(19) Deutsches Patent- und Markenamt

(10) **DE 11 2005 003 281 B4** 2012.02.16

(12) # Patentschrift

(21) Deutsches Aktenzeichen: **11 2005 003 281.7**
(86) PCT-Aktenzeichen: **PCT/US2005/047571**
(87) PCT-Veröffentlichungs-Nr.: **WO 2006/072047**
(86) PCT-Anmeldetag: **29.12.2005**
(87) PCT-Veröffentlichungstag: **06.07.2006**
(43) Veröffentlichungstag der PCT Anmeldung in deutscher Übersetzung: **31.01.2008**
(45) Veröffentlichungstag der Patenterteilung: **16.02.2012**

(51) Int Cl.: ***H04L 9/32*** (2006.01)
H04L 9/14 (2011.01)
G06Q 30/00 (2011.01)

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

(30) Unionspriorität:
11/027,525 **30.12.2004** **US**

(73) Patentinhaber:
TOPAZ Systems Inc., Simi Valley, Calif., US

(74) Vertreter:
Müller-Boré & Partner, Patentanwälte, European Patent Attorneys, 81671, München, DE

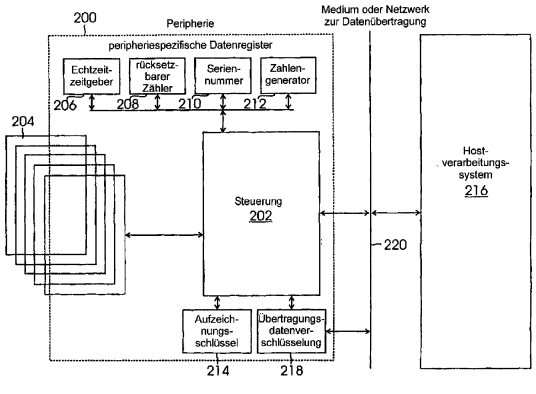
(72) Erfinder:
Zank, Anthony E., Simi Valley, Calif., US

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

GB 2 401 013 A
US 2004 / 0 059 924 A1

(54) Bezeichnung: **Elektronisches Signatursicherheitssystem**

(57) Hauptanspruch: Verfahren, umfassend die Schritte:
(a) Empfangen von Transaktionsdaten in einer ersten Vorrichtung;
(b) Erfassen einer Signatur in der ersten Vorrichtung;
(c) Verschlüsseln der erfassten Signatur mit den Transaktionsdaten in der ersten Vorrichtung; und
(d) Übertragen der Transaktionsdaten und der verschlüsselten Signatur von der ersten Vorrichtung an eine zweite Vorrichtung,
wobei die Signatur als getrennte Abtastpunkte verschlüsselt wird und wobei jeder Abtastpunkt mit einem anderen Verschlüsselungsschlüssel verschlüsselt wird.



Beschreibung

Gebiet der Erfindung

[0001] Verschiedene Ausführungsbeispiele der Erfindung betreffen die Sicherung von elektronischen Signaturen. Wenigstens ein Ausführungsbeispiel der Erfindung betrifft ein System und ein Verfahren zum Erfassen und Sichern von elektronischen Signaturen durch einen Hash-Codierungsalgorithmus.

Hintergrund der Erfindung

[0002] In den vergangenen Jahren hat die Anzahl von Transaktionen zugenommen, die über elektronische Medien abgewickelt werden. Es sind Gesetze, Vorschriften und Industriestandards entstanden, die den Einsatz von elektronischen Aufzeichnungen und Signaturen im Handel mit dem In- und Ausland vereinfachen. Einige dieser Gesetze und Vorschriften führen aus, dass eine Technologie dann akzeptabel ist, wenn elektronische Signaturen dergestalt mit Daten verknüpft werden können, dass bei einer Änderung der Daten die digitale Signatur ungültig wird.

[0003] Bei vielen dieser Techniken kommen Peripherievorrichtungen zum Einsatz, die mit einem Computer oder einem Netzwerk kommunikativ gekoppelt sind, der/das vom Signierenden zur Authentisierung einer Transaktion verwendet werden kann. Diese Peripherievorrichtungen kommen in einer Vielzahl von Umgebungen zum Einsatz, beginnend mit Vorrichtungen, die im häuslichen Bereich und bei Geschäften mit einzelnen Versicherungsagenten zum Einsatz kommen, bis hin zu Anwendungen im Großhandel und bei Bankgeschäften, einzelnen Desktopanwendungen und tragbaren Anwendungen mit Speichern und drahtlosen Vorrichtungen.

[0004] Mit Blick auf die genannten technologischen Richtlinien existieren Technologien, die diese Anforderungen zu erfüllen scheinen. Im Allgemeinen fallen sie in die nachfolgenden Kategorien: „Etwas, das du bist" („Something you are"), „Etwas, das du tust" („Something you do"), „Etwas, das du weißt" („Something you know") und „Etwas, das du hast" (Something you have"). Typische Beispiele für annehmbare elektronische Signaturen beinhalten handgeschriebene Signaturen bzw. Unterschriften, Fingerabdrücke, Irisabtastungen, Stimmaufzeichnungen, persönliche Identifikationsnummern (personal identification number PIN), Handgeometrien, PKI-Zertifikate (public key infrastructure PKI, Infrastruktur mit öffentlichem Schlüssel), Smart-Cards, Identifikationskarten oder Karten für Geldgeschäfte.

[0005] Mit Blick auf Datensicherheit und Datenübertragungssicherheit sind Techniken vorhanden und haben sich in der Praxis auch bereits verbreitet, um Daten zu sichern und zu verschlüsseln, die zwischen Computern, Netzwerken und Peripherievorrichtungen, wie sie im Handel heutzutage benutzt werden, übertragen werden.

[0006] Da derzeit Peripherievorrichtungen auch zum Signieren von Verträgen und zum Erfassen von elektronischen Signaturen verwendet werden, besteht die Gelegenheit, ihre Effektivität und Sicherheit zu verbessern. Diese Möglichkeit besteht sowohl für in der Vergangenheit übliche geschlossene Systeme wie auch bei weniger strukturierten offenen Systemen, die bei Einzelpersonen und Kleinunternehmen zum Einsatz kommen.

[0007] Im Stand der Technik wird versucht, sichere Transaktionsschemata bereitzustellen. Diese Schemata weisen verschiedene Nachteile auf. So beschreibt beispielsweise das US-Patent 5,297,202 von Kapp et al. ein zweistufiges Verschlüsselungsschema für den Schutz von elektronischen Signaturen. Es wird ein Transaktionscode erstellt und als Teil der Transaktionsaufzeichnung angezeigt. Dieser Transaktionscode besteht aus einem ersten Wort, das einen bestimmten Ort des Handels sowie gegebenenfalls die Zeit identifiziert, und einem zweiten Wort, das sequenziell zugewiesen wird. Bei einem ersten Schritt wird der Transaktionscode zur Verschlüsselung der Signaturdaten und zur Bereitstellung einer Datei mit der verschlüsselten Signatur verwendet. in einem zweiten Schritt werden anschließend sichere Verschlüsselungsschlüssel, die beiden Parteien der Transaktion bekannt sind, zur Verschlüsselung der sich ergebenden Datei mit der verschlüsselten Signatur verwendet. Dieser Lösungsansatz weist gewisse Schwächen auf. Zunächst wird die Transaktionsaufzeichnung, die zur Verschlüsselung der Signatur verwendet wird, mit den Transaktionsdaten angezeigt, was eine Anfälligkeit für einen nicht autorisierten Zugriff mit sich bringt. Zudem ist der Transaktionscode teilweise von einem Ortsidentifizierer und einer sequenziell zugewiesenen Zahl abhängig, wodurch es einfacher wird, den Transaktionscode durch Zugriff auf vorherige Transaktionen zu knacken.

[0008] Die Druckschrift US 2004/00 59 924 A1 offenbart eine Netzwerk-Infrastruktur, welche biometrische private Schlüssel (BioPKI) verwendet. Im Allgemeinen ist Bio PKI eine Kombination aus zwei Software-Lösungen, um eine elektronische Authentifizierung zu validieren, nämlich ein biometrisches Signatur-System und eine digitale Signatur für die Datenintegrität. Die kombinierte Software-Lösung ermöglicht es vernetzten Unternehmen sicherzustellen, daß eine Benutzer-Authentifizierung in einer sicheren Art und Weise innerhalb von Standard-Netzwerk-Umgebungen durchgeführt wird. Eine zusätzliche biometrische Signatur kann dabei eine digitale Standard-Signaturen erweitern und zwar durch Hinzufügen einer automatisierten, nicht-seriösen Benutzer-Authentifizierungs-Funktion zu der bestehenden digitalen Si-

gnatur. Im Gegensatz zur einfachen Überprüfung in einem reinen biometrisch basierten System oder einer digitale Signatur/Zertifikat-Umgebung offenbart die Druckschrift US 2004/00 59 924 A1 eine Kombination, um digitale Signaturen basieren auf biometrischen Authentifizierungs- und Industrie-Standard-PKT-Technologien zu schaffen.

[0009] Die Druckschrift GB 24 01 013 A offenbart ein kryptografisches Verfahren, wobei erste Daten von einem ersten Teilnehmer zu einem zweiten Teilnehmer gesendet werden. Die ersten Daten sind mit Hilfe eines Schlüssels verschlüsselt, der unter Verwendung von mindestens einem Hash-Wert des ersten Datensatzes gebildet ist. Der Hash-Wert ist von einer vertrauenswürdigen Partei klar lesbar. Die verschlüsselten ersten Daten und der Schlüssel werden dem zweiten Teilnehmer zur Verfügung gestellt, wobei der zweite Teilnehmer den Schlüssel-String zu der vertrauenswürdigen Partei leitet und den entsprechenden Schlüssel für die Entschlüsselung anfordert. Die vertrauenswürdigen Partei führt mindestens eine Kontrolle auf der Grundlage von im Schlüssel-String enthaltenen Daten aus und, wenn diese mindestens eine Kontrolle erfolgreiche ist, stellt einen Schlüssel für die Entschlüsselung dem zweiten Teilnehmer zur Verfügung.

[0010] Es ist daher eine Aufgabe der vorliegenden Erfindung, ein Verfahren und ein System bereitzustellen, welches die einen verbesserten Schutz von signierten Transaktionsdaten beim Übertragen von nicht autorisiertem Zugriff ermöglicht.

[0011] Diese Aufgabe wird durch das Verfahren gemäß Anspruch 1, eine Signaturvorrichtung gemäß Anspruch 21, ein System gemäß Anspruch 22, ein Transaktionssystem gemäß Anspruch 24 und eine Authentisierungsvorrichtung gemäß Anspruch 27 gelöst. Bevorzugte Ausführungsformen sind Gegenstand der abhängigen Ansprüche.

Zusammenfassung der Erfindung

[0012] Ein Ausführungsbeispiel der Erfindung stellt ein System, ein Verfahren und eine Vorrichtung bereit, die dafür ausgelegt sind, die Sicherheit zu verbessern und elektronische Signaturen mit bestehenden Vorschriften in Einklang zu bringen sowie diese praxistauglich zu machen. Bei einer Implementierung wird eine elektronische Signatur in einer Peripherievorrichtung erfasst, die nicht in dem Hauptprozessor enthalten ist, sondern von dem Prozessor einige wenige Fuß oder Tausende von Meilen entfernt angeordnet sein kann. Das System verbindet die Signatur und die Aufzeichnungsdaten am Ort der Verwendung, um die Wahrscheinlichkeit zu verringern, dass jemand in die Lage versetzt wird, mittels Hacken in das – verschlüsselte oder unverschlüsselte – Übertragungsmedium einzudringen und die Rohsignaturdaten zu ermitteln. Durch das Verbinden oder Verknüpfen der Signatur und der Aufzeichnungsdaten am Ort der Verwendung weist jede Aufzeichnung einen eindeutigen Schlüssel auf, was Versuche des Eindringens mittels Hacken zudem vereitelt. Durch die Verwendung eines gemeinsamen Geheimnisses, das nicht oder zumindest nicht mittels des Übertragungsmediums übertragen wird, sondern mit einem programmierten Wert, so beispielsweise einer Seriennummer oder einer mittels eines RTC-Wertes (real-time computed RTC, echtzeitberechnet) modifizierten Seriennummer verknüpft wird oder durch einen Befehl ohne Änderung der Daten rückgesetzt werden kann, wird die Sicherheit weiter erhöht.

[0013] Durch Verbinden der Signatur und der Aufzeichnungsdaten am Ort der Verwendung in Verbindung mit der Verwendung der Aufzeichnungsdaten und einer damit verknüpften Hash-Codierung können alle Arten von elektronischen Signatursystemen die durch Vorschriften vorgegebenen Anforderungen sicherer eingedenk dessen erfüllen, dass die Versuche, in weniger gesicherte Systems einzudringen, zunehmen. Durch Speichern der kryptografischen Darstellungen der Signatur und/oder der Aufzeichnungsdaten in der Peripherievorrichtung kann die Integrität der Gesamttransaktion weiter verbessert und verziert werden.

[0014] Das System ist zu Standardverschlüsselungstechniken, die heute zum Schutz der Übertragung von digitalen Daten verbreitet sind, kompatibel, jedoch nicht von diesen Techniken abhängig.

[0015] Ein Ausführungsbeispiel der Erfindung sieht ein Verfahren vor, das die nachfolgenden Schritte umfasst: (a) Empfangen von Transaktionsdaten in einer ersten Vorrichtung; (b) Erfassen einer Signatur in der ersten Vorrichtung; (c) Verschlüsseln der erfassten Signatur mit den Transaktionsdaten in der ersten Vorrichtung; und (d) Übertragen der Transaktionsdaten und der verschlüsselten Signatur von der ersten Vorrichtung an die zweite Vorrichtung.

[0016] Dieses Verfahren kann zudem einen Schritt des Verschlüsselns der erfassten Signatur mit einer Hash-Codierung der Transaktionsdaten beinhalten. Die Transaktionsdaten können neben weiteren Informationen eine Preisinformation für die Transaktion und/oder eine Identifikation der Waren, die von der Transaktion betroffen sind, beinhalten. Das Verfahren kann zudem das Empfangen einer Hash-Codierung der Transaktionsdaten in der ersten Vorrichtung und/oder das Erzeugen einer Hash-Codierung der Transaktionsdaten in der ersten Vorrichtung beinhalten. Das Verfahren kann zudem die nachfolgenden Schritte beinhalten: (a) Erzeugen einer lokalen Hash-Codierung der Transaktionsdaten in der zweiten Vorrichtung unter Verwendung desselben Algorithmus, der zur Erzeugung der Hash-Codierung in der ersten

Vorrichtung verwendet wird; (b) Decodieren der verschlüsselten erfassten Signatur in der zweiten Vorrichtung unter Verwendung der lokalen Hash-Codierung der Transaktionsdaten; und (c) Vergleichen der erfassten Signatur mit einer gespeicherten Signatur zur Verifizierung.

[0017] Ein Aspekt der Erfindung sieht das Erfassen einer digitalen Signatur und/oder einer biometrischen Signatur auf einer Punkt-für-Punkt-Basis (oder einer Segment-für-Segment-Basis) und das getrennte Verschlüsseln der Punkte zu Aufzeichnungsdaten vor. Die getrennt verschlüsselten Signaturabtastpunkte oder Segmente können in den Übertragungs- und/oder Empfangsvorrichtungen getrennt gespeichert werden, sodass die vollständige Signatur nicht gleichzeitig auf demselben Prozessor oder in demselben Speicher vorhanden ist. Hierdurch wird verhindert, dass bösartige Programme die Signatur durch Ausforschen des Prozessors oder Speichers erfassen oder bestimmen.

[0018] Ein weiterer Aspekt der Erfindung sieht vor: (a) Kombinieren der Transaktionsdaten mit einem Geheimschlüssel, der in der ersten Vorrichtung erzeugt wird; (b) Erzeugen einer Hash-Codierung der Kombination aus den Transaktionsdaten und dem Geheimschlüssel zur Erstellung eines abgeleiteten Aufzeichnungsschlüssels in der ersten Vorrichtung; und (c) Verschlüsseln der erfassten Signatur unter Verwendung des abgeleiteten Aufzeichnungsschlüssels als Eingabe für einen Verschlüsselungsalgorithmus in der ersten Vorrichtung.

[0019] Weder ein anderes Merkmal der Erfindung sieht ein sporadisches (oder in unregelmäßigen Intervallen erfolgendes) Senden des Geheimschlüssels zwischen der ersten Vorrichtung an die zweite Vorrichtung vor.

[0020] Ein weiteres Ausführungsbeispiel der Erfindung sieht darüber hinaus vor: (a) Erzeugen einer Hash-Codierung der Kombination aus den Transaktionsdaten und dem Geheimschlüssel zur Erstellung eines abgeleiteten Aufzeichnungsschlüssels in der zweiten Vorrichtung; und (b) Decodieren der verschlüsselten erfassten Signatur in der zweiten Vorrichtung unter Verwendung des abgeleiteten Aufzeichnungsschlüssels. Schlägt das Decodieren der verschlüsselten erfassten Signatur in der zweiten Vorrichtung fehl, so sucht die zweite Vorrichtung durch Modifizieren des Geheimschlüssels nach dem richtigen abgeleiteten Aufzeichnungsschlüssel. Die verschlüsselte Signatur kann auch in einer Mehrzahl von Datenfragmenten von der ersten Vorrichtung an die zweite Vorrichtung übertragen werden, wobei diese Mehrzahl von Datenfragmenten in einer pseudozufälligen Reihenfolge gesendet wird.

[0021] Wieder ein anderes Merkmal der Erfindung sieht von (a) Unterteilen der Signaturdaten in eine Mehrzahl von Fragmenten, (b) getrenntes Verschlüsseln von jedem aus der Mehrzahl von Fragmenten mit den Transaktionsdaten, (c) Übertragen der Mehrzahl von Fragmenten von der ersten Vorrichtung an die zweite Vorrichtung, (d) Erstellen eines ersten Zählwertes der Mehrzahl von Fragmenten, die von der ersten Vorrichtung übertragen werden, (e) Übertragen des ersten Zählwertes an die zweite Vorrichtung, (f) Erstellen eines zweiten Zählwertes der Mehrzahl von Fragmenten, die von der zweiten Vorrichtung empfangen werden, und (g) Vergleichen des ersten Zählwertes mit dem zweiten Zählwert zur Bestimmung, ob sämtliche Signaturfragmente empfangen worden sind.

[0022] Entsprechend einem Ausführungsbeispiel der Erfindung sieht das Signatursicherheitsverfahren vor: (a) Erzeugen eines ersten abgeleiteten Aufzeichnungsschlüssels durch Nehmen einer Hash-Codierung der Kombination aus einem ersten Zeitgeberwert mit den Transaktionsdaten, wobei der erste Zeitgeberwert in der ersten Vorrichtung zu finden ist; (b) Verwenden des ersten abgeleiteten Aufzeichnungsschlüssels zur Verschlüsselung der erfassten Signatur in der ersten Vorrichtung; (c) Erzeugen eines zweiten abgeleiteten Aufzeichnungsschlüssels durch Nehmen einer Hash-Codierung der Kombination eines zweiten Zeitgeberwertes, eines Offsetwertes und der Transaktionsdaten in der zweiten Vorrichtung, wobei der zweite Zeitgeber in der zweiten Vorrichtung zu finden ist; und (d) Entschlüsseln der verschlüsselten Signatur mit dem zweiten abgeleiteten Aufzeichnungsschlüssel in der zweiten Vorrichtung.

[0023] Die Erfindung sieht darüber hinaus ein Transaktionssystem vor, umfassend: eine Signaturerfassungsvorrichtung, die ausgelegt ist zum: (a) Erfassen einer elektronischen Signatur, (b) Erzeugen einer Hash-Codierung einer Transaktionsaufzeichnung, (c) Verschlüsseln der elektronischen Signatur mit der Hash-Codierung der Transaktionsaufzeichnung, (d) Übertragen der verschlüsselten elektronischen Signatur; und (e) eine Hostverarbeitungsvorrichtung, die kommunikativ mit der Signaturerfassungsvorrichtung gekoppelt ist, wobei die Hostverarbeitungsvorrichtung ausgelegt ist zum: (1) Empfangen der verschlüsselten elektronischen Signatur, (2) Entschlüsseln der elektronischen Signatur, (3) Vergleichen der elektronischen Signatur mit einer Bezugssignatur und (4) Annehmen einer Transaktion entsprechend der elektronischen Transaktionsaufzeichnung, wenn die empfangene elektronische Signatur zu der Bezugssignatur passt. Die Signaturerfassungsvorrichtung kann darüber hinaus zum Initiieren der Transaktionsaufzeichnung und Übertragen der Transaktionsaufzeichnung an die Hostverarbeitungsvorrichtung ausgelegt sein. Die Hostverarbeitungsvorrichtung kann zudem zum Empfangen einer Hash-Codie-

rung der Transaktionsaufzeichnung zur Verwendung bei der Entschlüsselung der elektronischen Signatur ausgelegt sein.

[0024] Entsprechend einem Ausführungsbeispiel der Erfindung ist die Signaturerfassungsvorrichtung des Weiteren ausgelegt zum: (a) Übertragen der verschlüsselten elektronischen Signatur als Mehrzahl von Datenpaketen, (b) Vorhalten eines Zählwertes der Anzahl von Datenpaketen der Übertragung für eine bestimmte Signatur, (c) sicheren Übertragen des Zählwertes der Datenpakete an die Hostverarbeitungsvorrichtung, wobei (d) die Hostverarbeitungsvorrichtung des Weiteren ausgelegt ist: zum Vergleichen des Zählwertes der Datenpakete, die von der Signaturerfassungsvorrichtung übertragen werden, mit der Anzahl der Datenpakete, die in Verbindung mit der bestimmten Signatur empfangen werden, um zu bestimmen, ob die Signatur vollständig empfangen worden ist.

[0025] Entsprechend einem weiteren Ausführungsbeispiel der Erfindung ist die Signaturerfassungsvorrichtung des Weiteren ausgelegt zum (a) Anordnen der verschlüsselten elektronischen Signatur als Mehrzahl von Datenpaketen, (b) Übertragen der Mehrzahl von Datenpaketen in einer pseudozufälligen Reihenfolge, wobei (c) die Hostverarbeitungsvorrichtung des Weiteren ausgelegt ist zum: (1) Empfangen der Mehrzahl von Datenpaketen in einer pseudozufälligen Reihenfolge und (2) Rekonstruieren der ursprünglichen Reihenfolge der Mehrzahl von Datenpaketen.

[0026] Wieder ein anderes Ausführungsbeispiel der Erfindung sieht eine Authentisierungsvorrichtung vor, umfassend: (a) eine Signaturerfassungsvorrichtung, die dafür ausgelegt ist, eine Signaturinformation zu erfassen; und (b) eine Steuerung, die kommunikativ mit der Signaturerfassungsvorrichtung gekoppelt ist, wobei die Steuerung ausgelegt ist zum: (1) Empfangen von Transaktionsdaten, (2) Erzeugen einer Hash-Codierung der Transaktionsdaten, (3) Verschlüsseln der erfassten Signaturinformation mit der Hash-Codierung der Transaktionsdaten und (4) Übertragen der verschlüsselten Signaturinformation. Eine derartige Authentisierungsvorrichtung kann darüber hinaus umfassen: (a) eine Ausgabevorrichtung zur Vorlage der Transaktionsdaten bei einem Anwender; und (b) eine Eingabevorrichtung, die einem Anwender die Modifizierung der Transaktionsdaten ermöglicht. Die Authentisierungsvorrichtung kann darüber hinaus die nachfolgenden Aufgaben wahrnehmen: (a) Kombinieren der Transaktionsaufzeichnung mit einem Geheimschlüssel, (b) Erzeugen einer Hash-Codierung der Kombination aus den Transaktionsdaten und dem Geheimschlüssel zur Erstellung eines abgeleiteten Aufzeichnungsschlüssels, (c) Verschlüsseln der erfassten Signatur mit dem abgeleiteten Aufzeichnungsschlüssel als Eingabe für einen Verschlüsselungsalgorithmus, (d) Unterteilen der erfassten Signaturinformation in eine Mehrzahl von Paketen, (e) getrenntes Verschlüsseln von jedem aus der Mehrzahl von Paketen mit den Transaktionsdaten, wobei (f) das Übertragen der verschlüsselten Signaturinformation das Übertragen der Mehrzahl von Paketen ohne bestimmte Abfolge in einer pseudozufälligen Reihenfolge beinhaltet.

[0027] Bei wieder einem anderen Ausführungsbeispiel der Erfindung sieht ein maschinenlesbares Medium eine oder mehrere Anweisungen zum Verarbeiten einer elektronischen Signatur in einer Peripherievorrichtung vor, die bei Ausführung durch einen Prozessor den Prozessor veranlassen, Operationen auszuführen, die umfassen; (a) Empfangen von Transaktionsdaten, (b) Erfassen einer Signatur von einem Anwender; (c) Erzeugen einer Hash-Codierung der Transaktionsdaten; (d) Verschlüsseln der erfassten Signatur mit der Hash-Codierung der Transaktionsdaten; und (e) Übertragen der verschlüsselten Signatur. Das Verschlüsseln der erfassten Signatur unter Verwendung der Transaktionsdaten kann umfassen: (a) das Kombinieren der Transaktionsdaten mit einem Geheimschlüssel, (b) das Erzeugen einer Hash-Codierung der Kombination aus den Transaktionsdaten und dem Geheimschlüssel zur Erstellung eines abgeleiteten Aufzeichnungsschlüssels und (c) das Verschlüsseln der erfassten Signatur unter Verwendung des abgeleiteten Aufzeichnungsschlüssels als Eingabe für einen Verschlüsselungsalgorithmus.

[0028] Die Anweisungen des maschinell lesbaren Mediums können des Weiteren Operationen ausführen zum: (a) Unterteilen der erfassten Signatur in eine Mehrzahl von Datenfragmenten; (b) getrennten Verschlüsseln der Mehrzahl von Datenfragmenten; und (c) Übertragen der Mehrzahl von Datenfragmenten in einer pseudozufälligen Reihenfolge.

[0029] Eine Implementierung der Erfindung sieht eine unabhängige Transaktionsauthentisierungsvorrichtung vor, umfassend: (a) eine Signaturerfassungsvorrichtung, die dafür ausgelegt ist, eine elektronische Signaturinformation zu erfassen; (b) eine Steuerung, die kommunikativ mit der Signaturerfassungsvorrichtung gekoppelt ist, wobei die Steuerung ausgelegt ist zum: (1) Empfangen von Transaktionsdaten einschließlich einer Preisinformation, (2) Erzeugen einer Hash-Codierung der Transaktionsdaten, (3) Unterteilen der erfassten Signaturinformation in eine Mehrzahl von Paketen, (4) getrennten Verschlüsseln von jedem aus der Mehrzahl von Paketen mit einer Hash-Codierung der Transaktionsdaten und (5) Übertragen der Mehrzahl von Paketen ohne bestimmte Abfolge in einer pseudozufälligen Reihenfolge; (c) eine Ausgabevorrichtung, die kommunikativ mit der Steuerung gekoppelt ist, wobei die Ausgabevorrichtung die Transaktionsdaten darstellt; und (d) eine Eingabevorrichtung, die kommunikativ mit

der Steuerung gekoppelt ist, wobei die Eingabevorrichtung das Modifizieren der Transaktionsdaten ermöglicht. Die Steuerung kann des Weiteren ausgelegt sein zum: (a) Kombinieren der Transaktionsdaten mit einem Geheimschlüssel; (b) Erzeugen einer Hash-Codierung der Kombination aus den Transaktionsdaten und dem Geheimschlüssel zur Erstellung eines abgeleiteten Aufzeichnungsschlüssels; und (c) getrennten Verschlüsseln von jedem aus der Mehrzahl von Paketen mit dem abgeleiteten Aufzeichnungsschlüssel als Eingabe für einen Verschlüsselungsalgorithmus. Die Signaturerfassungsvorrichtung kann eine digitalisierende Schreibfläche, eine Tastatur, eine Iriserkennungsvorrichtung, eine Fingerabdruckerkennungsvorrichtung oder eine Spracherkennungsvorrichtung oder auch eine andere geeignete elektronische Signaturvorrichtung sein.

Kurzbeschreibung der Zeichnung

[0030] Fig. 1 ist ein Blockdiagramm, das ein einem Ausführungsbeispiel der vorliegenden Erfindung entsprechendes System zum Bereitstellen von elektronischer Signatursicherheit darstellt.

[0031] Fig. 2 ist ein Blockdiagramm, das eine einem Ausführungsbeispiel der vorliegenden Erfindung entsprechende Peripherievorrichtung zur Sicherung von elektronischen Signaturen bei Transaktionen darstellt.

[0032] Fig. 3 ist ein Flussdiagramm, das ein einem Ausführungsbeispiel der vorliegenden Erfindung entsprechendes Verfahren zum Bereitstellen einer sicheren Transaktion zwischen einer Peripherievorrichtung und einem Hostverarbeitungssystem darstellt.

[0033] Fig. 4 ist ein Flussdiagramm, das ein einem Ausführungsbeispiel der vorliegenden Erfindung entsprechendes elektronisches Signaturverschlüsselungsverfahren auf Grundlage der Hash-Codierung einer Transaktionsaufzeichnung darstellt.

[0034] Fig. 5 ist ein Flussdiagramm, das ein einem Ausführungsbeispiel der vorliegenden Erfindung entsprechendes elektronisches Signaturverschlüsselungsverfahren auf Grundlage eines abgeleiteten Hash-Codierungsschemas darstellt.

[0035] **Fig.** 6 ist ein Flussdiagramm, das ein einem Ausführungsbeispiel der vorliegenden Erfindung entsprechendes Verfahren zum Suchen nach einem richtigen abgeleiteten Aufzeichnungsschlüssel in einem Hostverarbeitungssystem darstellt.

[0036] Fig. 7 ist ein Flussdiagramm, das ein einem Ausführungsbeispiel der vorliegenden Erfindung entsprechendes Verfahren zum Verwenden unterschiedlicher Zeitgeberwerte in einem Hostverarbeitungssystem und einer Peripherievorrichtung zum sicheren Umgang mit der Übertragung und zur Entschlüsselung der Signatur darstellt, die von der Peripherievorrichtung an das Hostverarbeitungssystem gesendet wird.

[0037] Fig. 8 ist ein Flussdiagramm, das ein weiteres einem Ausführungsbeispiel der vorliegenden Erfindung entsprechendes Verfahren zum Aufrechterhalten der Sicherheit der Signaturinformation zwischen einer Peripherievorrichtung und einem Hostverarbeitungssystem darstellt.

[0038] Fig. 9 ist ein Flussdiagramm, das ein einem Ausführungsbeispiel der vorliegenden Erfindung entsprechendes Verfahren zum Bestimmen darstellt, ob elektronische Signaturdaten, die von einer Peripherievorrichtung gesendet werden, vollständig von einem Hostverarbeitungssystem empfangen werden.

[0039] Fig. 10 ist ein Blockdiagramm, das einen einem Ausführungsbeispiel der vorliegenden Erfindung entsprechenden Signaturdatenübertragungsstrom von einer Peripherievorrichtung an ein Hostverarbeitungssystem mit gesicherten Zeitstempeln darstellt.

[0040] Fig. 11 ist ein Blockdiagramm, das einen einem weiteren Ausführungsbeispiel der Erfindung entsprechenden Signaturdatenübertragungsstrom von einer Peripherievorrichtung an ein Hostverarbeitungssystem mit gesicherten Zeitstempeln darstellt.

[0041] Fig. 12 ist ein Blockdiagramm, das einen einem weiteren Ausführungsbeispiel der Erfindung entsprechenden Signaturdatenübertragungsstrom von einer Peripherievorrichtung an ein Hostverarbeitungssystem darstellt, wobei die Zeitstempel zufällig in den Signaturdatenübertragungsstrom eingefügt sind.

[0042] Fig. 13 und Fig. 14 sind Blockdiagramme, die darstellen, wie verschiedenen Ausführungsbeispielen der vorliegenden Erfindung entsprechende Signaturdatenpakete, die zwischen einer Peripherievorrichtung und einem Hostverarbeitungssystem übertragen werden, verwürfelt werden, um die Signaturinformation zu sichern.

Detailbeschreibung

[0043] In der nachfolgenden Beschreibung werden spezifische Details erläutert, um ein weitergehendes Verständnis der Erfindung zu ermöglichen. Einem Fachmann auf dem einschlägigen Gebiet erschließt sich jedoch, dass die Erfindung auch ohne all diese spezifischen Details in der Praxis verwirklicht werden kann. Demgegenüber werden bekannte Verfahren, Prozeduren und/oder Komponenten nicht im De-

tail beschrieben, um die Aspekte der vorliegenden Erindung nicht unnötigerweise unklar zu machen.

[0044] Bei der nachfolgenden Beschreibung wird eine bestimmte Terminologie zur Beschreibung bestimmter Merkmale eines oder mehrerer Ausführungsbeispiele der Erfindung verwendet. So bezeichnet beispielsweise der Begriff „elektronisch" eine Technologie mit elektrischen, digitalen, magnetischen, drahtlosen, optischen, elektromagnetischen oder ähnlichen Funktionen. Der Begriff „elektronische Aufzeichnung" bezeichnet einen Vertrag oder eine andere Aufzeichnung, die mittels elektronischer Mittel erstellt, erzeugt, gesendet, mitgeteilt, empfangen oder gespeichert wird. Der Begriff „elektronische Signatur" bezeichnet eine elektronische Ton-, Symbol-, Verarbeitungs- oder andere Information, die an einen Vertrag oder eine andere Aufzeichnung angefügt oder logisch damit verknüpft ist und von einer Person mit der Absicht, die Aufzeichnung zu signieren oder zu authentisieren, ausgeführt oder eingesetzt wird. Der Begriff „Information" bezeichnet Daten, Text, Bilder, Töne, Codes, Computerprogramme, Software, Datenbanken und dergleichen. Der Begriff „Aufzeichnung" bezeichnet Information, die auf einem physischen Medium abgelegt oder in einem elektronischen oder anderen Medium gespeichert und in verwertbarer Form abrufbar ist. Der Begriff „Transaktion" bezeichnet eine Aktion oder eine Menge von Aktionen im Zusammenhang mit dem Durchführen eines Geschäftes, einer verbraucherbezogenen oder kommerziellen Angelegenheit zwischen zwei oder mehr Personen, darunter unter anderem (A) Verkaufen, Leasen, Tauschen, Lizenzieren oder eine andere Bereitstellung von (i) persönlichem Eigentum, darunter Güter und immaterielle Güter, (ii) Dienstleistungen und (iii) einer beliebigen Kombination hieraus; und (B) Verkaufen, Leasen, Tauschen oder eine andere Bereitstellung eines beliebigen Anspruches auf physisches Eigentum oder eine Kombination hieraus. Der Begriff „codiert" bezeichnet das Umwandeln von Daten in ein bestimmtes Format und kann die Verschlüsselung von Daten beinhalten. Der Begriff „Zertifizierung" bezeichnet das Validieren der Authentizität von jemandem oder etwas bzw. das Nachweisen der Gültigkeit von jemandem oder etwas. Im vorliegenden Fall beinhaltet der Begriff „Zertifizierung" die Authentisierung der elektronischen Signaturvorrichtung und des zugehörigen Zeitintervalls, der Raumauflösung und/oder anderer damit verknüpfter Maße, die zur Authentisierung einer elektronischen Signatur geeignet sind, und dergleichen mehr. Der Begriff „Stempel" bezeichnet das Hinzufügen eines Stempels im Sinne eines Hinzufügens eines Zeitstempels, Datumsstempels, Modellstempels oder Seriennummernstempels zu den Daten. Der Begriff „pseudozufällig" bezeichnet ein nach außen zufällig erscheinendes Aussehen, das jedoch nicht zufällig ist, sofern Kenntnisse über das Erstellen der Zufälligkeit vorliegen. Der Begriff „Steuerung" bezeichnet eine beliebige Vorrichtung, die dem Verarbeiten von Signalen dienen kann, darunter eine Anzahl von Datenverarbeitungsmitteln, beginnend mit einfachen 8-Bit-Mikrokontrollerchips bis einschließlich leistungsstarken Prozessoren wie RAMs, ROMs, Fleshes, Laufwerken, Hardwareverschlüsslern und Beschleunigern sowie mathematischen Koprozessoren.

[0045] Ein Ausführungsbeispiel der vorliegenden Erfindung sieht ein System, ein Verfahren und eine Vorrichtung vor, die die Sicherheit erhöhen und elektronische Signaturen mit bestehenden Vorschriften in Einklang bringen sowie praxistauglich machen. Die Erfindung bietet Sicherheit für eine Signatur, die in einer Peripherievorrichtung erfasst und an ein Hostverarbeitungssystem gesendet wird, wo die Signatur zum Zwecke des Ausführens einer Transaktion validiert oder bestätigt wird. Bei einer Implementierung der Erfindung wird eine elektronische Signatur in einer Peripherievorrichtung erfasst, die getrennt von der Hostverarbeitungseinheit angeordnet und auch nicht in dieser enthalten ist. Die Peripherievorrichtung kann von dem Hostverarbeitungssystem einige Fuß oder Tausende von Meilen entfernt angeordnet sein. Die Peripherievorrichtung ist dafür ausgelegt, die Signatur und die Aufzeichnungsdaten am Ort der Verwendung (beispielsweise in der Peripherievorrichtung) zu verbinden, um die Wahrscheinlichkeit zu verringern, dass jemand in die Lage versetzt wird, mittels Hacken in das – verschlüsselte oder unverschlüsselte – Übertragungsmedium einzudringen und die Rohsignaturdaten zu ermitteln. Durch Verbinden oder Verknüpfen der Signatur und der Aufzeichnung am Ort der Verwendung weist jede Aufzeichnung einen eindeutigen Schlüssel auf, der Versuche des Eindringens mittels Hacken zudem vereitelt. Ein Aspekt der Erfindung betrifft das Erfassen einer digitalen Signatur auf einer Punkt-für-Punkt-Basis und das Verbinden oder Verknüpfen der digitalen Signalpunkte, Segmente und dergleichen mit den Aufzeichnungsdaten.

[0046] Ein zweites Merkmal der Erfindung betrifft eine beidseitig bekannte Geheiminformation zwischen der Peripherievorrichtung und dem Hostverarbeitungssystem, um die Datenübertragung noch weiter zu sichern. Die Geheiminformation betrifft Daten, die nicht oder zumindest niemals mittels des Übertragungsmediums übertragen werden, sondern die mit einem programmierten Wert verknüpft sind, so beispielsweise mit einer Seriennummer oder einer Seriennummer, die von einem RTC-Wert (real-time computed RTC, echtzeitberechnet) modifiziert werden kann, oder die mittels eines Befehls ohne Ändern der Daten rückgesetzt werden kann. Die Geheiminformationen kann auch durch beliebige alternative Mittel bereitgestellt werden, so beispielsweise eine Hardware-Smartcard, ein alternatives Übertragungsverfahren, eine verschlüsselte Datenschnittstelle, ein alternatives Übertragungsmedium, das nicht mit der Primärdatenschnittstelle (das heißt der Signaturer-

fassungsvorrichtung) identisch ist, die von der Peripherievorrichtung zum Signieren oder Authentisieren der Handelstransaktionen verwendet wird.

[0047] Fig. 1 ist ein Blockdiagramm, das ein einem Ausführungsbeispiel der vorliegenden Erfindung entsprechendes System **100** zur Bereitstellung von Sicherheit für elektronische Signaturen darstellt. Eine Signaturerfassungsvorrichtung **102** ist am Ort der Verwendung angeordnet, wo eine Partei mittels elektronischen Signierens einer Transaktionsaufzeichnung eine Transaktion annehmen kann. Die Transaktionsaufzeichnungsdaten können entweder der Signaturerfassungsvorrichtung **102** oder dem Hostverarbeitungssystem **104** entstammen. Die Signaturerfassungsvorrichtung **102** ist kommunikativ über ein Übertragungsmedium **106** mit dem Hostverarbeitungssystem **104** gekoppelt. Die Signaturerfassungsvorrichtung **102** kann eine Vorrichtung sein, die entweder unabhängig ist oder einen Teil einer anderen Vorrichtung bildet, die wiederum in der Lage ist, die elektronische Signatur eines Anwenders oder eine andere Transaktionsauthentisierungsinformation zu erfassen. Eine „elektronische Signatur" oder eine „Signatur" bezeichnet im Sinne der vorliegenden Beschreibung unter anderem einen elektronischen Ton beziehungsweise elektronische Töne, ein Symbol beziehungsweise Symbole, einen Prozess beziehungsweise Prozesse, digitalisierte persönliche Unterschriften bzw. Signaturen, Nummerncodes, Fingerabdrücke, Handflächenabtastungen, Irisabtastungen und eine beliebige andere Information, die an einen Vertrag oder eine andere Aufzeichnung angefügt oder logisch damit verbunden werden kann und die von einer Person mit der Absicht, die Aufzeichnung zu signieren, ausgeführt oder eingesetzt werden kann.

[0048] Das Hostverarbeitungssystem **104** ist ein beliebiger Prozessor, ein beliebiger Computer, eine beliebige Vorrichtung und/oder ein beliebiges Netzwerk oder auch eine Kombination aus Vorrichtungen, die die elektronische Signatur validieren oder bestätigen und/oder die Transaktionsaufzeichnung verarbeiten.

[0049] Entsprechend einem Ausführungsbeispiel der Erfindung wird eine elektronische Signatur von der Signaturerfassungsvorrichtung **102** erfasst, die von der Hostverarbeitungseinheit **104** einige wenige Fuß oder Tausende von Meilen entfernt angeordnet ist. Die Signaturerfassungsvorrichtung **102** ist dafür ausgelegt, die erfassten Signatur- und Transaktionsaufzeichnungsdaten am Ort der Verwendung zu verbinden, um die Wahrscheinlichkeit zu verringern, dass jemand in die Lage versetzt wird, mittels Hacken in das – verschlüsselte oder unverschlüsselte – Übertragungsmedium **106** einzudringen und die Rohsignaturdaten zu ermitteln. Das Übertragungsmedium **106** kann ein sicherer Kommunikationsweg oder ein entsprechendes Netzwerk (das heißt eine eigens hierfür vorgesehene Leitung oder ein Privatdatennetzwerk), ein ungesicherter Kommunikationsweg oder ein entsprechendes Netzwerk (beispielsweise eine Telefonleitung, ein öffentliches Netzwerk, das Internet, Funkübertragungen und dergleichen) sein und/oder andere Kommunikationsvorrichtungen zusammen mit dem Übertragungsmedium **106** enthalten. Da in einigen Fällen das Übertragungsmedium gegebenenfalls nicht sicher ist, ist es überaus wichtig, dass die elektronische Signatur vor der Übertragung über dieses Medium geschützt wird. Dies bedeutet, dass ein unsicheres Übertragungsmedium sämtliche Übertragungen, darunter die elektronische Signatur, für die nicht autorisierte Ausforschung oder einen nicht autorisierten Zugriff offen darbietet. Die Transaktionsaufzeichnungsdaten oder die Transaktionsaufzeichnung können den Namen einer oder mehrerer Parteien der Transaktion, die Adressen, eine Liste von Waren und Dienstleistungen, die von der Transaktion betroffen sind, die Kosten der Waren oder Dienstleistungen, die Anzahl oder Einheiten, die von der Transaktion betroffen sind, das Transaktionsdatum und die Transaktionszeit, das Lieferdatum und die Lieferzeit oder beliebige andere Informationen oder Angaben enthalten, die zur Aufnahme in die Transaktionsaufzeichnung vor dem Signieren geeignet sind.

[0050] Bei einem Ausführungsbeispiel der Erfindung wird die erfasste Signatur vor der Übertragung von der Signaturerfassungsvorrichtung **102** mittels des Erstellens einer Hash-Codierung der Transaktionsaufzeichnungsdaten und des anschließenden Verwendens des Ergebnisses der Hash-Codierung als Verschlüsselungsschlüssel zur Verschlüsselung der erfassten Signatur verwendet. Bei einem anderen Ausführungsbeispiel der Erfindung kann zusätzliche Sicherheit durch Verwenden des Ergebnisses der Hash-Codierung der Transaktionsaufzeichnungsdaten, Kombinieren desselben mit einem oder mehreren Geheimschlüsseln (beispielsweise Echtzeitzeitgeber, Seriennummer der Peripherievorrichtung, interner Zähler oder eine andere sichere Zahl oder ein anderes sicheres Symbol), Verwenden eine Hash-Codierung der Kombination und Verwenden der sich ergebenden abgeleiteten Hash-Codierung als Schlüssel zur Verschlüsselung der erfassten Signatur vor einer Übertragung von der Signaturerfassurigsvorrichtung erfolgen. Man beachte, dass derselbe Hash-Codierungsalgorithmus oder auch ein anderer Hash-Codierungsalgorithmus bei bei der Erzeugung der Transaktionsaufzeichnungsdaten der Hash-Codierung und der abgeleiteten Hash-Codierung verwendet werden kann, ohne dass man hierbei den Schutzbereich der Erfindung verlassen würde.

[0051] Fig. 2 ist ein Blockdiagramm, das eine einem Ausführungsbeispiel der Erfindung entsprechende Peripherievorrichtung **200** darstellt, so beispielsweise die in Fig. 1 beschriebene Signaturerfassungs-

vorrichtung **102**, die dem Sichern von elektronischen Signaturen in Transaktionen dient. Die Peripherievorrichtung **200** kann eine Steuerung **202** mit einer Speicherkapazität (beispielsweise RAM, ROM, EEPROM und dergleichen) enthalten. Die Steuerung **202** kann kommunikativ mit einer oder mehreren Arten von elektronischen Signaturerfassungsschnittstellen **204** gekoppelt sein, wo ein Anwender oder eine Partei der Transaktion eine elektronische Signatur zur Annahme, zur Validierung und/oder Authentisierung der Transaktion bereitstellen kann. Die elektronischen Signaturerfassungsschnittstellen können einen oder mehrere Signaturschnittstellen enthalten, so beispielsweise eine Stift-/Schreibflächenschnittstelle, eine Fingerabdruckerkennungsschnittstelle, eine PIN-Tastatur, eine Spracherkennungsschnittstelle oder andere Authentisierungsschnittstellen. Vorzugsweise weisen die Signaturerfassungsschnittstellen **204** ihre eigenen Zeitgeberschaltungen und Werte auf, die zum Abtasten der Signaturdaten in regelmäßigen, periodischen und zertfizierten Intervallen verwendet werden. Sobald ein Anwender eine Signatur oder eine andere Authentisierungsinformation an der elektronischen Signaturerfassungsschnittstelle **204** bereitstellt, wird diese Information an die Steuerung **202** zur Verschlüsselung gesendet.

[0052] Ein Aspekt der Erfindung betrifft das Erfassen einer digitalen Signatur und/oder biometrischen Signatur auf einer Punkt-für-Punkt-Basis und das getrennte Verschlüsseln der Punkte mit den Aufzeichnungsdaten. Dies bedeutet, dass die digitale Signatur oder die biometrische Signatur als Punkte oder Segmente erfasst oder dargestellt werden können, darunter Lagekoordinaten (beispielsweise x-, y-, z-Punkte), Tonzeitsegmente oder Abtastungen, beim Eingeben bestimmter Punkte oder Segmente der digitalen Signatur ausgeübter Druck und/oder ein Zeitindex oder ein Inkrement des Punktes (beispielsweise die relative Zeit eines erfassten Punktes oder Segmentes, die Zeit zwischen erfassten Punkten/Segmenten, die zeitliche Länge eines erfassten Punktes oder Segmentes und dergleichen mehr). Die getrennt verschlüsselten Signaturabtastpunkte oder Segmente können in den Übertragungs- und/oder Empfangsvorrichtungen getrennt gespeichert werden, sodass die vollständige Signatur nicht auf demselben Prozessor oder in demselben Speicher zur gleichen Zeit vorhanden ist. Dies verhindert, dass böswillige Programme die Signatur durch Ausforschen des Prozessors oder des Speichers erfassen oder bestimmen.

[0053] Ein Aspekt der Erfindung befasst sich mit dem Schutz der erfassten Signatur, bevor diese die Peripherievorrichtung **200** verlässt. Entsprechend einem Ausführungsbeispiel der Erfindung ist die Steuerung **202** dafür ausgelegt, eine Transaktionsaufzeichnung zu initiieren oder zu empfangen. Eine derartige Transaktionsaufzeichnung enthält Information im Zusammenhang mit jener bestimmten Transaktion (beispielsweise rechtliche Vereinbarungen der Transaktion, Parteien der Transaktion, Adressen der Parteien, relevante Daten, Waren oder Dienstleistungen im Zusammenhang mit der Transaktion, Spezifizierung der Waren oder Dienstleistungen im Zusammenhang mit der Transaktion und dergleichen mehr). Die Steuerung **202** nimmt eine Hash-Codierungsoperation der Transaktionsaufzeichnung vor. Das Ergebnis der Hash-Codierungsoperation der Transaktionsaufzeichnungsdaten ist ein eindeutiger aufzeichnungsabhängiger Schlüssel, der als Aufzeichnungsschlüssel (record key) bezeichnet wird. Eine derartige Hash-Codierungsoperation wandelt die Eingabe von einem typischen großen Bereich in eine Ausgabe in einem kleinen Bereich um. Entsprechend einem weiteren Ausführungsbeispiel der Erfindung wird der Aufzeichnungsschlüssel außerhalb der Peripherievorrichtung **200** erzeugt und anschließend an die Steuerung **202** gesendet. Egal, welche der beiden Vorgehensweisen verwendet wird, es wird immer der sich ergebende Aufzeichnungsschlüssel anschließend von der Steuerung **202** zur Verschlüsselung der Signatur- oder Authentisierungsinformation innerhalb der Peripherievorrichtung **200** vor der Übertragung an die Hostverarbeitungseinheit **216** verwendet. So kann der Aufzeichnungsschlüssel beispielsweise als Eingabe für einen Verschlüsselungsalgorithmus zur Verschlüsselung der Signatur dienen. Eine Verschlüsselungseinheit **218** kann zudem eine zusätzliche Verschlüsselung, so diese erwünscht und spezifiziert ist, vor der Übertragung über ein Datenübertragungsmedium **220** bereitstellen.

[0054] Bei Ausführungsbeispielen, bei denen eine digitale Signatur auf einer Punkt-für-Punkt-Basis erfasst wird, können die erfassten Punkte oder Segmente getrennt verschlüsselt werden. Dies bedeutet, dass anstelle des Erfassens der gesamten Signatur und des anschließenden Verschlüsselns derselben gemäß einem Aspekt der Erfindung eine Verschlüsselung der Punkte oder Segmente der elektronischen Signatur unter Verwendung des Aufzeichnungsschlüssels, einer Hash-Codierung oder einer beliebigen hier beschriebenen Verschlüsselung erfolgt. Das getrennte Verschlüsseln der Punkte oder Segmente einer digitalen Signatur oder einer biometrischen Signatur erhöht die Sicherheit während der Übertragung.

[0055] Die Hostverarbeitungseinheit **216** stellt denjenigen Ort dar, an dem die Signatur bestätigt oder authentisiert wird und/oder an dem die Transaktionsaufzeichnung verarbeitet, validiert und/oder gespeichert wird. Entsprechend verschiedenen Ausführungsbeispielen der Erfindung kann die Hostverarbeitungseinheit **216** entweder eine Transaktionsaufzeichnung erstellen oder eine Transaktionsaufzeichnung von der Peripherievorrichtung **200** oder einer anderen Vorrichtung empfangen.

[0056] Ein Ausführungsbeispiel der Erfindung stellt ein oder mehrere Datenregister bereit, die verwendet werden können, um Informationen zu speichern, so beispielsweise einen Echtzeitzeitgeber **206**, einen rücksetzbaren Zähler **208**, eine Seriennummer **210** der Peripherievorrichtung oder einen Zahlengenerator **212** (beispielsweise einen Zufallszahlengenerator). Diese Datenregister sind kommunikativ derart mit der Steuerung **202** verbunden, dass ein oder mehrere Werte darin durch die Steuerung **202** beim Verschlüsseln der Signatur oder Authentisieren der Information aus der Signaturerfassungsschnittstelle **204** verwendet werden können. Entsprechend einem Ausführungsbeispiel der Erfindung kann beispielsweise eine Signatursicherheit durch Erstellen einer Hash-Codierung der Transaktionsaufzeichnung, Verwenden des Ergebnisses der Hash-Codierung der Transaktionsaufzeichnung und Kombinieren desselben mit einem oder mehreren Geheimschlüsseln (beispielsweise Echtzeitgeber, Seriennummer der Peripherievorrichtung, interner Zähler, pseudozufällige Zahl oder eine andere schere Zahl oder ein anderes sicheres Symbol), Verwenden einer Hash-Codierung jener Kombination und Verwenden der sich ergebenden abgeleiteten Hash-Codierung als Schlüssel zur Verschlüsselung der erfassten Signatur vor der Übertragung an die Peripherievorrichtung **200** bereitgestellt werden. Diese „Geheimschlüssel" stellen keine „Nachricht bzw. Mitteilung" dar, sondern Daten, die der Verbesserung der Sicherheit und Integrität des Prozesses dienen.

[0057] Entsprechend einigen Ausführungsbeispielen der Erfindung kann die Peripherievorrichtung **200** darüber hinaus eine Ausgabevorrichtung (beispielsweise einen Anzeigeschirm, einen Drucker und dergleichen) enthalten, an dem die Transaktionsaufzeichnung für einen Anwender oder eine Partei der Transaktion dargestellt werden kann. Diese Ausgabevorrichtung kann integral mit der Peripherievorrichtung **200** ausgebildet oder auch getrennt von der Peripherievorrichtung **200** angeordnet sein. Darüber hinaus kann eine Eingabevorrichtung vorgesehen sein, und zwar entweder integral mit der Peripherievorrichtung oder auch getrennt hiervon, wo der Anwender oder eine Partei der Transaktion die Transaktionsaufzeichnung modifizieren kann (beispielsweise durch Eingabe von persönlicher Information, Bestellinformation, Kontoinformation und dergleichen mehr).

[0058] Fig. 3 ist ein Flussdiagramm, das ein einem Ausführungsbeispiel der vorliegenden Erfindung entsprechendes Verfahren **300** zum Bereitstellen einer sicheren Transaktion zwischen einer Peripherievorrichtung und einem Hostverarbeitungssystem darstellt Eine Transaktionsaufzeichnung wird dem Signierenden **312** vorgelegt. Dies kann auf verschiedene Arten erfolgen, so beispielsweise mittels eines Ausdruckes auf Papier, durch Anzeigen des Inhalts an einer Peripherievorrichtung (beispielsweise einer Verkaufsstation, einem Bildschirm und dergleichen mehr), durch Anzeigen auf einer getrennten Anzeigevorrichtung in der Nähe des Signierenden oder durch eine andere geeignete Ausgabevorrichtung oder ein anderes geeignetes Ausgabemittel. Das Erzeugen einer endgültigen Transaktionsaufzeichnung kann eine durch den Anwender oder die Partei der Transaktion erfolgende Interaktion und Eingabe von Informationen beinhalten, so beispielsweise eines Namens beziehungsweise von Namen, einer Adresse beziehungsweise von Adressen, eines Dollarbetrages beziehungsweise von Dollarbeträgen und anderen Informationen oder Angaben, die geeignet sind, vor dem Signieren in der Transaktionsaufzeichnung abgelegt zu werden.

[0059] Man beachte, dass die Transaktionsaufzeichnung an einem beliebigen Ort erzeugt werden kann, darunter in einem Hostverarbeitungssystem (beispielsweise einem Computer oder einer anderen Vorrichtung, die von der signaturerfassenden Peripherievorrichtung getrennt ist), in einer signaturerfassenden Peripherievorrichtung, wenn die volle Aufzeichnung an die Peripherievorrichtung gesendet worden ist, oder auch beides. So kann eine Transaktionsaufzeichnung beispielsweise in einem Hostverarbeitungssystem entfernt von der Peripherievorrichtung initiiert und anschließend dem Anwender oder der Partei vorgelegt werden, der/die dann die Transaktionsaufzeichnung durch Eingabe von zusätzlicher Information modifzieren kann.

[0060] Eine Hash-Codierung der Übertragungsaufzeichnung wird erzeugt, siehe **304**. Die Hash-Codierungsoperation an der Transaktionsaufzeichnung kann in dem Hostverarbeitungssystem (beispielsweise einem Computer oder einer anderen Vorrichtung, die von der signaturerfassenden Peripherievorrichtung getrennt ist), der signaturerfassenden Peripherievorrichtung, wenn die volle Aufzeichnung an die Peripherievorrichtung gesendet worden ist, oder auch in beiden erfolgen. Wird die Hash-Codierung nur in dem Hostverarbeitungssystemen erstellt, wird sie anschließend über eine geeignete Schnittstelle an die Peripherievorrichtung gesendet.

[0061] Die Peripherievorrichtung erfasst anschließend die Signatur, siehe **306**, und verknüpft die Signatur mit der Hash-Codierung der Transaktionsaufzeichnung oder einer bestimmten Ableitung der Hash-Codierung der Transaktionsaufzeichnung, siehe **308**. Entsprechend einem Ausführungsbeispiel der Erfindung bedeutet dieses „Verknüpfen" der Signatur und der Hash-Codierung der Transaktionsaufzeichnung, dass die Hash-Codierung der Transaktionsaufzeichnung als Eingabe oder Schlüssel für einen Verschlüsselungsalgorithmus verwendet wird, der die erfasste Signatur verschlüsselt.

[0062] Anstatt der Verwendung lediglich der Hash-Codierung der Transaktionsaufzeichnung zur Sicherung der erfassten Signatur bedient sich ein Ausführungsbeispiel der Erfindung zu diesem Zweck einer abgeleiteten Hash-Codierung. Eine Ableitung der Hash-Codierung der Transaktionsaufzeichnung kann einfach eine zweite Hash-Codierung, eine Prüfsumme oder eine andere mathematische Operation sein, oder auch eine zweite Hash-Codierung oder Operation, die andere Daten zusätzlich zu den Transaktionsdaten enthält. Diese zusätzlichen Daten können innerhalb der Peripherievorrichtung vorhanden sein, so beispielsweise Zeit und Datum oder Zeitgeberzählerdaten oder Daten, die zum Zeitpunkt der Signaturerfassung ohne durch den Computer erfolgendes Sender als Teil der aktuellen Transaktion eingegeben werden, oder es handelt sich um eine Seriennummer oder andere codierte Daten im Zusammenhang mit der Peripherievorrichtung. Die abgeleitete Hash-Codierung kann zudem durch Mischen der Hash-Codierungsdaten mit einem Geheimschlüssel erzeugt werden, der zum Schutz der Datenübertragung verwendet werden kann. Alternativ kann die abgeleitete Hash-Codierung auf einer Gleichung oder einem Schlüssel beruhen, die/der in die Peripherievorrichtung geladen wird und die/der nur der Peripherievorrichtung und dem Prozessor bekannt ist. In jedem Fall wird unabhängig davon, welche endgültige Form die aus der Hash-Codierung der Transaktionsaufzeichnung abgeleiteten Daten aufweisen, nachstehend von einem Aufzeichnungsschlüssel gesprochen.

[0063] Die Signatur wird anschließend an das Hostverarbeitungssystem in einer Form übertragen, in der sie verschlüsselt ist, siehe **310**, und zwar entweder vollständig oder teilweise mit dem Aufzeichnungsschlüssel, oder sie wird anderweitig auf eine Weise gesendet, die mit dem Aufzeichnungsschlüssel in Zusammenhang steht. Man beachte, dass die Verschlüsselung oder Verknüpfung zusätzlich zu einer beliebigen Form oder einer geläufigen Verschlüsselung erfolgt, die als Teil eines Standarddatenübertragungssicherheitsprotokolls verwendet werden können. Bei einem Ausführungsbeispiel können die verschiedenen Abtastpunkte oder Segmente einer elektronischen Signatur oder einer biometrischen Signatur mit einem anderen Aufzeichnungsschlüssel oder einer anderen Hash-Codierung auf Grundlage desselben oder eines anderen Aufzeichnungsschlüssels verschlüsselt werden. So kann beispielsweise ein anderer Verschlüsselungsschlüssel in pseudozufälliger Weise oder auf andere Art erzeugt und zur Verschlüsselung der verschiedenen Signaturpunkte oder Abtastungen verwendet werden.

[0064] Fig. 4 ist ein Flussdiagramm, das ein einem Ausführungsbeispiel der vorliegenden Erfindung entsprechendes elektronisches Signaturverschlüsselungsverfahren auf Grundlage einer Hash-Codierung der Transaktionsaufzeichnung darstellt. Eine Transaktionsaufzeichnung wird von dem Hostverarbeitungssystem **104** erstellt, siehe **402**. Die Transaktionsaufzeichnung kann, siehe **404**, an eine Eingabe-/Ausgabevorrichtung (I/O) **405** gesendet werden (so beispielsweise eine Schreibfläche, eine Anzeige, ein berührungsempfindlicher Schirm, eine Tastatur, ein Drucker, ein Lautsprecher und ein Mikrofon, eine blindenschrifttechnische Vorrichtung und dergleichen), und zwar zur Darstellung für den Anwender und möglicherweise zur Bearbeitung **406**, so beispielsweise zum Hinzufügen von Kundeninformation und dergleichen mehr. Die Transaktionsaufzeichnung kann auch, siehe **408**, an dem Hostverarbeitungssystem **104** modifiziert werden, um eine endgültige Aufzeichnung **410** zu erstellen. Die endgültige Aufzeichnung kann ab diesem Punkt auf verschiedene Weisen verarbeitet werden.

[0065] Entsprechend einem Ausführungsbeispiel der Erfindung kann die Transaktionsaufzeichnung, siehe **412**, an die Eingabe-/Ausgabevorrichtung **405** zum optionalen Bearbeiten **414** gesendet werden. Die Signaturperipherievorrichtung **102** kann eine Hash-Codierung der Transaktionsaufzeichnung erzeugen, die zu einem Aufzeichnungsschlüssel führt, siehe **416**. Bei einigen Implementierungen erfolgt, wenn verschiedene Signaturpunkte oder Segmente getrennt verschlüsselt werden, eine andere Hash-Codierung auf Grundlage der Transaktionsaufzeichnung oder eines pseudozufälligen Wertes zum Ermitteln eines oder mehrerer Aufzeichnungsschlüssel, mit denen die verschiedenen Signaturabtastungen oder Segmente verschlüsselt werden sollen.

[0066] Entsprechend einem weiteren Ausführungsbeispiel der Erfindung kann das Hostverarbeitungssystem **104** eine Hash-Codierung **420** der Transaktionsaufzeichnung **410** zur Erstellung des Aufzeichnungsschlüssels erzeugen. Der Aufzeichnungsschlüssel wird anschließend an die Signaturperipherievorrichtung **102** gesendet.

[0067] Die Signaturperipherievorrichtung **102** fordert anschließend an, dass der Anwender oder eine Partei die Transaktion durch Eingabe einer elektronischen Signatur, siehe **418**, in die Signaturperipherievorrichtung **104** signiert oder authentisiert. Bei einigen Ausführungsbeispielen der Erfindung kann eine andere Authentisierungsvorrichtung anstatt der Signaturperipherievorrichtung **102** zum Aufnehmen anderer Authentisierungsinformation von dem Anwender oder der Partei der Transaktion bereitstehen. Die Signaturperipherievorrichtung **102** erfasst die Signatur des Anwenders und verschlüsselt sie, siehe **418**. Bei einem Ausführungsbeispiel der Erfindung kann die Signaturperipherievorrichtung **104** die Signatur des Anwenders unter Verwendung des Aufzeichnungsschlüssels als Eingabe für einen Verschlüsselungsalgorithmus enthalten.

[0068] Die verschlüsselte Signatur wird anschließend von der Signaturperipherievorrichtung **102** an den Prozessor **104** zum Zwecke der Bestätigung, siehe **422**, gesendet. Eine derartige Signaturbestätigung **422** beinhaltet das Entschlüsseln der verschlüsselten Signatur und das Vergleichen der elektronischen Signatur des Anwenders, die in die Signaturperipherievorrichtung **102** eingegeben worden ist, mit einer vorab eingegebenen elektronischen Signatur. Zum Entschlüsseln der verschlüsselten Signatur muss das Hostverarbeitungssystem **104** über den Aufzeichnungsschlüssel verfügen, den es aus den Transaktionsaufzeichnungsdaten erzeugen kann. Passen die elektronischen Signaturen zusammen, so wird die Transaktionsaufzeichnung als richtig signiert betrachtet, siehe **424**. Die endgültige Aufzeichnung **410** wird zusammen mit der elektronischen Signatur gespeichert oder verarbeitet, siehe **424**. Man beachte, dass wo verschiedene Punkte oder Segmente der Signatur getrennt verschlüsselt und anschließend getrennt übertragen werden, diese getrennten Punkte oder Segmente auch getrennt entschlüsselt und verifiziert werden können.

[0069] Ein weiteres Merkmal der Erfindung sieht vor, dass die Signaturperipherievorrichtung **102** zudem derart programmiert werden kann, dass sie eine Hash-Codierung der Signatur des Anwenders erzeugt, und zwar entweder gänzlich oder teilweise, und entweder die Hash-Codierung, den Aufzeichnungsschlüssel, die Hash-Codierung der Signatur oder eine Kombination von allen dreien in einem internen Speicher ablegt oder an den Host, an alternative Speicherstellen oder Hosts über ein beliebiges verfügbares Mittel zur späteren Verwendung überträgt. Im Vergleich sollten die Signatur des Anwenders und/oder die Transaktionsaufzeichnungsdaten hierfür in Frage kommen.

[0070] Durch das Verfahren (1) der Hash-Codierung der Transaktionsaufzeichnung durch Senden der Aufzeichnungsdaten an die Peripherievorrichtung oder Hash-Codierung der Daten in dem Hostverarbeitungssystem und anschließendes Senden an die Peripherievorrichtung und (2) durch die Peripherievorrichtung erfolgendes Verschlüsse in oder auf andere Weise erfolgendes Verknüpfen der Signatur mit der Hash-Codierung oder einer Ableitung der Hash-Codierung wird eine sichere elektronische Signatur erstellt, die den in jüngster Zeit in Kraft getretenen Gesetzen besser gerecht wird und am Ort der Verwendung einsetzbar ist. Man beachte, dass dasselbe Verfahren an getrennten Punkten oder Segmenten einer Signatur anstatt an der gesamten Signatur vorgenommen werden kann.

[0071] Bei dem in Fig. 4 beschriebenen Schema sind die Möglichkeiten eingeschränkt, dass ein bösartiges Programm, das auf dem Prozessor läuft, in der Lage ist, eine Signatur zu „stehlen”, wenn die Verschlüsselung jener Signatur mit einer transaktionsspezifischen Hash-Codierung und einem Aufzeichnungsschlüssel verbunden ist, die sich natürlich bei jeder Transaktion ändern, da der Aufzeichnungsschlüssel auf der Transaktionsaufzeichnung beruht. Diese Synergie löst im Wesentlichen zwei Probleme gleichzeitig, nämlich dasjenige der Sicherheit des Verschlüsselungsschlüssels und dasjenige der Verbindung von Signatur und Aufzeichnung.

[0072] Die Verwendung einer abgeleiteten Hash-Codierung stellt zusätzliche Vorteile mit Blick auf die Integrität des Systems entweder mit oder ohne Datenverschlüsselung bereit. So kann eine Bank beispielsweise eine derartige abgeleitete Hash-Codierung implementieren, um einen beliebigen Versuch des Ausforschens von Signaturen in dem Netzwerk für einen möglichen Betrug zu verhindern.

[0073] Fig. 5 ist ein Flussdiagramm, das ein einem weiteren Ausführungsbeispiel der vorliegenden Erfindung entsprechendes Verfahren zum Verschlüsseln einer elektronischen Signatur auf Grundlage eines abgeleiteten Hash-Codierungsschemas darstellt. Das anhand Fig. 5 beschriebene Verfahren ist im Wesentlichen ähnlich zu dem anhand Fig. 4 beschriebenen, wobei hier jedoch eine abgeleitete Hash-Codierung zur Bereitstellung zusätzlichen Sicherheit hinzugefügt ist. Sobald eine endgültige Transaktionsaufzeichnung erstellt ist, siehe **410**, wird die Transaktionsaufzeichnung hash-codiert, und zwar entweder in dem Hostverarbeitungssystem **420** oder der Signaturperipherievorrichtung **416**, um einen Aufzeichnungsschlüssel **522** zu erstellen. Die Signaturperipherievorrichtung kann einen oder mehrere Register mit einem Echtzeitzeitgeber, einer Seriennummer der Peripherievorrichtung, einem Pseudozufallszahlengenerator, einem rücksetzbaren Zähler oder einem anderen Geheimschlüssel enthalten, die zur Erstellung einer sicheren abgeleiteten Hash-Codierung **524** verwendet werden können. Entsprechend einem Ausführungsbeispiel der Erfindung kann in einem periodischen oder zufälligen Intervall in einem Bereich von beispielsweise Tagen oder Wochen bis hin zu Minuten oder auch bei jeder Transaktion das Hostverarbeitungssystem **104** auf jede Signaturperipherievorrichtung **102** zugreifen und einen Zeitgeber oder einen Zähler zurücksetzen, während gleichzeitig ein entsprechender Zeitgeber oder Zähler in der auf dem Hostverarbeitungssystem laufenden Software auf einen willkürlichen oder pseudozufälligen Wert zurückgesetzt oder gesetzt wird. Eine auslesbare Seriennummer in jeder Signaturperipherievorrichtung **102** kann zur Erleichterung der Verwaltung dieses Prozesses durch Verwendung der Peripherieseriennummer zur Identifizierung der verschiedenen Signaturperipherievorrichtungen **102** und/oder als Eingabe oder Wert zum Setzen des Zeitgebers, des Zählers oder des Pseudozufallszahlengenerators beitragen.

[0074] Unter Verwendung eines oder mehrerer Werte gemäß Bereitstellung durch einen Zeitgeber, Zähler, eine Seriennummer oder einen Pseudozufallszahlengenerator kann die Peripherievorrichtung **102** einen abgeleiteten Aufzeichnungsschlüssel auf Grundlage der Hash-Codierung der Transaktionsaufzeichnung und zusätzlicher Information aus einem oder mehreren Werten gemäß Bereitstellung allein durch die Peripherievorrichtung **102** erzeugen. Der abgeleitete Aufzeichnungsschlüssel kann auf eine oder mehrere Arten erzeugt werden, ohne den Schutzbereich der Erfindung zu verlassen. Bei einem Ausführungsbeispiel der Erfindung wird eine Hash-Codierung der Transaktionsaufzeichnung erzeugt, und der sich ergebende Aufzeichnungsschlüssel wird anschließend mit einem oder mehreren Werten gemäß Bereitstellung durch einen Zeitgeber, einen Zähler, eine Seriennummer und/oder einen Pseudozufallszahlengenerator kombiniert. Eine derartige Kombination kann das Anhängen dieser Werte an den Beginn, an das Ende und/oder an eine Stelle in der Mitte des Aufzeichnungsschlüsselwertes beinhalten. Eine Kombination kann darüber hinaus das Durchführen einer Operation unter Verwendung sowohl des Aufzeichnungsschlüssels und des einen oder der mehreren Werte beinhalten. Der sich ergebende Aufzeichnungsschlüssel und die Wertekombination werden anschließend einer Hash-Codierung unterzogen, um einen abgeleiteten Aufzeichnungsschlüssel zu erzeugen, der verwendet werden kann, um die Signatur in der Peripherievorrichtung **102** zu verschlüsseln.

[0075] Entsprechend einem weiteren Ausführungsbeispiel der Erfindung werden die Transaktionsaufzeichnung und ein oder mehrere Werte gemäß Bereitstellung durch den Peripheriezeitgeber, den Zähler, die Seriennummer oder den Pseudozufallszahlengenerator kombiniert. Die sich ergebende Kombination wird anschließend einer Hash-Codierung unterzogen, um einen abgeleiteten Aufzeichnungsschlüssel zu erstellen. Andere Vorgehensweisen zur Erstellung eines abgeleiteten Aufzeichnungsschlüssels auf Grundlage der Transaktionsaufzeichnung und zusätzlicher Information (beispielsweise Zählwerte, Zeitgeber und dergleichen mehr), die nur Von der Peripherievorrichtung **102** bereitgestellt werden (das heißt nicht an das Hostverarbeitungssystem **104** oder von diesem übertragen werden), sind von der Erfindung ebenfalls umfasst.

[0076] Eine Signatur wird anschließend in der Peripherievorrichtung **102** erfasst und mit dem abgeleiteten Aufzeichnungsschlüssel **524** verbunden, verschlüsselt oder auf andere Weise verknüpft (das heißt, der abgeleitete Aufzeichnungsschlüssel kann als Eingabe oder Schlüssel für einen Verschlüsselungsalgorithmus dienen). Die verschlüsselte Signatur wird anschließend an das Hostverarbeitungssystem **104** gesendet, und zwar im Wesentlichen in Echtzeit, zur Bestätigung der Signatur, siehe **528**. Vor dem Bestätigen der Signatur muss die empfangene verschlüsselte Signatur durch das Hostverarbeitungssystem entschlüsselt werden. Der Begriff „Bestätigung” soll dahingehend interpretiert werden, dass die Daten intakt angekommen sind, und zwar mittels Sicherstellung einer geeigneten Entschlüsselung und Identifizierug der Daten entweder zur einfachen Bestätigung, dass ein intaktes Ankommen erfolgt ist, oder zur Authentisierung einer Signatur, wobei die empfangene elektronische Signatur mit den Daten oder einer Mustervorlage, die für diesen Zweck geeignet ist, verglichen wird. Wie vorstehend bereits bemerkt wurde, kann dieser Prozess getrennt an Punkten oder Segmenten einer Signatur ausgeführt werden, anstatt dass er an der Signatur als Ganzes ausgeführt wird. Durch implementieren dieses Verfahrens an getrennten abgetasteten Punkten oder Segmenten kann eine größere Sicherheit bei der Übertragung der Signatur gewährleistet werden.

[0077] Da diese zusätzliche Information (das heißt beispielsweise Zählwerte, Zeitgeber und dergleichen mehr), die von der Peripherievorrichtung **102** zur Erzeugung des abgeleiteten Aufzeichnungsschlüssels verwendet wird, nicht durch die Peripherievorrichtung **102** übertragen wird, muss das Hostverarbeitungssystem **104** seinen eigenen entsprechenden abgeleiteten Aufzeichnungsschlüssel zur Entschlüsselung der verschlüsselten Signatur erstellen. Da der abgeleitete Aufzeichnungsschlüssel unter Verwendung von Echtzeitwerten (das heißt beispielsweise Zählerwerten, Zeitgebern und dergleichen mehr) erzeugt wird, muss das Hostverarbeitungssystem **104** seinen eigenen abgeleiteten Aufzeichnungsschlüssel im Wesentlichen in derselben Zeit berechnen, in der die Peripherievorrichtung **102** ihren abgeleiteten Aufzeichnungsschlüssel **530** erzeugt.

[0078] Da das Hostverarbeitungssystem **104** den Zeitgeber, den Zähler, den Pseudozufallszahlengenerator und dergleichen mehr der Peripherievorrichtung genauso wie seine eigenen entsprechenden internen Zeitgeber, Zähler, Pseudozufallszahlengeneratoren und dergleichen selbst setzen oder zurücksetzen kann, kann es sich selbst nach Bedarf mit der Peripherievorrichtung synchronisieren. Wenn also eine Berechnung im Wesentlichen in derselben Zeit erfolgt, so kann derselbe Wert des abgeleiteten Aufzeichnungsschlüssels von der Peripherievorrichtung **102** und dem Hostverarbeitungssystem **104** berechnet werden. Das Hostverarbeitungssystem **104** kann zufällig oder periodisch gesetzt werden oder periodisch seinen internen Zeitgeber, Zähler und/oder Pseudozufallszahlengenerator mit denjenigen der Peripherievorrichtung **102** synchronisieren oder diese periodisch oder willkürlich setzen oder zurücksetzen.

[0079] Ein weiteres Merkmal der Erfindung betrifft das Ausgleichen von Unterschieden bzw. Differen-

zen zwischen dem internen Zeitgeber, Zähler und/oder Pseudozufallszahlengenerator und dergleichen in der Peripherievorrichtung **102** und dem entsprechenden Wert beziehungsweise den entsprechenden Werten in dem Hostverarbeitungssystem **104**. Entsprechend einem Ausführungsbeispiel der Erfindung werden diese Werte nicht zwischen der Peripherievorrichtung und dem Hostverarbeitungssystem übertragen. Dennoch müssen bei diesem Ausführungsbeispiel der Erfindung das Hostverarbeitungssystem **104** und die Peripherievorrichtung **102** denselben abgeleiteten Aufzeichnungsschlüssel berechnen, damit die verschlüsselte Signatur geeignet von dem Hostverarbeitungssystem **104** entschlüsselt werden kann. Da sich diese Werte (beispielsweise Zeitgeber, Zähler und/oder Pseudozufallszahlen und dergleichen mehr) mit der Zeit ändern, ist wichtig, dass das Hostverarbeitungssystem **104** den abgeleiteten Aufzeichnungsschlüssel in im Wesentlichen derselben Zeit berechnet, in der dieser von der Peripherievorrichtung **102** berechnet oder ein anderweitiger Ausgleich für diesen Unterschied bereitgestellt wird. Unter bestimmten Umständen sind diese Werte (beispielsweise Zeitgeber, Zähler und/oder Pseudozufallszahlen und dergleichen mehr) jedoch in dem Hostverarbeitungssystem **104** und in der Peripherievorrichtung **102** nicht genau gleich. Dies kann von Übertragungsverzögerungen, Verarbeitungszeitgeberversetzungen oder Abdriftungen oder durch Unterschiede bei den Verarbeitungsgeschwindigkeiten bedingt sein.

[0080] Fig. 6 ist ein Flussdiagramm, das ein einem Ausführungsbeispiel der Erfindung entsprechendes Verfahren zum Suchen nach dem richtiger abgeleiteten Aufzeichnungsschlüssel in dem Hostverarbeitungssystem darstellt. Zunächst berechnet das Hostverarbeitungssystem einen ersten abgeleiteten Aufzeichnungsschlüssel gemäß Beschreibung in Fig. 5, siehe **602**. Es bedient sich dieses ersten abgeleiteten Aufzeichnungsschlüssels zur Entschlüsselung der verschlüsselten Signatur, die es von der Peripherievorrichtung empfangen hat, siehe **604**. Anschließend erfolgt ein Vergleichen der entschlüsselten Signatur mit einer gespeicherten Signatur, siehe **606**. Passen die beiden Signaturen nicht zusammen, so kann das Hostverarbeitungssystem gegebenenfalls einen bekannten Marker in Anfügung an die Signatur in der Peripherievorrichtung, um nachzuprüfen, ob eine Erkennung erfolgen kann. Kann eine Erkennung anhand dieses bekannten Markers erfolgen, so bedeutet dies, dass der richtige abgeleitete Aufzeichnungsschlüssel berechnet und die empfangene Signatur nicht gültig ist. Wird der bekannte Marker nicht erkannt, so kann das Hostverarbeitungssystem davon ausgehen, dass es sich nicht des richtigen abgeleiteten Aufzeichnungsschlüssels bedient hat. Man betrachte, dass andere Verfahren zum Bestimmen, ob der richtige abgeleitete Aufzeichnungsschlüssel verwendet worden ist, eingesetzt werden können, ohne dass man den Schutzbereich der vorliegenden Erfindung verlassen würde.

[0081] Das Hostverarbeitungssystem sucht anschließend nach dem richtigen abgeleiteten Aufzeichnungsschlüssel. Wird beispielsweise ein Zeitgeberwert X von dem Hostverarbeitungssystem zur Erzeugung des abgeleiteten Aufzeichnungsschlüssels verwendet, so berechnet das Hostverarbeitungssystem anstelle dessen beispielsweise einen zweiten abgeleiteten Aufzeichnungsschlüssel unter Verwendung von X – 1, siehe **610**. Der zweite abgeleitete Aufzeichnungsschlüssel wird anschließend zum Entschlüsseln der verschlüsselten Signatur verwendet, siehe **612**. Versagt der zweite abgeleitete Aufzeichnungsschlüssel bei der Erzeugung der richtigen Signatur, so berechnet das Hostverarbeitungssystem anstelle dessen anschließend einen dritten abgeleiteten Aufzeichnungsschlüssel unter Verwendung von X + 1, siehe **614**, und wiederholt den Bestätigungsprozess, siehe **616**. Diese Suche wird weitergeführt, bis die Signatur richtig entschlüsselt ist oder eine maximale Anzahl N von Vorgängen durchgeführt wurde, siehe **622**. Ein Neuversuchszähler wird bei jeder Iterierung, siehe **620**, inkrementiert, und der Berichtigungswert i, der zum Suchen nach der richtigen Zeitgeberzahl verwendet wird, wird ebenfalls inkrementiert, siehe **618**. Hat nach N Suchvorgängen das Hostverarbeitungssystem, siehe **624**, die Signatur immer noch nicht richtig entschlüsselt, so kann sie anfordern, dass die Peripherievorrichtung die verschlüsselte Signatur erneut sendet, oder es kann den Zeitgeber, die Zähler, die Pseudozufallszahl und dergleichen mehr in der Peripherievorrichtung lokal zurücksetzen und anfordern, dass die Peripherievorrichtung die Signatur erneut verschlüsselt und sendet.

[0082] Durch Verwenden des Schemas für einen abgeleiteten Aufzeichnungsschlüssel kann das System sehr effektiv Versuche des Ausforschens der Signaturen auf dem Datenkommunikationsweg oder auf andere Weise in der Software vereiteln, auf der das Hostverarbeitungssystem läuft, und es wird die Verwendung von „gestohlenen” Signaturdaten verhindert, die zwischen der Peripherievorrichtung **102** und dem Hostverarbeitungssystem **104** entnommen werden können.

[0083] Wird die Signalübertragung von der Peripherievorrichtung **102** an das Hostverarbeitungssystem **104** verzögert, so kann eine Echtzeitzeitgeber- und Dateninformation von dem Hostverarbeitungssystem **104** an die Peripherievorrichtung **102** gesendet werden, und die Peripherievorrichtung **102** gibt ihre eigene Echtzeitzeitgeber- und Dateninformation zusammen mit der verschlüsselten Signatur aus, damit ein bei der Übertragung aufgetretener Zeitversatz durch das Hostverarbeitungssystem **104** ausgeglichen werden kann.

[0084] Auf ähnliche Weise werden beliebige andere „Geheimnisse", die sowohl dem Hostverarbeitungssystem **104** wie auch der Peripherievorrichtung **102** bekannt sind, eher selten zwischen beiden übertragen oder sicher übertragen oder durch ein geeignetes anderes Mittel, so beispielsweise eine Smartcard oder ein alternatives Übertragungsmedium, bereitgestellt, können zu dem Prozess des Erstellens der abgeleiteten Hash-Codierung hinzugefügt werden, die zur Erstellung des abgeleiteten Aufzeichnungsschlüssels verwendet wird. Die Verwendung eines „Geheimschlüssels" kann erfolgen, um die Integrität und Sicherheit der transaktionsaufzeichnungsbasierten Hash-Codierungsverschlüsselung zu verbessern, wobei sich der Aufzeichnungsschlüssel, der jeder Transaktionsaufzeichnung entspricht, im Wesentlichen mit jeder Transaktion ändert.

[0085] Ein weiteres Merkmal der Erfindung betrifft ein Verfahren zur Verwendung eines Echtzeitzeitgebers zur Identifizierung einer signaturerfassenden Peripherievorrichtung und zur Verbesserung der Datenübertragungsintegrität und Sicherheit. Aus Gründen der Einfachheit erfolgt die Beschreibung aus der Perspektive des Hostverarbeitungssystems heraus, das die steuernde Einheit darstellt. Gleichwohl kann dieses Verfahren auch von der Peripherievorrichtung, dem Hostverarbeitungssystem oder einer dritten steuernden Einheit initiiert und/oder gesteuert werden.

[0086] Fig. 7 ist ein Flussdiagramm, das ein einem Ausführungsbeispiel der vorliegenden Erfindung entsprechendes Verfahren zur Verwendung verschiedener Zeitgeberwerte in dem Hostverarbeitungssystem und der Peripherievorrichtung darstellt, um mit der Übertragung und Entschlüsselung einer Signatur umzugehen, die von der Peripherievorrichtung an das Hostverarbeitungssystem gesendet worden ist. Ein erster Zeitwert wird bestimmt und von dem Hostverarbeitungssystem, siehe **702**, verwendet. Das Hostverarbeitungssystem weist die Peripherievorrichtung an, ihren internen Echtzeitzeitgeber (RTC) auf einen anderen Zeitwert, siehe **704**, (das heißt einen zweiten Zeitwert) zu setzen. Treten merkliche Verzögerungen in dem Datenübertragungskanal auf, so kann die Peripherievorrichtung an das Hostverarbeitungssystem einen Hinweis ausgeben, dass die Zeit oder das Datum gesetzt worden sind. Unter Verwendung dieser Angabe kann das Hostverarbeitungssystem anschließend bestimmen, dass eine nominelle Kommunikationsverzögerung zu oder von der Peripherievorrichtung, siehe **706**, gegeben ist. Der Zeitversatz kann auf Einrichtungs- oder Zweirichtungsbasis bestimmt werden, wobei die Zeitversatzinformation gegebenenfalls später in diesem Prozess verwendet werden kann.

[0087] Innerhalb der Peripherievorrichtung steuert der Echtzeitzeitgeber (RTC) den Zustand eines Zählers. Der Zähler kann durch eine Anweisung von dem Hostverarbeitungssystem zurückgesetzt werden, und sowohl der Zähler wie auch der RTC sind durch Verwendung eines Batteriebackups, falls notwendig, immer in Betrieb. Zu einem Zeitpunkt, der von dem Hostverarbeitungssystem bestimmt wird, weist das Hostverarbeitungssystem das Zurücksetzen des Zählers der Peripherievorrichtung an, siehe **708**. Zur selben Zeit setzt das Hostverarbeitungssystem einen Wert fest, der die Entsprechung zwischen seinem eigenen Zeitgeberwert (beispielsweise einem ersten Zeitwert), dem RTC-Wert der Peripherievorrichtung (das heißt dem zweiten Zeitwert) oder einem unabhängigen RTC-Wert, siehe **710**, herstellt. Das Hostverarbeitungssystem setzt zudem den Wert eines internen Zählers in dem Hostverarbeitungssystem, der dem Zähler in der Peripherievorrichtung, siehe **712**, entspricht. Gegebenenfalls kann der Kommunikationsversatz auch bei dieser Entsprechung durch Anpassen des Wertes des Hostverarbeitungssystems entsprechend dem Zeitversatz, siehe **714**, Berücksichtigung finden. Der Wert des Zählers des Hostverarbeitungssystems und seine Entsprechung zur Echtzeit werden geheimgehalten. So kann das Hostverarbeitungssystem beispielsweise einen Rücksetzbefehl an den Zähler der Peripherievorrichtung um 12:00 Uhr GMT senden, wodurch der Zähler in der Peripherievorrichtung auf Null (0) oder einen anderen Wert zurückgesetzt wird, der vorbestimmt, zufällig oder auf Grundlage von einigen anderen kryptografischen Daten, Daten im Zusammenhang mit der Peripherievorrichtung (beispielsweise ihre Seriennummer oder eine Hash-Codierung ihrer Seriennummer) oder anderen Daten sein kann. Zur selben Zeit zeichnet das Hostverarbeitungssystem seinen Echtzeitwert (das heißt den ersten Zeitwert) auf eine ihm zu eigene sichere Weise sowie optional eine Zahl auf, die direkt oder indirekt oder auf unbekannte Weise dem Ereignis entspricht.

[0088] Zu einem späteren Zeitpunkt, zu dem eine Transaktion zwischen der Peripherievorrichtung und dem Hostverarbeitungssystem stattfindet, haben nur das Hostverarbeitungssystem und die Peripherievorrichtung Kenntnis von der Entsprechung zwischen den Zähler- oder Zeitgeberwerten in jeder Einheit. Die Peripherievorrichtung bedient sich ihres Zähler- oder Zeitgeberwertes oder einer pseudozufälligen Zahl, die unter Verwendung eines dieser beiden Werten erzeugt ist, um die Signaturdaten, siehe **716**, sicher zu übertragen. Bei einem Ausführungsbeispiel der Erfindung bedient sich die Peripherievorrichtung beispielsweise des Zählers oder Zeitgeberwertes oder der Pseudozufallszahl als Stempel (beispielsweise Zeitstempel, Wertstempel und dergleichen) bei der Übertragung von einem oder mehreren Datenpaketen oder Segmenten an das Hostverarbeitungssystem. Bei einem anderen Ausführungsbeispiel der Erfindung bedient sich die Peripherievorrichtung des Zähler- oder Zeitgeberwertes oder der Pseudozu-

fallszahl zur Codierung oder Verschlüsselung der erfassten Signatur vor der Übertragung an das Hostverarbeitungssystem. Bei einer Implementierung der Erfindung können diese Zähler oder Zeitgeberwerte oder Pseudozufallszahlen beim getrennten Verschlüsseln von verschiedenen Abtastpunkten oder Segmenten einer Signatur verwendet werden.

[0089] Unter der Annahme, dass die Datenkommunikationsleitungen während eines kurzen Zeitraumes gestört sind oder dass die Kommunikation über einen anderen gegebenenfalls gestörten Datenkommunikationsweg erfolgt, kann dieses „beidseitig bekannte" Geheimnis zwischen den beiden Enden der Kommunikationsverbindung zur Verbesserung der Authentisierung der Transaktion verwendet werden. Der Zähler oder Zeitgeber wird in der Peripherievorrichtung durch die Übertragung eines Hash-Codierungswertes oder eines modifizierten Hash-Codierungswertes an das Hostverarbeitungssystem übertragen, wodurch aber nur die Inhalte des Zählers oder Zeitgebers der Peripherievorrichtung, siehe **718**, dargestellt werden. Das Hostverarbeitungssystem bedient sich des empfangenen Zähler- oder Zeitgeberwertes von der Peripherievorrichtung zum Empfangen und/oder Entschlüsseln der Signaturdaten, siehe **720**.

[0090] Ein weiteres Merkmal der Erfindung stellt ein Verfahren zum Bestätigen einer Signatur durch Vergleichen von Hash-codierten Werten anstelle der tatsächlichen Signaturdaten bereit. Zusätzliche Sicherheit kann durch Minimieren der Verwendung der ursprünglichen oder erfassten Signatur, der Bezugssignaturdaten und/oder beliebiger Echtzeitsignaturinformation erhalten werden.

[0091] Fig. 8 ist ein Flussdiagramm, das ein weiteres einem Ausführungsbeispiel der vorliegenden Erfindung entsprechendes Verfahren zum Aufrechterhalten der Sicherheit der Signaturinformation zwischen einer Peripherievorrichtung und einem Hostverarbeitungssystem darstellt. Man betrachte diejenige Situation, in der die erfasste Signatur beispielsweise eine PIN-Nummer ist. Die Hash-Codierung der PIN-Nummer wird in einer Datenbank gespeichert, auf die das Hostverarbeitungssystem zugreifen kann, anstatt dass die tatsächliche PIN-Nummer, siehe **802**, gespeichert würde. Die von der Peripherievorrichtung an das Hostverarbeitungssystem übertragenen Daten sind die Hash-Codierung der PIN-Nummer oder eine abgeleitete Hash-Codierung der PIN-Nummer, siehe **804**. Damit existiert die PIN-Nummer niemals als separate Aufzeichnung. In dem Hostverarbeitungssystem wird für den Fall, dass die Hash-Codierung der von der Peripherievorrichtung empfangenen PIN-Nummer zu der in der Datenbank, siehe **806**, gespeicherten Hash-Codierung der PIN-Nummer passt, die eingegebene PIN-Nummer als gültig betrachtet, siehe **808**. Bei diesem Verfahren hat niemand Zugriff auf die tatsächliche PIN-Nummer. Dies verhindert, dass jemand die PIN-Nummer entnehmen und an der Bedienerschnittstelle einer Peripherievorrichtung zu betrügerischen Zwecken verwenden kann.

[0092] Sind die Daten, die die Signatur darstellen, fest oder wiederholbar, wie dies bei einer PIN-Nummer der Fall ist, so ist der Vergleich der Hash-Codierungen vergleichsweise einfach. Stellt die Signatur jedoch biometrische Daten oder andere Daten dar, die jedesmal geringfügig variieren können (beispielsweise eine Handschrift), so können die biometrischen Daten mittels einer Analyse oder anderer Mittel zu wiederholbaren oder nahezu wiederholbaren Komponenten reduziert werden. Anschließend können diese wiederholbaren Elemente getrennt oder in einer Gruppe einer Hash-codierung zur Bildung einer wiederholbaren Hash-Codierung unterzogen werden, was den Vergleich ermöglicht. Sind kaum Schwankungen in den analysierten Elementen bezüglich der Signaturdaten zu finden, so kann ein Vergleich in dem Hostverarbeitungssystem einen Suchprozess implementieren, durch den analytische Elemente der Signatur, wenn kleine Schwankungen zulässig sind oder erwartet werden, geprüft werden können, und zwar durch den entsprechenden Hash-Codierungsalgorithmus in dem Prozessor, um zu bestimmen, ob ein geeigneter Treffer bezüglich der elektronischen Signatur der Aufzeichnung vorhanden ist.

[0093] Ein weiteres Merkmal der Erfindung betrifft ein Verfahren zur Prüfung von Übertragungsverlusten bei elektronischen Signaturdaten. Oftmals wird Information in mehrere Pakete oder Datensegmente zum Zwecke der Übertragung unterteilt. Aufgrund verschiedenartiger Kommunikationsprobleme kann es vorkommen, dass einige oder mehrere der übertragenen Pakete oder Segmente nicht empfangen werden. Bei einigen Anwendungen ist es nützlich, Kenntnis davon zu haben, dass sämtliche Dateien in Verknüpfung mit einer elektronischen Signatur gemäß Erfassung durch eine Peripherievorrichtung von dem Hostverarbeitungssystem empfangen worden sind. Um dies zu bewerkstelligen, kann die nachfolgende neuartige Technik verwendet werden, und zwar entweder unabhängig oder in Verbindung mit anderen Techniken der vorstehenden Offenbarung.

[0094] Fig. 9 ist ein Flussdiagramm, das ein einem Ausführungsbeispiel der vorliegenden Erfindung entsprechendes Verfahren darstellt, bei dem bestimmt wird, ob elektronische Signaturdaten, die von einer Peripherievorrichtung gesendet worden sind, vollständig von einem Hostverarbeitungssystem empfangen worden sind. Die Signaturerfassungs- und Übertragungsfunktion der Peripherievorrichtung wird ausgeschaltet, siehe **902**. Beliebige Daten, die in dem Datenübertragungsweg und/oder dem Hostverarbeitungssystem gepuffert sind, werden anschließend zurückgesetzt oder gelöscht, siehe **904**. Es er-

folgt ein Zurücksetzen eines Ereigniszählers in der Peripherievorrichtung und eines entsprechenden Ereigniszählers in dem Hostverarbeitungssystem, siehe **906**, der zum Zählen der von der Peripherievorrichtung über das Übertragungsmedium an das Hostverarbeitungssystem gesendeten Datenpakete oder Bytes verwendet wird.

[0095] Es erfolgen ein Einschalten der Signaturerfassungs- und Übertragungsfunktion der Peripherievorrichtung, siehe **908**, sodass eine Signatur erfasst und Signaturdaten (in verschlüsselter Form) übertragen werden können, siehe **910**. Werden die Signaturdaten übertragen, so erfolgt ein Beginnen des Zählens der Datenübertragungsereignisse in der Peripherievorrichtung, siehe **912**, und der entsprechenden Empfangsereignisse in dem Hostverarbeitungssystemen, siehe **914**.

[0096] Bei Beendigung der Signaturerfassung und Übertragung erfolgen ein Ausschalten der Datenerfassungs- und Übertragungsfunktion der Peripherievorrichtung, siehe **916**, und ein Senden des Ereigniszählerwertes des Peripheriezählers an das Hostverarbeitungssystem, siehe **918**, entweder als Hash-Codierungswert, in Klarform, verschlüsselt oder auf andere Weise codiert, darunter gegebenenfalls mittels einer Pseudozufallscodierung codiert. Es erfolgt ein Vergleichen der entsprechenden Zählerdatenwerte aus der Peripherievorrichtung und dem Hostverarbeitungssystem zur Sicherstellung, dass sämtliche Daten, die übertragen worden sind, von dem Host, siehe **920**, auch empfangen worden sind.

[0097] Einige Kommunikationsschemen übertragen Zeitstempel zusammen mit den Datenpaketen oder Segmenten zur Synchronisierung des Empfanges der übertragenen Daten in dem Empfangssystem. Gleichwohl kann hierdurch die Zeitinformation (beispielsweise der Zeitgeber des Übertragungssystems) offen liegen, was dazu führen kann, dass die Sicherheit der übertragenen Datenpakete oder Segmente beeinträchtigt ist.

[0098] Ein Ausführungsbeispiel der Erfindung stellt einen codierten Zertifizierungsstempel in einer Signaturperipherievorrichtung zur Sicherung der erfassten Signatur vor der Übertragung bereit. Fig. 10, Fig. 11 und Fig. 12 sind Blockdiagramme, die verschiedenen Ausführungsbeispielen der vorliegenden Erfindung entsprechende Codierungsverfahren darstellen, die zur Sicherung einer Signatur in einer Signaturperipherievorrichtung verwendet werden können.

[0099] Fig. 10 ist ein Blockdiagramm, das einen einem Ausführungsbeispiel der Erfindung entsprechenden Signaturdatenübertragungsstrom **1002** von einer Peripherievorrichtung an ein Hostverarbeitungssystem mit gesicherten Zeitstempeln **1004** darstellt. Zertifizierungszeitstempel **1004** werden codiert und können einfach nur die Daten aus der Zeitgeberschaltung **1006** darstellen, die mit einer absoluten, relativen oder inkrementellen Zeit versehen sind. Man beachte, dass die Zeitgeberschaltung **1006** wie auch die anderen Zeitgeber gemäß Fig. 11 bis Fig. 14 Zeitgeber darstellen können, die in einer signaturerfassenden Schnittstelle/Vorrichtung befindlich oder Teil einer Peripherievorrichtung sind. Damit können die hier beschriebenen Techniken zwischen der signaturerfassenden Schnittstelle/Vorrichtung und einer Peripherievorrichtung oder zwischen einer Peripherievorrichtung und einer weiteren Vorrichtung verwendet werden. Die Zeitstempel können mit der Übertragung jedes Datenpaketes vorgesehen werden, wobei die Daten nicht aus einer Signaturvorrichtung kommen, die die Rohsignaturdaten als regelmäßiges, perodisches oder zertifiziertes Zeitintervall abtastet. Die Zeitstempeldaten können jedoch zum Zwecke des Verifizierens der Verwendung eines regelmäßigen, periodischen oder zertifizierten Abtastintervalls innerhalb der Signaturerfassungsvorrichtung weniger häufig übertragen werden. In letzterem Fall erreicht das System eine größere Genauigkeit mit weniger Daten, da mit der Bestimmung die Kenntnis des genauen regelmäßigen, periodischen Abtastintervalls bei der Bestimmung des Signaturdatenabtastintervalls genauer ist, keinen Abtastungsquantisierungsfehler enthält und eine geringere Bandbreite sowie weniger Speicherraum benötigt, als dies bei Systemen der Fall ist, die die Signaturdaten zusammen mit individuellen Zeitstempelwerten in Verknüpfung mit jedem Datenpunkt oder Paket übertragen und speichern. Zur Bestimmung oder Zertifizierung des regelmäßigen Abtastintervalls, das von einer stift-/schreibflächenbasierten Signaturerfassungsschaltung verwendet wird, müssen Zeitstempel beispielsweise nur alle zehn (10) oder hundert (100) Punkte gesendet werden, und zwar zusammen mit der Anzahl der Datenpunkte zwischen den Zeitstempelübertragungen. Die Anzahl der Zeitstempelübertragungen, die zwischen den Zeitstempelwerten enthalten sind, kann einer Hash-Codierung unterworfen, codiert, verschlüsselt, pseudozufällig verwürfelt (scrambled) oder auf andere Weise vor einem nicht autorisierten Empfänger unter Verwendung der hier beschriebenen Techniken geheimgehalten werden, um den wahren Wert zu verbergen. Zusätzlich können die Zeitstempelwerte an natürlichen Grenzen des elektronischen Signaturerfassungssystems bereitgestellt werden. Für den Fall von Stift und Schreibfläche können beispielsweise die Zeitstempel zu Beginn und am Ende eines Signaturstriches gesendet werden. Bei Eingabe einer PIN-Nummer können die Zeitstempel beispielsweise am Anfang und bei Freigabe des PIN-Schlüssels gesendet werden. Durch Kombinieren der Kenntnisse hinsichtlich des beabsichtigten regelmäßigen, periodischen oder zertifizierten Zeitgeberintervalls der Signaturerfassungs- oder Umwandlungsschaltung ist das Hostverarbeitungssystem in der Lage, nach dem Decodieren der Information die

Anzahl der empfangenen Datenpunkte einfach durch das mitgeteilte Zeitintervall zu teilen, um die Signaturschaltungsabtastrate zu bestimmen. Die Zertifizierungsstempel **1004** können auch Information bereitstellen, die in der signaturerfassenden Peripherievorrichtung gespeichert ist, so beispielsweise eine Modellnummer und/oder eine Seriennummer. Durch Kenntnis der Korrelation zwischen der Modell- und Seriennummer der Peripherievorrichtung und der in der Peripherievorrichtung verwendeten zertifizierten Zeitgeberfrequenz kann das Hostverarbeitungssystem das Zeitintervall gemäß Bereitstellung durch die Zeitdaten mit Inhärenz in den Zertifizierungsstempeln **1004** für jedes Datenpaket **1002** mit Eigenschaften vergleichen, die für jedes Datenpaket **1002** auf Grundlage eines zertifizierten Zeitintervalls zu erwarten sind. Gleichwohl hat das einfache Senden von Zeit- und/oder Datumsinformation oder eines inkrementellen Zählerwertes mit jedem Datenpaket **1002** auch Nachteile, die hauptsächlich die Sicherheit betreffen. Wenn beispielsweise die – verschlüsselten oder unverschlüsselten – Signaturdaten von irgendjemand anderem als dem beabsichtigten Anwender abgefangen werden, so kann der nicht autorisierte Anwender die codierte Echtzeitinformation **1004** zum einfachen Bestimmen des präzisen Abstandes zwischen den Intervallen der Datenpakete **1002** verwenden und auf diese Weise eine sehr genaue falsche Signatur zur Verwendung bei Transaktionen rekonstruieren, die nicht zur Verwendung mit dieser Signatur autorisiert sind. Die Verwendung eines Echtzeitstempels, der mit jedem Datenpunkt gesendet wird, ermöglicht nicht nur ein Rekonstruieren der Daten in Echtzeit, sondern es sendet dieser Stempel auch inhärent Information über die Reihenfolge, in der die Abtastungen entlang des Signaturweges gehören.

[0100] Fig. 11 ist ein Blockdiagramm, das einen einem weiteren Ausführungsbeispiel der Erfindung entsprechenden Signaturdatenübertragungsstrom **1102** von einer Peripherievorrichtung an ein Hostverarbeitungssystem mit gesicherten Zeitstempeln **1104** darstellt. Bei diesem Ausführungsbeispiel der Erfindung kann der codierte Zertifizierungsstempel **1104**, der mit den Signaturkoordinatendaten gesendet wird, pseudozufällige Daten enthalten. Ein Pseudozufallszahlengenerator **1106** kann zur Bereitstellung der Zufallszahlen auf Grundlage des Zeitgeberwertes **1108** verwendet werden.

[0101] Fig. 12 ist ein Blockdiagramm, das einen einem weiteren Ausführungsbeispiel der vorliegenden Erfindung entsprechenden Signaturdatenübertragungsstrom von einer Peripherievorrichtung an ein Hostverarbeitungssystem zeigt, wobei die Zeitstempel **1104** zufällig in den Signaturdatenübertragungsstrom eingefügt werden. Es wird ein Pseudozufallszahlengenerator **1208** verwendet, der die verschlüsselte Zeitinformation **1204** entlang des Datenpaketstromes **1202** willkürlich einfügt. Ein Pseudozufallszahlengenerator **1208** kann sich des Zeitgeberwertes **1206** als Eingabe bedienen.

[0102] Anstelle des Bereitstellens der genauen linearen Zeitinformation über die Signaturdatenpakete auf eine erwartete, geordnete Weise kann die Zeitinformation auch auf eine nach außen hin zufällig erscheinende Weise bereitgestellt werden, und es kann die Abfolge der Datenpaketübertragungen verwürfelt (scrambled) wenden. Fig. 13 und Fig. 14 sind Blockdiagramme, die darstellen, wie das Datenpaketverwürfeln entsprechend verschiedenen Ausführungsbeispielen der Erfindung erfolgen kann.

[0103] Fig. 13 zeigt, wie Signaturdatenpakete von einer Peripherievorrichtung willkürlich derart übertragen werden, dass sogar für den Fall der Kenntnis der Codierungszeit die Signatur nicht rekonstruiert werden kann. Die Datenpakete **1302** werden in der Peripherievorrichtung gepuffert. Ein Pseudozufallszahlengenerator **1306** bedient sich des internen Zeitgebers **1310** zur Erzeugung von Zufallszahlen, die den Datenpaketauswähler **1304** veranlassen, aus den gepufferten Datenpaketen **1306** zufällig auszuwählen. Die Datenpakete **1302** werden dann ohne Reihenfolge mit einem codierten Zeitstempel **1308** zwischen den Datenpaketen übertragen.

[0104] Mit einer Software in dem Hostverarbeitungssystem mit Kenntnis des Pseudozufallscodes **1306**, der von der Peripherievorrichtung verwendet wird, kann ein Rekonstruieren der genauen Zeit und Abfolge der Datenpakete **1302** erfolgen. Diese Technik stellt eine große Herausforderung für einen Hacker dar, da eingedenk dessen, dass keine angreifbaren Daten in dem Datenstrom von der Peripherievorrichtung codiert sind und den Daten keine augenscheinliche Reihenfolge zu eigen ist, das Hostverarbeitungssystem, das Kenntnis von dem Pseudozufallszahlenerzeugungsalgorithmus hat, die Signaturdaten rekonstruieren und das Zeitintervall genau verifizieren kann.

[0105] Zur weiteren Verbesserung der in Fig. 13 dargestellten Technik zeigt Fig. 14, wie die Codierungszeit den Datenpaketen **1402** als Teil angehängt wird. Der Datenpaketauswähler **1404** bedient sich anschließend eines Pseudozufallszahlengenerators **1406**, der von einem Peripheriezeitgeber oder Zähler **1410** arbeitet, um die Datenpakete **1402** in einer zufälligen Abfolge zu übertragen.

[0106] Die anhand Fig. 10 bis Fig. 14 erläuterten codierten Zertifizierungsstempel können einfach die Modell- und Seriennummer der Peripherievorrichtung sein. Zu Sicherheitszwecken kann diese Stempelinformation eine Verschlüsselung oder eine Hash-Codierung der Modell- oder Seriennummer zusammen mit dem Echtzeitzeitgeber- oder Zählerwert, der

Hash-Codierung der Transaktionsaufzeichnung oder anderen derartigen Daten sein.

[0107] Alternativ kann die Software in dem Hostverarbeitungssystem bekannte Information über die Modell- und Seriennummer der Peripherievorrichtung, so beispielsweise den Namen der Firma oder des Eigentümers der Peripherievorrichtung, der in einer Datenbank abgelegt ist, vergleichen.

[0108] Bei verschiedenen anderen Ausführungsbeispielen der Erfindung können die anhand Fig. 10 bis Fig. 14 erläuterten Techniken zusammen eingesetzt werden. Darüber hinaus können diese Techniken zusammen mit den vorstehend offenbarten Sicherungstechniken verwendet werden. Das allgemeine System kann auch zum Übertragen und Empfangen der Zertifizierung von Daten anderer Typen von elektronischen Signatureingabevorrichtungen verwendet werden. Bei all diesen Systemen sind die Zeit und die geordnete Abfolge der Daten für die genaue Rekonstruktion wichtig. So kann die Zeit einer PIN-Dateneingabe beispielsweise als biometrisches Maß gestempelt werden. Die Abtastrate und Reihenfolge von Sprachdaten und dergleichen mehr ist mit Blick auf eine genaue Rekonstruktion der Authentisierung wichtig.

[0109] Obwohl bestimmte Ausführungsbeispiele in der begleitenden Zeichnung beschrieben und gezeigt worden sind, ist einsichtig, dass diese Ausführungsbeispiele bezüglich der Erfindung im Allgemeinen rein illustrativ und nicht restriktiv sind und dass die Erfindung nicht auf die spezifischen Ausgestaltungen und Anordnungen gemäß Darstellung und Beschreibung beschränkt ist, da verschiedene andere Modifikationen möglich sind. Einem Fachmann auf dem einschlägigen Gebiet erschließt sich, dass verschiedene Anpassungen und Abwandlungen an dem beschriebenen bevorzugten Ausführungsbeispiel vorgenommen werden können, ohne den Schutzbereich der Erfindung zu verlassen. Es sollte einsichtig sein, dass innerhalb des Schutzumfanges der beigefügten Ansprüche die Erfindung auch anders als vorstehend beschrieben verwirklicht wenden kann.

Patentansprüche

1. Verfahren, umfassend die Schritte:
(a) Empfangen von Transaktionsdaten in einer ersten Vorrichtung;
(b) Erfassen einer Signatur in der ersten Vorrichtung;
(c) Verschlüsseln der erfassten Signatur mit den Transaktionsdaten in der ersten Vorrichtung; und
(d) Übertragen der Transaktionsdaten und der verschlüsselten Signatur von der ersten Vorrichtung an eine zweite Vorrichtung,
wobei die Signatur als getrennte Abtastpunkte verschlüsselt wird und wobei jeder Abtastpunkt mit einem anderen Verschlüsselungsschlüssel verschlüsselt wird.

2. Verfahren nach Anspruch 1, bei dem der Schritt (c) das Verwenden eines Hashs der Transaktionsdaten zur Verschlüsselung der erfassten Signatur beinhaltet.

3. Verfahren nach Anspruch 1, bei dem die Transaktionsdaten eine Preisinformation für eine Transaktion bzw. Geschäft beinhalten.

4. Verfahren nach Anspruch 1, bei dem die Transaktionsdaten eine Identifikation von Waren beinhalten, die von der Transaktion betroffen sind bzw. für die eine Transaktion abgewickelt wurde.

5. Verfahren nach Anspruch 1, das des Weiteren den nachfolgenden zusätzlichen Schritt umfasst:
Empfangen eines Hashs der Transaktionsdaten in der ersten Vorrichtung.

6. Verfahren nach Anspruch 1, das des Weiteren den nachfolgenden zusätzlichen Schritt umfasst:
Erzeugen eines Hashs der Transaktionsdaten in der ersten Vorrichtung.

7. Verfahren nach Anspruch 6, das des Weiteren die nachfolgenden zusätzlichen Schritte umfasst:
(a) Erzeugen eines lokalen Hashs der Transaktionsdaten in der zweiten Vorrichtung unter Verwendung desselben Algorithmus, der zur Erzeugung des Hashs in der ersten Vorrichtung verwendet wird;
(b) Decodieren der verschlüsselten erfassten Signatur in der zweiten Vorrichtung unter Verwendung des lokalen Hashs der Transaktionsdaten; und
(c) Vergleichen der erfassten Signatur mit einer gespeicherten Signatur zur Verifizierung.

8. Verfahren nach Anspruch 1, bei dem der Schritt des Verschlüsselns der erfassten Signatur unter Verwendung der Transaktionsdaten in der ersten Vorrichtung beinhaltet:
(a) Kombinieren der Transaktionsdaten mit einem geheimen Schlüssel bzw. einem Geheimschlüssel, der in der ersten Vorrichtung erzeugt wird;
(b) Erzeugen eines Hashs der Kombination aus den Transaktionsdaten und dem Geheimschlüssel zur Erstellung eines abgeleiteten Aufzeichnungs- bzw. Dokumentationsschlüssels in der ersten Vorrichtung; und
(c) Verschlüsseln der erfassten Signatur unter Verwendung des abgeleiteten Aufzeichnungsschlüssels als Eingabe bzw. Eingang für einen Verschlüsselungsalgorithmus in der ersten Vorrichtung.

9. Verfahren nach Anspruch 8, das des Weiteren den nachfolgenden zusätzlichen Schritt umfasst:

Senden des Geheimschlüssels zwischen der ersten Vorrichtung an die zweite Vorrichtung in unregelmäßigen Intervallen.

10. Verfahren nach Anspruch 9, das des Weiteren die nachfolgenden zusätzlichen Schritte umfasst:
(a) Erzeugen eines Hashs der kombinierten Transaktionsdaten und des geheimen Schlüssels bzw. des Geheimschlüssels zur Erstellung eines abgeleiteten Aufzeichnungs- bzw. Dokumentationsschlüssels in der zweiten Vorrichtung; und
(b) Decodieren der verschlüsselten erfassten Signatur in der zweiten Vorrichtung unter Verwendung des abgeleiteten Aufzeichnungsschlüssels.

11. Verfahren nach Anspruch 10, bei dem für den Fall eines Fehlschlages beim Decodieren der verschlüsselten erfassten Signatur in der zweiten Vorrichtung ein Suchen nach dem richtigen abgeleiteten Aufzeichnungsschlüssel durch Modifizieren des Geheimschlüssels erfolgt.

12. Verfahren nach Anspruch 1, bei dem die verschlüsselte Signatur von der ersten Vorrichtung an die zweite Vorrichtung in einer Vielzahl bzw. Mehrzahl von Datenfragmenten übertragen wird und diese Mehrzahl von Datenfragmenten in einer pseudozufälligen Reihenfolge gesendet wird.

13. Verfahren nach Anspruch 1, bei dem der Schritt (d) die nachfolgenden zusätzlichen Schritte umfasst:
(a) Unterteilen der Signaturdaten in eine Mehrzahl von Fragmenten;
(b) getrenntes Verschlüsseln von jedem aus der Mehrzahl von Fragmenten mit den Transaktionsdaten;
(c) Übertragen der Mehrzahl von Fragmenten von der ersten Vorrichtung an die zweite Vorrichtung;
(d) Erstellen bzw. Erhalten bzw. Behalten eines ersten Zählwertes der Mehrzahl von Fragmenten, die von der ersten Vorrichtung übertragen werden;
(e) Übertragen des ersten Zählwertes an die zweite Vorrichtung.

14. Verfahren nach Anspruch 13, bei dem der Schritt (d) des Anspruchs 1 die nachfolgenden zusätzlichen Schritte umfaßt:
(f) Erstellen bzw. Erhalten bzw. Behalten eines zweiten Zählwertes der Mehrzahl von Fragmenten, die von der zweiten Vorrichtung empfangen werden; und
(g) Vergleichen des ersten Zählwertes mit dem zweiten Zählwert zur Bestimmung, ob sämtliche Signaturfragmente empfangen worden sind.

15. Verfahren nach Anspruch 1, das die nachfolgenden zusätzlichen Schritte umfasst:
(a) Erzeugen eines ersten abgeleiteten Aufzeichnungsschlüssels durch Nehmen eines Hashs der Kombination eines ersten Zeitgeber- bzw. Taktgeberwertes mit den Transaktionsdaten, wobei der erste Zeitgeberwert in der ersten Vorrichtung zu finden ist;
(b) Verwenden des ersten abgeleiteten Aufzeichnungsschlüssels zur Verschlüsselung der erfassten Signatur in der ersten Vorrichtung;
(c) Erzeugen eines zweiten abgeleiteten Aufzeichnungsschlüssels durch Nehmen eines Hashs der Kombination eines zweiten Zeitgeber- bzw. Taktgeberwertes, eines Offset- bzw. Verschränkungs- bzw. Abstandswertes und der Transaktionsdaten in der zweiten Vorrichtung, wobei der zweite Zeitgeberwert in der zweiten Vorrichtung zu finden ist; und
(d) Entschlüsseln der verschlüsselten Signatur mit dem zweiten abgeleiteten Aufzeichnungsschlüssel in der zweiten Vorrichtung.

16. Verfahren nach Anspruch 1, bei dem die Signatur als getrennte Abtast- bzw. Auswahlpunkte erfasst wird.

17. Verfahren nach Anspruch 16, bei dem die Abtastpunkte von wenigstens der Lage-, Druck- oder Zeitinformation der Signatur abhängen bzw. darauf basieren.

18. Verfahren nach Anspruch 1, bei dem die Signatur als getrennte verschlüsselte Abtastpunkte gespeichert wird.

19. Verfahren nach Anspruch 1, bei dem die Signatur als getrennte verschlüsselte Abtastpunkte übertragen wird.

20. Verfahren nach Anspruch 19, bei dem die verschlüsselten Abtastpunkte getrennt zur Rekonstruktion der Signatur in Echtzeit entschlüsselt werden.

21. Signaturerfassungsvorrichtung, die als eine erste Vorrichtung konfiguriert ist, ein Verfahren gemäß einem der vorigen Ansprüche auszuführen.

22. Ein System, umfassend:
eine Signaturerfassungsvorrichtung, die eine Information einer Signaturerfassungvorrichtung aufweist, wobei die Signaturerfassungsvorrichtung konfiguriert ist, die folgenden Schritte auszuführen:
(a) Erfassen von Signaturdaten basierend auf einer eingegebenen elektronischen Signatur;
(b) Generieren eines ersten Verschlüsselungsschlüssels von einem Hash der Information der Signaturerfassungsvorrichtung;
(c) Unterteilen der Signaturdaten in eine Mehrzahl von Datenfragmenten;
(d) getrenntes Verschlüsseln von jedem der Mehrzahl von Fragmenten der Signaturdaten mit dem ersten Verschlüsselungsschlüssel; und
(e) Übertragen der Informationen der Signaturerfassungsvorrichtung und der Mehrzahl von verschlüsselten Fragmenten der Signaturdaten; und

eine Hostverarbeitungsvorrichtung, die kommunikativ mit der Signaturerfassungsvorrichtung gekoppelt ist, wobei die Hostverarbeitungsvorrichtung konfiguriert ist, die folgenden Schritte auszuführen:
(a) Empfangen der Informationen der Signaturerfassungsvorrichtung und der Mehrzahl von verschlüsselten Fragmenten der Signaturdaten;
(b) Generieren eines zweiten Verschlüsselungsschlüssels durch Hashcodieren der empfangenen Informationen der Signaturerfassungsvorrichtung;
(c) Entschlüsseln der Mehrzahl von verschlüsselten Fragmenten der Signaturdaten unter Benutzung des zweiten Verschlüsselungsschlüssels; und
(d) Rekonstruieren der elektronischen Signatur basierend auf der Mehrzahl von empfangenen und entschlüsselten Fragmenten der Signaturdaten,
wobei der zweite Verschlüsselungsschlüssel gleich dem ersten Verschlüsselungsschlüssel ist.

23. Das System nach Anspruch 22, wobei die Informationen der Signaturerfassungsvorrichtung aus der Gruppe bestehend aus einer Seriennummer und einer Modellnummer ausgewählt ist.

24. Transaktionssystem, umfassend:
eine Signaturerfassungsvorrichtung, die ausgelegt ist zum:
– Erfassen einer elektronischen Signatur,
– Erzeugen einer Hash-Codierung einer Transaktionsaufzeichnung,
– Verschlüsseln der elektronischen Signatur mit der Hash-Codierung der Transaktionsaufzeichnung,
– Übertragen der verschlüsselten elektronischen Signatur; und
eine Hostverarbeitungsvorrichtung, die kommunikativ mit der Signaturerfassungsvorrichtung gekoppelt ist,
wobei die Hostverarbeitungsvorrichtung ausgelegt ist zum:
– Empfangen der verschlüsselten elektronischen Signatur,
– Entschlüsseln der elektronischen Signatur,
– Vergleichen der elektronischen Signatur mit einer Bezugssignatur und
– Annehmen einer Transaktion entsprechend der elektronischen Transaktionsaufzeichnung, wenn die empfangene elektronische Signatur zu der Bezugssignatur passt, wobei die Signaturerfassungsvorrichtung
darüber hinaus zum Initiieren der Transaktionsaufzeichnung und Übertragen der Transaktionsaufzeichnung an die Hostverarbeitungsvorrichtung ausgelegt ist, und die Hostverarbeitungsvorrichtung zudem zum Empfangen einer Hash-Codierung der Transaktionsaufzeichnung zur Verwendung bei der Entschlüsselung der elektronischen Signatur ausgelegt ist.

25. Transaktionssystem nach Anspruch 24, wobei die Signaturerfassungsvorrichtung des Weiteren ausgelegt zum:
– Übertragen der verschlüsselten elektronischen Signatur als Mehrzahl von Datenpaketen,
– Vorhalten eines Zählwertes der Anzahl von Datenpaketen der Übertragung für eine bestimmte Signatur,
– sicheren Übertragen des Zählwertes der Datenpakete an die Hostverarbeitungsvorrichtung, und
die Hostverarbeitungsvorrichtung des Weiteren ausgelegt ist zum Vergleichen des Zählwertes der Datenpakete, die von der Signaturerfassungsvorrichtung übertragen werden, mit der Anzahl der Datenpakete, die in Verbindung mit der bestimmten Signatur empfangen werden, um zu bestimmen, ob die Signatur vollständig empfangen worden ist.

26. Transaktionssystem nach einem der Ansprüche 24 oder 25, wobei die Signaturerfassungsvorrichtung des Weiteren ausgelegt ist zum
– Anordnen der verschlüsselten elektronischen Signatur als Mehrzahl von Datenpaketen,
– Übertragen der Mehrzahl von Datenpaketen in einer pseudozufälligen Reihenfolge, wobei
die Hostverarbeitungsvorrichtung des Weiteren ausgelegt ist zum:
– Empfangen der Mehrzahl von Datenpaketen in einer pseudozufälligen Reihenfolge und
– Rekonstruieren der ursprünglichen Reihenfolge der Mehrzahl von Datenpaketen.

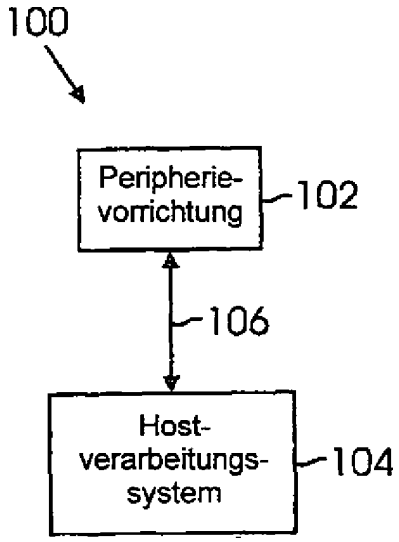
27. Authentisierungs- bzw. Authentifikationsvorrichtung, umfassend:
– eine Signaturerfassungsvorrichtung, die dafür ausgelegt ist, eine Signaturinformation zu erfassen; und
– eine Steuerung, die kommunikativ mit der Signaturerfassungsvorrichtung gekoppelt ist, wobei die Steuerung ausgelegt ist zum:
– Empfangen von Transaktionsdaten,
– Erzeugen einer Hash-Codierung der Transaktionsdaten,
– Verschlüsseln der erfassten Signaturinformation mit der Hash-Codierung der Transaktionsdaten und
– Übertragen der verschlüsselten Signaturinformation, wobei die Authentisierungsvorrichtung darüber hinaus die nachfolgenden Aufgaben wahrnimmt:
– Kombinieren der Transaktionsaufzeichnung mit einem Geheimschlüssel,
– Erzeugen einer Hash-Codierung der Kombination aus den Transaktionsdaten und dem Geheimschlüssel zur Erstellung eines abgeleiteten Aufzeichnungsschlüssels,
– Verschlüsseln der erfassten Signatur mit dem abgeleiteten Aufzeichnungsschlüssel als Eingabe für einen Verschlüsselungsalgorithmus,
– Unterteilen der erfassten Signaturinformation in eine Mehrzahl von Paketen,
– getrenntes Verschlüsseln von jedem aus der Mehrzahl von Paketen mit den Transaktionsdaten, wobei
das Übertragen der verschlüsselten Signaturinformation das Übertragen der Mehrzahl von Paketen ohne

bestimmte Abfolge in einer pseudozufälligen Reihenfolge beinhaltet.

28. Authentisierungs- bzw. Authentifikationsvorrichtung nach Anspruch 27, wobei die Authentisierungsvorrichtung darüber hinaus umfasst:
– eine Ausgabevorrichtung zur Vorlage der Transaktionsdaten bei einem Anwender; und
– eine Eingabevorrichtung, die einem Anwender die Modifizierung der Transaktionsdaten ermöglicht.

Es folgen 12 Blatt Zeichnungen

Anhängende Zeichnungen



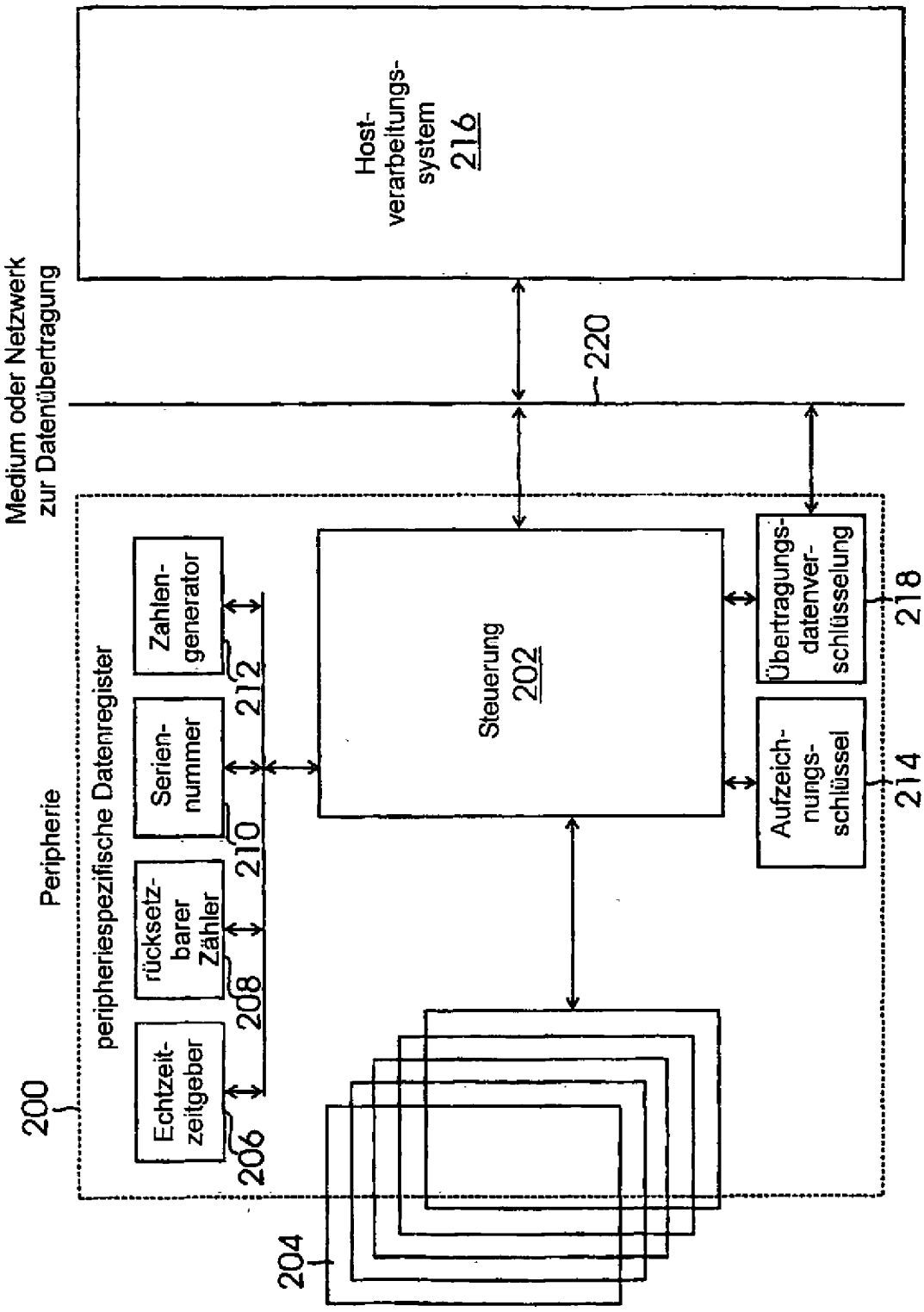

Host-verarbeitungs-system 216
220
Medium oder Netzwerk zur Datenübertragung
Peripherie
peripheriespezifische Datenregister
Zahlen-generator
Seriennummer
rücksetzbarer Zähler
Echtzeitzeitgeber
212
210
208
206
200
Steuerung 202
Übertragungsdatenverschlüsselung
Aufzeichnungsschlüssel
218
214
204

Fig. 2

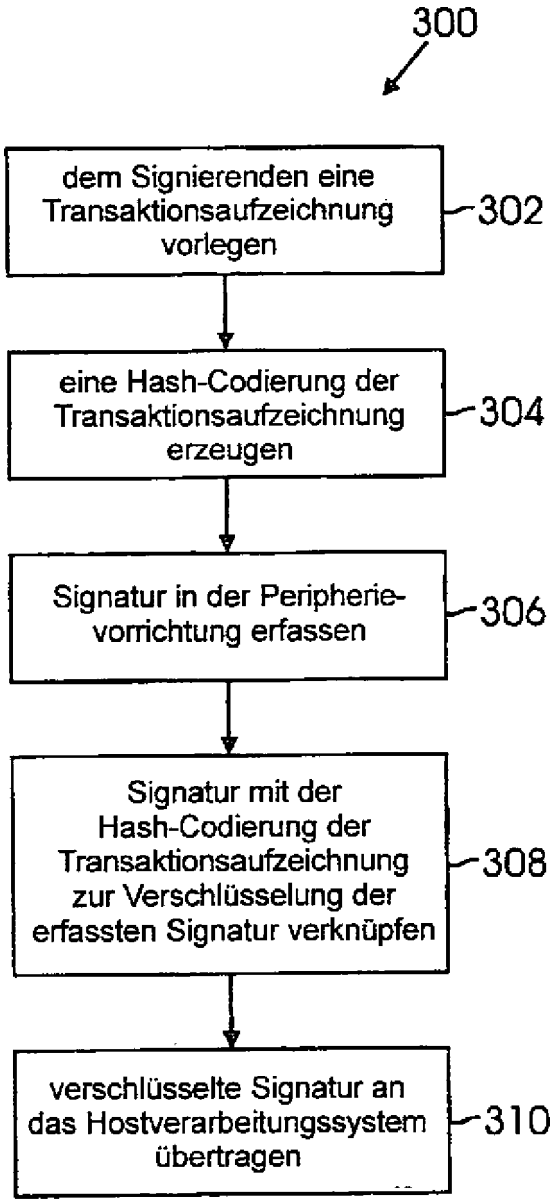

300
dem Signierenden eine Transaktionsaufzeichnung vorlegen
302
eine Hash-Codierung der Transaktionsaufzeichnung erzeugen
304
Signatur in der Peripherie-vorrichtung erfassen
306
Signatur mit der Hash-Codierung der Transaktionsaufzeichnung zur Verschlüsselung der erfassten Signatur verknüpfen
308
verschlüsselte Signatur an das Hostverarbeitungssystem übertragen
310

Fig. 3

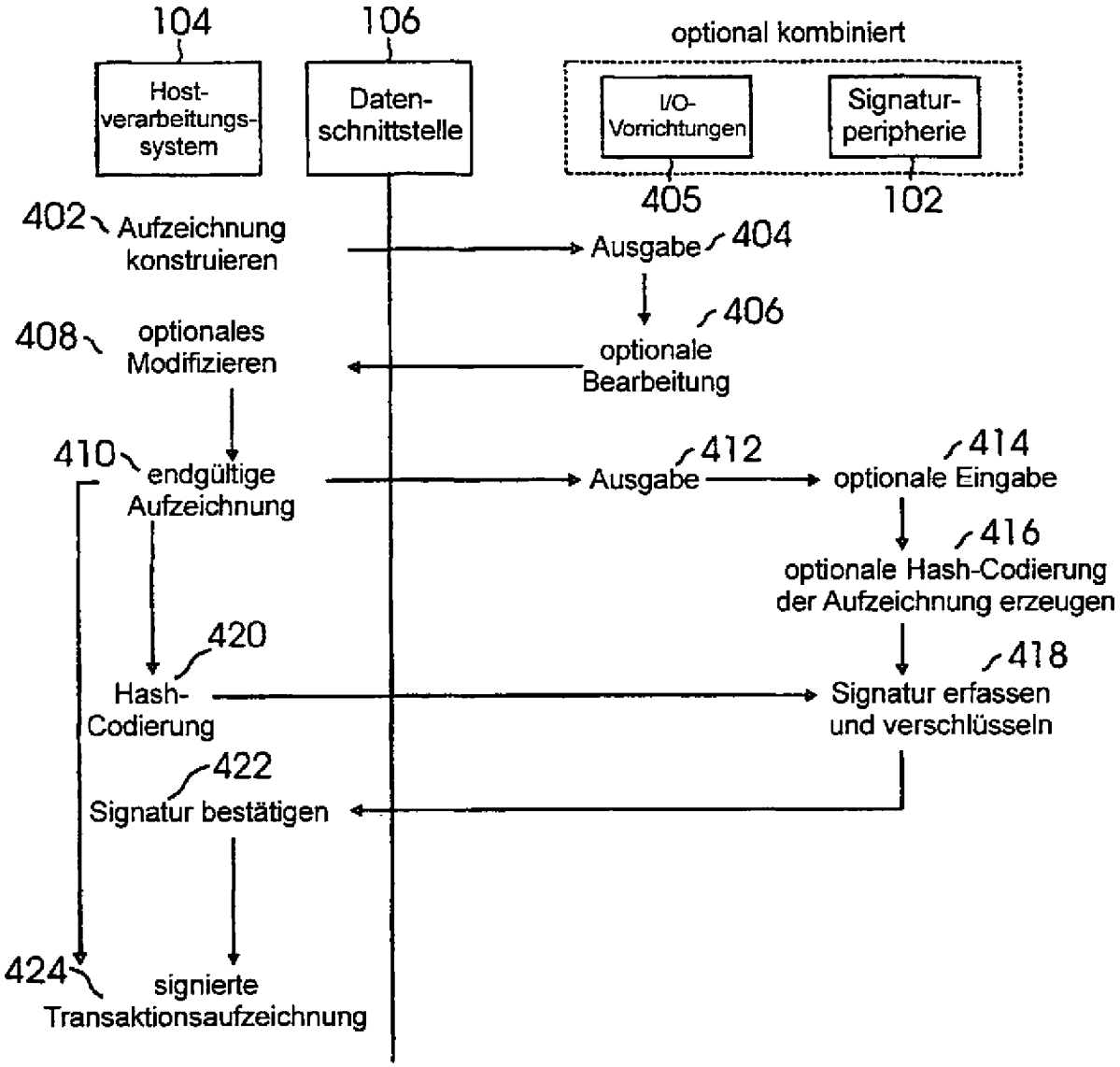

104
106
optional kombiniert
Host-verarbeitungs-system
Daten-schnittstelle
I/O-Vorrichtungen
Signatur-peripherie
405
102
402
Aufzeichnung konstruieren
Ausgabe
404
406
408
optionales Modifizieren
optionale Bearbeitung
410
endgültige Aufzeichnung
412
Ausgabe
414
optionale Eingabe
416
optionale Hash-Codierung der Aufzeichnung erzeugen
420
418
Hash-Codierung
Signatur erfassen und verschlüsseln
422
Signatur bestätigen
424
signierte Transaktionsaufzeichnung

Fig. 4

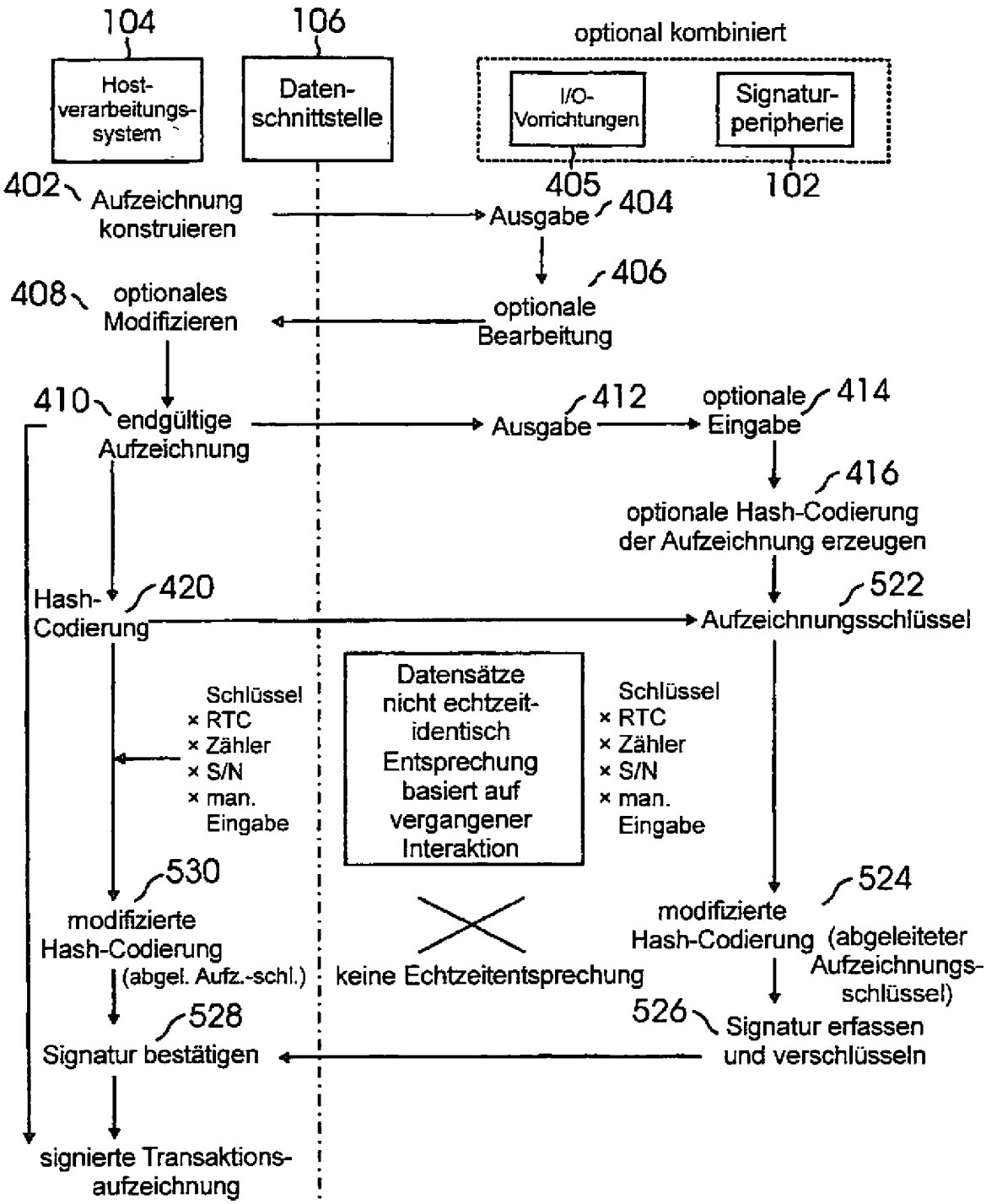

104
106
optional kombiniert
Host-verarbeitungs-system
Daten-schnittstelle
I/O-Vorrichtungen
Signatur-peripherie
405
102
402
Aufzeichnung konstruieren
Ausgabe
404
406
408
optionales Modifizieren
optionale Bearbeitung
410
endgültige Aufzeichnung
412
Ausgabe
optionale Eingabe
414
416
optionale Hash-Codierung der Aufzeichnung erzeugen
Hash-Codierung
420
522
Aufzeichnungsschlüssel
Schlüssel
× RTC
× Zähler
× S/N
× man. Eingabe
Datensätze nicht echtzeit-identisch Entsprechung basiert auf vergangener Interaktion
Schlüssel
× RTC
× Zähler
× S/N
× man. Eingabe
530
modifizierte Hash-Codierung (abgel. Aufz.-schl.)
keine Echtzeitentsprechung
524
modifizierte Hash-Codierung (abgeleiteter Aufzeichnungs-schlüssel)
528
Signatur bestätigen
526
Signatur erfassen und verschlüsseln
signierte Transaktions-aufzeichnung

Fig. 5

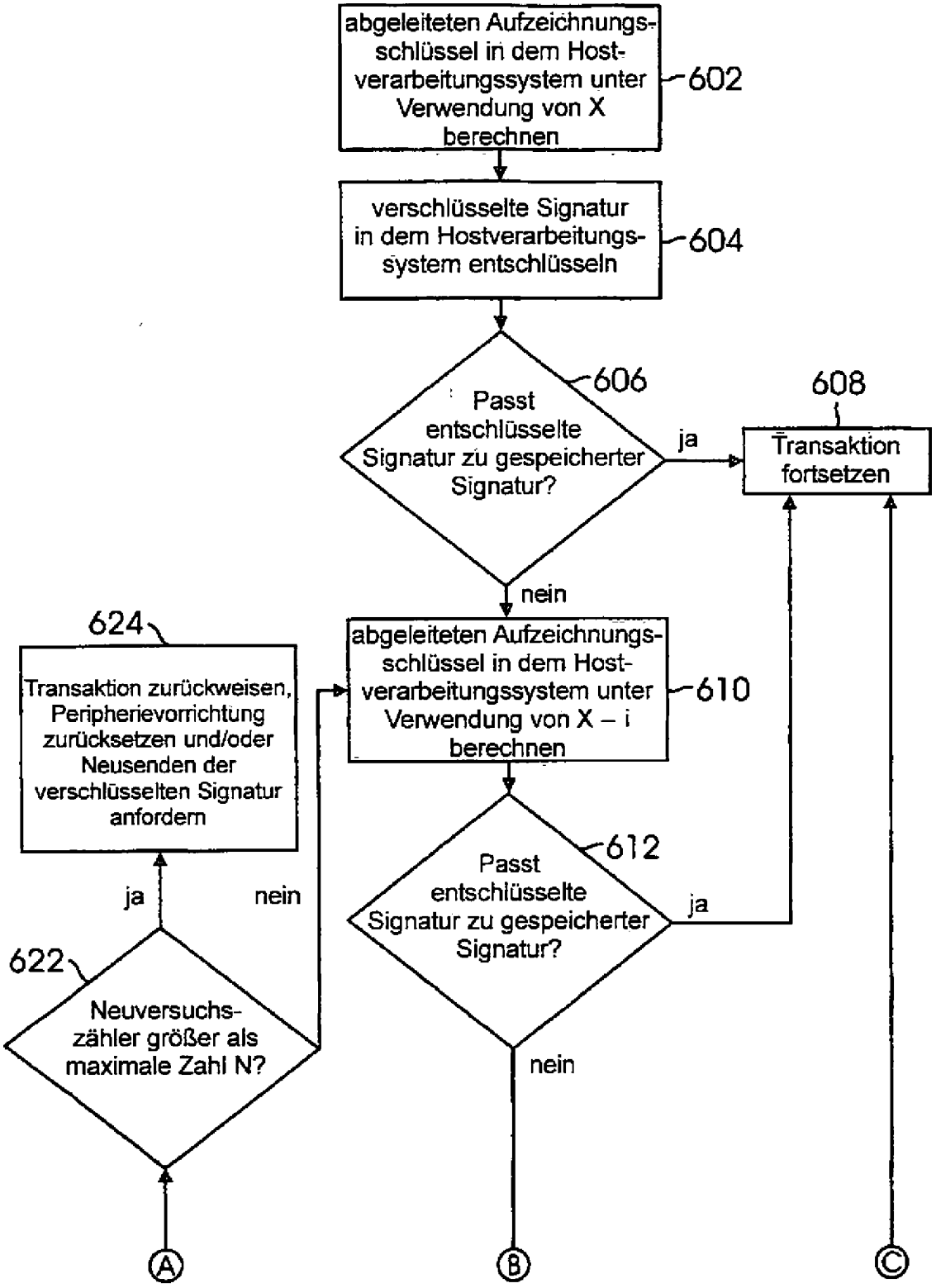

abgeleiteten Aufzeichnungsschlüssel in dem Hostverarbeitungssystem unter Verwendung von X berechnen
602
verschlüsselte Signatur in dem Hostverarbeitungssystem entschlüsseln
604
Passt entschlüsselte Signatur zu gespeicherter Signatur?
606
ja
608
Transaktion fortsetzen
nein
abgeleiteten Aufzeichnungsschlüssel in dem Hostverarbeitungssystem unter Verwendung von X – i berechnen
610
Passt entschlüsselte Signatur zu gespeicherter Signatur?
612
ja
nein
Neuversuchszähler größer als maximale Zahl N?
622
ja
nein
Transaktion zurückweisen, Peripherievorrichtung zurücksetzen und/oder Neusenden der verschlüsselten Signatur anfordern
624
A
B
C

Fig. 6A

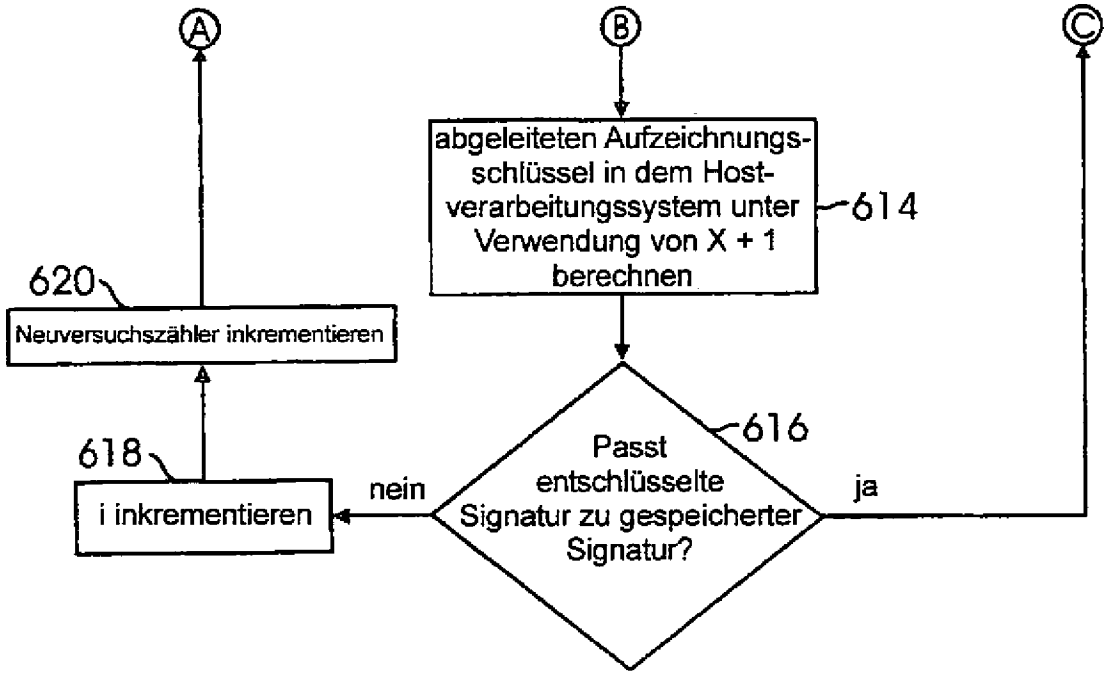


Fig. 6

Fig. 6B

6A
6B

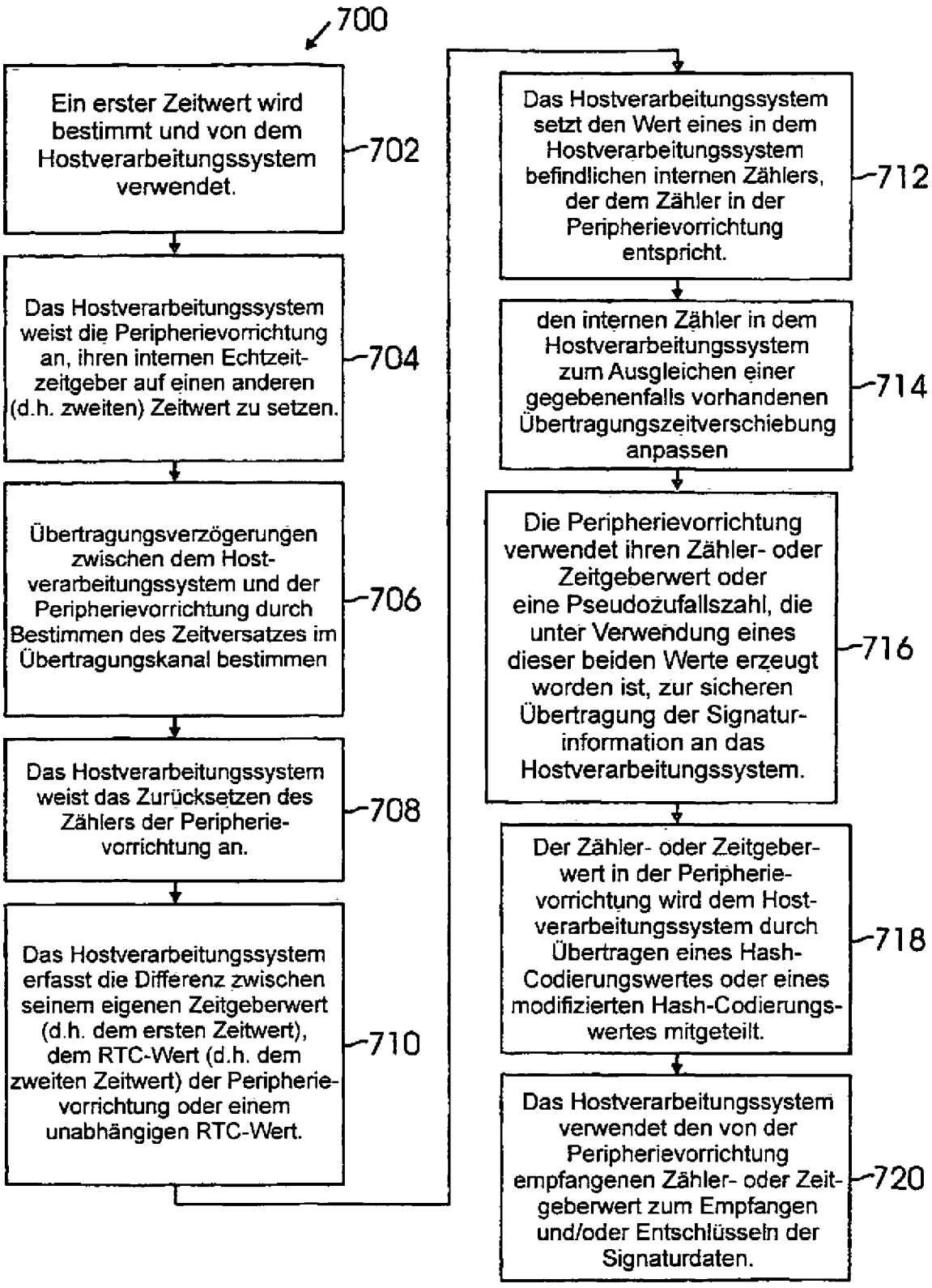

700
Ein erster Zeitwert wird bestimmt und von dem Hostverarbeitungssystem verwendet.
702
Das Hostverarbeitungssystem weist die Peripherievorrichtung an, ihren internen Echtzeitzeitgeber auf einen anderen (d.h. zweiten) Zeitwert zu setzen.
704
Übertragungsverzögerungen zwischen dem Hostverarbeitungssystem und der Peripherievorrichtung durch Bestimmen des Zeitversatzes im Übertragungskanal bestimmen
706
Das Hostverarbeitungssystem weist das Zurücksetzen des Zählers der Peripherievorrichtung an.
708
Das Hostverarbeitungssystem erfasst die Differenz zwischen seinem eigenen Zeitgeberwert (d.h. dem ersten Zeitwert), dem RTC-Wert (d.h. dem zweiten Zeitwert) der Peripherievorrichtung oder einem unabhängigen RTC-Wert.
710
Das Hostverarbeitungssystem setzt den Wert eines in dem Hostverarbeitungssystem befindlichen internen Zählers, der dem Zähler in der Peripherievorrichtung entspricht.
712
den internen Zähler in dem Hostverarbeitungssystem zum Ausgleichen einer gegebenenfalls vorhandenen Übertragungszeitverschiebung anpassen
714
Die Peripherievorrichtung verwendet ihren Zähler- oder Zeitgeberwert oder eine Pseudozufallszahl, die unter Verwendung eines dieser beiden Werte erzeugt worden ist, zur sicheren Übertragung der Signaturinformation an das Hostverarbeitungssystem.
716
Der Zähler- oder Zeitgeberwert in der Peripherievorrichtung wird dem Hostverarbeitungssystem durch Übertragen eines Hash-Codierungswertes oder eines modifizierten Hash-Codierungswertes mitgeteilt.
718
Das Hostverarbeitungssystem verwendet den von der Peripherievorrichtung empfangenen Zähler- oder Zeitgeberwert zum Empfangen und/oder Entschlüsseln der Signaturdaten.
720

Fig. 7

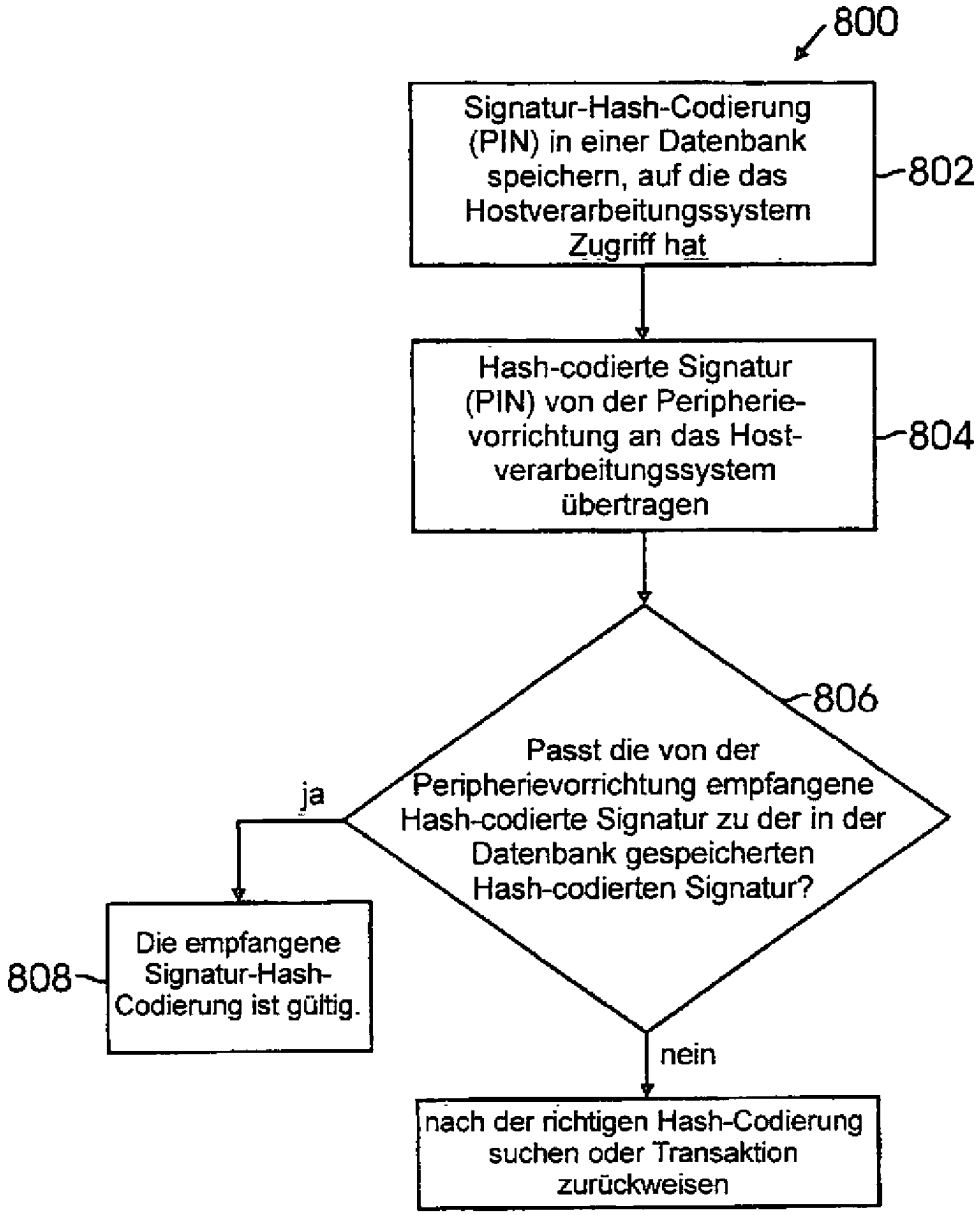

800
Signatur-Hash-Codierung (PIN) in einer Datenbank speichern, auf die das Hostverarbeitungssystem Zugriff hat
802
Hash-codierte Signatur (PIN) von der Peripherie-vorrichtung an das Host-verarbeitungssystem übertragen
804
806
Passt die von der Peripherievorrichtung empfangene Hash-codierte Signatur zu der in der Datenbank gespeicherten Hash-codierten Signatur?
ja
808
Die empfangene Signatur-Hash-Codierung ist gültig.
nein
nach der richtigen Hash-Codierung suchen oder Transaktion zurückweisen

Fig. 8

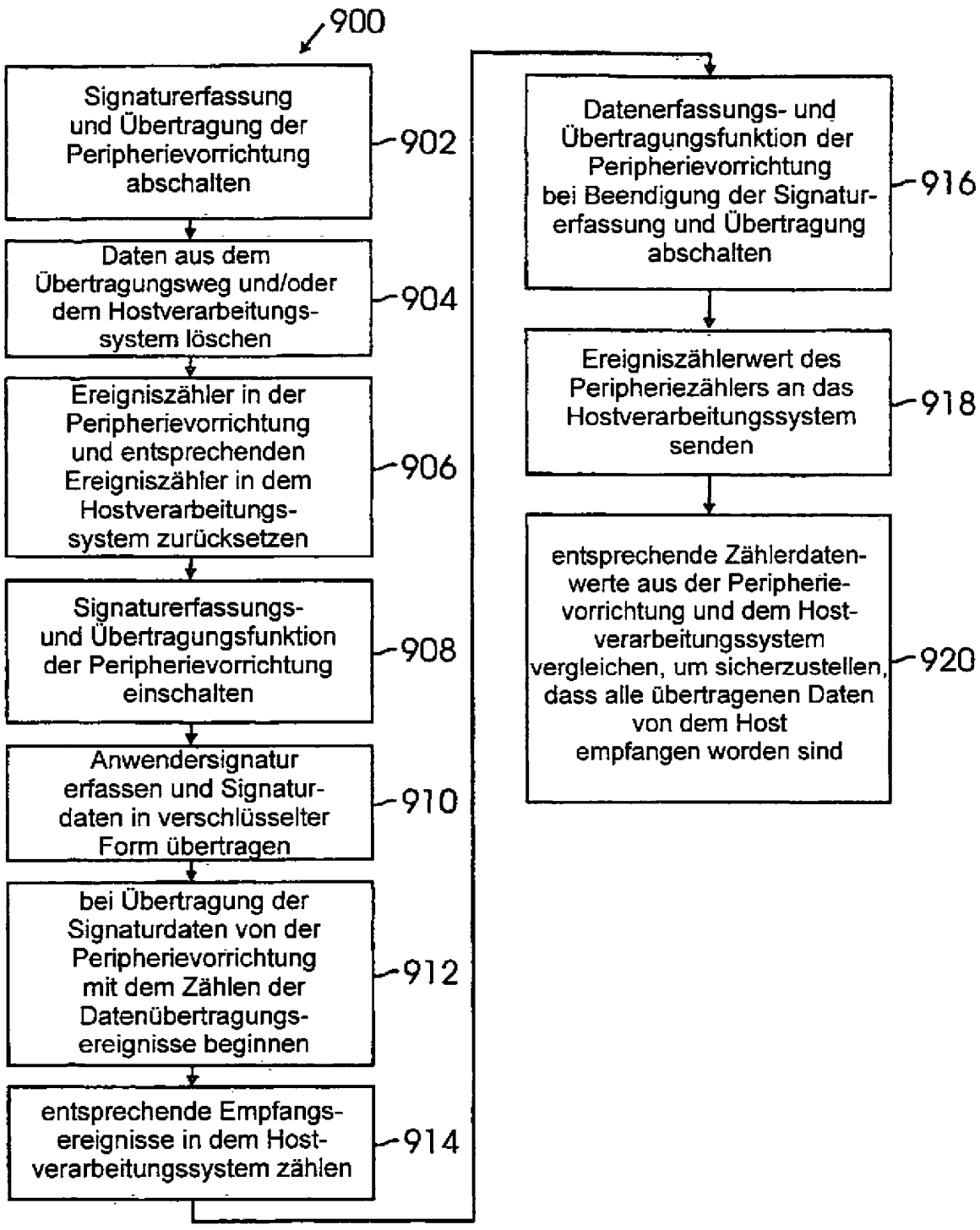

900
Signaturerfassung und Übertragung der Peripherievorrichtung abschalten
902
Daten aus dem Übertragungsweg und/oder dem Hostverarbeitungs-system löschen
904
Ereigniszähler in der Peripherievorrichtung und entsprechenden Ereigniszähler in dem Hostverarbeitungs-system zurücksetzen
906
Signaturerfassungs- und Übertragungsfunktion der Peripherievorrichtung einschalten
908
Anwendersignatur erfassen und Signatur-daten in verschlüsselter Form übertragen
910
bei Übertragung der Signaturdaten von der Peripherievorrichtung mit dem Zählen der Datenübertragungs-ereignisse beginnen
912
entsprechende Empfangs-ereignisse in dem Host-verarbeitungssystem zählen
914
Datenerfassungs- und Übertragungsfunktion der Peripherievorrichtung bei Beendigung der Signatur-erfassung und Übertragung abschalten
916
Ereigniszählerwert des Peripheriezählers an das Hostverarbeitungssystem senden
918
entsprechende Zählerdaten-werte aus der Peripherie-vorrichtung und dem Host-verarbeitungssystem vergleichen, um sicherzustellen, dass alle übertragenen Daten von dem Host empfangen worden sind
920

Fig. 9

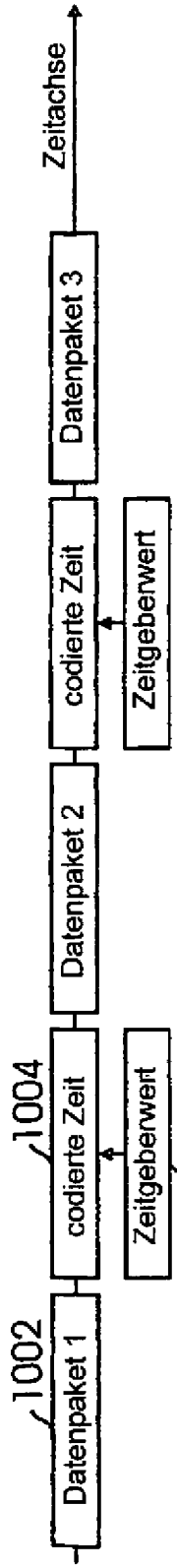


Fig. 10

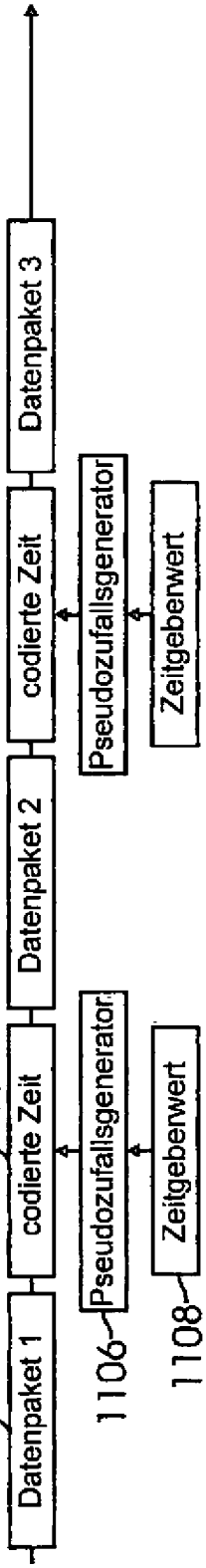


Fig. 11

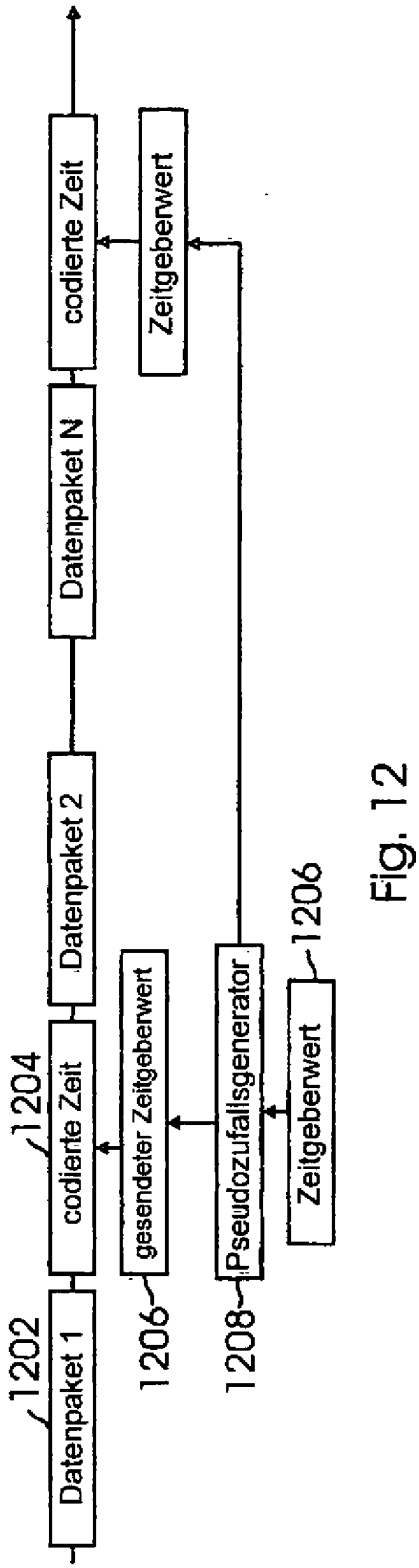


Fig. 12

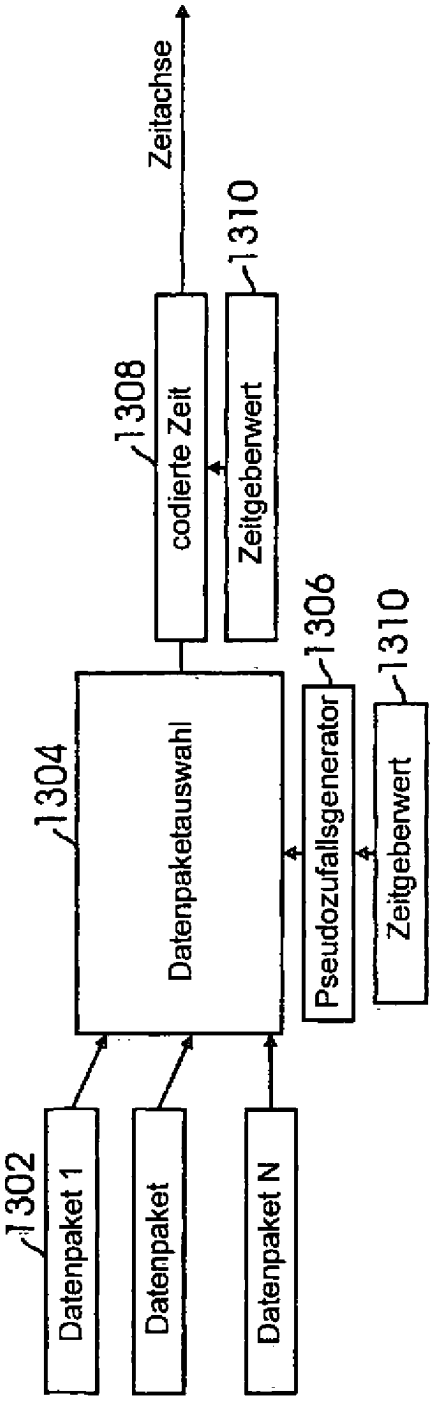

Zeitachse
1308
codierte Zeit
1310
Zeitgeberwert
1304
Datenpaketauswahl
1306
Pseudozufallsgenerator
1310
Zeitgeberwert
1302
Datenpaket 1
Datenpaket
Datenpaket N

Fig. 13

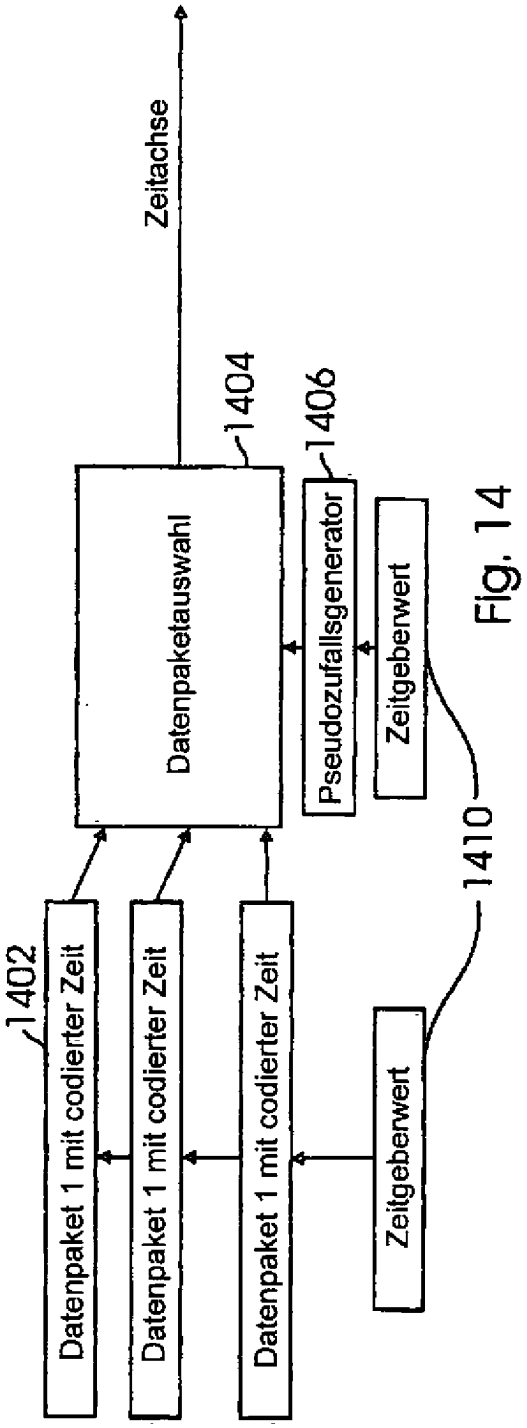

Zeitachse
1404
Datenpaketauswahl
1406
Pseudozufallsgenerator
Zeitgeberwert
1402
Datenpaket 1 mit codierter Zeit
Datenpaket 1 mit codierter Zeit
Datenpaket 1 mit codierter Zeit
Zeitgeberwert
1410

Fig. 14