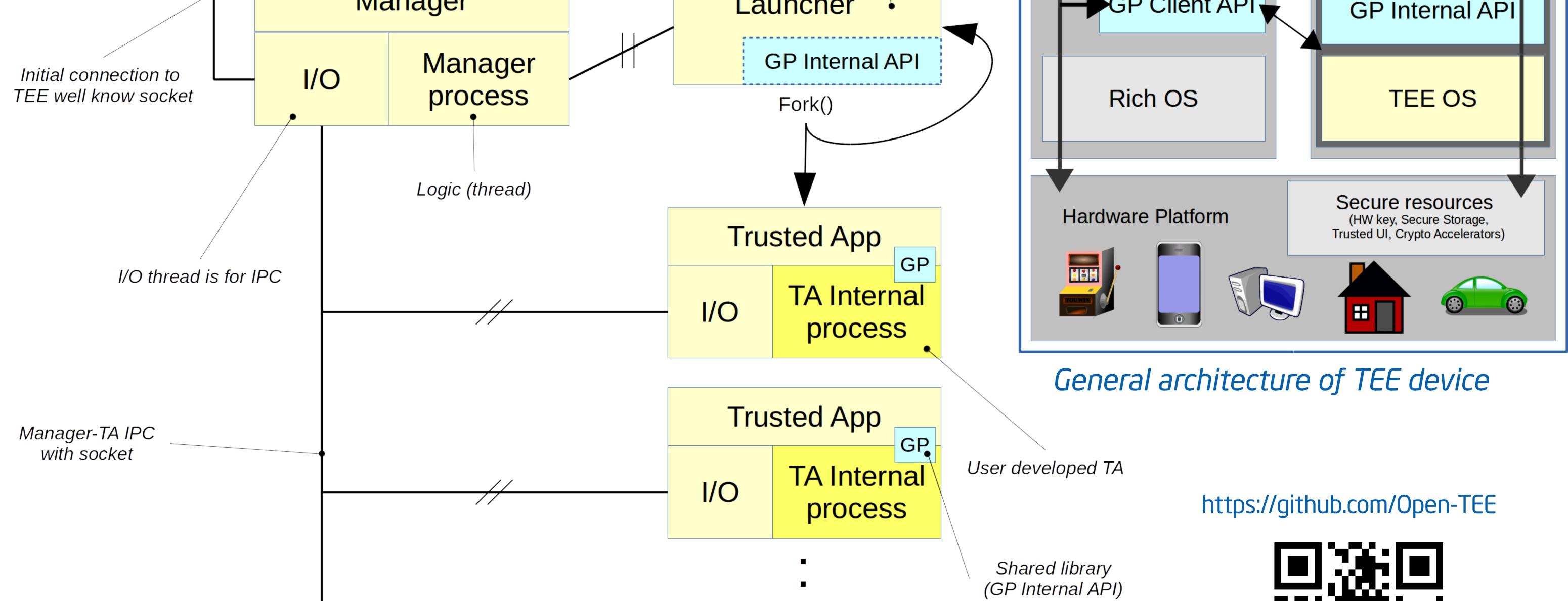
Open Virtual Trusted Execution Environment (TEE) Tanel Dettenborn and Brian McGillion

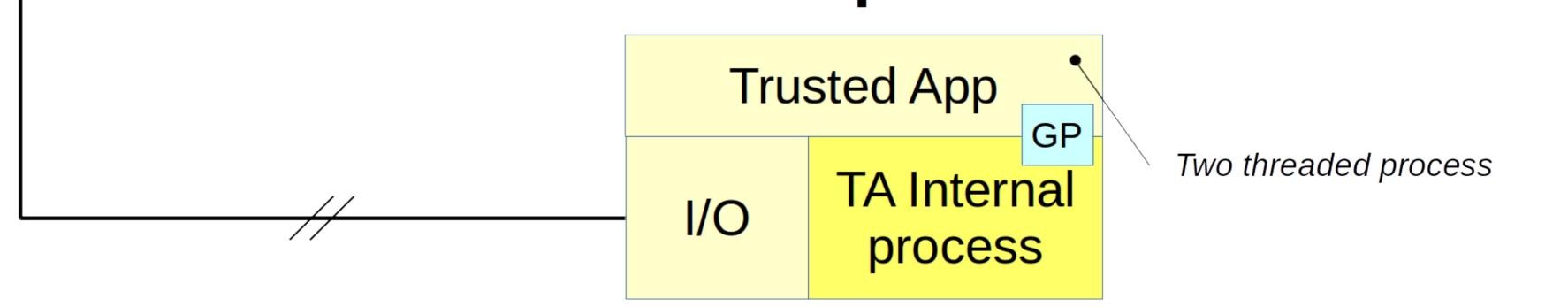
How to enable app developers to use trusted hardware?

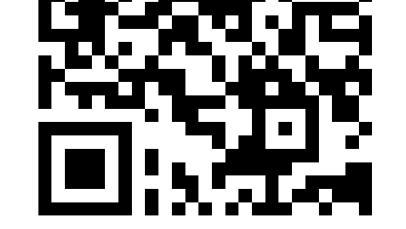
• Open-source s/w implementation of the GP¹ TEE standard

• Benefits: (1) Tool for developers and researchers (2) Fallback TEE on legacy devices

Launching **TEE** Device Open TEE User developed and Daemonizes Core owned process **Rich OS Application** Trusted Execution Fork() Environment Environment Client App Shared library GP Client API CA TA TA CA Loads and launch TA Manager act as a TEE OS Manager GP Client API Launcher







(intel[®])

[1] Global Platform

Implementation of open virtual 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.