(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 197 03 970 B4** 2006.02.02

(12) **Patentschrift**

(21) Aktenzeichen: **197 03 970.7**
(22) Anmeldetag: **03.02.1997**
(43) Offenlegungstag: **06.08.1998**
(45) Veröffentlichungstag der Patenterteilung: **02.02.2006**

(51) Int Cl.[8]: ***G07C 11/00*** (2006.01)
G06F 12/14 (2006.01)
G07C 9/00 (2006.01)
H04L 9/32 (2006.01)

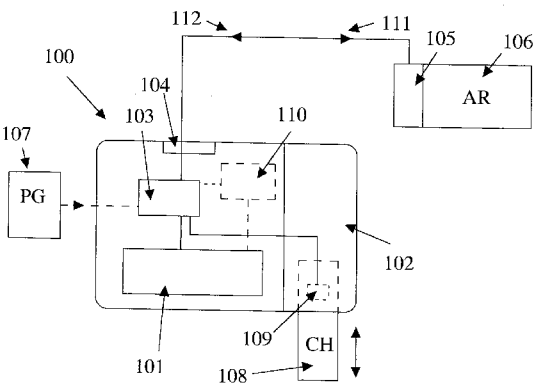
(73) Patentinhaber:
Wilke, Thomas, 10627 Berlin, DE

(72) Erfinder:
gleich Patentinhaber

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 195 48 387 C1
DE 195 21 264 A1
US 55 90 199
US 55 68 554
US 55 46 463
EP 07 52 635 A1
JYRI KURKI: "Die Struktur der Finanzdienstleistungen im Internet mit besonderer Berücksichtigung der Sicherheitsaspekte" BGI-Seminararbeit 7.12.1996 http://141.20.102.25/zza041/fd1.html;

(54) Bezeichnung: **Verfahren zur Erfassung von Daten und deren Übermittlung in authentischer Form**

(57) Hauptanspruch:) Verfahren zur Erfassung von Daten und deren Übermittlung in einer authentischen Darstellung, mit folgenden Schritten:
– Erfassung der Daten, die in einer authentischen Darstellung übermittelt werden sollen, mittels einer Datenerfassungseinheit im Datenerfassungsgerät (100, 200),
– Speicherung der erfassten Daten in einem Pufferspeicher im Datenerfassungsgerät (100, 200),
– Erfassung von benutzerspezifischen Daten sowie Authentifizierung des Benutzers mittels einer Identifikationseinheit im Datenerfassungsgerät (100, 200),
– Verschlüsselung der Daten, die in einer authentischen Darstellung übermittelt werden sollen, mittels einer Datenverschlüsselungseinheit im Datenerfassungsgerät (100, 200), wenn der Benutzer erfolgreich authentifiziert wurde, wobei die Programmanweisungen des Datenerfassungsgeräts (100, 200) ausschließlich in einem Festwertspeicher (ROM) des Datenerfassungsgeräts (100, 200) oder einer in dieses einführbaren Chipkarte abgelegt sind,
– Übermittlung der verschlüsselten Daten mittels einer Datenübermittlungseinheit im Datenerfassungsgerät (100, 200) an die Datenverarbeitungseinrichtung (500),
– Empfangen der verschlüsselten Daten mittels einer Datenempfangseinheit in der Datenverarbeitungseinrichtung (500),
–...



Beschreibung

Hintergrund der Erfindung

[0001] Die vorliegende Erfindung betrifft die Erfassung und Übermittlung von Daten. Genauer betrifft die vorliegende Erfindung ein Datenerfassungsgerät, das Daten nach ihrer Erfassung bzw. Eingabe an ein anderes Datenverarbeitungsgerät in einer authentischen Form übermitteln soll. Die authentische Form soll einen eindeutigen Rückschluß auf denjenigen Benutzer des Datenerfassungsgerätes ermöglichen, der nach Durchführung geeigneter Sicherheits- bzw. Kontrollmaßnahmen die Übermittlung der Daten freigegeben hat. Ergänzend kann die authentische Form auch eine Überprüfungsmöglichkeit dafür eröffnen, ob die Daten bei der Übermittlung zu einem anderen Datenverarbeitungsgerät unbefugt manipuliert worden sind. Außerdem betrifft die vorliegende Erfindung auch ein Verfahren zur Steuerung eines Datenerfassungsgerätes, insbesondere auch in seinem Zusammenwirken mit einem anderen Datenverarbeitungsgerät.

Anwendungsgebiet der Erfindung

[0002] Eine wichtige Anwendung von Datenverarbeitungsgeräten bzw. Computern ist die Übermittlung von Daten an andere Computer. Zur Übermittlung können zusammengeschaltete Netzwerke wie lokale Netzwerke (LAN) bzw. weiträumige Netzwerke (WAN) wie z.B. das Internet verwendet werden. Immer verbreiteter wird jedoch auch die mobile Datenkommunikation. Die zu übermittelnden Daten können direkt in ein Datenerfassungsgerät eingegeben bzw. von diesem erfasst werden, sie können jedoch auch von externen Geräten wie z.B. Peripheriegeräten, Videokameras, Scannern und dergleichen erfasst werden.

[0003] Dabei soll häufig die Benutzung des Datenerfassungsgerätes nur hierzu berechtigten Benutzern möglich sein. Alternativ hierzu ist es jedoch häufig auch erforderlich, daß der andere Computer feststellen kann, von welchem Benutzer die Übermittlung der Daten autorisiert worden ist. Dies ist insbesondere dann erforderlich, wenn die zu übermittelnden Daten zum Abschluß oder zur Durchführung eines Geschäftes dienen und deshalb rechtsverbindlich sein sollen, oder wenn die Daten als Beweis dienen sollen.

[0004] Ferner werden häufig Daten übermittelt, die einem Zugriff oder einer Manipulation durch unberechtigte Dritte nicht zugänglich sein sollen. Nur wenn der andere Computer ermitteln kann, daß die Daten während der Übermittlung nicht manipuliert worden sind, ist die Authentizität bzw. Glaubwürdigkeit der Daten, die von dem anderen Computer empfangen werden, gewährleistet.

Stand der Technik

[0005] Üblicherweise wird zu diesen Zwecken die Zugangsberechtigung des Benutzers geprüft und/oder die zu übertragenden Daten werden verschlüsselt.

[0006] **Fig.** 9 stellt einen Computer dar, wie er zur Datenerfassung und Datenübermittlung im Stand der Technik verwendet wird, wobei eine Zugangskontrolle vorgesehen ist, damit der Computer nur von hierzu Berechtigten genutzt werden kann.

[0007] Dabei ist ein Computer (**901**) mit Monitor (**902**) und Tastatur (**903**) dargestellt. Zur Ausführung von Programmanweisungen dient eine Prozessorkarte (**904**). Daten, die über die Tastatur eingegeben oder von der Maus ausgewählt werden, werden an die Prozessorkarte (**904**) übermittelt und von dieser an Anwendungsprogramme weitergereicht, die ebenfalls auf dieser Prozessorkarte oder aber auf anderen PC-Karten betrieben werden.

[0008] Es sei der Fall betrachtet, daß der Computer mit einem anderen Computer über den Übermittlungsweg (**905**) kommuniziert. Damit die Übermittlung der Daten nicht von hierzu Unberechtigten freigegeben bzw. autorisiert wird, kann ein Zugangskontrollsystem verwendet werden, wie z.B. ein Magnetstreifenleser (**906**), welcher auf einem auf einem Speichermedium (**907**) gespeicherte Daten abruft und diese ggf. mit weiteren benutzerspezifischen Daten, wie z.B. einem Persönlichen-IdentifizierNummer (PIN) oder einer TransAktionsNummer (TAN) vergleicht. War die Ermittlung der Identität des Benutzers erfolgreich, so wird die Benutzung des Computers für den als hierzu berechtigt ermittelten Benutzer freigegeben.

[0009] Damit nun nicht der Datenverkehr auf dem Übermittlungsweg (**905**) von unberechtigten Dritten belauscht und/oder manipuliert werden kann, werden üblicherweise Verschlüsselungsverfahren angewendet. Üblich sind symmetrische oder asymmetrische Verschlüsselungsverfahren. Zur Verschlüsselung der Daten wird häufig ein speziell ausgebildeter Verschlüsselungschip bzw. Kryptochip verwendet, der sich entweder direkt auf der Prozessorkarte (**904**) oder an einem anderen Ort im Gehäuse des Computers befindet.

[0010] In Kombination mit der oben beschriebenen Zugangskontrolle kann der Computer in einer Normalbetriebsweise betrieben werden, in welcher die Daten unverschlüsselt übermittelt werden, oder aber in einer Verschlüsselungsbetriebsweise, in welcher die Daten vor der Übermittlung verschlüsselt werden.

[0011] Falls eine Zugangskontrolle erfolgt, so wird bei herkömmlichen Systemen vereinbart, daß die

Übermittlung der Daten nur von dem hierzu Berechtigten autorisiert worden ist. Eine solche Vereinbarung ist für gewisse Belange der Datensicherheit ausreichend.

[0012] Nachteilig an der beschriebenen Vorgehensweise ist zunächst, daß die Verschlüsselung üblicherweise dynamisch ein- und ausgeschaltet wird. Dies bedeutet, daß die zu übermittelnden Daten zu gewissen Zeitpunkten während der beschriebenen Vorgehensweise in unverschlüsselter Form vorliegen und erst in einem abschließenden Schritt vor der Übermittlung verschlüsselt werden. Dies bietet einen Angriffspunkt für ungewünschte Manipulationen. Dies betrifft insbesondere diejenigen Daten, die ein Benutzer mit Hilfe eines Anwendungsprogramms ggf. einschließlich einer Menüauswahl in ein Datenerfassungsgerät eingibt und die dann an einen angeschlossenen Computer zum Zwecke der Übermittlung an einen anderen Rechner weitergeleitet werden. Weil die Daten zu gewissen Zeitpunkten unverschlüsselt vorliegen, wie z.B. während der Übertragung vom Datenerfassungsgerät zum Computer, können sie ohne größeren vorherigen Dechiffrieraufwand manipuliert werden.

[0013] Solange nicht sichergestellt ist, daß innerhalb des Datenerfassungsgerätes keine Manipulation der zu übermittelnden Daten erfolgen kann, bzw. solange der Benutzer die zu übermittelnden Daten vor ihrer Übermittlung nicht nochmals überprüft, kann nicht gewährleistet werden, daß diejenigen Daten, die der andere Rechner nach Übermittlung und ggf. nach deren Entschlüsselung erhält, auch wirklich die von dem Benutzer autorisierten Daten darstellen.

[0014] Ein weiterer Grund für die bestehende Unsicherheit ist, daß das Datenerfassungsgerät an sich unsicher sein kann. Beispielsweise deshalb, weil ein Unberechtigter die Hardware – von außen uneinsehbar – manipulieren kann, oder weil in die Software oder das Betriebssystem Viren, Würmer oder sonstige Manipulationsmittel eingebracht werden können.

[0015] Diese Unsicherheit wird dadurch erhöht, daß die Vernetzung von Computern üblich geworden ist. Häufig werden Computer untereinander nicht nur in lokalen Netzwerken (LAN) z.B. eines Unternehmens vernetzt sondern zunehmend verfügen entweder die Arbeitsplatzrechner (clients) selbst oder aber Server solcher Netze über einen Anschluß an unsichere Netzwerke, wie z.B. dem Internet. Dies eröffnet prinzipiell die Möglichkeit, daß Unberechtigte entweder unmittelbar Daten in solchen Netzwerken manipulieren können oder dadurch, daß Manipulationsmittel. wie Viren oder dergleichen in wichtige Programmteile eingebracht werden können, welche dann ihrerseits unberechtigte Manipulationen vornehmen.

[0016] Nachteilig ist außerdem, daß ein Nachweis dieser und ähnlicher Manipulationen der Daten nach deren Übermittlung bei bestehenden Systemen nicht möglich ist. Nachteilig ist insbesondere, daß ein sicherer Nachweis der Authentizität bzw. Echtheit der Daten nicht gewährleistet ist.

[0017] Nachteilig ist außerdem, daß Daten, die in Datenerfassungsgeräte eingegeben und/oder von diesen erfasst und/oder von diesen an andere Datenverarbeitungsgeräte übermittelt werden, nicht als rechtsverbindliche Grundlage zum Abschluß oder zur Durchführung von Geschäften jedwelcher Art verwendet werden können.

[0018] Die Druckschrift US 5546463 A beschreibt ein Verfahren, mit dem eine authentische Kommunikation zwischen zwei Datenverarbeitungseinheiten realisiert werden kann Dabei ist die Datenerfassungseinheit nicht Bestandteil des beschriebenen Geräts und somit anfällig für Manipulationen. Weiterhin weist das Gerät keine Einrichtung auf, mit der zu übermittelnde Daten auf Authentizität überprüft werden können.

[0019] Die Druckschrift DE 3704814 A1 beschreibt ein Verfahren zur Nutzung einer IC-Karte durch mehrere Parteien, wobei die korrekte Verwendung der Karte durch spezielle Kodieralgorithmen sichergestellt wird, die unter anderem eine Rückkopplung vorsehen. Im Unterschied zum vorliegenden Verfahren bezieht sich die Rückkopplung jedoch nur auf Vorgänge, die in der Karte ablaufen.

Aufgabenstellung

Aufgabe der Erfindung

[0020] Eine Aufgabe der vorliegenden Erfindung ist es, ein Verfahren zu finden, das es ermöglicht, Veränderungen bzw. Manipulationen von erfassten und zu übermittelnden Daten möglichst frühzeitig in ihrem Entstehungs- bzw. Kompositionsprozeß nachzuweisen, wobei

Lösung der Aufgabe

[0021] Die vorgenannte Aufgabe wird durch ein Verfahren gemäß dem Hauptanspruch Weitere zweckmäßige Ausführungsformen des erfindungsgemäßen Verfahrens zur Erfassung von Daten und deren Übermittlung in authentischer Form werden durch die Unteransprüche definiert.

Vorteile der Erfindung

[0022] Gemäß der Erfindung wird ein Datenerfassungsgerät vorgeschlagen, das nur aus einer Datenerfassungseinheit, aus einer Identifikationseinheit, aus einer Datenverschlüsselungseinheit und einer Datenübermittlungseinheit besteht. Durch Reduzie-

rung der Baugruppen auf ihr absolutes Minimum wird die Anzahl von Schwachstellen oder möglichen Angriffspunkten für eine Manipulation der erfassten Daten reduziert. Vorzugsweise befinden sich diese Baugruppen in einem mechanisch stabilen und geschützten Gehäuse, so daß vorteilhafterweise eine Manipulation der Hardware des Datenerfassungsgerätes unterbunden wird.

[0023] Das Datenerfassungsgerät führt nur solche Programmanweisungen aus, die sich auf einem Festwertspeicher bzw. ROM innerhalb des Gehäuses des Datenerfassungsgerätes befinden. Weil dieses in seiner bevorzugten Ausführungsform nicht über einen eigenen Direkt-Zugriffsspeicher bzw. RAM verfügt, ist vorteilhafterweise eine Manipulation der Geräte-Software durch Viren, Würmer oder sonstige Manipulationsmittel unterbunden.

[0024] Eine weitere der Erfindung zugrundeliegende Idee ist, die erfassten und zu übermittelnden Daten so früh wie möglich zu fixieren bzw. in eine authentische Datendarstellung zu transformieren. Bei einer bevorzugten Ausführungsform, wie z.B. bei der Eingabe von Daten in eine Computertastatur, werden somit die Daten bereits innerhalb der Tastatur verschlüsselt, in eine authentische Darstellung transformiert und in dieser Darstellung an einen angeschlossenen Computer übermittelt. Dies unterbindet vorteilhafterweise die Möglichkeit, daß die Daten während ihrer Übermittlung über das Verbindungskabel zwischen dem Datenerfassungsgerät und einem andere Rechner, oder bei der bevorzugten Ausführungsform zwischen der Computertastatur und dem Computer, belauscht und manipuliert werden.

[0025] Das erfindungsgemäße Verfahren verschlüsselt die Daten vor ihrer Übermittlung mit Hilfe eines üblichen Verschlüsselungsverfahrens. Hierbei können sowohl asymmetrische Verschlüsselungsverfahren als auch symmetrische Verschlüsselungsverfahren verwendet werden. Indem zur Verschlüsselung benutzerspezifische Schlüssel verwendet werden, ist vorteilhafterweise eine eindeutige Identifizierung des die Übermittlung autorisierenden Benutzers möglich. Voraussetzung hierfür ist, daß die Identität bzw. Berechtigung des Benutzers hinreichend sorgfältig überprüft wird. Zur Identifikation des Benutzers werden bevorzugterweise biometrische Verfahren, Paßwortverfahren, Shared-Secret-Schemes verwendet, eine bevorzugte Ausführungsform verwendet jedoch eine Chipkarte, die bevorzugterweise einen Kryptographiechip beinhaltet, der zur Verschlüsselung und Transformation der Daten in eine authentische Darstellung verwendet werden kann. Diese Identifikationsverfahren sind im Beschreibungsteil genannt und beschrieben, aus dem Stand der Technik hinreichend bekannt und brauchen deshalb nicht eingehender erläutert werden.

[0026] Symmetrische bzw. asymmetrische Verschlüsselungsverfahren sind aus dem Stand der Technik hinreichend bekannt und brauchen deshalb nicht eingehender erläutert werden.

[0027] Gemäß der vorliegenden Erfindung wird die Integrität bzw. Unversehrtheit der übermittelten Daten durch kryptographischer Prüfwerte bzw. Siegel gewährleistet, mit deren Hilfe Modifikationen der übermittelten Daten festgestellt werden können. Hierzu verwendet eine bevorzugte Ausführungsform digitale Signaturen unter Verwendung üblicher asymmetrischer Schlüssel. Eine andere Ausführungsform verwendet jedoch zu diesem Zwecke symmetrische Verschlüsselungsverfahren.

[0028] Bevorzugte Signaturverfahren sind die üblichen Digital Signatur Algorithmen (DSA), El-Gamal-Signatur-Verfahren, Fiat-Shamir-Protokolle, RSA-Verfahren bzw. Rivest-Shamir-Adleman-Verfahren und Schnorr-Verfahren. Bei Verwendung symmetrischer Verschlüsselungsverfahren bedient sich die erfindungsgemäße Ausführungsform bevorzugt einem Blockchiffre-Verfahren im CBC-Modus oder im CFB-Modus. Diese Verfahren, Methoden und Protokolle sind aus dem Stand der Technik hinreichend bekannt und brauchen deshalb nicht eingehender erläutert werden.

[0029] In einem bevorzugten Verfahren werden zumindest die verwendeten Schlüssel von einer sicheren Behörde bzw. secure-key-issuing-authority (SKIA) vergeben.

[0030] Aufgrund der Verwendung solcher Verschlüsselungs- und Signaturverfahren ist dem Empfänger von Daten vorteilhafterweise der Nachweis einer unberechtigten Manipulation der übermittelten Daten möglich.

[0031] Weil die bevorzugte Ausführungsform der Erfindung – je nach den einzuhaltenden Sicherheitsstandards – mehr oder weniger aufwendige Prüfschritte ausführt, bei dem die Identität und/oder Berechtigung des Benutzers überprüft wird, ist in Verbindung mit den oben genannten Verschlüsselungsverfahren und/oder digitalen Signaturverfahren ein vorteilhaft hoher Sicherheitsstandard bei der Übermittlung von Daten gewährleistet. Durch die besondere Ausbildung des Datenerfassungsgerätes ist vorteilhafterweise eine hohe Sicherheit bei der Datenerfassung sichergestellt.

[0032] Indem die Daten mit Hilfe eines benutzerspezifischen Schlüssels verschlüsselt und/oder mit einer digitalen Signatur versehen werden, und die Daten somit in einer bevorzugten Ausführungsform nur in einer authentischen Darstellung übermittelt werden, können die übermittelten Daten vom Empfänger vorteilhafterweise als rechtsverbindliche Daten zur Täti-

gung irgendeiner Art von Geschäften verwendet werden. Unter einer authentischen Datendarstellung sei im folgenden stets eine Datendarstellung verstanden, die es einem anderen Rechner ermöglicht festzustellen, von welchem Benutzer die übermittelten Daten zur Übermittlung autorisiert worden sind.

[0033] Die vorliegende Erfindung wird genauer mit Hilfe der folgenden ausführlichen Beschreibung und Bezugnahme auf die beigefügten Figuren verstanden werden. Die beigefügten Figuren, auf die in der Beschreibung Bezug genommen wird, stellen einige bevorzugte Ausführungsformen der Erfindung dar.

Ausführungsbeispiel

Figurenübersicht

[0034] Fig. 1 zeigt eine erste Ausführungsform des Datenerfassungsgerätes der vorliegenden Erfindung, welches die Daten direkt an einen anderen Rechner übermittelt.

[0035] Fig. 2 zeigt eine weitere Ausführungsform des Datenerfassungsgerätes, das eine Einheit zur Handhabung einer Chipkarte mit integriertem Kryptochip umfaßt.

[0036] Fig. 3 ist ein Flußdiagramm und zeigt eine einfache Betriebsweise des Datenerfassungsgerätes.

[0037] Fig. 4 stellt ein Zustandsübergangsdiagramm des Datenerfassungsgerätes dar.

[0038] Fig. 5 zeigt eine bevorzugte Ausführungsform des Datenerfassungsgerätes, das mit einem Computer verbunden ist, über den die Übermittlung an den anderen Rechner erfolgt.

[0039] Fig. 6 ist ein zu einer bevorzugten Ausführungsform gemäß Fig. 5 zugehöriges Flußdiagramm.

[0040] Fig. 7 zeigt eine weitere Ausführungsform des Datenerfassungsgerätes, das eine Rückkopplung zwischen dem angeschlossenen Computer und dem Datenerfassungsgerät ermöglicht.

[0041] Fig. 8 ist ein zur Ausführungsform gemäß Fig. 7 zugehöriges Flußdiagramm; und

[0042] Fig. 9 stellt einen Computer dar, wie er zur Datenerfassung- und Übermittlung im Stand der Technik verwendet wird, wobei eine Zugangskontrolle vorgesehen ist, damit der Computer nur von hierzu Berechtigten genutzt werden kann.

Spezieller Beschreibungsteil

[0043] Fig. 1 zeigt eine erste Ausführungsform eines Datenerfassungsgerätes gemäß der vorliegenden Erfindung. In seiner einfachsten Grundform umfaßt dieses Datenerfassungsgerät eine Datenerfassungseinheit (**101**), eine erste Identifikationseinheit (**102**), eine Datenverschlüsselungseinheit (**103**) und eine Datenübermittlungseinheit (**104**), welche die Daten an einen anderen Rechner (AR, **106**) übermittelt.

[0044] Um die Sicherheit zu erhöhen, werden gemäß der Erfindung möglichst alle wesentlichen Komponenten des Datenerfassungsgerätes in einem mechanisch stabilen und gesicherten Gehäuse untergebracht. Um die Sicherheit gegen Viren und andere Datenmanipulationsmittel zu gewährleisten, führt das Datenerfassungsgerät vorzugsweise nur Programmanweisungen aus, die sich auf einem Festwertspeicher (ROM) innerhalb des Gehäuses befinden. Indern das Datenerfassungsgerät vorzugsweise über keinen eigenen Schreib-Lese-Speicher (RAM) verfügt, können sich Manipulationsmittel zur Manipulation der Programmanweisungen nicht im Datenerfassungsgerät bzw. in dessen Prozessor festsetzen, um so dessen Ausführungen zu manipulieren.

[0045] Zur Datenerfassung dient die Datenerfassungseinheit (**101**). Hierbei handelt es sich bei einer Ausführungsform um eine herkömmliche Dateneingabetastatur. Um die Leistungsfähigkeit des Datenerfassungsgerätes jedoch zu erhöhen, können erfindungsgemäß auch komplexere Dateneingabe- und Datenerfassungsverfahren eingesetzt werden, wie etwa die Erfassung bewegter Bilder oder Standbilder mit Hilfe einer Videokamera, die Abtastung von Dokumenten mit Hilfe eines Scanners, wobei die erfaßte optische Information zusätzlich auch mit Hilfe von Filterung bzw. optischen Buchstabenerkennungsverfahren (OCR) vorverarbeitet werden kann, oder die Erfassung akustischer Informationen einschließlich von Spracherkennungssystemen, um den Informationsgehalt der erfaßten Daten zu reduzieren. Damit die Datensicherheit jedoch gewährleistet ist, werden die Programmanweisungen bevorzugt auf einem Festwertspeicher (ROM) abgespeichert, der sich innerhalb des Gehäuses des Datenerfassungsgerätes (**100**) befindet.

[0046] Zum Zwecke der Datenerfassung kann auch ein entsprechend ausgelegtes Peripheriegerät (PG, **107**) an das Datenerfassungsgerät angeschlossen werden.

[0047] Zur Verschlüsselung und Transformation der Daten in eine authentische Datendarstellung verwendet die in Fig. 1 abgebildete Ausführungsform einen Datenprozessor, der spezielle kryptographische Programmanweisungen abarbeitet. Dieser Datenprozessor kann jedoch auch ein handelsüblicher speziell ausgebildeter Kryptographieprozessor sein, was Rechenzeit spart und somit die Datenübermittlungsrate erhöht.

[0048] Nach Verschlüsselung der Daten im Kryptographieprozessor (**103**) werden die Daten mit Hilfe einer üblichen Datenübermittlungseinheit unter Verwendung üblicher Datenübermittlungsprotokolle an den anderen Rechner übermittelt.

[0049] Um die Identität des Benutzers zu ermitteln, verfügt das Datenerfassungsgerät über eine erste Identifikationseinheit (**102**), bei der es sich bevorzugt, wie in Fig. 1 abgebildet, um ein Gerät zur Handhabung von handelsüblichen Smart Cards bzw. Chipkarten (**108**) handelt. Solche Chipkarten, die aus dem Stand der Technik hinreichend bekannt sind, verfügen zumindest über einen integrierten Festwertspeicher (**109**), in den meisten Fällen jedoch auch über einen Prozessor (**109**), so daß die Abarbeitung einfacher Programmanweisungen auch unmittelbar durch die Chipkarte erfolgen kann, wobei sich die hierzu benötigten Programmanweisungen entweder im ROM des Datenerfassungsgerätes oder aber bevorzugt im Festwertspeicher (**109**) der Chipkarte (**108**) selbst befinden.

[0050] In anderen Anwendungen, in denen beispielsweise die Bilddaten einer Überwachungs-Videokamera oder eines eingescannten Textdokumentes in authentischer Form übermittelt werden sollen, genügt jedoch häufig auch eine einfache Tastatur, über die ein Benutzerkennwort, Codierschlüssel und dergleichen auf Anforderung durch die Identifikationseinheit eingegeben werden kann. Auch die oben genannten Datenerfassungsmethoden können einzeln oder in Kombination zur Ermittlung der Benutzeridentität verwendet werden. Der betriebene Aufwand zur Ermittlung der Benutzeridentität ist abhängig vom dem Sicherheitsstandard, den das System gewährleisten soll.

[0051] Zur Darstellung von eingegebenen bzw. erfassten Daten verfügt des Datenerfassungsgerät über eine Darstellungseinrichtung (**110**), die bevorzugt als ein LCD-Bildschirm ausgebildet ist, oder aber als berührungsempfindlicher Bildschirm, so daß die Verwendung einer zusätzlichen Tastatur als Datenerfassungseinheit nicht erforderlich ist.

[0052] Die Datenübermittlung mit dem anderen Rechner (AR, **106**) erfolgt in einer Einwegsbetriebsweise (**111**) oder in einer Zweiwegbetriebsweise (**112**) über eine Datenleitung, die Teil eines Computernetzwerks wie etwa einem lokalen Netzwerk (LAN) oder einem weiträumigen Netzwerk (WAN) oder des Internets ist. Dabei kommen übliche Datentransferprotokolle zum Einsatz, wie etwa Ethernet, Local Talk, FTP (file transfer protocol) oder dergleichen, die aus dem Stand der Technik hinreichend bekannt sind und deshalb hier nicht eingehend erläutert zu werden brauchen. Die Datenübermittlung erfolgt bei einer anderen Ausführungsform über drahtlose Telekommunikation in einem üblichen Datenformat erfolgen. Eine weitere vorgesehene Art der Datenübermittlung ist die Speicherung der Daten auf einem magnetischen oder optischen Datenspeichermedium und die Übergabe dieses Datenspeichermediums an den anderen Rechner.

[0053] Fig. 2 zeigt eine weitere Ausführungsform des Datenerfassungsgerätes, das eine Einheit zur Handhabung einer Chipkarte mit integriertem Kryptochip umfaßt.

[0054] Sofern diese Figur die gleichen Bezugszeichen wie in Fig. 1 enthält, sind damit auch diegleichen Einheiten gemeint. Im Gegensatz zur Ausführungsform gemäß Fig. 1 enthält dieses Datenerfassungsgerät jedoch keinen eigenen Krypto- bzw. Verschlüsselungsprozessor.

[0055] Zur Verschlüsselung dient vielmehr die von einem Benutzer einzuführende Chipkarte (**208**), die neben einem Festwertspeicher (ROM), der benutzerspezifische Daten enthält, auch einen Verschlüsselungsprozessor (**209**) umfaßt. Zusätzlich kann sich auf dieser Chipkarte auch ein gewöhnlicher Prozessor zur Durchführung des unten beschriebenen erfindungsgemäßen Verfahrens befinden.

[0056] Alle Daten, die von der Datenerfassungseinheit bzw. von dem Peripheriegerät (PG) erfasst worden sind, werden über einen zentralen Bus (**213**) an den Prozessor bzw. den Verschlüsselungsprozessor der Chipkarte übermittelt. Nach Verschlüsselung bzw. Transformation in eine authentische Darstellung gelangen die Daten zur Übermittlungseinheit, die diese dann wie vorgenannt beschrieben an den anderen Rechner übermittelt.

[0057] Fig. 3 ist ein Flußdiagramm und zeigt eine einfache Betriebsweise des Datenerfassungsgerätes.

[0058] Vor Eingabe bzw. Erfassung der Daten oder zumindest vor deren Übermittlung an den an das Datenerfassungsgerät angeschlossenen Computer erfolgt die Überprüfung (**302**) der Identität des Benutzers.

[0059] Je nach dem Informationsgehalt der dem Datenerfassungsgerät zur Verfügung stehenden benutzerspezifischen Daten können hierbei verschiedene Vorgehensweisen vorgenommen werden.

[0060] Bei einer Ausführungsform, der keine oder nur sehr eingeschränkt benutzerspezifische Vergleichs- bzw. Referenzdaten zur Verfügung stehen, wird dem Datenerfassungsgerät von dem anderen Rechner ein fester öffentlicher Schlüssel zur Verfügung gestellt, sobald das Datenerfassungsgerät feststellt, daß ein Benutzer die Übermittlung von Daten anfordert. Anschließend fordert das Datenerfas-

sungsgerät den Benutzer auf, Identifikationsdaten einzugeben. Dabei kann es sich im einfachsten Fall um personenspezifische Identifikationsnummern (PIN) und/oder Transaktionsaktionsnummern (TAN) oder andere alphanumerische Zeichenfolgen handeln, die über eine Datentastatur bzw. über die Datenerfassungseinheit des Datenerfassungsgerätes einzugeben sind.

[0061] Für höhere Sicherheitsanforderungen ist jedoch ein größerer Informationsgehalt der Identifikationsdaten von Vorteil. Hierzu wird in einer bevorzugten Ausführungsform der vorliegenden Erfindung eine Chipkarte verwendet, deren benutzerspezifischen Daten mit vom Benutzer einzugebenden alphanumerischen Zeichenkombinationen verglichen werden.

[0062] Bei einer weiteren bevorzugten Ausführungsform werden zusätzlich als Identifikationsdaten biometrische Daten erfaßt, die von körperlichen Merkmalen und/oder Eigenschaften des Benutzers abgeleitet werden. Hierbei handelt es sich um einen oder mehrere Fingerabdrücke, der bzw. die von einem Fingerprintscanner erfaßt werden, oder um einen Scanner zum Abtasten der Netzhaut bzw. des Augenhintergrundes des Benutzers, oder um einen Sprachanalysator, der ein Sprachprofil des Benutzers ermittelt. Durch Vergleich dieser biometrischen Daten mit benutzerspezifischen Daten kann die Identität des Benutzers sehr zuverlässig ermittelt werden. Dieser Vergleich kann sowohl im Datenerfassungsgerät selbst bzw. seinem Chipkartenlesegerät erfolgen oder aber im anderen Rechner. Im letztgenannten Fall müssen die erfaßten Identifikationsdaten bzw. die biometrischen Daten mit Hilfe des öffentlichen Schlüssels verschlüsselt und an den anderen Rechner übermittelt werden.

[0063] Der andere Rechner entschlüsselt die ankommenden Daten mit Hilfe des zugehörigen geheimen Schlüssels und nimmt den Vergleich der ankommenden Identifikationsdaten mit benutzerspezifischen Referenzdaten, die etwa einer Datenbank entnommen werden, vor. Nach erfolgreichem Vergleich geht das Datenerfassungsgerät in seinen authentischen Betriebszustand über. In diesem Betriebszustand werden alle Daten, die das Datenerfassungsgerät verlassen, nur in verschlüsselter Form und nach digitaler Unterschrift übermittelt (**304**, **305**). Optional kann überprüft werden, ob eine Betriebsstörung vorliegt (**305**), woraufhin das Datenerfassungsgerät in seinen Klartext-Betriebszustand zurückkehrt, in dem die Daten nur unverschlüsselt übermittelt werden (**303**).

[0064] Zur Verschlüsselung der Daten muß dem Datenerfassungsgerät vom anderen Rechner ein benutzerspezifischer öffentlicher Schlüssel übergeben werden. Alle zu übermittelnden Daten werden mit diesem Schlüssel verschlüsselt und mit einer digitalen Unterschrift versehen.

[0065] Somit können die übertragenen Daten eindeutig einem berechtigten Benutzer zugeordnet werden, und weil die Daten vor der Übermittlung mit einer digitalen Unterschrift versehen worden sind, kann eine unberechtigte Manipulation der Daten während der Übermittlung zum anderen Rechner entdeckt werden.

[0066] In einer anderen bevorzugten Ausführungsform stehen dem Datenerfassungsgerät zur Überprüfung der Benutzeridentität umfangreichere benutzerspezifische Referenzdaten zur Verfügung, etwa deswegen, weil der Benutzer vor Erfassung weiterer Identifikationsdaten eine Chipkarte in das Chipkartenlesegerät des Datenerfassungsgerätes einführen muß. Die im ROM der Chipkarte abgespeicherten benutzerspezifischen Daten lassen einen "zeroknowledge" Beweis der Benutzeridentität zu, also einen Beweis, zu dem das Datenerfassungsgerät nicht noch zusätzliche benutzerspezifische Referenzdaten benötigt, die ihm etwa von dem anderen Rechner zur Verfügung gestellt werden müssen. Zur Überprüfung der Benutzendentität werden die erfaßten Identifikationsdaten und die benutzerspezifischen Refernzdaten unmittelbar vom Chipkartenlesegerät oder aber im Prozessor der Chipkarte miteinander verglichen.

[0067] Ist diese Überprüfung erfolgreich, so wird der Verschlüsselungseinheit (**304**) des Datenerfassungsgerätes gemäß Fig. 1 der benutzerspezifische öffentliche Schlüssel (PK) übergeben. Bei einem Datenerfassungsgerät gemäß Fig. 2 braucht der öffentliche Schlüssel solange nicht an weitere Einheiten des Datenverarbeitungsgerätes weitergereicht werden, solange dieses nur in einer Einweg-Betriebsweise betrieben wird, in der das Datenerfassungsgerät Daten, die in dem Kryptochip der Chipkarte verschlüsselt werden, nur an den anderen Rechner übermittelt. Dadurch wird die Sicherheit des Datenerfassungsgerätes zusätzlich erhöht.

[0068] Soll das Datenerfassungsgerät jedoch zusätzlich auch in einer Zweiweg-Betriebsweise betrieben werden, in der das Datenerfassungsgerät mit dem benutzerspezifischen geheimen Schlüssel verschlüsselte Anweisungen oder Daten von dem anderen Rechner verwerten soll, so muß der Ver- bzw. Entschlüsselungseinheit des Datenerfassungsgerätes der benutzerspezifische öffentliche Schlüssel, der sich auf der Chipkarte befindet, übergeben werden.

[0069] War die Überprüfung der Benutzeridentität in Schritt **302** nicht erfolgreich, so bleibt das Datenerfassungsgerät im Klartext-Betriebszustand, so daß die Übermittlung der Daten sowohl an den anderen Rechner nur unverschlüsselt erfolgt.

[0070] Fig. 4 stellt ein Zustandsübergangsdiagramm des Datenerfassungsgerätes dar. Hierbei sei das Beispiel betrachtet, daß ein Bankkunde Daten zu einem Rechner übermitteln will. Unter Rechner sei in diesem Beispiel der Zugangsrechner einer Bank verstanden, der mit dem Datenerfassungsgerät über eine Datenleitung in Verbindung stehe. Bei dem Datenerfassungsgerät könnte es sich um einen Bankautomaten oder ein System zur Durchführung von Telebanking handeln.

[0071] Das hierzu verwendete Datenerfassungsgerät verfüge als Datenerfassungseinheit über eine übliche Tastatur und als erste Identifikationseinheit über einen Chipkartenleser. Hinzu komme ein Bildschirm zur Darstellung der Daten, bei denen es sich in diesem Beispiel um einfache alphanumerische Zeichen, wie etwa Kundenname, Bankkontonummer oder Bankleitzahl handelt. Der Bankkunde verfüge über eine Chipkarte, die zumindest benutzerspezifische Daten enthält, damit das Chipkartenlesegerät einen zero-knowledge Beweis der Benutzeridentität durchführen kann. Die Chipkarte kann zusätzlich auch den privaten Schlüssel (SK) und/oder den öffentlichen Schlüssel (PK) enthalten, die als Grundlage für ein asymmetrisches Verschlüsselungsverfahren verwendet werden können.

[0072] Solange der Kunde die Chipkarte nicht eingeführt hat (**401**), erfolgt die Übermittlung der vom Kunden eingegebenen Daten vom Datenerfassungsgerät zum anderen Rechner unverschlüsselt (**402**), wie durch die Schleife bei (**402**) angedeutet. Dieser Datenverkehr kann ohne Probleme von Unbefugten belauscht und zu dessen Vorteil manipuliert werden. Legt der Benutzer nun die Karte ein (**403**), so erfolgt zunächst die Überprüfung der Benutzeridentität (**404**) und ggf. auch die Überprüfung der Gültigkeit der Chipkarte. Bei negativem Ergebnis dieses Überprüfung (**405**) erfolt der Auswurf der Karte und das Datenerfassungsgerät nimmt wieder seinen Klartext-Betrieb auf.

[0073] Bei positivem Ergebnis der Überprüfung geht das Datenerfassungsgerät in den authentischen Betrieb über (**407**), in dem alle das Datenerfassungsgerät verlassenden Daten nur in einer authentischen Datendarstellung übermittelt werden. Weil anhand der authentischen Daten vom anderen Rechner festgestellt werden kann, ob die Daten während der Übermittlung manipuliert worden sind, können die so übermittelten Daten als echt betrachtet werden.

[0074] Falls das Datenerfassungsgerät unmittelbar mit dem Zugangsrechner der Bank kommuniziert, so benötigt das Datenerfassungsgerät zur Verschlüsselung einen öffentlichen Schlüssel (PK). Dieser kann dem Datenerfassungsgerät von der Chipkarte zur verfügung gestellt werden. Er kann dem Datenerfassungsgerät jedoch auch von dem Bankrechner zur Verfügung gestellt werden, nachdem dieser von der positiven Überprüfung der Benutzeridentität informiert worden ist.

[0075] Solange keine Betriebsstörung erfolgt, werden die Daten nur in authentischer Form an den Rechner übermittelt. Erfolgt jedoch eine Betriebsstörung (**409**), wie etwa eine Unterbrechung der Kommunikation, oder beendet der Bankkunde die Kommunikation, so erfolgt der Auswurf der Chipkarte und der Rechner kehrt wieder in seine Klartext-Betriebsweise zurück.

[0076] Fig. 5 zeigt eine bevorzugte Ausführungsform des Datenerfassungsgerätes.

[0077] Häufig ist es bei sensiblen Daten erforderlich, daß Daten, die ein Benutzer über eine Tastatur eingibt oder die in einer der oben genannten Weisen von einer Datenerfassungseinheit erfaßt wurden, über einen Computer an einen anderen Rechner übermittelt werden sollen. Eine typische Anwendung könnte die Tätigung einer Überweisung vom PC eines Bankkunden aus sein, der über eine Datenverbindung wie z.B. dem Internet mit dem Zugangsrechner einer Bank verbunden ist. Eine weitere bevorzugte Anwendung ist die authentische Übermittlung von Bild und/oder Tondaten von einem PC bzw. client innerhalb eines Computernetzwerks zu einem anderen PC, der ein client oder ein server sein kann. Dieses Computernetzwerk könnte das Internet sein oder aber ein Intranet eines Unternehmens.

[0078] Bei sensiblen Daten sollte es dem anderen Rechner möglich sein zu ermitteln, a) von welchem Benutzer des Computers die Datenübermittlung autorisiert worden ist und/oder b) ob die Daten während der Übermittlung manipuliert worden sind. Hierzu ist eine Übermittlung der Daten in einem authentischen Format erforderlich.

[0079] Weil jedoch der Computer (**500**) über das Netz (**504**) von außen her zugänglich ist und über einen manipulierbaren Speicherbereich verfügt, könnte der Benutzer des Computers die Übermittlung von Daten A autorisieren und diese noch innerhalb des Computers in Daten B von einem Virus oder dergleichen umgewandelt werden, ohne daß der Benutzer dies bemerkt. Dieses Problem läßt sich durch ein Datenerfassungsgerät beheben, das an den unsicheren Computer angeschlossen ist.

[0080] Hierzu ist bei der in Fig. 5 gezeigten Ausführungsform ein Datenerfassungsgerät (**100**; **200**) vorgesehen, welches als erste Identifikationseinheit über einen Chipkartenleser und als zweite Identifikationseinheit über einen Fingerprintscanner verfügt. Das Datenerfassungsgerät besitzt einen Bus (**502**) zur Kommunikation mit dem Computer (**500**) und optional auch über einen Dateneingangsanschluß zur

Entgegennahme von Daten eines Peripheriegerätes (PG).

[0081] Die Übermittlung der Daten erfolgt sowohl über den Bus (**502**) als auch über das Netz (**504**) in authentischer Datendarstellung. Zur Verschlüsselung und Entschlüsselung im Datenerfassungsgerät dient entweder der Kryptographiechip auf der von dem Benutzer einzuführenden Chipkarte oder aber eine Verschlüsselungseinheit. Auch der Computer und der Rechner benötigen eine Ver- und Entschlüsselungseinheit (**503**; **505**), die sich auf einer Einschubkarte befinden kann oder aber bevorzugt in einem speziellen Kryptographiechip.

[0082] Fig. 6 ist ein zu einer bevorzugten Ausführungsform gemäß Fig. 5 zugehöriges Flußdiagramm.

[0083] Vor Eingabe bzw. Erfassung der Daten oder zumindest vor deren Übermittlung an den an das Datenerfassungsgerät angeschlossenen Computer erfolgt die Überprüfung (**602**) der Identität des Benutzers. Ist diese Überprüfung erfolgreich, so wird der Verschlüsselungseinheit (**503**) des Computers der benutzerspezifische öffentliche Schlüssel (PK) übergeben. Dieser befindet sich entweder auf dem Festwertspeicher (ROM) der Chipkarte oder wird der Verschlüsselungseinheit von dem anderen Rechner zur Verfügung gestellt. Falls die Verschlüsselung der Daten in der Verschlüsselungseinheit des Datenerfassungsgerätes erfolgt, so wird ihr hierzu der geheime Schlüssel (SK) übergegeben, der sich auf dem ROM der Chipkarte befindet. Falls die Verschlüsselung der Daten hingegen – wie in der Ausführungsform gemäß Fig. 2 – auf dem Kryptochip der Chipkarte erfolgt, so benötigt das Datenerfassungsgerät den geheimen Schlüssel (SK) nur dann, wenn es Daten, die von dem Computer zum Datenerfassungsgerät in verschlüsselter Form übermittelt werden, wieder entschlüsseln muß.

[0084] Anschließend werden die Daten mit Hilfe des geheimen Schlüssel (SK) im Datenerfassungsgerät verschlüsselt, mit einer digitalen Unterschrift versehen (**604**) und an den Computer übermittelt (**605**). Falls ein Anwendungsprogramm, das auf dem Computer des Benutzers betrieben wird, die Daten weiterverarbeiten soll (Überprüfung in Schritt **606**), so erfolgt zunächst die Entschlüsselung der Daten (**607**) mit Hilfe des öffentlichen Schlüssels. Nach der Weiterverarbeitung der Daten (**608**) werden die Daten erneut mit Hilfe des öffentlichen Schlüssels verschlüsselt und mit einer digitalen Unterschrift versehen (**609**). Vor der Übermittlung der Daten (**610**) an den anderen Rechner kann optional eine Abfrage erfolgen, ob eine Betriebsstörung vorliegt, wie etwa eine Störung auf der Übertragungsleitung oder ein Fehler im Chipkartenlesegerät. Sollte eine Betriebsstörung vorliegen, so erfolgt entweder – wie im allgemeinen Zustandsübergangsdiagramm in Fig. 4 dargestellt – ein völliger Abbruch der Datenübermittlung oder aber eine Übermittlung der Daten in unverschlüsselter Form (**613**).

[0085] War hingegen die Überprüfung der Benutzeridentität in Schritt **602** nicht erfolgreich, so bleibt das Datenerfassungsgerät im Klartext-Betriebszustand, so daß die Übermittlung der Daten sowohl an den Computer (**612**) als auch an den anderen Rechner (**613**) unverschlüsselt erfolgt.

[0086] Fig. 7 zeigt eine weitere Ausführungsform des Datenerfassungsgerätes, das eine Rückkopplung zwischen dem angeschlossenen Computer und dem Datenerfassungsgerät ermöglicht. Diese Rückkopplung gewährleistet, daß der Benutzer die Daten vor Ihrer Übermittlung von dem Computer zu dem anderen Rechner auf einem Bildschirm des Datenerfassungsgeräts nochmals überprüfen kann. Stimmen diese Daten mit denjenigen Daten überein, die von dem Datenerfassungsgerät oder einem Peripheriegerät (PG) erfaßt, von dem Benutzer eingegeben oder von diesem in einem Anwendungsprogramm ausgewählt worden sind, so autorisiert der Benutzer die Übermittlung der Daten. Weil das Datenerfassungsgerät sicher ist und eine nachträgliche Manipulation der mit einer digitalen Unterschrift versehenen authentischen Daten möglich ist, ist sichergestellt, daß die am anderen Rechner ankommenden Daten vom Benutzer abgesendet worden sind. Diese Daten können von dem anderen Rechner somit als rechtsverbindliche Grundlage für die Tätigung von Rechtsgeschäften verwendet werden.

[0087] Die in Fig. 7 angeführten Bezugszeichen, die mit denjenigen aus Fig. 5 übereinstimmen, wurden bereits im Zusammenhang mit Fig. 5 erläutert. Zusätzlich verfügt das Datenerfassungsgerät dieser weiteren Ausführungsform über eine Datendarstellungseinheit (**711**), die vorzugsweise ein LCD-Bildschirm oder ein berührungsempflindlicher bzw. Touch-Screen ist. Die Daten werden zum Zwecke der Autorisierung ihrer Übermittlung von dem Computer (**500**) zu dem Datenerfassungsgerät (**100**; **200**) über eine Verbindung (**710**) ebenfalls in authentischer Form zurückübermittelt. Verbindung **710** kann mit Verbindung **502** übereinstimmen. Zusätzlich kann das Datenerfassungsgerät über eine gesonderte Bestätigungstaste (**712**) zur Autorisierung der Datenübermittlung verfügen.

[0088] Bezugszeichen **707** stellt eine Dateneingabemaske, wie etwa eine Internet-Webseite oder dergleichen dar, in dessen html-Formular der Benutzer Daten eintragen soll. Eine weitere Möglichkeit ist die Auswahl von Daten aus einem Menü (**708**), etwa durch Zeigen und Auswählen mittels einer Computermaus (**709**).

[0089] Fig. 8 ist ein zur Ausführungsform gemäß

Fig. 7 zugehöriges Flußdiagramm. Dieses Flußdiagramm setzt den Betriebsablauf aus Fig. 6 ab Schritt **603** fort.

[0090] Zur Übermittlung der Daten an den Computer werden diese mit Hilfe des benutzerspezifischen geheimen Schlüssels verschlüsselt, mit einer digitalen Unterschrift versehen (**802**). Anschließend erfolgt die Übermittlung (**803**) an den Computer in authentischer Form. Dieser verarbeitet die empfangenen Daten weiter (**805**), wobei dem Verarbeitungsschritt analog zu dem Schritten **607** in Fig. 6 eine Entschlüsselung der Daten (**804**) vorangeht bzw. eine Verschlüsselung der Daten folgt (**806**). Anschließend werden die Daten wieder in authentischer Form an das Datenerfassungsgerät übermittelt (**807**), wo zunächst die Entschlüsselung der Daten erfolgt (**808**).

[0091] Anschließend wird der Benutzer aufgefordert, die Übermittlung der so an das Datenerfassungsgerät übermittelten Daten zu autorisieren (**809**). Hierzu werden die zu übermittelnden Daten auf der Datendarstellungseinrichtung (**711**) dargestellt. Zur Autorisierung betätigt der Benutzer entweder eine separate Bestätigungstaste (**712**) oder er betätigt eine Taste wie z.B. die "Enter"-Taste einer üblichen Tastatur.

[0092] In einer Ausführungsform verfügt das Datenerfassungsgerät über einen Pufferspeicher, der die erfaßten Daten zwischenspeichert. Bevorzugt werden in den Pufferspeicher Tastatureingabedaten gegeben. Bei einer Anwendung, bei welcher der Benutzer Daten in eine Eingabemaske eingeben muß, indem er beispielsweise einen Formulareintrag in einer html-Webseite vornimmt, werden die so eingegebenen und vom Computer in die Eingabemaske eingesetzten Daten über die Verbindung (**710**) an das Datenerfassungsgerät zurückübermittelt. Statt diese Daten nun auf dem Bildschirm darzustellen, können die zurückübermittelten Daten auch unmittelbar mit den im Pufferspeicher zwischengespeicherten Daten verglichen werden. Ist der Vergleich erfolgreich, so entspricht dies einer Autorisierung der Übermittlung durch den Benutzer (**809**).

[0093] Anschließend werden die Daten im Datenerfassungsgerät wieder verschlüsselt (**810**) und in authentischer Darstellung an den Computer und von diesem an den anderen Rechner übermittelt (811). Optional kann wieder eine Überprüfung im Hinblick auf etwaige Betriebsstörungen erfolgen, was zum Abbruch der Übermittlung und zum übergang in die Klartext-Betriebsweise des Datenerfassungsgerätes (**612**) führt.

[0094] Somit ist ein Verfahren und eine Vorrichtung zur Erfassung von Daten und deren Übermittlung in authentischer Form gefunden worden. Somit kann ein größtmöglicher Sicherheitsstandard bei der Erfassung von Daten und deren Übermittlung gewährleistet werden. Die übermittelten Daten können aufgrund des vorteilhaft hohen Sicherheitsstandards insbesondere als rechtsverbindliche Grundlage für die Tätigung von Geschäften jedwelcher Art oder als authentischer bzw. glaubwürdiger Nachweis von Dokumenten oder Ereignissen, die von den Daten dargestellt werden.

[0095] Um die Erfindung noch umfassender aufzuzeigen, werden zusätzlich noch folgende zwei Varianten angeführt und ein weiteres konkretes Ausführungsbeispiel angegeben:

Variante 1:

1 Einführung

[0096] Elektronische Medien gewinnen gegenwärtig zunehmend eine wesentliche Bedeutung im Rahmen der Informationsrepräsentanz und Kommunikation der Menschen. Diese Technik zeichnet sich durch große Flexibilität, Informationsvielfalt, hohe Aktualität und Geschwindigkeit sowie relativ einfache Verfügbarkeit aus.

[0097] Aufgrund der Architektur und Implementierung der Transportprotokolle werden derzeit öffentlich zugänglichen Computernetzwerke in der Regel nur zum offenen Informationsaustausch genutzt werden. Da sich jeder für jeden ausgeben kann und die durch die Netze transportierten Daten sehr einfach durch dritte unrechtmäßig verändert werden können, bleibt es den Anwendern versagt rechtsverbindliche Dokumente auszutauschen.

[0098] Um Geschäfte über das Netz tätigen zu können, ist es notwendig über eine Technik zu verfügen, mit der die Authentizität der erfaßten und übermittelten Daten nachgewiesen werden kann. Das bedeutet, daß man in der Lage ist, die Herkunft und Unverfälschtheit eines elektronischen Dokument nachweisen zu können.

2 Gegenstand der zu schützenden Idee

[0099] Grundidee ist, Daten bei ihrem digitalen Entstehungsprozeß – bei ihrer Erfassung – zu fixieren. Das soll durch Datenerfassungsgeräte (wie z.B. Tastaturen, Scanner, Kartenleser von Zugangskontrollsystemen usw.) von Rechnersystemen bewerkstelligt werden, die durch kryptographische Verfahren die Darstellung der Daten derart umwandeln, so daß die Authentizität der erfaßten Daten nachgewiesen werden kann. Vorteil dieses Ansatzes ist es, daß die Geräte, die Daten übermitteln nicht notwendiger Weise sicher sein müssen, damit der Nachweis der Authentizität geführt werden kann. Sicher muß das Datenerfassungsgerät und die Verarbeitungseinheit sein, auf der Nachweise der Authentizität geführt wird.

3 Zielsetzung

[0100] Bereitstellung authentischer Daten durch ein Datenerfassungsgerät die eindeutig einer Person zugeordnet werden können. Die durch das Gerät erfaßte Daten werden durch kryptographische Verfahren im Datenerfassungsgerät transformiert. Die kryptographisch modifizierte Datendarstellung wird an andere Geräte oder Verarbeitungseinheiten weitergegeben. Durch die umgewandelte Darstellung der Daten ist es möglich:

- eine Veränderung an den vom Datenerfassungsgerät übergebenen Daten festzustellen
- die Daten einer Person und/oder dem Datenerfassungsgerät eindeutig zuzuordnen.

4 technische Realisierung

[0101] Das Datenerfassungsgerät z.B. Tastatur besitzt neben den technischen Vorrichtungen zum Erfassen der Daten

1. eine Einheit, um die benutzerspezifischen Daten (Benutzerschlüssel) entgegen zu nehmen und optional auf ihre Rechtmäßigkeit zu prüfen z.B. Chipkartenleser und (optional) Fingerprintscanner.
2. eine passive oder aktive Verschlüsselungseinheit (Firmware mit Verschlüsselungsalgorithmen oder Verschlüsselungshardware).
3. optional: eine Weltweit eindeutige Identität mit einem unveränderbaren Zeiteinheitenmesser.

[0102] Die genannten Einheiten können miteinander und/oder mit dem Datenerfassungsgerät untrennbar oder trennbar verbunden sein. Für größtmögliche Sicherheit erscheint es jedoch sinnvoll alle Komponenten untrennbar in einem Gehäuse unterzubringen.

[0103] Das Gerät oder die Verarbeitungseinheit, die die Daten des Datenerfassungsgerätes erhält besitzt einen speziellen Treiber, der

1. die Daten wieder in eine Klartextdarstellung (verarbeitbare Darstellung) zurücktransformiert,
2. (optional) einen Datenaustausch mit dem Datenerfassungsgerät ermöglicht, durch den eine Assoziierung der eingelesenen Daten und Daten von der Verarbeitungseinheit durch die Verschlüsselungseinheit ermöglicht.

5 Funktionsweise (am Beispiel einer Tastatur)

[0104] Der Bediener steckt seine Chipkarte (Träger seines spezifischen Geheimnisses) in den Kartenleser der Tastatur (könnte beispielsweise auch nur ein Paßwort eingeben, ist aber relativ unsicher). Die Tastatur sendet daraufhin nur noch verschlüsselte Daten an den Rechner. Der Tastaturtreiber entschlüsselt die erhaltenen Daten und stellt je nach Anforderung die authentische oder Klartextversion zur Verfügung.

[0105] Bei Anwendungen kann der Bedarf bestehen, Daten von Anwendungsprogrammen mit den Benutzereingaben zu assoziieren. Dazu muß die Applikation dem Eingabegerät seine Integrität nachweisen. Ist der Beweis erfolgreich, übergibt die Anwendung dem Tastaturtreiber die zu assoziierenden Daten verschlüsselt. Die Daten werden durch den Treiber an das Dateneingabegerät weitergeleitet, das durch seine Verschlüsselungseinheit die Anwendungsdaten mit den vom ihm erfaßten Daten assoziiert. Ist keine Karte eingelegt, so funktioniert die Tastatur wie eine gewöhnliche.

5.1 Allgemeine Funktionsmodie für Datenerfassungsgeräte

1. Das Gerät liefert nur kryptische Daten wenn ein benutzerspezifisches Geheimnis vorliegt, sonst normale Daten. Anwendung bei z.B. Scanner, Tastatur, Kartenleser bei Zugangskontrollsystemen (Zeitwirtschaft, Objektschutz usw.)
2. Das Gerät liefert immer kryptische Daten ob ein Benutzergeheimnis vorliegt oder nicht. Anwendung bei z.B. Kartenleser bei Zugangskontrollsystemen (Zeitwirtschaft, Objektschutz usw.)
3. Das Gerät liefert nur Daten (kryptisch oder normal), wenn ein Benutzergeheimnis vorliegt. Sonst versagt es den Dienst. Anwendung bei z.B. Scanner, Tastatur.

5.2 Option: Beweis der Rechtmäßigkeit der Kartennutzung

[0106] Bei Gebrauch von Chipkarten kann es sinnvoll sein, den Besitzer der Karte nachweisen zu lassen, daß er die Karte rechtmäßig benutzt. Hierzu wird der Benutzer nach dem Einlegen der Karten durch ein Signal aufgefordert einen oder mehrere Finger auf den Fingerprintscanner zu legen. Die Daten der Fingerabdrücke dienen mit den Daten die auf der Karte verfügbar sind zu Beweis der Rechtmäßigkeit.

6 Unterschiede zu bisherig verfügbaren Systemen

[0107] Die Transformierung der Daten kann nicht dynamisch ein- und abgeschaltet werden. Ist das Geheimnis bzw. Rechtmäßige Nutzung des Geheimnisses des Benutzers bewiesen, verlassen das Gerät nur noch authentische Daten.

[0108] Existierende Verfahren verwenden eine dynamische Ein- und Ausschaltung der kryptographischen Datendarstellung. Befindet sich aber auf der "unsicheren Verarbeitungseinheit" ein Virus, Wurm oder eine sonstige Manipulation, so besteht die prinzipielle Möglichkeit die Darstellungsart zu einem Zeitpunkt zu wechseln, zu dem die eigentlichen Nutzdaten – deren Authenzität zu beweisen ist – ungeschützt (im Klartext) übertragen werden. Diese können dann illegitim verändert werden. Die Verände-

rung wäre nicht Nachweisbar. Nach der Änderung würde der Angreifer den Text mit der elektronischen Unterschrift des Autors versehen und Autor sowie Empfänger würden zunächst von der illegalen Beeinflussung keine Kenntnis erlangen. Eine weitere Spielart wäre, daß der Angreife die Beschaften Daten als seine eigenen gegenüber dem Empfänger ausgeben könnte.

Variante 2:

1 Einführung

[0109] Die breite Akzeptanz von Computern in der Geschäftswelt als auch im privaten Bereich ist mitunter auf die mehr oder minder einheitlichen und leicht bedienbaren Benutzerschnittstellen zwischen Mensch und Systemeinheit zurückzuführen. Der Erfolg eines Programm hängt nicht nur vom Leistungsumfang seiner Funktionen ab, sondern zunehmend auch vom Schnittstellendesign und der Handhabbarkeit. Gut gestaltete Benutzeroberflächen zeichnen sich durch intuitive, schnelle und vor allem sichere Bedienbarkeit aus. Dazu zählt insbesondere, daß die Eingabemasken nur sinnvolle Eingaben zulassen und den Anwender von Tipparbeit durch entsprechende Auswahlangebote entlasten.

[0110] Der beschriebene Ansatz zum authentischen Austausch von Daten über offene Kommunikations- und Datennetze geht davon aus, daß die Daten, deren Authentizität nachweisbar sein sollen, über die entsprechenden sicheren Eingabegräte erfaßt sein müssen. Es ist dem Anwender also nicht möglich, bereits verfügbare Daten auszuwählen und deren Authentizität sicherzustellen. Das in diesem Text beschriebene Gerät soll diesen Mangel beseitigen.

2 Gegenstand der zu schützenden Idee

[0111] Grundidee ist Daten nicht beim Entstehungsprozeß, sondern bei ihrem Kompositionsprozeß zu fixieren. Das bedeutet, man benötigt ein Gerät, mit dem die Authentizität von Daten festgestellt werden kann und das anschließend diese Daten in eine Darstellung umwandelt, deren Authentizität durch entsprechende kryptographische Verfahren leicht nachgewiesen werden kann.

[0112] Dazu soll eine erweiterte Form eines Bildschirms oder einer Tastatur dienen, der bzw. die die Einrichtungen besitzt, wie sie im oben genannten Schriftsatz beschrieben sind, und die darüber hinaus in der Lage ist, bidirektional Nutzdaten mit dem angeschlossenen Rechner auszutauschen. Außerdem existiert ein Weg, mit dem die vom Rechner übermittelten Daten sicher auf deren Korrektheit von dem Bildschirm bzw. der Tastatur oder dem Anwender überprüft werden können. Sind die Daten authentisch, so werden diese akzeptiert und mit weiteren Eingaben über die Tastatur oder anderen authentischen Daten in einer authentisch nachweisbaren Darstellung an den Rechner gesandt.

3 Zielsetzung

[0113] Gerät zur Bereitstellung authentischer Daten, die eindeutig einer Person zugeordnet werden können. Durch das Gerät selbst oder mit Hilfe des Gerätes kann die Korrektheit von Daten, die von einer unsicheren Datenquelle stammen, auf Authentizität geprüft werden. Authentische Daten von diesen Quellen können mit Daten aus sicheren Datenquellen verknüpft werden. Die Darstellung der produzierten authentischen Daten wird durch entsprechende kryptographische Verfahren transformiert – so daß deren Authentizität nachgewiesen werden kann – und verlassen das Gerät nur in dieser Darstellung. Das Gerät verlassen ausschließlich Daten, die authentisch sind.

4 Technische Realisierung

[0114] Die Realisierung dieses Gerätes ist in drei Varianten vorstellbar:

1. erweitertes Bildschirmgerät
2. erweiterte Tastatur
3. Kombination aus Bildschirmgerät und Tastatur

[0115] Das Gerät besitzt neben den Baugruppen seiner handelsüblichen Bauformen folgende technische Vorrichtungen:

- eine Einheit, um benutzerspezifische Daten zur Datentransformierung entgegenzunehmen.
- eine Einheit, um die Rechtmäßigkeit der Benutzung der benutzerspezifischen Daten zur Datentransformierung kontrollieren zu können.
- weltweit eineindeutige Identität mit einem unveränderbaren Zeiteinheitenmesser.
- optional: ein LCD Display zur direkten Kommunikation mit dem Anwender.
- bei der Tastatur: ein Scanner, mit dem bestimmte Teile auf dem Bildschirm gescannt werden können.
- beim Bildschirmgerät: eine Elektronik, mit welcher bestimmte Bildschirmbereiche in digitaler Form dargestellt werden können.
- eine Einheit, die die vom Rechner erhaltenen Daten verifiziert: z.B. spezieller Schalter auf der Tastatur oder Vergleichereinheit, die Daten vom Bildschirmscanner bzw. von der Bildschirmelektronik mit denen vom Rechner vergleicht.

[0116] Die naheliegenste Form der Realisierung scheint der Bildschirm zu sein, da hier die Daten hier dem Benutzer präsentiert werden. Man benötigt nun noch einen Tastatureingang und einen Tastaturausgang zum Rechner. Die bidirektionale Kommunikation ist durch das eingehende Videosignal und die Daten der Tastatur gegeben.

[0117] Die Mischform Tastatur – Bildschirm könnte derart ausgeführt sein, daß statt dem expliziten Displayscanner die Daten von der Bildschirmelektronik an die Tastatur gesandt werden.

[0118] Die Tastaturausführung ist in einer einfachen Form denkbar: die vom Rechner erhaltenen Daten werden auf dem LCD-Display angezeigt, und der Benutzer kontrolliert diese. Befindet er die Daten als korrekt, quittiert er diese durch eine entsprechende Tastaturbedienung.

[0119] Eine aufwendigere Form mit Hilfe eines Bildschirmscanners werden die Bildschirmdaten erfaßt und direkt an die Tastatur gesandt, die die Überprüfung vornimmt.

5 Funktionsweise

[0120] Die Ausführungen werden durch die Authentizitätskontrolle der am Bildschirm ausgewählten Daten erweitert. Das Programm schickt die ausgewählten Daten zum Gerät, das die Bildschirmdarstellung in einem definierten Bereich so lange nicht ändert, bis es vom Gerät die Daten in authentischer Darstellung zurück geliefert bekommt. Das Gerät scannt den Bildschirm und überprüft die aus dem Scannvorgang gewonnen Daten mit denen, die es vom Rechner erhalten hat. Stimmen die Daten überein, werden diese in ihrer Darstellung transformiert und wieder an den Rechner gesandt. Für Daten von sicheren Geräten entfällt dieser Überprüfungsvorgang.

Konkretes Anwendungsbeispiel für das ADG (DATENERF. GERÄT)

[0121] Gegenstand der Idee ist es, ein Datenerfassungsgerät zu Verfügung zu haben, das nur authentische Daten an den Rechner liefert. Das Datenerfassungsgerät und die SKIA wird als sicher (also vertrauenswürdig) betrachtet, alles andere als unsicher!

[0122] Um die Authentizität sicherzustellen sind folgende Punkte zu gewährleisten (bereits bekannte Verfahren):

– keine Person kann eine Identität annehmen, die einer anderen Person zugeordnet ist,

– die Daten besitzen eine Repräsentanz, die es zuläßt, daß Manipulationen festgestellt werden können.

[0123] Anhand eines konkreten Beispiels (Bankkunde, der eine Überweisung tätigt) soll die Funktionsweise des ADG erklärt werden:

Vorbereitung:

1. Die Bank erzeugt einen privaten und einen öffentlichen Schlüssel für einen Kunden, dessen Identität in Form von Merkmalen (Name, Adresse, Geburtsdatum usw.) mit diesen Schlüsseln bei der Bank assoziiert werden.
2. Der private Schlüssel wird auf einer Eurochequekarte mit einem Chip übertragen. (Dieser Schlüssel kann erst nach Nachweis der Identität des Kunden gelesen werden, z.B. Paßwort, Fingerabdruck, usw. Dieser Nachweis für die Identität kann nicht explizit ausgelesen werden, sondern wird über ein sogenanntes zero-knowledge Verfahren überprüft.)
3. Der Kunde erhält seine Eurochequekarte.

[0124] Die Bank übernimmt die Aufgabe der Paßstelle (SKIA = Secure Key Issuing Authority)

Überweisung:

1. Der Kunde steckt seine Eurochequekarte in die Tastatur
2. Die Tastatur prüft die Gültigkeit der Karte
3. Der Kunde wird durch ein Signal aufgefordert, seine rechtmäßige Nutzung der eingelegten Ewochequekarte nachzuweisen, z.B. durch Eingabe eines Paßwortes, Auflegen eines oder mehrerer Finger auf einen in der Tastatur eingebauten Scanner, usw.
4. Kann die korrekte Identität (also die Rechtmäßigkeit der Kartennutzung) nachgewiesen werden, wird der Kryptoeinheit in der Tastatur der geheime Schlüssel des Kunden zur Verfügung gestellt. Außerdem erhält die Tastatur den öffentlichen Schlüssel. (Eine noch sicherere Alternative wäre, daß der Chip auf der Karte die kryptographischen Aufgaben über nimmt und nur den öffentlichen Schlüssel an die Tastatur übergibt.)
5. Der öffentliche Schlüssel wird dem angeschlossenen Rechner übergeben, dessen spezieller Tastaturtreiber die Transformierung der von der Tastatur erhaltenen Daten in die übliche Darstellung vornimmt.
6. Alle Daten, die vom Kunden über die Tastatur eingegeben werden, werden zunächst digital in der Tastatur unterschrieben (public-key Verfahren) und anschließend an den Rechner übermittelt. Der Tastaturtreiber stellt der Anwendungssoftware die Klartextversion (mit Hilfe des ihm zur Verfügung gestellten öffentlichen Schlüssels) sowie die authentische Version der Anwendungssoftware zu Verfügung.
7. Bei einer Übernahme von Daten durch Auswahloptionen der Software (z.B. Bankleitzahlen, Kontonummern von bereits getätigten Überweisungen, usw.) muß eine sichere Überprüfung (wie dargestellt) erfolgen, damit die Authentizität der Daten sichergestellt werden kann.

Patentansprüche

1.) Verfahren zur Erfassung von Daten und deren Übermittlung in einer authentischen Darstellung,

mit folgenden Schritten:
– Erfassung der Daten, die in einer authentischen Darstellung übermittelt werden sollen, mittels einer Datenerfassungseinheit im Datenerfassungsgerät (**100**, **200**),
– Speicherung der erfassten Daten in einem Pufferspeicher im Datenerfassungsgerät (**100**, **200**),
– Erfassung von benutzerspezifischen Daten sowie Authentifizierung des Benutzers mittels einer Identifikationseinheit im Datenerfassungsgerät (**100**, **200**),
– Verschlüsselung der Daten, die in einer authentischen Darstellung übermittelt werden sollen, mittels einer Datenverschlüsselungseinheit im Datenerfassungsgerät (**100**, **200**), wenn der Benutzer erfolgreich authentifiziert wurde,
wobei die Programmanweisungen des Datenerfassungsgeräts (**100**, **200**) ausschließlich in einem Festwertspeicher (ROM) des Datenerfassungsgeräts (**100**, **200**) oder einer in dieses einführbaren Chipkarte abgelegt sind,
– Übermittlung der verschlüsselten Daten mittels einer Datenübermittlungseinheit im Datenerfassungsgerät (**100**, **200**) an die Datenverarbeitungseinrichtung (**500**),
– Empfangen der verschlüsselten Daten mittels einer Datenempfangseinheit in der Datenverarbeitungseinrichtung (**500**),
– Entschlüsselung der verschlüsselten Daten mittels einer Entschlüsselungseinheit in der Datenverarbeitungseinrichtung (**500**),
– Ausgabe bzw. Weiterverarbeitung der entschlüsselten Daten in der Datenverarbeitungseinrichtung (**500**),
dadurch gekennzeichnet, dass zusätzlich folgende Schritte erfolgen:
– Übermittlung der Daten mittels einer Datenübermittlungseinheit in der Datenverarbeitungseinrichtung (**500**) an das Datenerfassungsgerät (**100**, **200**),
– Empfang der Daten durch das Datenerfassungsgerät (**100**, **200**),
– gegebenenfalls Entschlüsselung der empfangenen Daten durch das Datenerfassungsgerät (**100**, **200**),
– Vergleich der entschlüsselten Daten mit den im Pufferspeicher des Datenerfassungsgeräts (**100**, **200**) abgelegten Daten,
– Autorisierung der Daten bei Übereinstimmung oder Bestätigung der Richtigkeit der ausgegebenen Daten durch den Benutzer am Datenerfassungsgerät (**100**, **200**),
– Verschlüsselung der autorisierten Daten mittels einer Datenverschlüsselungseinheit im Datenerfassungsgerät (**100**, **200**) und
– Übermittlung der verschlüsselten Daten mittels einer Datenübermittlungseinheit im Datenerfassungsgerät (**100**, **200**).

2. Verfahren nach Anspruch 1, bei dem zur Erfassung der benutzerspezifschen Daten des Benutzers Daten erfasst werden, die auf einer Chipkarte gespeicheit sind.

3. Verfahren nach Anspruch 1 oder 2, bei dem zur Ermittlung der Identität des Benutzers Identifikationsdaten erfasst werden und überprüft wird, ob die benutzerspezifischen Daten und die Identifikationsdaten zueinander in einer Beziehung stehen, die für den Benutzer charakteristisch ist.

4. Verfahren nach Anspruch 3, bei dem die Identifikationsdaten und/oder benuttzerspezifischen Daten alphanumerische Zeichen sind.

5. Verfahren nach Anspruch 3, bei dem als Identifikationsdaten biometrische Daten erfasst werden, die von körperlichen Merkmalen und/oder Eigenschaften des Benutzers abgeleitet werden.

6. Verfahren nach einem der Ansprüche 1 bis 5, bei dem die Daten als optische Information in Form von bewegten Bildern oder von Standbildern erfasst werde.

7. Verfahren nach Anspruch 6, bei dem der Informationsgehalt der Daten durch elektronisches Filtern reduziert wird.

8. Verfahren nach einem der Ansprüche 4 oder 7, bei dem die Daten alphanumerische Zeichen darstellen, welche mit Hilfe eines optischen Buchstabenerkennungsverfahrens (OCR) aus den erfassten Daten ermittelt werden.

9. Verfahren nach einem der Ansprüche 1 bis 8 bei dem zur Erfassung der Daten akustische Daten erfasst werden.

10. Verfahren nach Anspruch 9,bei dein die Daten alphanumerische Zeichen darstellen, welche mit Hilfe eines Spracherkennungsverfahrens ermittelt werden.

11. Verfahren nach einem der Ansprüche 1 bis 10, bei dem zur Erfassung der Daten alphanumerische Zeichen über eine Tastatur eingegeben werden.

12. Verfahren nach einem der Ansprüche 1 bis 11, bei dem zur Erfassung der Daten eine Menüauswahl mit Hilfe einer Computermaus vorgenommen wird.

13. Verfahren nach Anspruch 12, bei dein zur Erfassung der Daten ein Formular auf einem Bildschirm dargestellt wird, in das die Daten über eine Tastatur eingegeben werden.

14. Verfahren nach Anspruch 12 oder 13, bei dem die erfassten Daten nur nach einen erfolgreichen Vergleich übermittelt werden.

15. Verfahren nach einem der Ansprüche 1 bis 14, bei dem die zu übermittelnden Daten auf einer

Darstellungseinrichtung eines Datenerfassungsgerätes dargestellt werden und der Benutzer die Übermittlung der Daten freigibt.

16. Verfahren nach einem der Ansprüche 1 bis 15, bei den die Daten zur Transformation in die authentische Datendarstellung verschlüsselt werden.

17. Verfahren nach einem der Anspruche 1 bis 16, bei dein die Daten mit, Hilfe eines asymmetrischen Verschlüsselungsverfahrens verschlüsselt werden.

18. Verfahren nach Anspruch 17, bei dem ein öffentlicher Schlüssel (public key) zum Verschlüsseln der Daten verwendet wird.

19. Verfahren nach Anspruch 18, bei dein der öffentliche Schlüssel auf der Chipkarte gespeichert ist.

20. Verfahren nach Anspruch 18, bei dem der öffentliche Schlüssel von einem anderen Computer bereitgestellt wird.

21. Verfahren nach Anspruch 20, bei dein ein sicherer Schlüssel (secure key) zum Verschlüsseln der Daten verwendet wird.

22. Verfahren nach Anspruch 21, bei dein der sichere Schlüssel auf der Chipkarte gespeichert ist.

23. Verfahren nach einem der Ansprüche 1 bis 22, bei dein die elektronischen Daten mit Hilfe eines digitalen Signaturverfahrens in die authentische Darstellung transformiert werden.

24. Verfahren nach einem der Ansprüche 1 bis 23, bei dem die Daten in authentischer Darstellung von einem Datenerfassungsgerät an einen Computer übermittelt werden.

25. Verfahren nach einem der Ansprüche 1 bis 24, bei dem die Daten über ein lokales Netzwerk (LAN) an einen anderen Rechner übermittelt werden.

26. Verfahren nach einem der Ansprüche 1 bis 24; bei dein die Daten über ein weiträumges Netzwerk (WAN) an einen anderen Rechner übermittelt werden.

Es folgen 9 Blatt Zeichnungen

Anhängende Zeichnungen

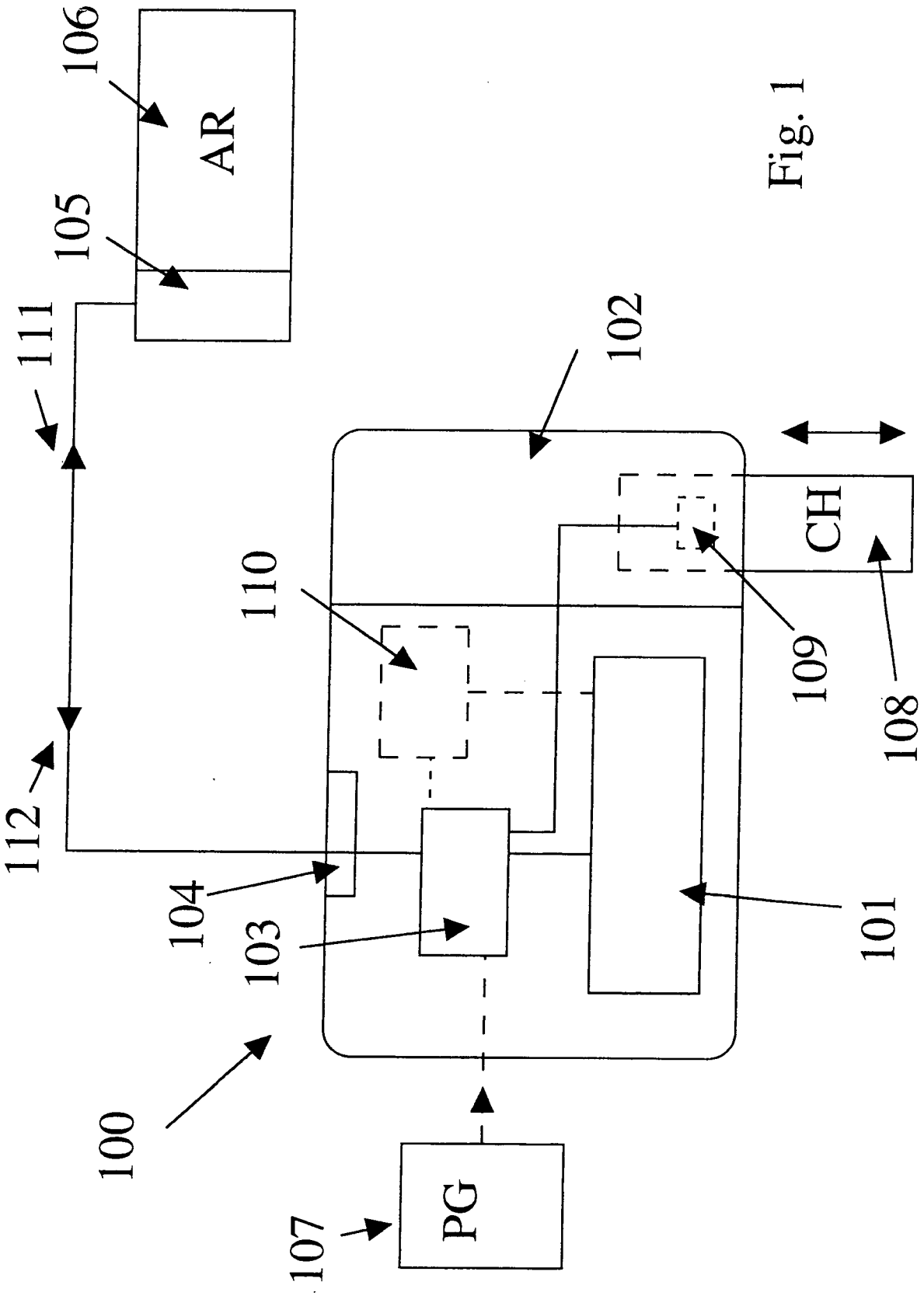


Fig. 1

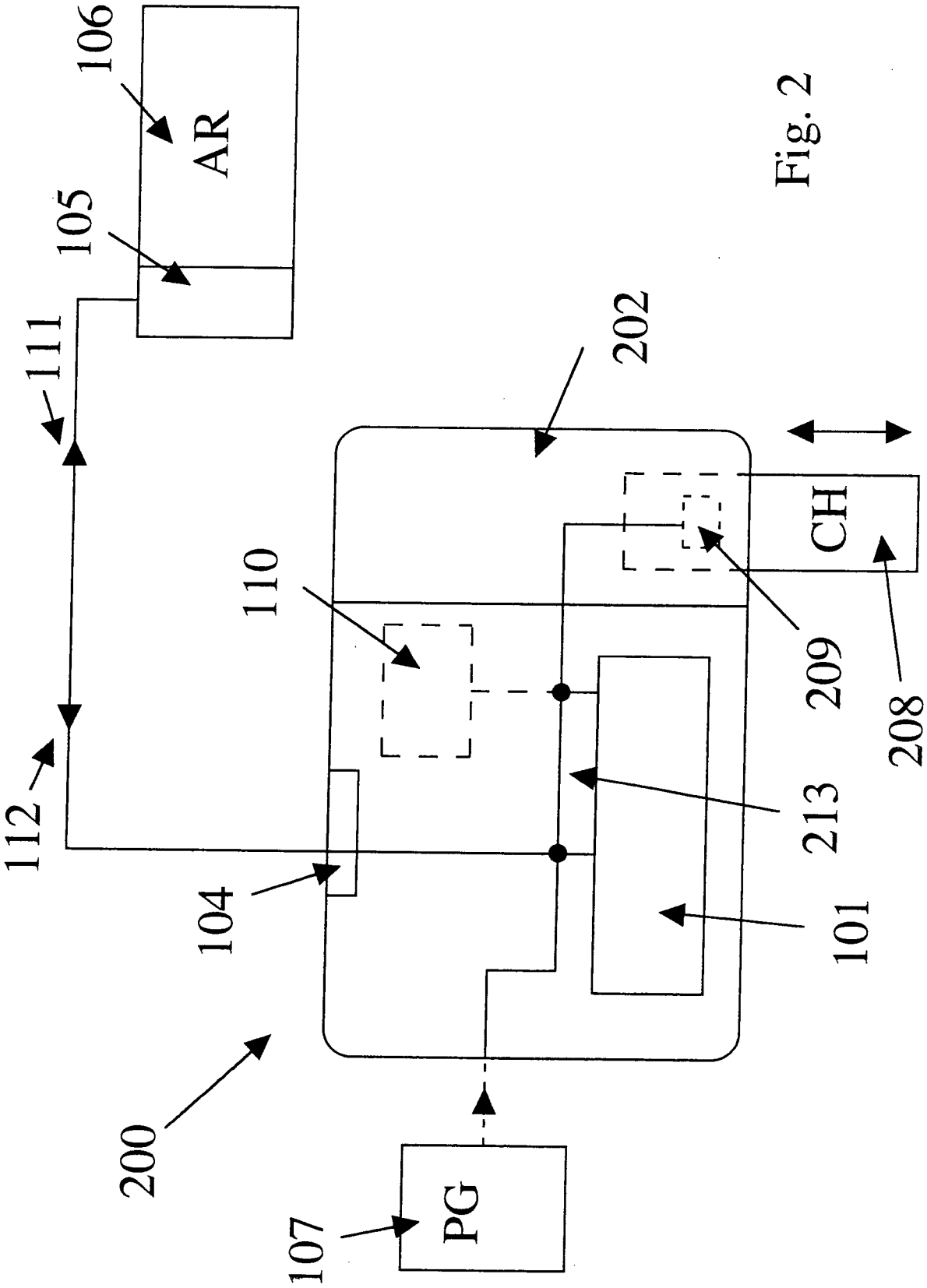


Fig. 2

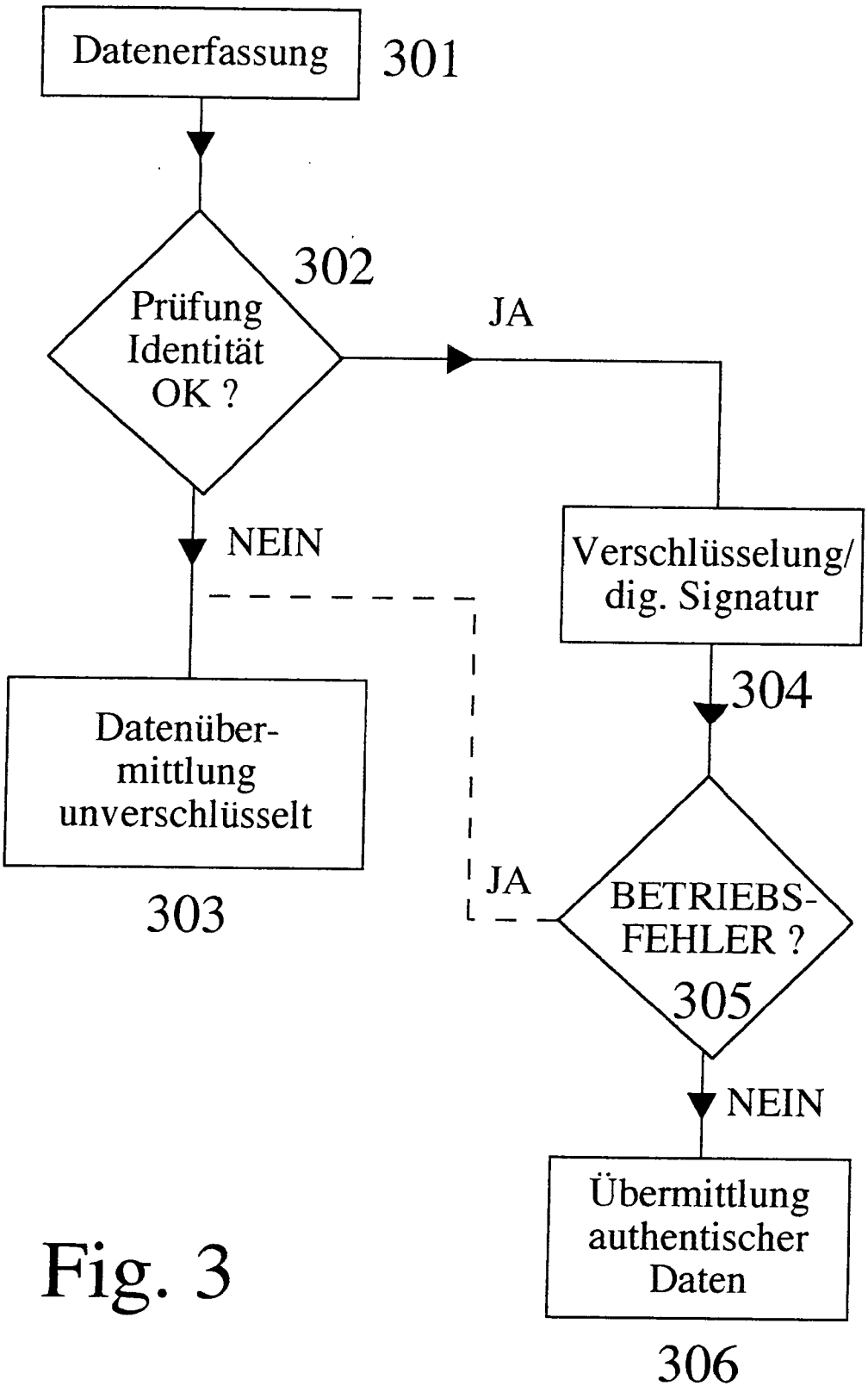

Datenerfassung
301
Prüfung Identität OK ?
302
JA
NEIN
Verschlüsselung/ dig. Signatur
304
Datenüber-mittlung unverschlüsselt
303
JA
BETRIEBS-FEHLER ?
305
NEIN
Übermittlung authentischer Daten
306

Fig. 3

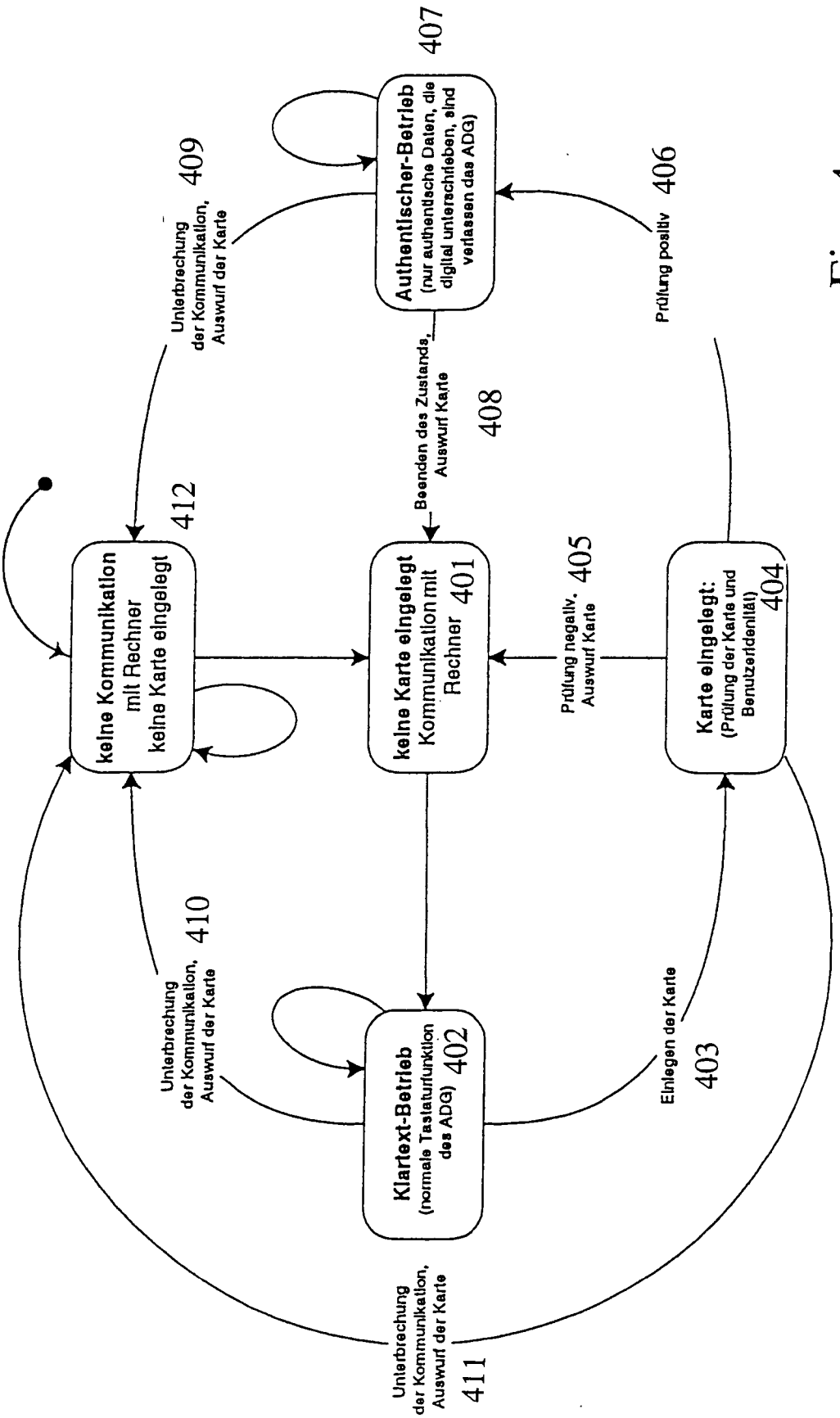

keine Kommunikation mit Rechner keine Karte eingelegt
412
keine Karte eingelegt Kommunikation mit Rechner
401
Karte eingelegt: (Prüfung der Karte und Benutzeridentität)
404
Klartext-Betrieb (normale Tastaturfunktion des ADG)
402
Authentischer-Betrieb (nur authentische Daten, die digital unterschrieben, sind verlassen das ADG)
407
Unterbrechung der Kommunikation, Auswurf der Karte
409
Beenden des Zustands, Auswurf Karte
408
Prüfung positiv
406
Prüfung negativ, Auswurf Karte
405
Einlegen der Karte
403
Unterbrechung der Kommunikation, Auswurf der Karte
410
Unterbrechung der Kommunikation, Auswurf der Karte
411

Fig. 4

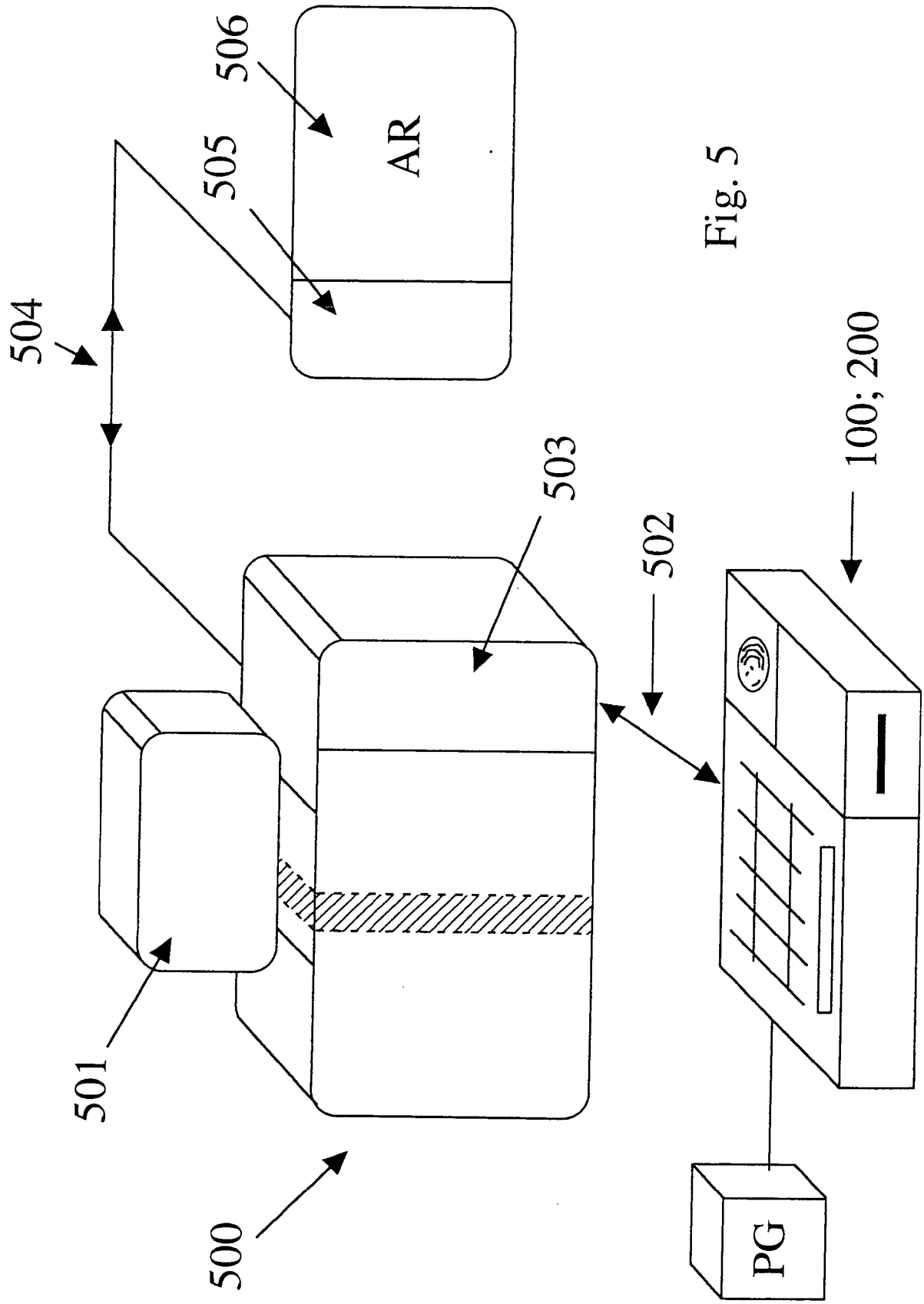


Fig. 5

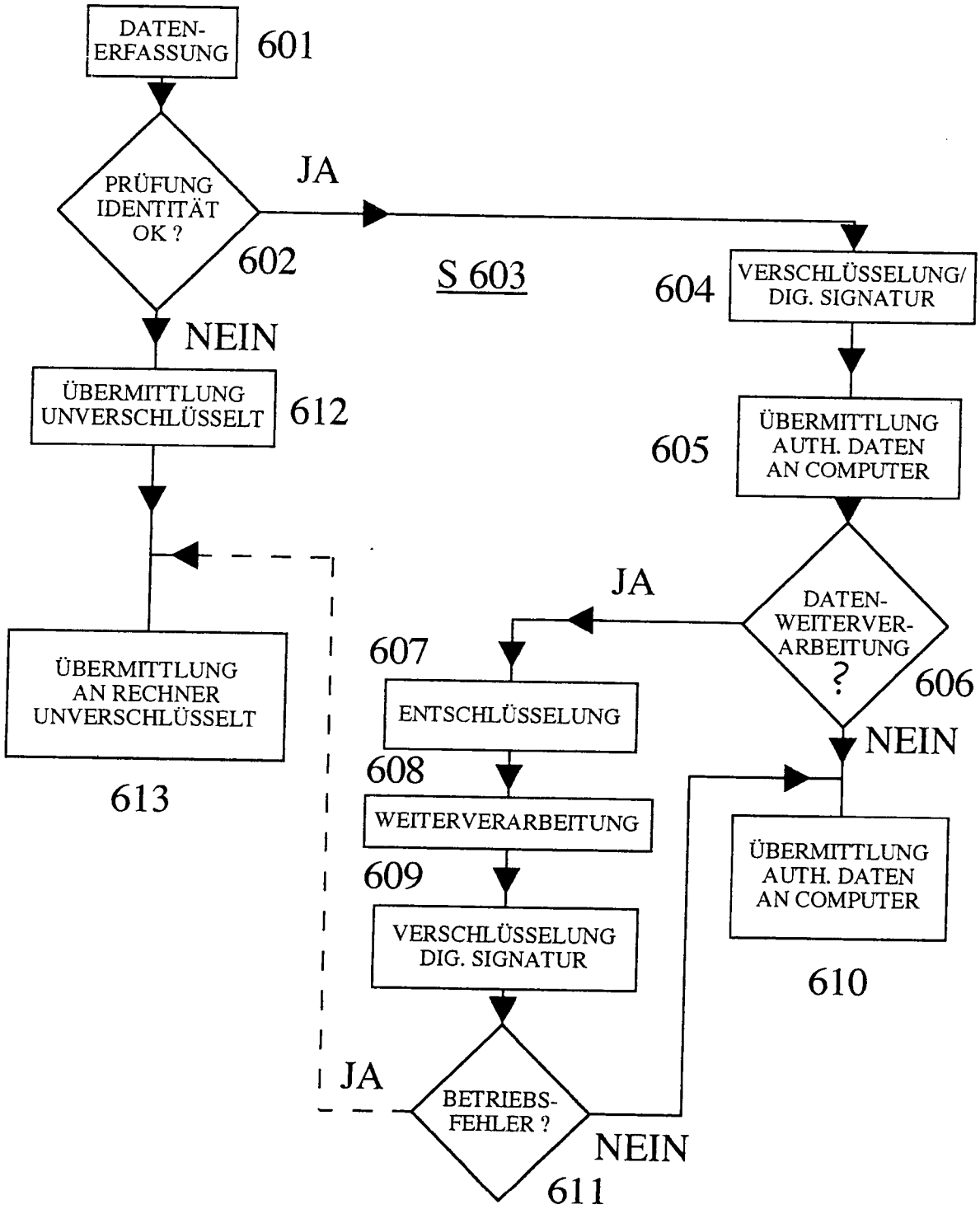

DATEN-ERFASSUNG
601
PRÜFUNG IDENTITÄT OK ?
602
JA
NEIN
S 603
VERSCHLÜSSELUNG/ DIG. SIGNATUR
604
ÜBERMITTLUNG AUTH. DATEN AN COMPUTER
605
DATEN-WEITERVER-ARBEITUNG ?
606
JA
NEIN
ÜBERMITTLUNG UNVERSCHLÜSSELT
612
ÜBERMITTLUNG AN RECHNER UNVERSCHLÜSSELT
613
607
ENTSCHLÜSSELUNG
608
WEITERVERARBEITUNG
609
VERSCHLÜSSELUNG DIG. SIGNATUR
BETRIEBS-FEHLER ?
JA
NEIN
611
ÜBERMITTLUNG AUTH. DATEN AN COMPUTER
610

FIG. 6

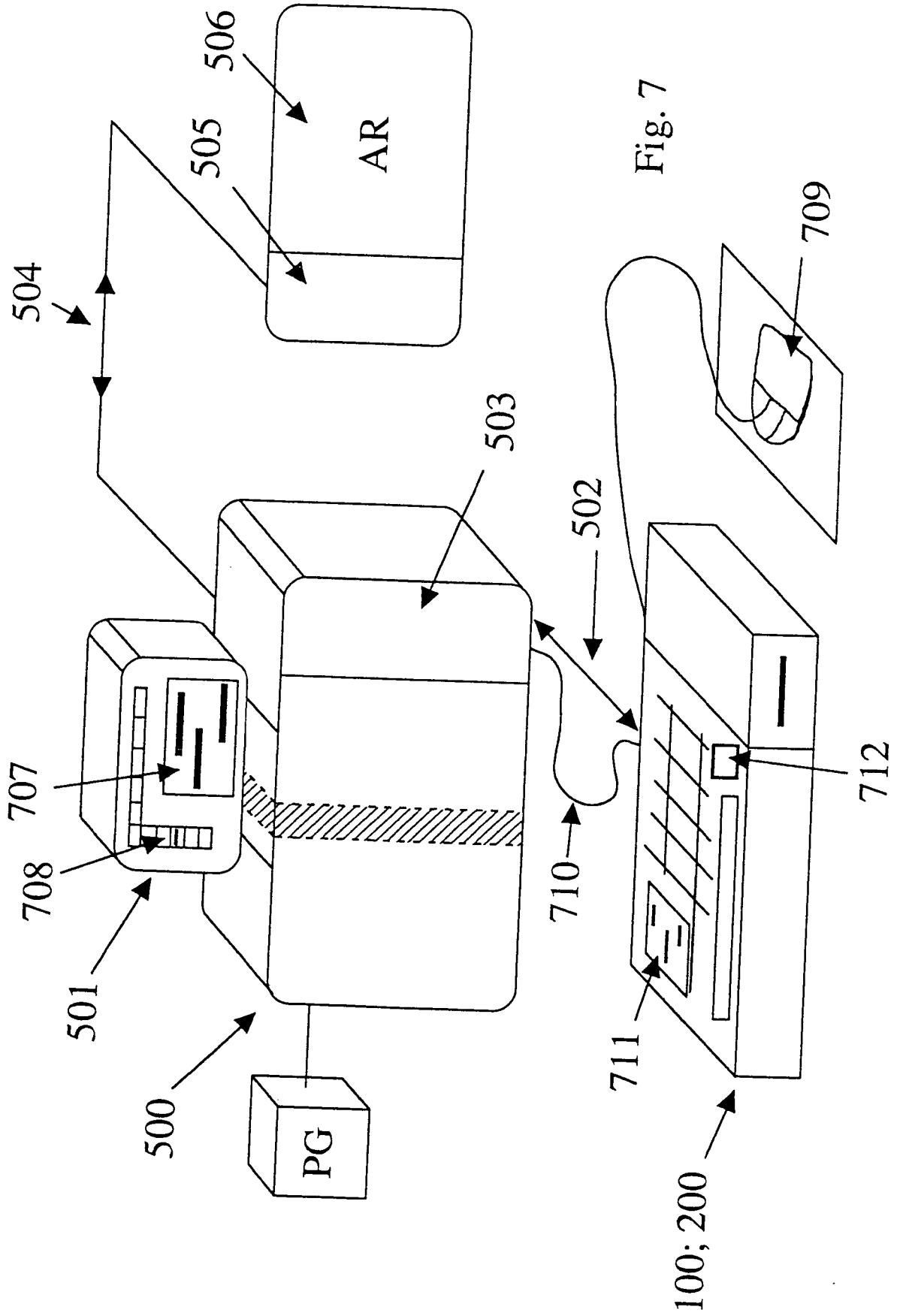


Fig. 7

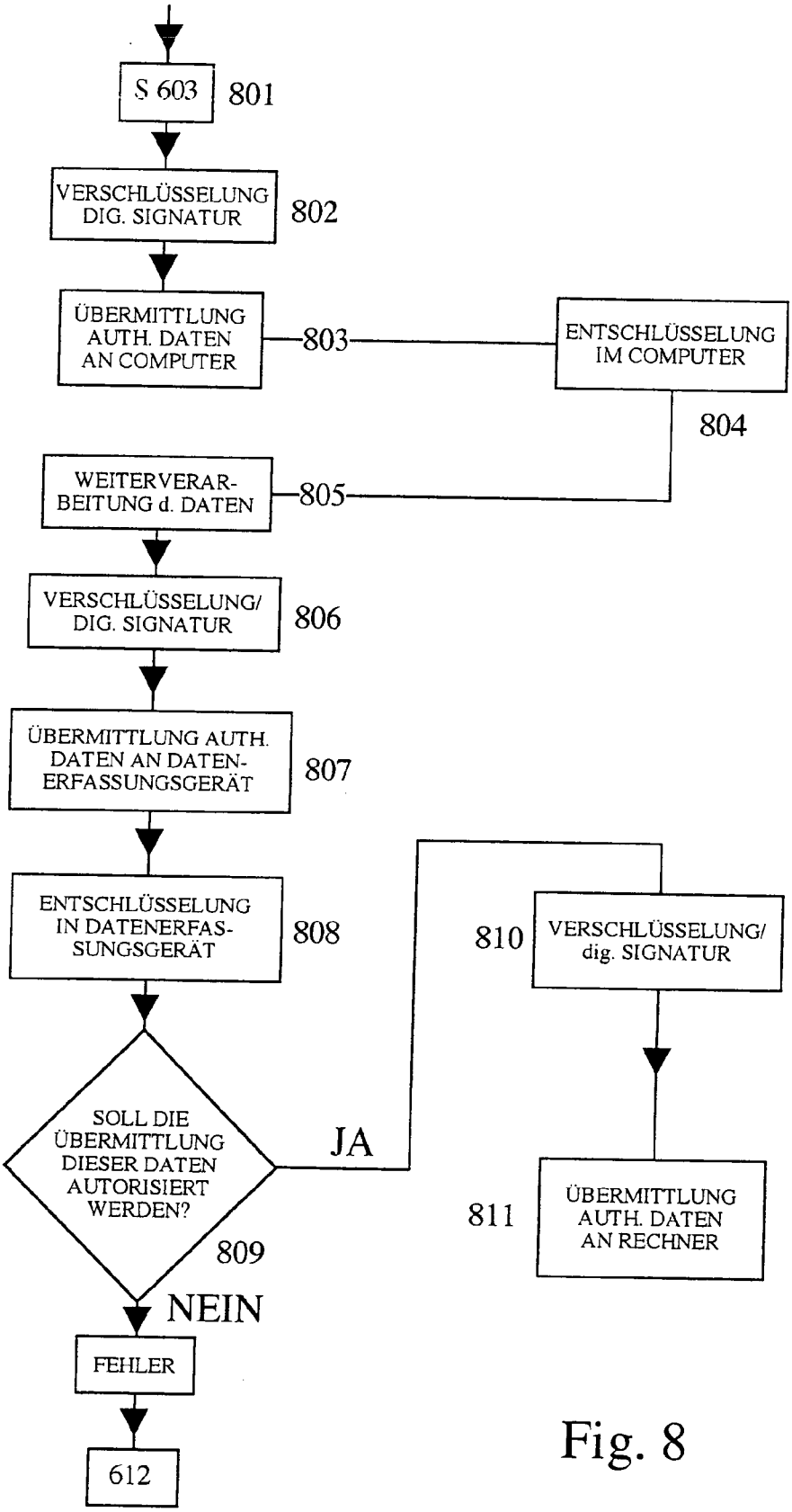

S 603
801
VERSCHLÜSSELUNG DIG. SIGNATUR
802
ÜBERMITTLUNG AUTH. DATEN AN COMPUTER
803
ENTSCHLÜSSELUNG IM COMPUTER
804
WEITERVERAR-BEITUNG d. DATEN
805
VERSCHLÜSSELUNG/ DIG. SIGNATUR
806
ÜBERMITTLUNG AUTH. DATEN AN DATEN-ERFASSUNGSGERÄT
807
ENTSCHLÜSSELUNG IN DATENERFAS-SUNGSGERÄT
808
SOLL DIE ÜBERMITTLUNG DIESER DATEN AUTORISIERT WERDEN?
809
JA
NEIN
810
VERSCHLÜSSELUNG/ dig. SIGNATUR
811
ÜBERMITTLUNG AUTH. DATEN AN RECHNER
FEHLER
612

Fig. 8

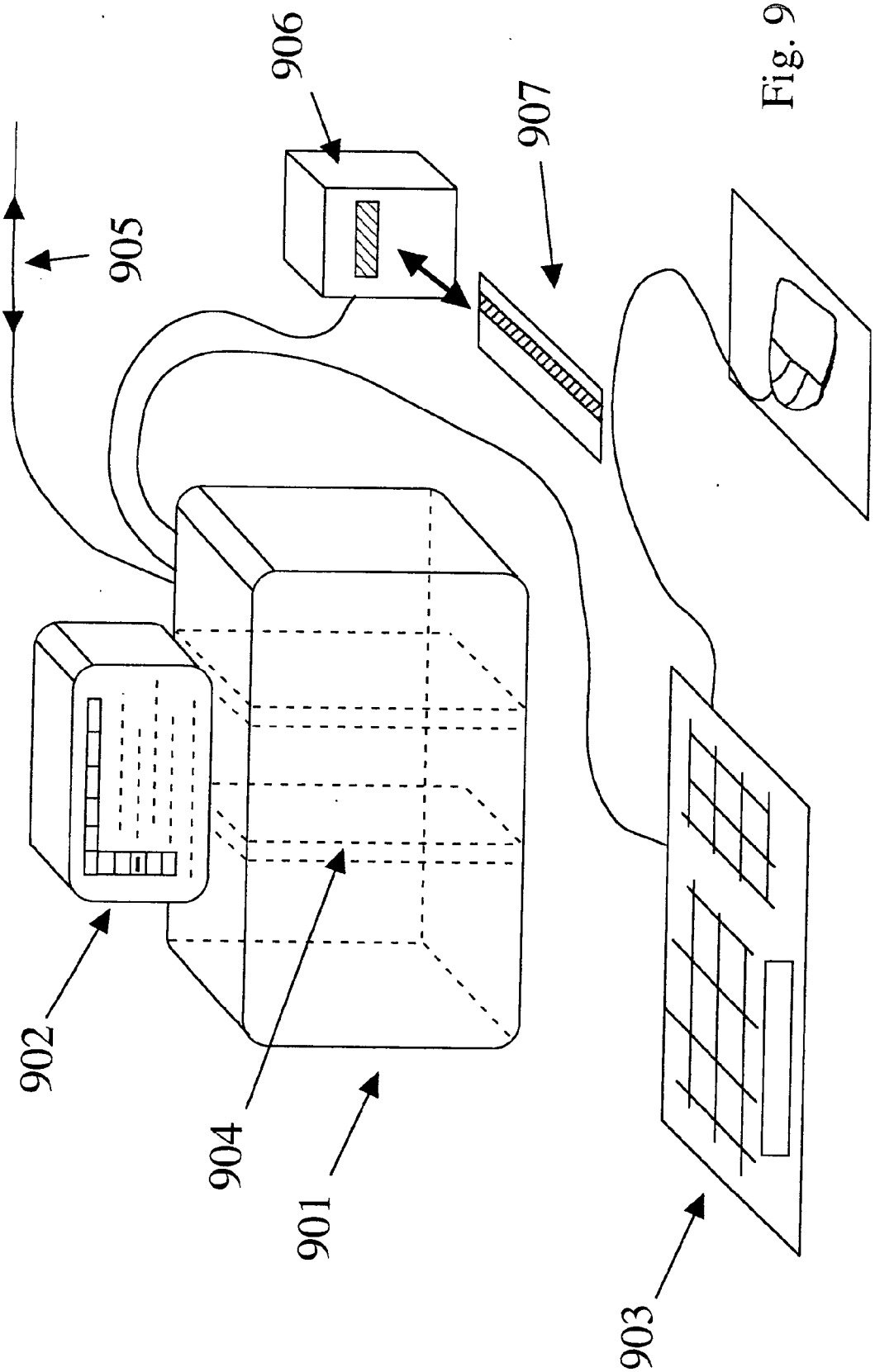


Fig. 9