(19) Deutsches Patent- und Markenamt

(10) **DE 10 2016 123 787 A1** 2018.06.14

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2016 123 787.6**
(22) Anmeldetag: **08.12.2016**
(43) Offenlegungstag: **14.06.2018**

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

(71) Anmelder:
Bundesdruckerei GmbH, 10969 Berlin, DE

(72) Erfinder:
Bütje, Rolf, Dr., 21227 Bendestorf, DE

(56) Ermittelter Stand der Technik:

EP 1 237 091 A1

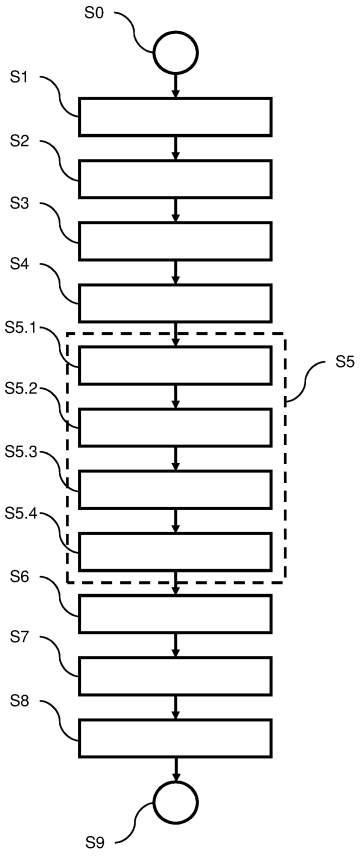
GRAAFSTRA, A.: Hands On. In: IEEE Spectrum, Vol. 44, 2007, Issue 3, S. 18 – 23. – ISSN 0018-9235

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Chipimplantat mit Zweifaktorauthentifizierung**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren für die Authentifizierung einer Person, ein Lesegerät (11), eine Zugangskontrollanordnung (10) sowie ein Chipimplantat (20). Das erfindungsgemäße Verfahren umfasst wenigstens die folgenden Schritte:
-- Erfassen eines biometrischen Merkmals der Person (S1);
-- Ableiten einer biometrischen Schlüsselinformation aus dem erfassten biometrischen Merkmal (S2);
-- Nachweisen der biometrischen Schlüsselinformation gegenüber einem Chipimplantat (20) der Person (S3);
-- Empfangen eines von dem Chipimplantat (20) übermittelten Attributs der Person in Antwort auf die nachgewiesene biometrische Schlüsselinformation (S4); und
-- Authentifizieren der Person in Abhängigkeit von dem empfangenen Attribut (S5).



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren für die Authentifizierung einer Person, ein Lesegerät, eine Zugangskontrollanordnung sowie ein Chipimplantat.

Technologischer Hintergrund

[0002] Das Prinzip der Zweifaktorauthentifizierung ist ein bekannter Ansatz, der in der Praxis üblicherweise durch Kombination von zwei der drei Faktoren Wissen, Besitz und biometrisches Merkmal realisiert wird. Die Kombination von zwei dieser Faktoren hat das Ziel, die Sicherheit der Authentifizierung zu erhöhen. Beispiele solcher Kombinationen von Faktoren im Rahmen der Zweifaktorauthentifizierung sind der Besitz einer Kontokarte sowie das Wissen einer persönlichen Identifikationsnummer (PIN), die Ermittlung eines biometrischen Merkmals im Rahmen einer Gesichtserkennung und das Wissen einer PIN für Zugangskontrollsysteme oder auch der Besitz einer Ausweiskarte und die Prüfung eines Finderabdrucks.

[0003] Allen üblichen Lösungen ist gemein, dass die zu identifizierende Person entweder eine gegenständliche Komponente und/oder die Kenntnis einer nur ihm bekannten alphanumerischen Zeichenkombination benötigt. Beide Faktoren sind risikobehaftet, da erstere gestohlen oder verloren werden kann und letztere ausgespäht oder erraten werden können. Wird die Zeichenkombination verlängert, um ein Ausspähen oder Erraten zu erschweren, steigt in der Praxis das Risiko, dass der Anwender die Zeichenkombination notiert und diese wiederum dem Diebstahl aussetzt.

[0004] Die Erfindung macht es sich daher zur Aufgabe, einen verbesserten Ansatz zur Authentifizierung einer Person bereitzustellen.

Zusammenfassung der Erfindung

[0005] Ein erster Aspekt der Erfindung löst diese Aufgabe durch ein verbessertes Verfahren für die Authentifizierung einer Person. Das erfindungsgemäße Verfahren umfasst wenigstens die folgenden Schritte:

-- Erfassen eines biometrischen Merkmals der Person;

-- Ableiten einer biometrischen Schlüsselinformation aus dem erfassten biometrischen Merkmal;

-- Nachweisen der biometrischen Schlüsselinformation gegenüber einem Chipimplantat der Person;

-- Empfangen eines von dem Chipimplantat übermittelten Attributs der Person in Antwort auf die nachgewiesene biometrische Schlüsselinformation; und

-- Authentifizieren der Person in Abhängigkeit von dem empfangenen Attribut.

[0006] Die Erfindung besitzt den Vorteil, dass ein Chipimplantat im Gegensatz zu einer Ausweiskarte oder einem anderen Identifikationstoken nicht verloren gehen kann. Auf diese Weise ist bereits der erste der zwei verwendeten Faktoren für die Zweifaktorauthentifizierung gesichert. Als weiterer Faktor tritt erfindungsgemäß ein biometrisches Merkmal hinzu, wobei dieses verwendet wird, um den Chip des Chipimplantats kryptographisch aufzuschließen. Das biometrische Merkmal wird also zur Authentifizierung eines Lesegerätes gegenüber dem Chipimplantat verwendet, welches mit der Übermittlung eines geschützt im Chipimplantat gespeicherten Attributes antwortet. Das Attribut stellt wiederum die Grundlage der abschließenden Authentifizierung der Person dar. Auf diese Weise werden die beiden für sich bereits mit einer hohen Sicherheit ausgestatteten Faktoren untrennbar miteinander verknüpft, wodurch ein Verfahren mit einer sehr hohen Sicherheit der Authentifizierung zur Verfügung gestellt wird. Ein weiterer Vorteil Erfindung besteht darin, dass die für die Authentifizierung verwendeten biometrischen Daten nicht in einem externen System gespeichert werden müssen, so dass etwaige datenschutzrechtliche Vorbehalte der zu authentifizierenden Person ausgeräumt werden können und ein Angriff auf ein solches externes System zur Erbeutung der hinterlegten biometrischen Daten sinnlos wird. Dadurch wird das Sicherheitsniveau des erfindungsgemäßen Authentifizierungsverfahrens zusätzlich erhöht.

[0007] Bei dem Attribut kann es sich um eine Bezeichnung der Person, einen Berechtigungsnachweis oder dergleichen handeln. Bei dem biometrischen Merkmal kann es sich beispielsweise um einen Irisscan oder einen Fingerabdruck beziehungsweise in bekannter Weise daraus abgeleitete Merkmale handeln. Solche abgeleiteten Merkmale werden üblicherweise im Zuge einer Datenreduktion einer photographischen Erfassung von Iris beziehungsweise Fingerabdruck gewonnen. Die abgeleitete Schlüsselinformation kann jedoch auch eine datentechnisch vollständige Repräsentation des erfassten biometrischen Merkmals sein.

[0008] Besonders vorteilhaft können ein oder mehrere Fingerabdrücke das biometrische Merkmal darstellen, da ein Chipimplantat häufig in die Hautfalte zwischen Daumen und Zeigefinger einer Hand implantiert wird. Dabei wird gewährleistet, dass sich das Chipimplantat bei der Erfassung des biometrischen Merkmals - hier also des wenigstens einen Fingerabdrucks - in räumlicher Nähe zu dem Chipimplantat befindet.

[0009] Das Verfahren kann einen zusätzlichen Schritt des Freigebens eines Zugangs zu einem geschützten Bereich aufweisen. Das Freigeben des Zugangs erfolgt nur dann, wenn der Schritt des Authentifizierens der Person erfolgreich abgeschlossen wurde. Bei dem geschützten Bereich kann es sich sowohl um einen virtuellen Bereich, also etwa vertrauliche Daten, als auch um eine räumliche Begebenheit wie ein Schließfach, ein Grundstück oder einen Zimmer handeln. In der zweiten Alternative kann der Schritt des Freigebens des Zugangs einen Schritt des Ansteuerns einer Schließanlage beinhalten.

[0010] Bei Ausführungsformen des erfindungsgemäßen Verfahrens kann vorgesehen sein, dass der Schritt des Authentifizierens der Person einen zusätzlichen Schritt des Vergleichens des empfangenen Attributs mit einem vorherbestimmten Referenzattribut beinhaltet. Hierbei signalisiert das Attribut selbst bereits eine Berechtigung der Person und kann direkt vom empfangenden Lesegerät geprüft werden.

[0011] Besonders bevorzugt kann der Schritt des Authentifizierens der Person einen zusätzlichen Schritt des Prüfens einer Signatur des empfangenen Attributs beinhalten. Das Prüfen der Signatur kann anhand eines bekannten öffentlichen Schlüssels erfolgen, mit dem geprüft werden kann, dass das Attribut nicht gefälscht oder verfälscht wurde. Insbesondere kann das Attribut in der Form eines kryptographisch gesicherten Zertifikats vorliegen.

[0012] Alternativ oder zusätzlich kann der Schritt des Authentifizierens der Person einen Schritt des Übermittelns des empfangenen Attributs an ein Register und einen Schritt des Empfangens eines Berechtigungssignals von dem Register in Antwort auf das übermittelte empfangene Attribut beinhalten, wobei der Schritt des Authentifizierens der Person in Abhängigkeit von dem empfangenen Berechtigungssignal erfolgt. Das Register kann beispielsweise ein Server sein, der zu den verschiedenen durch Attribute bezeichneten Personen die jeweiligen Berechtigungen speichert und auf eine Anfrage durch ein Lesegerät anhand des übermittelten empfangenen Attributs mit der Übermittlung des Berechtigungssignals reagiert. Das Berechtigungssignal kann beispielsweise als kryptographisch gesichertes Zertifikat an das Lesegerät übermittelt werden. Die Verwendung einer Signatur durch das Chipimplantat zur Absicherung des übermittelten Attributs der zu authentifizierenden Person erlaubt insbesondere bei Verwendung eines solchen Registers eine zusätzliche Absicherung, bei der das Chipimplantat das Attribut mit einem Zeitstempel versieht und anschließend signiert, so dass Angriffe auf das Register anhand eines zuvor abgehörten signierten Attributs schon wegen des veralteten Zeitstempels scheitern, weil der Zeitstempel ebenfalls durch die Signatur vor Veränderung geschützt ist. Die Verwendung eines Registers kann auch dadurch abgesichert werden, dass das Register nur eine lokal durchgeführte erfolgreiche Authentifizierung negativ überstimmen kann. Das Übermitteln des empfangenen Attributs an das Register erfolgt hierbei also unter der Bedingung einer erfolgreichen lokalen Authentifizierung, wobei das vom Register in Antwort übersandte Berechtigungssignal die erfolgreiche lokale Authentifizierung lediglich unverändert lassen oder invalidieren, nicht jedoch eine negative lokale Authentifizierung in eine positive Authentifizierung verändern kann.

[0013] Das erfindungsgemäße Verfahren kann auch einen zusätzlichen Schritt des Übermittelns eines in dem Chipimplantat zu speichernden Datensatzes an das Chipimplantat beinhalten. Bei dem Datensatz kann es sich beispielsweise um ein neues oder geändert in dem Chipimplantat zu speicherndes Attribut oder um eine elektronische Quittung für eine durch den erfolgreichen Abschluss der Authentifizierung bewirkten Vorgangs handeln.

[0014] Ein zweiter Aspekt der Erfindung betrifft Lesegerät mit einer Erfassungseinheit, einer Sende/Empfangseinheit und einer mit der Erfassungseinheit und der Sende/Empfangseinheit verbundenen Steuereinheit. Die Erfassungseinheit ist dabei dazu ausgebildet, ein biometrisches Merkmal einer Person zu erfassen. Die Sende/Empfangseinheit ist dazu ausgebildet, mit einem Chipimplantat der Person zu kommunizieren. Die Steuereinheit ist dabei dazu ausgebildet, das Verfahren des ersten Erfindungsaspektes durchzuführen. Beispielsweise kann es sich bei der Erfassungseinheit um eine Kamera oder einen Fingerabdrucksensor handeln.

[0015] Bei Verwendung eines Fingerabdrucksensors kann das Lesegerät vorteilhaft so ausgestaltet sein, dass die Sende/Empfangseinheit bei Auflegen des Fingers durch die zu authentifizierende Person auf den Fingerabdrucksensor in räumliche Nähe zu einem in die Hautfalte zwischen Zeigefinger und Daumen implantiertes Chipimplantat gelangt. Beispielsweise kann der Fingerabdrucksensor gegenüber der Sende/Empfangseinheit vertieft angeordnet sein. Ebenso ist vorstellbar, dass das Lesegerät (z.B. ähnlich einem Türgriff) von der zu authentifizierenden Person umgriffen werden muss, wobei das wie erwähnt platzierte Chipimplantat auf der Sende/Empfangseinheit und wenigstens ein Finger auf dem Fingerabdrucksensor zu liegen kommen. Hierbei kann das Lesegerät auf einer Tür oder Klappe angeordnet sein, die sich nach erfolgreicher Authentifizierung durch Zug oder Druck auf das Lesegerät öffnen lässt.

[0016] Als Lesegeräte können im Rahmen der Erfindung beispielsweise auch entsprechend eingerichtete Smartphones oder Computer angesehen werden. Für die Erfassung des biometrischen Merkmals könn-

ten ein Fingerabdrucksensor, für die Kommunikation mit dem Chipimplantat beispielsweise eine NFC-Einheit (NFC, Near Field Communication) vorgesehen sein, wie sie insbesondere bei Smartphones weit verbreitete Ausstattungsmerkmale sind. Ein Fingerabdrucksensor sowie eine räumlich dazu geeignet angeordnete Sende/Empfangseinheit für die Kommunikation mit dem Chipimplantat könnten problemlos auch in einer Computertastatur angeordnet werden. Eine Anmeldung an dem Smartphone oder Computer könnte dann durch Fingerauflegen vollzogen werden, wobei das Sicherheitsniveau jedoch gegenüber einer herkömmlichen Lösung deutlich erhöht ist.

[0017] Ein weiterer Erfindungsaspekt führt daher eine Zugangskontrollanordnung mit einem erfindungsgemäßen Lesegerät und einer Schließanlage ein, welche ausgebildet ist, Zutritt zu einem geschützten Bereich zu gewähren oder zu verweigern. Hierbei ist die Steuereinheit des Lesegeräts dazu ausgebildet ist, eine Schließanlage anzusteuern.

[0018] Die Erfindung betrifft außerdem ein Chipimplantat mit einer Sende/Empfangseinheit, einem Speicher und mit einer Steuereinheit ein. Die Sende/Empfangseinheit ist dazu ausgebildet, mit einem Lesegerät zu kommunizieren. Der Speicher ist dazu ausgebildet, eine biometrische Referenzinformation und ein Attribut zu speichern. Die Steuereinheit ist mit der Sende/Empfangseinheit und dem Speicher verbunden und dazu ausgebildet, über die Sende/Empfangseinheit einen Nachweis der biometrischen Schlüsselinformation zu empfangen, den empfangenen Nachweis der biometrischen Schlüsselinformation unter Verwendung der biometrischen Referenzinformation zu prüfen und das Attribut über die Sende/Empfangseinheit zu senden, wenn die Prüfung des Nachweises der empfangenen biometrischen Schlüsselinformation erfolgreich war, und andernfalls einen Zugriff auf das Attribut zu verweigern.

[0019] Das Chipimplantat kann außerdem dazu ausgebildet sein, über die Sende/Empfangseinheit einen in seinem Speicher zu speichernden Datensatzes zu empfangen und in seinem Speicher zu speichern. Hierbei gelten die oben gemachten Erläuterungen.

[0020] Weitere bevorzugte Ausführungsformen der Erfindung lassen sich der nachfolgenden Beschreibung entnehmen.

Figurenliste

[0021] Die Erfindung wird nachfolgend anhand von Abbildungen von Ausführungsbeispielen näher erläutert. Die Figuren zeigen:

Fig. 1 ein Ausführungsbeispiel des erfindungsgemäßen Verfahrens als Flussdiagramm;

Fig. 2 ein Ausführungsbeispiel einer Zugangskontrollanordnung mit einem erfindungsgemäßen Lesegerät als Blockdiagramm; und

Fig. 3 ein Ausführungsbeispiel eines erfindungsgemäßen Chipimplantats als Blockdiagramm.

Detaillierte Beschreibung der Erfindung

[0022] **Fig. 1** zeigt ein Ausführungsbeispiel des erfindungsgemäßen Verfahrens als Flussdiagramm. Das Verfahren beginnt in einem Startschritt **S0**, der beispielsweise durch eine Interaktion der zu authentifizierenden Person wie ein Auflegen eines Fingers auf eine Erfassungseinrichtung, ein Herantreten an ein Lesegerät oder dergleichen ausgelöst werden kann. In einem Schritt **S1** wird ein biometrisches Merkmal der zu authentifizierenden Person erfasst. Im Rahmen der Erfindung können beispielsweise ein oder mehrere Fingerabdrücke, eine Iris, ein Gesicht oder eine Kombination mehrerer solcher Einzelmerkmale als biometrisches Merkmal erfasst werden. Das biometrische Merkmal der Person kann insbesondere photographisch erfasst werden.

[0023] In einem nachfolgenden Schritt **S2** wird eine biometrische Schlüsselinformation aus dem erfassten biometrischen Merkmal abgeleitet, wobei die abgeleitete biometrische Schlüsselinformation im einfachsten Fall eine vollständige digitale Repräsentation des erfassten biometrischen Merkmals, wie sie im Schritt **S1** erzeugt wurde, sein kann. Es ist aber auch vorstellbar, dass besonders kennzeichnende Teile des erfassten biometrischen Merkmals extrahiert werden, wie beispielsweise Verlaufsformen von Papillarleisten in einem erfassten Fingerabdruck, Abstände von Gesichtsmerkmalen und deren relative Verhältnisse zueinander, farbreduzierte oder kontrastveränderte Wiedergaben der Iris und dergleichen mehr. Diese Informationen können direkt als Schlüsselinformation oder aber beispielsweise für die Erzeugung einer pseudozufälligen Zahl verwendet werden. Hierzu kann die extrahierte Information als „Seed“ eines festgelegten Pseudozufallsgenerators benutzt werden, wobei die Ausgabe des Pseudozufallsgenerators als abgeleitete biometrische Schlüsselinformation im Rahmen des erfindungsgemäßen Verfahrens verwendet wird.

[0024] Die derart abgeleitete biometrische Schlüsselinformation wird in einem anschließenden Schritt **S3** an ein Chipimplantat der zu authentifizierenden Person nachgewiesen. Dies kann beispielsweise per kapazitiver, induktiver oder per Fernfeldübertragung geschehen. Allgemein kann die elektrische Versorgung des Chipimplantats während der Durchführung des Verfahrens über eine induktive Anregung durch ein erfindungsgemäßes Lesegerät erfolgen.

[0025] Die Kommunikation erfolgt hierbei bevorzugt kryptographisch abgesichert und kann beispielsweise eine Aushandlung von Sitzungsschlüsseln und sonstige bekannte kryptographische Verfahren beinhalten. Beispielsweise kann ein an das Basic Access Control-Protokoll angelehntes kryptographisches Verfahren verwendet werden.

[0026] Insbesondere kann die abgeleitete biometrische Schlüsselinformation in einer Weise nachgewiesen werden, bei der die abgeleitete biometrische Schlüsselinformation nicht selbst übermittelt wird, sondern dem Chipimplantat deren korrektes Vorliegen im Lesegerät anhand eines übermittelten Datensatzes nachgewiesen wird. Hierzu ist z.B. denkbar, dass ein Challenge-Response-Verfahren eingesetzt wird, in dem das Chipimplantat eine Zufallszahl bestimmt und mit der im Chipimplantat vorhandenen Referenz des abgeleiteten biometrischen Schlüsselinformation (beziehungsweise bei Verwendung eines asymmetrischen Verschlüsselungsverfahren mit einem zugehörigen öffentlichen Schlüssel) verschlüsselt, an das Lesegerät übermittelt und sich von diesem die Zufallszahl zurückübertragen lässt, wodurch das Chipimplantat prüft, ob da Lesegerät über die für die erfolgreiche Entschlüsselung notwendige abgeleitete biometrische Schlüsselinformation verfügt.

[0027] Gelangt die Prüfung des Nachweises durch das Chipimplantat zu einem erfolgreichen Ergebnis, antwortet das Chipimplantat mit der Übermittlung eines in dem Chipimplantat gespeicherten Attributs. Demzufolge wird in einem auf den Schritt **S3** folgenden Schritt ein Attribut empfangen und in Schritt **S5** die eigentliche Authentifizierung der Person in Abhängigkeit von dem empfangenen Attribut durchgeführt.

[0028] Der Schritt **S5** kann mehrere Teilschritte umfassen, die in einzelnen Ausführungsformen in unterschiedlicher Reihenfolge oder auch parallel zueinander ausgeführt werden können. Im gezeigten Ausführungsbeispiel umfasst der Schritt **S5** vier Teilschritte, die jedoch in anderen Ausführungsbeispielen nicht zwingend vorhanden sein müssen. In einem Teilschritt **S5.1** wird eine Signatur des empfangenen Attributs geprüft. Die Signatur kann nach bekannten kryptographischen Verfahren erstellt sein und nachweisen, dass das Attribut von einer autorisierten Instanz (z.B. Trustcenter) erstellt wurde. Auf diese Weise wird mit einfachen Mitteln sichergestellt, dass das Attribut nicht gefälscht ist. Beispielsweise kann die Signatur mit einem geheimen Schlüssel der autorisierten Instanz erstellt und mit einem im Lesegerät hinterlegten oder von diesem abfragbaren zugehörigen öffentlichen Schlüssel geprüft werden. Beispielsweise kann es sich um eine Signatur gemäß X.509 Version 3 handeln.

[0029] Wird die Signatur als ungültig befunden, gelangt die Authentifizierung zu einem negativen Ergebnis und das Verfahren wird abgebrochen und/oder es werden Alarmmaßnahmen eingeleitet. In Schritt **S5.2** wird das empfangene Attribut mit einem vorherbestimmten Referenzattribut verglichen. Beispielsweise kann das Attribut unmittelbar anzeigen, dass die Person, die das Chipimplantat trägt, berechtigt ist, auf einen geschützten Bereich (virtuell oder physisch) zuzugreifen. In einem solchen Fall wird das Attribut also mit demjenigen Vorgabedatensatz verglichen, der eine solche Zugriffsberechtigung anzeigt. Das vorherbestimmte Referenzattribut kann aber auch als Teil eines Satzes von Referenzattributen gespeichert sein, welche alle mit dem empfangenen Attribut verglichen werden. So könnte das empfangene Attribut einen Namen oder eine Identifikationsnummer der zu authentifizierenden Person anzeigen und der Satz von Referenzattributen diejenigen Personen mit der notwendigen Berechtigung entsprechend bezeichnen.

[0030] In Schritt **S5.3** kann das empfangene Attribut an ein Register übermittelt werden, beispielsweise an einen über ein Netzwerk erreichbaren Server wie ein Trustcenter und in Antwort hierauf in Schritt **S5.4** ein Berechtigungssignal von dem Register empfangen werden. Dies kann dazu dienen, die Berechtigung der zu authentifizierenden Person von dem Register zu erfragen oder das Fortbestehen einer erteilten Berechtigung und durch das Attribut unmittelbar angezeigten Berechtigung zu prüfen. So könnte eine solche Berechtigung durch Hinterlegung eines Widerrufszertifikats in dem Register als ungültig gekennzeichnet werden. Liegt in dieser beispielhaften Ausführungsform ein solches Widerrufszertifikat in dem Register vor, antwortet das Register mit einem entsprechenden negativen Berechtigungssignal und die Authentifizierung scheitert, andernfalls mit einem positiven.

[0031] Nach erfolgreicher Authentifizierung in Schritt **S5** wird in Schritt **S6** ein Zugang zu einem geschützten Bereich freigegeben. Dieser geschützte Bereich kann physischer Natur sein, also beispielsweise ein Firmengelände, ein Schließfach oder ähnliches. Ebenso lassen sich die verschiedenen Aspekte der Erfindung aber auch auf geschützte Bereiche virtueller, also datentechnischer Natur anwenden. Beispiele hierfür wären bei einem Internetdienstleister geführte Konten wie Email- und Einkaufskonten oder aber auch Cloudspeicherbereiche oder geschützte Netzwerke wie z.B. für die Anlagensteuerung. Bei Zugriff auf einen physischen geschützten Bereich kann eine Schließanlage angesteuert werden (Schritt **S7**).

[0032] In einem optionalen Schritt **S8** kann ein in dem Chipimplantat zu speichernder Datensatz an das Chipimplantat übermittelt werden. Dies kann beispielsweise dazu verwendet werden, zusätzliche

Attribute wie einen Berechtigungsnachweis in dem Chipimplantat zu speichern. Ebenso ist denkbar, eine elektronische Quittung in Form des Datensatzes an das Chipimplantat zu übermitteln, so dass beispielsweise eine Zugriffshistorie der zu authentifizierenden Person anhand des Chipimplantats erstellt werden kann. Eine solche Quittung kann durch die zu authentifizierende Person auch dazu verwendet werden, die eigene Anwesenheit am Ort des verwendeten Lesegeräts zu einem bestimmten Zeitpunkt nachzuweisen. Anschließend wird das Verfahren in Schritt **S9** beendet.

[0033] Fig. 2 zeigt ein Ausführungsbeispiel einer Zugangskontrollanordnung **10** mit einem erfindungsgemäßen Lesegerät **11** als Blockdiagramm. Die erfindungsgemäße Zugangskontrollanordnung **10** verfügt in dem gezeigten Ausführungsbeispiel ein Lesegerät 11 und eine Schließanlage **17**, welche von dem Lesegerät **11** gesteuert wird und abhängig von dieser Steuerung Zugang zu einem geschützten Bereich gewährt oder verweigert. Das Lesegerät **11** besitzt eine Steuereinheit **12**, welche mit der Schließanlage **17** über eine Steuerschnittstelle **16** kommuniziert. Die Kommunikation kann drahtgebunden oder drahtlos und selbstredend kryptographisch abgesichert erfolgen. Die Steuereinheit **12** ist dazu ausgebildet, das erfindungsgemäße Verfahren durchzuführen.

[0034] Das Lesegerät **11** verfügt über eine Erfassungseinheit **13**, die mit der Steuereinheit **12** verbunden ist und ein biometrisches Merkmal erfassen kann. Beispielsweise kann die Erfassungseinheit **13** eine Kamera oder ein Fingerabdrucksensor sein. Ferner besitzt das Lesegerät **11** eine mit der Steuereinheit **12** verbundene Sende/Empfangseinheit **14**, welche für die Kommunikation mit dem Chipimplantat ausgebildet ist. Die Sende/Empfangseinheit **14** kann außerdem zusätzlich dazu ausgebildet sein, das Chipimplantat für die Dauer der Durchführung des erfindungsgemäßen Verfahrens mit Energie zu versorgen.

[0035] In dem gezeigten Ausführungsbeispiel besitzt das Lesegerät **11** zudem eine mit der Steuereinheit **12** verbundene Netzwerkschnittstelle **15**, über welche die Steuereinheit **12** wie oben beschrieben mit einem Register kommunizieren kann.

[0036] Die Steuereinheit **12** kann ein Prozessor mit einem integrierten Speicher für die im Rahmen der Durchführung des erfindungsgemäßen Verfahrens zu verwendenden Daten und Programme sein, alternativ aber auch als festverdrahtete Logik aufgebaut werden.

[0037] Fig. 3 zeigt ein Ausführungsbeispiel eines erfindungsgemäßen Chipimplantats **20** als Blockdiagramm. Das Chipimplantat **20** besitzt eine Steuereinheit **21**, einen mit der Steuereinheit **21** verbundenen Speicher **23** sowie eine mit der Steuereinheit **21** verbundene Sende/Empfangseinheit **22**. Das Chipimplantat **20** ist dabei dazu ausgebildet, eine das Implantat tragende Person im Rahmen der hierin beschriebenen Verfahren auszuweisen. Das Chipimplantat **20** kann in bekannter Weise bioverträglich gekapselt sein und über eine Empfangseinheit zur drahtlosen Energieversorgung durch externe Anregung verfügen (nicht gezeigt).

Bezugszeichenliste

S0	Start
S1	Erfassen eines biometrischen Merkmals einer Person
S2	Ableiten einer biometrischen Schlüsselinformation aus dem erfassten biometrischen Merkmal
S3	Nachweisen der biometrischen Schlüsselinformation gegenüber einem Chipimplantat der Person
S4	Empfangen eines von dem Chipimplantat übermittelten Attributs der Person in Antwort auf die nachgewiesene biometrische Schlüsselinformation
S5	Authentifizieren der Person in Abhängigkeit von dem empfangenen Attribut
S5.1	Prüfen einer Signatur des empfangenen Attributs
S5.2	Vergleichen des empfangenen Attributs mit einem vorherbestimmten Referenzattribut
S5.3	Übermitteln des empfangenen Attributs an ein Register
S5.4	Empfangen eines Berechtigungssignals von dem Register in Antwort auf das übermittelte empfangene Attribut
S6	Freigeben eines Zugangs zu einem geschützten Bereich
S7	Ansteuern einer Schließanlage
S8	Übermitteln eines in dem Chipimplantat zu speichernden Datensatzes an das Chipimplantat
S9	Ende
10	Zugangskontrollanordnung
11	Lesegerät
12	Steuereinheit
13	Erfassungseinheit
14	Sende/Empfangseinheit
15	Netzwerkschnittstelle

16 Steuerschnittstelle

17 Schließanlage

20 Chipimplantat

21 Steuereinheit

22 Sende/Empfangseinheit

23 Speicher

Patentansprüche

1. Ein Verfahren für die Authentifizierung einer Person und mit den Schritten:
-- Erfassen eines biometrischen Merkmals der Person (S1);
-- Ableiten einer biometrischen Schlüsselinformation aus dem erfassten biometrischen Merkmal (S2);
-- Nachweisen der biometrischen Schlüsselinformation gegenüber einem Chipimplantat (20) der Person (S3);
-- Empfangen eines von dem Chipimplantat (20) übermittelten Attributs der Person in Antwort auf die nachgewiesene biometrische Schlüsselinformation (S4); und
-- Authentifizieren der Person in Abhängigkeit von dem empfangenen Attribut (S5).

2. Das Verfahren des vorhergehenden Anspruchs, mit einem zusätzlichen Schritt (S6) des Freigebens eines Zugangs zu einem geschützten Bereich, wenn der Schritt (S5) des Authentifizierens der Person erfolgreich abgeschlossen wurde.

3. Das Verfahren des vorhergehenden Anspruchs, bei dem der Schritt (S6) des Freigebens des Zugangs einen Schritt (S7) des Ansteuerns einer Schließanlage (17) beinhaltet.

4. Das Verfahren eines der vorhergehenden Ansprüche, bei dem der Schritt (S5) des Authentifizierens der Person einen zusätzlichen Schritt (S5.2) des Vergleichens des empfangenen Attributs mit einem vorherbestimmten Referenzattribut beinhaltet.

5. Das Verfahren eines der vorhergehenden Ansprüche, bei dem der Schritt (S5) des Authentifizierens der Person einen zusätzlichen Schritt (S5.1) des Prüfens einer Signatur des empfangenen Attributs beinhaltet.

6. Das Verfahren eines der vorhergehenden Ansprüche, bei dem der Schritt (S5) des Authentifizierens der Person einen zusätzlichen Schritt (S5.3) des Übermittelns des empfangenen Attributs an ein Register und einen zusätzlichen Schritt (S5.4) des Empfangens eines Berechtigungssignals von dem Register in Antwort auf das übermittelte empfangene Attribut beinhaltet, wobei der Schritt (S5) des Authentifizierens der Person in Abhängigkeit von dem empfangenen Berechtigungssignal erfolgt.

7. Das Verfahren eines der vorhergehenden Ansprüche, mit einem zusätzlichen Schritt (S8) des Übermittelns eines in dem Chipimplantat (20) zu speichernden Datensatzes an das Chipimplantat (20).

8. Ein Lesegerät (11) mit einer Erfassungseinheit (13), welche ausgebildet ist, ein biometrisches Merkmal einer Person zu erfassen, mit einer Sende/Empfangseinheit (14), welche ausgebildet ist, mit einem Chipimplantat (20) der Person zu kommunizieren, und mit einer mit der Erfassungseinheit (13) und der Sende/Empfangseinheit (14) verbundenen Steuereinheit (12), welche ausgebildet ist, das Verfahren eines der vorhergehenden Ansprüche durchzuführen.

9. Eine Zugangskontrollanordnung (10) mit einem Lesegerät (11) gemäß dem vorhergehenden Anspruch und einer Schließanlage (17), welche ausgebildet ist, Zutritt zu einem geschützten Bereich zu gewähren oder zu verweigern, **dadurch gekennzeichnet**, dass die Steuereinheit (12) des Lesegeräts (11) dazu ausgebildet ist, das Verfahren des Anspruchs 3 auszuführen.

10. Ein Chipimplantat (20) mit einer Sende/Empfangseinheit (22), welche ausgebildet ist, mit einem Lesegerät (11) zu kommunizieren, mit einem Speicher (23), welcher ausgebildet ist, eine biometrische Referenzinformation und ein Attribut zu speichern, und mit einer Steuereinheit (21), welche mit der Sende/Empfangseinheit (22) und dem Speicher (23) verbunden und dazu ausgebildet ist, über die Sende/Empfangseinheit (22) einen Nachweis einer biometrischen Schlüsselinformation zu empfangen, den empfangenen Nachweis der biometrischen Schlüsselinformation unter Verwendung der biometrischen Referenzinformation zu prüfen und das Attribut über die Sende/Empfangseinheit (22) zu senden, wenn die Prüfung des Nachweises der empfangenen biometrischen Schlüsselinformation erfolgreich war, und andernfalls einen Zugriff auf das Attribut zu verweigern.

Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

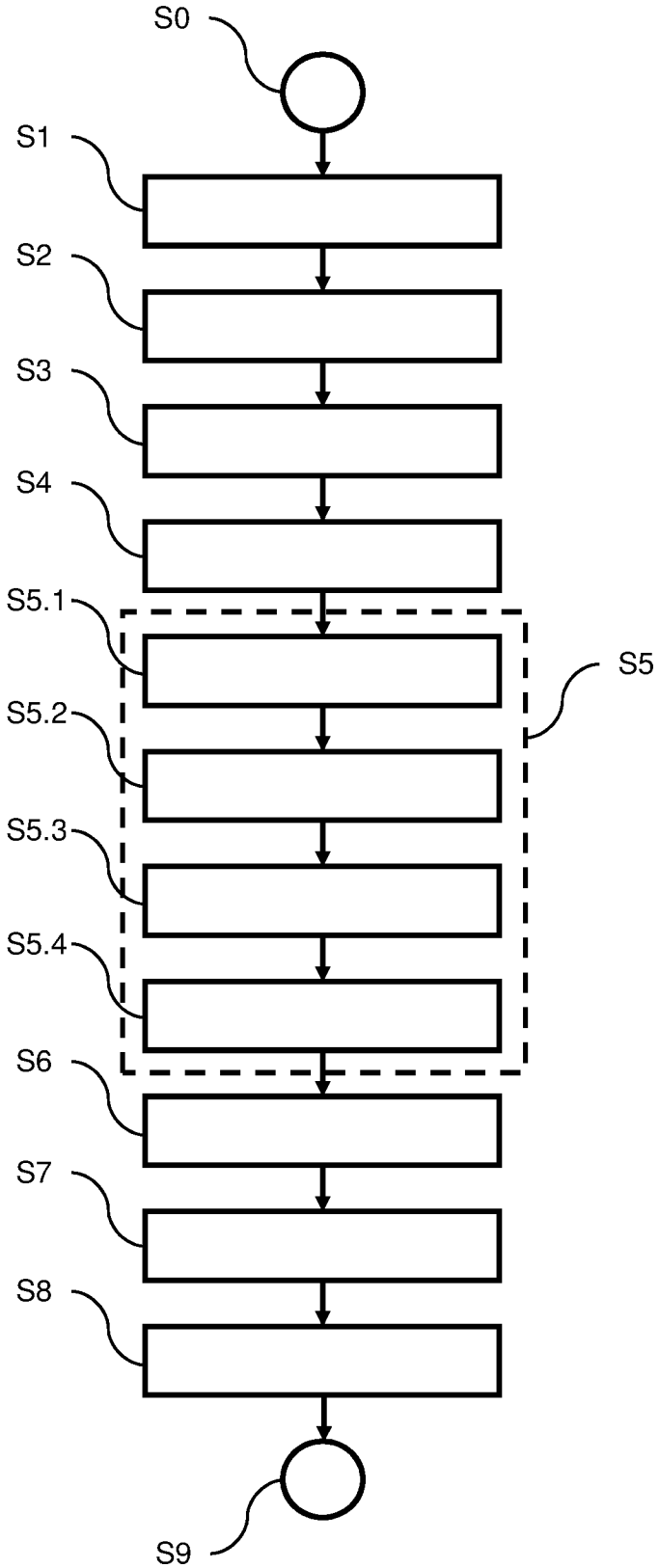


Fig. 1

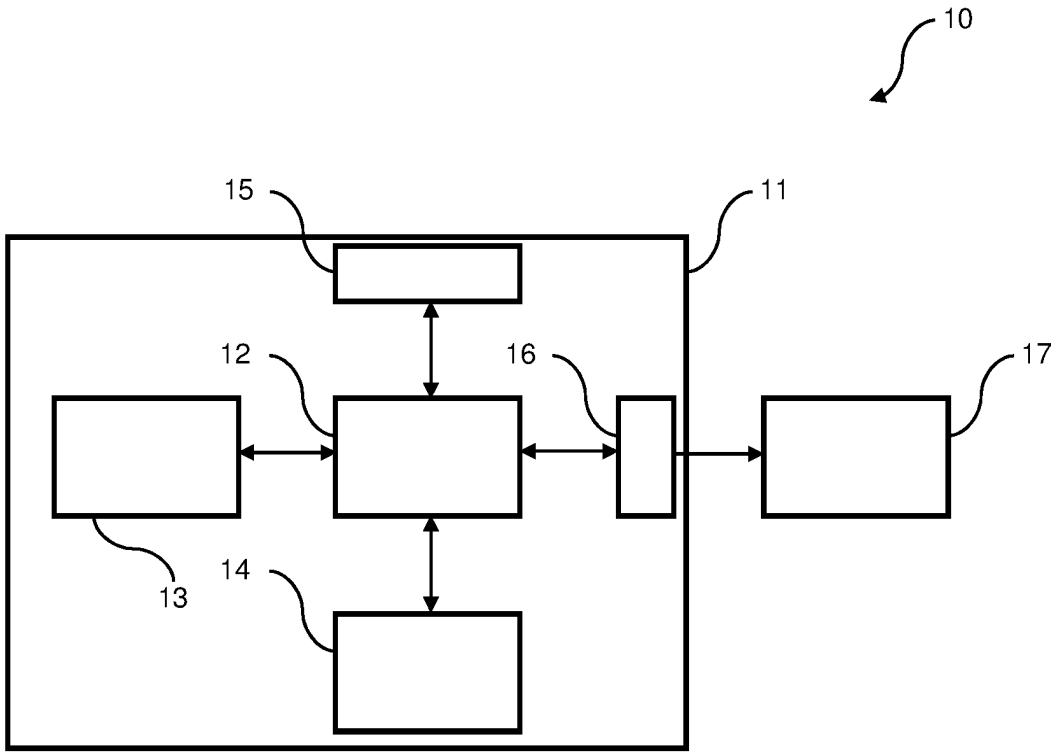


Fig. 2

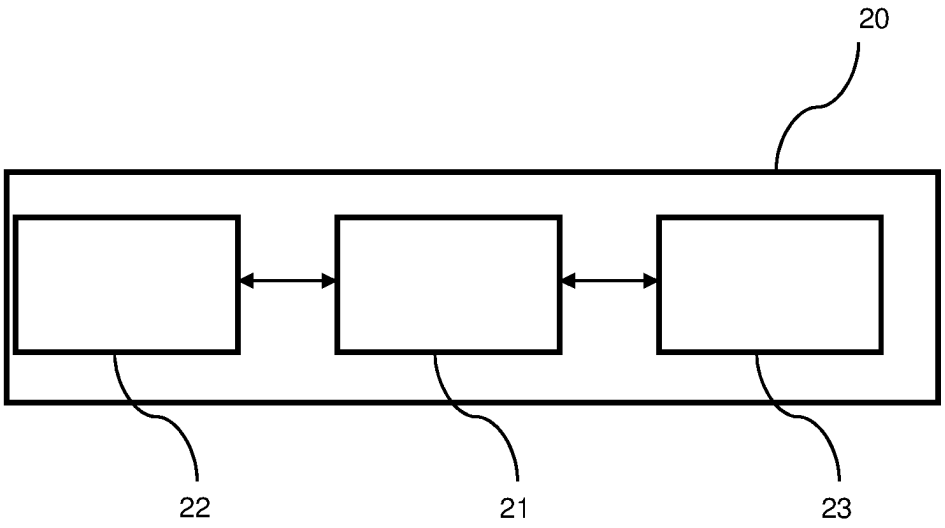


Fig. 3