

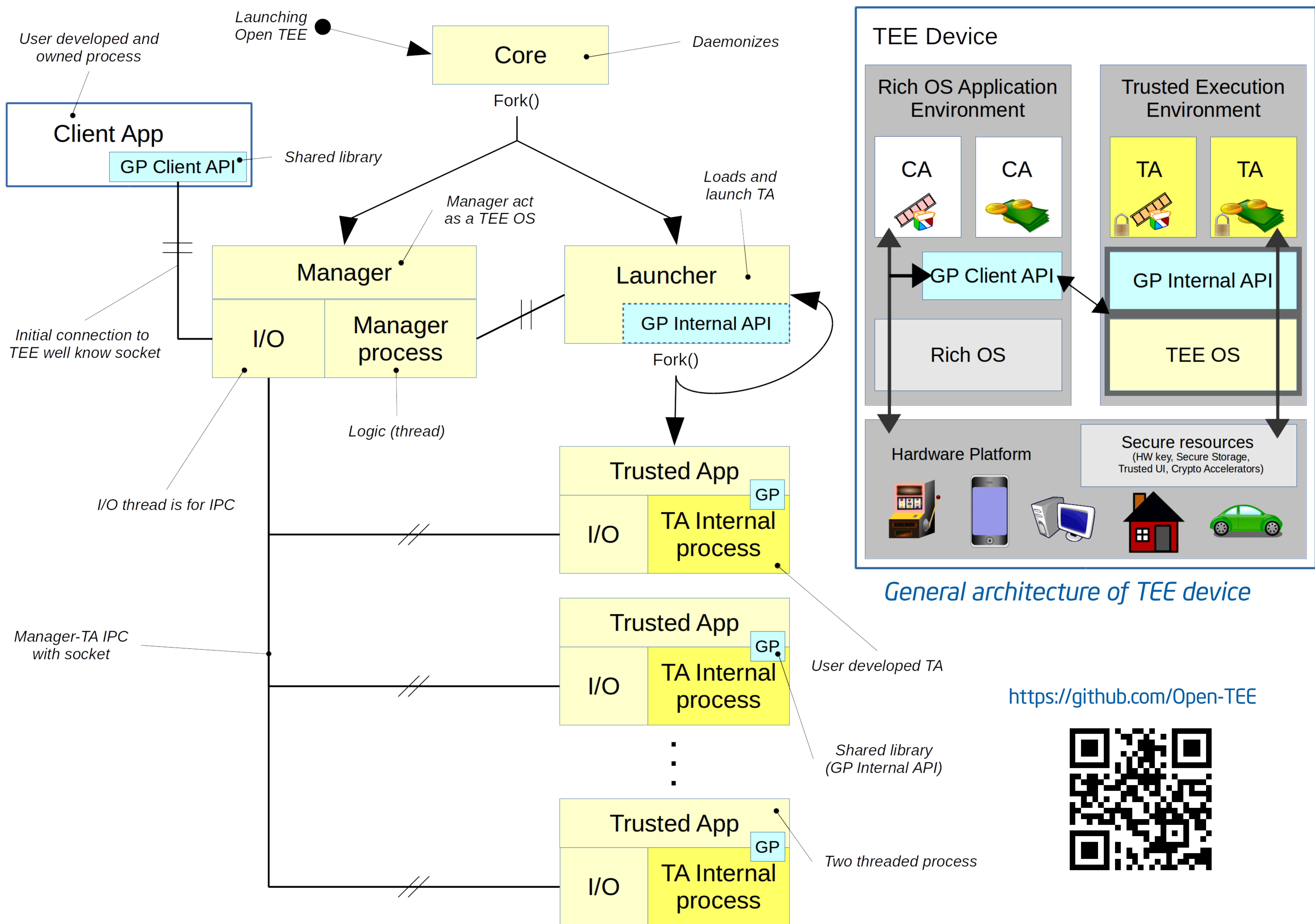
Open Virtual Trusted Execution Environment (TEE)



Tanel Dettenborn and Brian McGillion

- How to enable app developers to use trusted hardware?
- Open-source s/w implementation of the GP¹ TEE standard
- Benefits: (1) Tool for developers and researchers
(2) Fallback TEE on legacy devices

[1] Global Platform

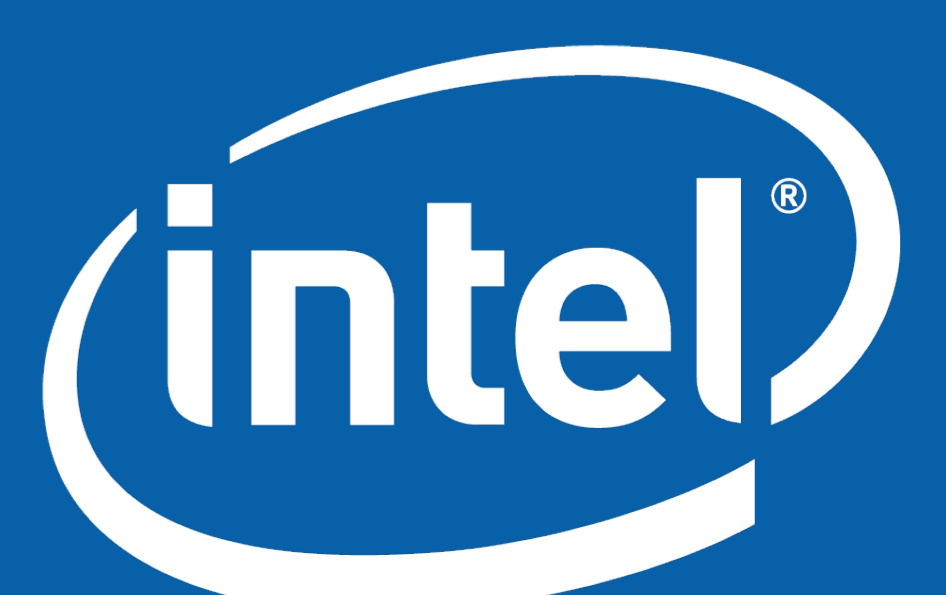


Implementation of open virtual TEE

<https://github.com/Open-TEE>



Intel CRI for Secure Computing



Intel and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
*Other names and brands may be claimed as the property of others.