(19) Deutsches Patent- und Markenamt

(10) **DE 600 07 724 T3** 2011.06.09

(12) Übersetzung der geänderten europäischen Patentschrift

(97) **EP 1 159 662 B2**
(21) Deutsches Aktenzeichen: **600 07 724.1**
(86) PCT-Aktenzeichen: **PCT/GB00/00752**
(96) Europäisches Aktenzeichen: **00 912 743.2**
(87) PCT-Veröffentlichungs-Nr.: **WO 2000/054126**
(86) PCT-Anmeldetag: **03.03.2000**
(87) Veröffentlichungstag der PCT-Anmeldung: **14.09.2000**
(97) Erstveröffentlichung durch das EPA: **05.12.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **14.01.2004**
(97) Veröffentlichungstag des geänderten Patents beim EPA: **06.10.2010**
(47) Veröffentlichungstag im Patentblatt: **09.06.2011**

(51) Int Cl.: ***G06F 1/00*** (2006.01)

Patentschrift wurde im Einspruchsverfahren geändert

(30) Unionspriorität:

9905056	**05.03.1999**	**GB**
9929697	**15.12.1999**	**GB**

(84) Benannte Vertragsanstalten:
DE, FR, GB

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

(72) Erfinder:
BALACHEFF, Boris, St. Michael's Hill, Bristol BS2 8DG, GB; CHAN, David, Monte Sereno, Calif., US

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

(54) Bezeichnung: **CHIPKARTEN-BENUTZERSCHNITTSTELLE FÜR EINE VERTRAUTE COMPUTERPLATTFORM**

Beschreibung

Gebiet der Erfindung

[0001] Die vorliegende Erfindung bezieht sich auf das Gebiet von Computern und insbesondere auf eine Rechenentität, die in einen vertrauenswürdigen Zustand versetzt werden kann, und ein Verfahren eines Betreibens der Computerentität, derart, daß ein Benutzer der Entität sicher ist, daß sich die Rechenentität in dem vertrauenswürdigen Zustand befindet.

Hintergrund der Erfindung

[0002] Herkömmliche bekannte Rechenplattformen für einen breiten Markt umfassen den gut bekannten Personalcomputer (PC) und konkurrierende Produkte, wie beispielsweise den Apple Macintosh™, und eine starke Verbreitung von bekannten Palmtop- und Laptop-Personalcomputern. Im allgemeinen fallen Märkte für derartige Maschinen in zwei Kategorien, wobei diese privat oder für Verbraucher und geschäftlich sind. Ein allgemeines Erfordernis für eine Rechenplattform für einen privaten oder Verbrauchergebrauch ist eine relativ hohe Verarbeitungsleistung, Internetzugriffsmerkmale und Multimediamerkmale zu einem Handhaben von Computerspielen. Bei diesem Typ einer Rechenplattform dominieren die Betriebssystemprodukte Microsoft Windows® '95 und '98 und Intel-Prozessoren den Markt.

[0003] Für einen geschäftlichen Gebrauch bei vielen Anwendungen stellt jedoch eine Serverplattform eine zentralisierte Datenspeicherung und eine Anwendungsfunktionalität für eine Mehrzahl von Client-Stationen bereit. Für einen geschäftlichen Gebrauch sind Schlüsselkriterien eine Verläßlichkeit, Netzwerkmerkmale und Sicherheitsmerkmale. Bei derartigen Plattformen ist das Betriebssystem Microsoft Windows NT 4.0™, sowie das Betriebssystem Unix™ verbreitet.

[0004] Mit der Erhöhung bei einer Handelsaktivität, die über das Internet ausgeführt wird, bekannt als „e-commerce", gab es im Stand der Technik viel Interesse an einem Ermöglichen von Datentransaktionen zwischen Rechenplattformen über das Internet von sowohl privaten als auch geschäftlichen Typen. Ein grundlegender Punkt bei einer Akzeptanz derartiger Systeme ist der eines Vertrauens zwischen in Wechselwirkung stehenden Computerplattformen für das Herstellen derartiger Transaktionen.

[0005] Es gab mehrere bekannte Schemata, die auf ein Erhöhen der Sicherheit und Vertrauenswürdigkeit von Computerplattformen abzielen. Vorherrschend stützen sich dieselben auf ein Hinzufügen von Sicherheitsmerkmalen bei der Anwendungsstufe, d. h., die Sicherheitsmerkmale sind nicht von Natur aus in dem Betriebssystemkern (Kernel) von Betriebssystemen eingebettet und nicht in die grundlegenden Hardwarekomponenten der Rechenplattform eingebaut. Es sind bereits tragbare Computergeräte auf dem Markt erschienen, die eine Smartcard umfassen, die Daten enthält, die für einen Benutzer spezifisch sind, die in einen Smartcard-Leser an dem Computer eingegeben wird. Derzeit befinden sich derartige Smartcards auf der Stufe von Nachrüstextras zu herkömmlichen Personalcomputern und sind in einigen Fällen in eine Verkleidung eines bekannten Computers integriert. Obwohl diese bekannten Schemata die Sicherheit von Computerplattformen ein Stück weit verbessern, können die Pegel einer Sicherheit und Vertrauenswürdigkeit, die durch bekannte Schemata gewonnen werden, als ungenügend betrachtet werden, um eine weitverbreitete Anwendung von automatisierten Transaktionen zwischen Computerplattformen zu ermöglichen. Damit Unternehmen Transaktionen von erheblichem Wert auf einer breiten Skala einem elektronischen Handel aussetzen, benötigen dieselben Vertrauen in die Vertrauenswürdigkeit der zugrundeliegenden Technologie.

[0006] Bekannte Rechenplattformen weisen mehrere Probleme auf, die einem Erhöhen der inhärenten Sicherheit derselben im Weg stehen:

- Der Betriebsstatus einer Computerplattform und der Status der Daten innerhalb der Plattform ist dynamisch und schwer vorauszusagen. Es ist schwierig zu bestimmen, ob eine Computerplattform korrekt wirksam ist, weil der Zustand der Computerplattform und Daten auf der Plattform sich ständig verändern und die Computerplattform selbst sich dynamisch ändern kann.
- Von einem Sicherheitsstandpunkt aus sind geschäftliche Computerplattformen, insbesondere Client-Plattformen, oft in Umgebungen eingesetzt, die für eine unbefugte Modifikation verletzlich sind. Die Hauptbereiche einer Verletzlichkeit umfassen eine Modifikation durch eine Software, die durch einen Benutzer geladen ist, oder über eine Netzwerkverbindung. Insbesondere, aber nicht ausschließlich, herkömmliche Computerplattformen sind eventuell für einen Angriff durch Virusprogramme mit variierenden Graden an Feindseligkeit verletzbar.
- Computerplattformen können hochgerüstet werden oder die Fähigkeiten derselben können durch eine physische Modifikation erweitert oder eingeschränkt werden, d. h., eine Hinzufügung oder Löschung von Komponenten, wie beispielsweise Festplattenlaufwerken, Peripheriegerätetreibern und dergleichen.

[0007] Es ist bekannt, Sicherheitsmerkmale für Computersysteme bereitzustellen, die in einer Betriebssoftware eingebettet sind. Diese Sicherheitsmerkmale zielen primär auf ein Bereitstellen einer Teilung von Informationen innerhalb einer Gemeinschaft von Benutzern eines lokalen Systems ab.

Bei dem bekannten Betriebssystem Microsoft Windows NT™ 4.0 existiert eine Überwachungseinrichtung, die ein „Systemprotokoll-Ereignis-Darstellungsprogramm" genannt wird und bei dem ein Protokoll von Ereignissen, die innerhalb der Plattform auftreten, in eine Ereignisprotokolldatendatei aufgezeichnet wird, die durch einen Systemadministrator überprüft werden kann, der die Betriebssystem-Software Windows NT verwendet. Diese Einrichtung ermöglicht es einem Systemadministrator ein Stück weit, eine Sicherheit von vorausgewählten Ereignissen zu überwachen. Die Ereignisprotokollierungsfunktion bei dem Betriebssystem Windows NT™ 4.0 liefert eine Systemüberwachung.

[0008] Hinsichtlich einer gesamten Sicherheit einer Computerplattform ist ein rein Software-basiertes System für einen Angriff verletzbar, z. B. durch Viren, von denen es Tausende von unterschiedlichen Varietäten gibt. Es sind mehrere proprietäre Virenfinde- und Korrigieranwendungen bekannt, z. B. das Virus-Toolkit-Programm Dr. Solomons™ oder die Antivirusausrüstung Norton™. Die Software Microsoft Windows NT™ 4.0 umfaßt eine Virenschutz-Software, die voreingestellt ist, um nach bekannten Viren zu suchen. Virenstämme entwickeln sich jedoch kontinuierlich und die Virenschutz-Software wird keinen verläßlichen Schutz gegen neuere unbekannte Viren geben. Es werden ständig neue Stämme von Viren entwickelt und in die Computer- und Internetumgebung freigegeben.

[0009] Bekannte Überwachungssysteme für Computerentitäten fokussieren auf Netzüberwachungsfunktionen, wo ein Administrator eine Netzwerkverwaltungs-Software verwendet, um ein Verhalten einer Mehrzahl von Netzwerkcomputern zu überwachen. Bei diesen bekannten Systemen liegt ein Vertrauen in das System nicht auf der Stufe eines einzelnen Vertrauens jeder Hardware-Einheit jeder Computerplattform in einem System, sondern stützt sich auf einen Netzwerkadministrator, der jeden Computer in dem Netzwerk überwacht. Bekannte Systeme können einen Betrieb von entfernten Computern nicht verifizieren, die mit unterschiedlichen Betriebssystemen in unterschiedlichen Netzwerken laufen, z. B. wie auf dieselben über das Internet zugegriffen wird.

[0010] Bei bekannten Systemen gibt es eine Schwierigkeit bei einem Einrichten eines Vertrauens zwischen einem Benutzer einer Rechenplattform und der Rechenplattform.

[0011] Eine allgemeine Erörterung einer Sicherheit bei Online-Banknetzwerken ist in Ferreira R: „The Practical Application of State of the Art Security in Real Environments", Proceedings of the International Conference on Cryptology – Auscrypt, DE, Berlin, Springer Bd. Conf. 1, 1990, S. 334–355, XP 000145211 ISBN: 3-540-53000-2, bereitgestellt. Ferreira beschreibt die Verwendung eines Sicherheitsservers in Verbindung mit einer Benutzer-Smartcard.

Zusammenfassung der Erfindung

[0012] Eine Aufgabe der vorliegenden Erfindung besteht darin, eine Computerentität zu schaffen, in die ein Benutzer einen hohen Grad an Vertrauen haben kann, daß die Computerentität nicht durch einen externen Einfluß verfälscht wurde und auf eine vorhersehbare und bekannte Weise wirksam ist.

[0013] Eine weitere Aufgabe der vorliegenden Erfindung besteht darin, eine Aufgabe eines Benutzers einer Computerentität zu vereinfachen, der beurteilt, ob die Vertrauenswürdigkeit der Computerentität ausreichend ist, um eine spezielle Aufgabe oder einen Satz von Aufgaben oder einen Typ einer Aufgabe durchzuführen, die durch den Benutzer verlangt wird.

[0014] Bei den spezifischen Ausführungsbeispielen ist der Benutzer mit einem vertrauenswürdigen Token-Gerät versehen, das tragbar und von einer Computerentität trennbar ist. Dem Token-Gerät wird durch den Benutzer vertraut, um zu verifizieren, daß eine Computerentität, die der Benutzer zu verwenden wünscht, vertrauenswürdig ist. In dem allgemeinen Fall ist das Token-Gerät nicht auf ein Verifizieren der Vertrauenswürdigkeit einer speziellen Computerentität beschränkt, sondern ist generisch, um mit einer jeglichen oder mehreren einer Mehrzahl von Computerentitäten wirksam zu sein.

[0015] Gemäß einem ersten Aspekt der vorliegenden Erfindung ist ein System einer Rechenvorrichtung bereitgestellt, das folgende Merkmale aufweist: eine Rechenplattform, die einen ersten Datenprozessor und eine erste Datenspeichereinrichtung aufweist; und ein Token-Gerät, das von der Rechenplattform physisch unterschiedlich und trennbar ist, dadurch gekennzeichnet, daß das System ferner eine Überwachungskomponente aufweist, die einen zweiten Datenprozessor und eine zweite Datenspeichereinrichtung aufweist, wobei die Überwachungskomponente konfiguriert ist, um eine Mehrzahl von Datenüberprüfungen bei der Rechenplattform durchzuführen, und wobei das Token-Gerät ferner von der Überwachungskomponente physisch unterschiedlich und trennbar ist; und wobei das Token-Gerät in einem Betriebsmodus wirksam ist, um eine Integritätsabfrage an die Überwachungskomponente zu richten, und das Token-Gerät keine spezifischen Schritte unternimmt, zu denen dasselbe in der Lage ist, wenn dasselbe keine zufriedenstellende Antwort auf die Integritätsabfrage empfängt.

[0016] Das Token-Gerät kann eine detaillierte Antwort auf die Integritätsabfrage empfangen und die Integritätsantwort verarbeiten, um die Integritätsantwort zu interpretieren.

[0017] Das System kann ferner einen Dritteilnehmerserver aufweisen, wobei eine Antwort auf die Integritätsabfrage zu dem Dritteilnehmerserver gesendet wird. Die Überwachungskomponente kann eine detaillierte Integritätsantwort zu dem Dritteilnehmerserver senden, falls dieselbe in der Integritätsabfrage durch das Token-Gerät aufgefordert wird. Die Überwachungskomponente kann eine detaillierte Integritätsantwort dem Token-Gerät berichten und das Token-Gerät kann die Integritätsantwort zu dem Dritteilnehmerserver senden, falls dasselbe den Dritteilnehmerserver benötigt, um die detaillierte Integritätsantwort interpretieren zu helfen. Der Dritteilnehmerserver kann die Integritätsantwort auf eine Form vereinfachen, in der das Token-Gerät die Integritätsantwort interpretieren kann. Der Dritteilnehmerserver kann die vereinfachte Integritätsantwort zu dem Token-Gerät senden. Das System kann ferner die Schritte eines Hinzufügens von Digitale-Signatur-Daten zu der vereinfachten Integritätsantwort betreiben, wobei die Digitale-Signatur-Daten den Dritteilnehmerserver dem Token-Gerät gegenüber authentifizieren.

[0018] Das Token-Gerät kann aufgefordert werden, eine Handlung zu unternehmen. Alternativ kann das Token-Gerät auffordern, eine Handlung zu unternehmen.

[0019] In einem Betriebsmodus kann das Token-Gerät Bilddaten zu der Computerplattform senden, falls die zufriedenstellende Antwort auf die Integritätsabfrage empfangen wird, und die Computerplattform kann die Bilddaten anzeigen.

[0020] Vorzugsweise ist die Überwachungskomponente zu einem Einrichten einer eigenen Identität in der Lage. Vorzugsweise weist das System ferner eine Schnittstelleneinrichtung zu einem Schnittstellenbilden zwischen der Überwachungskomponente und dem Token-Gerät auf. Vorzugsweise ist die Rechenentität konfiguriert, derart, daß die Überwachungskomponente die Datenüberprüfungen dem Token-Gerät berichtet, wobei die Datenüberprüfungen Daten enthalten, die einen Status der Computerplattform beschreiben.

[0021] Die spezifische Handlung kann ein Autorisieren der Rechenplattform aufweisen, eine Transaktion im Namen eines Benutzers des Systems zu unternehmen.

[0022] Es kann eine Schnittstelleneinrichtung zu einem Kommunizieren zwischen der Rechenplattform und dem Token-Gerät bereitgestellt sein, wobei die Schnittstelleneinrichtung mit der Überwachungskomponente kommuniziert, wobei die Rechenentität konfiguriert ist, derart, daß die Überwachungskomponente die Datenüberprüfungen dem Token-Gerät berichtet, wobei die Datenüberprüfungen Daten enthalten, die einen Status der Computerplattform beschreiben.

[0023] Vorzugsweise auf eine Kommunikation zwischen dem Token-Gerät und der Schnittstelleneinrichtung hin wird die Überwachungskomponente aktiviert, um eine Überwachungsoperation an der Computerplattform durchzuführen, bei der die Überwachungskomponente Daten erhält, die einen Betriebsstatus der Computerplattform beschreiben.

[0024] Die Schnittstelleneinrichtung ist bei einer bevorzugten Implementierung im wesentlichen ganz innerhalb der Überwachungskomponente gelegen. Bei einer alternativen Implementierung kann die Schnittstelleneinrichtung die Computerplattform aufweisen. Die Schnittstelleneinrichtung weist vorzugsweise einen PCSC-Stapel gemäß PCSC Workgroup PC/SC Specification 1.0 auf.

[0025] Die Überwachungskomponente kann eine Verifizierungseinrichtung aufweisen, die konfiguriert ist, um Zertifizierungsdaten zu erhalten, die die Statusdaten unabhängig zertifizieren, und um die Zertifizierungsdaten an die Schnittstelleneinrichtung zu liefern. Die Schnittstelleneinrichtung kann konfiguriert sein, um Daten gemäß einem proaktiven Protokoll zu senden und zu empfangen.

[0026] Gemäß einem zweiten Aspekt der vorliegenden Erfindung ist ein Verfahren gemäß Anspruch 29 bereitgestellt.

[0027] Die Überwachungsoperation kann folgende Schritte aufweisen: die Überwachungskomponente führt eine oder eine Mehrzahl von Datenüberprüfungen bei Komponenten der Rechenplattform aus; die Überwachungskomponente kann einen Satz von zertifizierten Referenzdaten zusammen mit den Datenüberprüfungen berichten.

[0028] Die zertifizierten Referenzdaten können einen Satz von Metriken umfassen, die zu erwarten sind, wenn bestimmte Komponenten der Rechenplattform gemessen werden, und Digital-Signatur-Daten umfassen, die eine Entität identifizieren, die die Referenzdaten zertifiziert.

[0029] Vorzugsweise weist der Schritt des Berichtens einer Verifizierung der Überwachungsoperation ein Senden eines Bestätigungssignals zu einem Token-Gerät auf, wobei das Bestätigungssignal ein Ergebnis der Überwachungsoperation beschreibt. Vorzugsweise werden die Integritätsdaten durch die Schnittstelle zu einem Token-Gerät außerhalb der Rechenentität gesendet.

[0030] Ein Ergebnis der Überwachungsoperation kann durch ein Erzeugen einer visuellen Anzeige von Bestätigungsdaten berichtet werden.

[0031] Das Verfahren kann ferner folgende Schritte aufweisen: Hinzufügen von Digitale-Signatur-Da-

ten zu den Integritätsdaten, wobei die Digital-Signatur-Daten die Überwachungskomponente identifizieren; Senden der Integritätsdaten und der Digitale-Signatur-Daten von der Schnittstelle.

[0032] Das Verfahren kann ferner einen Dritteilnehmerserver betreffen und kann eine Antwort auf eine Integritätsabfrage aufweisen, die zu dem Dritteilnehmerserver gesendet wird. Die Überwachungskomponente kann eine detaillierte Integritätsantwort zu dem Dritteilnehmerserver senden, falls dieselbe in der Integritätsabfrage durch das Token-Gerät aufgefordert wird. Die Überwachungskomponente kann dem Token-Gerät eine detaillierte Integritätsantwort berichten und das Token-Gerät kann die Integritätsantwort zu dem Dritteilnehmerserver senden, falls dasselbe den Dritteilnehmerserver benötigt, um die detaillierte Integritätsantwort zu interpretieren. Der Dritteilnehmerserver kann die Integritätsantwort zu einer Form vereinfachen, in der das Token-Gerät die Integritätsantwort interpretieren kann. Der Dritteilnehmerserver kann die vereinfachte Integritätsantwort zu dem Token-Gerät senden.

[0033] Das Verfahren kann ferner den Schritt eines Hinzufügens von Digitale-Signatur-Daten zu der vereinfachten Integritätsantwort betreiben, wobei die Digitale-Signatur-Daten den Dritteilnehmerserver dem Token-Gerät authentifizieren.

[0034] Das Token-Gerät kann aufgefordert werden, einen Schritt zu unternehmen. Alternativ kann das Token-Gerät auffordern, einen Schritt zu unternehmen.

[0035] Bei Ausführungsbeispielen kann ein Verfahren zu einem Überprüfen einer Integrität einer Operation einer Rechenentität bereitgestellt sein, wobei die Rechenentität eine Computerplattform, die eine erste Verarbeitungseinrichtung und eine erste Datenspeichereinrichtung aufweist, und eine Überwachungskomponente aufweist, die einen zweiten Prozessor und eine zweite Speichereinrichtung aufweist, mittels eines Token-Geräts, wobei das Token-Gerät einen dritten Datenprozessor und eine dritte Speichereinrichtung aufweist, wobei das Verfahren folgende Schritte aufweist: Programmieren des Token-Geräts, um auf ein empfangenes Abrufsignal von einem Anwendungsprogramm anzusprechen, wobei das Abrufsignal von der Computerplattform empfangen wird; wobei das Token-Gerät ein Abrufsignal von der Computerplattform empfängt; wobei das Token-Gerät ansprechend auf das empfangene Abrufsignal ein Signal zu einem Anfordern von Integritätsdaten durch die Überwachungskomponente erzeugt; und wobei die Überwachungskomponente Integritätsdaten der Computerplattform berichtet, ansprechend auf das empfangene Signal von dem Token-Gerät.

[0036] Gemäß einem dritten Aspekt der vorliegenden Erfindung ist ein Token-Gerät bereitgestellt, das einen Datenprozessor und ein Speichergerät aufweist, wobei das Token-Gerät konfiguriert ist, um eine Durchführung von zumindest einer Datenverarbeitungs- oder Signalisierungsfunktion zu erlauben:
dadurch gekennzeichnet, daß das Token-Gerät wirksam ist, um: eine Aufforderung von einem Element eines Rechensystems zu empfangen, um die zumindest eine Datenverarbeitungs- oder Signalisierungsfunktion durchzuführen; eine Anforderung nach Integritätsdaten von einer Überwachungskomponente in dem Rechensystem zu erzeugen, um die Integrität des Rechensystems zu bestätigen; die Integritätsdaten von der Überwachungskomponente zu empfangen; falls die Integritätsdaten, die dem Token-Gerät zugeführt werden, zufriedenstellend sind, dann erlaubt das Token-Gerät die Funktion; und falls die durch das Token-Gerät empfangenen Integritätsdaten unzufriedenstellend sind, dann verweigert das Token-Gerät die Funktion.

[0037] Das Token-Gerät kann ferner einen Datenprozessor aufweisen. Das Token-Gerät kann konfiguriert sein, um auf ein Abrufsignal anzusprechen, das gemäß PC/SC specification 1.0 wirksam ist. Das Token-Gerät kann zu einem Einleiten eines Befehls in der Lage sein, der durch einen Softwarestapel an der Computerentität gehandhabt werden soll, ansprechend auf das Abrufsignal gemäß einem proaktiven Protokoll.

[0038] Ausführungsbeispiele der Erfindung zeigen ein Verfahren zu einem Verifizieren eines Status einer Rechenentität mittels eines Token-Geräts, das außerhalb der Rechenentität bereitgestellt ist, wobei das Verfahren folgende Schritte aufweist: das Token-Gerät empfängt ein Abrufsignal; das Token-Gerät antwortet auf das Abrufsignal durch ein Bereitstellen einer Aufforderung zu einem Erhalten einer Verifizierung eines Zustands der Computerentität; und das Token-Gerät empfängt eine Ergebnisnachricht, wobei die Ergebnisnachricht das Ergebnis der Verifizierung beschreibt.

[0039] Das Verfahren kann ferner ein Senden einer Antwort auf die Integritätsabfrage zu dem Dritteilnehmerserver aufweisen. Die Überwachungskomponente kann eine detaillierte Integritätsantwort zu dem Dritteilnehmerserver senden, falls dieselbe durch das Token-Gerät in der Integritätsabfrage aufgefordert wird. Die Überwachungskomponente kann dem Token-Gerät eine detaillierte Integritätsantwort berichten, und das Token-Gerät kann die Integritätsantwort zu dem Dritteilnehmerserver senden, falls dasselbe den Dritteilnehmerserver benötigt, um die detaillierte Integritätsantwort interpretieren zu helfen. Der Dritteilnehmerserver kann die Integritätsantwort zu einer Form vereinfachen, in der das Token-Gerät die Integritätsantwort interpretieren kann. Der Dritteilneh-

merserver kann die vereinfachte Integritätsantwort zu dem Token-Gerät senden.

[0040] Das System kann ferner den Schritt eines Hinzufügens von Digitale-Signatur-Daten zu der vereinfachten Integritätsantwort betreiben, wobei die Digitale-Signatur-Daten den Dritteilnehmerserver dem Token-Gerät gegenüber authentifizieren.

[0041] Das Token-Gerät kann aufgefordert werden, einen Schritt zu unternehmen. Alternativ kann das Token-Gerät auffordern, einen Schritt zu unternehmen.

Kurze Beschreibung der Zeichnungen

[0042] Zu einem besseren Verständnis der Erfindung und um zu zeigen, wie dieselbe ausgeführt werden kann, werden nun lediglich durch ein Beispiel spezifische Ausführungsbeispiele, Verfahren und Prozesse gemäß der vorliegenden Erfindung mit Bezug auf die zugehörigen Zeichnungen beschrieben, in denen:

[0043] Fig. 1 ein Diagramm ist, das ein System darstellt, das zu einem Implementieren von Ausführungsbeispielen der vorliegenden Erfindung in der Lage ist;

[0044] Fig. 2 ein Diagramm ist, das eine Hauptplatine (Motherboard) darstellt, die ein vertrauenswürdiges Gerät umfaßt, das angeordnet ist, um über einen Smartcard-Leser mit einer Smartcard und mit einer Gruppe von Modulen zu kommunizieren;

[0045] Fig. 3 ein Diagramm ist, das das vertrauenswürdige Gerät detaillierter darstellt;

[0046] Fig. 4 ein Flußdiagramm ist, das die Schritte darstellt, die bei einem Gewinnen einer Integritätsmetrik der Rechenvorrichtung betroffen sind;

[0047] Fig. 5 ein Flußdiagramm ist, das die Schritte darstellt, die bei einem Einrichten von Kommunikationen zwischen einer vertrauenswürdigen Rechenplattform und einer entfernten Plattform betroffen sind, einschließlich eines Verifizierens der vertrauenswürdigen Plattform der Integrität derselben;

[0048] Fig. 6 ein Diagramm ist, das die Betriebsteile einer Benutzer-Smartcard zu einer Verwendung gemäß Ausführungsbeispielen der vorliegenden Erfindung darstellt:

[0049] Fig. 7 ein Flußdiagramm ist, das den Prozeß eines gegenseitigen Authentifizierens einer Smartcard und einer Host-Plattform darstellt;

[0050] Fig. 8 schematisch einen Satz von Prozeßschritten darstellt, die durch eine Smartcard und eine Rechenentität gemäß einem ersten Verwendungsmodell ausgeführt werden;

[0051] Fig. 9 schematisch einen zweiten Betriebsmodus der Rechenentität und der Smartcard darstellt, bei dem eine Anwendung eine Autorisierung von der Smartcard anfordert;

[0052] Fig. 10 schematisch eine Kommunikation zwischen der Smartcard und einem Schnittstellenmodul darstellt, das die Rechenentität aufweist;

[0053] Fig. 11 schematisch ein Rechensystem darstellt, das eine Rechenentität, ein Token-Gerät und einen entfernten vertrauenswürdigen Server aufweist, wobei das Token-Gerät eine Berechnung von verschlüsselten Integritätsmetriken an den vertrauenswürdigen Server dirigiert, um Informationen zu verifizieren, die von einer vertrauenswürdigen Komponente innerhalb einer Rechenentität empfangen werden;

[0054] Fig. 12 schematisch einen Betriebsmodus des Systems von Fig. 11 darstellt, bei dem Integritätsmetrikdaten von einer vertrauenswürdigen Komponente zu einem Token-Gerät gesendet werden und das Token-Gerät dann die Daten zu einem vertrauenswürdigen Server zu einer Datenverarbeitung sendet, gemäß einem dritten Betriebsmodus;

[0055] Fig. 13 schematisch eine weitere spezifische Ausführungsbeispielsimplementierung eines Systems gemäß der vorliegenden Erfindung darstellt, wobei eine herkömmliche PCSC-Technologie verwendet wird, um mit einer Smartcard zu kommunizieren, und wobei die Smartcard in der Lage ist, eine Autorisierung für eine Transaktion zu einem bekannten Anwendungsprogramm zu geben, das durch eine Teilsystem-Schnittstelle zu einer vertrauenswürdigen Komponente wirksam ist; und

[0056] Fig. 14 schematisch eine Operation des in **Fig.** 15 gezeigten Ausführungsbeispiels darstellt, wobei es einer Smartcard ermöglicht ist, eine Autorisierung für eine Transaktion zu erlauben, nachdem dieselbe eine Bestätigung eines vertrauenswürdigen Zustands einer Computerentität empfangen hat, mit der dieselbe zusammenwirkt.

Detaillierte Beschreibung des besten Modus zu einem Ausführen der Erfindung

[0057] Es wird nun durch ein Beispiel ein durch die Erfinder betrachteter bester Modus zum Ausführen der Erfindung zusammen mit alternativen Ausführungsbeispielen beschrieben. In der folgenden Beschreibung sind zahlreiche spezifische Details dargelegt, um ein genaues Verständnis der vorliegenden Erfindung zu liefern. Einem Fachmann auf dem Gebiet ist jedoch klar, daß die vorliegende Erfindung oh-

ne Begrenzung auf diese spezifischen Details praktiziert werden kann. In anderen Fällen wurden gut bekannte Verfahren und Strukturen nicht detailliert beschrieben, um die vorliegende Erfindung nicht unnötigerweise undeutlich zu machen.

[0058] Spezifische Implementierungen der vorliegenden Erfindung weisen eine Computerplattform, die eine Verarbeitungseinrichtung und eine Speichereinrichtung aufweist, und eine Überwachungskomponente auf, die physisch der Computerplattform zugeordnet ist und hierin im folgenden als eine „vertrauenswürdige Komponente" (oder „vertrauenswürdiges Gerät") bekannt ist, die eine Operation der Computerplattform durch ein Sammeln von Metrikdaten von der Computerplattform überwacht und zu einem Verifizieren der korrekten Funktionsweise der Computerplattform zu anderen Entitäten in der Lage ist, die mit der Computerplattform in Wechselwirkung stehen. Ein Token-Gerät, das für einen menschlichen Benutzer einer Computerplattform persönlich sein kann, steht in Wechselwirkung mit einer vertrauenswürdigen Komponente, die der Computerplattform zugeordnet ist, um dem menschlichen Benutzer die Vertrauenswürdigkeit der Computerplattform zu verifizieren.

[0059] Ein Benutzer einer Rechenentität richtete durch eine Verwendung eines derartigen vertrauenswürdigen Token-Geräts einen Pegel eines Vertrauens zu der Computerentität ein. Das vertrauenswürdige Token-Gerät ist ein persönliches und tragbares Gerät, das eine Datenverarbeitungsfähigkeit aufweist und in das der Benutzer einen hohen Pegel eines Vertrauens hat. Das vertrauenswürdige Token-Gerät kann folgende Funktionen durchführen:

- Verifizieren einer korrekten Operation einer Rechenplattform auf eine Weise, die dem Benutzer ohne weiteres augenscheinlich ist, z. B. durch Audio oder eine visuelle Anzeige;
- Abfragen einer Überwachungskomponente, um einen Beweis einer korrekten Operation einer Computerplattform bereitzustellen, der die Überwachungskomponente zugeordnet ist; und
- Einrichten eines Pegels einer Wechselwirkung des Token-Geräts mit einer Rechenplattform, abhängig davon, ob eine Überwachungskomponente einen zufriedenstellenden Beweis einer korrekten Operation der Computerentität bereitgestellt hat, und Vorenthalten spezifischer Wechselwirkungen mit der Computerentität, falls ein derartiger Beweis einer korrekten Operation nicht durch das Token-Gerät empfangen wird.

[0060] Das Token-Gerät kann aufgefordert werden, einen Schritt zu unternehmen, z. B. durch eine Anwendung, die auf der Rechenplattform gelegen ist, oder durch eine entfernte Anwendung, oder alternativ kann das Token-Gerät selbst eine Handlung einleiten.

[0061] In dieser Beschreibung wird der Begriff „vertrauenswürdig", wenn derselbe in Bezug auf eine physische oder logische Komponente verwendet wird, verwendet, um zu bedeuten, daß die physische oder logische Komponente sich immer auf eine erwartete Weise verhält. Das Verhalten dieser Komponente ist vorhersehbar und bekannt. Vertrauenswürdige Komponenten weisen einen hohen Grad eines Widerstands gegen eine unbefugte Modifikation auf.

[0062] In dieser Beschreibung wird der Ausdruck „Computerentität" verwendet, um eine Computerplattform und eine Überwachungskomponente zu beschreiben.

[0063] In dieser Beschreibung wird der Ausdruck „Computerplattform" verwendet, um auf zumindest einen Datenprozessor und zumindest eine Datenspeichereinrichtung Bezug zu nehmen, gewöhnlicherweise, aber nicht notwendigerweise, mit zugeordneten Kommunikationseinrichtungen, z. B. einer Mehrzahl von Treibern, zugeordneten Anwendungen und Datendateien, und die zu einem in Wechselwirkung Treten mit externen Entitäten in der Lage sind, z. B. einem Benutzer oder einer anderen Computerplattform, z. B. mittels einer Verbindung mit dem Internet, einer Verbindung mit einem externen Netzwerk oder durch ein Aufweisen eines Eingangstors, das zu einem Empfangen von Daten in der Lage ist, die auf einem Datenspeichermedium gespeichert sind, z. B. einer CD-Rom, einer Diskette, einem Bandstreifen oder dergleichen. Der Ausdruck „Computerplattform" umfaßt die Hauptdatenverarbeitungs- und Speichereinrichtung einer Computerentität.

[0064] Durch eine Verwendung einer vertrauenswürdigen Komponente bei jeder Rechenentität ist ein Pegel eines Vertrauens zwischen unterschiedlichen Rechenplattformen ermöglicht. Es ist möglich, eine derartige Plattform über einen Zustand derselben abzufragen und denselben mit einem vertrauenswürdigen Zustand zu vergleichen, entweder entfernt oder durch einen Monitor an der Computerentität. Die durch eine derartige Abfrage gesammelten Informationen werden durch die vertrauenswürdige Komponente der Computerentität bereitgestellt, die die verschiedenen Parameter der Plattform überwacht. Informationen, die durch die vertrauenswürdige Komponente bereitgestellt sind, können durch eine kryptographische Authentifizierung authentifiziert sein und es kann denselben vertraut werden.

[0065] Das Vorhandensein der vertrauenswürdigen Komponente macht es einem Stück einer Dritteilnehmer-Software möglich, entweder entfernt oder lokal zu der Computerentität, mit der Computerentität zu kommunizieren, um einen Nachweis der Authentizität und Identität derselben zu erhalten und gemessene Integritätsmetriken dieser Rechenentität wiederzuerlangen. Die Dritteilnehmer-Software kann dann die

von der vertrauenswürdigen Komponente erhaltenen Metriken mit erwarteten Metriken vergleichen, um zu bestimmen, ob ein Zustand der abgefragten Rechenentität für die Wechselwirkungen geeignet ist, die die Dritteilnehmer-Softwareeinheit mit der Rechenentität herzustellen versucht, z. B. Handelstransaktionsprozesse.

[0066] Dieser Typ einer Integritätsverifizierung zwischen Rechenentitäten funktioniert im Kontext einer Dritteilnehmer-Software gut, die mit einer vertrauenswürdigen Komponente einer Rechenentität kommuniziert, aber stellt keine Einrichtung für einen menschlichen Benutzer bereit, um einen Pegel einer vertrauenswürdigen Wechselwirkung mit der Rechenentität desselben oder einer jeglichen anderen Rechenentität zu gewinnen, mit der diese Person mittels einer Benutzerschnittstelle in Wechselwirkung treten kann.

[0067] Bei einer hierin beschriebenen bevorzugten Implementierung wird ein vertrauenswürdiges Token-Gerät durch einen Benutzer verwendet, um eine vertrauenswürdige Komponente einer Rechenentität abzufragen und dem Benutzer über den Zustand der Rechenentität zu berichten, wie es durch die vertrauenswürdige Komponente verifiziert wird.

[0068] Nun wird eine „vertrauenswürdige Plattform" beschrieben, die bei bevorzugten Ausführungsbeispielen der Erfindung verwendet wird. Dies ist durch die Eingliederung in eine Rechenplattform eines physisch vertrauenswürdigen Geräts erreicht, dessen Funktion es ist, die Identität der Plattform an zuverlässig gemessene Daten zu binden, die eine Integritätsmetrik der Plattform liefern. Die Identität und die Integritätsmetrik werden mit erwarteten Werten verglichen, die durch einen vertrauenswürdigen Teilnehmer (TP = Trusted Party) bereitgestellt werden, der präpariert ist, um für die Vertrauenswürdigkeit der Plattform zu bürgen. Falls es eine Übereinstimmung gibt, ist die Folgerung, daß zumindest ein Teil der Plattform korrekt wirksam ist, abhängig von dem Bereich der Integritätsmetrik.

[0069] Ein Benutzer verifiziert die korrekte Operation der Plattform vor einem Austauschen anderer Daten mit der Plattform. Ein Benutzer macht dies durch ein Auffordern des vertrauenswürdigen Geräts, um eine Identität desselben und eine Integritätsmetrik zu liefern. (Wahlweise weigert sich das vertrauenswürdige Gerät, einen Identitätsbeweis zu liefern, falls es selbst nicht in der Lage war, eine korrekte Operation der Plattform zu verifizieren.) Der Benutzer empfängt den Nachweis einer Identität und die Identitätsmetrik und vergleicht dieselben mit Werten, die derselbe für echt hält. Diese ordnungsgemäßen Werte werden durch den TP oder eine andere Entität geliefert, der durch den Benutzer vertraut wird. Falls Daten, die durch das vertrauenswürdige Gerät berichtet werden, die gleichen sind, wie dieselben, die durch den TP geliefert werden, vertraut der Benutzer der Plattform. Dies ist so, weil der Benutzer der Entität vertraut. Die Entität vertraut der Plattform, weil dieselbe vorhergehend die Identität validiert hat und die ordnungsgemäße Integritätsmetrik der Plattform bestimmt hat.

[0070] Wenn ein Benutzer eine vertrauenswürdige Operation der Plattform eingerichtet hat, tauscht derselbe andere Daten mit der Plattform aus. Bei einem lokalen Benutzer kann der Austausch durch ein in Wechselwirkung Treten mit einer gewissen Software-Anwendung sein, die auf der Plattform läuft. Bei einem entfernten Benutzer könnte der Austausch eine sichere Transaktion betreffen. In einem anderen Fall werden die ausgetauschten Daten durch das vertrauenswürdige Gerät „signiert". Der Benutzer kann dann ein größeres Vertrauen haben, daß Daten mit einer Plattform ausgetauscht werden, deren Verhalten zu trauen ist.

[0071] Das vertrauenswürdige Gerät verwendet kryptographische Prozesse, aber liefert diesen kryptographischen Prozessen nicht notwendigerweise eine externe Schnittstelle. Eine am meisten erwünschte Implementierung würde ferner das vertrauenswürdige Gerät gegen Eingriffe gesichert machen, um Geheimnisse durch ein Unzugreifbarmachen derselben für andere Plattformfunktionen zu schützen und eine Umgebung bereitzustellen, die im wesentlichen immun gegen eine unbefugte Modifikation ist. Da ein Sichern gegen Eingriffe unmöglich ist, ist die beste Annäherung ein vertrauenswürdiges Gerät, das gegen Eingriffe resistent ist oder Eingriffe erfaßt. Das vertrauenswürdige Gerät besteht daher vorzugsweise aus einer physischen Komponente, die gegen Eingriffe resistent ist.

[0072] Für eine Resistenz gegen Eingriffe relevante Techniken sind Fachleuten auf dem Gebiet einer Sicherheit gut bekannt. Diese Techniken umfassen Verfahren zu einem Widerstehen eines Eingreifens (wie beispielsweise eine geeignete Verkapselung des vertrauenswürdigen Geräts), Verfahren zu einem Erfassen eines Eingreifens (wie beispielsweise eine Erfassung nicht einer Spezifikation entsprechender Spannungen, Röntgenstrahlen, oder ein Verlust einer physischen Integrität bei der Verkleidung des vertrauenswürdigen Geräts), und Verfahren zu einem Eliminieren von Daten, wenn ein Eingreifen erfaßt wird. Eine weitere Erörterung von geeigneten Techniken kann unter http://www.cl.cam.ac.uk/~mgk25/tamper.html gefunden werden. Es sei darauf hingewiesen, daß, obwohl ein Sichern gegen Eingriffe ein höchst erwünschtes Merkmal der vorliegenden Erfindung ist, dasselbe nicht in die normale Operation der Erfindung eintritt und an sich jenseits des Schutzbereichs der vorliegenden Erfindung ist und hierin nicht detailliert beschrieben wird.

[0073] Das vertrauenswürdige Gerät ist vorzugsweise ein physisches, da dasselbe schwierig zu fälschen sein muß. Am bevorzugtesten ist dasselbe resistent gegen Eingriffe, da dasselbe schwer nachzumachen sein muß. Dasselbe weist typischerweise eine Maschine auf, die zu einem Verwenden von kryptographischen Prozessen in der Lage ist, da es erforderlich ist, eine Identität sowohl lokal als auch bei einem Abstand nachzuweisen, und dasselbe enthält zumindest ein Verfahren zu einem Messen einer gewissen Integritätsmetrik der Plattform, der dasselbe zugeordnet ist.

[0074] Eine vertrauenswürdige Plattform **10** ist in dem Diagramm in Fig. 1 dargestellt. Die Plattform **10** umfaßt die Standardmerkmale einer Tastatur **14** (die eine Bestätigungstaste eines Benutzers bereitstellt), eine Maus **16** und einen Monitor **18**, die die physische „Benutzerschnittstelle" der Plattform bereitstellen. Dieses Ausführungsbeispiel einer vertrauenswürdigen Plattform enthält ferner einen Smartcard-Leser **12**. Neben dem Smartcard-Leser **12** ist eine Smartcard **19** dargestellt, um eine vertrauenswürdige Benutzerwechselwirkung mit der vertrauenswürdigen Plattform zu erlauben, wie es weiter unten beschriebne werden soll. In der Plattform **10** gibt es eine Mehrzahl von Modulen **15**: diese sind andere funktionale Elemente der vertrauenswürdigen Plattform von im wesentlichen einer jeglichen für diese Plattform geeigneten Art. Die funktionale Signifikanz derartiger Elemente ist nicht für die vorliegende Erfindung relevant und wird hierin nicht weiter erörtert. Zusätzliche Komponenten der vertrauenswürdigen Computerentität umfassen typischerweise eines oder mehrere Lokales-Netzwerk-(LAN-)Tore, eines oder mehrere Modem-Tore und eine oder mehrere Leistungsversorgungen, Kühllüfter und dergleichen.

[0075] Wie es in Fig. 2 dargestellt ist, umfaßt die Hauptplatine **20** der vertrauenswürdigen Rechenplattform **10** (unter anderen Standardkomponenten) einen Hauptprozessor **21**, einen Hauptspeicher **22**, ein vertrauenswürdiges Gerät **24**, einen Datenbus **26** und jeweilige Steuerleitungen **27** und Leitungen **28**, einen BIOS-Speicher **29**, der das BIOS-Programm für die Plattform **10** enthält, und ein Eingabe/Ausgabe-(IO = Input/Output) Gerät **23**, das die Wechselwirkung zwischen den Komponenten der Hauptplatine und dem Smartcard-Leser **12**, der Tastatur **14**, der Maus **16** und dem Monitor **18** (und jeglichen zusätzlichen Peripheriegeräten, wie beispielsweise einem Modem, einem Drucker, einem Scanner oder dergleichen) steuert. Der Hauptspeicher **22** ist typischerweise ein Direktzugriffsspeicher (RAM). In Betrieb lädt die Plattform **10** das Betriebssystem, z. B. Windows NT™, von einer Festplatte (nicht gezeigt) in den RAM. Zusätzlich lädt in Betrieb die Plattform **10** die Prozesse oder Anwendungen, die durch die Plattform **10** ausgeführt werden können, von einer Festplatte (nicht gezeigt) in den RAM.

[0076] Die Computerentität kann als eine logische wie auch eine physische Architektur aufweisend betrachtet werden. Die logische Architektur weist eine gleiche grundlegende Teilung zwischen der Computerplattform und der vertrauenswürdigen Komponente auf, wie dieselbe bei der hierin in Fig. 1 bis Fig. 4 beschriebenen physischen Architektur vorliegt. Das heißt, die vertrauenswürdige Komponente ist logisch verschieden von der Computerplattform, mit der dieselbe physisch verwandt ist. Die Computerentität weist einen Benutzerraum, der ein logischer Raum ist, der physisch auf der Computerplattform (dem ersten Prozessor und der ersten Datenspeichereinrichtung) gelegen ist, und einen Vertrauenswürdige-Komponente-Raum auf, der ein logischer Raum ist, der physisch auf der vertrauenswürdigen Komponente gelegen ist. In dem Benutzerraum befinden sich eine oder eine Mehrzahl von Treibern, eines oder eine Mehrzahl von Anwendungsprogrammen, ein Dateispeicherbereich; ein Smartcard-Leser; eine Smartcard-Schnittstelle; und ein Software-Agent, der in dem Benutzerraum Operationen durchführen und zurück zu der vertrauenswürdigen Komponente berichten kann. Der Vertrauenswürdige-Komponente-Raum ist ein logischer Bereich, der auf der vertrauenswürdigen Komponente basiert und physisch in derselben gelegen ist, unterstützt durch den zweiten Datenprozessor und den zweiten Speicherbereich der vertrauenswürdigen Komponente. Der Monitor **18** empfängt Bilder direkt von dem Vertrauenswürdige-Komponente-Raum. Außerhalb der Computerentität befinden sich externe Kommunikationsnetzwerke, z. B. das Internet, und verschiedene lokale Netze, weite Netze, die über die Treiber (die eines oder mehrere Modemtore umfassen können) mit dem Benutzerraum verbunden sind. Eine externe Benutzersmartcard wird in einen Smartcard-Leser in dem Benutzerraum eingegeben.

[0077] Bei einem Personalcomputer ist das BIOS-Programm typischerweise in einem speziellen reservierten Speicherbereich positioniert, die oberen 64K des ersten Megabytes machen den Systemspeicher (Adressen FØØØH bis FFFFh), und der Hauptprozessor ist angeordnet, um zuerst zu dieser Speicherposition zu sehen, gemäß einem industrieweiten Standard.

[0078] Der erhebliche Unterschied zwischen der Plattform und einer herkömmlichen Plattform besteht darin, daß nach einer Rücksetzung der Hauptprozessor anfänglich durch das vertrauenswürdige Gerät gesteuert wird, das dann eine Steuerung dem plattformspezifischen BIOS-Programm übergibt, das wiederum alle Eingabe-/Ausgabe-Geräte wie normal initialisiert. Nachdem das BIOS-Programm ausgeführt hat, wird eine Steuerung durch das BIOS-Programm wie normal einem Betriebssystemprogramm übergeben, wie beispielsweise Windows NT (TM), das typi-

scherweise von einem Festplattenlaufwerk (nicht gezeigt) in den Hauptspeicher **22** geladen wird.

[0079] Natürlich erfordert diese Änderung von der normalen Prozedur eine Modifikation an der Implementierung des Industriestandards, wodurch der Hauptprozessor **21** angewiesen wird, das vertrauenswürdige Gerät **24** zu adressieren, um erste Befehle desselben zu empfangen. Diese Änderung kann einfach durch eine feste Codierung einer unterschiedlichen Adresse in den Hauptprozessor **21** vorgenommen werden. Alternativ kann dem vertrauenswürdigen Gerät **24** die Standard-BIOS-Programmadresse zugewiesen werden, wobei es in diesem Fall keinen Bedarf gibt, die Hauptprozessorkonfiguration zu modifizieren.

[0080] Es ist höchst erwünscht, daß der BIOS-Boot-Block innerhalb des vertrauenswürdigen Geräts **24** enthalten ist. Dies verhindert eine Untergrabung des Erhaltens der Integritätsmetrik (was andernfalls auftreten könnte, falls schurkische Software-Prozesse vorliegen) und verhindert, daß schurkische Software-Prozesse eine Situation erzeugen, in der das BIOS (sogar falls korrekt) versäumt, die ordnungsgemäße Umgebung für das Betriebssystem zu bauen.

[0081] Obwohl bei dem bevorzugten Ausführungsbeispiel, das beschrieben werden soll, das vertrauenswürdige Gerät **24** eine einzige, diskrete Komponente ist, ist es klar, daß die Funktionen des vertrauenswürdigen Geräts **24** alternativ in mehrere Geräte auf der Hauptplatine geteilt oder sogar in eines oder mehrere der existierenden Standardgeräte der Plattform integriert werden können. Es ist z. B. machbar, eine oder mehrere der Funktionen des vertrauenswürdigen Geräts in den Hauptprozessor selbst zu integrieren, vorausgesetzt, daß die Funktionen und Kommunikationen derselben nicht untergraben werden können. Dies würde jedoch wahrscheinlich getrennte Anschlußleitungen an dem Prozessor zu einer alleinigen Verwendung durch die vertrauenswürdigen Funktionen erfordern. Obwohl bei dem vorliegenden Ausführungsbeispiel das vertrauenswürdige Gerät ein Hardware-Gerät ist, das zu einer Integration in die Hauptplatine **20** angepaßt ist, wird zusätzlich oder alternativ erwartet, daß ein vertrauenswürdiges Gerät als ein „entfernbares" Gerät, wie beispielsweise eine Kopierschutzschaltung, implementiert sein kann, das an einer Plattform angebracht werden kann, wenn erforderlich. Ob das vertrauenswürdige Gerät integriert oder entfernbar ist, ist eine Frage einer Entwurfsauswahl. Wo jedoch das vertrauenswürdige Gerät trennbar ist, sollte ein Mechanismus zu einem Bereitstellen einer logischen Bindung zwischen dem vertrauenswürdigen Gerät und der Plattform vorhanden sein.

[0082] Das vertrauenswürdige Gerät **24** weist eine Anzahl von Blöcken auf, wie es in Fig. 3 dargestellt ist. Nach einer Systemrücksetzung führt das vertrauenswürdige Gerät **24** einen sicheren Boot-Prozeß durch, um sicherzustellen, daß das Betriebssystem der Plattform **10** (einschließlich des Systemtakts und der Anzeige auf dem Monitor) ordnungsgemäß und auf eine sichere Weise läuft. Während des sicheren Boot-Prozesses erlangt das vertrauenswürdige Gerät **24** eine Integritätsmetrik der Rechenplattform **10**. Das vertrauenswürdige Gerät **24** kann ferner einen sicheren Datentransfer und z. B. eine Authentifizierung zwischen demselben und einer Smartcard über eine Verschlüsselung/Entschlüsselung und Signatur/Verifizierung durchführen. Das vertrauenswürdige Gerät **24** kann ferner verschiedene Sicherheitssteuerrichtlinien durchsetzen, wie beispielsweise ein Verriegeln der Benutzerschnittstelle.

[0083] Genau gesagt, weist das vertrauenswürdige Gerät folgende Merkmale auf: eine Steuerung **30**, die programmiert ist, um die gesamte Operation des vertrauenswürdigen Geräts **24** zu steuern und mit den anderen Funktionen auf dem vertrauenswürdigen Gerät **24** und mit den anderen Geräten auf der Hauptplatine **20** in Wechselwirkung zu treten; eine Messungsfunktion **31** zu einem Erlangen der Integritätsmetrik von der Plattform **10**; eine kryptographische Funktion **32** zu einem Signieren, Verschlüsseln oder Entschlüsseln von spezifizierten Daten; eine Authentifizierungsfunktion **33** zu einem Authentifizieren einer Smartcard; und eine Schnittstellenschaltungsanordnung **34**, die geeignete Tore (**36**, **37** & **38**) zu einem Verbinden des vertrauenswürdigen Geräts **24** jeweils mit dem Datenbus **26**, Steuerleitungen **27** und Adreßleitungen **28** der Hauptplatine **20** aufweist. Jeder der Blöcke in dem vertrauenswürdigen Gerät **24** weist einen Zugriff (typischerweise über die Steuerung **30**) auf geeignete flüchtige Speicherbereiche **4** und/oder nicht-flüchtige Speicherbereiche **3** des vertrauenswürdigen Geräts **24** auf. Zusätzlich ist das vertrauenswürdige Gerät **24** auf eine bekannte Weise entworfen, um gegen Eingriffe resistent zu sein.

[0084] Aus Leistungsgründen kann das vertrauenswürdige Gerät **24** als eine anwendungsspezifische integrierte Schaltung (ASIC = Application Specific Integrated Circuit) implementiert sein. Zu einer Flexibilität ist das vertrauenswürdige Gerät **24** jedoch vorzugsweise eine geeignet programmierte Mikrosteuerung. Sowohl ASICs als auch Mikrosteuerungen sind auf dem Gebiet der Mikroelektronik gut bekannt und werden hierin nicht detaillierter betrachtet.

[0085] Ein in dem nicht-flüchtigen Speicher **3** des vertrauenswürdigen Geräts **24** gespeichertes Datenelement ist ein Zertifikat **350**. Das Zertifikat **350** enthält zumindest einen öffentlichen Schlüssel **351** des vertrauenswürdigen Geräts **24** und einen authentifizierten Wert 352 der durch einen vertrauenswürdigen Teilnehmer (TP = Trusted Party) gemessenen Plattformintegritätsmetrik. Das Zertifikat **350** wird

durch den TP unter Verwendung des privaten Schlüssels des TP signiert, bevor dasselbe in dem vertrauenswürdigen Gerät **24** gespeichert wird. Bei späteren Kommunikationssitzungen kann ein Benutzer der Plattform **10** die Integrität der Plattform **10** durch ein Vergleichen der gewonnenen Integritätsmetrik mit der authentischen Integritätsmetrik **352** verifizieren. Falls es eine Übereinstimmung gibt, kann der Benutzer sicher sein, daß die Plattform **10** nicht untergraben wurde. Eine Kenntnis des allgemein verfügbaren öffentlichen Schlüssels des TPs ermöglicht eine einfache Verifizierung des Zertifikats **350**. Der nichtflüchtige Speicher **35** enthält ferner ein Identitäts-(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 zu einem Indexieren und Etikettieren von Daten verwendet, die für das vertrauenswürdige Gerät **24** relevant sind, aber ist an sich ungenügend, um die Identität der Plattform **10** unter vertrauenswürdigen Bedingungen nachzuweisen.

[0086] Das vertrauenswürdige Gerät **24** ist zumindest mit einem Verfahren zu einem zuverlässigen Messen oder Gewinnen der Integritätsmetrik der Rechenplattform **10** ausgerüstet, der dasselbe zugeordnet ist. Bei dem vorliegenden Ausführungsbeispiel wird die Integritätsmetrik durch die Messungsfunktion **31** durch ein Erzeugen eines Auszugs der BIOS-Befehle in dem BIOS-Speicher gewonnen. Eine derartige gewonnene Integritätsmetrik, falls dieselbe wie oben beschrieben verifiziert ist, gibt einem möglichen Benutzer der Plattform **10** einen hohen Pegel eines Vertrauens, daß die Plattform **10** nicht bei einem Hardware- oder BIOS-Programm-Pegel untergraben wurde. Andere bekannte Prozesse, z. B. Virenprüfer, sind typischerweise zur Stelle, um zu überprüfen, daß das Betriebssystem und der Anwendungsprogrammcode nicht untergraben wurden.

[0087] Die Messungsfunktion **31** weist einen Zugriff auf folgende Merkmale auf: den nicht-flüchtigen Speicher **3** zu einem Speichern eines Hash-Programms **354** und eines privaten Schlüssels **355** des vertrauenswürdigen Geräts **24** und auf den flüchtigen Speicher **4** zu einem Speichern einer gewonnenen Integritätsmetrik in der Form eines Auszugs **361**. Bei geeigneten Ausführungsbeispielen kann der flüchtige Speicher **4** ferner verwendet werden, um die öffentlichen Schlüssel und zugeordneten ID-Etiketten **360a**–**360n** von einer oder mehreren authentischen Smartcards **19s** zu speichern, die verwendet werden können, um einen Zugriff auf die Plattform **10** zu erlangen.

[0088] Bei einer bevorzugten Implementierung umfaßt die Integritätsmetrik wie auch der Auszug einen Booleschen Wert, der in dem flüchtigen Speicher **4** durch die Messungsfunktion **31** aus Gründen gespeichert ist, die ersichtlich werden.

[0089] Ein bevorzugter Prozeß zu einem Gewinnen einer Integritätsmetrik wird nun mit Bezug auf Fig. 4 beschrieben.

[0090] Bei einem Schritt **400** überwacht bei einem Einschalten die Messungsfunktion **31** die Aktivität des Hauptprozessors **21** an den Daten, Steuer- und Adreßleitungen (**26**, **27** & **28**), um zu bestimmen, ob das vertrauenswürdige Gerät **24** der erste Speicher ist, auf den zugegriffen wird. Unter einer herkömmlichen Operation würde ein Hauptprozessor zuerst zu dem BIOS-Speicher gerichtet werden, um das BIOS-Programm auszuführen. Gemäß dem vorliegenden Ausführungsbeispiel wird der Hauptprozessor **21** jedoch zu dem vertrauenswürdigen Gerät **24** gerichtet, das als ein Speicher wirkt. Falls bei einem Schritt **405** das vertrauenswürdige Gerät **24** der erste Speicher ist, auf den zugegriffen wird, schreibt die Messungsfunktion **31** in einem Schritt **410** einen Booleschen Wert zu dem flüchtigen Speicher **3**, der angibt, daß das vertrauenswürdige Gerät **24** der erste Speicher war, auf den zugegriffen wurde. Andernfalls schreibt die Messungsfunktion bei einem Schritt **415** einen Booleschen Wert, der angibt, daß das vertrauenswürdige Gerät **24** nicht der erste Speicher war, auf den zugegriffen wurde.

[0091] Falls auf das vertrauenswürdige Gerät **24** nicht zuerst zugegriffen wurde, besteht natürlich eine Möglichkeit, daß auf das vertrauenswürdige Gerät **24** überhaupt nicht zugegriffen wird. Dies wäre z. B. der Fall, falls der Hauptprozessor **21** manipuliert wäre, um zuerst das BIOS-Programm auszuführen. Unter diesen Umständen wäre die Plattform wirksam, aber wäre nicht in der Lage, die Integrität derselben auf verlangen zu verifizieren, da die Integritätsmetrik nicht verfügbar wäre. Falls ferner auf das vertrauenswürdige Gerät **24** zugegriffen würde, nachdem auf das BIOS-Programm zugegriffen wurde, würde der Boolesche Wert klar ein Fehlen einer Integrität der Plattform angeben.

[0092] Wenn (oder falls) bei einem Schritt **420** durch den Hauptprozessor **21** auf dieselbe als ein Speicher zugegriffen wird, liest der Hauptprozessor **21** bei einem Schritt **425** die gespeicherten systemspezifischen Hash-Befehle **354** aus der Messungsfunktion **31**. Die Hash-Befehle **354** werden durch den Hauptprozessor **21** über den Datenbus **26** zu einem Verarbeiten übermittelt. Bei einem Schritt **430** führt der Hauptprozessor **21** die Hash-Befehle **354** aus und verwendet dieselben bei einem Schritt **435**, um einen Auszug des BIOS-Speichers **29** zu berechnen, durch ein Lesen der Inhalte des BIOS-Speichers **29** und ein Verarbeiten dieser Inhalte gemäß dem Hash-Programm. Bei einem Schritt **440** schreibt der Hauptprozessor **21** den berechneten Auszug **361** zu der geeigneten Nicht-Flüchtiger-Speicher-Position **4** in dem vertrauenswürdigen Gerät **24**. Die Messungsfunktion **31** ruft dann bei einem Schritt **445** das BIOS-Pro-

gramm in dem BIOS-Speicher **29** an und eine Ausführung geht auf eine herkömmliche Weise weiter.

[0093] Natürlich gibt es eine Anzahl von unterschiedlichen Weisen, auf die die Integritätsmetrik berechnet werden kann, abhängig von dem Bereich des erforderlichen Vertrauens. Die Messung der Integrität des BIOS-Programms liefert eine grundlegende Überprüfung der Integrität einer einer Plattform zugrundeliegenden Verarbeitungsumgebung. Die Integritätsmetrik sollte von einer derartigen Form sein, daß dieselbe ein Erörtern der Gültigkeit des Boot-Prozesses ermöglicht – der Wert der Integritätsmetrik kann verwendet werden, um zu verifizieren, ob die Plattform unter Verwendung des korrekten BIOS gebootet hat. Wahlweise könnten einzelne Funktionsblöcke innerhalb des BIOS ihre eigenen Auszugswerte aufweisen, wobei ein Gesamt-BIOS-Auszug ein Auszug dieser einzelnen Auszüge ist. Dies ermöglicht es einer Taktikeinheit, auszusagen, welche Teile einer BIOS-Operation zu einem beabsichtigten Zweck entscheidend sind und welche irrelevant sind (wobei in diesem Fall die einzelnen Auszüge auf eine derartige Weise gespeichert werden müssen, daß eine Gültigkeit einer Operation unter der Richtlinie eingerichtet werden kann).

[0094] Andere Integritätsprüfungen könnten ein Einrichten betreffen, daß verschiedene andere Geräte, Komponenten oder Vorrichtungen, die an der Plattform angebracht sind, vorhanden und in einer korrekten Arbeitsreihenfolge sind. Bei einem Beispiel könnten die BIOS-Programme, die einer SCSI-Steuerung zugeordnet sind, verifiziert werden, um sicherzustellen, daß Kommunikationen mit einer Peripherieausrüstung vertraut werden könnte. Bei einem anderen Beispiel könnte die Integrität von anderen Geräten, z. B. Speichergeräten oder Co-Prozessoren, auf der Plattform durch ein Durchführen von festen Abfrage-/Antwort-Wechselwirkungen verifiziert werden, um konsistente Ergebnisse sicherzustellen. Wo das vertrauenswürdige Gerät **24** eine trennbare Komponente ist, ist eine gewisse derartige Form einer Wechselwirkung erwünscht, um eine geeignete logische Bindung zwischen dem vertrauenswürdigen Gerät **14** und der Plattform bereitzustellen. Obwohl bei dem vorliegenden Ausführungsbeispiel das vertrauenswürdige Gerät **24** ferner den Datenbus als die Hauptkommunikationseinrichtung desselben mit anderen Teilen der Plattform verwendet, wäre es machbar, wenn auch nicht so zweckmäßig, alternative Kommunikationswege bereitzustellen, wie beispielsweise festverdrahtete Wege oder optische Wege. Obwohl bei dem vorliegenden Ausführungsbeispiel das vertrauenswürdige Gerät **24** ferner dem Hauptprozessor **21** befiehlt, die Integritätsmetrik zu berechnen, ist bei anderen Ausführungsbeispielen das vertrauenswürdige Gerät selbst angeordnet, um eine oder mehrere Integritätsmetriken zu messen.

[0095] Vorzugsweise umfaßt der BIOS-Boot-Prozeß Mechanismen, um die Integrität des Boot-Prozesses selbst zu verifizieren. Derartige Mechanismen sind bereits aus z. B. dem Entwurf von Intel „Wired for Management baseline specification v 2.0 – BOOT Integrity Service" bekannt und betreffen ein Berechnen von Auszügen einer Software oder Firmware vor einem Laden dieser Software oder Firmware. Ein derartiger berechneter Auszug wird mit einem Wert verglichen, der in einem Zertifikat gespeichert ist, das durch eine vertrauenswürdige Entität bereitgestellt ist, deren öffentlicher Schlüssel dem BIOS bekannt ist. Die Software/Firmware wird dann nur geladen, falls der berechnete Wert mit dem erwarteten Wert von dem Zertifikat übereinstimmt und das Zertifikat durch eine Verwendung des öffentlichen Schlüssels der vertrauenswürdigen Entität als gültig überprüft wurde. Andernfalls wird eine geeignete Ausnahmehandhabungsroutine aufgerufen.

[0096] Nach einem Empfangen des berechneten BIOS-Auszugs kann das vertrauenswürdige Gerät **24** wahlweise den ordnungsgemäßen Wert des BIOS-Auszugs in dem Zertifikat kontrollieren und eine Steuerung nicht an das BIOS übergeben, falls der berechnete Auszug nicht mit dem ordnungsgemäßen Wert übereinstimmt. Zusätzlich oder alternativ kann das vertrauenswürdige Gerät **24** den Booleschen Wert kontrollieren und eine Steuerung nicht an das BIOS zurückgeben, falls das vertrauenswürdige Gerät **24** nicht der erste Speicher war, auf den zugegriffen wurde. In jedem dieser Fälle kann eine geeignete Ausnahmehandhabungsroutine aufgerufen werden.

[0097] Fig. 5 stellt den Fluß von Schritten durch einen TP, das vertrauenswürdige Gerät **24**, das in eine Plattform eingegliedert ist, und einen Benutzer (eine entfernte Plattform) dar, der die Integrität der vertrauenswürdigen Plattform verifizieren will. Es sei darauf hingewiesen, daß im wesentlichen die gleichen Schritte betroffen sind, wie dieselben in Fig. 5 gezeigt sind, wenn der Benutzer ein lokaler Benutzer ist. In jedem Fall würde sich der Benutzer typischerweise auf eine gewisse Form einer Softwareanwendung stützen, um die Verifizierung durchzuführen. Es wäre möglich, die Softwareanwendung auf der entfernten Plattform oder der vertrauenswürdigen Plattform auszuführen. Es besteht jedoch eine Möglichkeit, daß selbst auf der entfernten Plattform die Softwareanwendung auf eine gewisse Weise untergraben werden könnte. Daher ist es für einen hohen Pegel einer Integrität bevorzugt, daß die Softwareanwendung auf einer Smartcard des Benutzers gelegen wäre, der die Smartcard in einen geeigneten Leser zu den Zwecken einer Verifizierung einbringen würde. Die vorliegende Erfindung bezieht sich auf eine derartige Anordnung.

[0098] Bei der ersten Instanz kontrolliert ein TP, der für vertrauenswürdige Plattformen bürgt, den Typ der Plattform, um zu entscheiden, ob derselbe für dieselbe bürgt oder nicht. Dies ist eine Frage einer Taktikeinheit. Falls alles gut ist, mißt der TP bei einem Schritt **500** den Wert einer Integritätsmetrik der Plattform. Dann erzeugt der TP ein Zertifikat für die Plattform in einem Schritt **505**. Das Zertifikat wird durch den TP durch ein Beifügen des öffentlichen Schlüssels des vertrauenswürdigen Geräts, und wahlweise des ID-Etiketts desselben, zu der gemessenen Integritätsmetrik und ein Signieren der Zeichenfolge mit dem privaten Schlüssel des TPs erzeugt.

[0099] Das vertrauenswürdige Gerät **24** kann nachfolgend die Identität desselben durch ein Verwenden des privaten Schlüssels desselben nachweisen, um gewisse Eingangsdaten zu verarbeiten, die von dem Benutzer empfangen werden, und Ausgangsdaten zu erzeugen, derart, daß das Eingangs-/Ausgangs-Paar ohne eine Kenntnis des privaten Schlüssels statistisch unmöglich zu erzeugen ist. Daher bildet eine Kenntnis des privaten Schlüssels in diesem Fall die Basis einer Identität. Es wäre natürlich machbar, eine symmetrische Verschlüsselung zu verwenden, um die Basis einer Identität zu bilden. Jedoch besteht der Nachteil eines Verwendens einer symmetrischen Verschlüsselung darin, daß der Benutzer sein Geheimnis mit dem vertrauenswürdigen Gerät gemeinschaftlich verwenden müßte. Als ein Ergebnis des Bedarfs, das Geheimnis mit dem Benutzer gemeinschaftlich zu verwenden, wäre es ferner, während eine symmetrische Verschlüsselung prinzipiell ausreichend wäre, um dem Benutzer eine Identität nachzuweisen, ungenügend, um einem Dritteilnehmer eine Identität nachzuweisen, der nicht vollständig sicher sein könnte, daß die Verifizierung von dem vertrauenswürdigen Gerät oder dem Benutzer stammte.

[0100] Bei einem Schritt **510** wird das vertrauenswürdige Gerät **24** durch ein Schreiben des Zertifikats **350** in die geeigneten Nicht-Flüchtiger-Speicher-Positionen **3** des vertrauenswürdigen Geräts **24** initialisiert. Dies geschieht vorzugsweise durch eine sichere Kommunikation mit dem vertrauenswürdigen Gerät **24**, nachdem dasselbe in der Hauptplatine **20** installiert ist. Das Verfahren eines Schreibens des Zertifikats zu dem vertrauenswürdigen Gerät **24** ist analog zu dem Verfahren, das verwendet wird, um Smartcards durch ein Schreiben von privaten Schlüsseln zu denselben zu initialisieren. Die sicheren Kommunikationen sind durch einen „Master-Schlüssel" unterstützt, der lediglich dem TP bekannt ist und während einer Herstellung zu dem vertrauenswürdigen Gerät (oder der Smartcard) geschrieben wird und verwendet wird, um das Schreiben von Daten zu dem vertrauenswürdigen Gerät **24** zu ermöglichen; ein Schreiben von Daten zu dem vertrauenswürdigen Gerät **24** ohne eine Kenntnis des Master-Schlüssels ist nicht möglich.

[0101] Zu einem gewissen späteren Punkt während einer Operation der Plattform, z. B. wenn dieselbe eingeschaltet oder rückgesetzt ist, gewinnt und speichert das vertrauenswürdige Gerät **24** bei einem Schritt **515** die Integritätsmetrik **361** der Plattform.

[0102] Wenn ein Benutzer wünscht, bei einem Schritt **520** mit der Plattform zu kommunizieren, erzeugt derselbe eine Einmalverfügung (Nonce), wie beispielsweise eine Zufallszahl, und fragt bei einem Schritt **525** das vertrauenswürdige Gerät **24** ab (das Betriebssystem der Plattform oder eine geeignete Software-Anwendung ist angeordnet, um die Abfrage zu erkennen und dieselbe dem vertrauenswürdigen Gerät **24** typischerweise über einen Aufruf vom BIOS-Typ auf eine geeignete Weise weiterzugeben). Die Einmalverfügung wird verwendet, um den Benutzer vor einer Täuschung zu schützen, die durch eine Wiedergabe von alten aber echten Signaturen (ein „Wiedergabeangriff" genannt) durch vertrauensunwürdige Plattformen bewirkt wird. Der Prozeß eines Bereitstellens einer Einmalverfügung und eines Verifizierens der Antwort ist ein Beispiel des gut bekannten „Abfrage-/Antwort"-Prozesses.

[0103] Bei einem Schritt **530** empfängt das vertrauenswürdige Gerät **24** die Abfrage und erzeugt eine geeignete Antwort. Dies kann ein Auszug der gemessenen Integritätsmetrik und der Einmalverfügung und wahlweise das ID-Etikett desselben sein. Dann signiert bei einem Schritt **535** das vertrauenswürdige Gerät **24** den Auszug unter Verwendung des privaten Schlüssels desselben und gibt den signierten Auszug zusammen mit dem Zertifikat **350** zu dem Benutzer zurück.

[0104] Bei einem Schritt **540** empfängt der Benutzer die Abfrage-Antwort und verifiziert das Zertifikat unter Verwendung des gut bekannten öffentlichen Schlüssels des TP. Der Benutzer extrahiert dann bei einem Schritt **550** den öffentlichen Schlüssel des vertrauenswürdigen Geräts **24** von dem Zertifikat und verwendet denselben, um den signierten Auszug von der Abfrage-Antwort zu entschlüsseln. Dann verifiziert bei einem Schritt **560** der Benutzer die Einmalverfügung im Inneren der Abfrage-Antwort. Als nächstes vergleicht bei einem Schritt **570** der Benutzer die berechnete Integritätsmetrik, die derselbe von der Abfrage-Antwort extrahiert, mit der ordnungsgemäßen Plattform-Integritätsmetrik, die derselbe von dem Zertifikat extrahiert. Falls ein jeglicher der vorhergehenden Verifizierungsschritte bei Schritten **545**, **555**, **565** oder **575** fehlschlägt, endet der gesamte Prozeß bei einem Schritt **580**, wobei keine weiteren Kommunikationen stattfinden.

[0105] Unter der Annahme, daß alles gut ist, verwenden der Benutzer und die vertrauenswürdige Plattform bei Schritten **585** und **590** andere Protokolle, um sichere Kommunikationen für andere Daten ein-

zurichten, wobei die Daten von der Plattform vorzugsweise durch das vertrauenswürdige Gerät **24** signiert sind.

[0106] Weitere Weiterentwicklungen dieses Verifizierungsprozesses sind möglich. Es ist erwünscht, daß sich der Abfrager durch die Abfrage sowohl des Werts der Plattform-Integritätsmetrik als auch des Verfahrens bewußt wird, durch das derselbe erhalten wurde. Diese beiden Informationen sind erwünscht, um es dem Abfrager zu erlauben, eine ordnungsgemäße Entscheidung über die Integrität der Plattform zu treffen. Der Abfrager hat ferner viele unterschiedliche Optionen verfügbar – derselbe kann akzeptieren, daß die Integritätsmetrik in dem vertrauenswürdigen Gerät **24** als gültig erkannt wird, oder kann alternativ lediglich akzeptieren, daß die Plattform den relevanten Pegel einer Integrität aufweist, falls der Wert der Integritätsmetrik gleich einem Wert ist, der durch den Abfrager gehalten ist (oder dort halten kann, um unterschiedliche Pegel eines Vertrauens in diesen zwei Fällen zu sein).

[0107] Die Techniken eines Signierens, eines Verwendens von Zertifikaten und Abfrage/Antwort und ein Verwenden derselben, um eine Identität nachzuweisen, sind Fachleuten auf dem Gebiet der Sicherheit gut bekannt und müssen daher hierin nicht detaillierter beschrieben werden.

[0108] Die Smartcard **19** des Benutzers ist ein Token-Gerät, das von der Rechenentität getrennt ist und mit der Rechenentität über das Smartcard-Leser-Tor **19** in Wechselwirkung steht. Ein Benutzer kann mehrere unterschiedliche Smartcards haben, die durch mehrere unterschiedliche Verkäufer oder Dienstanbieter ausgestellt sind, und kann einen Zugriff auf das Internet oder eine Mehrzahl von Netzwerk-Computern von einer jeglichen einer Mehrzahl von Rechenentitäten erlangen, wie es hierin beschrieben ist, die mit einer vertrauenswürdigen Komponente und einem Smartcard-Leser versehen sind. Ein Vertrauen eines Benutzers in die einzelne Rechenentität, die er verwendet, ist von der Wechselwirkung zwischen dem vertrauenswürdigen Smartcard-Token des Benutzers und der vertrauenswürdigen Komponente der Rechenentität abgeleitet. Der Benutzer stützt sich auf den vertrauenswürdigen Smartcard-Token desselben, um die Vertauenswürdigkeit der vertrauenswürdigen Komponente zu verifizieren.

[0109] Ein Verarbeitungsteil **60** einer Benutzer-Smartcard **19** ist in Fig. 6 dargestellt. Wie es gezeigt ist, weist der Verarbeitungsteil **60** der Benutzer-Smartcard **19** die Standardmerkmale eines Prozessors **61**, eines Speichers **62** und von Schnittstellenkontakten **63** auf. Der Prozessor **61** ist für einfache Abfrage-/Antwort-Operationen programmiert, die eine Authentifizierung der Benutzer-Smartcard **19** und eine Verifizierung der Plattform **10** betreffen, wie es unten beschrieben wird. Der Speicher **62** enthält einen privaten Schlüssel **620** desselben, einen öffentlichen Schlüssel **628** desselben, (wahlweise) ein Benutzerprofil **621**, den öffentlichen Schlüssel **622** des TP und eine Identität **627**. Das Benutzerprofil **621** listet die zulässigen Hilfssmartcards **20** AC1–Acn auf, die durch den Benutzer verwendbar sind, und die einzelne Sicherheitsrichtlinie **624** für den Benutzer. Für jede Hilfssmartcard **20** umfaßt das Benutzerprofil jeweilige Identifizierungsinformationen **623**, die Vertrauensstruktur **625** zwischen den Smartcards (falls eine existiert) und wahlweise den Typ oder das Fabrikat **626** der Smartcard.

[0110] In dem Benutzerprofil **621** umfaßt jeder Eintrag einer Hilfssmartcard **20** AC1–Acn zugeordnete Identifizierungsinformationen **623**, die abhängig von dem Kartentyp variieren. Zum Beispiel umfassen die Identifizierungsinformationen für eine Geldautomatenkarte typischerweise eine einfache Seriennummer, während bei einer Krypto-Karte die Identifizierungsinformationen typischerweise den öffentlichen Schlüssel (oder Zertifikat) der Krypto-Karte aufweisen (wobei der private Schlüssel geheim auf der Krypto-Karte selbst gespeichert ist).

[0111] Die „Sicherheitsrichtlinien" **624** diktieren die Befugnisse, die der Benutzer auf der Plattform **10** hat, während derselbe eine Hilfssmartcard **20** verwendet. Zum Beispiel kann abhängig von der Funktion der Hilfssmartcard **20** die Benutzerschnittstelle verriegelt oder entriegelt werden, während eine Hilfssmartcard **20** in Gebrauch ist. Zusätzlich oder alternativ ist es möglich, daß bestimmte Dateien oder ausführbare Programme auf der Plattform **10** zugreifbar gemacht werden oder nicht, abhängig davon, wie vertrauenswürdig eine spezielle Hilfssmartcard **20** ist. Ferner können die Sicherheitsrichtlinien **624** einen speziellen Betriebsmodus für die Hilfssmartcard **20** spezifizieren, wie beispielsweise „Krediterhalt" oder „temporäre Delegierung", wie es unten beschrieben wird. Eine „Vertrauensstruktur" **625** definiert, ob eine Hilfssmartcard **20** selbst weitere Hilfssmartcards **20** in das System „einbringen" kann, ohne zuerst die Benutzer-Smartcard **19** wiederzuverwenden. Bei den hierin detailliert beschriebenen Ausführungsbeispielen besteht die einzige definierte Vertrauensstruktur zwischen der Benutzer-Smartcard **19** und den Hilfssmartcards **20**, die durch die Benutzer-Smartcard **19** zu der Plattform **10** eingebracht werden können. Eine Einbringung kann in einer „Einzelsitzung" oder einer „Mehrfachsitzung" erfolgen, wie es unten beschrieben wird. Es besteht jedoch kein Grund dafür, warum bestimmte Hilfssmartcards **20** in der Praxis nicht weitere Hilfssmartcards **20** einbringen könnten. Dies würde erfordern, daß eine Hilfssmartcard **20** ein Äquivalent eines Benutzerprofils aufweist, das die oder jede Hilfssmartcard auflistet, die eingebracht werden kann.

[0112] Eine Verwendung von Hilfssmartcards **20** ist kein notwendiges Merkmal der vorliegenden Erfindung und wird in der vorliegenden Anmeldung nicht weiter beschrieben. Eine Verwendung von Hilfssmartcards ist der Gegenstand der ebenfalls anhängigen Internationalen Patentanmeldung gleichen Datums der vorliegenden Anmelderin mit dem Titel „Computing Apparatus and Methods of Operating Computing Apparatus", die hierin durch Bezugnahme aufgenommen ist.

[0113] Ein bevorzugter Prozeß zu einer Authentifizierung zwischen einer Benutzer-Smartcard **19** und einer Plattform **10** wird nun mit Bezug auf das Flußdiagramm in Fig. 7 beschrieben. Wie es beschrieben wird, implementiert der Prozeß zweckmäßigerweise eine Abfrage-/Antwort-Routine. Es existieren viele verfügbare Abfrage-/Antwort-Mechanismen. Die Implementierung eines Authentifizierungsprotokolls, das bei dem vorliegenden Ausführungsbeispiel verwendet wird, ist eine gegenseitige (oder 3-Schritt-)Authentifizierung, wie dieselbe in ISO/IEC 9798-3 beschrieben ist. Natürlich gibt es keinen Grund dafür, warum andere Authentifizierungsprozeduren nicht verwendet werden können, z. B. 2-Schritt oder 4-Schritt, wie dieselben ebenfalls in ISO/IEC 9798-3 beschrieben sind.

[0114] Zu Beginn bringt der Benutzer die Benutzer-Smartcard **19** desselben in den Smartcard-Leser **12** der Plattform **10** bei einem Schritt **700** ein. Zuvor ist die Plattform **10** typischerweise unter der Steuerung des Standardbetriebssystems derselben wirksam und führt den Authentifizierungsprozeß aus, der darauf wartet, daß ein Benutzer die Benutzer-Smartcard **19** desselben einbringt. Abgesehen davon, daß der Smartcard-Leser **12** auf diese Weise aktiv ist, wird die Plattform **10** typischerweise durch ein „Verriegeln" der Benutzerschnittstelle (d. h. des Bildschirms, der Tastatur und der Maus) für Benutzer unzugreifbar gemacht.

[0115] Wenn die Benutzer-Smartcard **19** in den Smartcard-Leser **12** eingebracht wird, wird ausgelöst, daß das vertrauenswürdige Gerät **24** durch ein Erzeugen und Senden einer Einmalverfügung A zu der Benutzer-Smartcard **19** bei einem Schritt **705** sich bei einem Schritt an eine gegenseitige Authentifizierung macht. Eine Einmalverfügung, wie beispielsweise eine Zufallszahl, wird verwendet, um den Urheber von einer Täuschung zu schützen, die durch eine Wiedergabe von alten aber echten Antworten (ein „Wiedergabeangriff genannt") durch vertrauensunwürdige Dritteilnehmer bewirkt wird.

[0116] Ansprechend darauf erzeugt und gibt die Benutzer-Smartcard **19** bei einem Schritt **710** eine Antwort zurück, die die Verkettung aufweist von: dem Klartext der Einmalverfügung A, einer neuen Einmalverfügung B, die durch die Benutzer-Smartcard **19** erzeugt wird, der ID **353** des vertrauenswürdigen Geräts **24** und einer gewissen Redundanz; der Signatur des Klartexts, erzeugt durch ein Signieren des Klartexts mit dem privaten Schlüssel der Benutzer-Smartcard **19**; und eines Zertifikats, das die ID und den öffentlichen Schlüssel der Benutzer-Smartcard **19** enthält.

[0117] Das vertrauenswürdige Gerät **24** authentifiziert die Antwort durch ein Verwenden des öffentlichen Schlüssels in dem Zertifikat, um die Signatur des Klartexts bei einem Schritt **715** zu verifizieren. Falls die Antwort nicht authentisch ist, endet der Prozeß bei einem Schritt **720**. Falls die Antwort authentisch ist, erzeugt und sendet das vertrauenswürdige Gerät **24** bei einem Schritt **725** eine weitere Antwort, die die Verkettung umfaßt von: dem Klartext der Einmalverfügung A, der Einmalverfügung B, der ID **627** der Benutzer-Smartcard **19** und der gewonnenen Integritätsmetrik; der Signatur des Klartexts, erzeugt durch ein Signieren des Klartexts unter Verwendung des privaten Schlüssels des vertrauenswürdigen Geräts **24**; und des Zertifikats, das den öffentlichen Schlüssel des vertrauenswürdigen Geräts **24** und die authentische Integritätsmetrik aufweist, die beide durch den privaten Schlüssel des TP signiert sind.

[0118] Die Benutzer-Smartcard **19** authentifiziert diese Antwort durch ein Verwenden des öffentlichen Schlüssels des TP und ein Vergleichen der gewonnenen Integritätsmetrik mit der authentischen Integritätsmetrik, wobei eine Übereinstimmung eine erfolgreiche Verifizierung angibt, bei einem Schritt **730**. Falls die weitere Antwort nicht authentisch ist, endet der Prozeß bei einem Schritt **735**.

[0119] Falls die Prozedur erfolgreich ist, hat sowohl das vertrauenswürdige Gerät **24** die Benutzer-Smartcard **19** authentifiziert als auch die Benutzer-Smartcard **19** die Integrität der vertrauenswürdigen Plattform **10** verifiziert und der Authentifizierungsprozeß führt bei einem Schritt **740** den sicheren Prozeß für den Benutzer aus. Dann setzt bei einem Schritt **745** der Authentifizierungsprozeß einen Intervallzeitnehmer. Unter Verwendung geeigneter Betriebssystem-Unterbrechungsroutinen wartet der Authentifizierungsprozeß danach den Intervallzeitgeber periodisch, um zu erfassen, wann der Zeitgeber bei einem Schritt **750** eine vorbestimmte Zeitablaufperiode einhält oder überschreitet.

[0120] Natürlich laufen der Authentifizierungsprozeß und der Intervallzeitgeber parallel mit dem sicheren Prozeß.

[0121] Wenn die Zeitablaufperiode eingehalten oder überschritten wird, löst der Authentifizierungsprozeß aus, daß das vertrauenswürdige Gerät **24** die Benutzer-Smartcard **19** wieder authentifiziert, durch ein

Senden einer Abfrage für die Benutzer-Smartcard **19**, um sich selbst zu identifizieren, bei einem Schritt **760**. Die Benutzer-Smartcard **19** gibt bei einem Schritt **765** ein Zertifikat zurück, das die ID **627** derselben und den öffentlichen Schlüssel **628** derselben umfaßt. Falls es bei einem Schritt **770** keine Antwort gibt (z. B. als ein Ergebnis davon, daß die Benutzer-Smartcard **19** entfernt wurde) oder das Zertifikat aus einem gewissen Grund nicht mehr gültig ist (z. B. die Benutzer-Smartcard mit einer unterschiedlichen Smartcard ersetzt wurde), wird die Sitzung durch das vertrauenswürdige Gerät **24** bei einem Schritt **775** beendet. Andernfalls wiederholt sich bei einem Schritt **770** der Prozeß von dem Schritt **745** durch ein Rücksetzen des Intervallzeitgebers.

[0122] Mehrere unterschiedliche Implementierungen der Erfindung sind möglich. Bei einer bevorzugten ersten Implementierung kann der Monitor **18** direkt durch ein Monitoruntersystem getrieben sein, das innerhalb der vertrauenswürdigen Komponente selbst enthalten ist. Bei diesem Ausführungsbeispiel sind in dem Vertrauenswürdige-Komponente-Raum die vertrauenswürdige Komponente selbst und Anzeigen gelegen, die durch die vertrauenswürdige Komponente auf dem Monitor **18** erzeugt werden. Diese Anordnung ist in der EP-A-1055989 der Anmelderin weiter beschrieben.

[0123] Bei einer bevorzugten ersten Implementierung ist dieses Untersystem auf der Computerplattform gelegen und stellt Schnittstellen zwischen dem Smartcard-Leser, der vertrauenswürdigen Komponente und dem Monitor bereit. Die Untersystemfunktionalität ist in die vertrauenswürdige Komponente eingebaut und ist innerhalb des vertrauenswürdigen Raums gelegen. Das Untersystem bildet Schnittstellen zwischen der Computerplattform und einer Smartcard und der vertrauenswürdigen Komponente.

[0124] Das Untersystem ist zu einem Beibehalten eines Vertrauens in die vertrauenswürdige Komponente nicht entscheidend, bei anderen Implementierungen kann das Untersystem wahlweise auf der Computerplattform in dem „vertrauensunwürdigen" Computerplattformraum gelegen sein.

[0125] Bei einer zweiten Implementierung wird auf die vertrauenswürdige Komponente (Gerät) über den Smartcard-Leser **19** und eine Smartcard-Schnittstelle über ein Software-Untersystem zugegriffen. Das Untersystem stellt auch eine Anwendungsschnittstellenfunktion zu einem Schnittstellenbilden zwischen Anwendungen und der vertrauenswürdigen Komponente; und eine Verifizierungsanwendung zu einem Verifizieren von Integritätsmetrikdaten, die durch eine vertrauenswürdige Komponente erhalten werden, über einen Dritteilnehmer, auf den über das Internet zugegriffen wird, oder über ein lokales Netz/weites Netz bereit.

[0126] Das durch einen Benutzer in die Computerentität gelegte Vertrauen ist aus drei getrennten Teilen gebildet:

- Ein Vertrauen, das in das vertrauenswürdige Token-Gerät des Benutzers gelegt wird.
- Das Vertrauen, das in die vertrauenswürdige Komponente gelegt wird.

[0127] Wie es hierin beschrieben ist, sind Pegel oder Grade an Vertrauen, das in die Computerentität gelegt wird, als relativ zu einem Pegel eines Vertrauens bestimmt, das in die vertrauenswürdige Komponente und die Smartcard gelegt wird. Obwohl die Größe eines Vertrauens in eine Computerentität auf viele Faktoren bezogen ist, sind die Typen, ein Ausmaß und eine Regelmäßigkeit von Integritätsmetrikü berprüfungen, die die vertrauenswürdige Komponente selbst an der Computerentität ausführt, und der Typ, eine Regelmäßigkeit und eine Qualität der Überprüfungen, die die Smartcard an der vertrauenswürdigen Komponente vornimmt, ein Schlüsselfaktor bei einem Messen dieses Vertrauens.

[0128] Wenn der Benutzer durch eine Verwendung einer Smartcard desselben eingerichtet hat, daß die vertrauenswürdige Komponente korrekt wirksam ist, wird der vertrauenswürdigen Komponente implizit vertraut. Die vertrauenswürdige Komponente ist als die Wurzel eines jeglichen Vertrauens eingebettet, das in die Rechenplattform gelegt wird, und der Rechenplattform als Ganzes kann nicht mehr vertraut werden als die Größe eines Vertrauens, das in die vertrauenswürdige Komponente gelegt wird.

[0129] Obwohl andere Rechenentitäten direkt mit einer vertrauenswürdigen Komponente mittels verschlüsselter Nachrichten in Wechselwirkung treten können, um die Operation einer vertrauenswürdigen Komponente zu verifizieren, kann ein menschlicher Benutzer, der eine Rechenentität betreibt, nicht direkt eine Schnittstelle mit einer vertrauenswürdigen Komponente bilden, da der menschliche Benutzer eine biologische Entität ist, die zu einem Erzeugen digitaler verschlüsselter Signale nicht in der Lage ist. Der menschliche Benutzer muß sich auf die visuellen und Audio-Sinne desselben stützen, um die Vertrauenswürdigkeit einer Rechenentität zu verifizieren. Der menschliche Benutzer hat bei dem allgemeinen Fall keine Kenntnis der Mechanismen, die im Inneren der Rechenentität tätig sind, und ist bei dem allgemeinen Fall von einem durchschnittlichen Pegel einer Erziehung und Kultiviertheit, d. h. eine normale durchschnittliche Person.

[0130] Der Benutzer ist daher mit einem vertrauenswürdigen Token in der Form einer Smartcard versehen, in den der Benutzer einen hohen Grad eines Vertrauens legen kann. Die Smartcard des Benutzers kann mit der vertrauenswürdigen Komponente der Computerentität in Wechselwirkung treten, um:

• die Identität einer vertrauenswürdigen Komponente dem Benutzer nachzuweisen.
• zu verifizieren, daß aufgrund einer Integritätsmetrikmessung, die durch die vertrauenswürdige Komponente auf der Computerplattform ausgeführt wird die Computerplattform im Inneren der Computerentität korrekt wirksam ist.

[0131] Daher gibt es bei dem System von Rechenentitäten Ketten eines Vertrauens, die wie folgt verstrickt sind:
• Der Benutzer muß dem vertrauenswürdigen Token vertrauen. Dieses Vertrauen basiert auf dem Ruf des Anbieters des vertrauenswürdigen Tokens, der typischerweise eine Gesellschaft ist, die einen Zugriff auf die notwendigen technischen und ingenieurmäßigen Betriebsmittel hat, um eine korrekte Operation des vertrauenswürdigen Tokens zu ermöglichen.
• Ein Vertrauen zwischen dem vertrauenswürdigen Token und einer vertrauenswürdigen Komponente. Die vertrauenswürdige Token-Smartcard muß in der Lage sein, eine korrekte Operation der vertrauenswürdigen Komponente zu verifizieren, die die Smartcard verwendet.
• Ein Vertrauen in die Computerplattform. Das Vertrauen in die Computerplattform leitet sich von dem Überwachen der Computerplattform durch die vertrauenswürdige Komponente ab, der selbst vertraut wird.

[0132] Innerhalb dieser Vertrauenskette kann die Verbindung zwischen dem Benutzer und einer Computerentität von der Perspektive des Benutzers, der vertrauenswürdigen Plattform, die der Benutzer verwendet, und von der Perspektive des vertrauenswürdigen Tokens (der Smartcard) betrachtet werden, wie es hierunter beschrieben ist.

[0133] Von dem Standpunkt des Benutzers betrachtet, kann der Benutzer lediglich dem vertrauen, was er auf dem Computerbildschirm sieht und was er auf der Audioausgabe und/oder gedruckten Ausgabe des Computers hört. Der Benutzer wird mit einem vertrauenswürdigen Token in der Form einer Smartcard **19** versehen, die in einen Smartcard-Leser **12** der Rechenentität eingebracht werden kann. Die Smartcard führt Wechselwirkungen unter Verwendung kryptographischer Nachrichten und Abfragen im Namen des Benutzers aus. Die Smartcard ist zu einem Einleiten einer Aufforderung an die vertrauenswürdige Komponente in der Lage, um Integritätsmetriken durchzuführen, und ist zu einem Verweigern einer Autorisierung gegenüber Anwendungsprogrammen in der Lage, in dem Fall, daß die Smartcard keine zufriedenstellende Antwort auf eine Aufforderung nach einer Verifizierung von einer vertrauenswürdigen Komponente empfängt.

[0134] Spezifische Implementierungen zu einem Ausführen der Erfindung sind beschrieben: in jeder weist die Rechenentität eine Mehrzahl von möglichen Betriebsmodi auf.

[0135] Unter Bezugnahme auf Fig. 8 hierin ist ein erster Betriebsmodus eines Computersystems dargestellt, das eine Rechenentität und eine Smartcard unter der Steuerung eines Benutzers aufweist, der einem ersten Prozeß folgt. Bei dem Prozeß von Fig. 8 gibt es keine Anwendung, die auf der Computerentität gelegen ist, die eine Verwendung der Smartcard des Benutzers erfordert. Der Benutzer verifiziert einfach die Vertrauenswürdigkeit der Rechenplattform innerhalb der Computerentität mit der Hilfe der Smartcard. Im allgemeinen wünscht ein Benutzer, die Integrität einer Rechenentität zu überprüfen, sobald der Benutzer sich einloggt und bevor der Benutzer jegliche empfindliche Operationen durchführt. Die Smartcard kann programmiert sein, um die Integrität der Rechenentität über eine vertrauenswürdige Komponente derselben zu verifizieren, bevor der Benutzer jegliche andere Aufgaben unter Verwendung der Rechenentität ausführt. Bei einem Schritt **7000** bringt ein Benutzer die Smartcard in den Smartcard-Leser der Rechenentität ein, die er verwenden wird. Bei einem Schritt **7010** beginnt der Benutzer die graphische Benutzerschnittstelle der Rechenplattform zu verwenden. Bei einem Schritt **7020** wird durch den Benutzer eine Verifizierungsanwendung aktiviert, deren Zweck es ist, es einem Benutzer zu ermöglichen, der eine Smartcard hat, die Integrität einer vertrauenswürdigen Komponente der Rechenentität zu überprüfen, und die auf die Computerplattform vorgeladen ist. Eine derartige Aktivierung kann durch ein Aktivieren eines Zeigegeräts sein, z. B. einer Maus oder eines Trackball, das visuell über einem Icon plaziert ist, das auf einer visuellen Anzeige der Rechenentität angezeigt ist. Die Verifizierungsschnittstelle empfängt die Befehle von der graphischen Benutzerschnittstelle zu einem Einleiten einer Überprüfung der vertrauenswürdigen Komponente durch die Smartcard und verarbeitet diese in Befehle in einer Form, in der der Smartcard durch die Anwendung befohlen werden kann, einen Verifizierungsprozeß zu beginnen. Bei einem Schritt **7030** sendet die Schnittstelle ein Aufforderungssignal zu der Smartcard, wobei die Smartcard aufgefordert wird, eine Verifizierungsoperation an der vertrauenswürdigen Komponente zu beginnen. Bei einem Schritt **7040** führt die Smartcard Integritätsüberprüfungen an der vertrauenswürdigen Komponente aus. Alle Kommunikationen zwischen der Smartcard und der vertrauenswürdigen Komponente sind in einem verschlüsselten Format. Das genaue Verfahren, durch das die Smartcard die Integrität der vertrauenswürdigen Komponente verifiziert, ist durch das oben mit Bezug auf Fig. 5 und Fig. 7 beschriebene Abfrage-Antwort-Integritätsüberprüfungsverfahren. Bei einem Schritt **7050** berichtet die Smartcard, die die Integritätsüberprü-

fung an der vertrauenswürdigen Komponente abgeschlossen hat, durch ein Anzeigen auf der graphischen Benutzerschnittstelle zurück zu dem Benutzer. Die vertrauenswürdige Komponente kann unter Verwendung der graphischen Benutzerschnittstelle durch eine Vielfalt von Methoden zurück zu dem Benutzer berichten, von denen einige der Gegenstand von getrennten Patentanmeldungen durch die Anmelderin sind und die außerhalb des Schutzbereichs dieser Offenbarung sind.

[0136] Bei einem derartigen Verfahren verwendet die Smartcard die vertrauenswürdige Komponente, um die Anzeige auf dem Monitor **18** zu steuern, um Informationen anzuzeigen, die die Computerplattform beschreiben, die durch die vertrauenswürdige Komponente bestimmt wurde und bei der ein Bild, das für die Smartcard spezifisch ist, auf der visuellen Anzeigeeinheit angezeigt wird. Zum Beispiel kann die Smartcard Bilddaten enthalten, die schwer wiederzuerzeugen sind und vorzugsweise lediglich dem Benutzer bekannt sind. Die vertrauenswürdige Komponente kann diese Bilddaten von der Smartcard wiedererlangen und dieselben auf dem Monitor anzeigen, zusammen mit anderen Informationen, die Integritätsmetriken und eine Operation der Computerplattform beschreiben. Da die Rechenentität keine andere Weise eines Erhaltens der Bilddaten aufweist, als von der Smartcard des Benutzers, wo dieselben vorgespeichert sind, und weil der Benutzer visuell mit einem hohen Grad einer Genauigkeit identifizieren kann, daß das Bild echt ist, hat der Benutzer dann durch eine visuelle Kontrolle ein Vertrauen, daß die Rechenentität tatsächlich mit der Smartcard in Wechselwirkung getreten ist (andernfalls wäre das Bild nicht zu erhalten).

[0137] Alternativ kann bei dem Schritt **7050** anstelle der Bilddaten, die auf dem Monitor einer Rechenentität angezeigt werden, die überprüft wird, der Benutzer seine Smartcard von dem Smartcard-Leser entfernen und die Smartcard in sein eigenes Palmtop-Gerät einbringen. Das Palmtop-Gerät ist für den Benutzer persönlich und der Benutzer kann daher dem Palmtop-Gerät zu einem höheren Ausmaß vertrauen, als der Computerentität. Der Palmtop-Leser liest Daten von der Smartcard, die verifizieren, daß die Computerentität die Abfrage-Antwort-Tests bestanden hat, die durch die Smartcard vorgenommen wurden. Der Palmtop-Computer zeigt dann dem Benutzer die Informationen an, daß die Computerentität den Abfrage-Antwort-Test bestanden hat, der durch die Smartcard gesetzt wurde. Der Benutzer nimmt dies als eine Verifizierung, daß die Rechenentität vertrauenswürdig ist.

[0138] Das obige Verfahren ist wirksam, wo ein Benutzer wünscht, eine Rechenentität zu verwenden, und einfach zu wissen wünscht, ob der Rechenentität vertraut werden kann. Dagegen zeigt Fig. 9 schematisch einen zweiten Betriebsmodus bei einem Fall, wo eine Anwendung, die auf der Rechenentität gelegen ist oder auf einer entfernten Rechenentität gelegen ist, mit der der Benutzer zu kommunizieren wünscht, es erfordert, daß ein Benutzer eine Operation autorisiert, z. B. eine kommerzielle Transaktionsoperation.

[0139] Die Smartcard ist durch einen Systemadministrator oder einen Smartcard-Dienstanbieter mit Details konfiguriert, die für den Benutzer speziell sind. Bei einem Schritt **800** bringt der Benutzer die Smartcard in den Smartcard-Leser der Rechenentität ein. Bei einem Schritt **801** fordert die Anwendung oder das Betriebssystem der Rechenentität Daten von der Smartcard an. Bei einem Schritt **803** spricht die Smartcard durch ein Senden einer Verzögerungsnachricht zu der Rechenentität und ein Anfordern eines Zugriffs auf die vertrauenswürdige Komponente der Rechenentität von der Rechenentität an, so daß die Smartcard die Integrität der Rechenentität verifizieren kann. Bei einem Schritt **804** korrespondiert die Smartcard mit der vertrauenswürdigen Komponente der Rechenentität mittels Integritätsüberprüfungen gemäß einem Abfrage-Antwort-Prozeß, wie derselbe hierin oben beschrieben ist, um die Integrität der Rechenentität zu überprüfen. Falls bei einem Schritt **805** die Smartcard bestimmt, daß die Integritätsüberprüfungen durch die vertrauenswürdige Komponente zufriedengestellt wurden, geht die Smartcard dazu über, auf die Anforderung von dem Betriebssystem oder der Anwendung nach Daten zu einem Abschließen der Operation anzusprechen.

[0140] Die Smartcard ist auf eine derartige Weise programmiert, daß die Smartcard niemals eine Wechselwirkung mit einer Anwendung annimmt, z. B. zu den Zwecken einer Authentifizierung oder um gewisse kryptographische Dienste bereitzustellen, wenn dieselbe nicht zuerst die Integrität der Rechenentität verifizieren kann, mit der dieselbe mittels einer Korrespondenz mit einer vertrauenswürdigen Komponente der Rechenentität verbunden ist, bei der die vertrauenswürdige Komponente Integritätsmetriken der Rechenplattform authentifiziert und überprüft. Auf diese Weise ist der Benutzer, der der Smartcard implizit vertraut, sicher, daß die Smartcard desselben lediglich akzeptiert durch eine Anwendung verwendet zu werden, wenn dieselbe verifiziert hat, daß sich dieselbe in einer vertrauenswürdigen Umgebung befindet. Die Smartcard muß die Ergebnisse der Integritätsüberprüfungen nicht notwendigerweise explizit dem Benutzer berichten. Die bloße Tatsache, daß eine Anwendung eine Wechselwirkung mit einer Smartcard angefordert hat und daß eine angeforderte Wechselwirkung zufriedengestellt wurde, ist ein Nachweis, daß die Smartcard in der Lage war, diese Überprüfung auszuführen und mit dem Ergebnis zufriedengestellt ist. Ob die Smartcard eine Wechselwirkung mit einer Anwendung akzeptiert oder ablehnt, basiert auf vorbestimmten Richtlinien,

die durch den Smartcard-Aussteller auf die Smartcard vorprogrammiert sind oder die durch einen Benutzer durch ein Programmieren der Smartcard konfiguriert werden können.

[0141] Eine Konfiguration des Smartcard-Speichers kann durch einen Benutzer vorgenommen werden, falls diese Einrichtung durch einen Smartcard-Verkäufer bereitgestellt ist. Zum Beispiel kann ein Käufer eines Personalcomputers in der Lage sein, seine eigene Smartcard zu konfigurieren, um gemäß Benutzerpräferenzen wirksam zu sein. Die Smartcard kann vorkonfiguriert sein, derart, daß ein Benutzer in der Lage sein kann, die Smartcard zu programmieren, um mit einer Rechenentität in einer Microsoft-Windows™-Umgebung in Wechselwirkung zu treten, selbst wo bei einer Rechenentität keine vertrauenswürdige Komponente existiert. Ein Smartcard-Verkäufer kann ein Programmieren einer Smartcard durch ein Gerät, wie beispielsweise einen PDA-Palmtop-Computer ermöglichen. Die präzise Konfiguration der Fähigkeiten jeder Smartcard sind durch den Smartcard-Anbieter als eine Entwurfsfrage spezifiziert.

[0142] Als ein anderes Beispiel kann ein Internetdienstanbieter eine Smartcard bereitstellen, die sich lediglich gegenüber dem Internetdienstanbieter korrekt identifiziert, wenn dieselbe verifizieren kann, daß die Rechenentität, in die dieselbe eingebracht ist, verschiedene Integritätsüberprüfungen bestanden hat, die durch die Smartcard spezifiziert sind. Dies liefert einen Schutz für den Internetdienstanbieter, um in der Lage zu sein, zu bestätigen, daß ein Benutzer nicht unter Verwendung eines vertrauensunwürdigen Computers, der Viren tragen kann, eine Verbindung zu dem Internetdienst herstellt.

[0143] Ein Merkmal der obigen zwei Verfahren besteht darin, daß dieselben keine Einleitung durch eine Benutzerwechselwirkung erfordern, sondern dadurch eingeleitet werden, daß die Smartcard in den Smartcard-Leser einer Computerentität eingebracht wird. Dies ist nicht wesentlich für die Erfindung, die auch auf eine Einleitung durch eine Benutzerwechselwirkung oder sogar durch Softwareanwendungen anwendbar ist. Beispiele derartiger Anordnungen werden weiter unten beschrieben.

[0144] Unter Bezugnahme auf Fig. 9 hierin wird nun ein Beispiel einer Operation der Computerentität während einer Wechselwirkung derselben mit einer Smartcard beschrieben, die als ein vertrauenswürdiger Token angepaßt ist. Dieses Beispiel basiert auf einer bekannten Technologie gemäß der PCSC-Spezifikation, gefunden in dem Standard ISO 7816 und betrachtbar unter www.pcscworkgroup.com, das bei einer bevorzugten Anordnung modifiziert ist, um eine Einleitung von Befehlen von der Smartcard zu erlauben.

[0145] Eine Wechselwirkung zwischen einer Smartcard und der vertrauenswürdigen Komponente erlaubt es der Smartcard, die korrekte Operation der vertrauenswürdigen Komponente zu authentifizieren und die Antwort der vertrauenswürdigen Komponente hinsichtlich einer Integrität der Computerplattform zu erhalten, die die vertrauenswürdige Komponente überwacht. Bei einer bevorzugten Implementierung erlaubt der Integritätsverifizierungsprozeß, daß die vertrauenswürdige Komponente ein interpretiertes Ergebnis einer Verifizierung einer korrekten Operation der Rechenentität der Smartcard berichtet. Bei einem anderen Modus einer Implementierung stellt die vertrauenswürdige Komponente jedoch den Mechanismus eventuell nicht bereit, um die Integritätsmessungen für die Smartcard zu interpretieren. In diesem Fall muß die Smartcard einen Zugriff auf einen vertrauenswürdigen Dritteilnehmerserver aufweisen, der diese Funktionalität bereitstellt.

[0146] Typischerweise erfordert ein Zugriff auf einen vertrauenswürdigen Dritteilnehmerserver durch die Smartcard das Vorhandensein eines Mechanismus, so daß die Smartcard anfordern kann, daß ein derartiger Zugriff durch die Rechenentität bereitgestellt wird.

[0147] Angenommen, man hat eine Smartcard, die einen Befehl an eine vertrauenswürdige Komponente einleiten, mit der vertrauenswürdigen Komponente zu einem Austausch von Nachrichten und Informationen kommunizieren, Anforderungen nach Informationen senden, Ergebnisse von der vertrauenswürdigen Komponente ansprechend auf diese Anforderungen empfangen und anfordern kann, daß ein Zugriff auf einen Dritteilnehmerserver durch die Rechenentität bereitgestellt wird, dann kann eine Integritätsverifizierung der vertrauenswürdigen Komponente gegenüber der Smartcard erreicht werden. Eine Implementierung einer Einleitung von Benutzerbefehlen von einer Smartcard ist in „Smartcards – from security tokens to intelligent adjuncts", von Boris Balacheff, Bruno Van Wilder und David Chan, veröffentlicht in CARDIS 1998 Proceedings, bekannt.

[0148] Die bei einer Einleitung von Benutzerbefehlen von einer Smartcard betroffenen Wechselwirkungen gemäß Balacheff et al. werden kurz mit Bezugnahme auf Fig. 9 erörtert (für mehr implementierungsmäßige Details wird der Leser auf den Artikel selbst verwiesen). Der verwendete Ansatz ist im wesentlichen ähnlich zu dem, der bei GSM (Spezifikation GSM 11,14) verwendet wird, um einem Teilnehmerkennungsmodul (SIM = Subscriber Identity Module) zu ermöglichen, Schritte einzuleiten, die durch eine mobile Ausrüstung unternommen werden sollen. Die funktionale Rolle, die durch eine mobile Ausrüstung bei dieser Anordnung eingenommen wird, wird durch etwas eingenommen, das ein PC-Intelligent-Adjunct-(PCIA-)Modul **900** innerhalb der Plattform

genannt werden kann – die Smartcard **901** steht in Wechselwirkung mit diesem Modul. Bei einem Schritt **902** erteilt das PCIA-Modul zuerst im wesentlichen einen jeweiligen Befehl (C1). Die Ergebnisse des C1-Befehls werden bei einem Schritt **903** zu dem PCIA-Modul rückgekoppelt, gefolgt durch eine Statusantwort „91 XX" bei einem Schritt **904** – dieser Schlüsselschritt (eine Alternative zu dem normalen „OK"-Code) ermöglicht es, daß die Smartcard **901** das PCIA-Modul **900** benachrichtigt, daß dasselbe Informationen zu senden hat, und die Länge (XX) der Antwortdaten. Das PCIA-Modul fordert dann diese zusätzlichen Daten durch ein FETCH (Abrufen) bei einem Schritt **905** an, mit dem Ergebnis, daß ein Befehl C2 durch die Smartcard bei einem Schritt **906** geliefert wird und ein Ergebnis bei einem Schritt **907** zurückgegeben wird. Bei einem Schritt **908** wird eine Bestätigung durch die Smartcard bereitgestellt – vorteilhafterweise sollte eine Bestätigung dann auch durch das PCIA-Modul (nicht gezeigt) bereitgestellt werden.

[0149] Unter Bezugnahme auf Fig. 11 hierin ist schematisch ein System einer Computervorrichtung dargestellt, die eine Rechenentität **1100**, die eine Computerplattform und eine Überwachungskomponente aufweist, wie es hierin zuvor beschrieben ist; ein vertrauenswürdiges Token-Gerät **1101**, das zu einem Kommunizieren mit der Rechenentität **1100** in der Lage ist; und einen entfernten Server **1102** aufweist, der zu einem Ausführen einer Datenverarbeitungsfunktionalität in der Lage ist. Der entfernte Server **1102** weist ferner eine zweite Rechenplattform und eine zweite Überwachungskomponente auf. Bei einer Verwendung kann der entfernte Server **1102** durch einen zuverlässigen Dienstanbieter, z. B. einen Internetdienstanbieter, verwaltet werden, in den ein Benutzer eines vertrauenswürdigen Token-Geräts einen Grad eines Vertauens haben kann, das z. B. durch eine Vertragsbeziehung mit dem Internetdienstanbieter eingerichtet ist, wie beispielsweise ein Teilnehmen an einem Dienst, der durch den Internetdienstanbieter bereitgestellt wird.

[0150] Unter Bezugnahme auf Fig. 12 hierin ist schematisch ein dritter Betriebsmodus eines Token-Geräts und einer Rechenentität innerhalb des Systems von Computern dargestellt, das in Fig. 11 dargestellt ist. Bei diesem Betriebsmodus wird eine Überwachungskomponente (vertrauenswürdige Komponente) innerhalb der Rechenentität **1100** durch die Smartcard **1101** aufgefordert, einen Satz von Datenüberprüfungen an der Rechenplattform innerhalb der Rechenentität **1100** zu liefern. Das vertrauenswürdige Token-Gerät **1101** weist eventuell keine ausreichend hohe Datenverarbeitungsfähigkeit auf, um ein Datenverarbeiten an Daten auszuführen, die durch die Rechenentität **1100** geliefert werden. Daher sendet die Computerentität die Integritätsmetrikdaten zu einem entfernten Server **1102**, dem durch eine Smartcard vertraut wird, der durch ein Vergleichen dieser mit einem Satz von erwarteten Integritätsmetriken verifiziert, daß die Integritätsmetrikdaten, die durch die Überwachungskomponente geliefert werden, korrekt sind. Die erwarteten Integritätsmetriken können entweder durch die Überwachungskomponente selbst, von vorgespeicherten Daten innerhalb dieser Komponente oder wo die Computerplattform von einem gemeinsamen Typ ist, geliefert werden, der vertrauenswürdige Server **1102** kann Sätze von erwarteten Integritätsmetriken für diesen Typ einer Computerplattform speichern. In jedem Fall führt der vertrauenswürdige Server **1102** das berechnungsmäßig schwere Datenverarbeiten durch, das zu einer Verifizierung der Integritätsmetriken mit den erwarteten Integritätsmetriken erforderlich ist, und signiert das Ergebnis dieser Verifizierung digital.

[0151] Abhängig davon, wie das Token-Gerät vorprogrammiert ist, und von der Größe einer Datenverarbeitungsfähigkeit, die auf dem vertrauenswürdigen Token-Gerät gelegen ist, sind verschiedene alternative Versionen dieses dritten Betriebsmodus verfügbar.

[0152] Bei einem Schritt **1200** authentifiziert der vertrauenswürdige Token die vertrauenswürdige Komponente, wie es hierin zuvor beschrieben ist. Bei einem Schritt **1201** fordert die Smartcard die vertrauenswürdige Komponente auf, die Integritätsmetriken der Computerplattform zu verifizieren und zu der Smartcard zurück zu berichten. Bei einem Schritt **1202** sendet die vertrauenswürdige Komponente, die die Integritätsmetrikdaten als einen Teil eines fortlaufenden Überwachens derselben der Rechenplattform verfügbar hat, die Integritätsmetrikdaten zu der Smartcard, zusammen mit einem Satz von zertifizierten erwarteten Integritätsmetriken für diese Computerplattform. Bei einem Schritt **1203** sendet die Smartcard die empfangenen Integritätsmetrikdaten und die zertifizierten erwarteten Integritätsmetrikdaten zu einer Berechnung zu dem vertrauenswürdigen Dritteilnehmerserver. Diese Nachricht umfaßt auch eine Identifizierung des Smartcard-Geräts selbst. Ein Senden der Integritätsmetrikdaten und erwarteten Integritätsmetrikdaten von der Smartcard zu dem vertrauenswürdigen Server findet über die Computerentität selbst statt, die die Daten, z. B. über das Internet, zu dem entfernten vertrauenswürdigen Server **1102** leitet. Bei einem Schritt **1204** verarbeitet der Server die Integritätsmetrikdaten und verifiziert, daß die zertifizierten erwarteten Integritätsmetriken aktuell zertifiziert sind und vergleicht dieselben mit den erwarteten Integritätsmetrikdaten, die von der Smartcard empfangen werden. Dies ist ein berechnungsmäßig schwerer Schritt, für den der vertrauenswürdige Server geeignet ist. Bei einem Schritt **1205** kann der Server dann, wenn derselbe die Integritätsmetrikdaten mit den erwarteten Integritätsmetrikdaten verglichen hat, Verifizierungsdaten über die Computerentität zurück zu der Smartcard senden. Die Verifizierungsda-

ten können eine digitale Signatur des Servers aufweisen. Bei einem Schritt **1206** empfängt die Smartcard die Verifizierungsdaten, die eine Datensignatur aufweisen, und akzeptiert entweder diese digitale Signatur als gültig oder lehnt dieselbe ab, und daher die Verifizierungsdaten.

[0153] Bei einer alternativen Anordnung kann die vertrauenswürdige Komponente direkt mit einem Dritteilnehmerserver kommunizieren. Anstelle der Schritte **1202** und **1203** sendet die vertrauenswürdige Komponente den Satz von gemessenen Integritätsmetriken der Computerplattform zu einem Dritteilnehmer (die vertrauenswürdige Komponente weiß entweder, welchem Dritteilnehmerserver durch die Smartcard vertraut wird, oder die Smartcard muß spezifizieren, welcher Dritteilnehmerserver verwendet werden sollte), zusammen mit der eigenen digitalen Signatur der vertrauenswürdigen Komponente und empfängt von dem Dritteilnehmerserver das Ergebnis der Verifizierung dieser Integritätsmetriken und zusammen mit einer digitalen Signatur. Der Dritteilnehmerserver vergleicht den Satz von Integritätsmetriken, die von der vertrauenswürdigen Komponente empfangen werden, mit dem eigenen gespeicherten Satz desselben oder einem wiedererlangten Satz von erwarteten Integritätsmetriken für den Typ einer Computerplattform, die durch die vertrauenswürdige Komponente identifiziert ist, und fügt eine digitale Signatur desselben hinzu. Die vertrauenswürdige Komponente sendet, wenn dieselbe die digitale Signatur empfangen hat, dann den Satz von Integritätsmetriken zusammen mit der digitalen Signatur zu der Smartcard.

[0154] Aus der Perspektive der Smartcard muß eine jegliche Anwendung, die mit der Smartcard in Wechselwirkung tritt, entweder eine graphische Benutzerschnittstelle oder eine andere Anwendung, sich der Tatsache bewußt sein, daß die Smartcard eine Wechselwirkung mit einer vertrauenswürdigen Komponente einer Plattform anfordern kann. In dem Fall, wo die Smartcard erfordert, mit einer Dritteilnehmer-Rechenentität in Wechselwirkung zu treten, muß die Anwendung, die mit der Smartcard in Wechselwirkung steht, auch der Smartcard erlauben, mit einem Netzwerkserver in Wechselwirkung zu treten. Bei einer bevorzugten Implementierung jedoch sollte die Smartcard in der Lage sein, einen Zugriff auf Integritätsverifizierungsdaten einer Computerplattform unabhängig von der Anwendung anzufordern, mit der dieselbe auf einer Computerentität spricht.

[0155] Auf ein Empfangen einer Anforderung von einer Anwendung einer Rechenentität hin, um eine Funktionalität der Smartcard zu verwenden, z. B. um eine Transaktion zu autorisieren, kann die Smartcard eine Anforderung einleiten, daß die Überwachungskomponente Überwachungsinformationen über die Vertrauenswürdigkeit des Zustands der Computerplattform liefert. Eine Kommunikation zwischen der Smartcard und der vertrauenswürdigen Komponente findet durch ein Protokollmodul statt, das auf der Computerplattform gelegen ist und das für Kommunikationen zwischen der Rechenentität und dem Smartcard-Token-Gerät verantwortlich ist. Wenn eine Anwendung auf dem PC einen Zugriff auf die Smartcard erfordert, handhabt der Protokollstapel diese Kommunikationen. Die Rechenentität kann daher Befehle filtern, die von der Karte kommen und unabhängig von der Rechenentitätsanwendung sind, wie beispielsweise ein Überprüfen der Integrität der Computerplattform, und kann Befehle aufnehmen, die von der Smartcard kommen. Von dem Standpunkt der Anwendung betrachtet, sind Wechselwirkungen der Smartcard mit anderen Betriebsmitteln auf der Rechenentität transparent. Dies kann unter Verwendung der Technologie in „smartcards – from security tokens to intelligent adjuncts", von Boris Balacheff, Bruno Van Wilder und David Chan veröffentlicht in CARDIS 1998 Proceedings, zusammengeführt mit einer PCSC-Technologie geschehen.

[0156] Der Schritt **1201** kann somit durch die Smartcard als ein Ergebnis eines einer Anzahl von unterschiedlichen Auslöseereignissen eingeleitet werden. Ein möglicher Auslöser ist der Empfang einer Anforderung von der graphischen Benutzerschnittstelle über das Monitor-Untersystem durch die Smartcard, um die Vertrauenswürdigkeit der Plattform zu überprüfen. Dieses Signal wird durch die graphische Benutzerschnittstelle ansprechend auf Tastenanschlagseingaben und/oder Zeigegeräteingaben von einem Benutzer erzeugt. Alternativ kann die Smartcard eine Anforderung nach einem Zugriff auf eine Funktionalität empfangen, die durch eine Anwendung erzeugt wird, die entweder auf der lokalen Rechenentität gelegen ist oder auf einer entfernten Rechenentität gelegen ist. Eine Verifizierung einer Integrität geht dann im wesentlichen weiter, wie es oben mit Bezug auf Fig. 12 gezeigt ist.

[0157] Idealerweise ist der Server mit der Smartcard verbunden: z. B. können sowohl der Server als auch die Smartcard durch den gleichen Verkäufer oder Körper ausgestellt sein, wie beispielsweise einen Internetdienstanbieter.

[0158] Wo z. B. die Smartcard durch einen Internetdienstanbieter bereitgestellt ist und die Smartcard nicht in der Lage ist, die Vertrauenswürdigkeit einer Rechenentität zu authentifizieren, kann dann der Internetdienstanbieter sich entweder weigern, mit der Rechenentität zu kommunizieren, oder kann einen begrenzten Satz einer Funktionalität, wie beispielsweise diejenigen, die der allgemeinen Öffentlichkeit verfügbar sind, der Rechenentität eher als einen vollen Satz von Diensten bereitstellen, die lediglich registrierten Teilnehmern verfügbar sind.

[0159] Wenn die vertrauenswürdige Komponente bereitgestellt ist, können bei einer spezifischen Implementierung gemäß der vorliegenden Erfindung die verbleibenden Elemente, die notwendig sind, damit die Smartcard und die Anwendung miteinander kommunizieren können, durch im wesentlichen routinemäßige Modifizierungen an herkömmlichen Anwendungen bereitgestellt werden. Die notwendige Wechselwirkung kann z. B. mit einer herkömmlichen Smartcard bereitgestellt werden, die vorprogrammiert ist, um auf ein Abrufsignal von einer Anwendung anzusprechen, durch ein Einleiten einer Aufforderung an eine vertrauenswürdige Komponente, um Integritätsmetriküberprüfungen durchzuführen.

[0160] Unter Bezugnahme auf Fig. 13 sind hierin schematische Elemente einer möglichen Implementierung der ersten Generation eines Systems gemäß der vorliegenden Erfindung dargestellt. Fig. 13 zeigt eine logische Ansicht von Komponenten einer Implementierung der ersten Generation. Eine vertrauenswürdige Komponente **1500** weist einen Prozessor und einen Speicher auf, die physisch von einer Computerplattform getrennt und in einem vertrauenswürdigen logischen Raum gelegen sind, wie es hierin zuvor beschrieben ist. Die Computerplattform weist einen weiteren Prozessor und eine Datenspeichereinrichtung auf und ist in einem Computerplattformraum **1501** gelegen. Ein Untersystem **1502** und Anwendungen **1503** sind in dem Computerraum **1501** gelegen. Das Untersystem **1502** enthält eine Anwendungsschnittstelle **1503**, eine Verifizierungsanwendung **1504** und eine Smartcard-Schnittstelle **1505**. Die Smartcard-Schnittstelle kommuniziert mit einem Smartcard-Leser **1506**, der sich ebenfalls in dem Computerplattformraum **1501** befindet und eine Smartcard **1507** annimmt. Die Anwendungsschnittstelle **1503** enthält den PCIA-Stapel.

[0161] Unter Bezugnahme auf Fig. 14 hierin ist schematisch ein Verfahren einer Operation der Implementierung der ersten Generation von Fig. 13 hierin dargestellt, wobei die Smartcard **1507** mit der vertrauenswürdigen Komponente in Wechselwirkung tritt, bevor dieselbe eine Funktionalität „X" ansprechend auf eine Anforderung nach einer Funktionalität „X" von einer Anwendung gibt. Bei diesem Betriebsverfahren könnten Aufrufe an den PCSC-Stapel durch den PCIA-Stapel vorgenommen werden, um die PCIA-Funktionalität transparent bereitzustellen. Bei dem besten Modus würde der PCSC-Stapel den PCIA-Stapel und eine Funktionalität umfassen. Bei einem Schritt **1600** sendet die Anwendung die Anforderung nach einer Funktionalität „X" über den PCSC-Stapel, der in der Anwendungsschnittstelle **1503** in dem Untersystem **1502** gelegen ist, an die Smartcard. Bei einem Schritt **1601** sendet der PCSC-Stapel einen Befehl an die Smartcard, wobei eine Funktionalität „X" von der Smartcard angefordert wird. Bei einem Schritt **1602** spricht die Smartcard mit einer Anforderung nach einer Verifizierung der Vertrauenswürdigkeit der Rechenentität an, die durch den PCSC-Stapel empfangen wird. Bei einem Schritt **1603** empfängt der PCSC-Stapel die Anforderung; durch eine PCIA-Funktionalität wird die Nachricht zu der vertrauenswürdigen Komponente gesendet. Entweder durch ein Verwenden des getrennten PCIA-Stapels oder durch eine existierende PCIA-Funktionalität wird die Nachricht zu der vertrauenswürdigen Komponente gesendet, um die Integritätsüberprüfungen einzuleiten. Dies kann direkt von der Anwendungsschnittstelle **1503** zu der vertrauenswürdigen Komponente **1500** gesendet werden. Bei der ersten spezifischen Implementierung werden die Verifizierungsanwendung **1504** und das Untersystem **1502** durch die vertrauenswürdige Komponente verwendet, um die Integritätsmetriküberprüfungen durchzuführen. Bei einer Implementierung eines besten Modus enthält die vertrauenswürdige Komponente **1500** eine Funktionalität innerhalb derselben, um diese Integritätsüberprüfungen an der Computerplattform direkt durchzuführen. Bei einem Schritt **1506** sendet die vertrauenswürdige Komponente (in Verbindung mit der Verifizierungsanwendung bei der ersten Implementierung, ganz alleine bei dem besten Modus) das Ergebnis der Integritätsverifizierung mit einer digitalen Signatur und Zertifikatdaten zu der Smartcard. Bei einem Schritt **1607** empfängt die Smartcard das Ergebnis der Integritätsverifizierung mit der digitalen Signatur, verifiziert die digitale Signatur, um die vertrauenswürdige Komponente zu authentifizieren, und, falls zufriedengestellt, vertraut dieselbe dem Ergebnis der Verifizierung einer Integrität. Basierend auf diesem Ergebnis entscheidet dieselbe dann, ob die Anwendung mit einer Funktionalität „X" versehen wird oder nicht. Die Anwendung kann dann fortfahren. Die Smartcard hat die Vertrauenswürdigkeit der Computerplattform durch ein Auffordern verifiziert, um eine Integritätsabfrage an der vertrauenswürdigen Komponente der Rechenentität durchzuführen, und lediglich wenn dieselbe über das Ergebnis dieser Abfrage zufriedengestellt ist, akzeptiert dieselbe, der Anwendung eine Funktionalität zu liefern.

Patentansprüche

1. Ein System einer Rechenvorrichtung, das folgende Merkmale aufweist:
eine Rechenplattform (**10**), die einen ersten Datenprozessor (**21**) und eine erste Datenspeichereinrichtung (**22**) aufweist; und
ein Token-Gerät (**19**, **1101**), das von der Rechenplattform (**10**) physisch unterschiedlich und trennbar ist,
dadurch gekennzeichnet, daß das System ferner folgende Merkmale aufweist:
eine Überwachungskomponente (**24**), die einen zweiten Datenprozessor (**30**) und eine zweite Datenspeichereinrichtung (**3**, **4**) aufweist, wobei die Überwachungskomponente (**24**) konfiguriert ist, um eine Mehrzahl von Datenüberprüfungen bei der Re-

chenplattform (**10**) durchzuführen, und wobei das Token-Gerät ferner von der Überwachungskomponente physisch unterschiedlich und trennbar ist; und
wobei das Token-Gerät (**19**, **1101**) in einem Betriebsmodus wirksam ist, um eine Integritätsabfrage an die Überwachungskomponente (**24**) zu richten, und das Token-Gerät (**19**, **1101**) keine spezifischen Schritte unternimmt, zu denen dasselbe in der Lage ist, wenn dasselbe keine zufriedenstellende Antwort auf die Integritätsabfrage empfängt.

2. Das System gemäß Anspruch 1, bei dem das Token-Gerät (**19**, **1101**) eine detaillierte Antwort auf die Integritätsabfrage empfängt und die Integritätsantwort verarbeitet, um die Integritätsantwort zu interpretieren.

3. Das System gemäß Anspruch 1, das ferner einen Dritteilnehmerserver (**1102**) aufweist, wobei eine Antwort auf die Integritätsabfrage zu dem Dritteilnehmerserver (**1102**) gesendet wird.

4. Das System gemäß Anspruch 3, bei dem die Überwachungskomponente (**24**) eine detaillierte Integritätsantwort an den Dritteilnehmerserver (**1102**) sendet.

5. Das System gemäß Anspruch 4, bei dem die Überwachungskomponente (**24**) eine detaillierte Integritätsantwort an einen Dritteilnehmerserver (**1102**) sendet, falls dieselbe in der Integritätsabfrage dazu aufgefordert wird.

6. Das System gemäß Anspruch 4, bei dem die Überwachungskomponente (**24**) dem Token-Gerät (**19**, **1101**) eine detaillierte Integritätsantwort berichtet und das Token-Gerät (**19**, **1101**) die Integritätsantwort an den Dritteilnehmerserver (**1102**) sendet, falls dasselbe den Dritteilnehmerserver (**1102**) benötigt, um die detaillierte Integritätsantwort interpretieren zu helfen.

7. Das System gemäß einem der Ansprüche 4 bis 6, bei dem ein Dritteilnehmerserver (**1102**) die Integritätsantwort auf eine Form vereinfacht, in der das Token-Gerät (**19**, **1101**) die Integritätsantwort interpretieren kann.

8. Das System gemäß Anspruch 7, bei dem ein Dritteilnehmerserver (**1102**) eine vereinfachte Integritätsantwort an das Token-Gerät (**19**, **1101**) sendet.

9. Das System gemäß Anspruch 8, das wirksam ist, um der vereinfachten Integritätsantwort Digitale-Signatur-Daten hinzuzufügen, wobei die digitale Signatur den Dritteilnehmerserver (**1102**) dem Token-Gerät (**19**, **1101**) gegenüber authentifiziert.

10. Das System gemäß einem der vorhergehenden Ansprüche, bei dem das Token-Gerät (**19**, **1101**) aufgefordert wird, eine Handlung zu unternehmen.

11. Das System gemäß einem der vorhergehenden Ansprüche, bei dem das Token-Gerät (**19**, **1101**) auffordert, eine Handlung zu unternehmen.

12. Das System gemäß einem der vorhergehenden Ansprüche, bei dem das Token-Gerät (**19**, **1101**) Bilddaten an die Rechenplattform sendet, falls eine zufriedenstellende Antwort auf die Integritätsabfrage empfangen wird, und die Rechenplattform die Bilddaten anzeigt.

13. Das System gemäß einem der vorhergehenden Ansprüche, bei dem die Überwachungskomponente (**24**) zum Einrichten einer eigenen Identität in der Lage ist.

14. Das System gemäß einem der vorhergehenden Ansprüche, das ferner eine Schnittstelleneinrichtung zum Bilden einer Schnittstelle zwischen der Überwachungskomponente (**24**) und dem Token-Gerät (**19**, **1101**) aufweist.

15. Das System gemäß einem der vorhergehenden Ansprüche, wobei das System einer Rechenvorrichtung derart konfiguriert ist, daß die Überwachungskomponente (**24**) die Datenüberprüfungen dem Token-Gerät (**19**, **1101**) berichtet, wobei die Datenüberprüfungen Daten enthalten, die einen Status der Rechenplattform beschreiben.

16. Das System gemäß einem der vorhergehenden Ansprüche, bei dem die spezifische Handlung ein Autorisieren der Rechenplattform (**10**) aufweist, eine Transaktion im Namen eines Benutzers des Systems zu unternehmen.

17. Das System gemäß einem der vorhergehenden Ansprüche, bei dem die spezifische Handlung ein Senden von Verifizierungsdaten an die Rechenplattform aufweist, wobei die Verifizierungsdaten eine korrekte Operation der Rechenplattform verifizieren; woraufhin die Rechenplattform angepaßt ist, um die Verifizierungsdaten auf einem visuellen Anzeigebildschirm anzuzeigen.

18. Das System gemäß einem der vorhergehenden Ansprüche, bei dem das Token-Gerät (**19**, **1101**) eine Smartcard ist.

19. Ein System gemäß einem der vorhergehenden Ansprüche, bei dem das Rechensystem ferner folgende Merkmale aufweist:
eine Schnittstelleneinrichtung für eine Kommunikation zwischen der Rechenplattform (**10**) und dem Token-Gerät (**19**, **1101**), wobei die Schnittstelleneinrichtung mit der Überwachungskomponente (**24**) kom-

muniziert und wobei das Rechensystem konfiguriert ist, derart, daß die Überwachungskomponente (**24**) die Datenüberprüfungen an das Token-Gerät (**19**, **1101**) berichtet, wobei die Datenüberprüfungen Daten enthalten, die einen Status der Rechenplattform beschreiben.

20. Das System gemäß Anspruch 19, bei dem die Überwachungskomponente (**24**) auf eine Kommunikation zwischen dem Token-Gerät (**19**, **1101**) und der Schnittstelleneinrichtung hin aktiviert wird, um bei der Rechenplattform eine Überwachungsoperation durchzuführen, wobei die Überwachungskomponente (**24**) Daten erhält, die einen Betriebsstatus der Rechenplattform beschreiben.

21. Das System gemäß Anspruch 19 oder Anspruch 20, bei dem die Schnittstelleneinrichtung im wesentlichen ganz innerhalb der Überwachungskomponente (**24**) gelegen ist.

22. Das System gemäß Anspruch 19 oder Anspruch 20, bei dem die Schnittstelleneinrichtung die Rechenplattform aufweist.

23. Das System gemäß einem der Ansprüche 19 bis 22, bei dem die Schnittstelleneinrichtung eine Smartcard-Lesevorrichtung aufweist.

24. Das System gemäß einem der Ansprüche 19 bis 23, bei dem die Schnittstelleneinrichtung einen PCSC-Stapel gemäß PCSC Workgroup PC/SC Specification 1.0 aufweist.

25. Das System gemäß einem der Ansprüche 19 bis 24, bei dem die Überwachungskomponente (**24**) eine Verifizierungseinrichtung aufweist, die konfiguriert ist, um Zertifizierungsdaten zu erhalten, die die Statusdaten unabhängig zertifizieren, und um die Zertifizierungsdaten an die Schnittstelleneinrichtung zu liefern.

26. Das System gemäß einem der Ansprüche 19 bis 25, bei dem die Schnittstelleneinrichtung konfiguriert ist, um Daten gemäß einem proaktiven Protokoll zu senden und zu empfangen.

27. Ein Token-Gerät, das einen Datenprozessor und ein Speichergerät aufweist, wobei das Token-Gerät (**19**, **1101**) konfiguriert ist, um eine Durchführung von zumindest einer Datenverarbeitungs- oder Signalisierungsfunktion zu erlauben:
dadurch gekennzeichnet, daß das Token-Gerät (**19**, **1101**) wirksam ist, um:
von einem Element eines Rechensystems eine Aufforderung zu empfangen, um die zumindest eine Datenverarbeitungs- oder Signalisierungsfunktion durchzuführen;
eine Anforderung nach Integritätsdaten von einer Überwachungskomponente (**24**) in dem Rechensystem zu erzeugen, um die Integrität des Rechensystems zu bestätigen;
die Integritätsdaten von der Überwachungskomponente zu empfangen;
falls die an das Token-Gerät (**19**, **1101**) gelieferten Integritätsdaten zufriedenstellend sind, dann erlaubt das Token-Gerät (**19**, **1101**) die Funktion; und
falls die durch das Token-Gerät (**19**, **1101**) empfangenen Integritätsdaten nicht zufriedenstellend sind, dann verweigert das Token-Gerät (**19**, **1101**) die Funktion.

28. Das Token-Gerät gemäß Anspruch 27, wobei das Gerät konfiguriert ist, auf ein Abrufsignal anzusprechen, das gemäß PC/SC Specification 1.0 wirksam ist, wobei das Token-Gerät (**19**, **1101**) zum Einleiten eines Befehls in der Lage ist, der durch einen Softwarestapel an der Computerentität gehandhabt werden soll, ansprechend auf das Abrufsignal gemäß dem Abrufsignal gemäß einem proaktiven Protokoll.

29. Ein Verfahren zum Erhalten einer Verifizierung eines Zustands einer Computerentität, wobei die Computerentität eine Computerplattform und eine Überwachungskomponente (**24**) aufweist, wobei das Verfahren folgende Schritte aufweist:
Anfordern eines Zugriffs auf eine Funktionalität von einem Token-Gerät (**19**, **1101**);
ansprechend auf die Anforderung eines Zugriffs auf die Funktionalität, Erzeugen eines Anforderungssignals, das Integritätsdaten von der Überwachungskomponente (**24**) anfordert, durch das Token-Gerät (**19**, **1101**), um die Integrität der Computerplattform zu bestätigen;
ansprechend auf die Anforderung nach Integritätsdaten, Berichten von Integritätsdaten an das Token-Gerät (**19**, **1101**) durch die Überwachungskomponente (**24**), wobei die Integritätsdaten ein Ergebnis einer Überwachungsoperation beschreiben;
bei Empfang von zufriedenstellenden Integritätsdaten, Anbieten der Funktionalität durch das Token-Gerät (**19**, **1101**); und
bei Empfang von nicht zufriedenstellenden Integritätsdaten, Verweigern der Funktionalität durch das Token-Gerät (**19**, **1101**).

30. Ein Verfahren gemäß Anspruch 29, bei dem die Anforderung einer Funktionalität durch eine Anwendung vorgenommen wird, die auf der Rechenplattform läuft.

31. Ein Verfahren gemäß Anspruch 29 oder Anspruch 30, bei dem die Überwachungsoperation folgende Schritte aufweist:
die Überwachungskomponente (**24**) führt eine oder eine Mehrzahl von Datenüberprüfungen bei Komponenten der Rechenplattform (**10**) aus; und
die Überwachungskomponente (**24**) kann einen Satz von zertifizierten Referenzdaten zusammen mit den Datenüberprüfungen berichten.

32. Das Verfahren gemäß Anspruch 31, bei dem die zertifizierten Referenzdaten einen Satz von Metriken umfassen, die zu erwarten sind, wenn bestimmte Komponenten der Rechenplattform (**10**) gemessen werden, und Digital-Signatur-Daten umfassen, die eine Entität identifizieren, die die Referenzdaten zertifiziert.

33. Das Verfahren gemäß einem der Ansprüche 29 bis 33, das den Schritt eines Berichtens der Integritätsdaten durch ein Erzeugen einer visuellen Anzeige von Bestätigungsdaten aufweist.

34. Das Verfahren gemäß einem der Ansprüche 29 bis 33, das ferner den Schritt eines Hinzufügens von Digitale-Signatur-Daten zu den Integritätsdaten aufweist, wobei die Digitale-Signatur-Daten die Überwachungskomponente (**24**) identifizieren; und Senden der Integritätsdaten und der Digitale-Signatur-Daten an das Token-Gerät (**19**, **1101**).

35. Das Verfahren gemäß einem der Ansprüche 29 bis 34, bei dem die Überwachungskomponente (**24**) eine detaillierte Integritätsantwort an einen Dritteilnehmerserver (**1102**) sendet, falls dieselbe durch das Token-Gerät (**19**, **1101**) in einer Integritätsabfrage aufgefordert wird.

36. Das Verfahren gemäß Anspruch 35, bei dem die Überwachungskomponente (**24**) eine detaillierte Integritätsantwort an das Token-Gerät (**19**, **1101**) berichtet und das Token-Gerät (**19**, **1101**) die Integritätsantwort an einen Dritteilnehmerserver (**1102**) sendet, falls dasselbe den Dritteilnehmerserver (**1102**) benötigt, um die detaillierte Integritätsantwort zu interpretieren.

37. Das Verfahren gemäß Anspruch 35 oder 36, bei dem ein Dritteilnehmerserver (**1102**) die Integritätsantwort zu einer Form vereinfacht, in der das Token-Gerät (**19**, **1101**) die Integritätsantwort interpretieren kann.

38. Das Verfahren gemäß Anspruch 37, bei dem ein Dritteilnehmerserver (**1102**) eine vereinfachte Integritätsantwort an das Token-Gerät (**19**, **1101**) sendet.

39. Das Verfahren gemäß Anspruch 38, das ferner folgende Schritte aufweist:
Hinzufügen von Digitale-Signatur-Daten zu einer vereinfachten Integritätsantwort, wobei die Digitale-Signatur-Daten einen Dritteilnehmerserver (**1102**) dem Token-Gerät (**19**, **1101**) authentifizieren.

40. Ein Verfahren gemäß einem der Ansprüche 29 bis 39, das ferner den Schritt eines Programmierens des Token-Geräts (**19**, **1101**) aufweist, um auf ein empfangenes Abrufsignal von der Rechenplattform anzusprechen;
wobei die Anforderung einer Funktionalität den Schritt eines Empfangens eines Abrufsignals von der Rechenplattform durch das Token-Gerät (**19**, **1101**) aufweist; und
wobei das Token-Gerät (**19**, **1101**) ansprechend auf das empfangene Abrufsignal die Anforderung nach Integritätsdaten durch die Überwachungskomponente (**24**) erzeugt.

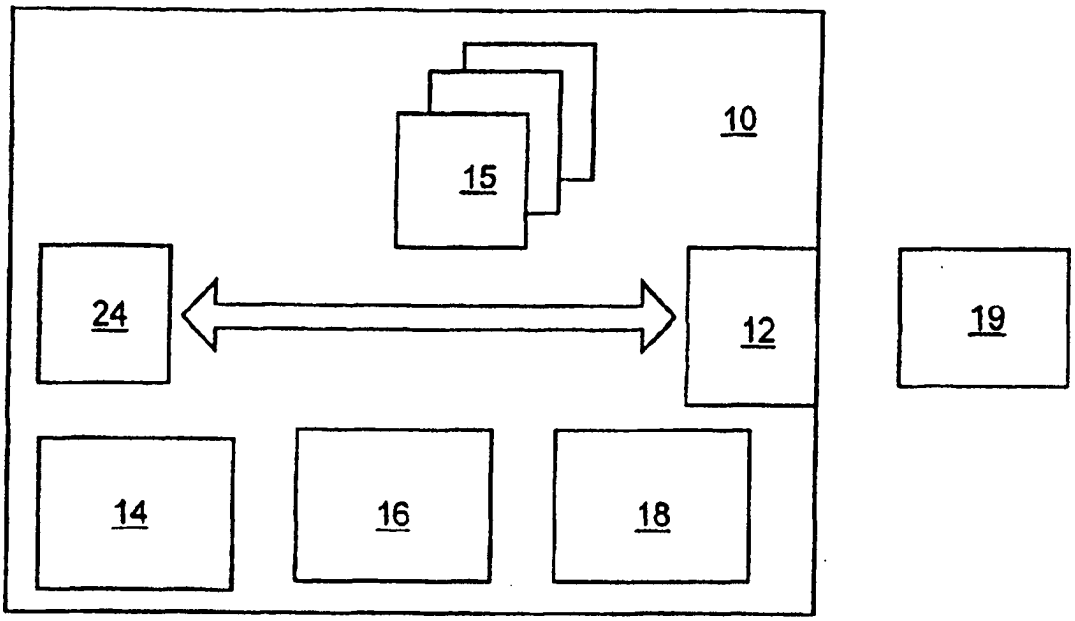
41. Ein Verfahren gemäß Anspruch 40, bei dem das Abrufsignal von einem Anwendungsprogramm empfangen wird, das auf der Rechenplattform läuft.

42. Ein Verfahren gemäß einem der Ansprüche 29 bis 41, bei dem das Token-Gerät (**19**, **1101**) eine Datenverarbeitungsfähigkeit aufweist und sich auf eine erwartete Weise verhält, physisch von der Rechenplattform (**10**) und der Überwachungskomponente (**24**) trennbar ist und eine Kryptographische-Daten-Verarbeitungsfähigkeit aufweist, wobei das Verfahren ferner folgenden Schritt aufweist:
Nachweisen der Identität derselben zu dem Token-Gerät (**19**, **1101**) und Einrichten eines Berichts an das Token-Gerät (**19**, **1101**) von zumindest einer Datenüberprüfung, die an der Rechenplattform (**10**) durchgeführt wird, durch die Überwachungskomponente (**24**).

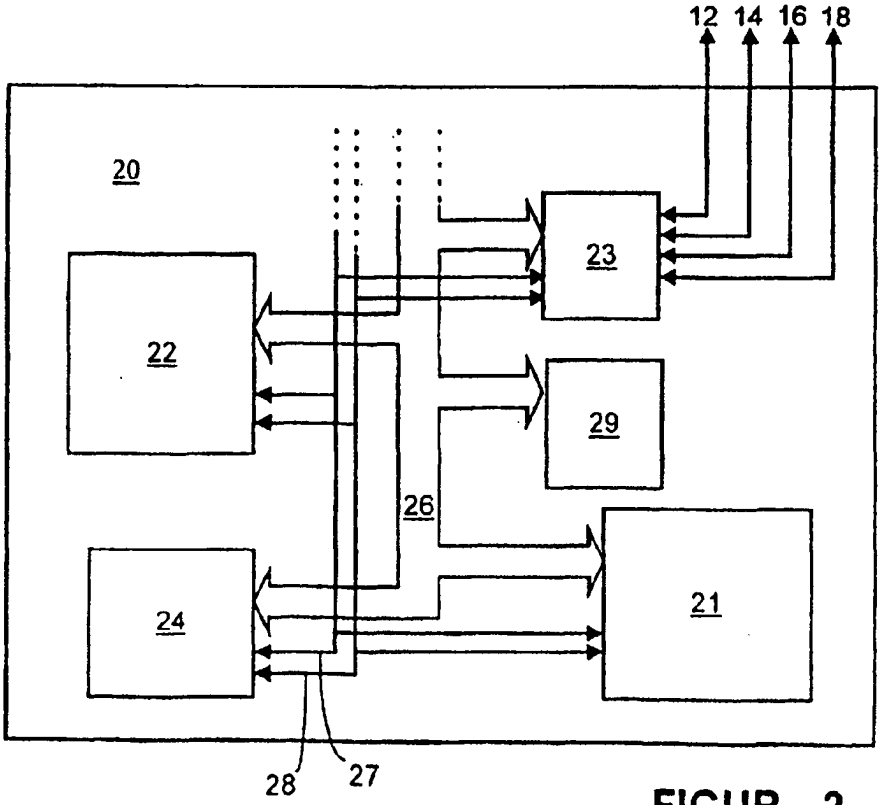
43. Ein Verfahren gemäß einem der Ansprüche 29 bis 42, bei dem das Token-Gerät (**19**, **1101**) eine Smartcard ist.

Es folgen 13 Blatt Zeichnungen

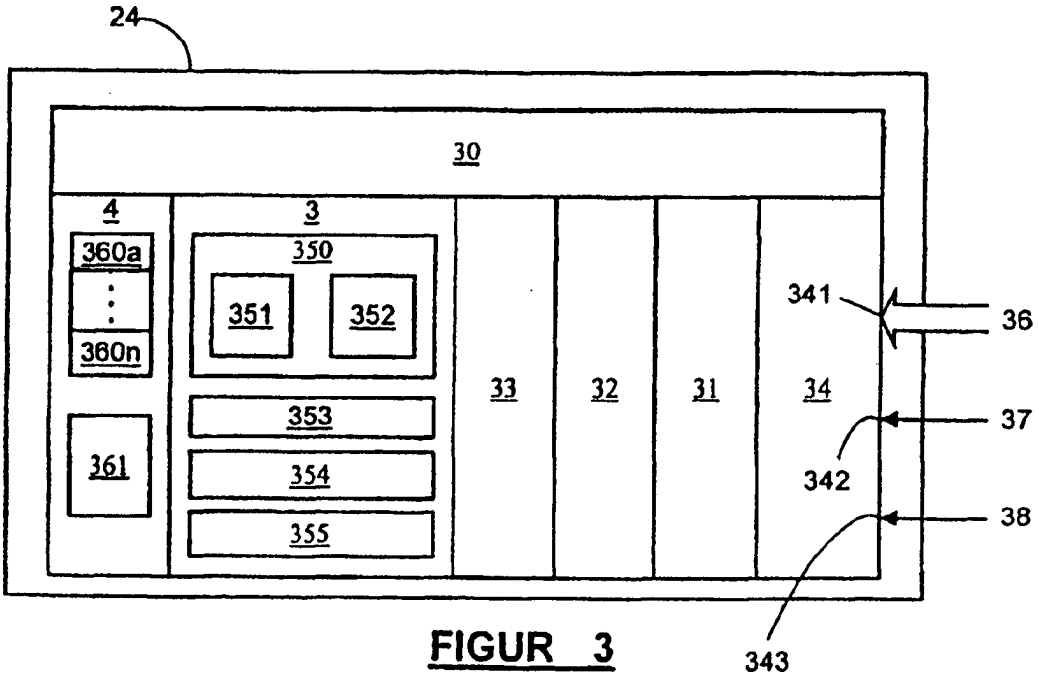
Anhängende Zeichnungen



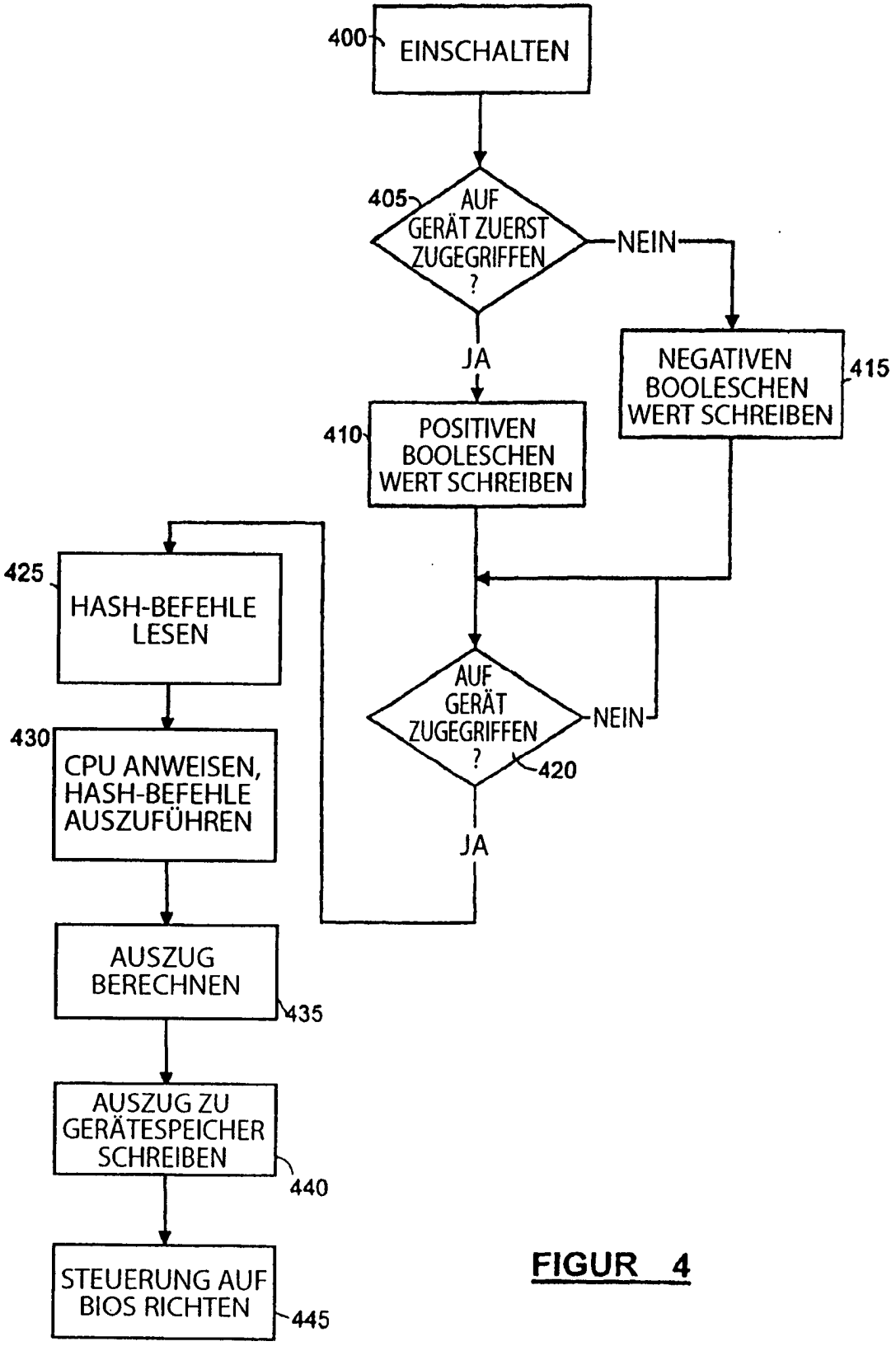
FIGUR 1



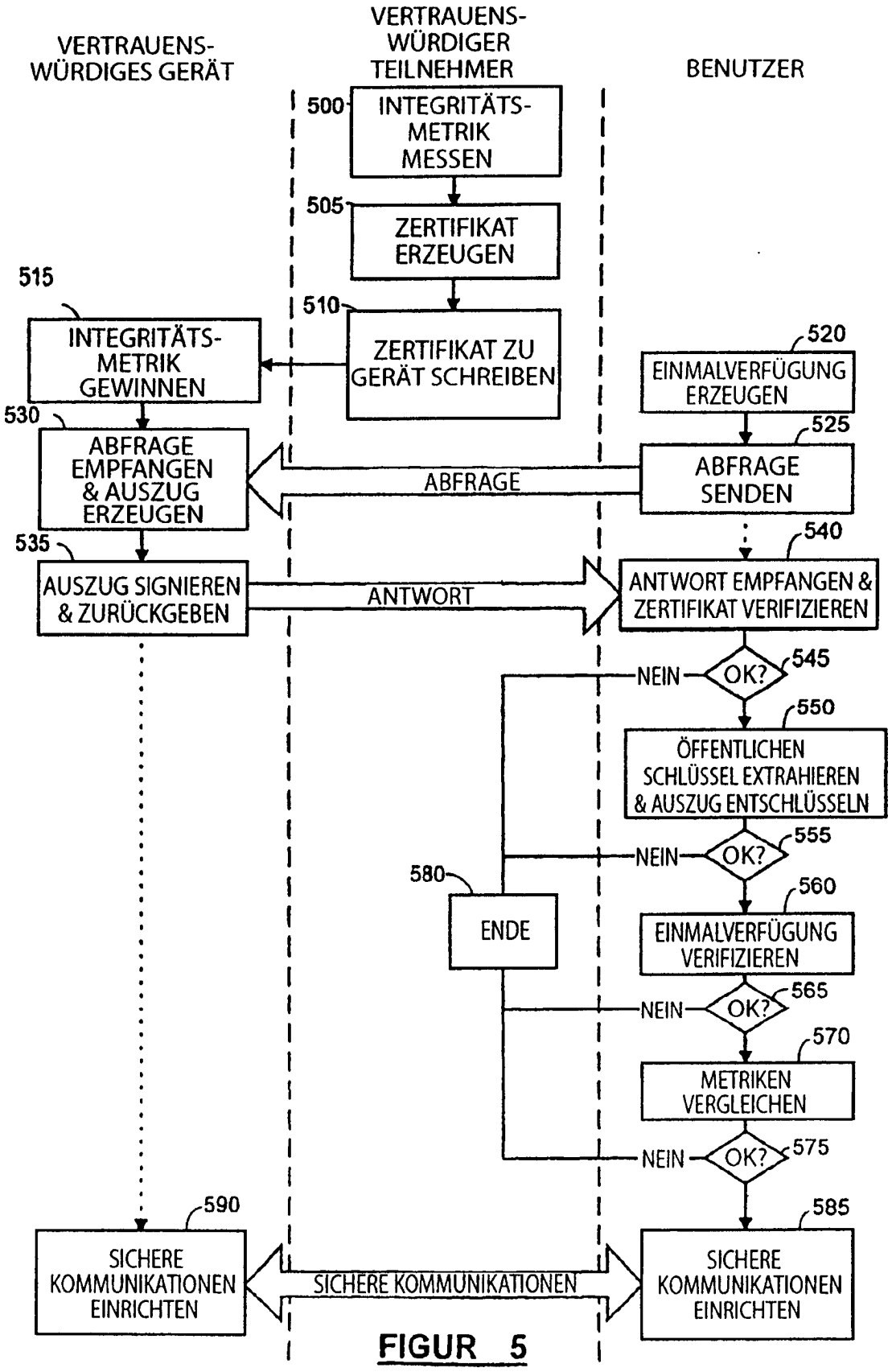
FIGUR 2


24
30
4
3
360a
360n
350
351
352
353
354
355
361
33
32
31
34
341
342
343
36
37
38

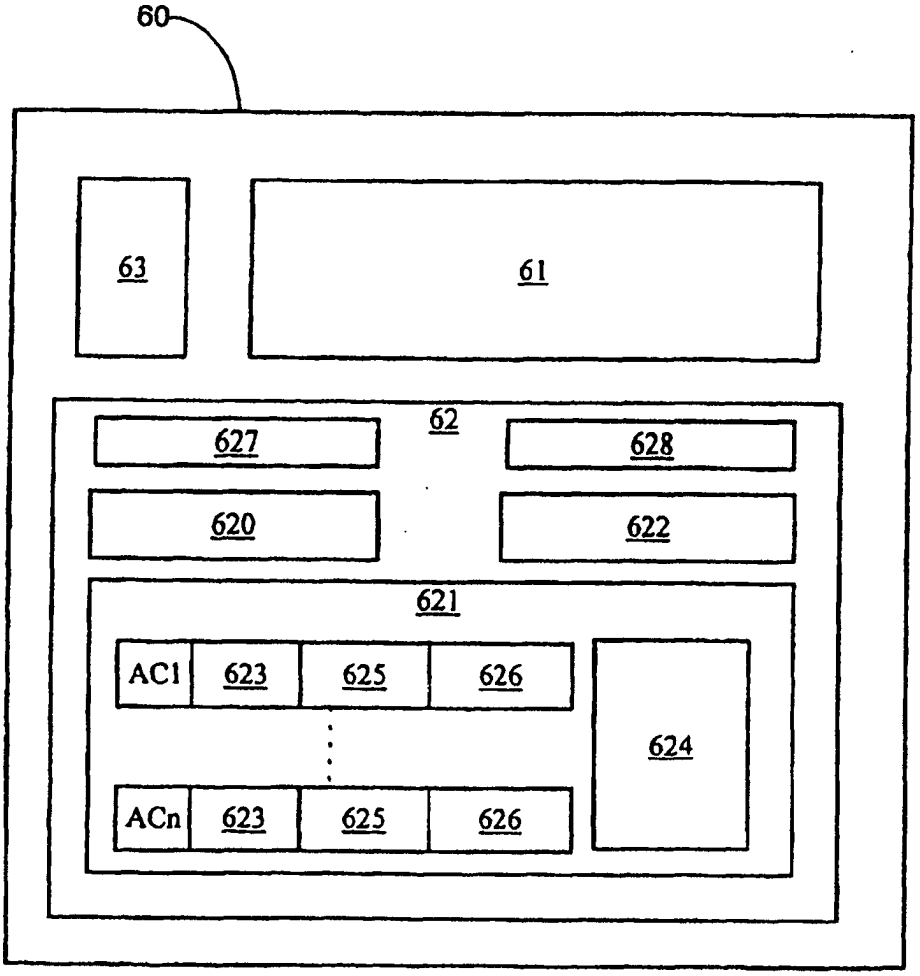
FIGUR 3


400
EINSCHALTEN
405
AUF GERÄT ZUERST ZUGEGRIFFEN ?
NEIN
JA
NEGATIVEN BOOLESCHEN WERT SCHREIBEN
415
410
POSITIVEN BOOLESCHEN WERT SCHREIBEN
425
HASH-BEFEHLE LESEN
AUF GERÄT ZUGEGRIFFEN ?
NEIN
420
JA
430
CPU ANWEISEN, HASH-BEFEHLE AUSZUFÜHREN
AUSZUG BERECHNEN
435
AUSZUG ZU GERÄTESPEICHER SCHREIBEN
440
STEUERUNG AUF BIOS RICHTEN
445

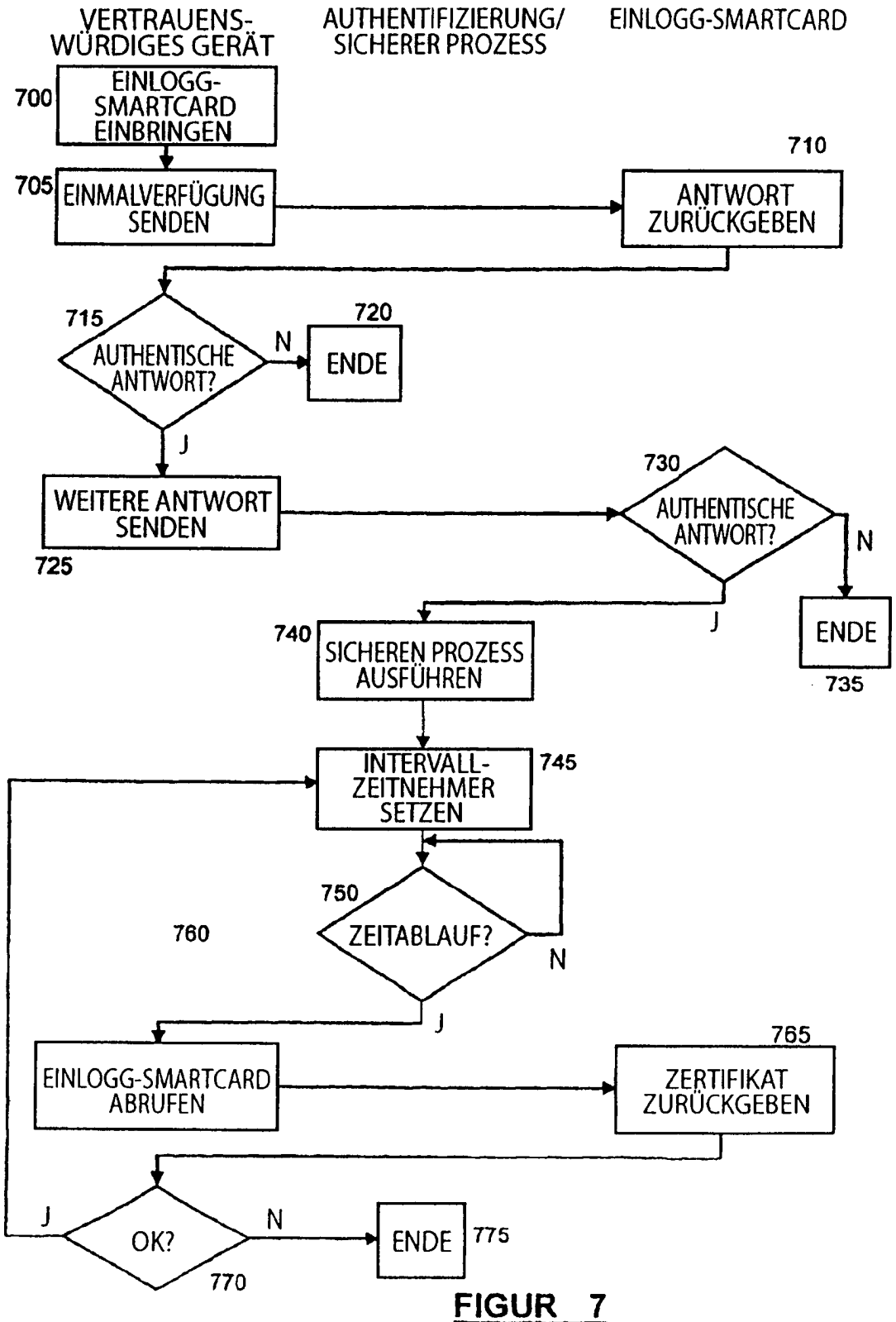
FIGUR 4


VERTRAUENS-
WÜRDIGES GERÄT
VERTRAUENS-
WÜRDIGER
TEILNEHMER
BENUTZER
500
INTEGRITÄTS-
METRIK
MESSEN
505
ZERTIFIKAT
ERZEUGEN
515
510
INTEGRITÄTS-
METRIK
GEWINNEN
ZERTIFIKAT ZU
GERÄT SCHREIBEN
520
EINMALVERFÜGUNG
ERZEUGEN
530
525
ABFRAGE
EMPFANGEN
& AUSZUG
ERZEUGEN
ABFRAGE
ABFRAGE
SENDEN
535
540
AUSZUG SIGNIEREN
& ZURÜCKGEBEN
ANTWORT
ANTWORT EMPFANGEN &
ZERTIFIKAT VERIFIZIEREN
NEIN
OK?
545
550
ÖFFENTLICHEN
SCHLÜSSEL EXTRAHIEREN
& AUSZUG ENTSCHLÜSSELN
NEIN
OK?
555
580
560
ENDE
EINMALVERFÜGUNG
VERIFIZIEREN
NEIN
OK?
565
570
METRIKEN
VERGLEICHEN
NEIN
OK?
575
590
585
SICHERE
KOMMUNIKATIONEN
EINRICHTEN
SICHERE KOMMUNIKATIONEN
SICHERE
KOMMUNIKATIONEN
EINRICHTEN

FIGUR 5


60
63
61
62
627
628
620
622
621
AC1
623
625
626
624
ACn
623
625
626

FIGUR 6


VERTRAUENS-WÜRDIGES GERÄT
AUTHENTIFIZIERUNG/ SICHERER PROZESS
EINLOGG-SMARTCARD
700
EINLOGG-SMARTCARD EINBRINGEN
705
EINMALVERFÜGUNG SENDEN
710
ANTWORT ZURÜCKGEBEN
715
AUTHENTISCHE ANTWORT?
N
720
ENDE
J
WEITERE ANTWORT SENDEN
725
730
AUTHENTISCHE ANTWORT?
N
J
ENDE
735
740
SICHEREN PROZESS AUSFÜHREN
INTERVALL-ZEITNEHMER SETZEN
745
750
ZEITABLAUF?
760
N
J
EINLOGG-SMARTCARD ABRUFEN
765
ZERTIFIKAT ZURÜCKGEBEN
J
OK?
N
770
ENDE
775

FIGUR 7

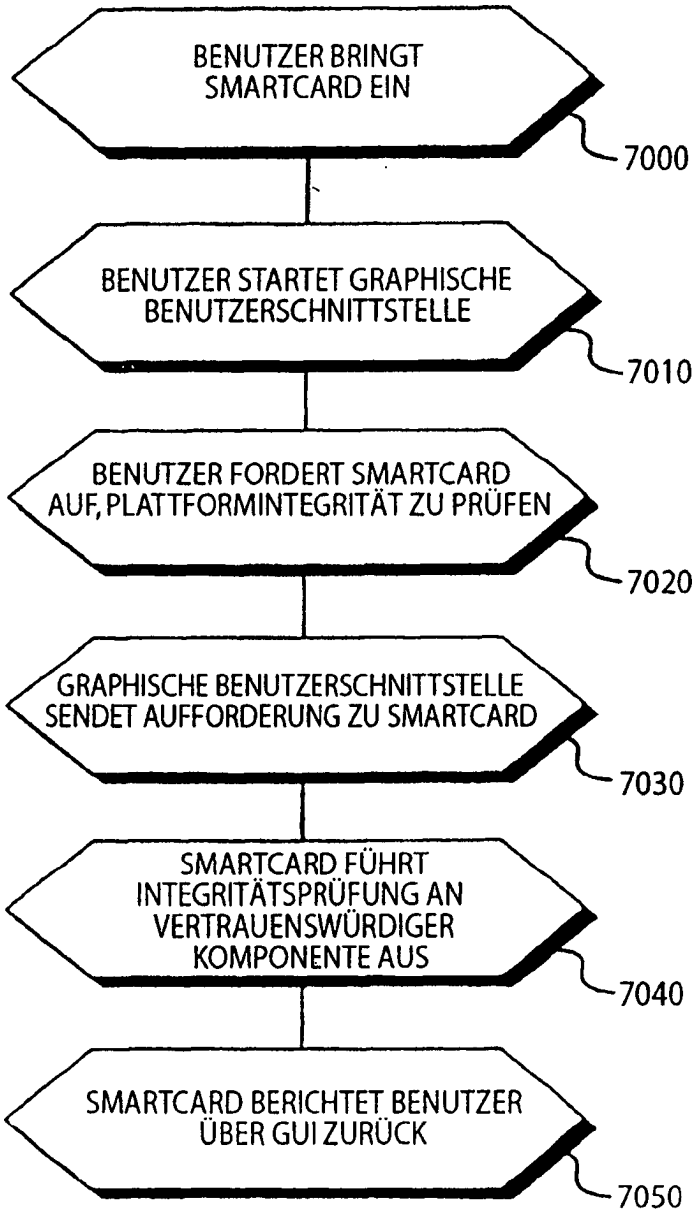

BENUTZER BRINGT SMARTCARD EIN
7000
BENUTZER STARTET GRAPHISCHE BENUTZERSCHNITTSTELLE
7010
BENUTZER FORDERT SMARTCARD AUF, PLATTFORMINTEGRITÄT ZU PRÜFEN
7020
GRAPHISCHE BENUTZERSCHNITTSTELLE SENDET AUFFORDERUNG ZU SMARTCARD
7030
SMARTCARD FÜHRT INTEGRITÄTSPRÜFUNG AN VERTRAUENSWÜRDIGER KOMPONENTE AUS
7040
SMARTCARD BERICHTET BENUTZER ÜBER GUI ZURÜCK
7050

Fig. 8

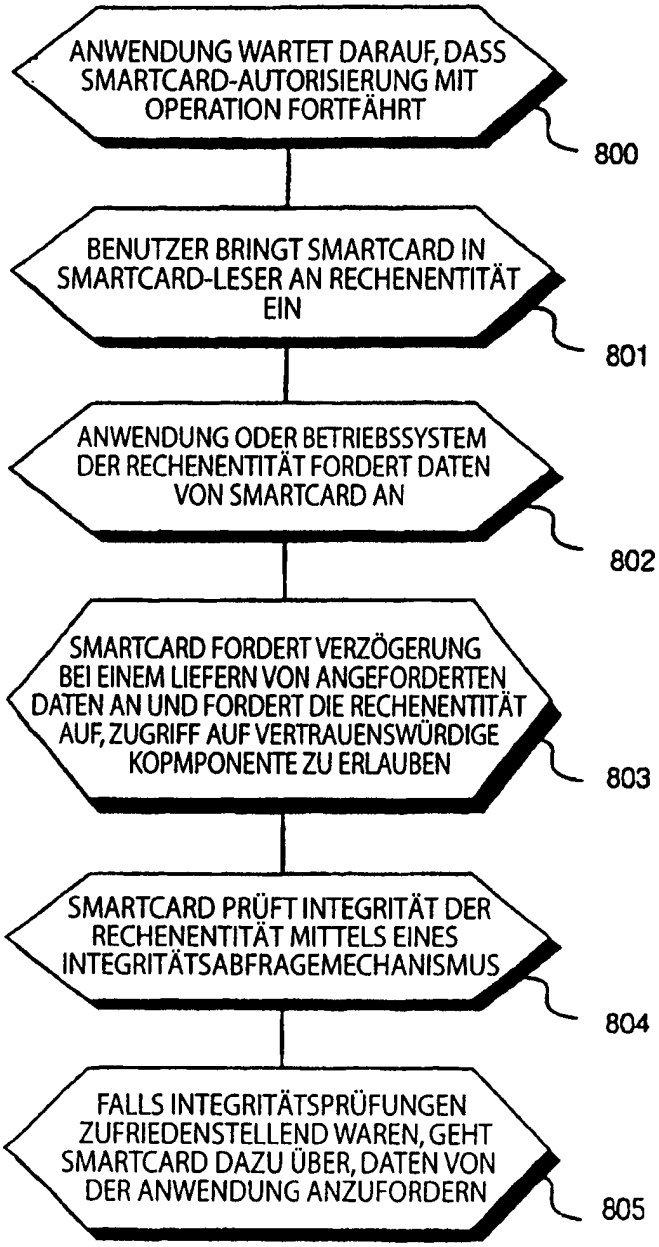

ANWENDUNG WARTET DARAUF, DASS SMARTCARD-AUTORISIERUNG MIT OPERATION FORTFÄHRT
800
BENUTZER BRINGT SMARTCARD IN SMARTCARD-LESER AN RECHENENTITÄT EIN
801
ANWENDUNG ODER BETRIEBSSYSTEM DER RECHENENTITÄT FORDERT DATEN VON SMARTCARD AN
802
SMARTCARD FORDERT VERZÖGERUNG BEI EINEM LIEFERN VON ANGEFORDERTEN DATEN AN UND FORDERT DIE RECHENENTITÄT AUF, ZUGRIFF AUF VERTRAUENSWÜRDIGE KOPMPONENTE ZU ERLAUBEN
803
SMARTCARD PRÜFT INTEGRITÄT DER RECHENENTITÄT MITTELS EINES INTEGRITÄTSABFRAGEMECHANISMUS
804
FALLS INTEGRITÄTSPRÜFUNGEN ZUFRIEDENSTELLEND WAREN, GEHT SMARTCARD DAZU ÜBER, DATEN VON DER ANWENDUNG ANZUFORDERN
805

Fig. 9

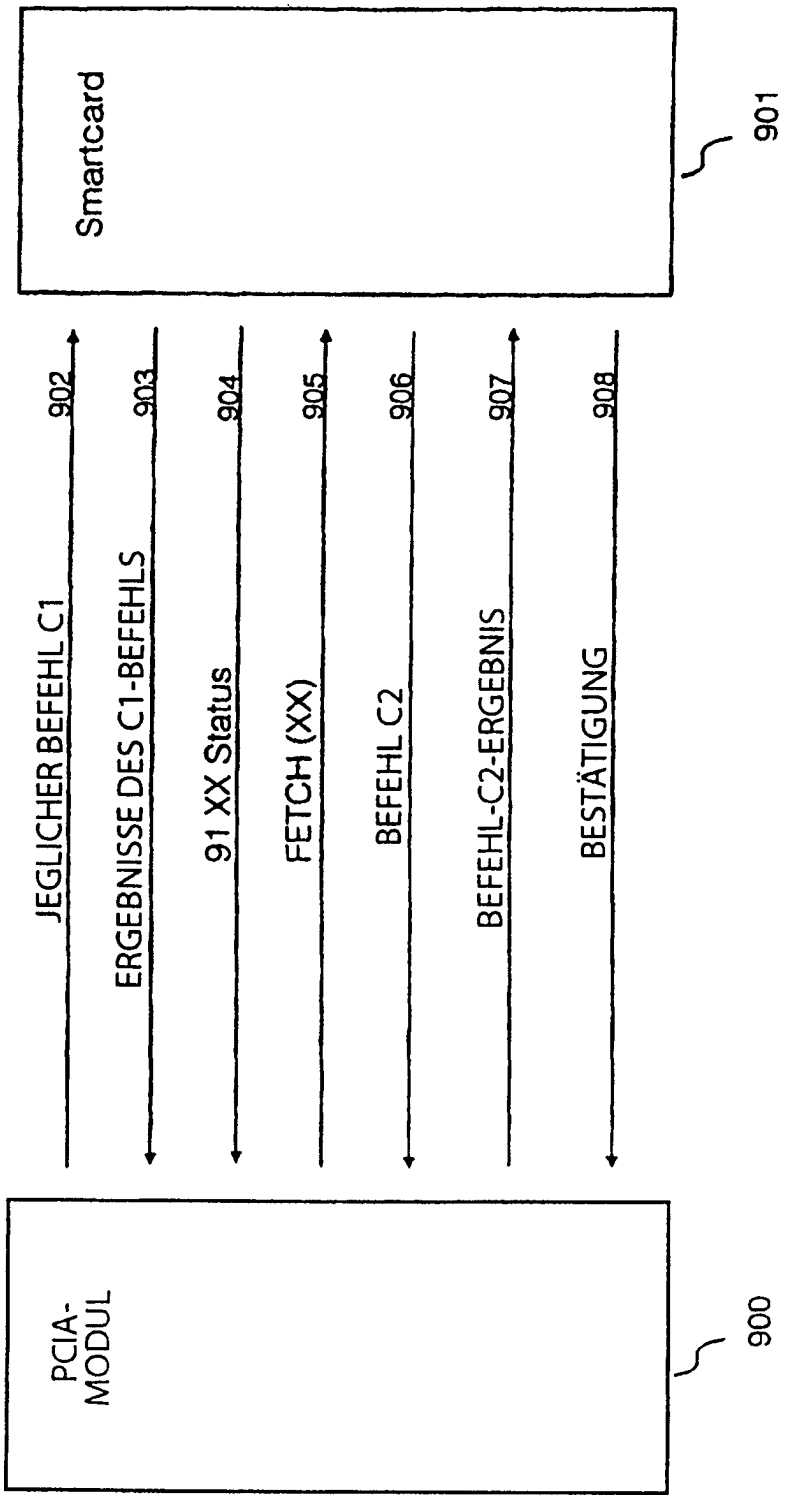

Smartcard
901
JEGLICHER BEFEHL C1
902
ERGEBNISSE DES C1-BEFEHLS
903
91 XX Status
904
FETCH (XX)
905
BEFEHL C2
906
BEFEHL-C2-ERGEBNIS
907
BESTÄTIGUNG
908
PCIA-MODUL
900

Fig.10

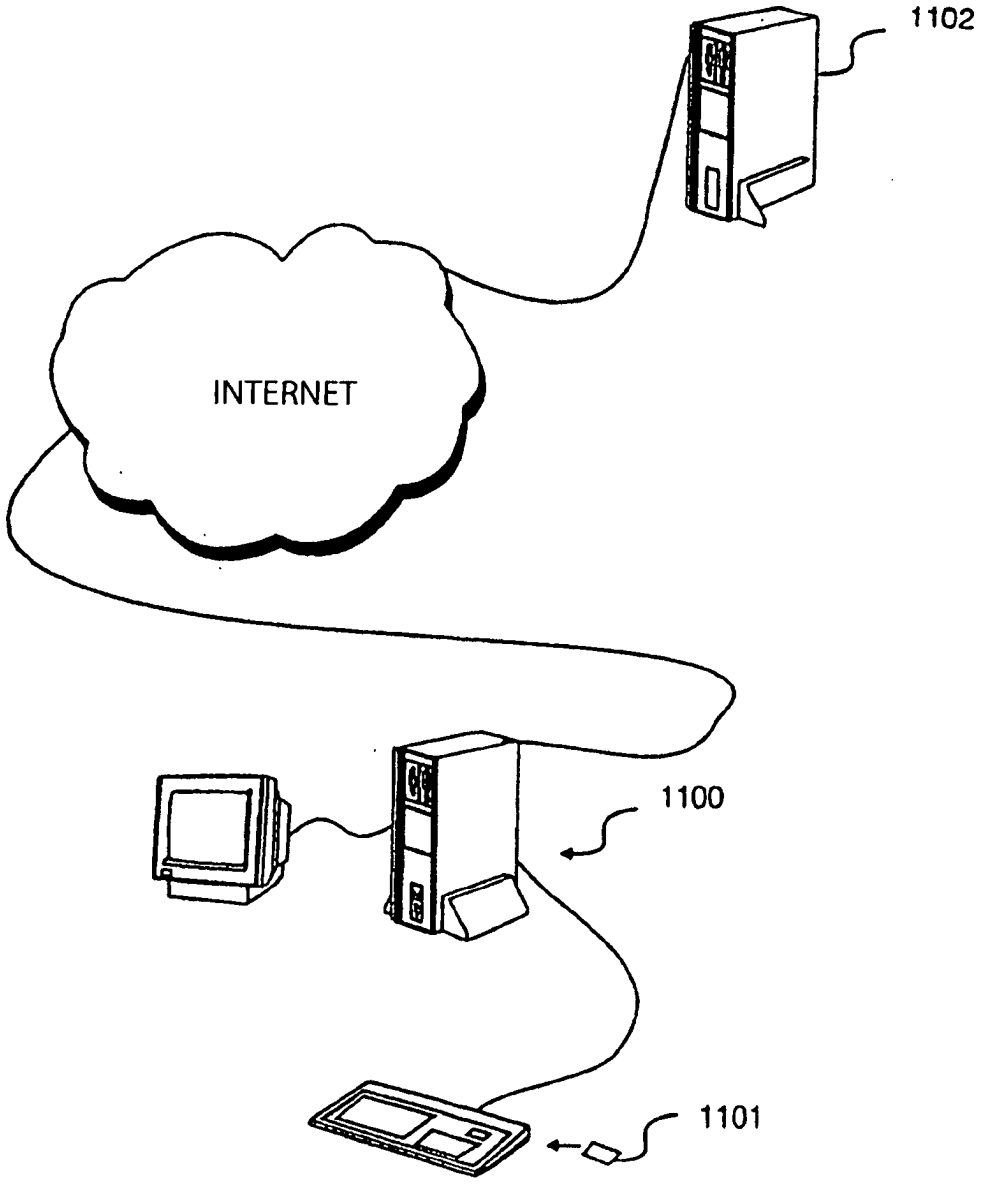


Fig. 11

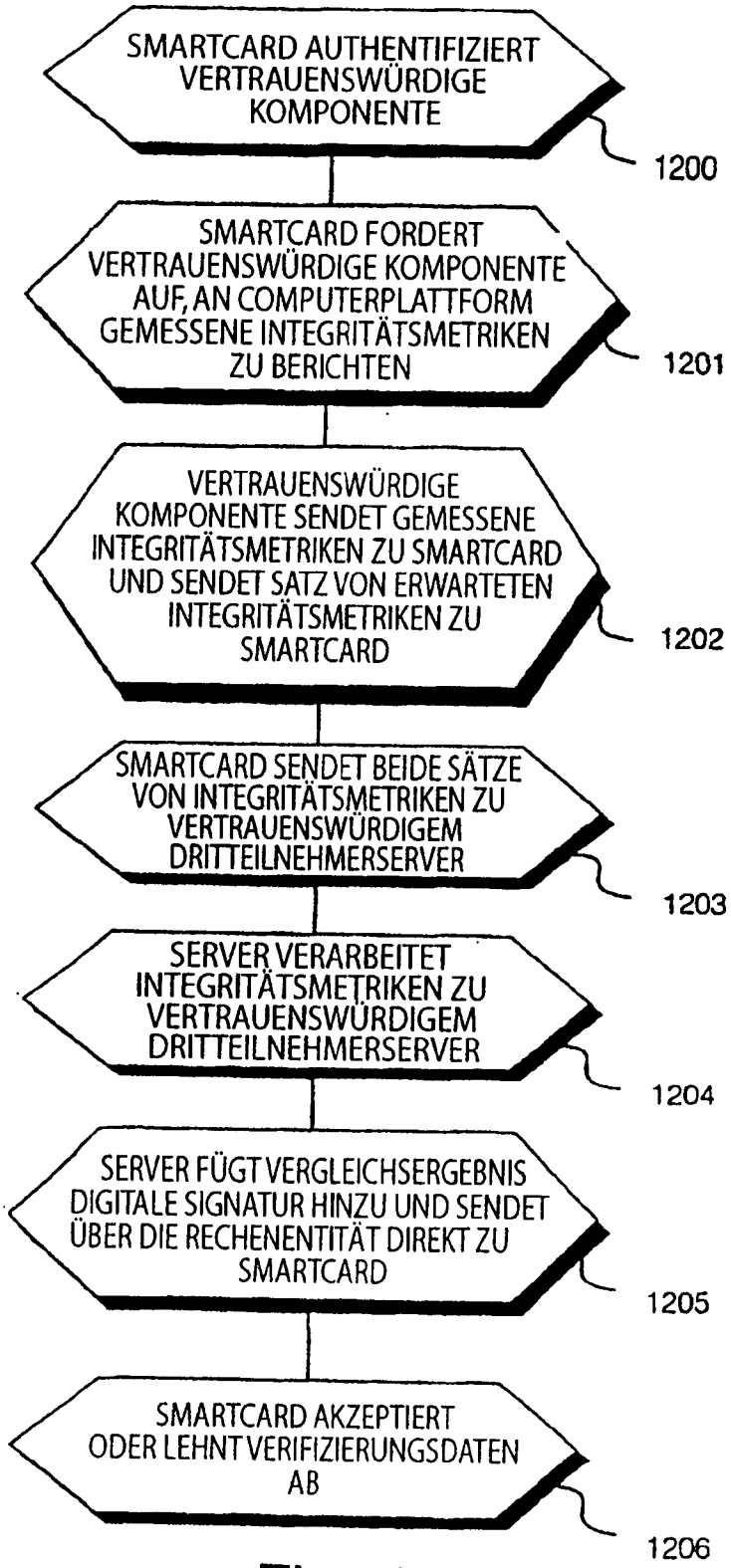

SMARTCARD AUTHENTIFIZIERT VERTRAUENSWÜRDIGE KOMPONENTE
1200
SMARTCARD FORDERT VERTRAUENSWÜRDIGE KOMPONENTE AUF, AN COMPUTERPLATTFORM GEMESSENE INTEGRITÄTSMETRIKEN ZU BERICHTEN
1201
VERTRAUENSWÜRDIGE KOMPONENTE SENDET GEMESSENE INTEGRITÄTSMETRIKEN ZU SMARTCARD UND SENDET SATZ VON ERWARTETEN INTEGRITÄTSMETRIKEN ZU SMARTCARD
1202
SMARTCARD SENDET BEIDE SÄTZE VON INTEGRITÄTSMETRIKEN ZU VERTRAUENSWÜRDIGEM DRITTEILNEHMERSERVER
1203
SERVER VERARBEITET INTEGRITÄTSMETRIKEN ZU VERTRAUENSWÜRDIGEM DRITTEILNEHMERSERVER
1204
SERVER FÜGT VERGLEICHSERGEBNIS DIGITALE SIGNATUR HINZU UND SENDET ÜBER DIE RECHENENTITÄT DIREKT ZU SMARTCARD
1205
SMARTCARD AKZEPTIERT ODER LEHNT VERIFIZIERUNGSDATEN AB
1206

Fig. 12

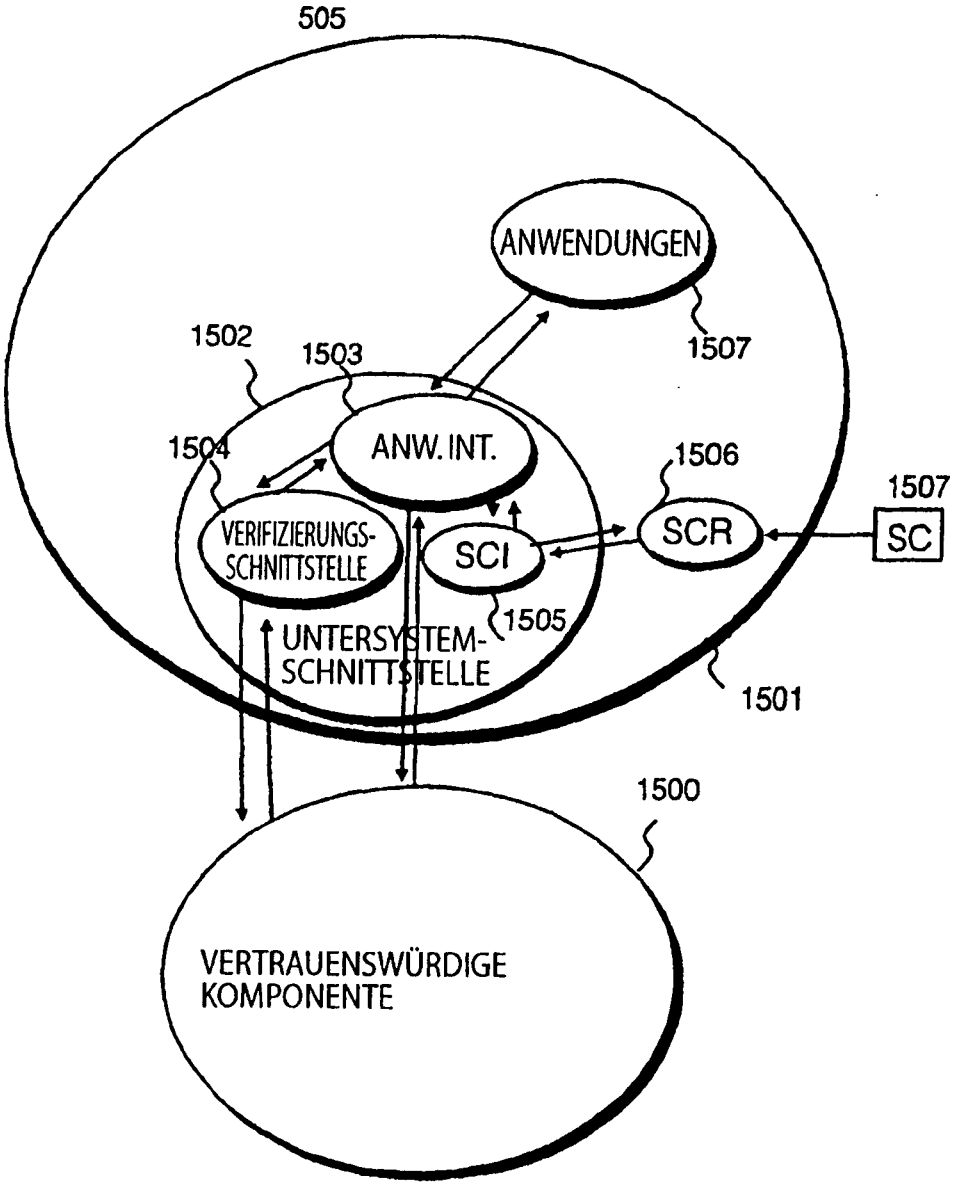

505
ANWENDUNGEN
1507
1502
1503
1504
ANW. INT.
1506
1507
SC
VERIFIZIERUNGS-SCHNITTSTELLE
SCI
SCR
1505
UNTERSYSTEM-SCHNITTSTELLE
1501
1500
VERTRAUENSWÜRDIGE KOMPONENTE

Fig. 13

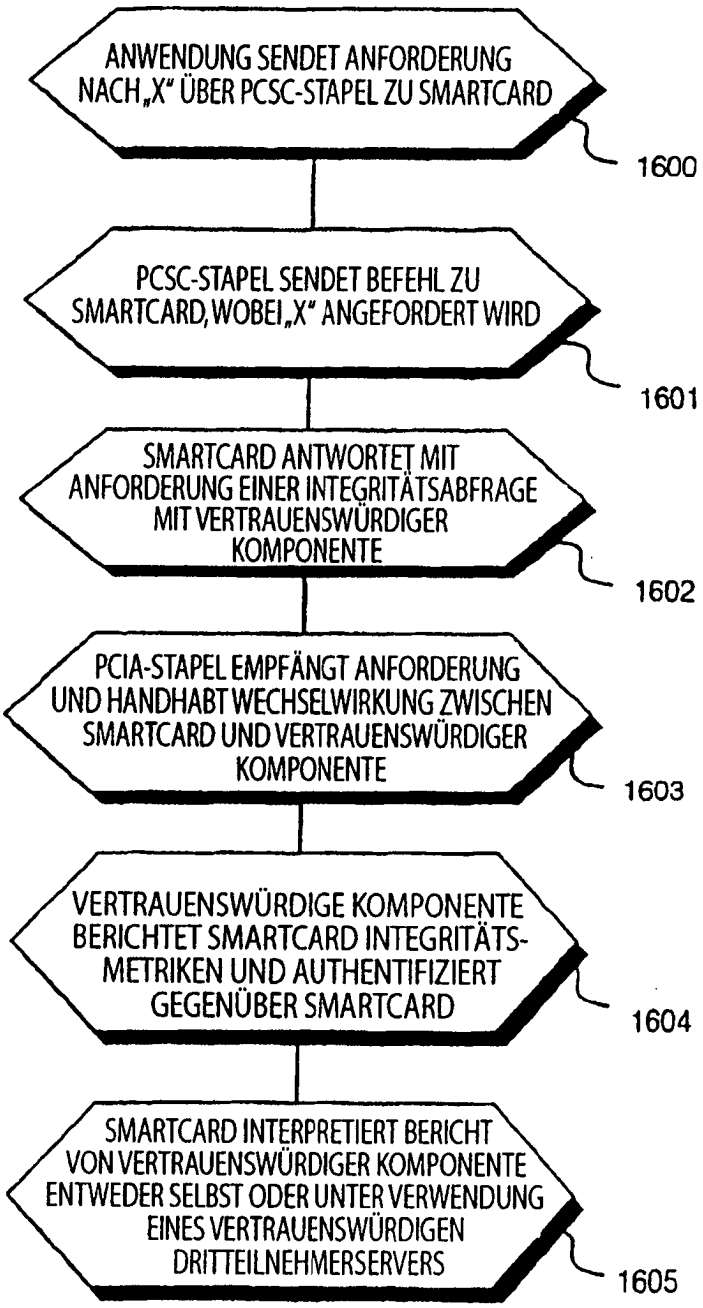

ANWENDUNG SENDET ANFORDERUNG NACH „X" ÜBER PCSC-STAPEL ZU SMARTCARD
1600
PCSC-STAPEL SENDET BEFEHL ZU SMARTCARD, WOBEI „X" ANGEFORDERT WIRD
1601
SMARTCARD ANTWORTET MIT ANFORDERUNG EINER INTEGRITÄTSABFRAGE MIT VERTRAUENSWÜRDIGER KOMPONENTE
1602
PCIA-STAPEL EMPFÄNGT ANFORDERUNG UND HANDHABT WECHSELWIRKUNG ZWISCHEN SMARTCARD UND VERTRAUENSWÜRDIGER KOMPONENTE
1603
VERTRAUENSWÜRDIGE KOMPONENTE BERICHTET SMARTCARD INTEGRITÄTS-METRIKEN UND AUTHENTIFIZIERT GEGENÜBER SMARTCARD
1604
SMARTCARD INTERPRETIERT BERICHT VON VERTRAUENSWÜRDIGER KOMPONENTE ENTWEDER SELBST ODER UNTER VERWENDUNG EINES VERTRAUENSWÜRDIGEN DRITTEILNEHMERSERVERS
1605

Fig. 14