(19) österreichisches patentamt

(10) **AT 010 306 U1 2008-12-15**

(12) # Gebrauchsmusterschrift

(21) Anmeldenummer: GM 8093/07
(22) Anmeldetag: 2006-10-31
(42) Beginn der Schutzdauer: 2008-10-15
Längste mögliche Dauer: 2016-10-31
(45) Ausgabetag: 2008-12-15
(51) Int. Cl.[8]: **G07F 7/10**
G07F 19/00
(67) Umwandlung aus Patentanmeldung: 1824/2006

(73) Gebrauchsmusterinhaber:
NEUBAUER THOMAS DIPL.ING. DR.
A-1070 WIEN (AT).
POHL ALFRED DIPL.ING. DR.
A-2130 MISTELBACH,
NIEDERÖSTERREICH (AT).
TSCHOFEN ROBERT DIPL.ING.
A-1140 WIEN (AT).

(72) Erfinder:
NEUBAUER THOMAS DIPL.ING. DR.
WIEN (AT).
POHL ALFRED DIPL.ING. DR.
MISTELBACH, NIEDERÖSTERREICH
(AT).
TSCHOFEN ROBERT DIPL.ING.
WIEN (AT).

(54) **VERFAHREN ZUR SPEICHERUNG VON DATEN MITTELS GELDAUTOMAT UND SPEICHERMEDIUM**

(57) Die Erfindung beschreibt ein Verfahren nach Fig. 1 zur Authentifizierung und Durchführung der sicheren Speicherung von persönlichen und wertvollen Daten auf einem meist zentralen Speicher. Als Dateneingabegeräte werden Geräte verwendet, die für diverse Banktransaktionen bereits vorhanden sind oder die aus diesem Bereich einfach adaptierbar sind. Als zentrales Gerät wird die Verwendung eines Geldausgabeautomaten z.B. Bankomats (1) beschrieben. Nach der strengen Authentifizierung durch Karte (7) und Geheimzahl besteht der Zugriff auf das Datenkonto (11). Das Speichermedium (7), von dem aus Daten gelesen werden oder auf das Daten gesichert werden sollen kann nun wahlweise ein freier Bereich auf der Karte (7) selbst, auf einer weiteren Karte oder einem sonstigen Speichermedium sein, wenn das Gerät eine Schnittstelle dafür bereitstellt.

Zusätzlich zur Übertragung der Daten von und zu einem meist zentralen sichern Speicher (11) und einem lokalen Speichermedium steht nach Authentifizierung optional auch die Verwaltung des Datenkontos vom Terminal (3) und (8) aus frei.

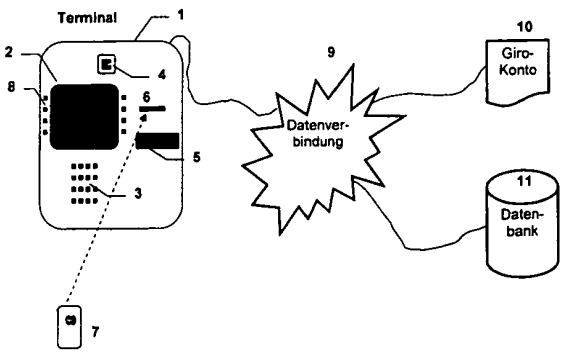

Fig. 1

AT 010 306 U1 2008-12-15

Die Erfindung betrifft ein Verfahren zur zentralen Sicherung von Daten, bei dem die zu sichernden Daten auf einem Datenträger, z.B. Smartcard, Scheckkarte, Kreditkarte, CD, USB, etc. gespeichert sind und über ein ohnehin vorhandenes Infrastrukturelement des Zahlungsverkehrs, z.B. Geldausgabeautomat, als Datenübertragungsgerät in eine gesicherte Umgebung übertragen werden. Zur Erhöhung der Zugriffssicherheit wird die dort bekannte verstärkte Authentifizierung des Eigentümers angewandt.

Diese notwendige Authentifizierung erfolgt dabei über das Besitzen eines Speichermediums, welches im Wesentlichen die Bankomat-, Scheck- oder Kreditkarte sein kann und das Kennen einer Geheimzahl. Die zu sichernden bzw. zu übertragenen Daten sind elektronische Dokumente, beispielsweise DOC, PDF, JPG, etc.

Zur Übertragung und Sicherung von elektronischen Dokumenten stehen gemäß *dem Stand der Technik* dem Eigentümer der Daten unterschiedliche technische Übertragungsverfahren zur Verfügung.

Dabei können die Daten mittels Heimcomputer und dem Datenzugang über das Internet und den entsprechenden Protokollen wie dem Internet Protokoll (IP), dem File Transfer Protokoll (FTP), über Mail, SNMP, etc. zu einer Datenbank übertragen werden. Die Übertragung der Daten nimmt dabei entsprechend der Datenmenge und der Internet Übertragungsgeschwindigkeit, diese entspricht dem Zugangverfahren wie z.B. Modem, ADSL, etc. eine gewisse Zeit in Anspruch. Während dieser Zeit muss die Verbindung zur Datenbank aufrechterhalten werden. Die Kosten für die Übertragung entsprechen den Anschlusskosten wie z.B. ADSL, Modem, etc. und den Kosten für die zu übertragenden Datenmengen. Zur sicheren Übertragung kommen im Allgemeinen verschlüsselte Protokolle z.B. ftps, https mit verschiedenen Verschlüsselungslängen wie z.B. 128 bit zum Einsatz. Die Authentifizierung für den Zugang erfolgt im Allgemeinen über Username und Passwort. Neue Ansätze schlagen für hochsichere Datenverbindungen die zusätzliche Bestätigung mit einmalig verwendbaren und durch eine autorisierte Stelle erstellte Schlüssel vor, sog. Transaktionsnummern, TAN.

Verschiedene Nachteile dieser Verfahren sind, dass der Benutzer selbst über einen entsprechenden Internet Zugang verfügen muss, die Zugangsmethoden über die Verschlüsselung und der Authentifizierung über Username und Passwort wenig Schutz bieten und die Übertragung der Datenmengen zu lange dauern kann. Eine wesentlich sichere Abhilfe bietet der Zugang über Datenübertragungsgeräte mit deutlich höheren Authentifizierungsanforderungen, wie z.B. dem heutigen Geldautomaten.

Aus dem Stand der Technik sind Geldautomaten bekannt, welche üblicherweise aus einem Standard-Industrie-PC bestehen. Dieser Standard-Industrie-PC wird mit angeschlossener Spezialperipherie erweitert (z.B. Geldtresor).

Die Grundausstattung jedes Geldautomaten beinhaltet folgende Peripherieteile:

- Ein Auszahlmodul zum Vereinzeln und Präsentieren von Geldscheinen oder anderer papierbasierter Medien, wie Briefmarken
- Ein ID-Kartenleser zum Lesen von Scheckkarten oder Kreditkarten (kurz KARTE)
- Ein Encrypting PIN Pad (EPP) zur Erfassung und Verarbeitung der Geheimzahl, weiteren Bedienfunktionen und zur sicheren Kommunikation.
- Ein Monitor (Bildschirm) zur Ausgabe von Meldungen, Anzeige der Funktionsauswahl, Überprüfung der Eingabe, etc
- Soft-Keys (unbeschriftete Tasten am Bildschirmrand. Der Bildschirm zeigt die jeweils zuge-

ordnete Funktion).

- Weitere Peripheriegeräte sind zum Beispiel: Videokamera, Journaldrucker, Quittungsdrucker, Kontoauszugdrucker, Touchscreen (ersetzt Bildschirm und Soft-Keys), alphanumerische Tastaturen, Geräte zur Scheck- und zur Bargeldeinzahlung, Geräte zum Einwurf und Lagerung von Briefumschlägen, Geräte zur Aus- und Eingabe von Münzen, Geräte zur Verarbeitung von Sparbüchern, Barcode-Scanner, Kopfhöreranschluss oder Lautsprecher (zur Unterstützung von Menschen mit Behinderung), Tastaturen mit Blindenschrift, etc.

- Netzwerkverbindung

Die Softwareausstattung besteht aus einem Industrie-Standard-Betriebssystem, Gerätetreibern, einer Kommunikationsschicht (z. B. CEN/XFS oder J/XFS) und einer Applikation, die den Geldautomat steuert und mit der Gegenstelle (Server/Host) kommuniziert. Weiters ist zur Anzeige ein Monitor (Bildschirm) angeschlossen.

Der Bargeldbezug an Geldausgabeautomaten ist denkbar einfach und verläuft schematisch wie folgt:

- Die KARTE wird eingeschoben.

- Die Option "Bargeldbehebung" wird gewählt (andere Menüpunkte sind - unterschiedlich nach Modell, Land und Region - auch noch Sprache, Kontostandabfrage, QUICK-Ladung oder -Entladung etc.)

- Die persönliche (kartengebundene) Geheimzahl (PIN) wird eingegeben und bestätigt.

- Eingabe des Betrages und Bestätigung

- Rückgabe der KARTE, die anschließend entnommen werden kann

- Geldauszahlung und Entnahme

- Durch Betätigung der Sonderfunktionstaste „Abbruch-Taste" kann der Vorgang jederzeit abgebrochen werden. Wird das Geld nicht innerhalb einer Sekundenfrist entnommen, wird es zur Eigentumssicherung einbehalten.

Das beschriebene Authentifizierungsverfahren stellt bislang lediglich die Verbindung zum eigenen Girokonto (Bankkonto) her und legitimiert lediglich zum Auszahlen von nach oben begrenzten Geldbeträgen.

Aus dem Stand der Technik ist das Speichern von Daten durch Einsenden von Speichermedien und der Daten online über das World Wide Web kurz www oder anderen Online Diensten bekannt.

Der gegenständlichen Erfindung liegt daher die Aufgabe zugrunde, ein neues Verfahren vorzulegen, bei dem die zugrunde liegende Authentifizierung über den Geldautomaten oder ein gleichwertiges Gerät des Zahlungsverkehrs sowohl für den Kontozugang zum Girokonto als auch zu einem sicheren Speicherbereich im Bankenserver, z.B. Datenkonto, als auch für die Übertragung von Daten vom Datenübertragungsgerät z.B. Geldautomaten zum Bankenserver, Datenbank, Bandspeichergerät, Zwischenspeicher etc. hergestellt werden kann. Weiters ermöglicht die gegenständliche Erfindung die Verwaltung der in der sicheren Umgebung gespeicherten Daten vom Datenübertragungsgerät aus.

Diese Aufgabe wird durch ein Verfahren gemäß den Ansprüchen 1 bis 19 gelöst.

Ausgestaltungen, Weiterbildungen und Anwendungen der Erfindung ergeben sich aus den von Anspruch 1 jeweils abhängigen Ansprüchen.

Gemäß Anspruch 1 betrifft die Erfindung ein Verfahren zur Übertragung von Daten in eine gesicherte Umgebung, bei dem die zu übertragenden Daten auf einem Speichermedium gespeichert sind und über ein Infrastrukturelement der Bank oder eines Bankdienstleisters, welches erhöhten Authentifizierungsanforderungen genügt, z.B. einem Geldautomaten, Serviceterminals oder einem Apparat zum Ausdrucken von Kontoauszügen, übertragen werden. Die Authentifizierung erfolgt dabei mittels KARTE (Träger des privaten Schlüssels, bzw. Geheimzahl z.B. PIN), der einzugebenden GEHEIMZAHL und dem eigentlichen SPEICHERMEDIUM, wobei eine Kombination zwischen Karte und Speichermedium denkbar und vorteilhaft ist.

Erfindungsgemäß wird also ein Verfahren zur Datenübertragung mit dem Authentifizierungsmechanismus privatem Schlüssel/Geheimzahl (digitale Signatur), Datenübertragungsgerät und Datenträger wie z.B. Smartcard, Scheckkarte, Kreditkarte, CD, USB verbunden.

Gemäß dem Authentifizierungsmechanismus mittels privatem Schlüssel/Geheimzahl wird über das Datenübertragungsgerät die digitale Signatur übertragen. Auf Basis der digitalen Signatur wird nun nicht nur die Verbindung zum privaten Bankkonto (Girokonto) sondern auch der Zugang zu einem Datenspeicher in einer gesicherten Umgebung, z.B. Datenbank in der Bank oder einem vertrauenswürdigen Dienstleister legitimiert. Dieser Datenspeicher, z.B. ein Datenkonto ist dem Benutzer eindeutig zugewiesen.

Basierend auf dem oben beschriebenen Stand der Technik zur Authentifizierung werden die zu übertragenden Daten nun über den ID-Kartenleser auf einen Datenträger wie z.B. Smartcard, Scheckkarte, Kreditkarte, etc. geschrieben oder von diesem ausgelesen und über die sichere Verbindung an den gesicherten Speicher transferiert.

Optional kann der Geldautomat auch um ein zusätzliches Datenträgerlese- und Datenschreibgerät erweitert werden, wie zum Beispiel zum Lesen und Schreiben von CDs, DVDs, USBs.

Bei der KARTE zur notwendigen Authentifizierung und dem Datenträger kann es sich also um zwei unterschiedliche physikalische Medien handeln. In einer besonders vorteilhaften Ausführung verfügt die KARTE aber über ausreichend Speicherkapazität in einem für den Besitzer zugänglichen Speicherbereich, um direkt auch als Datenträger zu dienen.

Weiters können alternativ auch Datenübertragungsgeräte speziell zur Übertragung der Daten zur Verfügung gestellt werden (z.B. spezielle Service Terminals) oder Geräte des elektronischen Zahlungsverkehrs mit verwendet werden (z.B. Apparate zum Ausdrucken von Kontoauszügen). Diese Datenübertragungsgeräte unterscheiden sich von einem Geldautomaten insbesondere dadurch, dass keine Geldbehebungsfunktion und kein Geldtresor vorhanden sind.

Die Datenübertragung über z.B. Geldautomaten, Datenübertragungsgerät ist denkbar einfach und verläuft schematisch wie folgt:

- Die KARTE wird eingeschoben.
- Die Option "Datenübertragung" wird gewählt (andere Menüpunkte sind - unterschiedlich nach Modell, Land und Region - auch noch Sprache, Kontostandabfrage, QUICK-Ladung oder -Entladung o.ä.)
- Die persönliche Geheimzahl (PIN) wird eingegeben und bestätigt.
- Der Datenträger (Speicherbereich auf der KARTE oder separater Datenträger) wird nach zu übertragenen Daten und Speichergröße überprüft. Alternativ besteht wie beim Aufladen

einer weiteren Quick-Karte die Möglichkeit, als Datenquelle oder Senke binnen einer Zeitspanne nach der Entnahme der Authentifizierungskarte (KARTE) einen weiteren Datenträger in das Datenübertragungsgerät einzuführen und zur Übertragung von Daten zu verwenden.

- Die Daten in der gesicherten Speicherumgebung der Bank (Datenbank) und die Daten auf dem Datenträger werden angezeigt.
- Der Kunde wählt die zu übertragenen Daten in der gesicherten Speicherumgebung der Bank oder dem angeschlossenen oder zugeordneten Datenträger aus.
- Die Auswahl wird bestätigt.
- Die Daten werden übertragen.
- Nach Abschluss der Transaktion werden die KARTE bzw. der Datenträger zurückgegeben und können entnommen werden.

Der Vorgang kann durch Betätigung der „Abbruch-Taste" jederzeit unterbrochen werden.

Die Erfindung wird nachfolgend anhand eines konkreten Ausführungsbeispiels weiter erläutert. Dabei wird auf die Darstellungen in Figur 1 Bezug genommen:

Figur 1 Die schematische Ansicht eines Geldautomaten und die Verbindungsstruktur die dem Verfahren zugrunde liegt.

Wie in Fig. 1 illustriert ist, wird in diesem konkreten Beispiel ein Geldautomat als Datenübertragungsgerät entsprechend der gegenständlichen Erfindung verwendet. Der Geldautomat besteht aus einem Gehäuse 1 das in verschiedenen Formen ausgeführt sein kann, einem Bildschirm 2 und den Soft-Keys 8 die in einer vorteilhaften Ausführung an der Seite des Bildschirms angeordnet sind. Weiters einem Tastenpad 3 zur Eingabe der Geheimzahl, Geldbeträgen, Verzeichnisauswahl etc. und der Funktionsanzeige 4 wie z.B. Datenlesefähig etc. Weiters verfügt der Geldautomat über eine Geldausgabeeinheit 5, und ein ID-Kartenlesegerät 6.

Als Speichermedium für die zu übertragenden Daten wird im konkreten Fall ein Datenträger 7 wie z.B. die Checkkarte, Smartcard, Kreditkarte etc. verwendet. Zur Kommunikation mit dem Rechenzentrum werden Datenverbindungen 9 verwendet wie z.B. LAN, Modem, Telefon, etc. Über diese erfolgt der bidirektionale Zugang vom Datenübertragungsgerät zum Girokonto 10 und der gesicherten Umgebung der Datenbank 11.

Die Übertragung der Daten erfolgt nun wie folgt:

- Die KARTE 7 wird in das ID-Kartenlesegerät 6 eingeschoben.
- Die KARTE 7 dient im Beispiel sowohl der Authentifizierung als auch als Datenträger
- Über den Bildschirm 2 werden verschiedene Optionen angeboten.
- Die Option "Datenübertragung" wird mittels Soft-Keys 8 gewählt.
- Die persönliche (KARTEN gebundene) Geheimzahl (PIN) wird über das Tastenpad 3 eingegeben und bestätigt.
- Der Benutzer wählt aus in welche Richtung die Datentransaktion durchgeführt werden soll, d.h. Speichern von Daten in die gesicherte Umgebung der Datenbank 11 oder Speichern

von Daten aus dem gesicherten zentralen Speicher auf den Datenträger 7.

- Die Daten in der gesicherten Umgebung der Datenbank, bzw. auf dem Datenkonto 11 der Bank bzw. die Daten auf dem Datenträger 7, die über das ID-Kartenlesegerät 6 an den Geldautomaten 1 angeschlossen ist werden angezeigt.

- Der Kunde wählt die zu übertragenen Daten aus der gesicherten Umgebung der Datenbank 11 der Bank oder auf dem Datenträger 7 aus.

- Die Auswahl wird über das Tastenpad 3 oder den entsprechenden Soft-Keys 8 bestätigt.

- Die Daten werden über die Datenverbindung 9 übertragen.

- Nach Abschluss der Datentransaktion hat der Benutzer die Möglichkeit eine neuerliche Datentransaktion auszuführen, möglicher Weise in die jeweils entgegen gesetzte Richtung (Datenträger 7 ←→ gesicherte Umgebung der Datenbank 11)

- Nach Abschluss der Transaktion werden die KARTE bzw. der Datenträger zurückgegeben und können entnommen werden.

In der in Figur 1 dargestellten, besonders vorteilhaften Ausführungsform sind KARTE und Datenträger ein und dasselbe physikalische Medium, also 7. Die KARTE verfügt also über einen entsprechenden Speicherbereich.

Alternativ dazu können die KARTE, welche die Authentifizierungsinformation inkludiert und der Datenträger separate Speichermedien sein. Beispielsweise könnte eine Checkkarte oder Kreditkarte für die Authentifizierung des Zugangs zum Datenkonto verwendet werden und eine weitere Speicherkarte, z.B. SmartCard, Bürgerkarte, ecard als Datenträger Verwendung finden. In einer besonders vorteilhaften Ausführung werden dabei die zu übertragenden Daten mit einer persönlichen Signatur, z.B. der Bürgerkarte, e-card verschlüsselt. In einer vorteilhaften Ausführung erfolgt die Übertragung verschlüsselt. Die Entschlüsselung erfolgt in der gesicherten Umgebung der Datenbank 11.

Es kann dabei für den Benutzer von großem Vorteil sein, dass KEINE Entschlüsselung in der gesicherten Umgebung der Datenbank 11 erfolgt. Ein Beispiel dafür sind streng vertrauliche Informationen die auf dem Datenkonto der gesicherten Umgebung der Datenbank langfristig gesichert werden, und welche mit einer persönlichen digitalen Signatur, z.B. mittels Bürgerkarte, verschlüsselt sind.

In einer vorteilhaften Ausführungsform kann der Speicherort, in dem Speicherbereich der dem Benutzer in der gesicherten Umgebung der Datenbank 11 zugewiesen ist frei ausgewählt werden.

Bevorzugt erfolgt die Speicherung der Daten auf der Datenbank 11 in einem dafür vorgesehenen Verzeichnis.

In einer vorteilhaften Ausführungsform kann ein neues Verzeichnis auf der Datenbank 11 in dem für den Kunden zugewiesenen Bereich zur Speicherung angelegt werden.

In einer vorteilhaften Ausführung wird die Verzeichnisstruktur bei der Übertragung vom Datenträger 7 zur gesicherten Umgebung der Datenbank 11, bzw. dem Datenkonto übernommen.

In einer vorteilhaften Ausführungsform sind die Daten inkl. Verzeichnisform auf dem Datenträger 7 gepackt z.B. ZIP, RAR, ...

In einer bevorzugten Ausführungsform können alle Dateitypen auf dem Datenschließfach auf der Datenbank 11 gespeichert werden.

Besonders vorteilhaft ist das Verfahren bei Übertragung von größeren Datenmengen und hohem Sicherheitsbedarf.

In einer weiteren Ausführungsform können den Daten vor, während oder nach der Übertragung verschiedene Sicherheitseigenschaften gegeben werden.

In einer besonders vorteilhaften Ausführung können die Daten in der gesicherten Umgebung der Datenbank 11 vom Datenübertragungsgerät über einen Bildschirm 2, einem Tastenpad 3, und weiteren Eingabeeinheiten, wie beispielsweise Soft-Keys 8 oder einem Touch-Pad am Bildschirm 2 verwaltet werden. Der Zugriff erfolgt dabei nach strenger Authentifizierung durch Karte und Code über das Terminal des Zahlungsverkehrs. Die Verwaltung inkludiert die Vergabe von Zugriffsrechten, das Löschen und Verschieben der Daten, die Verschiebung von Daten in Daten-Transfer-Konten, die Einteilung der Daten in unterschiedliche Datenklassen wie bspw. „private", „öffentlich", etc.

Darüber hinaus kann der Benutzer dem Eigentümer der gesicherten Umgebung, z.B. einer Bank, über die Kommunikationshilfen am Datenübertragungsgerät (Bildschirm 2, einem Tastenpad 3, und weiteren Eingabeeinheiten, wie beispielsweise Soft-Keys 8 oder einem Touch-Pad am Bildschirm 2) einen Auftrag zum Ausdrucken von Dokumenten erteilen.

In einer besonders vorteilhaften Ausführungsform hat der Benutzer auch die Möglichkeit Überweisungen von Daten auf andere Datenkonten mittels Kommunikationshilfen am Datenübertragungsgerät durchzuführen und in Auftrag zu geben. Diese Aufträge können auch das Drucken von Dokumenten und Versenden auf elektronischem oder anderen Wege beinhalten.

Fig. 2 zeigt ein Beispiel für den Anmelde- und Zugriffsvorgang im Ablaufschema.

Nach dem Authentifizierungsvorgang (12) mit Karte (7) und Code (13) werden dem Benutzer in der Auswahl 14 die bekannten Bankdienstleistungen 15 oder die Datenverwaltung 16 angeboten. In der Auswahl Datenverwaltung besteht dann beispielsweise die Möglichkeit Daten zu verwalten (17) und Datentransaktionen durchzuführen (18), wobei hier optional eine weitere Karte (19) oder ein weiteres Speichermedium (20) zur Anwendung kommen kann. Als weitere Auswahl kann ein Menü zur Verwaltung des Datenkontos angeboten werden.

Ansprüche:

1. Verfahren zur Speicherung von Daten mittels Geldautomat und Speichermedium durch Übertragung von Daten eines ungesicherten mitgebrachten Speichermediums (7) beispielsweise in Form eines USB Sticks oder einer Speicherkarte oder einem Bereich auf der Speicherkarte von und zu einem sicheren zentralen Datenspeicher (11) über gesicherte Kommunikationsnetzwerke (9), *dadurch gekennzeichnet*, dass als Datenschnittstelle zwischen dem unsicheren Speichermedium (7) und dem sicheren Kommunikationsnetzwerk (9) und dem zentralen Datenspeicher (11) ein Gerät des bargeldlosen Zahlungsverkehrs (1) verwendet wird.

2. Verfahren nach 1 *dadurch gekennzeichnet*, dass Authentifizierung für die sichere Verbindung (9) zum sicheren Datenspeicher (11) durch Eingabe des PIN und Verwendung der Codekarte (Bankomatkarte) (7) erfolgt, wie wenn über Zugriff auf das Konto (10) Bargeld behoben werden würde.

3. Verfahren nach 1 und 2 *dadurch gekennzeichnet*, dass die Schnittstelle (1) zum gesicher-

ten Netz (9) ein öffentlicher Geldausgabeautomat ist.

4. Verfahren nach 1 und 2 *dadurch gekennzeichnet*, dass die Schnittstelle (1) zum gesicherten Netz (9) ein privates bargeldloses Terminal zum Bezahlen, also ein Bankomatkassenterminal in Geschäften ist.

5. Verfahren nach 1 und 2 *dadurch gekennzeichnet*, dass die Schnittstelle (1) zum gesicherten Netz (9) ein privates, meist bankeigenes Terminal zum Verwalten des Kontos, also ein Kontoauszugsdrucker wie in Bankfoyers üblich, ist.

6. Verfahren nach 1 - 5, *dadurch gekennzeichnet*, dass der Datenträger zur Authentifizierung, z.B. Bankomatkarte, gleichzeitig der Datenspeicher ist bzw. ein frei zugänglicher Datenbereich für die eigenen zu übertragenen Daten genützt werden kann.

7. Verfahren nach 1 - 6, *dadurch gekennzeichnet*, dass der mitgebrachte unsichere Datenspeicher (7) über eine weitere serielle oder parallele, kontaktierte oder kontaktlose Datenschnittstelle, z.B. USB, NFC, Firewire, an das Gerät (1) angeschlossen wird.

8. Verfahren nach 1 - 6, *dadurch gekennzeichnet*, dass der mitgebrachte unsichere Datenspeicher (7) eine zweite Smartcard (Memorycard) mit gleichen physikalischen Schnittstellen wie die Bankomatkarte ist, die mit demselben Lesegerät (6) gelesen bzw. beschrieben wird und ausschließlich Datenspeicherfunktion hat.

9. Verfahren nach 1 - 6 und 8 *dadurch gekennzeichnet*, dass der weitere Datenspeicher innerhalb einer Zeit nach der Entnahme der den Benutzer authentifizierenden Karte in den Kartenleser (6) eingegeben werden muss, um diese Karte als zulässigen Datenspeicher anzuerkennen.

10. Verfahren nach 1 - 6, 8 und 9, *dadurch gekennzeichnet* dass der für dasselbe Lesegerät (6) verwendete Datenträger eine eigene Verschlüsselung mit eigenem Code verwendet und dieser Code über die Tastatur (3) eingegeben wird.

11. Verfahren nach 1 - 6, 8 und 9, *dadurch gekennzeichnet* dass der für dasselbe Lesegerät (6) verwendete Datenträger eine eigene Verschlüsselung mit eigenem Code verwendet und dieser Code auf der authentifizierenden Codekarte, z.B. Bankomatkarte, gespeichert ist.

12. Verfahren nach 1 - 6, 8 und 9, *dadurch gekennzeichnet* dass mit dasselben Lesegerät (6) eine erste Karte z.B. Bankomatkarte für die Authentifizierung bei der Datenbank (11), eine zweite Karte, z.B. Bürgerkarte für die Verschlüsselung der Übertragung über das Medium (9) und eine dritte Karte als Datenspeicher verwendet werden, die in einer vorgegebenen Reihenfolge in das Lesegerät eingegeben werden.

13. Verfahren nach 1 - 12, *dadurch gekennzeichnet* dass die gespeicherten und zwischen mitgebrachtem unsicheren Speicher (7) und dem sicheren Datenspeicher (11) zu übertragenden Daten beliebige Datenformate, z.B. doc, jpg, mpg, pdf, tif, rtf, wma haben können.

14. Verfahren nach 1 - 13, *dadurch gekennzeichnet* dass über zusätzliche Eingaben über die Tastatur (3) eine von mehreren zur Auswahl stehende zentrale sichere Datenspeicher (11) zur Speicherung oder zum Auslesen ausgewählt werden können.

15. Verfahren nach 1 - 13, *dadurch gekennzeichnet* dass einer von mehreren zur Auswahl stehenden zentralen sicheren Datenspeichern (11) zur Speicherung oder zum Auslesen durch die auf der zweiten Karte gemäß Anspruch (8) gespeicherten zusätzlichen Informationen ausgewählt werden können.

16. Verfahren nach 1 - 15, *dadurch gekennzeichnet* dass den Daten nach der Übertragung spezifische Dateneigenschaften, z.B. Ablaufdatum, Leseberechtigungen, Löschberechtigung, Änderungsberechtigungen über die Tastatur (8) oder (3) zugewiesen werden.

17. Verfahren nach 1 - 16, *dadurch gekennzeichnet* dass das Verwalten, also das Sichten, Löschen, Weiterleiten, Kopieren, Verschieben, Umbenennen, Senden der Daten direkt am Benutzerinterface mit Tastatur (3) und (8) und Display (2) Gerät des bargeldlosen Zahlungsverkehrs aus Anspruch 1 erfolgt.

Hiezu 2 Blatt Zeichnungen

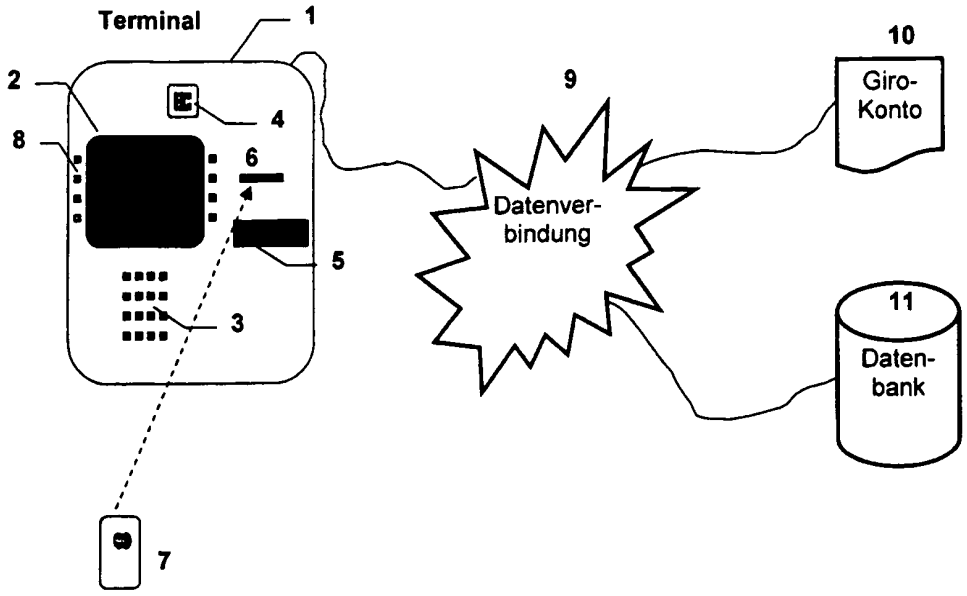
Terminal
1
2
4
8
6
5
3
7
9
Datenver-
bindung
10
Giro-
Konto
11
Daten-
bank

Fig. 1

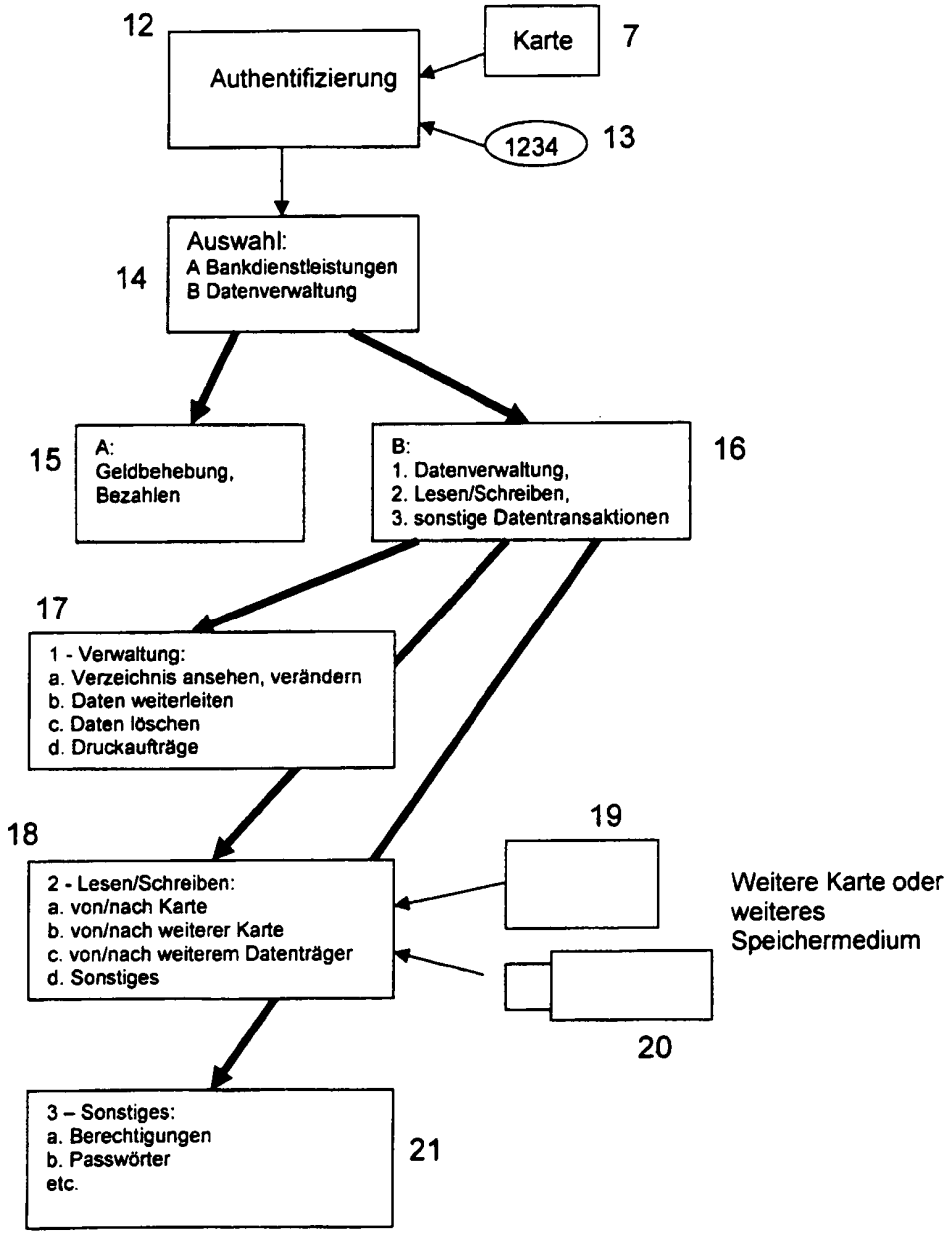

Fig. 2 - Ablauf von Datenverwaltung und Datentransaktion am Bankomat

Recherchenbericht zu **GM 8093/07**
Technische Abteilung 1A

österreichisches patentamt

Klassifikation des Anmeldungsgegenstands gemäß IPC[8]: ***G07F 7/10*** (2006.01); ***G07F 19/00*** (2006.01)	**AT 010 306 U1**
Klassifikation des Anmeldungsgegenstands gemäß ECLA: G07F 7/10D10M, G07F 7/10D16, G07F 19/00F	
Recherchierter Prüfstoff (Klassifikation): G07F	
Konsultierte Online-Datenbank: EPODOC, WPI, cl txtn	

Dieser Recherchenbericht wurde zu den **am 31.10.2006 eingereichten** Ansprüchen erstellt.

Die in der Gebrauchsmusterschrift veröffentlichten Ansprüche könnten im Verfahren geändert worden sein (§ 19 Abs. 4 GMG), sodass die Angaben im Recherchenbericht, wie Bezugnahme auf bestimmte Ansprüche, Angabe von Kategorien (X, Y, A), nicht mehr zutreffend sein müssen. In die dem Recherchenbericht zugrundeliegende Fassung der Ansprüche kann beim Österreichischen Patentamt während der Amtsstunden Einsicht genommen werden.

Kategorie*)	Bezeichnung der Veröffentlichung: Ländercode, Veröffentlichungsnummer, Dokumentart (Anmelder), Veröffentlichungsdatum, Textstelle oder Figur soweit erforderlich	Betreffend Anspruch
X	US 2002/0129257 (Parmelee et al.) 12. September 2002 (12.09.2002) Fig. 1, 2, 18, Seiten4 - 8	1 - 5, 13 - 16
Y	Fig. 1, 2, 18, Seiten4 - 8	6 - 9, 12
Y	US 5 521 363 A (Tannenbaum) 28. Mai 1996 (28.05.1996) Fig. 2, 3, Spalten 5, 6	6 - 9
Y	EP 0 936 583 A1 (Al-Khaja) 18. August 1999 (18.08.1999) Fig. 1, Spalte 2	12

*) **Kategorien** der angeführten Dokumente:

- **X** Veröffentlichung **von besonderer Bedeutung**: der Anmeldungsgegenstand kann allein aufgrund dieser Druckschrift nicht als neu bzw. auf erfinderischer Tätigkeit beruhend betrachtet werden.
- **Y** Veröffentlichung **von Bedeutung**: der Anmeldungsgegenstand kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren weiteren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese **Verbindung für einen Fachmann naheliegend** ist.
- **A** Veröffentlichung, die den **allgemeinen Stand der Technik** definiert.
- **P** Dokument, das **von Bedeutung** ist (Kategorien **X** oder **Y**), jedoch **nach dem Prioritätstag** der Anmeldung **veröffentlicht** wurde.
- **E** Dokument, das **von besonderer Bedeutung** ist (Kategorie **X**), aus dem ein **älteres Recht** hervorgehen könnte (früheres Anmeldedatum, jedoch nachveröffentlicht, Schutz in Österreich möglich, würde Neuheit in Frage stellen).
- **&** Veröffentlichung, die Mitglied derselben **Patentfamilie** ist.

Datum der Beendigung der Recherche:	☐ Fortsetzung siehe Folgeblatt	Prüfer(in):
26. Mai 2008		Dipl.-Ing. STEINZ-KRISMANIC