(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 587 584**

(21) Número de solicitud: 201500764

(51) Int. CI.:

G06F 21/00 (2013.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

22.10.2015

(43) Fecha de publicación de la solicitud:

25.10.2016

(71) Solicitantes:

UNIVERSIDAD DE MÁLAGA (100.0%)
Av. Cervantes, 2
29071 Málaga ES

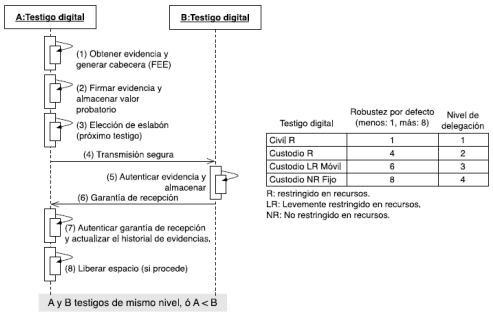
(72) Inventor/es:

NIETO JIMÉNEZ , Ana ;
ROMÁN CASTRO , Rodrigo y
LÓPEZ MUÑOZ , Francisco Javier

(54) Título: **Testigo digital: Procedimiento y dispositivos para la gestión segura de evidencias electrónicas con credenciales vinculantes**

(57) Resumen:

Testigo digital: Procedimientos y dispositivos para la gestión segura de evidencias electrónicas con credenciales vinculantes. La invención se refiere a un dispositivo para la gestión segura de evidencias electrónicas con credenciales vinculantes (testigo digital) sobre el que el usuario u objeto que obtiene, genera o recibe evidencias delega su identidad de forma vinculante e indisoluble mediante credencias vinculantes caracterizado por que comprende un gestor de operaciones entre el usuario u objeto y el dispositivo, mecanismos criptográficos aceptados dentro de un elemento seguro, medios de almacenamiento seguro con control de acceso, protegidos en un elemento seguro (núcleo de confianza), un gestor de evidencias electrónicas para objetos, y, opcionalmente, un gestor contractual. La invención también refiere procedimientos que hacen uso de dichos testigos digitales y que comprenden la obtención, firma, almacenamiento, delegación y, en su caso, borrado de evidencias electrónicas.



Testigo digital	Robustez por defecto (menos: 1, más: 8)	Nivel de delegación
Civil R	1	1
Custodio R	4	2
Custodio LR Móvil	6	3
Custodio NR Fijo	8	4

R: restringido en recursos.
LR: Levemente restringido en recursos.
NR: No restringido en recursos.

Figura 1

ES 2 587 584 A1

DESCRIPCIÓN

Testigo digital: Procedimientos y dispositivos para la gestión segura de evidencias electrónicas con credenciales vinculantes

SECTOR TÉCNICO

La presente invención se refiere a procedimientos y dispositivos para la gestión segura de evidencias electrónicas, particularmente para la gestión segura de evidencias electrónicas con credenciales vinculantes, más particularmente referidos al ámbito de la computación forense.

ESTADO DE LA TÉCNICA

Los dispositivos móviles de usuario están fuertemente arraigados en el corazón de la sociedad. En efecto, las redes sociales y la educación en las nuevas tecnologías han impulsado enormemente la aceptación de los dispositivos personales como parte de nuestra vida diaria. Son, desde el punto de vista funcional, una extensión de nuestras capacidades humanas, ya que en ellos almacenamos imágenes, proyectos y datos que, si bien pudieran tener su versión física (ej. el símil entre una carta manuscrita y un e-mail), en su versión virtual están siempre disponibles, con nosotros, y pasan a considerarse datos privados cuyo acceso incluso se regula por medio de leyes, como por ejemplo la ley orgánica de protección de datos (LOPD) para el acceso a datos de carácter personal.

Inevitablemente, los analistas forenses se han adaptado para aprovechar este apego a las nuevas tecnologías. En el caso que nos ocupa, los dispositivos móviles son una fuente muy valiosa de información sobre un individuo, y cuando son procesados como contenedores de evidencias, puede extraerse información de naturaleza probatoria - evidencias electrónicas - que arroje luz sobre un caso abierto.

En el paradigma actual, la manipulación de las evidencias electrónicas es un proceso muy delicado. Debido al carácter volátil de este tipo de pruebas, existen procedimientos mucho más exhaustivos para evitar que las evidencias electrónicas puedan ser repudiadas como pruebas. De hecho, por norma general, la adquisición de evidencias en los casos más delicados se lleva a cabo por parte de personal autorizado de la justicia, y, en la definición de *Sistemas de Gestión de Evidencias Electrónicas* (SGEE), dada en la multi-norma UNE 71505:2013, se hace hincapié en el propietario de la evidencia digital y en las personas como responsables [1].

Aunque la gestión de evidencias electrónicas se encuentra bastante regulada, consideramos que podría mejorarse considerablemente si se aprovechan aún más los últimos avances tecnológicos que confieren de arquitecturas de seguridad a los dispositivos móviles de usuario y, por tanto, los prepara mucho mejor que las arquitecturas tradicionales para atestiguar algunos hechos.

Por ejemplo, los dispositivos móviles están equipados con sensores que permiten realizar mediciones de su entorno, y su densidad permite que estos datos sean contrastados por otros dispositivos. Estas mediciones pueden ser tan heterogéneas como los sensores en los dispositivos móviles, y llegar tan lejos como lo permita el protocolo de comunicaciones, la densidad de la red, y las aplicaciones colaborativas que gestionen dichos datos. Pese a que los casos de engaño son frecuentes y de hecho numerosos trabajos abordan esta problemática [2], también es cierto que los nuevos avances en las arquitecturas de seguridad permiten dotar de un núcleo de confianza a ciertos dispositivos, que serían capaces de confesar conductas inadecuadas incluso de su usuario.

Este hecho, que podría considerarse contrario a los principios de privacidad, puede ser usado para incrementar la privacidad de un usuario sobre manera. De hecho, el uso de estos dispositivos de núcleo de confianza, apoyados por almacenamiento en forma de chip hardware blindado contra modificaciones (*anti-tampering*), está siendo usado para blindar los datos personales de los usuarios en los terminales móviles.

Desde el punto de vista de la computación forense, estos mecanismos dificultan mucho la extracción de evidencias digitales, pero abren un nuevo marco de trabajo y posibilidades muy interesantes. Y es que estos dispositivos confiables pueden ser muy robustos y fiables para atestiguar o custodiar evidencias electrónicas. Por ejemplo, la ventana de tiempo desde que un evento sucede en la red y este hecho se pierde puede ser lo suficientemente pequeña para que la evidencia electrónica del evento se pierda antes de que pueda ser capturada y custodiada por una persona autorizada, que ha de desplazarse o acceder al entorno afectado y tomar la evidencia. Primero, desde un punto de vista de preservación de la escena, cualquier nuevo acceso mientras que un evento sucede puede alterar los datos y las pruebas, y, segundo, parece más razonable que se puedan definir casos en los que las evidencias puedan ser custodiadas por dispositivos confiables, que ya se encuentren en la escena, hasta que puedan ser delegadas a un custodio oficial.

El ciclo de vida de la evidencia electrónica (CVEE) consta típicamente de seis pasos, definidos en [1]: generación, almacenamiento, transmisión, recuperación, tratamiento y comunicación, los cuales hemos dividido en dos grupos basándonos en su relación inmediata.

En primer lugar, la *generación* de la evidencia electrónica puede recaer en el uso de métodos y técnicas forenses. Sin embargo, el concepto de evidencia es muy amplio, un *log* de una aplicación o una imagen pudieran ser evidencias electrónicas. Cómo se genera la evidencia puede acreditar o restar credibilidad al valor de la evidencia. Pero, en cualquier caso, la generación de la evidencia conlleva el *almacenamiento* de la misma. Éste también es un paso crítico, ya que, si existe la posibilidad de que la evidencia electrónica haya podido ser manipulada por agentes no autorizados, o bien modificada de alguna forma, podría perder su valor como evidencia en un litigio. También la fase de *transmisión* de la evidencia electrónica está sujeta a interpretaciones de este tipo. Cómo se transmite la evidencia electrónica puede dar pie a dudar de su confiabilidad. En este punto, se consideran aspectos como el formato empleado, su trazabilidad a terceras partes, la seguridad en la transmisión, etc. Asegurar la integridad y la confiabilidad de la prueba, y las políticas para su transmisión a entidades autorizadas, es fundamental en este punto.

El segundo grupo de pasos, podría realizarse pasado un tiempo desde que la evidencia fue almacenada o transmitida a una entidad autorizada. Así, la evidencia electrónica ha de estar siempre disponible para el personal autorizado que lo solicite, garantizándose su *recuperación*. Para esto el requisito de disponibilidad es fundamental. Tras este paso, se establecen los métodos para el *tratamiento* de la evidencia electrónica, los procesos por los cuales se extraen los hechos. Este paso puede conllevar la correlación entre diferentes evidencias electrónicas. La evidencia debe mantener su integridad. Normalmente el proceso habitual es tratar copias digitales de la evidencia electrónica. Los resultados de este proceso deben elaborarse desde la imparcialidad.

Por último, el paso de *comunicación* está destinado que los hechos imparciales que reflejan la evidencia electrónica se empleen en su comunicación en un litigio, para resolver disputas entre los elementos involucrados, o bien de forma interna para mejorar las políticas organizativas y de seguridad de las organizaciones.

Durante todo el CVEE deben garantizarse las propiedades de confiabilidad de los datos e integridad de la evidencia electrónica, además de evitar que entidades no autorizadas accedan a los datos. Si la evidencia electrónica en algún momento del ciclo es susceptible de ser

modificada sin que pueda demostrarse su integridad, entonces la cadena de custodia se vería comprometida y la evidencia carecería de sentido como prueba en un juicio, por resultar fácilmente refutable.

El concepto de testigo digital definido en la presente invención surge de la necesidad de cubrir desafíos abiertos en la *Gestión de Evidencias Electrónicas* (GEE) para dar cabida a escenarios de la *IoT*. Algunos de estos desafíos se desprenden del trabajo [3], donde se defiende el concepto de *IoT-Forensics* como algo nuevo, que contempla desde los objetos más restringidos en recursos hasta el *Cloud*. A raíz de este trabajo, ya se percibe que la GEE en estos entornos ha de considerar requisitos adicionales a la GEE tradicional. Esto es así porque la *IoT* es un entorno dinámico, heterogéneo y distribuido, y los requisitos de identificación, preservación, análisis y presentación propios de la GEE requieren un control de grano fino sobre los datos informáticos, difícil de proporcionar en la *IoT*. Por ejemplo, el trabajo [4] identifica algunos de los desafíos abiertos para la GEE en la *IoT* tomando en consideración dichos requisitos. Entre estos desafíos, se encuentran: identificar de dónde procede la información y quién genera los datos, el almacenamiento local de los datos en *las cosas*, la transferencia de las evidencias entre los objetos y cómo la cadena de la evidencia se preserva. También se señala el posible inconveniente de la figura de proveedores de *IoT*, que almacenarían datos de los dispositivos, complicando el proceso de preservación. Otro desafío abierto es el análisis forense de los artefactos (evidencias) identificables en los objetos. La extracción de evidencias de los objetos no sólo no se encuentra definida en su totalidad (por ejemplo, en el caso de los sensores), sino que se enfrenta con formatos de presentación de la información de los objetos que puede diferir considerablemente según el estándar empleado.

Diversos trabajos aúnan esfuerzos en definir modelos para la adquisición de evidencias electrónicas en los dispositivos móviles [5], o bien para estandarizar la presentación y los formatos para el intercambio de evidencias electrónicas [6]. La preservación de las evidencias electrónicas mediante el concepto de *Cadena de Custodia Digital* (CCD) es empleado en otros trabajos como en [7], [8]. El objetivo de una CCD es agilizar el concepto de cadena de custodia permitiendo el envío de las evidencias electrónicas a través de equipos informáticos empleando medidas de seguridad, por ejemplo recogidas en normas como UNE 71505 [1]. Sin embargo, el concepto de CCD es aún muy reciente, y no considera las particularidades de la *IoT*; actualmente los objetos no podrían ser participantes sin comprometer la CCD. En [7] se propone una CCD para enviar evidencias digitales multimedia con estampillado de tiempo a una entidad

a través de Internet, mientras que en [8] se propone una CCD que considera *tag cabinets* para marcar las evidencias y facilitar su recuperación en el paso previo al análisis. En este último caso, la CCD se encuentra representada en el acceso a los datos. En [9] se proporciona un estado del arte sobre los últimos trabajos en materia de CCD. En dicho trabajo queda reflejado que la CCD sigue una orientación hacia las arquitecturas tradicionales de comunicación, donde la gestión de evidencias electrónicas es realizada por equipos no restringidos en recursos, y los dispositivos móviles, pese a integrar arquitecturas de seguridad, quedan dentro de esta cadena como meros contenedores de evidencias, y, en caso de participar (p.ej. para enviar la evidencia a través de Internet), el proceso requiere de la intervención directa del usuario en todo momento.

Sin embargo, los requisitos para hacer uso de una CCD en la *IoT* considerando las características de seguridad de los objetos para custodiar las evidencias no han sido discutidos aún, menos aún la colaboración entre objetos custodios. Sin embargo, consideramos que este es un paso básico para agilizar la intervención de personas en la gestión de evidencias digitales.

Además de estos trabajos, el concepto de identidad de las cosas, o *Identities of Things* (IDoT) está siendo ampliamente discutido [10] ante la proliferación de dispositivos, para definir la relación entre los dispositivos y sus usuarios. De hecho, como se detalla en [10], la identidad de los objetos agiliza las labores de autenticación, autorización, y presenta retos en la gestión de dichas identidades y la privacidad de los individuos.

Otro desafío en la GEE para la *IoT* se encuentra en el almacenamiento de evidencias electrónicas de forma masiva. Iniciativas como el proyecto EVIDENCE (*European Informatics Data Exchange Framework for Courts and Evidence*) centran sus esfuerzos, precisamente, en la búsqueda de un marco unificado para recopilar y compartir las evidencias electrónicas. Adaptar este tipo de enfoques para colaborar con SGEE definidos para la *IoT* podría significar un gran paso para enfoques distribuidos como el que proponemos en este trabajo.

La informática forense en los dispositivos personales surge como evolución natural de la computación forense tradicional, por lo que hereda parte de las comprobaciones y análisis sobre unidades de almacenamiento [11], [12], [3]. Los análisis forenses pueden ser (i) sobre el dispositivo (que actuaría como contenedor de evidencias), (ii) sobre la red (donde podrían entrar en juego analizadores de tráfico, y a su, vez pueden ser efectuados en (a) vivo) cuando el procedimiento forense no interrumpe el funcionamiento del dispositivo del que se extraen las evidencias, o (b) muertos (cuando las evidencias se obtienen de un dispositivo sin más función que la propia de ser analizado, por ejemplo cuando se adquieren los datos de una partición de

un disco duro requisado [13], [14]). Los análisis de este último tipo ocurren una vez que el delito ha ocurrido, *offline*, mientras que los análisis tipo (a) suelen tener como objetivo procesar las evidencias lo antes posible e incluso tal vez combinarlas con sistemas de detectores de intrusos, almacenando los eventos de estos sistemas como posibles evidencias.

Los dispositivos de seguridad hardware diseñados para salvaguardar información de carácter crítico como contraseñas, claves, etc., han evolucionado considerablemente rápido desde la aparición de los primeros *tokens* criptográficos. Éstos estaban ligados al usuario, mientras que otros diseños posteriores permitían proporcionar un núcleo de confianza (*core-of-trust*, CoT) a la plataforma donde se embebían, como es el caso del chip denominado *Trusted Platform Module* (TPM) desarrollado por el *Trusted Computing Group* (TCG). Los chips TPM integran una clave maestra de fábrica que nunca abandona el chip, ya que éste cuenta con su propio procesador criptográfico que permite operaciones de *hash*, cifrado y firma, y la generación de claves públicas y privadas que las aplicaciones del equipo pueden emplear para realizar sus propias operaciones.

Las claves privadas generadas por el TPM se almacenan en el mismo, y también permite realizar mediciones de los parámetros del entorno que se almacenan como *hashes* en registros PCRs, y que permiten validar la integridad de las mediciones.

Esta última característica estuvo disponible a partir de la versión 1.2 de TPM donde se introdujeron notables mejoras. Posteriormente el chip también se presentó en una placa independiente que podía incorporarse al equipo del usuario (GC-TPM). En este caso, el chip sigue estando integrado en placa.

El chip TPM ha tenido muchas aplicaciones en los últimos años, siendo analizado también como CoT en redes vehiculares. Dicho uso se encuentra detallado en documentos del TCG para la versión 2.0 del chip [15]. Uno de los puntos a favor del uso del TPM en vehículos es que éstos de por sí tienen que pasar periódicamente la inspección técnica por personal autorizado y que ese hecho permitiría actualizar el software que use el dispositivo convenientemente y efectuar un control sobre el estado del TPM.

Tal vez la evolución del TPM como concepto de almacenamiento *anti-tampering* recaiga en la figura del elemento seguro o *Secure Element* (SE). Acorde a la definición de MasterCard, hay tres formas básicas en las que se puede hacer uso del SE: (i) SIM Cards/UICC, (ii) microSD Cards, o (iii) embebido en el dispositivo móvil (eSE). Además, se puede

considerar que el SE hace uso de la antena del dispositivo móvil (*Single Wire Protocol*, SWP), o bien que las opciones (i-ii) cuentan con su propia antena integrada (*Dual Interface*).

El SE puede encontrarse en dispositivos móviles o dispositivos personales como *tablets*, e incluso *wearables*. Su funcionalidad más palpable en este ámbito se ha visto con la tecnología *Near Field Communication* (NFC), una tecnología de comunicación de rango corto para efectuar pagos electrónicos con los dispositivos móviles sin contacto con el terminal de pago. Pese a que NFC define el uso del SE embebido en diversos componentes, su uso más robusto es cuando está integrado en la propia circuitería del dispositivo móvil, ya que de esta forma se liga el SE al propio cuerpo del dispositivo. A fin de extender el pago móvil, soluciones como Boosted NFC SE integran el elemento seguro en dispositivos ultra pequeños, como es el caso de los *smart wearables*.

Cabe destacar, que las tarjetas identificativas y los *tokens* son por sí mismos mecanismos *anti-tampering* pero con un propósito mucho más limitado que los dispositivos *anti-tampering* de los que en este apartado nos hacemos eco. Por ejemplo, en el caso del TPM, las aplicaciones pueden definir cómo hacer uso del chip. Esta característica ha hecho que el chip TPM siga evolucionando hacia su vertiente virtual (vTPM), que permite su uso por parte de sistemas virtuales sin pérdida de generalidad. Por otra parte, el SE integrado en los dispositivos móviles también puede ser usado por otras tecnologías por sus características para almacenar claves, o *hashes* de datos biométricos (ej. huella dactilar) del propietario del dispositivo u autorizados [16]. Además, desde el W3C se aúnan esfuerzos para definir interfaces entre las aplicaciones Web y SEs.

No obstante, algunos ven en el uso del SE una limitación para efectuar transacciones, por lo que también surgen alternativas para evitar el uso del SE, como la tecnología *Host Card Emulation* (HCE), que emplea el *Cloud* para consultar los datos que se consultarían en un SE. Este tipo de tecnologías tiene como contrapartida la pérdida del núcleo físico de confianza integrado en el dispositivo, que se situaría en el *Cloud*, y por tanto el control de esos datos quedaría al cuidado de entidades externas, no de nuestro dispositivo, pudiéndose cuestionar la confiabilidad de la información.

Uno de los desafíos de la gestión de evidencias electrónicas es incluir los diferentes marcos legales que están en vigor a nivel nacional, europeo e internacional. Este requisito viene impuesto por la necesidad, ya que son las leyes las que definen las acciones aceptadas como válidas por la sociedad que las impulsa. Ya que los datos informáticos, y por tanto las evidencias

electrónicas, no entienden de fronteras, es vital que la gestión de las evidencias sí comprenda cuáles son las reglas por las que la adquisición de evidencias y su tratamiento se encuentran regidas. De lo contrario, una evidencia electrónica podría ser erróneamente manipulada y repudiada por ello.

La adquisición y gestión de evidencias electrónicas debe efectuarse de manera que las pruebas no puedan ser puestas en entredicho. Demostrar cualquiera de los supuestos anteriores puede ser inservible si, finalmente, el juez o el jurado (según el marco legal) dudan sobre el procedimiento para recabar las evidencias electrónicas.

No hay que olvidar el contexto que nos ocupa. Cuando un caso requiere el uso de evidencias electrónicas no es para ajusticiar un equipo informático, sino para llegar al individuo o corporación tras el equipo informático y asignar responsabilidades. Para que esto sea posible la vinculación de un dispositivo con un usuario es fundamental.

A día de hoy, ejemplos de vinculación entre una persona física y un objeto existen. El ejemplo más antiguo pudiera darse en el uso de la identificación de una persona. Los papeles que identifican un individuo y certifican que es quien dice ser, permiten realizar trámites. Así, estos objetos vinculantes han sido introducidos paulatinamente y con cierto grado de recelo en el mundo virtual. El ejemplo más claro es el uso del DNI-e que permite agilizar trámites que antaño requerirían nuestro desplazamiento. Esto es así porque se asume que nuestro DNI-e está en nuestra posesión; de lo contrario, el ciudadano tiene la obligación de notificar del extravío, pérdida o robo del DNI-e a las autoridades pertinentes empleando los mecanismos y procedimientos legales a su alcance para la notificación.

Cabe destacar que la fuerza o credibilidad de estos objetos y dispositivos vinculados, lo que les da potestad para realizar acciones en nuestro nombre, es nuestra identidad. La adopción de nuevas tecnologías sin contacto por su comodidad posibilita que los objetos que portan nuestra identidad realicen acciones más cómodamente, e integren nuevas tecnologías que aún están en el punto de mira, como es el caso del DNI-e v3.0, que incorpora NFC.

Por todo ello, la testificación digital es necesaria porque daría soporte a la GEE para los nuevos retos que vienen marcados por la implantación de paradigmas como la *IoT*:

DESCRIPCIÓN DE LA INVENCIÓN

Un aspecto de la presente invención se refiere a procedimientos para la gestión segura de evidencias electrónicas dentro del marco de la *IoT*. Aunque en el presente documento la invención se hace contextualizar en el ámbito legal o jurídico, su aplicación no necesariamente queda restringida a dicho ámbito, siendo extensible a otros ámbitos o contextos en los que sea posible, recomendable, o incluso obligada la gestión segura de evidencias electrónicas.

En primer lugar es preciso definir los requisitos y pasos necesarios para dicha salvaguarda de evidencias electrónicas haciendo uso de dispositivos personales de usuarios que actuarían como *testigos digitales* ante la ley. Concretamente, la presente invención se centra en las fases de generación, almacenamiento y transmisión (1-3) de evidencias electrónicas, y más en particular en el almacenamiento y la transmisión de las mismas, ya que las fases de recuperación, tratamiento y comunicación (4-6) pueden recaer en entidades con más recursos que se encarguen de realizar un análisis *a posteriori*. De hecho, un punto crítico en la gestión de evidencias en la *IoT* no considerado es precisamente cómo llevar las evidencias desde su lugar de ocurrencia hasta su custodia haciendo uso de los propios dispositivos del entorno.

Consideraremos que (i) la generación de una evidencia puede producirse en cualquier lugar, empleándose técnicas forenses reconocidas; (ii) el almacenamiento de la evidencia puede ser temporal o definitivo, pero en cualquier caso deben emplearse herramientas que aporten garantías de integridad y confiabilidad; (iii) dichas herramientas deben ser soportadas por los usuarios del sistema, en este caso los objetos autorizados; (iv) estos objetos, pertenecen a personas, que pueden dar fe de estos objetos; y, además, (v) durante la transmisión de las evidencias, debe mantenerse la cadena de custodia digital para preservar la evidencia manteniendo la confiabilidad de la prueba y la vinculación usuario-dispositivo. Como resultado final se propone en la presente invención una arquitectura funcional para la testificación digital.

La figura 1 muestra de forma simplificada los pasos básicos de una realización general del procedimiento que constituye un primer objeto de la invención desde que se obtiene la evidencia electrónica hasta que, en su caso, se libera el espacio de su almacenamiento. Cada uno de los pasos del proceso está sujeto a la gestión de información contextual.

Cuando se obtiene la evidencia (1), se genera una cabecera con la información pertinente según un determinado *Formato de Evidencia Electrónica* (FEE). En este proceso, se genera un identificador de la evidencia a partir del identificador vinculante del dispositivo electrónico que la genera, y el estampillado de tiempo. Éste será el identificador de la evidencia durante su ciclo de vida. La evidencia se firma y el valor probatorio se almacena (2) atendiendo a criterios de

almacenamiento seguro. La firma de la evidencia dependerá del mecanismo escogido para la vinculación de la identidad.

En algún momento, si la evidencia ha de ser delegada, se escoge un testigo digital al que transmitir la evidencia (3). Consideramos que la evidencia electrónica ha de ser delegada cuando:

a. A no es custodio digital. A debe transmitir la evidencia al menos una vez a un custodio.

b. El dispositivo alcanza un umbral de almacenamiento admitido (configurable).

c. La evidencia generada es de carácter crítico, o el tiempo de vida va a consumirse.

d. Si B tiene más posibilidades de alcanzar pronto el destino final y la transferencia no perjudica la vida de la evidencia más que si A la almacenase/custodiase.

Por otra parte, la elección del siguiente testigo digital, en su caso, está condicionada al cumplimiento de los siguientes requisitos:

rt1. B puede dar fe de que es un testigo digital y de su rol/nivel.

rt2. B es un testigo digital del mismo nivel que A, o A tiene nivel menor que B. Es decir, el conjunto de parejas posibles es: {(td, td), (cd, cd), (td, cd)}, con td: testigo digital, cd: custodio digital.

rt3. B satisface los criterios para salvaguardar la evidencia electrónica. Esto puede estar sujeto a la criticidad de la evidencia. Por ejemplo, las evidencias electrónicas de carácter penal deberían ser enviadas en exclusiva a custodios digitales.

rt4. B es el mejor candidato: candidato de mayor nivel de delegación de todos los posibles, o bien aquel candidato que ofrezca más garantías/probabilidad de que la evidencia alcance el destino final minimizando el pivotaje.

rt5. B es un custodio digital y solicita el envío de las evidencias, y A puede verificar la identidad de B.

Una vez que se escoge el testigo B, la información sobre la evidencia electrónica se envía (4) usando el FEE adaptado para la testificación digital, empleando un canal seguro. B

entonces autentica la evidencia electrónica y procede a su almacenaje. En este paso, B crea su propia evidencia para reflejar la recepción de esta evidencia en su histórico. Entonces, envía a A una prueba de que la recepción y el almacenamiento de la evidencia ha sido posible (6). Si B no envía esta prueba, A registra en el histórico que la evidencia fue enviada a B, pero no la elimina. La garantía de recepción es almacenada en el histórico (7).

El histórico de evidencias es un resumen de las evidencias gestionadas que debe ser almacenado de forma segura. Significa el acuse de recibo de las transacciones operadas por el testigo. Estará compuesto por el conjunto de identificadores de las evidencias generadas y un código que indique si fue transmitida, y la garantía dada por el receptor en el paso (6) (por ejemplo, el identificador de la evidencia firmado).

Por último, A puede liberar el espacio de la evidencia o conjunto de evidencias (8), si procede.

Almacenamiento y formato de las evidencias electrónicas

Las evidencias electrónicas pueden ocupar mucho espacio, ya que, a diferencia de una anomalía, una evidencia electrónica puede ser cualquier dato. Por lo que hay que (i) definir qué consideraremos evidencias, (ii) el formato para las evidencias del *IoT* (el definido en [1] es demasiado ambicioso para los pequeños objetos), (iii) la cantidad de información/evidencias que almacenaremos, (iv) qué evidencias resultarán más prioritarias.

Como se define en [1], en un SGEE se requiere un FEE que sirva tanto para el intercambio de la evidencia como para ayudar en la obtención forense. El objetivo de usar un formato es facilitar la comprensión de la evidencia y agilizar su procesamiento. Esto además permite resumir la información, usando identificadores, cuando se usan mecanismos estandarizados que podemos clasificar y poner a disposición de los participantes del entorno. Sustituiríamos así extensas descripciones por identificadores en un informe simplificado.

En [1] se proponen los siguientes datos para las cabeceras para el intercambio de la evidencia electrónica y su obtención segura para el análisis forense:

c1. Intercambio: versión, tamaño, identificador, organización, descripción, marca de tiempo, archivos totales, número de archivo, tamaño del archivo, formato del archivo, tipo de firma, tamaño de firma.

c2. Obtención forense: versión, tamaño, identificador, creador, fecha de creación, fecha de obtención, archivos totales, número de archivo, tamaño de archivo, formato de archivo, tipo de dispositivo, modelo de dispositivo, número serie del dispositivo, número de sectores del dispositivo, primer sector, número de sectores de la evidencia, tipo de firma, tamaño de firma.

Por ejemplo, el campo "versión" hace referencia a la versión del FEE empleado, el campo "identificador" incluye información sobre el NIF/CIF de la organización responsable. En c2, los datos referentes al dispositivo se refieren al medio de almacenamiento de la prueba (ej. disco duro del que se ha extraído la evidencia), y tienen una vertiente clara hacia la obtención de datos muertos (Sección II-B, caso b). Este tipo de FEE está diseñado para almacenamiento de diverso tipo, considerando la gran variedad de alternativas, por ejemplo, de discos duros, del mercado, y que los sistemas informáticos tradicionales se componen de piezas intercambiables.

Sin embargo, en el ámbito de los dispositivos móviles, considerando que éstos son sistemas embebidos con características conocidas en base al modelo del dispositivo, la información sobre las características del dispositivo pueden deducirse en base a los identificadores del modelo del dispositivo empleado para la captura de evidencias. De esta forma los campos del FEE para este tipo de dispositivos puede ser simplificado, obviándose las características conocidas de los dispositivos con un determinado perfil. Como el FEE cuenta con un identificador de versión, puede incluso definirse una versión para los dispositivos de esta índole, por lo que un SGEE podría usar tanto el formato indicado por la norma, como el simplificado para los dispositivos con menos recursos, sin pérdida de generalidad.

Cabe destacar, que la trazabilidad de la información incluye más aspectos a considerar. Por ejemplo, si se consideran sólo los datos del dispositivo que genera la evidencia o los datos de los dispositivos intermedios donde la evidencia es alojada temporalmente. El último caso, está estrechamente ligado a la transferencia de la evidencia electrónica entre los distintos participantes.

Además de simplificar las cabeceras considerando las limitaciones de los dispositivos, deben considerarse, como mínimo, los siguientes aspectos para implementar nuestro enfoque:

- Elemento Seguro. Datos relativos a qué implementación de elemento seguro se ha usado, o si no se ha usado.
- Tiempo de vida. Información sobre la posible caducidad de la evidencia. Puede componerse por un código que indique la interpretación del tiempo de vida (ej. en base al número de pivotajes) y un valor.
- Prioridad. Dato por ejemplo para priorizar el almacenamiento de unas evidencias frente a otras.
- Criticidad. Define el tipo de dispositivo que puede custodiar la evidencia.
- Pivotaje. Número de saltos (o intermediarios) de la evidencia.

Los campos del FEE deben ser relevantes para la comprensión de la evidencia, concisos, y contener información probatoria de la integridad de la evidencia. La limitación de espacio para almacenar las evidencias sugiere que como mínimo se preserve la integridad de la evidencia, esto es, almacenar como mínimo el valor *hash* de la evidencia firmado. Este valor se transmitiría junto con la evidencia firmada. El uso de mecanismos *anti-tampering* para almacenar valores *hash* se ha empleado, por ejemplo, para el inicio confiable, o *Root of Trust* (RoT) del chip TPM (Tabla I). En dicho caso, la integridad del software se verifica si el *hash* de los componentes coincide con las mediciones *hash* almacenadas en los registros PCR (*Platform Configuration Registers)* del chip. En el caso que nos ocupa, la integridad de la evidencia se verificaría si el *hash* coincide con el protegido en el medio de almacenamiento seguro.

Cabe destacar, que pese a que el formato de evidencias no ocupase demasiado espacio en el chip, el número de evidencias dependerá del contexto y del tipo de evidencias que se guarden en el dispositivo. En cualquier caso, parece inevitable y razonable que ésta información almacenada en el chip sea delegada, siempre que proceda, a una entidad con autoridad para ello lo antes posible, debido a dos factores: (i) espacio limitado y (ii) minimizar la ventana de compromiso de la evidencia. Además, para evidencias muy críticas debería poder definirse el perfil de los dispositivos que podrán salvaguardar la evidencia.

En otro orden, consideramos que existen diferentes roles o perfiles dentro de la testificación digital. La clasificación básica (figura 2) es distinguir entre testigo digital y custodio digital, como caso particular de testigo digital pero con más privilegios. Así, la evidencia podría ser recabada (figura 3) bien por (a) un objeto perteneciente a un civil actuando

como testigo digital reconocido, (b) un objeto personal en posesión de un usuario con privilegios, reconocido como custodio digital (testigo digital fuerte con privilegios), o por (c) un objeto o entidad con más recursos perteneciente al cuerpo de seguridad y reconocido como custodio digital.

La separación de los casos (b) y (c) es importante por el carácter delimitador de los recursos de los dispositivos que portaría el usuario con privilegios (o con potestad) en (b). Esta limitación haría que el número de evidencias registradas no pudiese superar un umbral determinado, por lo que, al igual que los objetos en (a), los objetos en (b) deben liberar la evidencia lo antes posible.

Delegación de identidad y firma de evidencias electrónicas

Es esencial que un usuario pueda delegar su identidad hacia el dispositivo o dispositivos que actúan como testigos digitales. Como primer paso, y en el contexto que nos ocupa, es necesario que la identidad de un usuario dentro de un dispositivo sea vinculante; es decir, debe permitir durante el manejo de las evidencias trazar de forma inequívoca a la persona física que esta detrás de dicha identidad. Actualmente, ya existen mecanismos y procesos que permiten asociar la identidad de un usuario a un dispositivo de forma vinculante. Un ejemplo es la información almacenada en una tarjeta SIM/UICC (p.ej. identificadores IMSI, MSISDN [17]), puesto que en determinados países como España la persona física necesita proporcionar un documento legal para obtener esa identidad. Otro ejemplo es el uso de documentos de identidad digitales (p.ej. DNI-e), ya que permiten a una persona física autenticarse ante un dispositivo o servicio usando dicha documentación [18]. También hay que tener en cuenta aquellos mecanismos que dependan de las características de la persona, como los sistemas biométricos.

Aunque una identidad pueda ser vinculante, existe un desafío principal que debe resolverse dentro del manejo de las evidencias: Cómo unir de forma indisoluble una evidencia a un usuario determinado durante todo el CVEE. Asegurar dicho enlace es algo necesario no sólo durante la transferencia de evidencias entre testigos digitales, sino también en el momento en el que una evidencia se utilice como prueba dentro de un juicio. Para este fin, es posible utilizar una primitiva criptográfica que precisamente permite una vinculación inequívoca entre un usuario y la información generada por sus dispositivos: las denominadas *proxy signatures* [19]. Es más, todas las estrategias para implementar esta primitiva criptográfica [19] nos

permiten implementar la vinculación entre usuario y evidencia, tal y como se muestra en la figura 4 y se desarrolla en el siguiente párrafo.

En su forma más sencilla (*full delegation*, FD), el usuario delega el uso de su clave privada al dispositivo. Ésta puede ser entonces utilizada para firmar las evidencias. Otra estrategia (*delegation by warrant*, DbW) consiste en el uso de un *token* (*warrant*), firmado con la clave privada del usuario, que indica la identidad del dispositivo y el periodo de validez de la delegación, entre otros datos. Este *token* se proporcionaría al dispositivo, el cual lo adjuntaría a las evidencias firmándolo con su propia clave. Finalmente, en el último esquema (PK) se utiliza la clave privada del usuario para generar un par de claves privada y pública, las cuales serán utilizadas por el dispositivo para firmar las evidencias. Al estar dichas claves asociadas a la identidad del usuario (p.ej. utilizando criptografía basada en identidad [20]), puede comprobarse la identidad del usuario que generó las evidencias.

En nuestro enfoque, al resultado de los esquemas FD, DbW o PK (o cualquier otro esquema que aporte una vinculación entre un usuario y su dispositivo) lo denominamos credenciales vinculantes (*binding credentials,*BD), ya que, sean claves (p.ej. caso del FD o PK) o *tokens* (p.ej. caso del *warrant*), son los medios empleados para firmar la evidencia electrónica creando la relación entre el usuario, el dispositivo y la evidencia electrónica.

Por otra parte, para el uso de *proxy signatures* es obligatorio que el usuario disponga de un par de claves pública y privada. Además, la clave privada debe estar convenientemente protegida dentro de un chip de seguridad (p.ej. eSE), el cual permitirá realizar operaciones de firma digital. Estos requisitos pueden resolverse utilizando los mecanismos subyacentes de las identidades vinculantes. Por ejemplo, en el caso de los dispositivos móviles, y según la norma 3GPP TS 33.221 [21], es posible con la asistencia del operador de telecomunicaciones incluir certificados y claves privadas dentro del UICC. En este caso, el sistema de gestión de evidencias se desarrollaría conjuntamente con el operador, pudiendo formar parte de los servicios incluidos dentro del UICC. Esto permitiría que las evidencias fuesen firmadas dentro del propio UICC e incluyan los identificadores (IMSI, MSISDN) necesarios.

Una alternativa que no necesita de una tercera parte confiable industrial, y que además involucra directamente al usuario puede ser el uso del DNI-e o equivalente. Actualmente es posible conectar un DNI-e a un dispositivo a través de un lector de tarjetas y un puerto USB, y a través de una conexión NFC usando el DNI-e v3.0. Esto permite usar la clave privada del individuo contenida dentro del DNI-e para, por ejemplo, firmar las evidencias directamente o

proporcionar un *warrant*. Una ventaja de este método es el uso de un documento con validez legal para el manejo de las evidencias, lo cual facilitaría su uso ante un tribunal de justicia sin tener que involucrar a terceras partes. Además, proyectos como STORK y STORK2 [22] han demostrado que es posible la interoperabilidad entre identificadores electrónicos Europeos, por lo que la vinculación de la evidencia puede tener validez a nivel continental.

Todos estos métodos funcionan en caso de que se utilice únicamente un dispositivo móvil para la adquisición y gestión de las evidencias. Sin embargo, su uso puede estar restringido en ecosistemas como la *IoT*, donde varios dispositivos con recursos bastante limitados podrían participar en el CVEE. Es más, el problema de la identificación de objetos *IoT* (y sus propietarios) sigue abierto a día de hoy [23]. No obstante, existen varios trabajos cuyo objetivo es desarrollar un entorno de red de área personal (PAN) confiable, en el que los dispositivos son propiedad de un único usuario. Trabajos como [24] demuestran que es posible intercambiar información de forma segura entre miembros de una PAN, delegando las tareas más complejas (p.ej. autenticación con dispositivos externos, almacenamiento de información) a aquellos elementos que tengan capacidad suficiente para realizarlas. Otros trabajos, como [25], desarrollan el concepto de PKIs personales, en los que cada dispositivo controlado por un usuario puede poseer su propio par de claves, las cuales son generadas por el propio usuario (p.ej. a través de su DNI-e). Todas estas propiedades permiten que, en determinados entornos PAN, pueda ser posible generar evidencias, almacenarlas, y verificarlas a través de *proxy signatures*.

Finalmente, hay otro aspecto que debe considerarse con cautela: el uso de las *proxy signatures* permite vincular una evidencia a un individuo determinado, pero no asegura que el individuo estuviese controlando el o los dispositivos en cada momento. Por ejemplo, un usuario puede generar un *warrant* a través de su DNI-e, pero no controlar el dispositivo durante el proceso de adquisición y/o transmisión de evidencias. Si esto fuera necesario, pueden utilizarse mecanismos de autenticación basados en contexto [26] o sistemas biométricos [27] para así ratificar la presencia del usuario. Otro enfoque a tener en cuenta, heredado de los principios de la *IoT*, es que sea el propio objeto u objetos los que recojan evidencias de la participación del usuario durante todo el proceso.

Transmisión segura de evidencias electrónicas

La transmisión segura de evidencias electrónicas conforme a la presente invención requiere establecer lo que se denomina una *cadena de custodia digital* (CCD) [9], pero donde los involucrados serían objetos de uso personal. Dicha transmisión o liberación segura de evidencias electrónicas se realizaría por medio de lo que denominaremos *pivotaje de evidencias* (o *delegación virtual de evidencias electrónicas),* un proceso mediante el cual las evidencias se transfieren desde el objeto del individuo que actúa como testigo digital, hasta la fuente final de la información, donde las evidencias serían almacenadas para su análisis final. Conforme a la figura 3, es posible considerar seis casos base de pivotaje:

da 1. Delegación de un usuario en otro usuario con más privilegios. Correspondería a la colaboración ciudadana para recabar evidencias y la notificación a un usuario con potestad para gestionarlas.

da 2. Delegación de un usuario en otro objeto (móvil) con más privilegios o recursos. Es similar al caso **da l**, pero la evidencia electrónica se entregaría a un objeto del cuerpo de seguridad con más recursos o mayor posibilidad de encontrar un objeto para el almacenamiento final de la evidencia.

da 3. Delegación de un usuario en otro objeto con más privilegios o recursos. Similar al caso anterior, pero en este caso la delegación se efectúa sobre estructuras fijas, que probablemente serán el almacenamiento final de las evidencias antes de su procesamiento o transferencias a otras entidades siguiendo los esquemas tradicionales para la transferencia de evidencias electrónicas.

db 1. Delegación de un usuario con potestad a otro usuario con potestad. Este caso contemplaría aquellos motivos por los cuales un usuario con potestad delega una parte o todas sus evidencias a otro usuario con potestad.

db 2. Delegación de un usuario con potestad a un objeto con potestad. Es el símil con **da 2**, pero donde el objeto puede ser móvil o no. En este caso no se hace distinción, porque la delegación de la evidencia proviene de un dispositivo que actúa como testigo fuerte, y por tanto, en principio, el nivel de confiabilidad se asume mayor.

db 3. Delegación de un objeto con potestad a otro objeto con potestad. Es el caso de delegación entre objetos menos restringidos con los recursos y menos ligados al uso personal.

Cabe destacar que los objetos como coches estarían en **db 3** porque, aunque son manejados por usuarios, el apego no es tan continuo como podría ser el de un terminal móvil, que acompaña al usuario incluso dentro de edificios. Por ello creemos conveniente separar estos tipos de casos. La diferencia entre los dispositivos y los usuarios permite establecer el contexto en el cual se produce la transferencia de la evidencia e identificar casos sospechosos de mal comportamiento.

Un segundo aspecto de la invención se refiere a dispositivos para la gestión segura de evidencias electrónicas, dispositivos capaces de implementar los procedimientos objeto del primer aspecto de la invención, dispositivos que, de forma genérica, denominamos testigos digitales, entendiéndose la figura de Testigo Digital como la de un dispositivo con un núcleo de confianza capaz de proteger una evidencia electrónica ante cualquier modificación y acceso no autorizado y de efectuar su transferencia a una entidad autorizada, que puede ser otro testigo digital o bien una entidad con potestad para alojar la evidencia electrónica. La interrelación entre dichos dispositivos o testigos digitales puede conformar diferentes sistemas de gestión segura de evidencias electrónicas.

Proponemos el uso de un dispositivo personal capaz de adquirir eventos de la red de comunicaciones, por ejemplo, un intento de conexión remoto no autorizado. También podemos considerar el uso del dispositivo personal para adquirir evidencias locales, por ejemplo, la presencia de un virus. Este uso requiere limitar el tipo de información que el dispositivo de usuario puede compartir sin comprometer la privacidad del usuario. Por ejemplo, podría ser factible tomar como evidencia un listado de aplicaciones, o la agenda de contactos, sin embargo, esto debería contar con la aprobación del usuario, y deben definirse los contextos en los que este tipo de información no debe ser empleada o compartida.

La figura 2 muestra dos tipos de testigo digital considerados en base a perfiles de usuario. Al hilo de la delegación de identidad comentada con anterioridad, entendemos que hay un principio básico, y es que el dispositivo que actúe como testigo tiene que ligar la identidad del usuario al dispositivo porque esto permite acercar el marco legal a la evidencia electrónica que se custodie. Además, esta postura permite también añadir un valor de responsabilidad del usuario al dispositivo, algo que por otra parte es necesario hoy día. De esta forma, la idea es que el extravío o robo de un dispositivo considerado testigo deberá notificarse a las autoridades pertinentes como si de un DNI-e se tratase (caso Español).

Podría entenderse que vincular la identidad del usuario a su dispositivo personal pudiera afectar a la privacidad del usuario, considerando que, por ejemplo, en un teléfono móvil las aplicaciones en ejecución pueden ser muy diversas y de distintas fuentes, carentes del control al que otros dispositivos oficiales están sometidos.

Sin embargo, este riesgo ya existe a día de hoy. El dispositivo móvil de per se guarda mucha información que permitiría identificar el propietario del terminal. Por todo ello, consideramos que ligar el terminal a la identidad del usuario sólo añade claridad al hecho de que un dispositivo móvil con datos personales es una responsabilidad. Así, el dispositivo móvil podría efectuar acciones en nombre de su propietario siempre y cuando se satisfagan una serie de requisitos que aseguren que dichas acciones fueron ordenadas por un propietario en concreto. Como requisitos básicos, podemos considerar:

- Existencia de un núcleo de confianza que aporte un grado de confiabilidad a la acción.
- Existencia de un responsable final humano de la acción, esto es, una vinculación de identidad humano-máquina.
- Existencia de un medio por el cual la acción queda registrada, ya sea de forma local, o estableciendo los procedimientos de seguridad necesarios para transmitirla a una entidad autorizada.

Así, consideramos que un testigo digital es *fuerte* si se trata de un dispositivo con núcleo de confianza y además cuenta con la identidad del usuario. Esto permite, por una parte, proteger la evidencia electrónica y, por otra, tener la potestad para actuar como testigo digital en nombre del usuario.

Por otra parte, al igual que sucede en el mundo físico, diferentes perfiles de usuario darían lugar a diferentes testigos digitales. Por ello, entendemos que cuando el dispositivo pertenece a un individuo con representación en el sistema legal (ej. un policía), actuando no como ciudadano sino, por ejemplo, como agente de la ley, es decir, el dispositivo no es propiedad privada, la obtención de la evidencia está más controlada y su salvaguarda también. Ésta es la figura de *custodio* representado en la figura 2. Así, aunque un testigo digital fuerte pueda salvaguardar información, el término custodio se reserva para este último tipo de testigo digital ligado a la administración, porque por norma general la custodia la realizan los cuerpos de seguridad del estado.

El objetivo final es que las evidencias electrónicas completen la primera fase del CVEE en el que están involucrados objetos, y que puede ser más crítico por los recursos de éstos. Para ello, en el contexto que nos ocupa, los testigos digitales pueden requerir transmitir las evidencias electrónicas a otros testigos digitales.

El concepto de Testigo Digital define la arquitectura básica de seguridad para adquirir evidencias electrónicas de naturaleza probatoria, aceptables en un posible litigio, en escenarios dinámicos, heterogéneos y distribuidos del *IoT*. Una ventaja clara del testigo digital, es que aprovecha arquitecturas de seguridad embebidas para proporcionar, por primera vez, la gestión de evidencias electrónicas en dispositivos personales como colaboradores, creándose el símil con la testificación humana. Otra ventaja añadida, es que el uso de testigos digitales permite agilizar la labor policial por medio de la colaboración ciudadana vinculante con los dispositivos.

Para que esto sea posible, la arquitectura de un escenario para la testificación digital comprende los componentes mostrados en la figura 5, si bien alguno de ellos opcional, que definen las características técnicas esenciales:

1) Gestor de operaciones entre el usuario y el dispositivo. Permite vincular la identidad de un usuario con su dispositivo personal. Como resultado, genera un conjunto de credenciales vinculantes (*binding credentials,* BD), que serán empleadas a lo largo del proceso de GEE. Además, proporcionaría opciones adicionales como solicitar pruebas biométricas al usuario para la GEE.
2) Gestor contractual. Es un componente de uso opcional que permite indicar al testigo digital los mecanismos criptográficos y la configuración más robusta aceptable para la adquisición de evidencias. Proporciona al testigo una prueba de asesoramiento de un testigo con más privilegios. Si este componente no se usa y el testigo usa mecanismos aceptados la evidencia tendrá la misma validez que si el gestor contractual se hubiese usado.
3) Mecanismos criptográficos aceptados. Son los mecanismos criptográficos dentro de un elemento seguro (chip *hw*, *anti-tampering*) que se usarán durante la GEE, y probablemente (aunque no obligatoriamente) por el gestor de operaciones usuario-dispositivo.
4) Almacenamiento seguro con control de acceso. Almacenamiento protegido en un elemento seguro (puede ser el mismo elemento seguro que el que contiene los

mecanismos criptográficos u otro distinto). En este componente se almacenarían claves y otros datos protegidos, como los *hashes* de las evidencias electrónicas, el contrato, y las credenciales vinculantes.

5) Gestor de evidencias electrónicas para objetos. Coordina las operaciones de adquisición de evidencias electrónicas, almacenamiento seguro, y transferencia de la evidencia electrónica a otro testigo de la cadena.

La inclusión de chips de seguridad hardware trae consigo diversas ventajas, como el hecho de que algunos de estos chips integran mecanismos para proporcionar un canal de comunicaciones seguro. También existen soluciones para definir transacciones que involucran la participación del elemento seguro, en el que se almacena la identidad del dispositivo [29].

En el caso que nos ocupa, no basta con que el chip integre mecanismos para establecer un canal de comunicaciones seguro, sino que, además, esos mecanismos deben emplear tecnologías que sean aceptables para la gestión de evidencias conforme a las normas que procedan y de acuerdo a la legalidad vigente (p.ej. considerando la privacidad de los datos). En concreto, en [1] se definen, como operaciones permitidas:

- Algoritmos de clave simétrica: 2TDEA, 3TDEA, AES l28bits-256 bits.
- Firmas electrónicas y aplicaciones *hash*: SHA224/ 256/ 384/ 512.
- HMAC, funciones de derivación de claves, generación de números aleatorios: SHA1/ 224/ 256/ 384/ 512.

El nivel de seguridad se clasifica atendiendo al tiempo de vida de la seguridad y al tipo de dato que guarda considerando la LOPD. Por ejemplo, atendiendo a los requisitos de [1], el chip *OPTIGA Trust authentication* usando RSA de 2048bits podría proteger información confidencial de nivel alto, y usando ECC de 512bits y AES 256 proteger información secreta de alto nivel (la escala máxima definida en [1]). Por lo tanto, constituye una buena opción para su uso como testigo digital fuerte. Además, permite el intercambio de claves usando *diffie hellman* (DH) o DH empleando criptografía de curva elíptica (ECDH), agilizando la creación de canales seguros de comunicación.

En la presente invención se establecen los requisitos mínimos que la tecnología del dispositivo debe satisfacer para ser un testigo digital acorde a nuestra definición, pero cabe

destacar que aunque se proponen ejemplos para demostrar que el esquema es implementable en la práctica, dicha implementación no se asocia específicamente a un único tipo de dispositivo, sino que los requisitos propuestos pueden ser satisfechos por un amplio espectro de dispositivos.

DESCRIPCIÓN DE LAS FIGURAS

Figura 1. Pasos básicos de la testificación digital y escala de valores.
Figura 2. Roles en la testificación digital y requisitos básicos.
Figura 3. Pivotaje de evidencias.
Figura 4. IDEEs en testigos digitales.
Figura 5. Componentes básicos para la testificación digital.
Figura 6. Arquitectura funcional básica para la testificación digital.
Figura 7. Diagrama de flujo con caso de uso simplificado.
Figura 8. Arquitectura funcional para la testificación digital basada en credenciales vinculantes (*binding credentials,*BD).
Figura 9. Diagrama de flujo para el caso (A) considerando el Gestor Contractual.
Figura 10. Diagrama de flujo para el caso (C) considerando el uso de mecanismos biométricos.
Figura 11. Biométricos como prueba adicional.

EJEMPLO DE REALIZACIÓN DE LA INVENCIÓN

La constitución y características de la invención se comprenderán mejor con ayuda de la siguiente descripción de ejemplos de realización, debiendo entenderse que la invención no queda limitada a estas realizaciones, sino que la protección abarca todas aquellas realizaciones alternativas que puedan incluirse dentro del contenido y del alcance de las reivindicaciones. Asimismo, el presente documento refiere diversos documentos como estado de la técnica, entendiéndose incorporado por referencia el contenido de todos estos documentos, así como de el contenido completo de los documentos a su vez referidos en dichos documentos, con objeto de ofrecer una descripción lo más completa posible del estado de la técnica en el que la presente invención se encuadra. La terminología utilizada a continuación tiene por objeto la descripción

de los ejemplos de modos de realización que siguen y no debe ser interpretada de forma limitante o restrictiva.

Interacción entre componentes

A continuación definimos tres casos básicos (A-C) de interacción entre los componentes mostrados en la figura 6. El diagrama de flujo que detalla la interacción entre los componentes se muestra en la figura 7:

(A) Establecimiento de políticas de actuación para el uso del testigo digital.

(B) Creación de credenciales vinculantes (*binding credentials,* BD).

(C) Gestión de evidencias con BDs.

En el caso (A), el objetivo es definir cuáles serán los mecanismos criptográficos y configuraciones aceptables, y aquellas políticas adicionales que son necesarias para definir el comportamiento del testigo digital. Por ejemplo, en este paso el usuario debe aceptar las condiciones del servicio, y esta información debe ser almacenada propiamente para su delegación a fuentes oficiales. Por lo tanto, hay dos partes diferenciadas en este punto. Por una parte, (GP1, *Group Policy 1*) las políticas que relacionan al usuario con el dispositivo, no sólo por los términos de servicio, sino por otras políticas que dependan del uso del dispositivo (p.ej. aceptación de permisos, configuración de recursos como el espacio que puede usarse para almacenar evidencias), y, por otra parte, (GP2, *Group Policy 2*) las políticas que definen el funcionamiento del Gestor de Evidencias Electrónicas para Objetos (Gestor EE). De forma general, GP1 y GP2 conforman el conjunto de asociaciones de seguridad (SA, *Security Associations*), del que hará uso el testigo digital.

Las políticas más generales, GP1, serán negociadas entre el usuario y el Gestor de Operaciones Usuario-Dispositivo, mientras que otro grupo de políticas, GP2, serán establecidas por medio del Gestor EE. Definir el conjunto de políticas aplicables es muy crítico, ya que definirá el comportamiento del testigo digital. En particular, definimos cuatro políticas que serían aplicables desde el Gestor EE: (P1) política de generación de evidencias, (P2) política de transmisión de evidencias, (P3) política de almacenamiento de evidencias, (P4) política de borrado o eliminación de evidencias. Todas las políticas incluyen la lista de mecanismos de

seguridad y criptográficos aceptados para cada caso y consideran la lista de requisitos mencionados anteriormente. En relación a (P1) se detallarán los mecanismos forenses empleados para la adquisición de las evidencias.

Se asume, por tanto, que, como caso básico, el Gestor EE integra información básica sobre los mecanismos aceptados para la gestión de evidencias electrónicas. Las políticas, una vez aceptadas, son salvaguardadas como evidencias electrónicas, constituyendo una prueba de los mecanismos que serán válidos en el esquema de testigo digital. Una mejora que posibilitaría el despliegue de un escenario más dinámico implica el uso del gestor contractual como asesor.

En el caso (B), el gestor de operaciones usuario-dispositivo es el responsable de realizar las operaciones pertinentes para la creación de las credenciales (claves o *tokens*) que vinculen al usuario con el dispositivo. Estas credenciales vinculantes serán empleadas de forma transparente por el GEE para operar con las evidencias, históricos y la transmisión de éstos. Las credenciales vinculantes satisfarán los requisitos de vinculación detallados anteriormente, y se generarán empleando los mecanismos criptográficos aceptados disponibles en el testigo digital. Además, las credenciales se almacenarán con protección *anti-tampering* en el testigo digital.

Por último, el caso (C), corresponde a los pasos mínimos realizados internamente en la arquitectura para tramitar una evidencia, desde que se obtiene hasta que se elimina. Mientras que la figura 1 obvia las operaciones internas entre los componentes de un testigo, aquí detallamos estos pasos. La evidencia se obtiene empleando mecanismos forenses aceptados, acordes a la normativa y la legalidad vigentes. El *hash* de la evidencia electrónica se realizará empleando los mecanismos criptográficos adecuados y, si este componente puede escribir directamente sobre el espacio protegido del elemento seguro del testigo digital, la escritura del *hash* será directa (a). En otro caso, será el gestor de evidencias electrónicas para objetos el componente encargado de solicitar la escritura del valor *hash* resultante en el espacio de almacenamiento. Finalmente, la obtención de una evidencia implica la actualización del histórico de evidencias.

El último paso correspondería con el envío de la evidencia (o conjunto de evidencias). El número de evidencias a enviar, el momento en el que se envían, y la forma de borrado o eliminación de la evidencia, dependerán del conjunto de políticas establecidas a tales fines. En la figura 7 se muestran los pasos que se realizarían una vez se requiere el envío de la evidencia, y también se asume que el siguiente testigo en la cadena (candidato para la delegación) ya fue escogido y que satisface los criterios ya detallados. La tarea de escoger el siguiente testigo

corresponde con los problemas típicos de selección del siguiente nodo en una comunicación salto-a-salto, pero empleando medidas de seguridad y privacidad. Dependiendo de la política, incluso puede requerirse el envío de la evidencia a través de otros medios (p.ej. Internet). Esta labor de decisión depende por tanto de las políticas para la transmisión de las evidencias y sería una de las funciones que el Gestor EE coordinaría (figura 8).

Además, el paso de transmisión conlleva una actualización del histórico de evidencias para reflejar la efectividad o no de la delegación de la evidencia. El primer paso es la obtención de la evidencia (en este caso el *hash* de la evidencia) y del histórico. Estos valores se envían al próximo testigo en la cadena empleando canales de comunicación seguros construidos usando mecanismos criptográficos aceptados, e indicando las credenciales que demuestran la vinculación entre el usuario y el dispositivo.

Como se ha mencionado anteriormente, la forma de borrado o eliminación de la evidencia dependerá de la política de borrado. En la figura 7 se implementa una política de borrado que implica la eliminación de cada evidencia que se delega correctamente. Sin embargo, no siempre tiene que ser así. Por ejemplo, si la evidencia se envía a un testigo digital con nivel de delegación 1 (figura 1), puede ser conveniente salvar la evidencia un breve periodo de tiempo adicional a fin de intentar reenviar la evidencia a otro testigo digital con mayor nivel si se tiene la posibilidad.

Por último, sea cual sea el resultado de la delegación (tanto si se consiguió enviar la evidencia como si no) el histórico se actualiza y los datos acreditativos de las operaciones y su éxito o fracaso se salvan en el espacio protegido del testigo digital.

La figura 8 muestra la figura 6 adecuada al uso de credenciales vinculantes con los casos expuestos en el apartado referido a delegación de identidad y firma de evidencias electrónicas (FD, DbW, PK). También se muestran tres funciones que realizaría, como mínimo, el Gestor EE: obtención de evidencias, almacenamiento (y borrado) de evidencias, y transmisión de evidencias. Este ejemplo más específico muestra también que sería deseable que el rol del dispositivo (p.ej. el nivel de delegación) sea almacenado en el elemento seguro, junto con el contrato establecido por el gestor contractual. Como mínimo, la prueba del contrato establecido con el usuario para el uso del dispositivo personal como testigo digital debe incluir el rol con el que el dispositivo participará en las comunicaciones.

Cabe destacar que, al margen de los ejemplos específicos mostrados para la implementación de las credenciales vinculantes, el esquema de testigo digital seguiría siendo

válido para otros mecanismos que permitan establecer credenciales vinculantes que ayuden a definir de forma unequívoca las relaciones entre los usuarios, los dispositivos y las evidencias electrónicas.

Interacción opcional entre componentes, componentes opcionales y ampliaciones

Gestor contractual

El caso (A) detallado en el apartado anterior puede mejorarse por medio del uso del componente opcional *Gestor Contractual* para establecer las políticas para el gestor de evidencias electrónicas de objetos. Si el gestor contractual es empleado para dicho caso, delegamos parte de la decisión sobre las opciones de configuración al gestor contractual. El caso (A) quedaría redefinido como la *obtención de recomendaciones sobr e mecanism os criptográficos y configuraciones aceptables para la gestión de evidencias electrónicas* (figura 9).

En este escenario, la interactuación se produce entre el gestor contractual y el Gestor EE. El primero indicaría al segundo las configuraciones aceptables para que la gestión de evidencias electrónicas se realice conforme a los niveles de seguridad estipulados por normas comúnmente aceptadas y el marco legal. Inicialmente, el testigo digital puede ser configurado con las políticas por defecto definidas por el Gestor EE, y, bajo petición de un custodio autenticado podría actualizar estas políticas según la asociación de seguridad establecida con el custodio. Esta actualización de políticas de GP2 puede ser requerida en cualquier momento, y, de influir en los términos de servicio, o cualquier otro factor detallado en el resto de políticas, sería comunicado al usuario para su aceptación.

Aunque el uso del gestor contractual es opcional para no limitar la usabilidad del testigo digital, es aconsejable su uso ya que el gestor contractual puede ayudar a optimizar los mecanismos seleccionados dependiendo del dispositivo y el contexto. Las asociaciones de seguridad (SA) acordadas entre el gestor de evidencias electrónicas para objetos y el gestor contractual se almacenarían en el testigo digital, y en el emisor de las SAs, así como también se recomienda el registro de la evidencia de esta colaboración entre los componentes.

Uso de mecanismos biométricos como parte del Gestor de Operaciones Usuario-Dispositivo

Como puede verse en las figuras 7 y 9, otro elemento opcional dentro de nuestra arquitectura es el uso de sistemas biométricos para probar la presencialidad del usuario. Dicho elemento puede utilizarse dentro del caso (B) (figura 7) antes de la creación de las credenciales vinculantes, o dentro del caso (C) (figura 7) durante el proceso de recogida y/o envío de evidencias. La forma en la que dichos sistemas biométricos se utilizan viene definida dentro de las configuraciones aceptables, que deben definir como mínimo i) el tipo de sistema biométrico a utilizar (p.ej. huella dactilar, iris, voz), ii) las combinaciones esperadas de sistemas biométricos, y iii) las características que debe cumplir la implementación del sistema biométrico. Estas configuraciones pueden especificarse de forma estática, o de forma dinámica en aquellas arquitecturas que dispongan del componente opcional *Gestor Contractual*.

Esta interacción opcional se realiza principalmente entre el usuario y el Gestor de Operaciones Usuario-Dispositivo (figura 10). Antes de realizar cualquier operación que requiera de la presencia del usuario, éste debe indicar al Gestor de Operaciones su disponibilidad (p.ej. respondiendo a una alerta del Gestor de Operaciones). En este punto el Gestor de Operaciones pedirá al Usuario que se autentique mediante los sistemas biométricos indicados en las configuraciones aceptables. El Usuario utilizará dichos sistemas biométricos, y si todos los resultados son correctos el Gestor de Operaciones continuará con las operaciones previstas.

Al ser parte de las políticas del testigo digital, el uso de mecanismos biométricos queda registrado como evidencia una vez que el usuario da su consentimiento a los términos del servicio. Pero, además, quedan rastros del uso de sistemas biométricos cada vez que una operación requiere la aprobación del usuario (p.ej. la prueba enviada por el usuario en la figura 10 sería parte integral de la evidencia a almacenar). El uso de pruebas biométricas puede quedar evidenciado empleándose desde un simple registro hasta información biométrica (p.ej. la imagen de la huella dactilar utilizada en ese momento) en aquellos mecanismos que lo permitan.

Respecto al uso de un sistema biométrico, cabe puntualizar la naturaleza de éstos datos. A día de hoy, la mayoría de los sistemas biométricos permiten almacenar información sobre un usuario que usará el dispositivo (p.ej. "*Touch ID*" de Apple [30]), pero nada garantiza que el usuario registrado en el dispositivo sea el mismo que el usuario que efectuó el proceso de las credenciales vinculantes. Este dato es relevante, porque son las credenciales vinculantes las que determinan el responsable final de la evidencia. El caso de la existencia de múltiples usuarios que pueden hacer uso del dispositivo por tanto requiere una consideración especial.

La figura 11 muestra diferentes casos de uso del dispositivo digital:

(1). Básico. Comportamiento por defecto del testigo digital sin el uso de biométricos.

(2). Biométrico fuerte (cotejado localmente). El dato biométrico fue cotejado localmente en un paso previo al envío. El dispositivo guarda el resultado de la verificación como prueba.

(3). Biométrico débil (no cotejado). El dato biométrico se aporta como prueba adicional a la evidencia, pero debe ser cotejado o autenticado por la entidad remota que recibe la evidencia.

Si se quiere responsabilizar a un usuario concreto del envío de las evidencias electrónicas, la información biométrica proporcionada por el usuario (p.ej. su huella dactilar) debe ser cotejada con una fuente legalmente válida (p.ej. la huella dactilar almacenada en un DNI-e) para establecer una vinculación robusta.

En el caso (2) la prueba biométrica es cotejada localmente empleando un elemento que pueda validar la prueba respecto a la identidad del individuo (p.ej. empleando un DNI-e para validar la huella dactilar del DNI-e respecto a la huella que el testigo identifique como huella del usuario). De esta forma, los usos sucesivos del sistema biométrico quedan validados antes de su uso. Cuando el usuario autoriza el envío de evidencias usando un mecanismo biométrico cotejado, el sistema reconoce antes del envío de la prueba que el usuario que autorizó la acción es el mismo que estableció las credenciales vinculantes.

También debe considerarse el supuesto en el que la prueba biométrica no sea cotejada localmente (caso (3)). Esto implica que posteriormente la entidad que procese la evidencia deberá cotejar la prueba proporcionada por el mecanismo biométrico (p.ej. la huella digital) con las bases de datos existentes para identificar al individuo que autorizó el envío de la evidencia. En este caso, el testigo digital no podría asegurar que el usuario que autoriza el envío sea el mismo usuario que estableció las credenciales vinculantes.

Por último, consideramos un tercer supuesto, y es que en el contrato inicial entre el usuario y el gestor de operaciones usuario-dispositivo para el uso del testigo digital, el usuario que establece las credenciales vinculantes pueda autorizar el uso del testigo a otros usuarios. Para ello, el usuario vinculado debería indicar los datos personales (identidad) de aquellos otros usuarios que vayan a hacer uso del testigo digital, así como otros datos que se consideren

relevantes en base al contexto (p.ej. los datos biométricos cotejados de los individuos autorizados). Esta información se proporcionará a las autoridades pertinentes para facilitar el tratamiento automatizado de las evidencias.

Otra opción que añadiría complejidad al esquema de testigo digital es permitir la activación simultánea de múltiples credenciales vinculantes, una por cada usuario. Aunque añadiría complejidad, considerar diferentes credenciales vinculantes puede proporcionar independencia entre las acciones de los usuarios. En el caso anterior, el responsable final es el usuario que estableció las credenciales vinculantes, ya que es el que da su consentimiento para el uso del dispositivo como testigo digital y el que registra a los usuarios.

Referencias

[1] Une 71505: Tecnologías de la información (ti). sistema de gestión de evidencias electrónicas (sgee). *Tecnología de la Información*, 2013.

[2] Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra. A survey on security for mobile devices. *Communications Surveys & Tutorials, IEEE*, 15(1):446–471, 2013.

[3] Edewede Oriwoh, David Jazani, Gregory Epiphaniou, and Paul Sant. Internet of things forensics: Challenges and approaches. In *Collaborative Computing: Networking, Applications and Worksharing (Collaborat ecom), 2013 9th International Conference Conference on*, pages 608–615. IEEE, 2013.

[4] RC Hegarty, DJ Lamb, and A Attwood. Digital evidence challenges in the internet of things. In *Proceedings of the T enth In ternational Network Conference (INC 2014)* , page 163. Lulu. com, 2014.

[5] S Omeleze and HS Venter. Towards a model for acquiring digital evidence using mobile devices. In *Proceedings of the Tenth International Network Conference (INC 2014)*, page 173. Lulu. com, 2014.

[6] Eoghan Casey, Greg Back, and Sean Barnum. Leveraging cybox^{TM} to standardize representation and exchange of digital forensic information. *Digital Inves tigation*, 12:S102–S110, 2015.

[7] Tomás Marqués Arpa and Jordi Serra Ruiz. Cadena de custodia en el análisis forense. implementación de un marco de gestión de la evidencia digital. In *XIII Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2014)*. Universidad de Alicante, 2014.

[8] Yudi Prayudi, Ahmad Ashari, and Tri K Priyambodo. Digital evidence cabinets: A proposed frameworks for handling digital chain of custody. *Int. J. Comput. Appl* , 109(9):30–36, 2014.

[9] Yudi Prayudi and SN Azhari. Digital chain of custody: State of the art. *International Journal of Computer Applications*, 114(5), March 2015.

[10] Ingo Friese, Jorg Heuer, and Ning Kong. Challenges from the identities of things: Introduction of the identities of things discussion group within kantara initiative. In

Internet of Things (WF-IoT), 2014 IEEE World Forum on, pages 1–4. IEEE, 2014.

[11] Cory Altheide and Harlan Carvey. *Digital Forensics with Open Source Tools: Using Open Source Platform Tools for Performing Computer Forensics on TargetSystems: Windows, Mac, Linux, Unix, etc*. Elsevier, 2011.

[12] Eoghan Casey. *Digital evidence and computer crime:forensic science, computers and the internet*. Academic press, 2011.

[13] Ray Hunt and Jill Slay. Achieving critical infrastructure protection through the interaction of computer security and network forensics. In *Privacy Security and Trust (PST) , 2010 Eighth Annual International Conference on*, pages 23–30. IEEE, 2010.

[14] Irfan Ahmed, Sebastian Obermeier, Martin Naedele, and Golden G Richard III. Scada systems: Challenges for forensic investigators. *Computer*, (12):44–51, 2012.

[15] Tcg tpm 2.0 automotive, committee draft. Technical report, Trusted Computing Group (TCG), 2014.

[16] Raul Sanchez-Reillo, Daniel Sierra-Ramos, Roberto Estrada-Casarrubios, and Jose A Amores-Duran. Strengths, weaknesses and recommendations in implementing biometrics in mobile devices. In *Security T echnology (ICCST), 2014 International Carnahan Conference on*, pages 1–6. IEEE, 2014.

[17] Rick Ayers, Sam Brothers, and Wayne Jansen. Sp 800-101 rev. 1, guidelines on mobile device forensics. Technical report, Gaithersburg, MD, United States, 2014.

[18] Víctor Gayoso Martinez, Luis Hernández Encinas, Antonio Martín Muñoz, and Juan Ignacio Sanchez García. Identification by means of a national id card for wireless services. In *2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, pages 1–5, June 2013.

[19] Alexandra Boldyreva, Adriana Palacio, and Bogdan Warinschi. Secure proxy signature schemes for delegation of signing rights. *Journal of Cryptology*, 25(1):57–115, 2012.

[20] He Debiao, Chen Jianhua, and Hu Jin. An id-based proxy signature schemes without bilinear pairings. *Annals of Telecommunications*, 66(11–12):657–662, 2011.

[21] 3GPP TS 33.221: Support for Subscriber Certificates. http://www.3gpp.org/DynaReport/33221.htm. Accessed on April 2015.

[22] STORK2: Secure Identity Across Borders Linked. https://www.eid-stork2.eu/. Accessed on April 2015.

24

[23] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. Security, privacy and trust in internet of things: The road ahead. *Computer Networks*, 76(0):146–164, 2015.

[24] Marc Barisch. Design and evaluation of an architecture for ubiquitous user authentication based on identity management systems. In *2011 IEEE 10th International Conference on Trust, Security and Privacy in Co mputing and Communications (TrustCom)* , pages 863–872, Nov 2011.

[25] John Lyle, Andrew Paverd, Justin King-Lacroix, Andrea Atzeni, Habib Virji, Ivan Flechais, and Shamal Faily. Personal pki for the smart device era. In Sabrina De Capitani di Vimercati and Chris Mitchell, editors, *Public Key In frastructures, Servic es an d Applications*, volume 7868 of *Lecture Notes in Computer Science*, pages 69–84. Springer Berlin Heidelberg, 2013.

[26] Seyed Amir Hoseini-Tabatabaei, Alexander Gluhak, and Rahim Tafazolli. A survey on smartphone-based systems for opportunistic user context recognition. *ACM Comput ing*

Surveys, 45(3):27:1–27:51, Jul 2013.

[27] Liam M. Mayron. Biometric authentication on mobile devices. *IEEE Security and Privacy*, 13(3):70–73, May 2015.

[28] Syed Rahat and Wayne Browning. Methods and systems for secure communications between client applications and secure elements in mobile devices, December 2 2014. US Patent 8,904,195.

[29] David T Haggerty, Ahmer A Khan, Christopher B Sharp, Jerrold Von Hauck, Joakim Linde, Kevin P McLaughlin, ZIAT Mehdi, and Yousuf H Vaid. Apparatus and methods for secure element transactions and management of assets, February 6 2014. US Patent App. 14/174,791.

[30] About Touch ID security on iPhone and iPad. https://support.apple.com/en-us/HT204587. Accessed on July 2015.

REIVINDICACIONES

1. Dispositivo para la gestión segura de evidencias electrónicas con credenciales vinculantes (testigo digital) sobre el que el usuario u objeto que obtiene, genera o recibe evidencias delega su identidad de forma vinculante e indisoluble mediante credencias vinculantes, y caracterizado por que comprende:
   a. Un *gestor de operaciones entre el usuario u objeto y el dispositivo*, responsable de establecer las políticas que relacionan al usuario u objeto con el objetivo y que permite vincular la identidad de un usuario u objeto con su dispositivo generándose al menos una credencial vinculante (*binding credential,* BD);
   b. un núcleo de confianza, responsable de asegurar la integridad de la evidencia electrónica, impedir el acceso no autorizado y permitir su transferencia a una entidad autorizada, y que comprende a su vez:
      1. Mecanismos criptográficos aceptados dentro de un elemento seguro (chip *hw*, *anti-tampering*) para establecer un canal de comunicaciones seguro; y
      2. medios de almacenamiento seguro con control de acceso, protegidos en un elemento seguro (puede ser el mismo elemento seguro que el que contiene los mecanismos criptográficos u otro distinto), para almacenar claves y otros datos protegidos, por ejemplo los *hashes* de las evidencias electrónicas y las credenciales vinculantes; y
   c. un *gestor de evidencias electrónicas para objetos*, que coordina las operaciones (y establece las políticas a aplicar sobre dichas operaciones) de adquisición o generación de evidencias electrónicas, almacenamiento seguro, transferencia de la evidencia electrónica a otro testigo de la cadena, y, en su caso, de borrado o eliminación de evidencias.

2. Dispositivo según la reivindicación anterior caracterizado por que el *gestor de operaciones entre el usuario u objeto y el dispositivo* demanda al usuario u objeto que se autentique mediante mecanismos de autenticación basados en contexto o, en el caso de un usuario, mediante sistemas biométricos.

3. Dispositivo según cualquiera de las reivindicaciones anteriores caracterizado por que los mecanismos criptográficos son utilizados por el *gestor de operaciones entre el usuario u objeto y el dispositivo*.

4. Dispositivo según cualquiera de las reivindicaciones anteriores caracterizado por que los mecanismos criptográficos que integra el elemento seguro para establecer un canal de comunicaciones seguro se escogen de entre las siguientes tecnologías: Algoritmos de clave simétrica (2TDEA, 3TDEA, AES l28bits-256 bits), firmas electrónicas y aplicaciones *hash* (SHA224/ 256/ 384/ 512), HMAC, funciones de derivación de claves, generación de números aleatorios (SHA1/ 224/ 256/ 384/ 512).

5. Dispositivo según cualquiera de las reivindicaciones anteriores caracterizado por que comprende además un *gestor contractual* , que permite indicar al testigo digital los mecanismos criptográficos y la configuración más robusta aceptable para la adquisición de evidencias.

6. Procedimiento para la gestión segura de evidencias electrónicas con credenciales vinculantes caracterizado por que hace uso de dos o más dispositivos conforme cualquiera de las reivindicaciones anteriores y por que comprende las siguientes etapas:
    1. Establecimiento de los mecanismos criptográficos, configuraciones y políticas que conforman el conjunto de asociaciones de seguridad (SA, *Security Associations*) del testigo digital mediante el *gestor de operaciones entre el usuario u objeto y el testigo digital* y mediante el *gestor de evidencias electrónicas*, asociaciones de seguridad que, una vez establecidas son salvaguardadas como evidencias electrónicas;
    2. Delegación vinculante e indisoluble de la identidad del usuario u objeto hacia el dispositivo electrónico (testigo digital o custodio digital -esto es, un testigo digital con más privilegios-) que permite la obtención o generación de la evidencia mediante credenciales vinculantes, dichas credenciales vinculantes (claves, *tokens*) generadas mediante el *gestor de operaciones entre el usuario u objeto y el testigo digital* haciendo uso de mecanismos criptográficos aceptados

y salvaguardadas mediante medios de almacenamiento seguro protegidos en un elemento seguro del testigo digital;

3. Cuando un usuario u objeto obtiene la evidencia (1) conforme a las asociaciones de seguridad del testigo digital, se genera una cabecera con la información pertinente según un determinado *Formato de Evidencia Electrónica* (FEE), generándose un identificador de la evidencia a partir del identificador vinculante del dispositivo electrónico que la genera, y el estampillado de tiempo, comprendiendo dicha cabecera (i) datos relativos a qué implementación de elemento seguro se ha usado, o si no ha usado elemento seguro; (ii) información sobre la posible caducidad de la evidencia, (iii) datos para priorizar el almacenamiento de unas evidencias frente a otras, (iv) tipo de dispositivo que puede custodiar la evidencia, y (v) número de saltos o intermediarios de la evidencia;
4. La evidencia se firma en función del mecanismo escogido para la vinculación de la identidad y el valor probatorio se almacena (2) atendiendo a criterios de almacenamiento seguro, dicho valor probatorio consistiendo como mínimo en el valor *hash* de la evidencia firmada, dicho *hash* siendo generado mediante mecanismos criptográficos adecuados y registrado en los medios de almacenamiento seguro del testigo digital bien de forma directa bien a instancias del *gestor de evidencias electrónicas*, actualizándose en su caso el histórico de evidencias y verificándose la integridad de la evidencia si dicho valor *hash* coincide con el protegido en el medio de almacenamiento seguro;
5. si la evidencia ha de ser delegada, se escoge un testigo digital al que transmitir la evidencia (3), considerándose que, conforme a la política de transferencia de la evidencia, ésta ha de ser delegada cuando:

    i. A no es custodio digital. A debe transmitir la evidencia al menos una vez a un custodio,
    ii. El dispositivo alcanza un umbral de almacenamiento admitido (configurable),
    iii. La evidencia generada es de carácter crítico, o el tiempo de vida va a consumirse, o

iv. Si B tiene más posibilidades de alcanzar pronto el destino final y la transferencia no perjudica la vida de la evidencia más que si A la almacenase/custodiase;

y considerando la elección del siguiente testigo digital al cumplimiento de los siguientes requisitos:

rt1. B puede dar fe de que es un testigo digital y de su rol/nivel;

rt2. B es un testigo digital del mismo nivel que A, o A tiene nivel menor que B; es decir, el conjunto de parejas posibles es {(td, td), (cd, cd), (td, cd)}, con td: testigo digital, cd: custodio digital;

rt3. B satisface los criterios para salvaguardar la evidencia electrónica;

rt4. B es el candidato de mayor nivel de delegación de todos los posibles, o bien aquel candidato que ofrezca más garantías/probabilidad de que la evidencia alcance el destino final minimizando el pivotaje; o

rt5. B es un custodio digital y solicita el envío de las evidencias, y A puede verificar la identidad de B;

6. Una vez que se escoge el testigo B, la información sobre la evidencia electrónica se delega o envía a dicho testigo B (4) usando el FEE adaptado para la testificación digital, preferentemente a través un canal seguro estableciendo una *cadena de custodia digital* (CCD) por medio de pivotaje o delegación virtual de evidencias electrónicas;

7. B autentica la evidencia electrónica y procede a su almacenaje creando su propia evidencia para reflejar la recepción de esta evidencia en su histórico, enviando o no a A una prueba de que la recepción y el almacenamiento de que la evidencia ha sido posible (6):

i. Si B envía a A una prueba de que la recepción y el almacenamiento de que la evidencia ha sido posible (6), A lo registra en el histórico (conjunto de identificadores de las evidencias generadas y un código que indique si fue transmitida, y la garantía dada por el receptor en el paso

(6)), procediendo A a eliminar o no la evidencia conforme a las políticas de almacenamiento y borrado de evidencias del testigo digital;

ii. Si B no envía esta prueba, A lo registra el envío de la evidencia en el histórico (conjunto de identificadores de las evidencias generadas y un código que indique si fue transmitida) pero no la elimina.

7. Procedimiento según la reivindicación anterior caracterizado por que en el establecimiento de los mecanismos criptográficos, configuraciones y políticas que conforman el conjunto de asociaciones de seguridad (SA, *Security Associations*) del testigo digital también interviene el *gestor contractual*, actualizando a demanda (por ejemplo, de un custodio digital) la información sobre los mecanismos criptográficos, configuraciones y políticas definidos por el *gestor de evidencias electrónicas* , dicha información actualizada por el gestor contractual igualmente salvaguardada como evidencias electrónicas en los medios de almacenamiento seguro del testigo digital.

8. Procedimiento según cualquiera de las reivindicaciones 6 ó 7 caracterizado por que la delegación vinculante de la identidad del usuario u objeto hacia el dispositivo o dispositivos electrónicos que permiten la obtención o generación de la evidencia se realiza mediante una tarjeta SIM/UICC, un certificado identificativo digital, o mediante un sistema biométrico.

9. Procedimiento según la reivindicación anterior caracterizado por que para la delegación vinculante indisoluble de la identidad del usuario u objeto hacia el dispositivo o dispositivos electrónicos que permiten la obtención o generación de la evidencia mediante credenciales vinculantes el usuario u objeto dispone de un par de claves pública y privada, la clave privada protegida dentro de un chip de seguridad (por ejemplo, eSE) y la delegación vinculante indisoluble de la identidad se realiza mediante una primitiva criptográfica (*proxy signature*).

10. Procedimiento según la reivindicación anterior caracterizado por que para la delegación vinculante indisoluble de la identidad del usuario u objeto hacia el dispositivo o dispositivos electrónicos que permiten la obtención o generación de la evidencia

mediante credenciales vinculantes el usuario u objeto delega el uso de su clave privada al dispositivo para firmar las evidencias mediante dicho dispositivo.

11. Procedimiento según la reivindicación 9 caracterizado por que la delegación vinculante indisoluble de la identidad del usuario u objeto hacia el dispositivo o dispositivos electrónicos que permiten la obtención o generación de la evidencia mediante credenciales vinculantes comprende el uso de de un *token* (*warrant*), firmado con la clave privada del usuario u objeto, que indica la identidad del dispositivo y el periodo de validez de la delegación, entre otros datos, dicho *token* una vez proporcionado al dispositivo se adjuntaría a las evidencias firmándolo con su propia clave.

12. Procedimiento según la reivindicación 9 caracterizado por que la delegación vinculante indisoluble de la identidad del usuario u objeto hacia el dispositivo o dispositivos electrónicos que permiten la obtención o generación de la evidencia comprende la utilización de la clave privada del usuario u objeto para generar un par de claves privada y pública asociadas a la identidad del usuario u objeto, las cuales son utilizadas por el dispositivo para firmar las evidencias a la vez que permiten la comprobación de la identidad del usuario u objeto que generó las evidencias.

13. Procedimiento según cualquiera de las reivindicaciones anteriores caracterizado por que la cabecera que se genera cuando se obtiene la evidencia (1) y que contienen la información pertinente según un determinado *Formato de Evidencia Electrónica*(FEE), comprende los siguientes datos:

    a. Intercambio: versión, tamaño, identificador, organización, descripción, marca de tiempo, archivos totales, número de archivo, tamaño del archivo, formato del archivo, tipo de firma, tamaño de firma; y

    b. Obtención forense: versión, tamaño, identificador, creador, fecha de creación, fecha de obtención, archivos totales, número de archivo, tamaño de archivo, formato de archivo, tipo de dispositivo, modelo de dispositivo, número serie del dispositivo, número de sectores del dispositivo, primer sector, número de sectores de la evidencia, tipo de firma, tamaño de firma.

14. Procedimiento según la reivindicación anterior caracterizado por que la cabecera de la evidencia también comprende información del rol (nivel de delegación) del dispositivo.

15. Procedimiento según cualquiera de las reivindicaciones anteriores caracterizado por que el usuario u objeto delega su identidad de forma vinculante e indisoluble a más de un dispositivo electrónico, dichos dos o más dispositivos electrónicos comprendidos dentro de un mismo entorno de red de área personal (PAN) confiable.

16. Procedimiento según cualquiera de las reivindicaciones 7 a 15 caracterizado por que el usuario u objeto delega su identidad de forma vinculante e indisoluble a más de un dispositivo electrónico, dichos dos o más dispositivos electrónicos poseyendo su propio par de claves que son generadas por el usuario u objeto (por ejemplo, a través de un certificado de identificación electrónica tal como un DNI-e).

17. Procedimiento según cualquiera de las reivindicaciones anteriores caracterizado por que la presencia del usuario u objeto que genera o recibe la evidencia se ratifica mediante mecanismos de autenticación basados en contexto o mediante sistemas biométricos.

18. Procedimiento según la reivindicación anterior caracterizado por que antes de realizar cualquier operación que requiera de la presencia del usuario u objeto, éste debe indicar al *gestor de operaciones* su disponibilidad (por ejemplo respondiendo a una alerta del *gestor de operaciones*) cuando dicho *gestor de operaciones* demanda al usuario u objeto que se autentique mediante mecanismos de autenticación basados en contexto o, en el caso de un usuario, mediante sistemas biométricos conforme a las asociaciones de seguridad establecidas para el testigo digital, de forma que si la autenticación es correcta, lo que queda registrado como evidencia, el *gestor de operaciones* continúa con las operaciones previstas.

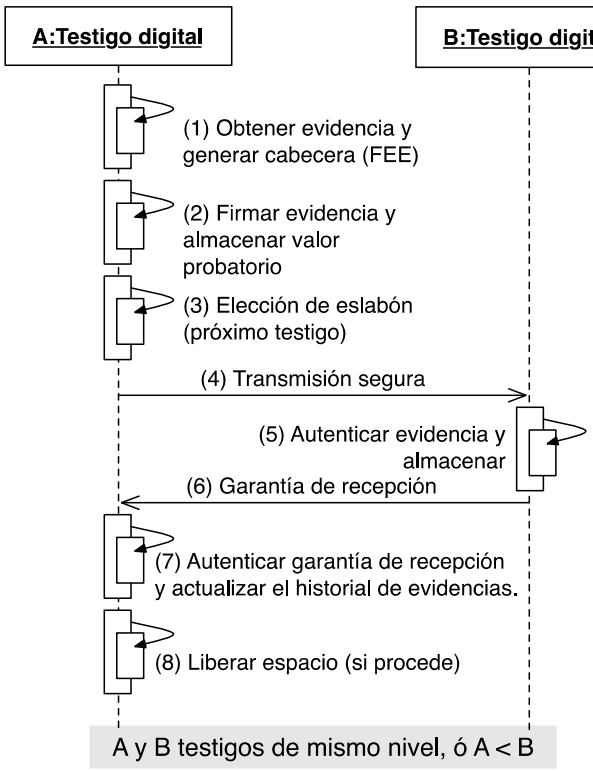
19. Procedimiento según la reivindicación anterior caracterizado por que la autenticación mediante mecanismos de autenticación basados en contexto o, en su caso (usuario, no objeto), mediante sistemas biométricos conforme a las asociaciones de seguridad establecidas para el testigo digital se realiza localmente en un paso previo al envío de la

evidencia a delegar, guardándose el resultado de la verificación como prueba y validando el uso de dichos mecanismos de autenticación basados en contexto o de dichos sistemas biométricos antes de cada uso sucesivo de los mismos.

20. Procedimiento según la reivindicación 18 caracterizado por que la autenticación mediante mecanismos de autenticación basados en contexto o, en su caso (usuario, no objeto), mediante sistemas biométricos conforme a las asociaciones de seguridad establecidas para el testigo digital se aporta como prueba adicional a la evidencia pero debe ser cotejado o autenticado por el testigo digital que recibe la evidencia recurriendo a bases de datos existentes que permiten la identificación del usuario u objeto que envía o delega la evidencia como el mismo usuario u objeto que estableció las credenciales vinculantes.

21. Procedimiento según cualquiera de las reivindicaciones 7 a 20 caracterizado por que el usuario u objeto que establece las credenciales vinculantes autoriza el uso del testigo digital a otros usuarios u objetos mediante mecanismos de autenticación basados en contexto o mediante sistemas biométricos asociados a dichos otros usuarios u objetos.

22. Procedimiento según cualquiera de las reivindicaciones 7 a 20 caracterizado por que el usuario u objeto que establece las credenciales vinculantes activa simultáneamente credencias vinculantes para otros usuarios u objetos (una credencial vinculantes por usuario u objeto).



Testigo digital	Robustez por defecto (menos: 1, más: 8)	Nivel de delegación
Civil R	1	1
Custodio R	4	2
Custodio LR Móvil	6	3
Custodio NR Fijo	8	4

R: restringido en recursos.
LR: Levemente restringido en recursos.
NR: No restringido en recursos.

Figura 1

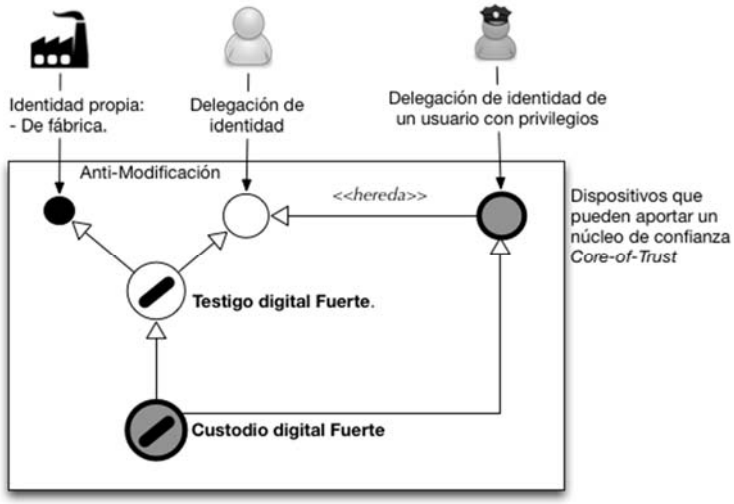


Figura 2

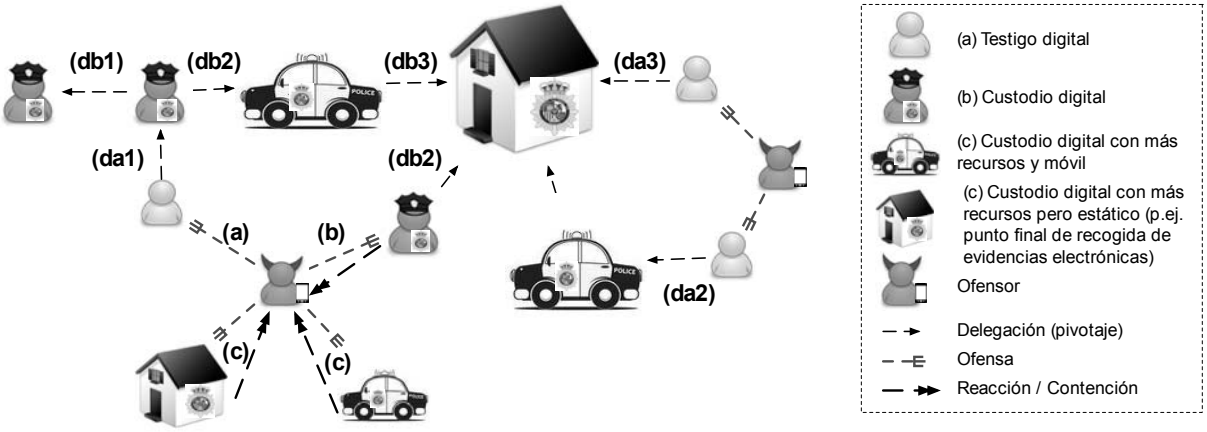


Figura 3

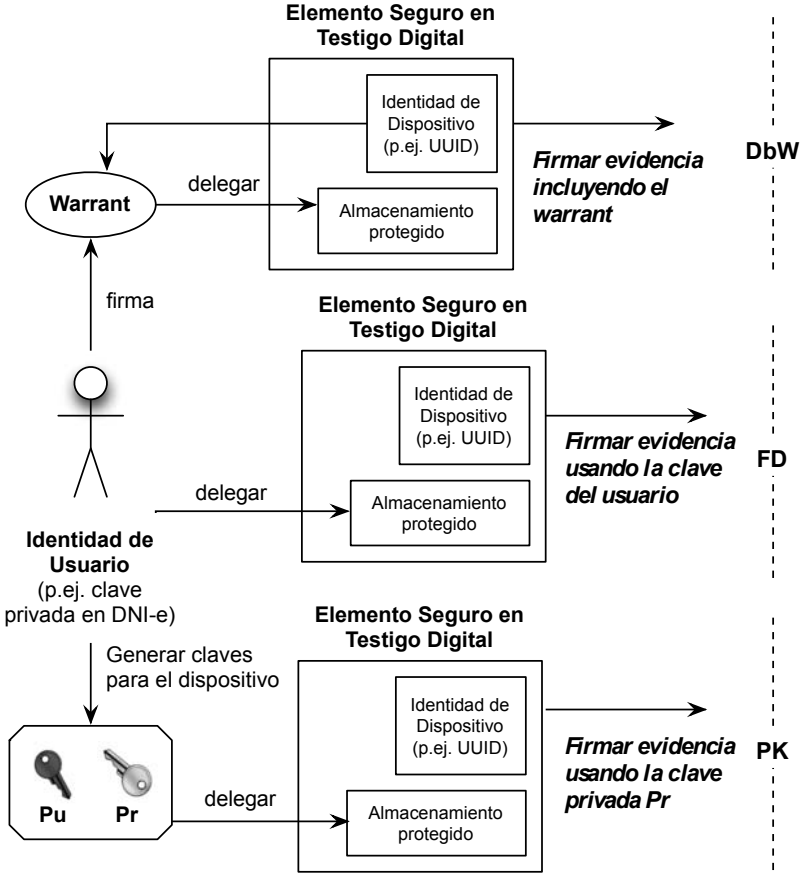


Figura 4

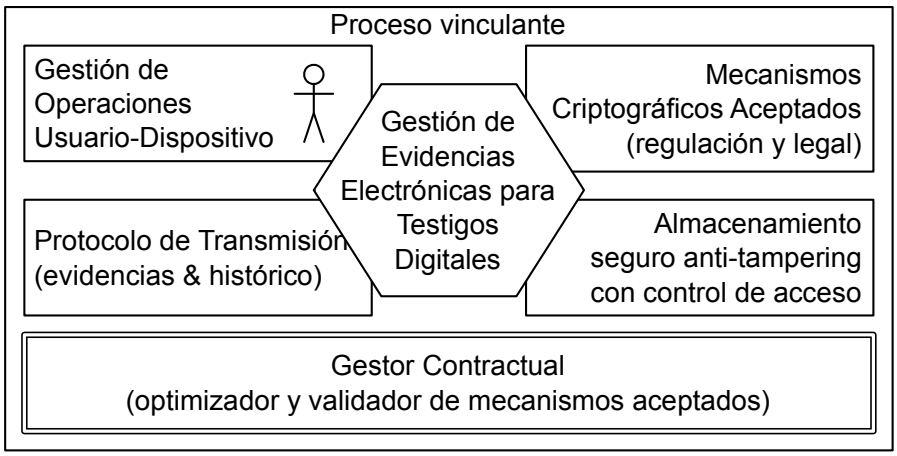


Figura 5

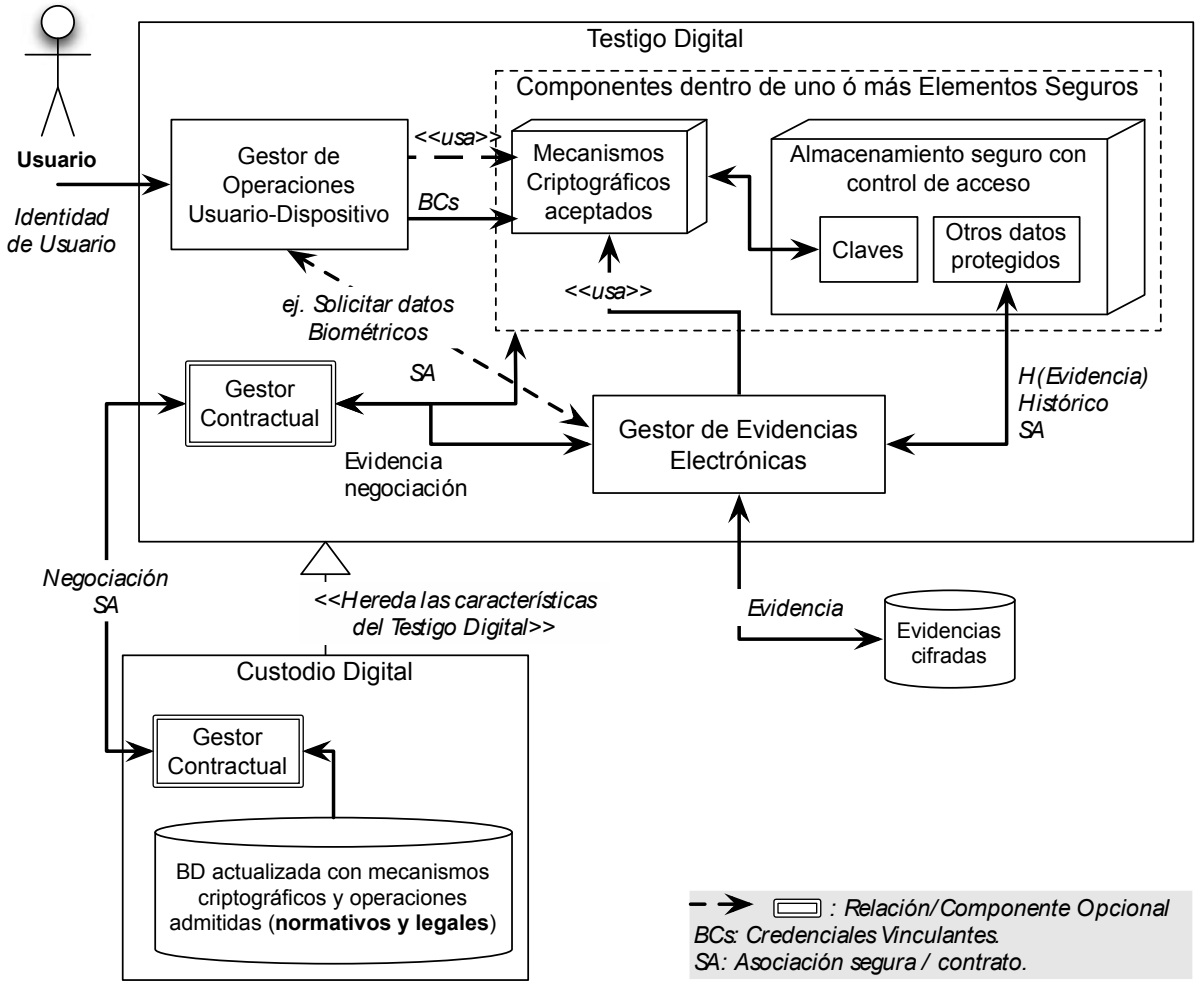


Figura 6

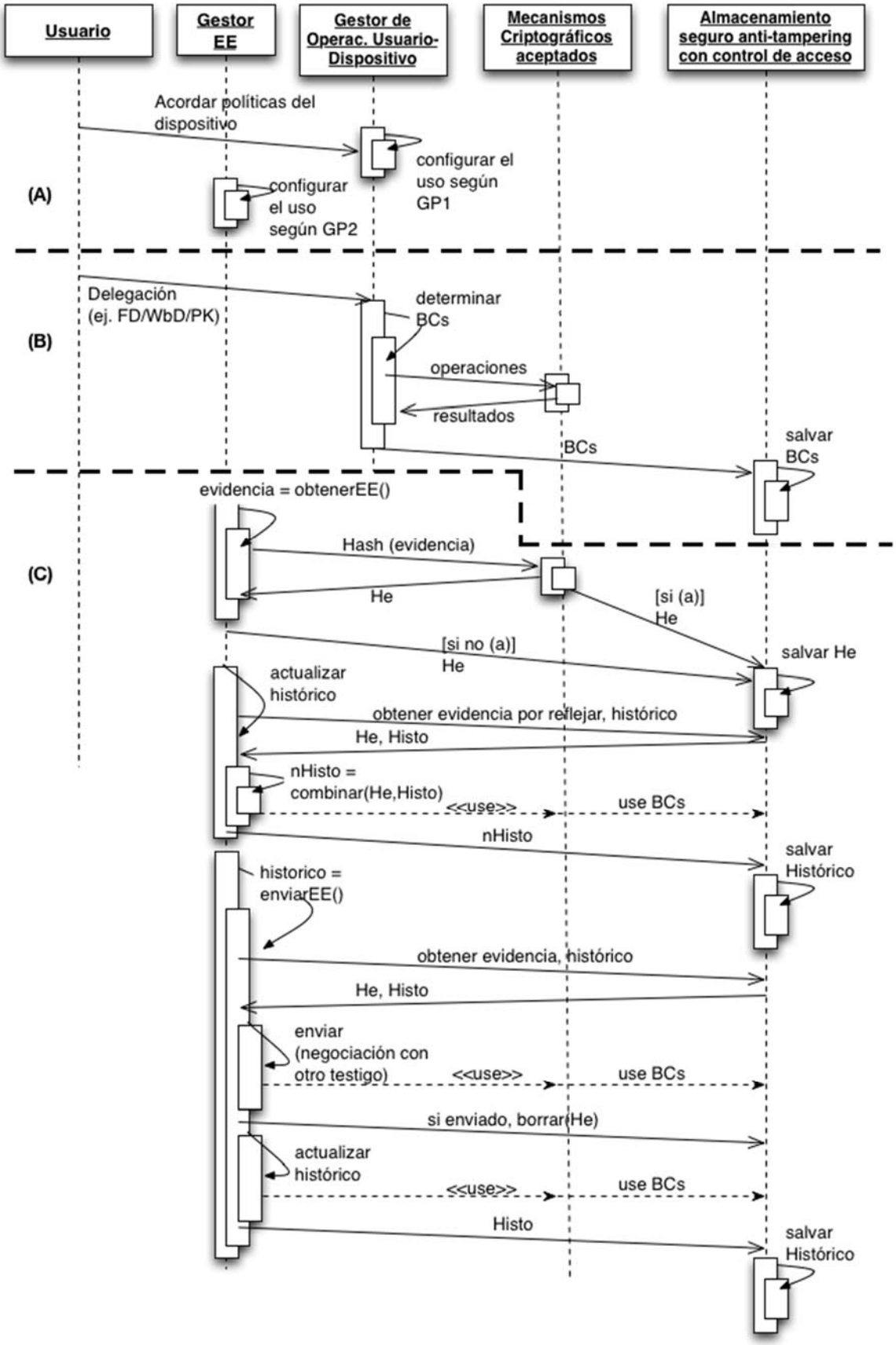

Usuario
Gestor EE
Gestor de Operac. Usuario-Dispositivo
Mecanismos Criptográficos aceptados
Almacenamiento seguro anti-tampering con control de acceso
Acordar políticas del dispositivo
configurar el uso según GP1
(A)
configurar el uso según GP2
Delegación (ej. FD/WbD/PK)
determinar BCs
(B)
operaciones
resultados
BCs
salvar BCs
evidencia = obtenerEE()
Hash (evidencia)
He
[si (a)] He
(C)
[si no (a)] He
salvar He
actualizar histórico
obtener evidencia por reflejar, histórico
He, Histo
nHisto = combinar(He,Histo)
<<use>>
use BCs
nHisto
salvar Histórico
historico = enviarEE()
obtener evidencia, histórico
He, Histo
enviar (negociación con otro testigo)
<<use>>
use BCs
si enviado, borrar(He)
actualizar histórico
<<use>>
use BCs
Histo
salvar Histórico

Figura 7

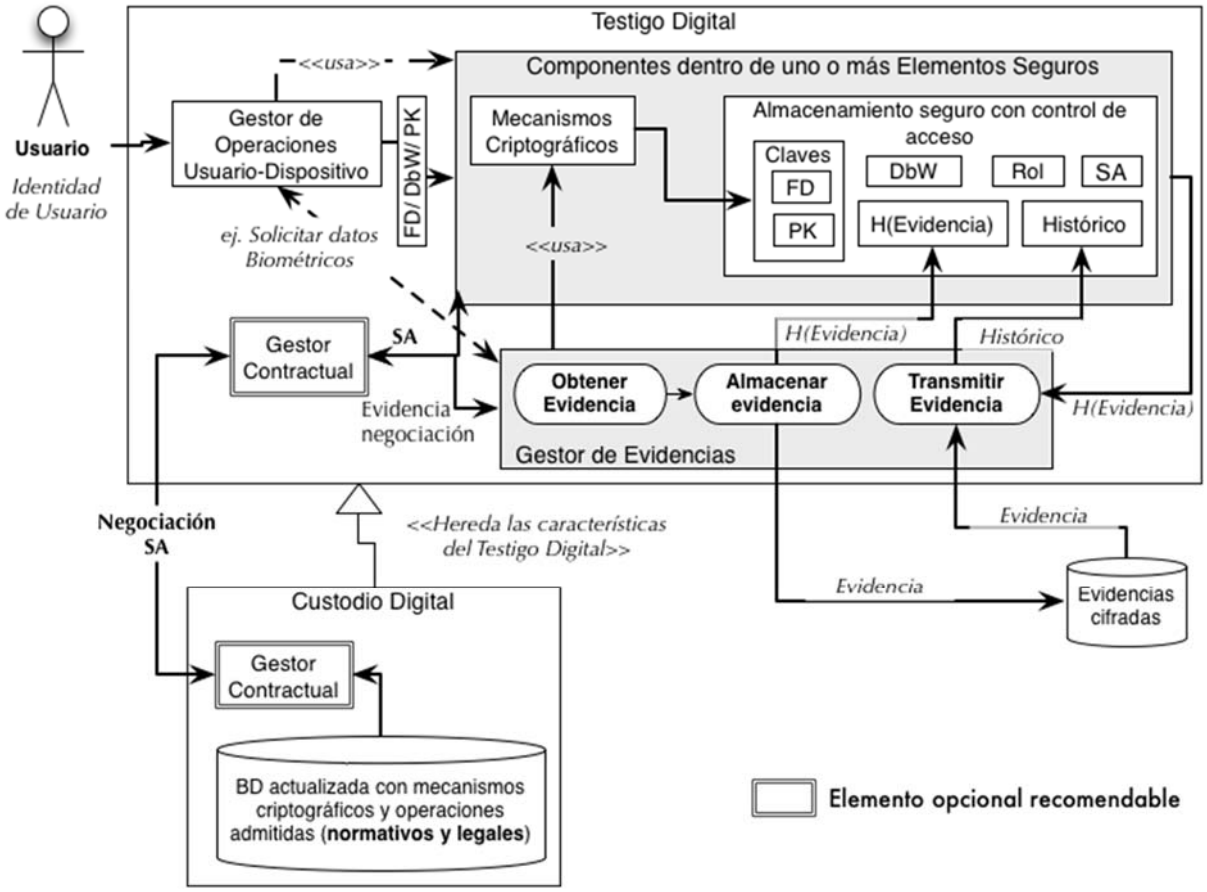


Figura 8

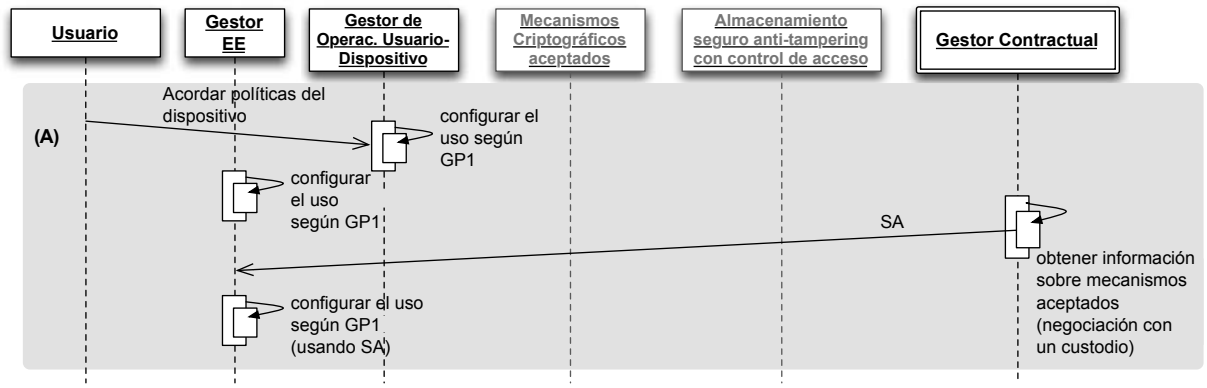


Figura 9

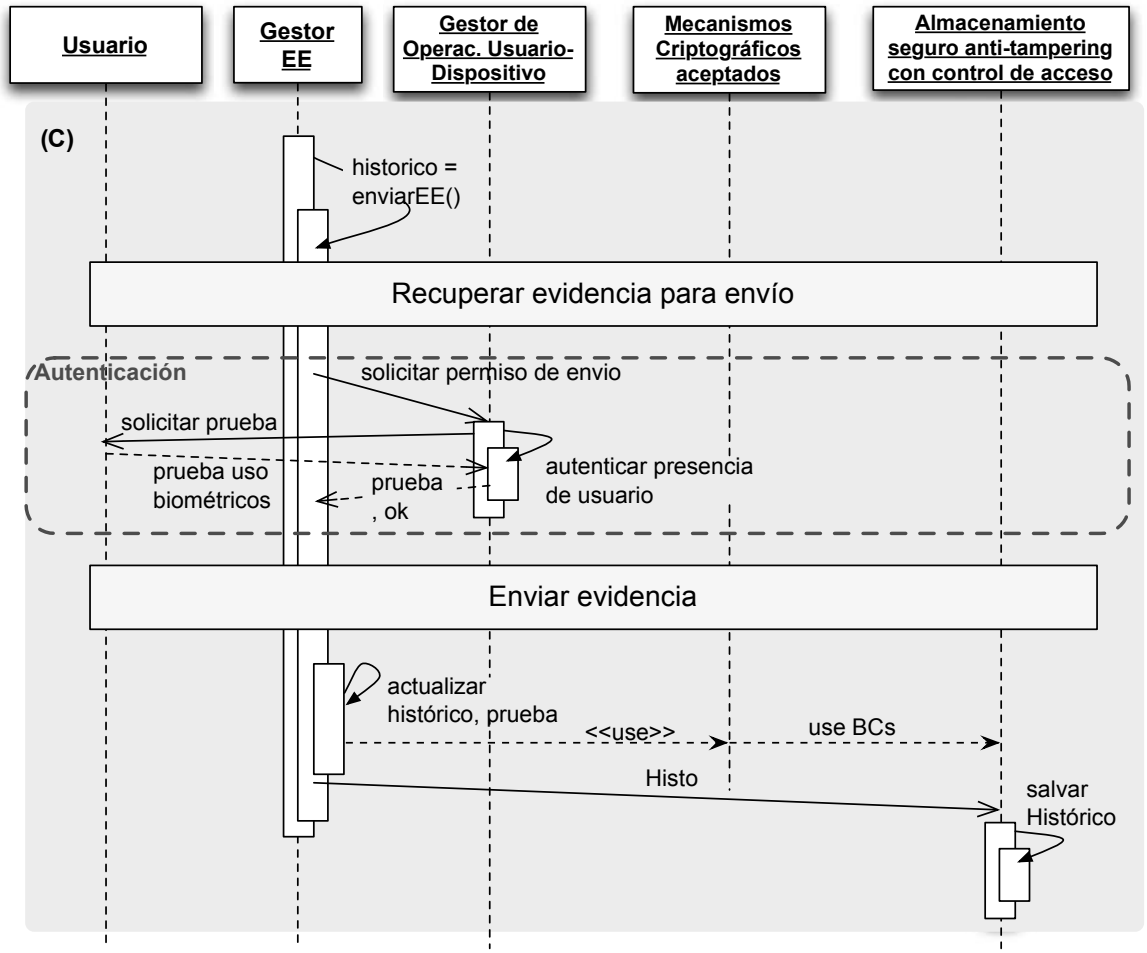

Usuario
Gestor EE
Gestor de Operac. Usuario-Dispositivo
Mecanismos Criptográficos aceptados
Almacenamiento seguro anti-tampering con control de acceso
(C)
historico = enviarEE()
Recuperar evidencia para envío
Autenticación
solicitar permiso de envio
solicitar prueba
prueba uso biométricos
prueba , ok
autenticar presencia de usuario
Enviar evidencia
actualizar histórico, prueba
<<use>>
use BCs
Histo
salvar Histórico

Figura 10

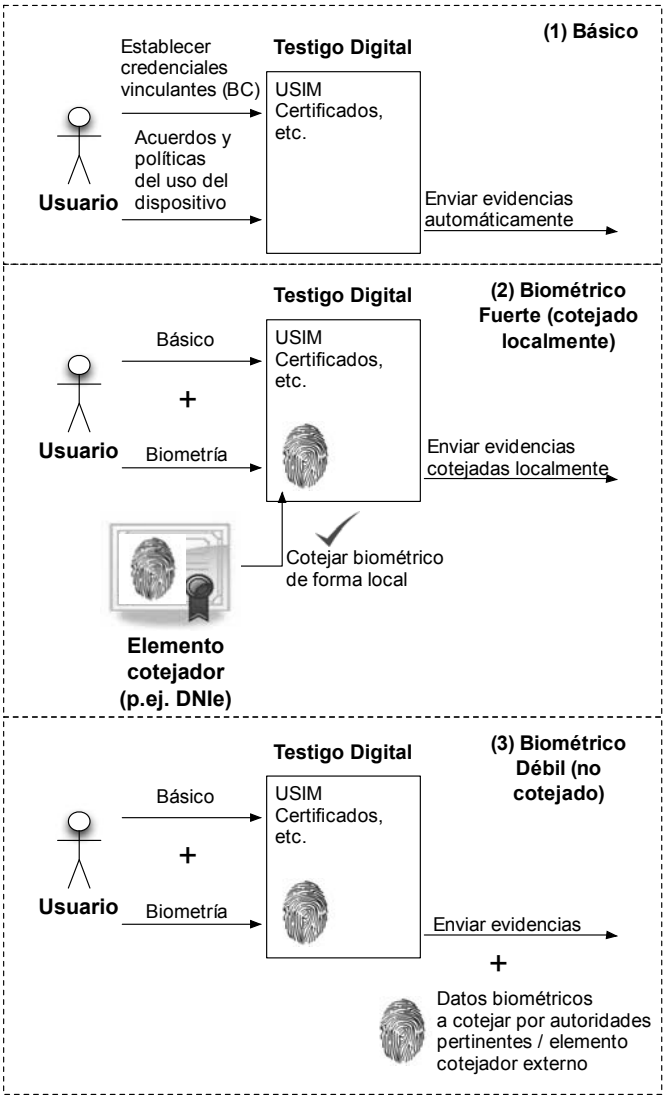

(1) Básico
Testigo Digital
Establecer credenciales vinculantes (BC)
USIM Certificados, etc.
Acuerdos y políticas del uso del dispositivo
Usuario
Enviar evidencias automáticamente
(2) Biométrico Fuerte (cotejado localmente)
Testigo Digital
Básico
USIM Certificados, etc.
+
Usuario
Biometría
Enviar evidencias cotejadas localmente
Cotejar biométrico de forma local
Elemento cotejador (p.ej. DNIe)
(3) Biométrico Débil (no cotejado)
Testigo Digital
Básico
USIM Certificados, etc.
+
Usuario
Biometría
Enviar evidencias
+
Datos biométricos a cotejar por autoridades pertinentes / elemento cotejador externo

Figura 11

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201500764

(22) Fecha de presentación de la solicitud: 22.10.2015

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***G06F21/00*** (2013.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
Y	ACCORSI R Safe-Keeping Digital Evidence with Secure Logging Protocols: State of the Art and Challenges.IT Security Incident Management and IT Forensics, 2009. IMF '09. Fifth International Conference on, 20090915 IEEE, Piscataway, NJ, USA 15/09/2009 VOL: Pags: 94 - 110 ISBN 978-0-7695-3807-5 ; ISBN 0-7695-3807-X	1-5
A		6-22
Y	HALBOOB WALEED et al. Data Warehousing Based Computer Forensics Investigation Framework.2015 12th International Conference on Information Technology - New Generations, 20150413 IEEE 13/04/2015 VOL: Pags: 163 - 168 Doi:10.1109/ITNG.2015.31	1-5
A		6-22
A	US 2015066785 A1 (FORTE DARIO V) 05/03/2015,	1-22
A	NICOLAI KUNTZE et al. Secure Digital Chains of Evidence.Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on, 20110526 IEEE 26/05/2011 VOL: Pags: 1 - 8 ISBN 978-1-4673-1242-4 ; ISBN 1-4673-1242-8 Doi:10.1109/SADFE.2011.16	1-22
A	ORIWOH EDEWEDE et al. Internet of Things Forensics: Challenges and approaches.9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, 20131020 ICST 20/10/2013 VOL: Pags: 608 - 615	1-22

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
14.10.2016	M. Muñoz Sanchez	1/5

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G06F

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI, XPIEE, XPI3E, NPL

Fecha de Realización de la Opinión Escrita: 14.10.2016

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-22	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones	6-22	**SI**
	Reivindicaciones	1-5	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	ACCORSI R Safe-Keeping Digital Evidence with Secure Logging Protocols: State of the Art and Challenges.IT Security Incident Management and IT Forensics, 2009. IMF '09. Fifth International Conference on, 20090915 IEEE, Piscataway, NJ, USA 15/09/2009 VOL: Pags: 94 - 110 ISBN 978-0-7695-3807-5 ; ISBN 0-7695-3807-X	15.09.2009
D02	HALBOOB WALEED et al. Data Warehousing Based Computer Forensics Investigation Framework.2015 12th International Conference on Information Technology - New Generations, 20150413 IEEE 13/04/2015 VOL: Pags: 163 - 168 Doi: 10.1109/ITNG.2015.31	13.04.2015
D03	US 2015066785 A1 (FORTE DARIO V)	05.03.2015
D04	NICOLAI KUNTZE et al. Secure Digital Chains of Evidence.Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on, 20110526 IEEE 26/05/2011 VOL: Pags: 1 - 8 ISBN 978-1-4673-1242-4 ; ISBN 1-4673-1242-8 Doi:10.1109/SADFE.2011.16	26.05.2011
D05	ORIWOH EDEWEDE et al. Internet of Things Forensics: Challenges and approaches.9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, 20131020 ICST 20/10/2013 VOL: Pags: 608 - 615	20.10.2013

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

Se considera D01 el documento más próximo del estado de la técnica al objeto de la solicitud.

Reivindicaciones independientes

Reivindicación 1: El documento D01, divulga una serie de protocolos de registro de eventos seguro para salvaguardar evidencias digitales (electrónicas). Una de las arquitecturas mencionadas incluye (ref. nº 28) dispositivos que detectan eventos y almacenan los correspondientes mensajes; en algunos casos el dispositivo los firma para la autenticación de la entidad. Dichos mensajes se envían a un recolector, firmados, cubriendo así en el sentido genérico expresado en la reivindicación 1, la operación de delegación de identidad y evidencia permitiendo la vinculación de la identidad de un usuario y su dispositivo (un gestor de operaciones entre el usuario y el dispositivo, en fin).
El documento D01, sin embargo, no detalla los aspectos de seguridad en el acceso a las evidencias, que impidan la manipulación, aunque fuera detectable y, por tanto, el problema técnico objetivo a la luz del documento D01, consistiría en garantizar que no se produzca dicha manipulación. El documento D02 por su parte plantea una infraestructura completa de control de acceso mediante certificados y mantenimiento de la integridad de evidencias, aplicando funciones hash (constituyendo un núcleo de confianza). La combinación de los gestores de los documentos D01 y D02, dada su compatibilidad, resultaría evidente para el experto en la materia así como la combinación del resto de características señaladas de ambos documentos. Por tanto, la combinación de los documentos D01 y D02 afecta a la actividad inventiva de la reivindicación 1 según el art. 8.1 de la Ley de Patentes.

Reivindicación 6: a diferencia de la reivindicación 1, la inclusión de la lógica de delegación de evidencias no queda cubierta por ninguno de los documentos D01 o D02 teniendo además el efecto de mejorar la gestión de evidencias. Por tanto, la reivindicación 6 tiene actividad inventiva según el art. 8.1 de la Ley de Patentes.

Reivindicaciones dependientes

Reivindicaciones 2-5: el contenido de estas reivindicaciones expresa solamente alternativas comúnmente conocidas en el estado de la técnica en el campo técnico de la solicitud (mecanismos autenticación, por contexto o biométrica; mecanismos criptográficos SHA, TDEA etc.; y su selección). Así, la combinación de los documentos D01 y D02 afecta a la actividad inventiva de las reivindicaciones 2-5 según el art. 8.1 de la Ley de Patentes.

Reivindicaciones 7-22: las reivindicaciones 7-22 tienen actividad inventiva según el art. 8.1 de la Ley de Patentes por depender de la reivindicación 6 que también la posee.