HAW HAMBURG

Bachelor-Thesis zur Erlangung des akademischen Grades B. Sc.

# Trusted Platform Module (TPM) 2.0 in Cyber-Sicherheit, Anwendung und Kritik

vorgelegt 30. März 2026

Mensur Muratovic
[redacted]

| | |
|---|---|
| Studienrichtung: | Media Systems |
| Erstprüfer: | Prof. Dr. Nils Martini |
| Zweitprüfer: | Thorsten Wagener |

**HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG**
Fakultät Informatik und Digitale Gesellschaft
Finkenau 35
22081 Hamburg

# Zusammenfassung

Diese Arbeit befasst sich mit dem Trusted Plattform Module der Spezifikation 2.0 und seiner Rolle in der Cyber-Sicherheit, das derzeit durch das verpflichtende Upgrade auf Windows 11 an Relevanz gewinnt, sowie mit der Frage, ob dieser gerechtfertigt ist. Es werden seine Anfänge, Entstehung und Entwicklung erfasst und dargestellt, die mit der Trusted Computing Group zusammenhängt. Es wird zudem das Konzept des Trusted Computings zusammengefasst und in Verbindung mit den grundlegenden Funktionen des Moduls in der Cyber-Sicherheit gebracht. Es werden einige Beispielfunktionen präsentiert, die auf der Technik und Stärken des Trusted Platform Module basieren. Im Anschluss werden seine Schwächen und Sicherheitsrisiken aufgelistet, sowie potenzielle einhergehende Probleme zum Schutz von IT-Systemen und Personenrecht. Diskussionen und Kritiken bezüglich der Trusted Computing Group und deren Absichten mit dem Trusted Platform Module werden aufgeführt. Zudem werden Folgen und Handeln durch Microsofts Zwangsupgrade im Konsumentenbereich dargestellt.



# Abstract

This thesis examines the Trusted Platform Module in its 2.0 specification and its role in cybersecurity, whose relevance has increased with Microsoft's mandatory upgrade to Windows 11. It explores whether this growing importance is justified by reviewing the origins, creation and development of the Trusted Platform Module in connection with the Trusted Computing Group. The concept of Trusted Computing is summarized and linked to the core security functions provided by said module. Several example applications are presented to illustrate the Trusted Platform Modules technical capabilities and strengths. The thesis then outlines its weaknesses and security risks, as well as potential challenges concerning IT system protection and individual rights. Finally, it discusses criticisms of the Trusted Computing Group's objectives and examines the implications of Microsoft's enforced adoption of TPM technology in the consumer market.

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# Abkürzungen und Begriffe

| Abk. | Bedeutung |
|---|---|
| AIK | Attestation Identity Keys |
| BIOS | Basic Input Output System |
| CC | Common Criteria for Information Technology Security Evaluation, international anerkannter Standard für Zertifizierung von Computersystemen (ISO/IEC 15408) |
| CRTM | Core Root of Trust for Measurement |
| dTPM | diskretes Trusted Platform Module |
| ECC | Elliptic Curve Cryptography |
| EK | Endorsement Key |
| fTPM | Firmware Trusted Platform Module |
| MOK | Machine Owner Key |
| NIST | National Institute of Standards and Technology |
| PSP | Platform Security Processor (AMD fTPM) |
| PCR | Platform Configuration Register |
| PTT | Platform Trust Technology (Intel fTPM) |
| RNG | Random Number Generator |
| RTM | Root of Trust for Measurement |
| RTS | Root of Trust for Storage |
| SoC | System on a Chip, Ein-Chip-System |
| SRK | Storage Root Key |
| TCPA | Trusted Computing Platform Alliance |
| TCB | Trusted Computing Base |
| TCG | Trusted Computing Group |
| TCM | Trusted Cryptography Module |
| TCP | Trusted Computing Platform |
| TC | Trusted Computing |
| TPM | Trusted Platform Module |
| UEFI | Unified Extensible Firmware Interface |
| VBS | Virtualization-Based Security |

# 1 Einleitung

## 1.1 Problemstellung

Trusted Platform Module (TPM), Trusted Computing (TC), Trusted Computing Group (TCG) enthalten jeweils das Wort „Trust“, was auf Englisch „Vertrauen“ bedeutet. Vertrauen ist jedoch ein emotional aufgeladener Begriff – insbesondere, wenn es sich um ein alltäglich genutztes Produkt handelt. Einer der größten Softwarehersteller, Microsoft, hat den Support für das Betriebssystem Windows 10 nach zehn Jahren am 14. Oktober 2025 eingestellt. Diese Ankündigung hat deutlich größere Auswirkungen als frühere Betriebssystemwechsel. Laut Microsoft (Mehdi, 2025) existieren weltweit etwa 1,4 Milliarden aktive Endgeräte mit Windows.
Das Nachfolgeprodukt Windows 11 erfordert strikte Hardwarevoraussetzungen, im Besonderen das TPM der aktuellen Spezifikation 2.0. Abgesehen von geschlossenen Systemen wie Produkten von Apple, bei denen regelmäßig funktionstüchtige Hardware als veraltet gilt und von Updates ausgeschlossen wird, ist dieser Schritt von Microsoft ungewöhnlich; laut Statcounter sind 66,6 % der weltweit vertriebenen Computer Windowssysteme (Statcounter, 2026a).
Hardware-Sicherheit stellt ein komplexes Themenfeld dar. Die von der TCG entwickelten Spezifikationen sind dabei nicht auf Benutzerfreundlichkeit ausgelegt. Mit der stetig zunehmenden Integration von Computern und Smartphones im Alltag wächst zugleich die Relevanz der Cybersicherheit. Wie selbstverständlich Module und Systeme miteinander interagieren, wie sie funktionieren und wie angreifbar sie sind, bleibt für viele Endnutzer undurchsichtig – sei es aufgrund mangelnder Transparenz, Aufklärung oder technischer Kenntnisse. Das TPM wurde von der TCG, einem Konsortium führender Technologieunternehmen, entwickelt und soll neue Sicherheitsstandards in Computern integrieren. Gleichzeitig steht es regelmäßig in der Kritik. So wurde es in Deutschland als ISO-Standard abgelehnt, insbesondere wegen der potenziellen Gefahr von Hintertüren, die sich nicht vollständig ausschließen lassen (Biselli, 2015).
Da sich Bedrohungsszenarien im Bereich der Cybersicherheit fortlaufend weiterentwickeln, müssen Sicherheitskonzepte kontinuierlich überprüft und verbessert werden. Vor diesem Hintergrund stellt sich die Frage, ob das TPM 2.0 tatsächlich einen Sicherheitsgewinn bietet

oder ob hier ein schleichender Kontrollverlust in den Markt integriert wird, ohne einen messbaren Mehrwert für die Cybersicherheit zu schaffen.

## 1.2 Ziele

Ziel dieser Arbeit soll sein, die Definition von Trusted Computing und die Technik und Funktionalität des Trusted Platform Module zu beleuchten, um die Auswirkung auf die Cyber-Sicherheit systematisch darzustellen. Hierbei wird die Entstehung, Entwicklung und Standardisierung des TPM sowie die Rolle der TCG historisch und fachlich analysiert. Dazu wird das Konzept vom Trusted Computing aufbereitet, und wie Vertrauen die Integrität von IT-Systemen gewähren soll. Darauf aufbauend wird untersucht, wie das TPM als solcher Vertrauensanker die Systemintegrität verifiziert und sicherheitsrelevante Information schützt. Zudem folgt eine Bewertung, ob das TPM für Unternehmensumgebung als auch in privatem Nutzen einen praktischen Sicherheitswert bietet. Daraufhin folgt eine systematische Darstellung der zentralen Funktionen, Einsatzbereiche, technische Schwächen sowie gesellschaftliche und politische Kritikpunkte. Dies bildet die Grundlage um abschließend den Stellenwert des TPM zu beurteilen, und ob die Anforderung von Windows 11 aus sicherheitstechnischer Perspektive gerechtfertigt sind.

## 1.3 Aufbau der Arbeit

Um ein besseres Verständnis über das Hardware Sicherheitsmodul TPM zu erlangen, ist es sinnvoll zunächst einen Einblick über die Herkunft und dem Konsortium hinter dieser Sache in Kapitel 2 zu erhalten. Hierbei wird auf die Entstehung vom Trusted Platform Module eingegangen, sowie der Ursprung der Trusted Computing Group und ihrer Aufgabe. Des weiteren braucht es ein Verständnis von Trusted Computing. Es wird ein Überblick über den Sicherheitschips erstellt und wie dieser funktioniert.
Kapitel 3 fokussiert sich auf verschiedene Anwendungsmöglichkeiten. Es handelt sich um Beispiele und Funktionen, die das TPM nutzen und ob das Prinzip von TC umgesetzt wird.
Der Hauptteil in Kapitel 4 handelt um Kritiken rund um das TPM und der TCG. Es werden Grenzen und Probleme des TPMs in seiner Funktion für Sicherheit aufgelistet. Anführend wird die Absicht der TCG und Auswirkung für Gesellschaft und Persönlichkeitsrecht im Diskurs gestellt, und was für eine Rolle Benutzerfreundlichkeit spielt.
Im Anschluss wird in Kapitel 5 alles einmal zusammengefasst.

# 2 Grundlagen zum Trusted Platform Module

Das Trusted Platform Module (TPM) ist ein Hardware-Sicherheitsmodul, welches fest in ein Motherboard, Mainboard oder auch in die Hauptplatine eines Computers eingebaut ist. Der kleine Mikroprozessor mit kryptographischen Funktionen ist die Hardwarekomponente des Trusted Computing (TC), welches Systeme manipulationssicher und vertrauenswürdig machen soll.
Um die Grundlagen des Moduls besser zu verstehen, wird hier ein Überblick über die Herkunft sowie ein Einblick in Trusted Computing, Spezifikationen und Funktionen gegeben.

## 2.1 Trusted Computing Group

Die Trusted Computing Group (TCG) hatte ihren Beginn als ein Konsortium mit dem Namen Trusted Computing Platform Alliance (TCPA) im Jahre 1999. Noch bevor dies für die herkömmliche IT-Landschaft bekannt war, existierten Begriffe wie Trusted Computing oder Trustworthy Computing innerhalb des amerikanischen Verteidigungsministeriums. Ihr Standard war um das Jahr 1983 herum eine Grundlage für die Common Criteria For Information Technology Security Evaluation, auch bekannt als CC, welche heute noch als anerkannten Standard für internationale Zertifizierung von IT-Systemen fungiert. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist hier autorisiertes Mitglied (Müller, 2008, S. 13).
In den Neunzigern stellten führende Persönlichkeiten in der Computerindustrie schon fest, dass durch das Internet und seine Kommerzialisierung die Art und Weise, wie PCs miteinander interagieren. Dieser Trend führte zu immer mehr Tatendrang, um die Sicherheit für solche Umgebungen zu erhöhen, denn schließlich waren Heimcomputer mehr auf Benutzerfreundlichkeit ausgelegt (Arthur et al., 2015, S. 1).
Die Vorgängerorganisation TCPA wurde von den großen Technikfirmen Microsoft, IBM, Compaq, Intel und Hewlett-Packard gegründet. Das Ziel des Konsortiums war ein Industriestandard für Computersysteme, sowohl Hard- als auch Software, der vertrauenswürdig ist, woher auch der Begriff „trust“ stammt. Dieser soll suggerieren, dass Plattformen, Hardware,

Software und Firmware, die alle zusammenwirken, stets sicher sind. Sie sollen sich so verhalten, wie beabsichtigt und designt. Ein Computer soll sicher hochfahren, kryptografische Schlüssel sollen sicher aufbewahrt werden, die Zusammensetzung eines Gerätes kann von externen Bestätigungsinstanzen attestiert und verifiziert werden. Die von der TCPA erlassenen Spezifikationen sollen Hardware-Module und Infrastrukturen erschaffen, die genau diese Sicherheitsfunktionen erfüllen (Eckert, 2023, S.592).

Die TCPA wuchs auf bis zu 200 Mitglieder an, mehrere Unternehmen wie Infineon, Siemens, Nokia und weitere waren Teil dieser Allianz. Da allerdings bei Entscheidungen Einstimmigkeit vorausgesetzt war, stellte sich die TCPA als zu rigide heraus. Aus der TCPA ging 2003 die Trusted Computing Group (TCG) hervor. Diese übernahm die Aufgaben und Ziele und existiert bis heute mit führenden Technikunternehmen. Abstimmungen benötigen nun eine Zweidrittelmehrheit, es gibt eine flexiblere Organisationsstruktur, und sie entwickeln weiterhin offene Standards für Trusted Computing (Eckert, 2023, S.593; TCG, 2026c unter *Membership*).

- Promoter haben eine exklusive Mitgliedschaft mit einem nicht einheitlichen oder bekannten Jahresbeitrag. Ihre Mitglieder sind im Vorstand und entscheiden über die Aufnahme neuer Firmen. Darunter befinden sich Microsoft, IBM, AMD, Nvidia und Intel. Stand: 15 Mitglieder.
- Contributor besitzen neben den Promotern die meisten Mitgliederrechte und können auch abstimmen. Ein Jahresbeitrag von $15000 ist zu entrichten. Stand: ca. 47 Mitglieder.
- Associates und Adopter bekommen Einblicke in Spezifikationen, Entwürfe und andere nicht öffentliche Informationen. Nur in gesonderten Arbeitsgruppen erhält Einblicke, Teilnahme und Stimmrecht, wer einen Jahresbeitrag von $10000 als Associate entrichtet. Für einen Jahresbeitrag von $7500 (bzw. $2500 bei Unternehmen mit weniger als 100 Mitarbeitenden), erhalten Mitglieder als Adopter Zugang, jedoch entfällt das Stimmrecht. Stand: 19 Mitglieder.
- Das Industry Liaison Program gewährt wissenschaftlichen Institutionen und Universitäten freien Zugang zu Technologie und Information. Es gibt kein Stimmrecht.

Die Promoter sind alle große Unternehmen aus der Halbleiterindustrie, Mikroelektronik, Informationstechnik, Hard- und Softwareentwicklung sowie Telekommunikationstechnologie, Consulting und Automobilbau. Die Prozessoren und Ein-Chip-Systeme (SoC), die in Heimcomputer, Server, Laptops, Smartphones, IoT Geräte und Tablets integriert sind, werden fast alle von diesen Unternehmen hergestellt.

## 2.2 Trusted Computing in der Cyber-Sicherheit

„Trusted Computing ist eine Cyber-Sicherheits- und Vertrauenswürdigkeitstechnologie. Mithilfe von Trusted Computing stehen moderne und intelligente Cyber-Sicherheitsarchitekturen, -konzepte und -funktionen zur Verfügung, mit denen IT-Systeme mit einer höheren Robustheit und einem höheren Cyber-Sicherheitslevel umgesetzt werden können. Der besondere Schwerpunkt liegt dabei auf der Verifikation der Integrität eines IT-Systems." (Pohlmann, 2022, S. XI und S. 269)

Trusted Computing ist komplex und kann unübersichtlich wirken. Im Grunde besteht es aus aufeinander folgenden Prozessen und Verankerungen, die eine Trusted Platform ausmachen. Sie ist eine verifizierte Sicherheitsplattform, die ihre Basis in kryptografischen Operationen hat. Daten, Ausführungen und Verfahren sollen vor Cyber-Sicherheitsproblemen schützen, wenn auch nur mitigierend. Pohlmann spricht hier auch von einer Veränderung von „reaktiven Cyber-Sicherheitssystemen" hin zu „proaktiven Cyber-Sicherheitssystemen". Seiner Ansicht nach ist das „Software- Qualitätsproblem", wo Trusted Computing eingreift und die Wirkung zu reduzieren hilft, die große Herausforderung. Während reaktive Cyber-Sicherheitssysteme wie ein Airbag funktionieren und Schaden reduzieren sollen (zum Beispiel Anti-Spam oder Intrusion-Detection-Systeme), sind proaktive Cyber-Sicherheitssysteme darauf ausgelegt, den Schaden komplett zu verhindern, sei es mit Virtualisierungen oder isolierten Umgebungen. Hier müssen aber Endgeräte grundlegend anders aufgestellt sein, die Organisation muss diese Sicherheitsinfrastruktur und Technologien übergreifend nutzen können. Dies ist vergleichbar mit dem elektronischen Stabilitätsprogramm bei Autos, man lässt das Schleudern also gar nicht erst zu (Pohlmann, 2022, S.269-270).

Das Software-Qualitätsproblem ist eine nicht zu unterschätzende Herausforderung, denn Software befindet sich heutzutage überall. Sie existiert in Heimcomputern für Entertainment oder Bürotätigkeiten, aber auch in Autos, Flugzeugen, Industriegeräten und auch in etlichen smarten Geräten. Ein Auto funktioniert heute nicht nur auf mechanischer Grundlage. Sensoren piepen und erkennen, ob man richtig einparkt, und erhöhen nicht nur den Komfort des Autofahrens, sondern auch die Sicherheit. Schlussfolgernd muss die Software in solchen Geräten auch einem sehr hohen Qualitätsstandard entsprechen. Sie darf und sollte nicht verändert werden, und muss daher regelmäßig verifizieren, dass dieser Stand auch so beibehalten wird. Außerdem muss die Fehlerdichte einer Software sehr gering gehalten werden, wenn Leib und Leben beeinflussbar sind (Fehlerquotient <0,5 in Fehler pro 1000 Programmzeilen). Ein Videospiel hingegen kann Kultstatus allein durch seine Bugs erhalten. Vergleichbar ist hier bei kritischer Software ein Fehlerquotient von kleiner als 0,5, normal gilt ein Quotient zwischen 2 und 5. Laut Pohlmann soll Trusted Computing das Software-Qualitätsproblem deutlich reduzieren können (Pohlmann, 2022, S.271).

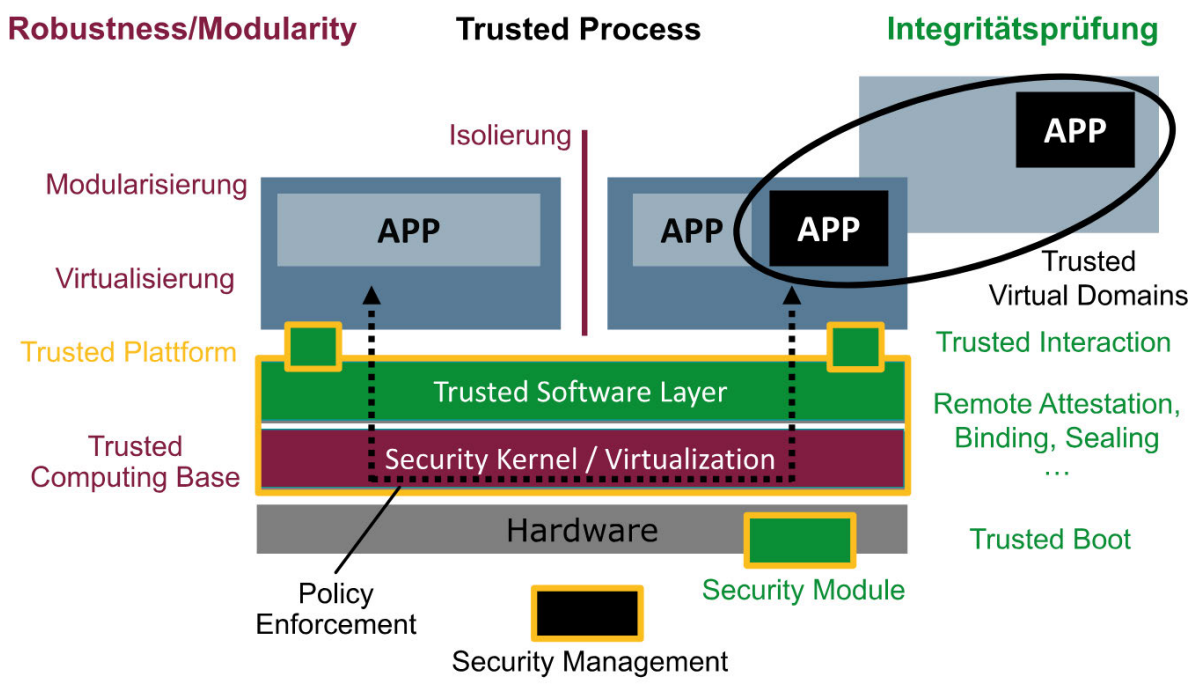


Abbildung 2.1: Modell in Architektur und Prinzip eines vertrauenswürdigen IT-Systems nach Trusted Computing (Quelle: Pohlmann, 2020, S.7 ; Pohlmann, 2022, S. 272)

Abbildung 2.1 zeigt eine Möglichkeit für ein vertrauenswürdiges IT-System sowie seine Cyber-Sicherheitsmechanismen und Prinzipien.

Die Trusted Computing Base (TCB) dient als Grundlage für Robustheit und Modularität. Man kann auch von einem Fundament sprechen, auf dem alle weiteren Komponenten aufgebaut sind. Als Basis ist sie daher der wohl kritischste Teil des Systems. Besitzt diese eine Schwachstelle, kann man das gesamte System als kompromittiert betrachten. Außerhalb dieser TCB kann man mit Sicherheitspolicies oder Policy Enforcement auf Schwachstellen reagieren und diese einschränken oder mitigieren, zum Beispiel die Virtualisierung einfach in den Urzustand versetzen und neu aufsetzen oder starten. Der Vorteil bei Virtualisierungen ist, dass Fehler und Schadsoftware innerhalb dieser Instanz verweilen und nur in diesem abgegrenzten geschlossenen Bereich funktionieren. Die Isolation ist vorteilhaft, da Einfluss auf andere Virtualisierungen ausbleiben. Gefahren von Malware und böswilligen Akteuren sind und bleiben ausgegrenzt. Im Aspekt der Modularisierung kann man ähnliche Programme und Anwendungen in einer virtuellen Maschine kombinieren, während man je nach Bedarf des Sicherheitsrichtlinie eine andere Anwendung in einer anderen Virtualisierung bereitstellt.

So kann man Anwendungen auch je nach Maschine und Sicherheitsbedarf nutzen. Während Textbearbeitung in einer virtuellen Maschine läuft, läuft der Browser in einer anderen Maschine, und so führt man weitere Separationen fort (Pohlmann, 2022, S. 272-273).
Um eine vertrauenswürdige Basis zu haben, wird ein Betriebssystem mit Mikrokernel dem monolithischen Kernel vorgezogen. Grund hierfür ist die Abgrenzung vom Kernel-Modus und User-Modus, wobei sich im Kernel nur Funktionen wie Prozesse und Speichermanagement sowie Funktionen für Synchronisation und Kommunikation zwischen Programmen befinden. Treiber-Ausfälle lassen nicht das System abstürzen, da jeder Dienst im eigenen User-Prozess läuft. Neue Dienste können ohne Kernel implementiert werden, sind also modular. Jede Anwendung oder Programmbibliothek ist ein Prozess im User-Modus. Auch wenn ein Mikrokernel grundsätzlich langsamer als ein monolithische Kernel ist, ist die Wartbarkeit allein durch die die geringere Anzahl von Programmzeilen – um die 20000 Zeilen Code gegenüber mehreren Millionen – um ein Vielfaches besser. Die Funktionsweise eines Mikrokernel hat jedoch eine komplexe Architektur zur Folge: Die getrennten Dienste und die Kommunikation zwischen ihnen führen zu Einbußen in Performance und Leistung. Aus diesem Grund eignet sich aber ein Mikrokernel auch als TCB (Pohlmann, 2022, S.276-277).

Die Integritätsprüfung ist der Bereich, in dem die Vertrauenswürdigkeit des Systems überprüft und attestiert wird. Jeglicher kryptographische Schlüssel sollte hier auch sicher aufbewahrt werden. Hier kommt das TPM ins Spiel, das genau dies gewährleisten kann. Der Trusted Software Layer dient als Schnittstelle für Dienste und IT-System. Er soll diese messbar und vertrauenswürdig gestalten, und die Integrität mit Hilfe des TPMs sicherstellen (Pohlmann, 2022, S.273; Eckert, 2023, S. 595).
Das Security Module ist für die Integritätsprüfung ausschlaggebend; im Grunde kann man hier von einem Hardware-Sicherheitsmodul sprechen. Fast immer handelt es sich um ein TPM, Ausnahmen sind verschiedene Standards, die später noch aufgeführt werden. Dieser Sicherheitschip mit kryptografischen Funktionen ist vergleichbar mit einer Smartcard, wobei der wesentliche Unterschied die Verifizierung des Gerätes statt einer Person ist. Das TPM hat ein paar weitere Funktionen für Speicherungen und Überprüfungen von Messdaten über den Zustand eines Systems (eine genauere Beschreibung über das Modul und die Funktionen selbst folgt in den nächsten Kapiteln). Trusted Boot sorgt für einen vertrauenswürdigen Zustand beim Aktivieren des Systems; dieser ist vorher definiert. Remote Attestation ist die Messung von Vertrauen gegenüber anderen, sogar auch fremden Systemen. Diese dient als Schritt vor Beginn einer Interaktion der Systeme. Bindung sowie Sealing sind spezifische Funktionen vom TC. Verschlüsselte Daten, wie zum Beispiel Schlüssel, werden sicher an ein TPM über Binding gebunden, und Sealing versiegelt und bindet solche Daten an Soft- und Hardware sowie das TPM. Trusted Interactions bezeichnet Sicherheitsdienste, die eine vertrauenswürdige Handhabe von Information gewährleisten. Beispielsweise können Darstellungen in Dokumenten nicht von anderen Anwendungen manipuliert werden (Pohlmann, 2022, S.274).

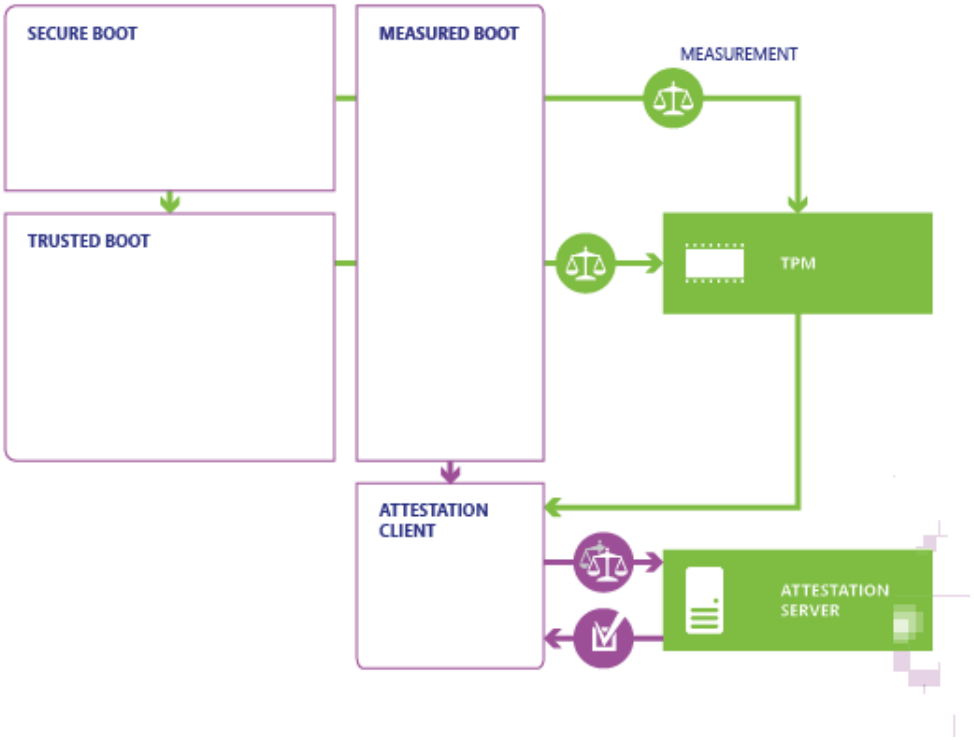


Abbildung 2.2: Darstellung einer Integritätsprüfung mit TPM über Secure Boot, Trusted Boot, Measured Boot und Remote Attestation (Quelle: Microsoft, 2025d)

Vereint man alle Sicherheitsaspekte, kann man von Trusted Process sprechen. Alle Abläufe in und mit dem kompletten System sind mit Hilfe von Security Management umfassend vertraulich zusammengefasst und nutzbar. Policy Enforcement gewährt Regelanwendungen und Richtlinien, die sowohl im eigenen als auch in anderen Systemen umsetzbar sind. Schlussendlich dienen Trusted Virtual Domains als reine Umsetzung, damit die Sicherheitskonzepte übergreifend ermöglicht werden. In der Theorie stellt das Konzept der Trusted Platform alle bis hier genannten Sicherheitsaspekte als eine vertrauenswürdige Basis. Trusted Computing liefert so die Sicherheitsplattform für ein widerstandsfähiges Cyber-Sicherheitskonzept, bei dem die Integrität von Systemen verifiziert ist und gegen Angriffe einen gewissen Schutz bietet (Pohlmann, 2022, S. 275).

### 2.2.1 TPM als Root of Trust

Die TCG spezifiziert beim Trusted Computing einen Sicherheitsanker, man kann auch von einem Root of Trust sprechen. Software hat schlichtweg Grenzen in der Cyber-Sicherheit, denn ihre Schutzmechanismen können manipuliert werden. Daher ist die Wahl geeigneter Hardware als Schutz für solche Software zu begrüßen. Sie kann als Vertrauensanker in der Sicherheit angewendet werden und so präventiv Gefahren abschwächen oder sogar komplett verhindern. Was Hardware-Sicherheitsmodule so interessant macht, ist ihr robuster Schutz vor Auslesen und Manipulation von sensiblen Sicherheitsinformation – so zumindest die Idee. Darunter fallen unter anderem geheime kryptographische Schlüssel, die für Verschlüsselung, Authentifizierung und Signaturen benutzt werden können, zum Schutz vor unerlaubtem Kopieren oder Veränderungen von Software sowie auch für sensible Daten wie die bei Transaktionen. Operationen, die kryptografische Berechnungen erfordern, verlassen das Sicherheitsmodul nicht. Schlüssel können also benutzt werden, ohne diese jemals zu kennen. Das Trusted Platform Module (Abb. 2.3) ist genau solch eine Hardware und soll diese Anforderungen erfüllen (Pohlmann, 2022, S. 119, S. 277).

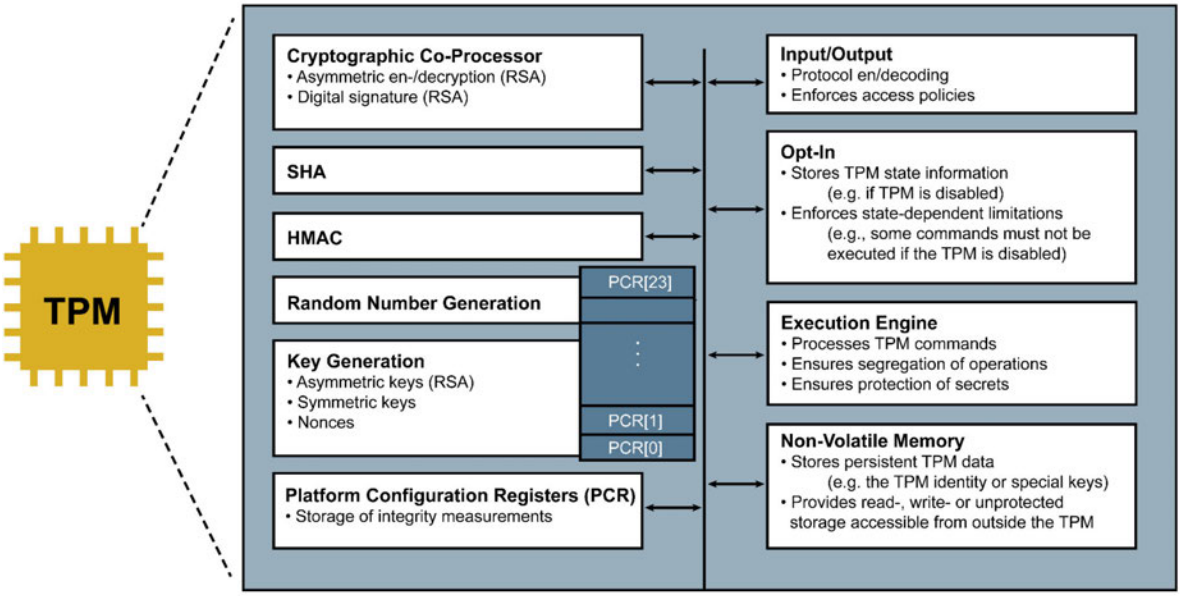


Abbildung 2.3: Trusted Platform Module (Quelle: Pohlmann, 2020, S.13 ; Pohlmann, 2022, S. 123)

Als Root of Trust funktioniert das TPM schon beim Start des Computers. Der Zustand von Hardware und Software, inklusive BIOS, Betriebssystem, Festplatten, Arbeitsspeicher, Treiber und weitere Komponenten, wird mit einer Hashfunktion gemessen und im Platform

Configuration Register (PCR) gespeichert. So ist die Messbarkeit des Systems gegeben. Der Zustand wird gespeichert. Sobald etwas ausgetauscht wird befindet sich das Gerät nicht mehr im Originalzustand, es verliert also an Vertrauen. Diese Form von Ausweisung gegenüber anderen IT-Systemen oder Nutzern wird auch Attestation genannt; sie dient der Verifizierung des Zustandes. Eine weitere Funktion bietet das TPM beim Sealing, bei dem wichtige Daten versiegelt und gespeichert werden. Entsiegelt werden diese nur bei korrekter Attestierung. Die Integrität ist also weiterhin gegeben, und man befindet sich in einer vertrauenswürdigen Umgebung (Pohlmann, 2022, S. 122-123).

Für normale IT-Systeme hat sich die TCG auf eine Spezifikation namens Core Root of Trust for Measurement (CRTM) geeinigt. Das CRTM funktioniert als Software und misst beim Booten den Systemzustand sowohl der Software als auch der Hardware, unabhängig davon, ob sie im TPM oder über das BIOS agiert. Die einzelnen gemessenen Zustände werden dann im PCR des TPMs gesichert, so dass mit dieser Information die Integrität überprüft werden kann. Der gesamte Prozess vom Aufbau der Vertrauenskette beschreibt man auch als Authenticated Boot. Vertrauenswürdige Bereiche sind im übrigen transitiv. Ist der Bootloader vertrauenswürdig, erfordert er auch Vertrauen vom BIOS. Ein Verlauf ist an Abbildung 2.4 zu erkennen (Pohlmann, 2022, S.278; Eckert, 2023, S. 614).

### 2.2.2 Schlüsselidentitäten eines TPM

Ein TPM besitzt mehrere Schlüssel, um die eigene Identität zu bestätigen und ordentlich zu operieren. Diese Schlüssel sind nicht migrierbar und werden auch Non-Migratable Keys genannt. Sie sind alle asymmetrische RSA-Schlüsselpaare, haben eine Länge von 2048-Bit und befinden sich im nicht-flüchtigen Speicher des TPMs (Pohlmann, 2022, S. 279, S. 281).

Der Endorsement Key (EK) ist die vom TPM-Hersteller eindeutig zugeordnete Identität an den Mikrochip. Er setzt sich aus einem RSA-Schlüsselpaar zusammen, bei dem der private Schlüssel fest im TPM gespeichert und nicht auszulesen ist. Dieser darf auch nur zum Entschlüsseln benutzt werden, Signierungen sind ausgeschlossen. Rein aus Sicherheits- und Datenschutzgründen darf der Schlüssel das TPM nie verlassen. Wird der Chip gebaut, wird der EK erzeugt, und der Hersteller zertifiziert diesen Schlüssel mit einem Endorsement-Zertifikat. Der EK befindet sich im nicht-flüchtigen Speicher des TPMs, ist einzigartig und kann nicht migriert werden. Genau diese Bedingungen machen den EK als wichtigste Grundlage des TPMs aus. Das Zertifikat für das TPM enthält den Herstellernamen, Modellnummer, Version und den öffentlichen Schlüssel des EKs, welcher eine Plattform identifizieren kann, was wiederum datenschutzrechtliche Rückschlüsse zulässt. Außerdem gibt es noch ein Plattform-Zertifikat, um die Gültigkeit der korrekten Montur an das jeweilige Motherboard zu bestätigen. Es gibt

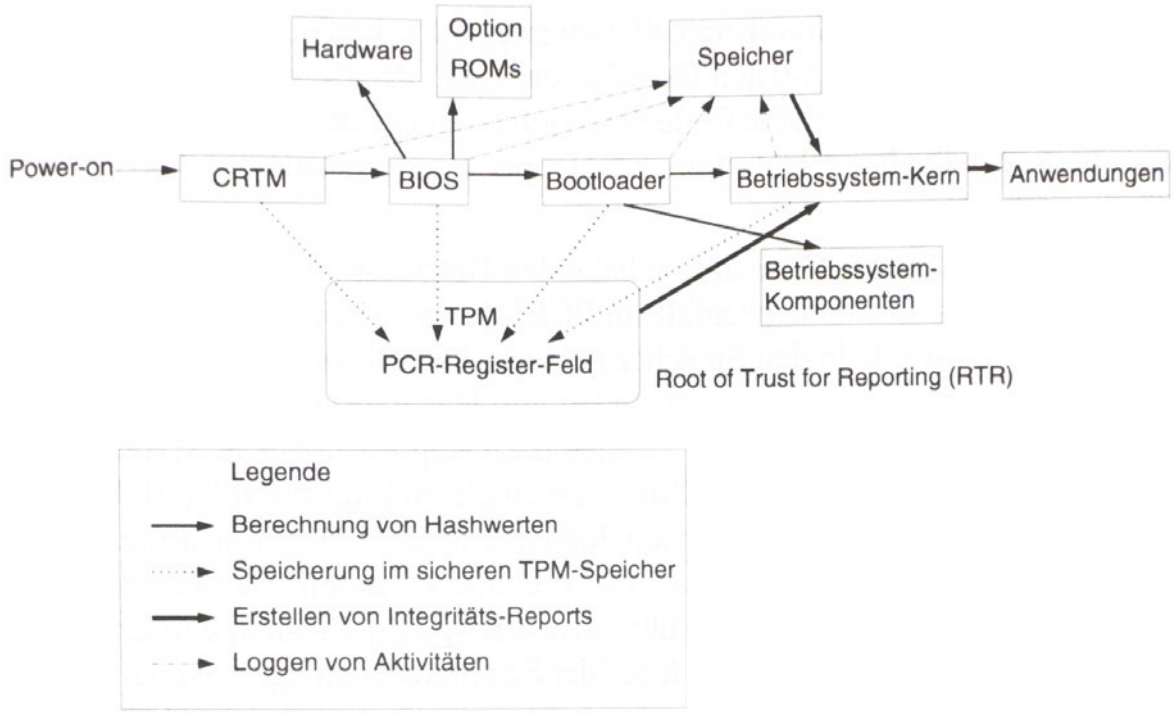


Abbildung 2.4: Berechnung von Integritätswerten beim Startvorgang nach TCG (Quelle: Eckert, 2023, S.615)

zwar Aufsteckmodule für Motherboards, doch heutzutage werden TPMs fest verlötet. Nur durch diese Zertifikate kann man bestätigen, dass es sich um eine Trusted Platform handelt (Pohlmann, 2022, S. 279-280; Eckert, 2023, S. 604).

Der Storage Root Key (SRK) ist ein weiterer nicht migrierbarer Schlüssel, der sich im nichtflüchtigen Speicher des TPMs befindet. Der SRK dient als Basis für die Root of Trust for Storage (RTS), welche als sicherer Datenspeicher im TPM implementiert ist. Wechselt das TPM den Besitzer, oder kommt ein neuer Nutzer hinzu, wird dieser eine neue Schlüsselhierarchie erstellen. Löscht man einen Benutzer, wird auch der SRK gelöscht (Pohlmann, 2022, S. 281; Eckert, 2023, S.606).

Die Attestation Identity Keys (AIK) sind, wie der Name schon vermuten lässt, zur Attestierung notwendig. AIKs sind vergleichbar mit Aliassen, denn sie verhindern eine Profilerstellung des TPMs. Da EKs Schlüssel nicht signieren dürfen, übernehmen AIKs diesen Schritt. Das TPM kann beliebig viele AIKs für jeden Dienst erstellen: So kann beispielsweise eins für E-Mail-Kommunikation und ein anderes für Online-Banking genutzt werden. Wiederum verifiziert ein AIK die Integrität der eigenen Plattform gegenüber Dritten, zum Beispiel einer Zertifizierungsstelle (CA). Es muss allerdings sichergestellt werden, dass nur richtige TCP

gültige AIKs erstellen können. Die AIKs werden im Prozess Remote Attestation gebraucht, um eine stetige Beglaubigung weiterer Anwendung und Kommunikation zu ermöglichen, die vertrauenswürdig bleibt (Pohlmann, 2022, S. 281; Eckert, 2023, S. 604-605).

## 2.3 Sicherheitsfunktionen eines TPM

Ein TPM besitzt zahlreiche Funktionen, um Trusted Computing zu ermöglichen. Hauptfunktionen sind Mittel für kryptographische Dienste wie einen Hardware-basierten Zahlen-Zufalls-Generator, auch bekannt als Random-Number-Generator (RNG). Software-basierte RNG sind bekanntlich nicht wirklich zufällig, weshalb sie auch den Namen Pseudo RNG tragen, da sie auf Simulation und Algorithmen aufbauen. In der Hardware spricht man von True RNG. Diese benutzen reine Physik, um wahre Zufälligkeit zu erzeugen, beispielsweise Thermik oder Spannung (Windows, 2024). Dieser Generator wird vom TPM für Schlüsselerstellung, Signierung und Erzeugen von Hashwerten genutzt. In den älteren Versionen waren nur RSA und SHA-1 als Verschlüsselungsalgorithmen verfügbar. Die aktuellen TPMs besitzen eine deutlich höhere Kryptoagilität. Bei Bedarf können sie die Algorithmen wechseln und weisen so eine deutlich höhere Lebensdauer und Beständigkeit auf. Darunter fallen SHA-2 und auch Elliptic-Curve-Cryptography (ECC) (Eckert, 2023, S. 600, S. 620).

Um die Funktion des RTS getreu nach TC umsetzen zu können, kann ein TPM Daten und Schlüssel per Binding und Sealing ordentlich verwalten.
Binding ist die Bindung von Daten, beispielsweise auf einer Festplatte, an das TPM. Wenn die Daten mit einem nicht migrierbaren Schlüssel verschlüsselt werden, kann kein anderes TPM die gebundenen Daten entschlüsseln. Es ist aber auch möglich, migrierbare Schlüssel zu benutzen. Diese sind dann mit einem RSA-Schlüsselpaar erstellt, welches wiederum mit Binding-Befehlen des TPMs erstellt werden muss (Pohlmann, 2022, S. 282-283, S. 286).
Sealing geht einen Schritt weiter und bindet die Daten nicht nur an das TPM, sondern auch an die spezifische Plattformkonfiguration. Hier kommen die PCR ins Spiel, da diese das Binding mit einem weiteren vertrauenswürdigen Wert versiegeln. Diese Redundanz könnte man als doppeltes Binding verstehen. Allerdings wird hier mit nicht-migrierbaren Schlüsseln gearbeitet, um die Datensicherheit zu gewährleisten. So kann man in der Security Policy ganz feste Bedingungen stellen, um vertrauenswürdigen Datenzugriff zu realisieren (Pohlmann, 2022, S. 282-283, S. 286; Eckert, 2023 S. 602).

Die Menge an Schlüsseln verlangt die Verwaltung einer Schlüsselhierarchie, die vom TPM übernommen werden kann. Als Basis zählt hierfür der SRK. Als nicht migrierbarer Schlüssel

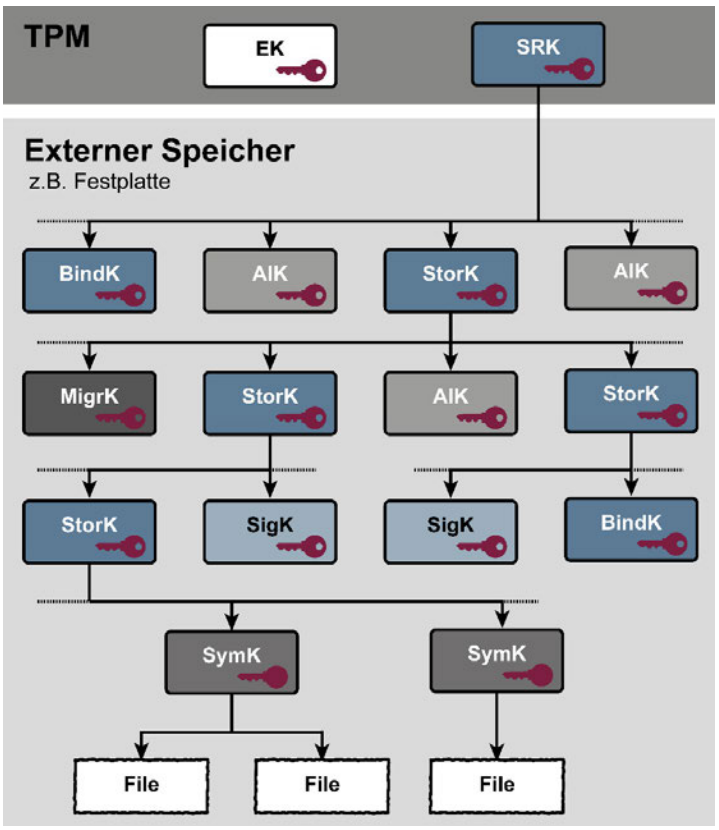


Abbildung 2.5: TPM-Schlüsselhierarchie ausgehend vom SRK (Quelle: Pohlmann, 2020, S.18; Pohlmann, 2022, S. 283)

schützt dieser alle anderen Schlüssel in der Hierarchie. Mit dieser Funktion lassen sich Schlüssel auch außerhalb des TPMs speichern. Die Hierarchie ist durch die Größe des externen Speichers begrenzt. Die Speicherschlüssel (`StorK`) schützen alle ihnen untergeordneten Schlüssel. In Abbildung 2.5 ist zu erkennen, dass der Speicherschlüssel `StorK` die ihm untergeordneten Schlüssel schützt. Der SRK liegt im TPM und verschlüsselt den `StorK`, Bindungsschlüssel (`BindK`) und AIKs. Dem verschlüsselten `StorK` untergeordnet sind weitere `StorK`, welche er wiederum verschlüsselt hat, zusätzlich dazu Migrationsschlüssel (`MigrK`), Bindungsschlüssel (`BindK`), Signaturschlüssel (`SigK`) und Symmetrische Schlüssel (`SymK`). Anzumerken ist, dass je nach Policy des IT-Systems solche `StorK` migrierbar sind. Verständlicherweise muss dies mit einem Wiederherstellungsschlüssel oder Recovery Key realisiert werden. Grundsätzlich werden `StorK` aber versiegelt, unterliegen also einer strikten Plattformkonfiguration (Pohlmann, 2022, S. 282-283, Eckert, 2023, S. 606-607).

Authenticated Boot und PCR sind wesentliche Funktionen des TPMs. In Abbildung 2.4 wird so ein Prozess verdeutlicht. Im Grunde wird über CRTM ein Hashwert berechnet und ins

PCR geschrieben, das sich im flüchtigen Speicher befindet. Der Vorgang wird vom BIOS bis zu mehreren Anwendungen wie in einer Kette fortgeführt. Werden neue Hashwerte beim Authenticated Boot erstellt und ins PCR eingefügt, so wird ein neuer Hashwert aus dem alten und neuen erzeugt. Diese Hashwerte können nun per Remote Attestation ausgelesen, gemessen und attestiert werden, um den Systemstatus als vertrauenswürdig einstufen zu können. Damit ein System als vertrauenswürdig eingestuft werden kann, bedarf es einer Instanz, die Zertifikate ausstellen (CA) kann. Die CA hat eine Konfigurationsliste an erlaubten Systemen. Besitzt ein System die Vorgaben aus der Liste, so werden Kommunikation und Anwendung beglaubigt (Pohlmann, 2022, S. 285-289; Eckert, 2023, S. 609-611).
Die prüfende CA übergibt dem IT-System eine zufällige Zahl Z, welche im TPM dann mit dem Hashwert der aktuellen PCRs und Z mit dem vorhandenen AIK signiert wird. Diese erhält dann die CA zurück und vergleicht die Konfiguration mit der ihr bekannten Liste. Stimmen die überein, wird das System beglaubigt (Pohlmann, 2022, S. 287-289, Eckert, 2023, S. 610-611).

## 2.4 Versionen und Standards

Im Folgenden werden verschiedene Ausführungen des TPMs sowie einige der Besonderheiten und Eigenschaften aufgelistet. Die Entwicklungsgeschichte umfasst eine Zeitspanne von mehr als 25 Jahren, durchlief viele Veränderungen, aber auch Diskussionen. Schwierigkeiten hat die Öffentlichkeit auch, weil die Spezifikationen komplex und schwer zu lesen sind; sie sind mehr für Hersteller und Anwendungsentwickler relevant. Die Versionen 1.2 und 2.0 sind jeweils als ISO-Standard (ISO/IEC 11889-1:2009 und ISO/IEC 11889-1:2015) veröffentlicht, wobei der Standard 2.0 sein älteres Pendant ablöst. Anzumerken ist, dass nur Deutschland und China gegen die Nominierung als ISO-Standard gestimmt haben (Biselli, 2015). Die verschiedenen Spezifikationen der TPM-Standards und -Spezifikationen sind auf der Website der TCG einsehbar (1.2: TCG, 2026a - 2.0: TCG, 2026b).

### 2.4.1 TPM Version 1.1b

Das erste richtige TPM, welches auf Hardware verbaut wurde, war die Spezifikation 1.1b. Im Jahre 2003 hatte diese Version schon viele der bereits oben genannten Funktionen inne, sie waren jedoch nicht ganz ausgereift. Die Algorithmen zur Schlüsselgenerierung waren auf RSA beschränkt, und es gab datenschutzrechtliche Bedenken bezüglich der Attestierung von AIKs. Die Zertifizierungsstellen (CA) konnten theoretisch ein Nutzerprofil erstellen, weil sie zu dieser Spezifikation Zugang zu dem öffentlichen EK des TPMs brauchten, da die

Beglaubigung sonst nicht gelänge (Arthur et al., 2015, S.2; Eckert, 2023, S. 611).
Ein weiteres Problem war die Hardware-Anbindung. Die Interfaces waren je nach Hersteller unterschiedlich, auch das Chipgehäuse und die Steckverbindungen waren nicht immer einheitlich: Es fehlte schlichtweg ein Standard. Abgesehen davon war der Chip nur mit einem Passwort geschützt, welcher mit einem Wörterbuchangriff irgendwann geknackt werden konnte. Noch unhandlicher war der Chip, da dieser keinen nicht-flüchtigen Speicher besaß. Zertifikate wurden gelöscht, falls man eine Festplatte formatierte. Wollte man Schlüssel auf ein anderes TPM migrieren, brauchte es den TPM und den Schlüssel-Besitzer, welche oft unterschiedliche Instanzen waren. Dementsprechend waren Policies und Richtlinien simpel und wiesen nur die Grundfunktionen auf (Arthur et al., 2015, S.3).

### 2.4.2 TPM Version 1.2

Die Spezifikation 1.2 wurde 2003 veröffentlicht; vertrieben und verbaut wurde sie erst gegen 2005. Viele der in der ISO/IEC-Ordnung hinterlegten Anforderungen sind umgesetzt und entsprechen den Anforderungen der TCG im Trusted Computing. Die Schwächen der 1.1b wurden ausgemerzt; man einigte sich auf den Hash-Algorithmus SHA-1 sowie optionale Nutzung von AES. Spezifikation 1.2 besitzt einen nicht-flüchtigen Speicher; ein standardisiertes Software-Interface ist implementiert, Chip und Steckleisten auf dem Motherboard sind normiert. Nachdem Datenschützer sich über die mangelnde Umsetzung der CA äußerten, wurde die Direct Anonymous Attestation (DAA) als Konzept eingeführt. Nach diesem Konzept wird die Privatsphäre der Plattform gestärkt, da kein EK bei der Beglaubigung benötigt wird, um das IT-System zu verifizieren. Dies basiert auf Zero-Knowledge, der CA kann das TPM authentifizieren, ohne dass eine eindeutige Identität des TPMs preisgegeben wird. 1.2 war im Übrigen rückwärts-kompatibel zu 1.1b, was allerdings nur mäßig gut funktionierte und zur Komplexität beitrug (Arthur et al., 2015, S. 2-3; Eckert, 2023, S. 611).

### 2.4.3 TPM Version 2.0

TPM 2.0 ist der bis heute funktionelle und gültige Standard als Hardware-Sicherheitsmodul, welcher mittlerweile ab Werk auf alle Motherboards gebaut wird. Die meisten der im vorherigen Kapitel beschriebenen Funktionen sind hier gültig. Ein wesentliches Upgrade war die Implementierung der Krypto-Agilität. Ein Ärgernis der Version 1.2 war, dass nur SHA-1 in der Hardware codiert war. Auch wenn es keine stärkeren kommerziellen Algorithmen gab, haben Kryptographie-Experten bereits im Jahr 2005 theoretische Angriffsszenarien auf diesen Algorithmus veröffentlicht. Da Algorithmen mit der Zeit an Stärke verlieren, hat

man sich auf eine agile Lösung geeinigt. Obwohl die Art und Weise des Angriffs nicht auf das TPM anzuwenden war, wollte man keine Zeit verlieren und für die Zukunft vorsorgen. Hinzugekommen sind SHA-2 mit unterschiedlichen Schlüssellängen, AES als Standard für symmetrische Schlüssel und der Elliptische Kurven Kryptographie (ECC), um einige zu nennen. Da AES nun nicht mehr optional war, hat man Daten symmetrisch und symmetrische Schlüssel asymmetrisch verschlüsselt. Der Chip musste also nicht ständig mit langsameren RSA-Operationen arbeiten, was der allgemeinen Performance zugutekam (Arthur et al., 2015, S. 3-4; Eckert, 2023, S.620).

In der Version 1.2 verlief die Autorisierung auf Passwortbasis. Eine Erweiterung der Dienste in 2.0 ist die enhanced authorization (EA), die erweiterte Autorisierung, die eine Richtlinienbasierte Autorisierung ermöglicht. Über solche Policies kann Zugriff auf bestimmte Bereiche und Funktionen wie Schlüssel und Speicherbereiche des TPMs erlaubt werden. Außerdem gibt es Möglichkeiten für Mehrfachfaktor-Authentifizierung oder Beschränkungen für Ressourcennutzung nach Anzahl oder Zeit. Hinzukommen flexibleres Management mit Privacy Administratoren; ein solcher kann unter verschiedenen Identitäten durch Nutzung mehrerer EK-Schlüssel Autorisierungen durchführen. Meistens ist das der Besitzer des TPMs. Im Gegensatz zu TPM 1.2 ist TPM 2.0 ab Werk aktiviert, lässt sich aber ausschalten. Mittlerweile benötigt Windows 11 eine strikte Nutzung von TPM 2.0 (Arthur et al., 2015, S. 24; Eckert, 2023, S. 620-621).

### 2.4.4 fTPM

Wird über TPM gesprochen, wird meist ein diskreter Hardwarechip auf dem Motherboard gemeint, auch dTPM abgekürzt. Es existieren aber auch firmware-basierte Lösungen, die man fTPM nennt. Namhafte Hersteller wie AMD (AMD Platform Security Processor) und Intel (Platform Trust Technology) haben solche Alternativen im Chipsatz oder in einem Mikrokern des CPUs implementiert, welche über das BIOS zu aktivieren sind. Die Funktion ist grundlegend mit einem dTPM identisch, nur sind sie kostengünstiger und leichter mit Updates zu pflegen. Da kein Chip verbaut wird, sind sie für kompakte Bauweisen wie bei Tablets und mobilen Endgeräten zu bevorzugen. Allerdings ist die Anwendungsweise entscheidend: Arbeitet man mit sicherheitskritischen Daten wie in Unternehmen und im Finanzsektor, werden dTPMs empfohlen. fTPMs könnten durch mangelnde Wartung Soft- und Firmware-Angriffen zum Opfer fallen, und da sie systemabhängigen Speicher nutzen, könnte auch die Computerperformance darunter leiden (Holger, 2025).

### 2.4.5 Weitere ähnliche Formen

TPMs müssen nicht immer in Computer eingebaut sein, sie finden auch Anwendung in der Automobil-Industrie. Autos verfügen über Internetanbindung, Software und mittlerweile auch komplexe IT-Systeme, so dass Angriffe potenziell ausführbar sind. Das Fraunhofer-Institut für Sichere Informationstechnologie hat eine Software-Plattform aufbauend auf TPM 2.0 entwickelt, die sichere Steuergeräte für Autos als Vertrauensanker bereitstellen kann (Fraunhofer-SIT, 2026).

Es gibt aber auch Unternehmen, Hersteller und auch Staaten, die den offenen Standard der TCG ablehnen und ihre eigenen umsetzen.
Apple hat seine eigene Form eines TPMs namens Secure Enclave als eigenen ARM Architektur SoC entwickelt, welcher neben dem Hauptprozessor als separater Kern integriert ist. Diese Technologie ähnelt mehr der ARM TrustZone, die in vielen IoT-Geräten und Smartphones integriert ist. Die Funktionalitäten sind denen eines TPMs nicht unähnlich: Auch hier gibt es TRNG, einen sicherer nicht-flüchtigen Speicher, Boot-Monitor als Vergleich zu Authenticated Boot und ähnliche Parallelen. Da Apple oft proprietär arbeitet, wurden die offenen Standards der TCG abgelehnt, um eigene Lösungen unabhängiger warten und integrieren zu können, wie zum Beispiel mit Apple-Pay oder die Face-ID-/Touch-ID-Technologie (Apple, 2024).

China hat seinen eigenen TPM mit dem Namen Trusted Cryptography Module (TCM) entwickelt (Feng et al., 2018, S. V). Der Chip referiert Konzepte und Architektur vom internationalen TC, soll sich aber vom TPM in Design und Technik etwas unterscheiden. Gründe hierfür können komplett andere Anforderungen an nationale Sicherheitsstandards für staatliche Behörden in der Informationstechnologie sein. Der TCM soll dem TPM überlegen sein, aber auch hier merkt Feng an, dass TC kein Allheilmittel ist, und weitere Bestrebungen in der Cyber-Sicherheit immer Thema sein werden (Feng et al., 2018, S. 44, S. 64-65).
Darunter könnten auch nur bestimmte kryptographische Algorithmen als Anforderung erlaubt gewesen sein, wie zum Beispiel den in China verbreiteten Signaturalgorithmus SM2. Die Ablehnung des ISO/IEC-Standards war auch durch die Forderung der Aufnahme von SM2 begründet (Biselli, 2015).

# 3 Funktionen und Anwendungen in der Cyber-Sicherheit

Es gibt viele Funktionen und Mittel, die das TPM als Root of Trust, als Vertrauensanker, nutzen. So soll die Vertrauenswürdigkeit zwischen System und Anwendung gewährleistet werden. Für Unternehmen sind diese Werkzeuge von großem Nutzen, aber auch Privatpersonen können von den Sicherheitsfunktionen profitieren.

## 3.1 Systemintegrität mit Secure Boot

Secure Boot ist eine Funktion im UEFI, die von der Nonprofit-Organisation The Unified Extensible Firmware Interface Forum (UEFI-Forum) ins Leben gerufen wurde. Ähnlich wie die TCG besteht diese Allianz seit 2006 aus mehreren Mitgliedern: große, namhafte Unternehmen wie Microsoft, Dell, Intel, AMD, Apple und mehr. Eine vollständige Liste ist der offiziellen Website zu entnehmen (UEFI-Forum, 2026, unter *Membership-List*). Die Mitgliederstruktur ist ähnlich wie bei der TCG mit Promoter, Contributor und Adopter aufgebaut. Das UEFI ersetzt in Computern die Schnittstelle zwischen Hardware und Betriebssystem, das BIOS, welches 1982 von IBM entwickelt wurde. Die Aufgaben von UEFI oder BIOS sind aber weitgehend identisch, weshalb man heute zwar immer noch vom BIOS spricht, oftmals aber UEFI meint. Beide sind das erste Programm, welches nach einem Start des Gerätes ausgeführt wird und das System initialisiert (Fritz et al., 2016, S. 721-723).
Das UEFI hat zahlreiche Funktionen eingeführt. Um Kompatibilität zu gewährleisten, kann immer noch unter Legacy Mode das BIOS für ältere Systeme emuliert werden, und es werden auch 32- und 64-Bit-Prozessoren unterstützt. Die Oberfläche lässt sich mit einer Maus steuern und hat eine hochauflösende Grafikausgabe, selbst Netzwerkverbindungen auf Firmware-Ebene sind möglich. Da die Firmware sich auf einem Flash-Speicher befindet, sind Updates leichter durchzuführen (Fritz et al., 2016, S. 723-724).
Da die Schwäche von update-fähiger Firmware für Schadsoftware ausgenutzt werden kann, soll Secure Boot auch hier Abhilfe schaffen. Secure Boot sorgt für sichere Update-Prozesse, prüft anhand einer Schlüsselverwaltung auf zulässige Treiber und signierte Programme, kann Signaturen widerrufen und erlaubt zudem nur, vertrauenswürdige Software während des

Startvorgangs auszuführen, darunter auch Bootloader. Windows verlangt Secure Boot, daher wird zumindest bei Windows Computern die Funktion ab Werk aktiviert. Wird der Legacy Modus für ältere Betriebssysteme verlangt, muss diese Funktion abgeschaltet sein (Fritz et al., 2016, S. 732-733).

Secure Boot erhält bei Aktivierung mehrere Variablen, die in ihrer eigenen Datenbank aufbewahrt werden. Diese können nur durch autorisierte Prozesse verändert werden.

- Plattform Key (PK) - Enthält den Master Key und wird vom Hersteller des Motherboards vergeben. Dieser öffentliche Schlüssel erlaubt Änderungen anderer Variablen, wenn er mit dem privaten Schlüssel authentifiziert wird. Der Besitzer des PK kann Werte im KEK verändern.
- Key Exchange Key (KEK) - Ablage für Zertifikate, die Updates an der Secure-Boot-Datenbank prüft und attestiert. Wird vom Hersteller gesetzt. Besitzer von Zertifikaten im KEK können Werte in den Datenbanken bearbeiten.
- db - Datenbank von Schlüsseln, Signaturen und Hashes. Hier wird während Secure Boot abgeglichen und nach Authentifizierung geprüft.
- dbx - Datenbank für die Sperrliste, speichert Information über nicht erlaubte Software und Treiber.
- SetupMode - Ist diese Variable aktiviert, gibt es keinen PK und Secure Boot ist deaktiviert.

(Fritz et al., 2016, S. 734-735).

In Bezug zum TPM ist Secure Boot ein komplementärer Ansatz zur Verhärtung des Systemstarts; man spricht hier auch von Measured Boot, was im TC dem Authenticated Boot entspricht. Secure Boot verhindert aktiv das Laden und Ausführen von nicht signierten Komponenten. Das TPM speichert Schlüssel und Messwerte sicher in der Hardware und macht diese nach CRTM messbar. Die Verkettung von kontrolliertem, sicheren Start und der Messung und Authentifizierung dessen, was gestartet wird, trägt zur modernen hardwarebasierten Sicherheit bei (Fritz et al., 2016, S. 736).

Die KEK von Windows, die seit 2011 im Einsatz sind, laufen im Juni 2026 und Oktober 2026 ab; offizielle Dokumentationen existieren bereits und die KEK werden auch über Windows-Updates bereitgestellt. Für Heimcomputer wird der KEK automatisch aktualisiert, vorausgesetzt man installiert Updates (Microsoft, 2025b).

## 3.2 Verschlüsselung mit Bitlocker

Bei Bitlocker handelt es sich um eine Festplattenverschlüsselungsfunktion, die seit 2007 auf dem Markt ist und hauptsächlich Nutzen in Windows-Betriebssystemen hat. Bitlocker ist nicht in Home-Editionen von Windows verfügbar; die Funktion ist nur in den Pro- und Enterprise-Versionen erhältlich. Mit Bitlocker lassen sich Partitionen, komplette Festplatten oder auch Wechseldatenträger wie USB-Sticks verschlüsseln. Als Verschlüsselungsalgorithmus wird AES-128 oder AES-256 verwendet. Die Verschlüsselung arbeitet als Blockchiffre, um Sektoren oder auch Blöcke der Festplatte zu verschlüsseln. Vor Windows 11 war der Algorithmus im Modus CBC-AES (Cipher Block Chaining Mode) als Standard im Einsatz, jetzt ist er ab Werk im XTS-AES Modus (XEX-based tweaked-codebook mode with ciphertext stealing). CBC-AES soll weiterhin von Bitlocker aus Kompatibilitätsgründen unterstützt werden, jedoch beseitigt XTS-AES Schwächen das Vorgängers, bei dem Angreifer den Inhalt entschlüsseln können, ohne jemals den Schlüssel für die Verschlüsselung zu kennen (Fritz et al., 2016, S. 646-647; Microsoft, 2025c, unter *Konfigurieren von Bitlocker*).
XTS-AES bietet laut BSI „relativ gute Sicherheitseigenschaften und gute Effizienz“, allerdings ist die Voraussetzung, dass der Angreifer nicht mehrere Abbilder der Festplatte zu verschiedenen Zeiten auswerten und zusammenführen kann (BSI, 2026, S. 25).

Ist eine Festplatte mit Bitlocker verschlüsselt, wird ein Wiederherstellungsschlüssel erstellt, damit man immer auf das Laufwerk zugreifen kann, falls ein Fehler auftritt. Diesen Schlüssel kann man Ausdrucken, Online im Microsoft Account sichern oder auf einem USB-Stick speichern. Startet man das System, muss im Bootprozess eine Authentifizierung stattfinden, um die Verschlüsselung zu entschlüsseln. Dies kann mit einem Passwort, PIN, einem konfigurierten USB-Stick oder auch durch mehrere Schritte kombiniert ausgeführt werden. Bitlocker lässt sich in einer vertrauenswürdigen Netzwerkumgebung entschlüsseln, vorausgesetzt im UEFI befinden sich die entsprechenden Treiber. Wenn man Bitlocker mit einem TPM benutzt, kann man vom TC Gebrauch machen. Das TPM prüft die Systemintegrität und entschlüsselt die Platte nur, wenn der Systemzustand vertrauenswürdig ist. Das TPM speichert und versiegelt den Bitlockerschlüssel, die Konfiguration ist im PCR messbar und kann dann automatisch beim Hochfahren das System entschlüsseln. Ist die Systemintegrität nicht im vorgesehenen Zustand, lässt sich die Festplatte ohne den Wiederherstellungsschlüssel nicht mehr wiederherstellen. Um die Sicherheit zu erhöhen, sollte man dennoch von der automatischen Entschlüsselung absehen und das TPM mit einem PIN absichern, so dass vor dem Bootprozess noch alles versiegelt ist (Fritz et al., 2016, S. 648-650; S. 663-665).

Falls man aus irgendeinem Grund die Systemintegrität willentlich, zum Beispiel durch ein Upgrade, verändern muss, so sieht Microsoft vor, dass man den Bitlocker-Schutz anhält und

nicht deaktiviert. Beim Anhalten wird der Schlüssel zur Verschlüsselung unverschlüsselt gespeichert. Der Vorteil ist hierbei eine Zeit- und Kosteneinsparung, da das gesamte Laufwerk nicht erneut ent- und verschlüsselt werden muss. Nach der Änderung kann man den Schutz wieder reaktivieren; so werden alle nötigen neuen Schlüssel erzeugt, das TPM kann den neuen Zustand messen und versiegeln. Der unverschlüsselte Schlüssel wird dann entfernt (Microsoft, 2025c, unter *Häufig gestellte Fragen*).

Falls man Linux verwendet und ein mit Bitlocker verschlüsseltes Laufwerk nutzen möchte, ist dies mit dem Tool Dislocker möglich. Besitzt man den Schlüssel auf USB-Stick oder hat das Laufwerk mit einem Passwort verschlüsselt, kann man hierüber auf die Daten zugreifen. Ist ein TPM im Einsatz, so ist der Zugang nur mit dem Wiederherstellungsschlüssel möglich (Aorimn, 2026).

Ab Windows 11 24H2 existiert für Windows-Home-Editionen eine hauseigene und automatische Geräteverschlüsselung, die sich nur an- und ausschalten lässt und keine anderen Konfigurationen ermöglichen. Diese Funktion wird kontrovers betrachtet und in Kapitel 4.2 kurz aufgeführt.

## 3.3 Windows Hello und Windows Hello for Business

Windows Hello ist eine moderne Anmeldefunktion für das Betriebssystem Windows 10 und 11. Diese unterstützt Biometrie wie Gesichts und Fingerabdruck sowie alphanumerische PIN-Eingaben. Windows Hello soll Anmeldungen mit Passwörtern ablösen, um so die Sicherheit beim Anmelden am Rechner oder Online in Accounts zu erhöhen. Unabhängig von der Anmeldeweise soll es böswilligen Akteuren die Möglichkeit nehmen, an Zugangsdaten zu gelangen, da sich der Anmeldeschlüssel nur auf dem Gerät befindet. Mit Hilfe des TPMs werden diese Schlüssel in der Hardware aufbewahrt und versiegelt. Da die Schlüssel niemals das TPM verlassen, ist die Angriffsfläche stark reduziert. Dieser Vorgang ist vergleichbar mit einer Bankkarte, bei der das Wissen (PIN) und die Karte (Besitz) den Zugang authentifizieren (Microsoft, 2026c).
Die biometrischen Authentifizierungen von Windows Hello sind vergleichbar mit denen von Apple und Android Smartphones. Windows läuft allerdings auf vielen verschiedenen Rechnern, daher sind Anforderungen für hardwarebasierte biometrische Authentifizierung festgelegt. Die Falschakzeptanzrate für Peripherie müssen bei Kameras unter 0,001%, bei Fingerabdrucksensoren bei 0,002% liegen, die Falschrückweisungsrate muss weniger als 5-10% aufweisen. Maßnahmen gegen Spoofing (Liveness Detection), beispielsweise Nutzen eines

Fotos statt Gesicht, müssen bei den Geräten vorliegen. Anzumerken ist, dass die Biometrie optional ist, ein PIN muss jedoch immer vergeben werden. Windows Hello funktioniert zudem auch als Authentifizierung für Passkeys und ist zertifiziert für das Sicherheitsprotokoll FIDO2 (Fast Identity Online 2), einen offenen Standard für Online-Multi-Faktor-Authentifizierung (Finnegan, 2021).
Für Unternehmen und Organisationen gibt es eine erweiterte Form namens Windows Hello for Business, welche exklusiv für Azure-Active-Directory und Entra-ID zugeschnitten ist, Microsofts eigenem Domänen- und Verzeichnisdienst. Diese Funktion setzt auf asymmetrische Verschlüsselung mit einer Public-Key Infrastruktur und unterstützt zudem zertifikatbasierte Authentifizierung. Hier wird der private Schlüssel im TPM gesichert. Das Gerät wird im Unternehmen registriert, und die öffentlichen Schlüssel werden ausgetauscht, dem Nutzer zugeordnet und dann zertifiziert. Zudem wird zweistufige Authentifizierung gefordert: neben PIN oder Biometrie wird eine Aufforderung in einer Authentifizierungsapp verlangt. Wird das Gerät gewechselt oder verlangt eine Richtlinie dies, muss erneut nach diesem Prozedere die Identität bestätigt werden (Microsoft, 2024b, Joos, 2025).

## 3.4 Virtuelle Umgebung und Azure Attestation

Azure Attestation ist rein nach der TCG-Spezifikation eine Remote Attestation. Die Fernnachweislösung prüft die Vertrauenswürdigkeit des Systems und kann die Integrität mit Hilfe des TPMs prüfen. Die Attestation (hier CA) nimmt vom IT-System oder einer virtuellen Maschine den Beweis des Gerätezustandes an; dies kann der Hashwert im PCR des TPMs kombiniert mit einem Event-Log beim Booten sein. Die CA hat bestimmte Richtlinien konfiguriert und prüft diese mit dem Hash. Stimmt alles überein, wird das System als vertrauenswürdig authentifiziert, Anwendungen und Kommunikation finden nun in einer gesicherten Umgebung statt (Microsoft, 2025a).
Die Funktion kann so auch auf virtuelle vertrauenswürdige Umgebungen angewendet werden, man spricht auch von virtualiserungsbasierter Sicherheit (VBS). Die VBS nutzt Hardwarevirtualisierung und erschafft eine isolierte Umgebung, die als Root of Trust den Kernel und andere wichtige Prozesse des Betriebssystem vor Schadsoftware schützt (Microsoft, 2024a).

### 3.4.1 Anti-Cheat

Ein Beispiel aus der Remote-Attestation-Funktion lässt sich anhand eines Anti-Cheat-Systems zeigen, einer Funktion, um Betrug und Hacking in Videospielen zu bekämpfen. Anti-Cheats

sind heutzutage im Kernel-Level aktiv und laufen als Treiber, die beim Booten im Hintergrund das System nach auffälligen Prozessen scannen und blockieren sollen. Der Zugang zu Systemressourcen erlaubt, Betrüger auf Hardware-Ebene zu sperren, hat aber so auch potenziell Zugriff auf sensible Informationen. Da sie auf Kernel-Ebene laufen, können sie das System in Performance und Stabilität beeinflussen. Ein positives Merkmal ist die Heuristik, um selbst unbekannte Cheats an bestimmten Mustern erkennen zu können. Jedoch sind sie kein Allheilmittel –- es geht hier mehr um die Steigerung des Aufwands, um überhaupt Cheats zu nutzen. Kernel-Level Anti-Cheats sind umstritten, da der Nutzen und mögliche Eingriffe in die Privatsphäre nicht immer transparent dargelegt werden (von Sydow, 2025).

Eine stärkere Form des Anti-Cheats ist mit mehreren Spezifikationen des TCG möglich. So hat Activision im August 2025 eine Lösung angekündigt, die TPM 2.0, Secure Boot, VBS und Remote Attestation nutzen wird. Dass TPM und Secure Boot benutzt werden, ist bei Anti-Cheat nicht unüblich, die Erweiterungen sollen die Videospiele gegen Angriffe deutlich verhärten. VBS isoliert das Spiel in einer virtuellen Umgebung, wodurch Manipulation stark erschwert wird. Remote Attestation kontrolliert regelmäßig das System, auf dem das Spiel läuft. Entspricht es nicht dem vorgesehenen Standard – zum Beispiel mit veralteten und auffälligen Treibern, die oft für Cheats benutzt werden –, kann der Nutzer einfach ausgesperrt werden (TCG, 2025, Bashir, 2025).
Auch Electronic Arts hat zur selben Zeit in einer Open-Beta eines Spiels ähnliche Funktionen umgesetzt und über 330.000 Manipulationsversuche verhindert. Laut Aussage sind diese Implementierungen „keine Silberne Kugel“, sie helfen aber Daten zu sammeln und Muster zu erkennen, um weitere Maßnahmen ergreifen zu können. Im Wesentlichen möchte man die Anstrengung des Betrugs erhöhen und die Bestrafungen in Form von Sperrungen auf Hardware-Ebene stärker durchsetzen, um eine faire Online-Mehrspieler-Umgebung zu gewährleisten (TCG, 2025, EA-Anticheat-Team, 2025).

## 3.5 Funktionen unter Linux

Obwohl Linux das TPM unterstützt, hat sich der Nutzen nicht als Standard etabliert. TPM bietet aus Linux-Perspektive kein uneingeschränktes und überzeugendes Sicherheitskonzept. Derweil bringt der praktische Einsatz häufig Kompatibilitätsprobleme mit sich. Der Konfigurationsaufwand ist hoch und die Wartbarkeit durch spezielle Firm- und Hardwarezustände lässt das TPM eher als spezialisierter Baustein in der Sicherheit erscheinen (Kumar, 2025).
Entscheidet man sich doch das TPM in Linux-Systemen zu verwenden, so kann auch hier ein Nutzen aus den Sicherheitsfunktionen gezogen werden. Linux-Betriebssysteme gelten durch ihre Open-Source-Beschaffenheit als sicher und transparent, sind fast immer kostenlos, und

ihre Entwicklung ist stark community-getrieben.

Linux gibt es in vielen Versionen und Distributionen. Will man Secure Boot mit Linux kombinieren, weil man beispielsweise Windows 11 und Linux auf einem System laufen haben möchte, gerät man schon mit der Wahl der Distribution in Schwierigkeiten, denn nicht alle Linux-Systeme sind im UEFI signiert. Selbst wenn Linux das einzige Betriebssystem auf dem Computer ist, wird oft empfohlen, Secure Boot zu deaktivieren, um Probleme bei der Installation und Wartung zu umgehen. Hier bieten sich Shims als Lösung für Secure-Boot-Inkompatibilitäten an.
Ein Shim ist ein von Microsoft oder Red Hat signiertes Programm, das im UEFI als Bindeglied zwischen dem Linux-Bootloader und Secure Boot agiert. Secure Boot erkennt das Betriebssystem und erzeugt ein Vertrauensanker. Das Betriebssystem wird von Secure Boot akzeptiert und kann gestartet werden. Bekannte und weit verbreitete Distributionen unterstützen Secure Boot ab Werk, da sie bereits signierte Bootloader und Shims beinhalten, darunter Ubuntu, openSUSE, Red Hat Enterprise Linux und Debian (Kumar, 2025).

Falls man dennoch Secure Boot mit einer Linux-Distribution und Treibern nutzen möchte, die ohne Shim signiert sind, kann man eigene Zertifikate kompilieren, signieren und in Secure Boot implementieren. Man nennt solche Schlüssel Machine Owner Key (MOK). Im Grunde erlaubt Secure Boot auch das Nutzen von MOKs, da es sich um die eigene Maschine handelt. Im Privaten ist das kein Problem, im Unternehmen muss das unter Transparenz stattfinden, da man Secure Boot mit selbst signierten Zertifikaten umgeht. Wenn ein MOK erstellt wird, befinden sich der private und öffentliche Schlüssel auf der Festplatte. Diese sind nur für den Root-User mit den höchsten Privilegien zugelassen (NextDoorNetAdmin, 2025).
Zuerst erzeugt man einen MOK, welcher ein Schlüsselpaar im Verzeichnis `/var/lib/shim-signed/mok/` erzeugt. Der öffentliche Schlüssel des Zertifikats muss dann in Secure Boot importiert werden.

```
update-secureboot-policy --new-key
mokutil --import /var/lib/shim-signed/mok/MOK.der
```

Beim Import wird ein Einmalpasswort erstellt, damit nach einem Neustart der Vorgang verifiziert wird, damit Secure Boot nicht jedes beliebige MOK-Zertifikat annimmt. Die Passworteingabe kann nicht über Fernzugriff erfolgen, da sie in einer Konsole während des Startvorgangs beim MOK-Management eingetragen wird. Mit folgendem Befehl lässt sich prüfen, ob der MOK erfolgreich eingetragen ist:

```
mokutil --test-key /var/lib/shim-signed/mok/MOK.der
```

Nun erlaubt Secure Boot eigene Kernel-Module und nicht mit Shim signierte Treiber. Für private Umgebungen ohne Remote Attestation erlaubt dieser Vorgang das Arbeiten unter Linux Distributionen ohne signierte Shims trotz Secure Boot (NextDoorNetAdmin, 2025).

In der Theorie ließen sich die Schlüssel in ein TPM speichern. Dafür benötigt man das Programm `tpm2-tools` [1] und führt `tpm2_import(1)` aus; die genauen Parameter sind der Dokumentation zu entnehmen. Der Schlüssel muss ein RSA-Schlüsselpaar sein.

Unter Linux gibt es auch Festplattenverschlüsselung mit TPMs. Unter openSUSE Tumbleweed mit YaST2 lässt sich eine Full Disk Encryption einrichten, die sich mit einem TPM 2.0 oder einem FIDO2-Hardwareschlüssel sichern lässt. Mithilfe des TPMs 2.0 lässt sich dazu Measured Boot und Remote Attestation[2] umsetzen. Dieses Projekt ist Open Source und läuft auch auf virtuelle Umgebungen (Kukuk, 2024).

[1] Ubuntu Dokumentation https://manpages.ubuntu.com/manpages/noble/man1/tpm2_import.1.html
[2] Tool: https://keylime.dev/

# 4 Kritiken

Wenn es um komplexe Technik geht, entstehen oft heikle Diskussionen. Werden einem die Rechte oder der Nutzen von Besitz eingeschränkt oder gar entwendet, hat dies Auswirkung auf das Persönlichkeitsrecht. Smartphones und Computer sind Alltagsgeräte und kaum mehr wegzudenken, weshalb Einschnitte in die Nutzbarkeit solcher Geräte vor allem für Techniklaien nicht immer nachvollziehbar sind, unabhängig davon, ob die Technik getestet, transparent und sicher ist. Schon vor Beginn von TCPA und TCG haben die Absichten dieser Konsortien immer scharfe Kritik geerntet. Im Folgenden werden einige Punkte zum TPM und seiner Funktion aufgegriffen und behandelt. In Bezug auf Sicherheitslücken wird nur ein Überblick verschafft.

## 4.1 Grenzen der Technik und Sicherheitslücken

TPMs haben Grenzen in ihrer Technik. Die Implementierung ist komplex und bei Weitem noch nicht verbreitet genug, obwohl seit über zehn Jahren das TPM 2.0 im Umlauf ist. Trotzdem arbeiten Sicherheitsforscher und Technikaffine weiter an Lösungen und versuchen, bestehende Techniken und Sicherheitsstandards zu brechen.

### 4.1.1 bitpixie Exploit um Bitlocker zu entschlüsseln

Der Exploit, welcher den Bug bitpixie (unter *CVE-2023-21563* in der Datenbank des National Institute of Standards and Technology (NIST) zu finden) ausnutzt, ist seit August 2022 von Rairii entdeckt und im Februar 2023 offiziell offengelegt worden (Lambertz, 2025). Thomas Lambertz hat auf dem 38ten Chaos Communication Congress (38C3)[1] und in seinem Blogpost (Lambertz, 2025) offengelegt, wie man sich mit Hilfe von bitpixie heute noch Zugang zu mit Bitlocker verschlüsselten Festplatten verschaffen kann. Der Bug ist mittlerweile behoben, lässt sich aber dennoch unter Bedingungen ausführen. Einige spezielle Kriterien müssen gegeben

[1] Die Durchführung wurde auf dem 38ten Chaos Communication Congress (38C3) präsentiert (https://media.ccc.de/v/38c3-windows-bitlocker-screwed-without-a-screwdriver#l=eng&t=3341)

sein, damit so ein Angriff überhaupt erfolgen kann. Bitlocker muss den automatischen Entsperrmodus aktiviert haben, welcher nur mit dem TPM möglich ist. Das Endgerät muss das Preboot Execution Environment (PXE) zulassen, welches Netzwerk-Startvorgänge erlaubt. Diese Funktion ist oft als Standardeinstellung auf Unternehmensgeräten verfügbar. Dann muss das Gerät mit einem anderen netzwerkfähigem Gerät mit Tastatur verbunden werden. Der stark vereinfachter Ablauf folgt mit A (Angreifer) und B (Ziel):

- B booted in PXE Boot. A dient als der Netzwerk-Server. Es wird per Downgrade ein ungepatcher bitpixie-fähiger Bootmanager ins System geladen, da aktuelle Windows Bootmanager den Bug behoben haben. Alte Bootmanager von Windows sind aber weiterhin signiert und funktionsfähig, daher akzeptieren Secure Boot und TPM diese.
- A verändert die Startreihenfolge auf B so, dass B in eine Wiederherstellungsschleife gerät, wo das TPM Bitlocker entschlüsselt, der Bootvorgang dennoch mit einem Fehler beendet wird. Wenn das System nach fehlgeschlagenem Boot erneut hochfährt, löscht der Bootmanager normalerweise die vom TPM in den Speicher geladenen Schlüssel und startet neu, bei bitpixie passiert das nicht.
- Die Wiederherstellungspartition ist A und wird über PXE Boot erreicht, welche ein Linux Bootloader benutzt, die Shim signiert ist und Secure boot erlaubt. Linux Kernel befindet sich nun im Lockdown. Eine weitere Schwachstelle (CVE-2024-1086 nach NIST) wird ausgenutzt, die A erlaubt, den Lockdown zu umgehen und den Speicher als root auszulesen.
- A kann ein Skript ausführen, um den noch im Speicher befindlichen Bitlockerschlüssel von B zu lesen. Mit dislocker wird die Festplatte von B eingebunden.

Dieser Angriff erfordert Expertise, würde aber mit einem TPM-PIN im Bootvorgang nicht mehr funktionieren, da sich der Bitlocker-Verschlüsselungsschlüssel beim Startvorgang nicht mehr im Speicher befindet. Die automatische Entschlüsselung als Nutzerfreundlichkeit weist hier eine Sicherheitslücke auf, die für fähige Angreifer wie ein entsperrter Computer keine große Barriere darstellt. PXE Boot lässt sich auch im UEFI ausschalten; dabei muss die Netzwerkfähigkeit im Bios deaktiviert werden. Dies würde aber je nach Unternehmensstruktur ein Problem darstellen (Lambertz, 2025).

### 4.1.2 Hardware Zugänge zum TPM

In der Norm kann auf verschlüsselte Laufwerke nur mit einer Entschlüsselung zugegriffen werden. Installiert man eine verschlüsselte Festplatte in ein anderes Gerät, kann man diese nur mit dem richtigen Schlüssel benutzen, unabhängig von TPMs oder anderen Systemen. Wenn ein Endgerät mit Bitlocker verschlüsselt ist und den Schlüssel im TPM speichert, ist

laut Microsoft oder der TCG ein hoher Sicherheitsstandard gegeben. Ist das System im vertrauenswürdigen Zustand, können Computer und TPM kommunizieren. Das TPM entsiegelt den Schlüssel und reicht den Schlüssel an den Prozessor. Das passiert jedoch in Klartext. Wenn man während der Kommunikation genau diese Datenübertragung abhört, erhält man den nötigen Bitlockerschlüssel. In einem Beispielszenario von Stacksmashing (stacksmashing, 2024) gelingt das Abhören über einen Low Pin Count Bus (LPC) auf dem Motherboard des Endgeräts. Dieser hat ein Taktsignal simuliert und so den Datenstrom mit einem Skript übersetzen können. Stacksmashing gelingt es, mit einem Mikrocontroller und Federkontakten ein Werkzeug zu bauen, um schnell und effizient die LPCs auslesen zu können. Was hier trivial klingt, erfordert dennoch Wissen über Schaltkreise und Elektronik, und auch wenn das Tool aufgrund unterschiedlicher Bauweisen nicht auf jedem Endgerät funktioniert, ist die Vorgehensweise ähnlich. Vorbereitet und mit Werkzeug dauert es keine 50 Sekunden, um an den Schlüssel zu gelangen; die Kosten belaufen sich auf ca. $10. Auch könnte man so einen Angriff durch einen alphanumerischen TPM-PIN abwehren. Der Angriff funktioniert nicht auf fTPMs (stacksmashing, 2024).

Ein weiterer Angriff ist auf dTPMs möglich, die über ein Modul auf das Mainboard gesteckt werden können. Sicherheitsforscher Jeremy Boone hat mit TPM Genie[2] einen Interposer gebaut, welcher die Kommunikation zwischen Mainboard und TPM-Modul nach einem Man-in-the-middle-Angriff abhören und manipulieren kann. TPM Genie kann jegliche TPM Spezifikationen untergraben, sei es Measured Boot, Remote Attestation oder RTS. Ein Vorschlag zum Mitigieren eines solchen Angriffes ist, keine steckbaren TPM-Module zu nutzen. Zukünftige Boards sollten die Busse in die inneren Schichten der Platine einbauen und den Chip fest verlöten, so dass solche Angriffe, wenn überhaupt, dann nur mit viel mehr Aufwand durchzuführen sind (Boone, 2018, S.20-21).

### 4.1.3 fTPM Schwächen

Auch fTPMs weisen Sicherheitsprobleme und Schwächen auf. So haben Sicherheitsforscher mit einem Angriff namens TPM-Fail[3] gravierende Schwächen an Chips von STMicroelectronics (Modell ST33TPHF2ESPI) und Intels fTPM vorgeführt. Durch eine Timing-Attacke konnte man den geheimen Schlüssel für den Elliptic Curve Digital Signature Algorithm auslesen und digitale Signaturen fälschen, um TC-Funktionen zu umgehen. Auch wenn Windows solche Schlüssel nicht genutzt hat, konnten andere Programme nicht ausgeschlossen werden. Firmware-Updates wurden von Intel und STMicroelectronics in Form von BIOS- und

[2]Github: https://github.com/nccgroup/TPMGenie
[3]Website: https://tpm.fail/ - Github: https://github.com/VernamLab/TPM-Fail

Softwareupdates bereitgestellt (Windeck, 2019).

Die fTPMs von AMD weisen auch Schwachstellen auf. Forscher konnten nach wenigen Stunden geheime Schlüssel aus dem TPM extrahieren. So war es ihnen möglich versiegelte TPM-Objekte mit Storage Keys aus dem nichtflüchtigen fTPM-Speicher zu entschlüsseln und zuzugreifen. Dieser Angriff namens faulTPM[4] wurde auf Hardware Ebene durchgeführt, obwohl es sich um einen fTPM handelt. Um Zugriff auf AMDs fTPM zu erlangen, wurde mit einem Voltage Fault Injection-Angriff (Seitenkanalangriff) gearbeitet. So konnte eigener Code implementiert und ausgeführt werden. Mit faulTPM wurde eine Bitlockerverschlüsselung ohne PIN-Schutz sofort ausgehebelt. Bei dem Einsatz eines PINs konnte man mit einer Grafikkarte 1000 Pins pro Sekunde per Brute-Force-Angriff testen; dTPMs haben im Gegensatz dazu einen Brute-Force-Schutz. Als Schutz dient hier nur ein alphanumerischer PIN in langer Form. Betroffen sind AMD-Prozessoren der Zen 2 und 3 Reihe (Knop, 2023).

Abgesehen von Sicherheitsproblemen gibt es auch andere Probleme, die ein TPM verursachen kann. So wurden Leistungseinbußen in Windowssystemen unter Windows 10 und 11 mit AMD Prozessoren festgestellt, bei denen das fTPM aktiviert ist. Mitunter gab es in unregelmäßigen Abständen sekundenlange Ruckler, wo das System und Peripherie hakten und die Tonausgabe gestört war. Laut AMD war dies auf das fTPM zurückzuführen, welches auf Speichersysteme auf dem Mainboard zugegriffen hat. Das Problem fiel erst zunehmend durch den TPM 2.0 Zwang auf, den Windows 11 als Mindestvoraussetzung vorschreibt. Lösungen waren die Deaktivierung des fTPMs, was aber nur mit einem dTPM als Ersatz zumindest in Windows 11 funktioniert. Später wurden BIOS Updates ausgerollt, die dieses Problem behoben haben (Mantel, 2022).

## 4.2 Kontrollverlust, Privatsphäre und Digital Rights Management

TPMs und vor allem der Begriff und die Idee des Trusted Computing standen noch vor Zeiten von TCPA und TCG unter kritischem Blick.
Digital Rights Management (DRM) und hardwaregesicherte Umgebungen mit Datenträgern wie CDs, DVDs und Videospielkasetten waren schon in den Neunzigern relevant. Die Medien waren teils verschlüsselt, um den Kopierschutz zu wahren. Die Systembusse von Videospielsystemen waren verschlüsselt, damit sie nicht mit Software zweckentfremdet werden

[4]Github: https://github.com/PSPReverse/ftpm_attack

konnten. Die Idee der Verlagerung von Sicherheit auf die Hardware war kein fremdes Konzept (Hoffmann und Neubauer, 2005, S. 4).
1993 hat die US-Regierung zusammen mit der NSA einen Verschlüsselungschip namens Clipper Chip für Telefonverbindungen konzipiert. Neben der ursprünglichen Idee sollte dieser Chip auch auf jegliche Konsumelektronik ausgerollt werden. Durch Zufall wurde eine sogenannte Backdoor im Verschlüsselungsverfahren entdeckt, die der NSA Zugang verschaffen konnte. Es lagen weitere Versionen vor, doch die Öffentlichkeit hat diesen Chip nicht akzeptiert, und so kam er nicht auf den Markt (Hoffmann und Neubauer, 2005, S. 4).
Schon Mitte der Neunzigerjahre wollte Intel CPUs produzieren, die etwas Ähnliches wie ein TPM integrieren, doch auch hier hat die Öffentlichkeit die Idee abgelehnt. Später wurde Intel Mitglied in der TCPA und ist weiterhin in der TCG als Promoter vertreten. Als es dann mit dem TPM 1.2 in die Produktion ging, wurde dieser in einigen Kreisen Fritz-Chip genannt. Der Name ist durch die Anlehnung an den US Senator Fritz Hollings entstanden, welcher sich für die Umsetzung von DRM-Modulen in jeglicher Unterhaltungselektronik einsetzte (Hoffmann und Neubauer, 2005, S. 4, Eckert, 2023, S. 598).
Der Tonus, dass TPMs in die Freiheit eingreifen und mit Verlust von Kontrolle über Geräte einhergehen, kommt daher nicht unbegründet. Einige der Befürchtungen sind de facto eingetroffen und zugleich auch nicht. Es ist tatsächlich ein TPM 2.0 verpflichtend mit Windows 11 eingetroffen, aber TPMs kann man immer noch ausschalten. Der Einsatz wird nicht für DRM benutzt sondern beispielsweise für Anti-Cheat Mechanismen, wo das Ziel auch eine lebenslange Sperrung von Betrügern sein könnte, was wiederum eine Profilerstellung bedeutet (Hoffmann und Neubauer, 2005, S. 24-25).
Deutschland hat wie China gegen den Standardisierungsvorschlag für das TPM 2.0 gestimmt. Aus technischer Sicht, weil SHA-1 aus Gründen der Kompatibilität als Algorithmus nicht verboten wird, und das TPM 2.0 ab Werk aktiviert ist. Es wird verlangt, diesen ausschalten zu können. Außerdem wird behauptet, ungewollte Updates könnten Systeme blockieren (was tatsächlich passieren kann, siehe Kapitel 4.4). In Bezug auf Vertrauen gibt es die Vermutung, dass „die Erfüllung des Grundrechts auf die Vertraulichkeit und die Integrität informationstechnischer Systeme“ nicht garantiert werden kann, da die TPMs nicht transparent genug sind, als dass man Hintertüren ausschließen kann (Biselli, 2015). Des weiteren gibt es auch Kritik bezüglich des Verfahrens, da die übliche systematische Überprüfung des bestehenden ISO-Standards umgangen wurde. Deutschland sieht die 2.0-Standardisierung als „verfrüht und davon abgesehen nicht empfehlenswert, betrachtet man die Weitgefasstheit dieser Spezifikation und den Mangel an Sicherheitsgarantien“ (Biselli, 2015)

Die Komplexität kommt der TCG und TPM auch nicht zugute. Früher gab es einen Mangel an Fachliteratur für TC, heute ist das Thema noch immer nicht einfach (Müller, 2008, S. 15). Fachliteratur wie Arthur et al., 2015 sind gesponsert (Arthur et al., 2015, S. 331) und eher etwas für die Technik und Dokumentation sauberer Implementierung, aber für die Öffent-

lichkeit schwer nachzuvollziehen. Wenn die Technik immer mehr in den Alltag integriert wird, entsteht hier irgendwann Aufklärungsbedarf.
Der US-amerikanischer Aktivist, Programmierer und Gründer der Freien Software Bewegung (FSF nach Free Software Foundation) hat Trusted Computing immer als „Treacherous Computing“ bezeichnet, wie er in seinem hin und wieder aktualisierenden Blogpost beschreibt (Stallman, n. d.). Einige Befürchtungen sind nicht eingetreten, wie die aktive Umsetzung von DRM, Marktausgrenzungen von Dokumentensystemen (d.h. Word Dokumente sind nur von Word lesbar) oder Verlust an Kontrolle am eigenen System. 2015 sagte Stallman, dass die FSF TPMs nicht gefährlich für Heimcomputer seien, da sie schlichtweg darin versagten, über Remote Attestation ein DRM zu forcieren. Sie seien nur für die Verifizierung des Zustandes eines Computersystems nutzbar. 2022 wird die Aussage zurückgenommen, da TPM 2.0 Remote Attestation unterstützt und technisch DRM umsetzen kann (Stallman, n. d.).

Ein Kritikpunkt gegen Windows 11 ist der Zwang zur Accounterstellung[5]. Die Funktion ist ein zweischneidiges Schwert. Zwar ist der Vorteil eines solchen Accounts die Synchronisation von Diensten und Dateien mit anderen Geräten. Der Nachteil ist die Abhängigkeit von Microsofts Verfügbarkeit. Gibt es Störungen bei den Diensten oder keine Internetverbindung, so sperrt man sich unwillentlich aus. Die herkömmliche lokale Nutzererstellung ist nicht bei der Ersteinrichtung sichtbar, ist aber nachträglich möglich. Im Microsoft-Account können Dienste wie Cloudspeicher oder Videospiele hinterlegt sein – wird der Account gesperrt, so ist aber alles verloren (DMW007, 2024).
Dabei können Sperren willkürlich vorfallen. Nutzende berichten über Besuche der Staatsanwaltschaft, weil Familienfotos mit Kleinkindern ohne Kleidung gefunden wurden. Wenn die Heuristik eines Programms hier Alarm schlägt, es aber keinen Kontext gibt und es strafrechtlich absolut unbedenklich ist, sind solche Fälle stark zu kritisieren. Das kann also zu weiteren Problemen bezüglich Kontrolle und Privatsphäre führen. Zwar gibt es Accountzwänge in Apple und Android Smartphones und deren Ökosysteme; der Autor DMW007 (2024) bewertet das aber als „Pseudo-Argument“. „Wenn alle aus dem Fenster springen, wird es dadurch gut, sodass du es ebenfalls tust?“ drückt eine generelle Ablehnung solch eines Systems aus. Die Abhängigkeit werde über Marketing verschönert und rationalisiert (DMW007, 2024).
Wer seinen Computer in Windows 11 Home mit der Geräteverschlüsselung verschlüsselt, der speichert den Wiederherstellungsschlüssel automatisch im eigenen Microsoft Account. Eine Festplattenverschlüsselung soll vor Zugriff von Fremden schützen. Verlangt aber eine Ermittlungsbehörde solch einen Schlüssel, gibt Microsoft diesen unter Strafverfolgungsbedingung heraus. Nicht jede Anfrage resultiert in einer Herausgabe. Man kann diesen Schlüssel aber auch aus dem Account löschen, also bedarf es hier nur einer Aufklärung (Mossdorf, 2026).

[5]Der Accountzwang kann samt TPM 2.0 Zwang umgangen werden. Es bedarf aber einer hohen technischen Affinität und erfordert regelmäßige Wartung. Es bleibt unklar, wie lange Microsoft diese Praktik billigt.

Wie Müller (2008) schreibt, reicht „die Bandbreite der möglichen Definition für *Trusted Computing* von sehr allgemeinen und somit wenig aussagekräftigen Umschreibungen wie: ‚Eine Technologie um die Sicherheit von Computersystemen zu erhöhen' über kritische Aussagen wie: ‚Eine Technologie um den Benutzern die Kontrolle über ihre Systeme zu entziehen' bis hin zur sehr ehrgeizigen Zielsetzung wie: ‚Eine Technologie für beweisbar sichere Computersysteme'" (Müller, 2008, S. 15)

### 4.2.1 Ausgrenzung von Free Open Source Software

Die Befürchtung, durch das TPM und Secure Boot keine freie Software oder Betriebssysteme nutzen zu können, war immer Gegenstand von Diskussion (Stallman, n. d.). Es ist korrekt, dass Open Source Software in der Theorie durch fehlender Signierung und mangelnde Remote Attestation ausgeschlossen werden kann. Wie in Kapitel 3.5 gesehen, scheint das aber keine böse Absicht der Hersteller zu sein, viel mehr handelt es sich um mangelnde Unterstützung oder Implementierung. Im Vergleich wird manchmal Tivoisierung benutzt. Darunter versteht man den Einsatz von Open Source Software, die auf proprietärer Hardware läuft und daher vom Hersteller signiert werden muss. Der Quellcode ist einsehbar, veränderbar, aber das Gerät verweigert die Ausführung, solange diese nicht signiert ist. Der Name leitet sich von TiVo ab, ein digitaler Videorekorder auf Linux Basis. Dieses Problem hat in der Open Source Community eine Debatte über Freiheit und Kontrolle entfacht (Kotulla, 2022).
Im entfernten Sinne könnte man das Beispiel der Tivoisierung analog auf das Prinzip des TC anwenden.
In einem Blog über Privatsphäre im digitalen Alltag beschreibt Blogger Cruiz, dass es „vor allem in Deutschland kollektive Vorbehalte gegen moderne Techniken wie TPM oder Secure Boot" gibt (Cruiz, 2022). Er beschreibt, wie „Fear, Uncertainty and Doubt (FUD)", also Ängste, Unsicherheit und Zweifel prominent vertreten sind, wenn es um diese Funktionen geht. Er verweist auf die englischen und deutschen Wikipedia Artikel zu Trusted Platform Module und Secure Boot, und hebt hervor, wie FUD hauptsächlich auf der deutschen Plattform zu erkennen ist. Ursache könnten Medienberichte sein, die zu Zeiten der Entstehung der TCG scharfe Kritik geäußert haben. Einige Berichterstatter räumten zumindest ein, dass solche Artikel nicht objektiv, sondern beeinflussend waren (Cruiz, 2022).
Cruiz verweist auf die Wikis einiger Distributionen wie Arch Linux oder Debian, welche TPM und Secure Boot sauber dokumentieren und neutral auf die Funktionen hinweisen, während einige deutsche Anleitungen für Anfänger von Secure Boot abraten. Dies könnte ein Grund für die mangelnde Unterstützung von Linux und diesen Funktionen sein (ein Beispiel guter Unterstützung wurde in Kapitel 3.5 geliefert). Da Bedrohungen sich ständig weiter entwickeln, müssen auch Sicherheitskonzepte nachziehen. Mobile Plattformen haben mit biometrischen Verifizierungen den Weg geebnet, Windows 11 zieht nur nach und gewährt

zugleich Linux, auch davon Vorteile zu ziehen (Cruiz, 2022).
Nicht zu ignorieren sind allerdings auch Komplikation die beispielsweise durch Secure Boot und Shim verursacht werden können.
So können Laptops mit bestimmter Hardware keine proprietären Treiber installieren, da sie nicht durch Secure Boot signiert werden können (Kumar, 2025). Dies könnte in der Theorie mit MOK-Signierungen umgangen werden.
Andere Probleme könnten jedoch gravierender sein, beispielsweise eine kritische Schwachstelle bei Shim (CVE-2023-40547 nach NIST). Angreifer können das Ziel durch Schadcode sowohl lokal als auch aus der Ferne komplett einnehmen. Zwar wurde die Lücke mit einem Sicherheitsupdate behoben, aber man muss darauffolgend noch ein Update für das Secure Boot einspielen, sonst bleibt die Wirkung aus (Stöckel, 2024).

## 4.3 Geplante Obsoleszenz und der Zwang zu Windows 11

Schon im September 2020 war offiziell bekannt, dass es nach dem 14. Oktober 2025 keine Sicherheitsupdates für das Betriebssystem Windows 10 mehr geben würde. Wie auch bei Windows 7 und 8.1 war der Lebenszyklus auf etwa zehn Jahre gesetzt (Tittel, 2021). Die Meldung fand allerdings erst gegen Juni 2021 Beachtung, kurz bevor Microsoft in einem virtuellen Event Windows 11 vorstellte, welches als kostenloses Upgrade für alle lauffähigen Windows 10 Geräte zur Verfügung gestellt werden sollte. Wirklich kommuniziert hat Microsoft das Ende von Windows 10 allerdings erst knapp zwei Jahre später, am 27. April 2023, in einem von ihnen veröffentlichen Windows Client Roadmap Update (Leznek, 2023).
Solange also die Hardware-Anforderungen erfüllt waren, stand einem kostenlosen Upgrade nicht viel im Weg. Für Kompatibilität reichten 4 GB RAM, 64 GB an Festplattenspeicher, und der Prozessor musste größer als 1 GHz Taktung sein und mindestens zwei Kerne besitzen. Die Anforderungen für Prozessoren waren allerdings spezieller als bei anderen Betriebssystemupgrades, denn Prozessoren von Intel mussten mindestens aus der achten Generation sein, sowie Zen 2 (mit einigen Ausnahmen auch Zen+) für die Ableger von AMD. Für Tablet und mobile Geräte mussten mindestens über die CPUs der Serie 7 und 8 von Qualcomm, auch bekannt als Snapdragon, verfügen. 32-Bit Prozessoren fielen komplett aus der Kompatibilität heraus. Generell kann man für die meisten Prozessoren mit Veröffentlichungsdatum von Ende 2017 und Anfang 2018 von den Mindestanforderung ausgehen. Hinzukommt auch der Hardwaresicherheitschip TPM 2.0 als angeforderte Komponente, dieser kann aber auch als fTPM laufen. Microsoft begründet die Anforderung damit, dass die Anforderungen grundlegend für einen neuen Sicherheitsstandard sind, um gegen die erhöhte Menge von Cyberangriffen anzukommen. Laut Microsofts eigenen Bedrohungsaufklärungen sowie zahlreichen Aussagen von Sicherheitsexperten von NSA, UK National Cyber Security Center und Canadian Center

for Cyber Security sei dies schlichtweg notwendig (Microsoft, 2021). Um einen Vergleich zu anderen Betriebssystemupgrades mit Hardwarezwang zu ziehen: FreeBSD hat den Support für den Prozessor i386, einen der ersten 32-bit Prozessoren aus dem Jahre 1985, und weitere 32-Bit-Architekturen nach über 30 Jahren beendet (arindam, 2024).
Für unzählige Geräte weltweit bedeutet dies nun eine Umstellung, deren Ausmaß noch nicht ganz absehbar ist. Laut Verbraucherzentrale laufen in Deutschland allein mehr als 30 Millionen Computer auf Windows 10 (Verbraucherzentrale, 2025), und der Bundesverband der Verbraucherzentrale kritisiert Microsoft zudem, Verbraucher vor die Wahl zu stellen, ob Geld für neue Hardware ausgegeben oder die eigene digitale Sicherheit gefährdet werde. Außerdem seien die Folgen für die Umwelt negativ: Die Produktion neuer Geräte verbrauche nicht nur begrenzt verfügbare Rohstoffe, auch der Elektroschrott werde oftmals nicht korrekt recycelt.

Tabelle 4.1: Steam Betriebssystem Nutzerzahlen aus freiwilligen anonymisierten Umfragen (Valve, 2026b)

| | Februar 2023 | Februar 2024 | Februar 2025 | Februar 2026 |
|---|---|---|---|---|
| Windows 7 | 1,43% | 0,57% | 0,10% | 0,05% |
| Windows 10 | 62,33% | 54,19% | 53,34% | 40,25% |
| Windows 11 | 32,06% | 41,96% | 44,10% | 56,28% |
| OSX (Mac) | 2,37% | 1,32% | 0,97% | 1,16% |
| Linux | 1.27% | 1,76% | 1,45% | 2,23% |

In Abbildung 4.1 sind die Betriebssystem-Zahlen von Nutzern aus der Spieleplattform Steam, die zu Valve gehört, sichtbar. Daten aus vorherigen Jahren sind aus dem Internetarchiv, da die Zahlen aus der Quelle immer aktuell gehalten werden. Aus den vorliegenden Daten zusammen mit den aktiven Nutzerzahlen von ungefähr 40 Million täglichen Nutzer (Valve, 2026a, täglich aktualisiert) lässt sich ein Trend erkennen: Einige Nutzer steigen auf Linux um, aber der erhebliche Anstieg bei Windows 11 zeigt auch, dass viele zum Ende des Support von Windows 10 doch eher das Upgrade vornehmen. Interessant ist hier auch zu beobachten, dass immer noch bis zu 95% bei Windows bleiben - trotz möglicher Kritik. Man muss allerdings beachten, dass es sich bei dieser Stichprobe um eine spezifische Nutzergruppe handelt. Es ist auch nicht ersichtlich, welchen Anteil unter Linux das eigene auf Arch Linux basierendes Betriebssystem vom Steam Deck, der von Valve selbst vertriebene Handheld, hat. Gemessen an den Microsoft-Daten, die auf ungefähr 1,4 Milliarden aktive Endgeräte (Mehdi, 2025) hinweisen, und Valves eigenen Angaben auf aktive Nutzer lässt sich ein eher langsamer bis schon stagnierenden Wechsel zu anderen Betriebssystem außer Windows erkennen (Callegari, 2026).

Über Statcounter, ein Web-Analyse-Tool über Besucherverhalten auf Websites, zeigen Windows-Versionen in Tabelle 4.2 vorerst einen langsamen, ab 2025 jedoch starken Wechsel von Windows 10 zu Windows 11 an. Leider können Zahlen für alle Betriebssysteme in Statcounter nicht zuverlässig angezeigt werden, da Analysedaten des Apple-Betriebssystems seit 2025 nicht mehr korrekt aufgenommen werden; daher wäre ein Vergleich nicht aussagekräftig.

Tabelle 4.2: Anteil der Desktop-Windows-Versionen weltweit Februar 2023 – Februar 2026 (Statcounter, 2026b)

| | Februar 2023 | Februar 2024 | Februar 2025 | Februar 2026 |
|---|---|---|---|---|
| Windows 10 | 73,31% | 67,26% | 58,70% | 26,45% |
| Windows 11 | 19,13% | 28,16% | 38,13% | 72,57% |
| Windows 7 | 5,34% | 3,10% | 2,30% | 0,62% |
| Andere Windows | 2,12% | 1,39% | 0,81% | 0,34% |

Microsoft hat mittlerweile eine Übergangslösung für erweiterte Sicherheitsupdates für Windows 10 in die Wege geleitet, und je nach Standort variieren diese. Im europäischen Raum erhalten Konsumenten ein kostenloses Jahr, vorausgesetzt es wird ein Microsoft-Account mit dem Computer verknüpft. Verzichtet man auf ein Konto und arbeitet nur mit einem lokalen Account, so muss man das Äquivalent zu $30 in der eigenen Währung zahlen. Dies gilt laut heutigem Stand nur bis Oktober 2026. Für Unternehmen gilt eine preisliche Staffelung, die sich jährlich verdoppelt und sich bis Oktober 2028 zieht (Microsoft, 2026b).
Nicht zu vernachlässigen sind auch die Trade-In Programme oder auch Leitlinien zum Recyclen für Altgeräte, die Microsoft selbst anbietet oder zumindest auf verantwortliche Standorten verweist (Microsoft, 2026a).
Ob man hier nun von geplanter Obsoleszenz sprechen kann, lässt sich anhand der dargelegten Lösungen nicht ganz klar definieren. Dass es sich hier aber um Hardwarezwang handelt, lässt sich nicht ausschließen, vorausgesetzt man kann sich die Alternativen nicht leisten. Die Probleme hinauszuzögern, mag zwar Zeit verschaffen, wird aber irgendwann doch zu Handlungsdruck führen. Dies verursacht nicht nur Druck für Entwickler, die ihre Programme auf neue Systeme portieren müssen. Auch Anwender werden dadurch höhere Kosten tragen müssen. Die wirtschaftliche Situation betrifft besonders die Technik durch die AI-Branche, welche große Mengen an Speicher benötigen (Eilhard, 2026).

## 4.4 Alternativlosigkeit durch Benutzerfreundlichkeit

24 August, 1995 - das ist das Jahr, in dem Windows 95 veröffentlicht wurde. Das Betriebssystem brillierte nicht durch Sicherheit oder Stabilität, sondern durch Benutzerfreundlichkeit. Es war simpel und intuitiv genug, um darin zu arbeiten und zu spielen, und auch die Kompatibilität zum ersten Betriebssystem MS-DOS (Microsoft Disk Operating System) war vorhanden. Es gab noch nicht einmal einen Webbrowser, und doch war die Idee des digitalen Schreibtisches - heute als Desktop bekannt - überzeugend und einfach (CHIP, 2020).
Doch das Design des Betriebssystems war keineswegs neu. Bill Gates selbst hat offen bekundet, die Idee käme von der grafischen Benutzeroberfläche von Computern des kalifornischen Forschungsinstituts Xerox PARC, heute nur als PARC bekannt. Im ersten Jahr verkaufte Microsoft über 60 Millionen Heimcomputer, 2005 war ihr Marktanteil mit 200 Millionen Geräten bei 95%, erreichte dann 2011 den Höhepunkt mit 365 Millionen Systemen. Smartphones und Tablets haben dann den Markt dominiert, wobei Microsoft zumindest im Smartphone-Bereich keinen Anschluss fand (CHIP, 2020).

Das Zwangsupgrade zu Windows 11 und die strikten Hardwareanforderungen verursachten zwar Diskussionen und ernteten Kritik, dennoch gibt es zumindest im Bereich der Videospiele keine großen Anzeichen eines Betriebssystemwechsels. Viele Spiele funktionieren nicht auf Linux, zumindest nicht ohne einen gewissen Aufwand. Über Proton, ein von Valve entwickeltes Kompatibilitätsprogramm, lassen sich viele Spiele, die auf Steam vertrieben werden und nur auf Windows funktionieren, spielen - allerdings nicht bei großen Titeln mit wettbewerbsfähiger Mehrspieler-Funktion. Genau diese Spiele belegen eine große Anzahl gleichzeitiger und wiederkehrender Spieler. Anti-Cheat ist eine große Barriere für Linux, und so sehen Videospiel-Publisher keinen Grund, für Linux zu entwickeln. Die Gewinnmarge wäre einfach nicht groß genug, daher bleiben Unterstützung und Entwicklung aus. Der Hardwarezwang für Windows 11 ist nicht störend genug für Videospieler. Eine gewohnte Plattform zu verlassen ist, in Kombination mit der Unsicherheit hinsichtlich Kompatibilität, eine nicht zu unterschätzende Barriere für einen Wechsel, weshalb der große Umschwung auf Linux zumindest für Gamer noch ausbleibt (Callegari, 2026).

Benutzerfreundlichkeit kann auch ihre Tücken haben. Gibt es keine Transparenz oder Anleitung, die genauso benutzerfreundlich ist, kann das beim privaten Betrieb mitunter zu Problemen führen.
In den Windows-Updates für Version 11 (24H2 und 25H2) und 10 (22H2) hat ein Update für bestimmte Computer eine Bitlocker-Sperre (Geräteverschlüsselung) zur Folge. Wer also in Windows 11 Home einen Account nutzt und gar nichts von den automatisierten Vorgängen weiß, muss nun einen Entsperrcode eingeben, von den er noch nie etwas gehört hat. Dieser

Vorgang ist vergleichbar mit Hardware-Veränderung, bei der das TPM einen unberechtigten Zustand erkennt (siehe 3.2) (Fuhrmann, 2025).
Microsoft verspricht einen neuen Sicherheitsstandard für Heimcomputer mit Windows 11 (Microsoft, 2021). Beachtet man aber die möglichen Sicherheitslücken (vgl. 4.1.1) und deren Mitigation (TPM-PIN), ist dieses Versprechen nicht so einfach einzuhalten.
Um einen TPM-PIN zu erstellen, muss man die Gruppenrichtlinien des Computers bearbeiten. Die Schritte hierfür sind keineswegs benutzerfreundlich, zumindest ist das kein Vergleich zur automatischen Geräteverschlüsselung. In Unternehmensnetzwerken lässt sich dies mit Richtlinien erzwingen, was vorteilhaft ist. Als Privatnutzer wird man sich eher für automatische Entsperrungen entscheiden. Dass man sich hier in falscher Sicherheit wiegt, ist nicht auszuschließen, aber irgendein Schutz ist immer noch vorteilhafter als gar kein Schutz (Sommergut, 2023).

# 5 Fazit

Zusammenfassend zeigt sich, dass das Trusted Platform Module 2.0 einen vielversprechenden Beitrag zur hardwaregestützten Cyber-Sicherheit leisten kann.
Insbesondere die gesonderte Speicherung kryptografischer Schlüssel, die Integritätsprüfung von IT-Systemen und ihrer Zustände, sowie die Unterstützung in der Cyber-Sicherheit relevanter Funktionen wie Secure Boot, Bitlocker und Remote Attestation verdeutlichen den praktischen Nutzen des Moduls.
Gleichzeitig verdeutlicht die Arbeit, dass TPM 2.0 kein universelles Sicherheitskonzept darstellt. Sicherheitslücken, Implementierungsdefizite, datenschutzrechtliche Herausforderungen sowie eine Abhängigkeit von herstellerspezifischen, plattformgebundenen und nutzungsabhängigen Faktoren schränken seine Rolle als allgemeine Vertrauensinstanz ein.
Während der Einsatz im Unternehmensumfeld aufgrund standardisierter Verwaltungs- und Sicherheitsstrukturen als effektiv eingeschätzt werden kann, offenbart sich im Privatbereich nur eine begrenzte Wirksamkeit technischer Schutzmechanismen bei fehlender Transparenz, unzureichender Benutzerfreundlichkeit und mangelnder Aufklärungsmaßnahmen. Die zunehmende Relevanz von TPM 2.0 aus sicherheitstechnischer Perspektive ist insofern nachvollziehbar, seine verpflichtende Implementierung im Konsumentenbereich lediglich nur bedingt gerechtfertigt.
Ob Microsofts Entscheidung wirtschaftlich motiviert ist oder einem technischen Modernisierungsbedarf aufgrund von Kompatibilitätsaspekten folgt, bleibt mangels offizieller Stellungnahme offen. Der gewählte Zeitpunkt dieses Vorgehens kann daher aus strategischer Perspektive als zumindest diskussionswürdig betrachtet werden.

# Literatur


Aorimn. (2026, 8. Januar). *dislocker*. https://github.com/Aorimn/dislocker (Letzter Zugriff: 20.03.2026).

Apple. (2024, 19. Dezember). *Secure Enclave*. https://support.apple.com/de-de/guide/security/sec59b0b31ff/web (Letzter Zugriff: 16.03.2026).

arindam. (2024, 13. Februar). *FreeBSD Announces End of Support for 32-bit Platforms in Future Releases*. https://debugpointnews.com/freebsd-32-bit-support-ending/ (Letzter Zugriff: 10.03.2026).

Arthur, W., et al. (2015). *A practical Guide to TPM 2.0* (1. Aufl.). Apress.

Bashir, S. (2025, 17. November). *Anti-Cheat am PC: Microsoft will mehr als nur TPM 2.0 und Secure Boot*. https://www.igorslab.de/en/anti-cheat-am-pc-microsoft-will-mehr-als-nur-tpm-2-0-und-secure-boot/ (Letzter Zugriff: 20.03.2026).

Biselli, A. (2015, 9. März). *Wir leaken: Deutschland und China gegen den Rest der Welt – Wundersame Einigkeit bei Trusted Computing*. https://netzpolitik.org/2015/wir-leaken-deutschland-und-china-gegen-den-rest-der-welt-wundersame-einigkeit-bei-trusted-computing/ (Letzter Zugriff: 13.03.2026).

Boone, J. (2018, 9. März). *TPM Genie: Interposer Attacks Against the Trusted Platform Module Serial Bus*. https://github.com/nccgroup/TPMGenie/blob/master/docs/NCC_Group_Jeremy_Boone_TPM_Genie_Whitepaper.pdf (Letzter Zugriff: 23.03.2026).

BSI. (2026, 1. Januar). *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=9 (Seite 25; Letzter Zugriff: 16.03.2026).

Callegari, A. (2026, 3. März). *Linux Gaming Hits a Wall: Steam's February 2026 Survey Reveals a Platform at a Crossroads*. https://www.webpronews.com/linux-gaming-hits-a-wall-steams-february-2026-survey-reveals-a-platform-at-a-crossroads/ (Letzter Zugriff: 26.03.2026).

CHIP. (2020, 24. August). *Mit einem großen Fehler: Wie Windows 95 vor 25 Jahren den PC-Boom auslöste*. https://www.chip.de/news/Wie-Windows-95-vor-25-Jahren-den-PC-Boom-ausloeste_182923647.html (Letzter Zugriff: 26.03.2026).

Cruiz. (2022, 8. Februar). *Kollektive Vorbehalte gegen TPM und Secure Boot – Ängste, Unsicherheit und Zweifel*. https://curius.de/2022/02/kollektive-vorbehalte-gegen-tpm-und-secure-

boot-aengste-unsicherheit-und-zweifel/ (Zuletzt bearbeitet: 30.09.2023; Letzter Zugriff: 23.03.2026).

DMW007. (2024, 24. August). *So gefährlich sind Microsoft-Konten in Windows*. https://u-labs.de/portal/so-gefahrlich-sind-microsoft-konten-in-windows/ (Letzter Zugriff: 26.03.2026).

EA-Anticheat-Team. (2025, 8. August). *[UPDATE] Battlefield 6 Update: On Secure Boot and Cheats*. https://forums.ea.com/discussions/battlefield-6-general-discussion-en/update-battlefield-6-update-on-secure-boot--cheats/12439803 (Letzter Zugriff: 20.03.2026).

Eckert, C. (2023). *IT-Sicherheit: Konzepte - Verfahren - Protokolle* (11. Aufl.). De Gruyter Oldenbourg.

Eilhard, H. (2026, 4. Februar). *Preise werden sich 2026 verdoppeln! Experten warnen Technik-Käufer*. https://www.inside-digital.de/news/preise-werden-sich-2026-verdoppeln-experten-warnen-technik-kaeufer (Letzter Zugriff: 26.03.2026).

Feng, D., et al. (2018). *Trusted Computing* (2. Aufl.). De Gruyter.

Finnegan, M. (2021, 6. September). *Was ist Windows Hello?* https://www.computerwoche.de/article/2806422/was-ist-windows-hello.html (Letzter Zugriff: 20.03.2026).

Fraunhofer-SIT. (2026). *Software-Plattform für TPM 2.0 - Mehr Sicherheit für Automotive IT*. https://www.sit.fraunhofer.de/de/angebote/projekte/sicherheit-fuer-automotive-it/ (Letzter Zugriff: 16.03.2026).

Fritz, M., et al. (2016). *Windows 10 Pro : Das umfassende Handbuch* (2. Aufl.). Rheinwerk Verlag.

Fuhrmann, M. (2025, 6. November). *Bitlocker sperrt plötzlich Windows-Nutzer aus: So bekommt ihr wieder Zugriff auf euren PC*. https://t3n.de/news/bitlocker-sperrt-windows-nutzer-aus-wieder-zugriff-auf-pc-bekommen-1715481/ (Letzter Zugriff: 23.03.2026).

Hoffmann, J., & Neubauer, J. (2005). *Trusted Computing - Proseminar SS05 - IT-Sicherheit*. https://eldorado.tu-dortmund.de/server/api/core/bitstreams/d3fbfae1-7a06-4f2b-8366-384d95a6b282/content (Letzter Zugriff: 16.03.2026).

Holger. (2025, 6. Juni). *Cybersicherheits-Tutorial: Unterschiede zwischen TPM, fTPM und dTPM*. https://mundobytes.com/de/Unterschiede-zwischen-tpm--ftpm-und-dtpm/ (Letzter Zugriff: 16.03.2026).

Joos, T. (2025, 7. Januar). *Biometrische Anmeldung an Windows, Ressourcen und Cloud - Windows Hello for Business konfigurieren*. https://www.security-insider.de/windows-hello-for-business-anleitung-und-vorteile-a-614098894736bd80619677b53c5f2050/ (Letzter Zugriff: 20.03.2026).

Knop, D. (2023, 3. Mai). *Firmware-TPM: faulTPM knackt AMD-CPUs nach drei Stunden lokalem Zugriff*. https://www.heise.de/news/faulTPM-Angriff-auf-AMDs-Firmware-TPM-etwa-zum-Knacken-von-Bitlocker-8985704.html (Letzter Zugriff: 23.03.2026).

Kotulla, A. (2022, 22. April). *Tivoisierung: Wann ist Software wirklich frei?* https://bitsea.de/blog/2022/04/tivoisierung-wann-ist-software-wirklich-frei/ (Letzter Zugriff: 23.03.2026).

Kukuk, T. (2024, 20. September). *Quickstart in Full Disk Encryption with TPM and YaST2*. https://news.opensuse.org/2024/09/20/quickstart-fde-yast2/ (Letzter Zugriff: 23.03.2026).

Kumar, A. (2025, 26. Juni). *Linux Jargon Buster: What are Secure Boot and Shim Files?* https://itsfoss.com/secure-boot-shim-file/ (Letzter Zugriff: 23.03.2026).

Lambertz, T. (2025, 17. Januar). *Windows BitLocker – Screwed without a Screwdriver*. https://neodyme.io/en/blog/bitlocker_screwed_without_a_screwdriver/#teaser (Letzter Zugriff: 23.03.2026).

Leznek, J. (2023, 27. April). *Windows client roadmap update: April 2023*. https://techcommunity.microsoft.com/blog/windows-itpro-blog/windows-client-roadmap-update-april-2023/3805227 (Letzter Zugriff: 10.03.2026).

Mantel, M. (2022, 8. März). *Ryzen-Prozessoren mit Windows: AMD bestätigt Ruckelprobleme*. https://www.heise.de/news/Ryzen-Prozessoren-mit-Windows-11-AMD-bestaetigt-fTPM-bedingte-Ruckler-6542097.html (Letzter Zugriff: 23.03.2026).

Mehdi, Y. (2025, 24. Juni). *Stay secure with Windows 11, Copilot+ PCs and Windows 365 before support ends for Windows 10*. https://blogs.windows.com/windowsexperience/2025/06/24/stay-secure-with-windows-11-copilot-pcs-and-windows-365-before-support-ends-for-win (Letzter Zugriff: 10.03.2026).

Microsoft. (2021, 27. August). *Update on Windows 11 minimum system requirements and the PC Health Check app*. https://blogs.windows.com/windows-insider/2021/08/27/update-on-windows-11-minimum-system-requirements-and-the-pc-health-check-app/ (Letzter Zugriff: 10.03.2026).

Microsoft. (2024a, 6. Juni). *Virtualisierungsbasierte Sicherheit (VBS)*. https://learn.microsoft.com/de-de/windows-hardware/design/device-experiences/oem-vbs (Letzter Zugriff: 20.03.2026).

Microsoft. (2024b, 22. November). *Windows Hello for Business*. https://learn.microsoft.com/de-de/windows/security/identity-protection/hello-for-business/ (Letzter Zugriff: 20.03.2026).

Microsoft. (2025a, 23. April). *Microsoft Azure Attestation*. https://learn.microsoft.com/de-de/azure/attestation/overview (Letzter Zugriff: 20.03.2026).

Microsoft. (2025b, 26. Juni). *Zertifikatupdates für den sicheren Start: Leitfaden für IT-Experten und Organisationen*. https://support.microsoft.com/de-de/topic/zertifikatupdates-f%C3%BCr-den-sicheren-start-leitfaden-f%C3%BCr-it-experten-und-organisationen-e2b43f9f-b424-42df-bc6a-8476db65ab2f (Letzter Zugriff: 16.03.2026).

Microsoft. (2025c, 29. Juli). *Bitlocker-Übersicht*. https://learn.microsoft.com/de-de/windows/security/operating-system-security/data-protection/bitlocker/ (Letzter Zugriff: 16.03.2026).

Microsoft. (2025d, 18. August). *Secure the Windows boot process*. https://learn.microsoft.com/en-us/windows/security/operating-system-security/system-security/secure-the-windows-10-boot-process (Letzter Zugriff: 25.03.2026).

Microsoft. (2026a). *End-of-life management and recycling*. https://www.microsoft.com/en-us/legal/compliance/recycling (Letzter Zugriff: 10.03.2026).

Microsoft. (2026b). *Erweiterte Sicherheitsupdates (ESU) für Windows 10*. https://www.microsoft.com/de-de/windows/extended-security-updates (Letzter Zugriff: 10.03.2026).

Microsoft. (2026c). *Windows Hello*. https://www.microsoft.com/de-de/windows/tips/windows-hello (Letzter Zugriff: 20.03.2026).

Mossdorf, K.-S. (2026, 25. Januar). *BitLocker: Microsoft gibt Schlüssel an Strafverfolger heraus*. https://www.heise.de/news/Microsoft-gibt-BitLocker-Schluessel-an-Strafverfolgungsbehoerden-11152988.html (Letzter Zugriff: 23.03.2026).

Müller, T. (2008). *Trusted Computing Systeme* (1. Aufl.). Springer Berlin.

NextDoorNetAdmin. (2025, 3. März). *Enrolling a MOK: making Linux work with Secure Boot [Video]. Youtube*. https://www.youtube.com/watch?v=O_aqPJ72p3E (Letzter Zugriff: 23.03.2026).

Pohlmann, N. (2020, 18. März). *Trusted Computing - Vorlesung Cyber-Sicherheit*. https://norbert-pohlmann.com/wp-content/uploads/2019/08/Trusted-Computing-Vorlesung-Cyber-Sicherheit-Prof-Norbert-Pohlmann-18_03_20.pdf (Letzter Zugriff: 13.03.2026).

Pohlmann, N. (2022). *Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung* (2. Aufl.). Springer Fachmedien Wiesbaden GmbH.

Sommergut, W. (2023, 7. Juli). *PIN für BitLocker einrichten*. https://www.windowspro.de/wolfgang-sommergut/bitlocker-key-pin-absichern (Letzter Zugriff: 23.03.2026).

stacksmashing. (2024, 3. Februar). *Breaking Bitlocker - Bypassing the Windows Disk Encryption [Video]. Youtube*. https://www.youtube.com/watch?v=wTl4vEednkQ (Letzter Zugriff: 23.03.2026).

Stallman, R. (n. d.). *Can You Trust Your Computer?* https://www.gnu.org/philosophy/can-you-trust.html.en (Letzter Zugriff: 23.03.2026).

Statcounter. (2026a). *Desktop Operating System Market Share Worldwide Feb 2026*. https://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-202602-202602-bar (Letzter Zugriff: 25.03.2026).

Statcounter. (2026b). *Desktop Windows Version Market Share Worldwide Feb 2023 - Feb 2026*. https://gs.statcounter.com/windows-version-market-share/desktop/worldwide/#monthly-202302-202602 (Letzter Zugriff: 10.03.2026).

Stöckel, M. (2024, 7. Februar). *Kritische Schwachstelle gefährdet Secure Boot unter Linux*. https://www.golem.de/news/shim-kritische-schwachstelle-gefaehrdet-secure-boot-unter-linux-2402-181956.html (Letzter Zugriff: 23.03.2026).

TCG. (2025, 30. September). *Using a TPM to bolster anti-cheat measures in gaming*. https://trustedcomputinggroup.org/using-a-tpm-to-bolster-anti-cheat-measures-in-gaming/ (Letzter Zugriff: 20.03.2026).

TCG. (2026a). *TPM 1.2 Main Specification*. https://trustedcomputinggroup.org/resource/tpm-main-specification/ (Letzter Zugriff: 13.03.2026).

TCG. (2026b). *TPM 2.0 Library*. https://trustedcomputinggroup.org/resource/tpm-library-specification/ (Letzter Zugriff: 13.03.2026).

TCG. (2026c). *Trusted Computing Group*. https://www.trustedcomputinggroup.org (Letzter Zugriff: 13.03.2026).

Tittel, E. (2021, 14. Juni). *Windows 10 Retirement Date is 2025*. https://www.edtittel.com/blog/windows-10-retirement-date-is-2025.html (Letzter Zugriff: 10.03.2026).

UEFI-Forum. (2026). *Unified Extensible Firmware Interface Forum*. https://uefi.org/ (Letzter Zugriff: 13.03.2026).

Valve. (2026a, 10. März). *Übersicht der Statistiken*. https://store.steampowered.com/charts/ (Letzter Zugriff: 10.03.2026).

Valve. (2026b, 11. März). *Steam-Hard- und Softwareumfrage: February 2026*. https://web.archive.org/web/20260304185722/https://store.steampowered.com/hwsurvey/ (Letzter Zugriff: 11.03.2026).

Verbraucherzentrale. (2025, 15. Dezember). *Support für Windows 10 endet: Das müssen Sie wissen*. https://www.verbraucherzentrale.de/wissen/digitale-welt/apps-und-software/support-fuer-windows-10-endet-das-muessen-sie-wissen-105980 (Letzter Zugriff: 10.03.2026).

von Sydow, E. (2025, 11. September). *Was sind Kernel-Level-Anti-Cheats und wie funktionieren sie? Alle Infos*. https://praxistipps.chip.de/was-sind-kernel-level-anti-cheats-und-wie-funktionieren-sie-alle-infos_190159 (Letzter Zugriff: 20.03.2026).

Windeck, C. (2019, 14. November). *Angriffe auf Trusted Platform Modules von Intel und STMicroelectronics*. https://www.heise.de/news/Angriffe-auf-Trusted-Platform-Modules-von-Intel-und-STMicroelectronics-4585573.html (Letzter Zugriff: 23.03.2026).

Windows, D. (2024, 15. August). *Zufallsgeneratoren in der modernen Sicherheitstechnologie von Windows: Ein Blick auf Windows Hello*. https://www.drwindows.de/news/zufallsgeneratoren-in-der-modernen-sicherheitstechnologie-von-windows-ein-blick-auf-windows-hello (Letzter Zugriff: 16.03.2026).

# Eigenständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Bachelorarbeit mit dem Titel

**Trusted Platform Module (TPM) 2.0 in Cyber-Sicherheit, Anwendung und Kritik**

selbstständig und nur mit den angegebenen Hilfsmitteln verfasst habe. Alle Passagen, die ich wörtlich aus der Literatur oder aus anderen Quellen wie z. B. Internetseiten übernommen habe, habe ich deutlich als Zitat mit Angabe der Quelle kenntlich gemacht.

Hamburg, 30. März 2026