(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 453 113**

(51) Int. CI.:

H04L 29/06 (2006.01)
G07F 7/10 (2006.01)
G06Q 20/04 (2012.01)
G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.05.2009 E 09006230 (8)**

(97) Fecha y número de publicación de la concesión europea: **19.02.2014 EP 2136528**

(54) Título: **Procedimiento y sistema para generar una identidad electrónica derivada a partir de una identidad electrónica principal**

(30) Prioridad:

17.06.2008 DE 102008028701

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.04.2014

(73) Titular/es:

GIESECKE & DEVRIENT GMBH (100.0%)
PRINZREGENTENSTRASSE 159
81677 MÜNCHEN, DE

(72) Inventor/es:

EICHHOLZ, JAN;
GROBBEL, HUBERTUS;
ASCHAUER, HANS y
MEISTER, GISELA, DR.

(74) Agente/Representante:

ARPE FERNÁNDEZ, Manuel

DESCRIPCIÓN

Procedimiento y sistema para generar una identidad electrónica derivada a partir de una identidad electrónica principal

La invención se refiere a un procedimiento y un sistema para generar una identidad electrónica derivada a partir de una identidad electrónica principal.

El usuario de una identidad electrónica principal, por ejemplo la identidad depositada en el soporte de datos de un pasaporte electrónico, tiene a menudo la necesidad de, además de su identidad principal, emplear también otra identidad para fines especiales, por ejemplo para procurarse con esta identidad el acceso al terreno de empresa de su lugar de trabajo o utilizar esta identidad para acceder a un ordenador. De este modo puede reducirse en particular la utilización de la muy importante identidad principal del usuario sólo a casos muy especiales, con lo que se reducen las oportunidades de un ataque a la misma. Dado que la identidad principal se utiliza ya sólo en contadas ocasiones, el desgaste físico del soporte de datos que contiene la identidad principal es menor y también se producen menos pérdidas de la identidad principal.

Por el documento US 2007/0078786 A1 se conoce el método de generar una segunda identificación para una persona, en particular en forma de una segunda dirección postal, dirección de correo electrónico, número de teléfono y similares. Esta segunda identificación se utiliza en combinación con servicios de identificación correspondientes, a los que también se dirige la petición de generar una segunda identificación. Por lo tanto, la generación de la identificación lleva asociada la presentación de una petición a un servicio de identificación, con lo que la generación de la identificación resulta costosa.

El documento WO0182092 da a conocer un procedimiento para la delegación de derechos de acceso de un usuario en otro, realizándose el control de acceso mediante un certificado en las tarjetas chip del usuario. El usuario puede a su vez registrar por sí mismo nuevos usuarios del sistema.

El objetivo de la invención es crear un procedimiento y un sistema para generar una identidad derivada a partir de una identidad principal, con los que sea posible generar en un soporte de datos predeterminado la identidad derivada de un modo fácil y seguro.

Este objetivo se consigue mediante las reivindicaciones independientes. En las reivindicaciones dependientes se definen perfeccionamientos de la invención.

A continuación se describen detalladamente unos ejemplos de realización de la invención por medio de las figuras adjuntas.

Muestran:

- figura 1 una representación esquemática del desarrollo de una primera forma de realización del procedimiento según la invención; y

- figura 2 una representación esquemática del desarrollo de una segunda forma de realización del procedimiento según la invención.

La figura 1 muestra el desarrollo de un procedimiento no correspondiente a la invención, en el que a partir de una identidad principal o maestra original 20 de un pasaporte electrónico 2, considerado en lo que sigue como representativo de un documento de identificación electrónico, se genera una identidad derivada 30 intercalando un servidor de identidad 40. La identidad maestra almacenada en el pasaporte electrónico incluye aquí una clave pública y una clave privada, así como un certificado que se ha generado, por ejemplo, mediante la firma de la clave pública por parte de una entidad de certificación de confianza. Entre el servidor de identidad y las identidades 20 o 30 puede establecerse una conexión de datos mediante una red 50 correspondiente, por ejemplo Internet.

Un usuario humano 10, cuyos datos de identidad están almacenados como identidad maestra 20 en el pasaporte electrónico 2, desea generar una identidad derivada a partir de su identidad maestra, ya que no desea emplear su pasaporte electrónico como tarjeta de autenticación en todas partes. En particular, la identidad derivada está destinada a ser utilizada en casos especiales, por ejemplo como tarjeta de identidad para el acceso al lugar de trabajo, para utilizar un PC y similares. La identidad derivada está designada en la figura 1 con la referencia 30 y ha de depositarse en un soporte de datos en forma de un testigo (*token)* USB 3.

Para generar la identidad derivada, el usuario 10 inicia la derivación de identidad. En primer lugar se realiza un proceso de autenticación entre la identidad maestra 20 y el servidor de identidad 40, pudiendo desarrollarse esta autenticación según cualesquiera procedimientos ya conocidos en el estado actual de la técnica, en particular incluyendo los certificados o las claves de la identidad maestra y del servidor de identidad. Tras la autenticación o basándose en la misma se establece entonces un canal de datos seguro entre la identidad maestra 20 y el servidor de identidad 40. Para poder establecer también una conexión segura y autenticada entre la identidad derivada 30 y el servidor de identidad 40, la identidad derivada 30 debe identificarse de forma unívoca. En el procedimiento según

la figura 1, esto se realiza intercalando al usuario 10 que, a través de una vía de comunicación segura, transmite al servidor de identidad 40 una identificación unívoca del testigo USB en el que ha de almacenarse la identidad derivada. La identificación unívoca puede ser el número de serie del testigo USB 3, que el usuario por ejemplo lee en el testigo.

Por último, incluyendo la identificación unívoca del testigo USB, el servidor de identidad 40 y la identidad derivada 30 se autentican uno ante otro y establecen un canal de datos seguro. Finalmente, la identidad derivada 30 genera una pareja de claves compuesta por una clave pública y una clave privada, pudiendo la pareja de claves ser generada también en caso dado por el servidor de identidad 40 y transmitida por el servidor de identidad a la identidad derivada a través del canal seguro. Para mantener el secreto de la clave privada, esta clave se almacena en el soporte de datos 3 de manera segura y no legible. La identidad derivada 30 se especifica además mediante un certificado que, según la figura 1, se genera por el método de firmarse la clave pública de la identidad derivada 30 en el servidor de identidad 40 con su clave privada, devolviéndose a la identidad derivada a través del canal de datos seguro esta clave pública firmada como certificado de la identidad derivada. A continuación, el certificado se guarda en el soporte de datos 3.

Adicionalmente a la pareja de claves generada en el soporte de datos 3, también pueden transmitirse a la identidad derivada 30 por medio del servidor de identidad 40 otros datos y derechos de acceso de la identidad maestra 20. En particular pueden especificarse en la identidad derivada derechos de acceso especiales, que pueden ser distintos de los derechos de acceso de la identidad maestra. Por ejemplo pueden depositarse restricciones en la identidad derivada relativas a la utilización prevista para la identidad. Para asegurarse de que la identidad derivada 30 pueda ser utilizada sólo por el usuario de la identidad principal, en una etapa final el usuario 10 deposita por último en la identidad derivada 30 un código de seguridad, en particular en forma de un PIN o de otra característica de seguridad. Una vez activada esta característica de seguridad por el usuario, la identidad derivada 30 puede finalmente emplearse para la identificación del usuario 10.

En principio, la identidad derivada 30 puede emplearse del mismo modo que la identidad maestra 20. Dado que el servidor de identidad 40 se ha encargado de generar el certificado para la identidad derivada 30, también es posible una diferenciación de la identidad maestra 20 y la identidad derivada 30 por parte de un comprobador, ya que los certificados de la identidad maestra y de la identidad derivada son diferentes. Por consiguiente, un comprobador puede decidir por medio de los certificados si un servicio está disponible sólo para la identidad maestra 20 y/o también para una determinada identidad derivada. Por medio del certificado de la identidad derivada 30 es posible además limitar fácil y adecuadamente la validez temporal de la identidad derivada 30, siempre que esto sea necesario.

La figura 2 muestra el desarrollo de una forma de realización del procedimiento según la invención. A diferencia del procedimiento de la figura 1, no se intercala ningún servidor de identidad en la generación de la identidad derivada 30 a partir de la identidad maestra 20. La identidad derivada se genera mediante un canal de datos directo entre la identidad maestra 20, almacenada en el pasaporte electrónico 2, y el soporte de datos 3 en el que se ha de almacenar la identidad derivada 30.

Análogamente a la figura 1, en primer lugar el usuario 10 inicia la derivación de identidad. Aquí se realiza una autenticación directa entre la identidad maestra 20 y la identidad derivada 30, pudiéndose emplear de nuevo en esta autenticación una identificación unívoca del soporte de datos 3 (por ejemplo su número de serie), como ya se ha explicado en el caso de la autenticación entre el servidor de identidad 40 y el soporte de datos 3 en el procedimiento de la figura 1. Tras la autenticación, se establece finalmente un canal seguro entre la identidad maestra 20 y el soporte de datos 3. A continuación, el soporte de datos 3 genera una pareja de claves compuesta por una clave pública y una clave privada, almacenándose nuevamente la clave privada en el soporte de datos 3 de manera segura y no legible.

A diferencia del procedimiento de la figura 1, la generación de un certificado para la identidad derivada ya no se realiza ahora intercalando un servidor de identidad, sino que la identidad maestra genera el certificado firmando con la clave privada de la identidad maestra la clave pública generada de la identidad derivada. Esta clave pública firmada se devuelve al soporte de datos 3 y se almacena en el mismo como el certificado de la identidad derivada. A continuación se leen del pasaporte 2 otros datos de la identidad maestra y derechos de acceso correspondientes válidos para la identidad derivada, que se devuelven a la identidad derivada y se almacenan en la misma en el soporte de datos 3.

En caso dado puede estar depositada en la identidad maestra una cadena de certificados que representa una serie de certificados, estando cada certificado firmado por otro certificado de la serie. La cadena de certificados termina finalmente en un certificado original o raíz. Siempre que en la identidad maestra 20 esté depositada una cadena de certificados de este tipo, esta cadena se devuelve a la identidad derivada 30 y se almacena en la misma. Se crea por lo tanto en la identidad derivada una cadena de certificados ampliada que, además de la cadena de certificados de la identidad maestra, contiene finalmente el certificado de la identidad derivada generado por la identidad maestra.

Por último, análogamente al procedimiento de la figura 1, antes de la activación de la identidad derivada el usuario 10 deposita en el soporte de datos 3 una característica de seguridad para la autenticación del usuario con la identidad derivada. La característica de seguridad puede ser aquí de nuevo un PIN u otra característica de seguridad. A continuación, una vez activada la característica de seguridad, puede emplearse la identidad derivada 30.

La identidad derivada 30 generada según la figura 2 puede emplearse en esencia del mismo modo que la identidad maestra 20. Sin embargo, es posible distinguir una de otra las dos identidades, ya que al comprobar la cadena de certificados de la identidad derivada 30 debe comprobarse adicionalmente el certificado generado por la identidad maestra 20. De este modo, un comprobador puede diferenciar por consiguiente la identidad maestra 20 de la identidad derivada 30. Por medio de los certificados, el comprobador puede decidir si un servicio debe estar disponible sólo para la identidad maestra 20 o también para una determinada identidad derivada. Análogamente a la forma de realización de la figura 1, con el certificado de la identidad derivada 30 generado en el procedimiento de la figura 2 también se puede limitar adecuadamente la validez temporal de la identidad derivada.

Según las formas de realización de la invención arriba descritas pueden generarse fácilmente una o varias identidades derivadas a partir de una identidad maestra. Las identidades derivadas pueden utilizarse entonces en lugar de la identidad maestra para la autenticación. La generación de la identidad derivada no se trata de un puro proceso de copia, sino de una verdadera derivación. En particular se asegura también que la identidad maestra y la identidad derivada se puedan diferenciar una de otra.

REIVINDICACIONES

1. Procedimiento para generar una identidad electrónica derivada (30) a partir de una identidad electrónica principal (20), **caracterizado porque**
a) entre un primer soporte de datos (2), en el que está almacenada la identidad principal (20), que comprende una primera pareja de claves compuesta por una primera clave pública y una primera clave privada, y un segundo soporte de datos (3), para el almacenamiento de la identidad derivada (30), se establece una conexión de datos autenticada, siendo la identidad principal (20) la identidad de un usuario (10) almacenada en un documento electrónico de identificación, especialmente en un pasaporte electrónico;
b) el segundo soporte de datos (30) genera una segunda pareja de claves que comprende una segunda clave pública y una segunda clave privada;
c) se genera un certificado de la identidad derivada (20) enviando al primer soporte de datos (2) la segunda clave pública y firmando esta última en el primer soporte de datos (2) con la primera clave privada de la identidad principal (20);
d) el segundo par de claves y el certificado de la identidad derivada (20) se almacenan en el segundo soporte de datos (3);
e) y en el segundo soporte de datos (3) se almacena una característica de seguridad determinada para la identidad derivada (30), para la autenticación de un usuario (10) con la identidad derivada (20).

2. Procedimiento según la reivindicación 1, caracterizado porque la conexión de datos autenticada de la etapa a) se establece intercalando un servidor de identidad (40).

3. Procedimiento según la reivindicación 2, caracterizado porque se establecen un primer canal de datos seguro basado en un proceso de autenticación entre el primer soporte de datos (2) y el servidor de identidad (40), y un segundo canal de datos seguro basado en un proceso de autenticación entre el servidor de identidad (40) y el segundo soporte de datos (3).

4. Procedimiento según la reivindicación 3, caracterizado porque en el servidor de identidad (40) se deposita una identificación unívoca del segundo soporte de datos (3), y el segundo soporte de datos (3) se autentica ante el servidor de identidad (40) mediante su identificación unívoca.

5. Procedimiento según la reivindicación 1, caracterizado porque la conexión de datos autenticada de la etapa a) se establece mediante un proceso de autenticación directo entre el primer soporte de datos (2) y el segundo soporte de datos (3).

6. Procedimiento según la reivindicación 5, caracterizado porque en el primer soporte de datos (2) se deposita un certificado de la identidad principal (20) o una cadena de certificados, almacenándose el certificado o la cadena de certificados en el segundo soporte de datos.

7. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque en la etapa b) en el segundo soporte de datos (3) se almacenan además derechos de acceso y/o limitaciones y/u otros datos de la identidad principal (20) válidos para la identidad derivada (30).

8. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque la segunda clave privada se almacena en el segundo soporte de datos (3) de manera no legible.

9. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque el primer y el segundo soporte de datos son testigo (*token)* de identidad electrónicos, siendo el primer soporte de datos (2) y/o el segundo soporte de datos (3) especialmente una tarjeta chip o un testigo (*token)* USB.

10. Sistema para generar una identidad electrónica derivada (30) a partir de una identidad electrónica principal (20), que comprende:
un primer soporte de datos (2), en el que está almacenada la identidad principal (20), que comprende una primera pareja de claves compuesta por una primera clave pública y una primera clave privada, y un segundo soporte de datos (3), para almacenamiento de la identidad derivada (30),
caracterizado porque
el primer y el segundo soporte de datos (2, 3) pueden cooperar operativamente de tal manera que es posible realizar un procedimiento según una de las reivindicaciones precedentes.

11. Sistema según la reivindicación 10, caracterizado porque el sistema comprende un servidor de identidad (40) para la realización de un procedimiento según una de las reivindicaciones 1 a 5.

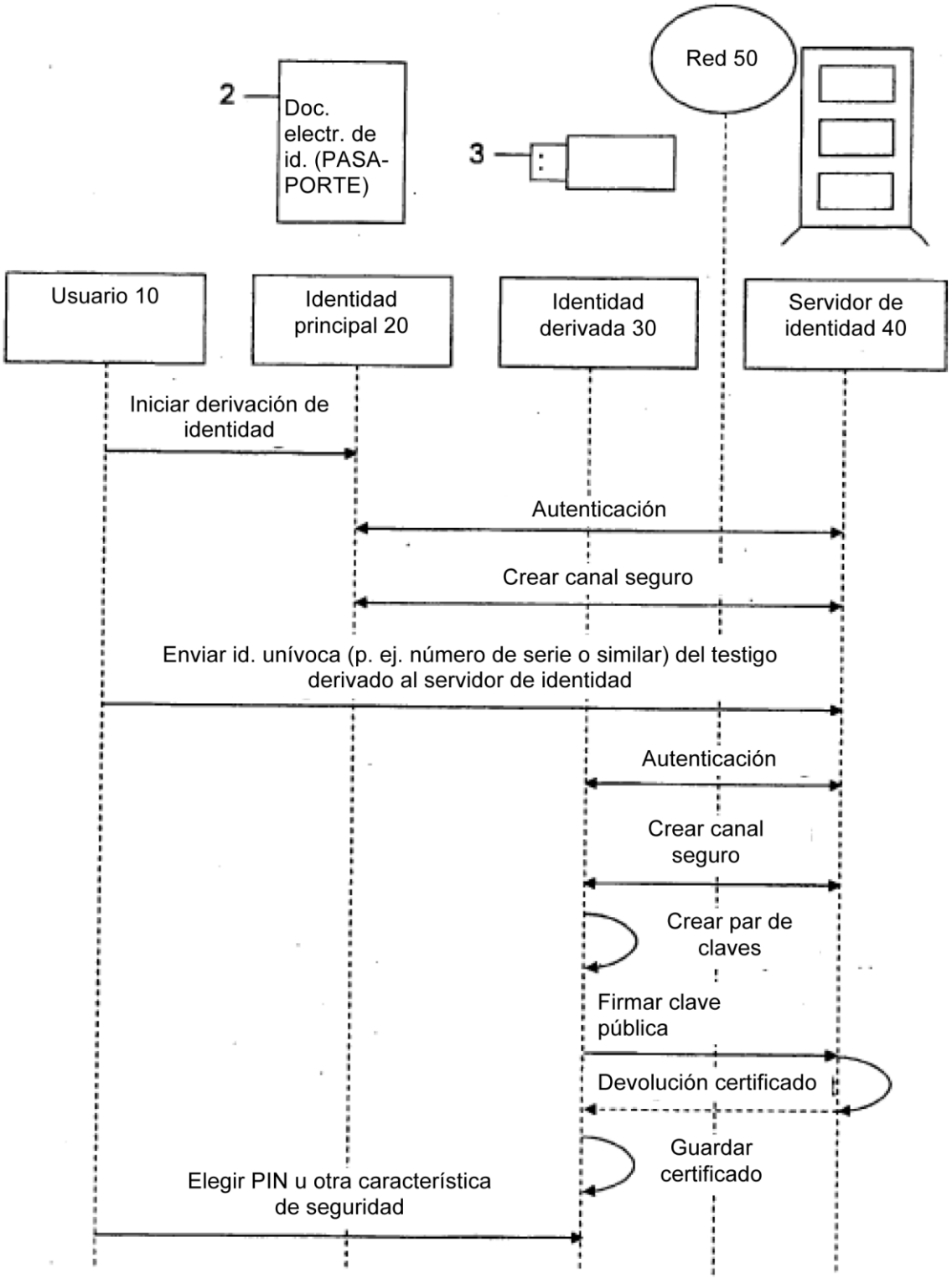
Red 50
2
Doc. electr. de id. (PASA-PORTE)
3
Usuario 10
Identidad principal 20
Identidad derivada 30
Servidor de identidad 40
Iniciar derivación de identidad
Autenticación
Crear canal seguro
Enviar id. unívoca (p. ej. número de serie o similar) del testigo derivado al servidor de identidad
Autenticación
Crear canal seguro
Crear par de claves
Firmar clave pública
Devolución certificado
Guardar certificado
Elegir PIN u otra característica de seguridad

FIGURA 1

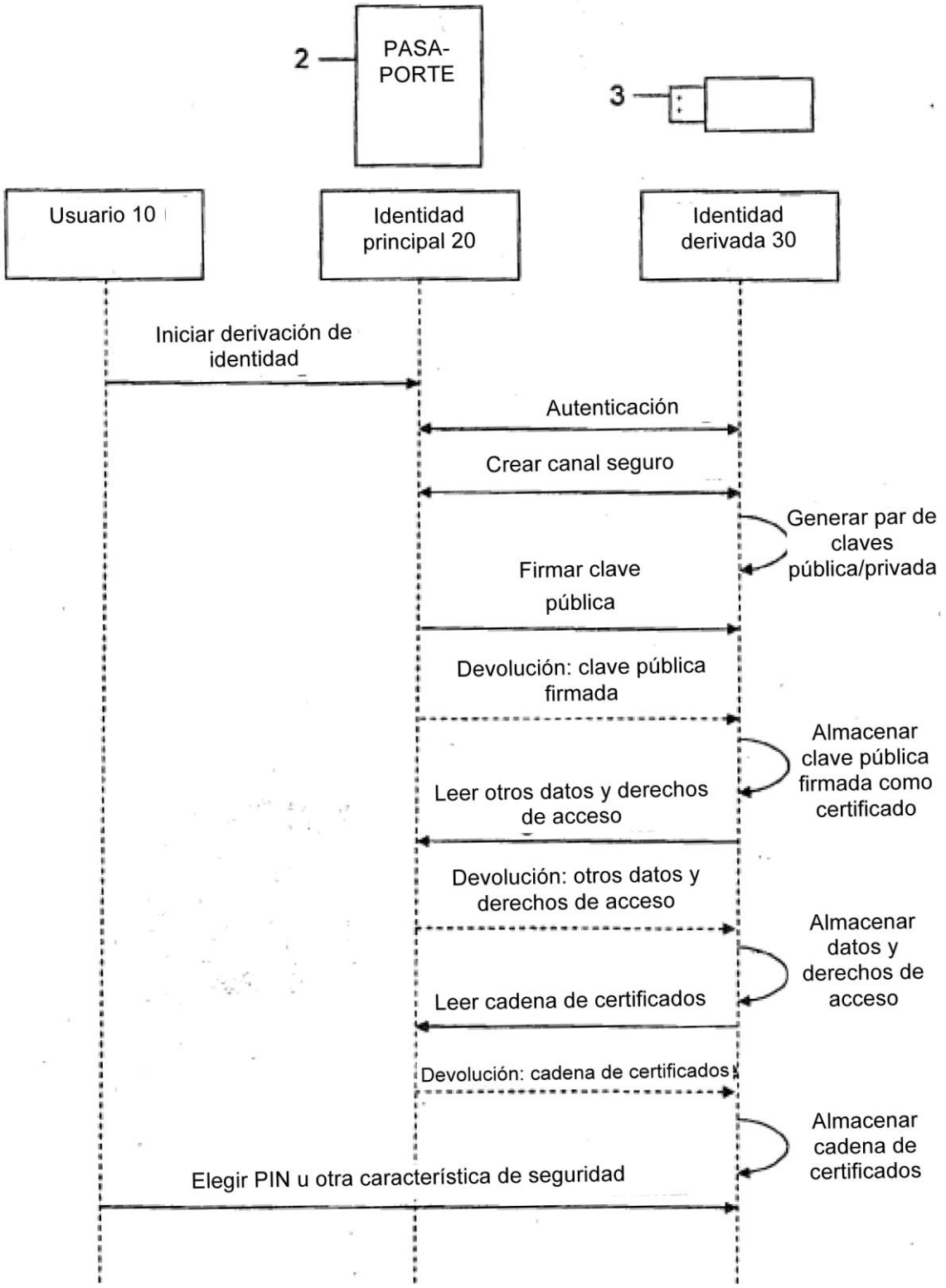
2
PASA-
PORTE
3
Usuario 10
Identidad
principal 20
Identidad
derivada 30
Iniciar derivación de
identidad
Autenticación
Crear canal seguro
Generar par de
claves
pública/privada
Firmar clave
pública
Devolución: clave pública
firmada
Almacenar
clave pública
firmada como
certificado
Leer otros datos y derechos
de acceso
Devolución: otros datos y
derechos de acceso
Almacenar
datos y
derechos de
acceso
Leer cadena de certificados
Devolución: cadena de certificados
Almacenar
cadena de
certificados
Elegir PIN u otra característica de seguridad

FIGURA 2

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

Documentos de patente citados en la descripción

- US 20070078786 A1 **[0003]**
- WO 0182092 A **[0004]**