(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) **CH 717 006 A2**

(51) Int. Cl.: **G06F 21/32** (2013.01)
G07D 7/00 (2016.01)
G06K 7/14 (2006.01)
G06K 9/00 (2006.01)
G06K 9/22 (2006.01)

Patentanmeldung für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTANMELDUNG

(21) Anmeldenummer: 01621/20

(22) Anmeldedatum: 18.12.2020

(43) Anmeldung veröffentlicht: 30.06.2021

(30) Priorität: 20.12.2019 CH 01690/19

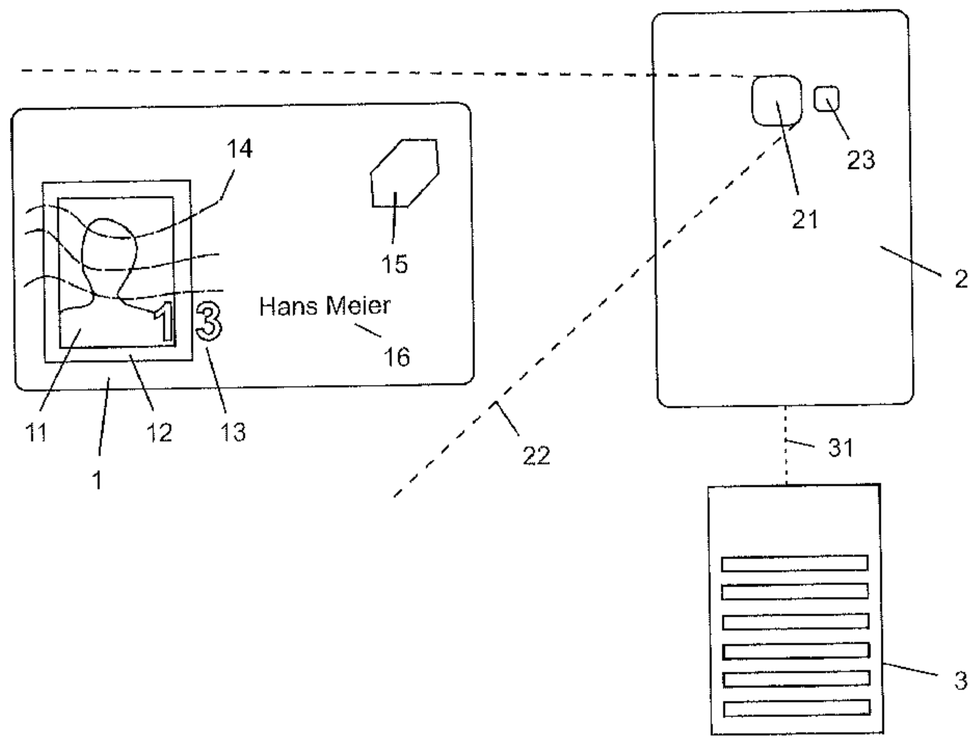
(71) Anmelder:
ti&m products AG, Buckhauserstrasse 24
8048 Zürich (CH)

(72) Erfinder:
Der Erfinder hat auf Nennung verzichtet

(74) Vertreter:
E. Blum & Co. AG Patent- und Markenanwälte VSP,
Vorderberg 11
8044 Zürich (CH)

(54) Verfahren zur Benutzeridentifikation.

(57) Ein computerimplementiertes Verfahren zur Identifikation eines Benutzers anhand eines Identifikationsdokuments (1) umfasst die folgenden Schritte: Empfangen von ersten Daten von einem Endgerät (2) auf einem Identifizierungsserver (3), wobei die ersten Daten ein Lichtbild (11) des Benutzers und ein Sicherheitsmerkmal umfassen; Prüfen einer Echtheit des Identifikationsdokuments (1) anhand des Sicherheitsmerkmals; Empfangen von zweiten Daten von dem Endgerät (2) auf dem Identifizierungsserver (3), wobei die zweiten Daten eine Gesichtspartie des Benutzers abbilden; Prüfen einer Übereinstimmung des Benutzers mit einem Inhaber des Identifikationsdokuments (1) durch Bestimmen einer Ähnlichkeit zwischen dem Lichtbild (11) und der Gesichtspartie des Benutzers; bei positiven Ergebnissen der Prüfungen Anerkennen der Identifikation des Benutzers als korrekt durch den Identifizierungsserver (3).



Beschreibung

Gebiet der Erfindung

[0001] Die Erfindung betrifft ein computerimplementiertes Verfahren zur Identifikation eines Benutzers anhand eines Identifikationsdokuments sowie ein zugehöriges System.

Hintergrund

[0002] Bei Vorgängen oder Handlungen, zu denen nur eine bestimmte Person berechtigt ist oder bei der die Feststellung der Identität einer Person zentral ist, stellt sich regelmässig das Problem der Identifikation der Person. Beispiele sind das Eröffnen eines Bankkontos, das Erwerben einer SIM-Karte für Mobiltelefone oder die Ausführung bestimmter Dienstleistungen bei öffentlichen Behörden. Herkömmlich wird die Identifikation in Anwesenheit der Person und mithilfe eines Identifikationsdokuments, z.B. einer ID-Karte, eines Personalausweises oder eines Passes, durchgeführt.

[0003] Bei einer Identifikation ohne Anwesenheit der Person, z.B. über Internet, besteht eine Herausforderung darin, die Identität der Person auch ohne Augenschein der Person und des Identifikationsdokuments sicher und zweifelsfrei feststellen zu können. Insbesondere sollte ein Verfahren zur Identifikation also möglichst wenige Möglichkeiten zur Manipulation bieten.

[0004] Es ist daher eine Aufgabe der vorliegenden Erfindung, ein Verfahren bereitzustellen, mit dem eine Person sicher und zweifelsfrei identifiziert werden kann, auch wenn die Person nicht von einer anderen Person durch Augenschein identifiziert werden kann.

Darstellung der Erfindung

[0005] Die Aufgabe wird gelöst durch ein computerimplementiertes Verfahren zur Identifikation eines Benutzers anhand eines Identifikationsdokuments nach Anspruch 1. Unter Identifikation wird dabei insbesondere die Feststellung der Identität des Benutzers verstanden oder in anderen Worten die Überprüfung, dass der Benutzer derjenige ist, der er zu sein vorgibt. Das Identifikationsdokument kann z.B. eine ID-Karte, ein Personalausweis, ein biometrischer Ausweis, ein Pass oder ein Führerausweis sein.

[0006] Das Verfahren umfasst die folgenden Schritte, insbesondere in der angegebenen Reihenfolge:

- Empfangen von ersten Daten von einem Endgerät auf einem Identifizierungsserver, wobei die ersten Daten ein Lichtbild des Benutzers und ein Sicherheitsmerkmal umfassen: Das Endgerät ist bevorzugt ein bei vielen Benutzern verfügbares Gerät, z.B. ein Mobiltelefon, ein Notebook oder ein Desktop-PC mit einer Kamera zum Aufnehmen von Bilddaten. Der Identifizierungsserver umfasst bevorzugt ein System zur Datenverarbeitung bei einer an der Identifikation interessierten Partei oder bei einem externen Dienstleister. Das Lichtbild ist üblicherweise ein Porträt oder Passfoto eines Inhabers des Identifikationsdokuments. Insbesondere sind das Lichtbild und das Sicherheitsmerkmal integrale Bestandteile des Identifikationsdokuments.

[0007] In einer Ausführungsform sind die ersten Daten zumindest teilweise auf einem Chip des Identifikationsdokuments gespeichert, z.B. auf einem biometrischen Ausweis oder Pass. Das Sicherheitsmerkmal kann eine elektronische Signatur, insbesondere eine digitale Signatur, umfassen. Die ersten Daten mit Lichtbild und Sicherheitsmerkmal sind dann bevorzugt durch das Endgerät digital auslesbar. Zu diesem Zweck weist das Endgerät z.B. einen NFC-Sensor auf.

- Prüfen einer Echtheit des Identifikationsdokuments anhand des Sicherheitsmerkmals: Im Fall, dass das Sicherheitsmerkmal eine elektronische Signatur umfasst, ist es sinnvoll, dass dieser Schritt das Prüfen einer Authentizität und Integrität der ersten Daten anhand der elektronischen Signatur umfasst. Authentizität meint dabei insbesondere, dass die ersten Daten tatsächlich von einem vorgeblichen Aussteller des Identifikationsdokuments stammen, z.B. von einer Pass-Ausstellungsbehörde. Integrität meint insbesondere, dass die ersten Daten nicht manipuliert wurden, also insbesondere noch die originalen Daten sind, die der Aussteller auf dem Chip abgespeichert hat. Zum Prüfen der Echtheit kann insbesondere die digitale Signatur verwendet werden. Ein zur Prüfung der elektronischen oder digitalen Signatur notwendiges Zertifikat kann beispielsweise für Schweizer Pässe auf der Webseite des Bundesamts für Informatik und Telekommunikation bezogen werden. Generell bilden die Signatur und das Zertifikat zusammen eine „Trust Chain“, bei der das eine Ende sicher bei der Ausstellungsbehörde des Identifikationsdokuments verankert und das andere Ende sicher auf dem Identifikationsdokument gespeichert ist
- Empfangen von zweiten Daten von dem Endgerät auf dem Identifizierungsserver, wobei die zweiten Daten eine Gesichtspartie des Benutzers abbilden: Die zweiten Daten umfassen also insbesondere eine Abbildung, die zumindest einen Teil des Gesichts des Benutzers zeigt. Bevorzugt werden die zweiten Daten während des Durchlaufens des Verfahrens zur Identifikation generiert. Insbesondere umfassen die zweiten Daten also eine fotografische Aufnahme mit einer Gesichtspartie, die der Benutzer zur Laufzeit des Verfahrens von sich selbst erstellt, vorteilhafterweise mit der Kamera des Mobilfunkgeräts.

[0008] Zur Verhinderung von Manipulationen ist es weiterhin vorteilhaft, dass bei der Erstellung der zweiten Daten eine Liveness Detection durchgeführt wird, dass also insbesondere festgestellt wird, dass die zweiten Daten tatsächlich die

Gesichtspartie des Benutzers zum aktuellen Zeitpunkt abbilden. Damit kann z.B. vermieden werden, dass als zweite Daten ein Foto des Inhabers des Identifikationsdokuments übermittelt wird, der aber nicht mit dem Benutzer übereinstimmt.

- Prüfen einer Übereinstimmung des Benutzers mit einem Inhaber des Identifikationsdokuments durch Bestimmen einer Ähnlichkeit zwischen dem Lichtbild und der Gesichtspartie des Benutzers: Die Ähnlichkeit wird insbesondere durch Verfahren der Bildverarbeitung bestimmt, z.B. durch eine Korrelation, durch Feature Detection oder durch eine Distanz-Metrik, ermittelt mit statistischen Methoden, z.B. neuronalen Netzen.
- bei positiven Ergebnissen der Prüfungen Anerkennen der Identifikation des Benutzers als korrekt durch den Identifizierungsserver: Die Prüfungen beziehen sich insbesondere auf das Prüfen einer Echtheit des Identifikationsdokuments sowie das Prüfen einer Übereinstimmung des Benutzers mit dem Inhaber des Identifikationsdokuments wie oben beschrieben. Weitere Prüfungen, die vorteilhafterweise vor der Anerkennung der Identifikation als korrekt durchgeführt werden, sind unten als bevorzugte Ausführungsformen beschrieben. Wenn die Identifikation des Benutzers als korrekt anerkannt wird, gibt der Identifizierungsserver bevorzugt ein Signal aus, das die korrekte Identifikation bestätigt und insbesondere eine Voraussetzung für weitere Schritte wie beispielsweise das Eröffnen eines Bankkontos ist.

[0009] Ein solches Verfahren hat den Vorteil, dass der Benutzer sich von einem entfernten Platz aus identifizieren kann. Insbesondere muss der Benutzer z.B. beim Eröffnen eines Bankkontos also nicht vor Ort in eine Bankfiliale gehen, sondern kann die Identifikation zeitsparend mithilfe seines Identifikationsdokuments und seines Endgeräts, z.B. ein Smartphone, durchführen.

[0010] In dem Fall, dass das Sicherheitsmerkmal eine elektronische Signatur umfasst, die auf dem Chip des Identifikationsdokuments gespeichert ist, ist die Sicherheit des Verfahrens weiter erhöht, da die elektronische Signatur ein zusätzliches Sicherheitsmerkmal darstellt, das schwer zu fälschen oder manipulieren ist. Durch Einbeziehen der elektronischen Signatur, die auf dem Chip gespeichert ist, entfallen beim Prüfen des Identifikationsdokuments bei der Online-Identifikation in einigen Ländern, z.B. der Schweiz, Sicherheitsmassnahmen wie ein Kontoübertrag von z.B. 1 Rappen, die ansonsten vom Regulator vorgeschrieben sind.

[0011] Das obige Verfahren kann aber auch mit einem optischen Sicherheitsmerkmal durchgeführt werden, wie im Folgenden beschrieben, oder eine Kombination von optischem Sicherheitsmerkmal und elektronischer Signatur als Sicherheitsmerkmal umfassen.

[0012] In einer Ausführungsform umfasst das Verfahren, insbesondere nach Anspruch 3, die folgenden Schritte, insbesondere in der angegebenen Reihenfolge:

- Empfangen von ersten Daten, insbesondere ersten Bilddaten, von einem Endgerät auf einem Identifizierungsserver, wobei die ersten Bilddaten mindestens einen Teil des Identifikationsdokuments mit einem Lichtbild und einem Sicherheitsmerkmal, insbesondere optischen Sicherheitsmerkmal, abbilden: Das Endgerät ist bevorzugt ein bei vielen Benutzern verfügbares Gerät, z.B. ein Mobiltelefon, ein Notebook oder ein Desktop-PC mit einer Kamera zum Aufnehmen von Bilddaten. Der Identifizierungsserver umfasst bevorzugt ein System zur Datenverarbeitung bei einer an der Identifikation interessierten Partei oder bei einem externen Dienstleister. In einer Ausführungsform umfassen die ersten Bilddaten eine fotografische Aufnahme einer Seite des Identifikationsdokuments. Unter Sicherheitsmerkmal wird ein Merkmal des Identifikationsdokuments verstanden, das die Echtheit des Identifikationsdokuments nachweist, insbesondere da es für Unberechtigte schwer zu reproduzieren oder zu manipulieren ist. Typische optische Sicherheitsmerkmale sind eine Gravur, eine Prägung, ein Sicherheitsfaden, ein Kinegramm, ein Hologramm oder ein optically variable device (OVD).
- Prüfen einer Echtheit des Identifikationsdokuments durch Vergleichen des in den ersten Bilddaten abgebildeten Sicherheitsmerkmals mit allgemeingültigen Eigenschaften des Sicherheitsmerkmals: Das Sicherheitsmerkmal zeichnet sich vorteilhafterweise durch eine Eigenschaft aus, die schwer, also nur mit grossem Aufwand, reproduzierbar oder manipulierbar ist und die der Allgemeinheit oder zumindest geschultem Personal bekannt ist, sodass das Vorhandensein der Eigenschaft leicht geprüft werden kann. Die Eigenschaft kann z.B. eine Beschaffenheit des Materials sein oder ein Erscheinungsbild des Sicherheitsmerkmals. In anderen Worten sind die allgemeingültigen Eigenschaften mit der Definition des Sicherheitsmerkmals durch einen Herausgeber des Sicherheitsmerkmals gegeben oder folgen direkt aus der Definition. Die allgemeingültigen Eigenschaften sind also insbesondere in jedem Sicherheitsmerkmal, das der Definition folgt, verwirklicht.
- Extrahieren des Lichtbilds aus den ersten Bilddaten: Das Lichtbild ist üblicherweise ein Porträt oder Passfoto eines Inhabers des Identifikationsdokuments. In einer Ausführungsform wird das Lichtbild durch ein Bildverarbeitungsverfahren, z.B. Kantenerkennung oder Klassifikation, aus den ersten Bilddaten, insbesondere dem Foto, extrahiert. Das Extrahieren des Lichtbilds kann auf dem Identifizierungsserver oder auf dem Endgerät durchgeführt werden. Auch kann der Schritt des Extrahierens zu einem anderen Zeitpunkt, also z.B. bereits vor dem Empfangen der ersten Bilddaten oder nach dem folgenden Schritt, durchgeführt werden.
- Empfangen von zweiten Daten, insbesondere zweiten Bilddaten, von dem Endgerät auf dem Identifizierungsserver, wobei die zweiten Bilddaten eine Gesichtspartie des Benutzers abbilden: Die zweiten Bilddaten umfassen also insbesondere ein Abbildung, das zumindest einen Teil des Gesichts des Benutzers zeigt. Bevorzugt werden die zweiten Bilddaten während des Durchlaufens des Verfahrens zur Identifikation generiert. Insbesondere umfassen die zweiten Bilddaten also eine fotografische Aufnahme mit einer Gesichtspartie, die der Benutzer zur Laufzeit des Verfahrens von sich selbst erstellt, vorteilhafterweise mit der Kamera des Mobilfunkgeräts. Zur Verhinderung von Manipulationen

ist es weiterhin vorteilhaft, dass bei der Erstellung der zweiten Bilddaten eine Liveness Detection durchgeführt wird, dass also insbesondere festgestellt wird, dass die zweiten Bilddaten tatsächlich die Gesichtspartie des Benutzers zum aktuellen Zeitpunkt abbilden. Damit kann z.B. vermieden werden, dass als zweite Bilddaten ein Foto des Inhabers des Identifikationsdokuments übermittelt wird, der aber nicht mit dem Benutzer übereinstimmt.

– Prüfen einer Übereinstimmung des Benutzers mit dem Inhaber des Identifikationsdokuments durch Bestimmen einer Ähnlichkeit zwischen dem Lichtbild und der Gesichtspartie des Benutzers: Die Ähnlichkeit wird insbesondere durch Verfahren der Bildverarbeitung bestimmt, z.B. durch eine Korrelation, durch Feature Detection oder durch eine Distanz-Metrik, ermittelt mit statistischen Methoden, z.B. neuronalen Netzen.
– bei positiven Ergebnissen der Prüfungen Anerkennen der Identifikation des Benutzers als korrekt durch den Identifizierungsserver: Die Prüfungen beziehen sich insbesondere auf das Prüfen einer Echtheit des Identifikationsdokuments sowie das Prüfen einer Übereinstimmung des Benutzers mit dem Inhaber des Identifikationsdokuments wie oben beschrieben. Weitere Prüfungen, die vorteilhafterweise vor der Anerkennung der Identifikation als korrekt durchgeführt werden, sind unten als bevorzugte Ausführungsformen beschrieben. Wenn die Identifikation des Benutzers als korrekt anerkannt wird, gibt der Identifizierungsserver bevorzugt ein Signal aus, das die korrekte Identifikation bestätigt und insbesondere eine Voraussetzung für weitere Schritte wie das Eröffnen eines Bankkontos ist.

Vorteilhafte Ausführungsformen umfassen die folgenden Merkmale:

[0013] In einer Ausführungsform umfasst das Verfahren weiterhin die Schritte

– Bestimmen von Identitätsdaten aus den ersten Bilddaten: Identitätsdaten können z.B. ein Name, eine Adresse, ein Geburtsdatum oder eine Identifikationsnummer des Inhabers des Identifikationsdokuments umfassen. Identitätsdaten können insbesondere über Bildverarbeitungsverfahren aus den ersten Bilddaten bestimmt werden, z.B. mit Texterkennung. Weiterhin kann unter diesen Schritt das Zuordnen von weiteren Identitätsdaten zu den direkt aus den Bilddaten bestimmten Identitätsdaten fallen, insbesondere indem die weiteren Identitätsdaten von einer Datenbank abgerufen werden, in der sie mit den bestimmten Identitätsdaten verknüpft sind.
– bei positiven Ergebnissen der Prüfungen Zuordnen der Identitätsdaten zum Benutzer: Wenn die Identitätsdaten aus den Bilddaten bestimmt werden, muss der Benutzer diese also insbesondere nicht erst zeitraubend eingeben. Dies ermöglicht ein zeitsparendes Feststellen der Identitätsdaten, insbesondere auch in standardisierter Form wie sie auf dem Identifikationsdokument und/oder in der Datenbank vorliegen.

[0014] In einer weiteren Ausführungsform umfasst das Verfahren zusätzlich die Schritte

– Bestimmen einer Art des Identifikationsdokuments: Die Art kann beispielsweise eine ID-Karte, ein Personalausweis, ein Pass oder auch ein Führerschein sein. Weiterhin kann die Art durch eine das Identifikationsdokument ausgebende Institution, z.B. eine nationale Behörde, gekennzeichnet sein. Die Bestimmung der Art kann wiederum über Bildverarbeitungsverfahren, z.B. Feature Detection und Klassifikation mit statistischen Modellen, oder auch banal über eine Benutzereingabe bestimmt werden.
– Laden der zur Art des Identifikationsdokuments gehörigen allgemeingültigen Eigenschaften des Sicherheitsmerkmals: Mit der Art des Identifikationsdokuments ist üblicherweise das Vorhandsein mindestens eines bestimmten Sicherheitsmerkmals in genau definierter Form verbunden. Somit können, wenn die Art bestimmt ist, die bei dieser Art vorhandenen Sicherheitsmerkmale und deren Eigenschaften z.B. aus einer Datenbank geladen werden.

[0015] Die nächsten beiden Ausführungsformen betreffen die Beschaffenheit des Sicherheitsmerkmals und wie diese in dem Verfahren zur Identifikation ausgenutzt werden können:

Bevorzugt ist das Sicherheitsmerkmal so beschaffen, dass es unter verschiedenen Blickwinkeln verschieden aussieht, insbesondere dass sich dabei eine Farbe oder eine in dem Sicherheitsmerkmal dargestellte Form ändert. Um dieses Merkmal prüfen zu können, umfassen die ersten Bilddaten mehrere Bilder des Sicherheitsmerkmals unter verschiedenen Blickwinkeln. Beispiele für ein solches Sicherheitsmerkmal sind ein Kinegramm, ein Hologramm oder ein OVD. Die mehreren Bilder unter verschiedenen Blickwinkeln werden insbesondere durch Kippen des Endgeräts relativ zum Identifikationsdokument oder durch Bewegen des Endgeräts relativ zum Identifikationsdokument zwischen den Bildern erreicht. Bevorzugt wird der Benutzer beim Aufnehmen der mehreren Bilder durch eine Ausgabe von Anweisungen auf dem Endgerät geführt.

[0016] Alternativ oder zusätzlich kann das Sicherheitsmerkmal des Identifikationsdokuments so beschaffen sein, dass es bei Veränderung einer Beleuchtung verschieden aussieht, insbesondere dass sich dabei eine Farbe oder eine in dem Sicherheitsmerkmal dargestellte Form ändert. Um dieses Merkmal prüfen zu können, umfassen die ersten Bilddaten mehrere Bilder des Sicherheitsmerkmals bei verschiedener Beleuchtung, insbesondere bei verschiedener Helligkeit der Beleuchtung. Beispiele für ein solches Sicherheitsmerkmal sind wiederum ein Kinegramm, ein Hologramm oder ein OVD. Bevorzugt wird also die Beleuchtung des Sicherheitselements zwischen der Aufnahme der Bilder geändert, sei es durch Dimmen oder An-/Abschalten einer Lichtquelle, durch Winkeländerung zum einfallenden Licht, durch eine Abstandsänderung zu einer Lichtquelle etc.

[0017] In einer Ausführungsform ist das Endgerät ein Mobilgerät mit einer Lichtquelle mit mindestens zwei Helligkeitsstufen. Mindestens zwei Bilder der ersten Bilddaten sind entsprechend bei verschiedenen Helligkeitsstufen der Lichtquelle aufgenommen. Da für viele Benutzer verfügbar, ist das Endgerät bevorzugt ein Mobiltelefon mit einem Blitz.

[0018] Weitere vorteilhafte Ausführungsformen zeichnen sich durch mindestens eine der folgenden Eigenschaften aus:

- das Sicherheitsmerkmal umfasst mindestens eines der folgenden Merkmale: einen Rahmen um das Lichtbild, ein Muster oder eine Gravur,
- das Sicherheitsmerkmal ist zumindest teilweise auf dem Lichtbild angebracht und umfasst insbesondere eines der oben genannten Merkmale,
- das Sicherheitsmerkmal umfasst ein OVD oder ein Kinegramm.

[0019] Ein weiterer Aspekt der Erfindung betrifft ein System zur Datenverarbeitung, insbesondere einen Identifizierungsserver, umfassend einen Prozessor, der so angepasst ist, dass er das beschriebene Verfahren ausführt. Noch weitere Aspekte beziehen sich auf ein Computerprogramm, umfassend Befehle, die bei der Ausführung des Programms durch einen Computer diesen veranlassen, das beschriebene Verfahren auszuführen, und ein Speichermedium mit dem Computerprogramm.

Kurze Beschreibung der Zeichnungen

[0020] Weitere Ausgestaltungen, Vorteile und Anwendungen der Erfindung ergeben sich aus den abhängigen Ansprüchen und aus der nun folgenden Beschreibung anhand der Figuren. Dabei zeigen:

Figur 1 ein Identifikationsdokument, ein Endgerät und einen Identifikationsserver in einer Ausführungsform der Erfindung;

Figur 2 ein Fliessdiagramm mit einem Verfahren zur Identifikation eines Benutzers gemäss einer Ausführungsform der Erfindung;

die Figuren 3 bis 5 jeweils ein Identifikationsdokument und ein Endgerät in weiteren Ausführungsformen der Erfindung;

Figur 6 ein Identifikationsdokument, ein Endgerät und einen Identifikationsserver in einer weiteren Ausführungsform der Erfindung;

Figur 7 ein Fliessdiagramm mit einem Verfahren zur Identifikation eines Benutzers gemäss einer weiteren Ausführungsform der Erfindung.

Wege zur Ausführung der Erfindung

[0021] Figur 1 zeigt Elemente, die in einem Verfahren gemäss einer Ausführungsform der Erfindung verwendet werden: eine Identitätskarte (ID-Karte, Identifikationsdokument) 1, ein Mobiltelefon (Endgerät) 2 und einen Server (Identifizierungsserver) 3. Die ID-Karte 1 ist beispielsweise die Schweizer ID und umfasst ein Passbild 11, einen Rahmen 12 um das Passbild 11, eine Gravur 13, z.B. die Zahl „13“, und ein Muster 14 aus Linien, die teilweise über das Passbild 11 verlaufen. Bestimmte Eigenschaften des Rahmens 12, der Gravur 13 und des Musters 14 sind vom Herausgeber der ID-Karte 1 genau definiert, z.B. die Art des Übergangs von Passbild 11 zu Rahmen 12, die Beschaffenheit und Anordnung der Gravur 13 und der Verlauf der Linien des Musters 14. Damit können diese Elemente als Sicherheitsmerkmale verwendet werden, anhand derer jedermann oder zumindest eine Person, welche die bestimmten Eigenschaften kennt, die Echtheit der ID-Karte 1 überprüfen kann.

[0022] Weiterhin umfasst die ID-Karte 1 in Figur 1 ein Kinegramm 15, dessen Form im Fall der Schweizer ID an einen Bergkristall erinnert. Das Kinegramm 15 dient ebenfalls als Sicherheitsmerkmal, da es definierte Eigenschaften aufweist und schwer zu reproduzieren ist. Ausserdem umfasst die ID-Karte 1 Identitätsdaten 16, im gezeigten Fall den Namen „Hans Meier“. Generell können auf der ID-Karte 1 zusätzlich oder alternativ auch andere Identitätsdaten 16 vermerkt sein, z.B. eine ID-Nummer oder Adresse. Vorteilhafterweise umfassen die Identitätsdaten 16 maschinenlesbare Zeichen, wie sie auf einem maschinenlesbaren Pass gemäss ICAO Standard Dokument 9303 bzw. ISO/IEC 7501-1 in einer dafür vorgesehenen maschinenlesbaren Zone (machine readable zone, MRZ) vorhanden sind. Auch kann die ID-Karte 1 eine andere Form haben und andere Elemente, insbesondere in anderer Anordnung, umfassen. Immer gleich sind hingegen die definierten und standardisierten Eigenschaften der ID-Karte 1 einer bestimmten Art, z.B. einer Schweizer ID, die eine Überprüfung auf Echtheit erst ermöglichen.

[0023] Das Mobiltelefon 2 in Figur 1 umfasst eine Kamera 21 zur Aufnahme von Bildern und/oder Videos in einem Sichtbereich 22 der Kamera 21 und einen Blitz (Lichtquelle) 23. Der Server 3 umfasst einen Prozessor zur Ausführung des Verfahrens sowie die dazu nötigen dauerhaften und vorübergehenden Speicher. Der Server 3 steht im Normalfall bei der Institution, die an der Identifikation des Benutzers interessiert ist, also im Fall einer Kontoeröffnung z.B. bei der Bank oder bei einer Behörde. Alternativ kann der Server 3 auch zu einem Dienstleister ausgelagert sein, welcher im Auftrag der

Institution die Identifikation durchführt und am Ende des Verfahrens an die Institution eine Information weitergibt, ob der Benutzer korrekt identifiziert wurde oder nicht. Der Server 3 hat zur Durchführung des Verfahrens eine Datenverbindung 31 zum Mobiltelefon 2, die insbesondere zur Übertragung von Bildern und/oder Videos geeignet ist und mindestens eine der folgenden Verbindungsarten umfasst: Mobilfunk, WLAN, Bluetooth, LAN, Ethernetkabel.

[0024] Ein Verfahren gemäss einer Ausführungsform der Erfindung, das mit der Anordnung von Figur 1 durchgeführt werden kann, ist in Figur 2 als Fliessdiagramm gezeigt. Der Benutzer, der sich gegenüber der Institution identifizieren möchte, macht in Schritt S1 mit der Kamera 21 des Mobiltelefons 2 ein erstes Bild von seiner ID-Karte 1, auf dem das Passbild 11 sowie zumindest eines der Sicherheitsmerkmale 12 bis 15 abgebildet ist. Das erste Bild wird vom Mobiltelefon 2 über die Datenverbindung 31 an den Server 3 geschickt und in Schritt S2 vom Server empfangen. In Schritt S3 wird auf dem Server 3 die Echtheit der ID-Karte 1 anhand von im ersten Bild abgebildeten Sicherheitsmerkmalen geprüft.

[0025] In einer Ausführungsform werden zur Prüfung in Schritt S3 die Sicherheitsmerkmale 12 bis 14 herangezogen, die im Zusammenhang mit dem Lichtbild 11 stehen. Insbesondere wird geprüft, ob alternativ oder kumulativ der Rahmen 12, die Gravur 13 und/oder das Muster 14 allgemeingültige Eigenschaften aufweist, die aus der Definition dieser Elemente folgen. Wenn dies nicht der Fall ist, wird die ID-Karte als unecht eingestuft, der Identifikationsvorgang abgebrochen und in Schritt S0 ein negative Information zur Identifikation ausgegeben. Alternativ oder kumulativ kann auch das Kinegramm 15 durch Vergleich seiner Abbildung im ersten Bild mit allgemeingültigen Eigenschaften geprüft werden.

[0026] Die allgemeingültigen Eigenschaften sind dabei als mindestens ein Kriterium implementiert, das mit Bildverarbeitungsverfahren anhand des ersten Bildes getestet werden kann. So können sich die allgemeingültigen Eigenschaften auf die Definition des Sicherheitsmerkmals selbst, z.B. eine genaue geometrische Anordnung des Musters 14, beziehen oder auf einen optischen Effekt, der durch das Sicherheitsmerkmal in definierter Form hervorgerufen wird und in dem ersten Bild sichtbar ist, z.B. ein Farbeffekt oder eine Farbänderung im Fall mehrerer Bilder von dem Kinegramm 15. Die allgemeingültigen Eigenschaften und Kriterien lassen sich einerseits aufgrund der Definition des Sicherheitsmerkmals aufstellen. Andererseits können sie durch künstliche Intelligenz mit Methoden des maschinellen Lernens, z.B. durch neuronale Netze, aufgestellt werden. Insbesondere werden die allgemeingültigen Eigenschaften und die Kriterien durch überwachtes Lernen aufgestellt, indem der künstlichen Intelligenz verschiedene echte und unechte ID-Karten gezeigt werden, jeweils zusammen mit der Information ob die ID-Karte echt oder unecht, also gefälscht, ist. So lassen sich belastbare und zuverlässige Kriterien zur Echtheitsprüfung nur anhand des ersten Bildes definieren.

[0027] Wenn die ID-Karte 1 in Schritt S3 als echt eingestuft wird, macht der Benutzer in Schritt S4 von Figur 2 ein zweites Bild von sich, auf dem sein Gesicht oder zumindest ein Teil seines Gesichts zu sehen ist. Das zweite Bild wird wiederum vom Mobiltelefon über die Datenverbindung 31 an den Server 3 geschickt und von diesem in Schritt S5 empfangen. In Schritt S6 findet eine Prüfung statt, ob die auf dem zweiten Bild abgebildete Person mit dem Inhaber der ID-Karte 1 übereinstimmt, also insbesondere die gleiche Person ist wie die auf dem Lichtbild 11. Dazu wird das Lichtbild 11 aus dem ersten Bild extrahiert. Das Extrahieren kann schon vorher und insbesondere bereits auf dem Mobiltelefon 2 durchgeführt werden. In diesem Fall empfängt der Server 3 das extrahierte Lichtbild 11 vom Mobiltelefon 2, z.B. in Schritt S2 zusammen mit dem ersten Bild oder in Schritt S5 zusammen mit dem zweiten Bild.

[0028] Die Prüfung der Übereinstimmung des Benutzers mit dem Inhaber der ID-Karte in Schritt S6 geschieht durch Bestimmen einer Ähnlichkeit zwischen dem Lichtbild 11 und dem Gesicht oder Teil des Gesichts auf dem zweiten Bild. Vorteilhaft wird das zweite Bild durch ein Video oder zwei zweite Bilder ersetzt, sodass festgestellt werden kann, dass die auf dem zweiten Bild abgebildete Person auch tatsächlich live vor dem Mobiltelefon 2 sitzt und nicht nur auf einem Foto abgebildet ist, das eine andere Person in die Kamera 23 hält. Dies wird z.B. dadurch bewerkstelligt, dass der Benutzer sich während des Videos oder zwischen den zwei zweiten Bildern bewegt und dann geprüft wird, ob der Bewegungsvorgang realistisch ist (Motion Detection). Eine solche Liveness Detection lässt sich alternativ auch über weitere Sensordaten des Mobiltelefons 2 erreichen, z.B. durch Einbezug eines Annäherungssensors.

[0029] Wenn die Ähnlichkeit zwischen dem Gesicht auf dem Lichtbild 11 und dem Gesicht auf dem zweiten Bild nicht ein gewisses Mass übersteigt, wird die Identifikation des Benutzers als inkorrekt eingestuft, der Identifikationsvorgang abgebrochen und in Schritt S0 ein negative Information zur Identifikation ausgegeben. Falls die Ähnlichkeit das gewisse Mass aber übersteigt, wird die Identifikation des Benutzers als korrekt eingestuft und in Schritt S7 entsprechend eine positive Information zur Identifikation ausgegeben.

[0030] Bevorzugt ist das beschriebene Verfahren in einem Computerprogramm implementiert, das auf dem Server 3 läuft. Dieses kommuniziert über die Datenverbindung 31 mit einer Applikation (App) oder einer Web-Applikation im Browser (Web-App) auf dem Mobiltelefon 2. Die App ist vorteilhafterweise so gestaltet, dass sie den Benutzer durch den Identifikationsvorgang führt, also insbesondere Anweisungen ausgibt, wann und wie ihr das erste und das zweite Bild oder Video aufnehmen soll. Weiterhin ist es vorteilhaft, dass die App in sicherer Art und Weise implementiert ist, also insbesondere ein Manipulieren des ersten und/oder zweiten Bilds oder Videos und gegebenenfalls des extrahierten Lichtbilds verhindert.

[0031] Grundsätzlich gibt der Benutzer seine persönlichen Daten, z.B. Name, Adresse, Geburtsdatum, z.B. zu Beginn des Verfahrens in Schritt S1 in die App ein. Die Daten werden ebenfalls auf den Server 3 übertragen und dort z.B. durch Abgleich mit einer anerkannten Personendatenbank, z.B. der Schweizer Post, verifiziert.

[0032] Anstatt die persönlichen Daten manuell einzugeben, macht sich eine optionale Erweiterung des Verfahrens in Figur 2 die Identifikationsdaten 16 auf der ID-Karte 1 zunutze: Das Identifikationsverfahren startet in Schritt S1 mit der Aufnahme des ersten Bilds und ohne Eingabe persönlicher Daten. Diese Daten werden dann aus dem ersten Bild, das auch die Identifikationsdaten 16 abbildet, extrahiert. Dies kann z.B. in Schritt S2 oder S3 geschehen. Zusätzlich kann der Server 3 die extrahierten Daten mit weiteren Daten von einer angeschlossenen Datenbank abgleichen oder anreichern. Dies ist speziell dann hilfreich, wenn nicht alle Identifikationsdaten 16 korrekt aus dem ersten Bild extrahiert werden können.

[0033] Die Figuren 3 bis 5 zeigen weitere Ausführungsformen des Verfahrens, die sich die allgemeingültigen Eigenschaften des Kinegramms 15 zur Überprüfung der Echtheit der ID-Karte 1 zunutze machen. Die entsprechenden Prüfungen können also zusätzlich oder alternativ in Schritt S3 der Figur 2 implementiert werden. Sie haben aber auch Auswirkungen darauf, wie der Benutzer in Schritt S1 mit seinem Mobiltelefon 2 das erste Bild bzw. mehrere erste Bilder oder ein erstes Video macht, die dann in Schritt S2 vom Server 3 empfangen werden.

[0034] Figur 3 bezieht sich auf die Eigenschaft des Kinegramms 15, unter verschiedenen Blickwinkeln verschiedene Farben oder verschiedene Formen zu zeigen. Aufgrund der standardisierten Definition des Kinegramms 15 geschieht dies immer in ähnlicher Weise, sodass sich daraus wiederum allgemeingültige Eigenschaften und Kriterien ableiten lassen, wie ein echtes Kinegramm auf einem Bild oder Video unter einem bestimmten Blickwinkel aussieht.

[0035] Entsprechend wird der Benutzer gemäss Figur 3 gebeten, zwei erste Bilder der ID-Karte 1 unter verschiedenen Blickwinkeln zu machen oder ein erstes Video, während dem der Benutzer die ID-Karte 1 kippt oder das Mobiltelefon 2 relativ zur ID-Karte 1 bewegt. Praktikabel ist besonders die Kippung 24 der ID-Karte 1 um eine definierte Achse, z.B. horizontal oder vertikal, da der Benutzer den Bewegungsvorgang generell möglichst genau gemäss Anweisungen der App durchführen muss, damit die allgemeingültigen Eigenschaften des Kinegramms 15 dann tatsächlich in den ersten Bildern oder dem ersten Video aufgefunden werden können.

[0036] Figur 4 stellt eine Variante zur Kippung 24 in Figur 3 dar. Hier macht der Benutzer zwei erste Bilder bei verschiedener Distanz zwischen ID-Karte 1 und Mobiltelefon 2 oder ein erstes Video, während dem er eine solche Distanzveränderung 25 durchführt, also entweder die ID-Karte 1 oder das Mobiltelefon 2 relativ zum jeweils anderen Objekt bewegt. Auch für diesen Fall lassen sich in den ersten Bildern oder dem ersten Video charakteristische Farb- oder Formänderungen des Kinegramms 15 feststellen, die in der Prüfung in Schritt S3 genutzt werden können. Dies liegt insbesondere an der Änderung der Beleuchtung und/oder des Sichtbereichs 22 der Kamera 21 relativ zum einfallenden Licht.

[0037] Figur 5 stellt eine weitere Variante dar, wobei keine Relativbewegungen 24 oder 25 wie in den Figuren 3 und 4 nötig sind, sondern die Beleuchtung der ID-Karte 1 zwischen den mindestens zwei ersten Bildern oder während des ersten Videos verändert wird. Dazu bietet sich insbesondere der Blitz 23 des Mobiltelefons 2 an, der so angesteuert wird, dass er auf den ersten Bildern oder während des ersten Videos verschiedene Helligkeiten hervorruft. Diese Ausführungsform ist besonders leicht zu implementieren, indem z.B. von der App in kurzem Abstand zwei erste Bilder aufgenommen werden, wobei bei dem einen Bild der Blitz 23 angeschaltet ist und auf dem anderen aus. Zusätzlich kann die Helligkeit des Blitzes 23 von der App in mehr als zwei Stufen gesteuert werden, sodass weitere optische Effekte des Kinegramms 15 auf den ersten Bildern oder dem ersten Video sichtbar werden.

[0038] Figur 6 zeigt (analog zu Figur 1) Elemente, die in einem Verfahren gemäss einer weiteren Ausführungsform der Erfindung verwendet werden: ein biometrischer Pass oder Ausweis 1a, ein Mobiltelefon (Endgerät) 2 und ein Server (Identifizierungsserver) 3. Der biometrische Pass 1a umfasst einen Chip 17, auf dem üblicherweise persönliche Daten des Benutzers, wie z.B. Name, Vorname, Adresse und Geburtsdatum, sowie Fingerabdrücke und ein Lichtbild des Gesichts des Benutzers gespeichert sind.

[0039] Der Chip 17 kann elektronisch über eine drahtlose Verbindung 27 ausgelesen werden, z.B. von einem NFC-Sensor 26, der in dem Mobiltelefon 2 enthalten ist.

[0040] Weiterhin ist auf dem Chip 17 als Sicherheitsmerkmal eine elektronische, insbesondere digitale, Signatur gespeichert, welche von der Passbehörde bei Ausstellung des Passes 1a erstellt wurde. Mit dieser Signatur lassen sich Authentizität und Integrität der Daten auf dem Chip 17 überprüfen. Das Auslesen des Chips 17 stellt also eine sichere Möglichkeit dar, die Echtheit des biometrischen Passes 1a zu überprüfen. Weiterhin stehen durch Auslesen des Chips 17 das Lichtbild 11 und die persönlichen Daten des Benutzers elektronisch in guter Qualität- zur Verfügung.

[0041] Im Vergleich zu dem Verfahren der Figuren 1 und 2 erübrigt sich bei Figur 6 also prinzipiell das Abfotografieren des Passes 1a und das Überprüfen der optischen Sicherheitsmerkmale 12-15. Eine Kombination mit dem in Bezug auf Figuren 1 und 2 beschriebenen Verfahren, also insbesondere die zusätzlich Prüfung der optischen Sicherheitsmerkmale 12-15, ist aber denkbar. Die obigen Ausführungen können daher auch auf die Figuren 6 und 7 angewendet werden.

[0042] Im Folgenden wird anhand des Fliessdiagramms der Figur 7 das Verfahren gemäss der weiteren Ausführungsform beschrieben. Der Benutzer, der sich gegenüber der Institution identifizieren möchte, liest in Schritt S11 mit seinem Mobiltelefon 2 die elektronische Signatur, die persönlichen Daten sowie das Lichtbild 11 seines Passes la elektronisch aus. Dies geschieht normalerweise durch eine App, die auf dem Mobiltelefon ausgeführt wird, und den NFC-Sensor 26 ansteuert, der die Daten von dem Chip 17 ausliest.

[0043] Dabei kann es nötig sein, dass der Name, das Geburtsdatum und/oder weitere persönliche Daten des Benutzers angegeben werden müssen, um die persönlichen Daten, das Lichtbild und die elektronische Signatur vom Chip 17 auslesen zu können. Dies kann dadurch geschehen, dass der Benutzer seinen Name und/oder sein Geburtsdatum in der App eingibt. Dieser Schritt kann alternativ aber auch durch Abfotografieren und Erkennen der Identifikationsdaten 16 in der MRZ des Passes 1a bewerkstelligt werden, was Zeit spart und weniger fehleranfällig ist als eine manuelle Eingabe.

[0044] Die elektronische Signatur, die persönlichen Daten sowie das Lichtbild werden dann vom Mobiltelefon 2 über die Datenverbindung 31 an den Server 3 geschickt und in Schritt S12 vom Server empfangen.

[0045] In Schritt S13 wird - ähnlich wie bei Figur 2 - die Echtheit des Passes 1a anhand der elektronischen Signatur als Sicherheitsmerkmal geprüft. Dabei kommt häufig eine Public-Key-Authentifizierung oder eine digitale Signatur zum Einsatz. Insbesondere verwendet der Server 3 bei der Echtheitsprüfung ein Zertifikat, das z.B. von der Ausstellungsbehörde des biometrischen Passes 1a oder auf einer Master-Liste von Zertifikaten der International Civil Aviation Organization (ICAO) bereitgestellt wird. Dabei bilden die Signatur und das Zertifikat zusammen eine „Trust Chain", bei der das eine Ende sicher bei der Ausstellungsbehörde des biometrischen Passes verankert ist und das andere Ende sicher auf dem Chip 17 des biometrischen Passes 1a gespeichert ist.

[0046] Wenn die Prüfung der Authentizität und Integrität des Passes in Schritt S13 zu einem negativen Ergebnis kommt, endet das Identifikationsverfahren in Schritt S10 als fehlgeschlagen. Dem Benutzer wird dann üblicherweise eine Fehlernachricht auf dem Mobiltelefon 2 angezeigt.

[0047] Wenn der Pass 1a in Schritt S13 hingegen als echt eingestuft wird, macht der Benutzer in Schritt S14 mit der Kamera 21 des Mobiltelefons 2 ein Bild von sich, auf dem sein Gesicht oder zumindest ein Teil seines Gesichts zu sehen ist. Dieses Bild wird wiederum vom Mobiltelefon 2 über die Datenverbindung 31 an den Server 3 geschickt und von diesem in Schritt S15 empfangen.

[0048] Auch die Prüfung der Übereinstimmung des Benutzers mit dem Inhaber der ID-Karte in Schritt S16 geschieht analog zu Schritt S6 oben. Wenn die Ähnlichkeit zwischen dem Gesicht auf dem Lichtbild und dem Gesicht auf dem Bild nicht ein gewisses Mass übersteigt, wird die Identifikation des Benutzers als inkorrekt eingestuft, der Identifikationsvorgang abgebrochen und in Schritt S10 ein negative Information zur Identifikation ausgegeben. Falls die Ähnlichkeit das gewisse Mass aber übersteigt, wird die Identifikation des Benutzers als korrekt eingestuft und in Schritt S17 entsprechend eine positive Information zur Identifikation ausgegeben.

[0049] Die weiteren Ausführungen zur bevorzugten Implementierung des Verfahrens von oben gelten hier analog.

[0050] Das Verfahren der Figuren 6 und 7 profitiert von einem, insbesondere gegenüber dem Verfahren der Figuren 1 und 2, erhöhten Sicherheitsniveau, welches durch das elektronische Auslesen der Daten inklusive der elektronischen Signatur erreicht wird. Gleichzeitig ist das Verfahren einfacher und weniger fehleranfällig, da prinzipiell ein Fotografieren des Passes 1a sowie das Extrahieren des Lichtbilds entfallen.

[0051] Während in der vorliegenden Anmeldung bevorzugte Ausführungen der Erfindung beschrieben sind, ist klar darauf hinzuweisen, dass die Erfindung nicht auf diese beschränkt ist und in auch anderer Weise innerhalb des Umfangs der folgenden Ansprüche ausgeführt werden kann.

Patentansprüche

1. Computerimplementiertes Verfahren zur Identifikation eines Benutzers anhand eines Identifikationsdokuments (1), umfassend die Schritte
   - Empfangen von ersten Daten von einem Endgerät (2) auf einem Identifizierungsserver (3), wobei die ersten Daten ein Lichtbild (11) des Benutzers und ein Sicherheitsmerkmal umfassen,
   - Prüfen einer Echtheit des Identifikationsdokuments (1) anhand des Sicherheitsmerkmals,
   - Empfangen von zweiten Daten von dem Endgerät (2) auf dem Identifizierungsserver (3), wobei die zweiten Daten eine Gesichtspartie des Benutzers abbilden,
   - Prüfen einer Übereinstimmung des Benutzers mit einem Inhaber des Identifikationsdokuments (1) durch Bestimmen einer Ähnlichkeit zwischen dem Lichtbild (11) und der Gesichtspartie des Benutzers,
   - bei positiven Ergebnissen der Prüfungen Anerkennen der Identifikation des Benutzers als korrekt durch den Identifizierungsserver (3).
2. Verfahren gemäss Anspruch 1,
   wobei die ersten Daten zumindest teilweise auf einem Chip (17) des Identifikationsdokuments (1) gespeichert sind,
   wobei das Sicherheitsmerkmal eine elektronische Signatur umfasst,
   wobei das Prüfen einer Echtheit des Identifikationsdokuments (1) den folgenden Schritt umfasst:
   - Prüfen von Authentizität und Integrität der ersten Daten anhand der elektronischen Signatur.
3. Verfahren gemäss Anspruch 1 oder 2,
   wobei die ersten Daten erste Bilddaten umfassen,
   wobei das Sicherheitsmerkmal ein optisches Sicherheitsmerkmal (12-15) umfasst,

wobei die ersten Bilddaten mindestens einen Teil des Identifikationsdokuments (1) mit dem Lichtbild (11) und dem optischen Sicherheitsmerkmal (12-15) abbilden,
wobei das Prüfen einer Echtheit des Identifikationsdokuments (1) ein Vergleichen des optischen Sicherheitsmerkmals (12-15) mit allgemeingültigen Eigenschaften des optischen Sicherheitsmerkmals umfasst,
zusätzlich umfassend den Schritt
- Extrahieren des Lichtbilds (11) aus den ersten Bilddaten.

4. Verfahren gemäss Anspruch 3, weiterhin umfassend die Schritte
- Bestimmen von Identitätsdaten aus den ersten Bilddaten,
- bei positiven Ergebnissen der Prüfungen Zuordnen der Identitätsdaten zum Benutzer.

5. Verfahren gemäss einem der Ansprüche 3 oder 4, weiterhin umfassend die Schritte
- Bestimmen einer Art des Identifikationsdokuments (1),
- Laden der zur Art des Identifikationsdokuments (1) gehörigen allgemeingültigen Eigenschaften des optischen Sicherheitsmerkmals (12-15).

6. Verfahren gemäss einem der Ansprüche 3-5,
wobei das optische Sicherheitsmerkmal (12-15) so beschaffen ist, dass es unter verschiedenen Blickwinkeln verschieden aussieht, insbesondere dass sich dabei eine Farbe oder eine in dem optischen Sicherheitsmerkmal (12-15) dargestellte Form ändert,
wobei die ersten Bilddaten mehrere Bilder des optischen Sicherheitsmerkmals (12-15) unter verschiedenen Blickwinkeln umfassen.

7. Verfahren gemäss einem der Ansprüche 3-6,
wobei das optische Sicherheitsmerkmal (12-15) des Identifikationsdokuments (1) so beschaffen ist, dass es bei Veränderung einer Beleuchtung verschieden aussieht, insbesondere dass sich dabei eine Farbe oder eine in dem optischen Sicherheitsmerkmal (12-15) dargestellte Form ändert,
wobei die ersten Bilddaten mehrere Bilder des optischen Sicherheitsmerkmals (12-15) bei verschiedener Beleuchtung, insbesondere bei verschiedener Helligkeit der Beleuchtung, umfassen.

8. Verfahren gemäss Anspruch 7,
wobei das Endgerät (2) ein Mobilgerät mit einer Lichtquelle (23) mit mindestens zwei Helligkeitsstufen ist,
wobei mindestens zwei Bilder der ersten Bilddaten bei verschiedenen Helligkeitsstufen der Lichtquelle (23) aufgenommen sind,
insbesondere wobei das Endgerät (2) ein Mobiltelefon mit einem Blitz ist.

9. Verfahren gemäss einem der Ansprüche 3-8, mit mindestens einer der folgenden Eigenschaften:
- das optische Sicherheitsmerkmal (12-15) ist zumindest teilweise auf dem Lichtbild (11) angebracht,
- das optische Sicherheitsmerkmal (12-15) umfasst mindestens eines der folgenden Merkmale: einen Rahmen (12) um das Lichtbild, ein Muster (14) oder eine Gravur (13),
- das optische Sicherheitsmerkmal umfasst ein OVD oder ein Kinegramm (15).

10. System zur Datenverarbeitung, umfassend einen Prozessor, der so angepasst ist, dass er das Verfahren nach einem der vorhergehenden Ansprüche ausführt.

11. Computerprogramm, umfassend Befehle, die bei der Ausführung des Programms durch einen Computer diesen veranlassen, das Verfahren nach einem der Ansprüche 1 bis 9 auszuführen.

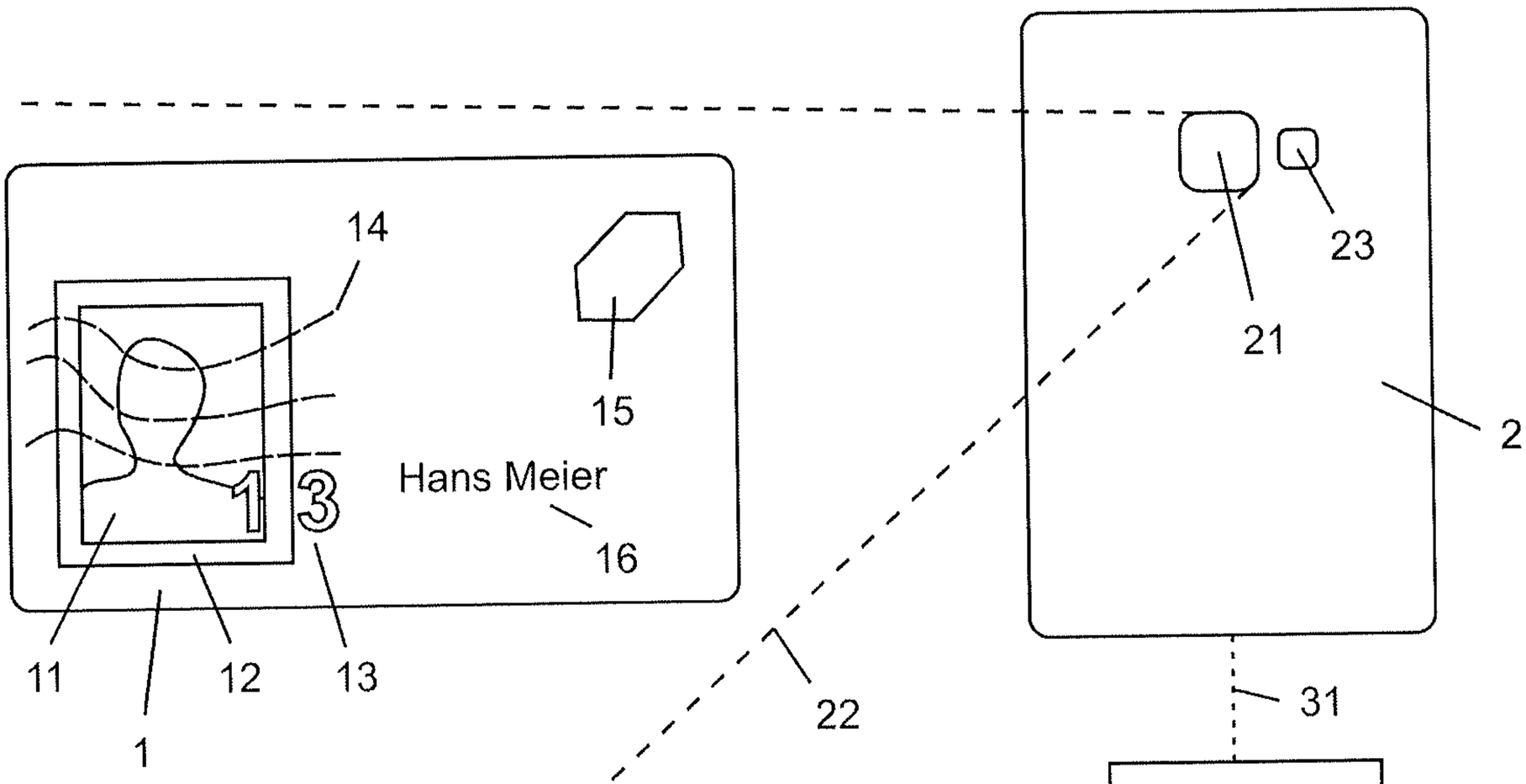

14
15
Hans Meier
16
1
3
11
12
13
1
22
23
21
2
31
3

Fig. 1

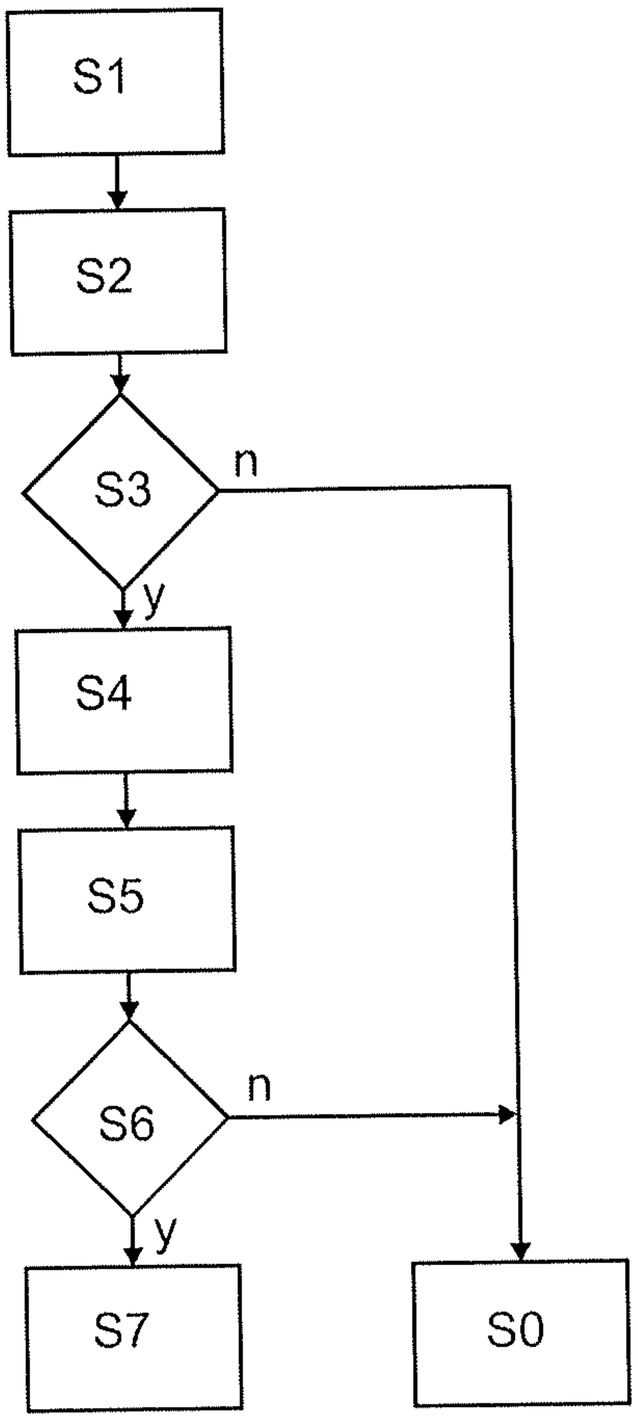

S1
S2
S3
n
y
S4
S5
S6
n
y
S7
S0

Fig. 2

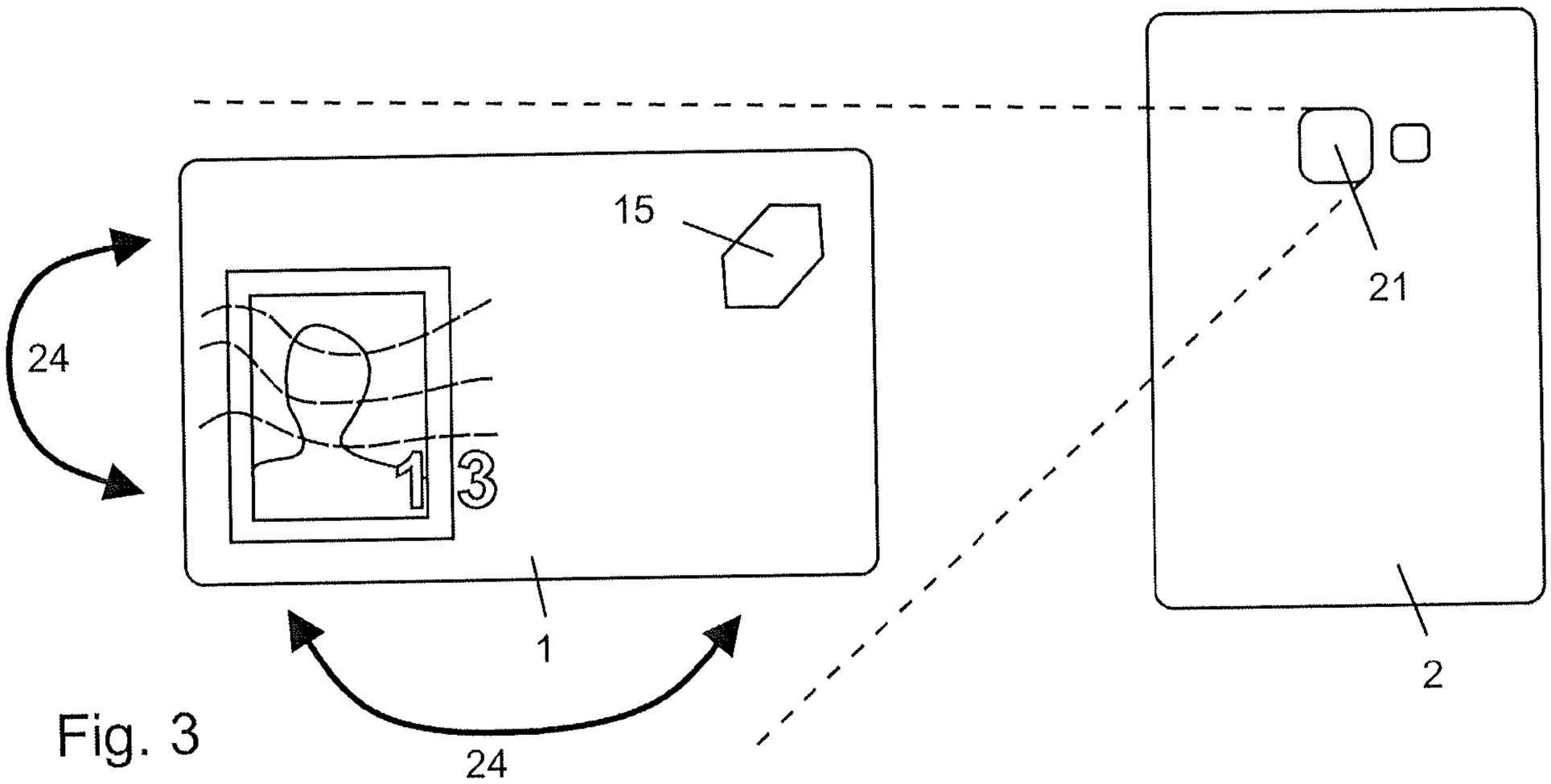


Fig. 3

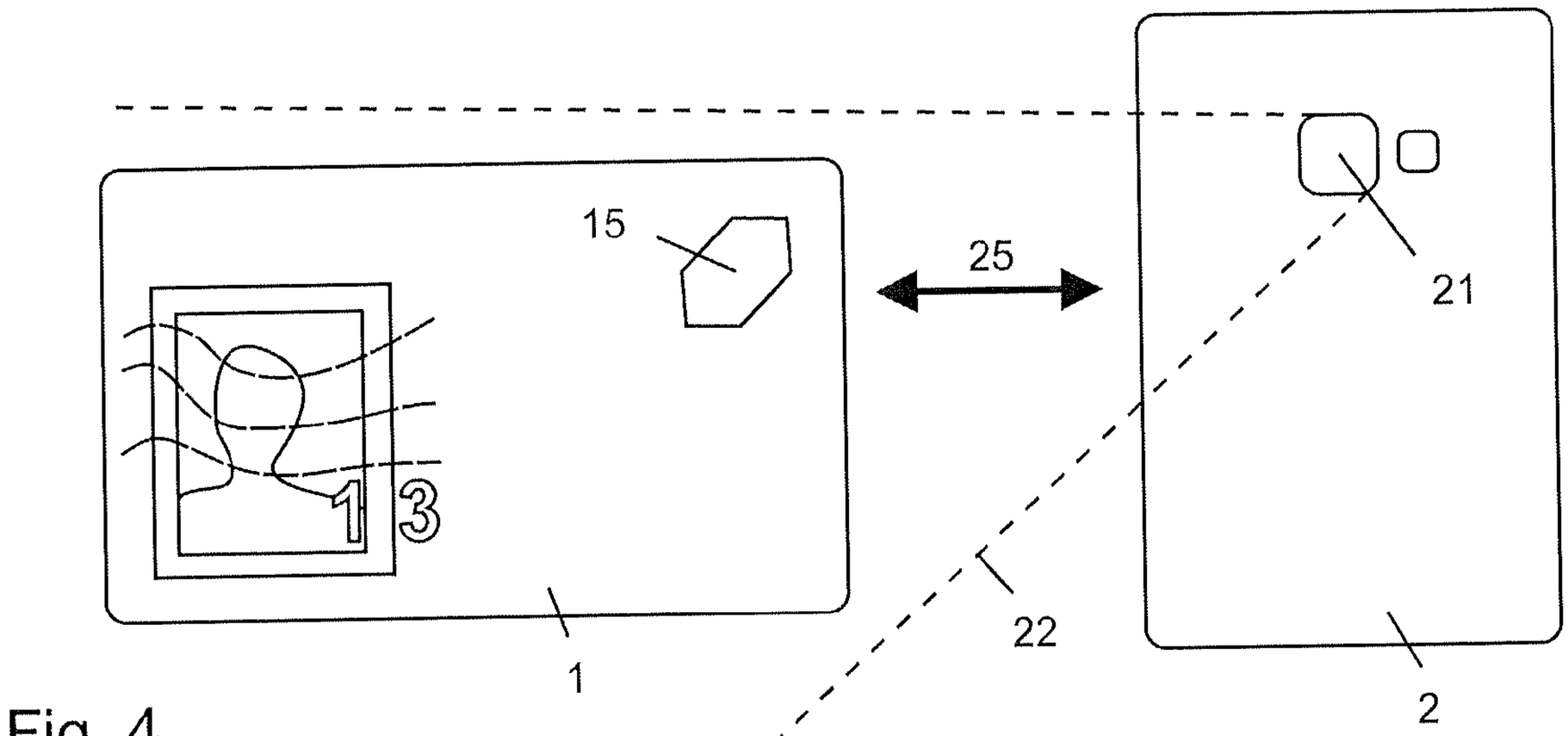


Fig. 4

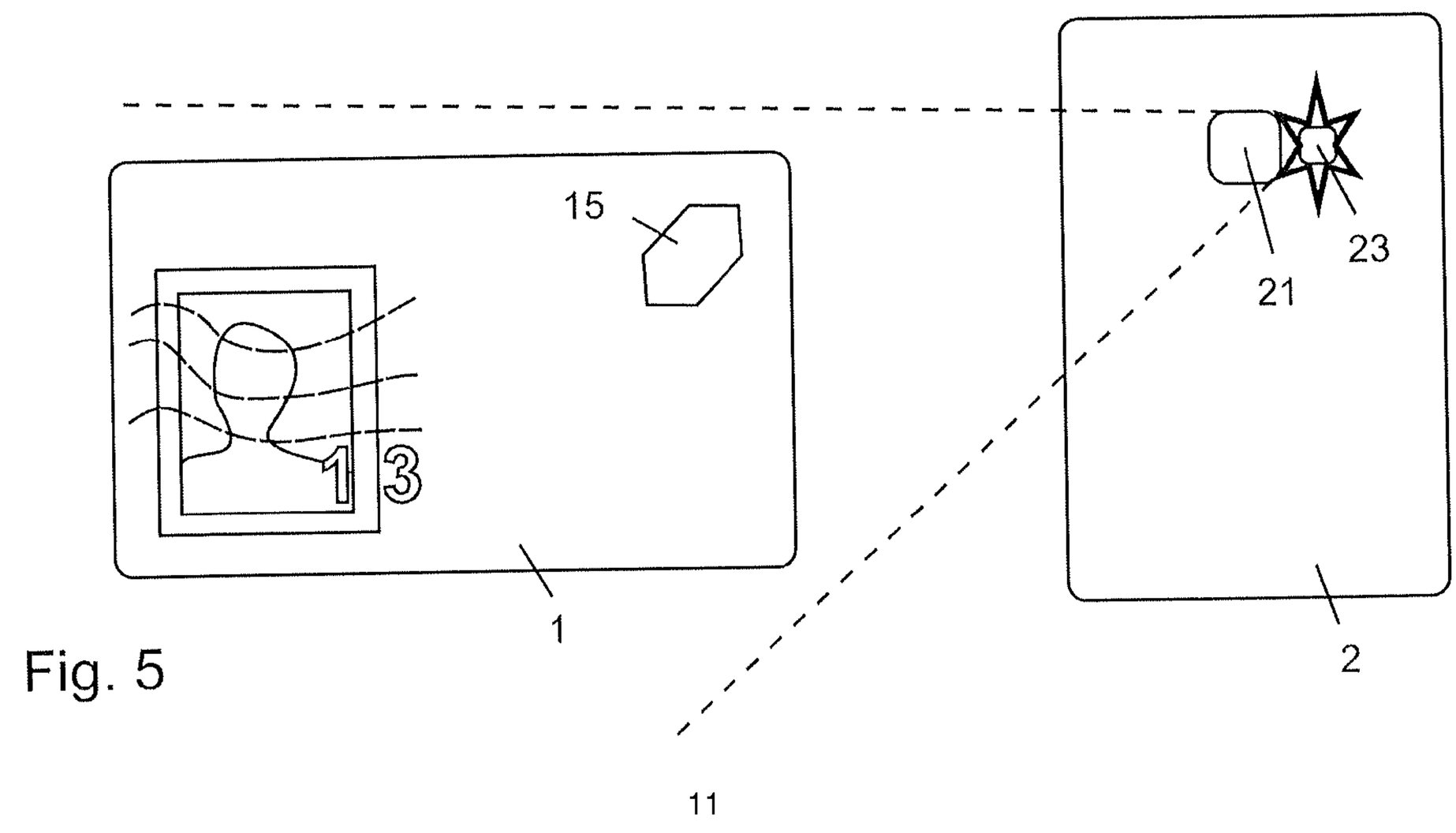


Fig. 5

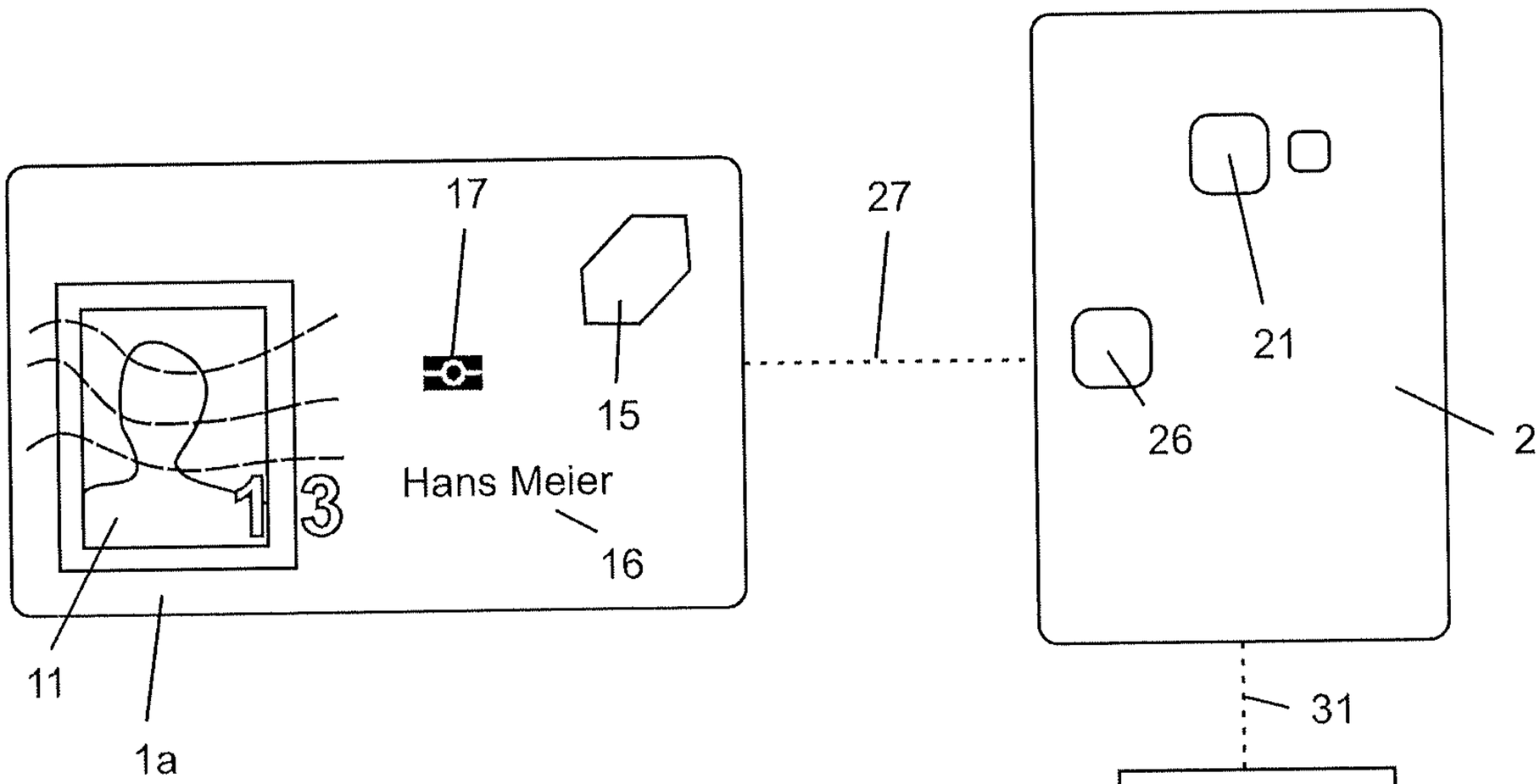

17
27
15
21
26
2
Hans Meier
16
11
1a
31
3

Fig. 6

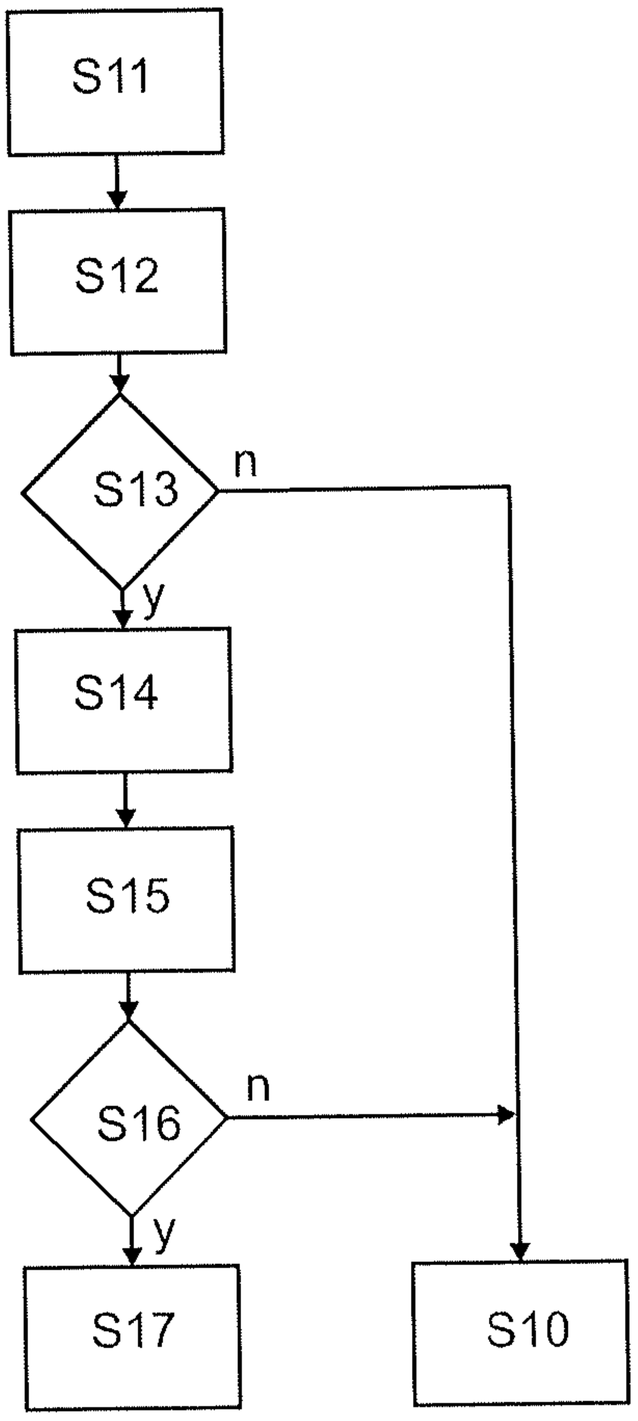

S11
S12
S13
n
y
S14
S15
S16
n
y
S17
S10

Fig. 7