Firmware tpm

Intel and AMD each offers a tpm integrated into some of their CPUs, called "firmware TPM" or "fTPM". Rather than a separate tpm device, which requires installation on the board and may be expensive, fTPM is implemented directly in the CPU and is exposed via the firmware.

- Intel offers the fTPM as Platform Trust Technology (PTT), generally available on 8th-generation or newer Core CPUs. It is compliant with TPM 2.0 specifications.
- AMD offers fTPM on most of the Ryzen, Athlon and EPYC CPUs

From the user's perspective, an fTPM, once enabled in BIOS, looks exactly like a tpm 2.0, presenting the usual devices of `/dev/tpmrm0` and `/dev/tpm0`.