

(12)

Patentschrift

(21) Anmeldenummer: A 1868/2008
(22) Anmeldetag: 02.12.2008
(45) Veröffentlicht am: 15.02.2013

(51) Int. Cl. : **G06K 17/00** (2006.01)
G06F 21/00 (2006.01)
G07F 7/10 (2006.01)
G07C 9/00 (2006.01)

(56) Entgegenhaltungen:
US 2003208684 A1
US 2004104265 A1
EP 1251468 A2
WO 2003100544 A2

(73) Patentinhaber:
HUMAN BIOS GMBH
8280 KREUZLINGEN (CH)

(54) **ANFORDERUNGSBASIERTES PERSONENIDENTIFIKATIONSVERFAHREN**

(57) Die Erfindung betrifft ein anforderungsbasiertes Personenidentifikationsverfahren umfassend die Schritte:

Empfang einer Authentifizierungsanforderung (7) von einem Dienstbereitstellungssystem (5) durch ein Authentifikations-Kontrollsystem (1);

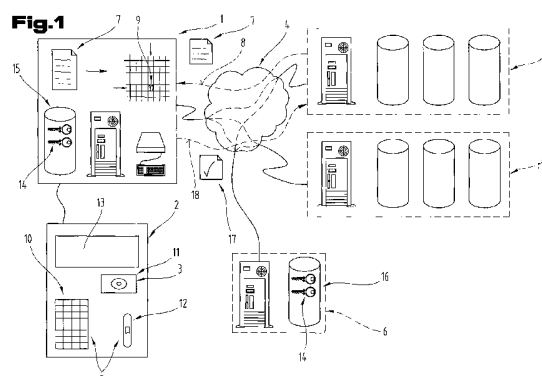
Ermitteln der erforderlichen Authentifizierungsstufe (9) durch das Authentifikations-Kontrollsystem (1) durch Analyse der Authentifizierungsanforderung (7);

Aktivieren (21) eines Erfassungsmittels (3) einer Erfassungsvorrichtung (2);

Erfassen (22) einer personenbezogenen Kennung durch das Erfassungsmittel (3);

Vergleich (23) der erfassten Kennung mit einem, in einer Speichereinheit (15, 16) hinterlegten, korrespondierenden Referenzmerkmal (14);

wobei bei Übereinstimmung ein Freigabesignal (17) an das Dienstbereitstellungssystem (5) abgegeben wird, und bei fehlerhafter Übereinstimmung (25) ein weiteres Erfassungsmittel (3) der Erfassungsvorrichtung (2) aktiviert wird und die entsprechenden Verfahrensschritte wiederholt werden.



Beschreibung

[0001] Die Erfindung betrifft ein anforderungsbasiertes Personenidentifikationsverfahren.

[0002] Zur Inanspruchnahme eines angebotenen Dienstes ist es bekannt, dass sich eine Person beim Dienstanbieter korrekt identifizieren und authentifizieren muss. Gerade bei der Inanspruchnahme eines nicht lokalen Dienstes besteht das Problem, dass über eine Entfernung hinweg, eine korrekte und zuverlässige Authentifikation einer anfragenden Person sichergestellt werden muss. Insbesondere besteht bei Inanspruchnahme eines Dienstes zumeist die Notwendigkeit, dass die Benützung des Dienstes selbst, oder die darüber angebotenen Leistungen, der anfragenden Person vergewährt werden müssen. Daher ist es von besonderer Bedeutung, dass nur eine korrekt identifizierte Person die bereitgestellten Dienstleistungen in Anspruch nehmen kann. Zur korrekten Authentifikation bzw. Identifikation einer Person ist es bekannt, ein eindeutiges Merkmal der Person zu erfassen und dieses mit einem Referenzmerkmal zu vergleichen. Ferner ist es bekannt, die Benutzung eines bereitgestellten Dienstes über eine Zugriffskennung zu verwalten. Es wird also eine Zugriffskennung und/oder eine eindeutige Benutzerkennung erfasst und bei Übereinstimmung mit einem Referenzmerkmal die Benutzung des Dienstes freigegeben.

[0003] Das Dienstbereitstellungs-System kann nun eine Mehrzahl unterschiedlicher Dienste verwalten bzw. zur Verfügung stellen, wobei auch unterschiedliche Anforderungen an die Qualität bzw. Sicherheit der Authentifizierung einer Person gegeben sind. Beispielsweise ist für den Zugriff auf einen Nachrichtendienst zumeist eine geringere Sicherheitsstufe erforderlich, als dies für einen Zugriff auf ein Finanztransaktionssystem erforderlich ist. Bei bekannten Systemen musste eine Person für jeden Zugriff auf einen unterschiedlichen Dienst eine unterschiedliche Authentifizierungsprozedur durchlaufen, wobei die einzelnen Authentifizierungsvorgänge zumeist auch an unterschiedlichen Erfassungsvorrichtungen durchgeführt werden mussten.

[0004] Die Druckschrift US 2003/0208684 A1 offenbart ein verteiltes System zur persönlichen digitalen Identifikation, welches eine rasche Identifikation einer Person mittels biometrischer Daten oder anderer Merkmale ermöglicht. Dabei wird von einem Benutzer eine Anforderung auf Online-Ressourcen erfasst und ermittelt, ob diese Anforderung eine Authentifikation erfordert oder nicht. Darauf basierend werden Merkmale einer physischen Identifikation vom Benutzer erfasst und diese Merkmale mit gespeicherten Merkmalen des Benutzers verglichen. Bei Übereinstimmung einer erfassten mit einer hinterlegten Kennung gilt die Person als positiv identifiziert.

[0005] Auch das Dokument US 2004/0104265 A1 offenbart ein System zur persönlichen Identifikation, wobei ein persönliches Identifikationsterminal vorgesehen ist, welches eine Mehrzahl von Identifikationsmitteln mit einer Mehrzahl von auswählbaren Identifikationsstufen anbietet. Die Identifikationsmittel werden in Übereinstimmung mit einer Identifikationseinstellungsinformation ausgewählt.

[0006] Das Dokument EP 1 251 468 A2 offenbart ein Verfahren, bei dem erfasste biometrische Merkmale mit Referenzmerkmalen verglichen werden und darauf aufbauend eine Authentifizierungssicherheit bestimmt wird.

[0007] Das Dokument WO 2003/100544 A2 offenbart eine Benutzerauthentifikation basierend auf einem Graphenmodell, wobei sich die einzelnen Authentifizierungsverfahren entlang dieses Graphenmodells abbilden und somit in jedem Graphenpunkt eine entsprechende Authentifikationsicherheit gegeben ist.

[0008] Gemäß dieser Verfahren werden abhängig von der geforderten Authentifizierungsstufe sämtliche Authentifizierungs- bzw. Erfassungsmittel aktiviert und bei fehlerhafter Übereinstimmung die Authentifizierung abgebrochen und ein Fehlersignal ausgegeben. Bestenfalls wird bei fehlgeschlagener Authentifizierung dasselbe Erfassungsmerkmal ein weiteres Mal abgefragt. Dies ist einerseits zeitraubend und andererseits fehleranfällig. Die Gefahr einer fehlerhaften Authentifikation wird durch derartige Identifikationsverfahren in der Regel erhöht.

[0009] Personenbezogene, individuelle Kennungen bergen aber auch die Gefahr, dass sie bei unregelmäßiger Verwendung in Vergessenheit geraten können und somit die Gefahr besteht, dass eine korrekte und eindeutige Identifikation bzw. Authentifikation einer Person unter Umständen nicht immer zuverlässig möglich ist. Eine weit verbreitete Vorgehensweise besteht nun darin, dass nur wenige personenbezogene individuelle Kennungen verwendet werden, bspw. nur eine kleine Anzahl von Kennwörtern, wodurch die Sicherheitsfunktionalität der Identifikations- und Authentifikationsprüfung umgangen wird. Ein Angreifer könnte somit durch Ausspionage eines derartigen Kennwortes Zugriff auf eine Vielzahl unterschiedlicher Dienste erlangen und somit beträchtlichen Schaden anrichten.

[0010] Wird beispielsweise aufgrund einer zu geringen Verwendung eine personenbezogene Kennung vergessen, besteht bei bekannten Systemen kaum eine Möglichkeit den gewünschten Dienst in Anspruch zu nehmen, da zumeist kein Notfallszenario vorgesehen ist, um dennoch eine Authentifikation zu erreichen.

[0011] Ferner basieren bekannte Authentifizierungsverfahren zumeist auf einer korrekten Wiedergabe einer vordefinierten personenbezogenen Kennung bzw. auf der korrekten Durchführung einer vordefinierten Handlungsabfolge durch die zu authentifizierende Person. In jedem Fall geht es dabei um die korrekte Wiedergabe einer vorher festgelegten Aktion, wobei ein potentieller Angreifer diese Handlungen ausspionieren kann und sich somit in missbräuchlicher Weise Zugriff auf das Dienstbereitstellungs-System verschaffen kann.

[0012] Bekannte Verfahren basieren zumeist auf einer so genannten 3-Faktor-Authentifikation. Dabei werden zur Personenauthentifikation Merkmale herangezogen, die im Wesentlichen in direktem Bezug zur Person stehen. Von Nachteil ist dabei, dass diese Merkmale teilweise recht leicht ausspionierbar sind und somit nur ein geringes Maß an Sicherheit bei der Identifikation einer Person bieten. Auch sind bekannte Verfahren zumeist nicht flexibel genug, um unterschiedliche personenbezogene Kennungen zur Authentifikation einer Person heranzuziehen. Ferner kommt es bei einer fehlerhaften Erfassung einer personenbezogenen Kennung bzw. bei einem fehlerhaften Vergleich, bei bekannten Verfahren zumeist zu einem Abbruch des Authentifikationsvorgangs.

[0013] Die Aufgabe der Erfindung liegt nun darin, ein Verfahren zur eindeutigen Identifikation und Authentifikation einer Person zu schaffen, wobei die Authentifikation nicht auf ein einzelnes personenbezogenes Merkmal beschränkt ist und wobei insbesondere die Nachteile des Standes der Technik behoben werden sollen.

[0014] Die Aufgabe der Erfindung wird durch die Verfahrensschritte gemäß Anspruch 1 gelöst.

[0015] In einem ersten Schritt wird vom Authentifikations-Kontrollsystem eine Authentifizierungsanforderung eines Dienstbereitstellungs-Systems empfangen. Durch die Übermittlung der Authentifizierungsanforderung an ein Authentifikations-Kontrollsystem lässt sich die Durchführung der Personenauthentifikation bzw. -identifikation von der Dienstbereitstellung trennen, insbesondere kann somit ein Dienstbereitstellungs-System mit mehreren Authentifikations-Kontrollsystemen zusammenarbeiten, bzw. kann ein Authentifikations-Kontrollsystem von mehreren Dienstbereitstellungs-Systemen eine Authentifikationsanforderung empfangen. Von Vorteil ist ferner, dass nur eine Authentifizierungsanforderung übertragen wird und somit die Durchführung der Personenidentifikation bzw. Authentifikation von der Durchführung der Dienstbereitstellung getrennt ist. Insbesondere ist es somit möglich, dass die einzelnen beteiligten Systeme separiert ausgebildet sein können. Die Authentifizierungsanforderung kann nun bspw. derart flexibel ausgebildet sein, dass nicht nur eine Authentifizierungsanforderung als solche übermittelt wird, auf die das Authentifikations-Kontrollsystem reagiert, sondern dass eine Anfrage betreffend des gewünschten Dienstes übertragen wird und somit das Authentifikations-Kontrollsystem darauf basierend, ein entsprechendes Erfassungsmittel aktivieren kann.

[0016] In einem weiteren Schritt wird die Authentifizierungsanforderung analysiert und daraus die erforderliche Authentifizierungsstufe ermittelt. Durch die vorteilhafte logische bzw. physikalische Trennung der Dienstbereitstellung von der Personenidentifikation bzw. -authentifikation ist

durch Übermittlung der Authentifizierungsanforderung eine Angabe möglich, welchen Zuverlässigkeitsgrad die durchzuführende Authentifikation erreichen muss, um der Person Zugriff auf den bereitgestellten Dienst gewähren zu können. Ein bevorzugt universell ausgebildetes Authentifikations-Kontrollsystem ist also in der Lage, unterschiedliche personenbezogene Kennungen zu erfassen und somit einen unterschiedlichen Grad an Authentifizierungssicherheit durch das erfindungsgemäße Verfahren gewährleisten zu können. Insbesondere kann für sicherheitstechnisch unkritische Dienste eine einfach ausgebildete personenbezogene Kennung erfasst werden, für sicherheitstechnisch hochkritische Dienste kann eine personenbezogene Kennung erfasst werden, die sich nur äußerst schwer ausspionieren bzw. verfälschen lässt.

[0017] Nachdem die erforderliche Authentifizierungsstufe ermittelt wurde, wird ein entsprechendes Erfassungsmittel einer Erfassungsvorrichtung aktiviert, um damit eine personenbezogene Kennung zu erfassen, die zumindest der geforderten Sicherheitsstufe entspricht. Die Erfassungsvorrichtung umfasst bevorzugt mehrere Erfassungsmittel, um somit eine Mehrzahl unterschiedlicher personenbezogener Kennungen erfassen zu können, ohne dass eine weitere Erfassungsvorrichtung erforderlich wäre. Diese integrierte Erfassungsvorrichtung hat im Hinblick auf sicherheitstechnische Beläge den ganz besonderen Vorteil, dass diese besonders gesichert ausgebildet sein kann und damit ein hohes Maß an Verfälschungs- bzw. Manipulationssicherheit erreicht wird. Von Vorteil ist ferner die autarke Durchführung der Erfassung einer personenbezogenen Kennung durch das Authentifikations-Kontrollsystem und insbesondere durch die Erfassungsvorrichtung.

[0018] Die erfasste Kennung wird anschließend mit einem, in einer Speichereinheit hinterlegten, korrespondierenden Referenzmerkmal verglichen, wobei die Speichereinheit in der Erfassungsvorrichtung oder im Authentifikations-Kontrollsystem angeordnet sein kann. Der Vergleich kann nun dahingehend ausgebildet sein, dass neben einem exakten Vergleichsergebnis, auch ein Übereinstimmungsgrad ermittelt wird, wobei durch entsprechende Parametrierung festgelegt werden kann, welcher Übereinstimmungsgrad für ein korrektes Vergleichsergebnis erforderlich ist.

[0019] Bei Feststellung einer Übereinstimmung wird vom Authentifikations-Kontrollsystem ein Freigabesignal an das Dienstbereitstellungs-System abgegeben, worauf dieses den angeforderten Dienst der Person zugänglich macht. Insbesondere ist für den Betreiber des Dienstes gewährleistet, dass eine eventuell anfallende Benützungsgebühr eindeutig und unverwechselbar einer Person zugeordnet werden kann. Auch kann durch eine entsprechende Authentifikationsstufe sichergestellt werden, dass die Person bei Inanspruchnahme des bereitgestellten Dienstes, eine rechtsverbindlich zuordenbare Handlung vornimmt und dies eindeutig dokumentierbar ist.

[0020] Ein besonderer Vorteil des erfindungsgemäßen Verfahrens liegt nun darin, dass bei einer fehlerhaften Übereinstimmung ein weiteres Erfassungsmittel der Erfassungsvorrichtung aktiviert wird und die Verfahrensschritte zur Erfassung einer personenbezogenen Kennung, sowie der Vergleich mit einem korrespondierenden Referenzmerkmal, wiederholt werden. Bei der Erfassung einer personenbezogenen Kennung kann es aufgrund äußerer Einflüsse vorkommen, dass der anschließende Vergleich fehlschlägt, obwohl kein Manipulationsversuch vorliegt. Bei bekannten Verfahren würde die Authentifikation in diesem Fall abgebrochen und die Person hätte somit keinen Zugriff auf den angeforderten Dienst. Mit dem erfindungsgemäßen Verfahren ist es nun in vorteilhafter Weise möglich, ein weiteres personenbezogenes Merkmal zu erfassen, um so die fehlgeschlagene Authentifikation durch eine erneute Authentifikation, in diesem Fall allerdings mit einer sicherheitstechnisch höherwertigen personenbezogenen Kennung erneut durchzuführen. Durch die Ermittlung einer Authentifizierungsstufe ist festgelegt, welches Mindestmaß an Sicherheit die erfasste personenbezogene Kennung bieten muss, um den Dienst in Anspruch nehmen zu können. Mit dem erfindungsgemäßen Verfahren ist es nun jedoch in vorteilhafter Weise möglich, bspw. die sicherheitstechnisch nächst höherliegende personenbezogene Kennung zu erfassen, um so die Authentifikation für den angeforderten Dienst durchführen zu können. Gegebenenfalls kann die Vergleichsoperation in diesem Fall einen geringeren Überdeckungsgrad erforderlich machen, da lediglich ein fehlgeschlagener

Vergleich einer sicherheitstechnisch niederwertigeren Authentifizierungsstufe behoben werden muss. In einer Weiterbildung ist es auch möglich, dass anstelle einer sicherheitstechnisch höherwertigen personenbezogenen Kennung, zumindest eine andere sicherheitstechnisch gleichwertige Kennung erfasst wird.

[0021] Mit dem erfindungsgemäßen Verfahren ist es in vorteilhafter Weise möglich, eine irrtümlich fehlgeschlagene Erfassung bzw. eine fehlerhafte Übereinstimmung dadurch zu beheben, dass eine personenbezogene Kennung, bspw. eine höhere sicherheitstechnische Klassifizierung, erfasst wird. Bei einem tatsächlichen Missbrauchsversuch wird nun auch dieser erneute Authentifizierungsversuch fehlschlagen, wodurch eine Weiterbildung von Vorteil ist, nach der bei eventuell mehrfach wiederholter fehlerhafter Übereinstimmung, ein Fehlerkennzeichensignal als ein Alarmsignal abgegeben wird. Dieses Alarmsignal kann beispielsweise eine Alarmausgabevorrichtung aktivieren, die mit dem Authentifikations-Kontrollsystem und/oder mit der Erfassungsvorrichtung kommunikativ verbunden ist, und somit gegebenenfalls vorhandenes Wachpersonal auf den Missbrauchsversuch aufmerksam machen. Es ist aber auch möglich, dass ein derartiges Alarmsignal an das Dienstbereitstellungs-System und/oder an ein Alarmkontrollsystem übermittelt wird, wobei das jeweilige System entsprechende Schritte einleitet, um den Missbrauchsversuch zu unterbinden bzw. um beispielsweise einen Sicherheitsdienst zu alarmieren. Diese Weiterbildung hat insbesondere den Vorteil, dass eine irrtümlich fehlerhafte Authentifizierung behoben werden kann, jedoch eine wiederholte, fehlerhafte Authentifizierung als Missbrauchsversuch erkennbar wird.

[0022] Mit der übermittelten Authentifizierungsanforderung kann gleichzeitig eine Sicherungskennzahl übermittelt werden, die direkt die Festlegung der Authentifizierungsstufe beeinflusst. Ein Manipulationsversuch zur Erreichung einer Authentifikation könnte beispielsweise darin bestehen, dass das Authentifikations-Kontrollsystem manipuliert wird und somit beispielsweise eine sicherheitstechnisch höherwertige Authentifizierungsstufe durch eine niederwertige Stufe ersetzt wird. Mit der anspruchsgemäßen Weiterbildung kann nun vom Dienstbereitstellungs-System ausgehend eine erforderliche Authentifizierungsstufe vorgegeben werden, um somit den Ermittlungsschritt durch das Authentifikations-Kontrollsystems zu umgehen. Insbesondere ist es somit auch möglich, nicht vorhersehbare Sicherheitsüberprüfungen durchzuführen, beispielsweise dadurch, dass zusammen mit einer sicherheitstechnisch niedrig priorisierten Authentifikationsanforderung eine Sicherungskennzahl einer sicherheitstechnisch hoch priorisierten Identifizierungsanforderung übermittelt wird, um stichprobenartig die Identität bzw. Authentizität der anfragenden Person auf einem sicherheitstechnisch hohen Niveau zu überprüfen. Beispielsweise kann auch eine missbräuchliche Verwendung eines sicherheitstechnisch niedrig priorisierten Dienstes über einen längeren Zeitraum hinweg bzw. bei oftmaliger Inanspruchnahme einen entsprechenden Schaden produzieren. Durch zufällig stattfindende Sicherheitsprüfungen lassen sich auch solche Manipulationsversuche erkennen. Insbesondere ist es mit dieser Weiterbildung möglich, für jede Authentifizierungsanforderung eine individuell angepasste Sicherungskennzahl und damit eine individuelle Authentifizierungsstufe festlegen zu können. Beispielsweise kann ein Zufallsgenerator diese Sicherungskennzahl derart beeinflussen, dass quasi nicht vorhersehbar eine Authentifizierungsanforderung übertragen wird und so eine Authentifizierungsstufe festlegt, die deutlich über der, für den angeforderten Dienst erforderlichen, liegt. Der Zufallsgenerator kann bspw. auch die Statistik der vergangenen Authentifikationsvorgänge berücksichtigen und bei einer Person mit einem erhöhten Aufkommen fehlerhafter Authentifikationsversuche, eine häufigere sicherheitstechnisch höherwertige Authentifikationsstufe verlangen.

[0023] Zur Authentifikation einer Person wird eine personenbezogene Kennung erfasst, die anschließend mit einem Referenzmerkmal zu vergleichen ist. Zur Erhöhung der Manipulationsicherheit kann das Authentifikations-Kontrollsystem derart ausgebildet sein, dass eine personenbezogene Kennung nur für die Dauer des Authentifizierungsvorgangs, insbesondere für die Dauer des Vergleichsvorgangs, in einem Speichermittel hinterlegt ist und anschließend sofort gelöscht wird. Nach der anspruchsgemäßen Weiterbildung wird mit der Authentifizierungsanforderung ein Referenzsatz eines personenbezogenen Merkmals übermittelt und steht somit für

den Vergleich zur Verfügung. Diese Ausbildung hat aber auch den weiteren Vorteil, dass das Authentifikations-Kontrollsystem erst dann eine personenbezogene Referenzkennung übermittelt bekommt, wenn sich die Person zum ersten Mal an diesem spezifischen Authentifikations-Kontrollsystem identifizieren möchte. Für ein verteiltes System, bei dem eine Mehrzahl von Authentifikations-Kontrollsystemen mit einem oder mehreren Dienstbereitstellungs-Systemen kommunikativ verbunden sind, hat dies den besonderen Vorteil, dass die Referenzmerkmale erst zum Zeitpunkt der durchzuführenden Authentifizierung übermittelt werden und somit die Gefahr wesentlich verringert wird, dass hinterlegte Referenzmerkmale gegebenenfalls ausspioniert werden könnten.

[0024] Wird zur Ermittlung der Authentifizierungsstufe die Authentifizierungsanforderung mit einem hinterlegten Sicherheits-Hierarchieprofil verglichen, ist dies insbesondere dahingehend von Vorteil, dass über das Hierarchieprofil die Authentifizierungsstufe ermittelt bzw. zugeordnet wird und somit auch eine individuell anpassbare Zuordnung möglich wird. Insbesondere kann somit das Sicherheits-Hierarchieprofil an das Authentifikations-Kontrollsystem angepasst werden und beispielsweise in einer Umgebung in der eine größere Gefahr einer Manipulation des Authentifikations-Kontrollsystems besteht, das Hierarchieprofil entsprechend angepasst werden, so dass grundsätzlich eine höhere Authentifizierungsstufe ermittelt wird. Diese Ausbildung hat den weiteren Vorteil, dass dieses Sicherheits-Hierarchiemodell individuell anpassbar ist und somit beispielsweise für jede Authentifizierungsanforderung ein individuelles Sicherheits-Hierarchieprofil angewendet werden kann. Insbesondere kann dieses Sicherheits-Hierarchieprofil beispielsweise von der Person selbst verwaltet werden und somit ein individualisierter Authentifizierungsvorgang geschaffen werden. Auch kann mittels dieses Sicherheits-Hierarchieprofils festgelegt werden, welcher Übereinstimmungsgrad beim Vergleich der erfassten personenbezogenen Kennung mit dem Referenzmerkmal erreicht werden muss. Ferner lässt sich festlegen wie im Fall einer negativen Übereinstimmung fortgefahren werden soll, insbesondere welche personenbezogene Kennung zur Behebung des fehlerhaften Vergleichs herangezogen werden kann.

[0025] Nach einer Weiterbildung stellt das Sicherheits-Hierarchieprofil eine Zuordnung zwischen dem Erfassungsmittel der Erfassungsvorrichtung und der Authentifizierungsstufe her. Mit der Authentifizierungsstufe wird prinzipiell festgelegt, welche sicherheitstechnische Anforderung an die durchzuführende Authentifikation gestellt wird, also welches Mindestmaß an Sicherheit im Hinblick auf eine eindeutige Identifikation bzw. Authentifikation einer Person die erfasste personenbezogene Kennung sicherstellen muss. Diese Weiterbildung hat ferner den Vorteil, dass individuell ausgebildete Authentifikations-Kontrollsysteme vorhanden sein können, die gegebenenfalls auch personenbezogene Kennungen unterschiedlich erfassen können, jedoch aufgrund der geforderten und insbesondere allgemeingültigen Authentifizierungsstufe eine entsprechend sichere Personenauthentifikation gewährleistet ist.

[0026] Im Hinblick auf eine Absicherung des Authentifikations-Kontrollsystems gegen unbefugte Manipulation ist eine Weiterbildung von Vorteil, nach der mit der Authentifizierungsanfrage eine Ablaufanweisung übermittelt wird. Durch diese Weiterbildung kann gewährleistet werden, dass eine Manipulation des Authentifikations-Kontrollsystems im Hinblick auf die Durchführung der Erfassung einer personenbezogenen Kennung erschwert bzw. verunmöglicht wird, da die Ablaufanweisung zur Durchführung der Erfassung der Kennung mit der Authentifizierungsanfrage übermittelt wird und somit gegebenenfalls bei jeder Authentifizierungsanfrage die Ablaufanweisung erneut übermittelt wird. Insbesondere kann das Authentifikations-Kontrollsystem derart ausgebildet sein, dass die vom Dienstbereitstellungs-System übermittelte Information nur für die Dauer des Authentifikationsprozesses temporär abgelegt wird und danach unwiederbringlich gelöscht wird. Somit kann ein Angreifer nicht auf eventuell sicherheitskritische Information zugreifen.

[0027] Von Vorteil ist ferner eine Weiterbildung nach der das Authentifikations-Kontrollsystem die Funktionalität der Erfassungsvorrichtung steuert, da somit wiederum eine weitere Steigerung der Manipulationssicherheit erreicht wird. Die Erfassungsvorrichtung mit dem Erfassungsmittel ist zumeist erster Angriffspunkt für einen Manipulationsversuch, da diese Vorrichtung als

letztes Glied der Kette zur Durchführung der Personenauthentifikation auch dem Zugriff durch nicht befugte Personen offen steht. Wird nun die Steuerung der Funktionalität der Erfassungsvorrichtung durch das Authentifikations-Kontrollsystem gesteuert, wird es potentiellen Angreifern wesentlich erschwert, die an die Erfassung der personenbezogenen Kennung anschließende Vergleichsoperation zu manipulieren. Auch ist es mit dieser Weiterbildung möglich, standardisierte und somit universell verwendbare Erfassungsvorrichtungen einzusetzen, da die konkrete Ablaufanweisung erst mit der Authentifizierungsanfrage übermittelt und anschließend vom Authentifikations-Kontrollsystem ausgeführt wird.

[0028] Gemäß einer Weiterbildung könnte als personenbezogene Kennung eine alphanumerische Kennung erfasst werden. Eine derartige alphanumerische Kennung kann beispielsweise eine Zahlenkombination sein, ein so genannter PIN - Code, der über ein standardisiertes und somit weit verbreitetes und kostengünstiges Eingabemittel eingegeben werden kann bspw. mittels einer alphanumerischen Tastatur. Aus dem Bereich der automatischen Geldausgabevorrichtungen ist bspw. eine Eingabevorrichtung bekannt, die mehrere Auswahl Tasten sowie einen Ziffernblock aufweist. Eine erweiterte Funktionalität und somit ein erhöhtes Maß an Sicherheit bietet beispielsweise eine Eingabevorrichtung, bei der neben Ziffern auch noch Buchstaben eingegbar sind, wodurch beispielsweise auch eine so genannte Passphrase eingegbar ist.

[0029] Eine personenbezogene Kennung, die aus dem Gedächtnis der Person abgerufen und über das Eingabemittel eingegeben wird, birgt insbesondere die Gefahr, dass ein potentieller Angreifer die Person bei der Eingabe beobachtet und somit die personenbezogene Kennung ausspioniert. Eine deutliche Steigerung der Authentifizierungssicherheit wird erreicht, wenn als personenbezogene Kennung ein biometrisches Merkmal erfasst wird, da biometrische Merkmale eindeutig einer Person zuordenbar sind und insbesondere nur äußerst schwierig manipuliert werden können. Auch ist bei der Erfassung die Gefahr einer unmittelbaren Manipulation wesentlich verringert, da zusammen mit dem biometrischen Merkmal beispielsweise auch Vitalzeichen erfasst werden können und somit eine außerordentlich hohe Authentifizierungssicherheit gegeben ist.

[0030] Eine weitere Möglichkeit eine Person sicher zu identifizieren bzw. zu authentifizieren besteht darin, dass als personenbezogene Kennung eine Abfolge von Handlungen erfasst wird, in der das Erfassungsmittel von der zu authentifizierenden Person bedient wird. Beispielsweise kann eine Bedienerhandlung darin bestehen, eine alphanumerische Kennung in einer bestimmten festgelegten Abfolge der einzelnen Typen einzugeben. Eine weitere Bedienhandlung könnte beispielsweise darin bestehen, dass bewusst ein oder mehrere Typ-Eingabefehler vorkommen, die durch Bedienen einer Löscho- bzw. Korrekturfunktion behoben werden. Wird beispielsweise eine Person bedroht und zur Eingabe der personenbezogenen Kennung gezwungen, kann diese Person bewusst an festgelegten Stellen der Kennung einen oder keinen Fehler machen, wobei diese bewusste Fehlbedienung als eindeutige personenbezogene Kennung registriert wird, jedoch nicht nur eine Authentifikation einer Person durchführt, sondern beispielsweise auch eine Alarmaktion auslöst, da die Person durch dieses bewusste Fehlverhalten diese Aktion ausgelöst hat. Ebenso kann eine bewusste Fehlbedienung des Erfassungsmittels als personenbezogene Kennung erfasst und interpretiert werden, beispielsweise indem eine Bestätigungsfunktion vor der vollständigen Eingabe der alphanumerischen Kennung ausgelöst wird. In jedem Fall kann mit der anspruchsgemäßen Weiterbildung eine Person Aktionen auslösen, ohne dass dadurch ein potentieller Angreifer diese scheinbar zufällige Fehlbedienung als personenbezogene Kennung interpretieren würde.

[0031] In eine ähnliche Richtung zielt eine Weiterbildung, nach der bei der Erfassung der personenbezogenen Kennung ein zeitlicher Ablauf der Bedienhandlungen erfasst wird. Wiederum am Beispiel der Erfassung einer alphanumerischen Kennung beschrieben, kann eine Person die einzelnen Typen in einer bestimmten, zeitlichen Abfolge eingeben. Beispielsweise kann an einer bestimmten Stelle eine längere Pause zwischen der Eingabe vorgesehen sein bzw. kann vorgesehen sein, dass die Kennung innerhalb einer bestimmten maximalen Zeitspanne angegeben werden muss. Im Bedrohungsfall kann die Person den festgelegten Zeitablauf bewusst nicht einhalten, um so eine scheinbar erfolgreiche Authentifizierung durchzuführen jedoch im

Hintergrund eine entsprechende Alarmaktion auszulösen. Auch wird ein Angreifer, der eine personenbezogene Kennung ausspioniert hat zumeist nicht die dahinter liegenden Zeitabläufe erkennen und somit würde ein Manipulationsversuch scheitern.

[0032] Insbesondere kann somit mit einer personenbezogenen Kennung, in Kombination mit einer Mehrzahl unterschiedlicher Bedienhandlungen und/oder unterschiedlicher Zeitabläufe eine Vielzahl möglicher Authentifizierungsvorgänge durchgeführt bzw. initiiert werden. Beispielsweise ist es möglich, dass durch Eingabe einer alphanumerischen Kennung in Kombination mit einer entsprechenden Bedienhandlung, vom Authentifikations-Kontrollsystem ein automatischer Rückruf auf eine mobile Kommunikationseinrichtung initiiert werden, der von der zu authentifizierenden Person in einer wohl definierten Art beantwortet werden muss. Erfolgt die Beantwortung der Rückfrage nicht in der festgelegten Art und Weise, beispielsweise dadurch, dass die Person den Rückruf nicht entgegennimmt, kann beispielsweise die Authentifikation scheinbar erfolgreich durchgeführt werden, jedoch wird im Hintergrund eine entsprechende Alarmaktion ausgelöst. Mittels einer Positionsbestimmung durch die mobile Kommunikationseinrichtung kann dies zu einer Lokalisation der betreffenden Person durch die Authentifizierungseinrichtung führen, sodass der Person gezielt zur Hilfe gekommen werden kann. Gegebenenfalls kann ferner vorgesehen sein, dass die Erfassungsvorrichtung auch eine Nahbereichs-Kommunikationseinrichtung aufweist, sodass sich zur erfolgreichen Authentifikation der Benutzer mit der mobilen Kommunikationseinrichtung, welche eine entsprechende Kommunikationsgegenstelle aufweist, innerhalb einer gut festlegbaren und insbesondere geringen Distanz befinden muss.

[0033] Die bisher beschriebenen personenbezogenen Kennungen basierten allesamt auf einer bewussten Handlung der zu authentifizierenden Person. Daneben besteht ferner noch die Möglichkeit, ein unbewusstes Verhalten einer Person als personenbezogene Kennung zu erfassen, indem die Erfassungsvorrichtung mittels einer Ein- Ausgabevorrichtung eine personalisierte Anfrage ausgibt und die Reaktion der Person darauf erfasst. Derartige Reaktionen sind kaum zu manipulieren, da diese auf einem unbewussten Reaktionsmodell der Person basieren, welches von einem potentiellen Angreifer nicht ausspioniert werden kann, da dadurch das Reaktionsmodell zumeist bereits verfälscht werden würde. Beispielsweise kann die Erfassungsvorrichtung eine Eingabeaufforderung ausgeben und mehrere Auswahlmöglichkeiten anbieten. Unabhängig von der aktuell präsentierten Eingabeaufforderung wird die Person intuitiv auf eine spezifische Klasse von Eingabeaufforderungen stets gleich reagieren, was sicherheitstechnisch gesehen einen hohen Authentifizierungsgrad darstellt. Die präsentierte Eingabeaufforderung wird bevorzugt aus einem Vorrat einer Mehrzahl möglicher unterschiedlicher Eingabeaufforderungen ausgewählt.

[0034] Eine deutliche Steigerung der Authentifizierungssicherheit erhält man, wenn das Sicherheits-Hierarchiemodell von einem Authentifizierungssystem an das Authentifikations-Kontrollsystem übertragen wird, da somit eine Trennung der Authentifikation von der Bereitstellung eines in Anspruch zu nehmenden Dienstes erreicht wird. Insbesondere ist von Vorteil, dass das Authentifizierungssystem beispielsweise innerhalb eines hochsicheren Bereichs angeordnet werden kann, während für ein Dienstbereitstellungs-System zumeist geringere Sicherheitsanforderungen erforderlich sind. Insbesondere wird somit verhindert, dass durch Manipulation eines Dienstbereitstellungs-System ein Zugriff auf das Authentifikations-Kontrollsystem erreicht werden kann, um darüber in missbräuchlicher Absicht einen weiteren Zugriff auf ein anderes, beispielsweise sicherheitstechnisch höherwertiges Dienstbereitstellungssystem zu erlangen.

[0035] Im Hinblick auf eine möglichst individuelle Anpassung des erfindungsgemäßen Verfahrens an die individuellen personenbezogenen Kennungen sowie an die individuellen Verhaltensweisen ist eine Weiterbildung von Vorteil, nach der das Sicherheits-Hierarchieprofil in einer Trainingsphase erstellt wird, wobei personenbezogene Kennungen als Referenzmerkmale erfasst und in einem Speichermittel hinterlegt werden. Bevorzugt wird dieses Speichermittel im Authentifizierungssystem angeordnet sein, wobei auch eine Anordnung im Dienstbereitstellungs-System möglich ist. Die Erfassung personenbezogener Kennungen in einer Trainingsphase hat den weiteren Vorteil, dass die dafür verwendete Erfassungsvorrichtung in einer si-

cherheitstechnisch besonders geschützten Umgebung angeordnet sein kann bzw. das ferner ein entsprechendes rechtliches Umfeld geschaffen werden kann, um die erfassten Kennungen auch rechtlich verbindlich ausbilden zu können. Insbesondere ist es in der Trainingsphase von Bedeutung, dass die Identität der Person eindeutig festgestellt wird und sich somit die erfassten Kennungen eindeutig dieser Person zuordnen lassen. Beispielsweise kann diese Authentifizierung durch ein Ausweisdokument erfolgen, welches einer juristischen Autorität wie bspw. einem Notar vorgelegt wird, der das Dokument mittels einer Kontrollvorrichtung, bspw. einem Passportreader, auf Gültigkeit prüft und anschließend personenbezogene Kennungen erfasst und diese rechtsverbindlich in einem Speichermittel hinterlegt. Die so erfassten Referenzmerkmale können nun bei der Produktion des Authentifikations-Kontrollsystems in diesem hinterlegt werden, es ist aber auch möglich diese in einem externen Speichermodul zu hinterlegen, welches zusammen mit dem Authentifikations-Kontrollsystem integriert angeordnet wird. Auch können die Referenzmerkmale über eine Kommunikationsverbindung an das Authentifikations-Kontrollsystem übermittelt werden.

[0036] Für die Erweiterung der Möglichkeiten zur Personenauthentifizierung bzw. zur Erhöhung der Sicherheit einer derartigen Authentifikation ist es von Vorteil, wenn ein bewusstes Verhaltensmuster als personenbezogenes Referenzmerkmal erfasst wird, in dem eine spezifische Abfolge von Bedienhandlungen an der Erfassungsvorrichtung erfasst wird. Für eine alphanumerische Kennung besteht beispielsweise die Möglichkeit, die Kennung in der festgelegten Reihenfolge anzugeben, jedoch ist es auch möglich, die Kennung in umgekehrter oder unterschiedlicher Weise einzugeben und beispielsweise durch eine bewusste Fehleingabe angeben zu können, um somit ein spezifisches Verhalten auslösen zu können. Insbesondere kann durch Kombination einer sicherheitstechnisch schwachen personenbezogenen Kennung mit einem bewussten Verhaltensmuster als personenbezogene Kennung eine wesentliche Steigerung der Authentifizierungssicherheit erreicht werden. Insbesondere sind somit auch bedingte Funktionen des Authentifikations-Kontrollsystems festlegbar, um bei einem Missbrauchsversuch Sicherheitsmaßnahmen auslösen zu können.

[0037] Ebenso kann ein unbewusstes Verhaltensmuster als personenbezogenes Referenzmerkmal erfasst werden, in dem die Person mittels einer Ein- und Ausgabevorrichtung eine Mehrzahl von Auswahlmöglichkeiten dargestellt bekommt und die jeweils getroffene Auswahl erfasst wird. Die Auswahlmöglichkeiten werden dabei bevorzugt aus einem Vorrat einfacher situationsbedingter Merkmalsbeschreibungen ausgewählt und dem Benutzer beispielsweise auf einer Anzeigevorrichtung präsentiert und die Reaktion mittels einer Tastatur bzw. eines Eingabemittels erfasst. Die Auswahlmöglichkeit ist derart ausgebildet, dass eine eindeutige und unzweifelhafte Auswahl sichergestellt ist.

[0038] Insbesondere ist es von Vorteil, wenn aus den erfassten Auswahlsergebnissen ein Reaktionsprofil erstellt wird, da sich aufgrund dieses Reaktionsprofils die Reaktion des Benutzers auf eine Auswahlmöglichkeit feststellen lässt, wenn diese Auswahlmöglichkeit dem Benutzer bei der späteren Authentifizierung zur Inanspruchnahme eines Dienstes präsentiert wird. Insbesondere lässt sich ein derartiges unbewusstes Verhaltensmuster im Wesentlichen nicht manipulieren, sodass bei der Erfassung eines unbewussten Verhaltensmusters als personenbezogene Kennung eine besonders hohe Sicherheitsstufe erzielen lässt. Auch ist eine derartige Weiterbildung dahingehend von besonderem Vorteil, dass ein potentieller Angreifer ein derartiges Reaktionsprofil durch Ausspionieren im Wesentlichen nicht erfassen kann.

[0039] Nach einer Weiterbildung sind Referenzmerkmale in der Speichereinheit des Authentifikations-Kontrollsystems hinterlegt, was den Vorteil hat, dass dieses ohne Verbindung zu einem zentralen Authentifikationssystem betreibbar ist und damit völlig autark eine eindeutige und zuverlässige Personenauthentifikation durchführen kann. Diese Weiterbildung ist insbesondere dann von Vorteil, wenn beispielsweise eine zuverlässige Personenauthentifikation für ein so genanntes Einzelplatzsystem gefordert ist, bei dem sich das Dienstbereitstellungs-System und das Personenauthentifikationssystem an einem Ort befinden und keine kommunikative Verbindung mit einem abgesetzten System erforderlich ist. Mit dieser Weiterbildung sind insbesondere so genannte „stand alone“ - Systeme ausbildbar, die beispielsweise durch entsprechende me-

chanische Sicherungs- bzw. Schutzmaßnahmen einen ausreichenden Zugriffsschutz bieten und aufgrund der hohen Manipulationssicherheit ein hohes Maß an Authentifikationssicherheit bieten.

[0040] Von Vorteil ist ferner eine Weiterbildung, nach der nach Ablauf eines Zeitgebers am Dienstbereitstellungs-System oder am Authentifikations-Kontrollsystem, eine Authentifizierungsanforderung generiert wird, da somit gezielt eine erneute Authentifikation ausgelöst werden kann. Nach einer erfolgreichen Authentifikation kann ein Benutzer den bereit gestellten Dienst in Anspruch nehmen, insbesondere bis zur Abmeldung vom Dienstbereitstellungs-System bzw. vom Authentifikations-Kontrollsystem. Mit zunehmender Benutzungsdauer steigt jedoch die Gefahr einer Manipulation durch unbefugte Dritte. Insbesondere fällt der Grad der zuverlässigen Authentizität des angemeldeten Benutzers, aufgetragen über der Benutzungsdauer, stark ab, meist sogar nichtlinear. Mit der Weiterbildung kann nun sichergestellt werden, dass in regelmäßigen bzw. wahlfrei vorgebbaren Zeitintervallen, vom Benutzer eine erneute Authentifikation verlangt wird, sodass ein Zustand verhindert wird, in dem ein Benutzer lange Zeit am Dienstbereitstellungs-System angemeldet ist. Die anspruchsgemäße Authentifizierungsanforderung kann nun vom Dienstbereitstellungs-System übermittelt werden und entspricht damit einer Anforderung, wie sie zur initialen Authentifikation nach den erfindungsgemäßen Verfahrensschritten einlangt. Ferner kann die Authentifizierungsanforderung aber auch vom Authentifikations-Kontrollsystem selbst herkommen, wobei jedoch die Verarbeitung der Anfrage gleich erfolgt, als wenn diese vom Dienstbereitstellungs-System eingelangt wäre. Beispielsweise hat eine erneute Authentifizierungsanforderung durch das Authentifikations-Kontrollsystem den Vorteil, dass dieses System auf das lokal herrschende Sicherheitsumfeld Rücksicht nehmen kann und bspw. in einer unsicheren Umgebung, nur einen kurzen Gültigkeitszeitraum der Authentifikation erlaubt, ohne dass dies am Dienstbereitstellungs-System spezifisch hinterlegt sein müsste.

[0041] Des Weiteren kann nach einer Weiterbildung als personenbezogene Kennung auch ein Abbild der Person erfasst werden. Damit ist bspw. ein optisch visueller Vergleich möglich, insbesondere können mittels bekannter Bildanalyseverfahren aus dem erfassten Abbild eindeutige bzw. charakteristische Merkmale ermittelt werden. Abbilder die nach einem international anerkannten Standard erfasst wurde, beispielsweise nach dem der ICAO (International Civil Aviation Organization), lassen sich eindeutig analytisch aufbereiten und somit mit einem hohen Zuverlässigkeitsfaktor mit einem Referenzmerkmal vergleichen.

[0042] Einen weiteren Faktor zur Steigerung der Authentifikationssicherheit erhält man, wenn das erfasste Abbild an eine mobile Kommunikationsvorrichtung übermittelt wird. Beispielsweise kann individuell für jeden Benutzer ein Personenkreis definiert werden, dessen Mitglieder bereit sind, eine optisch visuelle Authentifikation einer Person durchzuführen und die Authentizität derselben zu bestätigen. Automatisierte Authentifikationssysteme führen die Authentifikation einer Person nach streng festgelegten Regeln durch, eine individuelle Bewertung des Umfelds bzw. der Situation unterbleibt. Mit dieser Weiterbildung wird nun ein menschlicher Bewertungsfaktor eingeführt, insbesondere wird somit eine Bewertung der Situation möglich, in der die Authentifikationsanfrage erfolgt. Beispielsweise kann eine Person zur Authentifikation gezwungen werden und würde so möglicherweise eine korrekte personenbezogene Kennung eingeben. Mit der anspruchsgemäßen Weiterbildung wird das Abbild mittels eines Datendienstes wie bspw. MMS an eine mobile Kommunikationsvorrichtung übermittelt, woraufhin der Empfänger erkennen kann, dass die Person bedroht wird und somit nachfolgend Maßnahmen zum Schutz der bedrohten Person auslösen kann. Durch die Einbeziehung eines Personen-Netzwerks wird eine deutliche Steigerung der Authentifikationssicherheit erreicht, da jede Person dieses Netzwerks, als authentifizierende - als auch als zu authentifizierende Instanz, eine hohe Sicherheit anstrebt und somit ein besonderes Augenmerk auf eine zuverlässige Durchführung Authentifikation legen wird. Beispielsweise kann eine derartige Authentifikationsmethode über ein Bonus-system abgewickelt bzw. vergewährt werden.

[0043] Zum besseren Verständnis der Erfindung wird diese anhand der nachfolgenden Figuren näher erläutert.

[0044] Es zeigen jeweils in stark schematisch vereinfachter Darstellung:

[0045] Fig. 1 das erfindungsgemäße Verfahren anhand einer beispielhaften Vorrichtung;

[0046] Fig. 2 ein Ablaufdiagramm des erfindungsgemäßen Verfahrens;

[0047] Fig. 3 ein weiteres mögliches System zur Durchführung des erfindungsgemäßen Verfahrens.

[0048] Einführend sei festgehalten, dass in den unterschiedlich beschriebenen Ausführungsformen gleiche Teile mit gleichen Bezugszeichen bzw. gleichen Bauteilbezeichnungen versehen werden, wobei die in der gesamten Beschreibung enthaltenen Offenbarungen sinngemäß auf gleiche Teile mit gleichen Bezugszeichen bzw. gleichen Bauteilbezeichnungen übertragen werden können. Auch sind die in der Beschreibung gewählten Lageangaben, wie z.B. oben, unten, seitlich usw. auf die unmittelbar beschriebene sowie dargestellte Figur bezogen und sind bei einer Lageänderung sinngemäß auf die neue Lage zu übertragen. Weiters können auch Einzelmerkmale oder Merkmalskombinationen aus den gezeigten und beschriebenen unterschiedlichen Ausführungsbeispielen für sich eigenständige, erfinderische oder erfindungsgemäße Lösungen darstellen.

[0049] Sämtliche Angaben zu Wertebereichen in gegenständlicher Beschreibung sind so zu verstehen, dass diese beliebige und alle Teilbereiche daraus mit umfassen, z.B. ist die Angabe 1 bis 10 so zu verstehen, dass sämtliche Teilbereiche, ausgehend von der unteren Grenze 1 und der oberen Grenze 10 mitumfasst sind, d.h. sämtliche Teilbereiche beginnen mit einer unteren Grenze von 1 oder größer und enden bei einer oberen Grenze von 10 oder weniger, z.B. 1 bis 1,7, oder 3,2 bis 8,1 oder 5,5 bis 10.

[0050] Fig. 1 zeigt die erfindungsgemäßen Verfahrensschritte anhand einer beispielhaften Vorrichtung zur Durchführung des Verfahrens. Diese Vorrichtung umfasst zumindest ein Authentifikations-Kontrollsystem 1, welches kommunikativ mit einer Erfassungsvorrichtung 2 verbunden ist und wobei die Erfassungsvorrichtung 2 mehrere Erfassungsmittel 3 aufweist. Das Authentifikations-Kontrollsystem 1 ist über ein Kommunikationsnetzwerk 4 mit zumindest einem Dienstbereitstellungs-System 5 verbunden, gegebenenfalls ist ein Authentifizierungssystem 6 vorhanden, welches mit dem Authentifikations-Kontrollsystem 1 und/oder dem Dienstbereitstellungs-System 5 kommunikativ verbunden ist.

[0051] Das erfindungsgemäße Verfahren wird insbesondere dazu verwendet, für eine angeforderte Dienstleistung eines Dienstanbieters zu gewährleisten, dass der Benutzer der die Dienstleistung angefordert hat, eindeutig und unverwechselbar authentifiziert und identifiziert wird. Des Weiteren ist mit dem erfindungsgemäßen Verfahren eine individuell vorgebbare Authentifikation einer Person im Hinblick auf die Erfassungssicherheit möglich. Insbesondere ist dies von Bedeutung, da die Dienstleistung beispielsweise eine Finanztransaktion sein kann, oder auch rechtlich verbindliche Vorgänge umfasst. Der Benutzer wird also beim Dienstleistungsanbieter einen entsprechenden Vorgang auslösen, wobei diese Dienstanforderung nicht Gegenstand der Erfindung ist und daher hier nicht weiter ausgeführt wird. Beispielhaft könnte eine derartige Dienstanforderung dadurch ausgelöst werden, dass ein Benutzer auf einer Anforderungsvorrichtung die beispielsweise Teil oder Zusatz der Erfassungsvorrichtung 2 sein kann, eine Bedienerhandlung vornimmt, die an ein Dienstbereitstellungs-System 5 übermittelt wird und an diesem die entsprechenden Vorgänge auslöst. Im Hinblick auf die Zuverlässigkeit der Authentifikation einer Person sollte in einer ersten Überlegung immer mit der höchstmöglichen Sicherheitsstufe gearbeitet werden. Da personenbezogene Merkmale zur Erreichung dieser Sicherheitsstufe aufwändig und unter Umständen schwierig zu erfassen sind, ist es von ganz besonderem Vorteil, wenn die zu erfassenden Merkmale auf die erforderliche Sicherheitsstufe des angefragten Dienstes abgestimmt sind und somit für sicherheitstechnisch unkritische Dienste, auch schwächere personenbezogene Kennungen erfasst werden. Das erfindungsgemäße Verfahren bietet nun die Möglichkeit, integriert unterschiedliche Authentifizierungsstufen und eine Mängelbehebung im Fall einer fehlerhaften Vergleichsprüfung bereitstellen zu können.

[0052] In einem ersten Schritt des erfindungsgemäßen Verfahrens wird von einem Dienstbe-

reitstellungs-System 5 eine Authentifizierungsanforderung 7 an das Authentifikations-Kontrollsystem 1 übertragen. Durch Analyse der übertragenen Authentifizierungsanforderung 7 ermittelt das Authentifikations-Kontrollsystem 1 eine erforderliche Authentifizierungsstufe 9. Diese Authentifizierungsstufe legt fest, welches Niveau an Erfassungssicherheit die zu erfassende personenbezogene Kennung aufweisen muss, um den angeforderten Dienst in Anspruch nehmen zu dürfen. Insbesondere legt die Authentifizierungsstufe 9 somit fest, welches Erfassungsmittel 3 der Erfassungsvorrichtung 2 im nächsten erfindungsgemäßen Verfahrensschritt aktiviert werden muss, um eine personenbezogene Kennung zu erfassen. Für einen Dienst mit einer geringen sicherheitstechnischen Relevanz kann eine personenbezogene Kennung beispielsweise als alphanumerische Kennung erfasst werden, die über ein alphanumerisches Eingabemittel 10 beispielsweise eine Tastatur, eingegeben wird. Für sicherheitstechnisch höherwertige Dienste können biometrische Merkmale erfasst werden, beispielsweise kann mittels einer optischen Bilderfassungsvorrichtung 11 ein Abbild des Gesichts der Person oder ein Abbild der Iris erfasst werden, mit einem so genannten Fingerabdruckscanner 12 können ferner die Fingerminutien erfasst werden. Die Erfassungsvorrichtung 2 kann auch eine audiovisuelle Ein- /Ausgabevorrichtung 13 aufweisen, um beispielsweise ein unbewusstes und/oder ein bewußtes Benutzerverhalten als personenbezogene Kennung erfassen zu können.

[0053] Die erfasste benutzerbezogene Kennung wird mit einem oder mehreren korrespondierenden Referenzmerkmalen verglichen, wobei dieses korrespondierende Referenzmerkmal 14 in einem Speichermittel 15 des Authentifikations-Kontrollsystems 1 angeordnet sein kann. Das Referenzmerkmal 14 kann jedoch auch in einem Speichermittel 16 des Authentifizierungssystems 6 angeordnet sein, wobei diese Ausbildung den Vorteil hat, dass das Authentifizierungssystem 6 besonders gesichert bzw. besonders geschützt ausgebildet sein kann und somit eine sehr hohe Manipulationssicherheit bietet. Die Anordnung der Referenzmerkmale 14 im Speichermittel 15 des Authentifikations-Kontrollsystems 1 hat den Vorteil, dass das Authentifikations-Kontrollsystem den Vergleich der erfassten Kennung mit dem Referenzmerkmal selbst durchführen kann und somit die Authentifizierung bzw. Identifikation einer Person ohne zusätzliche Systeme möglich ist.

[0054] Der Vergleich der erfassten Kennung mit dem korrespondierenden Referenzmerkmal wird zumeist erfolgreich sein, wobei in diesem Fall vom Authentifikations-Kontrollsystem 1 ein Freigabesignal 17 an das Dienstbereitstellungs-System 5 abgegeben 18 wird.

[0055] Der wesentliche Unterschied des erfindungsgemäßen Verfahrens gegenüber bekannten Verfahren liegt nun auch in den weiteren Schritten die durchgeführt werden, wenn der Vergleich der erfassten Kennung mit dem korrespondierenden Referenzmerkmal fehlschlägt. Bei bekannten Verfahren würde in diesem Fall die Authentifizierung abgebrochen und dem Benutzer der Zugriff auf das Dienstbereitstellungs-System 5 verweigert. Um sich erneut authentifizieren zu können müsste der Benutzer daher eine erneute Dienstanforderungsanfrage 7 auslösen. Dem gegenüber hat das erfindungsgemäße Verfahren den besonderen Vorteil, dass im Fall eines fehlerhaften Vergleichs automatisch ein weiteres Erfassungsmittel 3 der Erfassungsvorrichtung 2 aktiviert wird, um die entsprechenden erfindungsgemäßen Verfahrensschritte zu wiederholen und insbesondere eine weitere personenbezogene Kennung zu erfassen.

[0056] Da aus der übermittelten Authentifizierungsanforderung 7 eine Authentifizierungsstufe 9 ermittelt wurde, ist damit auch die erforderliche Zuverlässigkeit der erfassten personenbezogenen Kennung festgelegt. Aufgrund statistisch unabhängiger Vorkommnisse kann es vorkommen, dass der Vergleich fehlschlägt, obwohl es sich um keinen Manipulationsversuch handelt. Durch das erfindungsgemäße Verfahren ist nun beispielsweise vorgesehen, dass eine personenbezogene Kennung mit einem Merkmal oder mehreren weiteren Merkmalen, oder mit einer nächst höheren Sicherheitsstufe erfasst wird, um damit den fehlgeschlagenen Vergleich zu beheben. Beispielsweise kann es bei der Eingabe einer alphanumerischen Kennung zu einer unbeabsichtigten Fehleingabe kommen, wodurch der darauf folgende Vergleich fehlschlagen wird. In einer Weiterbildung könnte der Benutzer dazu aufgefordert werden, die Kennung erneut einzugeben. Erfindungsgemäß kann jedoch insbesondere vorgesehen sein, dass vom Authentifikations-Kontrollsystem 1 ein weiteres Erfassungsmittel 3 der Erfassungsvorrichtung 2 aktiviert

wird und anschließend die entsprechenden Verfahrensschritte erneut durchgeführt werden.

[0057] Insbesondere kann somit durch Erfassung einer höherwertigen personenbezogenen Kennung, also einer Kennung mit einer höheren Authentifizierungsstufe 9, ein fehlerhafter Vergleich einer niederwertigeren erfassten personenbezogenen Kennung behoben werden, wobei es von besonderem Vorteil ist, wenn die Übereinstimmungskriterien des Vergleichs individuell anpassbar sind, sodass eine höherwertige personenbezogene Kennung zur Behebung eines mangelhaften Vergleichs einer niederwertigeren personenbezogenen Kennung einen geringeren Übereinstimmungsgrad aufweisen muss, als dies für eine, der höheren Authentifizierungsstufe entsprechende Vergleichsoperation erforderlich wäre. Es können auch mehrere niederwertige Kennungen zusammen eine höherwertige Kennung ersetzen, wenn sie in ihrer Summe sicherheitsmässig betrachtet mit dieser gleichwertig sind, was vorgängig festgelegt werden kann. Das erfindungsgemäße Verfahren kann nun insbesondere sooft wiederholt eine personenbezogene Kennung erfassen, als sicherheitstechnisch höhere Authentifizierungsstufen verfügbar sind. Schlägt der Vergleich einer personenbezogenen Kennung mit einem hinterlegten Referenzmerkmal wiederholt fehl, wird vom Authentifikations-Kontrollsystem 1 ein Fehlerkennzeichnungssignal als Alarmsignal abgegeben. Dieses Alarmsignal kann beispielsweise an das Dienstbereitstellungs-System 5 übermittelt werden, es ist jedoch auch eine Übermittlung an das Authentifizierungssystem 6 bzw. ein gegebenenfalls vorhandenes Alarmkontrollsystem möglich. Dieses Alarmsignal kann nun derart ausgewertet werden, dass die aktuell laufende Personenauthentifikation abgebrochen wird und beispielsweise an eine Sicherheits-Kontrolleinrichtung eine Alarmierung erfolgt, die entsprechende Sicherungsmaßnahmen auslöst, beispielsweise kann ein entsprechendes Sicherheitspersonal alarmiert werden. Das Alarmsignal kann jedoch auch derart ausgewertet werden, dass die Authentifizierungsanfrage scheinbar erfolgreich war und somit ein potentieller Angreifer dahingehend in die Irre geführt wird, dass dieser der Meinung ist, der Manipulationsversuch war erfolgreich, während im Hintergrund bereits entsprechende Alarm- bzw. Sicherungsmaßnahmen getroffen werden.

[0058] Fig. 2 zeigt eine vereinfachte Darstellung des Ablaufs des erfindungsgemäßen Verfahrens. Von einem Dienstbereitstellungs-System 5 wird eine Authentifizierungsanforderung 7 an das Authentifikations-Kontrollsystem 1 übermittelt. Diese Authentifizierungsanforderung 7 umfasst beispielsweise eine Kennung des anfordernden Dienstbereitstellungs-Systems 5 und weißt insbesondere eine Kennung auf, die es ermöglicht, die entsprechende Authentifizierungsstufe 9 zu ermitteln. Im Verfahrensschritt der Ermittlung der Authentifizierungsstufe 19 wird die Authentifizierungsanforderung 7 dahingehend analysiert bzw. aufbereitet, dass beispielsweise durch Vergleich mit einem hinterlegten Sicherheits-Hierarchieprofil 20 die entsprechende Authentifizierungsstufe 9 ermittelt wird. Für eine möglichst universelle Einsetzbarkeit des erfindungsgemäßen Verfahrens wird die Authentifizierungsanforderung 7 bevorzugt unspezifisch ausgebildet sein und somit beispielsweise nur eine generische Dienstbeschreibung bzw. Sicherheitsanforderung übermitteln. Die konkrete Umsetzung der erforderlichen Sicherheitsstufe der Authentifizierungsanforderung 7 geschieht bevorzugt durch das Authentifikations-Kontrollsystem 1 insbesondere wird dadurch die Beziehung hergestellt, welche personenbezogene Kennung von der Erfassungsvorrichtung 2 erfasst werden muss, um die durch das Sicherheits-Hierarchieprofil 20 festgelegte Authentifizierungsstufe 9 zumindest erreichen zu können.

[0059] Nachdem die Authentifizierungsstufe 9 ermittelt wurde 19, wird im nächsten Verfahrensschritt 21 ein Erfassungsmittel 3 der Erfassungsvorrichtung 2 aktiviert, wobei durch die Authentifizierungsstufe festgelegt ist, welches Erfassungsmittel aktiviert werden muss, um ein personenbezogenes Merkmal der entsprechenden Sicherheitsstufe bzw. Zuverlässigkeit erfassen zu können. Hier zeigt sich bereits einer der wesentlichen Vorteile des erfindungsgemäßen Verfahrens, als das mit einer Vorrichtung die zur Durchführung des erfindungsgemäßen Verfahrens ausgebildet ist, personenbezogene Kennungen derart erfasst werden können, dass eine unterschiedlich hohe Sicherheitsstufe erreichbar wird.

[0060] Das aktivierte Erfassungsmittel 3 der Erfassungsvorrichtung 2 erfasst in einem weiteren Verfahrensschritt 22 eine personenbezogene Kennung, die in einem anschließenden Ver-

gleichsschritt 23 mit einem hinterlegten, korrespondierenden Referenzmerkmal 24 verglichen wird. Das Referenzmerkmal 24, insbesondere jedoch eine Mehrzahl von Referenzmerkmalen, ist in einem Speichermittel abgelegt, welcher bevorzugt beim Authentifikations-Kontrollsystem 1 angeordnet ist. Der Speicher mit den Referenzmerkmalen kann jedoch auch bei einem externen Authentifizierungssystem angeordnet sein. Dieses Referenzmerkmal 24 stellt einen Schlüssel dar, um bspw. auf ein Dienstbereitstellungs-System zugreifen zu können. Daher ist es von besonderer Bedeutung, dass der Zugriff auf diese Referenzmerkmale derart gesichert ist, dass eine Manipulation weitestgehend verhindert wird und somit die Authentizität der Referenzmerkmale zuverlässig gegeben ist, was insbesondere für den Vergleich 23 ganz wesentlich ist.

[0061] War der Vergleich 23 der erfassten personenbezogenen Kennung mit dem hinterlegten Referenzmerkmal erfolgreich, wird ein so genanntes Freigabesignal 17 an das anfordernde Dienstbereitstellungs-System übermittelt, worauf dieses aufgrund der festgestellten Identität und Authentizität der Person, den gewünschten Dienst bereitstellen kann. Schlägt der Vergleich fehl, stimmt also die personenbezogene Kennung nicht mit dem Referenzmerkmal überein 25, ist es gegenüber bekannten Verfahren mit dem erfindungsgemäßen Verfahren nun möglich, einen erneuten Authentifikationsdurchlauf zu initiieren. Dazu wird in einer Vergleichsoperation 26 festgestellt, ob die ermittelte Authentifizierung einen erneuten Durchlauf der Authentifikations-schritte zulässt. Wurde beispielsweise eine sicherheitstechnisch hohe Authentifizierungsstufe ermittelt, kann ein fehlerhafter Vergleich beispielsweise nicht durch eine sicherheitstechnisch höherwertige Authentifizierungsstufe behoben werden. In diesem Fall kann vorgesehen sein, die personenbezogene Kennung erneut zu erfassen und auch den Vergleich erneut durchzuführen, oder mehrere, sicherheitstechnisch weniger hochwertige Kennungen zu summieren. Kommt es wiederum zu einem fehlerhaften Vergleich kann vorgesehen sein, dass ein Fehler-signal 27 abgegeben wird und die Authentifizierung der Person somit fehlgeschlagen ist.

[0062] Zusammen mit der Authentifizierungsanforderung 7 kann eine Sicherungskennzahl übermittelt werden, die direkt in die Authentifizierungskennzahl 9 einfließt. Ferner kann die Authentifizierungskennzahl durch eine Zuordnungstabelle ermittelt werden, in dem eine Zuordnung zwischen einem Dienstbereitstellungs-System bzw. einer Klasse von Dienstbereitstellungs-Systemen und einer entsprechenden Authentifizierungsstufe hergestellt wird. Mit dem Sicherheits-Hierarchieprofil 20 ist jedoch noch eine wesentlich feinere Abstufung der Authentifizierungsstufe und des dadurch festgelegten Verfahrensablaufs möglich. Für eine Authentifizierungsstufe, beispielsweise A bis E, können nun mehrere Optionen festgelegt werden, die einerseits die Anforderungen bei der Erfassung der personenbezogenen Kennung und andererseits das Verhalten des erfindungsgemäßen Verfahrens bei einem fehlgeschlagenen Vergleich der erfassten Kennung mit dem hinterlegten Referenzmerkmal festlegen. Beispielsweise kann dadurch festgelegt sein, welche Erfassungsmittel der Erfassungsvorrichtung zur Erreichung einer spezifischen Authentifizierungsstufe erforderlich sind. Somit kann beispielsweise eine personenbezogene Kennung mit einem spezifischen Erfassungsmittel erfasst werden und erfüllt dadurch die geforderten Sicherheitsanforderungen. Es ist jedoch auch möglich, dass beispielsweise ein oder mehrere Erfassungsmittel mit einer sicherheitstechnisch geringeren Erfassungssicherheit zusammengekommen werden können, um so die geforderte Erfassungssicherheit zu erreichen. Wie bereits zuvor erwähnt, kann auch eine sicherheitstechnisch höherwertige personenbezogene Kennung erfasst werden, um so die geforderte Authentifizierungsstufe zu gewährleisten. Auch kann über das Sicherheits-Hierarchieprofil 20 festgelegt werden, wie exakt die Übereinstimmung der personenbezogenen Kennung mit dem Referenzmerkmal beim Vergleich 23 durchgeführt werden muss bzw. welcher Übereinstimmungsgrad mindestens erreicht werden muss. Auch kann über das Sicherheits-Hierarchieprofil 20 festgelegt werden, welches Erfassungsmittel der Erfassungsvorrichtung für welche Authentifizierungsstufe zulässig ist und für welche Authentifizierungsstufe eine erneute Authentifikation erlaubt ist.

[0063] Das erfindungsgemäße Verfahren stellt somit eine Erweiterung der bekannten 3 - Faktor-Authentifikationsverfahren dar. Diese Verfahren nutzen bzw. verwenden als personenbezogene Kennung bspw. folgende Merkmalklassen:

What I am: Ein Merkmal das der Person eigen ist: körperliche Merkmale wie beispielsweise

Stimme, Fingerabdruck, Iris, Handfläche, Gesicht;

What I know: Ein Merkmal das nur die Person kennt: eine Kennziffer/Passwort und/oder eine Passphrase; persönliche Informationen und Vorlieben;

What I have: Ein Merkmal das die Person besitzt: eine Schlüsselkarte oder ein Token, insbesondere jegliche Vorrichtung die zur Hinterlegung eines Schlüsselmerkmals ausgebildet ist, oder die selbst ein Schlüsselmerkmal ist; eine Bank- bzw. Kreditkarte oder ein Ausweis.

[0064] Bekannte Verfahren zur Authentifikation einer Person basieren zumeist auf der Überprüfung eines Merkmals durch einen Vergleich mit einem hinterlegten Referenzmerkmal. Bei einem fehlerhaften Vergleich wird üblicherweise der Authentifikationsvorgang wiederholt, wobei bei einem erneuten fehlerhaften Vergleich der Authentifikationsvorgang abgebrochen wird und somit dem Benutzer der Zugriff auf den angeforderten Dienst verweigert wird. Ferner sind die Erfassungsvorrichtungen zur Durchführung der bekannten Authentifizierungsverfahren zumeist derart ausgebildet, nur ein Merkmal bzw. eine Merkmalklasse erfassen zu können, ein Austausch bzw. ein Wechsel von Merkmalen bzw. Merkmalklassen ist zumeist nicht möglich.

[0065] Zusätzlich zu den drei bekannten Faktoren bzw. Merkmalklassen bietet das erfindungsgemäße Verfahren nun zwei zusätzliche Klassen an, die als eigenständige personenbezogene Kennung erfassbar sind und/oder in Kombination mit einem oder mehreren Merkmalen der bekannten Klassen Verwendung finden. Eine neue Merkmalklasse wie sie beim erfindungsgemäßen Verfahren Anwendung findet, ist durch ein bewusstes Verhalten der Person bei der Präsentation bzw. Eingabe eines Merkmals gekennzeichnet. Wie bereits zuvor erwähnt, kann eine bewusste Aktion bzw. ein bewusstes Verhalten darin bestehen, Pausen und Unterbrechungen im Erfassungsvorgang zu setzen bzw. bewusste Fehleingaben zu machen, oder die Eingabereihenfolge zu ändern, beispielsweise durch Benutzen einer Skip-Funktion bei der Eingabe der Kennung. Somit kann beispielsweise die korrekte Eingabe einer persönlichen Identifikationskennung (PIN) dadurch gekennzeichnet sein, dass genau eine Fehleingabe mit anschließender Korrektur vorgesehen ist. Wird eine Person bedroht, kann diese beispielsweise die Kennung ohne Fehler eingeben, was vom Authentifikations-Kontrollsystem aufgrund des hinterlegten Sicherheits-Hierarchieprofils eindeutig als Alarmsignal erkennbar ist. Dieses bewusste Verhalten bei der Erfassung einer personenbezogenen Kennung erweitert die erreichbaren Sicherheitsstufen der bekannten drei Faktoren bzw. Merkmalklassen zur Authentifikation einer Person ganz beträchtlich. Insbesondere hat die Erfassung eines bewussten Verhaltens den ganz besonderen Vorteil, dass eine derartige personenbezogene Kennung von einem potentiellen Angreifer im Wesentlichen nicht ausspionierbar ist, da ein solches Verhalten bzw. eine derartige Aktion nur schwer von einem üblichen Verhalten einer Person zu unterscheiden ist. Ein potentieller Angreifer würde beispielsweise eine Fehleingabe als Zufall interpretieren und somit nicht erkennen, dass diese scheinbar zufällige Fehleingabe Teil einer personenbezogenen Kennung ist. Auch könnten mehrere Arten von Fehleingaben vom Benutzer aktiviert werden, so dass eine jede im Authentifizierungsprozess als gültig hinterlegt wäre und abwechselungsweise oder kombiniert vom Benutzer eingegeben werden könnte.

[0066] Insbesondere kann der Benutzer selbst festlegen, beispielsweise über ein Konfigurationswerkzeug, welche Typen personenbezogener Kennungen gruppiert als Auswahlmöglichkeit an der Erfassungsvorrichtung (2) präsentiert werden. Ferner kann der Benutzer eine Zuordnung zwischen einem oder mehreren Dienstbereitstellungssystemen und einer derartigen Authentifikationsgruppe festlegen, sodass bei der Authentifikation dem Benutzer bspw. mehrere solcher Gruppen dargeboten werden, wobei nur eine zur Authentifikation am angeforderten Dienst gültig bzw. zugelassen ist. Somit kann durch die Festlegung eines derartigen initialen Anmeldeprofils bereits eine weitere personenbezogene Kennung ausgebildet werden, da der Benutzer bspw. im Bedrohungsfall bewusst die falsche Gruppe auswählen kann und somit wiederum Alarm- bzw. Sicherungsmaßnahmen auslösen kann.

[0067] Neben einem bewussten Verhalten als Merkmalklasse zur Authentifikation einer Person, bietet das erfindungsgemäße Verfahren eine weitere Merkmalklasse, mit der auch ein unbewusstes Verhalten der Person zur Authentifikation derselben herangezogen werden kann.

Während die Merkmale der bekannten drei Klassen ausspioniert und gegebenenfalls nachgebildet werden können und dies auch unter sehr spezifischen Umständen auch für die vierte Klasse möglich ist, ist dies bei einem unbewussten Verhalten kaum möglich, da ein derartiges Verhaltensmuster ganz spezifisch jeder Person zu Eigen ist und somit bereits durch einen Spionageversuch verfälscht werden würde. Ein derartiges unbewusstes Verhaltensmuster kann in einer Trainingsphase dadurch ermittelt werden, dass die Reaktion bzw. das Verhalten der Person auf eine Mehrzahl standardisierter, insbesondere nach psychologischen Grundlagen, erstellter Fragen bzw. Auswahlmöglichkeiten erfasst wird. Zur Erstellung eines persönlichen Verhaltensmusters sind aus dem Fachgebiet der Verhaltensforschung eine Mehrzahl unterschiedlicher Test- bzw. Evaluierungsmethoden bekannt, auf die hier nicht weiter eingegangen wird. Insbesondere wird eine Person durch ihr Verhalten authentifizierbar, wobei dieses grundlegende Verhalten tief im Unterbewusstsein der Person verankert ist und somit eine außerordentlich hohe Authentifizierungssicherheit gegeben ist.

[0068] Eine Klasse personenbezogener Kennungen kann auch darin bestehen, dass die Art der gewählten Authentifikationsklasse, gesteuert beispielsweise durch das Sicherheits-Hierarchieprofil, als personenbezogene Kennung herangezogen wird. Beispielsweise kann vom Authentifikations-Kontrollsystem für den vom Benutzer angeforderten Dienst eine nicht korrekte Authentifikationsklasse bzw. Authentifizierungsstufe vorgegeben werden, beispielsweise in dem für die Anforderung eines Finanztransaktionsdienstes eine sicherheitstechnisch niederwertige Kennung erfasst werden soll. Zur korrekten Authentifikation der Person müsste diese beispielsweise den Authentifikationsvorgang abbrechen und erneut auslösen, oder die vorgegebene Authentifikationsklasse ablehnen und eine neue, insbesondere sicherheitstechnisch höherwertige Klasse anfordern.

[0069] Ferner kann mit einer Benutzergruppierung eine zusätzliche Hierarchieebene eingeführt werden, wobei sich ein Benutzer wahlfrei einer Gruppe zuordnen bzw. von dieser abmelden kann. Eine derartige Gruppierung lässt sich nun so ausbilden, dass für jede Gruppe spezifische Merkmale hinterlegt sind, die dem einzelnen Benutzer bekannt sind. Die Gruppierung wird bevorzugt derart vorgenommen werden, dass sich die einzelnen Gruppenmitglieder im Wesentlichen kennen und somit auch von personenspezifischen Details Kenntnis haben, die einem potentiellen Angreifer jedenfalls nicht zur Verfügung stehen. Beispielsweise könnte eine gruppenbezogene Kennung darin bestehen, dass der sich authentifizierende Benutzer die Kennung einer mobilen Kommunikationsvorrichtung eines Benutzers der Gruppe angeben muss.

[0070] Das erfindungsgemäße Verfahren bietet nun eine bedeutende Steigerung der individuell anpassbaren Sicherheitsstufe bei der Authentifikation einer Person, insbesondere im Hinblick auf die Möglichkeit der auslösbaren Aktionen, ohne dass dafür eine Vielzahl unterschiedlicher personenbezogener Kennungen festgelegt werden müssen. Je größer die Anzahl unterschiedlicher personenbezogener Kennungen ist, die sich eine Person merken muss, desto größer ist die Gefahr, dass die mögliche Vielzahl ignoriert wird und nur einige wenige personenbezogene Kennungen verwendet werden. Somit hat es ein potentieller Angreifer zumeist recht leicht, diese Kennungen auszuspionieren und somit Zugriff auf eine Vielzahl unterschiedlicher Dienste zu erlangen. Mit dem erfindungsgemäßen Verfahren ist es nun möglich, mit einer geringen Anzahl personenbezogener Kennungen, in Kombination mit den weiteren Authentifikations- bzw. Merkmalklassen, eine ganz besondere Steigerung der Identifikationssicherheit zu erlangen und gleichzeitig die Chance auf ein bewusstes Aushorchen der personenbezogenen Kennungen durch Dritte zu minimieren.

[0071] Der ganz wesentliche Vorteil des erfindungsgemäßen Verfahrens liegt nun darin, dass die Authentifikation einer Person durch Erfassung personenbezogener Kennungen erfolgen kann, die von einem potentiellen Angreifer im Wesentlichen nicht ausspionierbar sind. Ferner hat eine bedrohte Person die Möglichkeit, bewusst eine falsche Auswahl bzw. Eingabe zu tätigen, ohne dass dies für einen Angreifer ersichtlich ist, um so ggf. Sicherungsmaßnahmen in Gang zu setzen. Von ganz besonderem Vorteil ist ferner, dass die Authentifikation auf Basis der Erfassung personenbezogener Kennungen derart flexibel ausgebildet ist, dass die erforderliche Sicherheitsstufe der Authentifikation nicht nur durch die Erfassung einer vorgesehenen perso-

nenbezogenen Kennung möglich ist, sondern dass auch sicherheitstechnisch höherwertige und/oder mehrere sicherheitstechnisch niederwertige personenbezogene Kennungen herangezogen werden können. Zur Umgehung des erfindungsgemäßen Authentifikationsverfahrens müsste ein potentieller Angreifer daher eine Mehrzahl unterschiedlicher Kennungen ausspionieren, was äußerst unwahrscheinlich ist und üblicherweise in keiner Relation zum erreichbaren Nutzen bzw. zur Gefahr einer Erkennung des Manipulationsversuchs steht.

[0072] Des Weiteren ermöglicht dieses Verfahren innerhalb desselben Umfeldes, bspw. in einer Betriebsstätte mit einem POS-Gerät (Point of Sale), unterschiedlich sichere Authentifikationen vorzunehmen. Für die Abwicklung einer Transaktion mit einem geringen Volumen bzw. mit einem geringen Geldwert reicht die Erfassung einer sicherheitstechnisch niederwertigen personenbezogenen Kennung. Im Gegensatz dazu kann für ein großes Transaktionsvolumen bzw. für einen großen Geldwert die Erfassung einer sicherheitstechnisch hochwertigen personenbezogenen Kennung gefordert sein. Die Regeln für eine solche Festlegung der Sicherheitsstufen können am Dienstbereitstellungs-System und/oder am Authentifikations-Kontrollsystem hinterlegt sein. Ferner können diese Sicherheitsstufen mit weiteren erfindungsgemäßen Regel kombiniert werden, ferner kann ein Zufallsgeneratoren vorhanden sein, mit dem wahlfrei Stichproben gezogen werden, in dem sich ein Benutzer mit einer höheren Sicherheitsstufe authentifizieren muss, als dies für den angeforderten Dienst erforderlich wäre. Es kann also durchaus vorkommen, dass derselbe Benutzer bei Abwicklung derselben Transaktion, in derselben Betriebsstätte zwei verschiedenen Authentifizierungsabläufen folgen muss.

[0073] Fig. 3 zeigt eine weitere mögliche Vorrichtung zur Durchführung des erfindungsgemäßen Verfahrens. Dabei werden das Authentifikations-Kontrollsystem und das Authentifizierungssystem in ein Authentifikations-Steuerungssystem 28 integriert, welches somit alle wesentlichen sicherheitskritischen Vorrichtungen zu Durchführung des erfindungsgemäßen Verfahrens umfasst. Insbesondere wird somit erreicht, dass auf der Erfassungsvorrichtung 2 keine sicherheitstechnisch relevanten Daten wie beispielsweise Referenzmerkmale hinterlegt sind und dass ferner die Vergleichsprüfung in einem besonders gesicherten Authentifikations-Steuerungssystem 28 durchgeführt werden kann. Die Erfassungsvorrichtung 2 weist dazu eine Kommunikationsschnittstelle 29 auf, über die eine Kommunikationsverbindung mit dem Authentifikations-Steuerungssystem 28 hergestellt werden kann. Zur Durchführung der Erfassung der personenbezogenen Kennung kann es beispielsweise vorgesehen sein, dass das vom Authentifikations-Steuerungssystem 28 hinterlegte Steuerungsanweisungen an die Erfassungsvorrichtung 2 übermittelt werden und dort in einem Ausführungsmodul 31 temporär hinterlegt werden und von diesem zur Steuerung der Erfassungsmittel der Erfassungsvorrichtung 2 ausgeführt werden. Das Ausführungsmodul 31 kann beispielsweise derart ausgebildet sein, dass es eine Signaturprüfung der übertragenen Steuerungsanweisungen 30 durchführt, wodurch eine bewusste Manipulation der Erfassungsvorrichtung durch Einspielen einer nicht korrekt signierten Steueranweisung weitestgehend verhindert wird.

[0074] Insbesondere hat diese Ausbildung den Vorteil, dass technisch sehr einfache und damit kostengünstige Erfassungsvorrichtungen 2 einsetzbar sind, da die Steuerung des Ablaufs, sowie die Durchführung der Vergleichsoperation der erfassten personenbezogenen Kennung mit hinterlegten Referenzmerkmalen 14 von einem zentralen Authentifikationssteuerungssystem 28 durchgeführt wird und somit die Erfassungsvorrichtung keine wesentlichen sicherheitskritischen und manipulierbaren Komponenten aufweist.

[0075] Die Authentifizierungsanforderung wird bei dieser Ausbildung vom Dienstbereitstellungs-System 5 an das Authentifikationssteuerungssystem 28 übermittelt. Dieses führt anschließend die erfindungsgemäßen Verfahrensschritte durch und übermittelt bei erfolgreicher Authentifikation der Person ein Freigabesignal an das anfragende Dienstbereitstellungs-System 5.

[0076] Die Ausführungsbeispiele zeigen mögliche Ausführungsvarianten des anforderungs-basierten Personenidentifikationsverfahrens, wobei an dieser Stelle bemerkt sei, dass die Erfindung nicht auf die speziell dargestellten Ausführungsvarianten derselben eingeschränkt ist, sondern vielmehr auch diverse Kombinationen der einzelnen Ausführungsvarianten untereinander

der möglich sind und diese Variationsmöglichkeit aufgrund der Lehre zum technischen Handeln durch gegenständliche Erfindung im Können des auf diesem technischen Gebiet tätigen Fachmannes liegt. Es sind also auch sämtliche denkbaren Ausführungsvarianten, die durch Kombinationen einzelner Details der dargestellten und beschriebenen Ausführungsvariante möglich sind, vom Schutzzumfang mit umfasst.

[0077] In der Fig. 3 ist eine weitere und gegebenenfalls für sich eigenständige Ausführungsform des anforderungsbasierten Personenidentifikationsverfahrens gezeigt, wobei wiederum für gleiche Teile gleiche Bezugszeichen bzw. Bauteilbezeichnungen wie in den vorangegangenen Fig. 1 und 2 verwendet werden. Um unnötige Wiederholungen zu vermeiden, wird auf die detaillierte Beschreibung in den vorangegangenen Figuren hingewiesen bzw. Bezug genommen.

[0078] Der Ordnung halber sei abschließend darauf hingewiesen, dass zum besseren Verständnis des Aufbaus des anforderungsbasierten Personenidentifikationsverfahrens diese bzw. deren Bestandteile teilweise unmaßstäblich und/oder vergrößert und/oder verkleinert dargestellt wurden.

[0079] Die den eigenständigen erfinderischen Lösungen zugrundeliegende Aufgabe kann der Beschreibung entnommen werden.

[0080] Vor allem können die einzelnen in den Fig. 1 bis 3 gezeigten Ausführungen den Gegenstand von eigenständigen, erfindungsgemäßen Lösungen bilden. Die diesbezüglichen, erfindungsgemäßen Aufgaben und Lösungen sind den Detailbeschreibungen dieser Figuren zu entnehmen.

BEZUGSZEICHENAUFSTELLUNG

- | | |
|----|---|
| 1 | Authentifikations-Kontrollsystem |
| 2 | Erfassungsvorrichtung |
| 3 | Erfassungsmittel |
| 4 | Kommunikationsnetzwerk |
| 5 | Dienstbereitstellungs-System |
| 6 | Authentifizierungssystem |
| 7 | Authentifizierungsanforderung |
| 8 | Übertragung der Authentifizierungsanforderung |
| 9 | Authentifizierungsstufe |
| 10 | Alphanumerisches Eingabemittel, Tastatur |
| 11 | Optische Bilderfassungsvorrichtung |
| 12 | Fingerabdruckscanner |
| 13 | Audiovisuelle Ein-Ausgabevorrichtung |
| 14 | Referenzmerkmal |
| 15 | Speichermittel |
| 16 | Speichermittel |
| 17 | Freigabesignal |
| 18 | Abgabe eines Freigabesignals |
| 19 | Ermitteln der Authentifizierungsstufe |
| 20 | Sicherheits-Hierarchieprofil |
| 21 | Aktivieren eines Erfassungsmittel |
| 22 | Erfassen einer personenbezogenen Kennung |
| 23 | Vergleich mit Referenzmerkmal |
| 24 | Hinterlegte Referenzmerkmale |
| 25 | Fehlerhafte Übereinstimmung |

- 26 Vergleich
- 27 Fehlersignal
- 28 Authentifikations-Steuerungssystem
- 29 Kommunikationsschnittstelle
- 30 Steuerungsanweisungen
- 31 Ausführungsmodul

Patentansprüche

1. Anforderungsbasiertes Personenidentifikationsverfahren umfassend die Schritte:
 - a.) Empfang einer Authentifizierungsanforderung (7) von einem Dienstbereitstellungssystem (5) durch ein Authentifikations-Kontrollsystem (1);
 - b.) Ermitteln der erforderlichen Authentifizierungsstufe (9) durch das Authentifikations-Kontrollsystem (1) durch Analyse der Authentifizierungsanforderung (7);
 - c.) Aktivieren (21) eines Erfassungsmittels (3) einer Erfassungsvorrichtung (2);
 - d.) Erfassen (22) einer personenbezogenen Kennung durch das Erfassungsmittel (3);
 - e.) Vergleich (23) der erfassten Kennung mit einem, in einer Speichereinheit (15, 16) hinterlegten, korrespondierenden Referenzmerkmal (14);

dadurch gekennzeichnet, dass bei Übereinstimmung ein Freigabesignal (17) an das Dienstbereitstellungssystem (5) abgegeben wird, und bei fehlerhafter Übereinstimmung (25) ein weiteres Erfassungsmittel (3) der Erfassungsvorrichtung (2) aktiviert wird und die entsprechenden Verfahrensschritte wiederholt werden.
2. Anforderungsbasiertes Personenauthentifikationsverfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass bei wiederholter fehlerhafter Übereinstimmung, ein Fehlerkennzeichensignal (27) als ein Alarmsignal abgegeben wird.
3. Anforderungsbasiertes Personenauthentifikationsverfahren nach einem der Ansprüche 1 oder 2, **dadurch gekennzeichnet**, dass mit der Authentifizierungsanforderung (7) eine Sicherungskennzahl übermittelt wird, welche die Authentifizierungsstufe (9) festlegt.
4. Anforderungsbasiertes Personenauthentifikationsverfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, dass mit der Authentifizierungsanforderung (7) ein Referenzsatz (14) eines personenbezogenen Merkmals übermittelt wird.
5. Anforderungsbasiertes Personenauthentifikationsverfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet**, dass die Ermittlung der Authentifizierungsstufe (9) durch Vergleich der Authentifizierungsanforderung (7) mit einem hinterlegten Sicherheits-Hierarchieprofil (20) erfolgt.
6. Anforderungsbasiertes Personenauthentifikationsverfahren nach Anspruch 5, **dadurch gekennzeichnet**, dass das Sicherheits-Hierarchieprofil (20) eine Zuordnung zwischen Erfassungsmittel (3) und Authentifizierungsstufe (9) herstellt.
7. Anforderungsbasiertes Personenauthentifikationsverfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet**, dass mit der Authentifizierungsanfrage (7) eine Ablaufanweisung übermittelt wird.
8. Anforderungsbasiertes Personenauthentifikationsverfahren nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet**, dass das Authentifikations-Kontrollsystem (1) die Funktionalität der Erfassungsvorrichtung (2) steuert.
9. Anforderungsbasiertes Personenauthentifikationsverfahren nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet**, dass als personenbezogene Kennung (22) eine alphanumerische Kennung erfasst wird.

10. Anforderungsbasiertes Personenauthentifikationsverfahren nach einem der Ansprüche 1 bis 9, **dadurch gekennzeichnet**, dass als personenbezogene Kennung (22) ein biometrisches Merkmal erfasst wird.
11. Anforderungsbasiertes Personenauthentifikationsverfahren nach einem der Ansprüche 1 bis 10, **dadurch gekennzeichnet**, dass als personenbezogene Kennung (22) eine Bedienungshandlung erfasst wird, mit der das Erfassungsmittel (3) von der zu authentifizierenden Person bedient wird.
12. Anforderungsbasiertes Personenauthentifikationsverfahren nach einem der Ansprüche 1 bis 11, **dadurch gekennzeichnet**, dass bei der Erfassung der personenbezogenen Kennung (22) ein zeitlicher Ablauf erfasst wird.
13. Anforderungsbasiertes Personenauthentifikationsverfahren nach einem der Ansprüche 1 bis 12, **dadurch gekennzeichnet**, dass die Erfassungsvorrichtung (2) mittels einer Ein-/Ausgabevorrichtung (13) eine personalisierte Anfrage ausgibt, beispielsweise eine Eingabeaufforderung mit mehreren Auswahlmöglichkeiten, und die Reaktion der Person als personenbezogene Kennung (22) erfasst wird.
14. Anforderungsbasiertes Personenauthentifikationsverfahren nach Anspruch 5, **dadurch gekennzeichnet**, dass das Sicherheits-Hierarchieprofil (20) von einem Authentifizierungssystem (28) an das Authentifikations-Kontrollsystem (1) übertragen wird.
15. Anforderungsbasiertes Personenauthentifikationsverfahren nach Anspruch 5, **dadurch gekennzeichnet**, dass das Sicherheits-Hierarchieprofil (20) in einer Trainingsphase erstellt wird, wobei personenbezogene Kennungen (22) als Referenzmerkmale (14) erfasst und in einem Speichermittel (15, 16) hinterlegt werden.
16. Anforderungsbasiertes Personenauthentifikationsverfahren nach Anspruch 15, **dadurch gekennzeichnet**, dass ein bewusstes Verhaltensmuster als personenbezogenes Referenzmerkmal (14) erfasst wird, indem eine spezifische Abfolge von Bedienhandlungen an der Erfassungsvorrichtung (3) erfasst wird.
17. Anforderungsbasiertes Personenauthentifikationsverfahren nach Anspruch 15 oder 16, **dadurch gekennzeichnet**, dass ein unbewusstes Verhaltensmuster als personenbezogenes Referenzmerkmal (14) erfasst wird, indem die Person mittels einer Ein-/Ausgabevorrichtung (13) eine Mehrzahl von Auswahlmöglichkeiten dargestellt bekommt und die jeweils getroffene Auswahl erfasst wird.
18. Anforderungsbasiertes Personenauthentifikationsverfahren nach Anspruch 17, **dadurch gekennzeichnet**, dass aus den erfassten Auswahlsergebnissen ein Reaktionsprofil erstellt wird.
19. Anforderungsbasiertes Personenauthentifikationsverfahren nach einem der Ansprüche 1 bis 18, **dadurch gekennzeichnet**, dass Referenzmerkmal (14) in der Speichereinheit (15) des Authentifikations-Kontrollsystems (1) hinterlegt werden.
20. Anforderungsbasiertes Personenauthentifikationsverfahren nach einem der Ansprüche 1 bis 19, **dadurch gekennzeichnet**, dass nach Ablauf eines Zeitgebers am Dienstbereitstellungssystem (5) oder am Authentifikations-Kontrollsystem (1), eine Authentifizierungsanforderung (7) generiert wird.
21. Anforderungsbasiertes Personenauthentifikationsverfahren nach einem der Ansprüche 1 bis 20, **dadurch gekennzeichnet**, dass als personenbezogene Kennung ein Abbild der Person erfasst wird.
22. Anforderungsbasiertes Personenauthentifikationsverfahren nach Anspruch 21, **dadurch gekennzeichnet**, dass das erfasste Abbild an eine mobile Kommunikationsvorrichtung übermittelt wird.

Hierzu 3 Blatt Zeichnungen

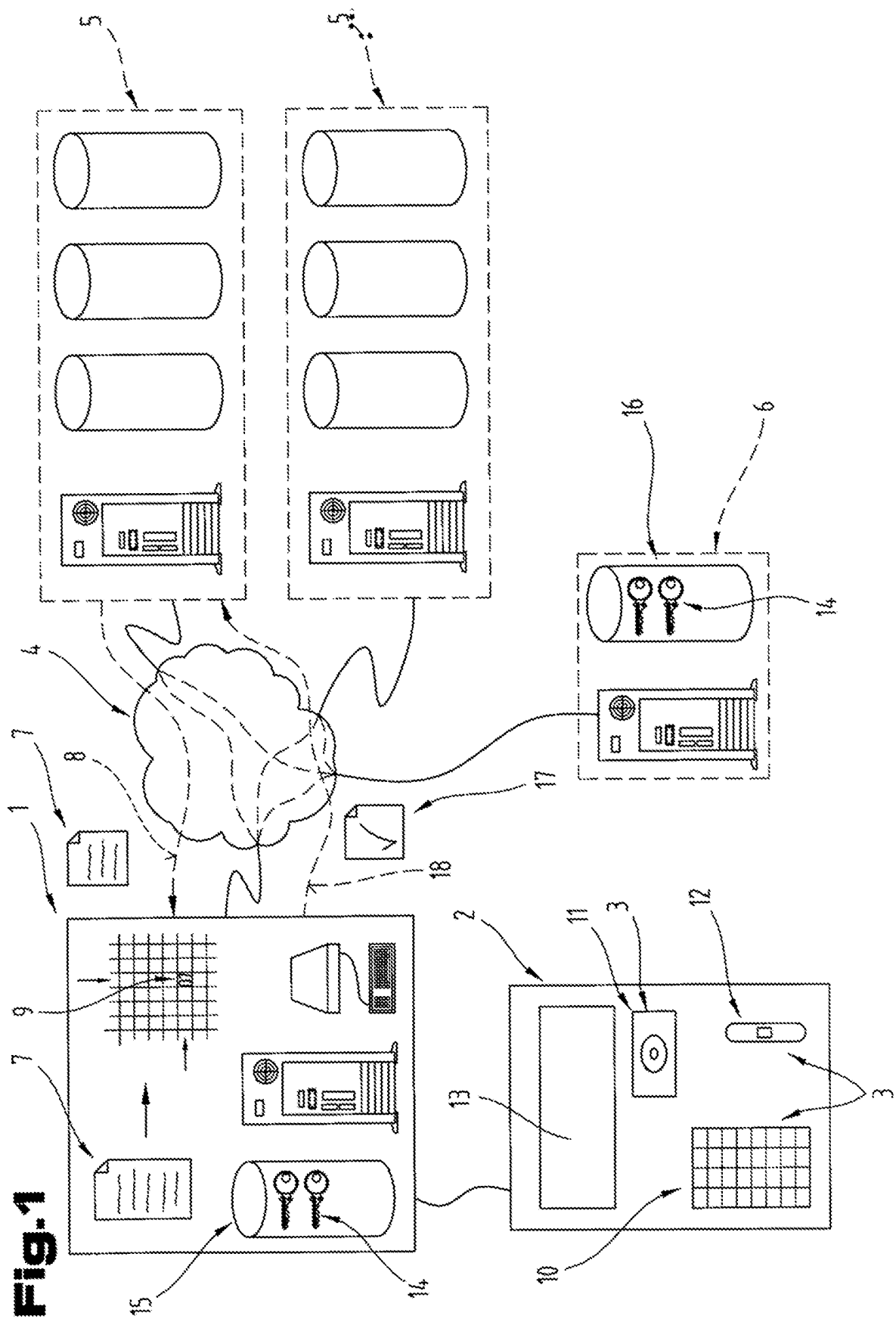


Fig.2

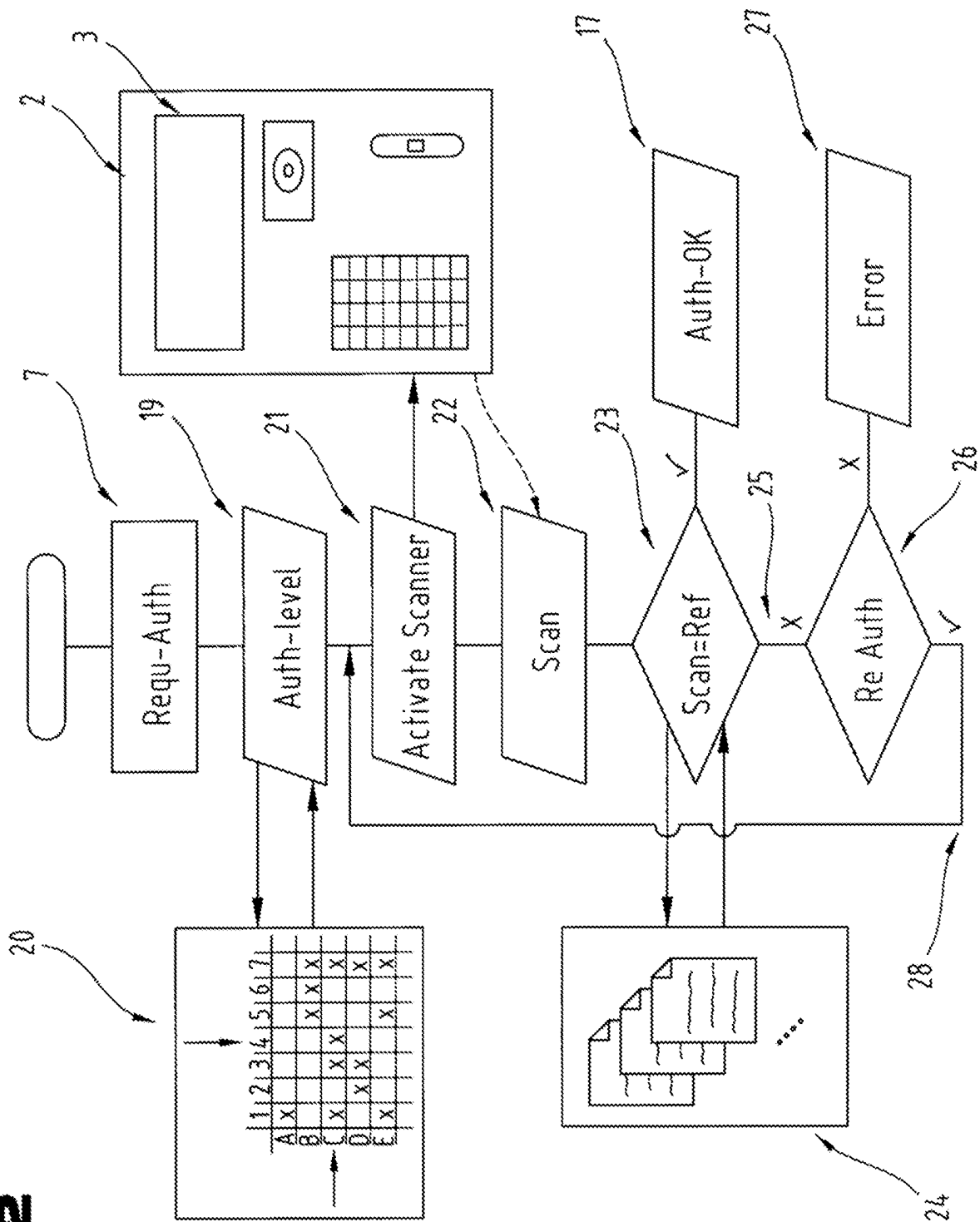


Fig. 3

