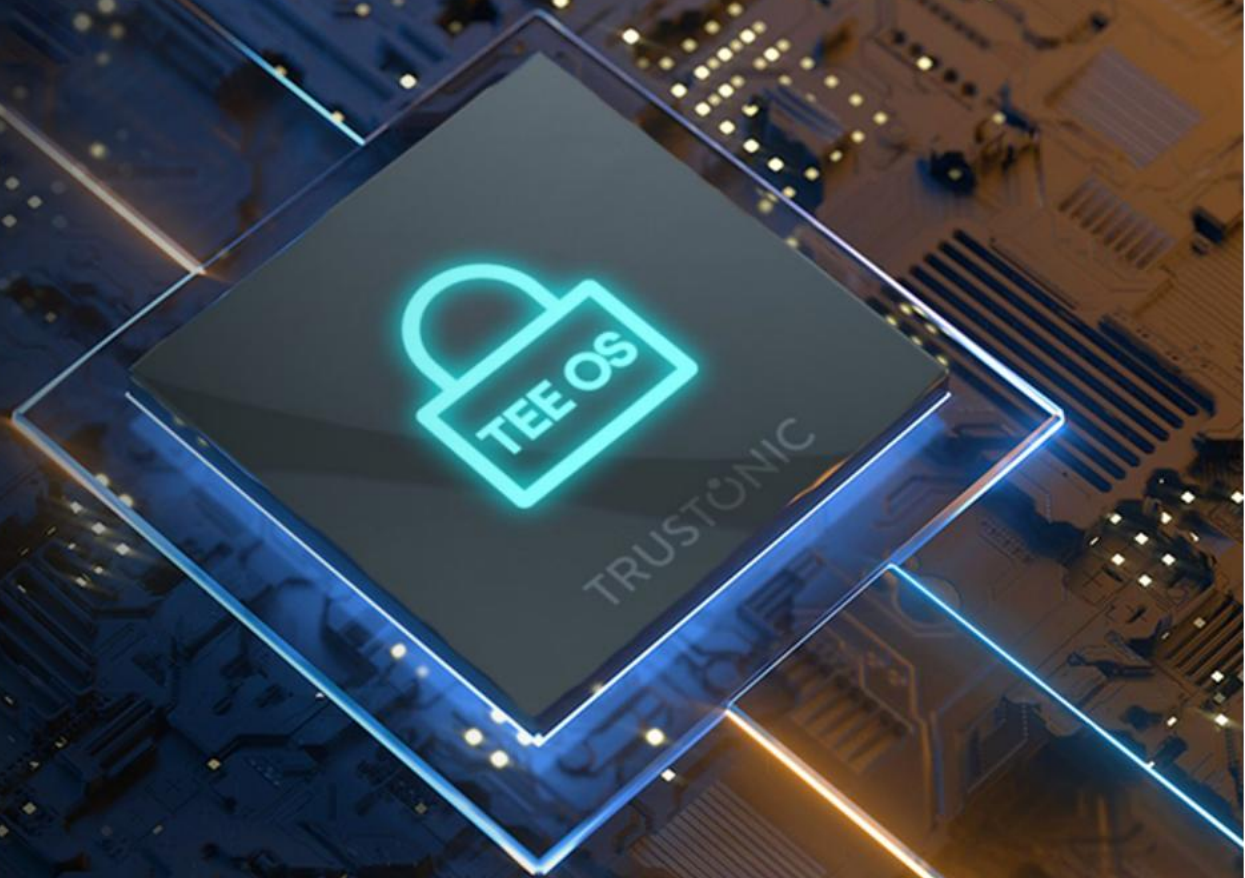
Trusted Execution Environments

Introduction & Current focus



Richard Hayton
- Trustonic Ltd
- Chair Automotive Task Force, GlobalPlatform
- Chair TES Committee, GlobalPlatform

TRUSTONIC

Global Platform™

Protecting a modern operating system

Modern operating systems such as Linux and Android are extremely complex

They are use *everywhere* from Phones to Computers, and increasingly within larger ECUs in vehicles

Think of the Operating System as a city, with many different activities going on at once

最新のオペレーティング・システムの保護

LinuxやAndroidのような最新のオペレーティング・システムは非常に複雑です。

携帯電話からコンピュータまで、*あらゆる場所*で使用されており、最近では自動車の大規模なECUでも使用されるようになっています。

ここでは、オペレーティング・システムを、さまざまな活動が一度に行われている都市にたとえてみます。

Protecting a modern operating system

Attacks can start in one building and then spread to another. The complexity of the operating system makes it inherently hard to protect.

最新のオペレーティング・システムの保護

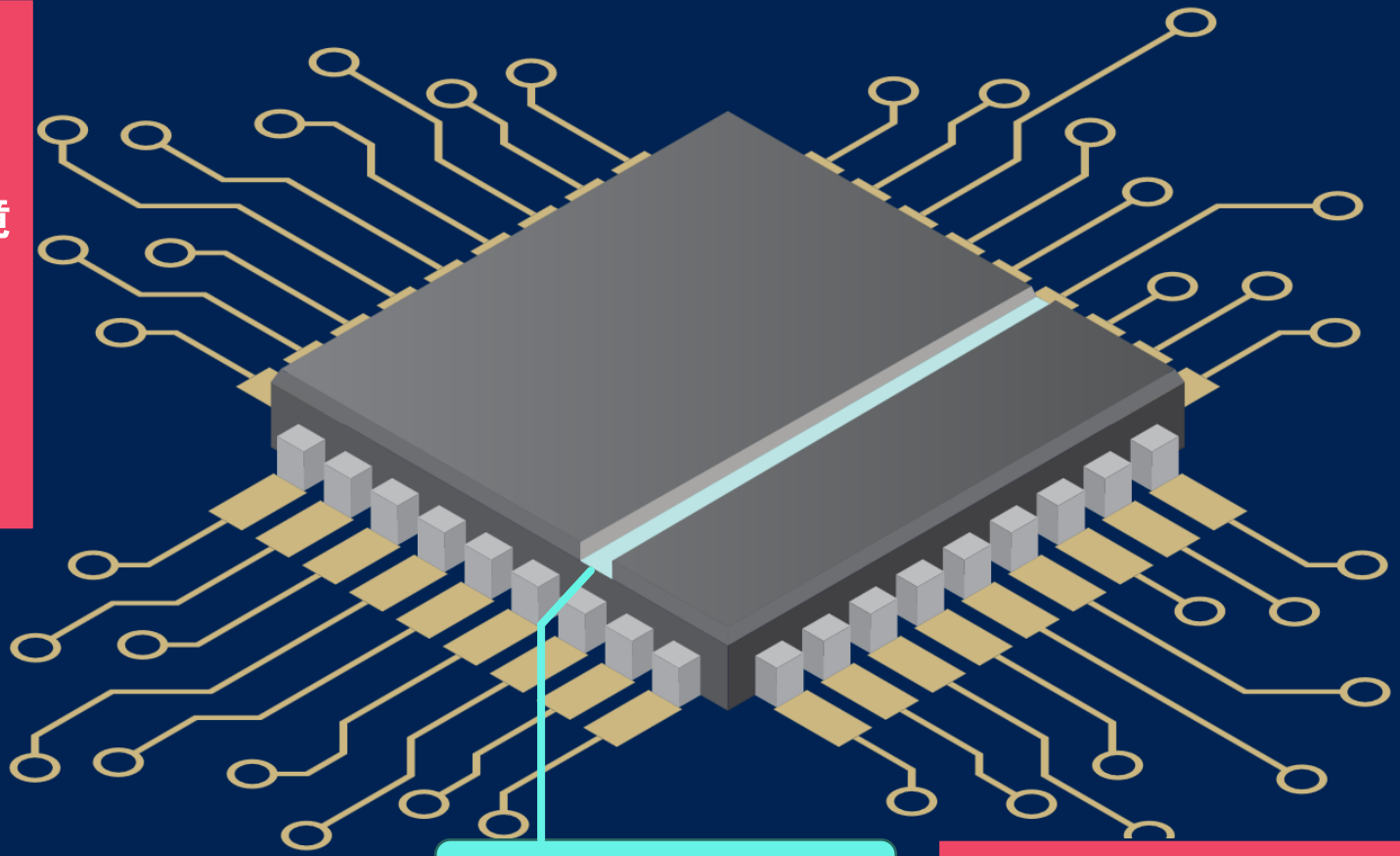
攻撃者は1つの建物から攻撃を始め、別の建物へと広げていきます。オペレーティング・システムは複雑なため、本質的に保護が難しい。

Trusted Execution Environments

Based on hardware capabilities to provide separation that is common in modern CPUs

Trusted Execution Environment (TEE)
= 信頼された実行環境

最近のCPUでは一般的となっている分離を実現するハードウェア機能に基づいています。



Hardware Isolation Support
(E.g. Arm TrustZone)

ハードウェア分離をサポート

(例：ArmのTrustZone)

Global Platform™

Trusted Execution Environments

GlobalPlatform defined a TEE Operating System that leverages this hardware capability to provide security functions

Trusted Execution Environment (TEE)
= 信頼された実行環境

GlobalPlatform は、このハードウェア機能を活用してセキュリティ機能を提供する TEE オペレーティングシステムを定義しました。

Regular Execution Environment

REE

REE = 通常の実行環境

TEE

Trusted Execution Environment

TEE = 信頼された実行環境

Hardware Isolation Support
(E.g. Arm TrustZone)

ハードウェア分離をサポート

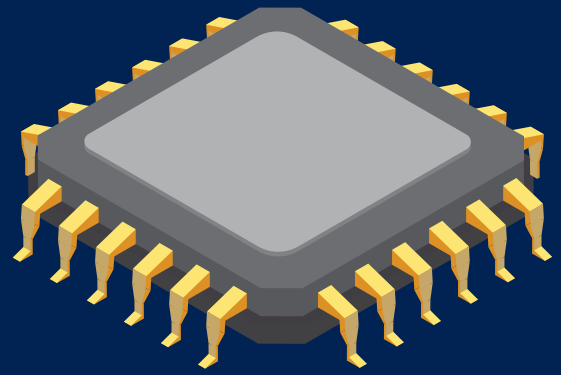
(例：ArmのTrustZone)

Global Platform™

Is there a TEE on my system?

私のシステムにTEEはありますか？

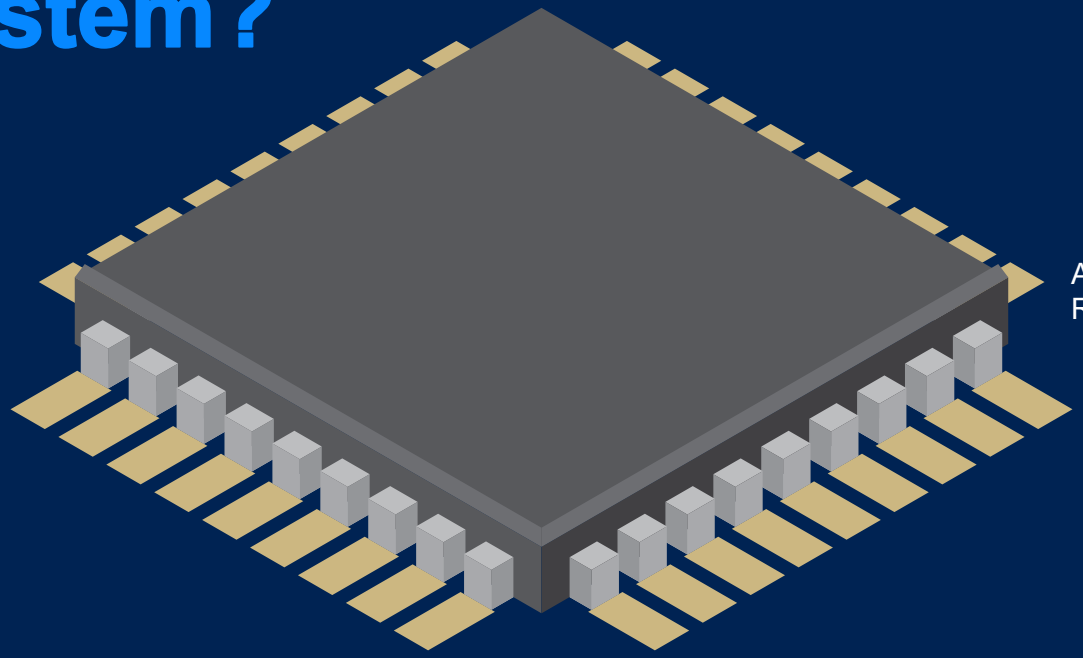
Arm Cortex-M
Risc-V embedded



Smaller “microcontrollers” commonly used in single-purpose ECUs typically do not have a TEE OS

Use of a hardware keystore is much more common in automotive.

単一目的のECUで一般的に使用される小型の「マイクロコントローラ」は、通常、TEE OSを搭載していません。
ハードウェア鍵ストアの使用は、自動車業界ではより一般的である。



Arm Cortex-A
Risc-V (soon)

Larger “microprocessors” used in larger ECUs and domain, or zonal, controllers typically DO have the hardware capabilities for a TEE and TEE Operating Systems are common.

大型のECUやドメイン（ゾーン）コントローラに使用される大型の「マイクロプロセッサ」は、通常、TEE用のハードウェア機能を備えており、TEEオペレーティングシステムが一般的です。

TEEs have evolved

TEEs were first standardized over 15 years ago

Whilst the security promise made by TEEs have not changed, the functional capabilities of TEEs have increased significantly

- Single Threaded → Symmetric Multi-Processing
- Small Memory → Effectively unlimited memory
- Limited Storage → Effectively unlimited storage
- Limited Function → Peripheral & Network access
- Single Client OS → Hypervisor Support

TEEの進化

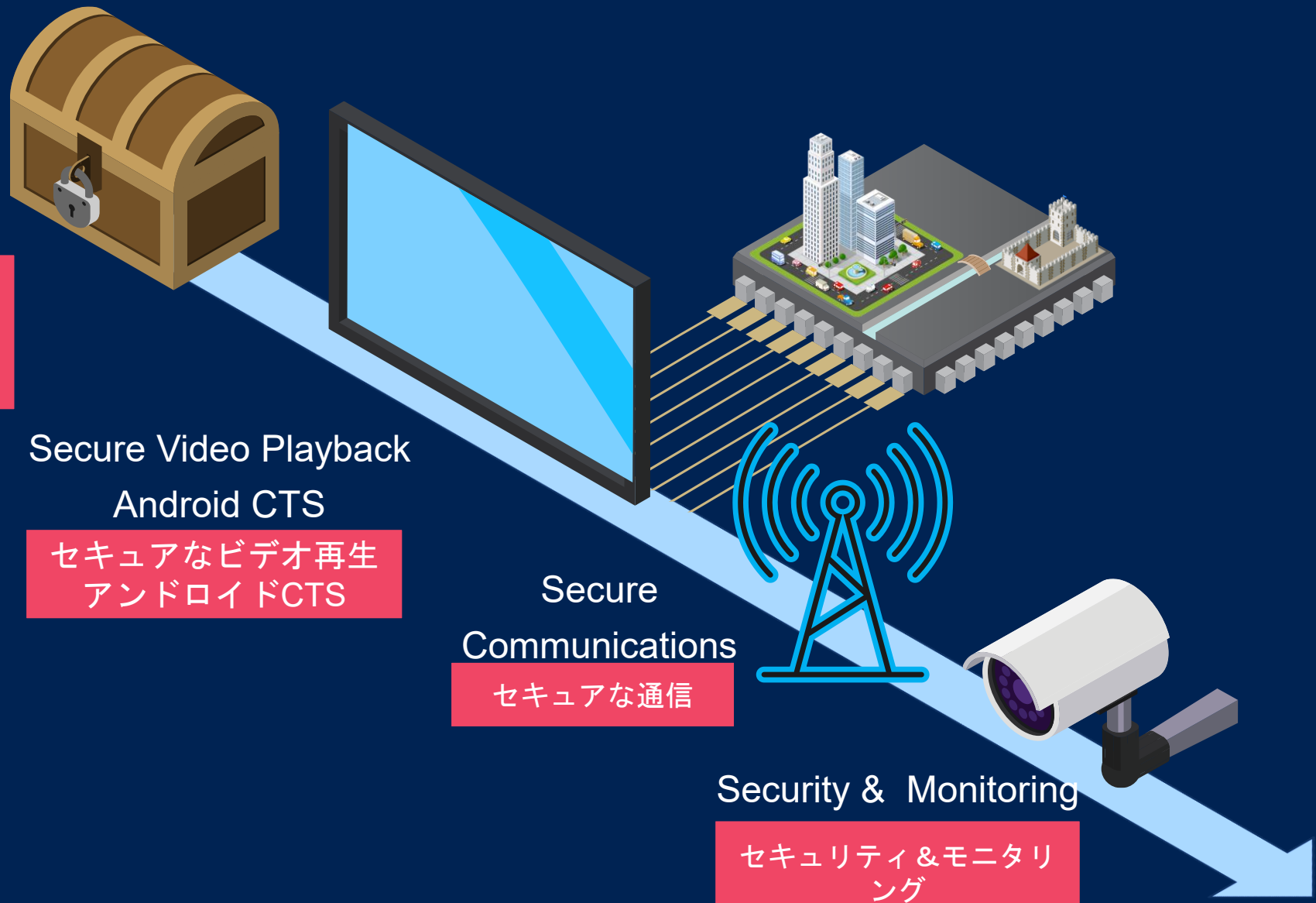
TEEが最初に標準化されたのは15年以上前。

TEE がコミットするセキュリティに変わりはありませんが、TEE の機能的な能力は大幅に向上しています。

- シングルスレッド → シンメトリック・マルチプロセッシング
- 小メモリ → 実質無制限メモリ
- 限定ストレージ → 実質無制限ストレージ
- 限定された機能 → 周辺機器とネットワークへのアクセス
- 単一のクライアントOS → ハイパーバイザーのサポート

Use Case Evolution in Automotive

自動車におけるユースケースの進化



Key Store
(TEE-HSM)

キーストア
= キーの安全な保存
(TEE-HSM)

Secure Video Playback
Android CTS

セキュアなビデオ再生
アンドロイドCTS

Secure
Communications

セキュアな通信

Security & Monitoring

セキュリティ＆モニタリング

Trends

Data Collection and Storage

- Diagnostic and Performance Data
- Personal / Driver Data (Privacy)
- Data collection for AI training

Secure & Robust Supply Chain

- Secure Manufacture & Attestation
- OTA Update
- Silicon / SW Vendor independency

Future & Regulation Readiness

- Post Quantum Cryptography
- Defensible design choices
- Global .v. Local designs

データの収集と保存

- 診断とパフォーマンス・データ
- 個人情報（プライバシー）
- AIトレーニングのためのデータ収集

安全で堅牢なサプライチェーン

- 安全な製造と認証
- OTAアップデート
- シリコン / SWベンダーの独立性

将来と規制への備え

- ポスト量子暗号
- 防御可能なデザインの選択
- グローバル・デザインvsローカル・デザイン

Data

Unlike HSMs that have a small and fixed amount of storage for keys, TEEs support effectively unlimited storage

GlobalPlatform standardized a simple flat file system, original used mainly for configuration and keys

Increasingly customers are asking for more

- Large files, such as biometric models
- Large numbers of files, such as to support user profiles and applications such as messaging and media
- Structured data storage, for on-device analysis of datasets

キー用のストレージが少量かつ固定なHSMと異なり、TEE は実質的に無制限のストレージをサポートしています。

GlobalPlatformはシンプルなフラットファイルシステムを標準化しました。

ユーザはますます多くのことを求めるようになってきています：

- バイオメトリックモデルなどの大容量ファイル
- ユーザープロファイルやメッセージング、メディアなどのアプリケーションをサポートするための大量のファイル
- 構造化されたデータストレージ、データセットのオンデバイス分析用

Data

Example, recording actual .v. posted speed in a database table in order to detect errors in mapping data.

例えば、マッピングデータのエラーを検出するために、データベースのテーブルに実際の vs.公示速度を記録する。

#	DriverId	Timestamp	RoadId	Start	Distance	PostedLimit	ActualSpeed	Discrepancy	ClearRoad
0	Driver1	1751130000	9000	4000	500	60	43	-17	true
1	Driver1	1839330000	9000	3800	700	60	40	-20	true
2	Driver1	1923510000	9000	3900	600	60	37	-23	false
3	Driver2	2154810000	9000	3900	600	60	39	-21	false
4	Driver2	2244810000	9000	3700	800	60	38	-22	true
5	Driver1	1717230000	9001	0	500	60	43	-17	true
6	Driver1	1803810000	9001	0	500	60	40	-20	true
7	Driver1	1887510000	9001	0	500	60	37	-23	false
8	Driver2	2148810000	9001	0	500	60	39	-21	false
9	Driver2	2237730000	9001	0	500	60	38	-22	true

Global Platform™

Attestation & Secure Supply Chain

Supply chain integrity is gaining focus, as it is significant attack path.

There is also a desire from OEMs to use components from many manufacturers, especially to comply with regional needs, or handle shortages.

During vehicle lifetime, software may be modified or updated, and configuration changed.

Attestation is a means to enable devices to securely report on their current status, and for third parties to rely on this data to make key decisions – for example whether to enable autonomous functionality.

サプライチェーンの完全性は、クリティカルな攻撃経路であるため、注目を集めている。

また、特に地域的なニーズに対応するため、あるいは供給不足に対応するため、多くのメーカーの部品を使用したいというOEMの要望もある。

車両のライフサイクルにおいて、ソフトウェアの修正や更新、構成変更を行う可能性がある。

認証(アテステーション)は、デバイスが現在の状態を安全に報告できるようにするための手段であり、第三者が重要な意思決定（例えば、自律機能を有効にするかどうかなど）を行う際に、このデータを信頼するに足ることを確認する手段である。

Attestation & Secure Supply Chain

GlobalPlatform TES committee has recently created an Entity Attestation Protocol Specification which will be publicly available soon.

It is based on the IEFT EAT standard, which has just been formally published, but has been in used for a while.

Future work is turning to standarizing the processing of Attestation, for example the open source Veraison project.

GlobalPlatform TES Committeeは最近、エンティティ認証プロトコル仕様書を作成し、間もなく一般公開される予定です。

これはIETFのEAT規格に基づいており、正式に発表されたばかりだが、すでに利用されている仕様です。

将来的には、例えばオープンソースのVeraisonプロジェクトなど、認証の処理を標準化することになるだろう。

Future Ready Crypto?

Looking to the future, much focus has been on Post Quantum Cryptography.

NIST has standardized a number of algorithms, and GP has added these to the TEE Core API

Some regions are adopting NIST recommendations, but it is unlikely we will get global standardization

- China is defining its own algorithms.
- Europe is recommending HYBRID schemes
- There is some disagreement over PQ-safe key sizes for AES.

将来を見据えて、ポスト量子暗号に注目が集まっています。

NIST は多くのアルゴリズムを標準化し、GP はこれらを TEE コア API に追加しました。

NISTの勧告を採用している地域もあるが、世界的な標準化が実現する可能性は低い

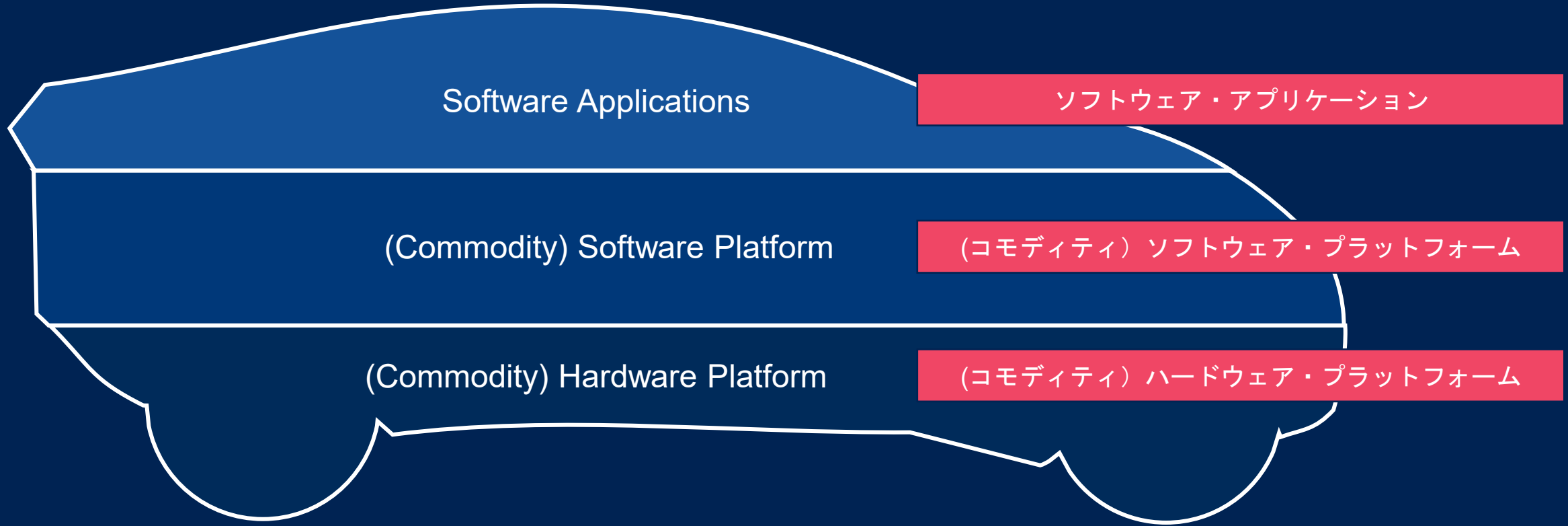
- 中国は独自のアルゴリズムを定義しています。
- 欧州はHYBRID方式を推奨しています
- AESのPQ-safeな鍵のサイズについては、意見が分かれています。

Future Ready Crypto?

- PQC algorithms generally have large keys sizes and/or large signature sized
- Some algorithms are not suitable for hardware implementations – but this does not affect most TEEs
- PQC performance is on a par with traditional algorithms.
- Symmetric algorithms (e.g. AES) remain safe.
  - NIST asserts 128 bit remains sufficient
  - Some European entities recommend 256 bit

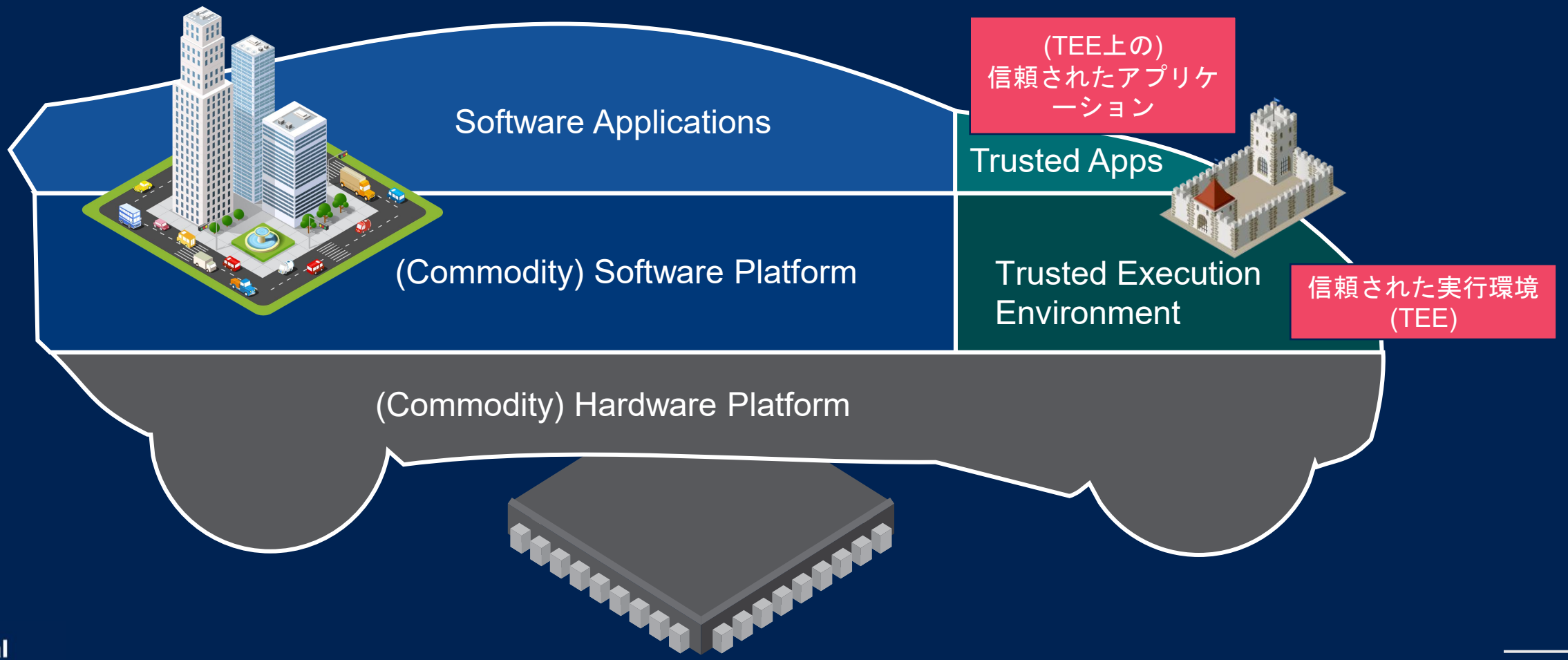
- PQC アルゴリズムは一般に、大きな鍵サイズと大きな署名サイズを持つ。
- アルゴリズムによっては、ハードウェア実装に適さないものもある。
- PQCの性能は従来のアルゴリズムと同等だ。
- 対称アルゴリズム（AESなど）は安全なままだ。
  - NISTは128ビットで十分であるとしている。
  - 256ビットを推奨する欧州の団体もある

Software Defined Vehicles



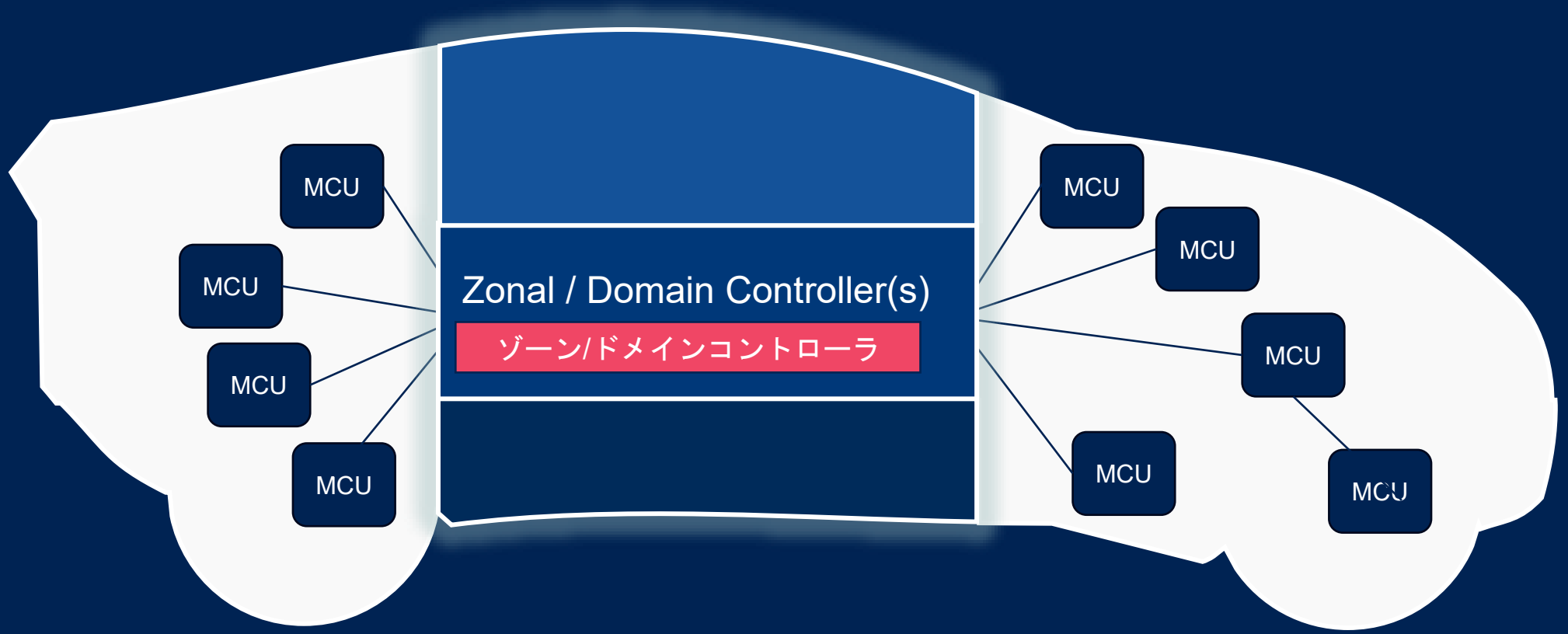
TEE within Software Defined Vehicle

TEEを活用したSDV



Reality is more complex – Lots of MCUs

実際はより複雑 . . . ― 数多くのMCUが存在



Q. Can we put TEEs on MCUs?

質問：MCUにTEEを搭載できますか？

Is the MCU problem different from the CPU problem?

MCUの問題はCPUの問題とは違うのですか？

Typically, similar needs but far less flexibility required
(e.g. single purpose)

通常、同様のニーズがあるが、必要な柔軟性ははるかに低い
(単一目的など)

Is the GlobalPlatform TEE suitable for MCUs?

GlobalPlatform TEEはMCUに適していますか？

Designed to be generic – but are arguably too broad / unnecessarily complex for MCU use cases

汎用的であるよう設計されているが、MCUのユースケースには広すぎる／不必要に複雑である。

What products exist today / will exist in future?

現在存在する／将来存在する製品は何か？

No commercial GP based MCU-TEEs
But many products using ARM PSA

市販のGPベースのMCU-TEEはない
しかし、ARM PSAを使用する製品は多い

A Micro-TEE?

マイクロTEE?

M-REE

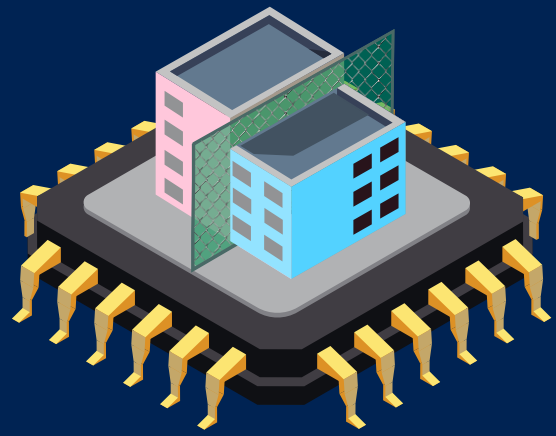
General Purpose Partition

M(マイクロ) REE
(=通常の実行環境)

通常処理のパーティション

APIs?
GlobalPlatform TEE APIs or
Arm Platform Security Architecture?

API？
GlobalPlatform TEE API
Armプラットフォームのセキュリティアーキテクチャ？



Certification / Compliance
Common Criteria, SESIP or other?

認証 / コンプライアンス
コモンクライテリア、SESIP、その他？

M-TEE

Security Focused Partition

M(マイクロ) TEE
(=信頼された実行環境)

セキュリティに特化したパーティション

Supporting Safety Critical Applications

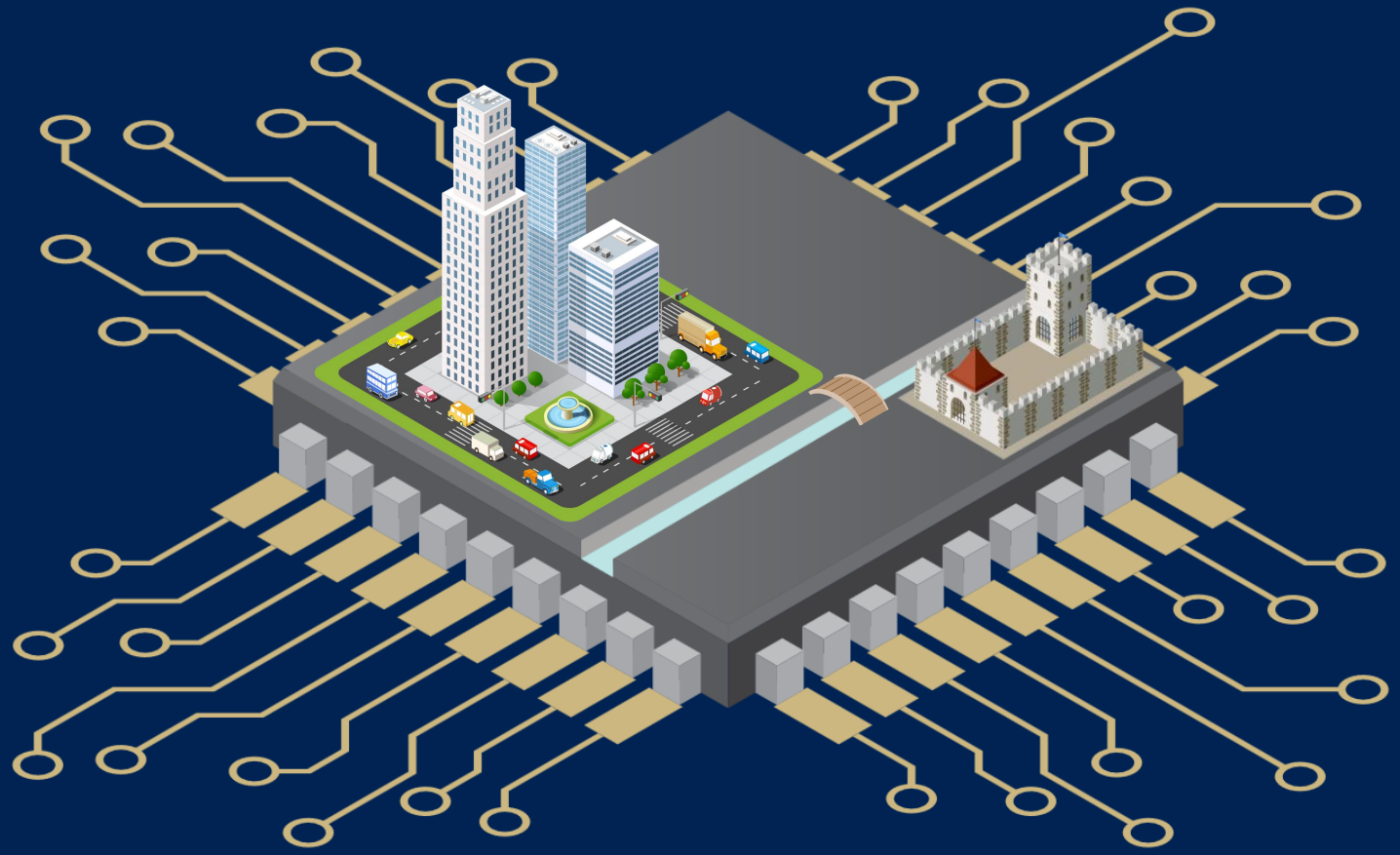
安全性への要求度が高いアプリケーションのサポート

A modern “City-like” operating system enables lots or different applications to run at once, but is generally not suitable for safety critical or real time functions

Supporting safety critical functionality in Software Defined Vehicles remains an active area of discussion

最新の “City-like(街になぞらえられる) ”オペレーティングシステムは、一度に多くのアプリケーションや異なるアプリケーションを実行することができるが、一般的に安全性への要求度が高い機能やリアルタイム機能には適していない。

Software Defined Vehicleにおける安全性への要求度が高い機能のサポートは、依然として活発な議論が行われている。

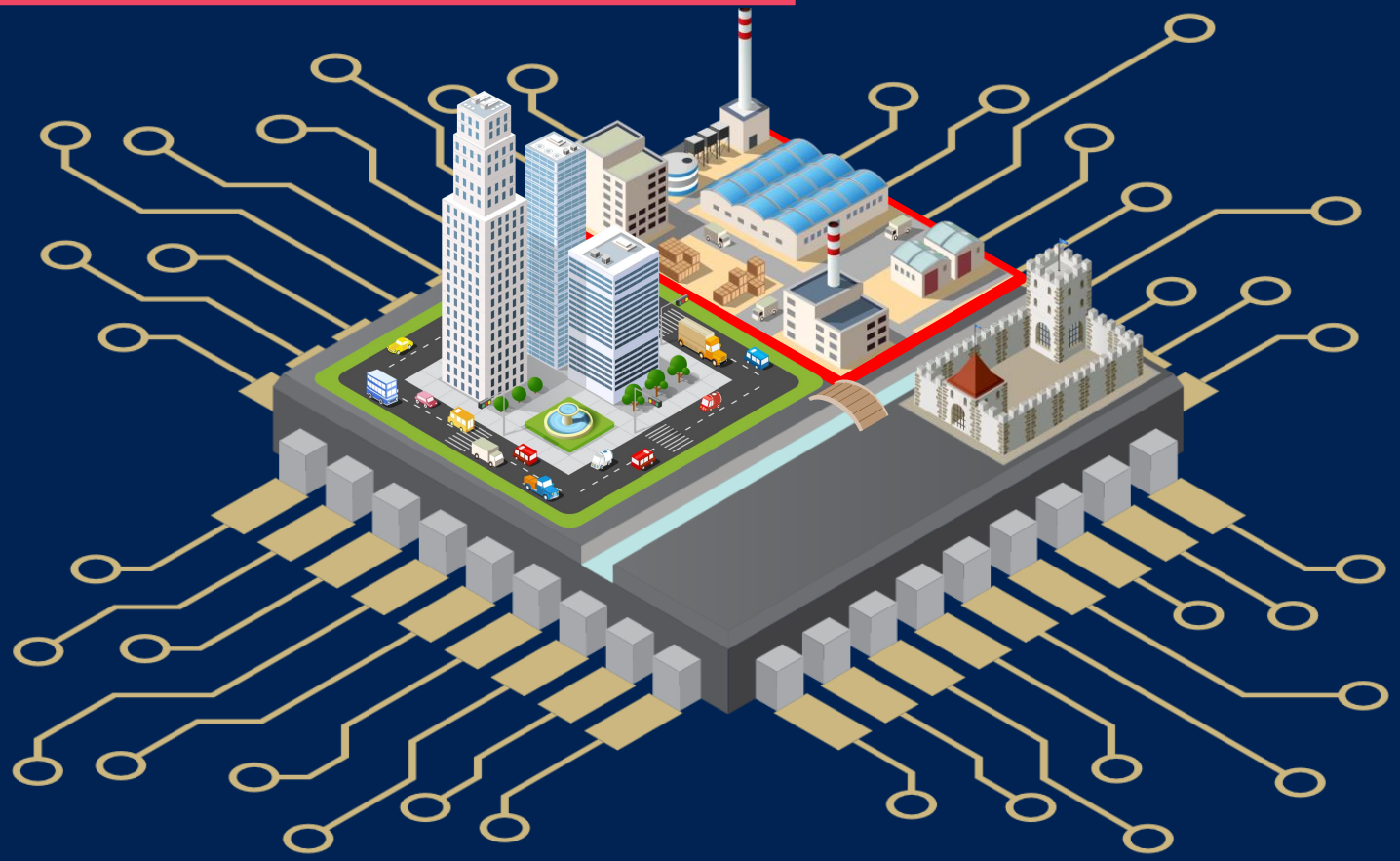


Supporting Safety Critical Applications

安全性への要求度が高いアプリケーションのサポート

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

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



一般的なアプローチとしては、安全性への要求度が高いアプリケーションに特化した第2、第3のオペレーティングシステムを追加する方法がある。

議論すべきポイントとして、TEEがどのように（あるいは、どのように）混合クリティカリティクライアントをサポートすべきかについて、がある。

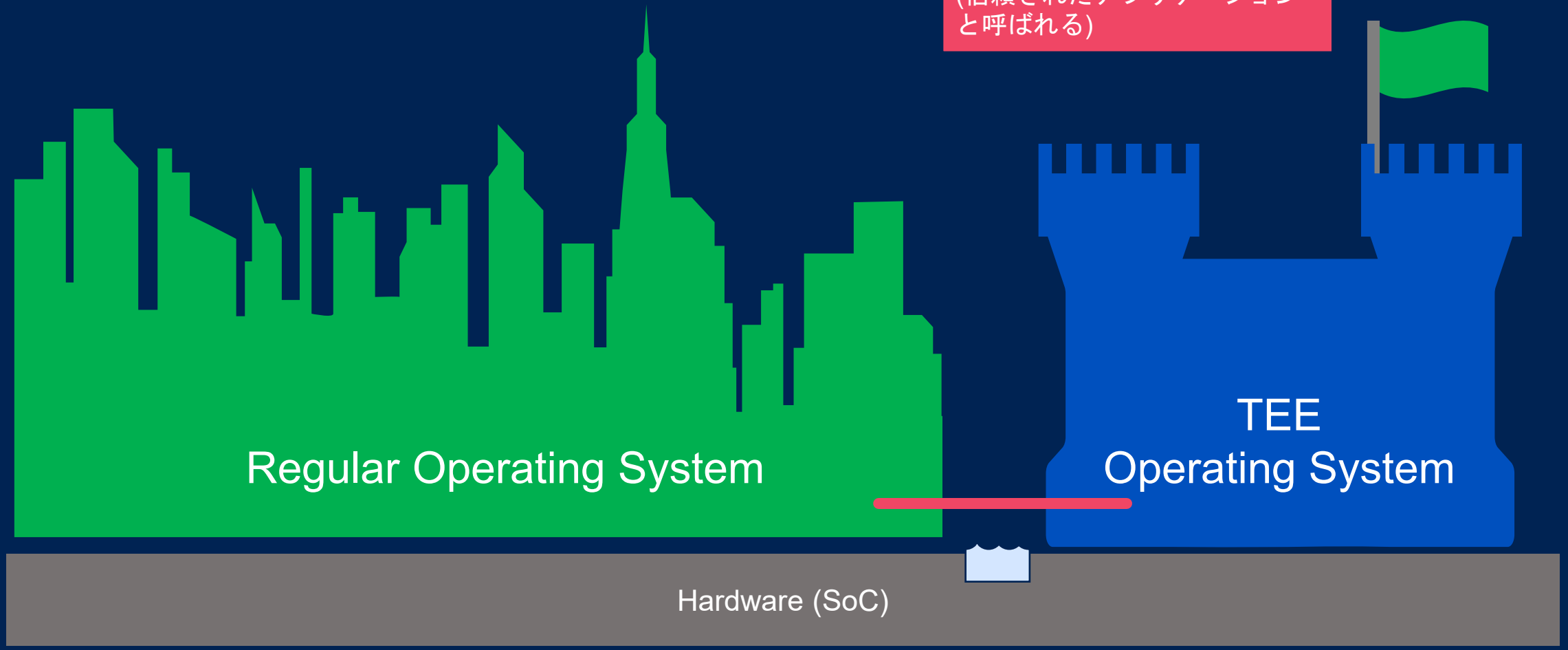
Architecture

TEE supports multiple isolated services
(called Trusted Applications)

Early TEE architecture

初期のTEEアーキテクチャ

TEE は、複数の分離された
サービスを提供
(信頼されたアプリケーション
と呼ばれる)



Architecture

Evolution – multiple Operating Systems, One TEE

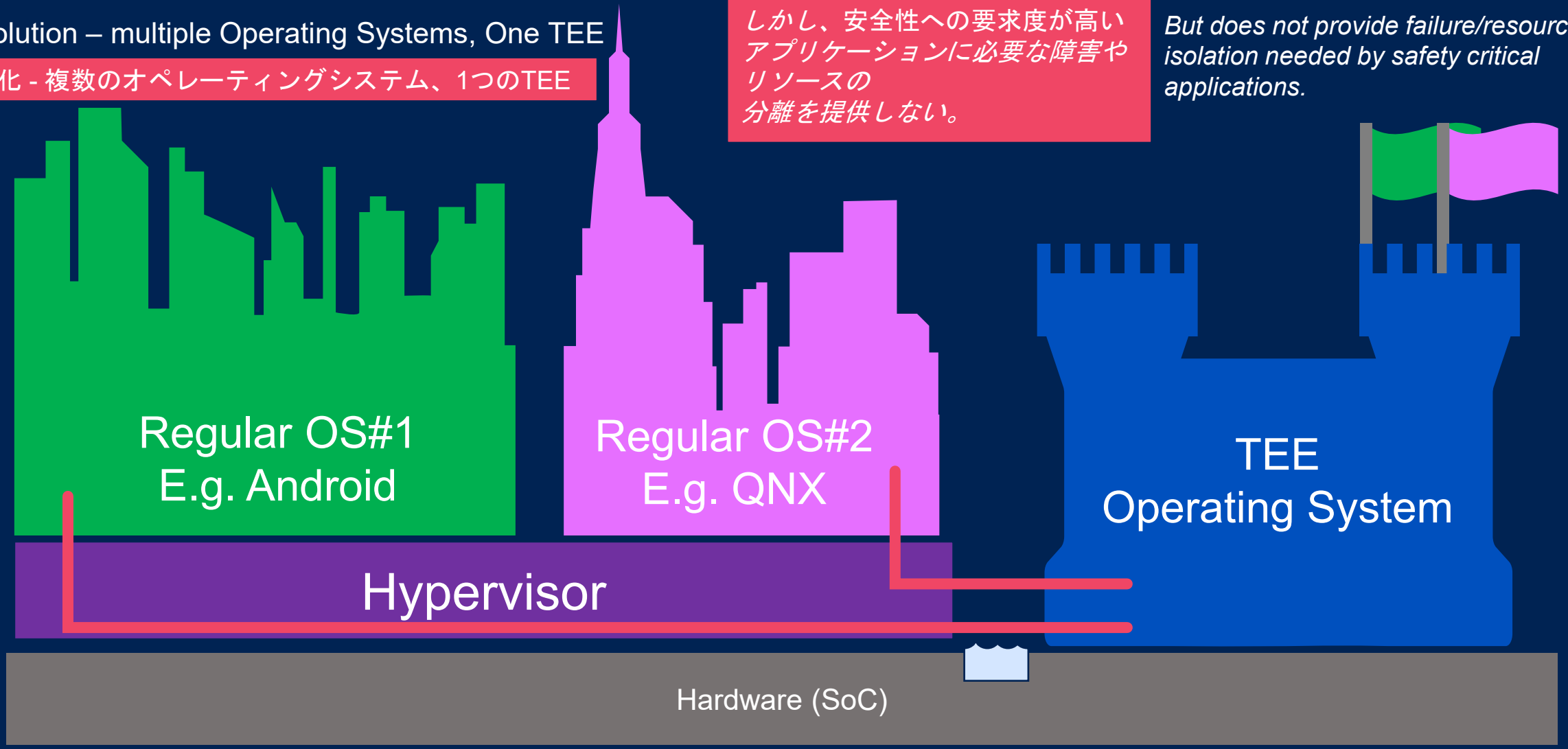
進化 - 複数のオペレーティングシステム、1つのTEE

既存の信頼されたアプリケーションの分離
セキュリティの境界を確保する

しかし、安全性への要求度が高いアプリケーションに必要な障害やリソースの
分離を提供しない。

Existing Trusted Application Isolation
Ensures security boundaries

But does not provide failure/resource isolation needed by safety critical applications.



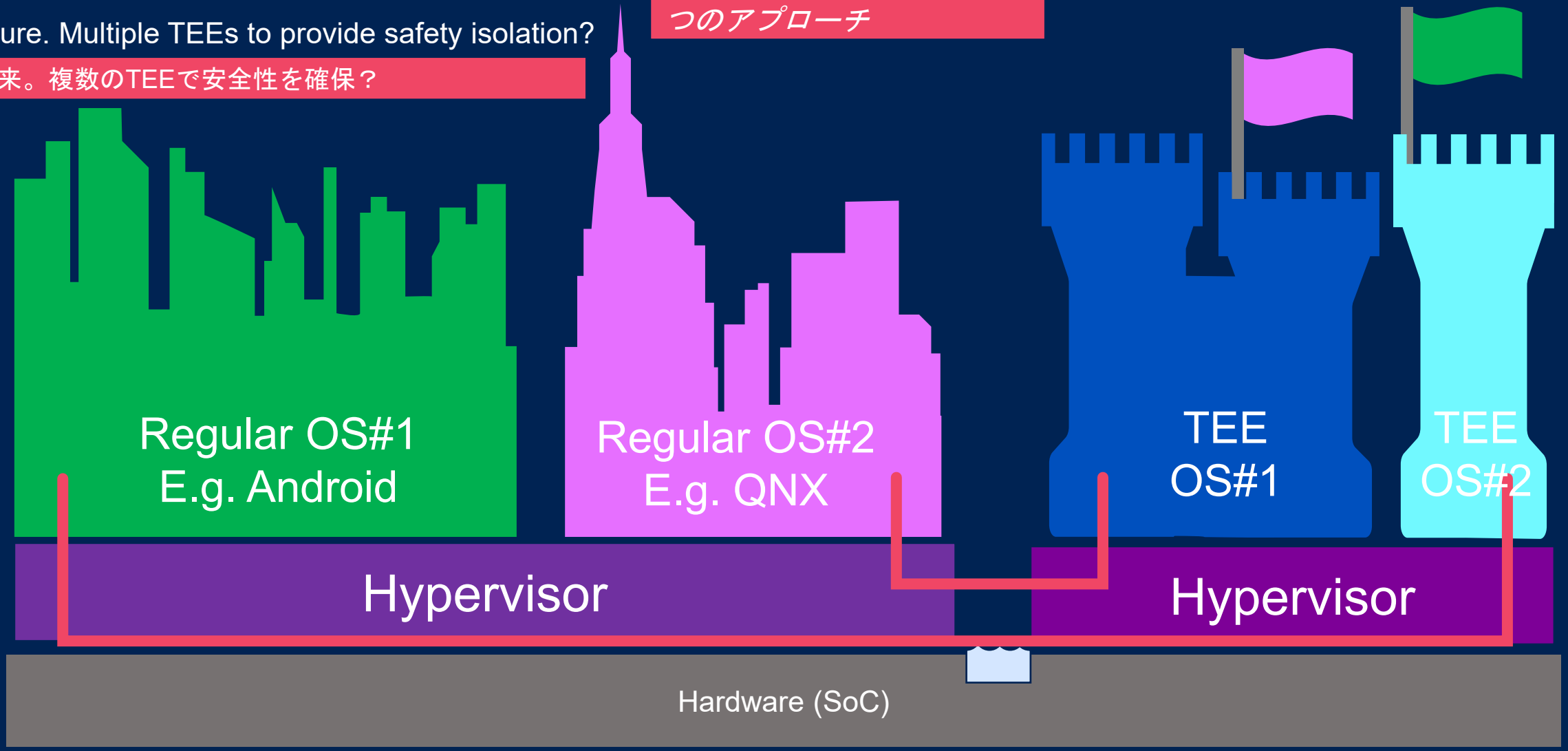
Architecture

Future. Multiple TEEs to provide safety isolation?

将来。複数のTEEで安全性を確保？

セキュアな領域におけるハイパーバイザーは
安全な分離を可能にする一つのアプローチ

Hypervisors in the secure world provide one approach to enabling safety isolation



Summary

Trusted Execution Environments are a mature technology used in billions of devices.

They are used extensively in IVI and other domain controllers, and use is growing significantly

GlobalPlatform offers TEE Certification, and many companies use Common Criteria labs, with TEE Operating Systems certified up to EAL5+ (TRUSTONIC)

There is also some interest in certifying broader solutions that leverage TEEs, likely using GlobalPlatform SESIP certification.

信頼された実行環境は、何十億ものデバイスで使用されている成熟した技術である。

IVIやその他のドメインコントローラで広く使用されており、その使用は著しく増加している。

GlobalPlatformはTEE認証を提供し、多くの企業がコモンクライテリアラボを利用しており、TEEオペレーティングシステムはEAL5+まで認証されています(Trustonic)。

また、GlobalPlatform SESIP 認証を使用して、TEE を活用する広範なソリューションの認証にも関心がある。

Summary

For automotive there are several key areas

- Replacing or augmenting HSMs for performance, crypto agility or other flexibility.
- More and larger secure applications – such as for data capture and processing.
- Support for Microcontrollers (Micro-TEE)
- Support for safety critical domains (Mixed-Criticality)
- Attestation and Lifetime services

TRUSTONIC

Some commercial TEEs address these needs today – and standardization work is ongoing in the TES committee at GlobalPlatform.

自動車にはいくつかの重要な分野がある。

- パフォーマンスのためのHSMの交換または増強、暗号の俊敏性、その他の柔軟性
- データの取得や処理など、より大規模で安全なアプリケーション。
- マイクロコントローラのサポート（Micro-TEE）
- 安全性への要求度が高いドメインのサポート（クリティカル度の混合）
- 認証およびライフタイム・サービス

現在、いくつかの商用TEEはこのようなニーズに対応しており、GlobalPlatformのTES committeeでは標準化作業が進行中です。