A. Nieto, R. Roman, and J. Lopez, "Testigo digital: delegación vinculante de evidencias electrónicas para escenarios IoT", *II Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2016)*, pp. 109-116, 2016.
NICS Lab. Publications: https://www.nics.uma.es/publications

Testigo digital: delegación vinculante de evidencias electrónicas para escenarios IoT

Ana Nieto, Rodrigo Roman, Javier Lopez

Departamento de Lenguajes y Ciencias de la Computación
Universidad de Málaga, España
Email:{nieto,roman,jlm}@lcc.uma.es

***Resumen*—En un mundo en el que los usuarios dependen cada vez más de sus dispositivos, éstos almacenan gran cantidad de datos y son una fuente muy valiosa de información sobre su entorno. Sin embargo, la heterogeneidad y la densidad de los objetos conectados, características propias de la Internet de las Cosas (IoT), sirven de velo para ocultar conductas maliciosas que afectan a estos dispositivos, sin que quede rastro de tales acciones. En este artículo definimos el concepto de testigo digital: funcionalidad que permitirá a los dispositivos personales y otros objetos colaborar para implementar una cadena de custodia digital en la IoT. El fin perseguido es ofrecer soluciones que mitiguen los efectos de la ciberdelincuencia, amparándose en la colaboración de los dispositivos con arquitecturas de seguridad embebidas para alertar de conductas maliciosas, y dejar constancia de éstas.**

***Index Terms*—Evidencia electrónica, computación forense, Internet de las Cosas, elemento seguro, no repudio.**

Tipo de contribución: *Investigación en desarrollo*

I. Introduction

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. Estos dispositivos forman parte del abanico de la Internet de las Cosas (IoT por sus siglas en inglés), donde dispositivos de muy diverso perfil coexisten dentro de un entorno dinámico, heterogéneo y distribuido.

Esto trae consigo varios problemas muy relevantes desde el punto de vista de la ciberseguridad. Por una parte, el creciente número de dispositivos y sus características cada vez más sofisticadas hace que perpetrar ataques empleando estas nuevas tecnologías sea muy factible. Por otra parte, cuando un dispositivo personal es comprometido, el atacante tiene acceso a una fuente muy valiosa de información sobre un individuo, y, a su vez, puede emplear esta información para perpetrar más ataques. De igual forma, los atacantes pueden aprovechar la existencia de dispositivos vulnerables para obtener información sobre infraestructuras críticas y causar el mayor daño posible.

Frenar este tipo de ataques lo antes posible es fundamental, así como registrar las trazas del ataque a diferentes niveles, centralizado en el dispositivo y distribuido en la red. Como si de un incidente en una vía pública se tratase, la idea fundamental que aquí perseguimos es la de proponer un concepto similar al del testigo humano pero novedoso en su campo: el *testigo digital*. El testigo digital es una solución forense para la obtención y manipulación de evidencias electrónicas, que sería integrada en dispositivos tales como móviles inteligentes y dispositivos IoT. Esta solución permitiría que la máquinas pudieran detectar ataques provocados por otras máquinas y dar fe de estos hechos, en vez de actuar como meros recipientes pasivos. Esto abriría un nuevo marco de trabajo y posibilidades muy interesantes, que permitirían luchar contra nuevas y dinámicas formas de ataques que se escudan en el anonimato y ocultan su rastro en un mar de dispositivos para no ser detectados.

No obstante, debido a la novedad de este concepto, es necesario estudiar no sólo los requisitos asociados a la idea del testigo digital, sino también cuáles serían las tecnologías y mecanismos de seguridad que permitirían el tratamiento seguro de las evidencias electronicas a todos los niveles: tanto en su adquisición y vinculación con entidades autorizadas, como en su transmisión a custodios como los cuerpos de seguridad del estado. Por lo tanto, en este trabajo definimos el concepto de testigo digital, y exploramos cuáles son los elementos necesarios para implementar este concepto en dispositivos personales.

La estructura del artículo es como sigue. La sección II introduce diversos trabajos que pueden considerarse dentro del estado del arte de este nuevo concepto. La sección III define el concepto de testigo digital, mientras que los mecanismos para implementar el concepto de credencial vinculante son descritos en la sección IV. Finalmente, la sección V ilustrará el proceso de delegación vinculante mediante casos de uso adecuados al contexto de la Internet de las Cosas, e incluirá un análisis del uso de arquitecturas de seguridad embebidas en este contexto. Las conclusiones y trabajo futuro se describen en la sección VI.

II. Estado del arte

Algunos desafíos abiertos en la gestión de evidencias electrónicas considerando las restricciones del paradigma IoT se desprenden del trabajo [1], donde se define 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 gestión de evidencias electrónicas (GEE) en estos entornos ha de considerar requisitos adicionales a los considerados tradicionalmente (véase la norma UNE71505:2013 [2]).

Por ejemplo, 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. Entre los desafíos abiertos, discutidos en [3],

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 no mencionado en el trabajo anterior es el análisis forense de los artefactos (evidencias) en los objetos como sensores y protocolos propietarios. La diversidad de objetos hace que la extracción de evidencias en los objetos no sólo no se encuentre definida en su totalidad, sino que se enfrenta con formatos de presentación de la información 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 [4], o bien para estandarizar la presentación y los formatos para el intercambio de evidencias electrónicas [5].

La preservación de las evidencias electrónicas mediante el concepto de *Cadena de Custodia Digital* (CCD) es empleado en otros trabajos como en [6], [7]. En [6] se propone una CCD para enviar evidencias digitales multimedia con estampillado de tiempo a una entidad a través de Internet, mientras que en [7] 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 [8] se proporciona un estado del arte sobre los últimos trabajos en materia de CCD hasta Marzo de 2015. 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. Además, una vez más, los dispositivos móviles, pese a integrar arquitecturas de seguridad, quedan dentro de esta cadena como meros contenedores de evidencias, y, en caso de participar, el proceso requiere de la intervención directa del usuario en todo momento.

Estas soluciones carecen de algo básico: de cara a enfrentar los problemas de ciberseguridad para la IoT los mecanismos para la gestión de evidencias deben adaptarse e integrarse en el entorno distribuido y heterogéneo. Los dispositivos no pueden en modo alguno ser vistos sólo como contenedores de evidencias, sino como participantes responsables y colaborativos. Además, no debe suponerse que la conectividad a Internet es siempre posible. Dentro de un entorno IoT los mecanismos deberán mimetizarse con el entorno y aprovechar los protocolos ad-hoc disponibles y las arquitecturas de seguridad embebidas en los dispositivos. De no considerarse estos puntos, estaremos infrautilizando los recursos disponibles para frenar los ataques.

Por otra parte, la identidad de las cosas, o *Identities of Things* (IDoT) es considerado otro desafío abierto [9]. Ante la proliferación de dispositivos, definir la relación entre los dispositivos y sus usuarios se antoja cada vez más necesario en los escenarios de ciberataque. 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 gestores de evidencias electrónicas definidos para la IoT podría significar un gran paso para enfoques distribuidos como el que proponemos en este trabajo.

III. El concepto de testigo digital

Definimos 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 hasta su transferencia a una entidad autorizada, que puede ser otro testigo digital o bien una entidad con potestad para alojar la evidencia electrónica.

Tal y como describe la Fig. 1, los testigos digitales permitirían desplegar cadenas de custodia dinámicas, amparándose en la colaboración entre los objetos de la IoT que actúen como testigos.

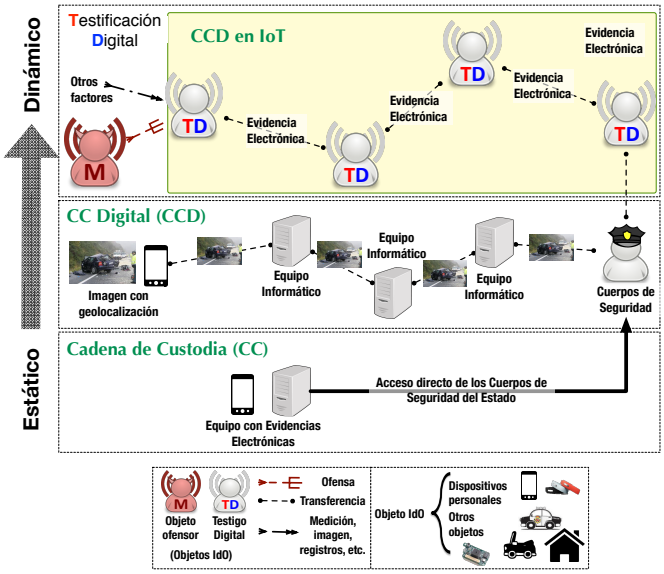

Fig. 1. Cadena de custodia digital empleando testigos digitales.

Los testigos digitales actuarán bajo diferentes perfiles o roles. El rol vendrá determinado principalmente por dos factores: (i) los privilegios del usuario para la gestión de las evidencias electrónicas y (ii) las capacidades de seguridad del dispositivo. La Fig. 2 muestra dos tipos de testigo digital considerados en base a perfiles de usuario.

Entendemos que hay un principio básico, y es que el dispositivo que actúe como testigo tiene que ligar la identidad del usuario al dispositivo para establecer responsables. No sólo para identificar un posible infractor, sino también para que la testificación del dispositivo tenga un supervisor humano que pueda dar fe del acto de ser requerido por la autoridad pertinente. Esta vinculación entre el usuario y su dispositivo hace que el extravío ó robo de un dispositivo considerado testigo deba notificarse a las autoridades pertinentes como si de un DNI-e se tratase.

Por otra parte, el testigo digital efectuará acciones en nombre de su propietario siempre y cuando se satisfagan

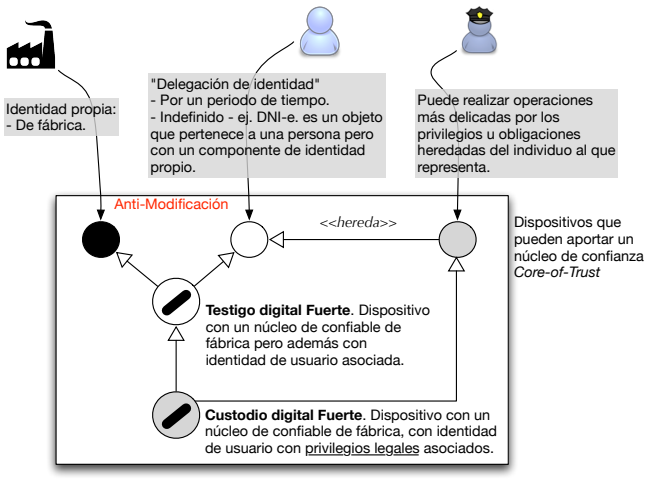

Fig. 2. Roles en la testificación digital.

una serie de requisitos que aseguren que las órdenes fueron emitidas 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 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 Fig. 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 ciclo de vida de la evidencia electrónica en el que estarán involucrados los 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.

IV. Esquemas para la integración de la delegación de identidad en la gestión de evidencias electrónicas (IDEEs)

Como se ha mencionado anteriormente, es esencial que un usuario pueda delegar su identidad hacia el dispositivo o dispositivos que actuan como testigos digitales. Como primer paso, y en el contexto que nos ocupa, sería necesario que la identidad de un usuario dentro de un dispositivo fuese vinculante; es decir, debería permitir durante el manejo de las evidencias trazar de forma inequívoca a la persona física que esta detras 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 [11]), puesto que en determinados paises 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 [12]. 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 toda la gestión de las evidencias electrónicas. 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. 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* [13]. Es más, todas las estrategias para implementar esta primitiva criptográfica [13] nos permiten implementar la vinculación entre usuario y evidencia, tal y como se muestra en la Fig. 3 y se desarrolla en el siguiente párrafo.

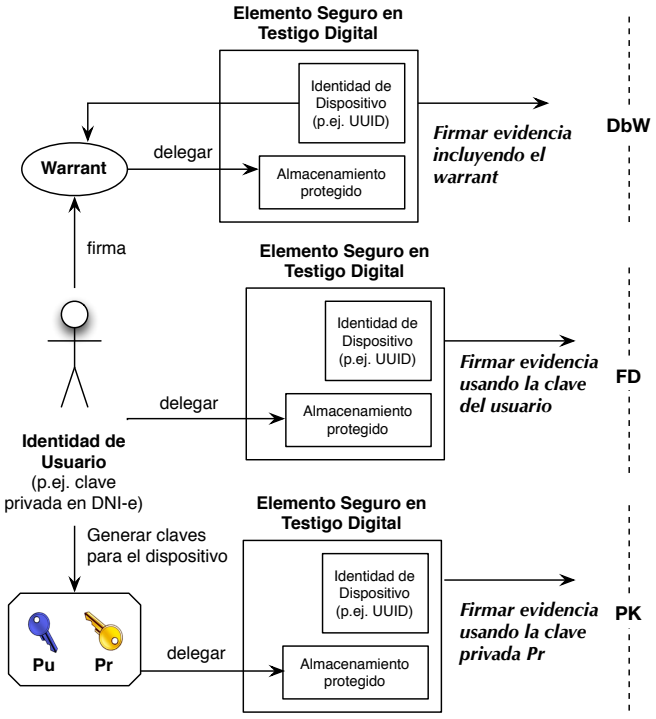

Fig. 3. IDEEs en Testigos Digitales.

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 [14]), puede comprobarse la identidad del usuario que generó las evidencias.

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

Sea cual sea la estrategia a emplear, hay otra incógnita a resolver: 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 [15], 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 incluyesen los identificadores (IMSI, MSISDN) necesarios. Hay que hacer notar que, en este caso, para que las evidencias fuesen validadas de forma irrefutable sería necesaria la participación del operador.

Existe otro método que no necesita de una tercera parte confiable industrial, y que además involucra directamente al usuario: el uso del DNI-e. 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 permitiría 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 [16] han demostrado que es posible la interoperabilidad entre identificadores electrónicos Europeos, por lo que una evidencia puede tener validez legal 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 la gestión de las evidencias electrónicas. Es más, el problema de la identificación de objetos IoT – y sus propietarios – sigue abierto a día de hoy [9]. 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 [17] 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 [18], 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 podría 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, podrían utilizarse mecanismos de autenticación basados en contexto [19] o sistemas biométricos [20] 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.

V. Delegación vinculante

Otro aspecto clave para la realización del concepto del testigo digital es la transferencia de las evidencias entre entidades autorizadas. Para lograr este objetivo, ha de establecerse lo que se denomina una *cadena de custodia digital* (CCD) [6] pero donde los involucrados serían objetos de uso personal. Este proceso es necesario, dado que los objetos cuentan con pocos recursos computacionales, y además porque se pretende minimizar la exposición de la evidencia electrónica.

La Fig. 4 muestra diferentes casos de lo que denominaremos *delegación de evidencias*; el 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 serán almacenadas para su análisis final. Para que un dispositivo sea un testigo digital, debe satisfacer la condición de ser un eslabón seguro de la cadena, y de que la delegación se efectúa con credenciales vinculantes, para mantener la trazabilidad sobre la evidencia y los responsables involucrados en su notificación.

La Fig. 4 muestra también varios casos de uso considerando tres perfiles distintos ó roles de testigo digital, en base a los recursos computacionales de éstos y los usuarios que los manejan. En los siguientes apartados describimos los participantes en este proceso, los pasos para la delegación

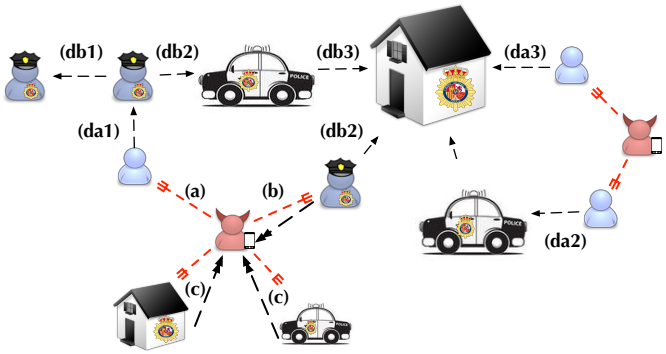

Fig. 4. Delegación de evidencias.

vinculante simplificados y algunas tecnologías que podrían ayudar a implementar el concepto de almacenamiento seguro.

V-A. *Participantes*

Consideramos que la evidencia podría ser recabada 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 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 delimilitador 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.

La liberación de la evidencia se haría por medio del proceso de delegación mostrado en la Fig. 4. Para estos casos, consideramos seis casos base de delegación:

da1. 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.

da2. Delegación de un usuario en otro objeto (móvil) con más privilegios ó recursos. Es similar al caso dal, pero la evidencia electrónica se entregaría a un objeto del cuerpo de seguridad con más recursos ó mayores posibilidad de encontrar un objeto para el almacenamiento final de la evidencia.

da3. Delegación de un usuario en otro objeto con más privilegios ó recuros. 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 ó transferencias a otras entidades siguiendo los esquemas tradicionales para la transferencia de evidencias electrónicas.

db1. 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.

db2. Delegación de un usuario con potestad a un objeto con potestad. Es el símil con da2, 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.

db3. 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 db3 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.

Finalmente, aunque en esta sección se considera el procesamiento de la evidencia en su emplazamiento final por el uso de recursos, las medidas de seguridad de los objetos podrían permitir en algunos casos implementar una respuesta temprana. Esto se considera para los casos en los que la evidencia se recaba por los objetos (b) ó (c).

La respuesta temprana dependería del tipo de evidencia recogida, así como los mecanismos de respuesta. Además, este tipo de medidas asume un pre-procesamiento de la evidencia en los objetos para determinar si es necesaria una respuesta inmediata. Este tipo de actuaciones dependen de un conjunto de factores que también estarían sujetos al marco legal. La dimensión de este problema hace inabordable plantear las medidas que habría que considerar para los diversos casos contemplables, y, aunque escapa al ámbito de este trabajo, creemos necesario abordar estos problemas en el futuro.

V-B. *Pasos para la delegación*

Una vez definidos los roles de cada una de las entidades que participan en la cadena de custodia digital, así como los diversos procesos de delegación de evidencias, podemos definir los pasos específicos que son necesarios para llevar a cabo esta delegación. Así, la Fig. 5 muestra de forma simplificada los pasos desde que se obtiene la evidencia electrónica hasta que 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 el formato de evidencia electrónica (FEE) empleado. En este proceso, se generará un identificador de la evidencia a partir del identificador vinculante del dispositivo electrónico que la genera, y el estampillado de tiempo. Este será el identificador de la evidencia durante su ciclo de vida. La evidencia se firma y el valor probatorio se almacena (2) atendiendo a los criterios de almacenamiento seguro. La firma de la evidencia dependerá del mecanismo escogido para la vinculación de la identidad (sección IV).

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:

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

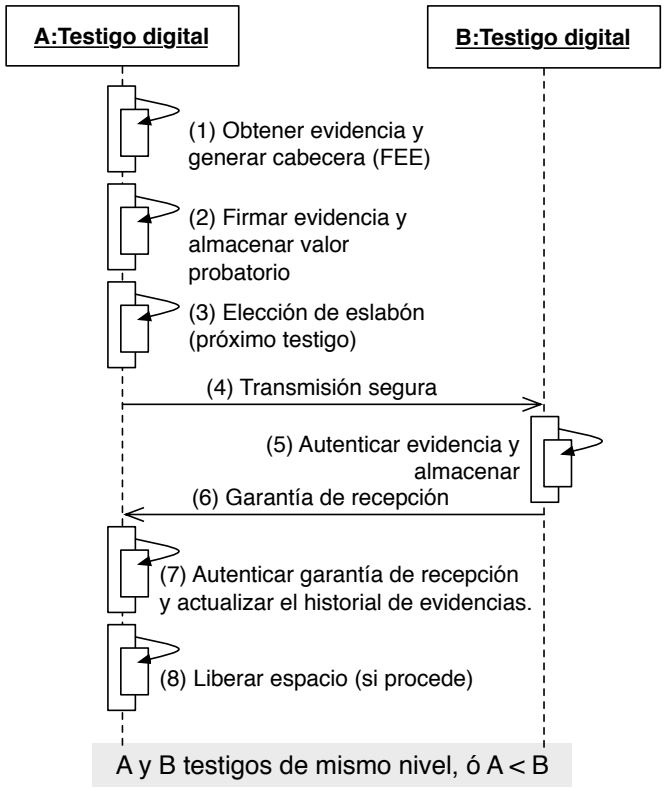

Fig. 5. Pasos de la testificación digital.

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.
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.

Además, la elección del siguiente testigo digital 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, ó 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 nivell-rol de todos los posibles, ó que ofrece más garantías/probabilidad de que la evidencia alcance el destino final minimizando el número de delegaciones.
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 formato de evidencia electrónica 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 ó conjunto de evidencias (8).

Cabe destacar, que la funcionalidad que no proporcione el chip de seguridad deberá proporcionarla una aplicación externa. Estos casos de comunicación interna segura entre las aplicaciones y los dispositivos de seguridad deben definirse acorde la especificación [21].

V-C. Tecnologías para el almacenamiento seguro

Como hemos mencionado en la Sección III, el testigo digital se apoya sobre la base de que los dispositivos cuentan con una arquitectura de seguridad que dispone de almacenamiento seguro. Pese a que este hecho encarece los dispositivos, bien es cierto que el pago electrónico está impulsando este tipo de medidas. Por otra parte, diferentes objetos de la Internet de las Cosas ya integran chips anti-tampering (p.ej. TPM en vehículos) y la tendencia es integrar mecanismos similares en objetos más pequeños, como wearables. La Tabla I muestra un resumen de diferentes soluciones para el almacenamiento seguro que podrían emplearse para la testificación digital.

La inclusión de chips de seguridad hardware trae consigo una ventaja adicional, y es 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 [22].

En el caso que nos ocupa, no basta con que el chip intere mecanismos para establecer un canal de comunicaciones seguro, sino que, además, esos mecanismos deben emplear tecnologías que sean aceptables para la gestión de evidencias electrónicas. En concreto, en [2] se definen, como operaciones pemitidas:

- 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. Atendiendo a los requisitos de [2] y a la información proporcionada en la Tabla I, 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 [2]). El tiempo de vida de la

Tabla I
CARACTERÍSTICAS DE LOS CHIPS DE ALMACENAMIENTO SEGURO INTEGRADOS EN DISPOSITIVOS PERSONALES

Dispositivo	Seguridad	Memoria	Interfaz	SDK
TPM v2.0 (auto). Posibilidad de SE si JavaCard	Al menos un asimétrico (RSA 2048 ó ECC P256), al menos un simétrico (AES 128), CBC, SHA-256, HMAC. Si ECC se implementa, deben soportarse: NIST_P256, BN_P256, y SM2_256. UUID. Secure boot, R0T (*). Si SE: gestión del SE por medio de VPN con TSM.	1.6 KBytes	APDU para comunicación con SE (**)	tpm-tools
SLE 97 SOLID FLASH Family. Modelos para UICC/SIM y eSE.	Fingerprint match-on-card. Asimétrico: RSA (SWP UICCs hasta 4096bits, eSE hasta 2048bits), ECC (hasta 521bits). Simétrico: 3DES, AES (hasta 256bits), certificación: CC EAL5+high EMVCo.	Desde 800KBytes a 1.5MBytes, dependiendo del modelo	ISO/IEC 7816, SWP, opcional (del modelo): SPI, I^2C, GPIOs	Application Development Toolkit, Java Card
OPTIGA Trust authentication chip	Asimétrico: RSA (hasta 2048bits), ECC (hasta 52lbits). Simétrico: AES (hasta 256bits), 3DES (hasta 256bits). Secure boot. True hardware random number generator. SHA1/224/256/384/512. DH/ECDH Key Agreement. GlobalPlatform ID configuration (identificador único de chip). Logs de incidentes. Certificación: EAL5+.	150KBytes	ISO/IEC 7816 UART (400kbps)	Crypto applets, host source code, Java Card
Boosted NFC SE. En SIM, SD y microSD con antena integrada	Asimétrico: RSA (hasta 4096bits), ECC (hasta 512bits). Simétrico: 3DES, AES, certificación: EAL5+ high EMVCo (SLE 77) ó EAL6+ high EMVCo.	240KBytes (SLE 77), hasta 500KBytes (SLE 78)	ISO/IEC 7816, ISO/IEC 14443 (***), opcional (del modelo) : SPI, GPIOs	

RoT: Root of Trust. For: Confidentiality (RTC), Integrity (RTI), Measurement (RTM), Reporting (RTR), Storage (RTS), Update (RTU), Verification (RTV).
UUID: Universally Unique Identifier. RRC 4122.
UEFI: Unified Extensible Firmware Interface. Protected Environment communications driver (Ej: TPM 2.0 Mobile Command Response Buffer Interface).
TSM: Trusted Service Managers (entidad remota).
APDU: Application Protocol Data Unit. (**): max 256bytes.
SWP: Single Wire Protocol/ Compatibilidad Mifare.
UICC: Universal Integrated Circuit Card.
SPI: Serial Peripheral Interface (transferencia de información entre circuitos integrados).
GPIO: General Purpose Input/Output.
I^2C: Inter-Integrated Circuit
ISO/IEC 7816: Smart Card Standard (1-6)
ISO/IEC 14443: Identification cards. (***) : Type A and Type E cards emulation via ACLE interface.
ACLB: Analog Contactless Eridge / plug and play para dispositivos con microSD, SD, o tarjeta SIM.
EAL: Evaluation Assurance Level. EAL5: Semiformally Designed and Tested, EAL6: Semiformally Verified Design and Tested, EAL7: Formally Verified Design and Tested.

seguridad para el primer caso se considera hasta 2030, y en el segundo caso más allá de 2030. Por lo tanto, se sitúa como un buen candidato para su uso por parte de un testigo digital fuerte. Además, permite el intercambio de claves usando *diffie hellman* (DH) ó DH empleando criptografía de curva elíptica (ECDH), agilizando la creación de canales seguros de comunicación.

Sin embargo, la definición de testigo digital debe ir más allá de un componente específico. Emplear arquitecturas de seguridad embebidas ofrece la posibilidad de proveer de mecanismos criptográficos aceptados y el almacenamiento seguro con control de acceso. No obstante, otros componentes destinados a formar parte del testigo digital deberán procurar la gestión de las operaciones entre el usuario y el dispostivo (p.ej. contratos, cláusulas de aceptación), y la gestión de evidencias electrónicas adaptada a la IoT, gestión que deberá hacer uso de estos elementos seguros embebidos.

Así, un elemento anti-tampering de estas características formará parte de un cuadro mucho más amplio, donde los requisitos detallados en las secciones anteriores converjan para implementar el concepto de testigo digital.

VI. CONCLUSIONES Y TRABAJO FUTURO

El uso de arquitecturas de seguridad embebidas en los dispositivos móviles y otros objetos de uso personal está por debajo de su potencial. Actualmente el propósito de estas arquitecturas es o bien proteger los datos del usuario o facilitar el pago electrónico. Avances recientes permiten la firma a través del móvil empleando la última versión de DNIe que incorpora NFC. Sin embargo, estas arquitecturas pueden ofrecer mucho más.

En este artículo definimos el concepto de *testigo digital*, destacando la importancia de elementos como la *identidad vinculable* entre el usuario y sus dispositivos, y la *delegación de evidencias electrónicas* entre entidades autorizadas para establecer una cadena de custodia digital. Cabe destacar que aunque aquí proponemos ejemplos para demostrar que el esquema podría ser implementado en la práctica, nuestro

enfoque no es necesariamente específico de un único dispositivo. Esto hace que, aunque en este artículo nos centramos en defender la importancia y posibilidades que este nuevo concepto queda un largo camino por recorrer hasta su implementación y despliegue. Por ejemplo, debererán definirse aquellos componentes que permitan la implementación del testigo digital en los objetos, ya que, como hemos visto en este artículo, este nuevo concepto permite afrontar varios de los problemas abiertos identificados en la sección II.

Así, hemos descrito cómo un dispositivo con esta funcionalidad puede convertirse en un elemento activo capaz no sólo de participar en una cadena de custodia digital, sino de transmitir las evidencias incluso cuando no existe una conectividad global. Además, gracias a la identidad vinculante, esta estrategia permite determinar la responsabilidad en el manejo de las evidencias, garantizando la trazabilidad en todo instante desde su generación sin mermar la escalabilidad de todo el sistema.

No obstante, existen algunos problemas abiertos que deben considerarse para refinar y expandir la aplicabilidad de la figura del testigo digital. Uno de ellos es la problemática de la identidad en la IoT, un campo que de por sí aún esta siendo investigado. Por ejemplo, queda por determinar cómo extraer la identidad unequívoca de los dispositivos en el contexto general de la IoT. Dicha identidad puede depender de muchos factores, como el propio contexto del objeto o sus características y/o capacidades. Además, existen diversas cuestiones éticas y legales asociadas al derecho de propiedad y al rol incriminatorio de las evidencias recabadas por los testigos digitales que deben ser propiamente discutidos.

Por otra parte, el despliegue de testigos digitales aumentaría el coste de los dispositivos, debido al coste adicional de las arquitecturas de seguridad embebidas. Aunque la venta de dispositivos móviles con estas características es cada vez más habitual, el uso que aquí le estamos dando a éstas puede ser más difícil de asimilar de buen grado por los usuarios. Actualmente los delitos telemáticos no gozan del mismo rechazo en la sociedad que un delito físico, aunque cada vez su repercusión en nuestra vida cotidiana es mayor. Proponer soluciones que conviertan los hasta ahora señalados como inconvenientes de la IoT (p.ej. heterogeneidad, densidad) en ventajas de ciberseguridad (p.ej. roles con privilegios, conectividad, colaboración) debe ser un objetivo prioritario en los próximos años.

AGRADECIMIENTOS

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

REFERENCIAS

[1] 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.

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

[3] R. Hegarty, D. Lamb, and A. Attwood, "Digital evidence challenges in the internet of things," in *Proceedings of the Tenth International Network Conference (INC 2014)*. Lulu. com, 2014, p. 163.

[4] 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.

[5] E. Casey, G. Back, and S. Barnum, "Leveraging cybox™ to standardize representation and exchange of digital forensic information," *Digital Investigation*, vol. 12, pp. S102–S110, 2015.

[6] T. Marqués Arpa and J. 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.

[7] Y. Prayudi, A. Ashari, and T. K. Priyambodo, "Digital evidence cabinets: A proposed frameworks for handling digital chain of custody," *Int. J. Comput. Appl*, vol. 109, no. 9, pp. 30–36, 2014.

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

[9] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, no. 0, pp. 146–164, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128614003971

[10] I. Friese, J. Heuer, and N. 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*. IEEE, 2014, pp. 1–4.

[11] R. Ayers, S. Brothers, and W. Jansen, "Sp 800-101 rev. 1, guidelines on mobile device forensics," Gaithersburg, MD, United States, Tech. Rep., 2014.

[12] V. Gayoso Martinez, L. Hernández Encinas, A. Martín Muñoz, and J. I. Sanchez García, "Identification by means of a national id card for wireless services," in *2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, June 2013, pp. 1–5.

[13] A. Boldyreva, A. Palacio, and B. Warinschi, "Secure proxy signature schemes for delegation of signing rights," *Journal of Cryptology*, vol. 25, no. 1, pp. 57–115, 2012. [Online]. Available: http://dx.doi.org/10.1007/s00145-010-9082-x

[14] H. Debiao, C. Jianhua, and H. Jin, "An id-based proxy signature schemes without bilinear pairings," *Annals of Telecommunications*, vol. 66, no. 11–12, pp. 657–662, 2011. [Online]. Available: http://dx.doi.org/10.1007/s12243-011-0244-0

[15] 3GPP TS 33.221: Support for Subscriber Certificates, http://www.3gpp.org/DynaReport/33221.htm, Accessed on April 2015.

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

[17] M. 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 Computing and Communications (TrustCom)*, Nov 2011, pp. 863–872.

[18] J. Lyle, A. Paverd, J. King-Lacroix, A. Atzeni, H. Virji, I. Flechais, and S. Faily, "Personal pki for the smart device era," in *Public Key Infrastructures, Services and Applications*, ser. Lecture Notes in Computer Science, S. De Capitani di Vimercati and C. Mitchell, Eds. Springer Berlin Heidelberg, 2013, vol. 7868, pp. 69–84. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-40012-4_5

[19] S. A. Hoseini-Tabatabaei, A. Gluhak, and R. Tafazolli, "A survey on smartphone-based systems for opportunistic user context recognition," *ACM Computing Surveys*, vol. 45, no. 3, pp. 27:1–27:51, Jul 2013. [Online]. Available: http://doi.acm.org/10.1145/2480741.2480744

[20] L. M. Mayron, "Biometric authentication on mobile devices," *IEEE Security and Privacy*, vol. 13, no. 3, pp. 70–73, May 2015.

[21] S. Rahat and W. Browning, "Methods and systems for secure communications between client applications and secure elements in mobile devices," Dec. 2 2014, uS Patent 8,904,195.

[22] D. T. Haggerty, A. A. Khan, C. B. Sharp, J. Von Hauck, J. Linde, K. P. McLaughlin, Z. Mehdi, and Y. H. Vaid, "Apparatus and methods for secure element transactions and management of assets," Feb. 6 2014, uS Patent App. 14/174,791.