(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 601 17 153 T2** 2006.11.02

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 312 033 B1**
(21) Deutsches Aktenzeichen: **601 17 153.5**
(86) PCT-Aktenzeichen: **PCT/IB01/01481**
(96) Europäisches Aktenzeichen: **01 963 288.4**
(87) PCT-Veröffentlichungs-Nr.: **WO 2002/015117**
(86) PCT-Anmeldetag: **17.08.2001**
(87) Veröffentlichungstag der PCT-Anmeldung: **21.02.2002**
(97) Erstveröffentlichung durch das EPA: **21.05.2003**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **08.02.2006**
(47) Veröffentlichungstag im Patentblatt: **02.11.2006**

(51) Int Cl.[8]: ***G06K 7/00*** (2006.01)

(30) Unionspriorität:
200004221 17.08.2000 ZA

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE, TR

(73) Patentinhaber:
Dexrad (Proprietary) Ltd., Parktown, ZA

(72) Erfinder:
TAME, Gavin Randall, 0181 Pretoria, ZA

(74) Vertreter:
Gleiss Große Schrell & Partner Patentanwälte Rechtsanwälte, 70469 Stuttgart

(54) Bezeichnung: **ÜBERTRAGUNG VON DATEN ZUR ECHTHEITSPRÜFUNG**

Beschreibung

HINTERGRUND DER ERFINDUNG

[0001] Diese Erfindung betrifft ein Verfahren und ein System zur sicheren Übertragung von Daten zur Echtheitsprüfung.

[0002] Smartcards werden auf Grund ihrer Fähigkeit, große Mengen von tragbaren Daten in einer sicheren und kompakten Art und Weise zu tragen, immer beliebter.

[0003] Insbesondere mit Bezug auf die Betrugsbekämpfung wächst auch zunehmend die Bedeutung von Verifikations- und Identifikationsfragen in der Smartcard-Technologie. Die meisten Anwender bevorzugen nach wie vor die Dokumentation auf Papierbasis und die mit einer derartigen Dokumentation verbundenen üblichen Verifikationsverfahren, so dass bestimmte Dokumentation wahrscheinlich niemals durch elektronische Formen ersetzt werden wird.

[0004] Ein weiteres Problem, das mit der Smartcard-Technologie verbunden ist, besteht darin, dass der Inhaber der Smartcard die Karte in seinem Besitz hat, was bedeutet, dass Institutionen wie etwa Banken nur bei Vorlage der Smartcard Zugriff auf die Daten zur Echtheitsprüfung haben. In vielen Fällen erschwert dies einer Institution den regelmäßigen Zugriff auf Sicherheitsdaten.

[0005] In vielen Ländern ist die multifunktionale Smartcard-Technologie bereits zur Verwendung mit Ausweisdokumenten und -karten akzeptiert. Es ist ein Ziel dieser Erfindung, die einfache Integration derartiger Ausweiskarten mit anderen Technologien für tragbare Datendateien sowie mit Dokumenten auf Papierbasis zu gestatten.

ZUSAMMENFASSUNG DER ERFINDUNG

[0006] Allgemein ausgedrückt zielt die Erfindung darauf ab, ein Verfahren zur Übertragung von Daten zur Echtheitsprüfung von einem ersten Träger auf zumindest einen zweiten Träger in einer sicheren Weise zu schaffen, so dass Daten auf dem zweiten Träger unabhängig verifiziert werden können.

[0007] Ein derartiges Verfahren wird allgemein in der FR-A-2 771 528 beschrieben. Dieser Stand der Technik wird im Oberbegriff der Ansprüche 1 und 17 gewürdigt.

[0008] In einem ersten Aspekt der Erfindung wird ein Verfahren zur Übertragung von Daten zur Echtheitsprüfung von einem ersten Träger, welcher eine tragbare Datenspeichereinrichtung ist, auf einen zweiten Träger geschaffen, wobei das Verfahren die Schritte umfasst: Verifizieren der Daten zur Echtheitsprüfung auf dem ersten Träger; Lesen der Daten zur Echtheitsprüfung mit einem Trägerleser; Sichern der Daten zur Echtheitsprüfung mit Verschlüsselungs- und/oder Komprimierungsmitteln; und Schreiben der Daten zur Echtheitsprüfung auf den zweiten Träger in einem maschinenlesbaren Format mit einem Kartenleser/-schreiber oder einem Drucker; dadurch gekennzeichnet, dass der Schritt des Verifizierens der Daten zur Echtheitsprüfung folgende Schritte umfasst: Steuern des Zugriffs auf den ersten Träger durch Verifizieren der Identität und/oder der Berechtigung eines Bedieners, der zur Implementierung zumindest des Leseschritts bestimmt ist; und Verifizieren der Identität des Inhabers des ersten Trägers, wobei die Schritte der Verifikation des Bedieners und des Inhabers PIN-/Passwort- und/oder auf Biometrie basierende Verifikationsverfahren umfassen.

[0009] In einer bevorzugten Ausführungsform der Erfindung umfasst das Verfahren die weiteren Schritte: Steuern des Zugriffs auf die Daten zur Echtheitsprüfung, die auf den zweiten Träger geschrieben sind, Lesen der Daten zur Echtheitsprüfung und Verifizieren der gelesenen Daten.

[0010] Der erste Träger kann eine erste Smartcard sein.

[0011] Der zweite Träger kann in ähnlicher Weise eine tragbare Datenspeichereinrichtung in der Form einer zweiten Smartcard sein.

[0012] Alternativ kann der zweite Träger ein Dokument umfassen, auf welches Daten zur Echtheitsprüfung in einem maschinenlesbaren Format, zum Beispiel durch Drucken, appliziert werden.

[0013] Der erste Träger kann ein zu einer Einzelperson gehörender identitätsbasierter Träger sein.

[0014] Die auf PIN/Passwort und auf Biometrie basierenden Verfahren werden vorzugsweise in Zusammenwirkung miteinander in einem Abgleichverfahren verwendet.

[0015] Der Sicherungsschritt kann die Schritte einschließen: Hinzufügen zusätzlicher Sicherheitsdaten zu den Daten zur Echtheitsprüfung und Komprimieren und Verschlüsseln der kombinierten Sicherheits- und Daten zur Echtheitsprüfung.

[0016] Der Schritt des Steuerns des Zugriffs auf die geschriebenen Daten zur Echtheitsprüfung auf dem zweiten Träger ist im Wesentlichen identisch mit dem entsprechenden Zugriffssteuerungsschritt in Bezug auf den ersten Träger.

[0017] In ähnlicher Weise ist der Schritt des Verifizierens der gelesenen Daten auf dem zweiten Träger

im Wesentlichen identisch mit dem entsprechenden Verifikationsschritt in Bezug auf den ersten Träger.

[0018] Das Verfahren kann noch die weiteren Schritte umfassen: Lesen der Daten zur Echtheitsprüfung von dem zweiten Träger und Schreiben der Daten zur Echtheitsprüfung auf einen dritten Träger in maschinenlesbarem Format.

[0019] Der zweite Träger ist typischerweise ein Dokument, auf welches die Daten zur Echtheitsprüfung in einem maschinenlesbaren Format appliziert werden, und der dritte Träger ist typischerweise eine tragbare Datenspeichereinrichtung wie zum Beispiel eine Smartcard.

[0020] Alternativ kann der zweite Träger eine tragbare Datenspeichereinrichtung sein, und der dritte Träger kann ein Dokument sein, auf welches die Daten zur Echtheitsprüfung in einem maschinenlesbaren Format appliziert werden.

[0021] Die Erfindung kann somit für die sichere Übertragung von Daten zur Echtheitsprüfung von einem ersten Träger auf einen n-ten Träger über n – 2 Träger sorgen, wobei jeder dazwischen liegende Datentransferschritt gesichert ist.

[0022] Die Erfindung erstreckt sich auch auf ein System zum Übertragen von Daten zur Echtheitsprüfung von einem ersten Träger, welcher eine tragbare Datenspeichereinrichtung ist, auf zumindest einen zweiten Träger in einer sicheren Weise, wobei das System Mittel zum Verifizieren der Daten zur Echtheitsprüfung auf dem ersten Träger, einen Trägerleser zum Lesen der Daten zur Echtheitsprüfung, Mittel zum Sichern der Daten zur Echtheitsprüfung, und einen Kartenleser/-schreiber oder einen Drucker zum Schreiben der Daten zur Echtheitsprüfung auf einen zweiten Träger in einem maschinenlesbaren Format einschließt; dadurch gekennzeichnet, dass das Mittel zum Verifizieren der Daten zur Echtheitsprüfung Mittel zum Steuern des Zugriffs auf den ersten Träger durch Verifizieren der Identität und/oder der Berechtigung eines Bedieners, der zur Implementierung zumindest des Lesens der Daten zur Echtheitsprüfung bestimmt ist; und Mittel zum Verifizieren der Identität des Inhabers des ersten Trägers umfasst, wobei das Mittel zum Steuern des Zugriffs auf den ersten Träger PIN-/Passwort- und/oder auf Biometrie basierende Verifikationsverfahren verwendet.

[0023] Vorzugsweise schließt das System des Weiteren Mittel zum Steuern des Zugriffs auf die Daten zur Echtheitsprüfung auf dem zweiten Träger in Bezug auf die Identität des Inhabers des zweiten Trägers, Mittel zum Lesen der Daten zur Echtheitsprüfung auf dem zweiten Träger und Mittel zum Verifizieren der gelesenen Daten zur Echtheitsprüfung auf dem zweiten Träger ein.

[0024] Das Sicherungsmittel schließt typischerweise Verschlüsselungs- und Entschlüsselungsmittel sowie Komprimierungs- und Dekomprimierungsmittel zum Komprimieren, Verschlüsseln, Entschlüsseln und Dekomprimieren der Daten zur Echtheitsprüfung ein.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0025] Fig. 1 zeigt ein schematisches Flussdiagramm einer ersten Ausführungsform eines Verfahrens zur Übertragung von Daten zur Echtheitsprüfung von einer ersten Smartcard auf eine zweite Smartcard;

[0026] Fig. 2 zeigt ein schematisches Flussdiagramm einer zweiten Ausführungsform eines Verfahrens zur Übertragung von Daten zur Echtheitsprüfung von einer ersten Smartcard auf ein Dokument;

[0027] Fig. 3 zeigt ein schematisches Flussdiagramm einer dritten Ausführungsform eines Verfahrens zur Übertragung von Daten zur Echtheitsprüfung, in welcher die Daten von einer ersten Smartcard auf eine zweite Smartcard über ein gesichertes Dokument übertragen werden; und

[0028] Fig. 4 ein herkömmliches Flussdiagramm, das die wichtigsten Schritte des Verfahrens zusammenfasst.

BESCHREIBUNG DER AUSFÜHRUNGSFORMEN

[0029] Die Erfindung wird nun anhand von drei Ausführungsformen beschrieben, welche verschiedene mögliche Anwendungen derselben veranschaulichen. Die erste Ausführungsform findet Anwendung bei der Ausstellung einer zweiten Smartcard, typischerweise durch eine Bank oder eine andere Finanzinstitution, an den Inhaber einer ersten Smartcard, welche typischerweise eine Ausweiskarte ist.

[0030] Unter Bezugnahme zuerst auf Fig. 1 wird eine erste Abfolge von Schritten zur Bediener-Zugriffssteuerung, Identifikation des Karteninhabers und Lesen der Smartcard schematisch in Block **10** veranschaulicht. Eine erste Smartcard in der Form einer Personalausweiskarte **12** wird einem Bediener einer Institution wie etwa einer Bank vorgelegt. Im ersten Schritt der Zugriffssteuerung ist die Verifikation des Bedieners erforderlich. Dies kann durch etliche Wege erreicht werden, entweder Verifizieren des PIN-Codes oder Passworts **14** des Bedieners oder durch Abgleichen des Fingerabdrucks **16** des Bedieners unter Verwendung von Fingerbiometrie. Naturgemäß ist der PIN-Code nicht so sicher wie das Verfahren zum Abgleichen des Fingerabdrucks, da es die Identität des Bedieners nicht sicherstellt. Wie bekannt, kann sich eine dritte Partei einen PIN-Code auf verschiedenen Wegen aneignen, so dass Biome-

trie bevorzugt wird.

[0031] Drei alternative Verfahren zur Verifikation der Fingerbiometrie des Bedieners wurden entwickelt. In dem ersten Verfahren, bekannt als "passwortgesteuertes Eins-zu-eins-Abgleichverfahren", gibt der Bediener das Passwort **14** in einen Computer ein und legt dann seinen Finger auf den Fingerabdruckscanner. Das Passwort dient als ein Suchschlüssel für den Datenbankeintrag, welcher die Fingerbiometrie des Bedieners enthält, und die biometrischen Daten von dem Live-Fingerscan werden mit den aus dem Datenbankeintrag abgerufenen Daten verglichen.

[0032] In dem zweiten Verfahren, bekannt als "Karte/Livescan-Fingerabgleichverfahren", ist der Bediener mit einer Zugangskarte ausgestattet. Diese Karte liegt entweder in der Form einer Smartcard oder einer Karte mit einem zweidimensionalen Strichcode vor, wobei die Fingerabdruckbiometrie in den maschinenlesbaren Daten der Karte enthalten ist. Um Zugriff zu erhalten, werden die von der Karte erhaltenen Fingerbiometriedaten mit den aus dem Live-Fingerscan abgeleiteten verglichen.

[0033] Das dritte Verfahren zur Identifikation der Fingerbiometrie umfasst ein Eins-zu-viele-Fingerabgleichverfahren. Dieses Verfahren ist der Art und Weise ähnlich, in der eine Anzahl von automatischen Fingerabdruck-Identifikationssystemen arbeitet. Ein Live-Fingerscan wird mit vielen in einer Datenbank registrierten Fingerabdrücken verglichen. Wenn eine Übereinstimmung auftritt, wird der Zugriff gewährt. Da viele Datenbankeinträge durchsucht werden müssen, werden die Fingerabdruckmuster üblicherweise klassifiziert, um die Suchzeit zu verringern. Dieses Verfahren ist typischerweise nur mit 150 oder weniger registrierten Benutzern wirklich praktisch. Eine Alternative dazu ist die Verwendung von Fingerabdruckscannern, die eine Firmware innerhalb des Scanners haben, welche einen biometrischen Livescan mit vielen Biometrien vergleichen kann, die innerhalb der Scannervorrichtung im Speicher abgelegt sind.

[0034] Sobald der Fingerabdruck **16** und/oder das Passwort **14** des Bedieners abgeglichen sind, werden die Daten aus der Bedienerdatenbank auf dem Computer protokolliert. Diese protokollierten Daten werden normalerweise zum Zweck der portablen Nachprüfbarkeit zu den von der Smartcard **12** gelesenen Daten hinzugefügt. Wenn eine positive Bedienerverifikation und -identifikation erfolgt ist, wird die Smartcard **12** in den an einen PC **22** angeschlossenen Smartcardleser **20** eingeführt. Anstelle eines herkömmlichen Desktop-PCs kann ein Laptop oder Notebook-PC, oder eine andere tragbare Rechnervorrichtung verwendet werden. Ein geheimer öffentlicher Schlüsselcode, der für den Zugriff auf die Daten der Smartcard erforderlich ist, wird im Verborgenen von dem Programm verwendet, um Zugriff auf die Daten der Smartcard des Benutzers zu erhalten sowie die Daten zur Echtheitsprüfung zusammen mit anderen Arten von Daten zu entschlüsseln.

[0035] Der nächste Schritt in dem Verfahren zur Echtheitsprüfung besteht darin, die Identität des Karteninhabers zu verifizieren. Die Natur des Verfahrens zur Verifikation der Identität hängt davon ab, welche Daten zur Echtheitsprüfung auf der Smartcard **12** verfügbar sind. In Fällen, in denen die Smartcard einfach einen PIN-Code oder Passwort für den Karteninhaber aufweist, gibt der Bediener oder vorzugsweise der Karteninhaber den PIN-Code auf der Tastatur des PCs ein, woraufhin der PIN-Code dann verifiziert wird. Vorzugsweise trägt die Smartcard ein digitalisiertes Porträtfoto und/oder ein digitalisiertes Unterschriftsbild. In diesem Fall werden diese auf dem Monitor des PCs **22** angezeigt, und die Identität des Karteninhabers wird visuell durch den Bediener bestätigt. Wenn Fingerabdruckbiometrie in den Daten zur Echtheitsprüfung verfügbar ist, kann diese mit einem Live-Fingerscan **28** des Karteninhabers verglichen werden. In diesem Fall erfolgt die Verifikation automatisch anstatt durch visuelles Abgleichen durch den Bediener, wie dies mit dem Porträtfoto **24** und Unterschriftsbild **26** der Fall war.

[0036] Nur in dem Fall der Verifikation von Bediener und Karteninhaber wird die Verifikation zum erneuten Schreiben einer zweiten Smartcard **30** verarbeitet, wie dies schematisch bei **32** angezeigt wird. Nun werden der Datenmenge, die auf die zweite Smartcard **30** geschrieben werden müssen, noch weitere Daten hinzugefügt. Diese Daten umfassen Details zum Bediener und mögliche hinzugefügte Verifikationsdetails, die von anderen Dokumentationen abgeleitet sind und welche die Institution verlangen mag. Dies sind beispielsweise Geldbeträge, Dauer und Ablaufdaten, Garantiedetails und dergleichen mehr. Auch Zeitstempel von Transaktionen können an die Daten angehängt werden.

[0037] Die von der ersten Smartcard gelesenen Daten werden nun zusammen mit den zusätzlichen erfassten Daten durch verschiedene Komprimierungstechniken komprimiert. Im Falle digitaler Bildkompression wird eine mit Verlust behaftete Komprimierungstechnologie verwendet. Diese kann entweder auf fraktaler oder Wavelet-Bildkompression basieren. Beide dieser Techniken komprimieren das Bild durch Herausfiltern der weniger relevanten Bildinformation, die weniger kritisch für das menschliche visuelle Identifikationsverfahren ist. Wenn die Daten nicht auf Bildern basieren, wird eine verlustfreie Komprimierung verwendet. Bei diesem Typ der Komprimierung, welche auf arithmetischer Kodierung basiert, werden keine Daten verworfen. Arithmetische Kodierung bietet die besten Komprimierungsverhältnisse, ist jedoch eine der langsamsten verlustfreien Komprimie-

rungstechnologien. Da die Datenmengen nicht besonders groß sind, ist diese Komprimierungstechnologie am besten geeignet. Unterschiedliche Datenelemente können unter Verwendung unterschiedlicher Verschlüsselungen komprimiert werden. Nachdem die Daten komprimiert wurden, werden sie erneut verschlüsselt, wobei der private Schlüssel der Institution (in diesem Fall der Bank) im Verborgenen von dem Programm verwendet wird, um die Daten erneut zu verschlüsseln.

[0038] Ein Verschlüsselungsschema mit privatem/öffentlichem Schlüssel wird verwendet. Der private Schlüssel kann nur verschlüsseln und ist keinem Bediener jemals bekannt. Der öffentliche Schlüssel kann die Daten nur entschlüsseln. Der öffentliche Schlüssel kann für die Entschlüsselung an vielen Stellen verteilt werden, wobei die private/öffentliche Verschlüsselung auf der RSA-Verschlüsselung basiert. Sowohl der private als auch der öffentliche Schlüssel werden üblicherweise aus digitalen Zertifikaten ermittelt, welche diese Schlüssel liefern, wenn die richtigen Passwörter eingegeben werden. Unterhalb der Schicht der öffentlichen/privaten Schlüssel liegen zwei weitere Verschlüsselungsschichten. Die eine Schicht erzeugt eindeutige Schlüssel aus der Eindeutigkeit der Daten der Datenmenge jeder Karte. Die andere Schicht verwürfelt bloß die Daten unter Verwendung einer Anzahl von Verwürfelungsalgorithmen.

[0039] Für zusätzliche Sicherheit wurde auch eine Technologie um den HASP-"Dongle" der Firma Aladdin entwickelt. Dies ist eine hochsichere Vorrichtung, welche an den parallelen, USB- oder seriellen Port des PCs angeschlossen ist und dazu verwendet wird, das digitale Zertifikat zu halten, welches den geheimen privaten und öffentlichen Schlüssel für die Verschlüsselung und Entschlüsselung von Daten liefert. Eine zusätzliche Alternative ist ein weiteres Produkt der Firma Aladdin, bekannt als "E-Token", das eine Vorrichtung ist, die an einen USB-Port eines PCs angeschlossen wird und welche insbesondere dafür entwickelt wurde, um Passwörter, Schlüssel und digitale Zertifikate für digitale Signaturen und Verschlüsselung mittels einer Infrastruktur für öffentliche Schlüssel zu liefern. Auf dem Dongle werden auch zusätzliche verwürfelte Codes zusammen mit Bedienerprotokolldaten gespeichert. Eine weitere Verwendung des HASP-Dongles besteht darin, ausführbare Programme dagegen zu schützen, dass sie beobachtet, manipuliert, kopiert oder auf einer anderen Maschine ausgeführt werden als die, für die sie registriert wurden. Dies wird durch eine Kombination aus geheimen Seed-Codes auf dem Dongle und einer das ausführbare Programm umgebenden Software erreicht.

[0040] Unter nochmaliger Bezugnahme auf den Schritt des Schreibens der Karte, der schematisch bei **32** dargestellt wird, wird nun die zweite Smartcard **30** in den Smartcardleser **20** eingeführt. Bevor die Daten auf die Smartcard **20** geschrieben werden können, wird ein weiterer Zugriff auf den privaten Schlüssel der Smartcard im Verborgenen durch das Programm durchgeführt. Sobald die Daten auf die Smartcard **30** geschrieben wurden, hat die Bank oder andere Institution die Merkmale zur Echtheitsprüfung, die ursprünglich auf der ersten Personalausweis-Smartcard **12** getragen wurden, auf der zweiten Smartcard **30** erfasst, sowie jegliche andere Daten, welche die Institution mit den erfassten Merkmalen zur Echtheitsprüfung kombiniert benötigen mag. Zusätzliche Details von anderen Institutionen können ebenfalls auf diese zweite Karte geschrieben werden.

[0041] Die nächste Stufe in dem Transferverfahren ist die Stufe zur Verifikation der bankeigenen Smartcard **30**, in welcher die Daten, die von der ersten Smartcard erfasst und auf die zweite Smartcard geschrieben wurden, abgerufen und verwendet werden. Dieses Verfahren ist schematisch in Block **34** dargestellt. Die Smartcard **30** wird in einen Smartcardleser **36** eingeführt, welcher an einen PC **38** angeschlossen ist. Wieder muss der Bediener die Verfahren zur Bediener-Verifikation/Zugriffssteuerung erfüllen, die oben unter Bezugnahme auf Block **10** beschrieben wurden. Nach positiver Bedieneridentifikation und -verifikation wird der öffentliche Schlüsselcode im Verborgenen an die Smartcard **30** übergeben, so dass Daten von der Smartcard gelesen werden können. Nach der Auslesung werden die Daten dann entschlüsselt, indem das Programm im Verborgenen ein Passwort an das digitale Zertifikat übergibt, welches den privaten Schlüssel für die Entschlüsselung der Daten liefert. Jeder Datentyp, ob bildbasiert oder nicht bildbasiert, wird dekomprimiert, sobald er entschlüsselt ist. Die dekomprimierten, entschlüsselten Daten werden dann derart auf dem Monitor des PCs angezeigt, wie bei **39** dargestellt, dass der Bediener die Identität des Karteninhabers **24** verifizieren kann. Im Fall von Fingerbiometrie legt der Karteninhaber einen Finger auf den Fingerscanner, wie bei **28** gezeigt, und die abgeleiteten biometrischen Daten werden in einem Eins-zu-eins-Abgleichverfahren mit jenen aus der Smartcard ausgelesenen verglichen, wobei die Verifikation automatisch erfolgt. Das Ergebnis der Verifikation kann zusammen mit den Details des Bedieners zum Zwecke der Nachprüfbarkeit protokolliert werden.

[0042] Unter Bezugnahme auf Fig. 2 wird nun eine zweite Ausführungsform eines Verfahrens zur Übertragung von Daten zur Echtheitsprüfung gezeigt. Die ersten Schritte der Bedienerzugriffssteuerung, Lesen der Smartcard und Verifikation und Identifikation des Karteninhabers sind identisch mit den in Fig. 1 illustrierten, wie jeweils in den Blöcken **40** bzw. **42** dargestellt. In Block **44** werden die Daten zur Echtheitsprü-

fung zusammen mit beliebigen zusätzlichen Daten wie etwa jene, auf die zuvor in Verbindung mit Fig. 1 Bezug genommen wurde, auf dieselbe Art und Weise, die in Verbindung mit Fig. 1 beschrieben wurde, komprimiert und verschlüsselt. Diese Daten werden dann in ein zweidimensionales Symbol oder Strichcode **46** kodiert. Der zweidimensionale Strichcode verfügt über eine Reed-Solomon-Fehlerkorrektur, welche eine vollständige Wiederherstellung im Fall einer teilweisen Zerstörung des Symbols ermöglicht. Das zweidimensionale Symbol kann entweder ein Bild auf der Grundlage zweidimensionaler Symbologie oder ein Font auf der Grundlage einer derartigen Symbologie sein. Es können im Handel verfügbare bildbasierte zweidimensionale Symbologien verwendet werden, einschließlich PDF417, Supercode, Aztec QR-Code und Datamatrix.

[0043] Es ist ersichtlich, dass derartige zweidimensionalen Symbole nicht auf herkömmliche Drucktechniken beschränkt sind, und zum Beispiel in Metalloberflächen geätzt, lasergraviert oder durch etliche andere Wege appliziert werden können. Die Verwendung anderer mehrdimensionaler maschinenlesbarer Codeformen, wie etwa gestapelte Strichcodes oder Matrix-Strichcodes, ist ebenfalls möglich.

[0044] Der Anmelder hat auch eine fontbasierte zweidimensionale Symbologie entwickelt, welche in Textform auf der Grundlage eines bestimmten Fontsatzes an einen Drucker gesendet werden kann. Ein besonders konstruierter TrueType-Font interpretiert den Text zeilenweise. Dieser Typ zweidimensionaler Symbologie kann auch im Massendruck verwendet werden, bei dem bildbasierte Symbole extremen Speicherbedarf haben und dazu neigen, Hochgeschwindigkeits-Produktionsverfahren zu verlangsamen. Dies bedeutet, dass die Daten zur Echtheitsprüfung, die von den Smartcards erhalten werden, in Massendruckeinrichtungen verwendet werden können, in welchen die Daten in zweidimensionalen Strichcodes integriert sind, die im Hochgeschwindigkeits-Massendruck gedruckt werden.

[0045] Der Anmelder hat auch eine zweidimensionale Symbologie entwickelt, die nicht kopiert werden kann, und die den Gegenstand der internationalen Patentanmeldung Nr. PCT/IB01/00362 bildet. Dies schafft zusätzlichen Schutz für die Daten zur Echtheitsprüfung innerhalb des zweidimensionalen Strichcodes oder Symbols **46** auf gedruckten Dokumenten, da es verhindert, dass derartige Symbole kopiert werden können.

[0046] Die von der Verifikations-Smartcard erhaltenen Daten werden in eines der oben erwähnten zweidimensionalen Symbole **46** kodiert, das dann auf ein Dokument **48**, wie etwa einen Scheck, aufgedruckt wird. Wenn das Dokument ein elektronisches Dokument ist, werden die gelesenen Daten in einem PC **50** elektronisch an das Dokument angehängt und dann über einen Drucker **52** gedruckt. Alternativ wird das Dokument, wenn es nicht elektronisch ist, in den Drucker **52** eingelegt, damit das Symbol **46** darauf gedruckt werden kann. Es kann auch ein Etikett, auf welches das Symbol aufgedruckt ist, an das Dokument angebracht werden. Nicht entfernbare Etiketten von dem Typ, der von der Firma 3M hergestellt wird, werden bevorzugt. Es ist manchmal einfacher, ein Etikett zu drucken und an dem Dokument anzubringen, insbesondere wenn man ein bereits bestehendes Dokument verifizieren möchte. Analoges gilt für ein elektronisch signiertes Papierdokument. Die Daten zur Echtheitsprüfung, die von der Verifikations-Smartcard erhalten werden, können mit zusätzlichen Daten kombiniert werden, die aus dem Dokument selbst abgeleitet werden, wie etwa Beträge oder Daten, die auf dem Dokument erscheinen, welche dann in die Daten, die in dem zweidimensionalen Symbol auf dem Dokument enthalten sind, einbezogen werden.

[0047] Unter Bezugnahme auf Block **54** findet nun ein Verifikationsverfahren statt, in welchem die Verifikationsdetails des Bedieners unter Verwendung eines in der Hand gehaltenen Scanners **56** gescannt, auf einem PC **58** entschlüsselt und unter Verwendung von Passwort- bzw. Fingerabdruck-Biometrie-Identifikationsmitteln **14** bzw. **16** verifiziert werden, wie zuvor unter Bezugnahme auf Block **34** von Fig. 1 beschrieben.

[0048] Der Scanner **56** kann entweder ein Laser- oder ein linearer zweidimensionaler CCD-Scanner, ein bildbasierter zweidimensionaler Scanner, oder ein Flachbettscanner sein. Wenn das Symbol von einem nicht reproduzierbaren Typ ist, muss ein spezieller Scanner verwendet werden, der in der Lage ist, diese Symbolform zu lesen, wobei der Scanner in der Lage ist, das Symbol während des Scanverfahrens von der Schutzschicht zu trennen.

[0049] Die Daten können dann durch die Scannervorrichtung **56** dekodiert und über den seriellen Port an den PC **58** (oder eine andere Rechnervorrichtung) gesendet werden. Alternativ wird das Bild des Symbols von einem Flachbettscanner "eingefangen" oder gescannt und von dem Host-PC **58** dekodiert. Die dekodierten Daten werden unter Verwendung eines öffentlichen Schlüssels, der im Verborgenen von dem System übergeben wird, entschlüsselt, und die Daten werden dann dekomprimiert, wie in Block **60** angezeigt. Die dekodierten und dekomprimierten Daten werden dann zur Bedienerverifikation oder zur automatischen Verifikation durch Fingerbiometrie durch Abgleichen eines Live-Fingerscans des Karteninhabers gegen den verschlüsselten Fingerscan **62**, der aus den von dem zweidimensionalen Symbol **46** gelesenen Daten erhalten wird, auf dem Monitor des Host-PCs **58** angezeigt.

[0050] Daten zur Echtheitsprüfung können für spätere Verifikation und Analyse gespeichert werden, und der Computer **58** kann auch verschiedene Formen von Daten zur Echtheitsprüfung, wie etwa die ID-Nummer des Karteninhabers, verifizieren. Die automatisierte Verifikation kann durch Scannen der Dokumente in einem Stapelverfahren unter Verwendung von Flachbettscannern, die mit einer Dokumentenzuführung ausgestattet sind, erfolgen.

[0051] Unter Bezugnahme auf Fig. 3 wird nun eine dritte Ausführungsform eines Verfahrens zur Übertragung von Daten zur Echtheitsprüfung dargestellt. Die ersten Zugriffssteuerung- und Kartenleseschritte, die bei Block **64** angezeigt werden, sowie der Schritt der Karteninhaber-Verifikation und -Identifikation, der in Block **66** gezeigt wird, sind im Wesentlichen identisch mit den entsprechenden ersten Schritten von Fig. 1 und Fig. 2. In ähnlicher Weise ist der Schritt des Kodierens und Druckens des zweidimensionalen Symbols, der in Block **68** angezeigt wird, identisch mit dem entsprechenden, in Block **44** von Fig. 2 dargestellten Schritt. Block **70** zeigt die darauf folgenden Schritte, in welchen das zweidimensionale Symbol **46** gescannt und auf eine dritte Smartcard **72** geschrieben wird. In diesem Schritt wird das zweidimensionale Symbol **46** auf dem Dokument **48** unter Verwendung des Scanners **56** gescannt, wie dies oben unter Bezugnahme auf Block **54** von Fig. 2 beschrieben wurde. Die gescannten Daten werden in der Folge mit einem Kartenleser/-schreiber **74** unter Verwendung genau des gleichen Verfahrens, das unter Bezugnahme auf Block **32** von Fig. 1 beschrieben wurde, auf die dritte Smartcard **72** geschrieben. Die dritte Smartcard wird in der Folge gelesen, die Daten werden verarbeitet und die Verifikation und Identifikation des Karteninhabers findet in genau derselben Weise statt, wie sie unter Bezugnahme auf die Blöcke **34** und **38** von Fig. 1 beschrieben wurde.

[0052] Das Flussdiagramm von Fig. 4 fasst die wichtigsten Schritte des zugrunde liegenden Verfahrens zusammen.

[0053] Die Erfindung wird nun unter Bezugnahme auf zwei bestimmte Anwendungen aus der „realen Welt" beschrieben.

[0054] Die drastische Zunahme von Fahrzeugdiebstählen und Entführungen hat zu einer weltweiten Nachfrage nach Gegenmaßnahmen geführt. Die in dieser Anmeldung beschriebene Erfindung kann als besonders nützlicher und kostengünstiger Schutz gegen Fahrzeugdiebstahl dienen. Diese Anmeldung zeigt auch den effektiven Einsatz dieser Erfindung mit der vorgeschlagenen neuen Smartcard-Ausweiskarte der Republik Südafrika.

[0055] Bei der Antragstellung für die Fahrzeugregistrierung wird die Ausweiskarte des Antragstellers dem Bediener vorgelegt. Die Ausweiskarte ist in diesem Fall eine Smartcard, die Identitätsdaten und Daten zur Echtheitsprüfung enthält. Der Bediener führt die Ausweis-Smartcard in den Kartenleser ein und erhält über ein Fingerbiometrie-Verfahren zur Echtheitsprüfung Zugriffssteuerung. Die Daten zur Echtheitsprüfung werden von der Smartcard gelesen. Der Antragsteller legt nun seinen Finger auf einen Fingerscanner und seine Biometriedaten werden mit den von der Ausweiskarte erhaltenen abgeglichen. Damit wurde sichergestellt, dass die Person wirklich der Inhaber der Karte ist. Die persönlichen Daten, die von der Karte erhalten wurden, werden nun gegenüber der Online-Fahrzeugbesitzerdatenbank geprüft, um sicherzustellen, dass der Karteninhaber wirklich der Besitzer des Fahrzeugs ist. Die Bedienerdetails, Fahrzeugregistrierungsdetails und Verifikationsdetails, die von der Karte erhalten werden, werden komprimiert und verschlüsselt. Die Daten werden dann in ein zweidimensionales Symbol kodiert und auf eine vorher gedruckte, leere Zulassungsplakette gedruckt. In diesem Fall erlaubt die vorher gedruckte, leere Zulassungsplakette die Erstellung eines nicht reproduzierbaren zweidimensionalen Symbols. Die Zulassungsplakette trägt nun alle Details der Ausweiskarte des Antragstellers in einer maschinenlesbaren Form auf der Fahrzeug-Zulassungsplakette. Zwischen dem Bediener und dem Antragsteller kann es keine geheimen Absprachen geben, und eigentlich trägt die Zulassungsplakette nun eine hochsichere Kopie des Identitätsdokuments des Antragstellers mit sich.

[0056] Die Erfindung findet auch sinnvolle Anwendung in medizinischen Versorgungssystemen, d. h. Systemen oder Programmen, die ihre Teilnehmer bei der Bezahlung von medizinischen Behandlungen unterstützen (derartige Programme sind in den USA als traditionelle Rückerstattungs-Krankenversicherungen bekannt). Eine Smartcard dient als besonders nützliche und sichere Karte für die medizinische Versorgung, besonders weil die Person, welche die Karte vorlegt, als wirklicher Inhaber der Karte verifiziert werden kann. Andere Verwendungen sind sicheres Schreiben von Diagnosen, Verschreibungen und ärztlichen Attesten auf die Smartcard. Fonds zur medizinischen Versorgung und ähnliche Institutionen verfügen nicht über eine Personalausweis-Infrastruktur, die es ihnen ermöglichen würde, Smartcards mit positiven Identitätsmerkmalen darauf zu erzeugen. Es ist sehr praktisch und kostengünstig, diese Daten zur Echtheitsprüfung der Personalausweis-Smartcard entnehmen zu können.

[0057] Ein weiteres Problem mit bestehenden Karten für die medizinische Versorgung ist die Tatsache, dass die Echtheitsprüfung in den Praxisräumen des Arztes oder Krankenhauses und nicht beim medizinischen Versorger selbst stattfindet. Der medizinische Versorger kann damit nie ganz sicher sein, dass die

Verifikation wirklich erfolgt ist. Die medizinische Einrichtung kann nicht sicher sein, dass die beanspruchte Untersuchung auch wirklich stattgefunden hat.

[0058] In dieser Anwendung werden die Daten zur Echtheitsprüfung von der Personalausweiskarte auf die Smartcard für die medizinische Versorgung (oder eine Karte für die medizinische Versorgung mit einem zweidimensionalen Strichcode) gelesen. Die Karte für die medizinische Versorgung weist nun dieselben Merkmale zur Echtheitsprüfung auf wie eine Personalausweiskarte. Wenn die Smartcard für die medizinische Versorgung einem Arzt oder Krankenhaus vorgelegt wird, kann der Patient identifiziert und verifiziert werden. Der positive Nachweis der Verifikation, die Daten zur Echtheitsprüfung von der Smartcard, die Diagnose des Arztes, Details zu Verschreibungen und Attesten werden dann komprimiert und verschlüsselt und in der Form eines zweidimensionalen Symbols auf ein Antragsformular für medizinische Leistungen aufgedruckt. Dieser Antrag wird zu einem sicheren Antragsformular, das nicht verändert, manipuliert oder in betrügerischer Absicht erstellt werden kann, und nun auf sichere Weise an einen medizinische Versorger übermittelt werden kann. Die Anlage bei dem medizinischen Versorger scannt und dekodiert das Antragsformular, analysiert und verifiziert den Patienten an Hand der Daten zur Echtheitsprüfung, und verarbeitet das Antragsformular automatisch.

[0059] Die Erfindung erweitert den Anwendungsbereich der Smartcard-Technologie insbesondere unter dem Gesichtspunkt der Sicherheit und Echtheitsprüfung, enorm. Sie integriert Smartcard-Technologie und Papierdokumentation auf wirksame Art und Weise. Die Erfindung führt auch zu beträchtlichen Kosteneinsparungen, da die durch die Smartcard-Identifikation geschaffenen Merkmale zur Echtheitsprüfung in effektiver Weise von vielen Institutionen verwendet werden können, ohne dass diese eine Infrastruktur zur Erzeugung dieser sicheren Merkmale zur Echtheitsprüfung benötigen. Die Ausgaben für ein sicheres Personalausweissystem (diese sind beträchtlich, wenn man die Kosten eines großen nationalen "automatischen Identitätssuchsystems" mit berücksichtigt, das aber erforderlich ist, um mehrfache Anmeldungen einer einzelnen Person zu verhindern) werden gerechtfertigt, wenn der Einsatz der Karte derart drastisch ausgedehnt werden kann.

[0060] Die Erfindung findet insbesondere Anwendung auf dem Gebiet der Verarbeitung behördlicher und geschäftlicher Anträge und dergleichen. Der Umfang des Gebiets wird nur durch dessen Vielfältigkeit übertroffen. Praktisch alle Anwendungen erfordern einen Identitätsnachweis. Derzeit wird das Ausweisbuch des Antragstellers verlangt und eine Fotokopie davon erstellt. Dies ist eine sehr unsichere Praxis und in Verbindung mit der neuen Smartcard-Ausweiskarte nicht besonders effektiv, da die meisten Details auf dem Chip der Karte enthalten sind. Für alle Arten von Anträgen werden die Verifikationsdetails in ein zweidimensionales Symbol kodiert und auf das relevante Antragsformular aufgedruckt. Das Antragsformular ist nun dauerhaft durch einen verifizierbaren Nachweis mit dem Antragsteller verbunden. Die von der Smartcard gelesenen Details können verwendet werden, um die persönlichen Daten des Antragstellers automatisch einzutragen. Die Daten innerhalb des zweidimensionalen Symbols können auch später gescannt werden, so dass der Antrag automatisch verarbeitet werden kann.

[0061] Einige wichtige Beispiele, in denen die Erfindung sich bei der Betrugsbekämpfung durch Schaffen eines geeigneten Verfahrens zur Echtheitsprüfung als wirksam erweisen wird, umfassen Vertragsdokumente, Versicherungsdokumente, Zertifikate und Anträge, Aufnahmedokumente in Krankenhäusern und medizinischen Einrichtungen, Karten für die medizinische Versorgung, Antragsformulare für medizinische Leistungen, ärztliche Atteste und Verschreibungen, sowie Bankdokumente, einschließlich Formulare für Mitarbeiterinformationen, Antragsformulare für Konten, Kredite und Hypotheken. Andere Anwendungsgebiete sind Dokumente und Anträge, die persönliche Informationen umfassen, Antragsformulare und Fragebögen für Beschäftigung und Konten, sowie von der Regierung erstellte Formulare wie derartige in Verbindung mit Volkszählungen, Wahlen, Anträge auf Registrierung im Wählerverzeichnis, und verschiedene Arten von Zulassungen, wie etwa Zulassungen für Rundfunk, Gewerbe sowie Waffenpässe. Auf dem Gebiet der Bildung kann die Erfindung auf Dokumente wie Prüfungsunterlagen, Studentenanmeldungsformulare und -karten sowie Diplomurkunden angewandt werden. Fahrzeugbezogene Dokumente wie etwa Fahrzeugzulassungspapiere und Zulassungsplaketten für die Windschutzscheibe, können ebenfalls Nutzen aus der Erfindung ziehen, sowie alle Arten von bankfähigen Papieren wie Schecks, Wechsel, Rechnungsbelege und Tickets.

[0062] Die obigen Beispiele sind nicht erschöpfend oder einschränkend und wurden rein beispielhaft angeführt.

Patentansprüche

1. Verfahren zur Übertragung von Daten zur Echtheitsprüfung von einem ersten Träger (**12**), welcher eine tragbare Datenspeichereinrichtung ist, auf einen zweiten Träger (**30**), wobei das Verfahren die Schritte umfasst:
Verifizieren der Daten zur Echtheitsprüfung auf dem ersten Träger (**12**);
Lesen der Daten zur Echtheitsprüfung mit einem Trägerleser;
Sichern der Daten zur Echtheitsprüfung mit Ver-

schlüsselungs- und/oder Komprimierungsmitteln; und
Schreiben der Daten zur Echtheitsprüfung auf den zweiten Träger (**30**) in einem maschinenlesbaren Format mit einem Kartenleser/-schreiber oder einem Drucker;
dadurch gekennzeichnet, dass der Schritt des Verifizierens der Daten zur Echtheitsprüfung folgende Schritte umfasst: Steuern des Zugriffs auf den ersten Träger (**12**) durch Verifizieren der Identität und/oder der Berechtigung eines Bedieners, der zur Implementierung zumindest des Leseschritts bestimmt ist; und Verifizieren der Identität des Inhabers des ersten Trägers (**12**), wobei die Schritte der Verifikation des Bedieners und des Inhabers PIN-/Passwort- und/oder auf Biometrie basierende Verifikationsverfahren umfassen.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Verfahren die weiteren Schritte einschließt: Steuern des Zugriffs auf die Daten zur Echtheitsprüfung, die auf den zweiten Träger (**30**) geschrieben sind, Lesen der Daten zur Echtheitsprüfung (**24**; **26**; **28**) in Bezug auf die Identität des Inhabers des zweiten Trägers und Verifizieren der gelesenen Daten.

3. Verfahren nach Anspruch 1 oder Anspruch 2, dadurch gekennzeichnet, dass der erste Träger (**12**) eine erste Smartcard ist.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der zweite Träger (**30**) eine tragbare Datenspeichereinrichtung ist.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass der zweite Träger (**30**) eine zweite Smartcard ist.

6. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass der zweite Träger (**30**) ein Dokument umfasst, auf welches die Daten zur Echtheitsprüfung in einem maschinenlesbaren Format appliziert werden.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass der erste Träger (**12**) ein zu einer Einzelperson gehörender identitätsbasierter Träger ist.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die auf PIN/Passwort und auf Biometrie basierenden Verfahren in Zusammenwirken miteinander in einem Abgleichverfahren verwendet werden.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass der Sicherungsschritt die Schritte einschließt: Hinzufügen zusätzlicher Sicherheitsdaten zu den Daten zur Echtheitsprüfung und Komprimieren und Verschlüsseln der kombinierten Sicherheits- und Daten zur Echtheitsprüfung.

10. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass der Schritt des Steuerns des Zugriffs auf die geschriebenen Daten zur Echtheitsprüfung auf dem zweiten Träger (**30**) im Wesentlichen identisch mit dem entsprechenden Zugriffssteuerungsschritt in Bezug auf den ersten Träger ist.

11. Verfahren nach Anspruch 2 oder Anspruch 10, dadurch gekennzeichnet, dass der Schritt des Verifizierens der gelesenen Daten auf dem zweiten Träger (**30**) im Wesentlichen identisch mit dem entsprechenden Verifikationsschritt in Bezug auf den ersten Träger ist.

12. Verfahren nach einem der Ansprüche 2, 10 oder 11, dadurch gekennzeichnet, dass das Verfahren noch die weiteren Schritte einschließt: Lesen der Daten zur Echtheitsprüfung von dem zweiten Träger (**30**) und Schreiben der Daten zur Echtheitsprüfung auf einen dritten Träger in maschinenlesbarem Format.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass der zweite Träger (**30**) ein Dokument ist, auf welches die Daten zur Echtheitsprüfung in einem maschinenlesbaren Format appliziert werden, und der dritte Träger eine tragbare Datenspeichereinrichtung ist.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass der dritte Träger eine Smartcard ist.

15. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass der zweite Träger (**30**) eine tragbare Datenspeichereinrichtung ist und der dritte Träger ein Dokument ist, auf welches die Daten zur Echtheitsprüfung in einem maschinenlesbaren Format appliziert werden.

16. Verfahren nach einem der Ansprüche 1 bis 15, dadurch gekennzeichnet, dass das Verfahren für die sichere Übertragung von Daten zur Echtheitsprüfung von einem ersten Träger auf einen n-ten Träger über n – 2 Träger sorgt, wobei jeder dazwischen liegende Datentransferschritt gesichert ist.

17. System zum Übertragen von Daten zur Echtheitsprüfung von einem ersten Träger (**12**), welcher eine tragbare Datenspeichereinrichtung ist, auf zumindest einen zweiten Träger (**30**) in einer sicheren Weise, wobei das System Mittel zum Verifizieren der Daten zur Echtheitsprüfung auf dem ersten Träger (**12**), einen Trägerleser zum Lesen der Daten zur Echtheitsprüfung, Mittel zum Sichern der Daten zur Echtheitsprüfung, und einen Kartenleser/-schreiber oder einen Drucker zum Schreiben der Daten zur

Echtheitsprüfung auf einen zweiten Träger in einem maschinenlesbaren Format einschließt; dadurch gekennzeichnet, dass das Mittel zum Verifizieren der Daten zur Echtheitsprüfung Mittel zum Steuern des Zugriffs auf den ersten Träger (**12**) durch Verifizieren der Identität und/oder der Berechtigung eines Bedieners, der zur Implementierung zumindest des Lesens der Daten zur Echtheitsprüfung bestimmt ist, und Mittel zum Verifizieren der Identität des Inhabers des ersten Trägers (**12**) umfasst, wobei das Mittel zum Steuern des Zugriffs auf den ersten Träger PIN-/Passwort- und/oder auf Biometrie basierende Verifikationsverfahren verwendet.

18. System nach Anspruch 17, des Weiteren dadurch gekennzeichnet, dass das System Mittel zum Steuern des Zugriffs auf die Daten zur Echtheitsprüfung auf dem zweiten Träger (**30**), Mittel zum Lesen der Daten zur Echtheitsprüfung (**24**; **26**; **28**) in Bezug auf die Identität des Inhabers des zweiten Trägers (**30**) und Mittel zum Verifizieren der gelesenen Daten zur Echtheitsprüfung auf dem zweiten Träger (**30**) einschließt.

19. System nach Anspruch 18, dadurch gekennzeichnet, dass das Sicherungsmittel Verschlüsselungs- und Entschlüsselungsmittel sowie Komprimierungs- und Dekomprimierungsmittel zum Komprimieren, Verschlüsseln, Entschlüsseln und Dekomprimieren der Daten zur Echtheitsprüfung einschließt.

Es folgen 4 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

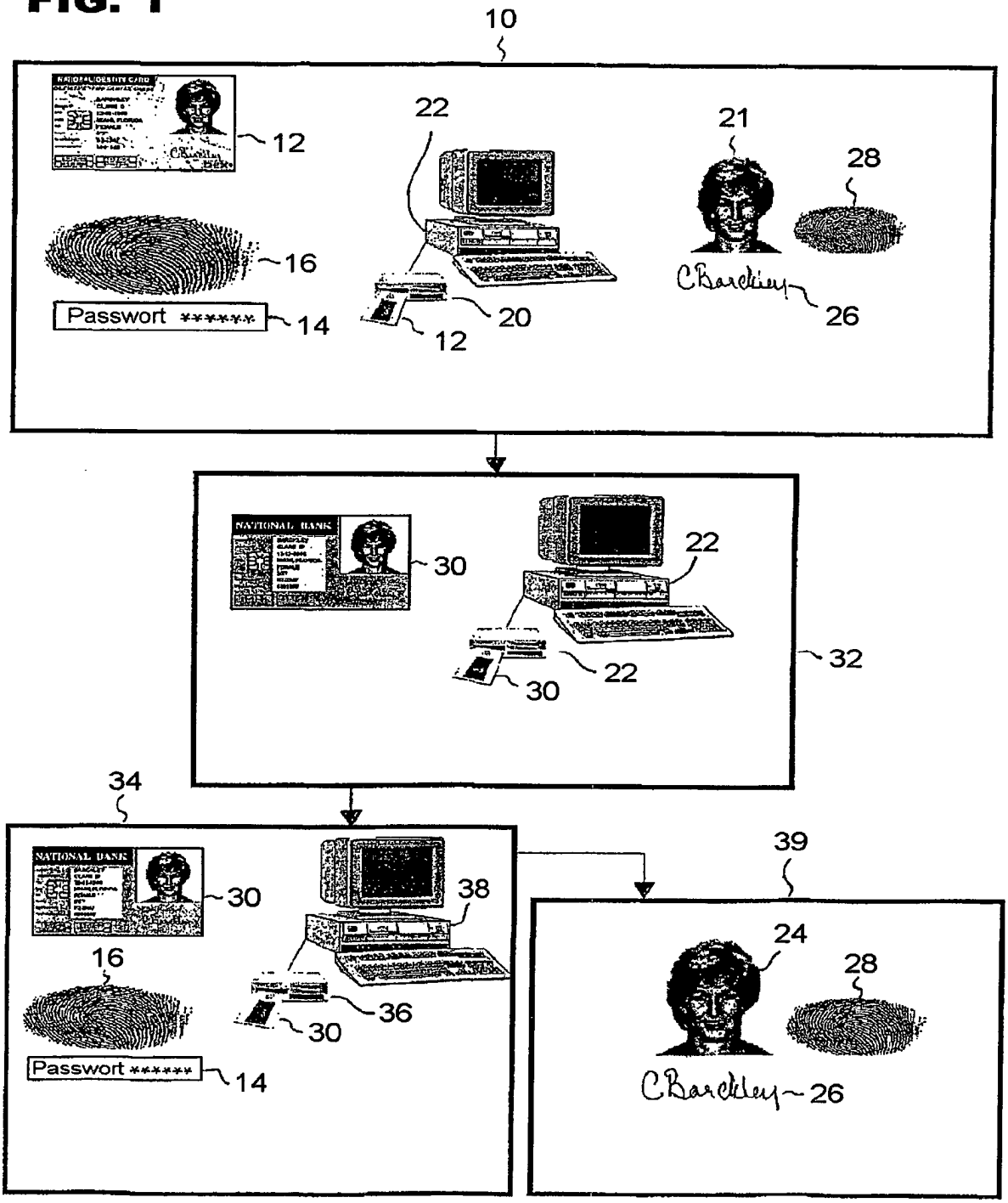


FIG. 2

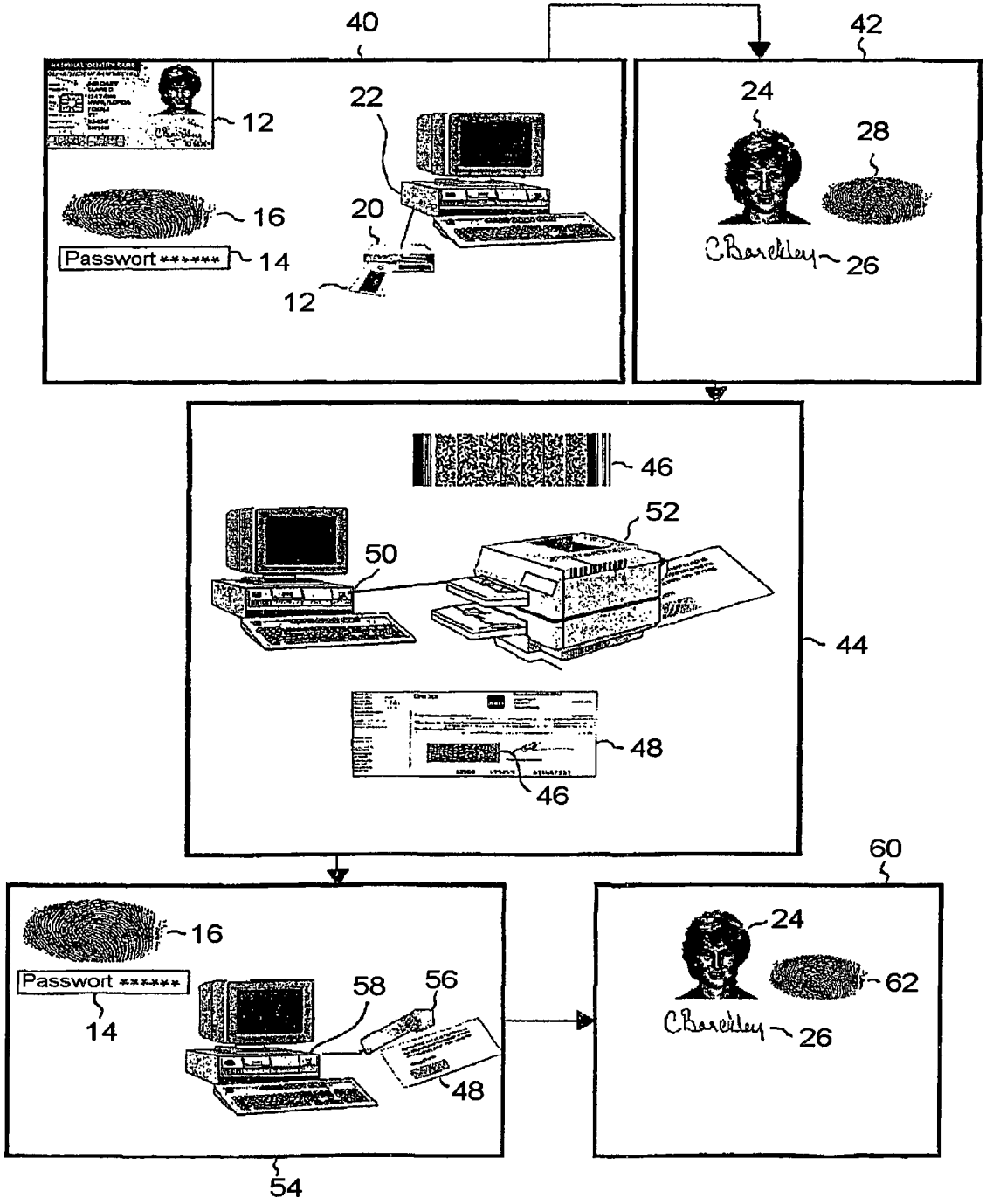

40
42
12
22
24
28
16
20
Passwort ******
14
12
C.Barckley
26
46
52
50
44
48
46
60
16
24
Passwort ******
58
56
62
14
48
C.Barckley
26
54

FIG. 3

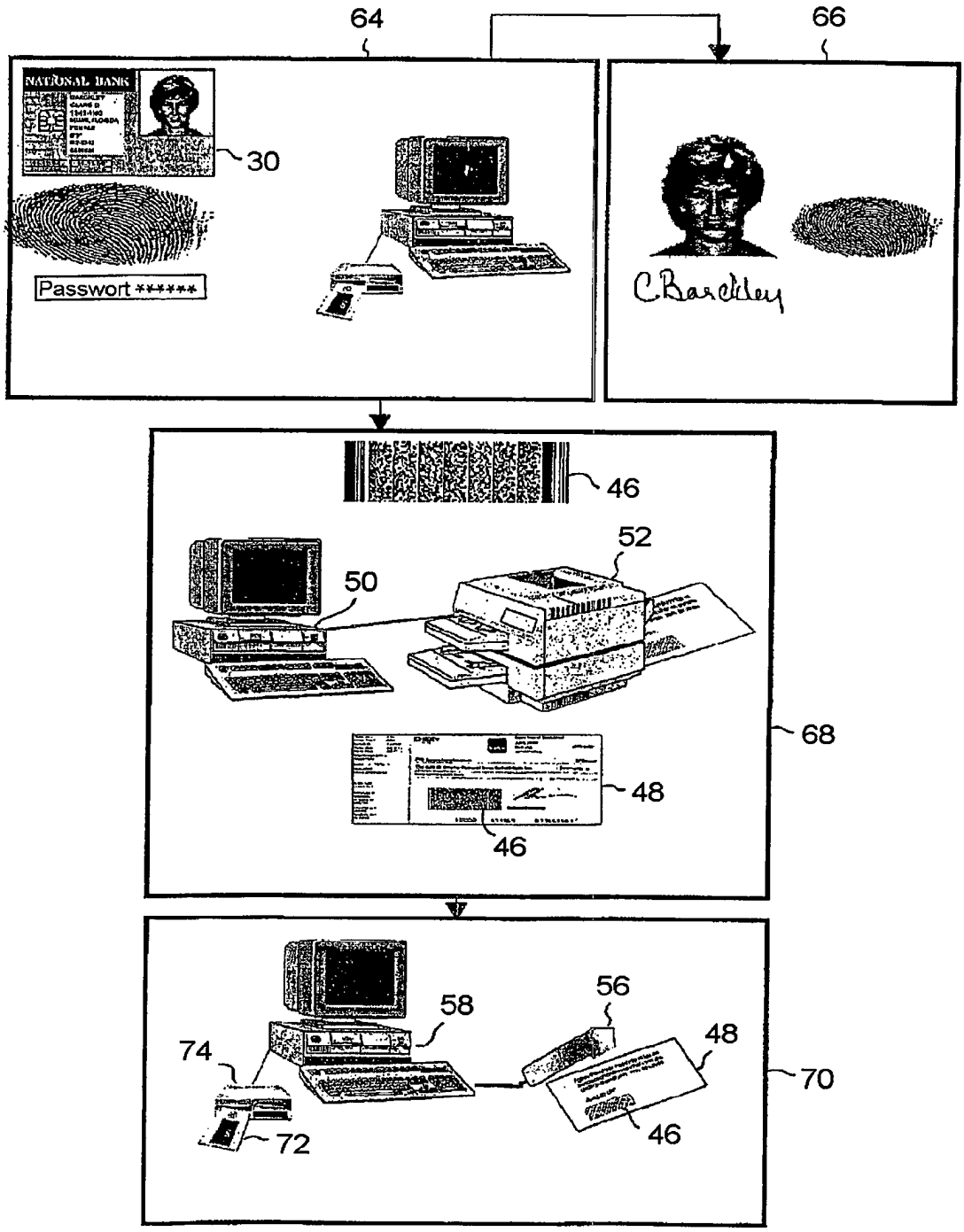
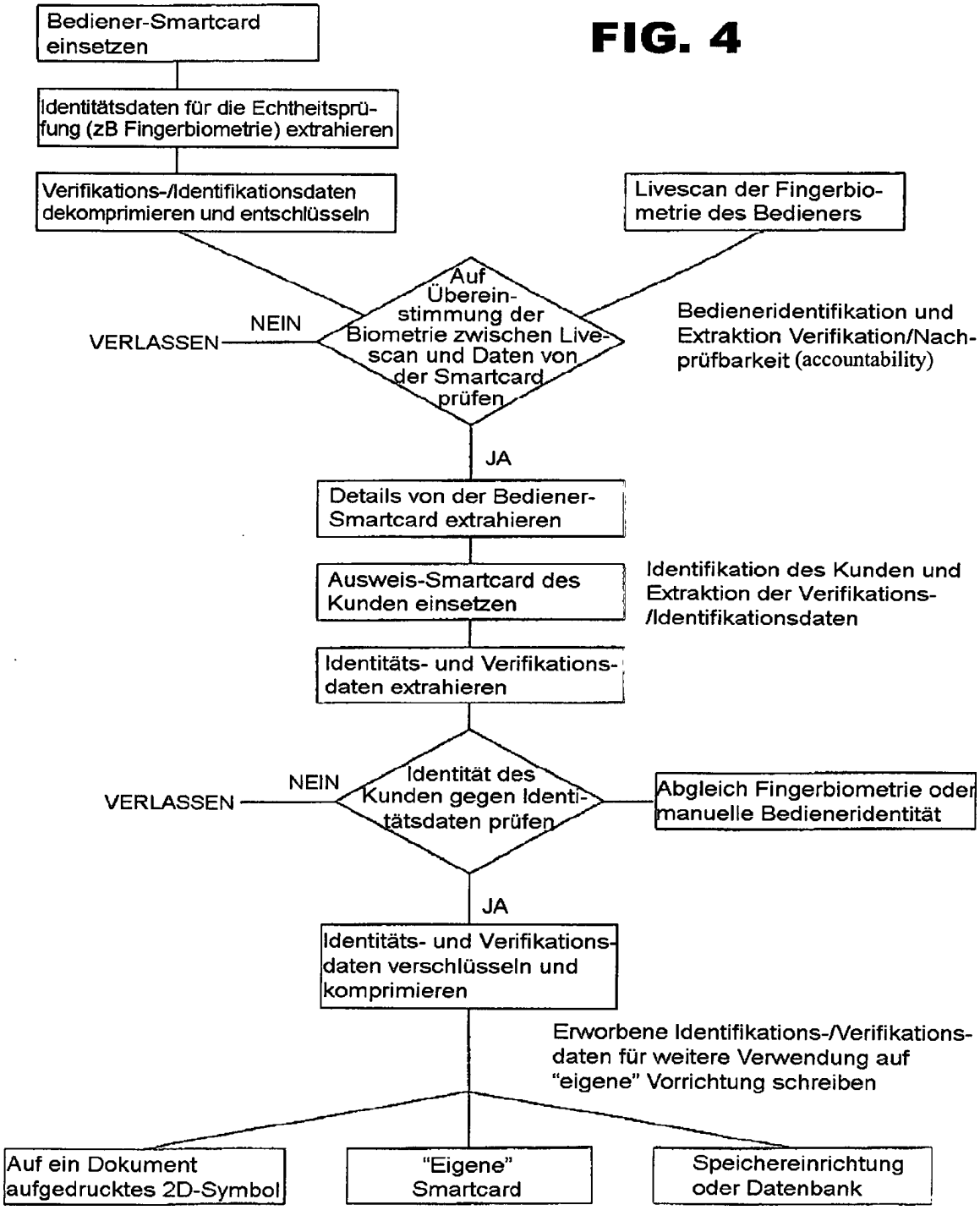

64
66
NATIONAL BANK
30
Passwort ******
C.Barckley
46
52
50
68
48
46
58
56
74
48
70
72
46

FIG. 4


Bediener-Smartcard einsetzen
Identitätsdaten für die Echtheitsprüfung (zB Fingerbiometrie) extrahieren
Verifikations-/Identifikationsdaten dekomprimieren und entschlüsseln
Livescan der Fingerbiometrie des Bedieners
Auf Übereinstimmung der Biometrie zwischen Livescan und Daten von der Smartcard prüfen
NEIN
VERLASSEN
Bedieneridentifikation und Extraktion Verifikation/Nachprüfbarkeit (accountability)
JA
Details von der Bediener-Smartcard extrahieren
Ausweis-Smartcard des Kunden einsetzen
Identifikation des Kunden und Extraktion der Verifikations-/Identifikationsdaten
Identitäts- und Verifikationsdaten extrahieren
Identität des Kunden gegen Identitätsdaten prüfen
NEIN
VERLASSEN
Abgleich Fingerbiometrie oder manuelle Bedieneridentität
JA
Identitäts- und Verifikationsdaten verschlüsseln und komprimieren
Erworbene Identifikations-/Verifikationsdaten für weitere Verwendung auf "eigene" Vorrichtung schreiben
Auf ein Dokument aufgedrucktes 2D-Symbol
"Eigene" Smartcard
Speichereinrichtung oder Datenbank