(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 903 124**

(51) Int. CI.:

H04L 9/08 (2006.01)
G06K 19/06 (2006.01)
G07D 7/00 (2006.01)
G06F 21/64 (2013.01)
H04L 9/32 (2006.01)
G06F 21/33 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.09.2016 PCT/EP2016/072256**

(87) Fecha y número de publicación internacional: **30.03.2017 WO17050736**

(96) Fecha de presentación y número de la solicitud europea: **20.09.2016 E 16767282 (3)**

(97) Fecha y número de publicación de la concesión europea: **27.10.2021 EP 3353944**

(54) Título: **Recertificación de documentos**

(30) Prioridad:

24.09.2015 EP 15186653
24.09.2015 EP 15186695

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
31.03.2022

(73) Titular/es:

SICPA HOLDING SA (100.0%)
Avenue de Florissant, 41
1008 Prilly, CH

(72) Inventor/es:

TALWERDI, MEHDI

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Recertificación de documentos

Campo técnico

La presente invención se refiere a sistemas, entidades, y métodos para la certificación de artículos tal como documentos, pasaportes, licencias, títulos, y artículos de valor tal como piezas de arte y similares. Más específicamente, la presente invención se refiere a volver a certificar un artículo/documento en el sentido de verificar y/o renovar un certificado/certificación ya existente.

Antecedentes

La publicación US 7.314.162 divulga un método y sistema para reportar el uso de documentos de identidad al almacenar en una base de datos y reportar a un propietario de documentos de identidad instancias en las que la licencia de conducir, pasaporte u otros documentos de identificación emitidos por el gobierno de esa persona se presentan como una forma de identificación, facilitando de esta manera la notificación temprana del robo de identidad.

Además, la publicación US 7.503.488 divulga un método para evaluar el riesgo de fraude antes de emitir una licencia de conducir a un solicitante con base en la incidencia relativa de fraude históricamente asociado con la combinación particular de documentos de identificación colaterales (por ejemplo, certificado de nacimiento, pasaporte, tarjeta de identificación de estudiante, etc.) presentada por el solicitante en su solicitud de licencia de conducir.

La publicación WO 2015/058948 A1 divulga el punto de control de seguridad que comprende un escáner de documentos para escanear un documento portado por la persona y que comprende además una impresora para imprimir sellos oficiales en un documento de identidad.

La publicación WO 2006/010019 A2 divulga un método para emitir un documento de identificación que comprende: escanear una imagen de al menos un primer documento proporcionado por un solicitante para verificar la identidad del solicitante; crear un registro de datos asociado con el solicitante, el registro de datos que incluye una imagen del primer documento; y emitir el documento de identificación, el documento de identificación que incluye información incorporada leíble por máquina que vincula el documento al registro de datos.

El documento US 2001/041214 A1 describe sistemas y métodos para marcar un artículo con material codificado, almacenar información con respecto al material codificado y el artículo en el que se fija para la recuperación posterior para verificar la autenticidad del artículo.

Es deseable volver a certificar, corregir y/o actualizar tarjetas oficiales (es decir, emitidas por el gobierno) u otros certificados (por ejemplo, certificado de nacimiento), títulos y diplomas educativos, y otros certificados, etc., especialmente aquellos que no tienen una fecha de vencimiento o renovación inherente. Además, puede ser deseable imprimir una marca de certificación en un documento comercial con propósitos de autenticación.

Además, es deseable marcar artículos tal como piezas (obras) de arte y otros artículos de valor ("artículos de valor") con una marca de certificación sin devaluar el artículo de valor (por ejemplo, sin alterar la apariencia visual de una obra de arte). Además, es deseable emplear la infraestructura existente en la medida más eficiente en esté comercialmente disponible impresoras de lectura específicas para uso en documentos tal como pasaportes.

Un objeto de la presente invención es proporcionar un sistema y método que aborda estas necesidades y resuelve los inconvenientes de las técnicas anteriores.

Sumario

Los problemas e inconvenientes mencionados anteriormente de los conceptos convencionales se resuelven por la presente materia de las realizaciones de la presente invención.

Descripción detallada

Las tarjetas y certificados se pueden volver a emitir para hacer correcciones o para actualizar sus características de seguridad, y las tarjetas o certificados antiguos se pueden entregar para su destrucción. Algunas tarjetas y certificados pueden mostrar una fecha de vencimiento y requieren renovación periódica (por ejemplo, pasaporte, licencia de conducir, etc.). Las impresoras de lectura específicas están comercialmente disponibles para uso en la impresión de reemisiones de tarjetas y certificados.

Una realización de la presente invención incluye un servidor de propósito especial que comprende uno o más de un servidor de aplicaciones, un módulo de recolección de datos, un módulo de análisis, un módulo de alerta, un módulo de cortafuegos y antimanipulación, y/o un módulo de comunicaciones seguras. Este servidor de aplicaciones puede

proporcionar control operativo basado en la nube de propiedad privada de un lector, impresora, y/o lector-impresora integrado, cualquiera que se pueda instalar, y otras funciones administrativas, aliviando de esta manera la carga de integrar un lector-impresora en sistemas electrónicos de terceros existentes.

El módulo de recolección de datos recolecta y almacena en una base de datos todos los datos permitidos por la ley nacional (por ejemplo, leyes de privacidad) que se asocia con cada uso o usos seleccionados de un pasaporte u otro artículo de valor, incluyendo: (i) escaneos del artículo de valor por lector o lector-impresora integrada, incluyendo escaneos múltiples en múltiples longitudes de onda de radiación electromagnética, ultrasonidos (por ejemplo, de artículos de valor líquido), escaneos de rayos X, escaneos láser; (ii) identificación de artículo de valor tal como un número de pasaporte, imágenes u otra identificación del pasaporte y sus contenidos, incluyendo la posición dentro de un pasaporte determinado de cualquier sello oficial anterior (por ejemplo, Visa) en ese pasaporte determinado; (iii) datos biométricos y biográficos del titular o propietario de artículo de valor, tal como huellas dactilares, escaneos oculares, escaneos faciales, escaneos corporales, datos de sensores de calor infrarrojos, registros audiovisuales (descritas además más adelante), etc.; (iv) fecha, hora y ubicación de cada uso o usos seleccionados del artículo de valor, incluyendo, por ejemplo, cuando se escanea un pasaporte en una instalación de escaneo de pasaportes, tal como un cruce de frontera, un centro de distribución de transporte, tal como aeropuertos, muelles de barcos y estaciones de tren, o en bancos, hoteles, etc., o cuando se escanea un artículo de valor en una instalación de escaneo (es decir, una instalación que tiene un lector o un lector-impresora integrado); (v) registros de sonido, imagen o vídeo de las interacciones entre los titulares de pasaportes y los funcionarios en una instalación de escaneo de pasaportes u otros registros con relación al uso del artículo de valor, metadatos de medios asociados (por ejemplo, número de cuadros registrados, firmas de frecuencia de voz u otros datos registrados) y las métricas calculadas a partir de estos metadatos de medios (por ejemplo, que se pueden cifrar y emplear para complementar las tecnologías antimanipulación existentes); (vi) datos de vídeo que muestren a personas que utilizan el pasaporte u otro artículo de valor; (vii) información de recorrido asociada con el titular o propietario de artículo de valor, por ejemplo, información de llegada y/o destino, tal como el número de vuelo de una aerolínea asociado con un pasaporte que se escanea en un aeropuerto u otra instalación de escaneo de pasaporte; (viii) información médica (por ejemplo, estado de salud, exposición previa a enfermedades transmisibles, reportes médicos, etc.) asociada con un titular de pasaporte, individuo (por ejemplo, refugiado) presente en un centro oficial de recolección de datos o propietario de un artículo de valor; (ix) documentación relacionada, tal como un escaneo de formularios de aduanas, escaneos de documentos de identificación secundarios, notas de los funcionarios implicados, etc. (x) identidad del oficial responsable implicado con el manejo un pasaporte u otro artículo de valor, por ejemplo, cuando el oficial se identifica por huella dactilar utilizando el lector-impresora, si está instalado, u otro parámetro biométrico, por ejemplo; y (xi) contenidos de RFID donde se instala un chip RFID en un pasaporte, etiqueta o calcomanía (por ejemplo, fijado a un objeto) o artículo de valor y escaneado en la instalación de escaneo (pasaporte). La base de datos también puede almacenar información con relación a la Visa, entrada nacional, salida nacional, formulario de aduana, sellos de pasaporte u otros sellos oficiales para uso en el control de manera central (es decir, remotamente) de un lector, impresora y/o lector-impresora integrado, cualquiera que se pueda instalar.

El módulo de análisis analiza los datos almacenados en la base de datos para determinar, en tiempo real, el uso potencialmente irregular de un pasaporte u otro artículo de valor, tal como donde una entrada en o salida de un país se intenta por un titular de pasaporte sin una salida o entrada anterior correspondiente, o donde un titular de artículo de valor está exhibiendo patrones de comportamiento notables tal como nerviosismo. El módulo de análisis también monitorea las bases de datos de INTERPOL, Europol, las bases de datos nacionales de antecedentes penales, y otras bases de datos para identificar individuos de interés que están intentando utilizar un pasaporte en una instalación de escaneo de pasaporte u otro artículo de valor en una instalación de escaneo. El módulo de análisis monitorea las restricciones de duración de la estancia para emitir una alerta si un titular de pasaporte tiene una estancia prolongada (por ejemplo, no ha salido de un país para la fecha de vencimiento de su visa) o tiene una estancia acortada (por ejemplo, no ha permanecido un tiempo suficiente en un país para calificar para un estado de inmigración especificable).

El módulo de alerta, El módulo de alerta advierte al oficial responsable u otro funcionario cuando el pasaporte u otro artículo de valor escaneado por el oficial se ha señalado por el módulo de análisis como que se asocia con el uso irregular o de otra manera problemático. También se generan alertas cuando se detecta manipulación u otro daño físico al servidor de propósito especial o al módulo del mismo. Las alertas se pueden proporcionar mediante el módulo de comunicaciones seguras (descrito a continuación), y/o por correo electrónico, mensaje de texto y/o de voz (por ejemplo, a un teléfono móvil), etc., al oficial responsable u otro funcionario. Las alertas se pueden proporcionar a cualquier agencia oficial en todo el mundo, como se permita por la ley, con los propósitos de seguridad proactiva.

El módulo cortafuegos y antimanipulación protege el servidor de propósito especial de ataques externos basados en Internet, y también monitorea la manipulación física, intrusión u otro daño a los componentes de hardware de propósito especial.

El módulo de comunicaciones seguras proporciona cifrado para las comunicaciones entre el servidor de propósito especial y los sistemas electrónicos de los gobiernos nacionales participantes, agencias de los mismos, empresas comerciales, u otros clientes, utilizando técnicas de cifrado consistentes con las preferencias de cliente y los requisitos legales. El módulo de comunicaciones seguras facilita las comunicaciones entre el Servidor de propósito especial y las computadoras de cliente, incluyendo lectores, impresoras y/o lector-impresoras integrados específicos, en las instalaciones de escaneo (de pasaportes). El módulo de comunicaciones seguras es operable para comunicarse con las

computadoras de cliente dentro de cada país mediante una VPN específica del país (red privada virtual). En algunas realizaciones, se emplea una VPN separada para cada instalación de escaneo (pasaporte). Las comunicaciones específicas del país facilitan la transferencia de información entre países (dentro de los límites de las leyes de ambos países) mediante el Servidor de propósito especial, a pesar de la incompatibilidad entre los respectivos sistemas electrónicos relacionados con pasaportes de diferentes países. De manera más general, el módulo de comunicaciones seguras facilita la transferencia de información entre clientes suscriptores a pesar de las incompatibilidades entre sus respectivos sistemas al recibir datos de un primer cliente suscriptor de acuerdo con un primer protocolo de comunicación y entonces transmitir datos desde el Servidor de propósito especial a un segundo cliente suscriptor de acuerdo con un segundo protocolo de comunicación donde el primer y segundo protocolos de comunicación no son necesariamente compatibles entre sí.

Cualquier número de módulos del servidor de propósito especial se puede integrar en una unidad de caja negra personalizada, y cualquier módulo determinado se puede comercializar como una unidad independiente adecuada para integrarse con sistemas electrónicos de terceros existentes.

Una impresora específica o lector-impresora integrado, se puede controlar directamente como una unidad independiente o controlar de manera central por el servidor de propósito especial para imprimir marcas de recertificación en tarjetas y certificados oficiales, imprimiendo de esta manera información correctiva y/o empleando características de seguridad más nuevas. A manera de ejemplo, una tarjeta o certificado oficial que se acepta como auténtico se puede escanear por un lector o un lector-impresora integrado, los resultados de escaneo se pueden almacenar por el servidor de propósito especial en su base de datos, una marca de certificación se genera con base en una plantilla seleccionada y datos de campo dinámicos (que opcionalmente incluye datos codificados producidos con base en los resultados de escaneo); y la marca de certificación se imprime en la tarjeta o certificado oficial.

En el caso de tiques de eventos u otros tiques comprados para servicios comerciales (por ejemplo, boletos de transporte), el uso del lector-impresora para sellar o imprimir de otra manera en el tique para indicar que ya se ha utilizado permite el uso de características de seguridad (por ejemplo, características de seguridad incorporadas en la tinta utilizada para la impresión). Hacer visible el sello impreso inhibe la reutilización inapropiada de estos tiques por otros.

A manera de ejemplo adicional, un conocimiento de embarque que se acepta como auténtico antes del uso muestra información que describe los productos (por ejemplo, estándar de calidad, cantidad, etc.) que se van a enviar. Esta información del conocimiento de embarque se cifra y se genera una marca de certificación que contiene la información cifrada. La marca de certificación se imprime en el conocimiento de embarque por la impresora o el lector-impresora integrado antes del envío. En el destino, se comparan el conocimiento de embarque y las mercancías realmente contenidas en el contenedor enviado. Si se encuentra alguna discrepancia, los datos cifrados de la marca de certificación se descifran y se comparan a la información mostrada en el conocimiento de embarque para determinar si el conocimiento de embarque se alteró (por ejemplo, manipuló) durante el envío. De manera adicional o alternativamente, la información descifrada se puede comparar con los productos recibidos.

Como un ejemplo adicional, los manojos de dinero en efectivo se pueden retener conjuntamente por una envoltura de papel que se ha impreso en el mismo, por la impresora o lector-impresora integrado antes de transportar, almacenar, etc., un certificado que contiene una indicación cifrada de la cantidad de dinero en el manojo.

En variaciones, se pueden imprimir múltiples marcas de certificación en múltiples ubicaciones que pueden ser ubicaciones aleatorias o ubicaciones seleccionadas por humanos, etc.

Como un paso opcional, se puede tomar una imagen del artículo de valor que tiene las marcas de certificación aplicadas (por ejemplo, por una cámara interna de lector-impresora) y entonces se almacena por el servidor de propósito especial para el uso posterior en la determinación de si se ha presentado la manipulación de las marcas de certificación. A manera de ejemplo, cuando se colocan múltiples marcas de certificación en ubicaciones seleccionadas aleatoriamente (por ejemplo, dentro de límites especificables), las ubicaciones relativas o absolutas de las marcas de certificación se pueden verificar posteriormente. En una variación, el objeto que tiene las marcas de certificación aplicadas a este se escanea por el lector o el lector-impresora integrado y los resultados de escaneo se almacenan por el servidor de propósito especial para la autenticación posterior del artículo de valor y sus marcas de certificación.

De acuerdo con otra realización de la presente invención, se proporcionan modificaciones a la mecánica tal que el lector-impresora se pueda adaptar para soportar la impresión en objetos de varias formas y tamaños. Por ejemplo, un lector/impresora específico puede ser una unidad portátil para escanear objetos de varias formas y tamaños.

De acuerdo con las realizaciones de método de operación de la presente invención, un artículo de valor que se acepta como auténtico se escanea opcionalmente y los datos escaneados se almacenan por el servidor de propósito especial; una marca de certificación se genera con base en una plantilla seleccionada y datos de campo dinámicos (que opcionalmente incluye datos codificados producidos con base en los resultados de escaneo); y la marca de certificación se imprime en el artículo de valor utilizando tinta no penetrante, no absorbente que es visible sólo bajo exposición a radiación electromagnética especificable (por ejemplo, luz ultravioleta).

En variaciones, se pueden imprimir múltiples marcas de certificación en múltiples ubicaciones que pueden ser ubicaciones aleatorias o ubicaciones seleccionadas por humanos, etc. A manera de ejemplo, se pueden emplear marcas de certificación en la parte posterior de una pintura en la unión entre la parte posterior del lienzo y el cuadro. Estas marcas de certificación de parte posterior no necesitan ser invisibles, a manera ejemplo.

En una variación, un escaneo del artículo de valor que tiene las marcas de certificación aplicadas a este se puede tomar por el lector o el lector-impresora integrado en longitudes de onda seleccionadas de radiación electromagnética y entonces se almacena por el servidor de propósito especial para el uso posterior en la determinación de si se ha presentado la manipulación de las marcas de certificación. A manera de ejemplo, cuando se colocan múltiples marcas de certificación en ubicaciones seleccionadas aleatoriamente (dentro de límites especificables), las ubicaciones relativas o absolutas de las marcas de certificación se pueden verificar posteriormente.

Aunque se han descrito realizaciones detalladas, estas sólo sirven para proporcionar una mejor comprensión de la invención definida por las reivindicaciones independientes, y no se van a ver como limitantes.

REIVINDICACIONES

1. Un sistema que comprende un lector-impresora para certificar un elemento de valor auténtico, tal como un documento o una pieza de arte, y un servidor de propósito especial, este lector-impresora que se controla por el servidor de propósito especial, el sistema que se configura para:

- escanear por el lector-impresora el artículo de valor que se acepta como auténtico;

- almacenar por el servidor de propósito especial un resultado del escaneo del artículo de valor en una base de datos;

- generar una marca de certificación que comprende datos codificados producidos con base en el resultado del escaneo del artículo de valor almacenado en la base de datos; y

- imprimir la marca de certificación en el artículo de valor,

caracterizado porque el lector-impresora se configura además para imprimir múltiples marcas de certificación en múltiples ubicaciones en el artículo de valor y escanear el artículo de valor que tiene las marcas de certificación impresas en las múltiples ubicaciones en el mismo, y el servidor de propósito especial se configura para almacenar en la base de datos el escaneo del artículo de valor que tiene las marcas de certificación impresas en las múltiples ubicaciones en el mismo para que una ubicación relativa o absoluta correspondiente de al menos una de las marcas de certificación impresas en las múltiples ubicaciones en el artículo de valor se puedan verificar posteriormente.

2. El sistema de la reivindicación 1, donde el lector-impresora se configura además para imprimir en un documento que incluye cualquiera de un pasaporte, una licencia, un título, y una tarjeta.

3. El sistema de la reivindicación 1 o 2, donde el lector-impresora se configura además para imprimir en objetos de varias formas y tamaños.

4. El sistema de la reivindicación 3, donde el lector-impresora se configura además para imprimir la marca de certificación en un artículo de valor utilizando tinta no penetrante y/o no absorbente que es visible sólo bajo exposición a radiación electromagnética especificable, preferentemente luz ultravioleta.

5. El sistema de la reivindicación 3 o 4, donde las múltiples ubicaciones son ubicaciones aleatorias o ubicaciones seleccionadas por humanos.

6. El sistema de la reivindicación 1, donde el escaneo del artículo que tiene las marcas de certificación impresas en las múltiples ubicaciones en éste se toma en longitudes de onda seleccionadas de radiación electromagnética.

7. El sistema de la reivindicación 1, donde el servidor de propósito especial incluye uno o más de un servidor de aplicaciones, un módulo de recolección de datos, un módulo de análisis, un módulo de alerta, un módulo de cortafuegos y antimanipulación, y/o un módulo de comunicaciones seguras.