Inhaltsverzeichnis

Trusted Platform Module

Der TPM Chip ist praktisch eine erweiterte SmartCard. Warum also nicht den TPM benutzen zum speichern der privaten Keys für z.B. SSH oder TLS Zertifikate oder für die HDD Verschlüsselung mit LUKS?

Andreas Fuchs erklärt das am 36c3 in einem halbstündigen Vortrag.

"Don't ask what you can do for TPMs, Ask what TPMs can do for you" Hacking (with) a TPM

TPM2 Software Community Homepage: tpm2-software.github.io