woven by TOYOTA

Trusted Execution Environment (TEE) in automotive

May 22nd, 2025

Vincent Mailhol

Senior Product Security Engineer
vincent.mailhol@woven.toyota

Meeting Agenda

About me

- Joined Woven by Toyota in October 2020
- Maintainer of the Linux kernel CAN subsystem (a.k.a Socket CAN)
- Member of GlobalPlatform ATF and TES working groups
- Member of the international standardization working group for the programming language C

01

Software defined vehicle

A story of reusability

Reusable Platform	**TNGA: Toyota New Global Architecture**
History	Physical platform that is used to build Toyota vehicles ● Accounts for 80%+ of all vehicles※ ● Defined variants ● Scales and is reusable

※https://global.toyota/en/mobility/tnga/powertrain2018/feature/

Reusable Platform	**Electronic Platform**
Software	Software platform that is used to build Toyota vehicles ● Defined variants ● Scales and is reusable ● Is certified

Reusable Platform

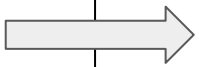
Common hardware components

ARM based chipset

Ideally Cortex-M or Cortex-A

Standardized APIs

Standardized security controls



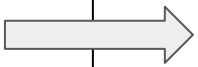
Supplier agnostic builds

Known technology

Known supported features

Reusable software

Testable functionality and features



Provide reusable components for engineers

Provide capability for platform to scale and be independent (loosely coupled) with the hardware

Provide a known secure and safe foundation for developing functionality

Capability to separate out the configuration of the software from the operation of said software

Automotive Specific Items

01
Functional Safety

Our software **must not** have any failure that impacts the safety of the road user, or any person that could be impacted by the road user.

02
Long Lifespan and Quality

It is possible to fix an issue via OTA in modern automobiles, but the cost is high and some items require a service visit.

03
Performance

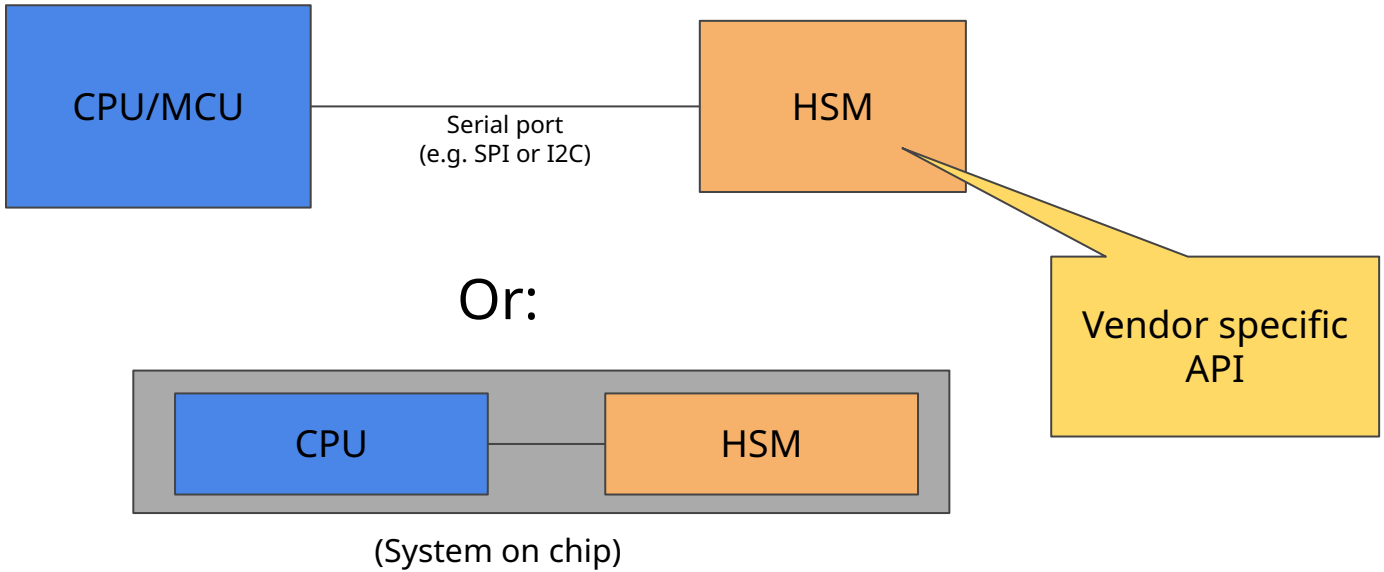
There are some scenarios, required for safety, security, or legislation that require specific actions to happen within a **defined amount** of time.

02

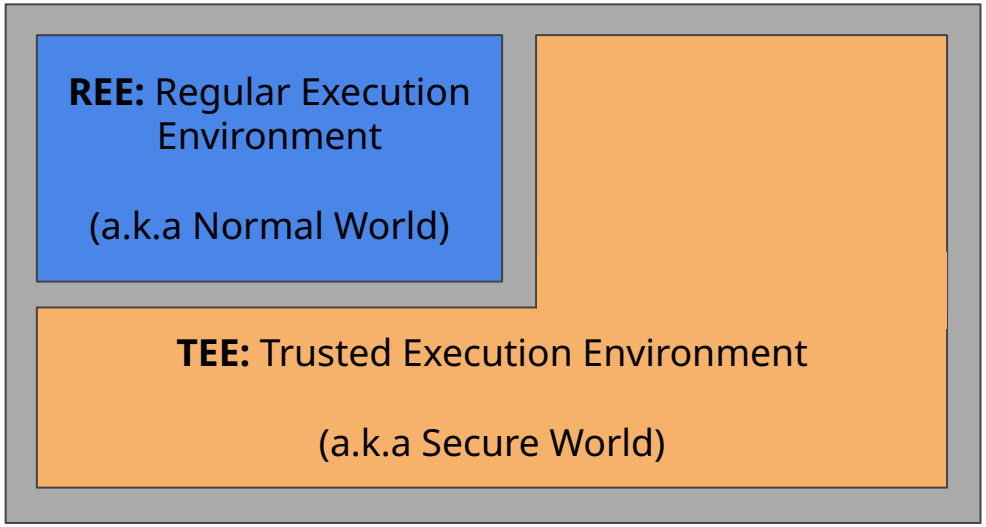
GlobalPlatform Standard API

A quick introduction

Classic automotive hardware security

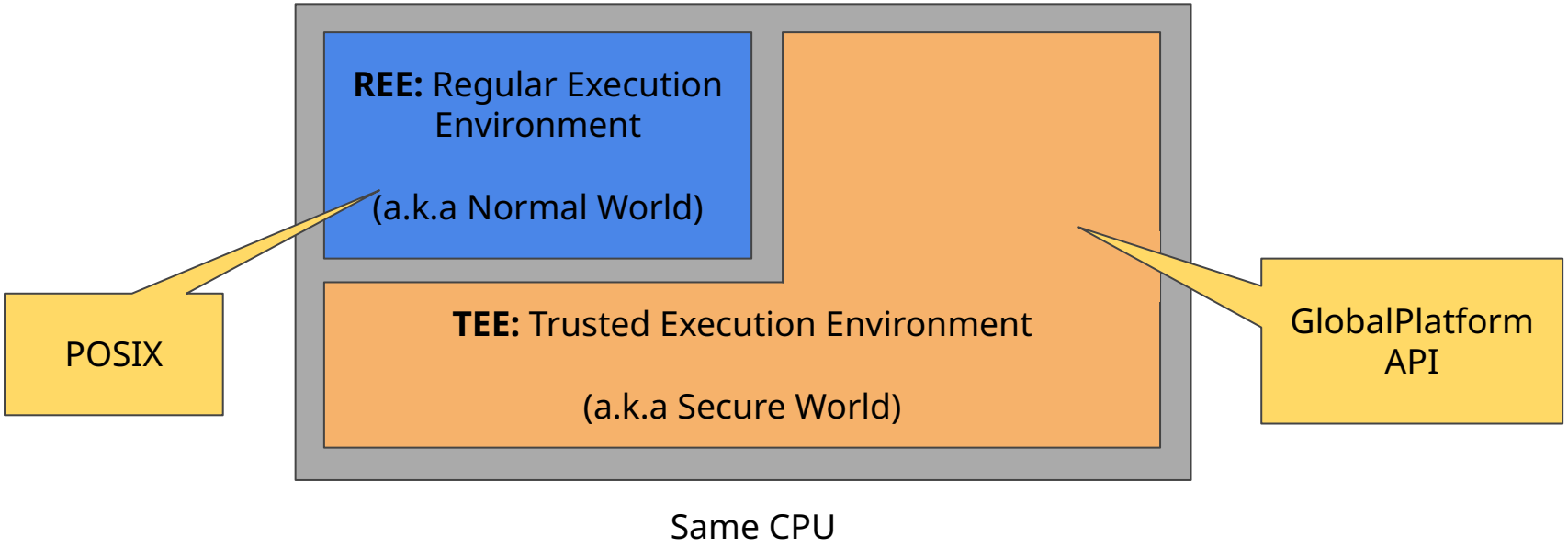


Trusted Execution Environment



Same CPU

Trusted Execution Environment



Benefits of TEE with GP API

01
Cost

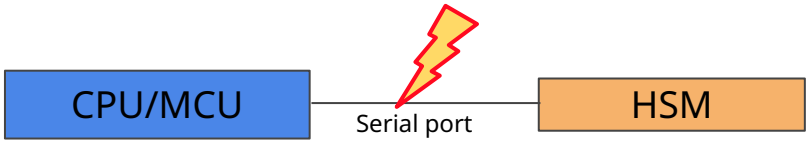
- Available by default on Armv8-A architectures.
- No additional module are needed.
- Code reusable

02
Speed

- Secure and normal operations run on the same CPU: less overhead communication cost.
- CPU is usually faster than HSM.

03
Security

- No serial port: no hardware attacks on PCB traces.



03-1

GlobalPlatform Properties

GlobalPlatform allows to query security properties

Example with time:

Table 7-1: Values of the `gpd.tee.systemTime.protectionLevel` Property

Value	Meaning
100	System time based on REE-controlled timers. Can be tampered by the REE. The implementation SHALL still guarantee that the system time is monotonic, i.e. successive calls to `TEE_GetSystemTime` SHALL return increasing values of the system time.
1000	System time based on a TEE-controlled secure timer. The REE cannot interfere with the system time. It may still interfere with the scheduling of TEE tasks, but is not able to hide delays from a TA calling `TEE_GetSystemTime`.

Source: TEE Internal Core API Specification v1.3.1 §7 Time API

GlobalPlatform allows to query security properties

Code:

```
uint32_t system_time_procection_level = 0;

TEE_GetPropertyAsU32(TEE_PROSPSET_TEE_IMPLEMENTATION,
                     "gpd.tee.systemTime.protectionLevel",
                     &system_time_procection_level);
switch (system_time_procection_level) {
case 100:
        ERROR("Warning: REE-controlled timer");
        break;
case 1000:
        /* TEE-Controller timer: OK */
        break;
default:
        ERROR("Unknown system time protection level?!");
        break;
}
```

GlobalPlatform allows to query security properties

Other properties:

- `gpd.tee.cryptography.*`: check which cryptography algorithms are supported. Allow for crypto agility
- `gpd.tee.trustedStorage.*`: check the protection level of the secure storage

GlobalPlatform allows to query security properties

Idea: introduce new properties for the random generator:

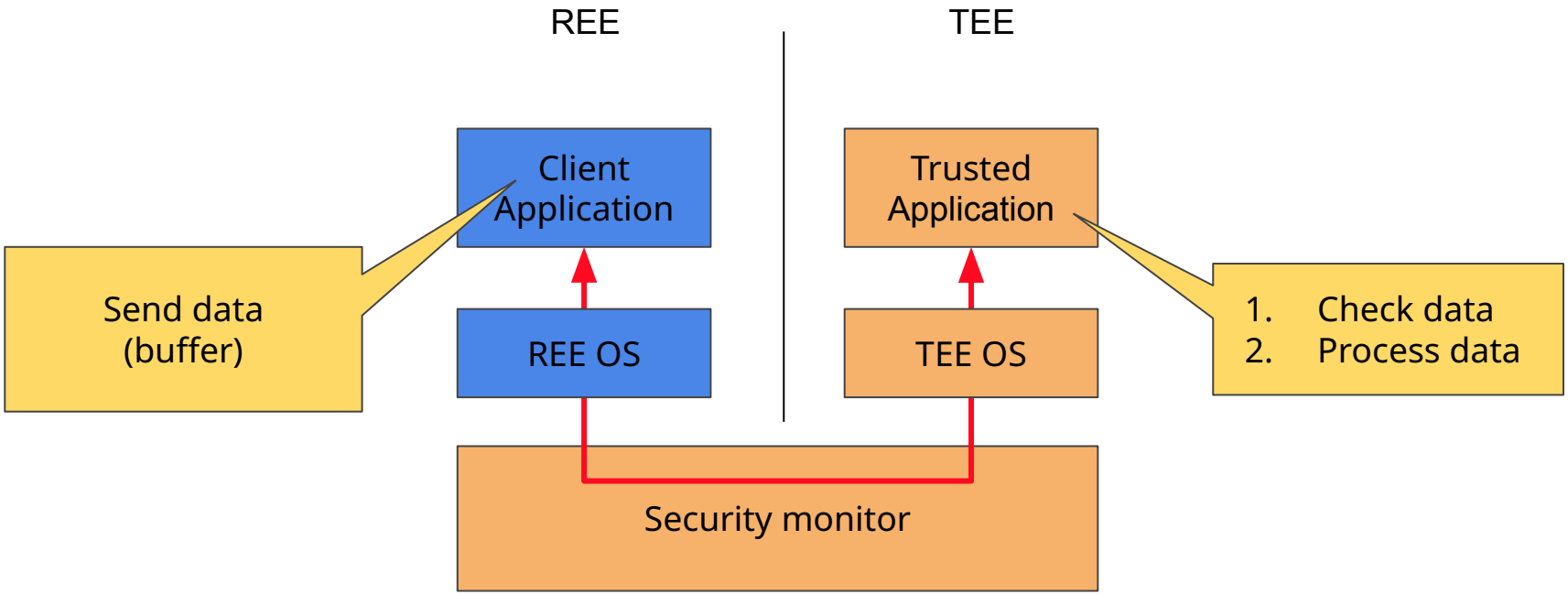
- `gpd.tee.rng.entropySource.protectionLevel`: describe the entropy source
- `gpd.tee.rng.nist`: compliance to NIST SP 800-90 series
- `gpd.tee.rng.bsi`: compliance to AIS 20 and AIS 31
- …

03-2

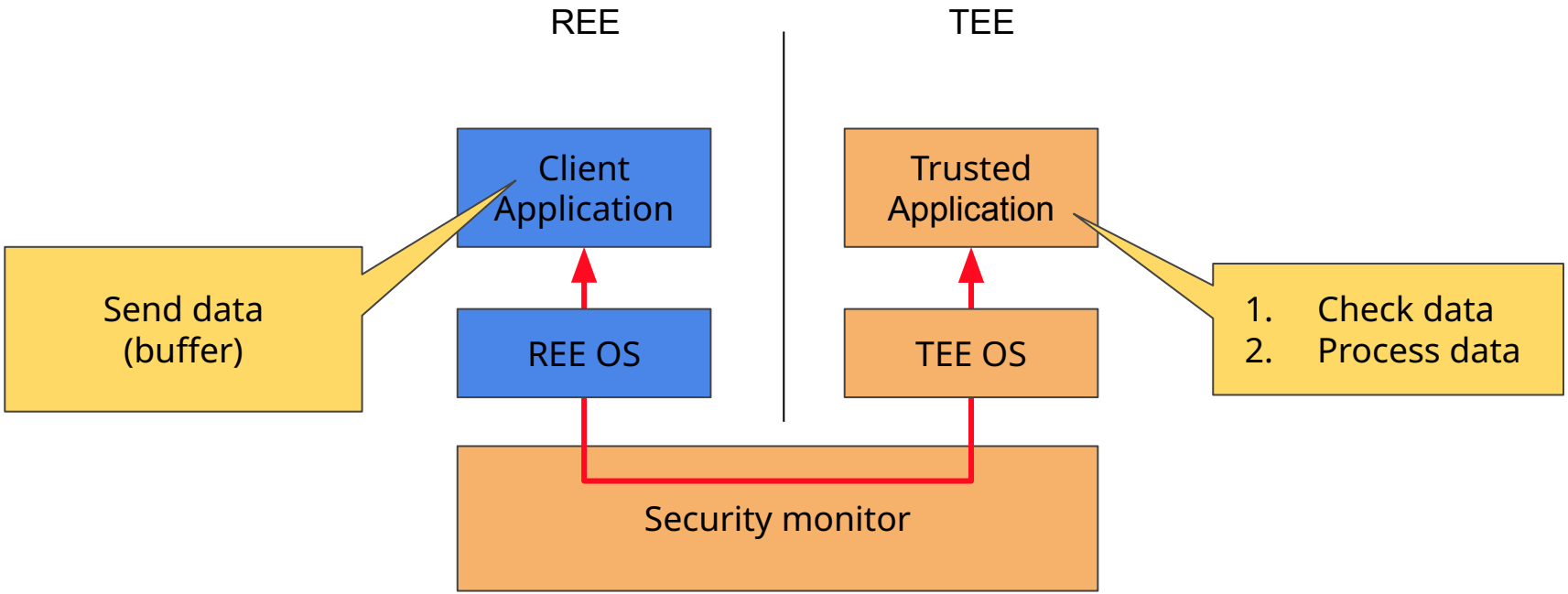
Security and performance

An example with REE ↔ TEE communication

Typical Data flow

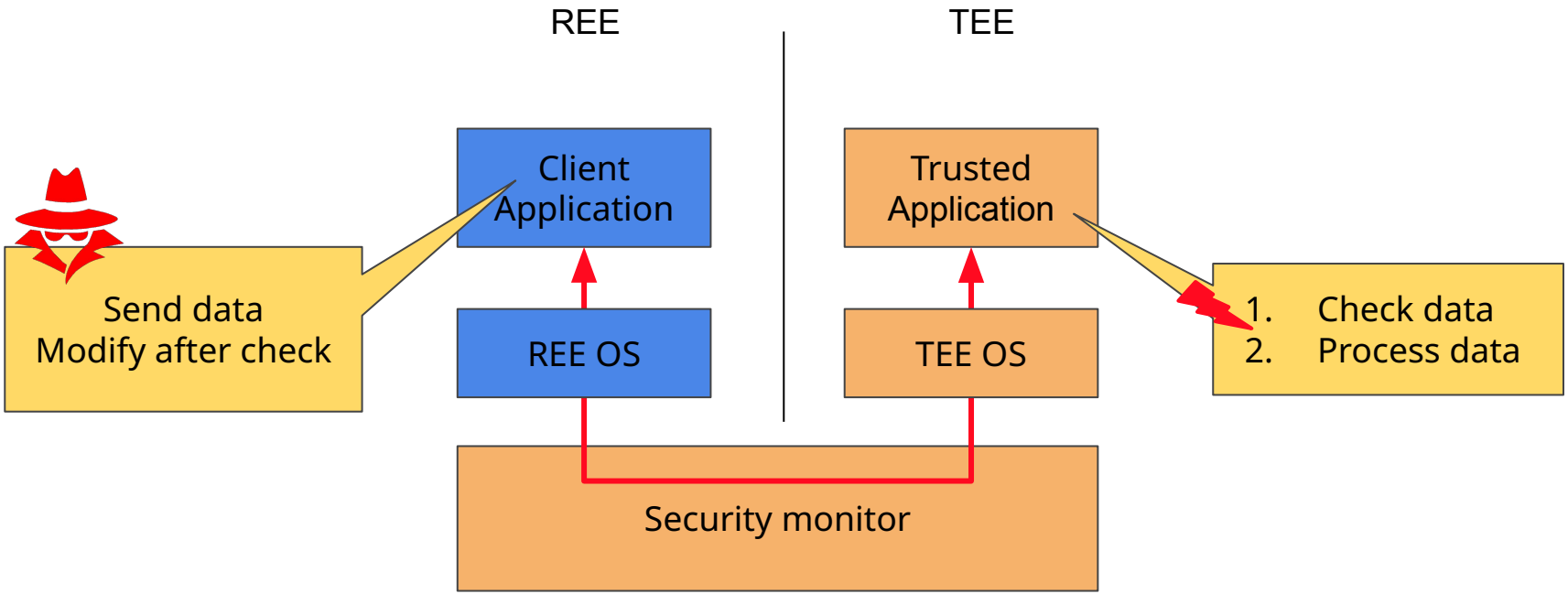


Typical Data flow



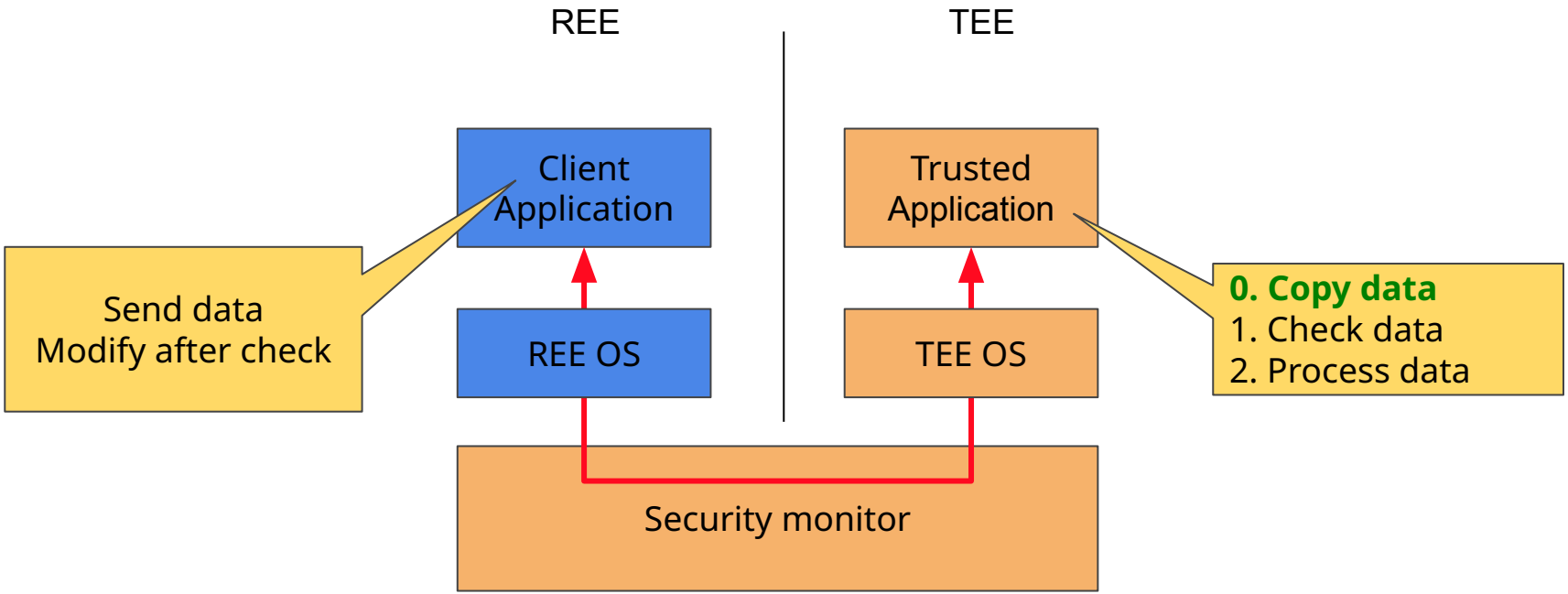
The REE still has access to the buffer

Typical Data flow



Time of Check/Time of Use (ToC/ToU) vulnerability

Typical Data flow



Typical mitigation: local copy of the data

A balance between **Security**, **Performance** and **Complexity**?

Problem: Copying the data reduces performance
Solution: Some hardware provide some memory firewall mechanisms

New Problem: how to balance priorities?

- Security? prevent ToC/ToU attacks
- Performance? zero copy
- Complexity? use of complex hardware mechanism + portability issue

GlobalPlatform TEE API Call Validation

```
typedef struct {
        uint32_t    type;
        bool        mayBeShared;
        size_t      minSize;
        size_t      maxSize; // 0=don't check
} TEE_ParameterPolicy;
```

Set one flag: the implementation does the rest for you

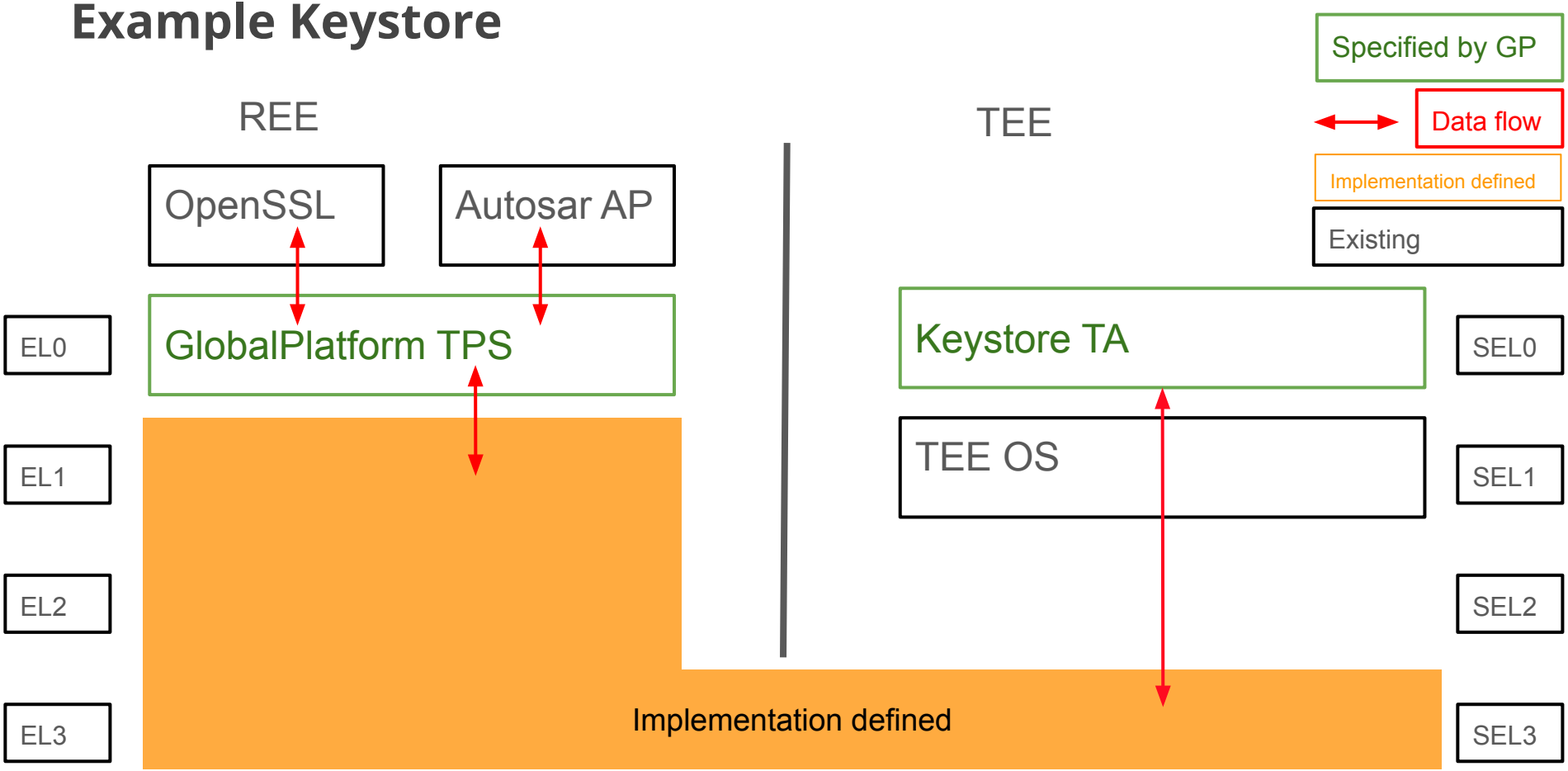
- Security: prevents ToC/ToU attacks
- Performance: Zero copy if your hardware supports it
- Complexity: set one flag

Source: TEE API Call validation §4.1.1 `TEE_ParameterPolicy`

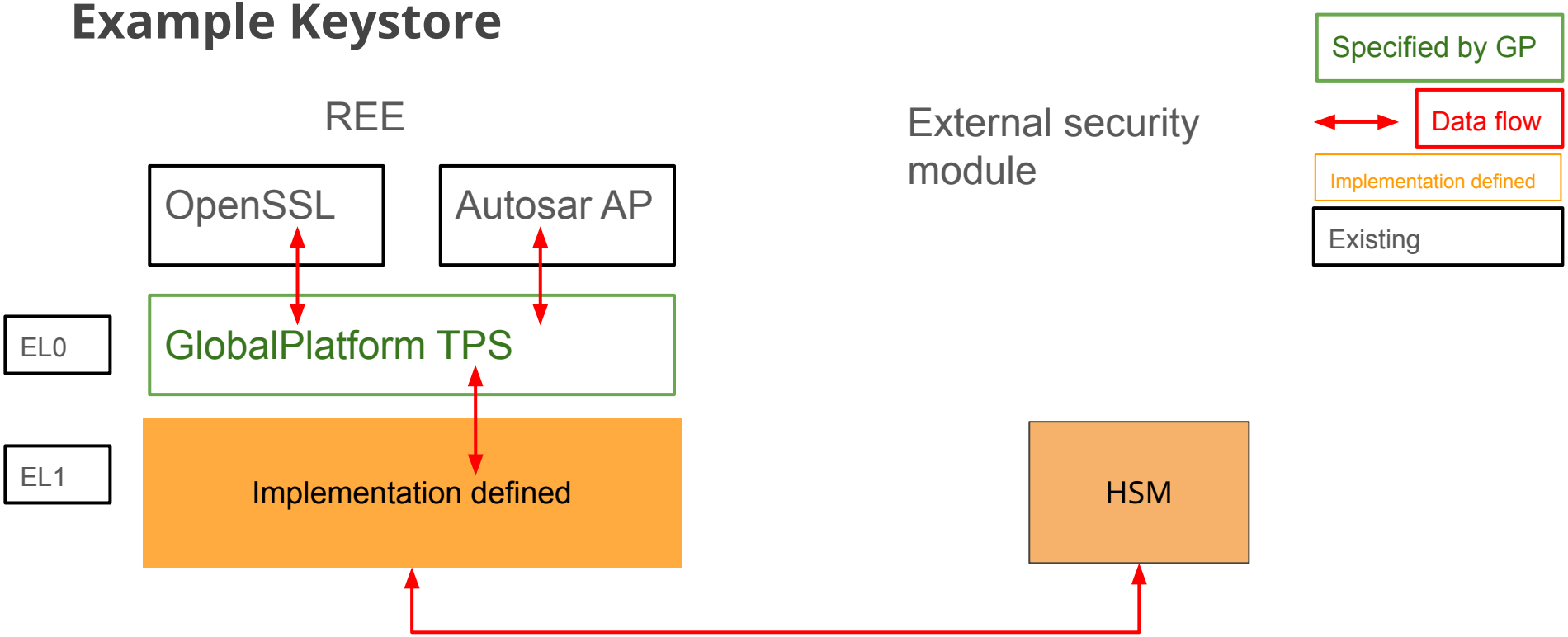
03-3

Trusted Platform Services (TPS)

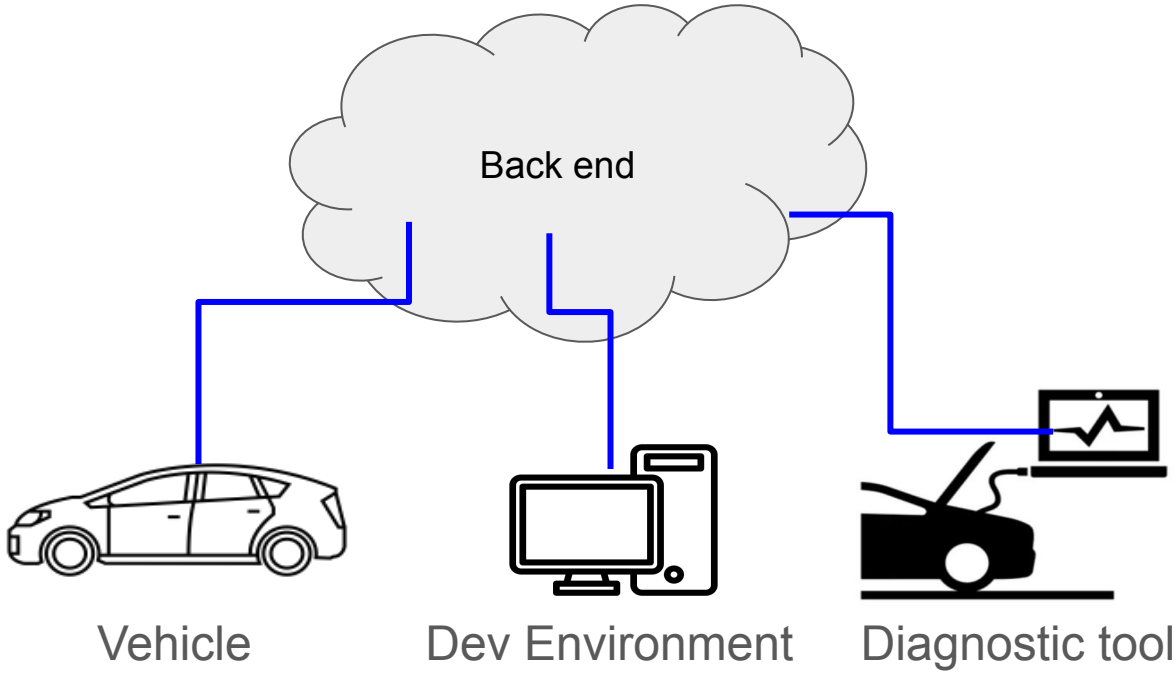
Example Keystore



Example Keystore



Example Keystore



Trusted Platform Service benefits

01
Standardised services

Open standard:
- developed and reviewed by experts
- less internal effort

Competition between vendor

02
Maximise portability

The same application could run regardless if the device has a TEE, a secure element or nothing (example during development).

03
Service discovery

Flexibility: can query which services are available.

Thank you