Digital Witness: Safeguarding Digital Evidence by using Secure Architectures in Personal Devices

Ana Nieto, Rodrigo Roman, and Javier Lopez

***Abstract*—Personal devices contain electronic evidence associated with the behaviour of their owners and other devices in their environment, which can help clarify the facts of a cyber-crime scene. These devices are usually analysed as containers of proof. However, it is possible to harness the boom of personal devices to define the concept of digital witnesses, where personal devices are able to actively acquire, store, and transmit digital evidence to an authorised entity, reliably and securely. This article introduces this novel concept, providing a preliminary analysis on the management of digital evidence and the technologies that can be used to implement it with security guarantees in IoT environments. Moreover, the basic building blocks of a digital witness are defined.**

***Index Terms*—Digital Evidence, IoT-Forensics, Secure Element, Identity Delegation.**

I. Introduction

Mobile user devices are deeply rooted at the heart of our society. Indeed, social networks and education in new technologies have greatly boosted the acceptance of personal devices as part of our daily lives. They are, from a functional point of view, an extension of our human abilities. Therefore, it is well known that our devices are a valuable source of electronic evidence (e.g. network events, user-generated events, user data) that can shed light on a particular case. At present, collecting and handling such electronic evidence is a very delicate process, in which different stakeholders can be involved. This is an almost artisan process; in order to avoid any doubt about the integrity of the digital evidence the majority of the cases require the involvement of humans during the seizure of evidence and the subsequent management process.

Traditional mechanisms for handling evidence are very robust but insufficient considering the new challenges that paradigms such as the *Internet of Things* (IoT) pose [1]. Until now, personal devices have been seen as containers of electronic evidence, in the same way as a corpse is analysed to find proofs to clarify the facts. However, how these devices can testify against malicious cyber-behaviours or cyber-offenses directed to harm their owners, or other individuals in a city, is not considered at all. Indeed, this will open the door to actively acquiring electronic evidence from the environment of a user (with his consent) that nowadays is inevitably lost. These new sources of evidence which have not been considered until now could be key in demonstrating unproved or hidden cyber-attacks and demotivate new ones.

The need to prepare our personal devices to cope with these open issues is the reason why the concept of *digital witness* is being defined here. The following objetives are addressed in this article:

- Formal definition of the requirements for a digital witness.
- Discussion about the feasibility of this new concept in personal devices.
- Definition of basic components to implement this concept in future works.

This article is written as follows. First, a brief background to the latest trends in electronic evidence management and other concepts related to our approach are discussed. Then we define the concept

A. Nieto, R. Roman and J. Lopez were with the Department of Computer Science, University of Malaga, Spain, e-mail: {nieto,roman,jlm}@lcc.uma.es.

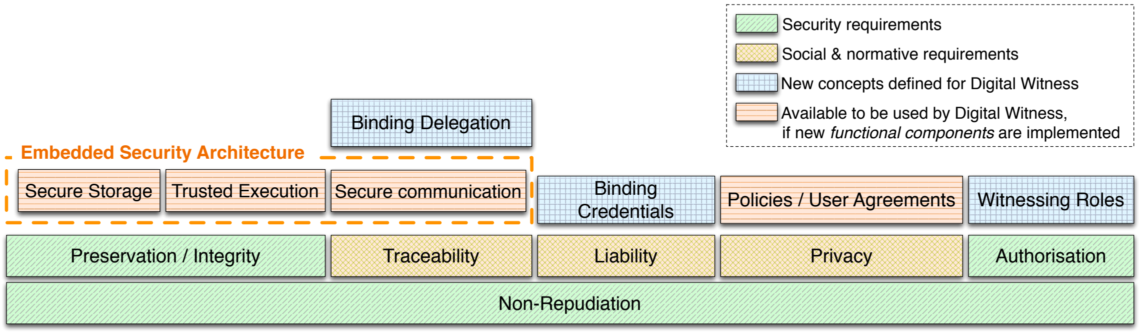
Security requirements
Social & normative requirements
New concepts defined for Digital Witness
Available to be used by Digital Witness, if new *functional components* are implemented
Binding Delegation
Embedded Security Architecture
Secure Storage
Trusted Execution
Secure communication
Binding Credentials
Policies / User Agreements
Witnessing Roles
Preservation / Integrity
Traceability
Liability
Privacy
Authorisation
Non-Repudiation

Figure 1. Requirements of a *Digital Witness* and definitions.

of *digital witness* and its requirements. After this definition, the feasibility of this new concept in personal devices given current technological trends is analysed. Finally, the relationships for the components of a digital witness are defined. Conclusions and future work are discussed at the end of the article.

II. Background

Traditionally, digital evidence is identified, collected, stored and analysed within a *Chain of Custody* to ensure the integrity, provenance and traceability of the proofs (cf. UNE 71505:2013, ISO/IEC 27042:2015). Due to the immaterial and volatile nature of digital evidence, there are extensive procedures whose aim is to ensure that this evidence is not repudiated in a court of law [2]. Furthermore, it is crucial to guarantee access to authorised entities and also identify the people who are responsible for the evidence.

Various researchers have proposed the concept of a *Digital Chain of Custody* (DCoC) [3], where certain evidence can be routed towards its destination through intermediary devices. While DCoC adds flexibility to the traditional approach, it has some drawbacks. For example, the type of evidence handled is very limited (e.g., pictures with geolocalisation), and they tend to be managed by powerful intermediary platforms (e.g., the cloud). Besides, all existing DCoC approaches require the intervention of their human owners at all times [4], [5].

Given the variety of scenarios where personal devices with limited resources (e.g. mobile user devices) are involved, including the IoT, it is necessary to explore new solutions that could include personal devices as collaborators in a DCoC. Such solutions must consider the basic requirements for digital evidence management shown in Figure 1, which are derived from the standards UNE 71505, ISO/IEC 27037 and ISO/IEC 27042. There are also standards related to digital forensics (UNE 71506, ISO/IEC 30121) that include the definition of formats and procedures during the analysis. One potential solution that we discuss in this article is to use the security architectures embedded in personal devices to define the concept of *digital witness*.

III. Digital Witness: Concept Overview

As an evolution of existing DCoC approaches, it seems reasonable to define cases in which multiple devices behave as human witnesses. Therefore, we define a *Digital Witness* as a device which is able to collaborate in the management of electronic evidence from both technological and legal standpoints. In order to realise this vision, a digital witness defines critical components to implement the security and legal requirements shown in Figure 1, and expands over various concepts and topics which are summarized in Table I. The link between the requirements and the principles behind the concept of digital witness will be detailed in the following paragraphs.

Table I
DIGITAL WITNESS - TECHNOLOGICAL LEAP.

Concept / Topic	New concept	Breakdown
Identity	Binding Credentials (BC)	• Binds all elements (*User-Device-Evidence*) • Binding Delegation – delegate evidence between witnesses
Privacy	IoT-based legal granularity	• Privacy and security policies must be accepted by the user. • The information depends on the granularity / options selected by the user.
Embedded Security Architecture	Improve the use of existing architectures in personal devices	• Solutions to store electronic evidence preserving its integrity • Electronic evidence management in compliance with standards and legal principles
IoT-Forensics	Enable heterogeneous devices to handle electronic evidence	• Taxonomy of evidence for IoT • Homogenisation of cooperative mechanisms • Objects: ranging from wearables to vehicles and buildings
Digital Chain of Custody (DCoC)	DCoC for IoT devices (DCoC-IoT)	The devices are collaborators, not only containers: • Format of documents for DCoC • Adapt security mechanisms for compliance with the standards and resources without compromising security • Hardiness of DCoC-IoT based on the user's profile
Role-based	Digital evidence management based in *inherited* roles	Acquisition of digital evidence based on the user's profile: • Digital Witness: basic digital witness to be used with the user's consent. • Digital Custodian: digital witness handled by a user with privileges (e.g., police officer authorised with a search warrant).

Digital witnesses are defined considering embedded security architectures to make use of a core of trust to i) implement trusted execution environments and ii) store and protect, with anti-tampering hardware-based solutions, the proof of *integrity* of the digital evidence. Note that the heterogeneity of solutions to do this in IoT devices requires new solutions for acquiring evidence (e.g., in propietary sensors) following IoT-forensics requirements [1], and also to homogeneise the access to security architectures as far as possible.

A digital witness also needs to prove that the user knows about the procedures that his/her device is carrying out, and therefore authorises the device to perform the acquisition, handling and processing of the evidence. This is related to the *liability* requirement; a digital witness is a powerful tool for obtaining digital evidence and how and why it is being used has to be controlled. Binding Credentials help solve this issue and also add *traceability* to the evidence during the delegation procedure. Furthermore, the user's *privacy* will be ensured according the policies accepted or not by the user. For example, certain policies can define the granularity of user's data based on the type of object and the context (e.g., a camera that reveals the number of individuals in the building but not who they are). Notice that the use of mobile devices in this approach is considered as a responsibility; the authorities should be notified of the loss or theft of a digital witness as if it were the loss or theft of an official id.

Moreover, a digital witness is defined to be collaborative, to allow the independence of a major network as in the case of DCoC approaches. Therefore, a digital witness will be able to send digital evidence to other digital witnesses or any other entity with the authority to safeguard the electronic evidence, opening the door for more varied scenarios. During this delegation of evidence, the existence of procedures such as the maintenance of a historical log will also help to keep the traceability of the digital evidence.

Finally, we consider two types of digital witnesses based on user profiles: citizen (or digital witness) and custodian (or digital custodian). While the first refers to a digital witness with the basic properties described in Table I, the second is a digital witness with privileges. This digital witness is able to perform more actions in the environment, some of them depending on search warrants properly handled by the device. So, this is a property that the device inherits from its user. Furthermore, *authorisation* is not only given by the role, this will depend on the user's identity.

IV. Technical Compliance with Requirements

The following section analyses how the new technological trends in personal devices can help implement the concept of digital witness, providing the basis on which to define the new components required (c.f., Figure 1).

A. Integrating a Core of Trust: Trusted Platform Modules and Secure Elements

In order to be used for the storage and transmission of digital evidence, these devices must employ technologies suitable for the management of digital evidence according to existing standards. Moreover, these devices should provide a protected space that cannot be tampered with, where the representative information of the electronic evidence management process can be stored.

Table II shows a representative set of hardware security devices that are integrated inside IoT devices, ranging from vehicles (e.g., TPM v2.0) to wearables (e.g., boosted NFC SE). For example, the *Trusted Platform Module* (TPM), is an anti-tampering chip that is embedded in a platform to provide a *Core of Trust* (CoT). A CoT is feasible because these chips integrate a master key that never leaves the chip, together with its own cryptographic processor that allows standarised operations. In addition, the TPM also provides support to validate the integrity of software components, allowing third-party applications using internal registers (PCRs) to store hash values.

Another, different approach is the use of a *Secure Element* (SE). An SE is integrated inside mobile devices, usually for mobile payments. However, SEs can also be used by other technologies to store keys or hashes of biometric data (e.g., fingerprints) [6]. Therefore, SEs can also be useful for providing additional security in other areas, such as the management of digital evidence.

Both the TPM and the SE also provide an additional advantage: most of these chips have mechanisms for deploying a secure communication channel (e.g., using *diffie hellman* (DH) or *Elliptic Curve DH* (ECDH)). In fact, there are also solutions for defining transactions involving a secure element, wherein the device identity is stored [7].

Note, however, that a serious limitation to these security devices is their limited storage capacity (Table III). For example, in some commercial SE chips, the available memory ranges from 800KBytes to 1.5MBytes (SLE 97 SOLID FLASH family - UICC/SIM and embedded), or from 240KBytes to 500KBytes (Boosted NFC SE - SIM, SD and microSD). This is a limitation, because digital evidence is classed as anything that is of interest given a context. So, the amount of electronic evidence can be very high. Therefore, at the very least a guarantee of integrity of the evidence (i.e. hash) must be preserved. The integrity of the digital evidence is verified if the hash matches the hash stored in the protected secure storage medium. This information is also stored in the chips and must be delegated to an entity with the necessary authority to process the digital evidence as soon as possible.

B. Schemes for Binding the User Identity

As mentioned, it is essential that a user can delegate his or her identity to the devices that act as digital witnesses, establishing an unbreakable link between a piece of evidence and the individual who generated it. One particular cryptographic primitive, *proxy signatures*, can fulfil the role of establishing

Table II
SECURITY FEATURES OF CHIPS EMBEDDED IN PERSONAL DEVICES.

Device	Asymmetric (max bits)	Symmetric (max bits)	Hash (max)	Others
TPM v2.0 (car). SE if JavaCard	RSA 2048, ECC 256	AES 128	SHA-256, HMAC	Universally Unique ID, CoT
SLE 97 SOLID FLASH Family. UICC/SIM	RSA 4096, ECC 521	3DES, AES 256	-	Fingerprint match-on-card
SLE 97 SOLID FLASH Family. eSE	RSA 2048, ECC 521	3DES, AES 256	-	Fingerprint match-on-card
OPTIGA Trust authentication chip	RSA 2048, ECC 52l	3DES, AES 256	SHA-512	GlobalPlatform ID configuration, CoT, DH/ECDH, Logs
Boosted NFC SE. SIM, SD and microSD with integrated antenna	RSA 4096, ECC 521	3DES, AES	-	-

Table III
OTHER FEATURES OF CHIPS EMBEDDED IN PERSONAL DEVICES.

Device	Memory (up to)	Interface	SDK
TPM v2.0 (car). SE if JavaCard	1.6KB	APDU for communication with SE	tpm-tools
SLE 97 SOLID FLASH Family. UICC/SIM and eSE.	1.5MB	ISO/IEC 7816, SWP	Application Development Toolkit, Java Card
OPTIGA Trust authentication chip	150KB	ISO/IEC 7816 UART (400kbps)	Crypto applets, host source code, Java Card
Boosted NFC SE. SIM, SD and microSD with integrated antenna	500KB	ISO/IEC 7816, ISO/IEC 14443	-

a link between a user and the information generated by his/her devices. [8]. In fact, all strategies that can be used to implement this particular cryptographic primitive allow us to create this link.

In the most basic approach, known as (*full delegation*, FD), the user delegates the use of his/her own private key to his/her digital witness device. This private key can then be used to sign the evidence. Another strategy (*delegation by warrant*, DbW) involves the use of a token (*warrant*), signed by the private key of the user. This token, which includes several fields such as the identity of the device and the validity period of the token itself, is stored within the device and appended to all pieces of evidence. All evidence is then signed using the private key of the device. Finally, in the last approach (PK), the user's private key is used to generate a pair of private and public keys, which, in turn are used by the device to sign the evidence. As these keys are associated with the user's identity (e.g. using identity-based cryptography [9]), it is possible to check the identity of the user who generated the evidence. In this article, we refer to the outcome of these approaches, or the outcome of any mechanism that provides a link between a user and his device, as *Binding Credentials* (BCs).

However there are some requirements that must be fulfilled in order to use the output of *proxy signatures* as binding credentials in the context of digital witnesses. First, it is mandatory for users to own a pair of public and private keys, and such keys must be linked to the identity of the person themselves. Second, the private key must be properly secured in a secure element that allows digital signature operations. Both requirements can be fulfilled by using technologies such as SIM/UICC cards and electronic identity cards.

In the first case (SIM/UICC cards), according to the 3GPP standard TS 33.221 [10], it is possible

– with the assistance of the telecommunications operator – to include certificates and private keys within the UICC. Moreover, as several countries require the mandatory registration of SIM card users by means of a national identity card or passport, all the information stored within a SIM/UICC card (including identifiers such as IMSI, MSISDN [11]) can be used to identify a particular individual. In this case, the evidence management system is developed in collaboration with the operator, becoming part of the services that are included within the UICC. This not only allows the SIM/UICC identifiers to be included within the evidence, but it also means that the evidence inside the UICC itself is signed.

Electronic identity cards (eIDs, such as the Spanish DNI-e), have a secure element preloaded with personal information (e.g. national ID, fingerprints), including a pair of private and public keys. By using the interfaces of the eID card, a natural person can be authenticated for a device or service using that card [12]. Such interfaces can also be used to meet the aforementioned requirements: the eID can act as a secure element, generating the necessary binding credentials using the private keys contained therein. Moreover, as the key pairs contained within an eID are issued by the government, there is no need to involve an industrial trusted third party in the management of the evidence. Furthermore, thanks to research projects like STORK2 [13], different national eIDs can interoperate with each other.

C. *Delegation of Evidence between Entities*

Figure 2 shows the basic steps to delegate one or more pieces of evidence between digital witnesses. We call this delegation procedure *Binding Delegation* because the first step depends on the agreement with the policies and creation of binding credentials.

This delegation procedure can be performed in an ad-hoc fashion, where the evidence is obtained and transmitted by different types of digital witnesses, as soon as possible, considering the role and characteristics of the digital witness. For example, a personal device belonging to a civilian always has to send the evidence to a digital custodian at the end of the DCoC-IoT. However, a digital custodian will never send evidence to a digital witness, it only collaborates with other digital custodians. The final destination of the evidence is an Official Collection Point of evidence (e.g., a building acting as a digital witness with more resources). In this last point of storage the evidence is processed.

During this entire transmission process, the DCoC has to be maintained. In order to do so, we follow a specific procedure that is detailed in the following paragraphs.

When the evidence is obtained, a header is generated with relevant information according to a format for electronic evidence (e.g. [14]) adapted to the requirements of the digital witness. During this process, an identifier of the evidence is generated using the binding credentials of the electronic device that generates the evidence and the timestamp. This identifier is present throughout the life cycle of the digital evidence. The digital evidence and the probative value are stored according to the criteria of secure, anti-tampering storage. The signature process depends on the mechanism chosen to perform the binding of the identity of the user to the device.

At some point, an entity A will need to delegate the evidence (e.g. the evidence is considered critical, a strong digital custodian is located in the vicinity, the device reaches the permitted threshold for storage). The choice of the next digital witness B is subject to compliance with several requirements: (i) B can attest that it is a digital witness and its role/level, (ii) B is a digital witness at the same level as A or higher, (iii) B meets the criteria for safeguarding the electronic evidence, (iv) B is the best candidate (e.g. B minimises the number of jumps to the collection point), and (v) B is a digital custodian and requests the evidence from A, and A can verify the identity of B.

Once witness B has been chosen, the information concerning the electronic evidence is sent over a secure channel. B then authenticates the electronic evidence and proceeds to safeguard it. In this step, B generates its own evidence to prove the reception of this evidence in its *historical of evidence*. The historical of evidence (or historical), is a summary of the evidence that has been handled, and ensures the traceability of the evidence. Then, B sends A

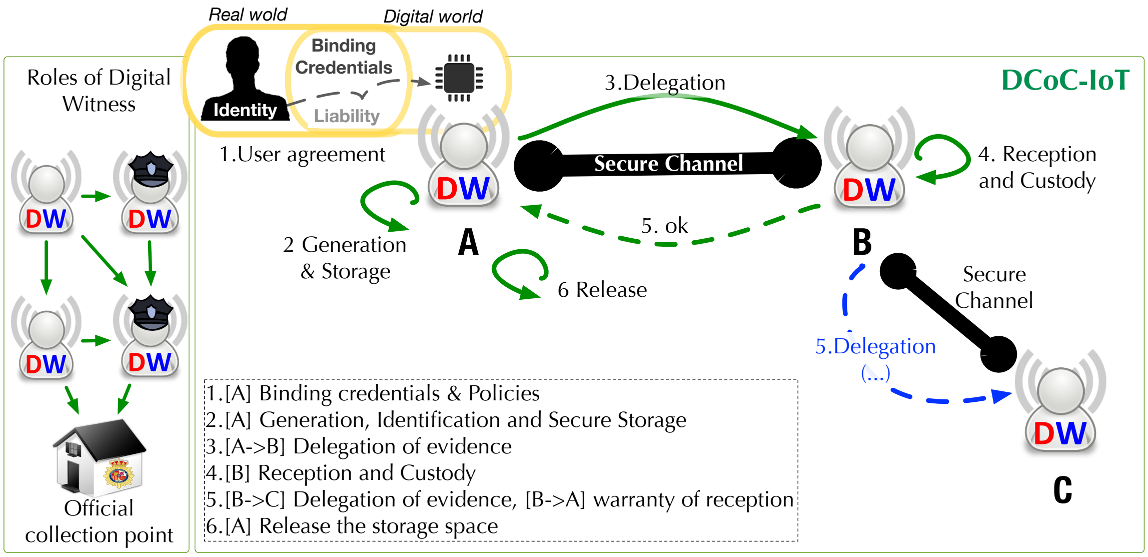

Figure 2. Binding Delegation.

the proof, indicating that the reception and storage of the evidence has been possible – a reception guarantee. If B does not send the proof, A records in its historical that the evidence was sent to B, but that the evidence has not been deleted in A. The reception guarantee is stored in the historical. Finally, A can release the storage space that was occupied by the evidence or the sets of evidence.

V. Functional Components and Relationships

Building on the analysis developed in the previous section, this section describes the main components that embodies the basic concept of a digital witness. These components enable the basic security architecture to acquire electronic evidence in dynamic, heterogeneous and distributed IoT scenarios. To do so, the requirements of the lifecycle of digital evidence are considered [5], [7], [14].

The functional requirements for digital witnesses must provide, at the very least, the components shown in Figure 3. As can be seen, ideally these components are provided or implemented using the basic capabilities of a secure element. The main components of this architecture are: the *Operations Manager User-Device* (OMUD), contract manager, cryptographic mechanisms, secure storage with access control, and *Digital Evidence Manager* (DEM).

The OMUD allows the identity of a user to be linked with his/her personal device. As a result, it generates a set of binding credentials that are used throughout the Digital Evidence Management process. In addition, it provides additional options such as request biometric inputs.

The contract manager is an optional component that advises as to the cryptographic mechanisms that are admissible in a court of law, and the different configuration alternatives for managing the evidence, such as the granularity of the data collected. When a digital witness requests advice from a contract manager, the system stores a proof about the advice given by the contract manager. If this component is not used the digital witness must be manually configured to use the cryptographic mechanisms that are allowed. These cryptographic mechanisms are implemented within a secure element, which is then used during the management process, and probably (but not necessarily) by the OMUD. Moreover, the keys and other critical resources (e.g., hashes, SAs, BCs) should be stored

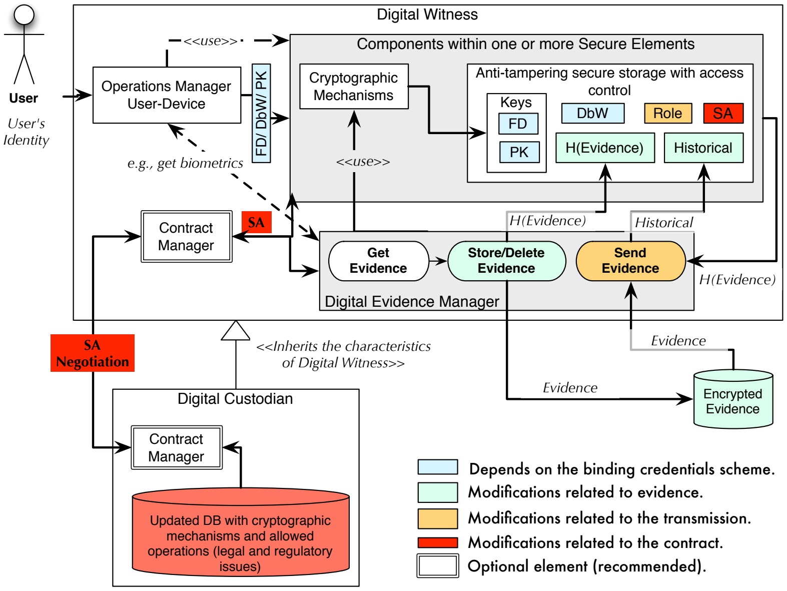
Digital Witness
User
User's Identity
<<use>>
Components within one or more Secure Elements
Operations Manager User-Device
FD/ DbW/ PK
Cryptographic Mechanisms
Anti-tampering secure storage with access control
Keys
FD
PK
DbW
Role
SA
H(Evidence)
Historical
<<use>>
e.g., get biometrics
Contract Manager
SA
H(Evidence)
Historical
Get Evidence
Store/Delete Evidence
Send Evidence
H(Evidence)
Digital Evidence Manager
SA Negotiation
<<Inherits the characteristics of Digital Witness>>
Evidence
Evidence
Encrypted Evidence
Digital Custodian
Contract Manager
Updated DB with cryptographic mechanisms and allowed operations (legal and regulatory issues)
Depends on the binding credentials scheme.
Modifications related to evidence.
Modifications related to the transmission.
Modifications related to the contract.
Optional element (recommended).

Figure 3. Functional requirements for digital witness based on Binding Credentials).

using the secure element.

Finally, the DEM coordinates the processes of the lifecycle of the digital evidence within the digital witness: generation, identification, secure storage, delegation, etc. [14].

A. *Interaction between components*

We define three basic cases of communication between the components shown in Figure 3:

C1 Establishment of action policies for the use of digital witnesses.
C2 Creation of binding credentials (BCs).
C3 DEM using BCs, delegation of evidence.

In C1, the objective is to define the cryptographic mechanisms and configurations that are acceptable, and those additional policies that are necessary to define the behaviour of the digital witness. We classify the policies in two groups. The first group (GP1, *Group Policy 1*) defines policies relating the user to the device. For example, the agreement of the terms of service (without which the digital witness cannot be started), the preferences of the user, or the way in which the resources in the device are managed. The second group (GP2, *Group Policy 2*) contains the policies used by the DEM (e.g. generation of evidence, transmission of evidence, storage and deletion of evidence).

The GP1 policies, which are more general, are negotiated between the user and the OMUD, while the policies in GP2 are set up through the DEM. Once accepted, all policies become part of the *Security Associations* (SA) that define the behaviour of the digital witness, and are safeguarded as electronic evidence, thus constituting a proof of the negotiation between the physical user and the digital witness. Subsequently, the policies are checked for each component, and the integrity of the policies files is periodically checked using the corresponding hash. Note that all policies include the list of security and cryptographic mechanisms that are accepted for each case, and consider the list of aforementioned requirements.

In C2, the OMUD is responsible for creating the credentials (passwords or tokens) that link the user to the device. The BCs are used transparently by the DEM to handle the evidence (e.g., storage, transmission) and the historical data. For this reason, these BCs have to be defined following the requirements discussed above, and generated using cryptographic accepted mechanisms available in the digital witness. Moreover, the BCs are stored in an anti-tampering device within the digital witness.

In C3, we detail the internal behaviour of the components when implementing the delegation procedure described earlier. The evidence is obtained using forensic mechanisms that are accepted in a court of law. The hash of the electronic evidence is created using the appropriate cryptographic mechanisms and is stored inside the protected area of the secure element when this functionality is available in the digital witness. Otherwise, the DEM is responsible for writing the resulting hash value in the storage space. In any case, when new evidence is acquired or used, the historical of evidence must be updated.

Regarding the delegation of evidence, first the next witness in the chain (candidate for the delegation) is chosen according to the criteria previously described. Note that the next witness can be chosen in a local context (e.g. hop-by-hop communication) or in a global context (e.g. Internet) if other communication methods and peers are available. The evidence (in this case the hash of the evidence) and the historical are then sent to the next witness in the chain using secure communication channels, which are built using accepted cryptographic mechanisms, and stating the BCs that demonstrate the link between the user and the device. Finally, regardless of the result of the delegation (whether or not it was possible to delegate the evidence), the historical is updated and the supporting data for the operations (digital proof of the operations) are stored in the digital witness.

B. *Optional interaction between components*

Case C1 can be improved by using the optional component Contract Manager to set up the policies for managing electronic evidence. In this case, the Contract Manager is responsible for assessing the best configuration that satisfies a set of criteria for the digital witness, plus other factors such as the granularity of the information.

In this scenario, the interaction mostly occurs between the Contract Manager and the DEM. The Contract Manager advises the DEM of the acceptable configurations for managing electronic evidence, in accordance with the security level required by the legal framework and the preferences of the user. Initially, the digital witness can be configured using the default policies defined by the DEM, and, under the request from an authenticated custodian, it may update these policies according to the security association negotiated with the digital custodian. In doing so, the GP2 is updated. This update can be required at any moment, and, in fact, it can affect the terms of service or any other factor detailed in the rest of the policies. If that is the case, the modifications requested are communicated to the user for acceptance.

Another security feature that could be very useful is the use of biometric systems. Such systems can be used in case C2, just before generating the Binding Credentials, and in case C3 during the process of acquisition and/or transferring of evidence.

The elements of the architecture that most actively participate in this optional process are the User and the OMUD. Before executing any operation that requires the user's presence (e.g. transmitting a batch of evidence), the User must advise the OMUD of its availability (e.g. by responding to an alert). At this point, the OMUD will prompt the User to authenticate him or helself by using the biometric systems listed in the acceptable configuration. After the authentication process, if the validation has been successful, the OMUD will continue with the planned operations. Note that evidence will be produced whenever an operation requires the user's authentication via the biometric systems. The information stored inside this piece of evidence can range from a simple registration of the event to specific biometric information (e.g. the image of a fingerprint), if allowed.

Regarding the implementation of the biometric systems, there is one important topic that requires further analysis in future work: the registration and verification of the user's biometric data. This is important because there is no inherent guarantee that a given user account which is registered in the device belongs to the same user who created the binding credentials. Note, however, that it is possible to unambiguously prove the presence of a specific user involved in a particular operation if the biometric information provided by the user is validated against a valid source, such as a legally binding token or similar device that stores biometric information (e.g. a national eID that stores the user's fingerprints). Moreover, if this validation process is performed during the user account registration phase, then the generated biometric proof that links the biometric data with the user account will be, in turn, linked to the user's identity.

VI. Conclusions and Future Work

In this article, we have introduced and analysed the concept of *digital witnesses*. We have explained the technological solutions and approaches (e.g. secure elements, binding credentials, DCoC-IoT) that could be used to turn this particular concept into a reality. Moreover, we have defined the basic components for the deployment of digital witnesses.

Whenever a novel concept is defined, there are always some open issues that must be considered in order to further refine and expand the applicability of that particular concept. In this article we have shown that it is possible to design a digital witness for mobile user devices and personal networks; however this particular design, which is based on the existence of a binding credential which links the identity of the object to the identity of a person, might not be applicable in all IoT contexts. This is because certain devices might not have unique identities, or even just one owner. Therefore, future work will be to implement the solution proposed in this article, but also to analyse use cases within IoT environments that have not been analysed here.

Acknowledgment

This work has been funded by the Spanish Ministry of Economy and Competitiveness through the project IoTest (TIN2015-72634-EXP), https://www.nics.uma.es/projects/iotest.

References

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

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

[4] 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.

[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] R. Sanchez-Reillo, D. Sierra-Ramos, R. Estrada-Casarrubios, and J. A. Amores-Duran, "Strengths, weaknesses and recommendations in implementing biometrics in mobile devices," in *Security Technology (ICCST), 2014 International Carnahan Conference on*. IEEE, 2014, pp. 1–6.

[7] 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.

[8] 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

[9] 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

[10] 3GPP TS 33.221: Support for Subscriber Certificates, http://www.3gpp.org/DynaReport/33221.htm, Accessed on April 2015.

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

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

Ana Nieto is postdoc researcher at the University of Malaga (Spain). She received her M.Sc. in Computer Engineering in 2008 and her Ph.D. in Computer Science in 2015. She has relevant publications in the topic of Security and Quality of Service (QoS) tradeoffs. Her current research activities are mainly focused on IoT-forensics; she is involved in new research topics related to *digital witnessing*.

Rodrigo Roman is a security researcher working at the University of Malaga (Spain), where he obtained his Ph.D. and M.Sc. degrees in Computer Engineering and Computer Science, respectively, in 2008 and 2003. Previously, he worked for the Institute of Infocomm Research (I2R) in Singapore in the areas of sensor network security and cloud security. Pursuing to make security simple and usable, his research is focused on the development of protection mechanisms for the Internet of Things and related paradigms, such as cloud computing and fog computing.

Javier Lopez is Full Professor, and his research activities focus on network and protocols security, where he has led more than fifty research projects and has co-authored above two hundred papers. He is Editor-in-chief of the “International Journal of Information Security”, and member of the editorial boards of “IEEE Wireless Communications” and “IEEE Internet of Things Journal”. He also is the Spanish representative at “IFIP Technical Committee 11 âĂŞ Security and Protection in Information Processing Systems”.