(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 1 936 572 A1**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
25.06.2008 Patentblatt 2008/26

(51) Int Cl.:
G07C 9/00 *(2006.01)*

(21) Anmeldenummer: **06026821.6**

(22) Anmeldetag: **22.12.2006**

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Benannte Erstreckungsstaaten:
AL BA HR MK RS

(71) Anmelder: **Armatix GmbH**
85774 Unterföhring (DE)

(72) Erfinder:
- **Parhofer, Stefan**
  München 81547 (DE)
- **Dietel, Bernd**
  Aurach 6370 (AT)
- **Lind, Bernd**
  Herrsching 82211 (DE)

(74) Vertreter: **Vossius & Partner**
Siebertstrasse 4
81675 München (DE)

(54) **Identifikationseinrichtung und Verfahren für den logischen und/oder physikalischen Zugang bzw. Zugriff auf eine Zieleinrichtung**

(57) Einrichtung (1) zum sicheren personalisierten Identifizieren und Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs bzw. Zugriffs zu einer bzw. auf eine Zieleinrichtung. Die Einreichtung weist ein tragbares Identmedium zum Ausgeben eines Berechtigungssignals mit mindestens einem Biometriesensor (2), mindestens einem Ausgabeelement (3), einem Prozessor mit einem Speicher und einer Software sowie einer Sende- und Empfangselektronik zum drahtlosen Datenaustausch auf. Das Identmedium ist derart ausgebildet, dass nach erfolgreicher Authentifizierung durch einen berechtigten Benutzer, ein Berechtigungssignal über das Ausgabeelement (3) ausgegeben wird. Das tragbare Identmedium ist an einem Armband (5) zur Befestigung am Handgelenk eines Benutzers angeordnet. Die Einrichtung weist mindestens ein Sicherheitsmittel auf, das eingerichtet ist, das Ausgeben des Berechtigungssignals im Falle eines Öffnen und/oder Lösens des Armbands (15) und/oder Entfernen der Einrichtung vom Handgelenk des Benutzers zu unterbrechen und/oder zu verhindern.

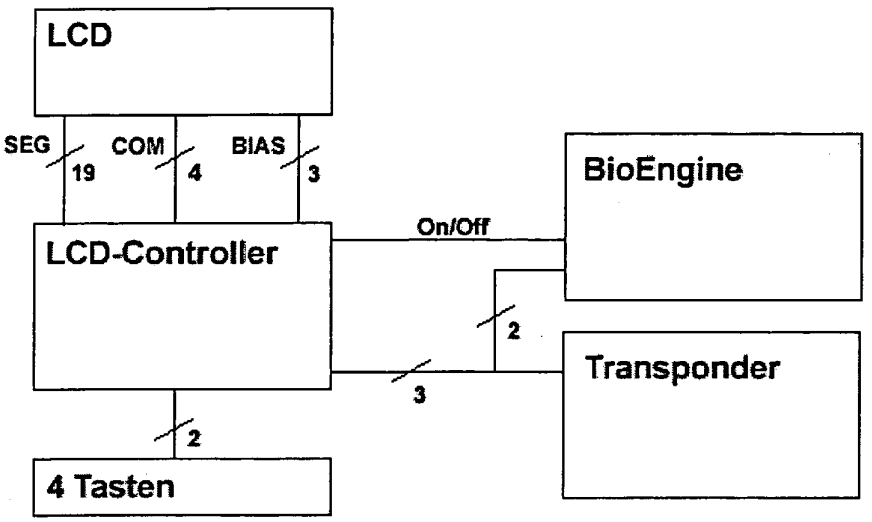

Fig. 2

EP 1 936 572 A1

Beschreibung

[0001] Die vorliegende Erfindung betrifft eine Verfahren und eine Einrichtung zum sicheren personalisierten Identifizieren und Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs bzw. Zugriffs zu einer bzw. auf eine Zieleinrichtung. Anwendungsbereich der vorliegenden Erfindung ist neben der traditionellen Zutrittskontrolle insbesondere für Gebäude, insbesondere auch der Bereich der elektronischen Waffenabsicherung. Auch andere dem Fachmann geläufige Anwendungen sind bevorzugt, z.B. Zugang zu Fahrzeugen, Safes, etc.

[0002] Im Stand der Technik ist es bekannt, einen Transponder biometrisch, bspw. über einen Fingerprintsensor, gegen unberechtigten Zugriff zu sichern. Ein solcher Transponder kann nur vom berechtigten Nutzer benutzt werden. Der Vorteil gegenüber einem fest an einer Zieleinrichtung, bspw. einer Tür installierten Biometrie-Leser besteht darin, dass ein Biometrie-Transponder keine Verkabelung an der Zieleinrichtung erfordert und beliebig viele Zieleinrichtungen freischalten kann.

[0003] Aus der DE-A-103 41 370 ist beispielsweise ein System zum sicheren personalisierten Identifizieren und Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs zu einer Zieleinrichtung bekannt. Hierbei erfolgt zunächst das Identifizieren eines Benutzers mittels eines tragbaren Identmediums, wobei biometrische Daten eines Benutzers durch einen Biometriesensor detektiert werden. Nach erfolgreichem Identifizieren eines autorisierten Benutzers und Überprüfen der Berechtigung des Identmediums bzw. des gesendeten Signals durch eine Gegenstation wird ein logischer und/oder physikalischer Zugang bzw. Zutritt zu einer Zieleinrichtung ermöglicht bzw. verhindert.

[0004] In der WO-A-2005/054771 wird eine Sicherheitseinrichtung für Handfeuerwaffen beschrieben, die einen Transponder zur Authentifizierung eines autorisierten Waffenbenutzers, der den Transponder trägt, oder zur Authentifizierung eines berechtigten Bereichs zur Verwendung der Waffe betrifft. Der Transponder ist dabei eingerichtet, vorzugsweise ein verschlüsseltes drahtloses Authentifizierungssignal abzugeben. Ferner weist die Sicherheitseinrichtung Sicherheitsmittel zum Greifen der Waffe auf, die eingerichtet sind, beim Greifen der Waffe notwendigerweise durch die Hand des Benutzers aktiviert zu werden, wobei sie ein drahtloses Requestsignal ausgeben. Der Transponder ist hierbei eingerichtet, das Authentifizierungssignal auf den Empfang des Requestsignals durch die Sicherheitsmittel auszugeben. Die Sicherheitsmittel sind ferner ausgebildet, das Authentifizierungssignal des Transponders zu empfangen und weiterzuverarbeiten sowie ein Feuern der Waffe durch den Bediener nur nach dem Empfang eines Authentifizierungssignals durch den Transponder zu gestatten, das einen autorisierten Bediener authentifiziert. Gemäß der WO-A-2005/054771 kann der Transponder beispielsweise als Ring- oder Armband ausgebildet sein.

[0005] Die DE-A-100 18 369 beschreibt eine Vorrichtung zum Auslösen eines Schusses oder einer Schusswaffe, wobei zur Sicherung von Waffen gegen unbefugte Benutzung die Auslösevorrichtung derart gestaltet wird, dass sie nur dann freigegeben wird, wenn ein vom Waffenbenutzer zu tragender und beim Ziehen des Abzugs von einem elektronischen Schaltkreis der Waffe abgefragter Transponder einen gültigen Lizenzcode zurücksendet. Der Transponder ist hierbei vorzugsweise als Chip ausgebildet und in einen flachen Träger nach Art einer bekannten Chipkarte eingesetzt.

[0006] Die US-A-54461812 betrifft ein Sicherheitssystem für eine Schusswaffe, bei der ein Benutzer einen Fingerring trägt, in dem ein Transponder untergebracht ist. Dieser Transponder wird durch eine in der Schusswaffe angeordnete Sicherheitsvorrichtung abgefragt.

[0007] Die US-A-2001/0032405 betrifft eine Feuerwaffe mit einem Sicherheitssystem, bei dem der berechtigte Benutzer beispielsweise durch einen in einem Fingerring angeordneten Transponder ausgewiesen wird. Alternativ kann ein Transponder in einem Armband, einem Schweißband oder einem Uniformärmel angeordnet sein.

[0008] In der WO-A-00/65291 wird ein Steuersystem für eine Feuerwaffe beschrieben, das eine Sicherheitseinrichtung aufweist, wobei ein Transponder in einem Identifikationselement, beispielsweise einem Fingerring oder einem Armband angeordnet ist, um den berechtigten Benutzer zu identifizieren.

[0009] Die WO-A-98/04880 betrifft eine Einrichtung zum Sichern einer Schusswaffe sowie zum Sichern und/oder Aufbewahren von Gegenständen mit einer Verriegelungsvorrichtung und einer Identifikationsvorrichtung, wobei die Identifikationsvorrichtung zum drahtlosen Austausch zumindest von unverwechselbaren Identifikationscodes ausgebildet ist und zumindest eine einem befugten Benutzer und eine weitere Identifikationsvorrichtung zugeordnete Sende-und/oder Empfangseinheit umfasst, wobei bei einer Distanz oder einem Distanzbereich zwischen Sende- und/oder Empfangseinheit und übereinstimmenden Identifikationscodes der Sende- und/oder Empfangseinheit des Benutzers und der Sende- und/oder Empfangseinheit der Identifikationsvorrichtung die Verriegelungsvorrichtung durch die Identifikationsvorrichtung deaktiviert ist. Gemäß einer bevorzugten Ausführungsvariante ist die Sende- und/oder Empfangseinheit als Transponder ausgebildet, der austauschbar in ein Uhrarmband eingeschoben werden kann.

[0010] Die im Stand der Technik bekannten Systeme, wie beispielsweise in der DE-A-103 41 370 beschrieben, ermöglichen ein sicheres personalisiertes Identifizieren und Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs zu einer Zieleinrichtung. Hierzu ist jedoch erforderlich, die Identifizierung und Berechtigung des Benutzers vor jedem Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs zu einer Zieleinrichtung erneut zu überprüfen und zu verifizieren. Dies erweist sich gegebenenfalls als um-

ständlich und für den Benutzer unbefriedigend.

[0011] Eine nach einmaliger Freischaltung dauerhaft oder für einen vorgegebenen Zeitrahmen aktivierte Identifikationsvorrichtung erweist sich dahingehend nachteilig gegenüber einem möglichen Mißbrauch, dass die Vorrichtung nach einmaliger Aktivierung durch einen berechtigten Benutzer die Waffe bzw. den Zugang auch für nicht berechtigte Benutzer frei schaltet. Dies gilt auch für die im Stand der Technik vorgeschlagene Ausbildung von Identifikationseinrichtungen als Fingerring oder Armband, da diese eine Entwendung durch und Verwendung von nicht-Berechtigten nicht ausschließen können. Es besteht somit eine erhöhte Gefahr des Mißbrauchs der im Stand der Technik bekannten Vorrichtungen.

[0012] Es ist somit eine Aufgabe der vorliegenden Erfindung, eine verbesserte Einrichtung und ein verbessertes Verfahren zum sicheren personalisierten Identifizieren und Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs bzw. Zugriffs zu einer Zieleinrichtung bereitzustellen. Insbesondere ist es eine Aufgabe der vorliegenden Erfindung, eine derartige Einrichtung sowie ein derartiges Verfahren mit verbesserten Handling-Eigenschaften und erhöhter Benutzerfreundlichkeit bei gleichzeitig verbesserter Sicherheit gegen unbefugten Zugang bzw. Zugriff bereitzustellen.

[0013] Diese Aufgabe wird gemäß den Merkmalen der unabhängigen Ansprüche gelöst. Die abhängigen Ansprüche stellten bevorzugte Ausführungsformen der vorliegenden Erfindung dar.

[0014] So betrifft die vorliegende Erfindung einerseits eine Einrichtung zum sicheren personalisierten Identifizieren und Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs bzw. Zugriffs zu einer bzw. auf eine Zieleinrichtung. Diese Einrichtung weist ein tragbares Identmedium zum Ausgeben eines Berechtigungssignals mit mindestens einem Biometriesensor, mindestens einem Eingabeelement und mindestens einem Ausgabeelement, einem Prozessor mit einem Speicher und einer Software sowie einer Sende- und Empfangselektronik auf. Das Identmedium ist hierbei ausgebildet, nach erfolgreicher Authentifizierung bzw. Identifikation durch einen berechtigen Benutzer, ein Berechtigungssignal auszugeben. Ein derartiges Signal kann entweder unmittelbar nach erfolgter erfolgreicher Identifikation dauerhaft, intermittierend, einmalig, n-malig oder als Antwort auf ein entsprechendes Requestsignal einer Gegenstation ausgegeben werden. Das tragbare Identmedium ist zur Befestigung am Handgelenk des Benutzers an einem Armband bzw. Armreif angeordnet.

[0015] Die Einrichtung weist ferner ein Sicherheitsmittel auf, das eingerichtet ist, das Ausgeben des Berechtigungssignals im Falle eines Öffnens des Armbands bzw. eines Reifens des Armbands oder dergleichen und/oder eines Entfernens der Einrichtung vom Handgelenk des Benutzers zu unterbrechen, zu verhindern und/oder zu deaktivieren. Vorzugsweise ist als Sicherheitsmittel ein Kontaktschalter oder -ring an bzw. auf der zum Handgelenk gerichteten Unterseite vorgesehen. Weiter bevorzugt ist an bzw. auf der Unterseite eine Batterie angeordnet, die von einem vorzugsweise konzentrischen Metallring umgeben ist, so dass Batterie und Metallring einen Kondensator bilden, dessen Kapazität sich ändert und eine Schaltfunktion übernimmt, wenn die Unterseite vom Handgelenk bzw. von der Haut eines Trägers entfernt wird. Alternativ bzw. vorzugsweise zusätzlich weist das Sicherheitsmittel einen Armbanddetektor auf, der weiter bevorzugt durch einen im oder am Armband vorgesehenen elektrischen Leiter gebildet wird. Dabei kann ein Teil des Leiters in das Armband integriert, beispielsweise eingewoben, und ein weiterer Teil des Leiters durch die Schließe gebildet werden. Vorzugsweise ist die Einrichtung derart ausgebildet, dass nach der Unterbrechung oder Verhinderung der Ausgabe des Berechtigungssignals bzw. der Deaktivierung des Identmediums durch das Sicherheitsmittel eine erneute Authentifizierung zum Ausgeben eines Berechtigungssignals erforderlich ist.

[0016] Unter Öffnen des Armbands wird hierbei sowohl das herkömmliche Öffnen als auch das beispielsweise gewaltsame Abreißen bzw. eine Beschädigung des Armbands verstanden. Insbesondere stellt das Sicherheitsmittel sicher, dass eine Aktivierung des Identmediums bzw. das Ausgeben eines Berechtigungssignals nur dann möglich ist, wenn die erfindungsgemäße Einrichtung mittels des Armbands am Handgelenks eines berechtigten Benutzers befestigt ist bzw. wenn das Armband seit der letzten erfolgreichen Authentifizierung eines Nutzers nicht mehr geöffnet wurde.

[0017] Von einer Aktivierung des Identmediums bzw. von einem aktiven Identmedium wird nachfolgend gesprochen, wenn eine erfolgreiche Identifikation durch einen berechtigten Benutzer erfolgt ist und ein Berechtigungssignal ausgegeben wird bzw. ausgegeben werden kann. Dahingegen wird von einem inaktiven bzw. deaktivierten Identmedium gesprochen, wenn keine erfolgreiche Identifikation durch einen berechtigten Benutzer erfolgt bzw. erfolgt ist oder wenn das Identmedium durch das Sicherheitsmittel deaktiviert wurde.

[0018] Nach erfolgreicher Identifikation durch einen berechtigten Benutzer erfolgt vorzugsweise eine Aktivierung des Identmediums für einen vom berechtigten Benutzer wählbaren und durch diesen einstellbaren oder fest voreingestellten Zeitraum.

[0019] Die erfindungsgemäße Einrichtung dient vorzugsweise zur Kommunikation mit einer Gegenstation, beispielsweise einer Schließeinrichtung an einer Tür, einer Sicherheitseinrichtung, einer Waffe oder dergleichen, wie nachfolgend detailliert erläutert, in einem sogenannten Proximitymodus.

[0020] Vorzugsweise ist die erfindungsgemäße Einrichtung derart ausgebildet, dass sich die Einrichtung bzw. das aktivierte Identmedium als Antwort auf ein von einer Gegenstation an die Einrichtung gesendetes Wake-up- oder Requestsignal authentifiziert, woraufhin die Gegenstation einen logischen und/oder physikalischen Zugang bzw. Zugriff zu einer bzw. auf eine Zieleinrich-

tung ermöglicht bzw. verhindert.

[0021] Vorzugsweise ist die Einrichtung derart ausgebildet, dass sie bei Überschreitung eines vorbestimmten Abstands von einer Gegenstation inaktiv ist bzw. deaktiviert wird. Sobald sich die Einrichtung wieder innerhalb des vorbestimmten Abstands von der Gegenstation befindet, wird diese vorzugsweise wieder aktiviert bzw. ist diese wieder aktiv.

[0022] Vorzugsweise ist die Einrichtung nach Ablauf des vorbestimmten bzw. vom berechtigten Benutzer gewählten Aktivierungszeitraums inaktiv. Als Zeitgeber fungiert hierbei vorzugsweise eine Uhr in einer integrierten Armbanduhr.

[0023] Gemäß einer bevorzugten Ausführungsform ist die Einrichtung in der Armbanduhr angeordnet oder weist ferner Merkmale wie eine Zeit- und/oder Datumsanzeige auf.

[0024] Die Einrichtung ist bevorzugt batteriebetrieben. Die Einrichtung weist vorzugsweise eine Antenne auf. Die Einrichtung ist ferner vorzugsweise nicht vollständig aus Metall ausgebildet.

[0025] Die erfindungsgemäß Vorrichtung ist vorzugsweise ausgebildet, das erfindungsgemäße Verfahren und die bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens auszuführen.

[0026] Die vorliegende Erfindung betrifft ferner ein Verfahren zum sicheren personalisierten Identifizieren und Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs bzw. Zugriffs zu einer bzw. auf eine Zieleinrichtung. Das erfindungsgemäße Verfahren weist die Schritte Identifizieren eines Benutzers mittels eines zur Befestigung am Handgelenk eines Benutzers an einem Armband angeordneten tragbaren Identmediums auf, wobei biometrische Daten mindestens eines Benutzers durch mindestens einen Biometriesensors detektiert werden und Daten und/oder Befehle über mindestens ein Eingabeelement eingegeben und Betriebszustände über mindestens ein Ausgabeelement angezeigt werden. Hierbei wird mittels eines Prozessors mit einem Speicher und einer Software, welcher eine dezentrale, für das Identmedium spezifische Datenbank mit eingelernten Geometriedaten aufweist, ein Vergleich zwischen den detektierten Geometriedaten und den eingelernten Geometriedaten durchgeführt. Nach erfolgreichem Identifizieren eines autorisierten Benutzers wird in Abhängigkeit vom kontinuierlichen Vorliegen zusätzlicher Sicherheitsbedingungen ein Berechtigungssignal gesendet. Sofern die zusätzlichen Sicherheitsbedingungen nicht mehr vorliegen oder unterbrochen wurden, wird das Identmedium deaktiviert bzw. wird das Senden eines Berechtigungssignals unterbrochen bzw. verhindert.

[0027] Vorzugsweise liegen die zusätzlichen Sicherheitsbedingungen bei geschlossenem Armband und Tragen des Identmediums durch einen Benutzer vor, wobei sie bei geöffnetem bzw. unterbrochenem Armband oder Nichtragen durch einen Benutzer nicht vorliegen.

[0028] Vorzugsweise ist nach der Unterbrechung oder Verhinderung der Ausgabe eines Berechtigungssignals bzw. der Inaktivierung des Identmediums durch das Sicherheitsmittel eine erneute Authentifizierung für das erneute Ausgeben eines Berechtigungssignals erforderlich.

[0029] Vorzugsweise ist die erfindungsgemäße Vorrichtung fernsteuerbar, beispielsweise via Satellit bzw. kann Informationen an einen Satelliten senden.

[0030] Vorzugsweise ist die Einrichtung, beispielsweise eine Uhr, zusätzlich mit einem GPS- bzw. Satellitensender ausgestattet und deckt vorzugswiese mindestens eine der folgende Funktionen ab:

- Betriebszustände, beispielsweise einer Waffe (wer hat wann gefeuert) werden über die Einrichtung an den Satelliten in eine Zentrale gegeben
- Zieleinrichtung, beispielsweise eine Waffe, kann über die Einrichtung, beispielsweise eine Uhr, fernfreigeschaltet werden
- Zieleinrichtung, beispielsweise eine Waffe, kann mittels eines in ihr eingebauten GPS-Senders nur an bestimmten Orten freigeschaltet werden.

[0031] So erreicht man noch eine höhere Administrationsebene für die Zieleinrichtung, beispielsweise eine Waffe.

[0032] Nachfolgend werden weitere bevorzugte Ausführungsformen der vorliegenden Erfindung unter Verweis auf die beigefügten Zeichnungen beschrieben. Es zeigen:

Fig. 1 eine schematische Darstellung einer erfindungsgemäßen Einrichtung;
Fig. 2 den schematischen Aufbau einer erfindungsgemäßen Einrichtung;
Fig. 3 eine bevorzugte Ausgabeeinheit einer erfindungsgemäßen Einrichtung;
Fig. 4 eine weitere Ausführungsform einer bevorzugten Ausgabeeinheit einer erfindungsgemäßen Einrichtung;

[0033] Fig. 1 zeigt eine bevorzugte erfindungsgemäße Ausführungsform 1 mit einem Biometriesensor in Form eines Fingerprint-Streifensensors 2, einem Ausgabeelement bzw. einer Anzeigeeinrichtung 3, Eingabeelementen 4 sowie einem Armband 5. Die erfindungsgemäße Einrichtung weist ferner ein Gehäuse 6 zur Aufnahme der vorstehend benannten Elemente sowie zur Befestigung am Armband 5 auf. Vorzugsweise ist der Biometriesensor bzw. der Streifensensor 2 so an der Einrichtung 1 bzw. am Gehäuse 6 positioniert, dass eine einfache und sichere Fingerführung gewährleistet ist. Bei der Wahl des Gehäusematerials gibt es keine Vorgaben. Vorzugsweise ist die Auswahl des Gehäusematerials lediglich dadurch eingeschränkt, dass nicht das gesamte Gehäuse rundherum aus Metall sein sollte, um eine Dämpfung des Signals zu vermeiden. Die erfindungsgemäße Einrichtung weist vorzugsweise Eingabeelemente wie den Biometriesensor sowie vorzugsweise minde-

stens vier, besonders bevorzugt sechs Tasten auf. Die Tasten dienen dazu, die Einstellungen der Einrichtung vorzunehmen.

[0034] Vorzugsweise ist die erfindungsgemäße Einrichtung derart ausgebildet, dass die Aktivierung des Transponders bzw. Identmediums für einen vom berechtigten Benutzer wählbaren Zeitraum aktiviert wird. In diesem Zeitraum kann die erfindungsgemäße Einrichtung mit einer Gegenstation, beispielsweise einer Schließeinrichtung oder einer Waffe kommunizieren. Hierzu sendet die Gegenstation vorzugsweise eine Request- bzw. Wake-up-Signal an die erfindungsgemäße Einrichtung, die Einrichtung authentisiert sich, und die Gegenstation führt eine vorgegebene Handlung aus oder initiiert eine solche. Beispielsweise wird eine Tür geöffnet, eine Waffe freigeschaltet oder der Zugriff auf einen Computer freigeschaltet. Sobald der Abstand zwischen der Gegenstation und der Einrichtung eine vorgegebene, vorzugsweise einstellbare Signalreichweite überschreitet, wird die durch die Gegenstation initiierte Handlung bzw. der initiierte Zustand wieder deaktiviert. So wird beispielsweise die Waffe wieder deaktiviert bzw. gesichert. Nähern sich Einrichtung und Gegenstation wieder aneinander an, so dass die Gegenstation des Funkfeldes oder innerhalb der Signalreichweite liegt, erfolgt die Freischaltung bzw. Handlung erneut. Beispielsweise ist eine Waffe unmittelbar wieder zu benutzen.

[0035] Wenn der Aktivierungszeitraum abgelaufen ist, muss sich der Berechtigte erneut per Fingerabdruck identifizieren.

[0036] Die Einstellung der erfindungsgemäßen Einrichtung auf eine beschränkte Wirkreichweite wird auch als Proximitymodus bezeichnet.

[0037] Dieser kann mittels der Eingabeelemente eingestellt werden. Vorzugsweise kann ebenso die Aktivierungszeit, also die Dauer der Aktivierung des Transponders bzw. Identmediums der Identifikation eines berechtigten Nutzers durch die Eingabeelemente variabel eingestellt werden. Je nach weiteren Funktionalitäten der erfindungsgemäßen Einrichtung dienen die Eingabeelemente bzw. die Tasten vorzugsweise auch zur Einstellung von Uhr, Datum etc. In erster Linie erlauben die Eingabeelemente jedoch eine einfachere und sicherere Bedienbarkeit der Biometrietransponderfunktion.

[0038] Als Ausgabeelemente weist die erfindungsgemäß Einrichtung vorzugsweise einen visuellen Signalgeber (Display, LED), einen akustischen Signalgeber (Piepser, Busser) und/oder ein RF-Interface (Antenne, vorzugsweise im Gehäuse angeordnet) auf.

[0039] Die erfindungsgemäße Einrichtung weist ferner ein Sicherungsmittel auf. Vorzugsweise ist das Sicherungsmittel derart ausgebildet, dass das Armband mit einem elektrischen Leiter bzw. Kontakt versehen ist. Dadurch ist die Einrichtung in der Lage, zu überprüfen, ob das Armband geschlossen ist. Vorzugsweise läuft ein geschlossener elektronischer Kontakt von der Einrichtung durch das gesamte Armband und wieder zur Einrichtung zurück. Gemäß einer weiteren bevorzugten Ausführungsform sind die Verbindungsstellen zwischen Gehäusearmband, Armband, also Schließe und Armbandgehäuse mit Sicherheitsmitteln versehen. Wird somit das Armband bei aktiviertem Transponder geöffnet, also an der regulären Schließe geöffnet oder abgerissen, so wird der Transponder bzw. das Identmedium automatisch deaktiviert.

[0040] Alternativ oder zusätzlich können am Gehäuse Mittel vorgesehen sein, die ein Aufliegen der Gehäuseunterseite am Handgelenk des Benutzers überwachen und den Transponder automatisch deaktivierten, wenn festgestellt wird, dass die Einrichtung nicht am Handgelenk eines Benutzers angeordnet ist.

[0041] Vorzugsweise ist als Sicherheitsmittel ein Kontaktschalter oder -ring an bzw. auf der zum Handgelenk gerichteten Unterseite vorgesehen. Weiter bevorzugt ist an bzw. auf der Unterseite eine Batterie angeordnet, die von einem vorzugsweise konzentrischen Metallring umgeben ist, so dass Batterie und Metallring einen Kondensator bilden, dessen Kapazität sich ändert und eine Schaltfunktion übernimmt, wenn die Unterseite vom Handgelenk bzw. der Haut eines Trägers entfernt wird.

[0042] Die erfindungsgemäße Einrichtung ist vorzugsweise batteriebetrieben.

[0043] Die drahtlose Kommunikation zwischen der elektronischen Steuereinheit der Sicherheitsvorrichtung und dem externen Gerät kann in beliebiger Art oder Frequenz, die für den Einsatzzweck geeignet sind, erfolgen, beispielsweise Niederfrequenz (NF, z.B. 25 kHz mit magnetischer Induktion), Radio-Frequenz (RFID, z.B. 13,56 MHz) oder Hochfrequenz (z.B. 868 MHz, 915 MHz, 2,4 GHz oder höher), und kann nach einem Standard-Protokoll (z.B., Bluetooth, ZigBee) oder einem herstellereigenem Protokoll oder einer Kombination aus beidem erfolgen. Unter dem Begriff "Kommunikation" soll in diesem Zusammenhang jegliche Form eines Datenaustausches verstanden werden, und diese kann entweder verschlüsselt oder unverschlüsselt und entweder unidirektional oder bidirektional erfolgen. Der Fachmann wird je nach den gewünschten Eigenschaften des Systems, z.B., Optimierung der Signalreichweite, Übertragungsgeschwindigkeit, Batteriehaltbarkeit, Kosten oder Anfälligkeit gegen externe elektromagnetische Störungen oder andere Kriterien, den geeigneten Ansatz und die geeignete Kombination wählen. Entweder die Steuereinheit oder das externe Gerät oder beide können über eine eigene Energieversorgung verfügen. Diese Energieversorgung kann entweder eine Batterie, eine Brennstoffzelle, eine Piezozelle oder eine Solarzelle umfassen. In einer bevorzugten Ausführungsform verfügen beide, die Steuereinheit und der Transponder über eine eigene Batterie. Falls entweder die Steuereinheit oder der Transponder nicht über eine eigene Energieversorgung verfügen, werden über die drahtlose Kommunikationsverbindung nicht nur Daten, sondern auch Energie übertragen.

[0044] Gemäß einer bevorzugten Ausführungsform ist die erfindungsgemäße Einrichtung ausgebildet, eine Schusswaffensicherung bereitzustellen. Eine solche

Waffensicherung besteht vorzugsweise aus zwei Instanzen. Die erste Instanz ist eine in der Waffe eingebaute Gegenstation, vorzugsweise ein Transponder, die bzw. der beispielsweise durch einen Ballenschalter an der Waffe aktiviert wird.

[0045] Als zweite Instanz wird die erfindungsgemäße Einrichtung, die am Handgelenk getragen wird, verwendet. Das Zusammenspiel zwischen erfindungsgemäßer Einrichtung und waffenseitiger Gegenstation ermöglicht ausschließlich autorisierten Personen den Gebrauch der Waffe. Hierbei erfolgt die Identifikation einer autorisierten Person an der erfindungsgemäßen Einrichtung durch Abfrage von Biometriedaten. Die erfindungsgemäße Einrichtung kann vorzugsweise ferner zusätzliche Funktionen, wie beispielsweise Zeit- und Datumsanzeige, vergleichbar mit einer herkömmlichen Uhr, aufweisen. Eine derartige Uhr ist vorzugsweise als Zeitgeber eingebunden.

[0046] Vor Gebrauch der Waffe ist eine einmalige Identifikation einer autorisierten Person notwendig. Dazu wird durch einen Sensor in der erfindungsgemäßen Einrichtung ein Fingerabdruck dieser Person eingelesen und durch die erfindungsgemäße Einrichtung ermittelt, ob diese autorisiert ist, die Waffe zu gebrauchen. Wenn der Ballenschalter an der Waffe betätigt wird, folgt die Anforderung einer Waffenfreigabe durch den Waffentransponder, also die Gegenstation, bei der erfindungsgemäßen Einrichtung. Geht der Anfrage eine gültige Identifikation der autorisierten Person voraus, so wird die Freigabe gewährt, andernfalls wird sie unterlassen. Nach Freigabe ist die Waffe scharf bzw. ungesichert.

[0047] Der Verbindungsabstand zwischen dem Waffentransponder, also der Gegenstation, und der erfindungsgemäßen Einrichtung wird gering gehalten. Eine Kommunikation zwischen Waffentransponder und erfindungsgemäßer Einrichtung kann also nur dann stattfinden, wenn die Waffe mit der Hand geführt wird, an deren Handgelenk die erfindungsgemäße Einrichtung getragen wird. Gerät dann die Waffe aus dem Sende- und Empfangsbereich der erfindungsgemäßen Einrichtung, ist keine erneute Identifikation erforderlich, wenn die Waffe innerhalb der Aktivitätsdauer der erfindungsgemäßen Einrichtung in den Sende- und Empfangsbereich zurückkehrt. Diese Aktivitätsdauer ist benutzerspezifisch einstellbar oder fest eingestellt. Darüber hinaus enthält das Armband der erfindungsgemäßen Einrichtung einen Sensor bzw. mindestens ein Sicherheitsmittel. Wird nach Identifikation das Armband geöffnet oder die erfindungsgemäße Einrichtung dem Träger entrissen, so erlischt die Identifikation und/oder die Waffe wird deaktiviert. Durch diese doppelte Sicherung wird gewährleistet, dass nur autorisierte Personen die Waffe gebrauchen können. Eine Verwendung einer erfindungsgemäßen Einrichtung zur Freischaltung einer durch eine nichtberechtigte Person wird wirksam verhindert, selbst wenn eine aktivierte Einrichtung dem Berechtigten Benutzer abgenommen wird.

[0048] Die Funktionen der erfindungsgemäßen Einrichtung umfassen vorzugsweise die Verwaltung von Fingerabdrücken, die Kommunikation mit der Gegenstation, bspw. einem Waffentransponder, und/oder die Funktion einer digitalen Armbanduhr.

[0049] Die Verwaltung von Fingerabdrücken beinhaltet bevorzugt das Einlernen von Fingerabdrücken, das Erkennen eingelernter Fingerabdrücke und das Löschen eingelernter Fingerabdrücke. Vorzugsweise wird zwischen zwei Fingertypen, den Benutzer- und den Adminstratorfingern unterschieden. Sowohl das Einlernen neuer Fingerabdrücke als auch das Löschen der gesamten Datenbank ist nur mit dem Adminstratorfinger möglich. Zur Kommunikation zwischen dem Träger der erfindungsgemäßen Einrichtung und dem Biometriesensor dient vorzugsweise ein LCD-Display. Alternativ oder zusätzlich ist auch eine Kommunikation über LED, beispielsweis rotes und grünes, ggf. blinkendes Licht, bevorzugt.

[0050] Die Kommunikationsfunktionen umfassen vorzugsweise die Initialisierung des Kommunikationsprotokolls nach einem Weckruf, das Aushandeln eines Session-Keys zur sicheren Kommunikation und/oder die Aufrechterhaltung einer bereits bestehenden Kommunikation. Die Kommunikation ist bevorzugt mittels Transponder als Punkt-zu-Punkt-Verbindung realisiert. Um energiesparend und einfach eine bereits bestehende Verbindung aufrechtzuerhalten, sendet die erfindungsgemäße Einrichtung vorzugsweise periodisch ein Zeitsignal. Um eine sichere Kommunikation zu ermöglichen, handeln die Gegenstation, bspw. der Waffentransponder, und die erfindungsgemäße Einrichtung vorzugsweise einen Session-Key aus, mit welchem das Zeitsignal versehen wird.

[0051] Eine weitere Kommunikationsfunktion ist das Aufzeichnen der Kommunikation sowie von Waffenfunktionen. Somit kann gespeichert werden, wann durch welchen Nutzer (Fingerprint) die erfindungsgemäße Einrichtung freigeschaltet wurde und wann bzw. wie oft die Waffe durch die erfindungsgemäße Einrichtung freigeschaltet wurde. Weiterhin kann die Waffe auch Informationen wie Betriebsdaten an die erfindungsgemäße Einrichtung senden, z.B. über Anzahl und Uhrzeit der abgegebenen Schüsse, Batteriezustand etc, sofern die Waffe über eine solche abgegebenen Schüsse, Batteriezustand etc, sofern die Waffe über eine solche Funktionalität verfügt.

[0052] Die Uhrfunktionen umfassen vorzugsweise die Ermittlung von Zeit und Datum, die Einstellung von Zeit und Datum, die Einstellung der Anzeigedauer des LCD-Displays. die Auswahl zwischen dem 12-Stunden- und dem 24-Stunden-Modus, die Einstellung der Dauer der Aktivität des Transponders, und/oder eine Tastenkombination, durch die der aktive Transponder im Notfall deaktiviert werden kann.

[0053] Die erfindungsgemäße Einrichtung hat vorzugsweise den in Fig. 2 wiedergegebenen schematischen Aufbau.

[0054] Das LCD-Display ist die Kommunikationsschnittstelle zwischen der erfindungsgemäßen Einrich-

tung und dem Benutzer. Es liefert Informationen über Vorgänge in der erfindungsgemäßen Einrichtung und zeigt ggf. die Uhrzeit und das Datum an. Fig. 3 und 4 sind bevorzugte Designs des LCD-Displays.

[0055] Das numerische Display 7 dient insbesondere zur Anzeige von Zeit und Datum. Auch kann damit die Anzahl der bisherigen Templates beim Einlernen eines Fingerabdrucks angezeigt werden. Zudem zeigt das numerische Display 7 die ggf. erforderliche PIN-Eingabe an.

[0056] Das Symbol 8 zeigt an, ob die Waffe scharf ist. Wurde eine erfolgreiche Identifikation durchgeführt und befindet sich die Waffe im Sende- und Empfangsbereich der erfindungsgemäßem Einrichtung, leuchtet dieses Symbol auf. Eventuell kann bei Betätigung des Ballenschalters der Waffe dieses Symbol 8 zusätzlich blinken.

[0057] Das Symbol 9 ist nur relevant, wenn als Anzeigemodus der Uhrzeit der 12-Stunden-Modus eingestellt ist. Dann ist die zusätzliche Information wünschenswert, ob es sich bei der angegebenen Zeit um den Vormittag (AM, ante meridiem) oder um den Nachmittag (PM, post meridiem) handelt.

[0058] Das Symbol 10 ist im Fingerpint-Modus relevant. Es gibt die Qualität des aktuell eingelesenen Fingerabdrucks an. Es gibt fünf Qualtitätsstufen.

[0059] Das Symbol 11 ist im Fingerprint-Modus relevant. Durch Blinken des Handsymbols wird das Einlesen des Fingers angefordert. Das Einlesen eines Administratorfingers wird durch das Blinken des Handsymbols+A angezeigt. Blinkt das Handsymbol+S, so wird der neu ein-zulernende Benutzerfinger angefordert. Blinkt das Handsymbol+D, so wird jener Benutzerfinger angefordert, der aus der Datenbank zu löschen ist. Sind die Administratorfinger einzulernen, so wird dies durch das Blinken des Handsymbols+A+S angezeigt. Dies ist beim Einlernen der ersten zwei Finger in der Datenbank der Fall. Das Löschen der gesamten Datenbank wird dadurch angezeigt, dass das Handsymbol+A+D aufblinkt. Zusätzlich ist eine Symbolkombination erforderlich, die anzeigt, ob das Einlesen der Fingers erfolgreich war oder nicht.

[0060] Vorzugsweise weist das Display ferner ein Transpondersymbol auf (ist in Fig. 3 nicht enthalten). Dieses Symbol dient zur Anzeige, ob die Autorisierung erfolgreich war, unabhängig davon, ob sich die Waffe im Sende- und Empfangsbereich der Transponderuhr befindet. Um Energie einzusparen blinkt dieses vorzugsweise Symbol alle 2 Sekunden für ungefähr 0,5 Sekunden auf. Befindet sich der Waffentransponder im Sende- und Empfangsbereich der erfindungsgemäßen Einrichtung, leuchtet dieses Symbol permanent.

[0061] Vorzugsweise kann über das LCD-Display angezeigt werden, in welchem Betriebsmodus sich die erfindungsgemäße Einrichtung befindet.

[0062] Da das Anzeigen der Uhrzeit von geringerer Bedeutung ist, als die Anzeige zur Verwaltung der Fingerabdrücke und der Kommunikation mit dem Waffentransponder, ist die numerische Anzeige vorzugsweise verhältnismäßig klein gegenüber den Symbolanzeigen ausgebildet. Das Transponder-Symbol ist ein wichtiges Symbol und soll daher gut sichtbar und auffällig dargestellt werden.

[0063] Der LCD-Controller (vgl. Fig. 2) nimmt eine zentrale Stellung ein. Von ihm werden alle Aktionen koordiniert. Insbesondere dient er zur Ansteuerung des LCD-Displays und zur Kommunikation mit dem Biometriesensor. Ferner ermöglicht er Tastatur-und Uhr-Funktionen.

[0064] In einer bevorzugten Ausführungsform der erfindungsgemäßen Einrichtung mit LCD-Controller wird die gesamte Kommunikation zwischen Mensch und Maschine über den LCD-Controller geregelt. Dies umfasst die Verarbeitung der Eingaben des Benutzers über die vier bzw. sechs zur Verfügung stehenden Tasten und die Generierung von Ausgaben, die durch das LCD-Display dargestellt werden. Die Zusammenschaltung von LCD-Controller mit dem Biometriesensor und dem Transponder bzw. dem Identmedium ist vorzugsweise mittels Master/Slave-Architektur realisiert. Des Weiteren werden in ihm die Uhrfunktionen implementiert.

[0065] Der LCD-Controller besitzt vorzugsweise alle Betriebsmodi, die für die erfindungsgemäße Einrichtung notwendig sind.

[0066] Als Kommunikationspartner werden der Waffentransponder und die Transponderuhr betrachtet, da der Transponder in der Uhr bei der Kommunikation nicht als eigene Einheit erscheint.

[0067] Wird der Ballenschalter an der Waffe betätigt, stößt der Waffentransponder die Kommunikation mit der Transponderuhr an, indem es ein Wakeup-Signal sendet. Empfängt die Transponderuhr dieses Signal, überprüft sie, ob eine erfolgreiche Identifikation einer autorisierten Person vorliegt. Ist dies nicht der Fall, unterlässt es die Kommunikation. Die Waffe erhält keine Freigabe. Andernfalls fragt die Transponderuhr die Programmierung und die Berechtigung ab. Nach erfolgreicher Abwicklung des Challenge-Response wird die Waffe freigegeben.

[0068] Erhält die Waffe die Freigabe, wird die Kommunikation durch die Transponderuhr aufrechterhalten, indem die Transponderuhr periodisch einen Zeitstempel versendet. Der Waffentransponder quittiert den Erhalt des Zeitstempels mit einem ACK-Signal.

[0069] Durch das Versenden eines Zeitstempels kann jeder Schuss zeitlich protokolliert werden, wobei die bevorzugte integrierte Uhr das Zeitsignal bereitstellen kann.

[0070] Verzögert sich die Ankunft des Zeitstempels beim Waffentransponder bzw. die Ankunft des ACK-Signals bei der Transponderuhr über eine gewisse Zeitgrenze hinaus, wird die Kommunikation abgebrochen und die Waffe deaktiviert. Um eine sichere Kommunikation zu ermöglichen, handeln beide Parteien ein Session-Key aus.

[0071] Wird das Armband der Transponderuhr beispielsweise gewaltsam geöffnet, wird wie bei Ablauf des Transponder-Timers der Uhrtransponder deaktiviert. Als Folge unterbricht die Transponderuhr die Kommunikati-

on und die Waffe wird deaktiviert. Vorzugsweise ist der Transponder nicht in der Lage, Daten zu empfangen. Nach erfolgreicher Freischaltung des Transponders wird vorzugsweise ein periodisches keep-alive Signal im Intervall von vorzugsweise etwa 500 Millisekunden ausgesendet. Nach Verstreichen einer einstellbaren Zeit wird dieses Versenden des keep-alive Signals unterlassen und somit die Waffe inaktiv. Dies entpricht der Rückkehr des LCD-Controllers vom TransponderActivity-Modus in den Display-Modus.

[0072] Die Absicherung von Waffen vor Missbrauch hat heutzutage eine große gesellschaftliche Bedeutung. Die vorliegende Erfindung stellt ein leistungsfähiges. aber einfach zu bedienendes System bereit, das den Missbrauch von Waffen durch nicht-autorisierte Personen sicher und zuverlässig verhindert.

Patentansprüche

1. Einrichtung (1) zum sicheren personalisierten Identifizieren und Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs bzw. Zugriffs zu einer bzw. auf eine Zieleinrichtung, aufweisend
   ein tragbares Identmedium zum Ausgeben eines Berechtigungssignals mit mindestens einem Biometriesensor (2),
   mindestens einem Ausgabeelement (3),
   einem Prozessor mit einem Speicher und einer Software
   sowie einer Sende- und Empfangselektronik zum drahtlosen Datenaustausch, wobei
   das Identmedium ausgebildet ist, nach erfolgreicher Authentifizierung durch einen berechtigten Benutzer, ein Berechtigungssignal über das Ausgabeelement (3) auszugeben, wobei
   das tragbare Identmedium an einem Armband (5) zur Befestigung am Handgelenk eines Benutzers angeordnet ist, und wobei
   die Einrichtung mindestens ein Sicherheitsmittel aufweist, das eingerichtet ist, das Ausgeben des Berechtigungssignals im Falle eines Öffnen und/oder Lösens des Armbands (15) und/oder Entfernen der Einrichtung vom Handgelenk des Benutzers zu unterbrechen und/oder zu verhindern.

2. Einrichtung nach Anspruch 1, wobei die Einrichtung derart ausgebildet ist, dass nach der Unterbrechung oder Verhinderung der Ausgabe des Berechtigungssignals durch das Sicherheitsmittel zum erneuten Ausgeben eines Berechtigungssignals eine erneute Authentifizierung erforderlich ist.

3. Einrichtung nach Anspruch 1 oder 2, wobei das Identmedium weiter mindestens ein Eingabeelement (4) aufweist und programmierbar ist.

4. Einrichtung nach einem der Ansprüche 1, 2 oder 3, wobei der Biometriesensor (2) als Fingerprintsensor (2) ausgebildet ist.

5. Einrichtung nach einem der vorstehenden Ansprüche, wobei der Biometriesensor (2) ein optischer, kapazitiver, thermischer oder mit Radiowellen arbeitender Biometriesensor (2) ist.

6. Einrichtung nach einem der vorstehenden Ansprüche, wobei der Biometriesensor (2) ein Flächen- oder Streifensensor (2) ist.

7. Einrichtung nach einem der vorstehenden Ansprüche, wobei das Eingabeelement (4) als Tastatur ausgebildet ist, die vorzugsweise mindestens 4, besonders bevorzugt 6 Tasten aufweist.

8. Einrichtung nach einem der vorstehenden Ansprüche, wobei das Ausgabeelement (3) als LED und/ oder als Display ausgebildet ist.

9. Einrichtung nach einem der vorstehenden Ansprüche, wobei das Identmedium drahtlos programmierbar ist.

10. Einrichtung nach einem der vorstehenden Ansprüche, wobei Identmedium örtlich mit Energie versorgt bzw. batterieversorgt ist.

11. Einrichtung nach einem der vorstehenden Ansprüche, wobei der Prozessor des Identmediums eine dezentrale, für das Identmedium spezifische, Datenbank mit eingelernten Biometriedaten aufweist.

12. Einrichtung nach Anspruch 11, wobei die Datenbank über das Identmedium veränderbar ist.

13. Einrichtung nach einem der vorstehenden Ansprüche, wobei die Sicherheitsmittel einen Kontaktschalter und/oder eine Armbanddetektor aufweisen, die ein Entferen der Einrichtung vom Handgelenk eines Benutzers oder ein Öffnen und/oder Lösen des Armbandes detektieren und das Ausgeben des Berechtigungssignals unterbrechen und/oder verhindern.

14. Einrichtung nach Anspruch 13, wobei der Kontaktschalter ein kapazitiver Schalter ist, der vorzugsweise durch eine Batterie an bzw. auf der Unterseite der Einrichtung und einem die Batterie umgebenden Metallring gebildet wird.

15. Einrichtung nach Anspruch 13 oder 14, wobei der Armbanddetektor durch ein elektrischen Leiter im oder am Armband gebildet wird, dessen Unterbrechen durch das Sicherheitsmittel erkannt wird.

16. Einrichtung nach Anspruch 15, wobei ein Teil des

Leiters in das Armband integriert, bspw. eingewoben, ist und ein weiterer Teil durch eine Schließe des Armbandes gebildet wird.

17. Einrichtung nach einem der Ansprüche 1 bis 16, wobei die Einrichtung geeignet ist, Informationen wie beispielsweise Betriebsdaten von der Zieleinrichtung zu empfangen bzw. an diese zu senden.

18. Armbanduhr, aufweisend eine Einrichtung nach einem der Ansprüche 1 bis 17.

19. Verfahren zum sicheren personalisierten Identifizieren und Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs bzw. Zugriffs zu einer bzw. auf eine Zieleinrichtung, insbesondere zum Betreiben einer Einrichtung nach einem der vorstehenden Ansprüche, aufweisend die Schritte
Identifizieren eines Benutzers mittels eines zur Befestigung am Handgelenk eines Benutzers an einem Armband angeordneten tragbaren Identmediums, wobei
biometrische Daten mindestens eines Benutzers durch mindestens einen Biometriesensor detektiert werden und
Betriebszustände über mindestens ein Ausgabeelement angezeigt werden, und wobei
mittels eines Prozessors mit einem Speicher und einer Software, welcher eine dezentrale, für das Identmedium spezifische, Datenbank- mit eingelernten Biometriedaten aufweist, ein Vergleich zwischen den detektierten Biometriedaten und den eingelernten Biometriedaten durchgeführt wird;
Senden eines Berechtigungssignals nach erfolgreichem Identifizieren eines autorisierten Benutzers entweder unmittelbar oder als Antwort auf ein empfangenes Request-Signal, in Abhängigkeit vom kontinuierlichen Vorliegen zusätzlicher Sicherheitsbedingungen, sowie
Unterbrechen bzw. Verhindern des Sendens eines Berechtigungssignals, sofern das Vorliegen der zusätzlichen Sicherheitsbedingungen unterbrochen wurde.

20. Verfahren nach Anspruch 19, wobei die Sicherheitsbedingungen bei geschlossenem Armband und Tragen des Identmediums durch den Benutzer vorliegen und bei geöffnetem bzw. unterbrochenem Armband oder nicht-Tragen durch den Benutzer nicht vorliegen.

21. Verfahren nach Anspruch 19 oder 20, wobei nach der Unterbrechung oder Verhinderung der Ausgabe des Berechtigungssignals durch das Sicherheitsmittel zum erneuten Ausgeben eines Berechtigungssignals eine erneute Authentifizierung erforderlich ist.

22. Verfahren nach einem der Ansprüche 19 bis 21, wobei die Datenbank über das Identmedium bearbeitbar bzw. veränderbar ist, indem weitere Biometriedaten eingelernt, gelöscht und/oder bearbeitet werden.

23. Verfahren nach einem der Ansprüche 19 bis 22, wobei die Detektion von Biometriedaten mittels eines Fingerprintsensors erfolgt, der Fingerabdrücke nach einem optischen und/oder kapazitiven Verfahren detektiert.

24. Verfahren nach einem der Ansprüche 19 bis 23, wobei der Sensor optisch, kapazitiv, thermisch oder mit Radiowellen arbeitet.

25. Verfahren nach einem der Ansprüche 19 bis 24, wobei die Daten und/oder Befehle über mindestens ein Eingabeelement eingegeben werden können und die Eingabe mittels einer Tastatur erfolgt, die vorzugsweise mindestens 4, besonders bevorzugt 6 Tasten, aufweist.

26. Verfahren nach einem der Ansprüche 19 bis 25, wobei die Ausgabe mittels einer LED und/oder eines Displays erfolgt.

27. Verfahren nach einem der Ansprüche 19 bis 26, wobei nicht nur zwischen berechtigten und unberechtigten Benutzern, sonder ferner zwischen Benutzern mit verschiedenen Berechtigungen bzw. verschiedenen Berechtigungshierarchien unterschieden wird.

28. Verfahren nach einem der Ansprüche 19 bis 27, wobei die Identifikationsversuche und/oder -vorgänge durch mindestens einen der Prozessoren protokolliert werden.

29. Verfahren nach einem der Ansprüche 19 bis 28, wobei zur Identifikation weiterhin die korrekte Eingabe einer PIN erforderlich ist.

30. Verfahren nach einem der Ansprüche 19 bis 29, wobei die in der Datenbank eingelernten benutzerspezifischen Daten einer Hierarchie zugeordnet sind, wobei das Identmedium je nach Hierarchiestufe des Identifizierten Benutzers nur definierte Aktionen zulässt.

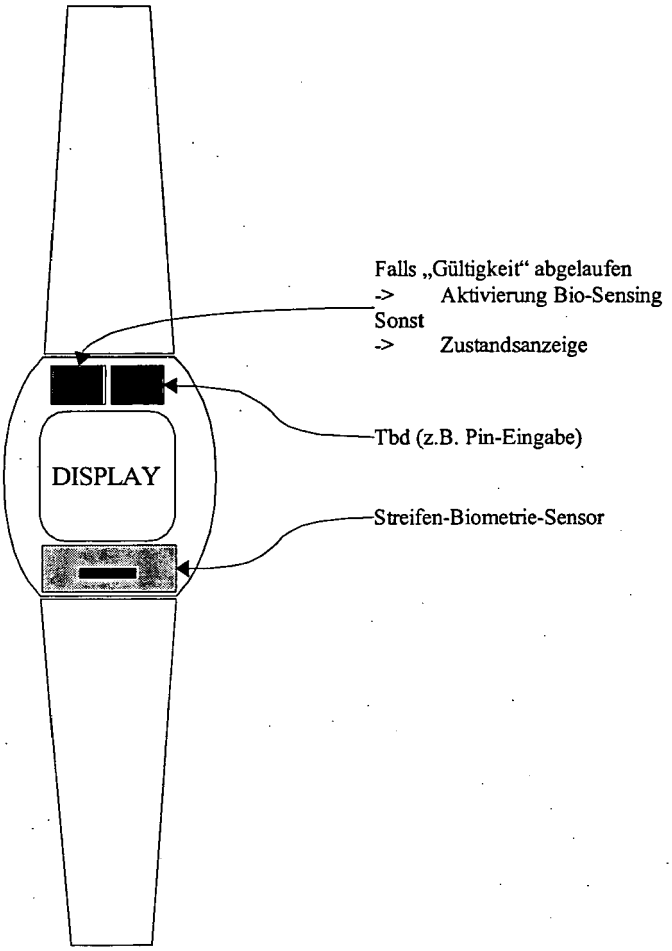
Falls „Gültigkeit" abgelaufen
-> Aktivierung Bio-Sensing
Sonst
-> Zustandsanzeige
Tbd (z.B. Pin-Eingabe)
DISPLAY
Streifen-Biometrie-Sensor

Fig. 1

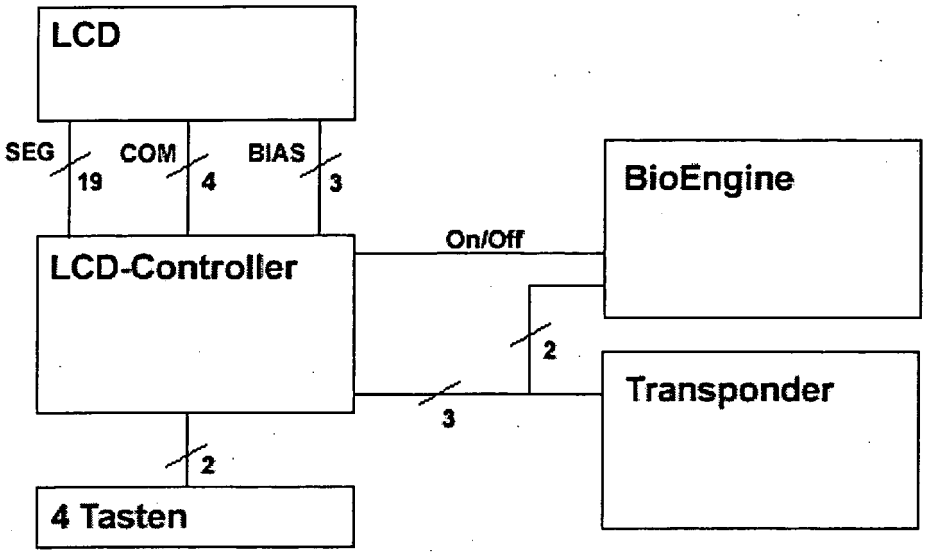
LCD
SEG
19
COM
4
BIAS
3
LCD-Controller
On/Off
BioEngine
2
Transponder
3
2
4 Tasten

Fig. 2

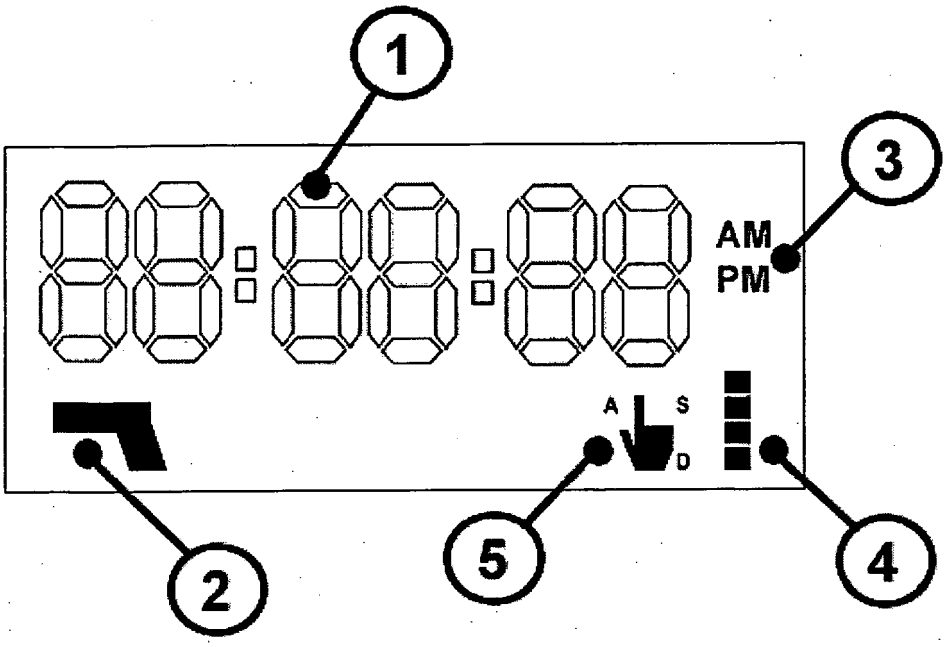

Fig. 3

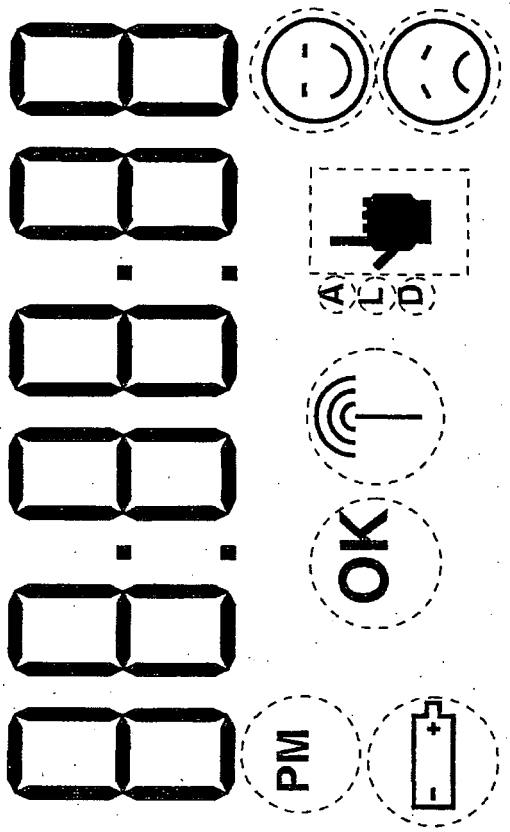

Fig. 4

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 06 02 6821

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X Y	US 2005/071647 A1 (FUJINUMA KEIICHI [JP] ET AL) 31. März 2005 (2005-03-31) * Seite 1, Absatz 9 - Absatz 11 * * Seite 2, Absatz 24 - Absatz 26 * * Seite 3, Absatz 34 - Seite 6, Absatz 65 * * Abbildungen 2-5 *	1-13, 17-27,30 14-16, 28,29	INV. G07C9/00
Y	US 2004/257202 A1 (COUGHLIN MICHAEL E [US] ET AL) 23. Dezember 2004 (2004-12-23) * Seite 2, Absatz 13 * * Seite 4, Absatz 53 *	14	
Y	WO 03/081515 A (PREC DYNAMICS CORP [US]) 2. Oktober 2003 (2003-10-02) * Seite 10, Absatz 52 - Seite 18, Absatz 61 * * Seite 25, Absatz 71 - Seite 37, Absatz 85 * * Abbildungen 2-9,12-25,30-32,35,36 *	15,16,29	
Y	WO 01/44836 A (ITALDATA INGEGNERIA DELL IDEA [IT]; BOCCACCI ROBERTO [IT]) 21. Juni 2001 (2001-06-21) * Seite 8, Zeile 1 - Zeile 24 *	28	
A	EP 1 300 647 A1 (GLOCK GASTON [AT]) 9. April 2003 (2003-04-09)	1-30	

RECHERCHIERTE SACHGEBIETE (IPC)

G07C
F41A

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	15. Mai 2007	VAN DER HAEGEN, D

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

1

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 06 02 6821

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

15-05-2007

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2005071647 A1	31-03-2005	CN 1591269 A	09-03-2005
		JP 2005071225 A	17-03-2005
		KR 20050021270 A	07-03-2005
		TW 259967 B	11-08-2006
US 2004257202 A1	23-12-2004	US 2007057800 A1	15-03-2007
		WO 2005001642 A2	06-01-2005
WO 03081515 A	02-10-2003	AU 2003209353 A1	08-10-2003
		CA 2478677 A1	02-10-2003
		CN 1639726 A	13-07-2005
		EP 1485856 A1	15-12-2004
		JP 2005521162 T	14-07-2005
		MX PA04008892 A	26-11-2004
		US 2005168340 A1	04-08-2005
		US 2007017136 A1	25-01-2007
		US 2003173408 A1	18-09-2003
		US 2004104274 A1	03-06-2004
WO 0144836 A	21-06-2001	AU 775345 B2	29-07-2004
		AU 2220501 A	25-06-2001
		BG 106797 A	30-05-2003
		BR 0016436 A	01-10-2002
		CA 2397667 A1	21-06-2001
		CN 1411559 A	16-04-2003
		CZ 20021988 A3	13-11-2002
		EE 200200313 A	16-06-2003
		EP 1242835 A1	25-09-2002
		HK 1053512 A1	22-09-2006
		HR 20020523 A2	31-08-2003
		HU 0203788 A2	28-03-2003
		IT RM990761 A1	18-06-2001
		MA 27588 A1	01-11-2005
		PL 358485 A1	09-08-2004
		SK 8742002 A3	06-11-2002
		UA 73544 C2	15-10-2002
		US 2002190864 A1	19-12-2002
		ZA 200205658 A	05-03-2004
EP 1300647 A1	09-04-2003	AT 261102 T	15-03-2004
		DE 10148676 A1	24-04-2003
		ES 2215958 T3	16-10-2004
		US 2003070343 A1	17-04-2003

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- DE 10341370 A **[0003] [0010]**
- WO 2005054771 A **[0004] [0004]**
- DE 10018369 A **[0005]**
- US 54461812 A **[0006]**
- US 20010032405 A **[0007]**
- WO 0065291 A **[0008]**
- WO 9804880 A **[0009]**