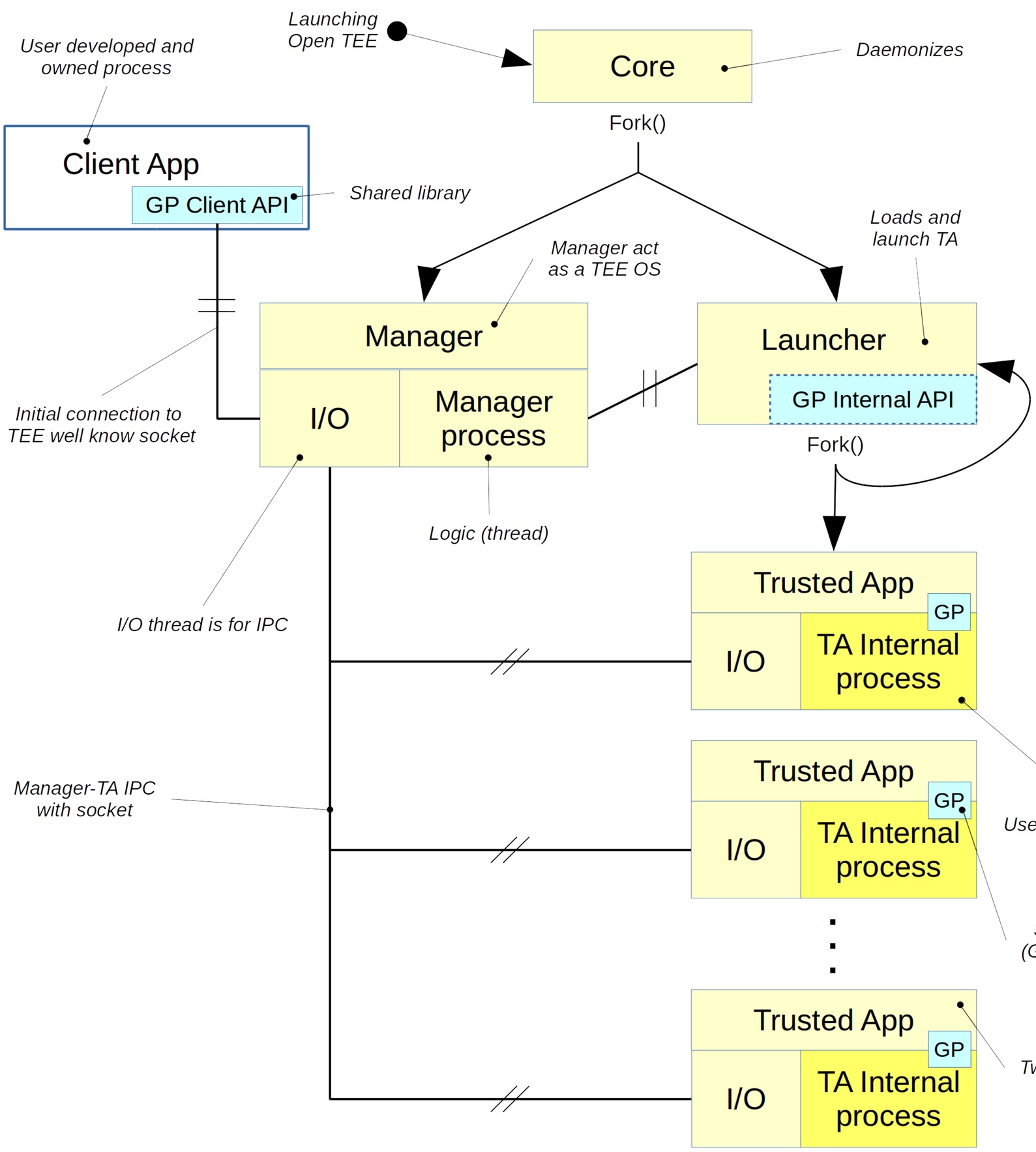
Open Virtual Trusted Execution Environment (TEE)

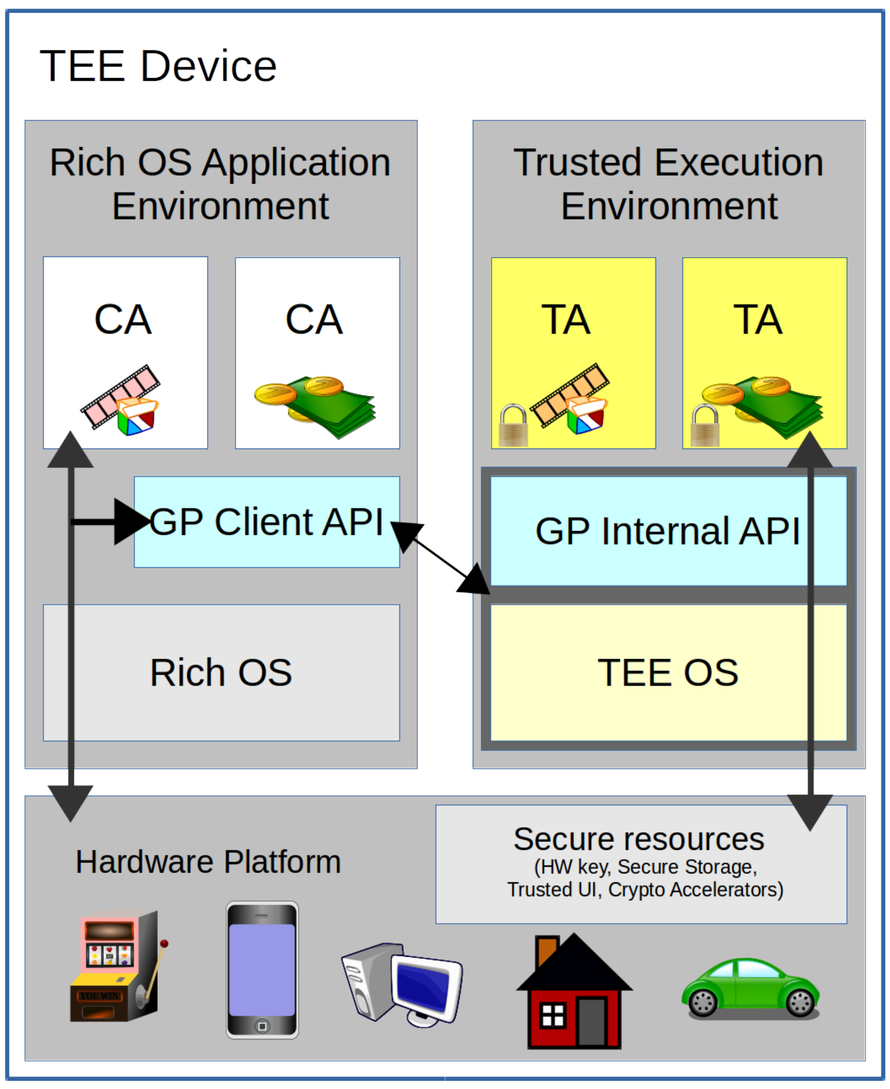
Tanel Dettenborn and Brian McGillion

UNIVERSITY OF HELSINKI

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

[1] Global Platform





General architecture of TEE device

https://github.com/Open-TEE

Implementation of open virtual TEE

Intel CRI for Secure Computing