(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 713 390**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.01.2013 PCT/FR2013/050197**

(87) Fecha y número de publicación internacional: **06.09.2013 WO13128091**

(96) Fecha de presentación y número de la solicitud europea: **31.01.2013 E 13706600 (7)**

(97) Fecha y número de publicación de la concesión europea: **28.11.2018 EP 2820795**

(54) Título: **Procedimiento de verificación de identidad de un usuario de un terminal comunicante y sistema asociado**

(30) Prioridad:

27.02.2012 FR 1251753

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.05.2019

(73) Titular/es:

IDEMIA IDENTITY & SECURITY FRANCE (100.0%)
11 Boulevard Galliéni
92130 Issy-les-Moulineaux, FR

(72) Inventor/es:

BERTEAU, GUILLAUME y
BENTEO, BRUNO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de verificación de identidad de un usuario de un terminal comunicante y sistema asociado

La presente invención concierne al condicionamiento de acceso y/o a la suscripción a un servicio mediante verificación de identidad de un usuario, a partir de un terminal comunicante (especialmente un terminal móvil) del usuario.

La noción de identidad está haciéndose omnipresente y cotidiana en el entorno llamado “móvil”. Esta identidad digital, sin embargo, debe ser protegida contra cualquier forma de usurpación, sin dejar de ser ergonómica en su utilización por su portador.

Las soluciones conocidas (de contraseña de un solo uso u “OTP”, por “One Time Password”, o de firma de un solo uso, OTS o SSO (por Single Signe On), o por SMS (Short Message Service), o normalizadas “Open ID”, u otras), basadas todas ellas en procesos de tipo “identificador de usuario/contraseña” o identificadores de red (número de teléfono, por ejemplo) asociados a una gestión de atributos del usuario, no son completamente satisfactorias.

El documento EP 2323308 da a conocer un procedimiento de asignación de un secreto a un testigo, que comprende la recepción de un primer dato biométrico de una característica biométrica de una persona, el almacenamiento del primer dato biométrico en el testigo de seguridad, el almacenamiento de un secreto no encriptado en el testigo de seguridad, la encriptación biométrica del secreto por medio del primer dato biométrico, y el almacenamiento del secreto encriptado en el testigo de seguridad.

El documento “*Chapter 10: Identification and Entity Authentication ED”*, Menezes A J; Van Oorschot P C; Vanstone S A, Handbook of applied cryptography, páginas 385 a 424, da a conocer técnicas que permiten, a una parte, asegurarse de que la identidad de otra parte realmente se corresponde con la que ha declarado.

El documento “*mCoupons: An Application for Near Field Communication (NFC)”*, Advanced Information Networking And Applications Workshops, 21 de mayo de 2007, páginas 421-428, apartados 5.5 y 5.6, da a conocer un método de autenticación de un usuario mediante la utilización de un par de claves secreta/pública.

La invención propone una solución. La invención propone, en especial, un procedimiento de verificación de identidad de un usuario de un terminal comunicante, que incluye las etapas según la reivindicación independiente 1.

Así, un terminal comunicante (teléfono, tableta, teléfono inteligente), si se asocia con una identidad derivada procedente de un título auténtico, se convierte en un soporte conectado que facilita la validación de los derechos (mediante autenticación fuerte especialmente) y la compartición de datos de seguridad con los agentes locales o remotos de una transacción.

De acuerdo con las formas de realización, el procedimiento de la invención puede presentar una o varias de las siguientes características:

- el cifrado utiliza una infraestructura de clave pública, utilizándose al menos el dato de identidad derivado para generar una clave de cifrado;
- el dato de identidad derivado es un certificado digital que certifica el cifrado por parte del terminal;
- en caso de verificación positiva, el testigo cifrado queda vinculado a un certificado digital de identificación del usuario;
- la comunicación al servidor del primer dato de identidad del usuario se autoriza previa verificación de un dato biométrico del usuario del terminal;
- la etapa actual incluye una verificación de un dato propio del usuario antes de iniciar en el terminal la utilización del segundo dato para el cifrado del testigo;
- se prevé una pluralidad de etapas previas con una pluralidad de comunicaciones a una pluralidad de servidores del primer dato de identidad del usuario, generando cada servidor respectivos segundos datos de identidad del usuario, definiendo cada segundo dato una identidad derivada del usuario, siendo cada identidad derivada propia de un servicio cuyo acceso está condicionado a una verificación de testigo cifrado ante un servidor dedicado a dicho servicio;
- la comunicación al servidor del primer dato de identidad se efectúa a través de un lector que incluye un módulo de comunicación de corto alcance o cableada e, incluyendo el terminal un módulo homólogo de comunicación de corto alcance o cableada, el segundo dato se transmite del servidor al lector, y luego del lector al terminal mediante comunicación a corto alcance o cableada;
- la transmisión del testigo que ha de cifrarse y/o del testigo cifrado, entre el servidor y el terminal, se efectúa a través de un equipo que solicita un acceso a un servicio al que está asociado el servidor, estando

condicionado el acceso al servicio a una verificación de la identidad del usuario a partir del terminal del usuario en dicha etapa actual;

- la transmisión del testigo que ha de cifrarse y/o del testigo cifrado, entre el terminal y el equipo, se efectúa mediante una comunicación de corto alcance o cableada, incluyendo el terminal un módulo de comunicación de corto alcance o cableada e incluyendo el equipo un módulo homólogo de comunicación de corto alcance o cableada;

- la transmisión del testigo que ha de cifrarse del servidor al terminal se efectúa por una red móvil, y la transmisión del testigo cifrado del terminal al servidor se efectúa a través de un equipo que solicita un acceso a un servicio al que está asociado el servidor, estando condicionado el acceso al servicio a una verificación de la identidad del usuario a partir del terminal del usuario en dicha etapa actual;

- la transmisión del testigo que ha de cifrarse del servidor al terminal se efectúa a través de un equipo que solicita un acceso a un servicio al que está asociado el servidor, y la transmisión del testigo cifrado del terminal al servidor se efectúa por una red móvil, estando condicionado el acceso al servicio a una verificación de la identidad del usuario a partir del terminal del usuario en dicha etapa actual.

La invención concierne también a un sistema de verificación de identidad de un usuario, que incluye al menos un terminal y un servidor para la puesta en práctica del procedimiento según la invención.

Otras características y ventajas de la invención se irán poniendo de manifiesto con la lectura de la descripción detallada que sigue, que presenta posibles ejemplos de realización, y con la observación detenida de los dibujos que se acompañan, en los cuales:

la figura 1 ilustra las principales operaciones puestas en práctica por un sistema con arreglo a la invención, durante la etapa previa de declaración del terminal; y

la figura 2 ilustra las principales operaciones puestas en práctica por un sistema con arreglo a la presente invención, durante una etapa actual de verificación de identidad, basada en el terminal.

Con referencia a la figura 1, un usuario presenta un soporte físico tal como, por ejemplo, una tarjeta nacional de identidad CNI, una tarjeta de fidelidad, una tarjeta de estudiante u otra, para la lectura por un lector LEC. Para verificar que este soporte CNI lo porta realmente su poseedor (“MR X”), el usuario presenta un dato biométrico, por ejemplo una huella dactilar, en un lector BIO enlazado con el lector LEC de la tarjeta CNI. En un ejemplo de posible realización, el lector lee (por ejemplo por exploración) los datos de la tarjeta CNI y los comunica, con los datos biométricos, por ejemplo a un servidor remoto. Este servidor remoto verifica una coincidencia entre los datos de la tarjeta CNI y los datos biométricos recogidos (validación de la prueba S13) y, en su caso, el procedimiento puede proseguirse. En otro ejemplo de posible realización, los datos biométricos pueden servir para proteger ciertos datos embarcados en el soporte físico; los datos biométricos son transmitidos entonces al soporte el cual efectúa una verificación local (por ejemplo, a través del “Match On Card”) y autoriza la explotación de dichos datos protegidos.

Como consecuencia de esta primera operación, el lector puede comunicar, en la etapa S10, un primer dato de identidad Id1 del usuario hacia un servidor remoto SER. Esta identidad Id1 puede ser, por ejemplo, una identidad administrativa del individuo, o también una identidad bancaria (en el caso en que la tarjeta CNI es una tarjeta bancaria) u otras. El primer dato de identidad Id1 puede ser asimismo un certificado digital transmitido al servidor remoto SER que verifica la validez de este certificado (cadena de certificación, estado de revocación, fecha de validez, ...).

En una forma de realización, el servidor remoto SER determina, a partir del primer dato de identidad Id1, una identidad derivada Id2, en la etapa S11 (por ejemplo, mediante aplicación de una función de resumen al dato Id1), y comunica un segundo dato de esta identidad derivada Id2 al lector LEC en el ejemplo representado. En un modo de realización, el lector LEC puede incluir medios de comunicación de corto alcance (por ejemplo, un módulo NFC, por “Near Field Communication”, o también una comunicación Wifi, Bluetooth o cableada (por ejemplo, por cable USB)), para transmitir el segundo dato de identidad derivada Id2 a un terminal comunicante TER a elección del usuario, en la etapa S12, estando también este terminal TER, por supuesto, equipado con un módulo de comunicación de corto alcance. Como variante, la identidad derivada Id2 puede ser transmitida directamente del servidor SER al terminal TER por una red móvil.

En otra forma de realización, la identidad derivada Id2 puede ser un certificado digital. Un elemento seguro del terminal comunicante TER genera localmente una biclave (es decir, un par clave pública - clave privada), siendo la clave privada un secreto inextraíble del elemento seguro del terminal. La clave pública se comunica entonces al servidor remoto SER con una petición de certificación de la biclave. El servidor remoto SER genera un certificado vinculado al título auténtico, es decir, ligado al primer dato de identidad Id1 del usuario. Este certificado se reenvía a continuación al terminal comunicante TER junto a la biclave.

Más en particular, el terminal TER del usuario almacena la identidad derivada Id2 en una memoria segura (por

ejemplo, en la tarjeta SIM, por “Subscriber Identity Module” o, más generalmente, en un módulo UICC por “Universal Integrated Circuit Card”, o también en cualquier elemento de seguridad del terminal). A tal efecto, se puede transmitir hacia el terminal una aplicación desde el servidor y a través del lector LEC, como por ejemplo una “cardlet” que se instala en el terminal TER para almacenar la identidad derivada Id2, por ejemplo según un procedimiento de tipo OTA, por “Over The Air”.

De acuerdo con una forma de realización, el terminal TER puede generar una clave o una biclave a partir del dato de la identidad derivada Id2, que permite un cifrado simétrico (o, respectivamente, asimétrico, para una criptografía asimétrica) que con posterioridad interviene en la verificación de la identidad del usuario, a partir de su terminal TER, como seguidamente se verá con referencia a la figura 2.

De acuerdo con otra forma de realización, cuando la identidad derivada Id2 es un certificado digital según se ha descrito antes, la biclave asociada al certificado del título auténtico se utilizará para el cifrado que con posterioridad interviene en la verificación de la identidad del usuario a partir de su terminal TER, como se describe con referencia a la figura 2.

En un ejemplo de realización, ilustrado en la figura 2, cualquier equipo, por ejemplo un ordenador PC, una terminal de servicio automático, u otro, se comunica con una plataforma de servicio a través de una red de tipo Internet. Antes de prestar un servicio seguro, el servidor SER asociado a este servicio debe verificar la identidad del usuario. De este modo, se recurre, en este punto, a la citada etapa de verificación de la identidad del usuario, a partir de su terminal TER. A tal efecto, con referencia a la figura 2, el servidor SER envía, en la etapa S21, un testigo C (es decir, un “desafío” que puede corresponder, por ejemplo, a un número aleatorio o un “hash” de un documento), por ejemplo con destino al equipo PC. Mediante comunicación de campo cercano NFC (estando el equipo PC equipado con un módulo NFC), el testigo es comunicado al terminal TER, el cual explota los datos almacenados en memoria segura (por ejemplo, en su tarjeta SIM) y sus recursos criptográficos para firmar este testigo en la etapa S23. Ventajosamente, se puede llevar a la práctica, ante el terminal TER, una operativa sistemática consistente en una verificación de un dato propio del usuario, a partir del instante en que se trate de utilizar la o las clave(s) de cifrado almacenada(s) en el terminal para generar una firma. Por ejemplo se puede proponer al usuario, a través de una interfaz hombre-máquina, que introduzca un código personal en la etapa S22, o también que introduzca un dato biométrico predeterminado (huella dactilar, iris u otros). De este modo, en caso de tenencia fraudulenta del terminal TER por parte de un tercero malintencionado, no puede generarse ninguna firma en la etapa S23 y, por supuesto, no podrá prestarse con posterioridad ningún servicio al ordenador PC o a la terminal de servicio.

El testigo firmado C* es devuelto, en la etapa S24, al servidor SER, por ejemplo a través del ordenador PC mediante una comunicación de campo cercano, a través del módulo NFC especialmente. En la etapa S25, el servidor SER verifica esta firma con el concurso de su propia o sus propia(s) clave(s) y, por supuesto, con el concurso del testigo C que él mismo ha iniciado. La validez de la firma puede comprender una verificación estándar de validez de certificado (cadena de certificación, estado de revocación, fecha de validez, ...). Por otro lado, conociendo el testigo enviado en la etapa S21, la “respuesta” (es decir, el testigo firmado mediante la clave privada del terminal TER) devuelta en la etapa S24 así como la clave pública presente en el certificado, un servidor de validación es capaz de controlar la validez de la firma.

Se comprenderá entonces que esta firma se corresponde con un certificado digital que identifica al usuario con respecto al citado servicio.

La etapa de verificación de la identidad del usuario descrita con referencia a la figura 2 puede ser bicanal, es decir, por ejemplo, el testigo C que ha de firmarse (“desafío” o “hash” de un documento) puede ser enviado por la red móvil del servidor SER directamente al terminal comunicante TER, firmado por el terminal comunicante y, luego, el testigo firmado C* es devuelto al servidor a través de una interfaz NFC del equipo (ordenador PC o terminal de servicio automático). Se entiende que la comunicación bicanal también puede comprender una comunicación del testigo C que ha de firmarse del servidor SER al terminal comunicante TER a través de una interfaz NFC del equipo (ordenador PC o terminal de servicio automático) y una comunicación del testigo firmado C* devuelto directamente del terminal TER al servidor SER por la red móvil.

En una realización particular, la citada identidad derivada Id2 se calcula, por ejemplo, a partir de una función de resumen aplicada al primer dato de identidad Id1 procedente de la lectura de la tarjeta CNI. A continuación, se puede calcular al menos una clave (o un par de claves pública y privada), almacenada en la memoria segura del terminal TER, a partir de esta identidad derivada Id2 (por ejemplo, la clave privada, en el caso de un cifrado asimétrico). Por otro lado, una vez que se verifica la identidad del usuario gracias a su terminal, se puede establecer una sesión para un servicio seguro. Por ejemplo, se puede utilizar a continuación una clave diversificada para los intercambios entre el equipo PC y una plataforma de servicio enlazada con el servidor SER.

Por supuesto, la presente invención no se limita al modo de realización anteriormente descrito a título de ejemplo. Ésta se extiende a otras variantes.

Por ejemplo, anteriormente se ha descrito una interacción con un lector mediante comunicación de campo cercano. En una variante, se puede establecer directamente una comunicación entre el terminal TER y el servidor SER, por

ejemplo a través de una red celular, tanto para la etapa previa de declaración del terminal como para la posterior etapa de verificación de identidad.

Por otro lado, anteriormente se ha descrito, con referencia a la figura 2, la utilización de un equipo PC (o también de un lector LEC, tal como una terminal comunicante). En una variante más simple, puede utilizarse directamente el terminal TER para acceder al servicio (o para el registro inicial del terminal) y la verificación de la firma del desafío (o el registro) se efectúa directamente mediante una comunicación entre el servidor y el terminal, sin equipo intermedio. No obstante, la utilización de un aparato comunicante (una terminal de lectura LEC, un ordenador PC, una tableta o también una televisión) ofrece ventajosamente una interfaz que mejora la ergonomía de utilización.

Por otro lado, anteriormente se ha descrito una interacción con un servidor de aplicación SER. Como variante, se puede prever de manera equivalente una interacción con un equipo de tipo CMS (por “Card Management System”) o TSM (por “Trusted Service Management”).

De este modo, la invención propone utilizar un (o varios) elemento(s) de seguridad embarcado(s) en un objeto comunicante para embarcar una identidad derivada, cuya evolución (robo, pérdida, repudio, etc.) ya puede ser gestionada por el emisor inicial del soporte CNI y que permite una validación simple, rápida, segura y anónima de los derechos asociados.

A tal efecto, se prevé un cálculo, seguido de una transferencia de la identidad derivada a través de interfaces (en muchos casos, estandarizadas) de los objetos comunicantes, por ejemplo mediante intercambios locales (de campo cercano o NFC, por “Near Field Communication”) o, como variante, a través de Internet (mediante un enlace WiFi u otros) o también, posiblemente, a través de interfaces de usuario de redes sociales (Facebook, LinkedIn, e incluso iTunes®), o también mediante comunicación por una red celular (3G, LTE u otras). La identidad derivada puede no estar sólo almacenada en la memoria segura. Cabe prever una memorización en el objeto comunicante de una aplicación de gestión de los retransmisores de peticiones externas transmitidas según las mismas interfaces que para la implementación de la etapa previa de declaración del terminal. Ventajosamente, se puede prever una autenticación local de los datos del portador (por ejemplo, mediante introducción de datos de biometría), antes de la declaración del terminal móvil. La invención permite, a continuación, una personalización de las operaciones criptográficas en función de las solicitudes o de los servicios en línea de que se trate, con creaciones de firmas digitales específicas de cada servicio. La invención permite, además, evitar la compartición de información significante con las partes interesadas en la transacción durante el servicio.

Ventajosamente, la validación del pareamiento del terminal, del título auténtico y del portador puede basarse en 2 ó 3 factores (los datos del título auténtico –lo que tengo–, un código PIN –lo que sé–, un dato de biometría –lo que soy–). Tras validación de los datos de autenticación por 2 ó 3 factores del portador auténtico, puede efectuarse un registro inicial del terminal mediante utilización de un título auténtico CNI, tarjeta de fidelidad, tarjeta de estudiante u otro. De este modo, la introducción de la biometría/criptografía en la generación de una firma digital es una realización opcional, pero ventajosa. La invención permite, entonces, una compartición de datos no significantes con una verificación ante servidores remotos, sin compartición de identidad. Ésta permite, además, una generación y una comunicación de certificado y/o de firma digital, ofreciendo, por tanto, una opción de auditoría *a posteriori*, y ello en condiciones de personalización previa emisión de aplicaciones firmadas sin necesidad de entornos específicos.

Así, queda asegurada una personalización de aplicaciones de sensibilidad fuerte basada en la identificación del portador inicial, debido a la creación de un vínculo único entre el portador auténtico y un dato calculado basándose en una información del soporte inicial CNI el cual, por lo demás, puede ser un producto de seguridad (tarjeta o sistema de procesador de seguridad). A continuación, es también una ventaja la creación de condiciones de generación de algoritmo diversificado basándose en datos producidos por el portador (y no disponibles en los objetos).

REIVINDICACIONES

1. Procedimiento de verificación de identidad de un usuario de un terminal comunicante (TER), que incluye:

una etapa previa que comprende:

- una comunicación, a al menos un servidor (SER) dedicado a un servicio, de un primer dato de identidad (Id1) del usuario (S10),
- una generación de una biclave, par clave pública - clave privada, por el terminal,
- una generación ante el servidor de un segundo dato de identidad (Id2) del usuario (S11), definiendo el segundo dato una identidad derivada del usuario propia de dicho servicio, siendo dicho segundo dato de identidad un certificado digital que relaciona dicha clave pública con dicho primer dato de identidad, y
- un almacenamiento del segundo dato de identidad (Id2) en una memoria segura (SIM) del terminal (S12),

una etapa actual de verificación de identidad que comprende:

- una transmisión del servidor al terminal de un testigo (C) que ha de firmarse (S21) con el fin de autorizar o no un acceso al servicio al que está dedicado el servidor,
- una utilización ante el terminal de la clave privada al menos para firmar el testigo (S23), transmitiéndose el testigo firmado (C*) al servidor y verificándose ante el servidor (S25) y
- en caso de verificación positiva del testigo firmado ante el servidor, el servidor valida la verificación de identidad del usuario del terminal y autoriza el acceso al servicio;

en el que la transmisión del testigo (C) que ha de firmarse y/o del testigo firmado (C*), entre el servidor y el terminal, se efectúa a través de un equipo (PC) que solicita un acceso al servicio al que está dedicado el servidor (SER), estando condicionado el acceso al servicio a una verificación de la identidad del usuario a partir del terminal del usuario en dicha etapa actual.

2. Procedimiento según la reivindicación 1, en el que, en caso de verificación positiva, el testigo firmado se vincula a un certificado digital de identificación del usuario.

3. Procedimiento según una de las reivindicaciones anteriores, en el que dicha comunicación al servidor del primer dato de identidad (Id1) del usuario se autoriza previa verificación de un dato biométrico del usuario del terminal (S13).

4. Procedimiento según una de las reivindicaciones anteriores, en el que la etapa actual incluye una verificación de un dato propio del usuario (S22) antes de iniciar en el terminal la utilización del segundo dato para la firma del testigo.

5. Procedimiento según una de las reivindicaciones anteriores, en el que se prevé una pluralidad de etapas previas con una pluralidad de comunicaciones a una pluralidad de servidores del primer dato de identidad del usuario, generando cada servidor respectivos segundos datos de identidad del usuario, definiendo cada segundo dato una identidad derivada del usuario, siendo cada identidad derivada propia de un servicio cuyo acceso está condicionado a una verificación de testigo firmado ante un servidor dedicado a dicho servicio.

6. Procedimiento según una de las reivindicaciones anteriores, en el que la comunicación al servidor (SER) del primer dato de identidad (Id1) se efectúa a través de un lector (LEC) que incluye un módulo de comunicación de corto alcance (NFC) o cableada, e, incluyendo el terminal un módulo homólogo de comunicación de corto alcance o cableada, el segundo dato (Id2) se transmite del servidor al lector, y luego del lector al terminal mediante comunicación a corto alcance o cableada.

7. Procedimiento según la reivindicación 1, en el que la transmisión del testigo (C) que ha de firmarse y/o del testigo firmado (C*), entre el terminal (TER) y el equipo (PC), se efectúa mediante una comunicación de corto alcance (NFC) o cableada, incluyendo el terminal (TER) un módulo de comunicación de corto alcance (NFC) o cableada e incluyendo el equipo (PC) un módulo homólogo de comunicación de corto alcance o cableada.

8. Procedimiento según una de las reivindicaciones 1 a 6, en el que la transmisión del testigo (C) que ha de firmarse del servidor (SER) al terminal (TER) se efectúa por una red móvil, y la transmisión del testigo firmado (C*) del terminal al servidor se efectúa a través del equipo (PC) que solicita el acceso al servicio al que está asociado el servidor (SER).

9. Procedimiento según una de las reivindicaciones 1 a 6, en el que la transmisión del testigo (C) que ha de firmarse del servidor (SER) al terminal (TER) se efectúa a través del equipo (PC) que solicita un acceso al servicio al que está asociado el servidor (SER), y la transmisión del testigo firmado (C*) del terminal al servidor se efectúa por

una red móvil.

10. Sistema de verificación de identidad de un usuario, que incluye al menos un terminal (TER), un servidor (SER) y para la puesta en práctica del procedimiento según una de las reivindicaciones anteriores.

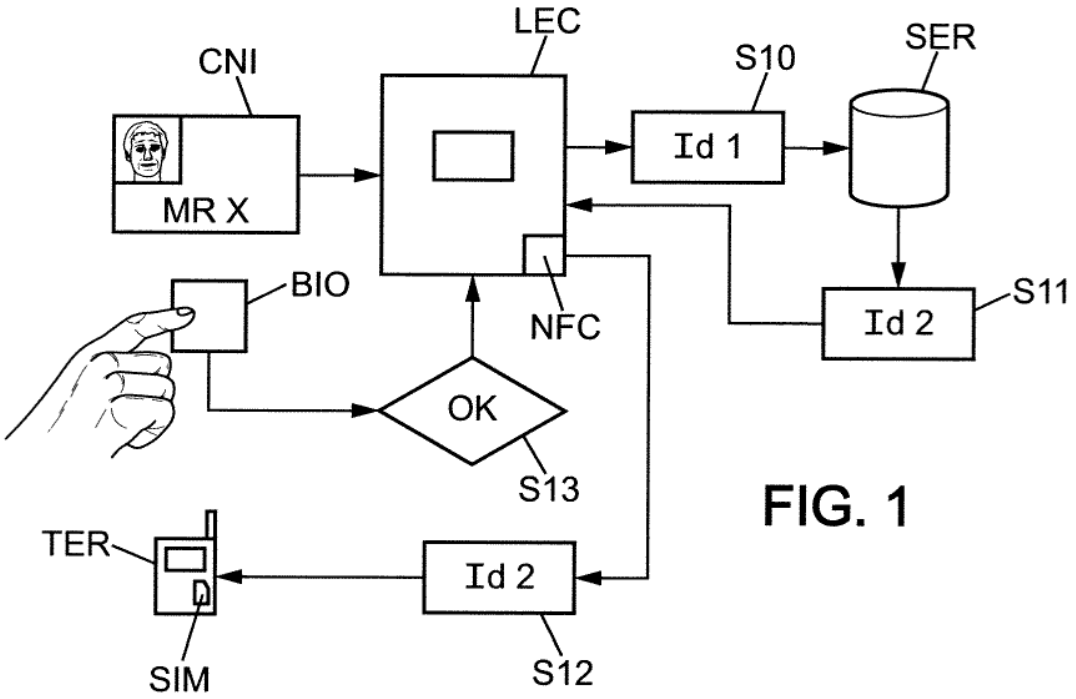
LEC
CNI
S10
SER
MR X
Id 1
BIO
NFC
Id 2
S11
OK
S13
TER
Id 2
SIM
S12

FIG. 1

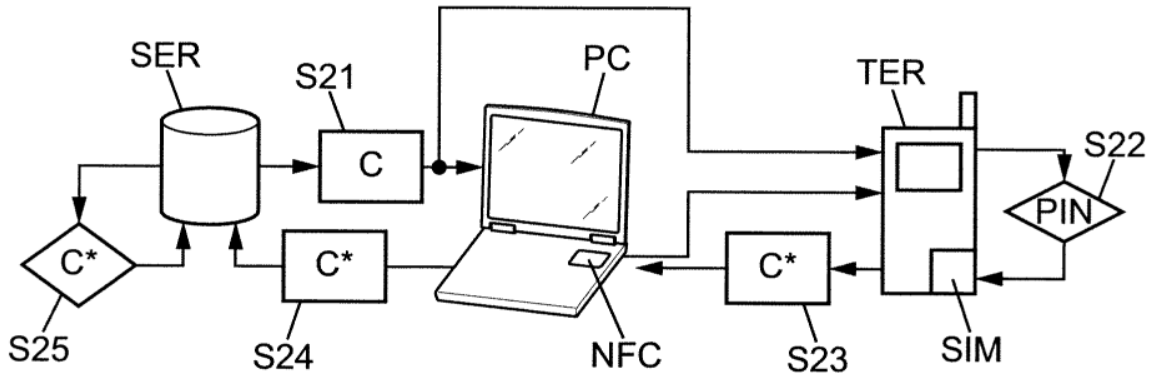
SER
S21
PC
TER
S22
C
PIN
C*
C*
C*
S25
S24
NFC
S23
SIM

FIG. 2