Implementation of GlobalPlatform TPS Keystore using OPTEE

Shahd Omer, Pekka Laitinen

What is GlobalPlatform and TPS Keystore?

Global Platform™ : is a technical standards organization that focuses on producing specifications and standards concerning secure component technologies and providing certifications for trusted digital services and devices. GlobalPlatform-certified SEs and TEEs are widely implemented in devices across multiple sectors. GlobalPlatform Standards are created in 3 committees: TES, SE and SESIP. The **Trusted Platform Service (TPS)** Working Group is under TES Committee.

TPS Goals

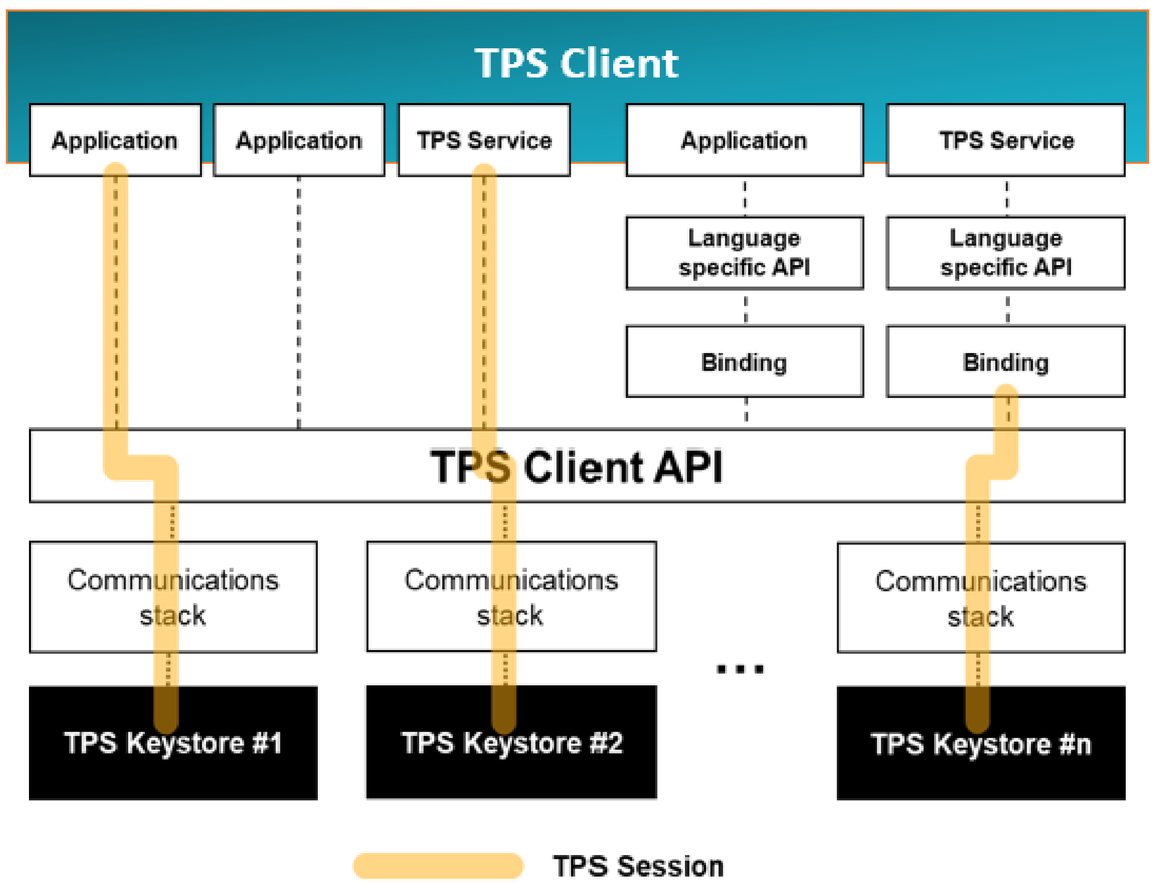
One of the main goals of **TPS** is to provide easy access from REE OS to the Secure Services implemented in Secure Components. It does so by creating an architecture that utilizes various hardware-assisted isolation implementations , abstracting away the details of the secure component and thus introducing ease of use for vendors and developers wishing to incorporate security services offered by Trusted Applications. As well as be Platform independent such that it supports various Operating system seamlessly.

- Secure hardware **architecture independence**
- Ease of integration
- Multiple **OS** support
- Compatible with **IoT** and **resource constrained** devices

The **TPS Keystore** is an example of a **TPS** accessible through the **TPS Client API**.

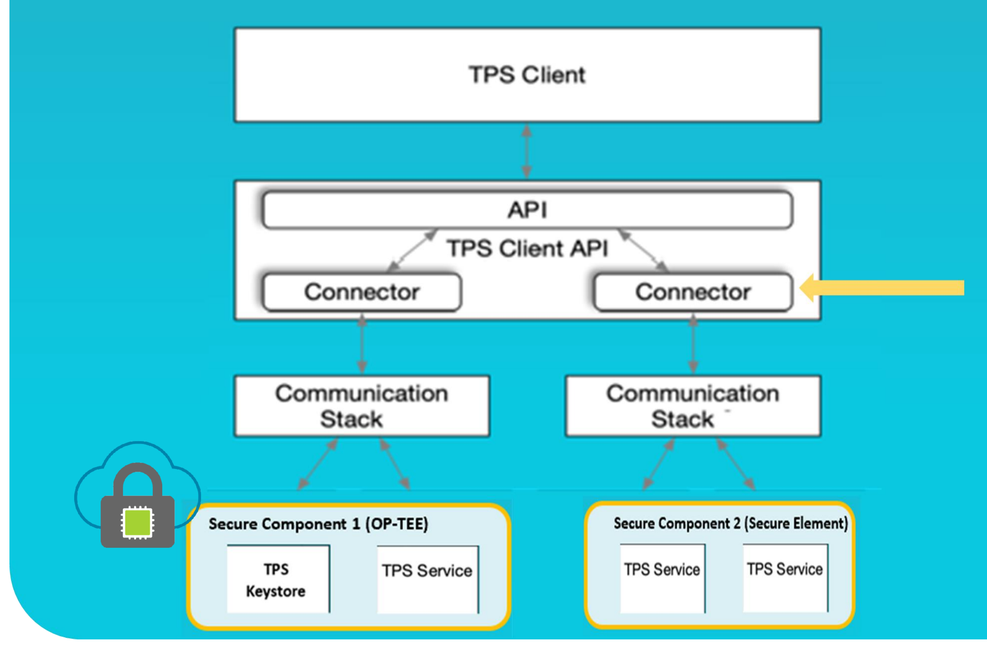
TPS Client APIs

TPS APIs define a universal language to access secure services provided ,in our case TPS Keystore, which could be implemented on different types of Secure Components for instance GlobalPlatform SEs and TEEs or TCG's TPM. These APIs are optimized for IoT and built with an attestation by design mindset.

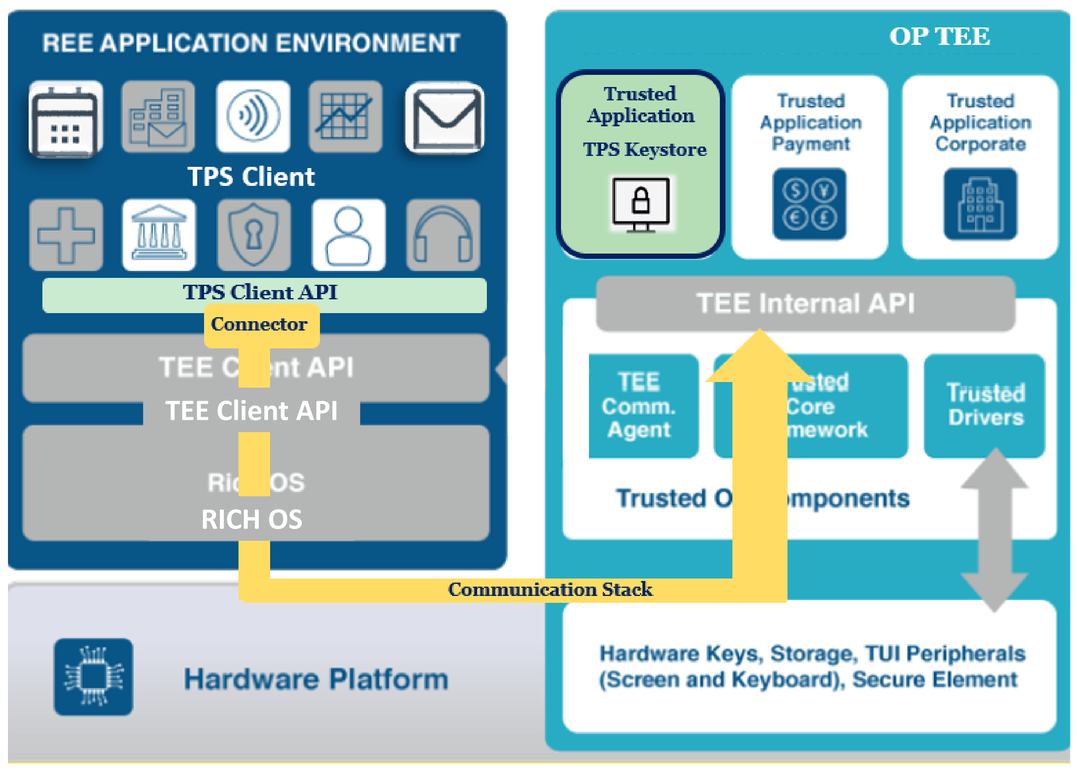


Connector

Since TPS Client API interacts with TPS Services that are implemented on varying Secure Components an abstraction for the communication between the Secure Component and TPS Client API is manifested in the form of a 'Connector' that simplifies the interaction with different backends.



OP-TEE is an open source implementation of TEE, based on ARM TrustZone. However OP-TEE is compatible with other isolations that are suitable with TEE concepts.



TPS Keystore Implementation: The TPS Client communicates via the TPS Client API that passes the request to the Connector. The connector is service oriented hence it handles interferences with the underlying architecture implementing the TPS Keystore. The TPS Keystore receives the request, decoding the CBOR message, matching it to the correct implementation that then utilizes the TEE Internal API to carry out cryptographic operations.

Helsinki System Security Lab (HSSL)

HSSL drives renewal and mastery in the field of platform and device related security technologies, especially for Huawei consumer devices such as mobile phones, laptops, televisions and automotive. We do research in topics such as hardware-assisted isolation and integrity, as well as in operating system protection (hypervisor, TEE, secure enclaves and kernel hardening). We also carry expertise in cryptography and systems security functionality such as device key management (PKI), device attestation and key-store solutions.

HUAWEI