(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 526 318**

(51) Int. CI.:

***H04L 9/32*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.07.2011 E 11730326 (3)**

(97) Fecha y número de publicación de la concesión europea: **10.09.2014 EP 2596595**

(54) Título: **Procedimiento y sistema de protección de firma electrónica**

(30) Prioridad:

**20.07.2010 ES 201031116**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**09.01.2015**

(73) Titular/es:

**TELEFÓNICA, S.A. (100.0%)**
**Gran Vía, 28**
**28013 Madrid, ES**

(72) Inventor/es:

**AMAYA CALVO, ANTONIO MANUEL y**
**OCHOA FUENTES, MIGUEL**

(74) Agente/Representante:

**CARPINTERO LÓPEZ, Mario**

## DESCRIPCIÓN

Procedimiento y sistema de protección de firma electrónica

**Campo técnico**

La presente invención se relaciona con seguridad en documentos electrónicos. Más particularmente, la presente invención se refiere a proteger la firma electrónica de documentos.

**Descripción del estado de la técnica**

Los documentos electrónicos se usan en todo tipo de negocios hoy día, complementando o sustituyendo a los documentos en papel. Cuando esos documentos se usan para cualquier tipo de transacción legal, normalmente requieren una firma, de la misma forma que los documentos en papel deben firmarse.

La firma manuscrita implica la intención del firmante pero no se liga a ningún documento particular. Es perfectamente posible "levantar" una firma manuscrita de un documento en papel, copiarla en otro y, salvo que se demuestre la falsificación de la firma, el nuevo documento sería considerado firmado. Las firmas digitales, sin embargo, son únicas para cada firmante y documento, de forma que las firmas están ligadas a un documento particular. Si algo cambia en el documento, la firma no sería válida.

Las firmas digitales se componen usando algoritmos de encriptación. Podemos modelar un esquema digital simple como sigue:

1. Los firmantes tienen dos claves, una clave de verificación (o pública) (PbK) y una firma o clave privada (PvK). PbK se conoce públicamente, y es computacionalmente inviable conseguir PvK a partir de PbK. Solo el firmante conoce y tiene acceso a PvK.

2. Existe un par de funciones $\mathrm{S(k,x)}$ (función firma) y $\mathrm{V(k,x)}$ (función verificación,) con la siguiente propiedad:

   - $\mathrm{V(PbK, S(PvK, x)) = x}$

3. Existe una función hash o función para generar claves H(x) con las siguientes propiedades:

   - La salida de H(x), siendo x un flujo de bits de cualquier longitud, es una longitud fija de bytes.
   - Dado x es computacionalmente eficiente computar H(x)
   - Dado cualquier valor *h* que sea una salida válida de H(), es computacionalmente inviable computar cualquier valor *x* tal que *H(x)=h.*

Así que dado el esquema (Pvk, PbK, S(), V(), H()), el algoritmo para computar una firma digital de un documento D es como sigue:

1. Computar $h = H(D)$.
2. Computar $\mathrm{s = S(PvK, h)}$

Mientras que el algoritmo para verificar una firma digital para un documento D es como sigue:

1. Computar $\mathrm{h = H(d)}$
2. Verificar que $\mathrm{V(PbK, s) = h}$

Con el esquema definido, las firmas digitales se ligan a un documento y no solo implican el consentimiento del firmante a los contenidos, sino que también previenen cualquier manipulación del documento.

Nótese que para que este esquema funcione, debe haber alguna forma de distribuir, verificar y ligar PbK al firmante.

Esquemáticamente, el proceso de firma convencional se representa en la Figura 1. En la figura 1, Bob es el firmante del documento y Alice la receptora/verificadora del documento firmado.

Un esquema que detalla el proceso de firma, en el que la clave privada PvK se almacena en hardware seguro, como se implementa normalmente, se representa gráficamente en la Figura 2. La figura 3 representa el mismo proceso en un esquema cronológico, por claridad. La siguiente tabla resume el proceso ilustrado:

| | |
|---|---|
| **100** | Una aplicación de firma (SA) lee el documento a firmar (D) del almacenamiento (local o en red) |
| **110** | La aplicación presenta una representación gráfica de D a Bob, de forma que él pueda revisarlo antes de firmar. Esta parte del proceso se requiere por la mayoría de las legislaciones de firma digital. |

| | |
|---|---|
| **120** | Bob lee (y entiende) la representación de D. |
| **130** | Bob afirma su intención de firmar el documento. Es posible que en esta etapa un PIN (Número de Identificación Personal) sea requerido. Este PIN se usará para "desbloquear" PvK. |
| **140** | La aplicación de firma (SA) computa H(D). |
| **150** | SA envía H(D) al dispositivo de firma, con el PIN del usuario si se ha requerido. |
| **160** | El dispositivo de firma, usando la clave privada almacenada de forma segura, computa y devuelve S(PvK,H(D)) |
| Nótese que el esquema representado es válido para cualquier triada de funciones (S(),V(), H()). | |

El Estándar de Firma Digital (DSS) presenta un esquema de firma que, si bien especifica las funciones hash y de encriptación concretas, sigue el esquema general que se acaba de describir. Este esquema se describe en completo detalle en el Estándar de Firma Digital (DSS) (http://www.itl.nist.gov/fipspubs/fip186.htm).

PKCS#7 (RFC-2315 http://tools.ietf.org/html/rfc2315) define un Formato de Mensaje para datos firmados. PKCS es el acrónimo de Estándares de Criptografía de Clave Pública.

XML-DSig (http://www.w3.org/TR/xmldsig-core/) es una recomendación de W3C (World Wide Web Consortium) que define una sintaxis XML (Lenguaje de Marcas Extensible) para firmas digitales. Funcionalmente, tiene mucho en común con PKCS#7 pero es más extensible y orientado hacia firmar documentos XML.

La solicitud de patente europea "Method and system for implementing a digital signature" (EP1142194 A1) describe un Procedimiento para realizar la firma digital en una estación móvil, pero no dice nada sobre el problema de la no-repudiación.

La solicitud de patente 'Electronic document processing system and method of forming digital signature' (US 5465299 A) describe un Procedimiento para crear 'versiones' de un documento firmado digitalmente, en el que cada versión sucesiva se firma e incluye la firma de la versión anterior.

La patente 'Method and apparatus for an adapted digital signature' (US 6615348 B1) describe un algoritmo para generar identidades de usuario usando un algoritmo de firma digital modificado.

La patente 'Method and apparatus for validating a digital signature' (US 7178029 B2) describe una forma de verificar que una firma que incluye un certificado digital es válida incluso si el certificado digital ha sido revocado. Es básicamente un servicio de sello de tiempo.

La solicitud de patente europea "Signatur erfahren" (EP 1261165 A1) describe un procedimiento para generar una firma sobre un dispositivo móvil y transferirla a un ordenador personal.

La solicitud de patente "Server-side digital signature system" (US 2003/0093678) describe un servicio de generación de firma a distancia basado en un navegador".

La solicitud de patente europea "Methods and system for providing a public key fingerprint list in a PK system" (EP 1401143 A1) describe un servidor que almacena una lista de huellas dactilares clave públicas.

La solicitud de patente "Toolbar signature" (US 2009/0110199) describe una barra de herramientas de un navegador Web para generar firmas.

Sin embargo, las soluciones actuales presentan varios problemas: Según Ross Anderson, Profesor de Ingeniería de la Seguridad en la Universidad de Cambridge: '*Simplemente no sé cómo tener confianza en una firma digital que hago incluso en mi propio PC – y llevo trabajando en seguridad más de quince años. Chequear todo el software en el camino crítico entre el display y el software de firma va más allá de mi paciencia*." Y: '*Sin embargo, si fuera lo suficientemente tonto como para aceptar un dispositivo avanzado de firma electrónica, entonces habría una presunción de la validez de cualquier firma que pareciese haber sido hecha con él. […] Esto, unido a los hechos de que las tarjetas inteligentes no tienen una interfaz de usuario de confianza y de que los PCs que la mayoría de la gente usaría para proporcionar esta interfaz son fácilmente y frecuentemente subvertidos, quita a las firmas electrónicas instantáneamente todo atractivo*.'

Esto es así porque, según el esquema presentado en la Figura 2, algún otro software que corre en el ordenador del usuario podría interceptar y cambiar datos en los pasos 100, 120, 140, 150 y 160. Y en el paso 130 podría capturar el PIN del usuario y usarlo para silenciosamente firmar más documentos (haciendo automáticamente todo el proceso excepto los pasos 110, 120 y 130).

En otras palabras, los sistemas actuales y definiciones de sistema aplican severas restricciones en la forma en que se construye la “Aplicación de Firma” (ver Figura 2). Por ejemplo, las aplicaciones construidas para el DNIe (documento nacional de identidad electrónico) tienen que cumplir con los Criterios Comunes EAL3 (Metódicamente Testados y chequeados). Así que podría pensarse que cualquier aplicación que está certificada es segura.

Pero en el mismo documento de certificación se indica específicamente que para que el esquema de firma completa sea seguro el dispositivo del usuario (ordenador) tiene que ser seguro. Y con la tecnología actual es virtualmente imposible atestiguar que ningún ordenador tiene “malware” instalado y funcionando. No importa hacerlo después de que haya pasado algún tiempo. Cualquier afirmación sobre la seguridad del ordenador de un usuario cuando se hace una firma (posiblemente varios meses o incluso años antes) es simplemente una azarosa adivinanza.

Así, el problema es que, si bien las firmas digitales son matemáticamente sólidas y computacionalmente fáciles, son demasiado complejas de hacer o verificar a mano, así que los usuarios no tienen ninguna forma de confianza de chequear lo que están firmando. Esto significa que, efectivamente, los usuarios no tienen control real sobre lo que firman.

Los inventores no han encontrado ningún documento de patente existente que intente solucionar este problema.

**Sumario de la invención**

La presente invención resuelve los problemas mencionados arriba haciendo la computación crítica (hash (generación de claves) del documento a firmar) remotamente, sobre una ubicación de confianza.

Esta divulgación se refiere a un Procedimiento y sistema que, basados en el desarrollo de hardware y software específicos que residen en un servidor de confianza, aseguran la validez de firmas digitales realizadas en él. El Procedimiento y sistema evitan o hacen evidentes cualquier alteración en el proceso normal de firma digital.

En un primer aspecto, se presenta un Procedimiento para firmar electrónicamente un documento (D) de forma segura. El Procedimiento comprende: leer un documento a firmar por una aplicación; presentar una representación gráfica de dicho documento a un usuario; aceptar el documento a firmar por dicho usuario. El Procedimiento comprende además: en un servidor, computar una función hash, una función validación extendida del hash y una función resumen legible del documento a firmar; desde dicho servidor, enviar dicha función hash y dicha función validación extendida del hash a dicha aplicación y a un dispositivo de firma; desde dicho servidor, enviar dicha función hash y dicha función resumen legible del documento a firmar a un dispositivo secundario.

Preferentemente, el Procedimiento comprende además: verificar por el usuario que dicha función resumen legible del documento a firmar recibida en el dispositivo secundario corresponde a dicho documento; verificar por el usuario que dicha función hash recibida en el dispositivo secundario es la misma que la que el dispositivo de firma está presentando al usuario para su revisión; si la verificación de datos es correcta, aceptarlo por el usuario. Preferentemente, la etapa de aceptación se hace introduciendo el PIN del usuario en el dispositivo de firma.

Preferentemente, el Procedimiento comprende también: computar por dicho dispositivo de firma una función firma; enviar dicha función firma por dicho dispositivo de firma (53, 63) a dicha aplicación (54, 64). Esa función firma depende de una clave privada almacenada de forma segura, de dicha función hash y de dicha función validación extendida del hash.

En una realización particular, el dispositivo secundario es un terminal móvil.

En una realización particular, la etapa de aceptar el documento a firmar por dicho usuario se hace sin requerir el PIN del usuario.

Una vez que el usuario ha aceptado el documento a firmar, la aplicación envía preferentemente a dicho servidor información sobre dicho documento y sobre el dispositivo de firma y el dispositivo secundario. Preferentemente, dicha información sobre dicho documento y sobre el dispositivo de firma y el dispositivo secundario es la dirección del dispositivo de firma y la dirección del dispositivo secundario.

En otro aspecto, se presenta un sistema que comprende medios adaptados para llevar a cabo el Procedimiento descrito más arriba.

Finalmente, se presenta un programa informático que comprende medios de código de programa informático adaptados para realizar las etapas del Procedimiento descrito más arriba.

**Breve descripción de los dibujos**

Para completar la descripción y proporcionar un mejor entendimiento de la invención, se proporciona un juego de dibujos. Estos dibujos forman una parte integral de la descripción e ilustran una realización preferida de la invención, que no debe interpretarse como restrictiva del ámbito de la invención, sino como un ejemplo de cómo realizar la invención. Los dibujos comprenden las siguientes figuras:

La figura 1 representa esquemáticamente un proceso de firma convencional.
La figura 2 representa un esquema que detalla el proceso de firma convencional, en el que la clave privada PvK se almacena en hardware seguro, como suele implementarse.
La figura 3 representa el mismo proceso en un esquema de línea de tiempo, por claridad.
La figura 4 muestra un esquema general del Procedimiento y sistema según una realización de la invención.
La figura 5 muestra un esquema detallado del Procedimiento según una realización de la invención.
La figura 6 muestra una línea de tiempo del proceso de firma protegida según una realización de la invención.

Los números y símbolos correspondientes de las distintas figuras se refieren a las partes correspondientes del resto de figuras, salvo que se indique lo contrario.

**Descripción de realizaciones preferidas**

La figura 4 muestra un sistema según una realización de la invención. El sistema comprende: un dispositivo de firma 43, que en el contexto de esta divulgación también se llama dispositivo de firma de confianza (TSD); y un servidor 40, que en el contexto de esta divulgación también se llama servidor de confianza (TS). El sistema también requiere una aplicación de firma de cliente (CSA), que es, con respecto a la descrita en el estado de la técnica, una aplicación de firma de cliente modificada.

El dispositivo de firma (TSD) 43 tiene una interfaz de usuario de confianza (incorporada en el dispositivo 43). Esta interfaz incluye, al menos, una pantalla y un teclado numérico. Preferentemente, el dispositivo de firma 43 también tiene capacidades inalámbricas. Además, está configurado para procesar solo solicitudes de firma que incluyan una validación extendida correcta (una firma de confianza) para el hash a firmar. El dispositivo de firma (TSD) 43 tiene una interfaz de tarjeta inteligente que sigue el estándar ISO 7816. El almacenamiento de la clave puede hacerse en una tarjeta inteligente externa preexistente (por ejemplo, pero no limitativamente, un DNI electrónico español).

El servidor (TS) 40 está configurado para:

-recibir documentos D a firmar de los usuarios;

- computar una función hash (o función para generar claves) H(D) para los documentos a firmar;

- computar una función de validación extendida para el hash EV(H(D));

- computar una función resumen legible del documento D, RS(D), que es una representación en texto simple del contenido incluido en D que permitirá a un firmante potencial reconocer a D;

- enviar EV(H(D)) y H(D) al dispositivo de firma (TSD) 43; y

- enviar RS(D) a un dispositivo secundario (SD) 42 del usuario 41. Este dispositivo secundario 42 es preferentemente un terminal móvil 42.

La aplicación de firma de cliente (CSA), también llamada aplicación de firma de cliente modificada, se configura para presentar D al usuario y para enviar D al servidor 40 (también llamado servidor de confianza TS) para empezar el proceso de firma, con los datos de conexión del dispositivo de firma (TSD) 43 y el dispositivo secundario (SD) 42.

La figura 4 muestra un esquema simplificado del Procedimiento y proceso de firma de la invención.

En la figura 5 se muestra un esquema detallado del Procedimiento según una realización de la invención.

En la figura 5, se muestra un sistema que comprende los siguientes elementos: una aplicación de firma de cliente (CSA) 54, un usuario o firmante 51, una interfaz de usuario gráfica 55, un servidor o servidor de confianza (TS) 50, un dispositivo de firma de confianza (TSD) o simplemente dispositivo de firma 53 y un dispositivo secundario (SD) 52. El Procedimiento de firma segura de un documento D es como sigue:

En una primera etapa 500, una aplicación de firma o aplicación de firma de cliente (CSA) 54 lee el documento a firmar D de un almacenamiento, que puede ser tanto local como en red (remoto). Esta etapa 500 es similar al Procedimiento convencional.

Después, la aplicación de firma (CSA) 54 presenta 510 a través de un dispositivo de salida o interfaz de usuario gráfica 55 (por ejemplo, una pantalla o monitor) una representación gráfica de D al firmante (usuario 51), de forma que éste pueda revisarlo antes de firmarlo. Esta parte del proceso se requiere a menudo por la mayoría de las legislaciones de firma digital.

Después, el firmante 51 lee (y entiende) 520 la representación de D. Esta etapa tampoco es diferente de los Procedimientos convencionales.

A continuación, el firmante 51 afirma 531 su intención de firmar el documento. Esto se hace a través de un dispositivo de entrada 56 que puede ser, por ejemplo, un teclado. En esta etapa 531 no se le requiere que introduzca su PIN (Número de Identificación Personal. Esto es diferente de la mayoría de procesos de firma convencionales.

Las siguientes etapas son también diferentes de los procesos convencionales de firma:

Entonces 541, la aplicación de firma de cliente (CSA) 54 envía D y las direcciones del dispositivo secundario (SD) 52 y del dispositivo de firma (TSD) 53 al servidor (TS) 50.

A continuación 542, el servidor (TS) 50 computa H(D), EV(H(D)) and RS(D) (el resumen legible de D).

Después 543, el servidor (TS) 50 envía H(D) y EV(H(D)) a la aplicación de firma de cliente (CSA) 54.

Entonces 551, el servidor (TS) 50 envía H(D) y EV(H(D)) al dispositivo de firma (TSD) 53. El dispositivo de firma (TSD) 53 verifica EV(H(D)) y, si es correcto, presenta esta información - H(D) y EV(H(D)) – en su interfaz incluida (tal y como una pantalla).

A continuación 552, el servidor (TS) 50 envía H(D) RS(D) al dispositivo secundario (SD) 52. En una realización preferida, este dispositivo secundario (SD) 52 es un teléfono móvil, en cuyo caso los datos son enviados por SMS o MMS.

Después 553, el firmante 51 verifica que RS(D) recibido en el dispositivo secundario (SD) 52 corresponde al documento (D) que quiere firmar.

Entonces 554, el firmante 51 verifica que H(D) recibido en el dispositivo secundario (SD) 52 es el mismo que el dispositivo de firma (TSD) 53 está presentando para su revisión en su pantalla incluida.

Seguidamente 555, si la verificación de los datos es correcta, el firmante 51 introduce su PIN en el teclado del dispositivo de firma (TSD) 53.

A continuación 561, el dispositivo de firma 53, usando la clave privada almacenada de forma segura y el PIN proporcionado por el usuario, computa una función firma S a partir de PvK y de EV(H(D)), $S(PvK, EV(H(D)))$.

Finalmente 571, el dispositivo de firma envía $S(PvK, EV(H(D)))$ a la aplicación de firma de cliente (CSA) 54. La función de validación extendida (EV) se incluye en la firma para atestiguar que la firma se realizó usando el sistema descrito en este documento, y para evitar la posibilidad de repudiación de la firma.

La línea de tiempo correspondiente al proceso de firma inventiva se describe en la figura 6, en la que se han usado referencias correspondientes (610 en vez de 510 etc.).

Tal y como se ha descrito, una de las principales ventajas de esta invención es que evita el sabotaje con datos de firma, o hace este sabotaje evidente al firmante, evitando así posibles problemas de repudiamiento.

Con las soluciones actuales, el firmante de un documento firmado digitalmente puede impugnar (repudiar) cualquier firma hecha con su clave privada sobre la base de que le es imposible (incluso según expertos en el campo, como el mencionado Ross Anderson) saber exactamente lo que está firmando. El firmante podría repudiar la firma diciendo que:

- El documento que se le mostró no es el documento que tiene la firma. Podría hacerse por una aplicación en su propio PC.
- Alguna aplicación podría haberle robado su PIN y usarlo para firmar cualquier número de documentos sin haberle informado.

Ya que las firmas digitales se están usando en más aplicaciones cada día (y en la Unión Europea serán obligatorias pronto para relaciones con el gobierno), es obligatorio encontrar una solución a este problema. La invención presentada en este documento es esa solución.

**REIVINDICACIONES**

1. Un procedimiento de protección de la firma electrónica de un documento (D), que comprende:

- leer (500, 600) un documento a firmar (D) por una aplicación (54, 64);
- presentar (510, 610) una representación gráfica de dicho documento (D) a un usuario (51, 61);
- aceptar (531, 631) el documento a firmar (D) por dicho usuario (51, 61);

estando el procedimiento **caracterizado por**:

- en un servidor (50, 60), computar (542, 642) una función hash (H(D)), una función validación extendida del hash (EV(H(D))) y una función resumen legible del documento a firmar (RS(D));
- desde dicho servidor (50, 60), enviar (543, 643; 551, 651;) dicha función hash (H(D)) y dicha función validación extendida del hash (EV(H(D))) a dicha aplicación (54, 64) y a un dispositivo de firma (53, 63);
- desde dicho servidor (50, 60), enviar (552, 652) dicha función hash (H(D)) y dicha función resumen legible del documento a firmar (RS(D)) a un dispositivo secundario (52, 62).

2. El procedimiento de la reivindicación 1, que comprende además:

- verificar (553, 653) por el usuario (51, 61) que dicha función resumen legible del documento a firmar (RS(D)) recibida en el dispositivo secundario (52, 62) corresponde a dicho documento (D);
- verificar (554, 654) por el usuario (51, 61) que dicha función hash (H(D)) recibida en el dispositivo secundario (52, 62) es la misma que la que el dispositivo de firma (53, 63) está presentando al usuario (51, 61) para su revisión;
- si la verificación de datos es correcta, aceptarlo (555, 655) por el usuario (51, 61).

3. El procedimiento de la reivindicación 2, en el que dicha aceptación (555, 655) se hace introduciendo el PIN del usuario en el dispositivo de firma (53, 63).

4. El procedimiento de cualquiera de las reivindicaciones 2 ó 3, que comprende además:

- computar (561, 661) por dicho dispositivo de firma (53, 63) una función firma;
- enviar (571, 671) dicha función firma por dicho dispositivo de firma (53, 63) a dicha aplicación (54, 64).

5. El procedimiento de la reivindicación 4, en el que dicha función firma depende de una clave privada almacenada de forma segura, de dicha función hash (H(D)) y de dicha función validación extendida del hash (EV(H(D))).

6. El procedimiento de cualquiera de las reivindicaciones anteriores, en el que dicho dispositivo secundario (52, 62) es un terminal móvil.

7. El procedimiento de cualquiera de las reivindicaciones anteriores, en el que dicha etapa de aceptar (531, 631) el documento a firmar (D) por dicho usuario (51, 61) se hace sin requerir el PIN del usuario.

8. El procedimiento de cualquiera de las reivindicaciones 2-7, en el que, una vez que el usuario (51, 61) ha aceptado (531, 631) el documento a firmar (D), dicha aplicación envía (541, 641) a dicho servidor (50, 60) información sobre dicho documento (D) y sobre el dispositivo de firma (53, 63) y el dispositivo secundario (52, 62).

9. El procedimiento de la reivindicación 8, en el que dicha información sobre el dispositivo de firma (53, 63) y el dispositivo secundario (52, 62) es la dirección del dispositivo de firma (53, 63) y la dirección del dispositivo secundario (52, 62).

10. Un sistema que comprende medios adaptados para llevar a cabo el procedimiento según cualquiera de las reivindicaciones anteriores.

11. Un programa informático que comprende medios de código de programa informático adaptados para realizar el procedimiento según cualquiera de las reivindicaciones de la 1 a la 9, cuando dicho programa se ejecuta en un ordenador, un procesador de señal digital, una disposición de puertas de campo programable, un circuito integrado de aplicación específica, un microprocesador, un microcontrolador, y cualquier otra forma de hardware programable.

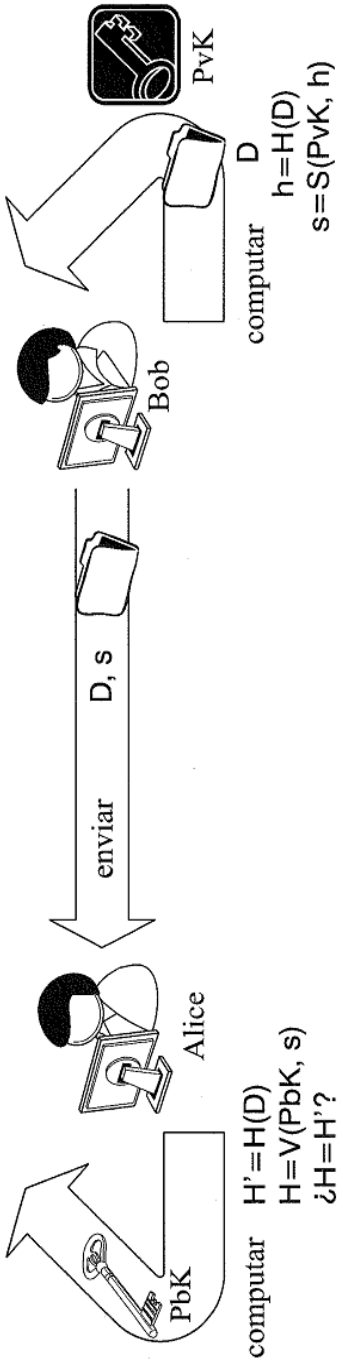


FIG. 1
**ESTADO DE LA TÉCNICA**

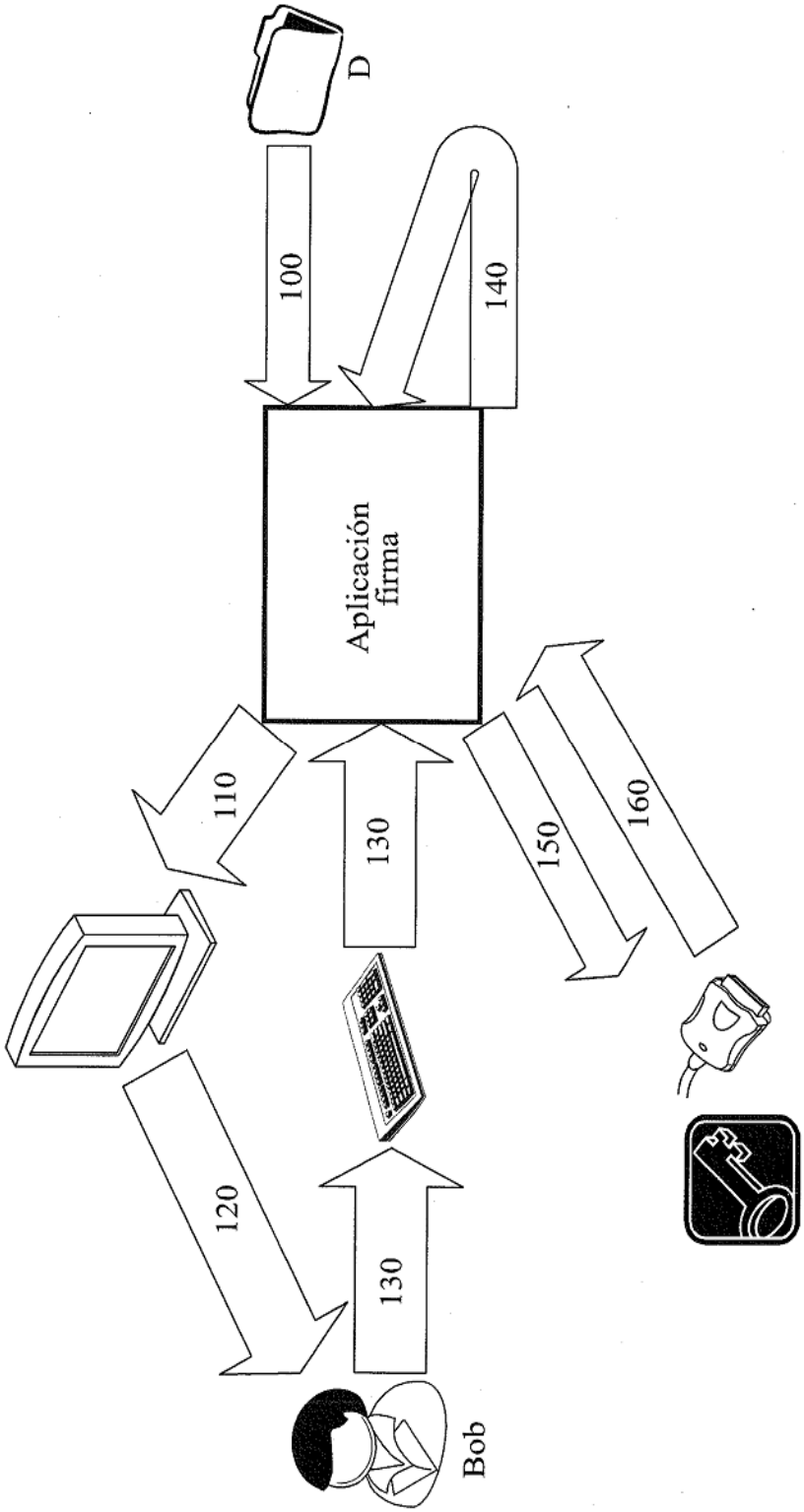


FIG. 2
ESTADO DE LA TÉCNICA

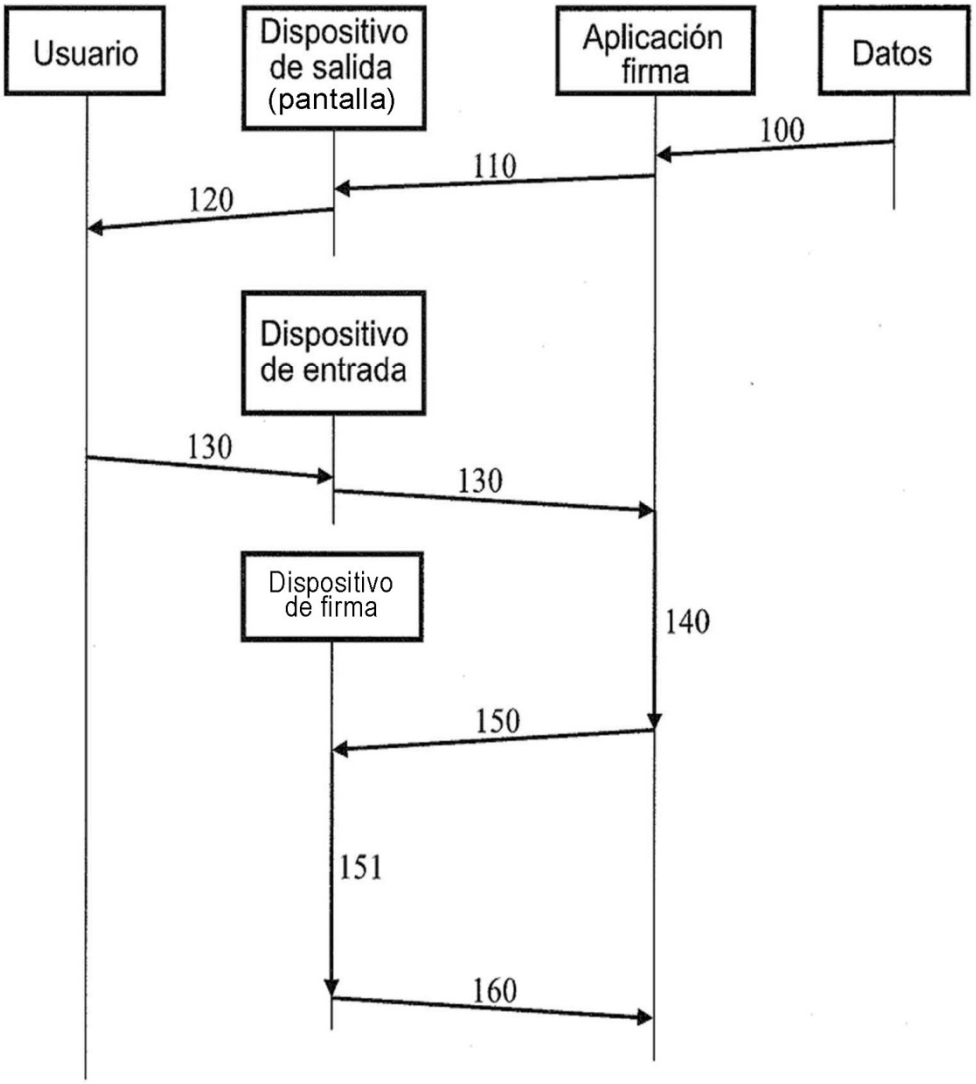


FIG. 3
**ESTADO DE LA TÉCNICA**

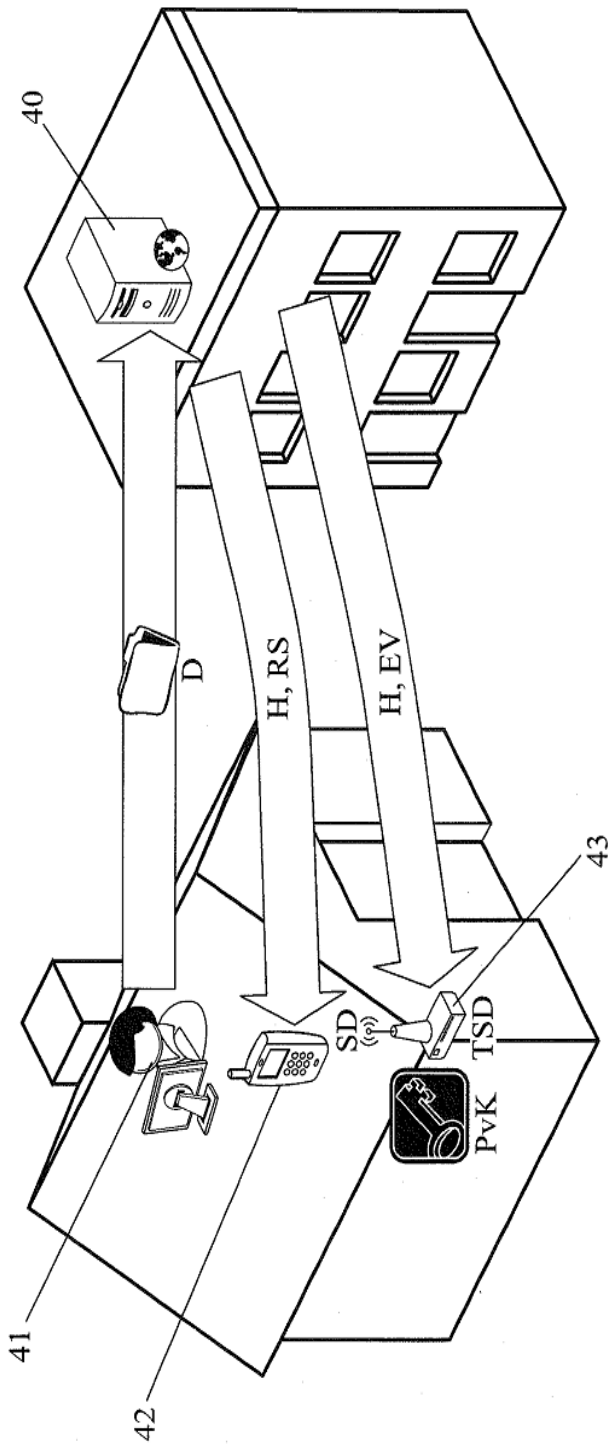


FIG. 4

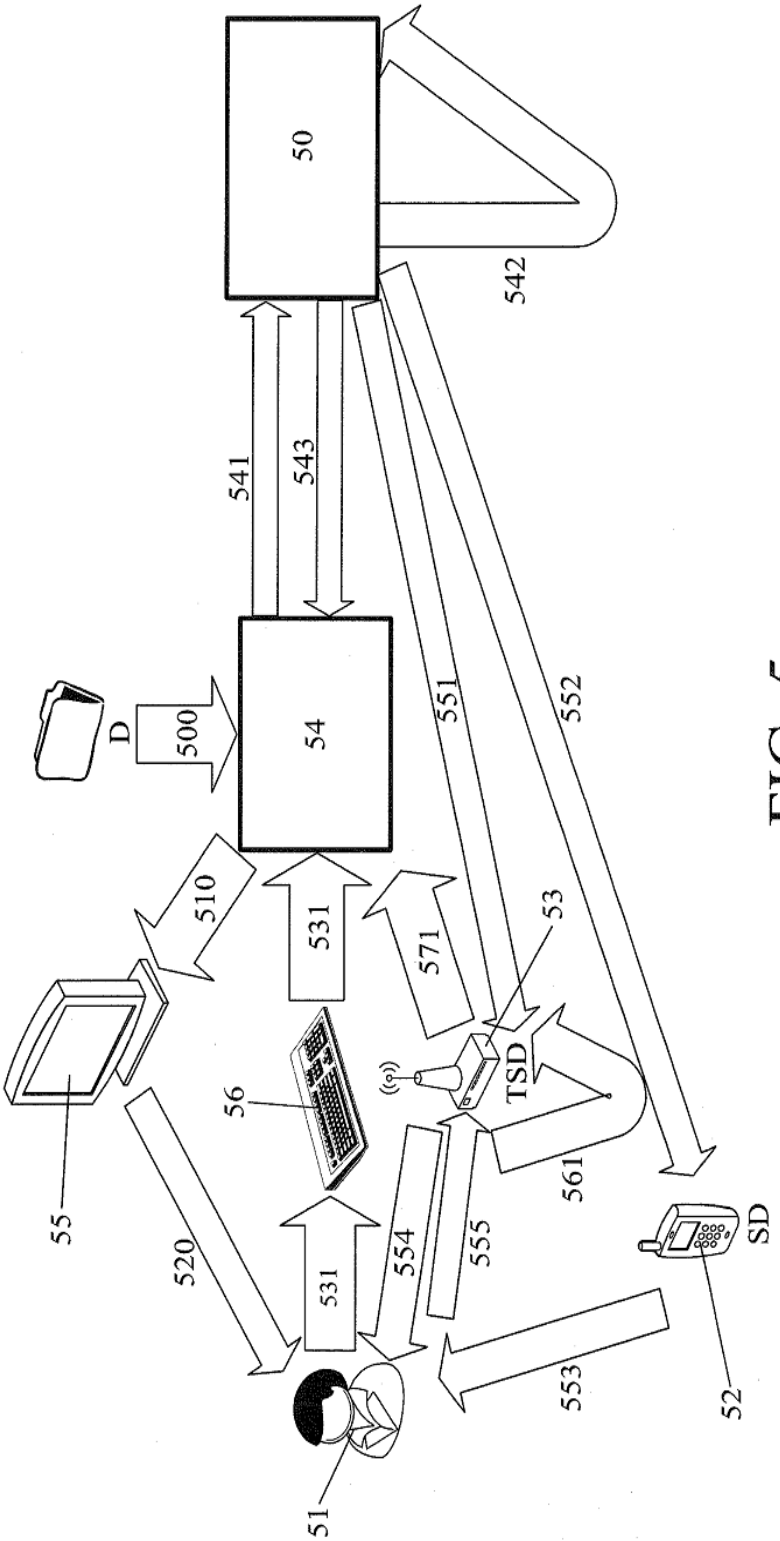
50
542
541
543
551
552
D
500
54
510
531
571
53
TSD
56
55
520
531
554
555
561
SD
553
52
51

FIG. 5

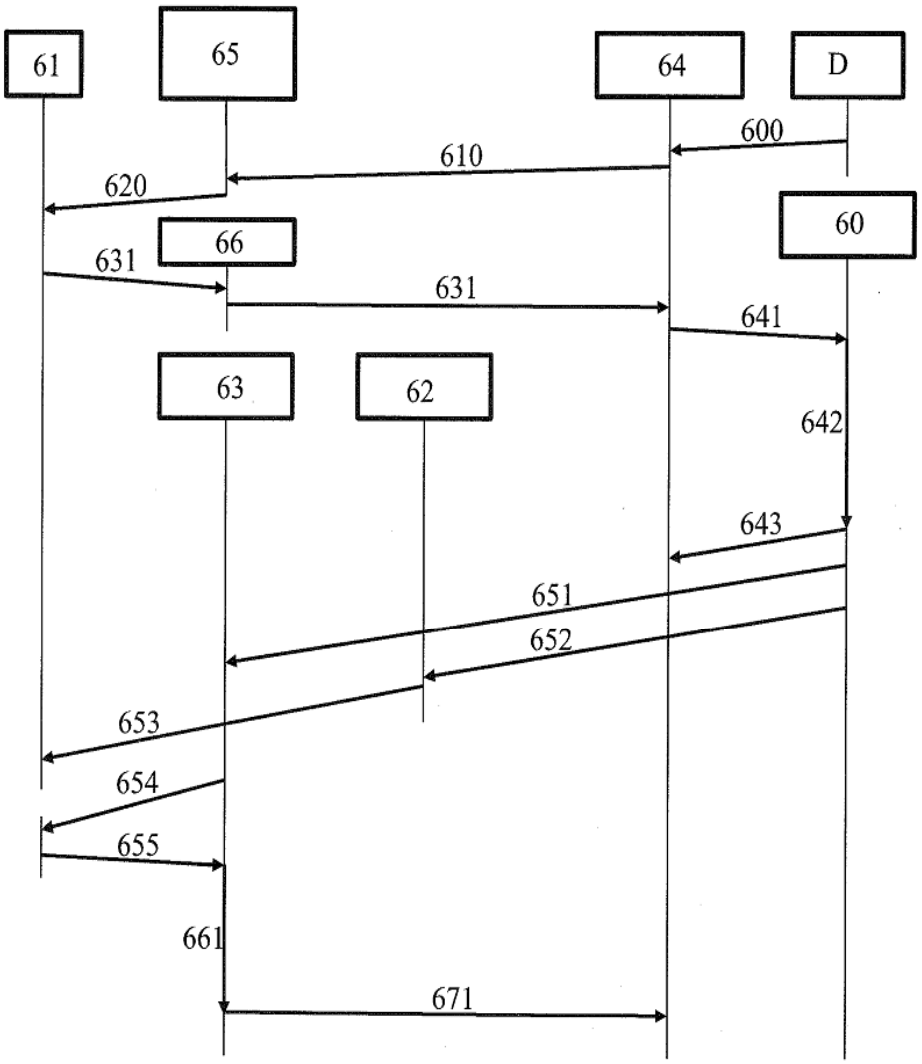
61
65
64
D
600
610
620
60
66
631
631
641
63
62
642
643
651
652
653
654
655
661
671

FIG. 6