(19) Deutsches Patent- und Markenamt

(10) **DE 20 2013 011 992 U1** 2015.05.28

(12) # Gebrauchsmusterschrift

(21) Aktenzeichen: **20 2013 011 992.6**
(22) Anmeldetag: **10.04.2013**
(47) Eintragungstag: **22.04.2015**
(45) Bekanntmachungstag im Patentblatt: **28.05.2015**

(51) Int Cl.: ***H04L 9/08*** (2006.01)

(30) Unionspriorität:

61/622,213	**10.04.2012**	**US**
1221469.8	**28.11.2012**	**GB**
13/829,185	**14.03.2013**	**US**

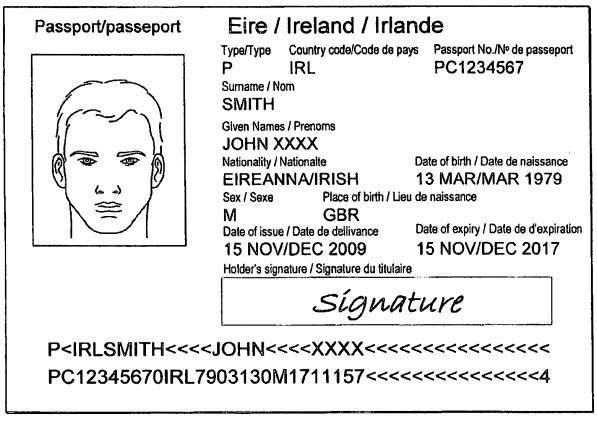
(73) Name und Wohnsitz des Inhabers:
Sita Information Networking Computing Ireland Ltd., Letterkenny, Donegal, IE

(74) Name und Wohnsitz des Vertreters:
Eisenführ Speiser Patentanwälte Rechtsanwälte PartGmbB, 28217 Bremen, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Sicherheitskontrollsystem an Flughäfen**

(57) Hauptanspruch: Entschlüsselungssystem zum Entschlüsseln von Benutzerinformationen, die auf einem mit einem Identitätsdokument eines Benutzers assoziierten Speichergerät verschlüsselt sind, wobei das System Folgendes umfasst:
einen Server, der zum Sammeln von Benutzeridentitätsdokumentdaten vom Benutzer und zum Konstruieren eines die Benutzeridentitätsdokumentdaten umfassenden Tokens konfiguriert ist, wobei der Server ferner zum Senden des Tokens zu einem mit dem Benutzer assoziierten Mobilgerät zum Speichen des Tokens auf dem Mobilgerät konfiguriert ist, und wobei das Mobilgerät physisch von dem genannten Speichergerät getrennt ist;
eine Schlüsselkonstruktionseinheit, kommunikativ mit einem Maschinenleser gekoppelt, der zum Lesen der Daten von dem Token durch Funkfrequenz-Identifikationskommunikation mit dem Mobilgerät konfiguriert ist,
wobei das Token ferner Benutzeridentifikationsinformationen umfasst und wobei der Leser insbesondere ferner zum Lesen der Benutzeridentifikationsinformationen von dem Token konfiguriert ist und wobei die Schlüsselkonstruktionseinheit die von dem auf dem Mobilgerät gespeicherten Token gelesenen Benutzeridentifikationsinformationen zum Konstruieren eines Schlüssels zum Entschlüsseln der auf dem genannten Speichergerät gespeicherten Benutzerinformationen benutzt;
einen Komparator zum Vergleichen der von dem auf dem Mobilgerät gespeicherten Token gelesenen Benutzeridentifikationsinformationen und der von dem genannten Speichergerät entschlüsselten Benutzerinformationen in Verbindung mit dem Benutzeridentitätsdokument; und
Authentifikationsmittel zum Authentifizieren des Benutzers je nach dem Ergebnis des Vergleichs.



Beschreibung

BEREICH DER ERFINDUNG

[0001] Die vorliegende Erfindung betrifft allgemein ein Sicherheitssystem. Spezieller betrifft die vorliegende Erfindung ein Sicherheitssystem für Passagiere, die einen Pass, ein offizielles Reisedokument oder ein anderes Identitätsdokument benötigen, das die Identität des Passagiers bescheinigt, damit er zu seinem Ziel reisen kann. Spezieller, die vorliegende Erfindung betrifft ein Sicherheitssystem zum Straffen und Beschleunigen der Passagierabfertigung im Sicherheitsbereich von Flughäfen sowie ein System zum Entschlüsseln von auf einem Speichergerät gespeicherten Benutzerinformationen.

HINTERGRUND DER ERFINDUNG

[0002] In vielen Pässen ist heute ein RFID-(Funkfrequenzidentifikation)-Chip eingebettet, der die Speicherung von biometrischen und anderen Daten auf dem Pass mittels des Chips zulässt. Daten können drahtlos mit von einem Leser erzeugten elektromagnetischen Feldern von dem Chip gelesen werden. Der Chip antwortet, indem er Daten über eine mit dem Chip assoziierte elektromagnetische Feldspule überträgt.

[0003] Biometrische Pässe sind mit Schutzmechanismen ausgestattet, um Angriffe zu vermeiden und/oder zu erkennen. Charakteristiken von biometrischen Pässen und Chips sind in Doc 9303 der Internationalen Zivilluftfahrtorganisation (ICAO) dokumentiert. Die meisten Pässe unterstützen zumindest BAC (Basic Access Control), die in Europa obligatorisch ist. BAC schützt den Kommunikationskanal zwischen dem Chip auf oder in dem Pass und dem Leser durch Verschlüsseln von übertragenen Informationen. Gewöhnlich werden Daten auf dem Pass in einer verschlüsselten oder gesicherten Form gespeichert, die mit einem Schlüssel zugängig ist. Dadurch wird verhindert, dass unbefugte Benutzer in dem Chip gespeicherte Daten skimmen, d. h. unbefugterweise lesen. Ferner kann ein Lauscher keine übertragenen Informationen mithören, ohne den richtigen Schlüssel zu kennen, wenn der Pass BAC unterstützt.

[0004] Typischerweise erfolgt an irgendeinem Punkt vor dem Abflug eines Passagiers eine Sicherheitskontrolle, um zu prüfen, dass Name und Bordkarte eines Passagiers mit dem Namen auf seinem Pass übereinstimmen. Die auf dem Chip gespeicherten Informationen, wie z. B. biometrische Informationen, können zum Authentifizieren der Identität eines Reisenden benutzt werden. Eine Bordkarte ist gewöhnlich ein Papierdokument, auf dem der Name des Passagiers, Flugdaten, Gate sowie Sitznummer aufgedruckt sind. Gewöhnlich ist die Sicherheitskontrolle eine visuelle Überprüfung, die von einem Sicherheitsbeauftragten durchgeführt wird, der prüft, dass der Name des Passagiers auf der Bordkarte mit dem Namen des Passagiers auf seinem Pass übereinstimmt. Der Sicherheitsbeauftragte prüft auch gewöhnlich, ob das Foto auf dem Pass das des ihn benutzenden Passagiers ist. Da es sich hierbei um eine visuelle Überprüfung handelt, ist sie für menschliche Fehler anfällig.

[0005] In einigen Fällen beinhaltet die Sicherheitskontrolle das Lesen der biometrischen Daten, die auf dem im Pass eingebetteten RFID-Chip gespeichert sind. Da jedoch die auf dem Chip gespeicherten Daten verschlüsselt sind, benötigt der Leser, bevor die Daten vom Pass gelesen werden können, einen Schlüssel, der von einer im Pass befindlichen MRZ (maschinenlesbare Zone) abgeleitet werden kann.

[0006] Um die Daten von der MRZ zu lesen, muss der Pass geöffnet und auf einen optischen Leser gelegt werden, der an der MRZ einen OCR-(Zeichenerkennung)-Vorgang durchführt. Zeichenerkennung ist die mechanische oder elektronische Umsetzung von gescannten Bildern von gedrucktem Text in maschinencodierten Text.

[0007] Der Leser leitet dann den Schlüssel aus der Datenauslesung von den Daten der maschinenlesbaren Zone des Passes ab. Dann wird ein zweiter RFID-Scan durchgeführt, der den vom OCR abgeleiteten Schlüssel zum Abrufen der biometrischen Daten von dem Pass benutzt. Dies ist ein zweistufiger Vorgang, der insbesondere während des OCR-Teils fehleranfällig ist. Der Grund ist, dass der OCR-Teil für die Stelle empfindlich ist, an der der Pass auf den Scanner gelegt wird, und dass es aufgrund von Schmutz auf dem Scanner-Glas auch zu einem Lesefehler kommen kann. Wenn während des OCR-Teils ein Fehler auftritt, dann verläuft der RFID-Scan erfolglos. Um die MRZ-Daten abzurufen, müssen sie manuell eingegeben werden, damit die biometrischen Daten gelesen werden können. Da die Interpretation der MRZ derzeit mit OCR erfolgt, können nur Genauigkeitsraten von 80% bis 90% erzielt werden.

ZUSAMMENFASSUNG DER ERFINDUNG

[0008] Die Erfindung ist in den beiliegenden Ansprüchen definiert, auf die nun Bezug genommen werden sollte. Ausgestaltungen der Erfindung gehen die obigen Probleme an, indem sie ein verbessertes Entschlüsselungssystem bereitstellen, bei dem die Notwendigkeit für einen OCR-Scan der maschinenlesbaren Zone entfällt. Somit wird der Passlesevorgang gestrafft und ergibt einen rascheren Durchlauf von Passagieren durch den Sicherheitsbereich. Ausgestaltungen der Erfindung können die Zeit zum Lesen eines Passes um etwa 4 Sekunden reduzieren. Bei einigen Ausgestaltungen der Erfindung erübrigt sich die Verwendung von OCR-Software, die typischerweise nur Genauigkeitsraten von 80% bis 90% an den Zeichen in der maschinenlesbaren Zone hat. Eine ungenaue OCR in der MRZ führt zu Fehlern beim Lesen der Biometrik von dem Pass. Indem der Passagier veranlasst werden muss, die APIS-Schlüsseldaten vor und während des Check-in einzugeben, und sie mit den Bordkarteninformationen für ein elektronisches Lesen verfügbar gemacht werden müssen, entfällt die Abhängigkeit von OCR. Einige Ausgestaltungen der Erfindung lassen sich auch weniger kostspielig implementieren, da gemäß Ausgestaltungen der Erfindung kostspielige duale OCR/RFID-Leser durch kostenärmere RFID-Leser ersetzt werden können.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0009] Es wird nun eine Ausgestaltung der Erfindung, jedoch nur beispielhaft, mit Bezug auf die Begleitzeichnungen beschrieben. Dabei zeigt:

[0010] **Fig.** 1 die Frontseite eines Passes mit einer maschinenlesbaren Zone;

[0011] **Fig.** 2 ein schematisches Diagramm der Hauptfunktionskomponenten einer Ausgestaltung der Erfindung;

[0012] **Fig.** 3a einen Passagier-Check-in-Schirm;

[0013] **Fig.** 3b einen Schirm, auf dem der Passagier zusätzliche Passdaten eingibt;

[0014] **Fig.** 4 einen Schirm mit Daten von der Bordkarte nach dem Lesen von dem mobilen Kommunikationsgerät;

[0015] **Fig.** 5 die von dem mobilen Kommunikationsgerät gelesenen Identifikationsdaten;

[0016] **Fig.** 6 ein schematisches Diagramm, das eine weitere Ausgestaltung zeigt, die ein von einem Pass gelesenes biometrisches Gesichtsbild mit einem mit einer Kamera aufgenommenen Bild des Passagiers vergleicht; und

[0017] **Fig.** 7 die von der Ausgestaltung von **Fig.** 6 durchgeführten Hauptschritte.

[0018] Die folgende Beschreibung bezieht sich auf ein System für den Einsatz in der Luftfahrtindustrie, aber dies ist nur beispielhaft und es werden auch andere Anwendungen der Erfindung erörtert. So kann das Sicherheitssystem beispielsweise in jeder Umgebung eingesetzt werden, in der Sicherheitsprozeduren verlangen, dass authentifiziert wird, dass ein Identifikationsdokument eines Benutzers sowie ein Token für die Leistung eines Dienstes für einen Benutzer diesem Benutzer gehören, bevor der Benutzer ein(en) Produkt oder Service erhält. So finden Ausgestaltungen der Erfindung insbesondere in der Reisebranche (z. B. Eisenbahn, Luft, Bus usw.), aber auch in der Eintrittskartenbranche, z. B. bei Eintrittskarten für Theater, Kino und dergleichen, Anwendung.

[0019] **Fig.** 1 der Begleitzeichnungen zeigt eine Datenseite eines Passes, der in eine Reihe von Zonen unterteilt ist. Eine visuelle Inspektionszone befindet sich in der oberen Hälfte der Seite und enthält Daten, die nicht speziell zum Lesen durch eine Maschine gedacht sind. Eine MRZ des Passes befindet sich in der unteren Hälfte der Datenseite und enthält Daten, die sowohl von einem Menschen als auch von einer Maschine gelesen werden können.

[0020] Die MRZ-Daten können Folgendes umfassen: die Dokumentennummer, das Ablaufdatum und optional das Geburtsdatum des Benutzers. Darunter befindet sich ein Beispiel für die in der MRZ des Passes enthaltenen Daten, obwohl einige persönliche Einzelheiten mit einem X ausgeblendet wurden, um die Identität des Besitzers zu schützen:

```
P<IRLSMITH<<<<JOHN<<<<XXXX<<<<<<<<<<<<<<<<<<<
PC12345670IRL7903130M1711157<<<<<<<<<<<<<<<4
```

[0021] Die Daten in der MRZ können als 2 Zeilen von alphanumerischen Zeichen strukturiert werden. Die Daten in jeder Zeile können durch ein oder mehrere durch **<** repräsentierte Füllzeichen getrennt werden. Jede Datenzeile kann eine Länge von 44 Zeichen haben.

[0022] Nun mit Bezug auf **Fig.** 2, diese zeigt die Hauptfunktionskomponenten eines die Erfindung ausgestaltenden Systems **201**. Die in der gestrichelten Linie **203** von **Fig.** 2 gezeigten Komponenten können sich an einem Flughafen befinden, obwohl sich der Server **205** nicht unbedingt an einem Flughafen zu befinden braucht. Das System kann einen Fern-Check-in-Server **205** umfassen, der von einer Fluggesellschaft oder einer Fremdpartei bereitgestellt wird. Der Fern-Check-in-Server **205** ist so konfiguriert, dass er es einem Passagier gestattet, sich für einen Flug einzuchecken, für den der Passagier ein Reiseticket gekauft hat.

[0023] Typischerweise greift der Passagier von einer fernen Stelle über einen Computer oder ein mobiles Kommunikationsgerät wie z. B. einen tragbaren Laptop oder ein Mobiltelefon auf den Server **205** zu. Der Benutzer kann sich jedoch auch persönlich auf dem Flughafen **203** am Check-in-Schalter einchecken.

[0024] Unabhängig davon, wie der Benutzer das Check-in durchführt, ist mit jedem Benutzer ein Token-Speichermedium wie z. B. ein portables oder mobiles Gerät **207** assoziiert, das eine Bordkarte wie z. B. eine elektronische Bordkarte oder eine E-Bordkarte speichern kann. Die Bordkarte kann man sich als ein Token vorstellen, das von einem Diensteanbieter an einen Benutzer ausgegeben wird, so dass der Benutzer den Dienst gegen Bezahlung erhalten kann.

[0025] Der Server **205** ist gewöhnlich drahtlos, z. B. über ein drahtloses Kommunikationsnetz, mit dem Mobilgerät **207** des Benutzers gekoppelt, aber im Prinzip kann jedes Kommunikationsmittel, wie z. B. ein verdrahtetes Netzwerk, benutzt werden, vorausgesetzt, dass die E-Bordkarte auf das Mobilgerät **207** des Benutzers übertragen und dort gespeichert werden kann.

[0026] Das Mobilgerät **207** umfasst gewöhnlich einen NFC-(Nahfeldkommunikation)-Tag oder -Chip, der kommunikativ mit dem Mobilgerät gekoppelt ist. Typischerweise ist die/der NFC-fähige integrierte Schaltung oder Chip mit dem Mobilgerät festverdrahtet, aber dies ist in der Tat fakultativ. Das Mobilgerät umfasst jedoch ein Kommunikationsmittel, mit dem Daten vom Mobilgerät **207** auf eine Schlüsselkonstruktionseinheit **209** übertragen werden können. Das Mobilgerät **207** kann beispielsweise über einen USB-(Universal Serial Bus)-Port mit einem verdrahteten Kommunikationsmittel gekoppelt werden.

[0027] In der in **Fig.** 2 gezeigten Ausgestaltung sind die Schlüsselkonstruktionseinheit **209** und der Sicherheitspassleser **211** auf einer einzigen Einheit **212** integriert vorgesehen. Die Schlüsselkonstruktionseinheit **209** kann jedoch auch als separate Komponente zu dem Sicherheitspassleser **211** bereitgestellt werden. In jedem Fall ist die Schlüsselkonstruktionseinheit **209** kommunikativ mit einem Pass- oder Identitätskartenleser **211** gekoppelt. Die Schlüsselkonstruktionseinheit **209** kann drahtlos mit dem Leser **211** gekoppelt sein, z. B. über WiFi oder über ein anderes drahtloses Funkkommunikationsmittel oder über eine verdrahtete Verbindung.

[0028] Der Betrieb des Sicherheitssystems **201** wird nun mit Bezug auf die **Fig.** 2 bis **Fig.** 5 der Zeichnungen beschrieben. Die **Fig.** 3a und **Fig.** 3b zeigen den Vorgang des Eincheckens eines Passagiers und illustrieren die typischen Details, die von einem Passagier beim Check-in eingeholt werden können.

[0029] Der Passagier gibt gewöhnlich seinen Namen und fakultativ eine Mobiltelefonnummer und eine Email-Adresse ein. Diese Daten werden gewöhnlich als APIS-(Advanced Passenger Information System)-Daten bezeichnet. Der Passagier führt diesen Schritt gewöhnlich an einer Stelle fern vom Flughafen **203** aus.

[0030] Zusätzlich zu den oben beschriebenen Informationen, die beim Check-in eingegeben oder vom Passagierprofil beim Check-in gesammelt werden, kann in einigen Ausgestaltungen der Erfindung ein Benutzer auch aufgefordert werden, vom Passagier gesammelte zusätzliche Passdetails einzugeben. **Fig.** 3b unten illustriert die zusätzlichen Passdetails oder Informationen, die von einem Passagier beim Check-in gesammelt werden können.

[0031] Die beim Check-in eingegebenen zusätzlichen Informationen können eine oder mehrere aus Passnummer, Geburtsdatum und Ablaufdatum des Passes umfassen. Der Server integriert diese Informationen dann in eine Bordkarte oder eine E-Bordkarte, die über der Fachperson bekannte verdrahtete oder drahtlose

Kommunikationsmittel zum Mobiltelefon des Benutzers übertragen wird. Die Daten werden gewöhnlich als alphanumerische Daten codiert, aber es können auch andere Codierschemata verwendet werden.

[0032] Die Bordkarte kann als 2D-Barcode oder als NFC-Bordkarte dargestellt werden. Die zusätzlichen APIS-Daten können in einem Feld für die Benutzung durch eine individuelle Fluggesellschaft gespeichert und dann als 2D-Barcode oder als NFC-Daten codiert werden. Die alphanumerischen Daten in diesem Feld können das folgende Format haben:

[0033] Eine alphanumerische Passnummer mit 9 Zeichen. Wenn die Passnummer kleiner als 9 Zeichen ist, dann können die übrigen Zeichen mit dem Zeichen „<" aufgefüllt werden, z. B.: „ABC123XY<".

[0034] Ein numerisches Geburtsdatum mit 6 Zeichen in dem Format JJMMTT, zum Beispiel "720823".

[0035] Ein numerisches Ablaufdatum mit 6 Zeichen in dem Format JJTTMM, zum Beispiel "210922".

[0036] Die Daten werden dann in eine barcodierte Bordkarte umgesetzt. Eine NFC-Bordkarte kann die Informationen in einem alphanumerischen Format haben.

[0037] Die zusätzlichen Informationen können APIS-(Advanced Passenger Information System)-Daten sein. Diese zusätzlichen Informationen können eine oder mehrere aus Pass- oder Identitätskartennummer, Geburtsdatum und Ablaufdatum des Passes umfassen. Beim Eingeben der Informationen kann der Passagier auch aufgefordert werden, eine Checkbox anzukreuen, um anzuzeigen, dass die eingegebenen Details den im Pass gezeigten entsprechen.

[0038] Wenn der Passagier diese Details eingegeben hat, dann überträgt der Server **205** diese Informationen zusammen mit der Bordkarte zu dem mit dem Passagier assoziierten Mobiltelefon oder -gerät **207**. Gewöhnlich werden die vom Passagier eingegebenen zusätzlichen Informationen auf eine bestimmte Region der Bordkarte als Textdaten oder als Barcodedaten oder andere Daten codiert. So können die Erfindung ausgestaltende Sicherheitspassleser so konfiguriert werden, dass sie die zusätzlichen Informationen von der Bordkarte durch Lesen von Daten von dieser speziellen Region lesen. Alte Passleser, die nicht zum Lesen von Daten von dieser Region der Bordkarte konfiguriert sind, ignorieren die zusätzlichen Daten.

[0039] Das Mobiltelefon oder -gerät **207** speichert dann die zusätzlichen Informationen und die Bordkarte als NFC-Bordkarte. Die Bordkarte wird in einem Speicher wie z. B. einem Flash-Speicher oder einem IC-Speicherchip gespeichert.

[0040] In einem Beispiel sind mit der Bordkarte zusätzliche Benutzeridentitätsdokumentdaten oder Informationen assoziiert, die zusätzlich zum Namen des Passagiers auf der Bordkarte weitere Benutzeridentitätsdokumentdaten oder Informationen bereitstellen.

[0041] Wenn dann der Passagier am Flughafen ankommt und eine Sicherheitskontrolle an dem Passagier durchgeführt wird, dann wird die NFC-Bordkarte zusammen mit diesen Passinformationen von seinem Mobiltelefon oder -gerät **207** gelesen. Zum Lesen der NFC-Bordkarte von dem Mobilgerät bewegt der Passagier sein Mobilgerät in unmittelbarer Nähe an einem mit der Schlüsselkonstruktionseinheit **209** assoziierten NFC-Leser vorbei. Gewöhnlich wird die NFC-Bordkarte von dem Mobiltelefon oder -gerät **207** mit dem NFC-Chip gelesen, der kommunikativ mit dem Mobiltelefon oder -gerät **207** gekoppelt ist. So kann der Chip auch kommunikativ mit dem mit dem Mobilgerät assoziierten Speichermittel gekoppelt sein. Anstatt Nahfeldkommunikation können auch andere verdrahtete oder drahtlose Kommunikationsmittel zum Übertragen der NFC-Bordkarte vom Mobilgerät **207** zur Schlüsselkonstruktionseinheit verwendet werden. **Fig.** 4 der Zeichnungen zeigt den Inhalt der Bordkarte nach dem Lesen vom Mobilgerät. Das in **Fig.** 4 gezeigte Bild kann auf einem mit dem Leser **211** assoziierten Terminal angezeigt werden. Die von dem Gerät gelesenen Daten können ein oder mehrere aus Name des Passagiers, Fluggesellschaft, Flugnummer, Abflugdatum, Abflugstadt, Ankunftsstadt, Sitznummer, Klasse, Vielfliegernummer, e-Ticketnummer, Einstiegszeit, Dokumentnummer, Geburtsdatum und Ablaufdatum umfassen. In dem in **Fig.** 4 gezeigten Bild werden zwar alle diese Daten angezeigt, aber dies ist nicht wesentlich und es können auch ein oder mehrere der vom Mobilgerät gelesenen Datenfelder auf dem Terminal angezeigt werden. Ein Sicherheitsbeauftragter kann dann die Bordkarte des Benutzers zulassen oder zurückweisen, indem er/sie das entsprechende Feld auf dem Terminal mit der Markierung „Approve" (Zulassen) oder „Deny" (Zurückweisen) drückt.

[0042] Die Schlüsselkonstruktionseinheit **209** extrahiert dann die zusätzlichen Daten von der NFC-Bordkarte durch Lesen der in der speziellen Region der Bordkarte enthaltenen Daten. Die Daten werden auf oder in der Bordkarte codiert.

[0043] Die Schlüsselkonstruktionseinheit **209** rekonstruiert dann den Schlüssel anhand der zusätzlichen Daten. Die Schlüsselkonstruktionseinheit **209** kann den Schlüssel mit einem Schlüsselableitungsmechanismus konstruieren, der der Fachperson bekannt sein wird. Die Schlüsselkonstruktionseinheit **209** sendet oder leitet dann den Schlüssel zum Passsicherheitsleser **211**.

[0044] Der Passagier oder Sicherheitsbeauftragte scannt oder bewegt dann den Pass **213** in unmittelbarer Nähe am Leser **211** vorbei. So beginnt der/die in dem Pass eingebettete RFID-Chip oder integrierte Schaltung **214** mit der Kommunikation mit dem Leser. Diese anfänglichen Kommunikationen zwischen dem Leser und dem RFID-Chip können einen Authentifizierungsschritt beinhalten, bei dem der Leser als echter Leser antatt als ein unbefugter Benutzer authentifiziert wird, der versucht, die auf dem Chip gespeicherten Daten zu lesen oder zu skimmen. Der Leser kann sich mit dem von der Schlüsselkonstruktionseinheit konstruierten Schlüssel selbst authentifizieren.

[0045] Wenn der Leser als echt authentifiziert wurde, dann können vom Leser angeforderte Daten vom Chip **214** zum Leser **211** gesendet werden. Gewöhnlich werden die Daten in verschlüsselter Form zum Leser gesendet. Dadurch kann verhindert werden, dass ein Lauscher vom Chip **214** zum Leser **211** gesendete Daten abfängt.

[0046] Der Leser **211** empfängt dann die vom Chip **214** gesendeten verschlüsselten Daten und entschlüsselt die Daten mit dem anhand der zusätzlichen Daten konstruierten Schlüssel.

[0047] Es können auch andere kontaktlose integrierte Schaltungen **214** in dem Pass **213** oder einem anderen offiziellen Reisedokument eingebettet sein, ohne vom Umfang der Erfindung abzuweichen.

[0048] Der Pass wird gewöhnlich gescannt, unmittelbar nachdem der Benutzer mit seinem Mobilgerät an dem mit der Schlüsselkonstruktionseinheit assoziierten NFC-Leser vorbei gefahren ist. So kann die Schlüsselkonstruktionseinheit **209** den Schlüssel nur als Reaktion darauf konstruieren, dass er die zusätzlichen Daten vom Mobilgerät **207** empfangen hat. Auf diese Weise wird der Leser **211**, wenn der Sicherheitspassleser **211** einen Schlüssel von der Schlüsselkonstruktionseinheit **209** empfängt, so mit einem Schlüssel angewiesen, der die Entschlüsselung von Daten auf einem mit dem Pass **213** assoziierten nachfolgend gescannten RFID-Chip **214** zulässt. Der Leser **211** kann unterschiedliche Schlüssel zur Authentifikation und zur Verschlüsselung oder Entschlüsselung konstruieren.

[0049] Die auf dem RFID-Chip **214** gespeicherten verschlüsselten Daten können biometrische Daten wie z. B. Iriserkennungsdaten, Gesichtserkennungsdaten und Fingerabdruckerkennungsdaten sein, aber im Prinzip können beliebige Daten auf dem Chip oder einem anderen drahtlosen Speichermittel oder Gerät in Assoziation mit dem Pass gespeichert werden. So können beliebige Daten entschlüsselt und von dem Chip gelesen werden. In einer bevorzugten Ausgestaltung liest der Leser **211** jedoch den Vor- und Nachnamen eines Benutzers von dem Chip.

[0050] Der Leser **211** kann dann die von den verschlüsselten Daten auf dem RFID-Chip **214** gelesenen Informationen mit den Daten auf der Bordkarte vergleichen. Wenn die vom Chip **214** gelesenen entschlüsselten Informationen mit entsprechenden von der Bordkarte des Benutzers gelesenen Informationen übereinstimmen, dann kann festgestellt werden, dass der Benutzer die Sicherheitskontrolle bestanden hat. So entfällt die Notwendigkeit für einen zweiten Scan des Passes **213**. Dies ist deshalb nützlich, weil ein zusätzlicher Scan des Passes **213** vermieden werden kann, wodurch OCR-Lesefehler reduziert und die Passagierabfertigung im Sicherheitsbereich beschleunigt werden kann.

[0051] **Fig.** 5 zeigt ein Bild, das auf einem mit dem Leser **211** assoziierten Terminal angezeigt wird und die vom Pass **213** gelesenen Details wie z. B. die Benutzeridentifikationsinformationen zeigt. Wie in **Fig.** 5 gezeigt, können die Informationen ein oder mehrere aus: Nachname des Benutzers, Vorname, Dokumentnummer, persönliche Nummer, Staatsangehörigkeit, Passausgabestatus, Geburtsdatum, Passauslaufdatum und Geschlecht umfassen, welche vom RFID-Chip gelesen werden können. Mit einem Bild des Passagiers assoziierte Daten können ebenfalls vom Chip gelesen werden. Die in der maschinenlesbaren Zone enthaltenen Daten können ebenfalls auf dem Terminal angezeigt werden.

[0052] **Fig.** 5 zeigt auch eine visuelle Anzeige der Ergebnisse des Vergleichs der vom Chip gelesenen Daten und der auf die Bordkarte codierten Daten, wie z. B. den Namen auf der Bordkarte und den vom Pass gelesenen Namen. In **Fig.** 5 kann neben dem Nachnamen und dem Vornamen jeweils ein Haken stehen. Dies zeigt an, dass sowohl der Nachname als auch der Vorname auf dem Pass **213** mit dem Namen auf der Bordkarte übereinstimmen. So entfällt die Notwendigkeit für eine visuelle Überprüfung der Bordkarte und des Passes **213** durch einen Menschen, wodurch die Genauigkeit verbessert und die Check-in-Zeit verkürzt wird.

[0053] Wie oben umrissen, kann seit der Einführung von NFC-Bordkarten eine Bordkarte direkt zu einem Mobiltelefon eines Passagiers gesendet und mit einem NFC/RFIC-Scanner gelesen werden. Es können neue ergänzende (APIS) Passagierpassdaten wie Passnummer, Geburtsdatum und Ablaufdatum beim Check-in vom Passagier eingeholt werden. Diese ergänzenden Informationen können dann mit der NFC-Bordkarte zum Mobiltelefon des Passagiers geleitet werden. Wenn die NFC-Bordkarte bei der Sicherheitskontrolle gelesen wird, dann können die ergänzenden Passinformationen zum Ableiten des Schlüssels zum Zugreifen auf die biometrischen Passdaten benutzt werden. Mit diesen ergänzenden Passinformationen entfällt die Notwendigkeit für einen OCR-Scan der Passdaten. Indem einfach der Pass nahe an den RFID-Scanner gelegt wird, werden die biometrischen Informationen selbst dann vom Pass gelesen, wenn der Pass geschlossen ist.

[0054] Die vorliegende Erfindung wurde zwar mit Bezug auf ein Mobilgerät **207** wie z. B. ein tragbares Telefon beschrieben, das die E-Bordkarte speichert, aber das Mobilgerät **207** ist in der Tat fakultativ. In einigen Ausgestaltungen kann, nachdem der Benutzer ein Fern-Check-in mit dem Server **205** durchgeführt hat, auch eine Papierbordkarte vom Benutzer oder an einem anderen Ort alternativ oder zusätzlich zum Erzeugen und Speichern der NFC-Bordkarte gedruckt werden. So können Ausgestaltungen der Erfindung auch so konfiguriert werden, dass der Server **205** eine Bordkarte mit den physisch auf der Bordkarte ausgedruckten zusätzlichen Informationen erzeugt, um die zusätzlichen Informationen auf der Papierbordkarte zu codieren. Der Benutzer kann die Bordkarte, auf der die zusätzlichen Informationen in einer bestimmten Region der Bordkarte codiert sind, mit einem Standarddrucker ausdrucken. So ist es nicht in allen Ausgestaltungen wesentlich, dass die elektronische Bordkarte zu einem elektronischen Gerät des Benutzers gesendet wird, vorausgesetzt, dass ein Token-Speichermedium vorgesehen ist.

[0055] Ferner verlangen einige offizielle Reisedokumente ausstellende Behörden auch, dass das Reisedokument mit einem Faradayschen Käfig versehen ist, der einen RFID-Chip in dem Käfig vor elektromagnetischen Wellen schützt. Um auf den in dem Käfig geschützten Chip zuzugreifen, muss das offizielle Reisedokument vor dem Lesen geöffnet werden, und dies bedeutet eine zusätzliche Sicherheitsschicht, um ein unbefugtes Lesen von Daten vom RFID-Chip zu verhüten.

[0056] Das Lesen oder NFC/RFID-Scannen erfolgt vorzugsweise mit einem Mobiltelefon oder einem anderen mobilen oder tragbaren Leser oder Scanner.

[0057] In einigen Ausgestaltungen kann der Pass zuvor auf dem Mobiltelefon gespeichert werden. Der Pass kann auf eine gesicherte oder ungesicherte Weise in dem Mobiltelefon oder einem anderen tragbaren Kommunikationsgerät gespeichert werden. So werden in einigen Ausgestaltungen die Passinformationen von einem Mobiltelefon gegeben. Ferner kann ein Sicherheitskontrollvergleich stattfinden, wenn das Reisedokument wie z. B. die Bordkarte gesendet wird, oder beim Check-in.

[0058] In einem weiteren Beispiel kann zusätzlich zu der Sicherheitskontrolle, die durchgeführt wird, um zu überprüfen, dass ein Passagiername auf einer Bordkarte mit dem Namen auf dessen Pass übereinstimmt, das Foto im Pass mit dem Passagier verglichen werden. Ausgestaltungen der Erfindung können diese Prüfung voll automatisieren, indem das biometrische Gesichtsbild des Passes, auch als Referenzbild bezeichnet, mit dem tatsächlichen Bild des Passagiers verglichen wird, der in das Flugzeug einsteigen möchte. Dies kann beinhalten, dass ein Foto von dem Passagier gemacht und automatisch ein Gesichtserkennungsalgorithmus ausgeführt wird, um es mit dem Passreferenzbild zu vergleichen.

[0059] In diesem Beispiel können Ausgestaltungen der Erfindung die folgenden Schritte ausführen:

1. Beim Einchecken eines Passagiers für einen Flug werden die BAC-Mindestinformationen gesammelt, d. h. Passnummer, Geburtsdatum und Ablaufdatum. Die Bordkarteninformationen zusammen mit den BAC-Informationen werden auf dem Mobiltelefon des Passagiers als NFC-Bordkarte übertragen und gespeichert. Dies kann durch Legen des Telefons auf den Pass erfolgen. Das Telefon kann dann in Schritt **701** die BAC-Informationen von der auf dem Telefon gespeicherten aktuellen Bordkarte lesen.
2. Typischerweise erfolgt eine Sicherheitskontrolle, um die Identität des Reisenden zu authentifizieren. Es kann ein NFC-fähiges Telefon wie z. B. Samsung S3 oder ein Desktop-Leser zum Lesen der auf dem Te-

lefon des Passagiers gespeicherten NFC-Bordkarte benutzt werden. Wie zuvor beschrieben, kann anhand der BAC-Details von der NFC-Bordkarte der Pass des Passagiers auch mit einem NFC-fähigen Telefon oder Desktop-Leser im Sicherheitsbereich gelesen werden. BAC bietet Zugang zu den Passdetails des Passagiers und, was noch wichtiger ist, zu dem biometrischen Gesichtsbild des Passagiers. Dies kann in Schritt **703** durch Lesen des biometrischen Gesichtsbildes im Pass mit den BAC-Informationen erfolgen, wobei vorzugsweise das Bild auf dem Telefon gespeichert wird. Die Passdetails können dann automatisch mit den Details auf der NFC-Bordkarte verglichen werden, z. B. der Vor- und der Nachname. Zusätzlich kann der Passagier oder Sicherheitsbeauftragte ein Bild des Passagiers mit einer nach vorne zeigenden Kamera eines Telefons oder einer anderen Kamera aufnehmen. Der Passagier kann sich in Schritt **704** für einen Schnappschnuss mit einer nach vorne zeigenden Kamera auf einem Telefon aufstellen. Nach der Aufnahme des Bildes kann dieses mit einem Gesichtserkennungsalgorithmus automatisch mit dem biometrischen Gesichtsbild des Passes verglichen werden. Der Algorithmus vergleicht in Schritt **707** das biometrische Gesichtsbild des Passes mit dem Schnappschuss.

[0060] Die folgenden nummerierten Klauseln sollen die Erfindung näher beschreiben:

1. Ein Entschlüsselungssystem zum Entschlüsseln von Benutzerinformationen, die auf einem mit einem Benutzeridentitätsdokument assoziierten Speichergerät verschlüsselt sind, wobei das System Folgendes umfasst:
einen Server, der zum Sammeln von Benutzeridentitätsdokumentdaten von dem oder einem Benutzer und zum Konstruieren eines Token konfiguriert ist, das die Benutzeridentitiätsdokumentdaten beinhaltet;
eine Schlüsselkonstruktionseinheit, die kommunikativ mit einem Leser gekoppelt ist, der zum Lesen von Daten von dem Token konfiguriert ist;
wobei die Schlüsselkonstruktionseinheit die von dem Token gelesenen Benutzeridentitätsdokumentdaten zum Konstruieren eines Schlüssels benutzt, der es dem oder einem Leser ermöglicht, die auf dem Speichergerät gespeicherten Benutzerinformationen zu entschlüsseln.
2. Ein Entschlüsselungssystem gemäß Klausel 1, wobei die Schlüsselkonstruktionseinheit den Schlüssel auf der Basis von einem oder mehreren aus Benutzeridentitätsdokumentnummer, Ablaufdatum des Benutzeridentitätsdokuments und vorzugsweise dem Geburtsdatum eines Benutzers ableitet.
3. Ein Entschlüsselungssystem gemäß Klausel 1, wobei der oder ein Benutzer die Benutzeridentitätsdokumentdaten manuell eingibt, bevor der Leser die auf dem Token codierten Daten liest.
4. Ein Entschlüsselungssystem gemäß Klausel 1, bei dem der Leser zum Lesen der auf dem Speichergerät gespeicherten Benutzerinformationen konfiguriert ist.
5. Ein Entschlüsselungssystem gemäß Klausel 1, bei dem das Token ferner Benutzeridentifikationsinformationen umfasst und bei dem der Leser insbesondere ferner zum Lesen der Benutzeridentifikationsinformationen von dem Token konfiguriert ist.
6. Ein Entschlüsselungssystem gemäß Klausel 7, das ferner einen Komparator zum Vergleichen der von dem Token gelesenen Benutzeridentifikationsinformationen und der von dem mit dem Benutzeridentitätsdokument assoziierten Speichergerät entschlüsselten Benutzerinformationen umfasst.
7. Ein Entschlüsselungssystem gemäß Klausel 7, das ferner einen Komparator zum Vergleichen der von dem Token gelesenen Benutzeridentifikationsinformationen und der von dem mit dem Benutzeridentitätsdokument assoziierten Speichergerät entschlüsselten Benutzerinformationen umfasst und das ferner Authentifikationsmittel zum Authentifizieren des Benutzers je nach dem Ergebnis des Vergleichs umfasst.
8. Ein Entschlüsselungssystem gemäß Klausel 1, das ferner ein mit einem Benutzer assoziiertes Mobilgerät zum Speichern des Tokens umfasst.
9. Ein Entschlüsselungssystem gemäß Klausel 1, bei dem das Token eine Bordkarte ist, auf der die Benutzeridentitätsdokumentdaten in einer bestimmten Region der Bordkarte codiert sind.
10. Ein Entschlüsselungssystem gemäß Klausel 1, das ferner ein mit einem Benutzer assoziiertes Mobilgerät zum Speichern des Tokens umfasst, wobei das Mobilgerät einen NFC-(Nahfeldkommunikation)-Chip umfasst, der kommunikativ mit dem Mobilgerät gekoppelt ist, zum Übertragen des Tokens zu dem Leser wie z. B. einem Check-in-Sicherheitsschalter an einem Flughafen.
11. Ein Entschlüsselungssystem gemäß Klausel 1, bei dem die Schlüsselkonstruktionseinheit zum Konstruieren des Schlüssels als Reaktion darauf konfiguriert ist, dass der Leser die in maschinenlesbarer Form auf oder in dem Token codierten Benutzeridentitätsdokumentdaten liest.
12. Ein Entschlüsselungssystem gemäß Klausel 1, bei dem der Identitätsdokumentleser zum Entschlüsseln der auf oder in dem Speichergerät verschlüsselten Benutzeridentifikationsinformationen als Reaktion darauf angewiesen wird, dass der Leser die Benutzeridentitätsdokumentdaten von dem Token liest.
13. Ein Entschlüsselungssystem gemäß Klausel 1, bei dem der Leser ein drahtloses Lesemittel ist, das vorzugsweise ein NFC-(Nahfeldkommunikation)-Lesemittel umfasst, das zum Kommunizieren mit einem Mobilgerät zum Speichern des Token-Speichergeräts konfiguriert ist, und ferner ein RFID-(Funkfrequenzidentifikation)-Mittel umfasst, das zum Kommunizieren mit dem Speichergerät konfiguriert ist.

14. Eine Bordkarte zur Verwendung mit dem Entschlüsselungssystem von Klausel 1, wobei die Karte Folgendes umfasst:
mit einem Benutzeridentitätsdokument assoziierte Benutzeridentitätsdokumentdaten, wobei die Daten in einer maschinenlesbaren Form codiert sind, wobei die Daten auf oder in einer vorbestimmten Region des Tokens codiert sind und wobei die Daten eine Benutzeridentitätsdokumentnummer und ein Ablaufdatum des Benutzeridentitätsdokuments und vorzugsweise das Geburtsdatum des Benutzers beinhalten.
15. Ein Token-Erzeugungssystem zum Erzeugen einer Bordkarte und dergleichen, das Folgendes umfasst:
einen Server, der zum Sammeln von Benutzeridentitätsdokumentdaten von einem Benutzer und zum Konstruieren eines Tokens wie z. B. einer Bordkarte konfiguriert ist, die die Benutzeridentitätsdokumentdaten in einer maschinenlesbaren Form codiert beinhaltet, wobei der Server zum Erzeugen des Tokens konfiguriert ist, auf dem die Daten auf oder in einer vorbestimmten Region codiert sind, und die Daten eine Benutzeridentitätsdokumentnummer und ein Ablaufdatum des Benutzeridentitätsdokuments und vorzugsweise das Geburtsdatum des Benutzers beinhalten.
16. Ein Entschlüsselungssystem zum Entschlüsseln von Benutzerinformationen, die auf einem mit einem Benutzeridentitätsdokument assoziierten Speichergerät verschlüsselt sind, wobei das System Folgendes umfasst:
einen Leser, der zum Lesen von Daten von einem Token wie z. B. einer Bordkarte und dergleichen konfiguriert ist, wobei das Token Benutzeridentitätsdokumentdaten in einer maschinenlesbaren Form codiert beinhaltet, wobei der Leser zum Lesen der auf dem Speichergerät codierten Daten konfiguriert ist; und
eine Schlüsselkonstruktionseinheit, die zum Ableiten eines Schlüssels von den auf oder in dem Token codierten Benutzeridentitätsdokumentdaten konfiguriert ist, so dass der Leser die auf dem Speichergerät gespeicherten Benutzerinformationen entschlüsseln kann.
17. Ein Entschlüsselungssystem gemäß Klausel 1, bei dem der Leser zum Lesen der Benutzeridentitätsdokumentdaten von einer vorbestimmten Region des Tokens konfiguriert ist.
18. Ein Entschlüsselungsverfahren zum Entschlüsseln von Benutzerinformationen, die auf einem mit einem Benutzeridentitätsdokument assoziierten Speichergerät verschlüsselt sind, das die folgenden Schritte beinhaltet:
Sammeln, mit einem Server, von Benutzeridentitätsdokumentdaten von dem oder einem Benutzer;
Konstruieren eines Tokens, das die in einer maschinenlesbaren Form codierten Benutzeridentitätsdokumentdaten beinhaltet;
Lesen, mit einem Leser, der Daten von dem Token;
Konstruieren, mit einer Schlüsselkonstruktionseinheit, eines Schlüssels mit den von dem Token gelesenen Benutzeridentitätsdokumentdaten, wobei der Schlüssel es ermöglicht, dass der Identitätsdokumentleser die auf dem Speichergerät gespeicherten Benutzerinformationen entschlüsselt; und
vorzugsweise Lesen, mit dem Leser, der Informationen von dem Speichergerät.
19. Ein Entschlüsselungsverfahren gemäß Klausel 18, wobei die Schlüsselkonstruktionseinheit den Schlüssel auf der Basis von einem oder mehreren aus Benutzeridentitätsdokumentnummer, Ablaufdatum des Benutzeridentitätsdokuments und vorzugsweise dem Geburtsdatum eines Benutzers ableitet.
20. Ein Entschlüsselungsverfahren gemäß Klausel 18, wobei der oder ein Benutzer die Benutzeridentitätsdokumentdaten manuell eingibt, bevor die auf dem Token codierten Daten gelesen werden.
21. Ein Entschlüsselungsverfahren gemäß Klausel 18, das ferner den Schritt des Lesens der auf dem Speichergerät gespeicherten Benutzerinformationen beinhaltet.
22. Ein Entschlüsselungsverfahren gemäß Klausel 18, bei dem das Token ferner Benutzeridentifikationsinformationen umfasst und das insbesondere den Schritt des Lesens der Benutzeridentifikationsinformationen von dem Token beinhaltet.
23. Ein Entschlüsselungsverfahren gemäß Klausel 18, bei dem das Token ferner Benutzeridentifikationsinformationen umfasst und das insbesondere den Schritt des Lesens der Benutzeridentifikationsinformationen von dem Token beinhaltet und das ferner den Schritt des Vergleichens der von dem Token gelesenen Benutzeridentifikationsinformationen und der von dem mit dem Benutzeridentitätsdokument assoziierten Speichergerät entschlüsselten Benutzerinformationen beinhaltet.
24. Ein Entschlüsselungsverfahren gemäß Klausel 18, bei dem das Token ferner Benutzeridentifikationsinformationen umfasst und das insbesondere den Schritt des Lesens der Benutzeridentifikationsinformationen von dem Token beinhaltet und ferner den Schritt des Vergleichens der von dem Token gelesenen Benutzeridentifikationsinformationen und der von dem mit dem Benutzeridentitätsdokument assoziierten Speichergerät entschlüsselten Benutzerinformationen und das Authentifizieren des Benutzers je nach dem Ergebnis des Vergleichs beinhaltet.
25. Ein Entschlüsselungsverfahren gemäß Klausel 18, das ferner ein mit einem Benutzer assoziiertes Mobilgerät zum Speichern des Tokens umfasst.

26. Ein Entschlüsselungsverfahren gemäß Klausel 18, bei dem das Token eine Bordkarte ist, das ferner den Schritt des Codierens der Benutzeridentitätsdokumentdaten in einer vorbestimmten Region der Bordkarte beinhaltet.
27. Ein Entschlüsselungsverfahren gemäß Klausel 18, das ferner ein mit einem Benutzer assoziiertes Mobilgerät zum Speichern des Tokens umfasst, wobei das Mobilgerät einen NFC-(Nahfeldkommunikation)-Chip umfasst, der kommunikativ mit dem Mobilgerät gekoppelt ist, zum Übertragen des Tokens zu dem Leser wie z. B. einem Check-in-Sicherheitsschalter an einem Flughafen.
28. Ein Entschlüsselungsverfahren gemäß Klausel 18, das ferner den Schritt des Konstruierens des Schlüssels als Reaktion auf das Lesen der in maschinenlesbarer Form auf oder in dem Token codierten Benutzeridentitätsdokumentdaten beinhaltet.
29. Ein Entschlüsselungsverfahren gemäß Klausel 18, bei dem der Identitätsdokumentleser zum Entschlüsseln der auf dem Speichergerät verschlüsselten Benutzerinformationen als Reaktion auf das Lesen der Benutzeridentitätsdokumentdaten von dem Token angewiesen wird.
30. Ein Entschlüsselungsverfahren gemäß Klausel 18, bei dem der Leser ein drahtloses Lesemittel ist, das vorzugsweise ein NFC-(Nahfeldkommunikation)-Lesemittel umfasst, das zum Kommunizieren mit einem Mobilgerät zum Speichern des Token-Speichergeräts konfiguriert ist und ferner RFID (Funkfrequenzidentifikation) umfasst, das ferner den Schritt des Kommunizierens mit dem Speichergerät beinhaltet.
31. Ein Token-Erzeugungsverfahren zum Erzeugen einer Bordkarte und dergleichen, das die folgenden Schritte beinhaltet:
Sammeln, mit einem Server, von Benutzeridentitätsdokumentdaten von einem Benutzer;
Konstruieren, mit einer Schlüsselkonstruktionseinheit, eines Tokens wie z. B. einer Bordkarte, das die Benutzeridentitätsdokumentdaten in einer maschinenlesbaren Form codiert beinhaltet; und
Erzeugen, mit dem oder einem Server, des Tokens mit den auf oder in einer vorbestimmten Region codierten Daten, wobei die Daten eine Benutzeridentitätsdokumentnummer und ein Ablaufdatum des Benutzeridentitätsdokuments und vorzugsweise das Geburtsdatum des Benutzers beinhalten.
32. Ein Entschlüsselungsverfahren zum Entschlüsseln von auf einem mit einem Benutzeridentitätsdokument assoziierten Speichergerät verschlüsselten Benutzerinformationen, wobei das Verfahren die folgenden Schritte beinhaltet:
Lesen, mit einem Leser, von Daten von einem Token wie z. B. einer Bordkarte und dergleichen, wobei das Token in einer maschinenlesbaren Form codierte Benuzeridentitätsdokumentdaten beinhaltet;
Ableiten, mit einer Schlüsselkonstruktionseinheit, eines Schlüssels anhand der auf oder in dem Token codierten Benutzeridentitätsdokumentdaten; und
Entschlüsseln der auf dem Speichergerät gespeicherten Benutzerinformationen mit dem abgeleiteten Schlüssel.
33. Ein Entschlüsselungsverfahren gemäß Klausel 18 oder 32, das ferner den Schritt des Lesens der Benutzeridentitätsdokumentdaten von einer vorbestimmten Region des Tokens beinhaltet, und wobei vorzugsweise der Leser die auf dem Speichergerät codierten Daten liest.
34. Ein Computerprogrammprodukt, das bei Ausführung das Verfahren gemäß Klausel 18 oder 32 ausführt.
35. Ein Entschlüsselungssystem zum Entschlüsseln von Benutzerinformationen, die auf einem mit einem Benutzeridentitätsdokument assoziierten Speichergerät verschlüsselt sind, wobei das System Folgendes umfasst:
einen Server, der zum Sammeln von Benutzeridentitätsdokumentdaten von dem oder einem Benutzer und zum Konstruieren eines Tokens konfiguriert ist, das die Benutzeridentitätsdokumentdaten beinhaltet;
einen Leser, der zum Lesen der Daten von dem Token konfiguriert ist, wobei der Leser die von dem Token gelesenen Benutzeridentitätsdokumentdaten zum Entschlüsseln der auf dem Speichergerät gespeicherten Benutzerinformationen benutzt.
36. Ein Entschlüsselungssystem gemäß Klausel 35, wobei der Leser ein tragbarer Leser oder Scanner wie z. B. ein Mobiltelefon ist.
37. Ein Entschlüsselungssystem gemäß Klausel 35, bei dem das Benutzeridentitätsdokument ein Pass ist und bei dem vorzugsweise das Benutzeridentitätsdokument oder der Pass zuvor auf einem Mobilkommunikationsgerät vorzugsweise auf eine gesicherte Weise gespeichert wird.
38. Das Entschlüsselungssystem gemäß einer der Klauseln 1 bis 17, das ferner den Schritt des Lesens eines biometrischen Gesichtsbildes auf einem Benutzeridentitätsdokument mit dem Schlüssel beinhaltet.
39. Das Entschlüsselungssystem gemäß einer der Klauseln 1 bis 17 oder 38, das ferner den Schritt des Erfassens eines Bildes des Benutzers mit einer Kamera und vorzugsweise das Vergleichen des erfassten Bildes mit dem von dem Benutzeridentitätsdokument gelesenen biometrischen Gesichtsbild des Passes beinhaltet.

Schutzansprüche

1. Entschlüsselungssystem zum Entschlüsseln von Benutzerinformationen, die auf einem mit einem Identitätsdokument eines Benutzers assoziierten Speichergerät verschlüsselt sind, wobei das System Folgendes umfasst:
einen Server, der zum Sammeln von Benutzeridentitätsdokumentdaten vom Benutzer und zum Konstruieren eines die Benutzeridentitätsdokumentdaten umfassenden Tokens konfiguriert ist, wobei der Server ferner zum Senden des Tokens zu einem mit dem Benutzer assoziierten Mobilgerät zum Speichen des Tokens auf dem Mobilgerät konfiguriert ist, und wobei das Mobilgerät physisch von dem genannten Speichergerät getrennt ist;
eine Schlüsselkonstruktionseinheit, kommunikativ mit einem Maschinenleser gekoppelt, der zum Lesen der Daten von dem Token durch Funkfrequenz-Identifikationskommunikation mit dem Mobilgerät konfiguriert ist,
wobei das Token ferner Benutzeridentifikationsinformationen umfasst und wobei der Leser insbesondere ferner zum Lesen der Benutzeridentifikationsinformationen von dem Token konfiguriert ist und wobei die Schlüsselkonstruktionseinheit die von dem auf dem Mobilgerät gespeicherten Token gelesenen Benutzeridentifikationsinformationen zum Konstruieren eines Schlüssels zum Entschlüsseln der auf dem genannten Speichergerät gespeicherten Benutzerinformationen benutzt;
einen Komparator zum Vergleichen der von dem auf dem Mobilgerät gespeicherten Token gelesenen Benutzeridentifikationsinformationen und der von dem genannten Speichergerät entschlüsselten Benutzerinformationen in Verbindung mit dem Benutzeridentitätsdokument; und
Authentifikationsmittel zum Authentifizieren des Benutzers je nach dem Ergebnis des Vergleichs.

2. Entschlüsselungssystem nach Anspruch 1, wobei die Schlüsselkonstruktionseinheit den Schlüssel auf der Basis von einem oder mehreren aus Benutzeridentitätsdokumentnummer, Ablaufdatum des Benutzeridentitätsdokuments und Geburtsdatum des Benutzers ableitet.

3. Entschlüsselungssystem nach einem vorherigen Anspruch, wobei der Benutzer die Benutzeridentitätsdokumentdaten manuell eingibt, bevor der Leser die auf dem Token codierten Daten liest.

4. Entschlüsselungssystem nach einem vorherigen Anspruch, wobei der Leser zum Lesen der auf dem Speichergerät gespeicherten Benutzerinformationen konfiguriert ist.

5. Entschlüsselungssystem nach einem vorherigen Anspruch, wobei das Token eine Bordkarte ist, auf der die Benutzeridentitätsdokumentdaten in einer speziellen Region der Bordkarte codiert sind.

6. Entschlüsselungssystem nach einem vorherigen Anspruch, wobei das Mobilgerät einen NFC-(Nahfeldkommunikation)-Chip umfasst, der kommunikativ mit dem Mobilgerät gekoppelt ist, zum Übertragen des Tokens zu dem Leser.

7. Entschlüsselungssystem nach einem vorherigen Anspruch, wobei die Schlüsselkonstruktionseinheit zum Konstruieren des Schlüssels als Reaktion darauf konfiguriert ist, dass der Leser die in einer maschinenlesbaren Form auf oder in dem Token codierten Benutzeridentitätsdokumentdaten liest.

8. Entschlüsselungssystem nach einem vorherigen Anspruch, wobei der Identitätsdokumentleser zum Entschlüsseln der auf oder in dem Speichergerät verschlüsselten Benutzeridentifikationsinformationen als Reaktion auf das Lesen der Benutzeridentitätsdokumentdaten von dem Token durch den Leser angewiesen wird.

9. Entschlüsselungssystem nach einem vorherigen Anspruch, wobei der Leser ein drahtloses Lesemittel ist.

10. Entschlüsselungssystem nach Anspruch 9, wobei das drahtlose Lesemittel ein NFC-(Nahfeldkommunikation)-Lesemittel, das zum Kommunizieren mit einem Mobilgerät zum Speichern des Token-Speichergeräts konfiguriert ist, und ferner ein RFID-(Funkfrequenzidentifikation)-Lesemittel umfasst, das zum Kommunizieren mit dem Speichergerät konfiguriert ist.

11. Entschlüsselungssystem nach einem vorherigen Anspruch, wobei der Leser zum Lesen der Benutzeridentitätsdokumentdaten von einer vorbestimmten Region des Tokens konfiguriert ist.

12. Entschlüsselungssystem nach einem vorherigen Anspruch, wobei der Leser ein tragbarer Leser oder Scanner oder ein Mobiltelefon ist.

13. Entschlüsselungssystem nach einem vorherigen Anspruch, wobei das Benutzeridentitätsdokument ein Pass ist und wobei das Benutzeridentitätsdokument oder der Pass auf einem mobilen Kommunikationsgerät auf eine gesicherte Weise vorgespeichert ist.

14. Entschlüsselungssystem nach einem vorherigen Anspruch, das ferner Mittel zum Lesen eines biometrischen Gesichtsbildes des Benutzeridentitätsdokuments von dem Speichergerät anhand der von dem Token gelesenen Benutzeridentitätsdokumentdaten umfasst.

15. Entschlüsselungssystem nach einem vorherigen Anspruch, das ferner Mittel zum Erfassen eines Bildes des Benutzers mit einer Kamera umfasst und Vergleichsmittel zum Vergleichen des erfassten Bildes mit dem vom Benutzeridentitätsdokument gelesenen biometrischen Gesichtsbild des Passes umfasst.

16. Token-Erzeugungssystem zum Erzeugen einer Bordkarte, das Folgendes umfasst:
einen Server, der zum Sammeln von Benutzeridentitätsdokumentdaten und Benutzeridentifikationsinformationen von einem Benutzer und zum Konstruieren eines Bordkartentokens konfiguriert ist, das die in einer maschinenlesbaren Form codierten Benutzeridentitätsdokumentdaten und Benutzeridentifikationsinformationen beinhaltet, wobei der Server zum Erzeugen des Tokens mit den auf oder in einer vorbestimmten Region codierten Daten konfiguriert ist und die Daten eine Benutzeridentitätsdokumentnummer, ein Ablaufdatum des Benutzeridentitätsdokuments und das Geburtsdatum des Benutzers beinhalten, wobei das System ferner zum Senden des Tokens zu einem mit einem Benutzer assoziierten Mobilgerät zum Speichern des Tokens auf dem Mobilgerät konfiguriert ist; und wobei
ein Speichergerät, separat von dem Mobilgerät, konfiguriert zum Speichern von mit dem Benutzeridentitätsdokument assoziierten verschlüsselten Benutzerinformationen;
eine Schlüsselkonstruktionseinheit, kommunikativ gekoppelt mit einem Maschinenleser, konfiguriert zum Lesen von Daten von dem Token, das auf dem Mobilgerät gespeichert ist, assoziiert mit dem Benutzer durch Funkfrequenz-Identifikationskommunikation mit dem Mobilgerät, und wobei die Schlüsselkonstruktionseinheit ferner die von dem Token gelesenen Benutzeridentitätsdokumentdaten zum Konstruieren eines Schlüssels zum Entschlüsseln der auf dem genannten Speichergerät verschlüsselten Benutzerinformationen benutzt;
einen Komparator zum Vergleichen der von dem auf dem Mobilgerät gespeicherten Token gelesenen Benutzeridentifikationsinformationen und der von dem genannten Speichergerät entschlüsselten Benutzerinformationen, die mit dem Benutzeridentitätsdokument assoziiert sind; und
Authentifikationsmittel zum Authentifizieren des Benutzers in Abhängigkeit von dem Ergebnis des Vergleichs.

17. Bordkarte zur Verwendung mit dem Entschlüsselungssystem nach einem vorherigen Anspruch, wobei die Karte Folgendes umfasst:
mit einem Benutzeridentitätsdokument assoziierte Benutzeridentitätsdokumentdaten und Benutzeridentifikationsinformationen, wobei die Daten in einer maschinenlesbaren Form codiert sind, wobei die Daten auf oder in einer vorbestimmten Region des Tokens codiert sind und wobei die Daten eine Benutzeridentitätsdokumentnummer und ein Ablaufdatum des Benutzeridentitätsdokuments und das Geburtsdatum des Benutzers beinhalten.

Es folgen 6 Seiten Zeichnungen

Anhängende Zeichnungen

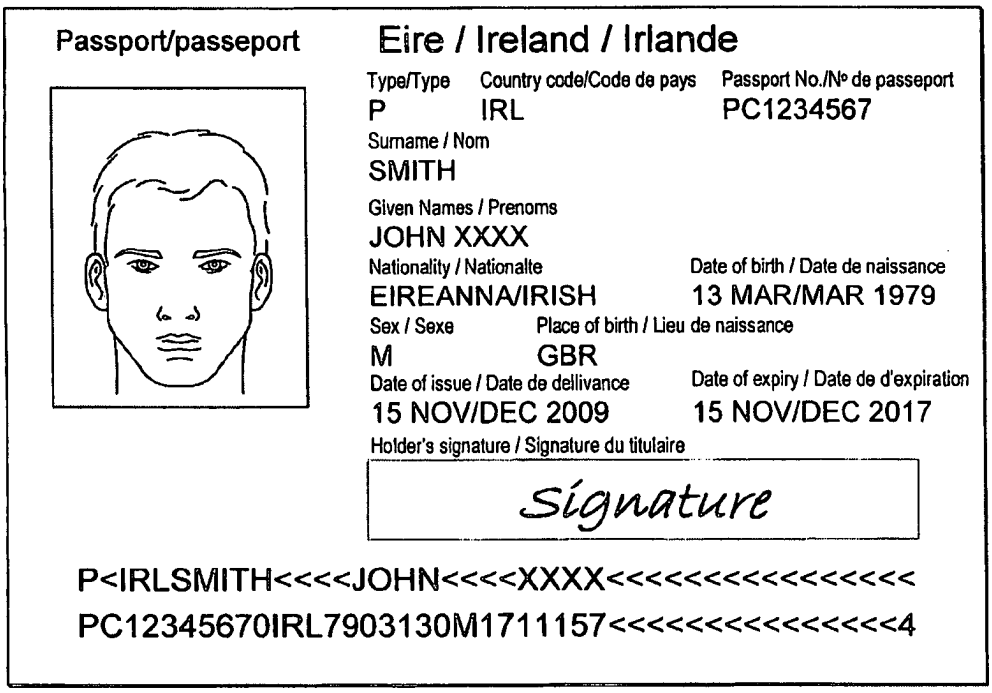


FIG. 1

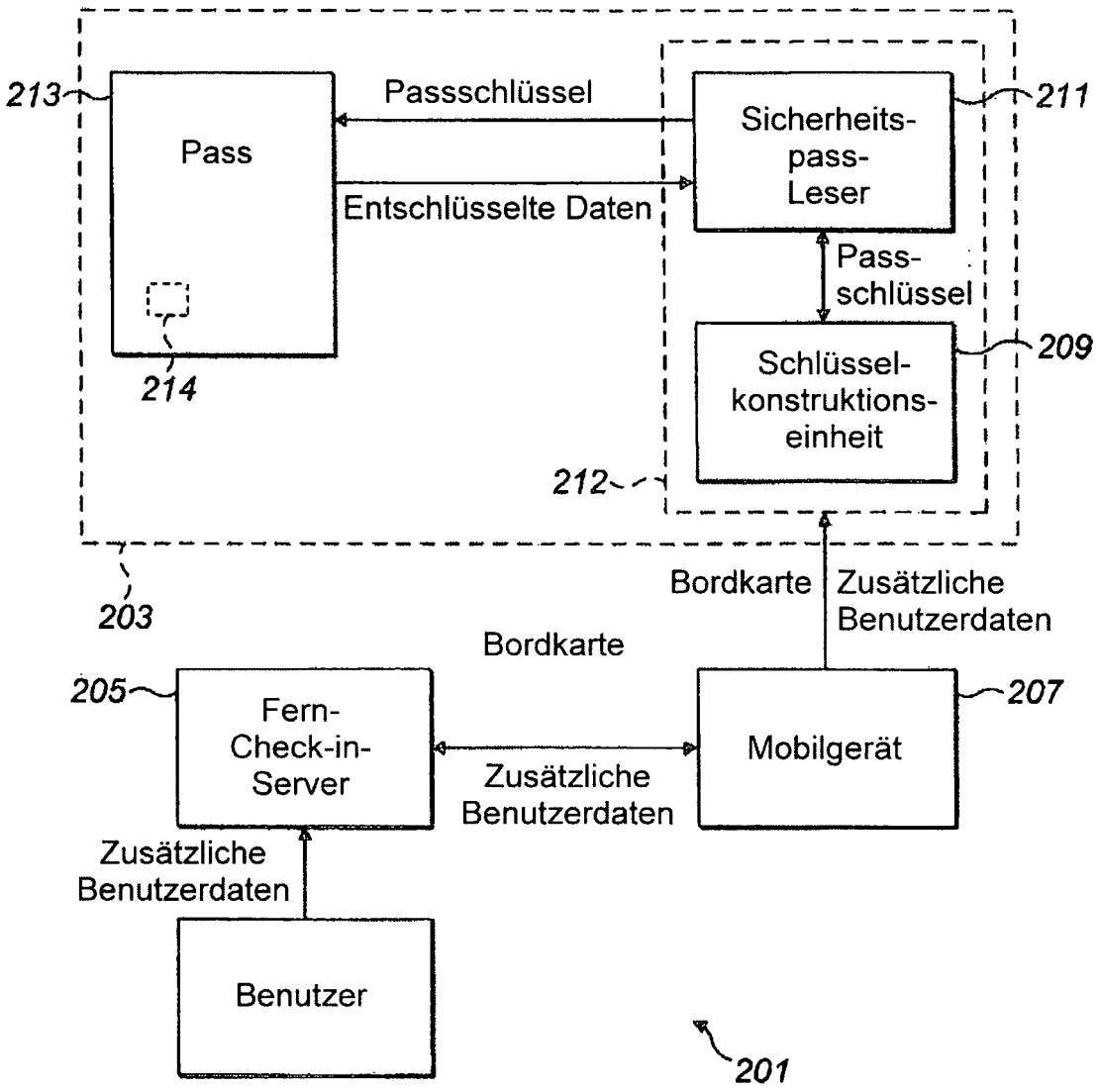

213
Pass
214
Passschlüssel
Entschlüsselte Daten
211
Sicherheits-
pass-
Leser
Pass-
schlüssel
209
Schlüssel-
konstruktions-
einheit
212
203
Bordkarte
Zusätzliche
Benutzerdaten
Bordkarte
205
Fern-
Check-in-
Server
Zusätzliche
Benutzerdaten
207
Mobilgerät
Zusätzliche
Benutzerdaten
Benutzer
201

FIG. 2

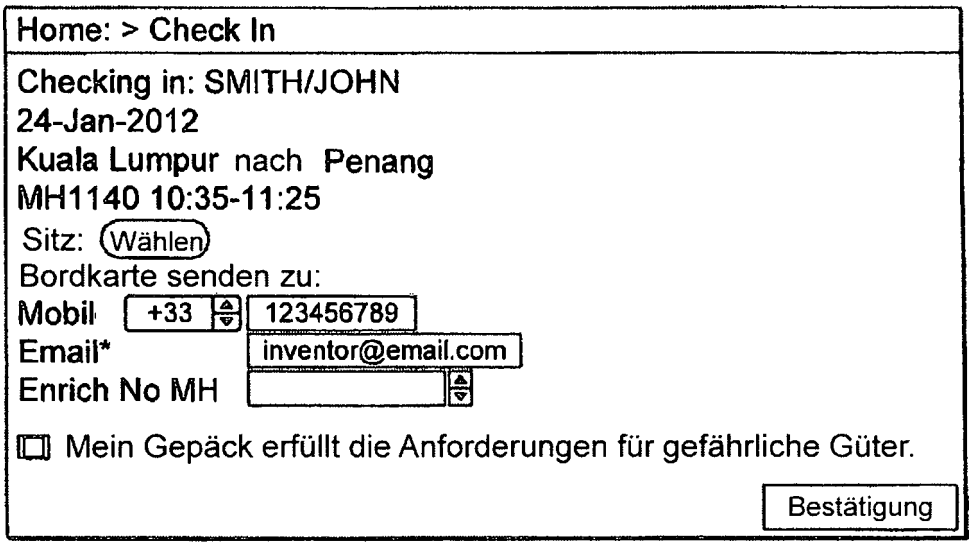

Home: > Check In
Checking in: SMITH/JOHN
24-Jan-2012
Kuala Lumpur nach Penang
MH1140 10:35-11:25
Sitz: Wählen
Bordkarte senden zu:
Mobil +33 123456789
Email* inventor@email.com
Enrich No MH
Mein Gepäck erfüllt die Anforderungen für gefährliche Güter.
Bestätigung

FIG. 3a

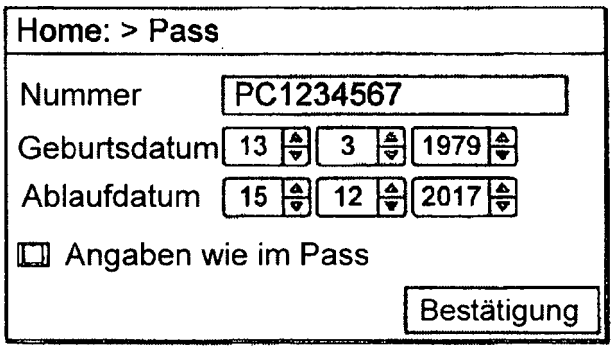

Home: > Pass
Nummer PC1234567
Geburtsdatum 13 3 1979
Ablaufdatum 15 12 2017
Angaben wie im Pass
Bestätigung

FIG. 3b

SITA Labs - Security Checkpoint

Passenger Name	SMITH/JOHN
Airline	MH
Flight Number	1140
Departure Date	24Jan
Departure City	KUL
Arrival City	PEN
Seat Number	001D
Class	F
Frequent Flyer	MH
E-ticket	2322274421
Boarding Time	10:05 Gate Not Assigned
Document Number	PC1234567
Date of Birth	13/03/1979
Date of Expiry	15/11/2017

Approve Deny

FIG. 4

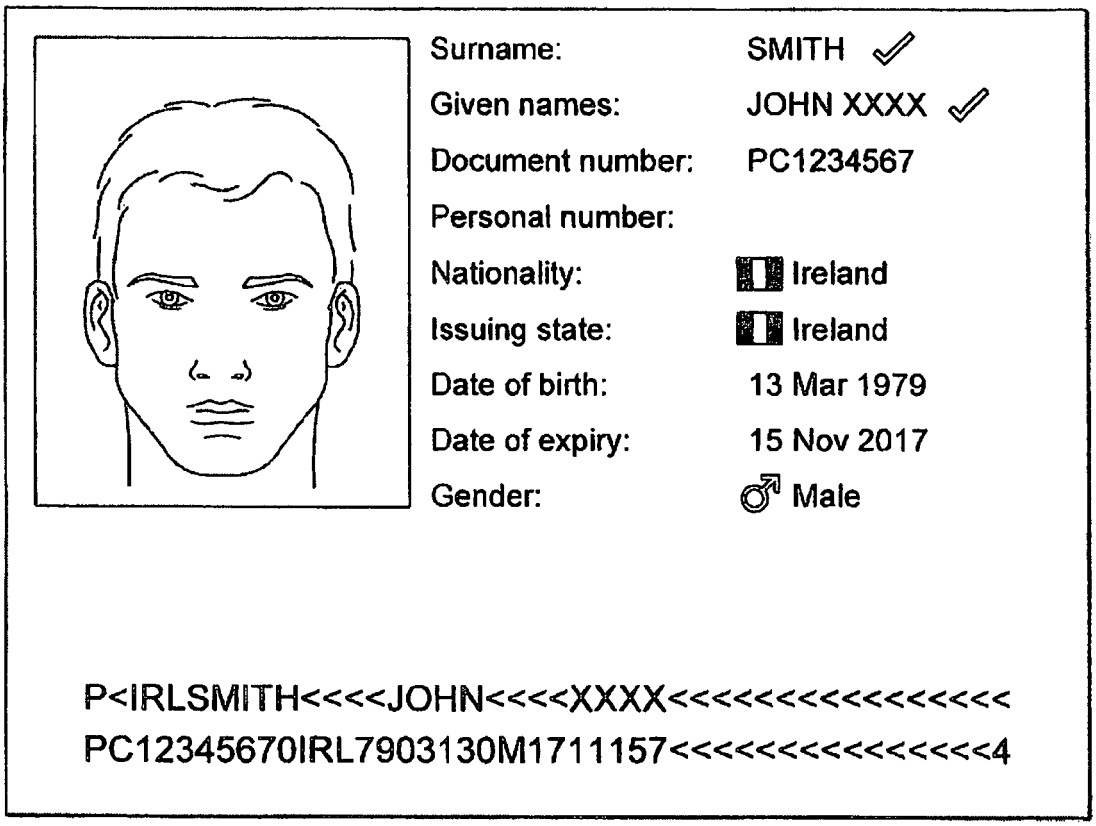

Surname: SMITH
Given names: JOHN XXXX
Document number: PC1234567
Personal number:
Nationality: Ireland
Issuing state: Ireland
Date of birth: 13 Mar 1979
Date of expiry: 15 Nov 2017
Gender: Male
P<IRLSMITH<<<<JOHN<<<<XXXX<<<<<<<<<<<<<<<<
PC12345670IRL7903130M1711157<<<<<<<<<<<<<<4

FIG. 5

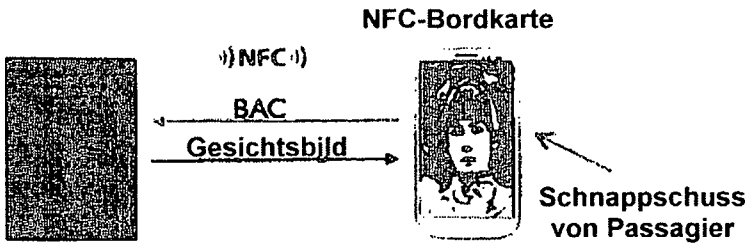

NFC-Bordkarte
NFC
BAC
Gesichtsbild
Schnappschuss
von Passagier

FIG. 6

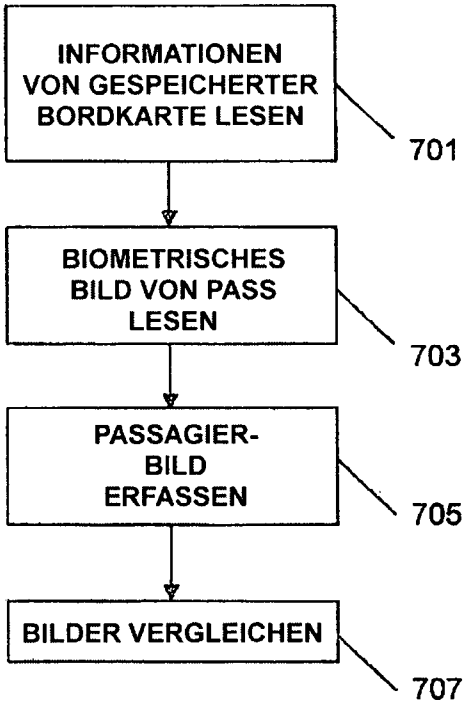

INFORMATIONEN VON GESPEICHERTER BORDKARTE LESEN
701
BIOMETRISCHES BILD VON PASS LESEN
703
PASSAGIER-BILD ERFASSEN
705
BILDER VERGLEICHEN
707

FIG. 7