(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 377 548**

(51) Int. CI.:
G06K 19/07 (2006.01)
G06K 19/077 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09761943 .1**
(96) Fecha de presentación: **29.04.2009**
(97) Número de publicación de la solicitud: **2286372**
(97) Fecha de publicación de la solicitud: **23.02.2011**

(54) Título: **Documento de seguridad. Sistemas y métodos de seguridad para controlar el acceso a una zona**

(30) Prioridad:
12.06.2008 GB 0810807
06.10.2008 GB 0818272

(45) Fecha de publicación de la mención BOPI:
28.03.2012

(45) Fecha de la publicación del folleto de la patente:
28.03.2012

(73) Titular/es:
De La Rue International Limited
De La Rue House Jays Close
Basingstoke, Hampshire RG22 4BS, GB

(72) Inventor/es:
GREEN, Stephen Banister

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Documento de seguridad. Sistemas y métodos de seguridad para controlar el acceso a una zona.

Esta invención está relacionada con documentos y sistemas de seguridad, en particular pasaportes y tarjetas de identificación, pero podría aplicarse a cualquier tipo documento, y con métodos para controlar el acceso a una zona, en particular, métodos de inmigración.

Se sabe cómo mejorar la seguridad de un documento mediante la incorporación de un almacén de datos sin contacto en el documento, en forma de una etiqueta de RFID. Normalmente, la etiqueta de RFID se programa en el momento de fabricar el documento con los datos relacionados con el propietario del documento. Esto no sólo vuelve el documento más difícil de falsificar o modificar, sino que también mejora la comprobación de la validez del documento ya que esto puede automatizarse hasta cierto punto. El documento DE 10 2005 062 827 A1 describe tal documento de seguridad.

Convencionalmente, las etiquetas de RFID incorporadas en pasaportes son etiquetas de RFID de Alta Frecuencia (HF), que funcionan en una frecuencia de 13,56 MHz. Se prefieren las etiquetas de RFID de HF ya que pueden almacenar un volumen razonable de datos y sólo pueden ser leídas a corta distancia. Preferiblemente, esta distancia es menos de 1 metro, pero si se desea podría ser de hasta 1,5 metros o, si se utiliza un lector de gran potencia, un máximo de alrededor de 3 metros. Esto restringe la zona dentro de que la que se puede interrogar a la etiqueta de RFID, y así se salvaguardan los datos guardados en el chip para preservar la intimidad del usuario. Para proteger aún más los datos en el chip, el documento puede incluir un protector electromagnético tal como una capa de malla metálica, que impide que el chip sea leído hasta que (por ejemplo) el libro de pasaporte sea abierto.

Es deseable mejorar la seguridad de tales documentos cuando sea posible para aumentar la dificultad de falsificación del documento y para mejorar la detección de tales falsificaciones. Además es deseable agilizar la comprobación de tales documentos.

De acuerdo con un primer aspecto de la presente invención, un documento de seguridad comprende una primera etiqueta de RFID legible sólo dentro de un primer alcance, y una segunda etiqueta de RFID legible dentro de un segundo alcance, la primera etiqueta de RFID contiene los datos que pertenecen al propietario del documento de seguridad y un código de identificación, y la segunda etiqueta de RFID contiene el mismo código de identificación o uno relacionado, y en el que el segundo alcance es mayor que el primer alcance.

Al proporcionar de esta manera al documento dos etiquetas de RFID con códigos relacionados entre sí, se mejora la seguridad ya que la eliminación o sustitución de cualquier etiqueta se detectaría fácilmente. Además, el uso de la etiqueta de RFID de más largo alcance no compromete la intimidad del usuario ya que contiene un código de identificación en vez de datos personales. Los códigos de identificación contenidos por las primeras y segundas etiquetas de RFID pueden ser idénticos o en cambio pueden estar relacionados entre sí, por ejemplo a través de una base de datos que pone en correlación cada código de identificación de una primera etiqueta de RFID con un determinado código de identificación de la segunda etiqueta de RFID. Como alternativa, uno u otro de los códigos de identificación podrían incluir todo o parte del otro código.

Preferiblemente, el primer alcance comprende una máxima distancia de lectura de entre cero y aproximadamente 3 metros de la primera etiqueta de RFID, preferiblemente entre cero y aproximadamente 1 metro de la primera etiqueta de RFID. La primera etiqueta de RFID no es legible desde fuera de la máxima distancia de lectura, pero es legible desde cualquier lugar dentro de la máxima distancia de lectura (es decir entre la primera etiqueta de RFID y la máxima distancia de lectura).

Ventajosamente, el segundo alcance comprende una máxima distancia de lectura de sobre aproximadamente 1 metro de la segunda etiqueta de RFID, preferiblemente sobre aproximadamente 3 metros de la segunda etiqueta de RFID, todavía preferiblemente sobre aproximadamente 10 metros de la segunda etiqueta de RFID. Según se ha indicado anteriormente, la máxima distancia de lectura de la segunda etiqueta de RFID es mayor que el de la primera. La segunda etiqueta de RFID es legible desde cualquier sitio dentro de su máxima distancia de lectura.

En una realización preferida, el código de identificación identifica la segunda etiqueta de RFID, y en la primera etiqueta de RFID se programa el mismo código de identificación. Como alternativa, el código de identificación identifica la primera etiqueta de RFID, y en la segunda etiqueta de RFID se programa el mismo código de identificación.

Preferiblemente, los datos contenidos en la primera etiqueta de RFID incluyen los datos personales relacionados con el propietario (p. ej. datos biográficos) y/o los datos biométricos relacionados con el propietario, preferiblemente datos de huellas dactilares, plantillas de iris y/o datos de reconocimiento facial.

Ventajosamente, la primera etiqueta de RFID comprende un chip de RFID de Alta Frecuencia (HF), y la segunda etiqueta de RFID comprende un chip de RFID de Ultra Alta Frecuencia (UHF). En determinadas realizaciones, el

chip de RFID de HF funciona en una frecuencia en el intervalo de 3 MHz a 29 MHz, preferiblemente de 13 MHz a 14 MHz, todavía preferiblemente aproximadamente a 13,56 MHz. Ventajosamente, el chip de RFID de UHF funciona en una frecuencia en el intervalo de 433 a 950 MHz, preferiblemente de 860 a 870 MHz.

En algunas realizaciones preferidas, las etiquetas primeras y segundas de RFID se forman integralmente en un único chip.

Preferiblemente, la segunda etiqueta de RFID no contiene datos pertenecientes al propietario del documento.

Para el uso en la presente invención se prefieren las etiquetas de RFID pasivas, en vez de las activas. Las etiquetas de RFID pasivas se basan enteramente en el lector como fuente de alimentación, y no es necesario que estén provistas de una batería o algo similar. Las etiquetas pasivas de RFID de UHF pueden leerse normalmente hasta a 10 m de distancia, y tienen menores costes de producción que las etiquetas de RFID activas o semi-pasivas.

Sin embargo, las etiquetas de RFID activas y semi-pasivas también son adecuadas para la presente invención. Las etiquetas de RFID activas y semi-pasivas utilizan baterías internas para alimentar a sus circuitos. Una etiqueta activa también utiliza su batería para transmitir ondas de radio a un lector, mientras que una etiqueta semi-pasiva depende del lector para suministrar su energía para la transmisión. Como estas etiquetas contienen más hardware que las etiquetas de RFID pasivas, son más caras. Las etiquetas de RFID de UHF activas y semi-pasivas se reservan generalmente para aplicaciones que requieren que el documento sea leído a mayores distancias y ellas transmiten normalmente altas frecuencias de 850 a 950 MHz que pueden ser leídas a 30 m o más lejos.

El primer aspecto de la invención proporciona además un sistema de seguridad que comprende una pluralidad de documentos de seguridad, cada uno como se ha descrito anteriormente, el código de identificación de cada documento de seguridad es único para ese documento de seguridad, un primer lector adaptado para leer los datos de las primeras etiquetas de RFID, un segundo lector adaptado para leer los datos de las segundas etiquetas de RFID, una base de datos que tiene registros de datos que contienen los detalles de cada propietario de documento de seguridad y el correspondiente código de identificación, y un procesador adaptado para, tras el reconocimiento de un código de identificación por parte del primer o segundo lector, recuperar el correspondiente registro de la base de datos.

Los primeros y segundos lectores pueden, en la práctica, combinarse en una única unidad que se puede configurar para leer cada una de las primeras y segundas etiquetas de RFID.

Preferiblemente, el procesador se enlaza además con por lo menos una base de datos externa y se adapta además para recuperar registros correspondientes al propietario del documento de seguridad identificado de por lo menos una base de datos externa.

Según un segundo aspecto de la invención, se proporciona un sistema de comprobación biométrica, que comprende un lector de etiquetas de RFID para leer los datos de un documento de seguridad que tiene por lo menos una etiqueta de RFID, cada etiqueta de RFID contiene un código de identificación que identifica el documento de seguridad, por lo menos un módulo de entrada biométrica para probar un parámetro biométrico de un poseedor del documento de seguridad, una base de datos que tiene registros de datos que contienen detalles de cada propietario de documento de seguridad y el correspondiente código de identificación, y un procesador adaptado para, tras el reconocimiento de un código de identificación, recuperar los correspondientes registros de datos y comparar la salida del módulo de comprobación biométrica con datos biométricos en el registro recuperado de datos para determinar si el poseedor de la tarjeta de seguridad coincide con los registros de datos para el propietario del documento de seguridad.

Al recuperar el perfil del propietario del documento, el sistema puede llevar a cabo una comparación de uno con uno de la entrada biométrica con los datos almacenados para ese usuario, para determinar si hay una coincidencia. Esto requiere significativamente menos capacidad de procesamiento que comparar la entrada biométrica con todos los registros de datos para identificar al poseedor (es decir llevando a cabo una comparación de uno con uno), y así que se acelera el proceso de comprobación.

Preferiblemente, el lector de etiquetas de RFID se adapta para leer la etiqueta de RFID desde una distancia de sobre aproximadamente 1 metro de la etiqueta de RFID, preferiblemente sobre aproximadamente 3 metros de la etiqueta de RFID, todavía preferiblemente sobre aproximadamente 10 metros de la etiqueta de RFID. Ventajosamente, el lector de etiquetas de RFID es un lector de etiquetas de RFID de Ultra Alta Frecuencia (UHF) y cada etiqueta de RFID es una etiqueta de RFID de UHF.

Preferiblemente, el módulo(s) de entrada biométrica está adaptado para explorar el patrón del iris y/o huellas dactilares del poseedor, y/o realizar un reconocimiento facial.

En una realización preferida, el lector de etiquetas de RFID se sitúa a distancia de los módulos de entrada biométrica. Esto puede permitir que el perfil del propietario sea recuperado antes de que el poseedor llegue al

módulo de entrada biométrica. Ventajosamente, el lector de etiquetas de RFID se sitúa en una entrada a una zona de control que contiene los módulos de entrada biométrica.

Un problema al que hacen frente muchos sistemas de inmigración es cómo mejorar la velocidad de verificación de cada pasajero y, en última instancia, mejorar el régimen de paso de pasajeros. Por ejemplo, es común experimentar largas colas en aeropuertos, puertos de embarque y lugares por el estilo mientras se examina y comprueba con otros registros el pasaporte de cada persona u otro documento de seguridad.

De acuerdo con un tercer aspecto de la presente invención, se proporciona un método para el control del acceso a una zona, cada persona que busca el acceso lleva una identificación única detectable, el método comprende:

detectar, en una primera ubicación, una identificación única relacionada con una persona en la primera ubicación;

utilizar la identificación única detectada para recuperar información con respecto a la persona de una o más bases de datos externas;

suministrar la información recuperada a una segunda ubicación a distancia de la primara ubicación; y

utilizar, en la segunda ubicación, la información recuperada para tomar una decisión en cuanto a si permitir el acceso de la persona que lleva la identificación única a la zona controlada.

A detectar una identificación única, tal como un número de pasaporte o número de chip, etc., en una primera ubicación y utilizar esto para recuperar información tal como el perfil del propietario del documento de bases de datos externas (es decir bases de datos que se mantienen generalmente separadas del sistema de inmigración), los detalles de cada propietario (es decir la persona a que corresponde la identificación única) se puede obtener sin que el poseedor deba presentar el documento de seguridad a un inspector. A continuación se puede tomar una decisión (por ejemplo si permitir o no la entrada del poseedor) en una segunda ubicación sin necesitad de detener al poseedor durante mucho tiempo mientras se comprueban los registros, permitiendo de este modo un régimen de paso mucho más grande. Esto puede utilizarse por ejemplo en aeropuertos u otras terminales de transporte, o en fronteras entre países.

La primera ubicación se sitúa con ventaja para cubrir un área por la que deben pasar todas las personas que desean entrar a la zona controlada (por ejemplo las personas que entran al aeropuerto desde un avión). La segunda ubicación es espaciada de alguna manera de la primera a lo largo del camino seguido por las personas. Por ejemplo, la segunda ubicación puede situarse poco antes o poco después del vestíbulo de equipajes en un aeropuerto, como es el caso para el control convencional de pasaporte. Preferiblemente, las dos ubicaciones se espacian lo suficiente para que las personas que andan desde la primera ubicación a la segunda ubicación tarden por lo menos un tiempo mínimo predeterminado en hacerlo. Esto se mide para proporcionar el tiempo suficiente para que los datos pertinentes sean recuperados y sean suministrados a la segunda ubicación. En la práctica, esto es preferiblemente menos de 60 segundos y, más preferiblemente, menos de 30 segundos.

Sin embargo, el sistema también podría implementarse estando las primeras y segundas ubicaciones más separadas entre sí de manera significativa. Por ejemplo, la primera ubicación podría estar en una puerta de embarque en un aeropuerto en el que se detectan las identificaciones únicas llevadas por los pasajeros que embarcan en un avión. La segunda ubicación podría estar en el aeropuerto de destino.

Los datos recuperados podrían suministrarse directamente (es decir en su forma sin tratar) a la segunda ubicación en forma de una alarma, mensaje u otra transmisión, tal como un correo electrónico. Sin embargo, preferiblemente, el método comprende agregar la información recuperada a una base de datos transitoria relacionada con esas personas para las que se han detectado las identificaciones únicas, en el que la información recuperada es suministrada a la segunda ubicación mediante el acceso a la base de datos transitoria. De esta manera la información puede verse rápidamente, puesto que ya se ha accedido y almacenado localmente, al tiempo que se minimizan los requisitos de almacenamiento de datos de la propia segunda ubicación y se libera ancho de banda de las comunicaciones. La llegada de la identificación única detectable a la segunda ubicación podría ser utilizada para provocar la recuperación de estos datos de la base de datos transitoria de modo que se minimiza la aportación del operario.

Con el sistema se puede acceder a cualquier base de datos adecuada con el fin de obtener la información necesaria con respecto a cada pasajero. Se podrían consultar una o más bases de datos “locales” (es decir integrantes del sistema de inmigración) además de a las bases de datos externas. Preferiblemente, las bases de datos externas incluyen uno o más de lo siguiente: una base de datos de IPS (*Identity and Passport Service*: Servicio de Identidad y Pasaporte) que contiene información personal para poseedores de pasaportes (por ejemplo, poseedores de pasaportes del RU), una base de datos de pérdidas y robos que contiene detalles de identificaciones únicas pérdidas y robadas, una base de datos nacional de lista de detenciones que contiene detalles de determinadas

personas y correspondientes identificaciones únicas de interés y bases de datos de información de avance de pasajeros que contienen detalles de personas que se espera que quieran acceso a la zona.

En muchos casos, por lo menos una de las bases de datos externas contendrá los datos biográficos relacionados con por lo menos algunas de las personas, como el nombre de una persona, la dirección, el lugar de nacimiento, la fecha de nacimiento, la edad, etc.

En una realización particularmente preferida, una o más de las bases de datos externas contiene los datos biométricos relacionados con por lo menos algunas de las personas. Ventajosamente, los datos biométricos comprenden uno o más datos de huellas dactilares, datos de iris y datos de reconocimiento facial, en los que los datos de reconocimiento facial comprenden preferiblemente una fotografía de la persona. Los datos biométricos son particularmente útiles ya que permiten que una máquina lleve a cabo una comparación del poseedor del pasaporte y el propietario, según la base de datos, que puede ser a la vez más rápida y más precisa que una evaluación comparable por un operario humano.

De ahí, preferiblemente, si una o más de las bases de datos externas contiene datos biométricos correspondientes a la identificación única detectada, los correspondientes datos biométricos se incluyen en la información recuperada suministrada para la segunda ubicación.

En algunas realizaciones puede ser deseable obtener toda la información correspondiente a la identificación única de todas las bases de datos disponibles simultáneamente y hacer que todo esté disponible en la segunda ubicación. Sin embargo, en muchos casos es preferible hacer que la cantidad de información transferida sea mínima, para reducir el ancho de banda de las comunicaciones y reducir el almacenamiento necesario en cualquier base de datos transitoria o en la segunda ubicación. Por lo tanto es ventajoso que la etapa de utilizar la identificación única detectada para recuperar información con respecto a la persona de una o más bases de datos externas deba comprender:

preguntar por lo menos a alguna de las bases de datos externas para recuperar una primera información relacionada con la persona;

tomar una decisión, basada en la primera información, en cuanto a si debe permitirse a la persona entrar a la zona controlada; y

si es así, preguntar por lo menos a alguna de las bases de datos externas para recuperar una segunda información relacionada con la persona;

en el que las dos informaciones primera y segunda se suministran a la segunda ubicación. De esta manera, solo debe recuperarse la segunda información si la primera información apoya la entrada de la persona a la zona controlada.

Preferiblemente, la segunda información comprende datos biométricos. Normalmente esto sólo se utilizará si la primera información recuperada sugiere que se debe permitir a la persona la entrada a la zona, ya que cualquier otro resultado requerirá que el poseedor sea ayudado por un funcionario de control de fronteras, no utilizando por tanto sistemas de comprobación biométrica automatizada.

Cada uno de los pasajeros podría ser dirigido a la misma segunda ubicación (o múltiples mostradores que conforman una segunda ubicación) en la que la naturaleza de la información recuperada se utiliza para determinar hasta qué punto es necesaria ahora la comprobación para permitir el acceso del poseedor a la zona controlada. Por ejemplo, se podría disponer un aparato de comprobación biométrica y un funcionario en la segunda ubicación para que cualquiera esté disponible para realizar la comprobación y tomar la decisión. Sin embargo, esto todavía requiere el tratamiento en serie de los pasajeros y podría llevar a la creación de colas detrás de personas cuya recuperación de datos ha causado problemas. Como tal, es preferible tratar diferentes “tipos” de pasajeros en paralelo. Ventajosamente, por lo tanto, una vez que la información ha sido recuperada, el método comprende además seleccionar una o más de múltiples segundas ubicaciones basándose en la información recuperada, y dirigir al portador de la identificación única a las segundas ubicaciones seleccionadas.

Dependiendo de la información recuperada, el poseedor de cada identificación puede ser dirigido a medios diferentes para realizar la etapa final de decisión: por ejemplo, si el perfil del poseedor revela problemas, pueden ser dirigidos a un funcionario del control de fronteras para obtener ayuda, mientras que si no se identifican problemas de las bases de datos, el poseedor puede ser dirigido a una ruta automatizada más rápida, tal como un punto de comprobación biométrica. Esto mejora aún más el rendimiento.

Como se ha indicado anteriormente, la manera en la que se toma la decisión en la segunda ubicación depende de la información recuperada. Sin embargo, generalmente es preferible que la etapa de utilizar la información recuperada para tomar una decisión en cuanto a si permitir el acceso a la persona que lleva la identificación única a la zona controlada, comprende determinar si la información recuperada indica que debe permitirse a la persona

correspondiente a la identificación única el acceso a la zona, y si ése es el caso realizar una comprobación en cuanto a si la persona que lleva la identificación única es la persona correspondiente a la identificación única en las bases de datos externas.

En una realización preferida, realizar la comprobación comprende comparar un documento de identificación llevado por la persona que lleva la identificación única con esa persona, el documento de identificación incorpora preferiblemente la identificación única. Por ejemplo, esto puede adoptar la forma de un pasaporte.

En otra realización preferida, si la información recuperada incluye datos biométricos, realizar la comprobación comprende comparar la persona que lleva la identificación única con por lo menos parte de los datos biométricos recuperados correspondientes a la identificación única en las bases de datos externas, realizando preferiblemente uno o más de entre un análisis de huella dactilar, análisis de iris o reconocimiento facial. Ventajosamente, la comprobación es realizada por un sistema de comprobación biométrica según el segundo aspecto de la invención.

Sin embargo, ventajosamente, varias o todas estas técnicas de comprobación se hacen disponibles y se selecciona la apropiada para cada persona dependiendo de la información recuperada.

En una realización especialmente preferida, cada identificación única es proporcionada por un documento de seguridad según el primer aspecto de la invención, preferiblemente en forma de la segunda etiqueta de RFID. Como en otros ejemplos, la identificación única podría proporcionarse por separado en cualquier documento de identificación, por ejemplo en una tarjeta publicada en facturación, una tarjeta de viajero frecuente o incluso una etiqueta. El uso de una etiqueta de RFID (UHF) de largo alcance es particularmente adecuada para proporcionar la identificación única ya que, como se ha explicado anteriormente, puede ser leída a distancias relativamente largas sin molestar al poseedor y, en particular, sin necesitad de pararlo. Todavía, la intimidad de cada propietario no se ve comprometida ya que sólo se puede conseguir acceso a sus datos personales por parte del personal con acceso a las bases de datos.

El uso de tales documentos ofrece la posibilidad de incorporar una etapa de autenticación de documentos en el método de inmigración. Por lo tanto, preferiblemente la etapa de utilizar la información recuperada para tomar una decisión en cuanto a si permitir el acceso de la persona que lleva la identificación única a la zona controlada comprende además determinar si el documento de seguridad es auténtico mediante la interrogación a la primera etiqueta de RFID y la comprobación de que el código de identificación contenido en la misma corresponde a (es decir coincide o está relacionado correctamente con) la identificación única (que puede ser el código de identificación de la segunda etiqueta de RFID). Esto proporciona una comprobación automatizada de autenticación y puede ser utilizada en lugar o a la vez que otros métodos tales como una comprobación visual de elementos de seguridad en el documento como hologramas, tintas ópticamente variables, características UV e IR, etc.

El tercer aspecto de la invención proporciona además un sistema para controlar el acceso a una zona, comprendiendo

un detector adaptado para detectar una identificación única llevada por una persona en una primera ubicación, la identificación única corresponde a una persona;

un controlador adaptado para recibir la identificación única detectada del detector, recuperar información con respecto a la persona a la que corresponde la identificación única detectada de una o más bases de datos externas, y suministrar la información recuperada para una segunda ubicación a distancia de la primera ubicación; y

por lo menos un terminal, en la segunda ubicación, adaptado para permitir la toma de una decisión basándose en la información recuperada en cuanto a si permitir a la persona que lleva la identificación única el acceso a la zona controlada.

Preferiblemente, el detector comprende una antena de radiofrecuencia adaptada para leer etiquetas de RFID para detectar con ello identificaciones únicas almacenadas en la misma, preferiblemente etiquetas de RFID de UHF.

Ventajosamente, el sistema comprende además una base de datos transitoria, en la que el controlador está adaptado para almacenar la información recuperada en la base de datos transitoria y el por lo menos un terminal en la segunda ubicación está adaptado para conseguir acceso a la base de datos transitoria.

Preferiblemente el por lo menos un terminal comprende un ordenador y un monitor para mostrar por lo menos parte de la información recuperada, o un módulo de comprobación biométrica.

En una realización particularmente preferida, el por lo menos un terminal comprende un segundo detector que está adaptado para detectar una identificación única llevada por una persona en la segunda ubicación, el por lo menos un terminal está adaptado para identificar la información recuperada correspondiente a la identificación única detectada por el segundo detector.

Ventajosamente, el sistema comprende una pluralidad de terminales en la segunda ubicación, y comprende además unos medios de dirección adaptados para dirigir a cada persona a uno o un subconjunto seleccionado de la pluralidad de terminales, basándose en la información recuperada correspondiente a la identificación única llevada por la persona.

Preferiblemente, los medios de dirección comprenden un tercer detector adaptado para detectar una identificación única llevada por una persona junto a los medios de dirección, los medios de dirección están adaptados para identificar la información recuperada correspondiente a la identificación única detectada por el tercer detector. Ventajosamente, los medios de dirección comprenden además un módulo de salida adaptado para dirigir a cada persona indicando el uno o el subconjunto seleccionado de la pluralidad de terminales.

Ejemplos de documentos de seguridad, sistemas y métodos según la invención se describirán ahora haciendo referencia a los dibujos adjuntos, en los que:

La Figura 1 muestra esquemáticamente un sistema para controlar la entrada a una zona;

La Figura 2 muestra un documento de seguridad que puede utilizarse en el sistema de la Figura 1;

La Figura 3 muestra un dispositivo esquemático para dirigir que puede utilizarse en el sistema de la Figura 1;

La Figura 4 muestra un terminal esquemático de comprobación biométrica que puede utilizarse en el sistema de la Figura 1;

La Figura 5 es un diagrama de flujo que representa un método para controlar la entrada a una zona; y

La figura 6 es un diagrama de flujo que ilustra las etapas de la Figura 5 con más detalle.

La siguiente descripción se centrará en el uso de documentos, sistemas y métodos de seguridad en escenarios de inmigración, es decir que controlan el acceso a un país, tal como podría implementarse en un aeropuerto, puerto marítimo u otro concentrador de transportes. Sin embargo, se apreciará que la invención es igualmente aplicable a al control de acceso a cualquier otro tipo de zona a la que se desea impedir el acceso a determinadas personas, u opuestamente, para permitir el acceso sólo a determinada personas. Otros ejemplos incluyen las oficinas, plantas de fabricación, campus de escuelas y universidades, lugares de actuaciones de entretenimiento, etc.

La Figura 1 muestra a unas personas P acercándose a una zona controlada R. Cada persona P lleva una identificación única que puede ser detectada por un sistema de inmigración 10. El sistema de inmigración 10 incluye un controlador 11 que está configurado para recibir señales desde un detector 15 dispuesto para abarcar una primera ubicación 1. Según se describe con más detalle más adelante, el detector 15 puede detectar identificaciones únicas llevadas por las personas P en la primera ubicación 1, y proporcionar las identificaciones únicas detectadas al controlador 11.

El controlador 11 está en comunicación con una o más bases de datos externas 14a, 14b y 14c. En la práctica, se podría acceder a las bases de datos externas a través de una conexión de red (14a) o a través de cualquier medio conocido de intercambio de datos incluyendo internet, una intranet, una red pública telefónica conmutada o una red inalámbrica, todas representadas por el elemento 16 en la Figura 1.

El controlador 11 puede acceder a cualquier base de datos externa que contiene información pertinente a si se debe permitir el acceso de personas a la zona controlada. Con “base de datos externa” se indican bases de datos que son mantenidas en gran parte independientemente del propio sistema de inmigración, por ejemplo por cuerpos gubernamentales o de seguridad, o por sistemas independientes de inmigración (es decir los de los aeropuertos y otros similares).

En el caso de sistemas de inmigración, el controlador 11 puede acceder a bases de datos tales como la base de datos de IPS (que contiene detalles de todos los poseedores de pasaportes del RU, y que es mantenida por el Gobierno del RU), base de datos de pérdidas y robos de la Interpol, una o más listas nacionales de detención, la Lista de Índices de Sospechosos del RU y en EE.UU. la base de datos de AVISOS del Departamento de Estado. También se puede acceder a las bases de datos que contienen información suministrada por otros sistemas de inmigración. En por lo menos una, posiblemente cada base de datos, la información está asociada con la identificación única perteneciente a la persona implicada.

El controlador 11 está adaptado para recuperar información de una o de más de las bases de datos 14 basándose en identificaciones únicas detectadas por el detector 15. En la práctica esto puede implicar el uso de cada identificación única detectada para preguntar a cada base de datos seleccionada. Como alternativa, una base de datos (normalmente la base de datos de IPS o su equivalente fuera del RU) es interrogada primero para identificar a la persona correspondiente a la identificación única. La información recuperada (tal como el nombre de la persona, por ejemplo) puede utilizarse entonces para llevar a cabo búsquedas predefinidas a través de una o más de otras

bases de datos. Los resultados de estas búsquedas pueden devolverse entonces a la base de datos de IPS de tal manera que se pueda tomar una decisión acerca de si otorgar acceso a la persona. Opcionalmente, se pueden recuperar datos adicionales de bases de datos locales (internas) 12, tales como registros mantenidos por el propio sistema de inmigración 10.

Una vez cotejados, los datos recuperados se hacen disponibles para por lo menos una segunda ubicación 2. La segunda ubicación 2 se dispone a alguna distancia de la primera ubicación 1, a lo largo del camino que es seguido por las personas P hacia la zona controlada R. En un sistema típico de inmigración, por ejemplo, la primera ubicación podría situarse en una puerta de llegadas en un aeropuerto, y la segunda ubicación podría estar en un área de control de pasaportes situada poco antes de la recogida de equipajes. La segunda ubicación está provista normalmente con uno o más terminales dispuestos para utilizar la información recuperada. En el sistema de la Figura 1, se representan tres de tales terminales 40, 50a y 50b en la segunda ubicación 2. El primer terminal 40 comprende un ordenador tal como un PC con un monitor para el uso por parte de un funcionario de fronteras. Los terminales segundo y tercero 50a y 50b comprenden un aparato de comprobación biométrica, descrito más adelante. Todo se utiliza para tomar una decisión en cuanto a si se debe permitir o no a una persona P la entrada a la zona controlada R, basándose en la información que ha sido recuperada.

La información recuperada puede ser suministrada a la segunda ubicación de varias maneras. En un ejemplo, la información podría ser pasada a uno o más (o todos) de los terminales en forma de un mensaje, tal como un correo electrónico, o alguna otra cadena de datos. Si se puede deducir cuál de los terminales realizará la comprobación, el mensaje puede ser enviado solo a ese terminal (o subconjunto de terminales). Como alternativa el envío puede ser indeterminado. Sin embargo en una realización preferida la información recuperada es almacenada por el controlador 11 en una base de datos transitoria local 13. Aquí, “transitoria” significa simplemente que el contenido de la base de datos está relacionado con las personas para las que se han detectado las identificaciones únicas - es decir personas que han llegado al sistema de inmigración - en comparación con bases de datos de información relacionadas con personas en general. Normalmente, se establece un registro para cada identificación única detectada y se le asocia cualquier información recuperada correspondiente Dependiendo de la naturaleza y el volumen de la información recuperada, puede no ser necesario ni deseable incluir todos los datos que hay en el registro. El registro también puede incluir el resultado de decisiones tomadas por el controlador 11 basándose en la información recuperada, por ejemplo “PARADA” (STOP) si una o más de las bases de datos plantea un problema, o “CORRECTO” (OK) si no se revela ningún problema.

Cada terminal 40, 50a y 50b puede acceder entonces a la base de datos transitoria 13 para recuperar el registro de datos apropiado a medida que cada persona P se acerca a la segunda ubicación 2. Esto puede realizarse manualmente (por ejemplo tras introducir el nombre de la persona), pero preferiblemente el terminal incluye un detector que detecta la identificación única llevada por una persona que se acerca al terminal, y un procesador que pregunta a la base de datos transitoria 13 para recuperar los datos pertinentes.

A continuación se puede tomar una decisión en la segunda ubicación 2 en cuanto a si se debe permitir a la persona que lleva la identificación única el acceso a la zona controlada R. Esto podría basarse únicamente en la información recuperada: por ejemplo si se recupera una decisión de “CORRECTO”, la persona puede ser admitida directamente en la zona controlada. Sin embargo, para mejorar la seguridad, la decisión incluye preferiblemente realizar una comprobación de que la persona que lleva la identificación única es la persona a quien corresponde la identificación única en las bases de datos. La manera como se puede realizar esto depende de la información que ha sido recuperada, según se describe con más detalle más adelante. Una mejora adicional es incluir una comprobación de la autenticidad de la identificación única.

La identificación única puede ser llevada por cada persona de varias maneras. Es preferible que la identificación única sea detectable a distancia sin necesitad de parar a la persona. Las etiquetas de RFID son un método especialmente preferido para aplicar esto, aunque son posibles otras técnicas, incluyendo el uso de códigos de barras o códigos de barras 2D. Se cree que las etiquetas de RFID de Ultra Alta Frecuencia (UHF) son especialmente adecuadas dado el largo alcance sobre el que pueden ser interrogadas por un lector. Tales etiquetas podrían ser incorporadas en un documento tal como una tarjeta entregada al pasajero en facturación o en un pase de viajero frecuente, por ejemplo. Como alternativa las etiquetas que contienen etiquetas de RFID podrían adherirse a pases de embarque. Un ejemplo de un documento de seguridad 20 particularmente preferido que contiene una identificación única se muestra en la Figura 2, que puede ser utilizado en el sistema de la Figura 1 (y encuentra aplicaciones adicionales en otras partes), y se describe con más detalle más adelante.

En algunas realizaciones, cada persona P puede moverse directamente desde la primera ubicación a la segunda ubicación y, si hay más de un terminal, selecciona uno de su elección o es dirigido según criterios tales como su nacionalidad, país de salida, etc. Esto es especialmente apropiado si el sistema es implementado de tal manera que todas las personas P son sometidas a la misma forma de comprobación independientemente de la naturaleza de la información recuperada, por ejemplo si se desea que un funcionario de control de fronteras realice cada comprobación utilizando la información recuperada (como en el terminal 40 en la Figura 1). Sin embargo, como se

indicó anteriormente, es ventajoso proporcionar más de un método para realizar la comprobación, dependiendo del tipo de información que ha sido recuperada. Por ejemplo, si se han recibido datos biométricos, la comprobación puede ser realizada por un aparato de comprobación biométrica como los terminales 50a o 50b, y si no todavía puede ser necesaria una comprobación por parte de un funcionario. Además, cada terminal 40, 50a y 50b puede ser capaz por sí mismo de realizar diferentes tipos de comprobación: por ejemplo, un aparato 50a, 50b de comprobación biométrica, puede ser utilizable por parte de un funcionario autorizado para acceder a los datos recuperados de la misma manera que un ordenador 40, o puede incorporarse en un terminal 40 el hardware necesario para realizar la comprobación biométrica.

Por consiguiente, las personas P pueden llegar simplemente a cualquier terminal en la segunda ubicación y llevarse a cabo una comprobación adecuada para decidir si se debe permitir a esa persona P el acceso a la zona controlada R. Sin embargo, puesto que algunas formas de comprobación llevan más tiempo que otras, esto puede llevar a hacer una cola innecesaria. Por consiguiente, en una realización particularmente preferida, el sistema 10 comprende además un dispositivo de dirección 30 situado a lo largo del recorrido entre la primera ubicación 1 y la segunda ubicación 2 en una tercera ubicación 3. El dispositivo de dirección 30 dirige a cada persona P a uno de los terminales 40, 50a o 50b (o un subconjunto de terminales) basándose en la información recuperada correspondiente a esa identificación única de persona. De esta manera, las personas para las que se han recuperado datos biométricos (por ejemplo) pueden ser dirigidas a un terminal 50a o 50b de comprobación biométrica, para una comprobación más rápida, mientras que las personas para las que no hay disponibles datos biométricos pueden ser dirigidas a un funcionario de control de fronteras en el terminal 40. Esto reduce la creación de colas por “rastreo rápido” de determinadas personas a través de procedimientos de comprobación más rápidos mientras sólo ésos cuyos detalles requieran una investigación adicional (o para quien no existe información en las bases de datos) deben ser manejados por un funcionario de control de fronteras.

Un ejemplo de un dispositivo de dirección 30 se muestra en la Figura 3. El dispositivo 30 incluye un procesador 31 para comunicase con el controlador 11 o la base de datos transitoria 13, y unos medios de salida tal como un display visual 30 para indicar a la persona P a cuál de los terminales 40, 50a o 50b (denominados análogamente múltiples ubicaciones segundas) informar. El dispositivo 30 puede identificar de varias maneras a una persona que se acerca P. Preferiblemente, el dispositivo 30 incluye un lector 33 dispuesto para leer la identificación única de persona de una manera análoga al detector 15. Por ejemplo, el lector 33 puede ser un lector de etiquetas de RFID. La potencia de la antena del lector puede ser, sin embargo, menor que la del detector 15 de modo que sólo se detecta la identificación única de una persona que se acerque al dispositivo de cerca (por ejemplo a menos de 1 metro, o que incluso haga que la identificación única toque contra el dispositivo 30). La identificación única detectada es utilizada por el procesador 33 para acceder a los datos pertinentes recuperados por el controlador 11 (preferiblemente a través de la base de datos transitoria 13). Basándose en los datos recuperados, el procesador 33 decide a cuál de los terminales (o segundas ubicaciones) debe dirigirse la persona correspondiente a la identificación única y se produce una salida apropiada. Como alternativa, esta decisión podría ser hecha por el controlador 11 y el resultado ser incluido en los datos recuperados por el procesador 33. La salida del dispositivo de dirección 30 puede ser audible así como, o en vez de, visual. Cada persona que llega desde la primera ubicación puede presentar entonces su identificación única al dispositivo 30 para que sea asignado a un terminal de comprobación, y continuar al que sea apropiado para la comprobación, minimizando de este modo la cola. Normalmente, muchos de tales dispositivos 30 serían dispuestos en las inmediaciones de la tercera ubicación de modo que muchas personas P puedan ser dirigidas inmediatamente.

Un ejemplo de un terminal de comprobación biométrica 50a o 50b se muestra en la Figura 4. Normalmente este comprenderá un procesador 51 dispuesto para comunicarse con el controlador 11 y/o la base de datos transitoria 13, un dispositivo de salida tal como un display visual 52 y un módulo de entrada biométrica 54. El módulo 54 de entrada biométrica incluirá unos medios de entrada apropiados para la medición biométrica que se ha de hacer. Por ejemplo, el módulo puede incluir un escáner de huella dactilar o de iris, o una cámara para el reconocimiento facial. En el terminal puede incluirse más de un tipo diferente de medios de entrada de modo que, por ejemplo, cualquier terminal es capaz de realizar exploración de iris y coincidencia de huellas dactilares. También hay incorporados unos medios para detectar una identificación única de persona, tal como el detector 53. Como en el caso del dispositivo de dirección 30, el detector 53 puede ser de cualquier tipo apropiado para la naturaleza de las identificaciones únicas utilizadas. En el presente caso, esto puede ser un lector de RFID de UHF y su potencia puede ajustarse para detectar sólo identificaciones únicas muy cerca del terminal 50. La identificación única detectada es utilizada por el procesador 51 para recuperar los datos correspondientes que han sido cotejados por el controlador 11, normalmente mediante el acceso a la base de datos transitoria 13. Generalmente, sólo las personas para las que se incluyen datos biométricos en la información recuperada serán dirigidas a un módulo 50 de comprobación biométrica, de modo que el procesador 51 es capaz entonces de llevar a cabo una comparación 1:1 entre la entrada que recibe del módulo 54 de comprobación biométrica (tal como escáner de iris o de huella dactilar del poseedor) y los correspondientes datos contenidos en su registro de datos. Esto permite un emparejamiento 1:1 mucho más rápido, en lugar de tener que hacer una búsqueda más complicada y más lenta de 1 a N (muchos) por todos los datos biométricos disponibles para personas en general. Por consiguiente, se aumenta el rendimiento y la seguridad. La posibilidad de una comparación de uno a uno también mejora la fiabilidad de realizar el reconocimiento facial.

Las figuras 5 y 6 son diagramas de flujo que representan las etapas implicadas en un ejemplo de proceso de inmigración. La figura 5 muestra una perspectiva general. Cada persona P lleva una identificación única incorporada en un documento 20 de tipo pasaporte, una tarjeta 20' que puede ser expedida por el IPS o una tarjeta 20" de viajero frecuente que por ejemplo también puede incluir el número del pasaporte de la persona. Podría utilizarse, según se desee, cualquier otra manera adecuada de llevar la identificación única. En el ejemplo, la identificación única es un código contenido en una etiqueta de RFID, preferiblemente una etiqueta de RFID de UHF que puede ser leída a una distancia relativamente de larga. En la primera ubicación 1, por ejemplo al salir del avión, en el pasillo entre el avión y la zona de la puerta, un detector tal como un lector de chips a UHF explora el pasaporte 20 de la persona desde una distancia de varios metros (pies) y la identificación única del chip a UHF leído. Como el chip a UHF no tiene datos personales en el mismo no habría asuntos de seguridad con esto.

La identificación única sería utilizada entonces para acceder a los datos según se ha descrito anteriormente de bases de datos externas 14 tales como la base de datos principal de pasaportes del gobierno (por ejemplo la base de datos de IPS del RU) en la que los datos habrían sido guardados anteriormente durante el proceso de expedición del pasaporte. En el tiempo que tarda la persona en pasar de la primera ubicación a la segunda ubicación 2, tal como un mostrador de inmigración, utilizando los datos buscados de la base de datos 14 de pasaportes del gobierno, también se pueden llevar a cabo varias búsquedas adicionales de otras bases de datos externas (Interpol, etc.). Cualquier dato recogido se mantendría entonces localmente en una base de datos transitoria y estaría disponible para un funcionario de inmigración mucho antes de que el viajero alcanzara el mostrador de inmigración. El tiempo adicional permite comprobaciones de seguridad mayores y más exhaustivas y autorizaciones más rápidas para los nativos del país implicados ya que el funcionario de inmigración tendría toda la información pertinente disponible antes de que el viajero llegara al mostrador de inmigración.

En las realizaciones preferidas, también está la opción de tener un espacio libre de inmigración por un carril rápido. Con la exploración del chip a UHF en la aproximación a la inmigración en una tercera ubicación intermedia 3, las personas que habían sido separadas previamente por el sistema como que no era necesaria una inspección detallada de pasaporte podrían ser desviadas por un canal separado en el que sólo sería necesaria una comprobación rápida por parte de los funcionarios de inmigración (por ejemplo una inspección visual del documento). Los que tienen pasaportes sin chip a UHF en sus pasaportes, o que han sido señalados por el sistema como que tienen algún problema en el procedimiento de separación previa, irían por el procedimiento normal de inmigración más exhaustivo. En esencia esto equivale a una autorización previa a la inmigración que podría reducir significativamente el tiempo que tardan los nativos en ser autorizados a través de inmigración y aumentaría la seguridad.

La Figura 6 muestra este proceso con más detalle. En la etapa S100, se detecta una identificación única de persona en la primera ubicación 1. En las etapas S102 y S104, el controlador 11 recibe la identificación única detectada y lo utilizan para buscar datos de varias bases de datos externas 14. En la etapa S106, el controlador decide si se han identificado o no problemas en los datos recuperados. Si es el caso, en la etapa S107, algunos o todos los datos recuperados son almacenados en la base de datos transitoria 13, destacando preferiblemente la razón para el rechazo o la preocupación. Si no, en la etapa S108 el controlador identifica si los datos recuperados incluyen datos biométricos o indica que hay disponibles datos biométricos. Si no es el caso, en la etapa S109, algunos o todos los datos recuperados son almacenados en la base de datos transitoria 13, preferiblemente con una indicación de que se ha aprobado a la persona. Si hay datos biométricos disponibles, en la etapa S110 esto es recuperado (si no se ha recuperado ya en la etapa S104), y en la etapa S112 los datos recuperados (incluyendo los datos biométricos) se almacenan en la base de datos transitoria 13, preferiblemente con una indicación de aprobación.

En este ejemplo, las personas P que se acercan a la segunda ubicación 2 son dirigidas a uno de varios terminales 40a, 40b, 50a, 50b y 50c dependiendo de los datos recuperados. Esto se lleva a cabo en una tercera ubicación 3 por medios tales como el dispositivo 30 descrito anteriormente. En la etapa S300 se hace un intento para detectar una identificación única llevada por una persona en la tercera ubicación 3. Si no se detecta una identificación única, la persona es dirigida a un terminal estándar de comprobación 40a a cargo de un funcionario, ya que no hay información adicional para el sistema. Si se detecta una identificación única, en la etapa S302 la identificación detectada es utilizada para buscar la información recuperada correspondiente en la base de datos transitoria 13. Si se han identificado problemas, el registro se considera un "fallo" y la persona es dirigida a un terminal estándar de comprobación 40a. Si no se detectan problemas en los datos, en la etapa S304 se determina si hay disponibles datos biométricos (ya sea formando parte de los datos recuperados o disponibles de otro modo para el sistema, por ejemplo con el uso de una clave de datos para recuperar información biométrica de otra base de datos). En este ejemplo, esto implica una serie de hasta tres comprobaciones para determinar si una plantilla de huella dactilar, una plantilla facial o una plantilla de iris están disponibles para la persona. Sin embargo, estas etapas podrían ser realizadas en cualquier orden y no se limitan a las mostradas en este ejemplo. En la primera comprobación S304a, se determina si hay disponible una plantilla de huella dactilar. Si es el caso, la persona puede ser dirigida a un terminal 50a de comprobación biométrica de huella dactilar. Si no, en la etapa S304b, se determina si hay disponible una plantilla facial. Si es el caso, la persona puede ser dirigida a un terminal 50c de comprobación biométrica de reconocimiento facial. Si no, en la etapa S304c, se determina si hay disponible una plantilla de iris. Si es el caso, la

persona puede ser dirigida a un terminal 50b de comprobación biométrica de iris. Si no, lo que significa que en este ejemplo no hay disponibles datos biométricos, la persona es dirigida a otro terminal estándar de comprobación 40b en el que se puede llevar a cabo una inspección rápida para comprobar que la imagen del pasaporte muestra al portador del pasaporte.

Una vez que la persona P llega al terminal designado en la segunda ubicación 2, se realiza una comprobación apropiada. Esto implica normalmente la comprobación de que la persona que lleva la identificación única es la misma persona que a la que se ha asignado la identificación en las bases de datos. Sin embargo, en sistemas que requieren un menor nivel de seguridad esto puede no ser necesario y la decisión podría tomarse simplemente sobre únicamente los datos recuperados.

En el presente ejemplo, si una persona es dirigida a un terminal de comprobación a cargo de un funcionario tal como 40a o 40b, el nivel de comprobación por parte del funcionario necesario dependerá de qué datos se recuperan y si se ha identificado algún problema. Las personas que llegan al mostrador 40a son las que no tienen registros de datos o se han indicado problemas. Como tal su documentación de pasaporte requerirá un examen completo en la etapa 200, llevando un mínimo de alrededor de 10 segundos por persona. Las personas que llegan al mostrador 40b tienen registros de datos “aprobados” y en este caso todo lo que se necesita es una comprobación rápida para asegurar que el poseedor coincide con la foto del pasaporte, en la etapa S204, llevando normalmente alrededor de 2 segundos por persona.

Las personas que llegan al terminal 50a de comprobación biométrica se someten un procedimiento automatizado para comprobar sus huellas dactilares contra sus registros en la etapa S202. Tras la aproximación al terminal 50a, su identificación única es detectada (etapa S202a) y los datos biométricos necesarios son recuperados de la base de datos transitoria 13 (etapa S202b). Entonces se puede realizar una comparación 1:1. El proceso es similar en el terminal 50b de comprobación biométrica en el que se utiliza un escáner de iris para la comparación con registros en la etapa S208. Normalmente, los registros de iris se mantienen en una base de datos independiente y una vez que se detecta la identificación única de persona (etapa S208a) esto se utiliza para acceder a la base de datos transitoria 13 para recuperar los datos incluyendo una clave (etapa S208b) que entonces puede utilizarse para buscar los datos biométricos en una base de datos de iris (etapa S208c). Entonces se puede realizar una comparación 1:1. En el terminal 50c de reconocimiento facial, se toma una imagen del poseedor del pasaporte y se compara con datos recuperados de reconocimiento facial en la etapa S206. De nuevo, se detecta la identificación única llevada por el poseedor del pasaporte (etapa S206a) y se utiliza para recuperar los correspondientes datos de reconocimiento facial (etapa S206b), que entonces pueden utilizarse para realizar una comparación 1:1.

Cabe señalar que la primera, segunda y (opcionalmente) tercera ubicación podrían configurarse de muchas maneras diferentes dependiendo de la aplicación en cuestión. Uno de los asuntos en viajes es asegurar que la persona correcta embarca en el avión correcto, y si bien hay varias sugerencias en cómo esto podría mejorarse utilizando la biometría, en una realización de la presente invención, podría leerse una identificación única de persona (por ejemplo en un pasaporte de RFID de UHF) en la comprobación (primera ubicación) y leerse otra vez en la puerta de embarque (segunda ubicación). En este caso la base de datos externa podría contener listas de los pasajeros esperados y la decisión final en cuanto a si permitir el embarque supondría simplemente la comprobación de que cada identificación única detectada corresponde. El uso de un chip de RFID de UHF haría que esto fuera sencillo de implementar y no tendría asuntos de protección de datos. Verdaderamente esto permite potencialmente la colocación a posteriori en pasaportes existentes con funcionalidad de UHF, ya que la línea aérea podría poner una etiqueta segura de RFID de UHF durante la facturación y pasar los datos de nuevo al gobierno que publica los sistemas y otras bases de datos externas.

Otro aspecto con la seguridad de un sistema de seguridad tal como el que se ha descrito anteriormente es la autenticidad de las propias identificaciones únicas. Como se ha mencionado anteriormente estos se incorporarán normalmente en documentos tales como pasaportes. Ahora se describirá un documento de seguridad particularmente ventajoso adecuado para el uso en el sistema de inmigración descrito anteriormente (y otros sistemas en los que es importante la autenticidad de los documentos).

Un ejemplo de tal documento 20 se muestra en la Figura 2. La idea es combinar ambos chips de RFID de HF (Corto Alcance - Estilo Pasaporte Electrónico, ePassport) y RFID de UHF (Largo Alcance) y antenas asociadas en un documento de seguridad único tal como un pasaporte o documento de identificación.

Las etiquetas de RFID de Alta Frecuencia (HF) funcionan en el intervalo de frecuencias de 3 MHz a 28 MHz, más preferiblemente de 13 MHz a 14 MHz y más preferiblemente a 13,56 MHz. Dependiendo del diseño del chip (especialmente el tamaño de la antena) y la potencia del lector, la distancia a la que es posible la lectura de los datos que hay en el chip es a lo sumo alrededor de 3 metros. Normalmente alrededor de 1 metro se considera un máximo aceptable. En algunos casos puede ser deseable restringir esto aún más, a unos centímetros o incluso al contacto directo con el lector.

Las etiquetas de RFID de Ultra Alta Frecuencia (UHF) funcionan en el intervalo de frecuencias de 433 MHz a 950 MH y más preferiblemente de 860 a 870 MHz. Las etiquetas UHF ofrecen mayores distancias de lectura de hasta alrededor de 10 metros (pero más normalmente alrededor de 3 metros, de nuevo dependiendo del diseño del chip), y velocidades de lectura más altas.

En este ejemplo, el documento 20 es un documento de tipo cuadernillo con una tapa delantera 21, una tapa trasera 22 y páginas interiores 23. Las etiquetas de RFID primeras y segundas pueden incorporarse normalmente en una o en ambas tapas. Por ejemplo, en la Figura 2, una etiqueta de RFID de corto alcance (HF) 25 y una etiqueta de RFID de largo alcance (UHF) 26 se disponen las dos en la tapa trasera 22 del cuadernillo, juntas con respectivas antenas 25a y 26a. En otros casos, una etiqueta puede estar en la tapa delantera y la otra en la tapa trasera.

La combinación de una etiqueta HF 25 y una etiqueta UHF 26 proporciona al documento 20 funcionalidad y seguridad adicionales. Por ejemplo el chip (HF) 25 de ePassport puede contener los detalles del chip de UHF 26 (y/o viceversa), de modo que la inclusión de un chip de UHF en la tapa delantera de un ePassport podría proporcionar una prueba de que la incrustación no ha sido sustituida en el pasaporte.

Los chips de UHF como la etiqueta 26 son capaces de contener sólo una cantidad muy pequeña de datos (generalmente sólo contienen un código individual tal como una identificación única), a diferencia del chip de HF 25 de ePassport que puede tener varias decenas de miles de bytes de datos. Las etiquetas de UHF también se adecuan mejor a lectura a distancias más largas y por lo tanto pueden ser más convenientes y menos indiscretas para el poseedor cuando son leídas. Como no hay los datos contenidos en el chip de UHF no hay significativos asuntos sobre privacidad/libertades civiles a diferencia de los chips de ePassport. Los chips de UHF también son relativamente económicos en comparación con los chips HF de tipo ePassport, que normalmente cuestan cada uno sólo unos pocos céntimos de Euro o centavos en EEUU. Generalmente las dos tecnologías pueden utilizarse estrechamente entre sí mientras todavía retienen la funcionalidad de ambas tecnologías.

La combinación de las dos tecnologías en un solo documenta 20 ofrece varias ventajas.

Normalmente, un chip de HF 25 de ePassport tiene una zona en el mismo designada como “Datagroup 13” que puede contener los datos que no se necesitan como parte de la especificación de la OACI (Organización de Aviación Civil Internacional). En una realización de la presente invención, esta zona podría contener un código de identificación en forma de detalles del Chip de UHF, o el chip de UHF podría programarse con un código de identificación en forma del mismo número que la Identificación Única de Chip contenida en el chip de HF o los datos programados en el Datagroup 13. Si se utiliza esta metodología entonces la eliminación o sustitución de cualquier chip sería fácilmente detectable y proporcionaría al pasaporte con un nivel más alto de seguridad.

Los códigos de identificación en las dos etiquetas de RFID no deben ser idénticos pero en su lugar podrían estar relacionados entre sí, por ejemplo a través de una base de datos o un algoritmo adecuado.

La provisión de un chip de UHF también proporciona varios beneficios adicionales. En particular, el control y consideración de pasaportes durante la producción es un proceso difícil y costoso debido a las muchas fases de la producción y los montajes resultantes que se requieren a menudo. Tener un chip de UHF en el pasaporte haría este proceso mucho más sencillo y más fiable al hacer posible el rastreo de cada documento a pesar del proceso (“Que se puede rastrear y se puede encontrar”), por lo tanto mejorando la eficiencia y ahorrando costes. El uso de un chip de UHF permite que el pasaporte sea rastreado y seguido más fácilmente porque el chip puede ser leído de lejos, de modo que los pasaportes pueden ser monitorizados cuando se producen en la fábrica, cuando se empaquetan en cajas, durante el tránsito al lugar en el que los pasaportes serán personalizados, durante el proceso de personalización del pasaporte y durante el despacho al solicitante del pasaporte. Dentro de la misma fábrica, el pasaporte puede ser rastreado y ser identificado de una estación a la siguiente. Una dificultad particular que se encuentra convencionalmente en el proceso de fabricación del pasaporte es que, para identificar cada pasaporte, es necesario que el operario abra el cuadernillo y examine la información de dentro (tal como el número de pasaporte, o como el nombre del propietario del pasaporte), que es incómodo y ralentiza la producción. El uso de un chip de UHF vence este problema ya que el pasaporte puede ser identificado automáticamente con un lector adecuado cuando llega dentro del alcance de ese lector. Ya no hay más requisitos de que el operario estudie el cuadernillo y no hay posibilidad de error del usuario. Con ePassports (es decir pasaportes que también contienen un chip de RFID de HF que almacena datos personales) esto sería aún más importante debido a su valor mucho más alto comparado con pasaportes convencionales. Si bien se prefiere la provisión de ambos chips de RFID a HR y UHF como características permanentes del pasaporte, un ePassport convencional, o verdaderamente un pasaporte estándar sin chip de RFID, puede hacerse “Que se puede rastrear y se puede encontrar” con la provisión de un chip de RFID de UHF que se conecta temporalmente al pasaporte durante fabricación y/o la personalización, y que pueden ser quitado más adelante, si se desea. Por ejemplo, el chip de UHF podría ser contenido en una etiqueta que se adhiere al acceso de paso y separarse luego.

En casos en los que la funcionalidad UHF y HF va a ser una característica permanente del pasaporte, los dos dispositivos podrían combinarse en un solo chip, lo que reduciría el coste global de implementar ambas tecnologías

en un solo documento dando al mismo tiempo al pasaporte una funcionalidad adicional. Esto proporcionaría el nivel adicional de autenticación descrito anteriormente así como que se convertiría en “Que se puede rastrear y se puede encontrar”.

Por todas estas razones es ventajoso utilizar el documento de seguridad 20 en el sistema de inmigración descrito anteriormente para llevar las identificaciones únicas. El chip de RFID de UHF 26 es idealmente adecuado para contener un código único de identificación que puede ser detectado por un lector adecuado de RFID de UHF. Además, la comprobación llevada a cabo en la segunda ubicación puede incluir una comprobación de la autenticidad del documento leyendo los datos del chip de UHF 26 y el chip de HF 25 y llevando a cabo una comparación. Por ejemplo, si ambos chips 25 y 26 se programan para incluir la misma identificación única, una comparación de los códigos en cada uno confirmará si uno o el otro ha sido sustituido. Similarmente, cuando cada una de las etiquetas 25 y 26 está provista con códigos relacionados, se puede hacer una comprobación utilizando la base de datos o el algoritmo apropiados para determinar si la relación entre ellos es correcta, con el fin de detectar cualquier sustitución de chip.

Los terminales dispuestos en la segunda ubicación 2 pueden incluir por lo tanto un aparato de autenticación que comprende lectores adecuados para interrogar a la primera etiqueta de RFID así como a la segunda etiqueta de RFID, y unos medios de procesamiento para realizar una comparación entre los datos recuperados de cada uno. Un solo lector de RFID puede ser suficiente cuando puede ser configurado para leer ambos tipos de etiqueta de RFID (por ejemplo puede funcionar en ambas frecuencias necesarias). Como alternativa pueden disponerse dos lectores dedicados. El aparato de autenticación puede integrarse con los terminales 50a de comprobación biométrica, 50b, 50c y los terminales 40a, 40b de comprobación estándar, o podrían proporcionarse por separado.

REIVINDICACIONES

1. Un documento de seguridad (20) que comprende una primera etiqueta de RFID legible sólo dentro de un primer alcance de distancia, y una segunda etiqueta de RFID legible dentro de un segundo alcance de distancia, la primera etiqueta de RFID contiene datos pertenecientes al propietario del documento de seguridad y un código de identificación, y la segunda etiqueta de RFID contiene el mismo o un código de identificación relacionado, y en el que el segundo alcance de distancia es más largo que el primer alcance de distancia.

2. Un documento de seguridad según la reivindicación 1, en el que el primer alcance de distancia comprende una máxima distancia de lectura entre cero y aproximadamente 3 metros desde la primera etiqueta de RFID, preferiblemente entre cero y aproximadamente 1 metro desde la primera etiqueta de RFID.

3. Un documento de seguridad según la reivindicación 1 o la reivindicación 2, en el que el segundo alcance de distancia comprende una máxima distancia de lectura de sobre aproximadamente 1 metro desde la segunda etiqueta de RFID, preferiblemente sobre aproximadamente 3 metros desde la segunda etiqueta de RFID, todavía preferiblemente más de 10 metros desde la segunda etiqueta de RFID.

4. Un documento de seguridad según cualquiera de las reivindicaciones anteriores, en el que el código de identificación identifica la segunda etiqueta de RFID, y el mismo código de identificación está programado en la primera etiqueta de RFID.

5. Un documento de seguridad según cualquiera de las reivindicaciones 1 a 3, en el que el código de identificación identifica la primera etiqueta de RFID, y el mismo código de identificación se programa en la segunda etiqueta de RFID.

6. Un documento de seguridad según cualquiera de las reivindicaciones anteriores, en el que los datos contenidos en la primera etiqueta de RFID incluyen datos personales relacionados con el propietario y/o datos biométricos relacionados con el propietario, preferiblemente datos de huellas dactilares, plantillas de iris y/o datos de reconocimiento facial.

7. Un documento de seguridad según cualquiera de las reivindicaciones anteriores, en el que la primera etiqueta de RFID comprende un chip de RFID de Alta Frecuencia (HF) y la segunda etiqueta de RFID comprende un chip de RFID de Ultra Alta Frecuencia (UHF).

8. Un documento de seguridad según la reivindicación 7, en el que el chip de RFID de HF funciona en una frecuencia en el intervalo de 3 MHz a 29 MHz, preferiblemente de 13 MHz a 14 MHz, todavía preferiblemente aproximadamente a 13,56 MHz.

9. Un documento de seguridad según la reivindicación 7 u 8, en el que el chip de RFID de UHF funciona en una frecuencia en el intervalo de 433 MHz a 950 MHz, preferiblemente de 860 MHz a 870 MHz.

10. Un documento de seguridad según cualquiera de las reivindicaciones anteriores, en el que las primeras y segundas etiquetas de RFID se forman integralmente en un único chip.

11. Un documento de seguridad según cualquiera de las reivindicaciones anteriores, en el que la segunda etiqueta de RFID no contiene datos pertenecientes al propietario del documento.

12. Un documento de seguridad según cualquiera de las reivindicaciones anteriores, en el que el documento de seguridad es un pasaporte.

13. Un sistema de seguridad (10) que comprende una pluralidad de documentos de seguridad (20) según cualquiera de las reivindicaciones anteriores, el código de identificación de cada documento es único para ese documento, un primer lector adaptado para leer los datos de las primeras etiquetas de RFID, un segundo lector adaptado para leer los datos de las segundas etiquetas de RFID, una base de datos que tiene unos registros de datos que contienen detalles de cada propietario de documento de seguridad y el correspondiente código de identificación, y un procesador adaptado para, tras el reconocimiento de un código de identificación por parte del primer o segundo lector, recuperar los correspondientes registros de datos de la base de datos.

14. Un sistema de seguridad según la reivindicación 13, en el que el procesador se vincula además a por lo menos una base de datos externa y está adaptado además para recuperar registros correspondientes al propietario identificado del documento de seguridad de por lo menos una base de datos externa.

Fig.1.

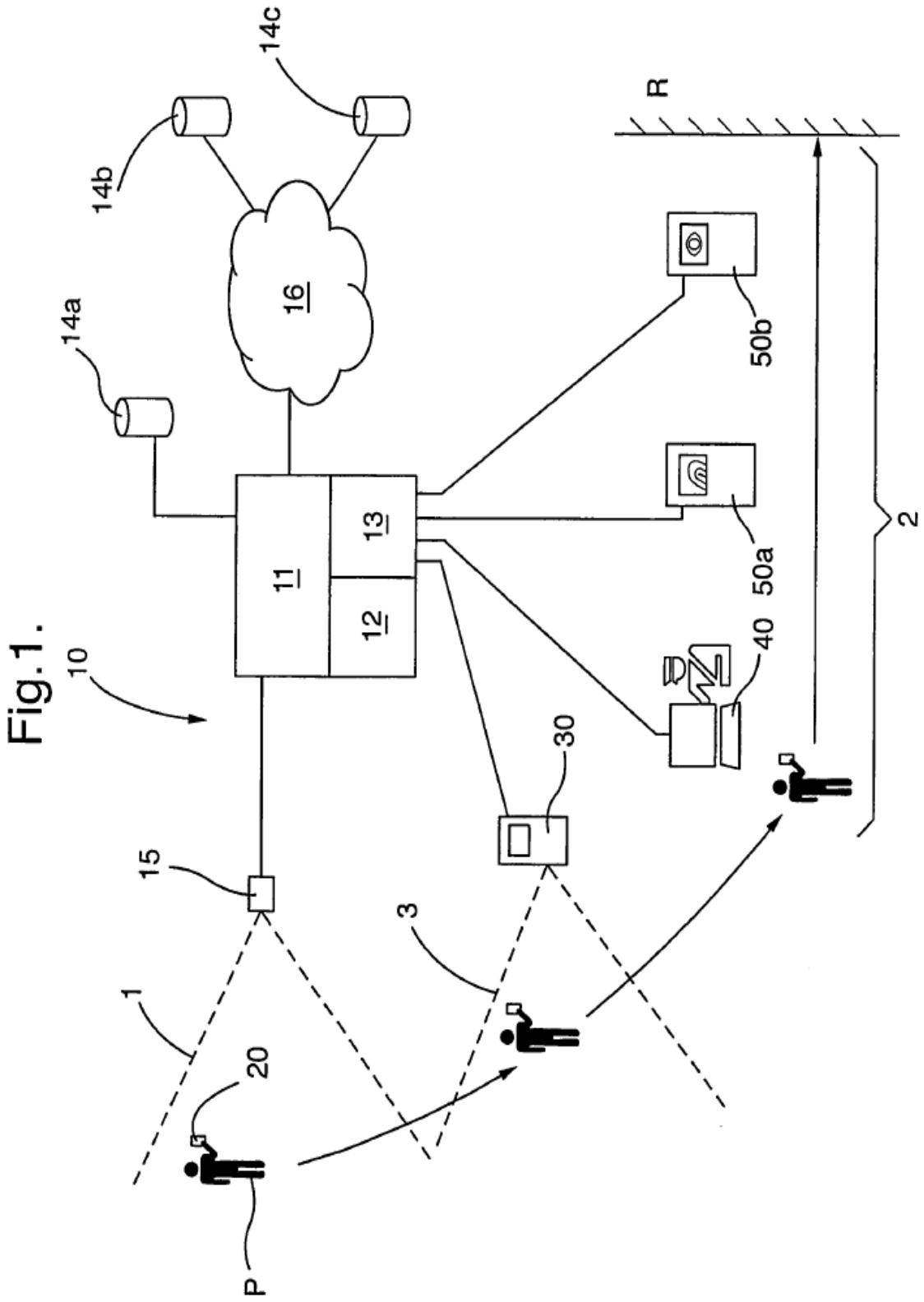


Fig.2.

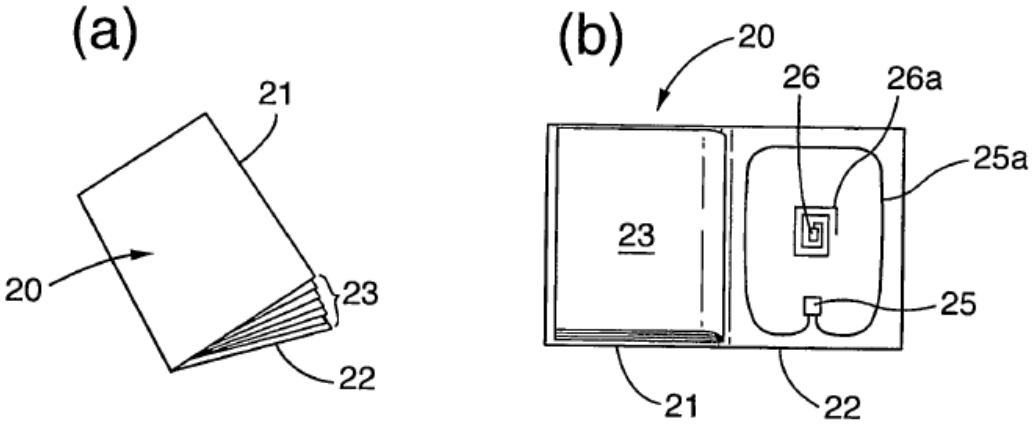


Fig.3.

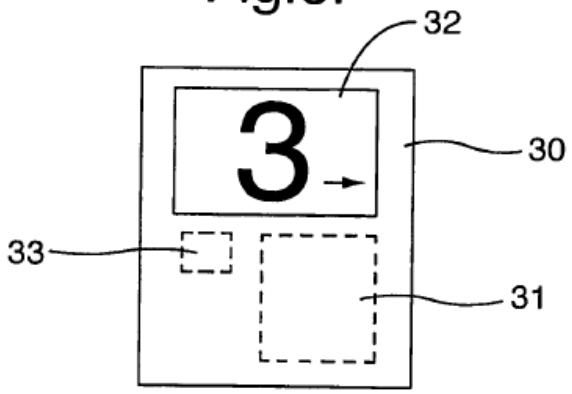


Fig.4.

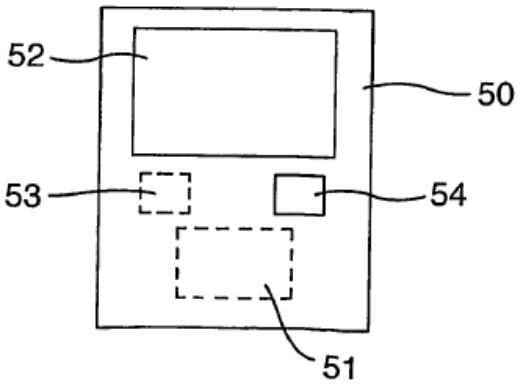
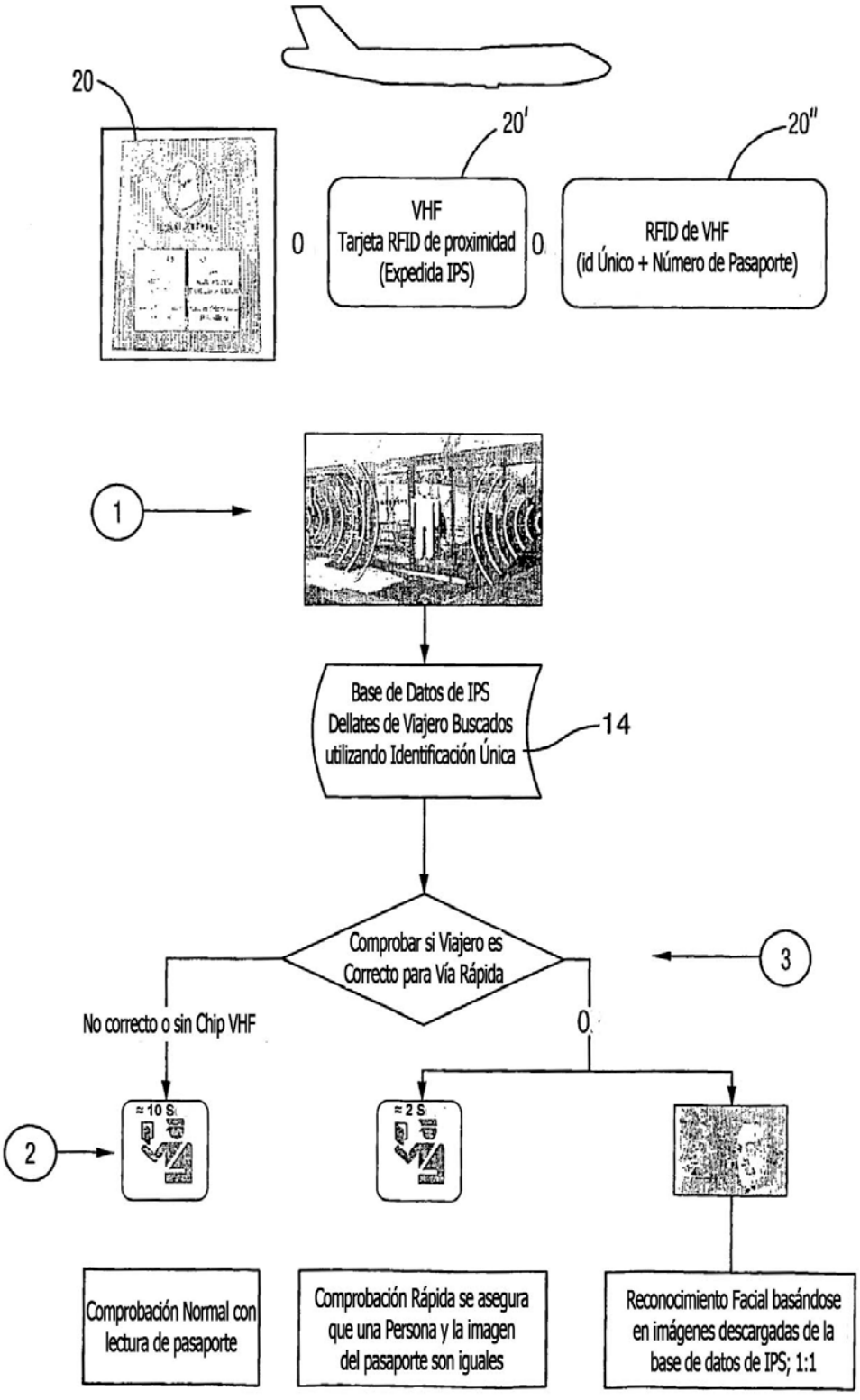


Fig.5.


20
20'
20''
VHF
Tarjeta RFID de proximidad
(Expedida IPS)
O
O
RFID de VHF
(id Único + Número de Pasaporte)
1
Base de Datos de IPS
Dellates de Viajero Buscados
utilizando Identificación Única
14
Comprobar si Viajero es
Correcto para Vía Rápida
3
No correcto o sin Chip VHF
O
2
≈ 10 S
≈ 2 S
Comprobación Normal con
lectura de pasaporte
Comprobación Rápida se asegura
que una Persona y la imagen
del pasaporte son iguales
Reconocimiento Facial basándose
en imágenes descargadas de la
base de datos de IPS; 1:1

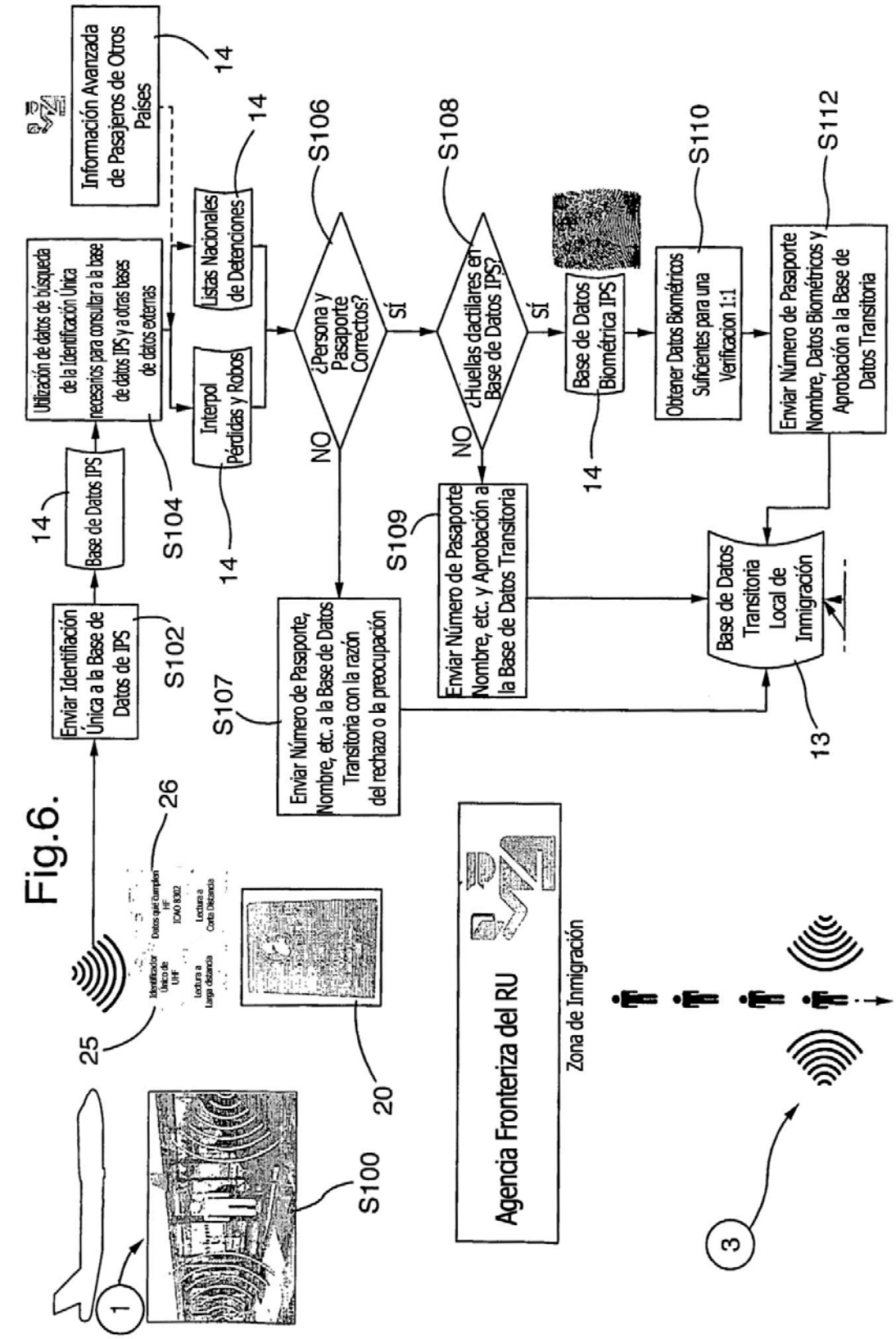
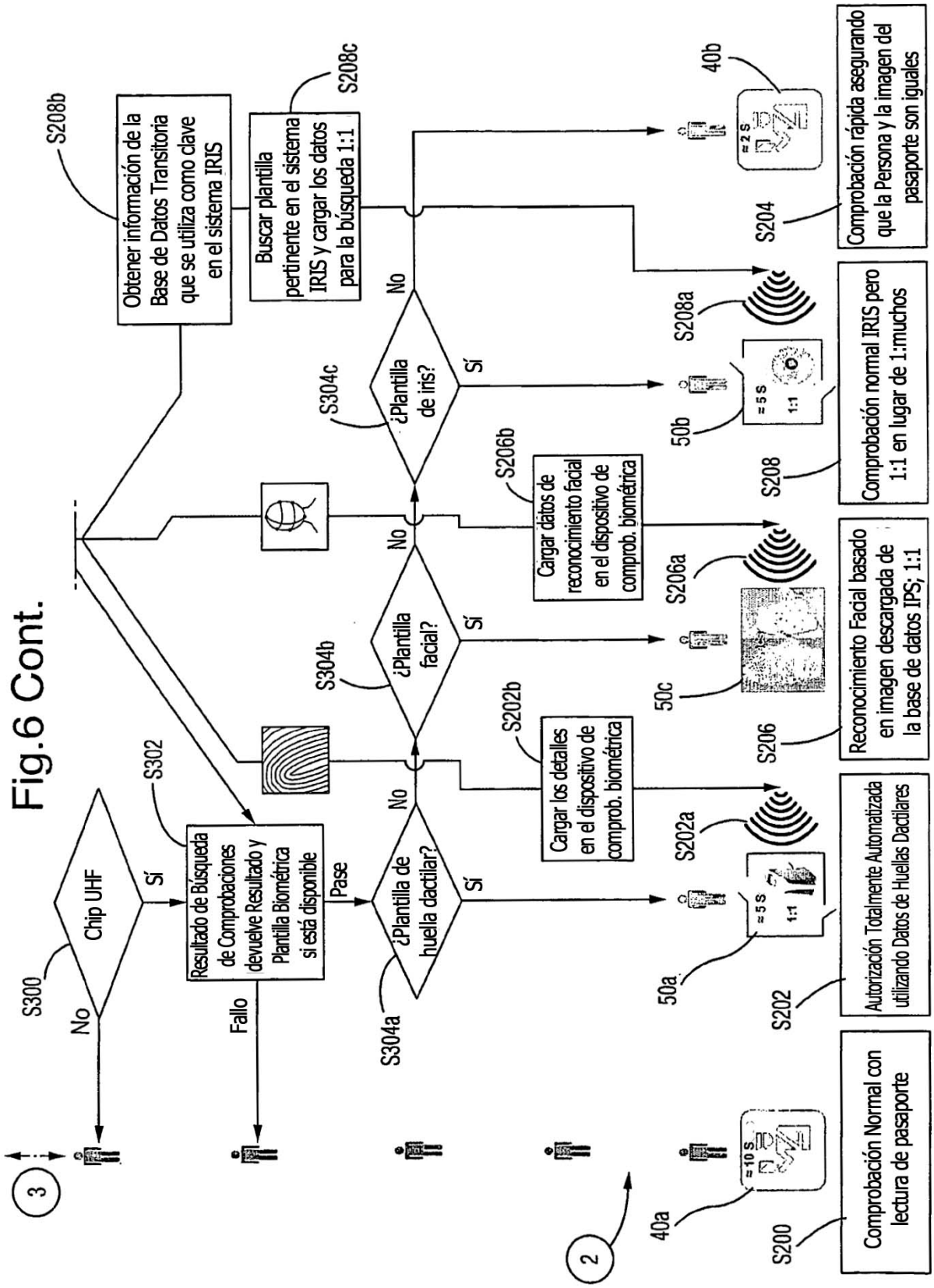

Información Avanzada de Pasajeros de Otros Países
14
Utilización de datos de búsqueda de la Identificación Única necesarios para consultar a la base de datos IPS y a otras bases de datos externas
Base de Datos IPS
14
Enviar Identificación Única a la Base de Datos de IPS
S102
S104
Interpol Pérdidas y Robos
Listas Nacionales de Detenciones
14
S106
¿Persona y Pasaporte Correctos?
SÍ
NO
S108
¿Huellas dactilares en Base de Datos IPS?
SÍ
NO
Base de Datos Biométrica IPS
14
S110
Obtener Datos Biométricos Suficientes para una Verificación 1:1
S112
Enviar Número de Pasaporte Nombre, Datos Biométricos y Aprobación a la Base de Datos Transitoria
S107
Enviar Número de Pasaporte, Nombre, etc. a la Base de Datos Transitoria con la razón del rechazo o la preocupación
S109
Enviar Número de Pasaporte Nombre, etc. y Aprobación a la Base de Datos Transitoria
Base de Datos Transitoria Local de Inmigración
13
26
Identificador Único de UHF
Datos del Pasaporte UHF ICAO 9303
Lectura a Larga distancia
25
20
S100
1
Agencia Fronteriza del RU
Zona de Inmigración
3

Fig.6.

Fig.6 Cont.


S300
Chip UHF
No
Sí
S302
Resultado de Búsqueda de Comprobaciones devuelve Resultado y Plantilla Biométrica si está disponible
Fallo
Pase
S304a
¿Plantilla de huella dactilar?
No
Sí
S202b
Cargar los detalles en el dispositivo de comprob. biométrica
S202a
50a
≈5 s
1:1
S202
Autorización Totalmente Automatizada utilizando Datos de Huellas Dactilares
S304b
¿Plantilla facial?
No
Sí
S206b
Cargar datos de reconocimiento facial en el dispositivo de comprob. biométrica
S206a
50c
S206
Reconocimiento Facial basado en imagen descargada de la base de datos IPS; 1:1
S304c
¿Plantilla de iris?
No
Sí
S208b
Obtener información de la Base de Datos Transitoria que se utiliza como clave en el sistema IRIS
S208c
Buscar plantilla pertinente en el sistema IRIS y cargar los datos para la búsqueda 1:1
S208a
50b
≈5 s
1:1
S208
Comprobación normal IRIS pero 1:1 en lugar de 1:muchos
40b
≈2 s
S204
Comprobación rápida asegurando que la Persona y la imagen del pasaporte son iguales
40a
≈10 s
S200
Comprobación Normal con lectura de pasaporte
3
2