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

(11) **EP 4 361 977 A1**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
01.05.2024 Patentblatt 2024/18

(21) Anmeldenummer: **23205102.9**

(22) Anmeldetag: **23.10.2023**

(51) Internationale Patentklassifikation (IPC):
G07C 9/25 *(2020.01)* ***G07C 9/26*** *(2020.01)*

(52) Gemeinsame Patentklassifikation (CPC):
G07C 9/25; G07C 9/26; G07C 9/28; G07C 2209/04

(84) Benannte Vertragsstaaten:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC ME MK MT NL NO PL PT RO RS SE SI SK SM TR
Benannte Erstreckungsstaaten:
BA
Benannte Validierungsstaaten:
KH MA MD TN

(30) Priorität: **26.10.2022 DE 102022128377**

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

(72) Erfinder:
- **Dressel, Olaf**
  14641 Wustermark (DE)
- **Dr. Wolf, Andreas**
  13158 Berlin (DE)
- **Graupner, Hendrik**
  14050 Berlin (DE)

(74) Vertreter: **Hentrich Patent- & Rechtsanwaltspartnerschaft mbB**
Syrlinstraße 35
89073 Ulm (DE)

(54) VERFAHREN ZUR AUTHENTIFIZIERUNG EINER PERSON MITHILFE EINES ZUGANGSKONTROLLSYSTEMS

(57) Die Erfindung betrifft ein Verfahren zur Authentifizierung einer Person (200) mit den Schritten:
- Erfassen von personenspezifischen Daten und Vergleichen mit einem Vergleichsdatensatz, wobei ein erstes erfolgreiches Authentifizierungsergebnis erstellt wird, wenn eine Abweichung hinter einem Schwellenwert zurückbleibt;
- Aufbauen einer Kommunikationsverbindung zwischen dem mobilen Endgerät (106) und einer Zugangskontrollstation (102) mit einem ersten Sicherheitsniveau;
- Übertragen des ersten Authentifizierungsergebnisses an die Zugangskontrollstation (102), wobei im Falle eines erfolgreichen ersten Authentifizierungsergebnisses eine Freigabe durch die Zugangskontrollstation (102) erteilt wird;
- Erfassen von weiteren personenspezifischen Daten mittels eines weiteren Sensors und Vergleichen mit einem weiteren Vergleichsdatensatz, wobei ein erfolgreiches zweites Authentifizierungsergebnis erstellt wird, wenn eine Abweichung hinter einem Schwellenwert zurückbleibt;
- Aufbauen einer Kommunikationsverbindung zwischen dem mobilen Endgerät und einer Zugangskontrollstation (104) mit einem zweiten Sicherheitsniveau; und
- Übertragen des ersten erfolgreichen und des zweiten erfolgreichen Authentifizierungsergebnisses an die Zugangskontrollstation (104), wobei dann eine Freigabe von der Zugangskontrollstation (104) erteilt wird.

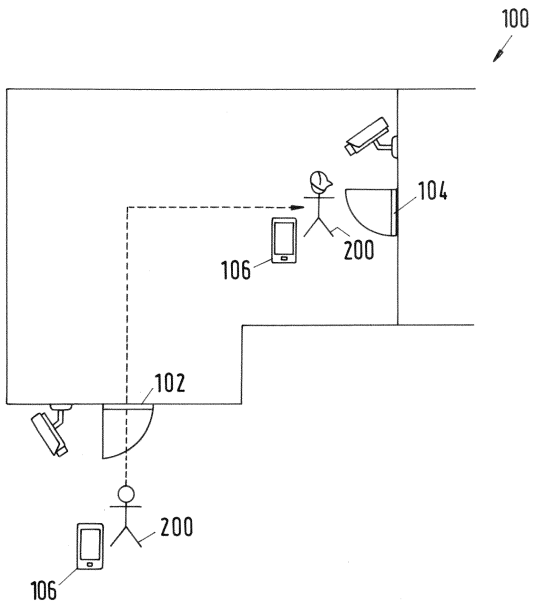

Fig.1

EP 4 361 977 A1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Authentifizierung einer Person mithilfe eines Zugangskontrollsystems, das aus mehreren Zugangskontrollstationen und einem mobilen Endgerät gebildet ist.

[0002] Verfahren zur Nutzerauthentifizierung mithilfe eines Zugangskontrollsystems, das mehrere solche Zugangskontrollstationen und ein mobiles Endgerät umfassen, kommen überall dort zum Einsatz, wo ein Schlüssel, eine Schlüsselkarte oder dergleichen zur Authentifizierung bzw. zur Zutrittskontrolle verwendet wird. Hierbei sind Zugangskontrollsysteme bekannt, bei denen sich ein Nutzer authentifizieren muss, um Einlass zu einem durch die Zugangskontrolle geschützten Bereich zu erlangen. Beispielweise gibt der Nutzer eine PIN in ein dafür vorgesehenes Eingabemittel ein. Bei erfolgreicher Authentifizierung steuert die Zugangskontrolleinrichtung eine Tür oder ein Verriegelungsmittel an, um dem Nutzer den Zugang zu dem geschützten Bereich zu ermöglichen. Zum Erlangen eines unberechtigten Zugangs genügt es in diesem Fall bereits, dass ein unberechtigter Nutzer die PIN bei der Eingabe ausspäht.

[0003] In der DE 10 2017 208 234 A1 der Anmelderin wird ein Verfahren und ein System zur verhaltensbasierten Authentifizierung eines Nutzers mittels eines mobilen, tragbaren ersten Kommunikationssystems gegenüber einem zweiten Kommunikationssystem beschrieben. Dieses hat sich in der Praxis sehr gut bewährt.

[0004] Bei der durch Durchführung von Authentifizierungsschemata oder Authentifizierungsverfahren werden die Daten oft erst zum Zeitpunkt der gewünschten Authentifizierung erfasst. Bei besitzbasierten Verfahren stört das nicht weiter, denn die Arbeit für die Authentifizierung erfolgt dabei hardwareseitig. Aufwendiger ist die Authentifikation bei wissensbasierten oder bei biometrischen Schemata zur Authentifikation. Hierfür müssen dann "ad hoc" ein Kennwort eingegeben oder eines oder mehrere biometrische Merkmale erfasst werden. Dies ist oft sehr zeitaufwendig und erfordert eine Verhaltensanpassung durch den Nutzer.

[0005] Es ist daher die Aufgabe der vorliegenden Erfindung, ein verbessertes Verfahren zur Authentifizierung eines Nutzers bei unterschiedlichen Zugangskontrollstationen mit unterschiedlichen Sicherheitsniveaus bereitzustellen.

[0006] Diese Aufgabe wird durch ein Verfahren zur Authentifizierung einer Person mithilfe eines Zugangskontrollsystems mit den Merkmalen des Anspruchs 1 gelöst. Vorteilhafte Ausgestaltungen mit zweckmäßigen Weiterbildungen der Erfindung sind in den abhängigen Ansprüchen angegeben.

[0007] Das Zugangskontrollsystem zur Durchführung des erfindungsgemäßen Verfahrens umfasst insbesondere eine Zugangskontrollstation mit einem ersten Sicherheitsniveau und mindestens eine weitere Zugangskontrollstation mit einem zweiten Sicherheitsniveau, wobei das zweite Sicherheitsniveau eine höhere Sicherheitsanforderung als das erste Sicherheitsniveau stellt. Außerdem umfasst das Zugangskontrollsystem ein von der zu authentifizierenden Person mitgeführtes mobiles Endgerät, welches einen Sensor umfasst, der eingerichtet ist, Daten der Person zu erfassen, die in einen Speicher des mobilen Endgeräts gespeichert werden, wobei in dem Speicher mindestens ein Vergleichsdatensatz für einen Abgleich der vom Sensor erfassten Daten gespeichert ist, und welches einen Prozessor umfasst, der dazu eingerichtet ist, die vom Sensor erfassten Daten und den mindestens einen Vergleichsdatensatz aus dem Speicher auszulesen und für eine Authentifizierung miteinander zu vergleichen. Das Zugangskontrollsystem umfasst auch ein zentrales Kommunikationssystem, welches aus einer Mehrzahl von Kommunikationsmodulen mit Kommunikationsschnittstellen besteht, wobei jede der Zugangskontrollstationen und auch das mobile Endgerät wenigstens eines der Kommunikationsmodule umfasst, wodurch das mobile Endgerät und die Zugangskontrollstationen eingerichtet sind, zumindest zeitweise über eine Kommunikationsverbindung miteinander zu kommunizieren.

[0008] Das erfindungsgemäße Verfahren selbst durchläuft dabei insbesondere die folgenden Schritte:

- Erfassen von personenspezifischen Daten der Person mittels des Sensors und Vergleichen der erfassten Daten mit den Werten des mindestens einen Vergleichsdatensatzes, wenn sich die Person mit dem mobilen Endgerät zumindest in der Nähe der Zugangskontrollstation mit dem ersten Sicherheitsniveau befindet oder eine Bewegung des mobilen Endgeräts zu der Zugangskontrollstation mit dem ersten Sicherheitsniveau erfasst wird, wobei der Prozessor des mobilen Endgeräts dann ein erstes erfolgreiches Authentifizierungsergebnis erstellt und gegebenenfalls im Speicher ablegt, wenn eine Abweichung beim Vergleich der Daten hinter einem Schwellenwert zurückbleibt oder wenn die Abweichung beim Vergleich der Daten sogar Null (0) ist;
- zeitlich dem Erfassen vorangehend, zeitlich diesem nachfolgend oder zeitgleich mit dem Erfassen: Aufbauen der Kommunikationsverbindung zwischen dem mobilen Endgerät und der Zugangskontrollstation mit dem ersten Sicherheitsniveau;
- Übertragen des ersten Authentifizierungsergebnisses an die Zugangskontrollstation mit dem ersten Sicherheitsniveau, wobei im Falle des Vorliegens von einem erfolgreichen ersten Authentifizierungsergebnis eine Freigabe durch die Zugangskontrollstation mit dem ersten Sicherheitsniveau erteilt wird;
- Erfassen von weiteren personenspezifischen Daten der Person mittels eines weiteren Sensors, wobei sich die weiteren personenspezifischen Daten der Person von den zuerst erfassten personenspezifischen Daten unterscheiden, Vergleichen der erfassten weiteren Daten mit den Werten eines weiteren Vergleichsdatensatzes, wenn sich die Person mit

dem mobilen Endgerät zumindest in der Nähe der Zugangskontrollstation mit dem zweiten Sicherheitsniveau befindet oder eine Bewegung des mobilen Endgeräts zu der Zugangskontrollstation mit dem zweiten Sicherheitsniveau erfasst wird, wobei der Prozessor des mobilen Endgeräts dann ein erfolgreiches zweites Authentifizierungsergebnis erstellt und gegebenenfalls im Speicher ablegt, wenn eine Abweichung beim Vergleich der weiteren Daten hinter einem, gegebenenfalls weiteren, Schwellenwert zurückbleibt,

oder wenn eine solche Abweichung sogar Null ist;

- zeitlich dem Erfassen vorangehend, zeitlich diesem nachfolgend oder zeitgleich:
  Aufbauen der Kommunikationsverbindung zwischen dem mobilen Endgerät und der Zugangskontrollstation mit dem zweiten Sicherheitsniveau;
- Übertragen des ersten Authentifizierungsergebnisses an die Zugangskontrollstation mit dem zweiten Sicherheitsniveau, wobei im Falle des Vorliegens sowohl von einem erfolgreichen ersten Authentifizierungsergebnis als auch von einem erfolgreichen zweiten Authentifizierungsergebnis eine Freigabe durch die Zugangskontrollstation mit dem zweiten Sicherheitsniveau erteilt wird.

[0009] Mit dem erfindungsgemäßen Verfahren ist ein physisches und logisches Zugangsmonitoring und eine Zugangskontrolle geschaffen, die eine Authentifizierung abhängig vom jeweils zu erreichenden Sicherheitsniveau ermöglicht. Somit liegt kontinuierlich die nötige Authentifizierung vor, sodass zum Zeitpunkt und am Ort einer antizipierten Zugangskontrolle ein Authentifikationsergebnis im Sinne eines geeigneten Sicherheitsniveaus bereitsteht.

[0010] Dabei ist die Möglichkeit vorhanden, dass das Erfassen der weiteren personenspezifischen Daten durch den weiteren Sensor erfolgt, welcher zumindest einer der Zugangskontrollstationen zugeordnet ist. Somit müssen also nicht nur die Daten von dem mobilen Endgerät aufgezeichnet werden, um ein gewünschtes (zweites) Sicherheitsniveau zu erreichen, sondern auch Werte von Sensoren erfasst werden, die einer der Zugangskontrollstationen zugewiesen ist, wozu beispielsweise ein Sensor in Form einer Kamera in Betracht kommt. Weitere mögliche Sensoren sind jedoch auch Venensensoren, Iriserkennungssensoren, Fingerabdrucksensoren, Feldinformationen von Kommunikationsmitteln (z.B. über eine Luftschnittstelle wie WiFi, Bluetooth, USB, NFC, etc.).

[0011] Um das mobile Endgerät datensparsam nutzen zu können, hat es sich als vorteilhaft erwiesen, wenn das erfolgreiche erste Authentifizierungsergebnis vom Kommunikationsmodul der Zugangskontrollstation mit dem ersten Sicherheitsniveau an das Kommunikationsmodul der Zugangskontrollstation mit dem zweiten Sicherheitsniveau unmittelbar übertragen wird.

[0012] Es ist jedoch alternativ auch die Möglichkeit gegeben, dass das erfolgreiche erste Authentifizierungsergebnis im Speicher des mobilen Endgeräts abgespeichert wird, und dass das erfolgreiche erste Authentifizierungsergebnis vom Kommunikationsmodul des mobilen Endgeräts an das Kommunikationsmodul der Zugangskontrollstation mit dem zweiten Sicherheitsniveau unmittelbar übertragen wird. Auf diese Weise muss eine Kommunikationsverbindung zwischen den beiden Zugangskontrollstationen nicht aufgebaut werden und der Nutzer behält mit dem mobilen Endgerät die Datenhoheit über seine Daten, die dem ersten Authentifizierungsergebnis zugrunde liegen.

[0013] Es ist von Vorteil, wenn in dem Speicher des mobilen Endgeräts eine Authentifizierungshistorie gespeichert wird, in welcher alle bisher durchgeführten Authentifizierungsverfahren oder Authentifizierungsschemata enthalten sind. Auf diese Weise ist es möglich, dass aus den bisherigen Erfahrungen und/oder nach Kommunikation des mobilen Endgeräts mit einem die Authentifizierung anfordernden System, das mobile Endgerät zu jeder Zeit das demnächst zu erreichende Sicherheitsniveau kennt und somit die entsprechenden Authentifizierungsschemata einleiten kann. Das mobile Endgerät prüft dabei, ob es anhand der aktuell vorliegenden Daten das gewünschte Sicherheitsniveau erreichen kann und versucht dann gegebenenfalls weitere Sensordaten zu erhalten, sollten der bisherige Datenbestand nicht ausreichen, um eine Authentifikation im Sinne des antizipierten Sicherheitsniveaus erfolgreich durchzuführen.

[0014] In diesem Zuge ist es daher von Vorteil, wenn das mobile Endgerät anhand der Authentifizierungshistorie automatisch das oder diejenigen Authentifizierungsverfahren zur Authentifizierung der Person durchführt, welche an das Sicherheitsniveau der betreffenden Zugangskontrollstation angepasst sind.

[0015] Um beispielsweise eine Vielzahl von Zugangskontrollstationen besonders schnell durchschreiten oder überwinden zu können, hat es sich als vorteilhaft erwiesen, wenn das mobile Endgerät bei Erfassung einer vorgegebenen Position oder beim Erfassen eines vorgegebenen Abstands von einer der Zugangskontrollstationen das oder die benötigten Authentifizierungsverfahren automatisch einleitet.

[0016] Dieses Einleiten oder der Beginn des Authentifizierungsverfahrens kann dabei sehr frühzeitig geschehen. Auf diese Weise ist es dann möglich, dass das erste und das zweite Authentifizierungsergebnis bereits vorliegen, wenn die Person mit dem mobilen Endgerät die Kontrollstation mit dem zweiten Sicherheitsniveau erreicht.

[0017] Als zweckmäßig hat sich der Einsatz von aus Authentifikationsschemata erwiesen, die biometrische Verfahren verwenden. Somit ist es bevorzugt, wenn die mittels des Sensors erfassten personenspezifischen Daten und/oder die mittels des Weiteren Sensors erfassten personenspezifischen weiteren Daten biometrische Daten, insbesondere solche der Person sind.

[0018] Handelt es sich beispielsweise beim Sensor um die Kamera des mobilen Endgeräts, so kann diese zur Erfassung von Gesichtsbildern oder auch zur Gangerkennung genutzt werden. Es kann aber auch beim mobilen Endgerät ein Fingerabdrucksensor vorhanden sein, der bereits in der Tasche genutzt werden kann, wobei auch die Eingabe von geeigneten Wischmustern für die Authentifizierung genutzt wird. Der weitere Sensor kann ebenfalls eine Kamera sein, die aber geräteextern, also außerhalb des mobilen Endgeräts, positioniert ist und vorzugsweise einer der Kontrollstationen zugeordnet wurde. Auch diese Kamera kann biometrische Informationen der zu authentifizierenden Person erfassen, wie beispielsweise das Gesicht oder auch den Gang. Auf diese Weise ist es zudem möglich, eine sogenannte "Presentation-Attack-Detection" durchzuführen, sollte ein unbefugter Dritter unerwünscht Zutritt verlangen.

[0019] Die vorstehend in der Beschreibung genannten Merkmale und Merkmalskombinationen sowie die nachfolgend in der Figurenbeschreibung genannten und/oder in den Figuren alleine gezeigten Merkmale und Merkmalskombinationen sind nicht nur in der jeweils angegebenen Kombination, sondern auch in anderen Kombinationen oder in Alleinstellung verwendbar, ohne den Rahmen der Erfindung zu verlassen. Es sind somit auch Ausführungen als von der Erfindung umfasst und offenbart anzusehen, die in den Figuren nicht explizit gezeigt oder erläutert sind, jedoch durch separierte Merkmalskombinationen aus den erläuterten Ausführungen hervorgehen und erzeugbar sind.

[0020] Weitere Vorteile, Merkmale und Einzelheiten der Erfindung ergeben sich aus den Ansprüchen, der nachfolgenden Beschreibung bevorzugter Ausführungsformen sowie anhand der Zeichnung. Dabei zeigen:

Fig. 1 eine schematische Darstellung des Zugangskontrollsystems, wobei die zu authentifizierende Person einmal an einer Zugangskontrollstation mit einem ersten Sicherheitsniveau und einmal an einer Zugangskontrollstation mit einem zweiten Sicherheitsniveau gezeigt ist, und

Fig. 2 eine schematische Illustration des Verfahrens zur Authentifizierung der Person mithilfe des Zugangskontrollsystems nach Figur 1, wobei jede der Zugangskontrollstationen mit einer Türsteuerung versehen ist.

[0021] In der Figur 1 ist ein Zugangskontrollsystem 100 schematisch illustriert. Dieses Zugangskontrollsystem 100 umfasst eine Zugangskontrollstation 102 mit einem ersten Sicherheitsniveau und mindestens eine weitere Zugangskontrollstation 104 mit einem zweiten Sicherheitsniveau, wobei das zweite Sicherheitsniveau eine höhere Sicherheitsanforderung als das erste Sicherheitsniveau stellt. Außerdem ist eine Person 200 gezeigt, die ein dem Zugangskontrollsystem 100 zugehöriges mobiles Endgerät 106 mitführt. Bei diesem mobilen Endgerät 106 kann es sich beispielsweise um eine Smartwatch, ein Smartphone oder ein anderweitiges "Smartdevice" handeln. Jedenfalls umfasst das mobile Endgerät 106 einen oder mehrere Sensoren, die eingerichtet sind, Daten der Person 200 zu erfassen, welche in einen Speicher des mobilen Endgeräts 106 gespeichert werden, wobei in dem Speicher mindestens ein Vergleichsdatensatz für einen Abgleich der von den Sensoren erfassten Daten gespeichert ist. Das mobile Endgerät 106 des Zugangskontrollsystems 100 umfasst einen Prozessor, der dazu eingerichtet ist, die vom Sensor erfassten Daten und den mindestens einen Vergleichsdatensatz aus dem Speicher auszulesen und für eine Authentifizierung der Person 200 miteinander zu vergleichen. Das Zugangskontrollsystem 100 umfasst außerdem ein dezentrales Kommunikationssystem 108, welches aus einer Mehrzahl von Kommunikationsmodulen mit Kommunikationsschnittstellen besteht, wobei jede der Zugangskontrollstation 102, 104 und auch das mobile Endgerät 106 wenigstens eines der Kommunikationsmodule umfasst, wodurch das mobile Endgerät 106 und die Zugangskontrollstationen 102, 104 eingerichtet sind, zumindest zeitweise über eine Kommunikationsverbindung miteinander zu kommunizieren.

[0022] Wenn sich die Person 200 nun Zugang zu einem gesicherten Bereich verschaffen will, so erfolgt zunächst eine Authentifizierung an den Zugangskontrollstationen 102, 104, und zwar in Abhängigkeit ihres jeweils zugewiesenen Sicherheitsniveaus.

[0023] Gelangt die Person 200 mit ihrem mobilen Endgerät 106 zur ersten Zugangskontrollstation 102, so werden personenspezifisch Daten der Person 200 mittels des Sensors des mobilen Endgeräts 106 erfasst und die erfassten Daten mit den Werten des mindestens einen Vergleichsdatensatzes, der im Speicher des mobilen Endgeräts 106 hinterlegt ist, verglichen. Dies erfolgt immer dann, wenn sich die Person 200 mit dem mobilen Endgeräts 106 zumindest in der Nähe der Zugangskontrollstation 102 mit dem ersten Sicherheitsniveau befindet oder eine Bewegung des mobilen Endgeräts 106 zu der Zugangskontrollstation 102 mit dem ersten Sicherheitsniveau erfasst wird, wobei der Prozessor des mobilen Endgeräts 106 dann ein erstes erfolgreiches Authentifizierungsergebnis erstellt und gegebenenfalls im Speicher abgelegt, wenn eine Abweichung beim Vergleich der Daten hinter einem Schwellenwert zurückbleibt. Selbstverständlich wird auch dann ein erfolgreiches Authentifizierungsergebnis erstellt, wenn die Abweichung beim Vergleich der Daten sogar Null ist.

[0024] Die erfassten personenspezifischen Daten sind vorliegend biometrische Daten der Person 200. Hierfür kommen beispielsweise eine Gesichtserkennung oder auch ein Daktylogramm (Fingerabdruck) in Betracht. Ferner ist auch eine die Iridenerkennung möglich. Die vorliegende Erfindung ist nicht auf diese Erkennungsmethoden beschränkt, so dass auch weitere - hier nicht näher genannte - Methoden Einsatz finden können.

[0025] Zeitlich dem Erfassen der personenspezifi-

schen Daten mittels des Sensors vorangehend oder zeitlich diesem Erfassen nachfolgend oder sogar zeitgleich wird eine Kommunikationsverbindung zwischen dem mobilen Endgerät 106 und der Zugangskontrollstation 102 mit dem ersten Sicherheitsniveau aufgebaut. Anschließend wird das erste Authentifizierungsergebnis an die Zugangskontrollstation 102 mit dem ersten Sicherheitsniveau übertragen, wobei im Falle des Vorliegens von einem erfolgreichen ersten Authentifizierungsergebnis eine Freigabe durch die Zugangskontrollstation 102 mit dem ersten Sicherheitsniveau erteilt wird. Unter "Freigabe" kann vorliegend verstanden werden, dass die Zugangskontrollstation 102 eine entsprechende Türsteuerung 110 beauftragt, die Verriegelung der Zugangstüre zu öffnen, damit die Person 200 Zutritt oder Durchtritt durch die Türe erhält. Eine "Freigabe" kann aber auch eine bloße "Freischaltung" von Bedienelementen oder dergleichen sein, durch die sich beispielsweise dann eine Tür betätigen lässt.

[0026] Gelangt die Person 200 dann zur Zugangskontrollstation 104 mit dem zweiten Sicherheitsniveau, so werden hier wiederum weitere personenspezifischen Daten der Person 200 mittels eines weiteren Sensors erfasst, wobei sich die weiteren personenspezifischen Daten der Person 200 von den zuerst erfassten Personen spezifischen Daten unterscheiden, insbesondere weil vorliegend beispielhaft das Gesicht der Person 200 durch eine Schildkappe verdeckt ist.

[0027] Auch hier hat es sich als vorteilhaft erwiesen, wenn die weiteren personenspezifischen Daten ebenfalls biometrische Daten sind, so beispielsweise die Daten eines Fingerabdrucks oder die Daten des Gangmusters der Person, die sich auf die Zugangskontrollstation 104 mit dem zweiten Sicherheitsniveau zubewegt. Der weitere Sensor kann dabei geräteextern, also außerhalb des mobilen Endgeräts 106 angeordnet sein und ist hier beispielhaft als Kamera in der Figur gezeigt.

[0028] Die auf diese Weise erfassten weiteren Daten werden mit den Werten eines weiteren Vergleichsdatensatzes verglichen, insbesondere dann, wenn sich die Person 200 mit dem mobilen Endgerät 106 zumindest in der Nähe der Zugangskontrollstation mit dem zweiten Sicherheitsniveau befindet oder eine Bewegung des mobilen Endgeräts 106 zu der Zugangskontrollstation 104 mit dem zweiten Sicherheitsniveau erfasst wird. Der Prozessor des mobilen Endgeräts 106 erstellt dann ein erfolgreiches zweites Authentifizierungsergebnis, wenn eine Abweichung beim Vergleich der weiteren Daten hinter einem Schwellenwert zurückbleibt, oder wenn eine solche Abweichung sogar Null beträgt.

[0029] Zeitlich dem Erfassen der weiteren personenspezifischen Daten vorangehend, zeitlich diesem Erfassen nachfolgend oder auch zeitgleich mit dem Erfassen wird eine Kommunikationsverbindung zwischen dem mobilen Endgerät 106 und der Zugangskontrollstation 104 mit dem zweiten Sicherheitsniveau aufgebaut. Dann wird das erste Authentifizierungsergebnis, welches vorliegend an der ersten Zugangskontrollstation 102 mit dem ersten Sicherheitsniveau erfasst und zeitweise gespeichert wurde, an die Zugangskontrollstation 104 mit dem zweiten Sicherheitsniveau übertragen. Im Falle des Vorliegens von einem erfolgreichen ersten Authentifizierungsergebnis als auch des Vorliegens von einem erfolgreichen zweiten Authentifizierungsergebnis wird dann eine Freigabe durch die Zugangskontrollstation 104 mit dem zweiten Sicherheitsniveau erteilt. Auch diese Freigabe kann, wie beispielhaft gezeigt, wiederum an eine zweite Türsteuerung 112 übergeben werden, die die Verriegelung der Tür der zweiten Zugangskontrollstation 104 öffnet und der Person 200 den Durchtritt oder den Zugang gewährt.

[0030] Die Authentifizierungsergebnisse werden nur für eine vorbestimmte Zeitdauer im Speicher gespeichert oder vom Zugangskontrollsystem zentral zeitlich begrenzt verwahrt. Für eine Person 200, die auf diese Weise mehrere Zugangskontrollstationen 102, 104 überwinden muss, entfällt daher das Erfordernis wiederholter Authentifizierungsmaßnahmen entsprechend dem gewählten Sicherheitsniveau. Nach Ablauf der vorgegebenen Zeitdauer werden die Authentifizierungsergebnisses aber gelöscht und eine erneute Authentifizierung wird erforderlich (sogenanntes "session timeout").

[0031] Dennoch wird eine Authentifizierungshistorie in dem Speicher des mobilen Endgeräts 106 gespeichert, in welcher alle bisher durchgeführten Authentifizierungsverfahren / Authentifizierungsschemata enthalten sind. Auf diese Weise ist die vorteilhafte Möglichkeit gegeben, dass das mobile Endgerät 106 anhand der Authentifizierungshistorie automatisch das oder diejenigen Authentifizierungsverfahren zur Authentifizierung der Person 200 durchführt, welche an das Sicherheitsniveau der betreffenden Zugangskontrollstation 102, 104 angepasst ist oder angepasst sind. Um einen besonders schnellen Zutritt zu gesicherten Bereichen zu erhalten, kann vorgesehen sein, dass das mobile Endgerät 106 bei Erfassung einer vorgegebenen Position oder beim Erfassen eines vorgegeben Abstands von einer der Zugangskontrollstationen 102, 104 das oder die benötigten Authentifizierungsverfahren automatisch einleitet. Dieses Einleiten erfolgt dabei so frühzeitig, dass das erste Authentifizierungsergebnis bereits vorliegt, wenn die Person 200 mit dem mobilen Endgerät 106 die Kontrollstation 102 mit dem ersten Sicherheitsniveau erreicht. Das Einleiten des zweiten Authentifizierungsverfahrens erfolgt dabei ebenfalls so frühzeitig, dass das erste und das zweite Authentifizierungsergebnis bereits vorliegen, wenn die Person 200 mit dem mobilen Endgerät 106 die Kontrollstation mit dem zweiten Sicherheitsniveau erreicht.

[0032] In Figur 2 ist nochmals das Schema der Authentifizierung der Person 200 mit einem Zugangskontrollsystem 100 nach Figur 1 zu erkennen. In der ersten Zeile sind dabei die "Akteure" des Zugangskontrollsystems 100 aufgelistet. In den weiteren Zeilen ist die Authentifizierung an der Zugangskontrollstation 102 und die Authentifizierung an der Zugangskontrollstation 104 zu erkennen.

[0033] Gelangt die Person 200 mit dem mobilen Endgerät 106 an der Zugangskontrollstation 102 mit dem ersten Sicherheitsniveau an, so fragt das mobile Endgerät 106 den Benutzer 200, ob er das Durchführen einer Authentifizierung genehmigt (S100). Der Nutzer oder die Person 200 wird dann die Genehmigung erteilen (S200). Das mobile Endgerät 106 erbittet dann die Freigabe des Zutritts bei der Zugangskontrollstation 102 (S300). Die Zugangskontrollstation 102 fordert dann vom mobilen Endgerät 106 die Erfassung von biometrischen Daten, insbesondere des Gesichts der Person 200 (S400). Mit dem mobilen Endgerät 106 und dem darin als Kamera gebildeten Sensor wird dann ein Gesichtsbild aufgezeichnet, welches mit einem Vergleichsdatensatz zu Gesichtsbildern im Speicher verglichen wird (S500). Wenn der Vergleich erfolgreich ist, wird vom Prozessor des mobilen Endgeräts 106 ein erstes erfolgreiches Authentifizierungsergebnis (vorliegend in Form eines Authentifizierungsvektors) an die Zugangskontrollstation 102 mit dem ersten Sicherheitsniveau übertragen (S600). Die Zugangskontrollstation 102 erteilt dann die Freigabe, weil ein erfolgreiches erstes Authentifizierungsergebnis vorliegt (S700). Diese Freigabe wird beispielsweise an einem Display des mobilen Endgeräts 106 ausgegeben. Außerdem sendet die Zugangskontrollstation 102 dann auch einen entsprechenden Antrag an die erste Türsteuerung 110, mit der Bitte, die Verriegelung zu öffnen (S800). Die erste Türsteuerung 110 meldet dann den entriegelten Zustand an die Zugangskontrollstation 102 zurück und gegebenenfalls auch an das mobile Endgerät 106 (S900).

[0034] Nun kann die Person 200 einen ersten gesicherten Bereich betreten, der jedoch an der Zugangskontrollstation 104 mit dem zweiten Sicherheitsniveau endet.

[0035] Sobald das mobile Endgerät 106 an der Zugangskontrollstation 104 mit dem zweiten Sicherheitsniveau angelangt, wird hierbei der Benutzer 200 gefragt, ob die Bewegungsdaten genutzt werden dürfen, die beispielsweise von der der Zutrittskontrollstation 104 zugeordneten Kamera als weiterer Sensor erfasst wurden, um eine Authentifizierung durchzuführen (S11 00). Wenn die Person 200 Zutritt an der zweiten Zugangskontrollstation 104 begehrt, so wird der Benutzer 200 die Erlaubnis hierfür erteilen (S1200). Das mobile Endgerät 106 erbittet dann Zutritt an der zweiten Zugangskontrollstation 104 (S1300). Weil die Zugangskontrollstation 104 mit dem zweiten Sicherheitsniveau eine höhere Sicherheitsanforderung als das erste Sicherheitsniveau an der ersten Zugangskontrollstation 102 besitzt, fordert die Zutrittskontrollstation 104 mit dem zweiten Sicherheitsniveau zunächst das erste Authentifizierungsergebnis an (S1400). Im vorliegenden Fall wird das erste Authentifizierungsergebnis von der Zugangskontrollstation 102 angefordert. Alternativ wäre jedoch auch die Möglichkeit gegeben, dass das erste Authentifizierungsergebnis im Speicher des mobilen Endgeräts 106 hinterlegt ist, und von dort ausgelesen wird. Jedenfalls wird dann das erste Authentifizierungsergebnis an die Zugangskontrollstation 104 mit dem zweiten Sicherheitsniveau übergeben (S1500). Die Zugangskontrollstation 104 fordert außerdem die weiteren Daten vom mobilen Endgerät 106 an, welche hier beispielsweise Bewegungsdaten sind (S1600). Das mobile Endgerät 106 führt dann wiederum einen Vergleich der Bewegungsdaten mit einem weiteren Vergleichsdatensatz durch und übermittelt dann das zweite Authentifizierungsergebnis an die Zugangskontrollstation 104 mit dem zweiten Sicherheitsniveau (S1700). Ist das zweite Authentifizierungsergebnis als ein erfolgreiches Authentifizierungsergebnis gekennzeichnet, so wird der Zutritt gewährt, was entsprechend an das mobile Endgerät 106 zurückgemeldet wird (S1800). Anschließend wird auch eine Öffnungsanfrage an eine zweite Türsteuerung 112 der Zugangskontrollstation 104 mit dem zweiten Sicherheitsniveau gestellt (S1900). Die zweite Türsteuerung meldet dann den Status über die erfolgte Entriegelung an die Zugangskontrollstation 104 zurück (S2000). Auf diese Weise erhält also die Person 200 dann auch Zugang zum gesicherten Bereich der zweiten Zugangskontrollstation 104.

[0036] Im Ergebnis zeichnet sich die vorliegende Erfindung durch ein verbessertes und beschleunigtes Verfahren zur Authentifizierung einer Person an einer Vielzahl von Zugangskontrollstationen 102, 104 aus, da vorangehende Authentifizierungen für spätere Zutrittskontrollen mit erhöhtem Sicherheitsniveau genutzt werden können.

BEZUGSZEICHENLISTE

[0037]

100	Zugangskontrollsystem
102	Zugangskontrollstation (erstes Sicherheitsniveau)
104	Zugangskontrollstation (zweites Sicherheitsniveau)
106	mobiles Endgerät (z.B. Smartphone, Smartwatch, etc.)
108	Kommunikationssystem
110	erste Türsteuerung
112	zweite Türsteuerung
200	Person

Patentansprüche

1. Verfahren zur Authentifizierung einer Person (200) mithilfe eines Zugangskontrollsystems (100), wobei

das Zugangskontrollsystem (100) umfasst

- eine Zugangskontrollstation (102) mit einem ersten Sicherheitsniveau;
- mindestens eine weitere Zugangskontrollstation (104) mit einem zweiten Sicherheitsniveau, wobei das zweite Sicherheitsniveau eine höhere Sicherheitsanforderung als das erste Sicherheitsniveau stellt;
- ein von der Person (200) mitgeführtes mobiles Endgerät (106), welches einen Sensor umfasst, der eingerichtet ist, Daten der Person (200) zu erfassen, die in einen Speicher des mobilen Endgeräts (106) gespeichert werden, wobei in dem Speicher mindestens ein Vergleichsdatensatz für einen Abgleich der vom Sensor erfassten Daten gespeichert ist, und welches einen Prozessor umfasst, der dazu eingerichtet ist, die vom Sensor erfassten Daten und den mindestens einen Vergleichsdatensatz aus dem Speicher auszulesen und für eine Authentifizierung miteinander zu vergleichen; und
- ein zentrales Kommunikationssystem (108), welches aus einer Mehrzahl von Kommunikationsmodulen mit Kommunikationsschnittstellen besteht, wobei jede der Zugangskontrollstationen (102, 104) und das mobile Endgerät (106) wenigstens eines der Kommunikationsmodule umfasst, wodurch das mobile Endgerät (106) und die Zugangskontrollstationen (102, 104) eingerichtet sind, zumindest zeitweise über eine Kommunikationsverbindung miteinander zu kommunizieren;

wobei das Verfahren die folgenden Schritte umfasst:

- Erfassen von personenspezifischen Daten der Person (200) mittels des Sensors und Vergleichen der erfassten Daten mit den Werten des mindestens einen Vergleichsdatensatzes, wenn sich die Person (200) mit dem mobilen Endgerät (106) zumindest in der Nähe der Zugangskontrollstation (102) mit dem ersten Sicherheitsniveau befindet oder eine Bewegung des mobilen Endgeräts (106) zu der Zugangskontrollstation (102) mit dem ersten Sicherheitsniveau erfasst wird, wobei der Prozessor des mobilen Endgeräts (106) dann ein erstes erfolgreiches Authentifizierungsergebnis erstellt, wenn eine Abweichung beim Vergleich der Daten hinter einem Schwellenwert zurückbleibt;
- Aufbauen der Kommunikationsverbindung zwischen dem mobilen Endgerät (106) und der Zugangskontrollstation (102) mit dem ersten Sicherheitsniveau;
- Übertragen des ersten Authentifizierungsergebnisses an die Zugangskontrollstation (102) mit dem ersten Sicherheitsniveau, wobei im Falle des Vorliegens von einem erfolgreichen ersten Authentifizierungsergebnis eine Freigabe durch die Zugangskontrollstation (102) mit dem ersten Sicherheitsniveau erteilt wird;
- Erfassen von weiteren personenspezifischen Daten der Person (200) mittels eines weiteren Sensors, wobei sich die weiteren personenspezifischen Daten der Person (200) von den zuerst erfassten personenspezifischen Daten unterscheiden, Vergleichen der erfassten weiteren Daten mit den Werten eines weiteren Vergleichsdatensatzes, wenn sich die Person (200) mit dem mobilen Endgerät (106) zumindest in der Nähe der Zugangskontrollstation (104) mit dem zweiten Sicherheitsniveau befindet oder eine Bewegung des mobilen Endgeräts (106) zu der Zugangskontrollstation (104) mit dem zweiten Sicherheitsniveau erfasst wird, wobei der Prozessor des mobilen Endgeräts (106) dann ein erfolgreiches zweites Authentifizierungsergebnis erstellt, wenn eine Abweichung beim Vergleich der weiteren Daten hinter einem Schwellenwert zurückbleibt;
- Aufbauen der Kommunikationsverbindung zwischen dem mobilen Endgerät (106) und der Zugangskontrollstation (104) mit dem zweiten Sicherheitsniveau; und
- Übertragen des ersten Authentifizierungsergebnisses an die Zugangskontrollstation (104) mit dem zweiten Sicherheitsniveau, wobei im Falle des Vorliegens sowohl von einem erfolgreichen ersten Authentifizierungsergebnis als auch von einem erfolgreichen zweiten Authentifizierungsergebnis eine Freigabe durch die Zugangskontrollstation (104) mit dem zweiten Sicherheitsniveau erteilt wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** das Erfassen der weiteren personenspezifischen Daten durch den weiteren Sensor erfolgt, welcher zumindest einer der Zugangskontrollstationen (102, 104) zugeordnet ist.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** das erfolgreiche erste Authentifizierungsergebnis vom Kommunikationsmodul der Zugangskontrollstation (102) mit dem ersten Sicherheitsniveau an das Kommunikationsmodul der Zugangskontrollstation (104) mit dem zweiten Sicherheitsniveau unmittelbar übertragen wird.

4. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** das erfolgreiche erste Authentifizierungsergebnis im Speicher des mobilen Endgeräts (106) abgespeichert wird, und dass das erfolgreiche erste Authentifizierungsergebnis vom Kommunikationsmodul des mobilen Endgeräts (106) an das Kommunikationsmodul der Zugangs-

kontrollstation (104) mit dem zweiten Sicherheitsniveau unmittelbar übertragen wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, dass** in dem Speicher eine Authentifizierungshistorie gespeichert wird, in welcher alle bisher durchgeführten Authentifizierungsverfahren enthalten sind.

6. Verfahren nach Anspruch 5, **dadurch gekennzeichnet, dass** das mobile Endgerät (106) anhand der Authentifizierungshistorie automatisch das oder diejenigen Authentifizierungsverfahren zur Authentifizierung der Person (200) durchführt, welche an das Sicherheitsniveau der betreffenden Zugangskontrollstation (102, 104) angepasst sind.

7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet, dass** das mobile Endgerät (106) bei Erfassung einer vorgegebenen Position oder beim Erfassen eines vorgegeben Abstands von einer der Zugangskontrollstationen (102, 104) das oder die benötigten Authentifizierungsverfahren automatisch einleitet.

8. Verfahren nach Anspruch 6 oder 7, **dadurch gekennzeichnet, dass** das erste Authentifizierungsergebnis bereits vorliegen, wenn die Person (200) mit dem mobilen Endgerät (106) die Kontrollstation (102) mit dem ersten Sicherheitsniveau erreicht.

9. Verfahren nach einem der Ansprüche 6 bis 8, **dadurch gekennzeichnet, dass** das erste und das zweite Authentifizierungsergebnis bereits vorliegt, wenn die Person (200) mit dem mobilen Endgerät (106) die Kontrollstation (104) mit dem zweiten Sicherheitsniveau erreicht.

10. Verfahren nach einem der Ansprüche 1 bis 9, **dadurch gekennzeichnet, dass** die mittels des Sensors erfassten personenspezifischen Daten und/oder die mittels des weiteren Sensors erfassten personenspezifischen weiteren Daten biometrische Daten sind.

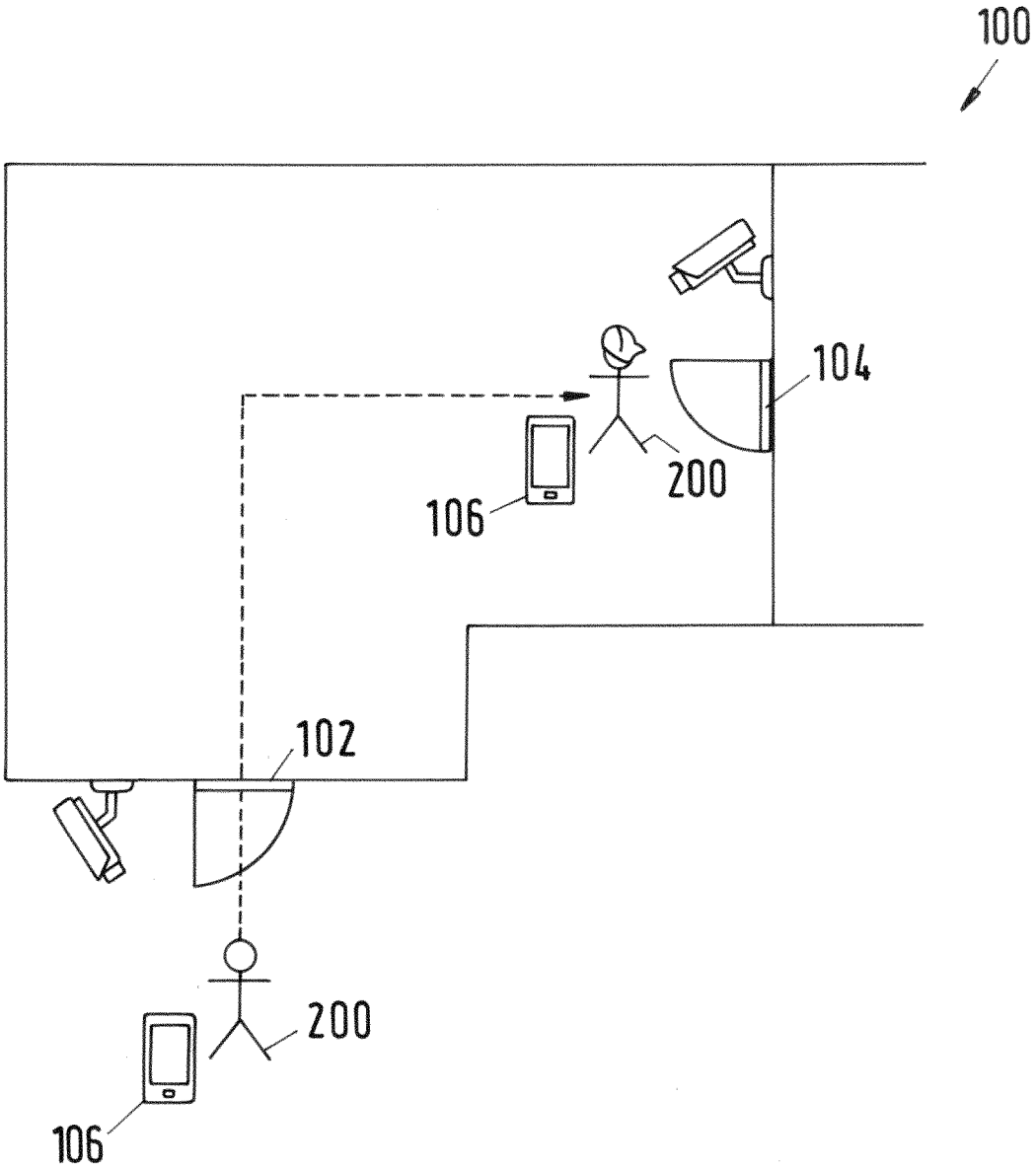

Fig.1

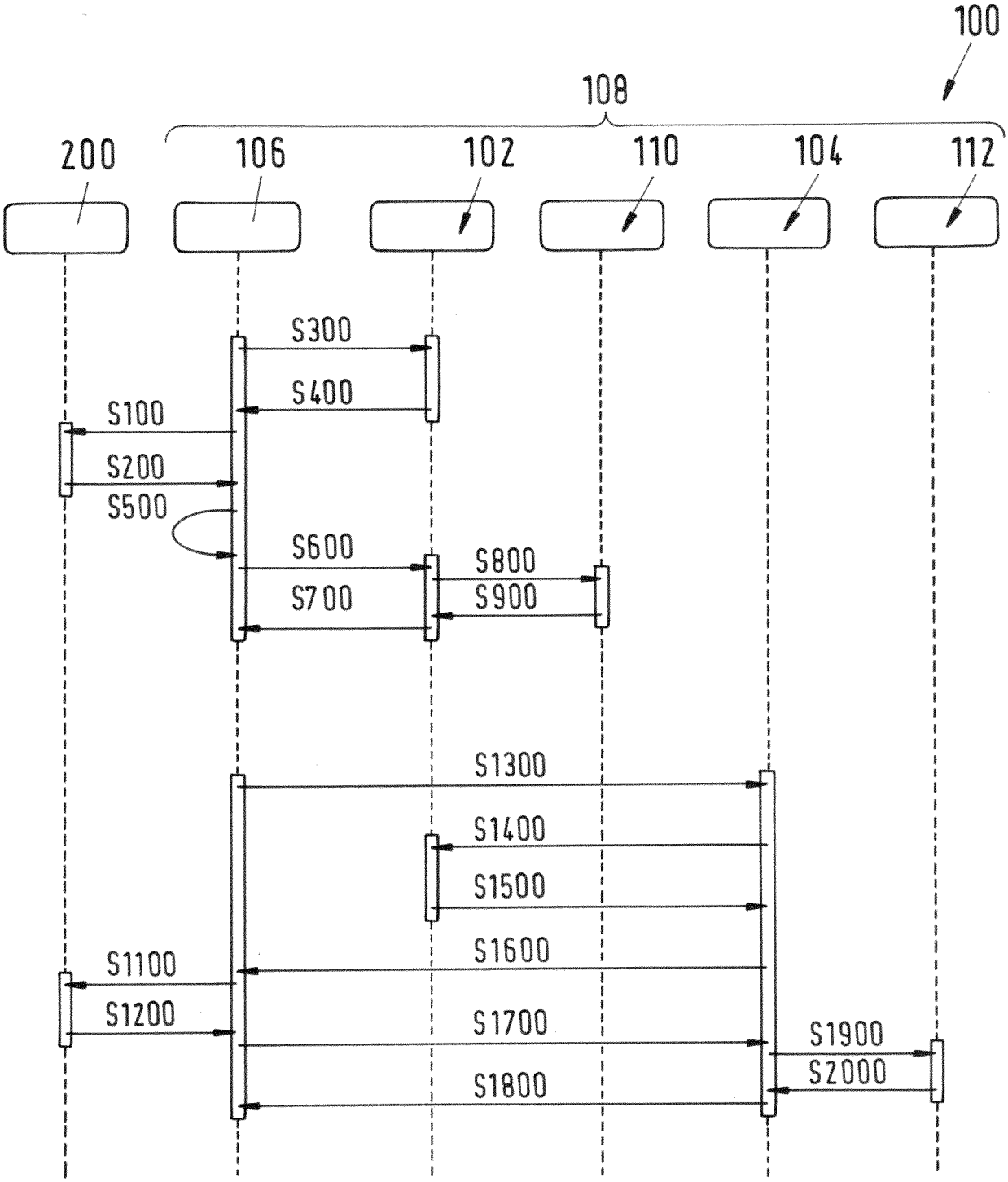
100
108
200
106
102
110
104
112
S300
S400
S100
S200
S500
S600
S700
S800
S900
S1300
S1400
S1500
S1600
S1100
S1200
S1700
S1900
S2000
S1800

Fig.2

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 23 20 5102

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	DE 10 2010 031932 A1 (SIEMENS AG [DE]) 26. Januar 2012 (2012-01-26) * Zusammenfassung; Abbildungen 1-3 * * Ansprüche 1-4 * * Absatz [0007] - Absatz [0022] *	1-10	INV. G07C9/25 G07C9/26
A,D	DE 10 2017 208234 A1 (BUNDESDRUCKEREI GMBH [DE]) 22. November 2018 (2018-11-22) * Absatz [0160] - Absatz [0161] *	1-10	
A	US 2021/134096 A1 (PUKARI MIKA [FI]) 6. Mai 2021 (2021-05-06) * Zusammenfassung * * Absatz [0032] - Absatz [0033] *	1-10	

RECHERCHIERTE SACHGEBIETE (IPC)

G07C

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	19. März 2024	Holzmann, Wolf

KATEGORIE DER GENANNTEN DOKUMENTE

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

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

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 23 20 5102

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

19-03-2024

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 102010031932 A1	26-01-2012	KEINE	
DE 102017208234 A1	22-11-2018	DE 102017208234 A1	22-11-2018
		EP 3404570 A1	21-11-2018
		PT 3404570 T	10-11-2021
US 2021134096 A1	06-05-2021	KEINE	

EPO FORM P0461

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

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

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

In der Beschreibung aufgeführte Patentdokumente

- DE 102017208234 A1 **[0003]**