TPM

Inhaltsverzeichnis

Ein TPM (Trusted Platform Module) ist ein Hardwaresicherheitschip für Keys, Messung des Bootzustands und geschützte kryptografische Operationen. Private Schlüssel verlassen den Chip typischerweise nicht.

1 Funktionsweise

Das TPM speichert Schlüsselmaterial und kann Plattformmessungen (PCR) für Attestation oder Disk-Encryption nutzen. Operationen erfolgen im Chip.

- **Key Storage:** nicht exportierbare Keys
- **Measured Boot:** Integrität der Startkette
- **Sealing:** Daten nur in bekanntem Zustand freigeben

2 Typische Einsatzbereiche

- BitLocker/LUKS mit Hardware-Bindung
- Device Trust und Attestation
- Sichere Geräteidentitäten

3 Wichtige Hinweise

- Firmware- und Ownership-Setup beachten.
- Hardwaretausch kann versiegelte Daten unbrauchbar machen.
- TPM ersetzt keine vollständige Endpoint-Strategie.

4 Fazit

TPMs verankern Vertrauen in Hardware – stark für Key-Schutz und Boot-Integrität in modernen Geräten und Servern.