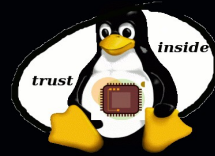


softtpm v1.0

TPM Emulator Module on Linux

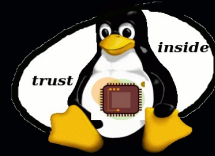
Arun Viswanathan (aviswana@usc.edu)
University of Southern California

High Level Objectives



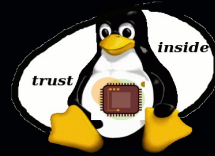
- ✓ Allow prototype applications for trusted computing to be coded on linux without requiring a hardware TPM.
- ✓ Allow standard TSS stacks like Trousers to be used to build real applications.
- ✓ Allow applications to be ported as is on real TPMs once they have been tested on the emulator.
- ✓ Allow fast and easy modifications to comply with latest TPM specs as stated by the TCG.

Low Level Requirements



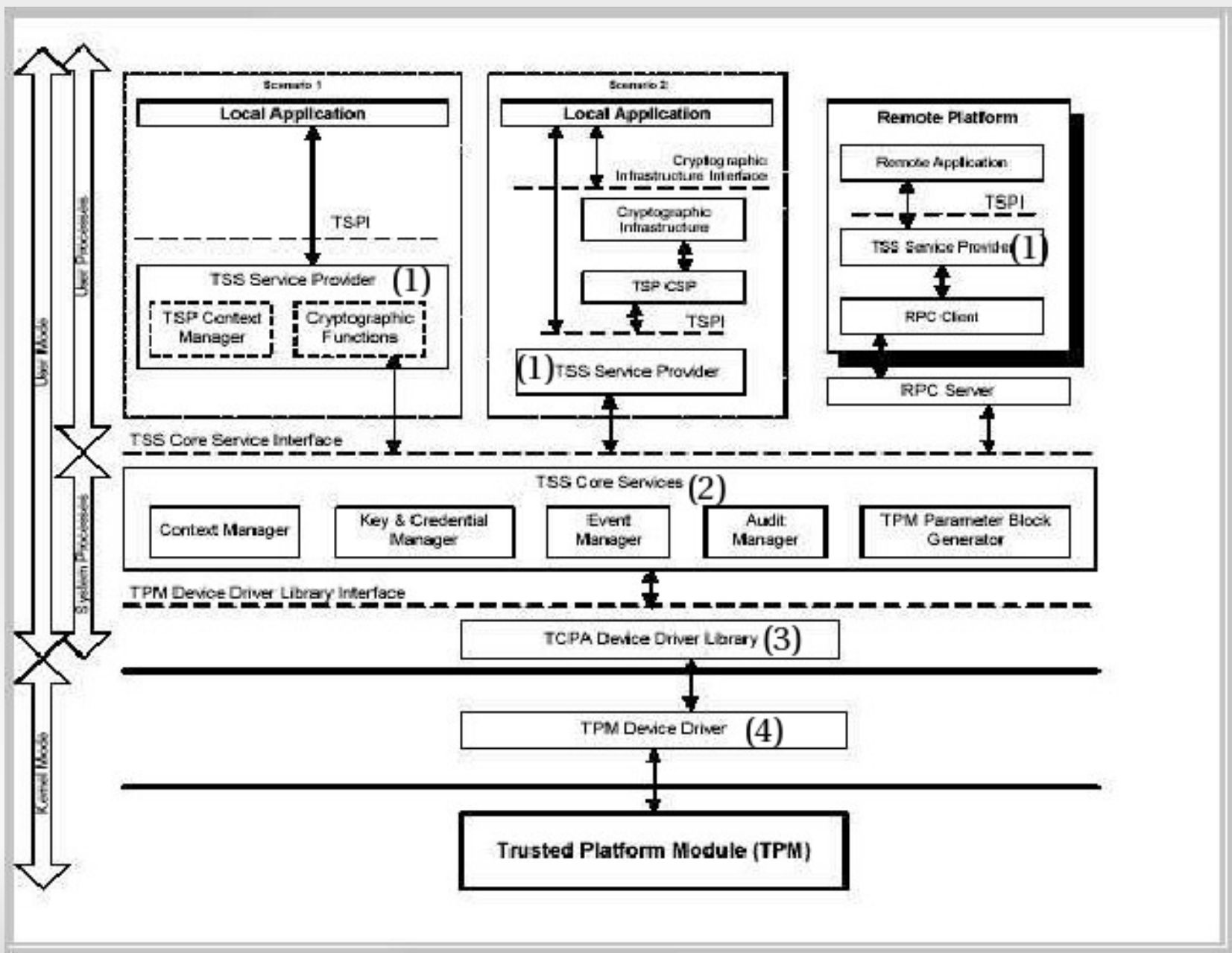
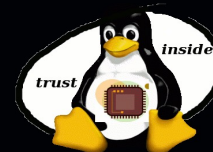
- ✓ Be fully spec compliant with the TPM v1.1 spec.
- ✓ Support the following categories of TPM commands.
 - a) Protected Storage commands
 - b) Key Management Commands
 - c) Migration Commands
 - d) Maintenance Commands
 - e) Measurement collection commands
 - f) Measurement reporting commands
 - g) TPM Endorsement Key commands
 - h) AIK Commands

Low level objectives (cont..)

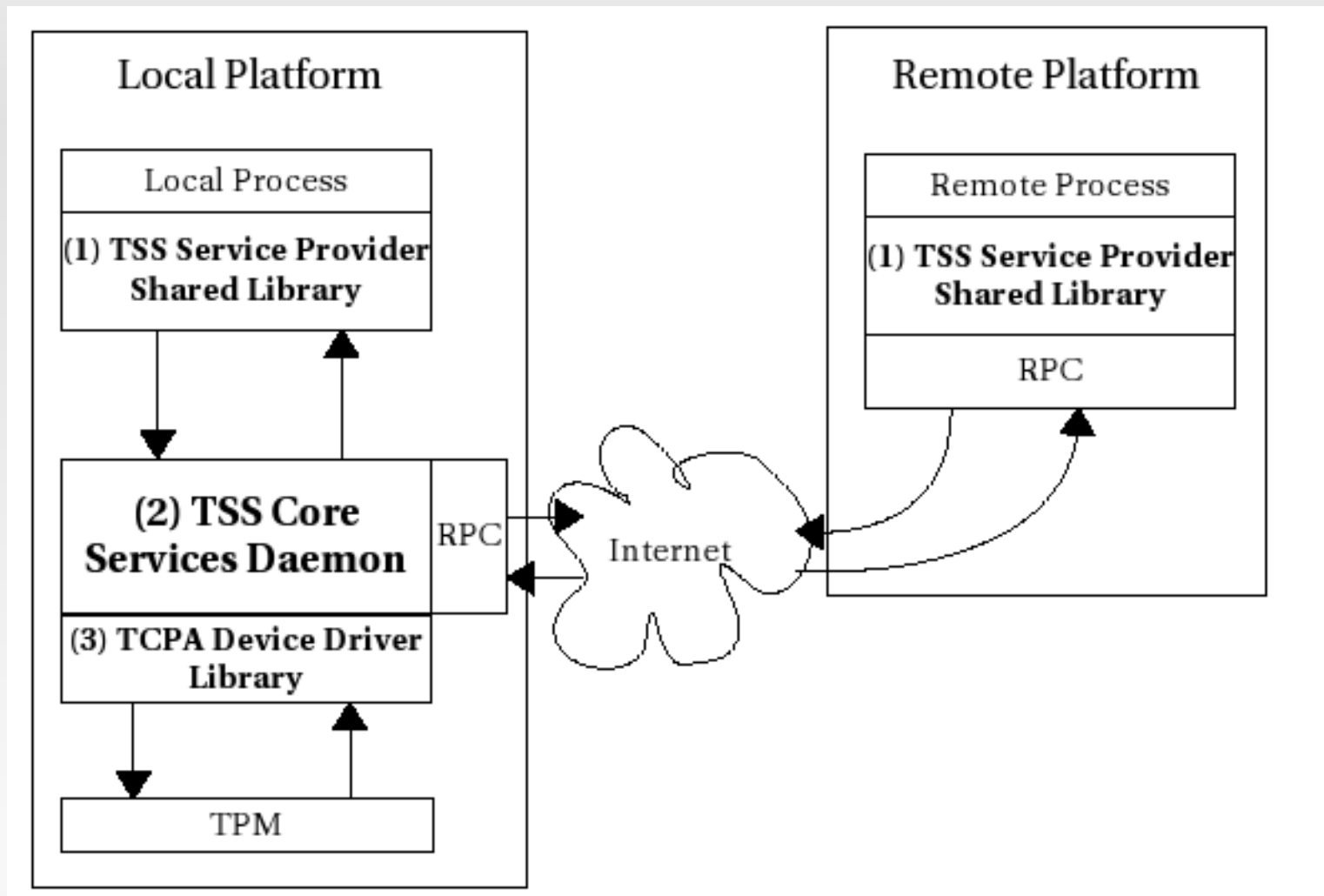
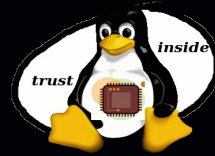


- i) Authentication Protocols and Authorization commands
 - j) Cryptographic Commands
 - k) Auditing commands
 - l) Capability reporting commands
 - m) TPM Ownership commands
 - n) Operational Flags commands
 - o) Self Test commands
 - p) Startup commands
- ✓ Integrate seamlessly with the Trousers Open Source TSS stack the emulated TPM.
 - ✓ Be accessible using the generic TPM driver interface TPMDD on linux.

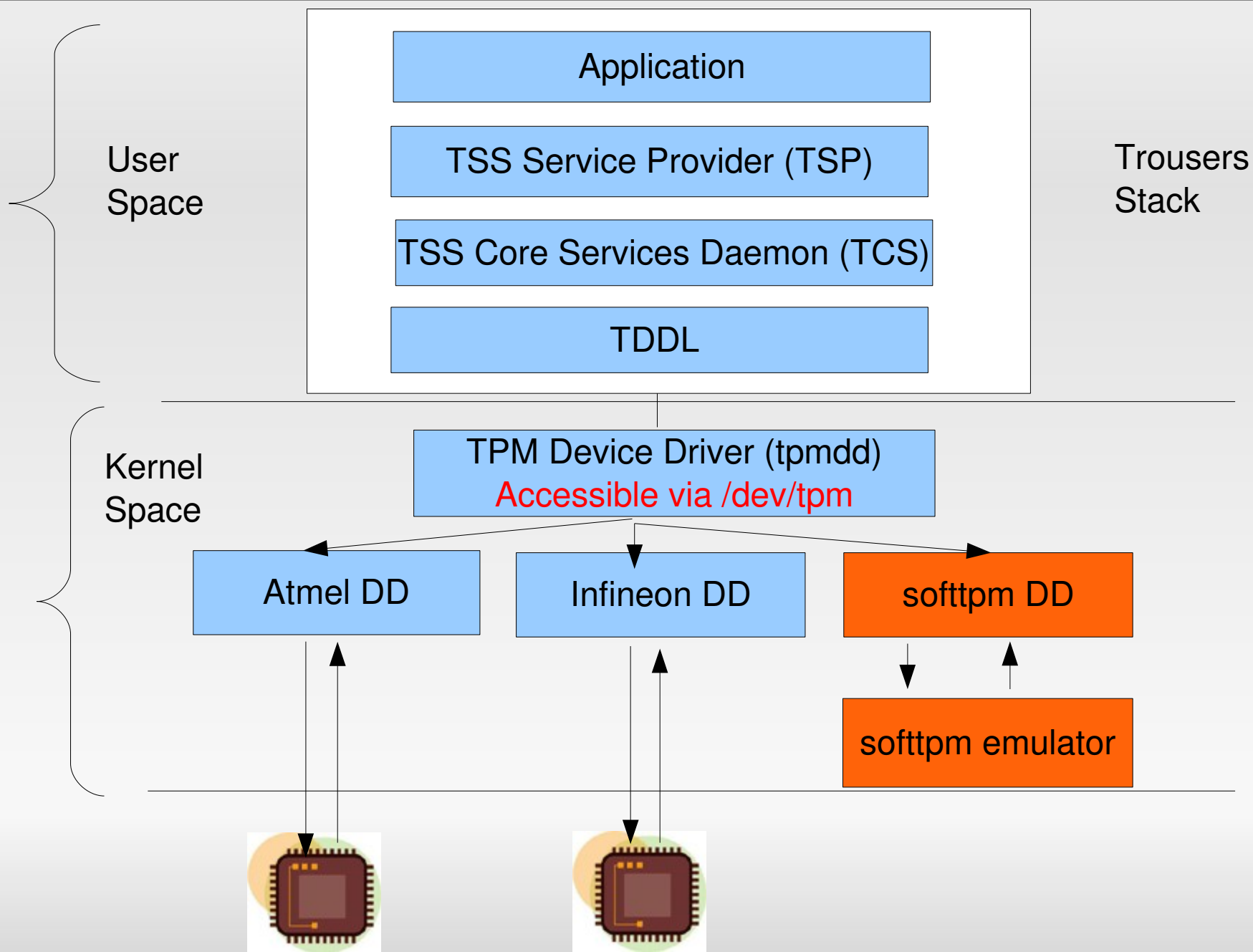
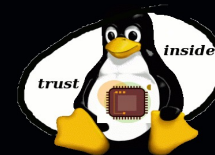
Trusted Software Stack Specification



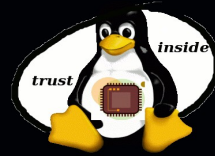
TrouSerS TSS Stack (IBM)



softtpm architecture (Big Picture)



Lower Level Design



TPM Device Driver

Supports generic commands like open, read, write etc to /dev/tpm

Softtpm Driver

Reissues the commands in a device dependent manner. In this case this would involve making calls to the softtpm s/w module

softtpm

TPM Command Interpreter and dispatcher

Crypto APIs

Storage Manager

Key Manager

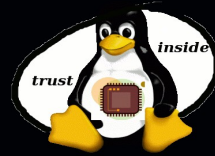
PCR Storage

Hash APIs

Auth Manager

Auth Manager

Caveats



- Performance will not be considered in v1.0
- It will be difficult to provide security that matches the hardware TPM.
- softtpm v1.0 will only focus on functionality.