A. Nieto, R. Roman, and J. Lopez, "Arquitectura funcional para la cadena de custodia digital en objetos de la IoT", *XIV Reunión Española sobre Criptología y Seguridad de la Información*, pp. 168-173, 20XX.
XIV Reunión Española sobre Criptología y Seguridad de la Información
NICS Lab. Publications: https://www.nics.uma.es/publications

Arquitectura funcional para la cadena de custodia digital en objetos de la IoT

Ana Nieto, Rodrigo Román y Javier Lopez
Lenguajes y Ciencias de la Computación
Universidad de Málaga
Email: {nieto, roman, jlm}@lcc.uma.es

***Resumen*—En la Internet de los Objetos (IoT, por sus siglas en inglés), los ataques pueden ser perpetrados desde dispositivos que enmascaran su rastro ayudándose de la densidad de objetos y usuarios. Actualmente la idea de que los dispositivos de usuario almacenan evidencias que pueden ser muy valiosas para frenar ataques es bien conocida. Sin embargo, la colaboración de éstos para denunciar posibles abusos telemáticos aún está por definir. Los testigos digitales son dispositivos concebidos para definir la participación de dispositivos de usuario en una cadena de custodia digital. La idea es que las evidencias se generan, almacenan y transfieren siguiendo los requisitos marcados por las normas actuales (p.ej. UNE 71505), pero respetando las restricciones en recursos de los dispositivos. En este artículo proponemos una arquitectura funcional para la implementación del concepto de testigo digital en dispositivos de la IoT.**

***Palabras clave*—Cadena de custodia digital; Identidad de las cosas; Testigo digital.**

I. Introducción

La seguridad en redes siempre es un excelente caldo de cultivo para nuevos retos de investigación. Esto es así, porque la tecnología, los avances en informática, suelen ir un paso por delante de las medidas de seguridad necesarias para solventar los problemas desconocidos. Existe sin duda un riesgo tecnológico-humano; las máquinas fallan, los protocolos pueden introducir problemas de seguridad, y las personas nos equivocamos, mentimos y también falseamos. Y, detrás de todo esto, hay un componente de responsabilidad que en muchos casos es muy difícil de establecer.

Como no podía ser de otra forma, actualmente el marco de la ciberseguridad plantea suculentos retos de investigación para hacer frente al amplio abanico de amenazas que se cierne sobre las nuevas tecnologías de comunicación y socialización. Uno de esos retos es social, ya que los ciudadanos aún no son plenamente conscientes de la repercusión que los delitos telemáticos tienen en nuestra forma de vida. De hecho, el concepto de *delito telemático* en sí mismo es desconocido por gran parte de la población. Lejos de ser insignificantes, estos y otros factores, como la facilidad de perpetrar los ataques y ocultar el rastro de origen, amenazan la libertad de las personas físicas, porque finalmente estos delitos afectan a la confianza de las personas en las infraestructuras, y pueden ocasionar cuantiosas pérdidas económicas y personales cuando se dirigen hacia, por ejemplo, sistemas de monitorización críticos.

La Agencia de Seguridad en las Redes y de la Información de la Unión Europea (ENISA, *European Union Agency for Network and Information Security*) pone de manifiesto en el último informe [1] la importancia de recabar evidencias electrónicas de los dispositivos de los usuarios para aprender sobre los sucesos ocurridos, a posteriori, y así mejorar las políticas de actuación.

En general, la trazabilidad de los ataques no es nada simple, por lo que establecer responsabilidades sobre una acción delictiva telemática no es trivial. Sin embargo, aportar medidas para ello es necesario para evitar que el ciberdelincuente siga actuando y para desmotivar futuros ataques de otros infractores. Los dispositivos personales dificultan en gran medida la gestión de evidencias electrónicas por su heterogeneidad, densidad y sensibilidad, al almacenar datos de usuario. Al ser cada vez más potentes, estos dispositivos representan una nueva fuente de amenazas, pero también pueden ser un gran aliado para proteger los sistemas futuros.

Este es el núcleo en el que se sustenta la idea de *testigo digital* descrita en [2]; introducir los dispositivos personales en la gestión de evidencias electrónicas para desplegar cadenas de custodia digitales (CCD) dinámicas en aras de que actúen como testigos de un suceso. En este artículo ahondamos en este concepto y definimos una arquitectura para su implementación en dispositivos con elementos de seguridad embebidos.

La arquitectura propuesta servirá para responder a una pregunta crítica en la gestión de evidencias en la IoT no considerada hasta la fecha: cómo llevar las evidencias electrónicas desde su lugar de ocurrencia hasta su custodia haciendo uso de los propios dispositivos del entorno de forma segura y con garantías de no-repudio.

El artículo se estructura como sigue. La sección II presenta los antecedentes que motivan este trabajo. En la sección III enumeramos los requisitos de un testigo digital que serán considerados en la arquitectura, definida en la sección IV. Por último, la sección V sintetiza las principales conclusiones.

II. Antecedentes

La gestión de evidencias electrónicas (GEE) es un proceso muy delicado que comprende diferentes fases. En la norma UNE 71505 [3] se definen los procesos para la GEE dentro del ciclo de vida de la evidencia electrónica (CVEE), dividida en seis fases: generación, almacenamiento, transición, recuperación, tratamiento y comunicación. El modelo EDRM (*Electronic Discovery Reference Model*) [4] define nueve procesos,

divididos en seis niveles: gestión de la información, identificación, preservación | colección, procesamiento | revisión | análisis, producción y presentación.

Estos modelos comparten la necesidad de mantener la integridad de la evidencia electrónica, y su trazabilidad. Sin embargo, están orientados a sistemas para la GEE tradicionales, que no tienen por qué ser restringidos en recursos. En [5], los autores proponen el modelo ONW (*Online Neighbourhood Watch*) para emplear dispositivos móviles y otros objetos personales en la captura de evidencias electrónicas preservando la integridad de la evidencia electrónica. Sin embargo, al igual que otros modelos, la solución no involucra la colaboración con otros dispositivos restringidos en recursos, sino que depende de la conectividad con repositorios remotos. La integridad de las evidencias se basa en aplicar mecanismos criptográficos aceptados en las normas para la gestión actuales.

En [6] se define el concepto de IoT-Forensics, en el que el Cloud aparece como elemento intermediario en las comunicaciones entre los dispositivos.

En nuestro caso, los testigos digitales, definidos en [2], persiguen delegar la evidencia electrónica en un marco colaborativo, preservando su integridad. Para ello, extiende el concepto de *cadena de custodia digital* (CCD) que ya es conocido de trabajos previos [7], [8]. Precisamente, en [9], se propone un marco de trabajo para la gestión de CCDs, en el que aparece el TPM (*Trusted Platform Module*) como una de las herramientas bajo investigación. Las CCDs emplean mecanismos de cifrado especificados por las normas actuales para enviar las evidencias electrónicas. Sin embargo, aunque los dispositivos móviles forman parte de la adquisición de evidencias físicas, como por ejemplo imágenes (cf. [7]), envían las evidencias directamente a equipos con mayores recursos, y, normalmente, a través de Internet.

La extensión que en [2] se hace de la definición de CCD (denotada CCD-IoT) pretende que los dispositivos personales con arquitectura de seguridad embebida, y, siempre que satisfagan una serie de requisitos, sean capaces de colaborar para desplegar CCD más dinámicas. Así, los eslabones de una CCD-IoT son los testigos digitales.

III. Requisitos de un testigo digital

Un testigo digital es un dispositivo con arquitectura de seguridad embebida, que cuenta con un núcleo de confianza capaz de auto-delatarse y funcionalidad para participar en la gestión de evidencias electrónicas [2]. Actualmente no existe ningún dispositivo personal que pueda actuar como testigo digital, porque es un concepto nuevo. Este trabajo pretende sentar las bases para su implementación en un futuro.

Los requisitos básicos de un testigo digital listados a continuación pueden extraerse de [2]:

- R1 Contar con una arquitectura de seguridad embebida con núcleo de confianza.
- R2 Permitir establecer un responsable final de la acción.
- R3 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.

La arquitectura de seguridad embebida - requisito R1 - es necesaria para definir los procesos que permitan salvaguardar las evidencias electrónicas. Por otro lado, el requisito R2 es determinante para que los usuarios entiendan la repercusión y responsabilidad del uso de testigos digitales. Este requisito se consigue por medio del uso de credenciales vinculantes (BC, *Binding Credentials*), tal y como se describe en [2]. En particular, nosotros consideramos el uso de tres tipos de BC: *full delegation* (FD), *delegation by warrant* (DbW) y clave privada (PK). Por último, el requisito R3 se consigue por medio del (i) almacenamiento seguro que algunos chips de seguridad incorporan y (ii) el proceso de delegación vinculante descrito en [2].

El proceso de delegación vinculante es necesario atendiendo a los requisitos de los objetos de la IoT. Dado que la capacidad de almacenamiento seguro es muy restringida, la evidencia electrónica debe delegarse a otros testigos digitales lo antes posible. Pero, además, para permitir su trazabilidad y establecer el valor de responsabilidad en la GEE, la delegación de la evidencia se efectúa teniendo en cuenta al menos una BC, de ahí el nombre de *delegación vinculante*. Las BCs constituyen la prueba de que el usuario dio su consentimiento para el uso del dispositivo como testigo digital, y que el dispositivo actúa bajo la tutela del usuario. Este hecho tiene unas connotaciones que son detalladas en la sección IV.

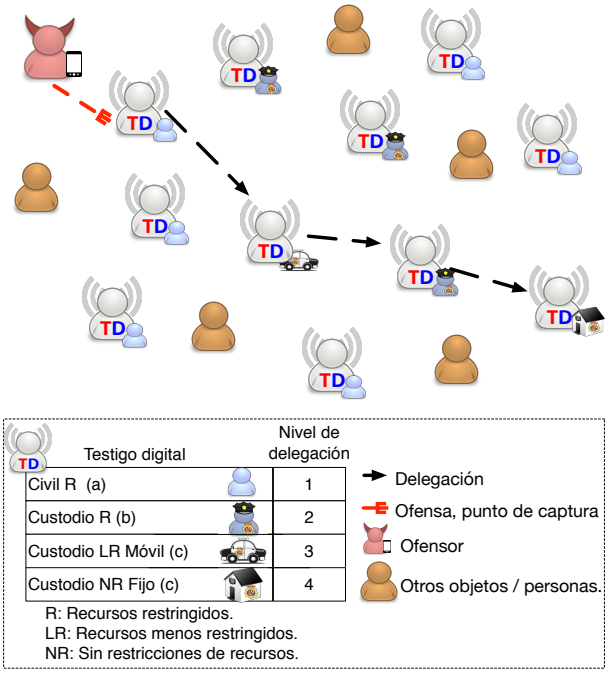

Figura 1. Testigos digitales.

Por último, la Figura 1 muestra un ejemplo de entorno donde existen testigos digitales capaces de recabar e informar de las evidencias electrónicas. Los testigos digitales no sólo dependen de la implementación de los requisitos anteriores o

de sus recursos computacionales, sino que, además, dependen del usuario que los porta para tener más o menos privilegios en la toma de decisiones. Así, de forma simplificada consideramos la división de los testigos digitales en dos perfiles que generan a su vez sub-perfiles dependiendo de los recursos.

- Testigo digital. Dispositivo que cumple los requisitos marcados acorde a la definición en [2] y que implementa la arquitectura descrita en la sección IV.
- Custodio digital. Testigo digital que pertenece a un usuario ó entidad con privilegios para la custodia formal de la evidencia (p.ej. un agente de la ley, una comisaría).

La idea tras este enfoque es, que los usuarios con privilegios previsiblemente pasarán cerca de una entidad con privilegios donde se puedan almacenar las evidencias electrónicas sin problemas de recursos. Por ello, el enfoque perseguido en [2] defiende que los testigos digitales deben delegar lo antes posible las evidencias, y, a ser posible, a testigos digitales de mayor nivel, ya sea por sus recursos, o privilegios. Cabe recordar que este enfoque se hace bajo la restricción de que los testigos digitales pueden auto-delatarse, en caso de no ser adecuados para la tranferencia de la evidencia electrónica.

IV. Arquitectura Funcional

En esta sección describimos la arquitectura funcional de un testigo digital basándonos en sus componentes. Cabe destacar, que la implementación de estos componentes dependerá de (i) las capacidades del dispositivo que actúe como testigo digital y (ii) el desempeño del testigo digital.

IV-A. Componentes funcionales

La Figura 2 muestra los componentes funcionales que implementará un dispositivo para actuar como testigo digital. Además, se ha destacado la parte correspondiente a las credenciales vinculantes (FD, BdW, PK) y otros conceptos estrechamente relacionados con el testigo digital descritos en la sección anterior.

A continuación describimos cada uno de los componentes.

IV-A1. 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 (BCs), que serán empleadas a lo largo del proceso de GEE. Además, proporcionaría opciones adicionales; p.ej. solicitar pruebas biométricas al usuario para la gestión de evidencias electrónicas.

IV-A2. 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.

IV-A3. 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.

IV-A4. 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). Se almacenarían claves y otros datos protegidos, como los hashes de las evidencias electrónicas, el contrato, y las credenciales vinculantes.

IV-A5. Gestor de evidencias electrónicas: Coordina las operaciones de adquisición de evidencias electrónicas, almacenamiento seguro, y transferencia de la evidencia electrónica a otro testigo de la cadena.

Cabe destacar, que el rol del dispositivo (p.ej. el nivel de delegación) podría ser otro valor almacenado en el elemento seguro, junto con el contrato establecido por el gestor contractual. Sin embargo, al igual que ocurre con los mecanismos para implementar las credenciales vinculantes, el esquema de testigo digital seguiría siendo válido para otros mecanismos similares que permitan definir de forma unequívoca las relaciones entre los usuarios, los dispositivos y las evidencias.

IV-B. Interacción entre componentes

A continuación, definimos tres casos básicos (A-C) de interacción entre los componentes mostrados en la Figura 2. El diagrama de flujo que detalla la interacción entre los componentes se muestra en la Figura 3:

(A) Establecimiento de políticas de actuación para el uso del testigo digital.
(B) Creación de credenciales vinculantes (BCs).
(C) Gestión de evidencias con BCs.

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. No incluimos el registro de este tipo de evidencias en la Figura 3 por simplicidad, pero requiere la colaboración entre el Gestor de Operaciones de Usuario-Dispositivo y el Gestor EE. Posteriormente, las políticas se consultan por cada componente, y la integridad de los ficheros de políticas será comprobada periódicamente empleando el hash correspondiente como si de una evidencia se tratase.

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 (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

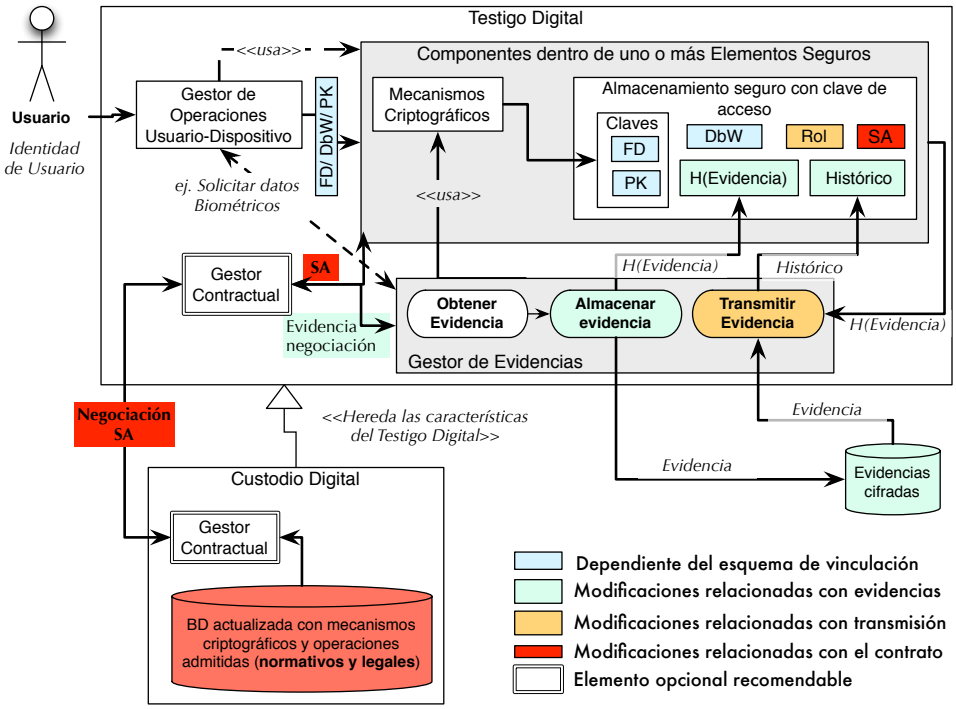

Figura 2. Arquitectura Funcional para un testigo digital empleando credenciales vinculantes.

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 ó 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 en las normas actuales [3]. 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. Una mejora que posibilitaría el despliegue de un escenario más dinámico se detalla en la sección IV-C mediante 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 ó tokens) que vinculen al usuario con el dispositivo. Estas BCs serán empleadas de forma transparente por el GEE para operar con las evidencias, históricos y la transmisión de éstos.

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.

La evidencia se obtiene empleando mecanismos forenses aceptados, acordes a la normativa y la legalidad vigentes (c.f. [2]). El hash de la evidencia electrónica se realizará empleando los mecanismos criptográficos adecuados y, si éste 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 el componente encargado de solicitar la escritura del valor hash resultante en el espacio de almacenamiento. Aunque se obvia por motivos de claridad (en la Figura 3 se asume que la generación y el envío van unidos), la obtención de una evidencia requeriría la actualización del histórico de evidencias electrónicas.

El último paso correspondería con el envío de la evidencia (ó conjunto de evidencias). El número de evidencias a enviar, el momento en el que se envían, y la forma de borrado ó eliminación de la evidencia, dependerán de la política establecida a tal fin. En la Figura 3 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 de acuerdo a las preferencias mencionadas en la sección III. Este 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.

En la Figura 3, los registros hashes de las evidencias se eliminan una vez éstas han sido delegadas para salvar espacio en el dispositivo. Sin embargo, no siempre tiene que ser así, ya que dependería de la política de borrado. Por ejemplo, si la

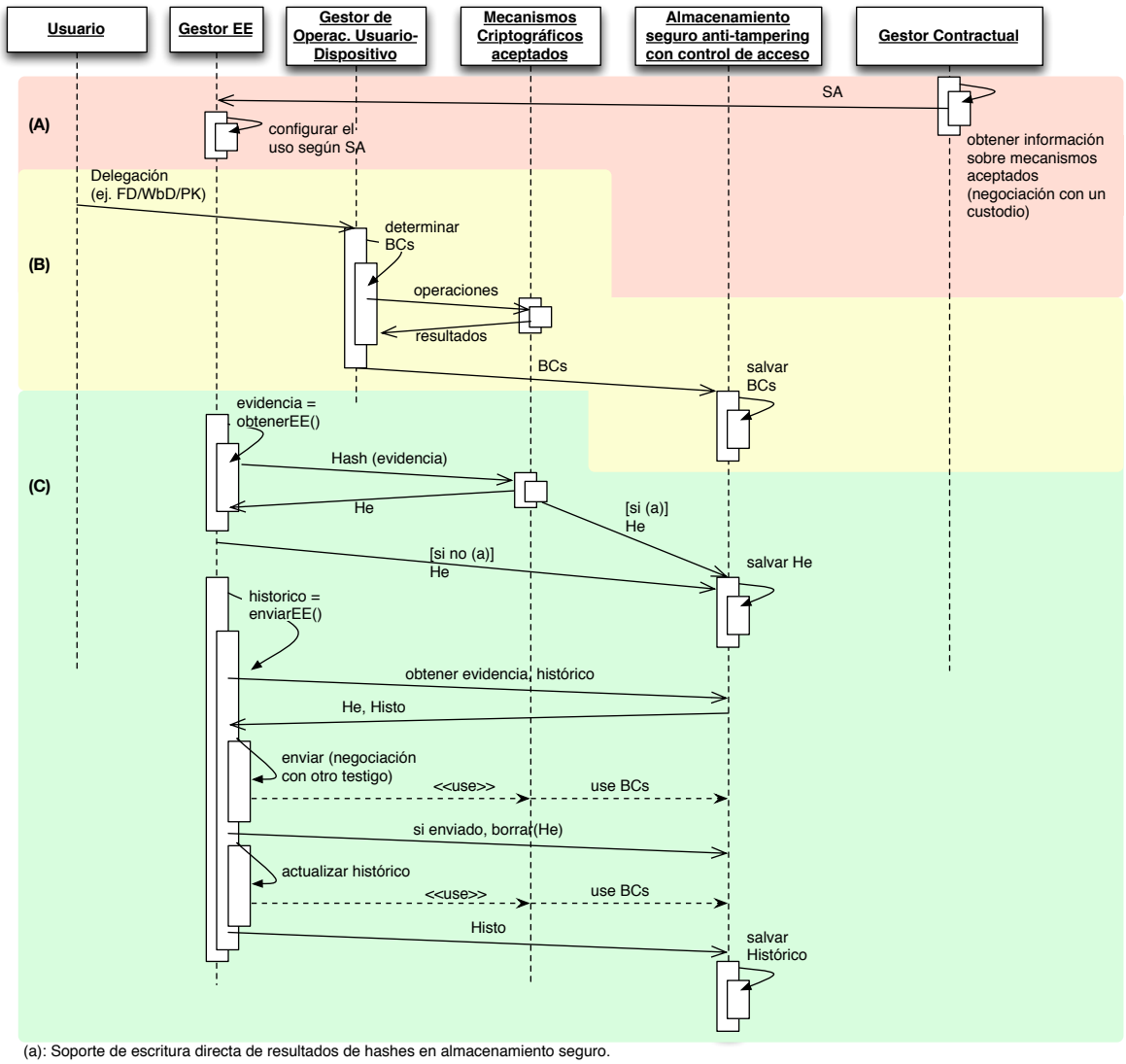

Figura 3. Diagrama de flujo con caso de uso simplificado.

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 el histórico se actualiza y los datos acreditativos de las operaciones se salvan en el espacio protegido del testigo digital.

IV-C. Interacción opcional entre componentes, componentes opcionales y ampliaciones

IV-C1. Gestor contractual: En caso **(A)**, detallado en la Sección IV-B puede mejorarse por medio del uso del componente opcional *Gestor Contractual* para establecer las políticas para el gestor de evidencias electrónicas. 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 sobre mecanismos criptográficos y configuraciones aceptables para la gestión de evidencias electrónicas*.

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 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 requerido 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 dispositivo 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 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.

IV-C2. Uso de mecanismos biométricos como parte del Gestor de Operaciones Usuario-Dispositivo: Como puede verse en la Figura 2, 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)** (cf. Figura 3) antes de la creación de las BCs, o dentro del caso **(C)** (cf. Figura 3) 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 el tipo de sistema biométrico a utilizar (p.ej. huella dactilar, iris, voz), las combinaciones esperadas de sistemas biométricos, y 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. Antes de realizar cualquier operación que requiera de la presencialidad 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. Como paso opcional final, el Gestor de Operaciones interactuará con el Gestor de Evidencias Electrónicas para crear una evidencia que pruebe el uso de los mecanismos biométricos por parte del Usuario. Esta evidencia puede abarcar 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 a la creación de la evidencia del uso de un sistema biométrico, cabe puntualizar la naturaleza de dicha evidencia. A día de hoy, la mayoría de los sistemas biométricos permiten detectar al dueño del dispositivo utilizado como testigo digital, pero no enlazar la identidad de ese dueño con la identidad de la persona física. Esto es así porque dentro del funcionamiento de los mecanismos biométricos no se coteja la información proporcionada por el usuario (p.ej. su huella dactilar) con una fuente legalmente válida (p.ej. la huella dactilar almacenada en un DNI electrónico). No obstante, a día de hoy es también posible implementar mecanismos que puedan establecer este enlace, como por ejemplo utilizando un lector de huellas digitales en conjunción con el DNI-e.

Es por tanto necesario indicar, dentro de la evidencia del uso de un sistema biométrico, la naturaleza probatoria de dicha evidencia: dueño del terminal vs. persona física. No obstante, tal y como hemos mencionado anteriormente (cf. sección III), un usuario tiene una responsabilidad ante el uso de su terminal como Testigo Digital.

V. Conclusiones y trabajo futuro

En este artículo proponemos una arquitectura funcional para la implementación del concepto de testigo digital en los objetos de la IoT. Esta arquitectura sienta las bases para la inclusión de un objeto en una cadena de custodia digital (CCD). Cabe destacar, que los testigos digitales comprenden usuarios con distintos roles que marcan la funcionalidad de los testigos. Esto tiene también una consecuencia adicional no discutida, y es que la probabilidad de encontrar un custodio digital antes que un testigo del mismo nivel puede ser inferior. La delegación de la evidencia por tanto depende de la movilidad del usuario y del resto de testigos. Un análisis para determinar cómo afecta este juego de roles a la CCD dinámica es requerido para trabajos futuros. Por otra parte, ligar la identidad de los usuarios a los objetos tiene un sin fin de connotaciones que es muy dificil abordar sin afectar al núcleo de este artículo. Es decir, el uso de credenciales vinculantes es una línea de investigación que puede ser fruto de nuevos trabajos futuros por sí solo. De hecho, la gestión de *la identidad de las cosas* es un desafío abierto actualmente en el marco de la IoT.

Agradecimientos

Este trabajo ha sido financiado por el Ministerio de Economía y Competitividad a través de los proyectos IoTest (TIN2015-72634-EXP) y PERSIST (TIN2013-41739-R). Adicionalmente, ha sido financiado por la Junta de Andalucía a través del proyecto FISICCO (TIC-07223).

Referencias

[1] E. U. A. for Network and I. Security, "Enisa threat landscape 2015," 2016.

[2] A. Nieto, R. Roman, and J. Lopez, "Testigo digital: delegación vinculante de evidencias electrónicas para escenarios iot," in *II Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2016)*, in Press.

[3] A. 71, "Une 71505: Tecnologías de la información (ti). sistema de gestión de evidencias electrónicas (sgee)." *Tecnología de la Información*, 2013.

[4] E. project, "Electronic discovery reference model," 2005. [Online]. Available: http://bit.ly/183V8l1

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

[6] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of things forensics: Challenges and approaches," in *Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on*. IEEE, 2013, pp. 608–615.

[7] T. Marqués Arpa and J. Serra Ruiz, "Cadena de custodia en el análisis forense. implementación de un marco de gestión de la evidencia digital," 2014.

[8] Y. Prayudi and A. Sn, "Digital chain of custody: State of the art," *International Journal of Computer Applications*, vol. 114, no. 5, 2015.

[9] Y. Prayudi, A. Ashari, and T. K. Priyambodo, "Digital evidence cabinets: A proposed framework for handling digital chain of custody," *International Journal of Computer Applications*, vol. 107, no. 9, 2014.