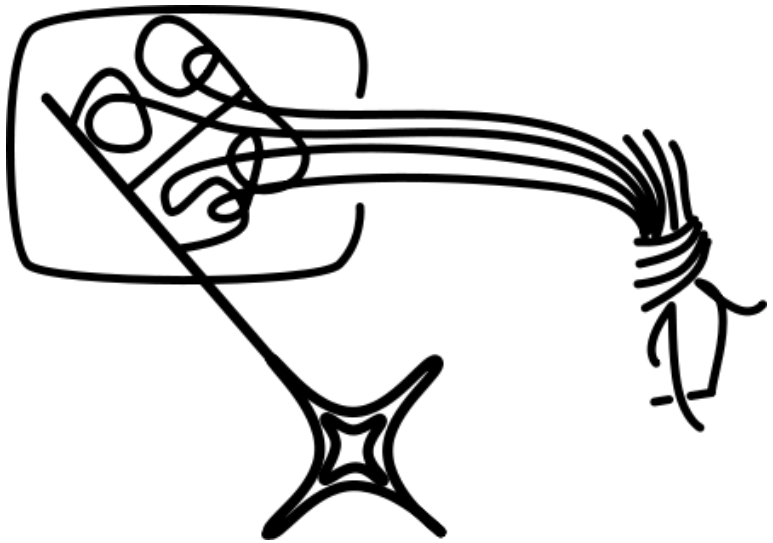


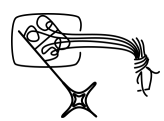
Trusted Platform Module (TPM) und Remote Attestation

Von Measured Boot bis Trusted Monitoring

genofire
geno@fireorbit.de
27. April 2020

Inhaltsverzeichnis

1. Trusted Platform Modul (TPM)
   - Idee vom TPM
   - Verbreitung des TPMs
   - Aufbau des TPMs
     - Kryptoprozessor
     - Speicher
   - Einsatzmöglichkeiten
     - Measured Boot
2. Trusted Software Stack (TSS)
3. Trusted Attestation Protokoll (TAP)
4. Monitoring



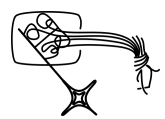
Idee vom TPM

Hardware Security Modul (HSM):

- 3rd Party Crypto Bibliotheken
- Leaks von Schlüsseln verhindern
  z.B. Dateisystem, Memory-Dump

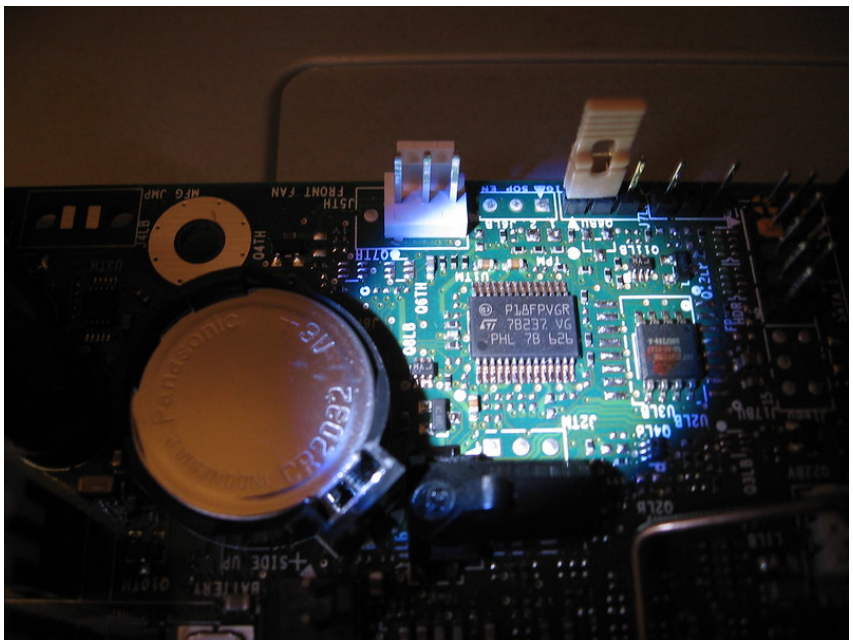
Besonderheit für TPM

- Smartcard dauerhaft im PC
- Security per Computer
  vs. per Person

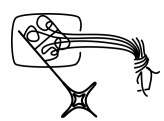


Verbreitung des TPMs

Auf einem Motherboard

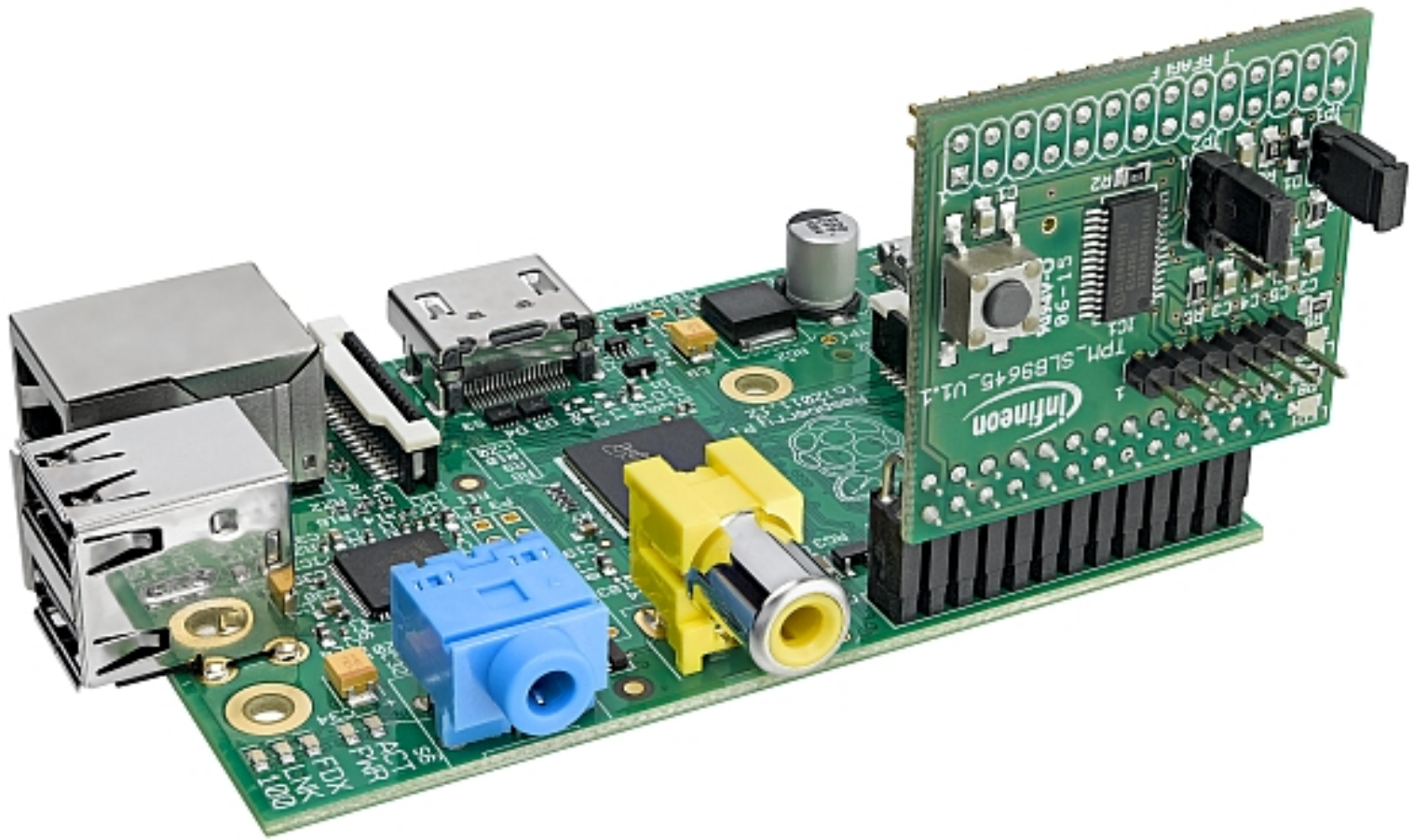


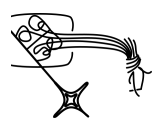
- Dank Microsoft und UEFI nun in fast allen Computern
- Ebenfalls in Chromebooks



Verbreitung des TPMs

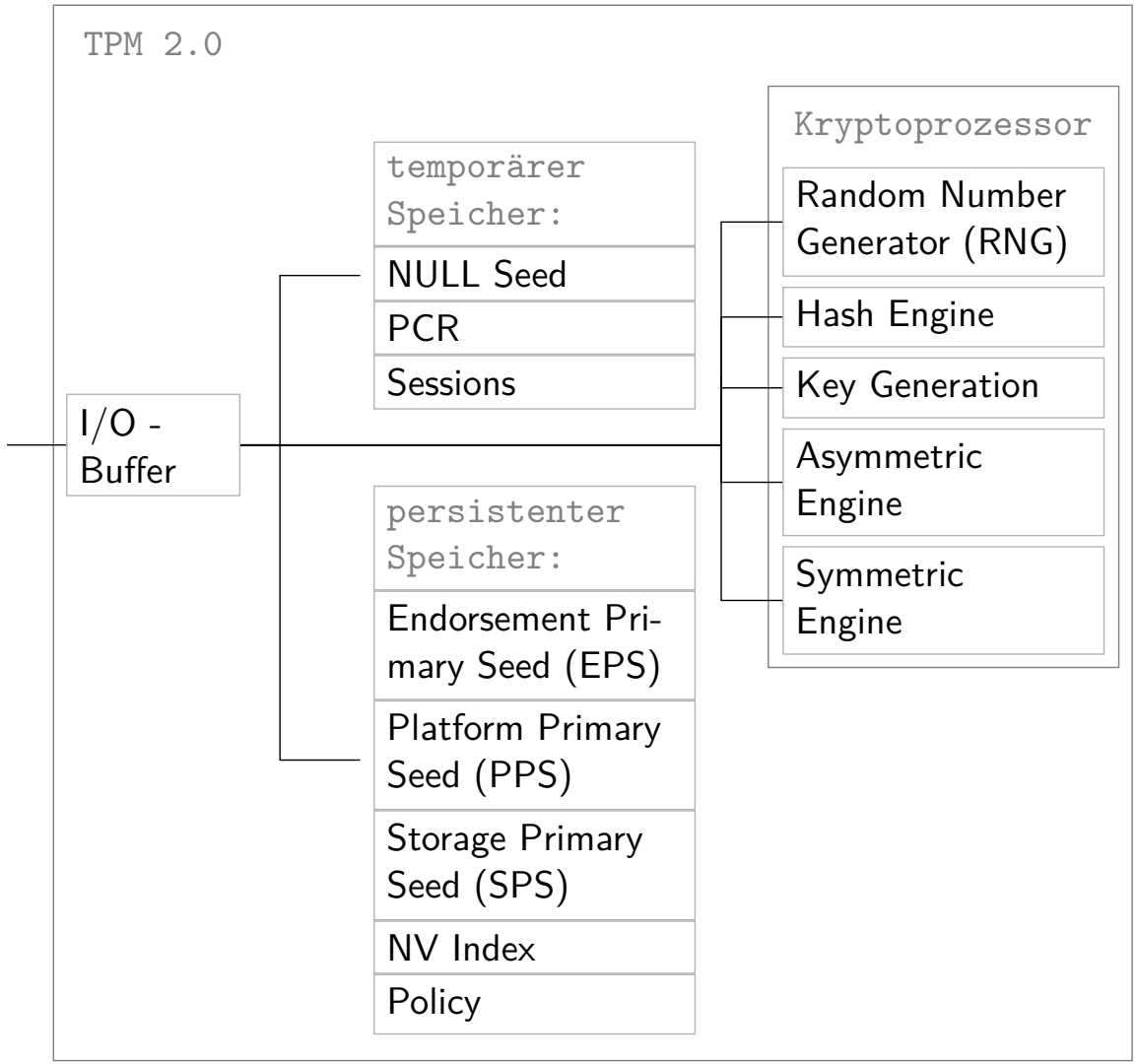
Für den Raspberry Pi

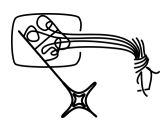




Trusted Platform Modul (TPM)

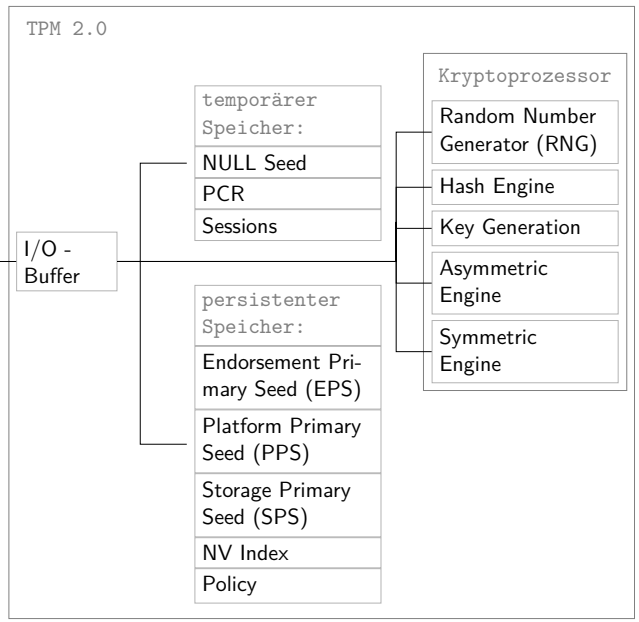
Aufbau des TPMs





Aufbau des TPMs

Kryptoprozessor



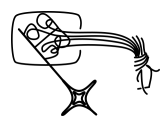
RNG max 32 Byte

Hash SHA, HMAC

Key Gen KDF

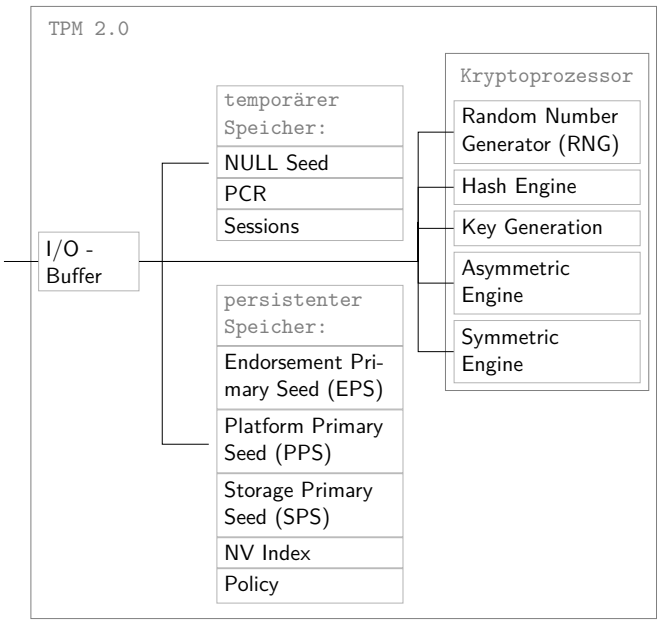
Asym RSA, ECC

Sym AES, SM4, Camellia, Triple DES



Aufbau des TPMs

Persistenter Speicher

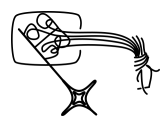


Seeds Zufallszahl, per KDF für alles nutzbar

NV Index "Freier Speicher"

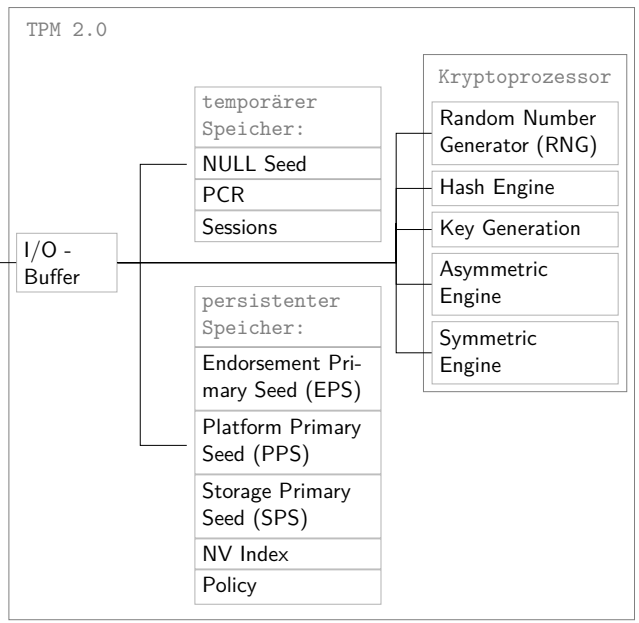
Policy PIN bis Enhanced Authorization

- Dictionary Attack Protection



Aufbau des TPMs

Seeds

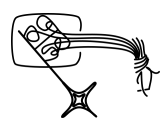


Endorsement vom Hersteller:
für Zertifikat-Kette
echtes TPM

Platform für Firmware z.B. UEFI

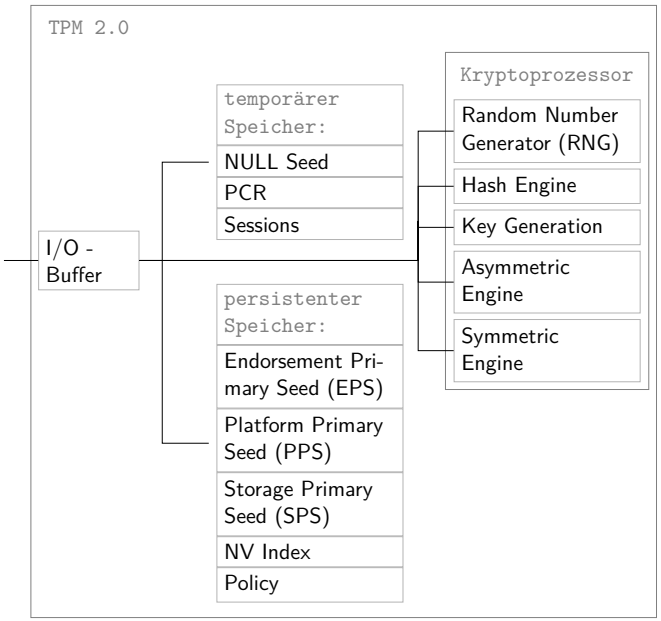
Storage für eigene Zwecke
zum reseten gedacht

NULL bei jeden Hochfahren
reseted



Aufbau des TPMs

Temporärer Speicher

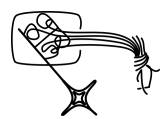


PCR-Bänke nur Extends oder Clean:

$$PCR_{new\_value} = Digest(PCR_{old\_value}||data)$$

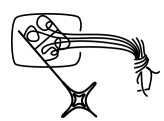
Quote PCR-Values + Nonce signiert

Session mit Context für Policies



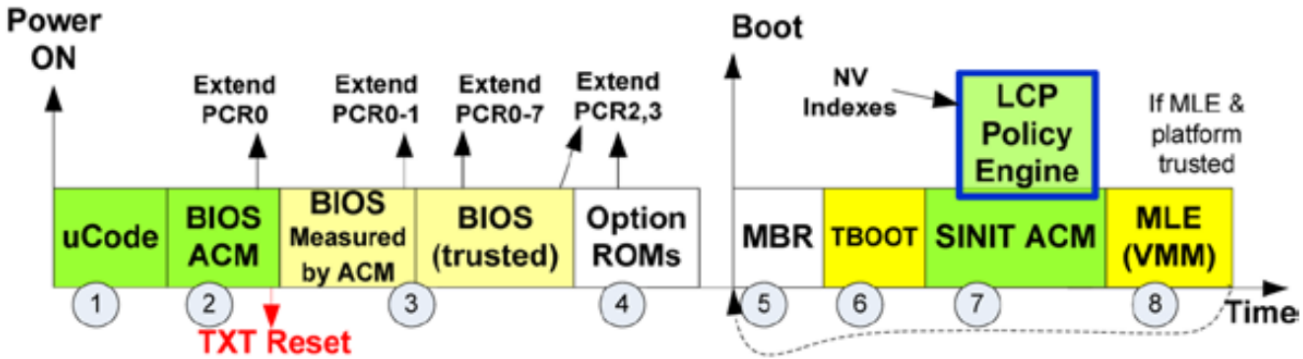
Einsatzmöglichkeiten

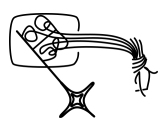
- TLS Zertifikat (z.B. für Web- oder Mailserver)
- VPN-Server
- “Hacking (with) a TPM” von Andreas Fuchs:
  `https://media.ccc.de/v/36c3-10564-hacking_with_a_tpm`
- Vieles Mehr ;)
  z.B. Measured Boot



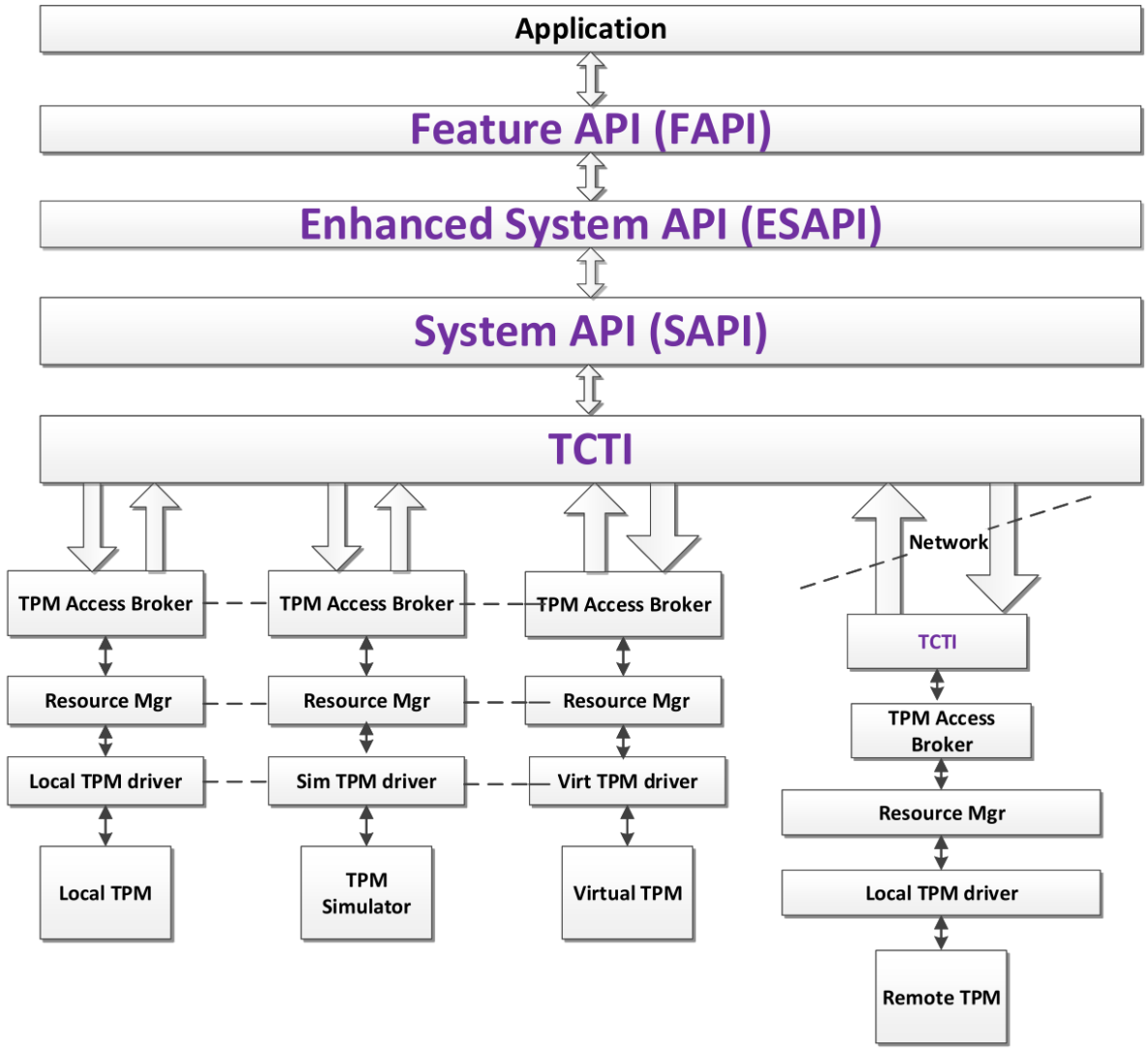
Einsatzmöglichkeiten

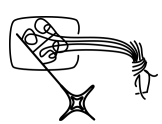
Measured Boot





Trusted Software Stack (TSS)

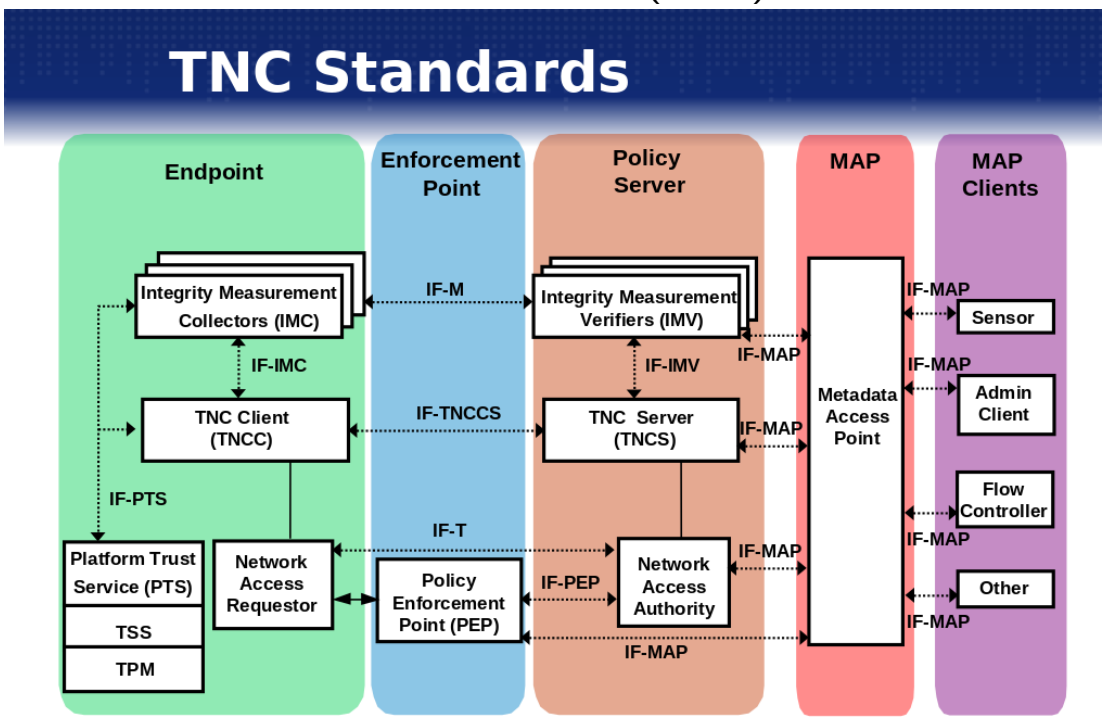




Trusted Attestation Protokoll (TAP)

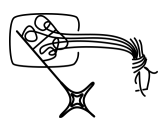
Funktionsweise

Trusted Attestation Protokoll (TAP) wurde im Herbst 2019 veröffentlicht



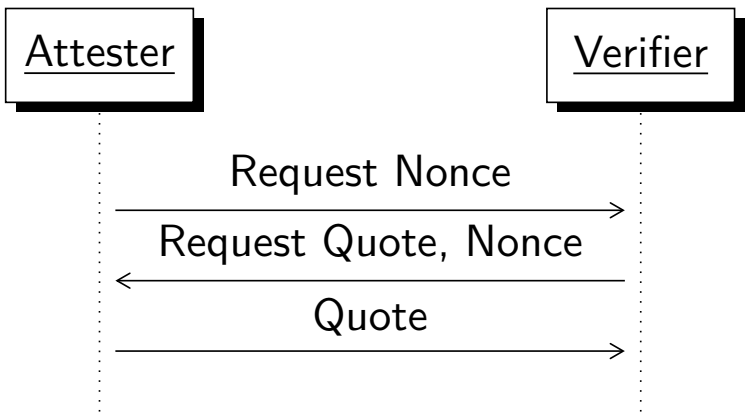
http://www.trustedcomputinggroup.org/developers/trusted_network_connect/specifications

- TNC für TPM 1.2
- TAP für TPM 2.0

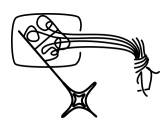


Trusted Attestation Protokoll (TAP)

Einsatzmöglichkeiten

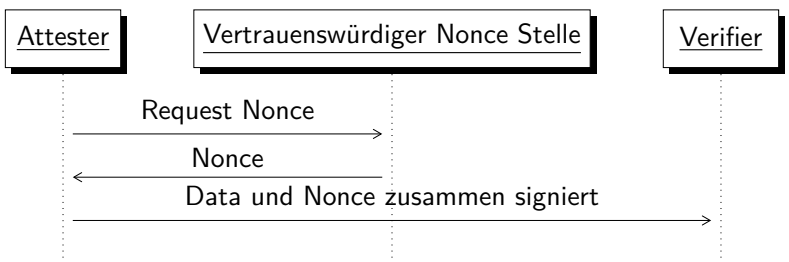


- Zugang zum Netzwerk
- Remeasurement



Trusted Attestation Protokoll (TAP)

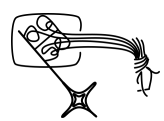
Einsatzmöglichkeiten



- Zugang zum Netzwerk
- Remeasurement
- Unidirektion

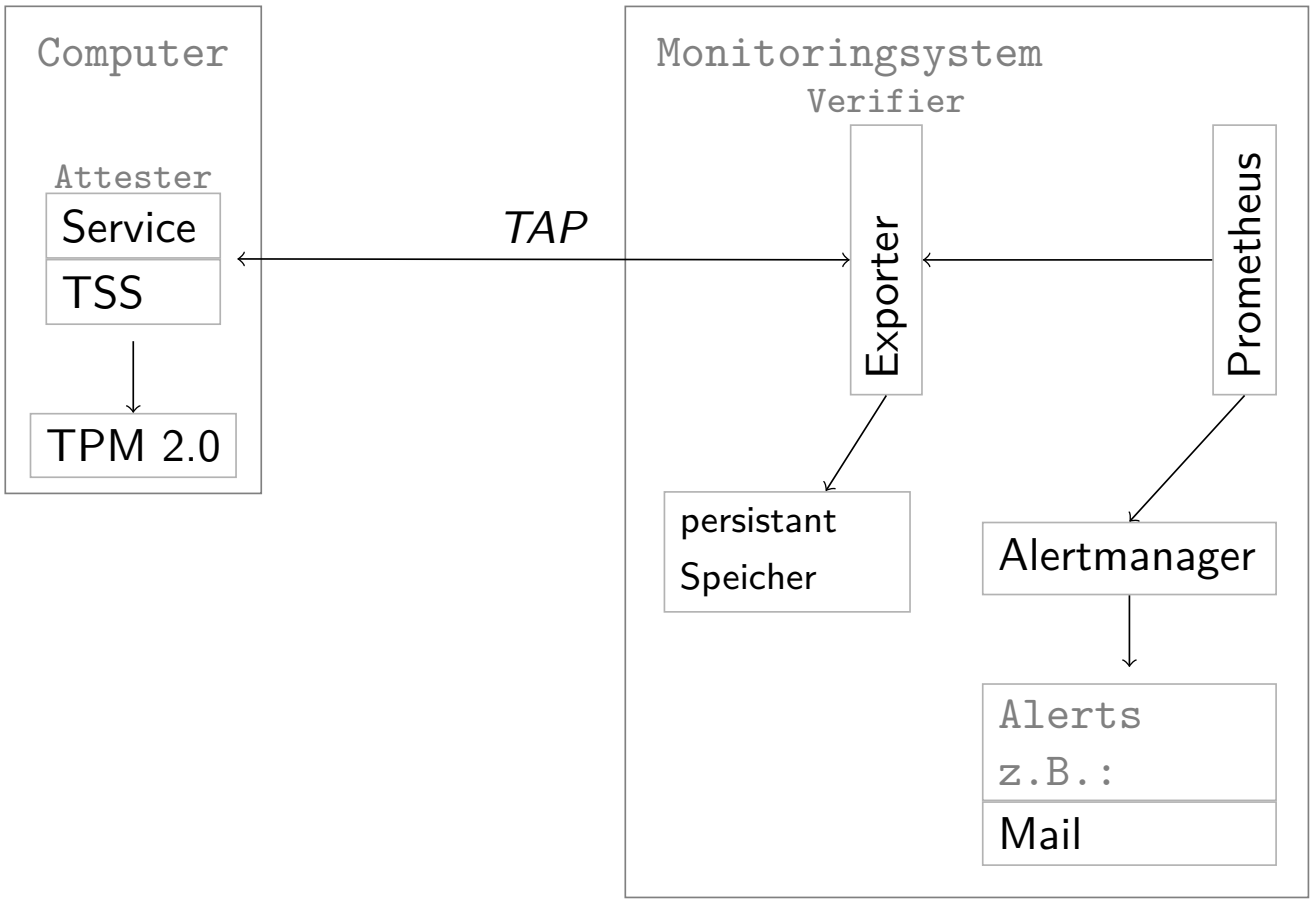
  UDP
- Sitzungloses

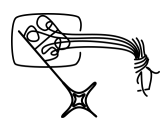
  UDP / Nonce per 3rd-Party



Monitoring

Idee meiner Thesis





Trusted Platform Module (TPM)
und Remote Attestation

Vielen Dank für Ihre Aufmerksamkeit

Im Browser zum Experimentieren:
`https://google.github.io/tpm-js/`