(19) Deutsches Patent- und Markenamt

(10) **DE 102 54 621 B4** 2013.09.19

(12) # Patentschrift

(21) Aktenzeichen: **102 54 621.5**
(22) Anmeldetag: **22.11.2002**
(43) Offenlegungstag: **12.06.2003**
(45) Veröffentlichungstag der Patenterteilung: **19.09.2013**

(51) Int Cl.: ***G06F 9/445*** (2006.01)

Innerhalb von drei Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(30) Unionspriorität:
01279785 **22.11.2001** **GB**

(73) Patentinhaber:
Hewlett-Packard Development Co., L.P., Houston, Tex., US

(74) Vertreter:
Schoppe, Zimmermann, Stöckeler, Zinkler & Partner, 82049, Pullach, DE

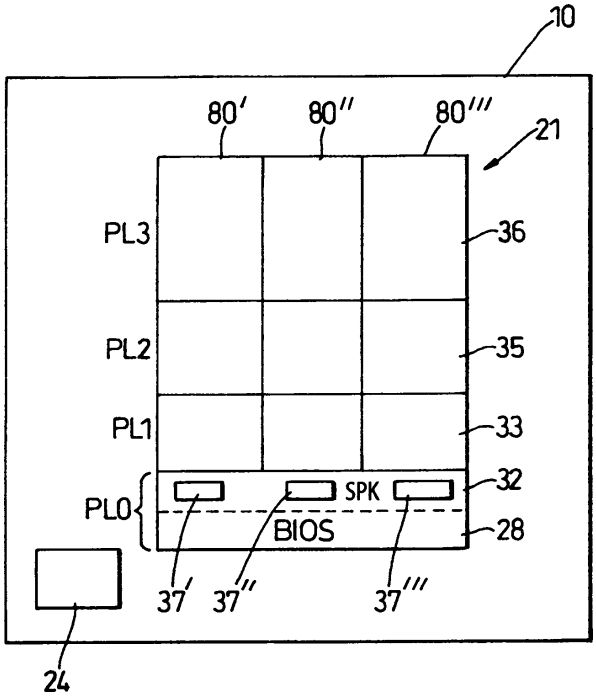
(72) Erfinder:
Proudler, Graeme John, Bristol, GB; Balacheff, Boris, Bristol, GB; Worley, John S., Fort Collins, Col., US; Hyser, Chris D., Fort Collins, Col., US; Worley jr., William S., Denver, Col., US

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

US	6 185 678	B1
US	6 263 431	B1
US	6 009 518	A
WO	01/ 27 722	A1
WO	01/ 63 415	A2
JP	2000- 215 065	A

(54) Bezeichnung: **Computervorrichtung, Verfahren und Computersystem zum Erzeugen einer vertrauenswürdigen Umgebung**

(57) Hauptanspruch: Computervorrichtung zum Erzeugen einer vertrauenswürdigen Umgebung, mit folgenden Merkmalen:
einer physischen, vertrauenswürdigen Einrichtung (24), die angeordnet ist, um ein erstes Integritätsmaß zu erwerben, um eine Bestimmung darüber zu ermöglichen, ob die Computervorrichtung auf eine vertrauenswürdige Weise arbeitet,
einem Prozessor (21) und einem Programmcode, der auf dem Prozessor ausführbar ist, um mehrere Betriebsumgebungen (80', 80'', 80''') einzurichten, von denen jede ihre eigene jeweilig zugeordnete virtuelle vertrauenswürdige Einrichtung (37', 37'', 37''') aufweist, und
einer Einrichtung zum Sicherstellen, dass der Zugriff der Betriebsumgebungen (80', 80'', 80''') auf die Ressourcen eingeschränkt ist, die für die jeweilig zugeordnete virtuelle vertrauenswürdige Einrichtung (37', 37'', 37''') verfügbar sind,
wobei jede virtuelle vertrauenswürdige Einrichtung (37', 37'', 37''') angeordnet ist, um sowohl das erste Integritätsmaß als auch ein zweites Integritätsmaß zu erwerben, wobei das zweite Integritätsmaß eine Bestimmung darüber ermöglicht, ob die Betriebsumgebung, die dieser virtuellen vertrauenswürdigen Einrichtung (37', 37'', 37''') zugeordnet ist, auf eine vertrauenswürdige Weise arbeitet.



Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf eine Computervorrichtung, ein Verfahren und ein Computersystem zum Erzeugen einer vertrauenswürdigen Umgebung.

[0002] Computerplattformen, die für handelsübliche Anwendungen verwendet werden, arbeiten üblicherweise in einer Umgebung, in der ihr Verhalten anfällig für eine Modifikation durch lokale oder entfernte Entitäten ist.

[0003] Zusätzlich dazu, in Anbetracht der andauernden Steigerung der Computerleistung wurde es immer üblicher für Computerplattformen, mehrere Benutzer zu unterstützen, wobei jeder Benutzer seine eigene Betriebsumgebung aufweisen kann, die auf der Computerplattform installiert ist.

[0004] Die Betriebssystemsoftware läuft üblicherweise auf der Systemprivilegebene eines Prozessors, wobei die Systemprivilegebene den individuellen Betriebssystemen ermöglicht, sowohl privilegierte als auch nicht-privilegierte Befehle zu verwenden, die durch die Prozessorhardware bereitgestellt werden. Als solches, wo eine Anzahl von separaten Betriebssystemen gleichzeitig auf einer Computerplattform läuft, verwenden die Betriebssysteme das Gesamtsystemprivileg gemeinschaftlich und sind nicht notwendigerweise voneinander isoliert oder geschützt. Das Volumen des Quellcodes für Softwarekomponenten, die ein Gesamtsystemprivileg gemeinschaftlich verwenden, ist üblicherweise bei modernen Betriebssystemen so groß, daß es praktisch unmöglich ist, die Richtigkeit des Quellcodes und ob das Verhalten des Quellcodes sich wie erwartet verhält, sicherzustellen.

[0005] Dementsprechend ist diese potentielle Unsicherheit der Plattform eine Einschränkung für dessen Verwendung durch Parteien, die anderweitig bereit wären, die Plattform zu verwenden.

[0006] Erhöhen des Pegels an Vertrauen bei Plattformen ermöglicht daher ein größeres Benutzerzutrauen (confidence), daß sich die Plattform- und die Betriebssystem-Umgebung auf eine bekannte Weise verhalten.

[0007] Die WO01/27722A1 bezieht sich beispielsweise auf eine Operation eines vertrauenswürdigen Zustands in einer Computerplattform. Eine Computerentität umfasst eine vertrauenswürdige Überwachungskomponente mit einer ersten Verarbeitungseinrichtung und einer ersten Speichereinrichtung, wobei die vertrauenswürdige Überwachungskomponente eine eigenständige, autonome Datenverarbeitungseinheit aufweist, und eine Computerplattform mit einer Hauptverarbeitungseinrichtung und einem Hauptspeicherbereich, zusammen mit einer Mehrzahl von zugeordneten physikalischen und logischen Ressourcen, wie zum Beispiel peripheren Geräten einschließlich Druckern, Modems, Anwendungsprogrammen, Betriebssystemen und dergleichen. Die Computerplattform ist in der Lage, in eine Mehrzahl von unterschiedlichen Betriebszuständen einzutreten, wobei jeder Betriebszustand eine unterschiedliche Sicherheits- und Vertrauenswürdigkeitsebene aufweist. Ausgewählte Zustände weisen vertrauenswürdige Zustände auf, bei denen ein Benutzer sensitive vertrauliche Informationen mit einem hohen Maß an Sicherheit eingeben kann, dass die Computerplattform nicht durch äußere Einflüsse, wie zum Beispiel Viren, Hacker oder feindliche Attacken in Mitleidenschaft gezogen worden ist. Um in einen vertrauenswürdigen Zustand einzutreten, werden Bezugnahmen automatisch auf die vertrauenswürdige Komponente gemacht, wobei zum Verlassen eines vertrauenswürdigen Zustands eine Referenz zu der vertrauenswürdigen Komponente hergestellt werden muss. Beim Verlassen des vertrauenswürdigen Zustands werden alle Referenzen zu dem vertrauenswürdigen Zustand aus der Computerplattform gelöscht. Beim Eintreten in den vertrauenswürdigen Zustand wird in den Zustand auf eine reproduzierbare und bekannte Art und Weise mit einer reproduzierbaren bekannten Konfiguration, die durch die vertrauenswürdige Komponente bestätigt wird, eingetreten.

[0008] Die US 6,185,678 B1 bezieht sich auf eine Architektur zum Initialisieren eines Computersystems. Diese Architektur soll die Sicherheit des Boot-Prozesses erhöhen, indem die Integrität eines Bootstrap-Codes (Bootstrap = Vorladen) sichergestellt wird. Dies soll erreicht werden, indem eine Kette von Integritätsüberprüfungen aufgebaut wird, beginnend beim Einschalten und solange fortgesetzt, bis der abschließende Transfer der Steuerung von den Bottstrap-Komponenten zu dem Betriebssystem selbst stattgefunden hat. Die Integritätsüberprüfungen vergleichen einen berechneten kryptographischen Hash-Wert mit einer gespeicherten digitalen Signatur, die jeder Komponente zugeordnet ist. Dies wird mittels Modifikationen und Hinzufügungen zu dem BIOS erreicht. Die Architektur umfasst ferner einen Wiederherstellungsmechanismus zum Reparieren von Integritätsfehlern, wodurch ein Schutz gegenüber einigen Klassen von Dienstverweigerungen (Ablehnungen) und Modifikationen an Komponenten erreicht werden soll. Bei dem Bootprozess wird entweder der Betriebssystemkern gestartet oder es wird in einen Wiederherstellungsprozess eingetreten, um jeglichen erfassten Integritätsfehler zu reparieren. Sobald die Reparatur abgeschlossen ist, wird das System erneut gestartet, um sicherzustellen, dass das System bootet. Dieser gesamte Prozess findet ohne einen Benutzereingriff statt.

[0009] Es ist die Aufgabe der vorliegenden Erfindung, eine Computervorrichtung, ein Verfahren und ein Computersystem zum Erzeugen einer vertrauenswürdigen Umgebung zu schaffen.

[0010] Diese Aufgabe wird durch eine Computervorrichtung gemäß Anspruch 1, ein Verfahren gemäß Anspruch 17 und ein Computersystem gemäß Anspruch 21 gelöst.

[0011] Gemäß einem ersten Aspekt der vorliegenden Erfindung wird eine Computervorrichtung zum Erzeugen einer vertrauenswürdigen Umgebung geschaffen, die eine vertrauenswürdige Einrichtung, die angeordnet ist, um ein erstes Integritätsmaß zu erwerben, um eine Bestimmung zu ermöglichen, ob die Computervorrichtung auf eine vertrauenswürdige Weise arbeitet, einen Prozessor, der angeordnet ist, um die Ausführung einer ersten Vertrauensroutine zu ermöglichen und der einer ersten Betriebsumgebung zugeordnet ist, und eine Einrichtung zum Einschränken des Zugriffs der ersten Betriebsumgebung auf Ressourcen, die für die Vertrauensroutine verfügbar sind aufweist, wobei die Vertrauensroutine angeordnet ist, um das erste Integritätsmaß und ein zweites Integritätsmaß zu erwerben, um eine Bestimmung zu ermöglichen, ob die erste Betriebsumgebung auf eine vertrauenswürdige Weise arbeitet.

[0012] Gemäß einem zweiten Aspekt der Erfindung wird eine Computervorrichtung zum Erzeugen einer vertrauenswürdigen Umgebung geschaffen, die eine vertrauenswürdige Einrichtung, die angeordnet ist, um ein erstes Integritätsmaß zu erwerben, um eine Bestimmung zu ermöglichen, ob die Computervorrichtung auf eine vertrauenswürdige Weise arbeitet, und einen Prozessor aufweist, der angeordnet ist, um die Ausführung einer ersten Vertrauensroutine und einer zugeordneten ersten Betriebsumgebung zu ermöglichen, wobei der Prozessor angeordnet ist, um den Zugriff der ersten Betriebsumgebung auf Ressourcen einzuschränken, die für die Vertrauensroutine verfügbar sind, wobei die Vertrauensroutine angeordnet ist, um das erste Integritätsmaß und ein zweites Integritätsmaß zu erwerben, um eine Bestimmung zu ermöglichen, ob die erste Betriebsumgebung auf eine vertrauenswürdige Weise arbeitet.

[0013] Gemäß einem dritten Aspekt der vorliegenden Erfindung wird eine Computervorrichtung zum Erzeugen einer vertrauenswürdigen Umgebung geschaffen, die eine vertrauenswürdige Einrichtung, die angeordnet ist, um ein erstes Integritätsmaß zu erwerben, um eine Bestimmung zu ermöglichen, ob die Computervorrichtung auf eine vertrauenswürdige Weise arbeitet, und einen Prozessor aufweist, der angeordnet ist, um die Ausführung einer ersten Vertrauensroutine in einer ersten Privilegebene des Prozessors zu ermöglichen und um die Ausführung einer zugeordneten ersten Betriebsumgebung in einer zweiten Privilegebene des Prozessors zu ermöglichen, derart, daß ein Zugriff auf Ressourcen, die für einen Code verfügbar sind, der in der ersten Privilegebene ausgeführt wird, auf einen Code beschränkt ist, der in der zweiten Privilegebene ausgeführt wird, wobei die Vertrauensroutine angeordnet ist, um das erste Integritätsmaß und ein zweites Integritätsmaß zu erwerben, um eine Bestimmung zu ermöglichen, ob die erste Betriebsumgebung auf eine vertrauenswürdige Weise arbeitet.

[0014] Vorzugsweise ist die vertrauenswürdige Einrichtung eine fälschungsresistente Einrichtung.

[0015] Vorzugsweise ist der Prozessor angeordnet, um die Ausführung einer Mehrzahl von Vertrauensroutinen in der ersten Privilegebene zu ermöglichen und um die Ausführung jeweiliger zugeordneter Betriebsumgebungen in der zweiten Privilegebene zu ermöglichen; wobei jede Vertrauensroutine angeordnet ist, um das erste Integritätsmaß und ein Integritätsmaß, das der jeweiligen zugeordneten Betriebsumgebung zugeordnet ist zu erwerben, um eine Bestimmung zu ermöglichen, ob die jeweilige Betriebsumgebung auf eine vertrauenswürdige Weise arbeitet.

[0016] Vorzugsweise ist die Vertrauensroutine angeordnet, um eine kryptographische Funktionalität zum Einschränken des Zugriffs auf Daten einzulagern, die der Vertrauensroutine zugeordnet sind.

[0017] Vorzugsweise ist die vertrauenswürdige Einrichtung angeordnet, um eines oder mehrere Geheimnisse zu speichern.

[0018] Geeigneterweise sind der Vertrauensroutine eines oder mehrere Geheimnisse zugeordnet.

[0019] Am geeignetsten ist zumindest ein Geheimnis ein privater, asymmetrischer Verschlüsselungsschlüssel.

[0020] Vorzugsweise ist die vertrauenswürdige Einrichtung angeordnet, um beim Abschalten der Computervorrichtung Geheimnisse zu speichern, die durch eine Vertrauensroutine verwendet werden.

[0021] Vorzugsweise weist der Code, der in der zweiten Privilegebene ausgeführt wird, einen begrenzten Zugriff auf Daten auf, die einer Vertrauensroutine zugeordnet sind, die in der ersten Privilegebene ausgeführt wird.

[0022] Vorzugsweise sind alle Daten, die dem Vertrauensmodul zugeordnet sind, vor einer Änderung von dem Code geschützt, der in der Privilegebene 2 ausgeführt wird.

[0023] Vorzugsweise sind Geheimnisse, die einem Vertrauensmodul zugeordnet sind, für einen Code nicht zugreifbar, der in der Privilegebene 2 ausgeführt wird.

[0024] Geeigneterweise bürgt die vertrauenswürdige Einrichtung für einen öffentlichen Schlüssel, der dem Vertrauensmodul zugeordnet ist, unter Verwendung eines privaten Schlüssels der vertrauenswürdigen Einrichtung.

[0025] Geeigneterweise bürgt eine vertrauenswürdige dritte Partei für einen öffentlichen Schlüssel, der dem Vertrauensmodul zugeordnet ist, unter Verwendung eines privaten Schlüssels der vertrauenswürdigen Parteien.

[0026] Vorzugsweise ist die vertrauenswürdige Einrichtung angeordnet, um Bootsequenzbefehle zu übertragen, um eine Initiierung des Bootens der Computervorrichtung zu ermöglichen.

[0027] Vorzugsweise ist der Prozessor angeordnet, um zu verursachen, daß die Bootsequenzbefehle die ersten Befehle sind, die durch den Prozessor nach der Freigabe von der Rücksetzung (reset) ausgeführt werden.

[0028] Gemäß einem vierten Aspekt der vorliegenden Erfindung wird ein Verfahren zum Erzeugen einer vertrauenswürdigen Umgebung geschaffen, das das Erwerben eines ersten Integritätsmaßes, um eine Bestimmung zu ermöglichen, ob eine Computervorrichtung auf eine vertrauenswürdige Weise arbeitet und das Ausführen einer ersten Vertrauensroutine in einer ersten Privilegebene eines Prozessors und das Ausführen einer zugeordneten ersten Betriebsumgebung in einer zweiten Privilegebene des Prozessors, das Einschränken des Zugriffs auf Ressourcen, die für einen Code verfügbar sind, der in der ersten Privilegebene ausgeführt wird, von einem Code, der in der zweiten Privilegebene ausgeführt wird, das Erwerben des ersten Integritätsmaßes und eines zweiten Integritätsmaßes, um eine Bestimmung zu ermöglichen, ob die erste Betriebsumgebung auf eine vertrauenswürdige Weise arbeitet, aufweist.

[0029] Gemäß einem fünften Aspekt der vorliegenden Erfindung wird ein Verfahren zum Erzeugen einer vertrauenswürdigen Umgebung geschaffen, das das Erwerben eines ersten Integritätsmaßes, um eine Bestimmung zu ermöglichen, ob eine Computervorrichtung auf eine vertrauenswürdige Weise arbeitet, das Ausführen einer ersten Vertrauensroutine und einer zugeordneten ersten Betriebsumgebung, das Einschränken des Zugriffs der ersten Betriebsumgebung auf Ressourcen, die für die Vertrauensroutine verfügbar sind, und das Anordnen der Vertrauensroutine, um das erste Integritätsmaß und ein zweites Integritätsmaß zu erwerben, um eine Bestimmung zu ermöglichen, ob die erste Betriebsumgebung auf eine vertrauenswürdige Weise arbeitet, aufweist.

[0030] Gemäß einem sechsten Aspekt der vorliegenden Erfindung wird ein Verfahren zum Erzeugen einer vertrauenswürdigen Umgebung geschaffen, das das Erwerben eines ersten Integritätsmaßes, um eine Bestimmung zu ermöglichen, ob eine Computervorrichtung auf eine vertrauenswürdige Weise arbeitet und das Ausführen einer ersten Vertrauensroutine und einer zugeordneten ersten Betriebsumgebung, das Beschränken des Zugriffs der ersten Betriebsumgebung auf Ressourcen, die für die Vertrauensroutine verfügbar sind, das Erwerben des ersten Integritätsmaßes und eines zweiten Integritätsmaßes, um eine Bestimmung zu ermöglichen, ob di erste Betriebsumgebung auf eine vertrauenswürdige Weise arbeitet, aufweist.

[0031] Gemäß einem siebten Aspekt der vorliegenden Erfindung wird ein Computersystem zum Erzeugen einer vertrauenswürdigen Umgebung geschaffen, das eine vertrauenswürdige Einrichtung, die angeordnet ist, um ein erstes Integritätsmaß zu erwerben, um eine Bestimmung zu ermöglichen, ob die Computervorrichtung auf eine vertrauenswürdige Weise arbeitet, einen Prozessor, der angeordnet ist, um die Ausführung einer ersten Vertrauensroutine und einer zugeordneten ersten Betriebsumgebung zu ermöglichen, und eine Einrichtung zum Einschränken des Zugriffs der ersten Betriebsumgebung auf Ressourcen, die für die Vertrauensroutine verfügbar sind, aufweist, wobei die Vertrauensroutine angeordnet ist, um das erste Integritätsmaß und ein zweites Integritätsmaß zu erwerben, um eine Bestimmung zu ermöglichen, ob die erste Betriebsumgebung auf eine vertrauenswürdige Weise arbeitet.

[0032] Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend Bezug nehmend auf die beiliegenden Zeichnungen näher erläutert. Es zeigen:

[0033] Fig. 1 ein System, das in der Lage ist, Ausführungsbeispiele der vorliegenden Erfindung zu implementieren;

[0034] Fig. 2 eine Hauptplatine, die eine vertrauenswürdige Einrichtung umfaßt;

[0035] Fig. 3 Privilegebenen eines Prozessors;

[0036] Fig. 4 die vertrauenswürdige Einrichtung detaillierter;

[0037] Fig. 5 die Schritte, die beim Erwerben eines Integritätsmaßes der Rechenvorrichtung umfaßt sind;

[0038] Fig. 6 ein System, das in der Lage ist, Ausführungsbeispiele der vorliegenden Erfindung zu implementieren;

[0039] Fig. 7 eine virtuelle vertrauenswürdige Einrichtung;

[0040] Fig. 8 ein Ausführungsbeispiel der vorliegenden Erfindung.

[0041] Das vorliegende Ausführungsbeispiel liefert die Einlagerung einer physischen, vertrauenswürdigen Einrichtung und einer Softwarevertrauensroutine (d. h. einer virtuellen, vertrauenswürdigen Einrichtung) in eine Rechenplattform. Die Funktion der tatsächlichen vertrauenswürdigen Einrichtung ist es, die Identität der Plattform an zuverlässig gemessene Daten zu binden, die ein Integritätsmaß der Plattform liefern, während die virtuelle vertrauenswürdige Einrichtung die Identität einer zugeordneten Softwarebetriebsumgebung (z. B. eines Betriebssystems) an zuverlässig gemessene Daten bindet, die ein Integritätsmaß der Betriebsumgebung liefern. Die Identitäten und die Integritätsmaße werden mit erwarteten Werten verglichen, die durch eine vertrauenswürdige Partei (TP = trusted party) geliefert werden, die vorbereitet ist, um für die Vertrauenswürdigkeit der Plattform zu bürgen. Optional werden die erwarteten Werte, die durch die vertrauenswürdige dritte Partei geliefert werden, sicher in der jeweiligen tatsächlichen vertrauenswürdigen Einrichtung und der virtuellen vertrauenswürdigen Einrichtung gespeichert. Falls eine Übereinstimmung besteht, ist die Folgerung, daß zumindest ein Teil der Plattform und des Betriebssystem korrekt arbeitet, abhängig von dem Umfang des Integritätsmaßes.

[0042] Ein Benutzer verifiziert die korrekte Operation der Plattform und der Betriebsumgebung vor dem Austauschen anderer Daten mit der Plattform. Ein Benutzer tut dies durch Anfordern der Identitäten und Integritätsmaße der tatsächlichen vertrauenswürdigen Einrichtung und der virtuellen vertrauenswürdigen Einrichtung. (Optional lehnen die vertrauenswürdigen Einrichtungen ab, einen Nachweis der Identität zu liefern, falls dieselbe selbst nicht in der Lage war, eine korrekte Operation der Plattform zu verifizieren.) Der Benutzer empfängt den Beweis der Identität und des Identitätsmaßes und vergleicht dieselben mit den Werten, die durch die vertrauenswürdige dritte Partei geliefert werden. Wenn die gemessenen Daten, die durch die vertrauenswürdigen Einrichtungen berichtet werden, die gleichen wie die sind, die durch die vertrauenswürdige dritte Partei geliefert wurden, kann der Benutzer der Plattform vertrauen.

[0043] Zusätzlich dazu, wenn die Computerplattform angeordnet ist, um eine Mehrzahl von separaten Betriebsumgebungen zu unterstützen, wobei jede Betriebsumgebung ihre eigene jeweilige virtuelle vertrauenswürdige Einrichtung aufweist, können die Benutzer der jeweiligen Betriebsumgebungen darauf vertrauen, daß ihre Betriebsumgebung von einer anderen Betriebsumgebung isoliert ist, die auf der Computerplattform läuft.

[0044] Sobald ein Benutzer eine vertrauenswürdige Operation der Plattform und der Betriebsumgebung eingerichtet hat, tauscht er andere Daten mit der Plattform aus. Für einen lokalen Benutzer könnte der Austausch durch eine Wechselwirkung mit einer bestimmten Softwareanwendung erfolgen, die innerhalb der Betriebsumgebung auf der Plattform läuft. Für einen entfernten Benutzer könnte der Austausch eine sichere Transaktion umfassen. In jedem Fall werden die Daten üblicherweise durch eine der vertrauenswürdigen Einrichtungen „unterzeichnet" ausgetauscht. Der Benutzer kann dann ein größeres Zutrauen haben, daß Daten mit einer Plattform ausgetauscht werden, deren Verhalten vertrauenswürdig ist.

[0045] Die vertrauenswürdigen Einrichtungen verwenden kryptographische Prozesse, liefern jedoch nicht notwendigerweise eine externe Schnittstelle für diese kryptographischen Prozesse.

[0046] Um sicherzustellen, daß ein minimales Risiko besteht, daß die virtuelle vertrauenswürdige Einrichtung anfällig für eine Softwareattacke durch eine bösartige Software ist, die auf der Computerplattform läuft, ist die virtuelle vertrauenswürdige Einrichtung angeordnet, um in einer Prozessorprivilegebene ausgeführt zu werden, die den Zugriff auf andere Softwareanwendungen einschränkt, die auf der Computerplattform ausgeführt werden (wie nachfolgend beschrieben wird). Zusätzlich dazu werden Geheimnisse, die der virtuellen vertrauenswürdigen Einrichtung zugeordnet sind, derart gespeichert, daß die Geheimnisse für Softwareanwendungen nicht zugreifbar sind, die in einer Prozessorprivilegebene ausgeführt werden, die niedriger ist als die, in der die virtuelle vertrauenswürdige Einrichtung ausgeführt wird. Ferner wäre es eine äußerst wünschenswerte Implementierung, die tatsächliche vertrauenswürdige Einrichtung fälschungssicher zu machen, um Geheimnisse dadurch zu schützen, daß dieselben für andere Plattformfunktionen nicht zugreifbar sind, und eine Umgebung zu liefern, die im wesentlichen immun gegen eine nicht autorisierte Modifikation ist. Da eine Fälschungssicherung unmöglich ist, ist die beste Annäherung eine vertrauenswürdige Einrichtung, die fälschungsresistent oder fälschungserfassend ist. Die vertrauenswürdige Einrichtung besteht daher vorzugsweise aus einer physikalischen Komponente, die fälschungsresistent ist.

[0047] Techniken, die für Fälschungsresistenz relevant sind, sind Fachleuten auf dem Gebiet der Sicherheit bekannt. Diese Techniken umfassen Verfahren

für eine Fälschungsresistenz (wie z. B. eine angemessene Einkapselung der vertrauenswürdigen Einrichtung), Verfahren zum Erfassen einer Fälschung (wie z. B. der Erfassung aus Spezifikationsspannungen, Röntgenstrahlen oder einem Verlust an physikalischer Integrität in dem Gehäuse der vertrauenswürdigen Einrichtung), und Verfahren zum Eliminieren von Daten, wenn eine Fälschung erfaßt wird.

[0048] Eine vertrauenswürdige Plattform **10** ist in dem Diagramm in Fig. 1 dargestellt. Die Plattform **10** umfaßt die Standardmerkmale einer Tastatur **14**, einer Maus **16** und einer visuellen Anzeigeeinheit (VDU = visual display unit) **18**, die die tatsächliche „Benutzerschnittstelle" der Plattform liefern. Bei der Plattform **10** besteht eine Mehrzahl von Modulen **15**: dies sind andere Funktionselemente der vertrauenswürdigen Plattform von im wesentlichen einer Art, die angemessen für diese Plattform ist (die funktionelle Bedeutung derartiger Elemente ist für die vorliegende Erfindung nicht relevant und wird daher hierin nicht weiter erörtert).

[0049] Wie in Fig. 2 dargestellt ist, umfaßt die Hauptplatine **20** der vertrauenswürdigen Rechenplattform **10** (unter anderen Standardkomponenten) einen Hauptprozessor **21** mit einem internen Speicher **25**, einem Hauptspeicher **22**, einer vertrauenswürdigen Einrichtung **24**, einem Datenbus **26** und jeweiligen Steuerleitungen **27** und Leitungen **27-1**, einem BIOS-Speicher **29**, der das BIOS-Programm **28** für die Plattform **10** enthält und eine Eingabe-/Ausgabe-Einrichtung (I/O) **23**, die die Wechselwirkung zwischen den Komponenten der Hauptplatine, der Tastatur **14**, der Maus **16** und der VDU **18** steuert.

[0050] Der Hauptspeicher **22** ist üblicherweise ein Direktzugriffsspeicher (RAM = random access memory).

[0051] Bei diesem Ausführungsbeispiel weist der Prozessor **21** vier Ausführprivilegebenen PL0, PL1, PL2, PL3 auf. Beispiele derartiger Prozessoren sind der PA-RISC-Prozessor von Hewlett-Packard oder der IA-64-Prozessor von Intel, es können jedoch auch andere Prozessorkonfigurationen mit einer Mehrzahl von Privilegebenen verwendet werden.

[0052] In dem Prozessor **21** läuft eine sichere Plattformarchitektur (SPA) **31**, wie in Fig. 3 gezeigt ist.

[0053] Die SPA **31** umfaßt ein BIOS-Programm oder eine Firmware **28**, die auf dem Prozessor **21** auf der Ausführprivilegebene 0 (PL0) läuft, die privilegierteste Ebene des Prozessors **21**. Die SPA **31** umfaßt einen Vierschicht-Softwarering, der auf der BIOS-Firmware **28** in dem Prozessor **21** läuft.

[0054] Der innerste Softwarering, der auf der BIOS-Firmware **28** läuft, wird als der sichere Plattformkernel (SPK) **32** bezeichnet und ist der einzige Softwarering, der eine privilegierte Aufgabe abspielt. Der SPK **32** läuft auf PL0 und bildet die Fundamentschicht der SPA **31** und ist die einzige Ringschicht, die auf privilegierte Systemregister zugreift und privilegierte Befehle ausführt.

[0055] Ein sicheres Plattform-Global-Dienstemodul (SPGS) **33** läuft auf dem SPK **32** als eine unprivilegierte Aufgabe. Das SPGS **33** läuft auf der Ausführprivilegebene 1 (PL1), der zweitprivilegierten Ebene des Prozessors **21**. Der SPK **32** und das SPGS **33** werden kollektiv als die sichere Plattform (SP) **34** bezeichnet.

[0056] Zumindest ein Betriebssystembild **35** läuft auf dem SPGS **33** als eine unprivilegierte Aufgabe. Das Betriebssystembild **35** läuft auf der Ausführprivilegebene 2 (PL2), der drittprivilegierten Ebene des Prozessors **31**. Endbenutzeranwendungen **36** laufen auf dem/den Betriebssystembild/ern **35** als unprivilegierte Aufgaben. Endbenutzeranwendungen **36** laufen auf der Ausführprivilegebene 3 (PL3), der viertprivilegierten Ebene (d. h. der am wenigsten privilegierten Ebene) des Prozessors **21**.

[0057] Der SPK **32** ist vorzugsweise ein kleiner Kernel mit einem vertrauenswürdigen, beweisbar korrekten Code, der sicherheitskritische Dienste ausführt, wobei die geringe Größe zu der Sicherheit und der Korrektheit des SPK beiträgt. Beispiele von sicherheitskritischen Diensten umfassen Speicher- und Prozeß-Verwaltung, Fallen- und Interrupt-Handhabung und kryptographische Dienste, wobei einige dieser Sicherheitsdienste über eine virtuelle Vertrauenseinrichtung durchgeführt werden können, wie nachfolgend beschrieben wird. Das SPGS **33** ist mit einem vertrauenswürdigen Code aufgebaut, verwendet aber Hardwaresicherheitsfähigkeiten der Prozessoren **21**, wie z. B. der IA-64-Prozessoren, um die Auswirkung eines Fehlers zu minimieren. Das SPGS **33** läuft als eine unprivilegierte Aufgabe und verwendet den SPK **32**, um privilegierte Operationen auszuführen.

[0058] Zusätzlich dazu umfaßt der SPK **32** einen Code, um die Ausführung von einer oder mehreren virtuellen vertrauenswürdigen Einrichtungen **37** innerhalb des SPK **32** zu ermöglichen. Die eine oder mehreren virtuellen vertrauenswürdigen Einrichtungen **37** sind einer Betriebsumgebung zugeordnet, die in PL2 und PL3 ausgeführt wird, und ermöglichen es einem Benutzer, einzurichten, ob die zugeordnete Betriebsumgebung vertrauenswürdig ist, wie nachfolgend beschrieben wird. Es ist jedoch nicht wesentlich für den Code der virtuellen vertrauenswürdigen Einrichtung, innerhalb des SPK-Codes eingelagert zu sein, der Code kann anderswo gehäust sein, z. B. in der vertrauenswürdigen Einrichtung **24**.

[0059] Um sicherzustellen, daß der virtuellen vertrauenswürdigen Einrichtung **37** vertraut werden kann, ist es für den Hersteller des SPK-Codes wünschenswert, durch eine vertrauenswürdige dritte Partei validiert zu werden. Bei der Validierung wird ein Validierungszeugnis, das mit dem privaten Schlüssel der vertrauenswürdigen dritten Parteien signiert ist, dem SPK-Code zugeordnet.

[0060] Das SPGS **33** umfaßt üblicherweise alle Dienste, die nicht in dem SPK **32** umfaßt sein müssen. Ein Grund dafür, daß die sichere Plattform **34** in SPK **32** und SPGS **33** aufgespalten wird ist es, zu ermöglichen, daß der SPK **32** klein, stabil und verifizierbar ist.

[0061] Schnittstellen zwischen der BIOS-Firmware **28** und der Prozessorhardware **21** umfassen eine privilegierte Binäranwendungsschnittstelle (ABI = application binary interface) und eine nicht-privilegierte ABI. Die Schnittstellen zwischen dem SPK **32** und der BIOS-Firmware **28** umfassen eine privilegierte ABI, eine nicht-privilegierte ABI und eine Prozessorabstraktionsschicht (PAL = processor abstraction layer)/Systemabstraktionsschicht (SAL = system abstraction layer)/erweiterbare Firmwareschnittstelle (EFI)-Schnittstellen. Die Schnittstellen zwischen dem SPGS **33** und dem SPK **32** umfassen eine sichere Plattformschnittstelle (SPI = secure platform interface) und eine nicht-privilegierte ABI. Die Schnittstellen zwischen den Betriebssystembildern **35** und dem SPGS **33** umfassen eine SPI, eine Globaldienste-schnittstelle (GSI = global services interface) und eine nicht-privilegierte ABI. Die Schnittstellen zwischen Endbenutzeranwendungen **36** und Betriebssystembildern **35** umfassen eine Anwendungsprogrammschnittstelle (EPI) und eine nicht-privilegierte ABI.

[0062] Das SPGS **33** kann die Betriebssystembildschicht **35** in mehrere unabhängige Schutzdomänen partitionieren, die auf der PL2 arbeiten. Eine Schutzdomäne wird hierin als eine Softwarepartition und eine zugeordnete Sammlung von Systemressourcen, wie z. B. Speicher, I/O, Prozessoren und ähnliches bezeichnet, die durch das SPGS **33** zum Zweck des Ladens und Ausführens eines einzelnen Betriebssystembildes **35** erzeugt werden. Jede der mehreren unabhängigen Schutzdomänen ist in der Lage, ein Betriebssystembild **35** oder ein anderes Programm, das in der Lage ist, betrieben zu werden, urzuladen und auszuführen, nur unter Verwendung der SPK **32** – und der SPGS **33** – Dienste, wie z. B. eines spezialisierten Anwendungssteuerungsprogramms.

[0063] Die mehreren unabhängigen Schutzdomänen, die auf der PL2 laufen, werden voneinander durch die Speicherschutzfähigkeiten der Vierprivilegebenen-Prozessorhardware **21** geschützt, wie z. B. die Prozessorschutzfähigkeiten des Prozessors IA-64. Daher hat ein Ausfall in einer der unabhängigen Schutzdomänen üblicherweise keine Auswirkung auf die anderen unabhängigen Schutzdomänen, sogar wenn der Ausfall ein Betriebssystemzusammenbruch ist. Die unabhängigen Schutzdomänen liefern die Fähigkeit, die Systemverwendung auf einer Feinkornbasis zu verwalten, während die Sicherheit beibehalten wird. Betriebssystembilder **35** werden zur sicheren Plattform **34** der SPA **31** getragen, ähnlich dazu, wie Betriebssysteme zu einer neuen Hardwareplattform-Industriestandardarchitektur ISA in der klassischen Architektur für Betriebssysteme portiert (getragen) werden.

[0064] Endbenutzeranwendungen **36** laufen auf der am wenigsten privilegierten Ebene, PL3, als unprivilegierte Aufgaben unter der Steuerung eines Betriebssystembildes **35** in einer Schutzdomäne einer sicheren Plattform **34**. Üblicherweise, von der Perspektive der Endbenutzeranwendung aus, arbeitet die Endbenutzeranwendung **36** unter der Steuerung eines Betriebssystembildes **35**, da die Endbenutzeranwendung unter der Steuerung eines Betriebssystems in der klassischen Architektur für Betriebssysteme laufen würde.

[0065] Damit die Computerplattform **10** und die Betriebsumgebung(en) vertrauenswürdig sind, wird eine Vertrauenskette von der Systemhardware über den Bootprozeß bis zu einem abschließenden laufenden Code eingerichtet. Zusätzlich dazu wird der gesamte Softwarecode vorzugsweise authentifiziert, bevor derselbe ausführt wird, und ein ordnungsgemäß authentifiziertes Codestück ist vorzugsweise unänderbar, außer durch eine ähnlich vertrauenswürdige Komponente, um die Vertrauenskette beizubehalten. Die Softwareauthentifizierung sollte mehr sein als eine einfache Prüfsumme oder ein anderes schmiedbares Schema. Somit verwendet die SPA **31** vorzugsweise eine starke Authentifizierung unter Verwendung kryptographischer Verfahren, wie z. B. der Öffentlicher-Schlüssel-Verschlüsselung, derart, daß Software nur unerfaßbar fehlerhaft sein kann, wenn ein privater Schlüssel bekannt ist.

[0066] Die Vertrauenskette erstreckt sich zurück zu der vertrauenswürdigen Einrichtung **24**. Wie nachfolgend beschrieben wird, wird der Prozessor **21** nach dem Zurücksetzen des Systems zuerst durch die vertrauenswürdige Einrichtung **24** gesteuert, die dann nach dem Durchführen eines sicheren Bootprozesses die Steuerung an die BIOS-Firmware **28** übergibt. Während des sicheren Bootprozesses erwirbt die vertrauenswürdige Einrichtung **24** ein Integritätsmaß von der Computerplattform **10**, wie nachfolgend beschrieben wird.

[0067] Genauer gesagt weist die vertrauenswürdige Einrichtung **24**, wie in Fig. 4 gezeigt ist, folgende Merkmale auf: eine Steuerung **40**, die programmiert ist, um die Gesamtoperation der vertrauens-

würdigen Einrichtung **24** zu steuern und mit den anderen Funktionen auf der vertrauenswürdigen Einrichtung **24** und mit den anderen Einrichtungen auf der Hauptplatine **20** zu interagieren; eine Meßfunktion **41** zum Erwerben des Integritätsmaßes von der Plattform **10**; eine kryptographische Funktion **42** zum Signieren, Verschlüsseln oder Entschlüsseln spezifizierter Daten; eine Authentifizierungsfunktion **43** und eine Schnittstellenschaltungsanordnung **44**, die geeignete Tore (**46**, **47** und **48**) zum Verbinden der vertrauenswürdigen Einrichtung **24** mit dem Datenbus **26**, den Steuerungsleitungen **27** bzw. den Adreßleitungen **27-1** der Hauptplatine **20** aufweist. Jeder der Blöcke in der vertrauenswürdigen Einrichtung **24** hat Zugriff (üblicherweise über die Steuerung **40**) zu den geeigneten flüchtigen Speicherbereichen **4** und/oder nicht-flüchtigen Speicherbereichen **3** der vertrauenswürdigen Einrichtung **24**. Zusätzlich dazu ist die vertrauenswürdige Einrichtung **24** auf eine bekannte Weise entworfen, um fälschungsresistent zu sein.

[0068] Aus Gründen des Verhaltens kann die vertrauenswürdige Einrichtung **24** als eine anwendungsspezifische integrierte Schaltung (ASIC) implementiert sein. Der Flexibilität halber ist die vertrauenswürdige Einrichtung **24** jedoch vorzugsweise eine geeignet programmierte Mikrosteuerung. Sowohl ASICs als auch Mikrosteuerungen sind in der Technik der Mikroelektronik bekannt und werden hierin nicht detaillierter berücksichtigt.

[0069] Ein Datenartikel, der in dem nicht-flüchtigen Speicher **3** der vertrauenswürdigen Einrichtung **24** gespeichert ist, ist ein Zertifikat **350**. Das Zertifikat **350** enthält zumindest einen öffentlichen Schlüssel **351** der vertrauenswürdigen Einrichtung **24** und optional einen authentifizierten Wert **352** des Plattformintegritätsmaßes, der durch eine vertrauenswürdige Partei (TP) gemessen wird. Das Zertifikat **350** wird durch die TP unter Verwendung des privaten Schlüssels der TP signiert, bevor dasselbe in der vertrauenswürdigen Einrichtung **24** gespeichert wird. Bei späteren Kommunikationssitzungen kann ein Benutzer der Plattform **10** die Integrität der Plattform **10** und der Betriebsumgebung verifizieren, durch Vergleichen des erworbenen Integritätsmaßes (d. h. des gemessen Integritätsmaßes) mit einem authentischen Integritätsmaß **352**, wie nachfolgend beschrieben wird. Die Kenntnis des allgemein verfügbaren öffentlichen Schlüssels der TP ermöglicht eine einfache Verifizierung des Zertifikats **350**. Der nicht-flüchtige Speicher **3** enthält ferner ein Identitätsetikett (ID-Etikett) **353**. Das ID-Etikett **353** ist ein herkömmliches ID-Etikett, z. B. eine Seriennummer, die innerhalb eines bestimmten Kontexts eindeutig ist. Das ID-Etikett **353** wird allgemein zum Indizieren und Etikettieren von Daten verwendet, die für die vertrauenswürdige Einrichtung **24** relevant sind, ist aber an sich nicht ausreichend, um die Identität der Plattform **10** unter vertrauenswürdigen Umständen zu belegen.

[0070] Die vertrauenswürdige dritte Partei, die aufgefordert wird, das authentische Integritätsmaß zu liefern, inspiziert den Typ der Plattform, um zu entscheiden, ob sie für dieselbe bürgen sollte oder nicht. Dies ist eine Frage der Police (policy). Wenn alles in Ordnung ist, mißt die TP den Wert des Integritätsmaßes der Plattform. Dann erzeugt die TP ein Zertifikat für die Plattform. Das Zertifikat wird durch die TP durch Anbringen des öffentlichen Schlüssels der vertrauenswürdigen Einrichtung und optional dessen ID-Etiketts an das gemessene Integritätsmaß und durch Signieren der Zeichenfolge mit dem privaten Schlüssel der TP erzeugt.

[0071] Die vertrauenswürdige Einrichtung **24** kann nachfolgend ihre Identität durch Verwenden ihres privaten Schlüssels belegen, um bestimmte Eingangsdaten zu verarbeiten, die von dem Benutzer empfangen wurden, und Ausgangsdaten zu erzeugen, derart, daß es statistisch unmöglich ist, das Eingangs-/Ausgangs-Paar ohne Kenntnis des privaten Schlüssels zu erzeugen. Somit bildet die Kenntnis des privaten Schlüssels in diesem Fall die Basis der Identität. Es wäre eindeutig machbar, eine symmetrische Verschlüsselung zu verwenden, um die Basis der Identität zu bilden. Der Nachteil der Verwendung einer symmetrischen Verschlüsselung ist jedoch, daß der Benutzer sein Geheimnis mit der vertrauenswürdigen Einrichtung gemeinschaftlich verwenden müßte. Ferner, als Ergebnis des Bedarfs zum gemeinschaftlichen Verwenden des Geheimnisses mit dem Benutzer, wäre es nicht ausreichend, die Identität für eine dritte Partei zu belegen, die nicht vollständig sicher sein könnte, ob die Verifizierung von der vertrauenswürdigen Einrichtung oder dem Benutzer stammt, während eine symmetrische Verschlüsselung im Prinzip ausreichend wäre, um die Identität für den Benutzer zu belegen.

[0072] Die vertrauenswürdige Einrichtung **24** wird durch Schreiben des Zertifikats **350** in die geeigneten nicht-flüchtigen Speicherpositionen **3** der vertrauenswürdigen Einrichtung **24** initialisiert. Dies wird vorzugsweise durch eine sichere Kommunikation mit der vertrauenswürdigen Einrichtung **24** durchgeführt, nachdem dieselbe in der Hauptplatine **20** installiert wurde. Das Verfahren des Schreibens des Zertifikats zu der vertrauenswürdigen Einrichtung **24** ist analog zu dem Verfahren, das verwendet wird, um intelligente Karten durch Schreiben privater Schlüssel auf dieselben zu initialisieren. Die sichere Kommunikation wird durch einen „Hauptschlüssel" unterstützt, der nur der TP bekannt ist, der an die vertrauenswürdige Einrichtung (oder die intelligente Karte) während der Herstellung geschrieben wird und verwendet wird, um das Schreiben von Daten an die vertrauenswürdige Einrichtung **24** zu ermöglichen; das Schrei-

ben von Daten an die vertrauenswürdige Einrichtung **24** ohne Kenntnis des Hauptschlüssels ist nicht möglich.

[0073] An einem späteren Punkt während der Operation der Plattform, z. B. wenn dieselbe eingeschaltet oder zurückgesetzt wird, mißt und speichert die vertrauenswürdige Einrichtung **24** das Integritätsmaß **361** der Plattform.

[0074] Die vertrauenswürdige Einrichtung **24** ist mit zumindest einem Verfahren zum zuverlässigen Messen oder Erwerben des Integritätsmaßes der Rechenplattform **10** ausgerüstet, der dieselbe zugeordnet ist, um einen Vergleich mit dem authentischen Integritätsmaß zu ermöglichen, das durch die vertrauenswürdige dritte Partei geliefert wird. Bei dem vorliegenden Ausführungsbeispiel wird das Integritätsmaß durch die Meßfunktion **41** erworben, durch Erzeugen einer Auswahl der BIOS-Befehle in dem BIOS-Speicher und dem SPK-Code. Das gemessene Integritätsmaß wird unter Verwendung des privaten Schlüssels der vertrauenswürdigen Einrichtung **24** signiert, um das Zutrauen zu liefern, daß das Integritätsmaß durch die vertrauenswürdige Einrichtung **24** erworben wurde. Ein derart erworbenes Integritätsmaß, falls dieselbe wie oben beschrieben verifiziert wurde, gibt einem potentiellen Benutzer der Plattform eine hohe Zutrauensebene, daß die Plattform **10** nicht an einer Hardware oder einem BIOS-Programm oder einer Ebene abgeändert wurde.

[0075] Die Meßfunktion **41** hat Zugriff auf folgende Teile: den nicht-flüchtigen Speicher **3** zum Speichern eines Hash-Programms **354** und eines privaten Schlüssels **355** der vertrauenswürdigen Einrichtung **24** und einen flüchtigen Speicher **4** zum Speichern des erworbenen Integritätsmaßes in der Form einer Auswahl **361**. Bei geeigneten Ausführungsbeispielen kann der flüchtige Speicher **4** ferner verwendet werden, um die öffentlichen Schlüssel und zugeordnete ID-Etiketten **360a**–**360n** von einer oder mehreren authentischen intelligenten Karten (nicht gezeigt) zu speichern, die verwendet werden können, um Zugriff zu der Plattform **10** zu erlangen.

[0076] Bei einer bevorzugten Implementierung umfaßt sowohl die Auswahl als auch das Integritätsmaß einen Boolschen Wert, der in dem flüchtigen Speicher **4** durch die Meßfunktion **41** gespeichert wird, aus den nachfolgend beschriebenen Gründen.

[0077] Ein bevorzugter Prozeß zum Erwerben eines Integritätsmaßes für die Computerplattform **10** wird nun Bezug nehmend auf Fig. 5 beschrieben.

[0078] Bei Schritt **500**, beim Einschalten, überwacht die Meßfunktion **41** die Aktivität des Hauptprozessors **21** an den Daten, der Steuerung und den Adreßleitungen (**26**, **27** und **27-1**), um zu bestimmen, ob die vertrauenswürdige Einrichtung **24** der erste Speicher ist, auf den zugegriffen wurde. Der Prozessor **21** wird zu der vertrauenswürdigen Einrichtung **24** gerichtet, die als ein Speicher agiert. Bei Schritt **505**, wenn die vertrauenswürdige Einrichtung **24** der erste zugegriffene Speicher ist, schreibt die Meßfunktion **41** bei Schritt **510** einen Boolschen Wert in den flüchtigen Speicher **4**, der anzeigt, daß die vertrauenswürdige Einrichtung **24** der erste zugegriffene Speicher war. Anderweitig schreibt die Meßfunktion bei Schritt **515** einen Boolschen Wert, der anzeigt, daß die vertrauenswürdige Einrichtung **24** nicht der erste zugegriffene Speicher war.

[0079] In dem Fall, daß auf die vertrauenswürdige Einrichtung **24** nicht zuerst zugegriffen wurde, besteht natürlich eine Möglichkeit, daß auf die vertrauenswürdige Einrichtung **24** überhaupt nicht zugegriffen wird. Dies wäre z. B. der Fall, wenn der Hauptprozessor **21** gehandhabt wird, um zuerst das BIOS-Programm abzuspielen. Unter diesen Umständen würde die Plattform arbeiten, wäre jedoch nicht in der Lage, ihre Integrität nach Bedarf zu verifizieren, da das Integritätsmaß nicht verfügbar wäre. Ferner, wenn auf die vertrauenswürdige Einrichtung **24** zugegriffen würde, nachdem auf das BIOS-Programm zugegriffen wurde, würde der Boolsche Wert eindeutig eine fehlende Integrität der Plattform anzeigen.

[0080] Wenn jedoch ein Benutzer bereit ist, dem BIOS zu vertrauen, kann die Computerplattform **10** angeordnet werden, um die BIOS-Befehle als die ersten Befehle zu verwenden, auf die zugegriffen wurde.

[0081] Bei Schritt **520**, wenn (oder falls) durch den Hauptprozessor **21** auf die vertrauenswürdige Einrichtung **24** als ein Speicher zugegriffen wird, liest der Hauptprozessor **21** die gespeicherten, systemeigenen Hash-Befehle **354** aus der Meßfunktion **41** bei Schritt **525**. Die Hash-Befehle **354** werden zum Verarbeiten durch den Hauptprozessor **21** über den Datenbus **26** weitergeleitet. Bei Schritt **530** führt der Hauptprozessor **21** die Hash-Befehle **354** aus und verwendet dieselben bei Schritt **535**, um einen Auswahl des BIOS-Speichers **29** zu berechnen, durch Lesen der Inhalte des BIOS-Speichers **29** und durch Verarbeiten dieser Inhalte gemäß dem Hash-Programm. Bei Schritt **540** schreibt der Hauptprozessor **21** die berechnete Auswahl **361** in die geeignete, flüchtige Speicherposition **4** in der vertrauenswürdigen Einrichtung **24**. Auf ähnliche Weise initiiert die Meßfunktion **41** die Berechnung einer Auswahl für den SPK **32**, der momentan in einer geeigneten, nicht-flüchtigen Speicherposition **3** in der vertrauenswürdigen Einrichtung **24** gespeichert ist. Die Meßfunktion **41** ruft dann bei Schritt **545** die BIOS-Firmware **28** in dem BIOS-Speicher **29** auf und die Ausführung wird fortgesetzt, wie nachfolgend beschrieben ist.

[0082] Es besteht offensichtlich eine Anzahl von unterschiedlichen Möglichkeiten, auf die das Integritätsmaß der Plattform berechnet werden kann, abhängig von dem Umfang des erforderlichen Vertrauens. Die Messung der Integrität des BIOS-Programms liefert eine grundlegende Prüfung der Integrität der zugrundeliegenden Verarbeitungsumgebung einer Plattform. Das Integritätsmaß sollte von einer derartigen Form sein, daß sie ein Schlußfolgern über die Gültigkeit des Bootprozesses ermöglicht – der Wert des Integritätsmaßes kann verwendet werden, um zu verifizieren, ob die Plattform unter Verwendung des korrekten BIOS urgeladen hat. Optional könnten individuelle Funktionsblöcke innerhalb des BIOS ihre eigenen Auswahlwerte aufweisen, wobei eine gemeinsame BIOS-Auswahl eine Auswahl dieser individuellen Auswahlen ist. Dies ermöglicht es einer Police anzugeben, welche Teile der BIOS-Operation für einen beabsichtigten Zweck kritisch sind, und welche irrelevant sind (wobei in diesem Fall die individuellen Auswahlen auf eine Weise gespeichert werden müssen, derart, daß die Gültigkeit der Operation unter der Police eingerichtet werden kann).

[0083] Andere Integritätsprüfungen könnten das Einrichten umfassen, das verschiedene andere Einrichtungen, Komponenten oder Vorrichtungen, die an die Plattform angebracht sind, vorhanden und in richtigem Betriebszustand sind. Bei einem Beispiel könnten die BIOS-Programme, die einer SCSI-Steuerung zugeordnet sind, verifiziert werden, um sicherzustellen, daß Kommunikationen mit Peripheriegeräten vertraut werden kann. Bei einem anderen Beispiel könnte die Integrität anderer Einrichtungen, z. B. Speichereinrichtungen oder Coprozessoren, auf der Plattform verifiziert werden, durch Ausführen fester Challenge/Response-Interaktionen (Aufforderung-/Antwort-Interaktionen), um konsistente Ergebnisse sicherzustellen. Wenn die vertrauenswürdige Einrichtung **24** eine abtrennbare Komponente ist, ist eine derartige Form der Interaktion wünschenswert, um eine geeignete logische Bindung zwischen der vertrauenswürdigen Einrichtung **24** und der Plattform zu liefern. Ferner, obwohl die vertrauenswürdige Einrichtung **24** bei dem vorliegenden Ausführungsbeispiel den Datenbus als deren Hauptkommunikationseinrichtung mit anderen Teilen der Plattform verwendet, wäre es durchführbar, obwohl nicht so bequem, alternative Kommunikationswege zu liefern, wie z. B. hartverdrahtete Wege oder optische Wege. Ferner, obwohl die vertrauenswürdige Einrichtung **24** bei dem vorliegenden Ausführungsbeispiel den Hauptprozessor **21** anweist, das Integritätsmaß zu berechnen, ist die vertrauenswürdige Einrichtung bei anderen Ausführungsbeispielen selbst angeordnet, um eines oder mehrere Integritätsmaße zu messen.

[0084] Vorzugsweise umfaßt der BIOS-Bootprozeß Mechanismen, um die Integrität des Bootprozesses selbst zu verifizieren. Derartige Mechanismen sind bereits z. B. aus dem Entwurf von Intel „Wired for Management baseline specification v 2,0-BOOT Integrity Service" bekannt, und umfassen die Berechnung von Auswahlen von Software oder Firmware vor dem Laden dieser Software oder Firmware. Eine derartige berechnete Auswahl wird mit einem Wert verglichen, der in einem Zertifikat gespeichert ist, das durch eine vertrauenswürdige Entität geliefert wird, deren öffentlicher Schlüssel dem BIOS bekannt ist. Die Software/Firmware wird dann nur geladen, wenn der berechnete Wert mit dem erwarteten Wert aus dem Zertifikat übereinstimmt, und das Zertifikat als gültig belegt wurde, durch Verwendung des öffentlichen Schlüssels der vertrauenswürdigen Entität. Anderweitig wird eine geeignete Ausnahmehandhabungsroutine aufgerufen.

[0085] Optional, nach dem Empfangen der berechneten BIOS-Auswahl, kann die vertrauenswürdige Einrichtung **24** den richtigen Wert der BIOS-Auswahl in dem Zertifikat inspizieren und die Steuerung nicht an das BIOS weiterleiten, wenn die berechnete Auswahl nicht mit dem richtigen Wert übereinstimmt. Zusätzlich oder alternativ dazu kann die vertrauenswürdige Einrichtung **24** den Boolschen Wert inspizieren und die Steuerung nicht zurück an das BIOS geben, wenn die vertrauenswürdige Einrichtung **24** nicht der erste zugegriffene Speicher war. In jedem dieser Fälle kann eine geeignete Ausnahmehandhabungsroutine aufgerufen werden.

[0086] Optional, wie in Fig. 6 gezeigt ist, ist ein Systemverwaltungsrat (SMC = system management counsel) **60** mit der Computerplattform **10** über eine Verbindung **62** gekoppelt, um eine Steuerung und Unterstützung für die Computerplattform **10** zu liefern. Bei einem Ausführungsbeispiel umfaßt der SMC **60** separate, unabhängige Prozessoren (nicht gezeigt), wie z. B. standardmäßige, nicht vernetzte Personalcomputer (PC). Die Verbindung **62** kann serielle Schnittstellen (z. B. RS-232 und USB) und/oder private LAN-Verbindungen umfassen. Der SMC **60** wird primär verwendet, um den SPK **32** während der Initialisierung der Computerplattform **10** zu authentifizieren. Zusätzlich dazu ist die Computerplattform **10** über SMC **60** konfiguriert. Bei einem Ausführungsbeispiel führt der SMC **60** eine entfernte Fehlerbeseitigung für den SPK **32** und das SPGS **33** durch.

[0087] Bei einem Ausführungsbeispiel sind die GUI-Schnittstellen für die System-Steuerung und -Verwaltung nur auf dem SMC **60** implementiert. Dieses Ausführungsbeispiel ermöglicht eine Entwicklung und ein Testen der Systemverwaltungsschnittstellen und der menschlichen Faktoren parallel zu der Entwicklung des Rests der Computerplattform **10**, ohne darauf warten zu müssen, daß die gesamte Computerplattform **10** hochgefahren wird.

[0088] Es kann mehr als ein SMC **60** mit der Computerplattform **10** über eine serielle Schnittstelle und/oder eine LAN-Verbindung **62** gekoppelt sein. Bei einem Ausführungsbeispiel sind die Funktionen des SMC **60** in das SPGS **33** in einer Computerplattform **10** integriert, die einen einzelnen Prozessor aufweist, wie z. B. eine Arbeitsstation.

[0089] Zusätzlich dazu könnte die vertrauenswürdige Einrichtung **24** in dem SMC lokalisiert sein und als die vertrauenswürdige Einrichtung entfernt von der Computerplattform **10** agieren.

[0090] Sobald die vertrauenswürdige Einrichtung **24** eine vertrauenswürdige Bootsequenz initiiert hat, wie oben beschrieben ist, ist es immer noch notwendig sicherzustellen, daß die Vertrauenskette durch die Initialisierung der Betriebsdomänen beibehalten wird. Daher, zusätzlich zur Verwendung der vertrauenswürdigen Einrichtung **24**, um Informationen darüber zu liefern, ob der Computerplattform vertraut werden kann, ist es nötig zu bestimmen, daß der Betriebsumgebung eines Benutzers vertraut werden kann.

[0091] Dementsprechend, sobald die vertrauenswürdige Einrichtung **24** die Steuerung an die BIOS-Firmware **28** weitergegeben hat, ist die SPA **31** angeordnet, um eine vertrauenswürdige Betriebsumgebung zu liefern, wie nachfolgend beschrieben wird.

[0092] Zuerst, beim Weitergeben der Steuerung an die BIOS-Firmware **28** urlädt und authentifiziert die BIOS-Firmware **28**, inter alia, die EFI.

[0093] Ein EFI-Dateisystem speichert ein Ladeprogramm einer sicheren Plattform (SP), eine Systemkonfigurationsdatenbank (SCD), ein SPK-Bild **32** und ein SPGS-Bild **33**. Die EFI lädt das SP-Ladeprogramm von dem EFI-Dateisystem in den Speicher **25**. Die EFI authentifiziert dieses Bild unter Verwendung des öffentlichen Schlüssels des Herstellers des Prozessors **21**. Diese Authentifizierung erfordert, daß das SP-Ladeprogramm digital mit dem privaten Schlüssel des Herstellers des Prozessors **21** signiert wird.

[0094] Die EFI überträgt dann die Steuerung zu dem SP-Ladeprogramm, das in dem Speicher **25** gespeichert ist. Das SP-Ladeprogramm ist ein EFI-basiertes, sekundäres Ladeprogramm, das spezifisch für die sichere Plattform ist. Das SP-Ladeprogramm ist für das Laden von SP-Bildern in den Speicher **25** verantwortlich.

[0095] Bei einem Ausführungsbeispiel ist es möglich, daß die Ausführung an eine EFI-Hüllenaufforderung (EFI-Shell Prompt) übertragen wird, um eine erstmalige Systeminstallation und andere Handhabungsdetails zu ermöglichen, was die SP-Vertrauenskette durchbricht. In diesem Fall erkennt die EFI, daß das Vertrauen verloren wurde, und fährt nicht mit dem Laden des SP-Ladeprogramms fort. Statt dessen wird die Computerplattform **10** zurückgesetzt, so daß alle Prozessoren **21** wieder mit dem Suchen nach Befehlen von der vertrauenswürdigen Einrichtung **24** beginnen.

[0096] Das SP-Ladeprogramm, das aus dem Speicher **25** läuft, lädt die SCD von dem EFI-Dateisystem in den Speicher **25**. Das SP-Ladeprogramm authentifiziert dann die SCD unter Verwendung eines öffentlichen Schlüssels, der in dem SP-Ladeprogrammbild enthalten ist. Das SP-Ladeprogramm verwendet die SCD, um zu bestimmen, welche Bilder des SPK **32** und des SPGS **33** von dem EFI-Dateisystem in den Speicher geladen werden sollen. Das SP-Ladeprogramm verwendet den oben genannten öffentlichen Schlüssel zum Authentifizieren der Bilder des SPK **32** und des SPGS **33**. Das SP-Ladeprogramm erzeugt eine virtuelle Abbildung für einen Eingangsbereich des SPK **32** ausschließlich mit Lese- und Ausführ-Erlaubnissen. Das SP-Ladeprogramm schaltet dann in den virtuellen Modus und zweigt zu dem Eingangspunkt des SPK **32** ab.

[0097] Bei der Bootsequenz zum Hochfahren des SPK **32** initialisiert der SPK **32**, der aus dem Speicher **25** auf dem Prozessor **21** läuft einen Privilegstatus (z. B. eine Unterbrechungsvektortabelle (NT), Steuerregister und eine bestimmte Interrupt-Konfiguration) und erzeugt andere zusätzliche Speicherabbildungen, die für den SPK **32** erforderlich sind, wie z. B. beschreibbare Bereiche für SPK-Daten. Der SPK **32** erzeugt dann erforderliche Speicherabbildungen und einen zusätzlichen Aufbau, der erforderlich ist, um das SPGS **33** zu betreiben.

[0098] Eine sichere Plattform (SP) **34** mit gespiegeltem Dateisystem speichert zwei redundante Steuerblockbilder. Der SPK **32** liest die zwei redundanten Steuerblockbilder aus dem gespiegelten Dateisystem der SP in den SPK **32** in dem Speicher **25** als redundante Steuerblockbilder. Die zwei redundanten Steuerblockbilder enthalten Steuerungsinformationen, die an der ersten Computerplattform **10** initialisiert wurden. Die redundanten Steuerblockbilder werden verwendet, um zu testen, ob die Computerplattform **10** bereits initialisiert wurde.

[0099] Bei einem Ausführungsbeispiel enthalten die redundanten Steuerblockbilder jeweils zumindest drei einzelne Steuerbereiche. Der erste Steuerbereich enthält ein Bild, das ebenfalls durch den öffentlichen Schlüssel des Herstellers des Prozessors **21** signiert wurde, der geschrieben wurde, als die Computerplattform **10** zum ersten Mal urgeladen wurde. Der erste Steuerbereich wird verwendet, um einen Wurzelsystemschlüssel (RSK = root system key) in dem zweiten Steuerbereich zu speichern. Der zweite Steuerbereich enthält den RSK, der unter dem-

selben verschlüsselt ist. Der zweite Steuerbereich wird verwendet, um zu validieren, daß ein korrekter RSK bei nachfolgenden Bootvorgängen geliefert wurde. Das Verschlüsseln des RSK unter demselben ermöglicht eine Validierung des RSK, durch Vergleichen der Ergebnisse mit dem Wert, der bereits in dem zweiten Steuerbereich gespeichert ist. Der dritte Steuerbereich enthält ein Verzeichnis von Plattformsteuerungsinformationen der obersten Ebene, einschließlich Schlüssel, Pseudozufallszahlengeneratorstatus (PRNG-Status) und einen Letzte-Entropie-Pool-Schnappschuß, wobei alle verschlüsselt und durch den RSK nach Integrität geprüft wurden.

[0100] Der SPK **32** weist üblicherweise eine minimale oder keine I/O-Fähigkeit auf. Bei einem Ausführungsbeispiel führt das SP-Ladeprogramm I/O-Zugriffe vor der Übertragung der Steuerung an den SPK **32** aus. Bei einem anderen Ausführungsbeispiel wird das SPGS **33** in einen I/O-Bereitzustand hochgefahren, vor der I/O-Operation, um von der Platte zu lesen, und die Steuerung fährt zurück zu dem SPK **32**. Bei einem anderen Ausführungsbeispiel lädt das SPGS **33** den Speicher **25** und nachfolgend wird ein Ruf an den SPK **32** durchgeführt, der die obige Operation ausführt.

[0101] Der SPK **32** bestimmt, ob die Steuerbereiche der zwei redundanten Steuerblockbilder übereinstimmen und die digitale Signatur prüft. Wenn die Steuerbereiche nicht übereinstimmen, werden die Steuerbereiche des redundanten Steuerblockbildes, dessen Integritätsprüfungen gültig sind verwendet, und die Steuerbereiche des anderen redundanten Steuerblocks, dessen Integritätsprüfungen ungültig sind, werden zurückgespeichert, um mit den verwendeten Steuerbereichen des gültigen, redundanten Steuerblockbildes übereinzustimmen. Wenn die Steuerbereiche beider redundanten Steuerblockbilder beschädigt sind, werden Protokolle verwendet, um die Steuerbereiche beider redundanten Steuerblockbilder wiederzugewinnen und zurückzuspeichern, ähnlich zu vielen Datenbanksystemen. Sobald der RSK erhalten wird, wird der Bootprozeß fortgesetzt.

[0102] Der SPK **32** liest und entschlüsselt die Schutzschlüssel aus dem gespiegelten Dateisystem der SP.

[0103] Die erste Domäne des SPGS **33** initialisiert die Entdeckung des I/O und führt dieselbe durch, um Zugriff auf den SMC **60** zu umfassen. Die erste Domäne des SPGS **33** lädt eine verschlüsselte SCD aus dem gespiegelten Dateisystem der SP. Die erste Domäne des SPGS **33** fordert den SPK **32** auf, die verschlüsselte SCD zu entschlüsseln. Die entschlüsselte SCD spezifiziert die Anzahl von Domänen des SPGS **33**, die erzeugt werden sollen, und welche Systemressourcen zu welcher Domäne des SPGS **33** gehören. Die erste Domäne des SPGS **33** erzeugt dann jede zusätzliche Domäne des SPGS **33**, die den entsprechenden Teilsatz der Systemressourcen spezifiziert, um in dem Prozessor **21** umfasst zu sein, auf dem die Domäne des SPGS **33** abgespielt wird.

[0104] Jede Domäne des SPGS **33** liest die verschlüsselte SCD auf ähnliche Weise und erzeugt die spezifizierten Domänen. Jede durch das SPGS erzeugte Domäne umfaßt folgendes: Systemressourcen werden jeder Domäne des SPGS **33** auf einer Pro-Domäne-Basis zugeordnet. Ein Domänenanfangsbild (DII = domain initial image) wird von dem EFI-Dateisystem in den Speicher **25** als DII geladen. Das DII ist üblicherweise ein Betriebssystem-spezifisches Ladeprogramm zum Initiieren des Ladens eines Betriebssystems für eine spezifische Domäne in PL2. Wenn die SCD anzeigt, daß die gegebene Domäne des SPGS **33** eine sichere Domäne ist, dann wird der unabhängige öffentliche Schlüssel des SP-Ladeprogramms verwendet, um das DII zu authentifizieren. Somit werden die DIIs, die in sicheren Domäne des SPGS **33** laufen sollen, vorzugsweise digital mit dem privaten Schlüssel des SP-Ladeprogramms signiert. Eine Verwendung einer nicht sicheren Domäne des SPGS **33** ist es, die Entwicklung und Fehlerbeseitigung von DIIs zu ermöglichen.

[0105] Bei der Erzeugung von jeder der spezifizierten Domänen wird eine zugeordnete, virtuelle vertrauenswürdige Einrichtung in dem SPK **32** erzeugt.

[0106] Wenn die virtuellen vertrauenswürdigen Einrichtungen **37** in dem SPK **32** ausgeführt werden, der auf der PL0-Ebene läuft, der einzigen Ebene, die privilegierte Befehle ausführt, können die virtuellen vertrauenswürdigen Einrichtungen **37** effektiv von der Software isoliert werden, die in den anderen Prozessorprivilegebenen ausgeführt wird. Dementsprechend, da der SPK **32** ein vertrauenswürdiger Code ist, kann ein Benutzer vertrauen, daß die virtuellen vertrauenswürdigen Einrichtungen von einer nicht-vertrauenswürdigen Software abgeschirmt sind.

[0107] Jede virtuelle vertrauenswürdige Einrichtung **37** weist wie in Fig. 7 gezeigt ist eine zentrale Routine **70** zum Steuern der Gesamtoperation der virtuellen vertrauenswürdigen Einrichtung; eine Meßfunktion **71** zum Erwerben eines Integritätsmaßes für eine zugeordnete Betriebsumgebung und zum Erhalten des Integritätsmaßes, die durch die vertrauenswürdige Einrichtung **24** erworben wurde und Messungen an der Software durchführt, die in der zugeordneten Betriebsumgebung ausgeführt werden sollen; eine kryptographische Funktion **72** zum Signieren, Verschlüsseln oder Entschlüsseln spezifizierter Daten auf. Zusätzlich dazu ist jede virtuelle vertrauenswürdige Einrichtung **37** in der Lage, das Integritätsmaß zu verifizieren, das durch die vertrauenswürdige Einrichtung **24** unter Verwendung des öffentli-

chen Schlüssels der vertrauenswürdigen dritten Parteien erworben wurde. Die virtuellen vertrauenswürdigen Einrichtungen **37** haben Zugriff zu dem Speicher, der der PL0-Ebene zugeordnet ist. Zusätzlich dazu ist jede virtuelle vertrauenswürdige Einrichtung **37** angeordnet, und von einer anderen virtuellen vertrauenswürdigen Einrichtung **37** isoliert zu sein, die einer separaten Betriebsumgebung zugeordnet ist.

[0108] Bei der Erzeugung einer zugeordneten Betriebsumgebung in PL1 wird die zugeordnete virtuelle vertrauenswürdige Einrichtung **37** in PL0 mit einem Zertifikat versehen, das dem Benutzer der Betriebsumgebung zugeordnet ist.

[0109] Jedes Zertifikat der virtuellen vertrauenswürdigen Einrichtungen **37** wird in einem lokalen Speicher in der PL0-Ebene gespeichert. Das Zertifikat enthält einen öffentlichen Schlüssel der jeweiligen virtuellen vertrauenswürdigen Einrichtung **37** und optional einen authentifizierten Wert eines Integritätsmaßes zum Messen durch eine vertrauenswürdige dritte Partei, um eine Verifizierung des Integritätsmaßes zu ermöglichen, das durch die vertrauenswürdige Einrichtung **24** erworben wurde. Das Zertifikat wird durch die vertrauenswürdige dritte Partei unter Verwendung des privaten Schlüssels der vertrauenswürdigen dritten Partei signiert, bevor das Zertifikat in der virtuellen vertrauenswürdigen Einrichtung **37** gespeichert wird, wodurch bestätigt wird, daß die vertrauenswürdige dritte Partei für die virtuelle vertrauenswürdige Einrichtung **37** bürgt. Bei diesem Ausführungsbeispiel könnten mögliche vertrauenswürdige dritte Parteien entweder die physikalische vertrauenswürdige Einrichtung **24** oder der SMC **60** sein.

[0110] Wie nachfolgend beschrieben wird, kann ein Benutzer beim Zugreifen auf eine virtuelle vertrauenswürdige Einrichtung **37**, die der jeweiligen Betriebsumgebung zugeordnet ist, das Computerplattformintegritätsmaß, das durch die vertrauenswürdige Einrichtung **24** gemessen und signiert wurde, mit dem privaten Schlüssel der vertrauenswürdigen Einrichtung **24**, und das Integritätsmaß, das durch die virtuelle vertrauenswürdige Einrichtung **37** gemessen und signiert wurde und den privaten Schlüssel der virtuellen vertrauenswürdigen Einrichtung **37** für die jeweilige Betriebsumgebung erhalten. Dementsprechend ist der Benutzer in der Lage, alle Integritätsmaßinformationen zu erhalten, die erforderlich sind, um eine Verifizierung zu ermöglichen, daß der jeweiligen Betriebsumgebung von der virtuellen vertrauenswürdigen Einrichtung **37** vertraut werden kann, ohne daß der Benutzer direkt auf die vertrauenswürdige Einrichtung **24** zugreifen muß.

[0111] Da virtuelle vertrauenswürdige Einrichtungen bei der Erzeugung und Zerstörung von Betriebsumgebungen erzeugt und zerstört werden, ist es nötig sicherzustellen, daß ihre vorübergehende Existenz nicht die Vertrauenswürdigkeit von entweder der Computerplattform **10** oder den zugeordneten Betriebsumgebungen beeinträchtigt. Als solches, um sicherzustellen, daß ein Vertrauen beibehalten werden kann ist es wichtig, daß Geheimnisse, die der/den virtuellen vertrauenswürdigen Einrichtung/en **37** zugeordnet sind zu einer gegebenen Zeit nicht in mehr als einer aktiven vertrauenswürdigen Einrichtung existieren. Dies erfordert, daß strikte und zuverlässige Verfahren in der Computerplattform **10** sicherstellen, daß bei der Erzeugung und Zerstörung einer virtuellen vertrauenswürdigen Einrichtung **37** nur eine Kopie von relevanten Geheimnissen (z. B. für beispielhafte private Schlüssel) beibehalten wird.

[0112] Als solches erfordert die Zerstörung einer virtuellen vertrauenswürdigen Einrichtung **37** die permanente, sichere und geheime Zerstörung der Geheimnisse der virtuellen vertrauenswürdigen Einrichtungen. Wenn eine virtuelle vertrauenswürdige Einrichtung **37** für eine Wiederverwendung zu einem späteren Datum gespeichert werden soll, müssen deren Geheimnisse sicher und geheim für eine spätere Verwendung bewahrt werden.

[0113] Die Geheimnisse, die zu der virtuellen vertrauenswürdigen Einrichtung **37** gehören, könnten in der tatsächlichen vertrauenswürdigen Einrichtung **24** oder dem SMC **60** unter Verwendung der geschützten Speicherungsgeräte von z. B. einem vertrauenswürdigem Plattformmodul gespeichert werden. Geheimnisse von virtuellen vertrauenswürdigen Einrichtungen **37** können sicher unter Verwendung des Beibehaltungsprozesses der vertrauenswürdigen Computerplattformzuordnung (TCPA = trusted computer platform association) gespeichert werden.

[0114] Für Betriebsumgebungen, die trotzdem weiter existieren müssen, daß die Computerplattform **10** herunter- und wieder hochgefahren werden muß, ist es möglich, die gespeicherte, zugeordnete, virtuelle vertrauenswürdige Einrichtung **37** neu anzuordnen. Dies ermöglicht, daß dieselbe virtuelle vertrauenswürdige Einrichtung **37** für dieselbe Betriebsumgebung beibehalten wird, trotz dem temporären Herunterfahren der Betriebsumgebung.

[0115] Das Verfahren, das erforderlich ist, um eine virtuellen vertrauenswürdige Einrichtung **37** neu anzuordnen, hängt jedoch von dem Verfahren ab, das verwendet wird, um die erste virtuelle vertrauenswürdige Einrichtung **37** abzubauen.

[0116] Wenn eine virtuelle vertrauenswürdige Einrichtung **37** unter Verwendung des TCPA-Beibehaltungsprozesses gespeichert wurde, wie in Abschnitt 7.3 der TCPA-Spezifikation beschrieben ist, muß eine neue virtuelle vertrauenswürdige Einrichtung **37** und eine vertrauenswürdige Plattform (d. h. Betriebsumgebung) erzeugt werden (z. B. neuer Ver-

merkschlüssel, Paßwörter können über das Zertifikat der virtuellen vertrauenswürdigen Einrichtungen geliefert werden). Der TCPA-Beibehaltungsprozeß wird verwendet, um die angemessenen Geheimnisse der virtuellen vertrauenswürdigen Einrichtung an die neue virtuelle vertrauenswürdige Einrichtung **37** in der neuen Betriebsumgebung zu übertragen. Dies ist ein Zweischrittprozeß, der zuerst erfordert, daß der Eigentümer/Benutzer der neuen Betriebsumgebung prüft, daß die neue virtuelle vertrauenswürdige Einrichtung **37** und die Betriebsumgebung zumindest dieselbe Sicherheitsebene aufweisen wie die ursprüngliche virtuelle, vertrauenswürdige Einrichtung **37** und die Betriebsumgebung, derart, daß die existierenden Paßwörter die Sicherheitseigenschaft der neuen virtuellen vertrauenswürdigen Einrichtung **37** und der zugeordneten Betriebsumgebung nicht überschreiten.

[0117] Wenn die vorangehende virtuelle vertrauenswürdige Einrichtung **37** vollständig gespeichert wurde, wird eine leere virtuelle vertrauenswürdige Einrichtung **37** und eine zugeordnete Betriebsumgebung in PL0 bzw. PL1 erzeugt und die Originalgeheimnisse, die von der virtuellen vertrauenswürdigen Originaleinrichtung **37** gespeichert wurden, werden in die neue virtuelle vertrauenswürdige Einrichtung geladen. Wie oben erwähnt wurde, muß die neue Betriebsumgebung überprüft werden, daß die neue virtuelle vertrauenswürdige Einrichtung **37** und die Betriebsumgebung zumindest dieselbe Sicherheitsebene aufweisen wie die virtuelle vertrauenswürdige Originaleinrichtung **37** und die zugeordnete Betriebsumgebung, derart, daß die existierenden Paßwörter die Sicherheitseigenschaften der neuen virtuellen vertrauenswürdigen Einrichtung **37** und der Betriebsumgebung nicht überschreiten. Wenn ein SMC **60** die Geheimnisse hält, ist ein bestimmter separater Sicherheitsdienst erforderlich, um die Geheimnisse vertraulich von dem SMC **60** an die Computerplattform **10** zu kommunizieren. Dies erfordert einen Schlüsselverteilungsdienst, wie Fachleuten auf dem Gebiet bekannt ist.

[0118] Dies ermöglicht, daß mehrere Betriebsumgebungen erzeugt werden, wobei jede Betriebsumgebung ihre eigene zugeordnete virtuelle vertrauenswürdige Einrichtung **37** aufweist, derart, daß jede virtuelle vertrauenswürdige Einrichtung **37** das Integritätsmaß für die Computerplattform **10** von der vertrauenswürdigen Einrichtung **24** herleitet und zusätzlich ein Integritätsmaß für die zugeordnete Betriebsumgebung mißt. Dies ermöglicht, daß eine Computerplattform **10** mehrere Benutzer aufweist, wobei jeder seine eigene jeweilige Betriebsumgebung hat, wobei jede Betriebsumgebung von der anderen isoliert ist und jede Betriebsumgebung ein Integritätsmaß sowohl für sich selbst als auch die Computerplattform **10** liefern kann. Dies ermöglicht es einem Benutzer einer Betriebsumgebung zu bestimmen, ob seiner jeweiligen Betriebsumgebung vertraut werden kann, ohne Informationen darüber zu benötigen, ob eine andere Betriebsumgebung auf der Computerplattform **10** läuft.

[0119] Zusätzlich dazu, da jede Domäne isoliert ist und die virtuellen vertrauenswürdigen Einrichtungen **37** in einer privilegierten Prozessorebene PL0 ausgeführt werden, kann eine bösartige Software, die in einer Domäne ausgeführt wird, keine Software attackieren, die in einer anderen Domäne ausgeführt wird.

[0120] Fig. 8 stellt eine Computerplattform **10** dar, die eine vertrauenswürdige Einrichtung **24** aufweist, wobei BIOS- und SPK-Code auf dem Prozessor **21** installiert sind. Die Computerplattform **10** agiert als ein Server, der drei Betriebsumgebungen **80'**, **80"** und **80"'** aufweist, die in der Privilegebene **1** ausgeführt werden, wo jeder Benutzer üblicherweise mit der Betriebsumgebung **80'**, **80"**, **80"'** über eine Netzwerkverbindung kommunizieren würde. Jede der Betriebsumgebungen **80'**, **80"**, **80"'** weist ihre eigene jeweilige virtuelle vertrauenswürdige Einrichtung **37'**, **37"**, **37"'** auf, die in dem SPK **32** auf der Privilegebene PL0 ausgeführt wird. Jede virtuelle vertrauenswürdige Einrichtung **37'**, **37"**, **37"'** weist ihr eigenes eindeutiges Zertifikat (nicht gezeigt) für ihre jeweilige Betriebsumgebung auf. Wenn ein Benutzer für jede Betriebsumgebung **80'**, **80"**, **80"'** mit seiner jeweiligen Betriebsumgebung **80'**, **80"**, **80"'** kommunizieren möchte, erzeugt er etwas vorübergehendes (nouce) (nicht gezeigt), wie z. B. eine zufällige Zahl, und gibt eine Anforderung an seine jeweilige virtuelle vertrauenswürdige Einrichtung **37'**, **37"**, **37"'** aus. Das Vorübergehende wird verwendet, um den Benutzer vor einer Täuschung zu schützen, die durch das Wiederabspielen von alten aber echten Signaturen (genannt eine „Wiederabspielattacke") durch nichtvertrauenswürdige Plattformen verursacht wird. Der Prozeß des Bereitstellens von etwas Vorübergehendem und des Verifizierens der Antwort ist ein Beispiel des bekannten Challenge/Response-Prozesses („Aufruf-/Antwort"-Prozesses).

[0121] Die jeweilige virtuelle vertrauenswürdige Einrichtung **37'**, **37"**, **37"'** empfängt den Aufruf und erzeugt eine angemessene Antwort. Dies kann eine Auswahl des gemessenen Integritätsmaßes des Computerplattformintegritätsmaßes sein, das von der vertrauenswürdigen Einrichtung **24** empfangen und mit dem privaten Schlüssel der vertrauenswürdigen Einrichtung **24** signiert wurde, und des gemessenen Integritätsmaßes für die jeweilige Betriebsumgebung **80'**, **80"**, **80"'**, die mit dem privaten Schlüssel und dem Vorübergehenden und optional mit dessen ID-Etikett der jeweiligen virtuellen vertrauenswürdigen Einrichtung **37** signiert wurde. Die jeweilige vertrauenswürdige Einrichtung **37'**, **37"**, **37"'** sendet das signierte Integritätsmaß zurück, begleitet durch das

Zertifikat der jeweiligen virtuellen vertrauenswürdigen Einrichtungen **37'**, **37''**, **37'''** und das Zertifikat **350** der vertrauenswürdigen Einrichtung **24**, an den Benutzer zurück.

[0122] Der Benutzer empfängt die Challenge-Response (Aufrufantwort) und verifiziert das Zertifikat unter Verwendung des bekannten öffentlichen Schlüssels der TP(s). Der Benutzer extrahiert dann den öffentlichen Schlüssel der virtuellen vertrauenswürdigen Einrichtung **37'**, **37''**, **37'''** und den öffentlichen Schlüssel der vertrauenswürdigen Einrichtung **24** aus dem Zertifikat und verwendet dieselben, um die signierten Integritätsmaße von der Aufrufantwort zu entschlüsseln. Dann verifiziert der Benutzer das Vorübergehende innerhalb der Aufrufantwort. Als nächstes vergleicht der Benutzer die berechneten Integritätsmaße, die er aus der Aufrufantwort extrahiert, mit den ordnungsgemäßen Plattformintegritätsmaßen, die in diesem Ausführungsbeispiel aus den Zertifikaten extrahiert werden. Wenn einer der vorangehenden Verifizierungsschritte fehlschlägt endet der gesamte Prozeß, wobei keine weitere Kommunikation stattfindet.

[0123] Vorausgesetzt alles funktioniert, verwenden der Benutzer und die vertrauenswürdige Plattform andere Protokolle, um sichere Kommunikationen für anderen Daten einzurichten, wobei die Daten von der Plattform vorzugsweise durch die vertrauenswürdige Einrichtung **37'**, **37''**, **37'''** signiert werden, ohne eine Kenntnis der anderen zwei Betriebsumgebungen, die auf der Computerplattform **10** installiert sind.

Patentansprüche

1. Computervorrichtung zum Erzeugen einer vertrauenswürdigen Umgebung, mit folgenden Merkmalen:
einer physischen, vertrauenswürdigen Einrichtung (**24**), die angeordnet ist, um ein erstes Integritätsmaß zu erwerben, um eine Bestimmung darüber zu ermöglichen, ob die Computervorrichtung auf eine vertrauenswürdige Weise arbeitet,
einem Prozessor (**21**) und einem Programmcode, der auf dem Prozessor ausführbar ist, um mehrere Betriebsumgebungen (**80'**, **80''**, **80'''**) einzurichten, von denen jede ihre eigene jeweilig zugeordnete virtuelle vertrauenswürdige Einrichtung (**37'**, **37''**, **37'''**) aufweist, und
einer Einrichtung zum Sicherstellen, dass der Zugriff der Betriebsumgebungen (**80'**, **80''**, **80'''**) auf die Ressourcen eingeschränkt ist, die für die jeweilig zugeordnete virtuelle vertrauenswürdige Einrichtung (**37'**, **37''**, **37'''**) verfügbar sind,
wobei jede virtuelle vertrauenswürdige Einrichtung (**37'**, **37''**, **37'''**) angeordnet ist, um sowohl das erste Integritätsmaß als auch ein zweites Integritätsmaß zu erwerben, wobei das zweite Integritätsmaß eine Bestimmung darüber ermöglicht, ob die Betriebsumgebung, die dieser virtuellen vertrauenswürdigen Einrichtung (**37'**, **37''**, **37'''**) zugeordnet ist, auf eine vertrauenswürdige Weise arbeitet.

2. Computervorrichtung gemäß Anspruch 1, wobei der Prozessor (**21**) die Einrichtung zum Sicherstellen, dass ein Zugriff der Betriebsumgebungen auf Ressourcen, die für die jeweilig zugeordnete virtuelle vertrauenswürdige Einrichtung verfügbar sind, eingeschränkt ist, aufweist und angeordnet ist, um die Ausführung der virtuellen vertrauenswürdigen Einrichtungen in einer ersten Privilegebene (PL1) des Prozessors (**21**) zu ermöglichen und die Ausführung der jeweilig zugeordneten Betriebsumgebung in einer zweiten Privilegebene des Prozessors zu ermöglichen, derart, daß für einen Code, der in der zweiten Privilegebene (PL2) ausgeführt wird, der Zugriff auf die Ressourcen beschränkt ist, die für einen Code verfügbar sind, der in der ersten Privilegebene ausgeführt wird.

3. Computervorrichtung gemäß einem der vorangehenden Ansprüche, bei der die physische, vertrauenswürdige Einrichtung (**24**) eine fälschungsresistente Einrichtung ist.

4. Computervorrichtung gemäß einem der vorangehenden Ansprüche, bei der der Prozessor (**21**) angeordnet ist, um eine Ausführung einer Mehrzahl von virtuellen vertrauenswürdigen Einrichtungen in der ersten Privilegebene (PL1) zu ermöglichen und um die Ausführung jeweiliger zugeordneter Betriebsumgebungen in der zweiten Privilegebene (PL2) zu ermöglichen, wobei jede virtuelle vertrauenswürdige Einrichtung angeordnet ist, um das erste Integritätsmaß und ein Integritätsmaß, das der jeweiligen zugeordneten Betriebsumgebung zugeordnet ist, zu erwerben, um eine Bestimmung darüber zu ermöglichen, ob die jeweilige Betriebsumgebung auf eine vertrauenswürdige Weise arbeitet.

5. Computervorrichtung gemäß einem der vorangehenden Ansprüche, bei der die virtuellen vertrauenswürdigen Einrichtungen angeordnet sind, um eine kryptographische Funktionalität zum Sicherstellen, dass der Zugriff auf Daten, die den virtuellen vertrauenswürdigen Einrichtungen zugeordnet sind, eingeschränkt ist, aufzunehmen.

6. Computervorrichtung gemäß einem der vorangehenden Ansprüche, bei der die physische, vertrauenswürdige Einrichtung (**24**) angeordnet ist, um eines oder mehrere Geheimnisse zu speichern.

7. Computervorrichtung gemäß einem der vorangehenden Ansprüche, bei der den virtuellen vertrauenswürdigen Einrichtungen eines oder mehrere Geheimnisse zugeordnet sind.

8. Computervorrichtung gemäß Anspruch 6 oder 7, bei der zumindest ein Geheimnis ein privater asymmetrischer Verschlüsselungsschlüssel ist.

9. Computervorrichtung gemäß Anspruch 7 oder 8, bei der die physische, vertrauenswürdige Einrichtung (**24**) angeordnet ist, um beim Herunterfahren der Computervorrichtung Geheimnisse zu speichern, die durch eine der virtuellen vertrauenswürdigen Einrichtungen verwendet werden.

10. Computervorrichtung gemäß einem der Ansprüche 2 bis 9, bei der der Code, der in der zweiten Privilegebene (PL2) ausgeführt wird, einen eingeschränkten Zugriff auf Daten aufweist, die einer der virtuellen vertrauenswürdigen Einrichtungen zugeordnet sind, die in der ersten Privilegebene (PL1) ausgeführt wird.

11. Computervorrichtung gemäß einem der Ansprüche 2 bis 10, bei der Daten, die den virtuellen vertrauenswürdigen Einrichtungen zugeordnet sind, vor einer Änderung durch den Code geschützt werden, der in der zweiten Privilegebene (PL2) ausgeführt wird.

12. Computervorrichtung gemäß einem der Ansprüche 2 bis 11, bei der Geheimnisse, die den virtuellen vertrauenswürdigen Einrichtungen zugeordnet sind, für einen Code nicht zugreifbar sind, der in der zweiten Privilegebene (PL2) ausgeführt wird.

13. Computervorrichtung gemäß einem der vorangehenden Ansprüche, bei der die physische, vertrauenswürdige Einrichtung (**24**) für einen öffentlichen Schlüssel bürgt, der einem Vertrauensmodul zugeordnet ist, unter Verwendung eines privaten Schlüssels der physischen, vertrauenswürdigen Einrichtung (**24**).

14. Computervorrichtung gemäß einem der Ansprüche 1 bis 12, bei der eine vertrauenswürdige dritte Partei für einen öffentlichen Schlüssel bürgt, der dem Vertrauensmodul zugeordnet ist, unter Verwendung eines privaten Schlüssels der vertrauenswürdigen Parteien.

15. Computervorrichtung gemäß einem der vorangehenden Ansprüche, bei der die physische, vertrauenswürdige Einrichtung (**24**) angeordnet ist, um Bootsequenzbefehle zu übertragen, um eine Initiierung des Bootens der Computervorrichtung zu ermöglichen.

16. Computervorrichtung gemäß Anspruch 15, bei der der Prozessor (**21**) angeordnet ist, um zu bewirken, daß die Bootsequenzbefehle die ersten Befehle sind, die durch den Prozessor (**21**) nach der Freigabe von dem Zurücksetzen ausgeführt werden.

17. Verfahren zum Erzeugen einer vertrauenswürdigen Umgebung, mit folgenden Schritten:
Erwerben eines ersten Integritätsmaßes, um eine Bestimmung darüber zu ermöglichen, ob eine Computervorrichtung auf eine vertrauenswürdige Weise arbeitet,
Einrichten mehrerer Betriebsumgebungen, von denen jede ihre eigene jeweilige zugeordnete virtuelle vertrauenswürdige Einrichtung aufweist,
Sicherstellen, dass der Zugriff der Betriebsumgebungen auf die Ressourcen eingeschränkt ist, die für die jeweilig zugeordnete virtuelle vertrauenswürdige Einrichtung verfügbar sind, und
Anordnen jeder virtuellen vertrauenswürdigen Einrichtung, um das erste Integritätsmaß und ein zweites Integritätsmaß zu erwerben, wobei das zweite Integritätsmaß eine Bestimmung darüber ermöglicht, ob die Betriebsumgebung, die dieser virtuellen vertrauenswürdigen Einrichtung zugeordnet ist, auf eine vertrauenswürdige Weise arbeitet.

18. Verfahren nach Anspruch 17, bei dem das Ausführen von virtuellen vertrauenswürdigen Einrichtungen in einer ersten Privilegebene eines Prozessors ausgeführt wird, und das Ausführen der zugeordneten Betriebsumgebungen in einer zweiten Privilegebene des Prozessors ausgeführt wird, und wobei das Sicherstellen, das der Zugriff der Betriebsumgebungen auf Ressourcen, die für die jeweilig zugeordnete virtuelle vertrauenswürdige Einrichtung verfügbar sind, eingeschränkt ist, ferner für einen Code, der in der zweiten Privilegebene ausgeführt wird, ein Einschränken des Zugriffs auf die Ressourcen, die für einen Code verfügbar sind, der in der ersten Privilegebene ausgeführt wird aufweist.

19. Verfahren nach Anspruch 17, bei dem das erste Integritätsmaß erworben wird, um eine Bestimmung darüber zu ermöglichen, ob die Computervorrichtung auf eine vertrauenswürdige Weise arbeitet und die virtuellen vertrauenswürdigen Einrichtungen in der ersten Privilegebene (PL1) des Prozessors (**21**) ausführt und die zugeordnete Betriebsumgebungen in der zweiten Privilegebene (PL2) des Prozessors (**21**) ausführt, bei dem sichergestellt wird, das der Zugriff auf Ressourcen, die für den Code verfügbar sind, der in der ersten Privilegebene (PL1) ausgeführt wird, für den Code, der in der zweiten Privilegebene (PL2) ausgeführt wird, beschränkt ist, und bei dem das erste Integritätsmaß und ein zweites Integritätsmaß erworben wird, um eine Bestimmung darüber zu ermöglichen, ob die Betriebsumgebungen auf eine vertrauenswürdige Weise arbeitet.

20. Verfahren nach Anspruch 17, bei dem das erste Integritätsmaß erworben wird, um eine Bestimmung darüber zu ermöglichen, ob die Computervorrichtung auf eine vertrauenswürdige Weise arbeitet und die virtuellen vertrauenswürdigen Einrichtungen und die zugeordneten Betriebsumgebungen aus-

führt, und bei dem sichergestellt wird, dass der Zugriff der Betriebsumgebungen auf die Ressourcen beschränkt ist, die für die jeweilig zugeordnete virtuelle vertrauenswürdige Einrichtung verfügbar sind, und bei dem das erste Integritätsmaß und ein zweites Integritätsmaß erworben wird, um eine Bestimmung darüber zu ermöglichen, ob die Betriebsumgebung, die dieser virtuellen vertrauenswürdigen Einrichtung zugeordnet ist, auf eine vertrauenswürdige Weise arbeitet.

21. Computersystem zum Erzeugen einer vertrauenswürdigen Umgebung, mit folgenden Merkmalen:
einer physischen, vertrauenswürdigen Einrichtung, die angeordnet ist, um ein erstes Integritätsmaß zu erwerben, um eine Bestimmung darüber zu ermöglichen, ob die Computervorrichtung auf eine vertrauenswürdige Weise arbeitet,
einem Prozessor und einem Programmcode, der auf dem Prozessor ausführbar ist, um mehrere Betriebsumgebungen einzurichten, von denen jede ihre eigene jeweilig zugeordnete virtuelle vertrauenswürdige Einrichtung aufweist, und
einer Einrichtung zum Einschränken des Zugriffs der Betriebsumgebungen auf die Ressourcen, die für die jeweilig zugeordnete virtuelle vertrauenswürdige Einrichtung verfügbar sind,
wobei jede virtuelle vertrauenswürdige Einrichtung angeordnet ist, um sowohl das erste Integritätsmaß als auch ein zweites Integritätsmaß zu erwerben, wobei das zweite Integritätsmaß eine Bestimmung darüber ermöglicht, ob die Betriebsumgebung, die dieser virtuellen vertrauenswürdigen Einrichtung zugeordnet ist, auf eine vertrauenswürdige Weise arbeitet.

Es folgen 6 Blatt Zeichnungen

Anhängende Zeichnungen

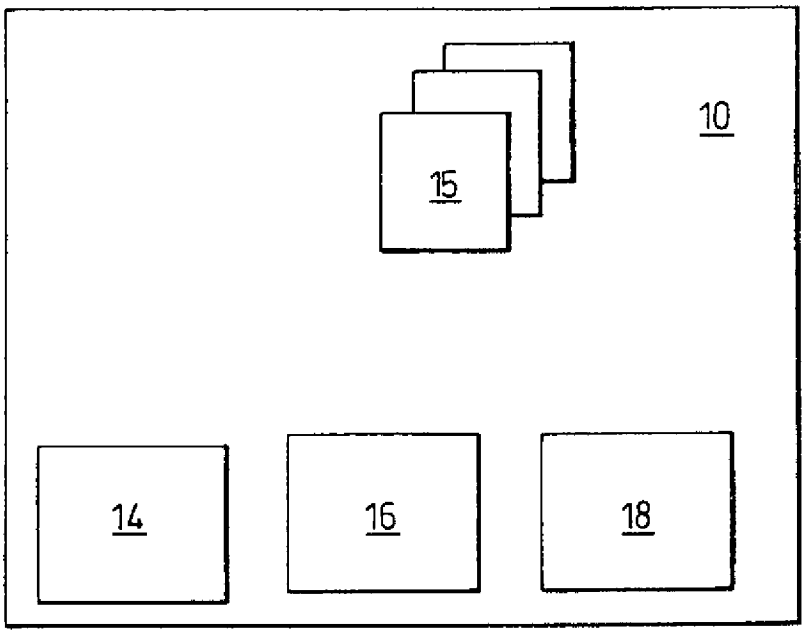


Fig. 1

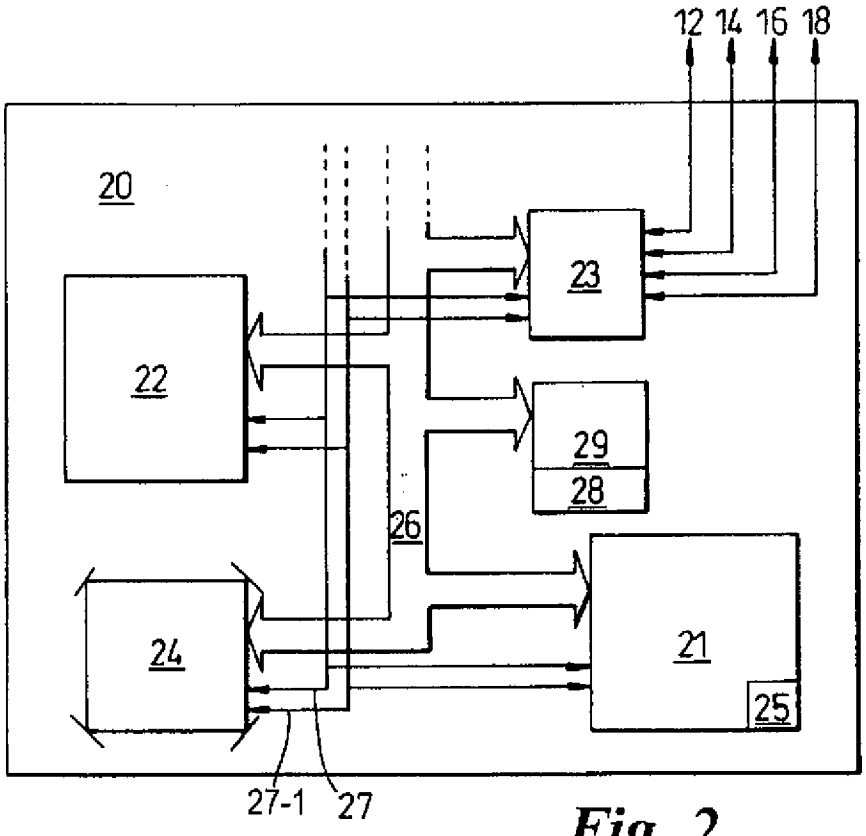


Fig. 2

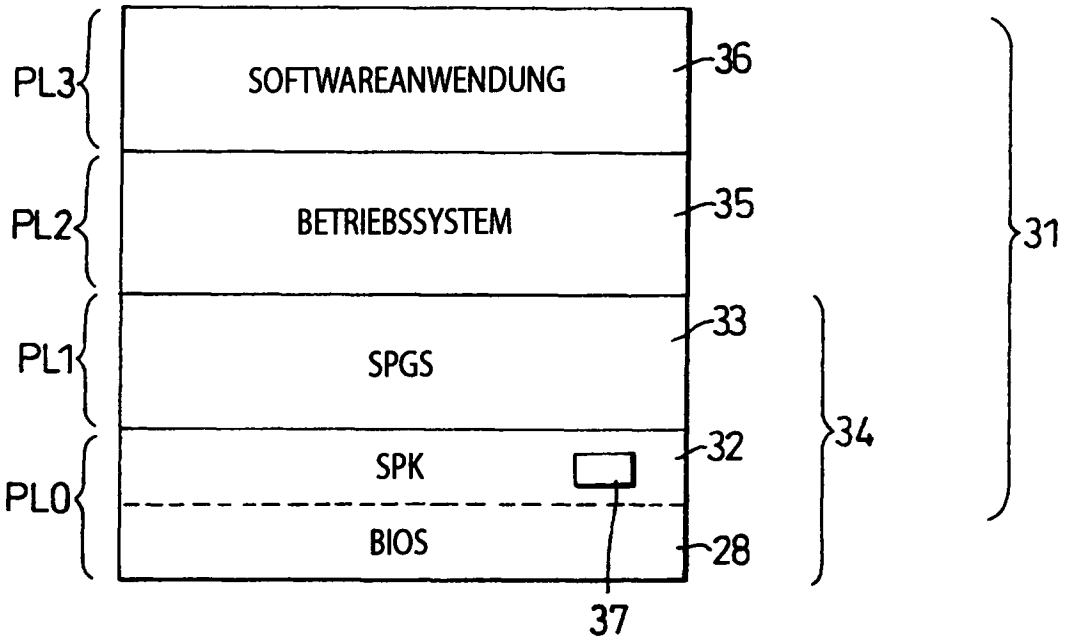

PL3
SOFTWAREANWENDUNG
36
PL2
BETRIEBSSYSTEM
35
31
PL1
SPGS
33
34
PL0
SPK
32
BIOS
28
37

Fig. 3

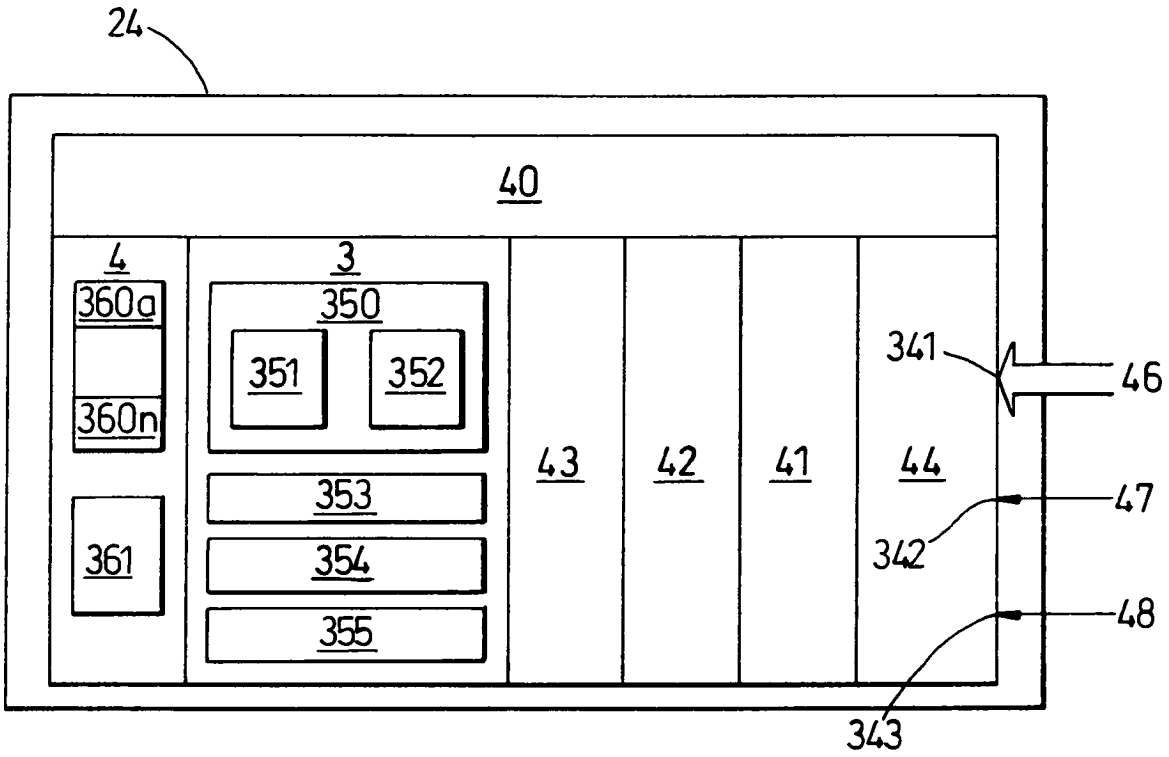

24
40
4
360a
360n
361
3
350
351
352
353
354
355
43
42
41
44
341
46
47
342
48
343

Fig. 4

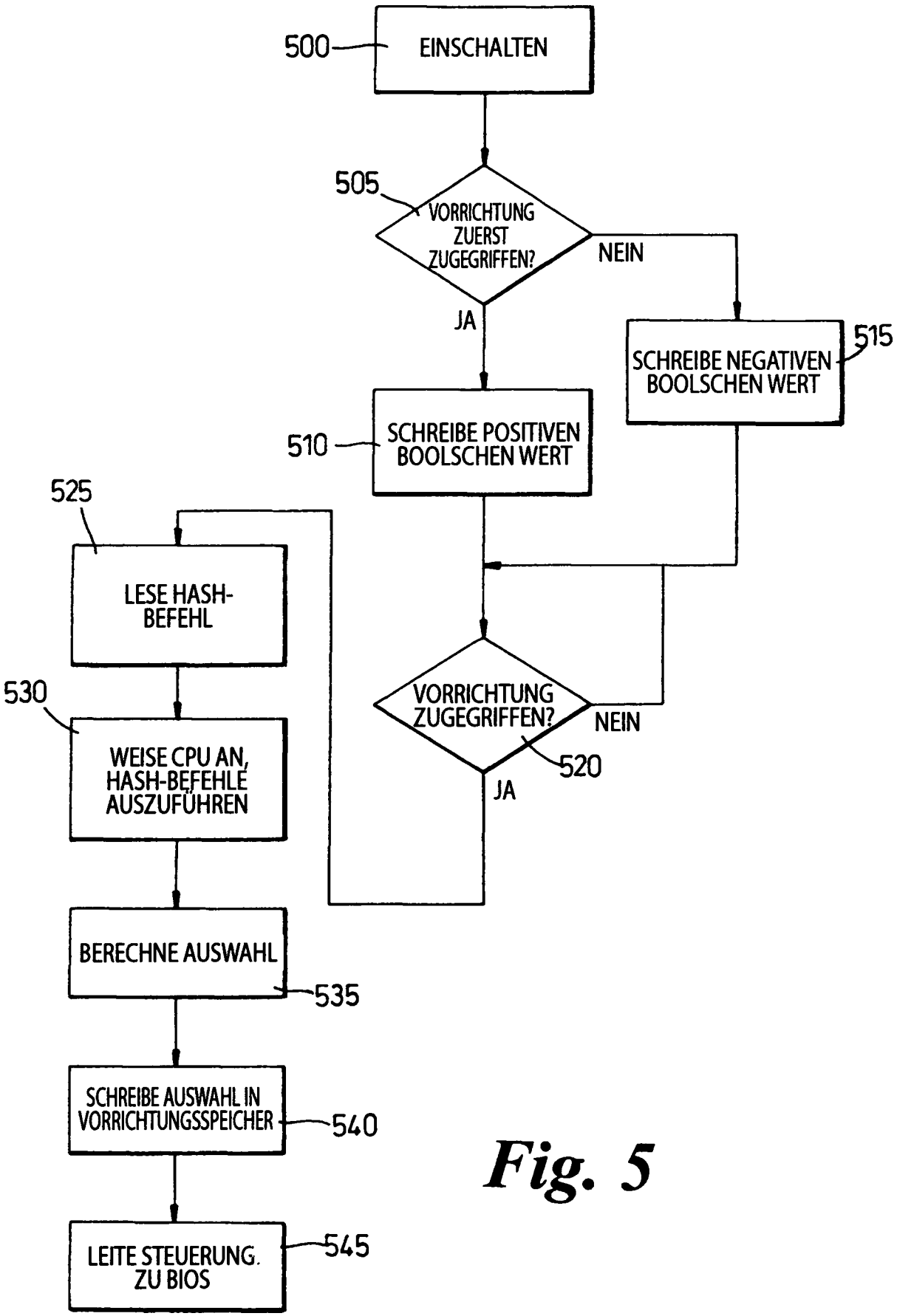

500
EINSCHALTEN
505
VORRICHTUNG ZUERST ZUGEGRIFFEN?
NEIN
JA
515
SCHREIBE NEGATIVEN BOOLSCHEN WERT
510
SCHREIBE POSITIVEN BOOLSCHEN WERT
525
LESE HASH-BEFEHL
530
WEISE CPU AN, HASH-BEFEHLE AUSZUFÜHREN
VORRICHTUNG ZUGEGRIFFEN?
NEIN
520
JA
BERECHNE AUSWAHL
535
SCHREIBE AUSWAHL IN VORRICHTUNGSSPEICHER
540
LEITE STEUERUNG ZU BIOS
545

Fig. 5

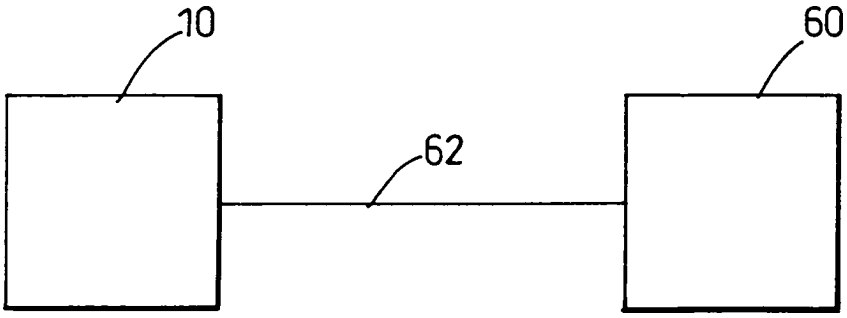


Fig. 6

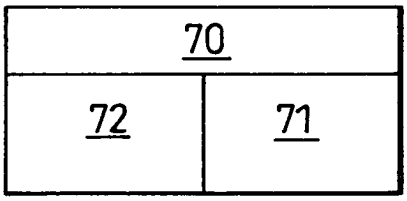


Fig. 7

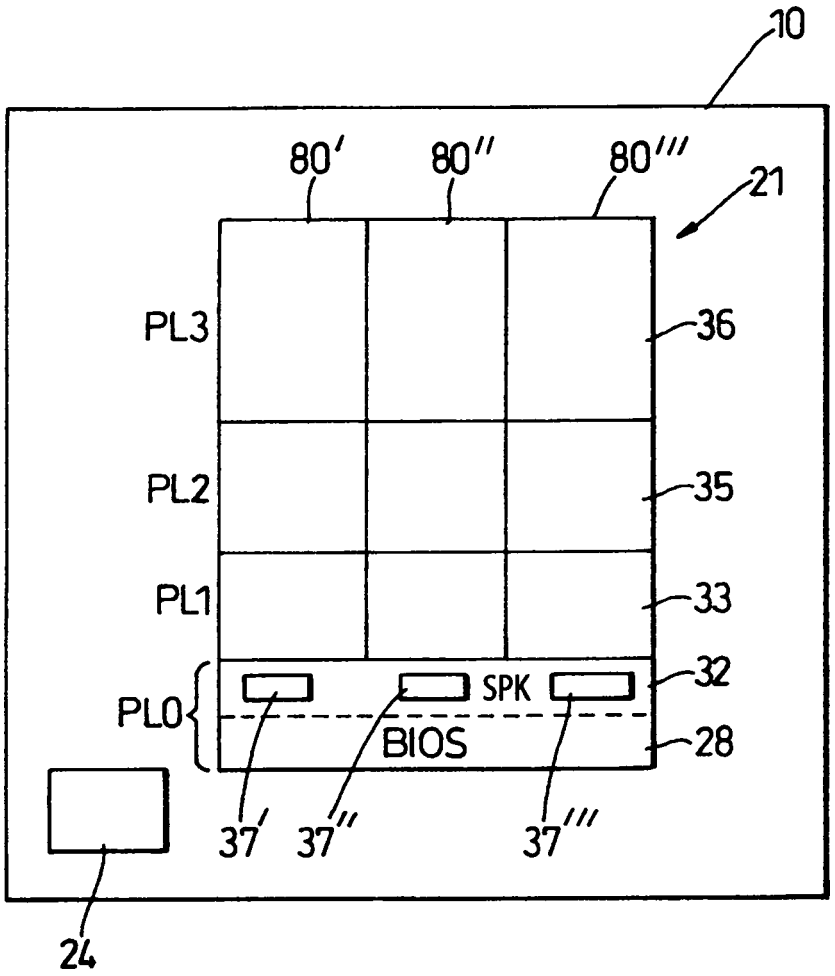


Fig. 8