(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
28. August 2003 (28.08.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/071492 A2

(51) Internationale Patentklassifikation[7]: G07C 9/00

(21) Internationales Aktenzeichen: PCT/EP03/01678

(22) Internationales Anmeldedatum:
19. Februar 2003 (19.02.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 07 056.3 20. Februar 2002 (20.02.2002) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **MEISTER, Gisela** [DE/DE]; Stademannstrasse 11, 81737 München (DE).

(74) Anwalt: **KLUNKER, SCHMITT-NILSON, HIRSCH**; Winzererstrasse 106, 80797 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(54) **Title:** METHOD FOR DETERMINATION OF THE AUTHORISATION OF A PERSON TO USE A PORTABLE DATA SUPPORT

(54) **Bezeichnung:** VERFAHREN ZUM NACHWEIS DER BERECHTIGUNG EINER PERSON ZUR NUTZUNG EINES TRAGBAREN DATENTRÄGERS

(57) **Abstract:** A method for determination of the authorisation of a person to use a portable data support (10), with a checking device (32) is disclosed. A biometric feature of the authorised person is used by the checking device (32) to reproduce a data support code also stored on the data support (10) on a utilisation occurring. The data support code (DTK, CV) is formed by modification of a reference data set (BIO_R) derived from the biometric feature. The data support code (DTK, CV) unequivocally assigns the data support (10) to a present authorised person. As the biometric feature is only used in modified form it is not possible to simulate a data support (10) merely with knowledge of the biometric reference data set (BIO_R).

(57) **Zusammenfassung:** Vorgeschlagen wird ein Verfahren zum Nachweis der Berechtigung einer Person zur Nutzung eines tragbaren Datenträgers (10) gegenüber einer Prüfeinrichtung (32). Für eine Nutzung wird durch die Prüfeinrichtung (32), ausgehend von einem biometrischen Merkmal der berechtigten Person eine auch auf dem Datenträger (10) gespeicherte Datenträgerkennung nachgebildet. Die Bildung der Datenträgerkennung (DTK, CV) erfolgt durch Verfremdung eines aus dem biometrischen Merkmal abgeleiteten Referenzdatensatzes (BIO_R); die Datenträgerkennung (DTK, CV) ordnet den Datenträger (10) eindeutig einer präsenten, berechtigten Person zu. Da das biometrische Merkmal nur in veränderter Form genutzt wird, ist es selbst bei Kenntnis des biometrischen Referenzdatensatzes (BIO_R) nicht möglich, einen Datenträger (10) zu simulieren.

WO 03/071492 A2

Verfahren zum Nachweis der Berechtigung einer Person zur Nutzung eines tragbaren Datenträgers

Die Erfindung geht aus von einem Verfahren nach der Gattung des Hauptanspruchs. Ein solches ist z.B. aus der US 5,280,527 bekannt. Danach wird auf einer IC-Karte eine Dateninformation abgelegt, die aus einem biometrischen Merkmal einer zur Nutzung berechtigten Person abgeleitet wurde. Die IC-Karte besitzt desweiteren einen Sensor zur Erkennung des biometrischen Merkmales. Um den Datenträger zu nutzen, muß die nutzende Person das biometrische Merkmal an dem Sensor erneut bereitstellen. Die IC-Karte bildet daraus wiederum eine abgeleitete Information und vergleicht sie mit der gespeicherten biometrischen Dateninformation. Bei Übereinstimmung gibt sie die beabsichtigte Nutzung frei. Das Verfahren gewährleistet, daß eine IC-Karte nur von einer anwesenden, berechtigten Person genutzt werden kann. Es erfordert allerdings die Bereitstellung von aufwendigen und damit teuren IC-Karten.

WO 01/15378 offenbart ein Verfahren zum Schutz einer digitalen Signatur, das sicherstellt, daß eine digitalen Signatur nur durch die berechtigte Person verwendet werden kann. Hierzu wird zunächst ein biometrisches Merkmal der Person ermittelt und durch Digitalisierung in eine binäre Repräsentation überführt. Desweiteren wird der Signaturschlüssel unter Verwendung eines fehlertoleranten Kodierungsverfahrens in einen Schlüsselkode überführt. Anschließend wird der Schlüsselkode mit der binären Repräsentation des biometrischen Merkmales verknüpft. Um den in dem verknüpften Schlüsselkode enthaltenen Signaturschlüssel nachfolgend wiederzuerlangen, muß erneut das biometrische Merkmal der berechtigten Person bereitgestellt werden, welches darauf wiederum digitalisiert und in eine binäre Repräsentation überführt wird. Mit der binären Repräsentation wird sodann der verknüpfte Schlüsselkode entschlüsselt. Aus dem Ergebnis wird schließlich unter Einbeziehung des eingesetzten fehlertoleranten Kodierungsverfahrens

der Signaturschlüssel wiederhergestellt. Die Rückgewinnung gelingt nur, wenn das von der Person gelieferte biometrische Merkmal höchstens im Rahmen der zulässigen Toleranz von den zur Verknüpfung der geheimzuhaltenden Daten eingesetzten abweicht.

Eine gemäß diesem bekannten Verfahren gesicherte Signatur ist gegen kryptologische Ausspähungsversuche gut geschützt. Angreifbar ist es gleichwohl, wenn das zur Entschlüsselung verwendete biometrische Merkmal manipuliert wurde und nicht von der berechtigten Person bereitgestellt wird. So kann der Fingerabdruck einer Person beispielsweise von einem von dieser Person verwendeten Gebrauchsgegenstand ohne das Wissen der Person genommen werden. Die Verwendung des Verfahrens zum Schutz von geheimzuhaltenden Daten bietet sich deshalb bevorzugt für Anwendungen in sicheren Nutzungsumgebungen an, in denen gewährleistet ist, daß ein biometrisches Merkmal nur von einer tatsächlich anwesenden, berechtigten Person bereitgestellt werden kann. Bei Anwendung in Chipkartensystemen erfordert das Verfahren zudem die Durchführung der Signaturrückgewinnung direkt auf der Chipkarte, weil die Signatur anderenfalls zumindest vorübergehend im Klartext außerhalb der Chipkarte vorliegen würde und dort angreifbar wäre.

WO 98/50875 offenbart ein Verfahren zur Authentisierung einer elektronischen Transaktion, welches auf einer Kopplung eines biometrischen Identifikationsverfahrens mit einem Signaturverfahren sowie einem Zertifizierungskonzept beruht. Zum Nachweis der Berechtigung eines Nutzers zur Durchführung einer Transaktion werden einer Transaktionsausführungseinrichtung über ein Datennetz zum einen biometrische Daten des Nutzers, zum anderen eine mittels dieser biometrischen Daten gebildete digitale Signatur übermittelt. In der Transaktionsausführungseinrichtung werden die

übermittelten biometrischen Daten mit aus zertifizierten Referenzdaten zurückgenommenen biometrischen Musterdaten verglichen. Die zertifizierten Referenzdaten sind in der Transaktionsausführungseinrichtung in einem Speicher abgelegt, der in Gestalt einer Chipkarte realisiert sein kann. Desweiteren wird die übermittelte Signatur geprüft, indem in der Prüfeinrichtung aus den übermittelten biometrischen Daten eine Referenzsignatur gebildet wird. Indem es biometrische Daten mit vom Nutzer einzugebenden Identifizierungsdaten verknüpft, verhindert das Verfahren Manipulationen mittels unrechtmäßig erworbener Biometriedaten. Für die Rückgewinnung der biometrischen Musterdaten erfordert das Verfahren allerdings notwendig die Einbindung einer Zertifizierungsstelle.

Aufbau, Herstellung und Handhabung tragbarer Datenträger sowie der zugehörigen Systeme sind z.B. in dem „Handbuch der Chipkarte", Rankl, Effing, 3. Auflage, 1999, Hanser-Verlag, beschrieben. Eine Übersicht über die eingesetzten kryptographischen Techniken und ihre Grundlagen findet sich unter anderem in „Angewandte Kryptographie",B. Schneider, 1996, Addison-Wesley-Verlag.

Der Erfindung liegt nun die Aufgabe zugrunde, für ein auf einem tragbaren Datenträger basierendes Transaktionssystem ein einfach realisierbares Authentisierungsverfahren anzugeben, das es erlaubt, die Nutzung eines tragbaren Datenträgers nur durch eine dazu berechtigten Person sicherzustellen.

Diese Aufgabe wird gelöst durch ein Verfahren mit den Merkmalen des Hauptanspruchs.

Erfindungsgemäß werden die Datenträger mit einer Datenträgerkennung versehen, die durch Verfremdung eines aus einem biometrischen Merkmal

einer berechtigten Person abgeleiteten Referenzdatensatzes gebildet wird. Mittels einer solchermaßen gebildeten Datenträgerkennung wird ein Datenträger eindeutig einer bestimmten Person zugeordnet. Da das biometrische Merkmal nur in veränderter Form genutzt wird, ist es selbst bei Kenntnis des biometrischen Merkmales nicht möglich, einen Datenträger zu simulieren. Das erfindungsgemäße Verfahren hat weiter den Vorteil, daß keine Übertragung eines biometrischen Merkmales oder daraus abgeleiteter Daten zu dem tragbaren Datenträger hin notwendig ist. Die Authentisierung eines tragbaren Datenträgers erfolgt vollständig in der beteiligten Prüfeinrichtung. Der tragbare Datenträger muß nicht dazu ausgebildet sein, auf dem Datenträger eine Berechtigungsprüfung vorzunehmen. Als tragbare Datenträger können deshalb, ohne daß Änderungen an der technischen Realisierung vorzunehmen wären, gängige Bauformen, wie insbesondere gängige Chipkarten eingesetzt werden. Das erfindungsgemäße Verfahren ist entsprechend einfach einrichtbar und läßt sich insbesondere in der Regel als Softwarelösung auf vorhandenen Geräten einrichten.

In einer vorteilhaften ersten Ausführungsform erfolgt die Verfremdung des zu einem biometrischen Merkmal gebildeten digitalen Datensatzes nach einem symmetrischen Verschlüsselungsverfahren unter Verwendung eines Hauptschlüssels. Dieser Hauptschlüssel wird auch einer Prüfeinrichtung mitgeteilt und ermöglicht dieser die Durchführung einer Berechtigungsprüfung. In einer bevorzugten Ausführung wird ein symmetrisches Verschlüsselungsverfahren, etwa eine DES3-Verschlüsselung eingesetzt.

In einer zweiten vorteilhaften Ausführungsvariante des erfindungsgemäßen Verfahrens erfolgt die Verfremdung des aus dem biometrischen Merkmal gebildeten Datensatzes durch Bildung eines Zertifikats über den digitalen Datensatz und Verwendung asymmetrischer Schlüsselpaare.

In einer zweckmäßigen Weiterbildung des erfindungsgemäßen Verfahrens wird die zu prüfende Datenträgerkennung des Vergleichsdatensatzes nicht aus einem hierzu aufgenommenen biometrischen Merkmal der nutzenden Person abgeleitet, sondern durch die Prüfeinrichtung von dem Datenträger angefordert. Der angeforderte digitale Datensatz wird dann in der Prüfeinrichtung nach dem gleichen kryptographischen Verfahren verschlüsselt wie es zur Bildung der Datenträgerkennung für den tragbaren Datenträger eingesetzt wurde. Das von der Prüfeinrichtung erzielte Ergebnis wird mit der von dem tragbaren Datenträger erhaltenen Datenträgerkennung verglichen.

In einer Variante dieser Ausführungsform kann vorgesehen sein, daß an der Prüfeinrichtung ein biometrisches Merkmal der nutzenden Person aufgenommen, daraus ein digitaler Vergleichsdatensatz abgeleitet und dieser mit dem von dem tragbaren Datenträger angeforderten digitalen Datensatz verglichen wird, bevor mit dem angeforderten digitalen Datensatz die Datenträgerkennung in der Prüfeinrichtung nachgebildet wird. Die Verwendung dieser Variante bietet sich z.B. an, wenn die Aufnahme des biometrischen Merkmales an der Prüfeinrichtung und seine nachfolgende Digitalisierung zu einem digitalen Vergleichsdatensatz führt, der verfahrensbedingt stark von dem auf dem tragbaren Datenträger gespeicherten digitalen Datensatz abweichen kann, so daß eine Verwendung eines solchen Vergleichsdatensatzes zur Nachbildung einer Datenträgerkennung zu unbrauchbaren Ergebnissen führen würde.

Unter Bezugnahme auf die Zeichnung werden nachfolgend Ausführungsbeispiele der Erfindung näher erläutert.

Es zeigen:

Fig. 1 die Struktur eines Transaktionssystems, in dem eine berechtigte Person bei Präsentation eines tragbaren Datenträgers Transaktionen ausführen kann,

Fig. 2 die Struktur einer Anordnung zur Personalisierung eines tragbaren Datenträgers,

Fig. 3 die Durchführung einer Berechtigungsprüfung basierend auf der Verwendung einer symmetrischen Verschlüsselungstechnik,

Fig. 4 die Durchführung einer Berechtigungsprüfung basierend auf der Verwendung einer symmetrischen Verschlüsselungstechnik.

Fig. 1 zeigt die Struktur eines Transaktionssystems, in dem zur Nutzung berechtigte Personen Transaktionen ausführen oder Dienste in Anspruch können. Das System wird gebildet von einem tragbaren Datenträger 10, einem Terminal 20, einem Hintergrundsystem 30 sowie einer Transaktionszentrale 34. Die Transaktionen bzw. Dienste selbst sowie die Prüfung der Berechtigung einer Person zur Nutzung bzw. Inanspruchnahme basieren wesentlich aus Softwarelösungen.

Der tragbare Datenträger 10 dient zum Nachweis der Berechtigung einer Person zur Nutzung des Transaktionssystems. Er ist hierzu mit einem integrierten Schaltkreis 12 ausgestattet, in dem auf eine berechtigte Person bezogene Daten abgelegt sind. Dem integrierten Schaltkreis 12 ist eine Schnitt-

stelle 14 zugeordnet, über welche die personenbezogenen Daten auslesbar sind. In zweckmäßiger Ausgestaltung besitzt der tragbare Datenträger 10 die Form einer Chipkarte im ISO/IEC-Norm-Format. Die Schnittstelle 14 besitzt dann bei kontaktbehafteter Ausführung wie in Fig. 1 angedeutet, die Gestalt eines Kontaktfeldes oder, alternativ, bei nichtkontaktierender Ausführung die Gestalt einer Spule. Neben Chipkartenform kann der tragbare Datenträger 10 beliebige andere geeignete Bauformen aufweisen, etwa die einer Armbanduhr oder eines Handys. Der integrierte Schaltkreis 12 ist ferner dazu eingerichtet, über die Schnittstelle 14 eingehende Informationen einer kryptographischen Bearbeitung zu unterziehen. Die genaue Realisierung der eingesetzten kryptographischen Technik ist dabei nicht Gegenstand dieser Erfindung. Hinsichtlich der Ausführung wird vielmehr auf die einschlägige Literatur verwiesen, etwa auf das eingangs zitierte Buch von B. Schneider.

Wesentliche Elemente des Terminals 20 sind ein Sensor 22 zur Erfassung eines biometrischen Merkmales einer Nutzung beabsichtigenden Person, eine zu der Schnittstelle 14 des tragbaren Datenträgers 10 korrespondierende Datenträgerschnittstelle 24 zum Zugriff auf die im integrierten Schaltkreis 12 des tragbaren Datenträgers 10 abgelegten personenbezogenen Daten sowie ein mit dem Sensor 22 und der Datenträgerschnittstelle 24 verbundenes Sicherheitsmodul 26, welches die Prüfung der Berechtigung einer Person zur Ausführung einer Transaktion vornimmt.

Der Sensor 22 nimmt ein von einer Person bereitgestelltes biometrisches Merkmal auf und bildet daraus einen -auch als *Template* bezeichneten - biometrischen Datensatz BIO, der ein in dem biometrischen Merkmal enthaltenes Muster wiedergibt. Bei dem Sensor 22 kann es sich, wie in Fig. 1 angedeutet, um einen Fingerabdrucksensor handeln. In anderer Ausführung kann der Sensor 22 eine Iris-Scanner-Einrichtung, eine Stimmerkennungs-

Einrichtung, ein Temperaturfühler oder eine andere Anordnung zur Erfassung eines biometrischen Merkmales sein. Der Sensor 22 kann auch aus einer Kombination von Einrichtungen zur Erfassung verschiedener biometrischer Merkmale bestehen, etwa aus der Kombination eines Fingerabdrucksensors und einer Iris-Erkennung. Der Sensor 22 verfügt desweiteren über Datenverarbeitungsmittel, um ein aufgenommenes biometrisches Merkmal in einen Datensatz umzusetzen.

Die Datenträgerschnittstelle 24 hat bei Ausführung des tragbaren Datenträgers als kontaktbehaftete Norm-Chipkarte die Gestalt einer üblichen Lese-/Schreibeinheit. Bei kontaktlos kommunizierenden tragbaren Datenträgern 10 hat sie typischerweise die Form einer Sende-/Empfangsantenne.

Das Sicherheitsmodul 26 ist mit den Mitteln einer üblichen Datenverarbeitungsanordnung realisiert und basiert auf den Komponenten eines üblichen Computers. Es ist als eigenständige Einheit innerhalb des Terminals 20 oder als Teil einer zentralen Prozessoreinheit des Terminals 20 realisiert.

Das Terminal 20 kann z.B. ein Bankautomat, ein Fahrkartenautomat oder ein Warenautomat sein und entsprechend z.B. zur Durchführung von Banktransaktionen, zur Ausgabe von Fahrkarten oder zur Ausgabe von Waren dienen.

Mit dem Terminal 20 über ein Datennetz 36 verbunden ist eine Transaktionszentrale 34. Sie führt nach erfolgreichem Nachweis der Berechtigung einer Person die von der Person gewünschte Transaktion ganz oder in Teilen aus bzw. stellt den gewünschten Dienst zur Verfügung. Ist das Terminal 20 etwa ein Bankautomat und die von der Nutzung beabsichtigenden Person gewünschte Transaktion eine Geldbewegung zwischen zwei Konten, führt

die Transaktionszentrale 34 z.B. die entsprechenden Last- bzw. Gutschriften aus. Die Transaktionszentrale 34 ist optional. Ist eine Transaktion vollständig an einem Terminal 20 ausführbar, entfällt sie.

Das Hintergrundsystem 30 ist mit dem Sicherheitsmodul 26 verbunden. Es besitzt die typischen Elemente eines Computers und ist z.B. in einem Rechenzentrum oder innerhalb einer Transaktionszentrale 34 realisiert. Bei ausreichender Leistungsfähigkeit des Sicherheitsmodules 26 kann das Hintergrundsystem 30 auch entfallen. Das Hintergrundsystem 30 führt solche Teile der von dem Sicherheitsmodul 26 ausgeführten Berechtigungsprüfungen aus, deren Ausführung in dem Sicherheitsmodul 26 nicht möglich oder nicht zweckmäßig ist. Beispielsweise verwaltet das Hintergrundsystem 30 die im Zuge einer Berechtigungsprüfung benötigten Schlüssel und stellt sie dem Sicherheitsmodul 26 zur Verfügung. Zweckmäßig sind in dem Hintergrundsystem 30 vor allem solche Teile einer Berechtigungsprüfung realisiert, die von einer Mehrzahl von Terminals 20 in Anspruch genommen werden. Das Hintergrundsystem 30 kann entsprechend mit einer Mehrzahl von Terminals 20 verbunden sein. Im Hinblick auf die hier beschriebene Erfindung bildet das Hintergrundsystem 30 eine funktionale Einheit mit dem Sicherheitsmodul 26. Sicherheitsmodul 26 und Hintergrundsystem 30 werden deshalb nachfolgend zusammengefaßt als Prüfeinrichtung 32 bezeichnet. Die Prüfeinrichtung 32 ist gleichfalls dazu eingerichtet, eingehende Informationen einer kryptographischen Bearbeitung zu unterziehen. Die genaue Realisierung der eingesetzten kryptographischen Techniken ist dabei wiederum nicht Gegenstand dieser Erfindung. Hinsichtlich der Ausführung wird vielmehr ebenfalls auf die einschlägige Literatur verwiesen, etwa auf das zitierte Buch von B. Schneider.

Fig. 2 zeigt eine Anordnung zur Personalisierung eines tragbaren Datenträgers 10 durch Einbringen von personenbezogenen Daten in den integrierten Schaltkreis 12. Sie umfaßt einen Sensor 22 zur Aufnahme eines biometrischen Merkmales einer Person, eine Registrierungsstelle 80 sowie eine Personalisierungsstelle 82.

Der Sensor 22 ist vom gleichen Typ wie der in Fig. 1 als Teil des Transaktionssystems wiedergegebene Sensor 22 und ermöglicht die Erfassung desselben biometrischen Merkmals. Zu einem erfaßten biometrischen Merkmal liefert er einen biometrischen Referenzdatensatz BIO_R (*template*), welcher ein in dem aufgenommenen biometrischen Merkmal enthaltenes Referenzmuster beschreibt. Die Erzeugung des Referenzdatensatzes BIO_R erfolgt im wesentlichen durch Ausführung eines Softwareprogrammes. Der Sensor 22 verfügt über entsprechende Datenverarbeitungsmittel.

Der Sensor 22 ist direkt mit der Registrierungsstelle 80 verbunden und zweckmäßig unmittelbar bei dieser aufgestellt. Die Registrierungsstelle 80 wiederum befindet sich vorzugsweise beim Herausgeber der tragbaren Datenträger 10, bei einem Betreiber eines Terminals 20 oder bei einem Anbieter eines Dienstes.

Die Personalisierungsstelle 82 befindet sich in der Regel vorzugsweise bei einem Hersteller oder einem Herausgeber von tragbaren Datenträgern 10. Sie beinhaltet alle üblichen Elemente eines Computers und ist insbesondere dazu eingerichtet, auf zugeführte Informationen kryptographische Techniken anzuwenden. Die verschiedenen möglichen Bearbeitungen sind in der Regel in Form von Softwareprogrammen angelegt.

Die Personalisierung eines tragbaren Datenträgers 10 erfolgt in der Regel im Rahmen einer einmalig durchgeführten Vorbereitungsphase und geschieht beispielsweise wie folgt. Mittels des Sensors 22 wird an einer Registrierungsstelle 80 ein biometrischer Referenzdatensatz BIO_R einer Person, die zur Nutzung eines tragbaren Datenträgers 10 berechtigt sein soll, aufgenommen. Der aufgenommene biometrische Referenzdatensatz BIO_R wird authentisch an die Personalisierungsstelle 82 weitergeleitet.

In der Personalisierungsstelle 82 wird der biometrische Referenzdatensatz BIO_R verfremdet. Hierzu wird er einer Digitalisierungsstufe 40 zugeführt und einer Digitalisierung unterworfen. Dabei wird der biometrische Referenzdatensatz BIO_R durch Anwendung geeigneter mathematischer Methoden in einen digitalen Referenzdatensatz DRT überführt. Vorzugsweise hat der digitale Referenzdatensatz DRT die Gestalt eines Digitalwertes mit einer vorbestimmten Anzahl von Stellen. Geeignete mathematische Methoden zur Durchführung der Digitalisierung finden sich in der einschlägigen Literatur, etwa in der eingangs referierten WO 01/15378.

Weiterhin wird in der Personalisierungsstelle 82 ein Hauptschlüssel (*master key*) MK bereitgestellt. Unter Verwendung dieses Hauptschlüssel MK wird der digitale Referenzdatensatz DRT in einer Verschlüsselungsstufe 82 einer Verschlüsselung mittels eines symmetrischen Verschlüsselungsverfahrens unterworfen. Vorzugsweise wird er, wie in Fig. 2 angedeutet, durch Ausführung eines DES3-(*Triple-DES*)-Verfahrens verschlüsselt. Das DES3-Verfahren ist u.a. in dem eingangs zitierten Buch von B. Schneider beschrieben. Aus der Verschlüsselung resultiert eine Datenträgerkennung DTK. Der digitale Referenzdatensatz DRT und die Datenträgerkennung DTK werden sodann als Personalisierungsdaten auf den tragbaren Datenträger 10 gebracht und in dessen integrierten Schaltkreis 12 gespeichert.

Alternativ oder zusätzlich ist die Personalisierungsstelle 82 dazu eingerichtet, unter Verwendung eines geheimen Schlüssels GS_Z (*secret key*) einer - nicht gezeigten - Zertifizierungsstelle in einer Zertifizierungsstufe 88 ein Zertifikat CV über einen öffentlichen Schlüssel $ÖS_K$ (*public key*) des tragbaren Datenträgers 10 sowie über den digitalen Referenzdatensatz DRT zu bilden. Weiterhin ist die Personalisierungsstelle 82 dazu eingerichtet, ein aus einem öffentlichen Schlüssel $ÖS_K$ und einem geheimen Schlüssel GS_K bestehendes Schlüsselpaar zur Verwendung in einem asymmetrischen Verschlüsselungsverfahren (*public key Kryptographie*) bereitzustellen. In dieser auf Verwendung eines asymmetrischen Verschlüsselungsverfahrens beruhenden Variante werden als Personalisierungsdaten der digitale Referenzdatensatz DRT, das Zertifikat CV, der öffentliche Schlüssel $ÖS_K$ sowie der korrespondierende geheime Schlüssel GS_K auf den tragbaren Datenträger 10 gebracht.

Anhand der Fig. 3 und 4 wird nachfolgend die Durchführung einer Berechtigungsprüfung basierend auf der Verwendung einer symmetrischen Verschlüsselungstechnik bzw. basierend auf der Verwendung einer asymmetrischen Verschlüsselungstechnik beschrieben. Die einzelnen Verfahrensschritte sind dabei in der Regel durch Ausführung entsprechender Softwareprogramme realisiert. Dies gilt insbesondere für die Prüfeinrichtung 32.

Bei der in Fig. 3 dargestellten Variante sind im integrierten Schaltkreis 12 des tragbaren Datenträgers 10 ein biometrischer Referenzdatensatz BIO_R, ein digitaler Referenzdatensatz DRT sowie eine Datenträgerkennung DTK angelegt. Die Datenträgerkennung DTK ist dabei durch Verschlüsselung des biometrischen Referenzdatensatzes DRT gemäß einem symmetrischen Verschlüsselungsverfahren unter Verwendung eines Hauptschlüssels MK gebildet. Der integrierte Schaltkreis 12 ist ferner dazu eingerichtet, eine zugeführ-

te Dateninformation gemäß einem definierten Verschlüsselungsverfahren mittels der Datenträgerkennung DTK als Schlüssel zu verschlüsseln.

Die Prüfeinrichtung 32 ist zur Durchführung derselben definierten Verschlüsselung eingerichtet wie der tragbare Datenträger 10. Desweiteren steht der Prüfeinrichtung 32 derselbe Hauptschlüssel MK zu Verfügung, mit dem die Datenträgerkennung DTK gebildet wurde.

Um ihre Berechtigung zur Durchführung einer Transaktion oder Nutzung eines Dienstes nachzuweisen, präsentiert die Nutzung beabsichtigende Person den tragbaren Datenträger der Prüfeinrichtung 32, welche darauf über die Schnittstellen 24, 14 in einen Datenaustausch mit dem tragbaren Datenträger 10 tritt.

Dabei übermittelt eine in der Prüfeinrichtung 32 eingerichtete Anforderungsstufe 46 dem integrierten Schaltkreis 12 des tragbaren Datenträgers 10 eine Zufallszahl ZZ.

Der integrierte Schaltkreis 12 überführt die erhaltene Zufallszahl ZZ durch Verschlüsselung gemäß dem definierten Verschlüsselungsverfahren in eine Authentifizierungsbotschaft A. Dabei dient die in dem Datenträger 10 vorhandene Datenträgerkennung DTK als Schlüssel. Die Authentifizierungsbotschaft A übermittelt der integrierte Schaltkreis 12 sodann der Prüfeinrichtung 32, welche sie an eine Vergleichsstufe 50 weiterleitet.

Unabhängig von der Präsentation des tragbaren Datenträgers 10 stellt die Nutzung beabsichtigende Person an dem Sensor 22 erneut das biometrische Merkmal bereit, von dem ausgehend auch die Datenträgerkennung DTK gebildet wurde. Der von dem Sensor 22 daraufhin aus dem erfaßten biome-

trischen Merkmal erzeugte biometrische Datensatz BIO_V, etwa ein Fingerabdruck, wird einer Digitalisierungsstufe 40 zugeführt und einer Digitalisierung unterworfen. Dabei wird es in einen digitalen Vergleichsdatensatz DVT umgesetzt, der vorzugsweise eine vorbestimmte Länge aufweist. Die Umsetzung erfolgt grundsätzlich auf dieselbe Weise wie die Ableitung des im tragbaren Datenträger 10 abgelegten digitalen Referenzdatensatzes DRT aus dem biometrischen Referenzdatensatz BIO_R. Zur Vereinfachung und Beschleunigung der Auswertung kann jedoch vorgesehen sein, daß der Vergleichsdatensatz DVT weniger umfangreich ist als der Referenzdatensatz DRT und beispielsweise weniger Stellen aufweist als jener.

Der digitale Vergleichsdatensatz DVT wird einer Verschlüsselungsstufe 42 zugeführt. Dieser steht auch der Hauptschlüssel MK zur Verfügung, mittels dessen die Bildung der Datenträgerkennung DTK erfolgte. Mit dem Hauptschlüssel MK verschlüsselt die Verschlüsselungsstufe 42 den digitalen Vergleichsdatensatz DVT gemäß demselben symmetrischen Verschlüsselungsverfahren, das auch im tragbaren Datenträger 10 zur Bildung der Datenträgerkennung DTK eingesetzt wurde und erzeugt so Probekennungsdaten PRK. Die Probekennungsdaten PRK werden sodann an eine weitere Verschlüsselungsstufe 48 weitergeleitet.

Dort bilden sie einen Schlüssel, mit dem die an den tragbaren Datenträger 10 ausgesandte Zufallszahl ZZ nach demselben definierten Verschlüsselungsverfahren verschlüsselt werden, wie es von dem Datenträger 10 eingesetzt wird. Es resultiert eine Prüfbotschaft B, welche an die Vergleichseinrichtung 50 übermittelt wird, wo sie mit der Authentifizierungsbotschaft A verglichen wird. Stellt die Vergleichseinrichtung 50 Übereinstimmung zwischen der Prüfbotschaft B und der Authentifizierungsbotschaft A fest, erkennt sie die

Nutzung beabsichtigende Person als berechtigt an und gibt die Transaktion frei bzw. eröffnet den Zugang zu dem gewünschten Dienst.

In einer Variante des in Fig. 3 dargestellten Verfahrens wird als Grundlage für die Durchführung der Digitalisierung in der Digitalisierungsstufe 40 nicht ein mittels des Sensors 22 erzeugter biometrischer Datensatz BIO_V verwendet. Stattdessen fordert die Prüfeinrichtung 32 mittels einer Anforderungsstufe 52 von dem tragbaren Datenträger 10 die Übermittlung des in dem integrierten Schaltkreis 12 gespeicherten biometrischen Referenzdatensatzes BIO_R an. Der integrierte Schaltkreis 12 übermittelt darauf den angeforderten biometrischen Datensatz BIO_R an die Prüfeinrichtung 32. Diese vergleicht nun in einer Vergleichsstufe 53 den von dem tragbaren Datenträger 10 erhaltenen biometrischen Referenzdatensatz BIO_R mit dem von dem Sensor 22 übermittelten biometrischen Datensatz BIO_V. Stimmen beide überein, stammen mithin beide von derselben Person, führt die Prüfeinrichtung 32 anschließend die von dem tragbaren Datenträger 10 übermittelten biometrischen Referenzdatensatz BIO_R der Verschlüsselungsstufe 42 zu, wo er durch Anwendung eines symmetrischen Verschlüsselungsverfahrens unter Verwendung des Hauptschlüssels MK in Probekennungsdaten PRK überführt wird.

Aus den Probekennungsdaten PRK wird nachfolgend in der Verschlüsselungsstufe 48 wiederum eine Prüfbotschaft B gebildet, indem die zur Anforderung der Authentifizierungsbotschaft A vom tragbaren Datenträger 10 ausgesandte Zufallszahl ZZ mit den Probekennungsdaten PRK verschlüsselt wird. Die Prüfbotschaft B wird schließlich in der Vergleichsstufe 50 mit der von dem tragbaren Datenträger 10 übermittelten Authentifizierungsbotschaft A verglichen.

Fig. 4 zeigt eine Ausführung der Erfindung, bei der die Datenträgerkennung durch ein aus einem biometrischen Datensatz BIO_R abgeleitetes Zertifikat CV gebildet wird, welches bei der Personalisierung auf den Datenträger 10 gebracht wurde. In dem integrierten Schaltkreis 12 des tragbaren Datenträgers 10 befinden sich weiter der digitale Referenzdatensatz DRT, ein öffentlicher Schlüssel $ÖS_K$ des Datenträgers 10 sowie ein korrespondierender geheimer Schlüssel GS_K des Datenträgers 10. Der integrierte Schaltkreis 12 ist ferner dazu eingerichtet, eine zugeführte Dateninformation mit einer mittels des geheimen Schlüssels GS_K gebildeten Signatur zu versehen.

Die Prüfeinrichtung 32 ist zur Durchführung asymmetrischer Verschlüsselungstechniken eingerichtet. Insbesondere ist sie dazu ausgebildet, ein von einem Datenträger 10 zugesandtes Zertifikat mittels des öffentlichen Schlüssels $ÖS_Z$ einer Zertifizierungsstelle zu verifizieren. Sie hat hierzu Zugriff auf den öffentlichen Schlüssel $ÖS_Z$. Desweiteren hat die Prüfeinrichtung 32 Zugriff auf die öffentlichen Schlüssel $ÖS_K$ der tragbaren Datenträger 10.

Um die Berechtigung zur Nutzung einer Transaktion oder eines Dienstes nachzuweisen, präsentiert die Nutzung beabsichtigende Person den tragbaren Datenträger 10 der Prüfeinrichtung 32.

Diese fordert darauf durch Übersenden einer Zufallszahl ZZ durch eine Anforderungsstufe 62eine Authentifizierungsbotschaft C von dem tragbaren Datenträger 10 an.

Auf den Eingang der Zufallszahl ZZ bildet der integrierten Schaltkreis 12 die Authentifizierungsbotschaft C. Dazu bildet er eine Signatur SIGN, indem er die zugesandte Zufallszahl ZZ mit dem geheimen Schlüssel GS_K des Datenträgers 10 signiert. Der Signatur SIGN fügt er ferner das Zertifikat CV bei.

Die resultierende Authentifizierungsbotschaft C mit der Signatur SIGN über und dem Zertifikat CV übermittelt der tragbare Datenträger 10 an die Prüfeinrichtung 32.

Dort wird sie einer Authentizititätsprüfung unterzogen. Dazu wird in einer Entschlüsselungsstufe 66 zunächst die Authentizität des Zertifikats CV geprüft. Die Prüfung erfolgt unter Verwendung des zu dem geheimen Schlüssel GS_Z, der bei der Erzeugung des Zertifikates CV verwendet wurde, korrespondierenden öffentlichen Schlüssels $ÖS_Z$ der Zertifizierungsstelle. Wird das Zertifikat CV danach als echt erkannt, akzeptiert die Prüfeinrichtung 32 auch den mit dem Zertifikat CV übermittelten Referenzdatensatz DRT als authentisch. Mittels des öffentlichen Schlüssels $ÖS_K$ des Datenträgers 10 prüft die Prüfungseinrichtung 32 in einer Prüfstufe 64 sodann unter Heranziehung der Zufallszahl ZZ die Richtigkeit in der Authentifizierungsbotschaft C übersandten Signatur SIGN. Stimmen die signierte Zufallszahl ZZ und die an den tragbaren Datenträger 10 ausgesandte Zufallszahl ZZ überein, sendet die Prüfeinrichtung 32 den in der Authentifizierungsbotschaft C enthaltenen digitalen Referenzdatensatz DRT einer Vergleichsstufe 68 zu.

Unabhängig von der Präsentation des tragbaren Datenträgers 10 stellt die Nutzung beabsichtigende Person der Prüfeinrichtung 32 desweiteren das biometrische Merkmal, das auch zur Bildung des digitalen Referenzdatensatzes DRT herangezogen wurde, über den Sensor 22 zur Verfügung. Der Sensor 22 bildet darauf zu dem erneut bereitgestellten biometrischen Merkmal erneut einen biometrischen Datensatz BIO_V, welcher der Prüfeinrichtung 32 und darin einer Digitalisierungsstufe 40 zugeführt wird. Diese unterwirft den biometrischen Datensatz BIO_V einer Digitalisierung, aus der ein digitaler Vergleichsdatensatz DVT resultiert. Bei der Digitalisierung wird dasselbe Digitalisierungsverfahren eingesetzt, das auch zur Bildung des im integrier-

ten Schaltkreis 12 des tragbaren Datenträgers 10 gespeicherten digitalen Referenzdatensatzes DRT herangezogen wurde.

Der digitale Vergleichsdatensatz DVT wird nachfolgend der Vergleichsstufe 68 übergeben. Diese vergleicht den erhaltenen digitalen Vergleichsdatensatz DVT mit dem von der Entschlüsselungsstufe 66 erhaltenen, von dem tragbaren Datenträger 10 stammenden digitalen Referenzdatensatz DRT. Stimmen beide überein, wird die Berechtigung der benutzenden Person zur Durchführung der gewünschten Transaktion bzw. zur Inanspruchnahme des gewünschten Dienstes als gegeben angesehen.

Unter Beibehaltung des grundlegenden Gedankens, einen tragbaren Datenträger mit einer Datenträgerkennung zu versehen, die durch Verfremdung mittels mathematischer Methoden aus einem der berechtigten Person zugeordneten biometrischen Datensatz abgeleitet wird, gestattet das beschriebene Verfahren eine Vielzahl zweckmäßiger Ausgestaltungen. So kann vorgesehen sein, daß der tragbare Datenträger 10 und die Prüfeinrichtung 32 vor der Übersendung der Authentifizierungsbotschaft A, C Sitzungsschlüssel aushandeln und diese zur weiteren Sicherung der zwischen tragbarem Datenträger 10 und Prüfeinrichtung 32 ausgetauschten Daten einsetzen. Die Datenträgerkennung DTK kann außer dem verfremdeten biometrischen Merkmal weitere Informationen enthalten, etwa eine Seriennummer. Weiter kann die softwaremäßige und technische Realisierung der einzelnen Bearbeitungsstufen auf vielfältige Weise erfolgen. Beispielsweise kann die Prüfeinrichtung physisch verteilt auf mehrere Einheiten ausgebildet sein und die Durchführung einzelner Stufen in verschiedenen physischen Einheiten erfolgen. Das sinngemäß gleiche gilt für die Personalisierungsstelle.

Patentansprüche

1. Verfahren zum Nachweis der Berechtigung einer Person zur Nutzung eines tragbaren Datenträgers gegenüber einer Prüfeinrichtung, wobei in einer Vorbereitungsphase eine Kennung auf den Datenträger gebracht wird und wobei für eine Nutzung die Kennung zumindest teilweise erneut bereitgestellt werden muß, dadurch **gekennzeichnet**, daß:
in der Vorbereitungsphase:
aus einem der Person zugeordneten biometrischen Datensatz (BIO_R) die Kennung (DTK) abgeleitet wird, indem der biometrische Datensatz (BIO_R) mittels eines Digitalisierungsverfahrens in einen digitalen Datensatz (DRT) überführt und auf diesen nachfolgend ein kryptographisches Verfahren angewendet wird,
und bei einer Nutzung
der biometrische Datensatz (BIO_V) der Prüfeinrichtung (32) erneut bereitgestellt wird,
in der Prüfeinrichtung (32) aus dem erneut bereitgestellten biometrischen Datensatz (BIO_V) Probekennungsdaten (PRK) abgeleitet werden, indem aus dem erneut bereitgestellten biometrischen Datensatz (BIO_V) mittels des genannten Digitalisierungsverfahrens ein digitaler Vergleichsdatensatz (DVT) erzeugt und auf diesen das genannte kryptographische Verfahren angewendet wird,
die Kennung (DTK) von dem Datenträger (10) an die Prüfeinrichtung übermittelt (32) wird, und
die Probekennungsdaten (PRK) in der Prüfeinrichtung (32) mit der Kennung (DTK) verglichen werden.

2. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß der erneut bereitgestellte biometrische Datensatz (BIO_V) aus Informationen gewonnen wird, die von einem der Prüfeinrichtung (32) zugeordneten Sensor (22) geliefert werden.

3. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß die erneute Bereitstellung des biometrischen Datensatzes erfolgt, indem der biometrische Referenzdatensatz (BIO_R) von dem Datenträger (10) an die Prüfeinrichtung (32) übermittelt wird.

4. Verfahren nach Anspruch 3, dadurch **gekennzeichnet**, daß die Übermittlung des biometrischen Referenzdatensatzes (BIO_R) von dem Datenträger (10) nur ausgeführt wird, wenn die Anwendung des Digitalisierungsverfahrens auf einen aus Informationen des Sensors (22) gebildeten biometrischen Datensatz (BIO_V) nicht möglich ist.

5. Verfahren nach Anspruch 3, dadurch **gekennzeichnet**, daß der aus Informationen des Sensors (22) gebildete biometrische Datensatz (BIO_V) mit dem von dem Datenträger (10) übermittelten biometrischen Referenzdatensatz (BIO_R) verglichen wird.

6. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß das in der Vorbereitungsphase eingesetzte kryptographische Verfahren eine symmetrische Verschlüsselung unter Verwendung eines Masterkeys (MK) beinhaltet.

7. Verfahren nach Anspruch 6, dadurch **gekennzeichnet**, daß der Masterkey (MK) von einer Zertifizierungsstelle bereitgestellt wird.

8. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß das in der Vorbereitungsphase eingesetzte kryptographische Verfahren eine DES3-Verschlüsselung beinhaltet.

9. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß der digitale Datensatz (DRT) eine alphanumerische Zeichenfolge bildet, welcher einer zur Benutzung des tragbaren Datenträgers (10) berechtigten Person bekannt gemacht wird.

10. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß die Übermittlung der Kennung (DTK) an die Prüfeinrichtung (32) verschlüsselt erfolgt, wobei die Kennung (DTK) als Schlüssel dient, mit dem eine Anforderungsbotschaft (ZZ) verschlüsselt wird.

11. Verfahren zum Nachweis der Berechtigung einer Person zur Nutzung eines tragbaren Datenträgers gegenüber einer Prüfeinrichtung, wobei in einer Vorbereitungsphase eine Kennung auf den Datenträger gebracht wird und wobei für eine Nutzung die Kennung zumindest teilweise erneut bereitgestellt werden muß, dadurch **gekennzeichnet**, daß
in der Vorbereitungsphase
aus einem der Person zugeordneten biometrischen Datensatz (BIO_R) eine Kennung (CV) abgeleitet wird, indem der biometrische Datensatz (BIO_R) mittels eines Digitalisierungsverfahrens in einen digitalen Referenzdatensatz (DRT) überführt und auf diesen nachfolgend ein kryptographisches Verfahren angewendet wird,
und bei einer Nutzung
der biometrische Datensatz (BIO_V) der Prüfeinrichtung (32) erneut bereitgestellt wird,
in der Prüfeinrichtung (32) aus dem erneut bereitgestellten biometrischen Datensatz (BIO_V) mittels des genannten Digitalisierungsverfahrens ein digitaler Vergleichsdatensatz (DVT) erzeugt wird,
von dem Datenträger (10) die Kennung (CV) an die Prüfeinrichtung übermittelt (32) wird,

in der Prüfeinrichtung (32) durch Anwendung eines kryptographischen Prüfverfahrens die Authentizität der Kennung (CV) festgestellt wird, und der digitale Vergleichsdatensatz (DVT) in der Prüfeinrichtung (32) mit dem aus der Kennung (CV) entnommenen digitalen Referenzdatensatz (DRT) verglichen wird.

12. Verfahren nach Anspruch 11, dadurch **gekennzeichnet**, daß in der Vorbereitungsphase die Kennung (CV) gebildet wird, indem der digitale Referenzdatensatz (DRT) mit einem Zertifikat versehen wird, das über den digitalen Referenzdatensatz (DRT) durch Ausführung eines asymmetrischen Verschlüsselungsverfahrens unter Verwendung des geheimen Schlüssels (GS_Z) einer Zertifizierungsstelle gebildet wird.

13. Verfahren nach Anspruch 11, dadurch **gekennzeichnet**, daß in der Vorbereitungsphase die Kennung (CV) gebildet wird, indem ein dem Datenträger (10) zugeordneter öffentlicher Schlüssel ($ÖS_K$) unter Verwendung des geheimen Schlüssels (GS_Z) einer Zertifizierungsstelle gemäß einem asymmetrischen Verschlüsselungsverfahren verschlüsselt wird.

14. Verfahren nach Anspruch 11, dadurch **gekennzeichnet**, daß zusammen mit der Kennung (CV) eine Signatur (SIGN) übermittelt wird, die unter Verwendung des geheimen Schlüssels (GS_K) des Datenträgers (10) zu einer Anforderungsbotschaft (ZZ) gebildet wurde.

15. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß das in der Prüfeinrichtung (32) angewandte kryptographische Prüfverfahren die Durchführung einer Entschlüsselung mit Hilfe des zu dem bei der Bildung der Kennung (CV) eingesetzten geheimen Schlüssel (GS_Z) korre-

spondierenden öffentlichen Schlüssels ($\ddot{O}S_Z$) der Zertifizierungsstelle beinhaltet.

16. Verfahren nach Anspruch 11, dadurch **gekennzeichnet**, daß das in der Prüfeinrichtung (32) angewendete kryptographische Prüfverfahren die Durchführung einer Signaturprüfung mit Hilfe des zu dem bei der Bildung der Signatur (SIGN) eingesetzten geheimen Schlüssel (GS_K) korrespondierenden öffentlichen Schlüssels ($\ddot{O}S_K$) des Datenträgers (10) beinhaltet.

17. Tragbarer Datenträger zur Durchführung eines Verfahrens zum Nachweis der Berechtigung einer Person zu seiner Nutzung mit einer Schnittstelle zur Führung eines Datenaustausches mit einer Prüfeinrichtung sowie einer Speichereinrichtung, dadurch **gekennzeichnet**, daß in der Speichereinrichtung eine Kennung (DTK, CV) abgelegt ist, welche durch Anwendung eines kryptographischen Verfahrens auf einen der berechtigten Person zugeordneten biometrischen Datensatz (BIO_R) gebildet wurde.

18. Prüfeinrichtung zur Durchführung eines Verfahrens zum Nachweis der Berechtigung einer Person zur Nutzung eines tragbaren Datenträgers mit einem Sensor zur Aufnahme eines biometrischen Merkmales, einer Schnittstelle zur Führung eines Datenaustausches mit einem tragbaren Datenträger sowie Mitteln zur Prüfung einer von einem tragbaren Datenträger zugesandten Kennung, dadurch **gekennzeichnet**, daß sie Mittel (22, 42, 48) besitzt, um einen biometrischen Datensatz (BIO_V) durch Anwendung eines kryptographischen Verfahrens in Probekennungsdaten (PRK) zu überführen, welche bei gegebener Berechtigung mit der Kennung (DTK) des Datenträgers (10) übereinstimmen.

19. System zum Nachweis der Berechtigung einer Person zur Nutzung eines tragbaren Datenträgers, **gekennzeichnet** durch einen tragbaren Datenträger nach Anspruch 17 sowie eine Prüfeinrichtung nach Anspruch 18.

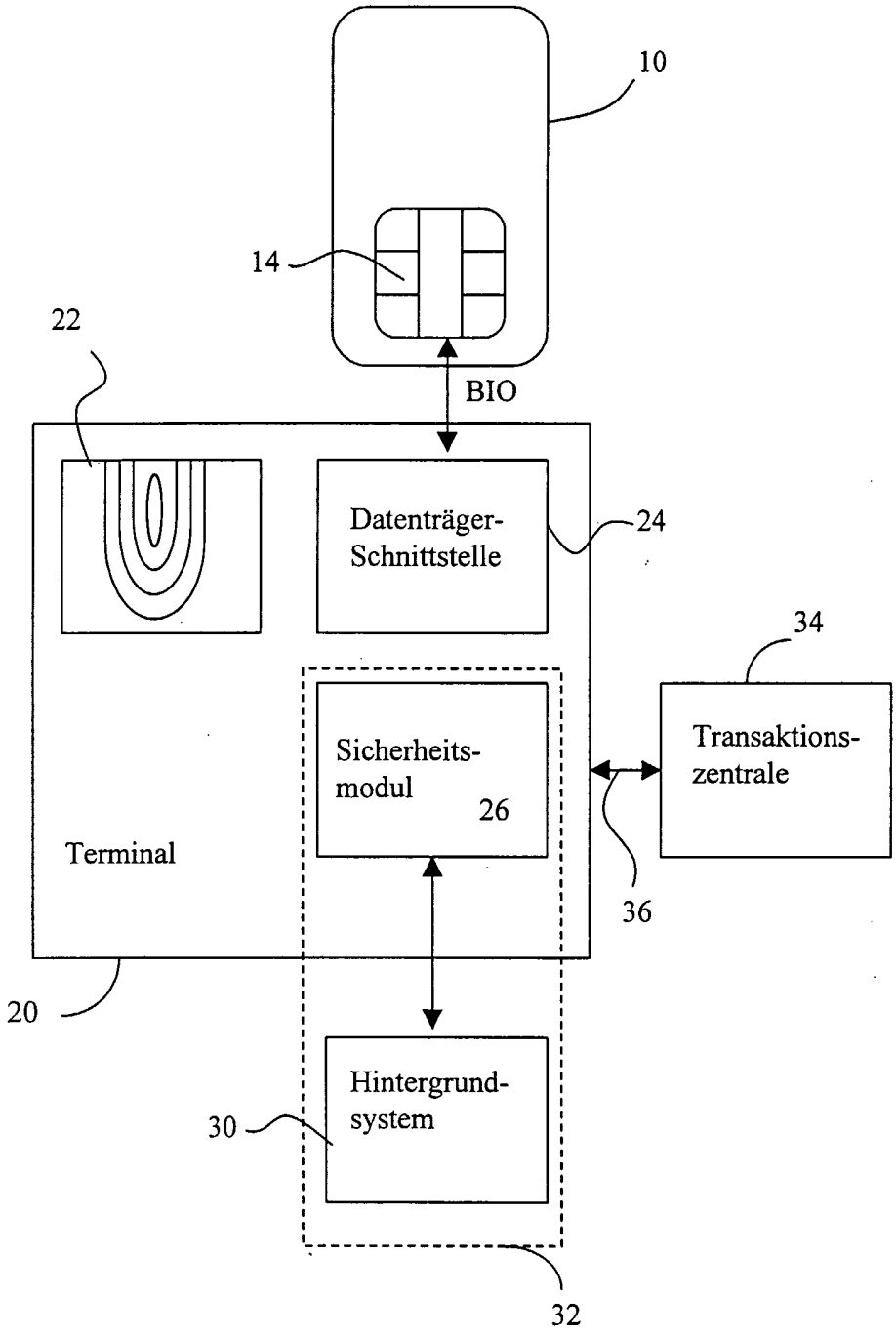
10
14
22
BIO
Datenträger-
Schnittstelle
24
34
Transaktions-
zentrale
Sicherheits-
modul
26
Terminal
36
20
Hintergrund-
system
30
32

Fig. 1

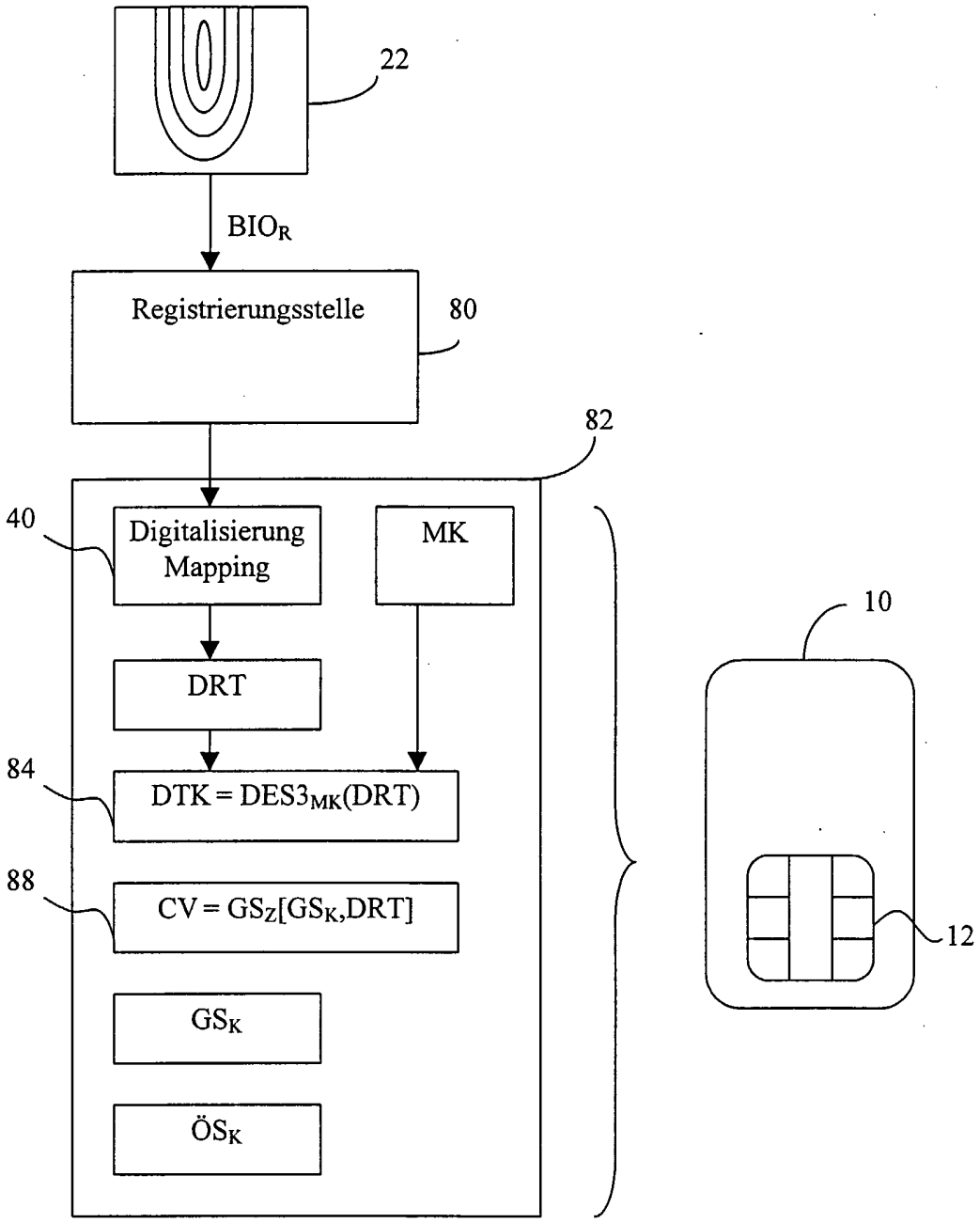
22
BIO_R
Registrierungsstelle
80
82
40
Digitalisierung Mapping
MK
10
DRT
84
$DTK = DES3_{MK}(DRT)$
88
$CV = GS_Z[GS_K,DRT]$
GS_K
$ÖS_K$
12

Fig. 2

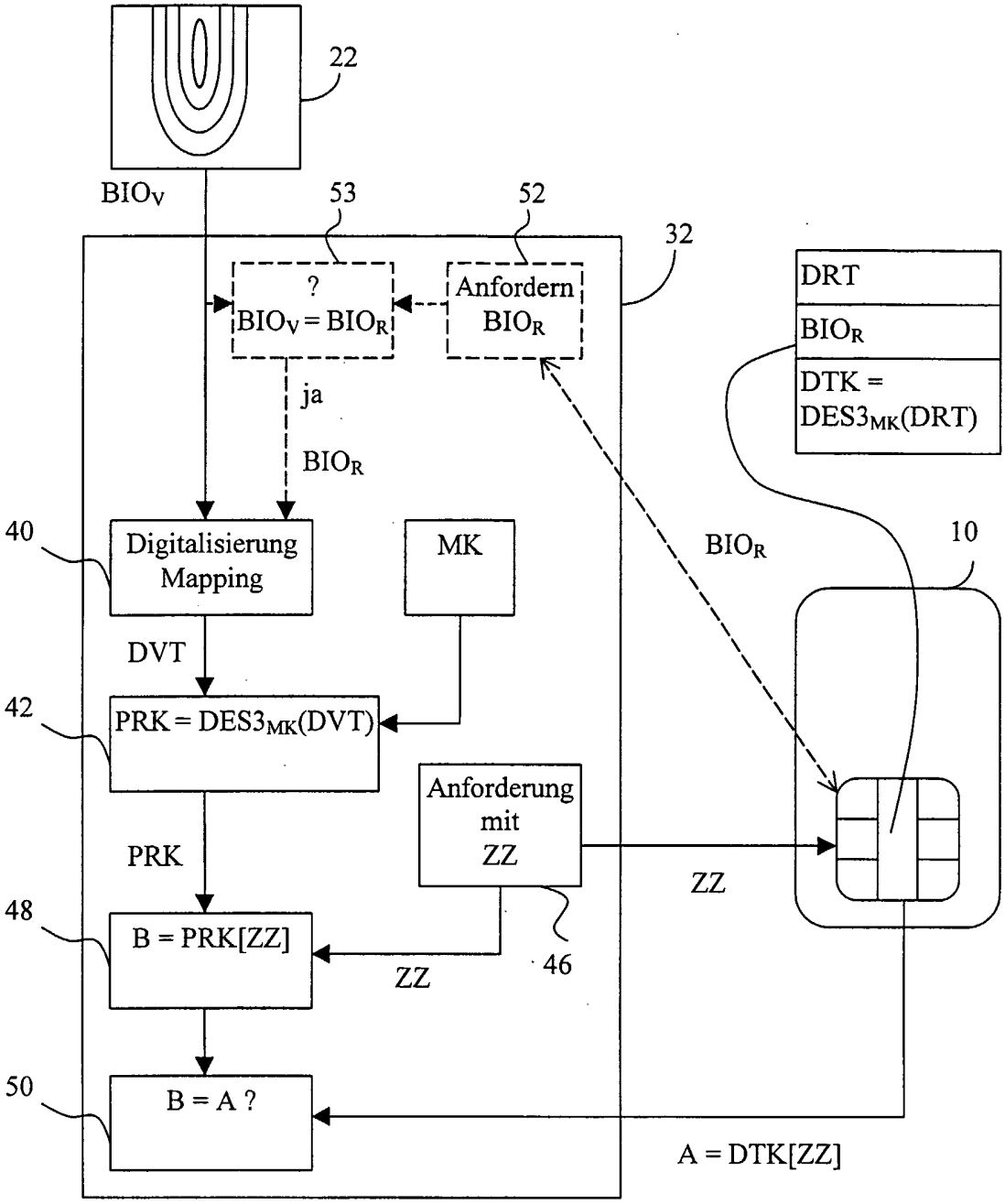
22
BIOV
53
52
32
?
BIOV = BIOR
Anfordern
BIOR
DRT
BIOR
DTK =
DES3MK(DRT)
ja
BIOR
40
Digitalisierung
Mapping
MK
BIOR
10
DVT
42
PRK = DES3MK(DVT)
Anforderung
mit
ZZ
PRK
ZZ
48
B = PRK[ZZ]
ZZ
46
50
B = A ?
A = DTK[ZZ]

Fig. 3

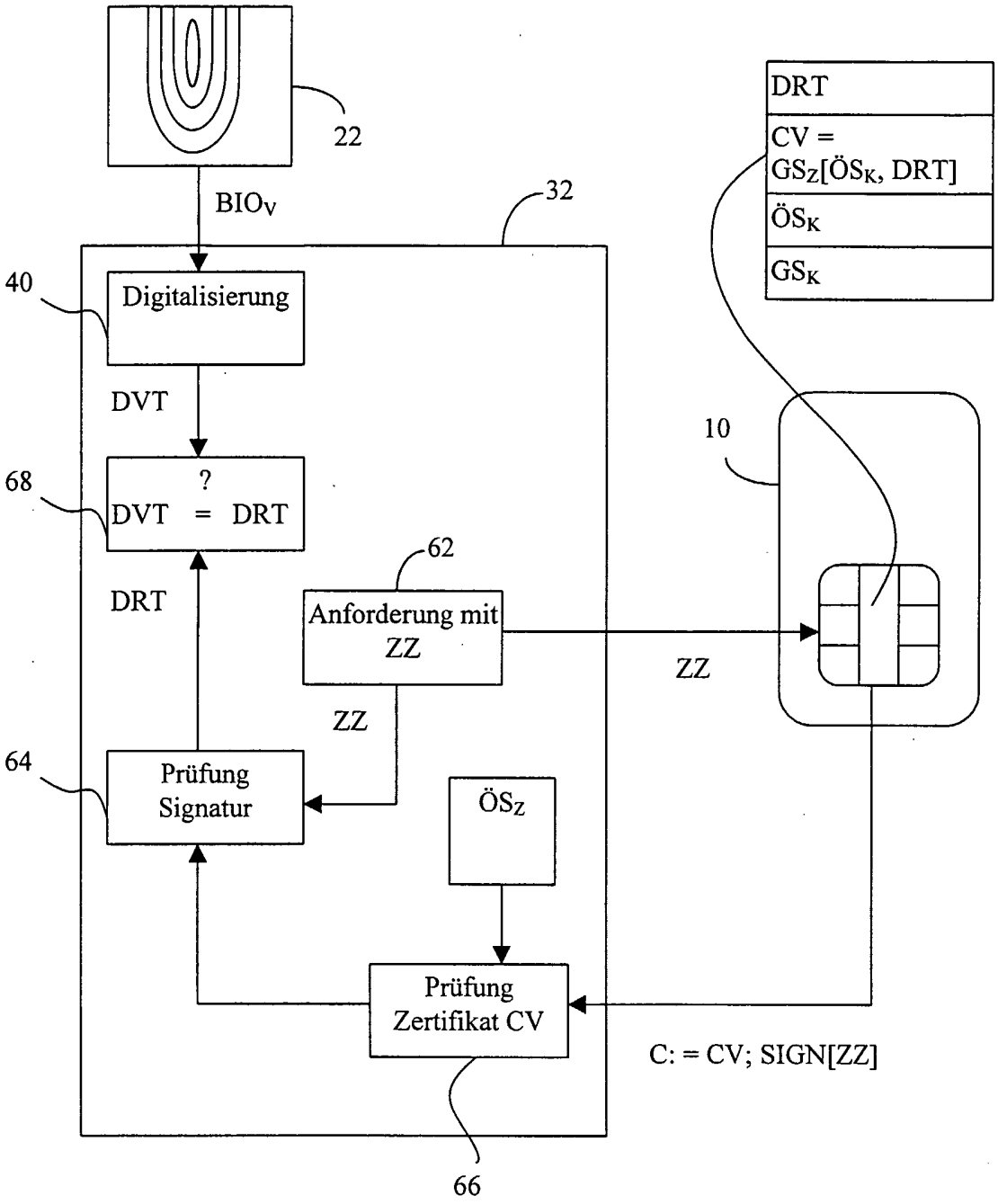
22
BIOV
32
40
Digitalisierung
DVT
68
?
DVT = DRT
DRT
62
Anforderung mit ZZ
ZZ
64
Prüfung Signatur
ZZ
ÖSZ
Prüfung Zertifikat CV
66
DRT
CV = GSZ[ÖSK, DRT]
ÖSK
GSK
10
ZZ
C: = CV; SIGN[ZZ]

Fig. 4