NECS
EUROPEAN NETWORK FOR CYBERSECURITY

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

Ana Nieto

Network, Information and Computer Security Lab

NICS
Network, Information and Computer Security Lab

22 May 2017

Contents

Plan

Computer Forensics - Definition

Definition

Digital forensics is "represented by the application of forensic science disciplines to electronic-based crime scenes following certain legal procedures." (E.Casey).

Known principles:

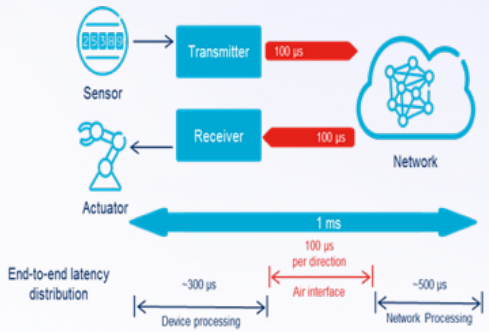
- Locard's Exchange Principle (1877-1966): "with contact between two items, there will be an exchange".
- Daubert Standard (1993): Any scientific evidence presented in a trial has to have been retrieved and tested by the relevant scientific community.

Computer forensics is **NOT** data recovery.

Computer Forensics - Definition

Definition

Digital forensics is "represented by the application of forensic science disciplines to electronic-based crime scenes following certain legal procedures." (E.Casey).



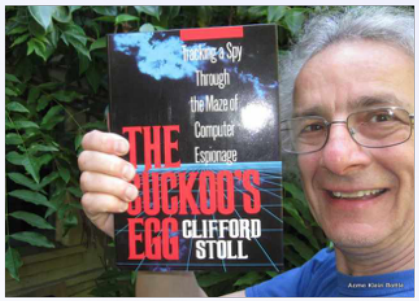
Computer Forensics - Characteristics

- Digital evidence is identifed, collecteed, stored, and analyzed within a **Chain of Custody** to ensure the integrity, provenance, and traceability of the proof (cf. UNE 71505:2013, ISO/IEC 27042:2015).
- **Admissibility**.Due to the non-material and volatile nature of digital evidence, there are extensive procedures aimed at ensuring that this evidence is not repudiated in a **court of law**.



Computer Forensics Timeline

- 1970s - Electronic crimes - **financial sector**. Most law enforcement officers didn't know enough about computers to ask the right questions or to preserve evidence for trial.
- 1980s - Boom Personal Computers.
- 1984 - CART - Computer Analysis Response Team.
- 1988 - Morris Worm- One of the first computer worms distributed via the Internet. It was a unleashed by mistake with serious consequences. The cost of the damage at 100,000 - 10,000,000 dollars.
- 1993 - First International Conference on Computer Evidence.
- 1995 - International Organization on Computer Evidence (IOCE).
- 1998 - EnCase (Expert Witness)
- 2000 - First FBI Regional Computer Forensic Laboratory
- 2003 - FBI CART case load exceeds 6500 cases, examining 782 TBytes of data.
- 2005 - ISO/IEC 17025:2005 Accreditation of the Digital Forensics Dsicipline - ASCLD-LAB.
- 2007 - Boom Social Networks.
- 2012 - ISO/IEC 27037:2012. Guidelines for identification, collection, acquisition, and preservation of digital evidence.
- 2013 - Research article about IoT-Forensics.
- 2015 - ISO/IEC 27042, ISO/IEC 30121.
- 2016 - ISO/IEC 27050:2016 - Electronic Discovery.
- 2017 - Vehicular forensics (it is expected a good year for this topic).



Computer Forensics Standards

International:

- ISO/IEC 27037:2012. Guidelines for identification, collection, acquisition, and preservation of digital evidence.
  - "... exchange of potential digital evidence between jurisdictions."
- ISO/IEC 27042:2015 - Guidelines for the analysis and interpretation of digital evidence.
  - "... proficiency and competence of the investigative team."
- ISO/IEC 30121:2015 - Governance of digital forensic risk framework.
  - "... prepare an organization for digital investigations before they occur."

Spanish:

- UNE 71505:2013 (multi-norm). Digital Evidence Management.
- UNE 71506:2013. Computer Forensics Methodologies.

Computer Forensics Standards

- ISO/IEC 27050:2016 - Electronic Discovery -

ISO/IEC 27050-1: Overview and concepts

ISO/IEC 27050-2: Guidance for governance and management of electronic discovery

ISO/IEC 27050-3: Code of practice for electronic discovery

ISO/IEC 27050-4: ICT readiness for electronic discovery

ISO/IEC 27050:2016

Custodian

Person or entity that has custody, control or possession of ESI.

Common sources of ESI (Electronically Stored Information):

- Custodian data sources: - a single custodian
  - Computers: custodians' desktops, laptops or home computers as well as removable storage media, such as thumb fdrives, external hard drives, DVDs or CDs;
  - Mobile devices: custodians' personal devices such as mobile phones, smart phones, tablets, Global Positioning Systems (GPS), etc.
  - From an enterprise perspective, databases and applications, network storage, backups, and electronic archives, can also be considered custodian sources.

ISO/IEC 27050:2016

Custodian

Person or entity that has custody, control or possession of ESI.

Common sources of ESI (Electronically Stored Information):

- Non-custodian data sources
  - Internals to the organisation:
    - Databases and applications: EDMS, ERMS, or collaborative tools.
    - Network storage: NAS, SAN.
    - Backups.
    - Electronic archives: ESI contained in electronic or digital archives (data repository) is typically official business records, documents retained for compliance purposes, legacy documents (historical value), etc.
  - Externals to the organisation:
    - Cloud storage.
    - Social media.

ISO/IEC 27050:2016

Custodian

Person or entity that has custody, control or possession of ESI.

Common sources of ESI (Electronically Stored Information):

- Potentially excluded sources of ESI - "not all sources of ESI need to be preserved"
  - Deleted, slack, or unallocated data on hard drives;
  - Random access memory (RAM) or other ephemeral data;
  - Data in metadata fields that are frequently updated automatically, such as last-opened dates;
  - Backup data that are substantially duplicative of data that are more accessible elsewhere;
  - Test data for temporary use;
  - Other forms of ESI whose preservation requires **extraordinary affirmative measures that are not utilized in the ordinary course of business**;

ISO/IEC 27050:2016

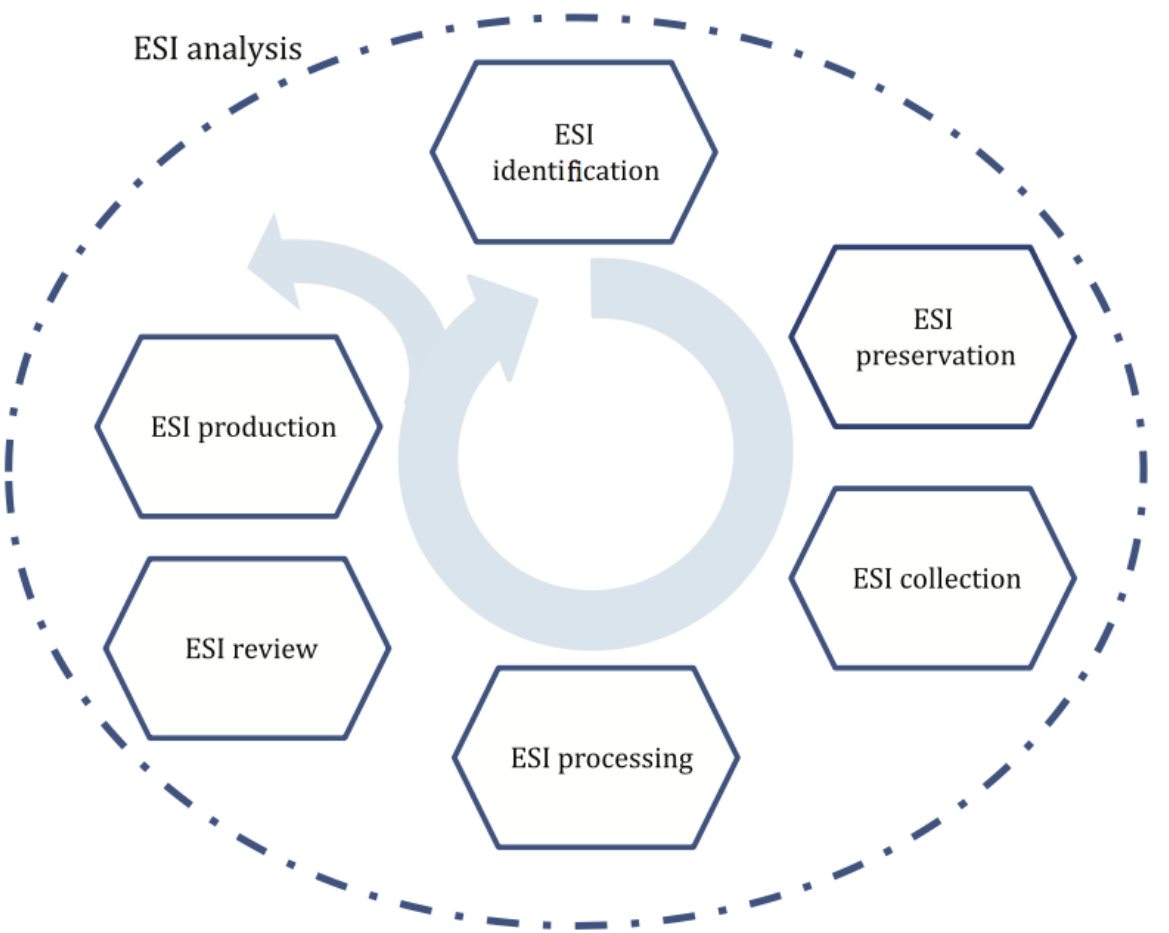


Figure 2 — Electronic discovery process elements

Tools & Techniques (Examples)

Software for *traditional* analysis:

- Apps (e.g., EnCase, AccessData FTK and MPE+, Autopsy).
- Linux packages, libraries and tools (e.g., Sleuth Kit (TSK)).
- Suites: SIFT Workstation, Kali-Linux, Caine, etc.

Tools & Techniques (Examples)

Software for *traditional* analysis:

- Apps (e.g., EnCase, AccessData FTK and MPE+, Autopsy).
- Linux packages, libraries and tools (e.g., Sleuth Kit (TSK)).
- Suites: SIFT Workstation, Kali-Linux, Caine, etc.

Hardware tools and manual techniques:

- Drive Cloning Hardware Solutions.
- JTAGulator - Access to the JTA debugging port (e.g. used for vehicle forensics).
- Chip-off - take the chips of the circuit-board.

Tools & Techniques (Examples)

Software for *traditional* analysis:

- Apps (e.g., EnCase, AccessData FTK and MPE+, Autopsy).
- Linux packages, libraries and tools (e.g., Sleuth Kit (TSK)).
- Suites: SIFT Workstation, Kali-Linux, Caine, etc.

Hardware tools and manual techniques:

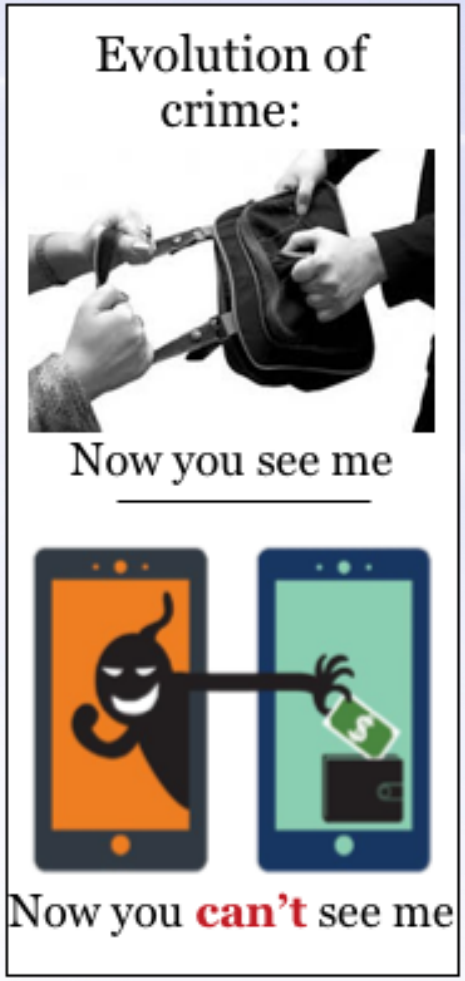
- Drive Cloning Hardware Solutions.
- JTAGulator - Access to the JTA debugging port (e.g. used for vehicle forensics).
- Chip-off - take the chips of the circuit-board.

Remote Live Forensics - Some *"agents in host"*-based solutions:

- Google Rapid Response (GRR)
- Facebook osquery
- Mozilla InvestiGator (MIG)

IoT-Forensics

- One common mistake is to consider that forensic-IoT is the same as traditional forensic computing , but applied to a greater number of devices.
  - Explosion of heterogeneous devices, whose communication leaves a trace in several environments.
  - There is a need to define new forensic techniques for wearables, vehicles, etc.
- There is more:
  - There is a chain of paradigm: the scene of the crime is distributed, and
  - It will be highly impossible to understand the **context** without the **collaboration** of the participants, that are, the devices, in the environment.



IoT-Forensics

Limitations in the **standards**:

- Mechanisms to acquire digital evidence from IoT devices.
- Live Forensics
- Remote Live Forensics
- Cooperation between entities to provide digital evidences.
- Digital Chain of Custody applied to IoT.

IoT-Forensics

Limitations in the **standards**:

- Mechanisms to acquire digital evidence from IoT devices.
- Live Forensics
- Remote Live Forensics
- Cooperation between entities to provide digital evidences.
- Digital Chain of Custody applied to IoT.

Limitations in the **tools**:

- Cooperation between digital devices is not considered.
- Training required - e.g., case of vehicular forensics.

IoT-Forensics

Limitations in the **standards**:

- Mechanisms to acquire digital evidence from IoT devices.
- Live Forensics
- Remote Live Forensics
- Cooperation between entities to provide digital evidences.
- Digital Chain of Custody applied to IoT.

Limitations in the **tools**:

- Cooperation between digital devices is not considered.
- Training required - e.g., case of vehicular forensics.

Some **IoT-Forensic** approaches:

- Focuses on how to acquire digital evidence from the IoT devices - containers of digital evidence.
- Highlight the open challenges.
- **Digital Witness**: IoT-devices as participants in the digital evidence management process.

Plan

Motivation

- To acquire environmental digital evidences requires the cooperation between devices and entities
- We need new frameworks to enable this cooperation without affecting the chain of custody and, therefore, the admissibility of the digital evidence.
- To define trustworthy IoT-entities is a clear challenge.
  - IoT devices have limited resources, so it is very difficult to apply security mechanisms without affecting the performance and main functionality/purpose of the device.
  - IoT environments are highly dynamic making very difficult (nor impossible) to store and maintain a updated record of past behaviours of digital devices.

What can we do?

Digital Witness - Definition

Definition

Personal device that is capable of...

- identifying and collecting digital evidence,
- preserve it in a protected space, and
- send it to other digital witnesses who are authorised to participate in the safeguarding of a digital evidence,
- maintaining the *traceability* of the digital evidence.

Objective

Delegation of digital evidence considering the *requirements* to a proper digital evidence management defined by the standards and/or validated by a scientific community.

Digital Witness - Definition

Definition

Personal device that is capable of...

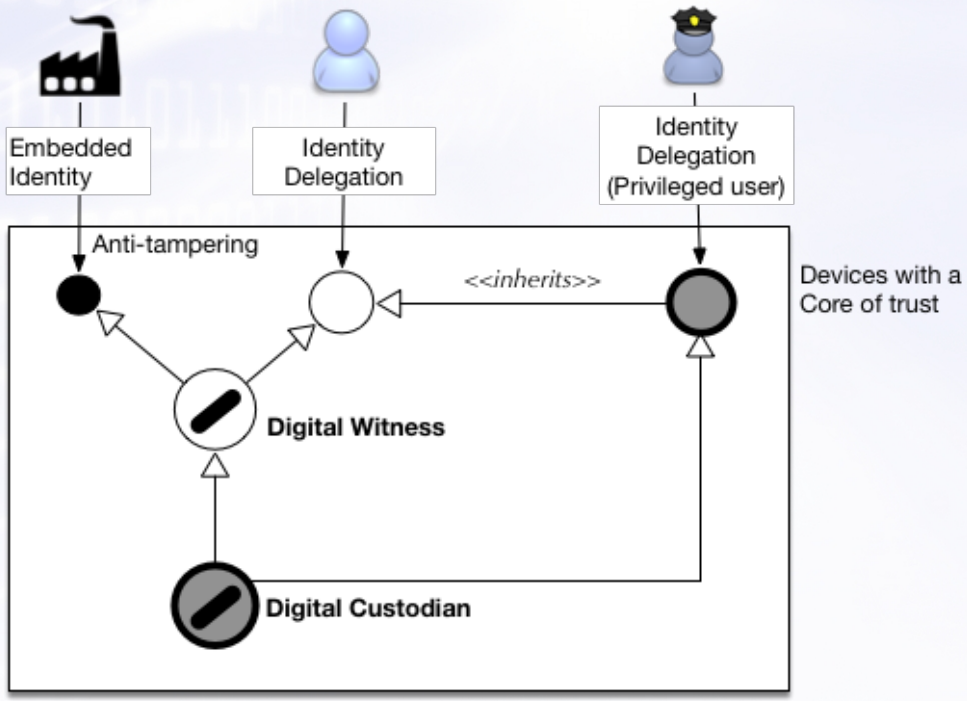
- identifying and collecting digital evidence,
- preserve it in a protected space, and
- send it to other digital witnesses who are authorised to participate in the safeguarding of a digital evidence,
- maintaining the *traceability* of the digital evidence.

Objective

Delegation of digital evidence considering the *requirements* to a proper digital evidence management defined by the standards and/or validated by a scientific community.

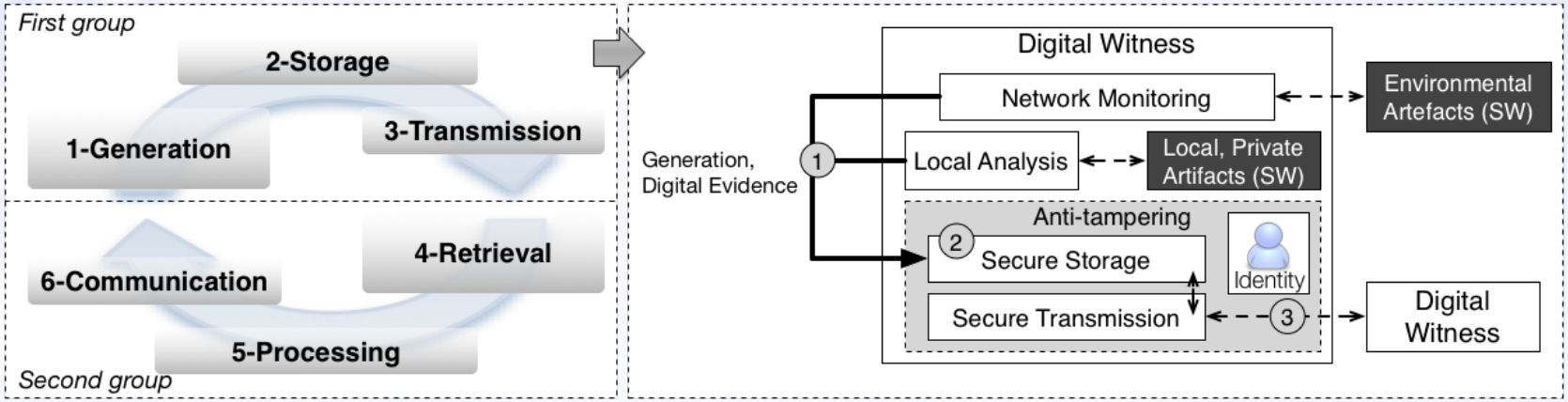
Digital Witness - Definition

- Types of digital witness (DW):
  - **Citizen** (basic DW).
  - **Custodian** (DW with privileges).
- **Game of roles:** A *digital witness* always try to delegate the digital evidence to a *digital custodian*.



Digital Witness - Definition

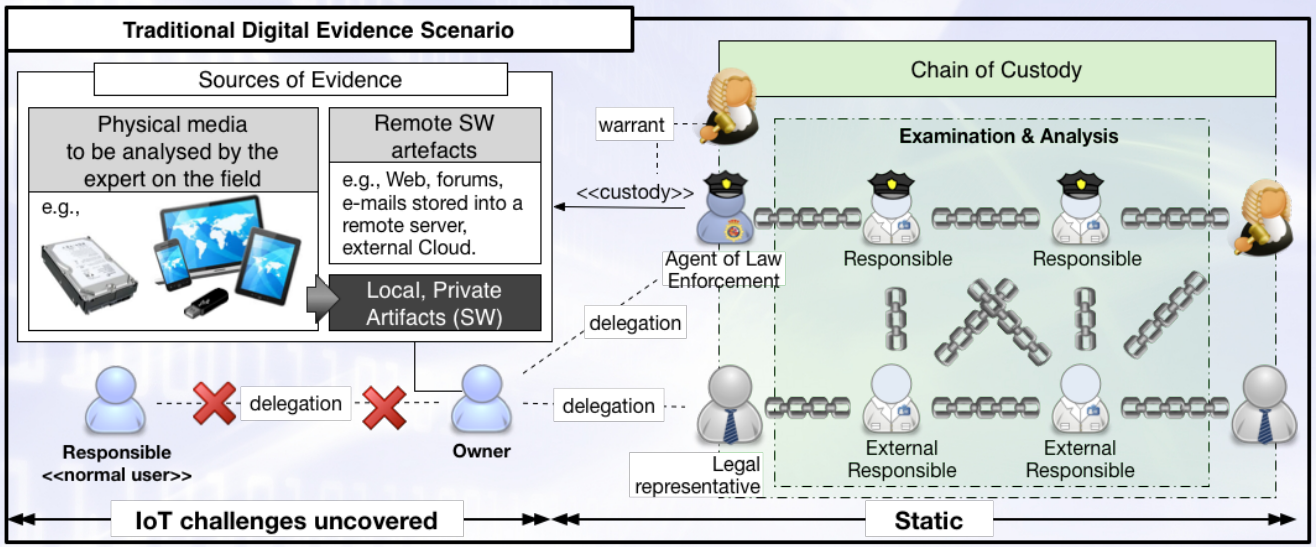
- Focused on the generation, storage and transmission of the digital evidence to an authorised entity.
- Requires anti-tampering *Trusted Computing Hardware* (TCH).
- If the device is corrupted in any way, it cannot participate in the *Digital Chain of Custody* (DCoC).

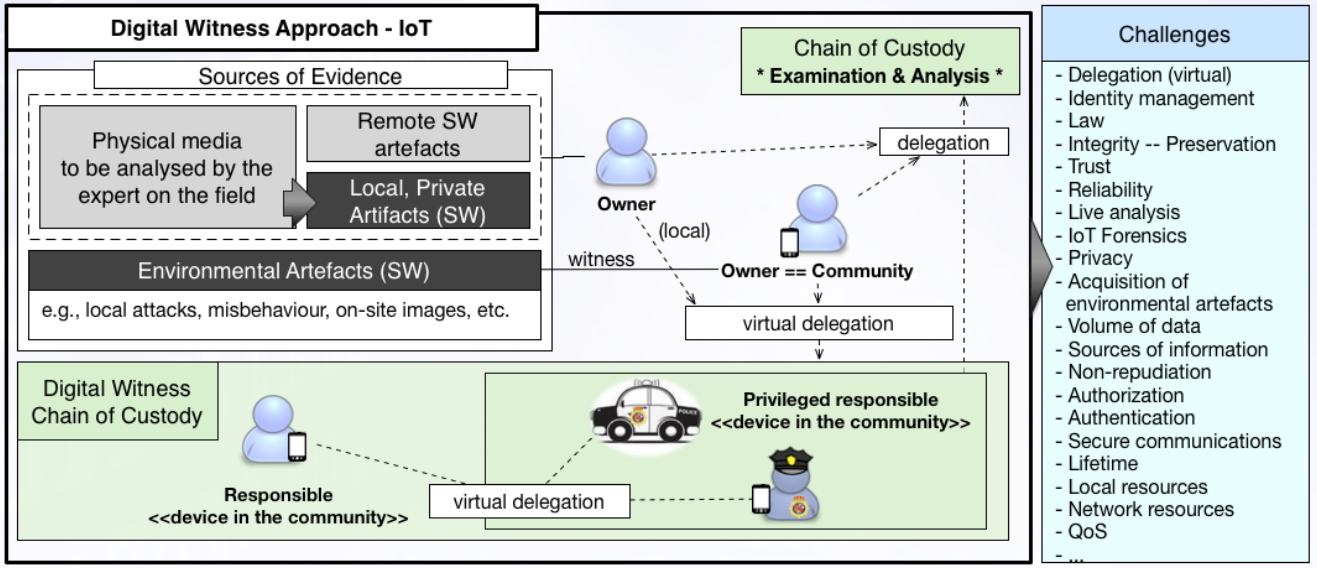


(a): LDE phases.

(b): Digital witness: Local management of digital evidences.

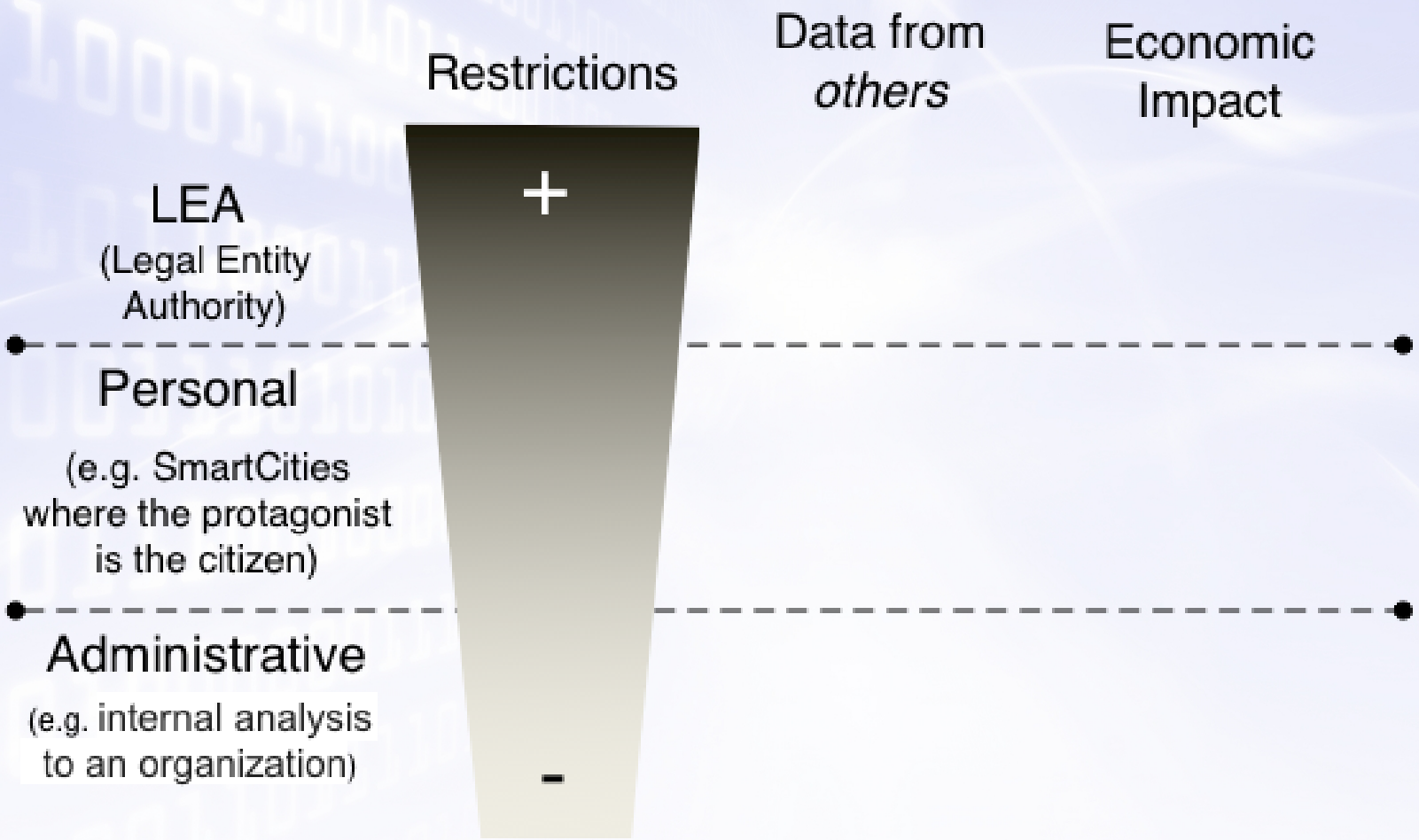
Evolution


Traditional Digital Evidence Scenario
Sources of Evidence
Physical media to be analysed by the expert on the field
e.g.,
Remote SW artefacts
e.g., Web, forums, e-mails stored into a remote server, external Cloud.
Local, Private Artifacts (SW)
Chain of Custody
warrant
Examination & Analysis
<<custody>>
Agent of Law Enforcement
Responsible
Responsible
delegation
delegation
delegation
Responsible
<<normal user>>
Owner
Legal representative
External Responsible
External Responsible
IoT challenges uncovered
Static

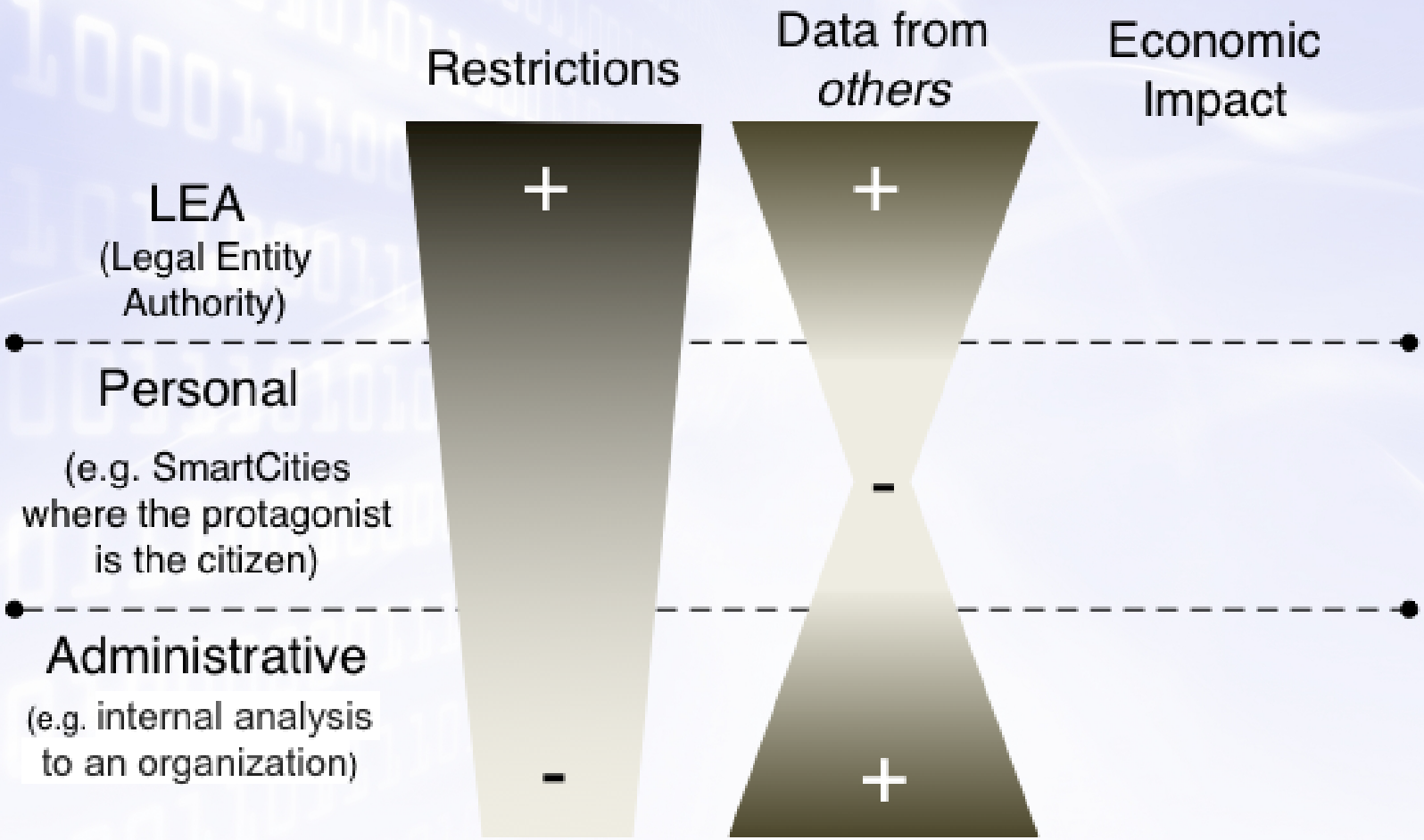

Digital Witness Approach - IoT
Sources of Evidence
Physical media to be analysed by the expert on the field
Remote SW artefacts
Local, Private Artifacts (SW)
Environmental Artefacts (SW)
e.g., local attacks, misbehaviour, on-site images, etc.
Chain of Custody
* Examination & Analysis *
Owner
delegation
(local)
Owner == Community
witness
virtual delegation
Digital Witness Chain of Custody
Privileged responsible
<<device in the community>>
Responsible
<<device in the community>>
virtual delegation
Challenges
- Delegation (virtual)
- Identity management
- Law
- Integrity -- Preservation
- Trust
- Reliability
- Live analysis
- IoT Forensics
- Privacy
- Acquisition of environmental artefacts
- Volume of data
- Sources of information
- Non-repudiation
- Authorization
- Authentication
- Secure communications
- Lifetime
- Local resources
- Network resources
- QoS

General use cases

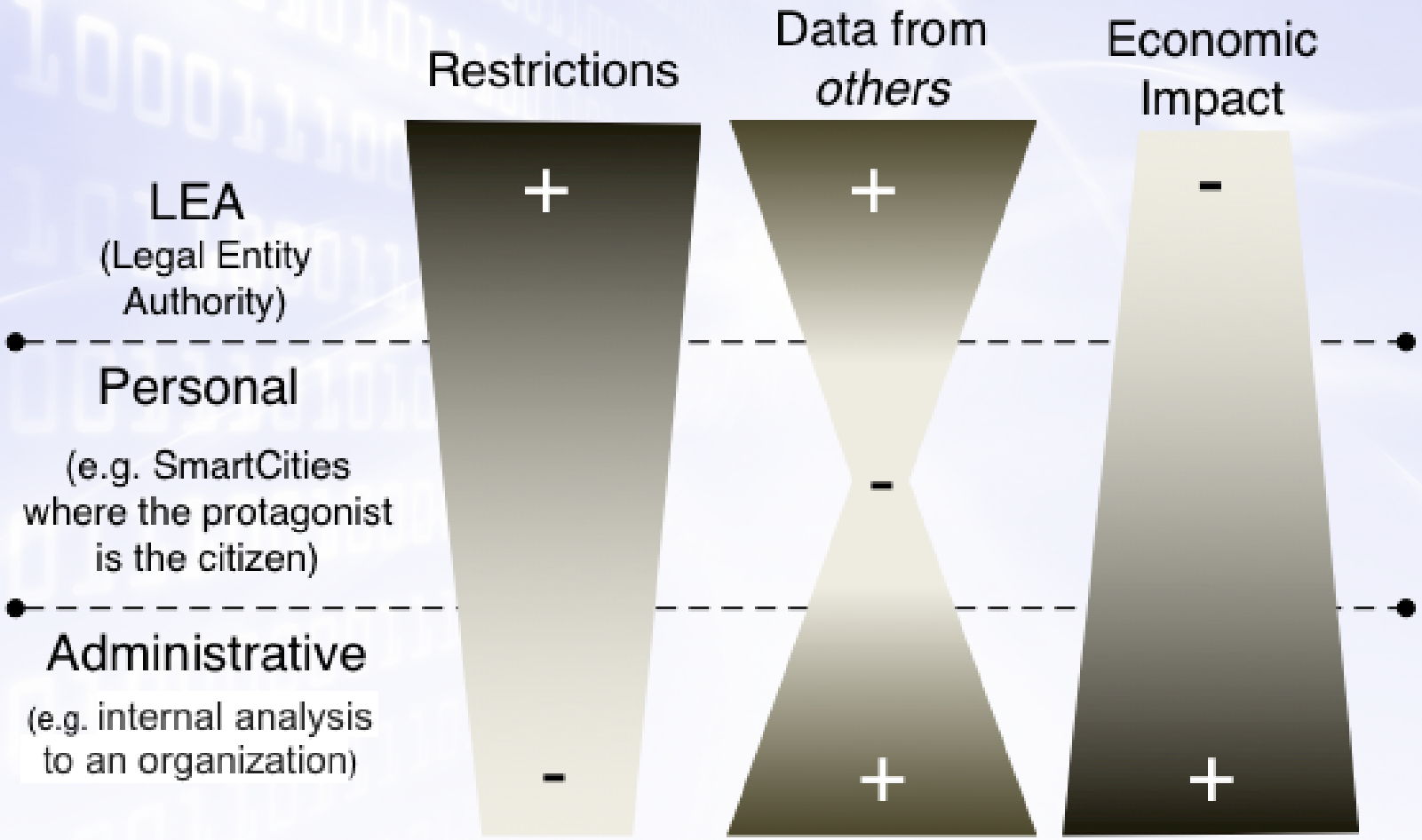
General use cases



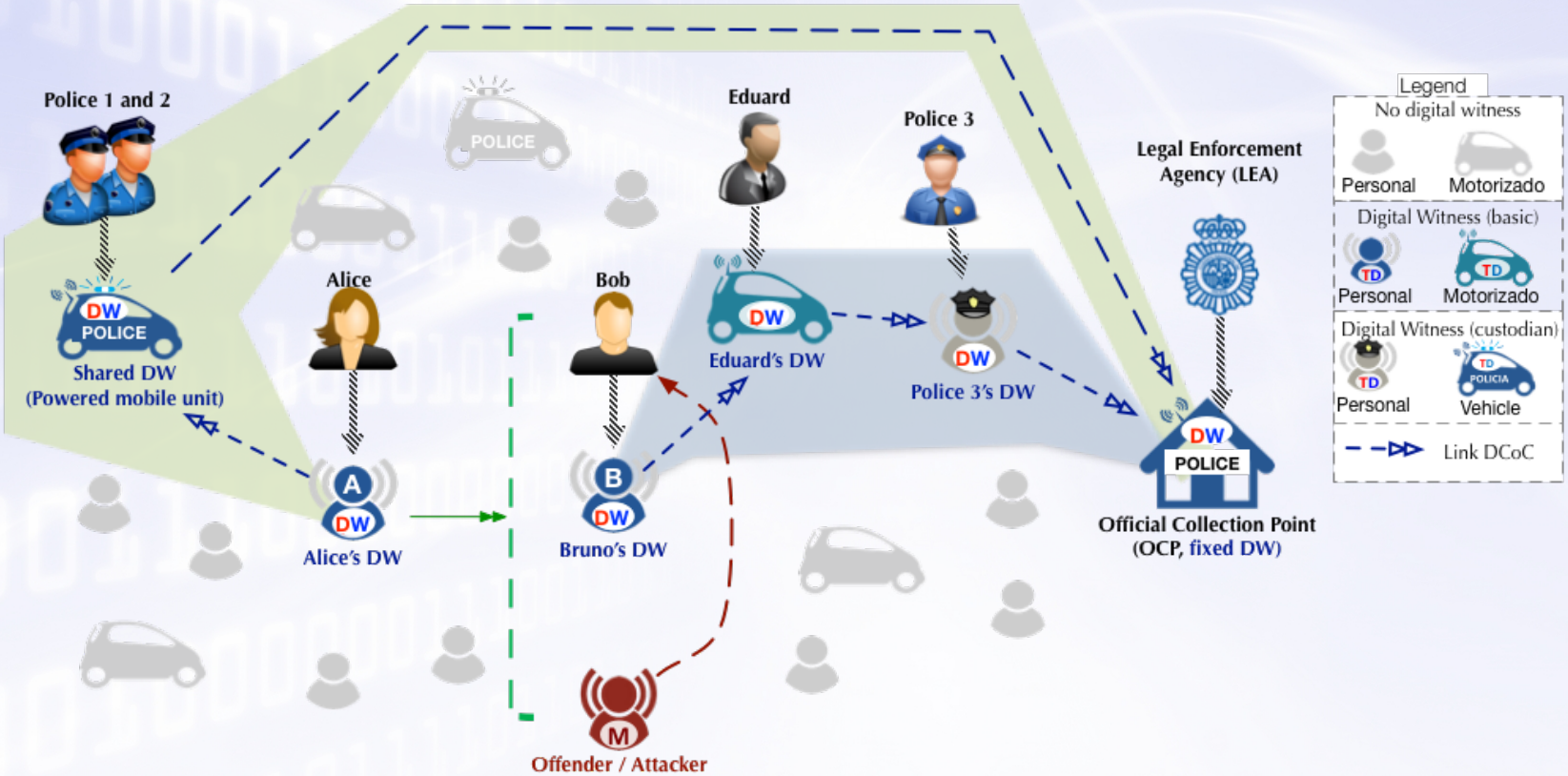
General use cases



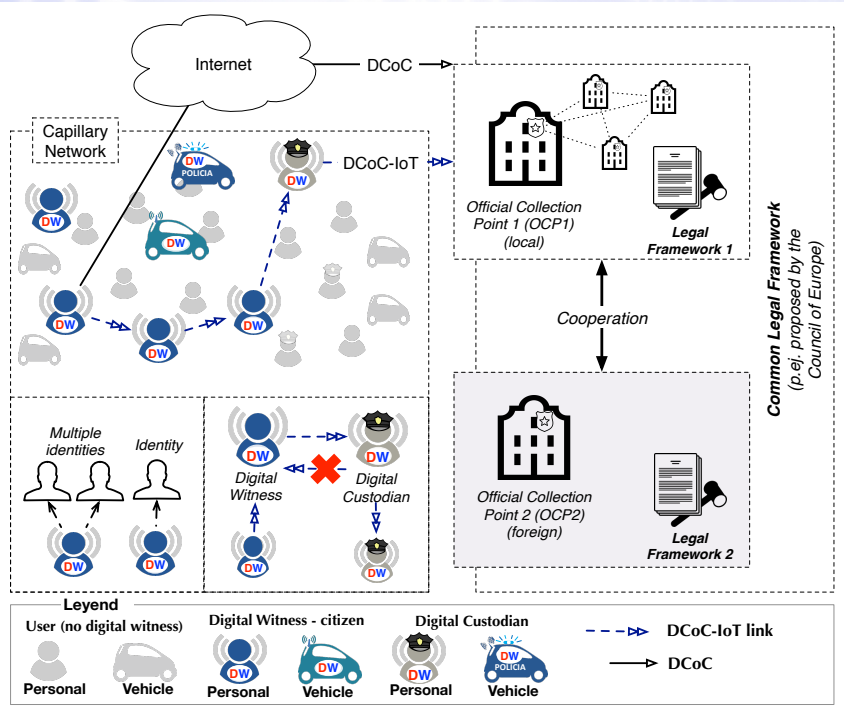
General use cases

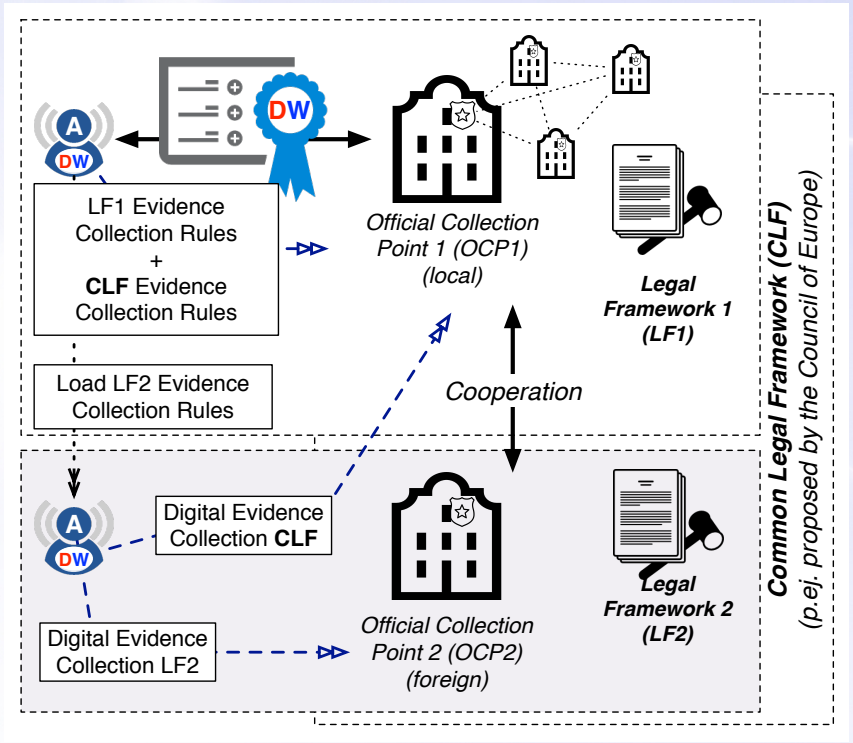


Participants (example)



Participants (example)



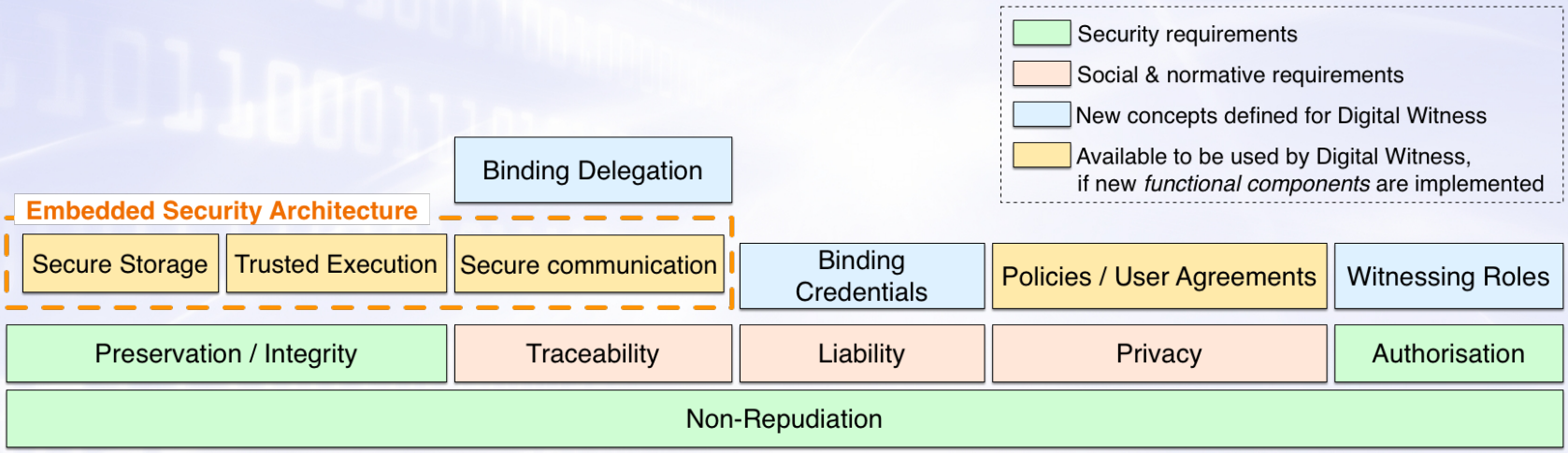


- Digital witness source (A).
- Third-party witnesses (B).
- Digital witnesses links in a DCoC-IoT.
- Digital Custodian.

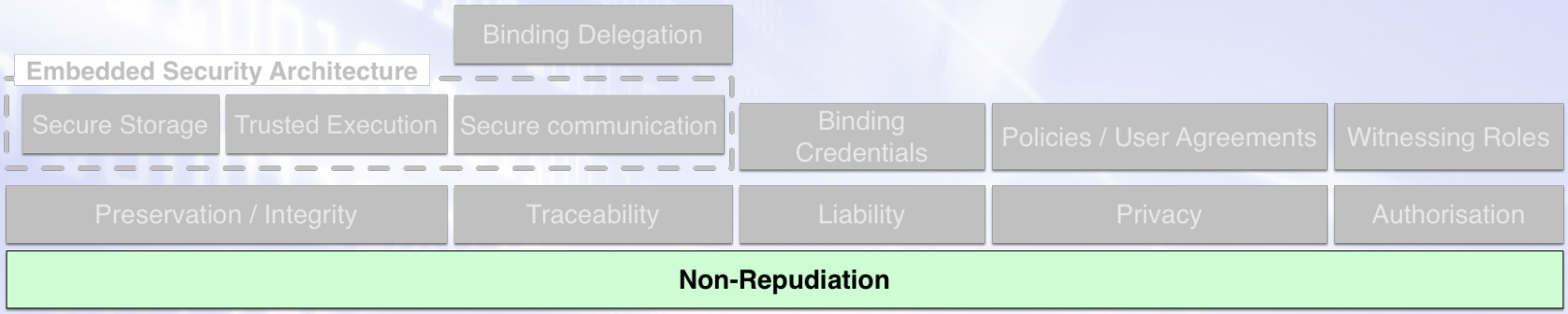
- Digital witness that changes jurisdiction (A), registered in OCP1.
- Local OCP (OCP1).
- Foreign OCP (OCP2).

Plan

Requirements - General map



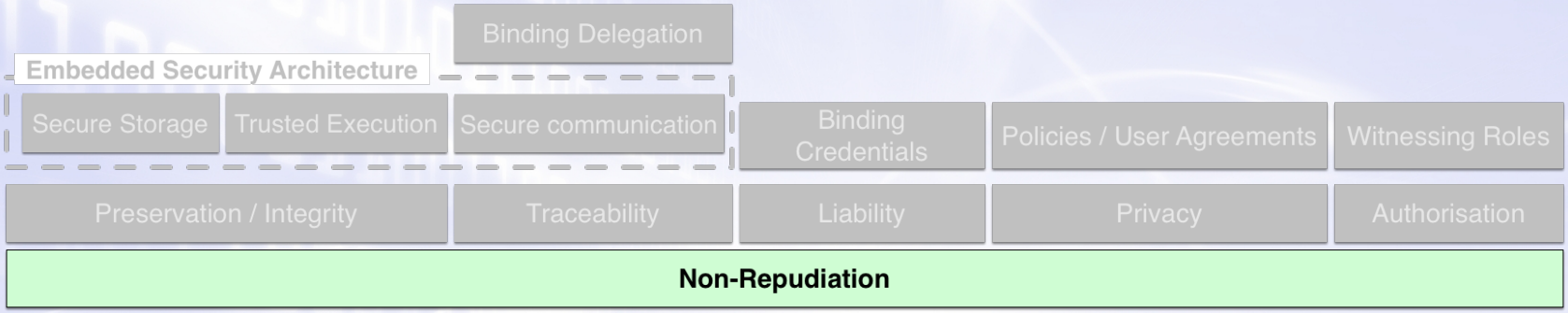
Requirements - Non-Repudiation



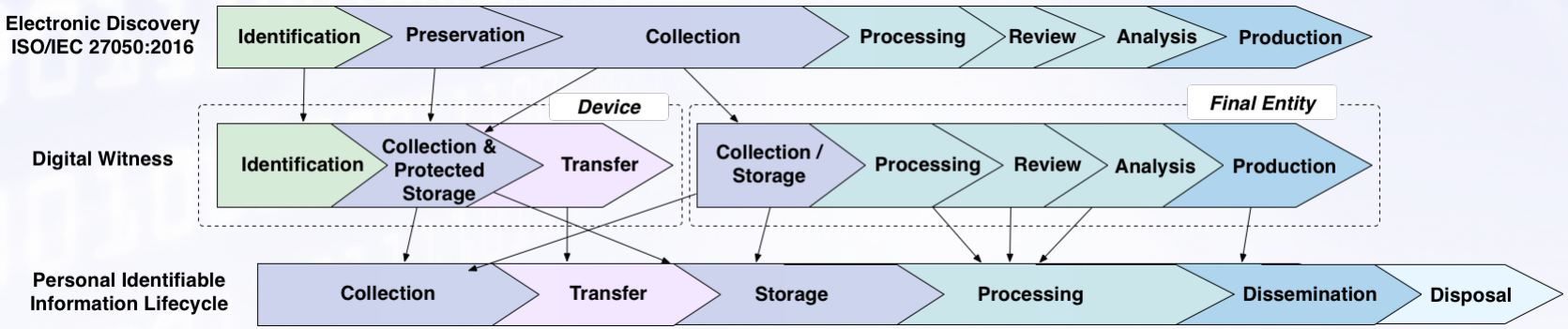
"State of affairs where the author of a statement will not be able to successfully challenge the authorship of the statement or validity of an associated contract."

- The owner of the digital witness cannot state that she/he did not authorise to her/his device to act as a digital witness.
- The entities involved during the process cannot deny their acts or involvement in the process.
- A DW will act following a set of well-defined and established standards about the digital evidence management process.

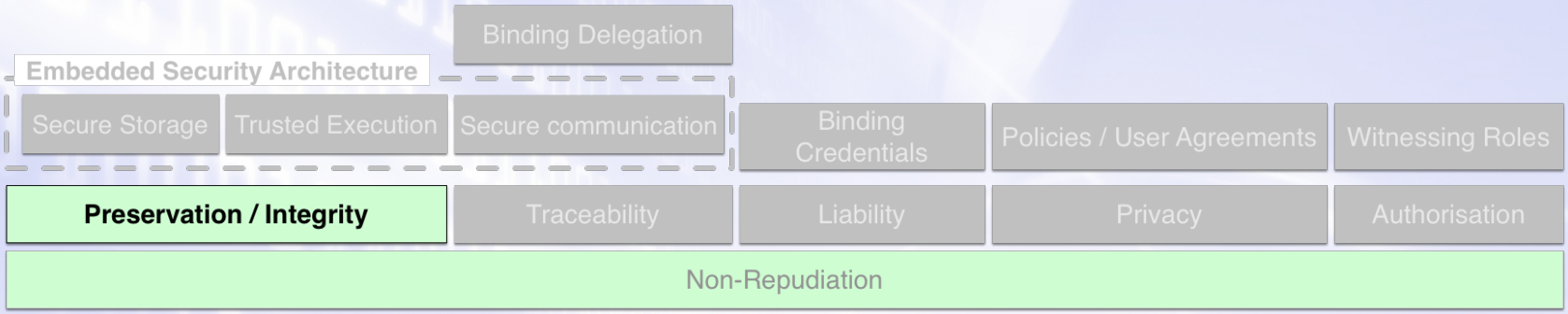
Requirements - Non-Repudiation



"State of affairs where the author of a statement will not be able to successfully challenge the authorship of the statement or validity of an associated contract."



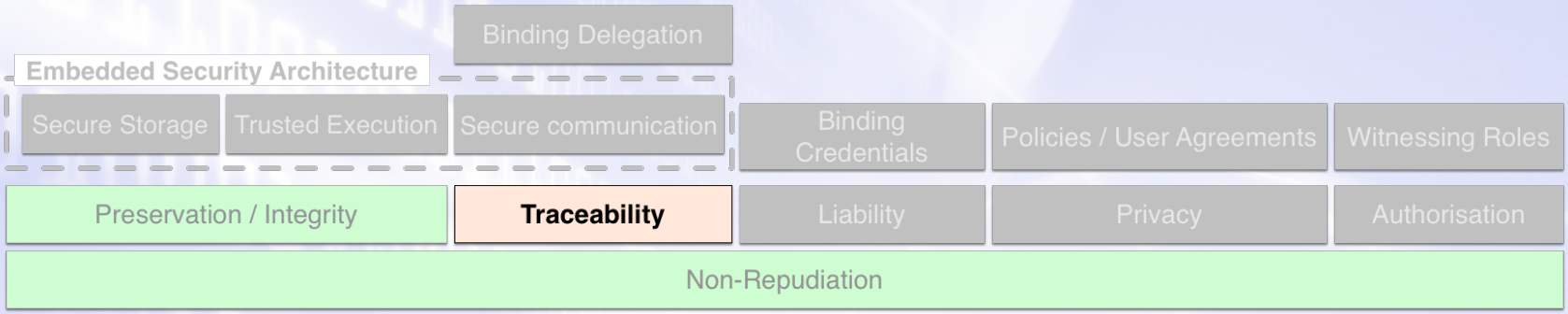
Requirements - Preservation - Integrity



"Maintaining and assuring the accuracy and completeness of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner."

- The integrity of the proof should be checked using hashes in case the volume of the data allows this.
- We consider small piece of information due the expected restrictions of capacity in the personal device. Following the normative processes the digital witness will hash the digital evidence before send it to check its integrity in a posterior phase.

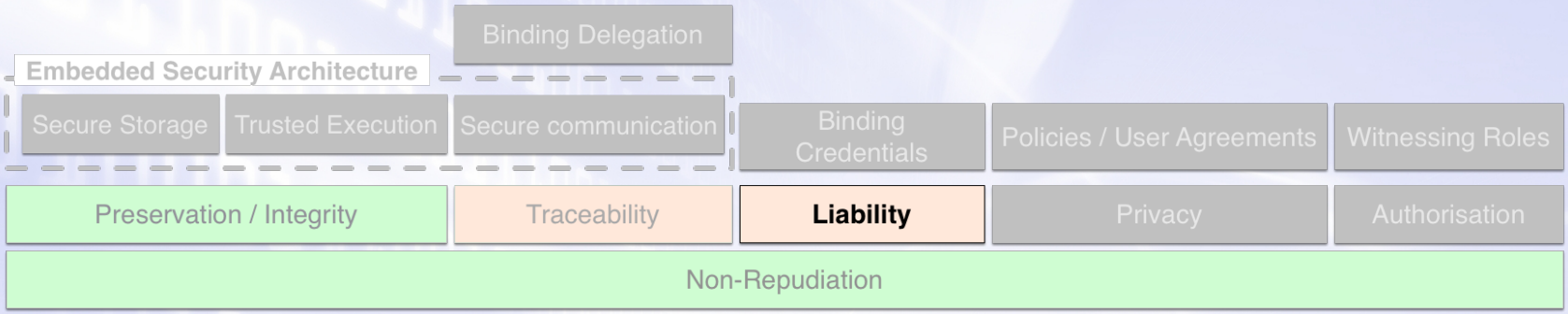
Requirements - Traceability



"Is the ability to verify the history, location, or application of an item by means of documented recorded identification."

- Affects to the provenance of the data. If this cannot be ensured, then the digital evidence can be questioned.
- In this context, the traceability ensures that it is possible to known who has access to the digital evidence at any moment.
- Binding credentials are used to determine *who*.
- During the 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.

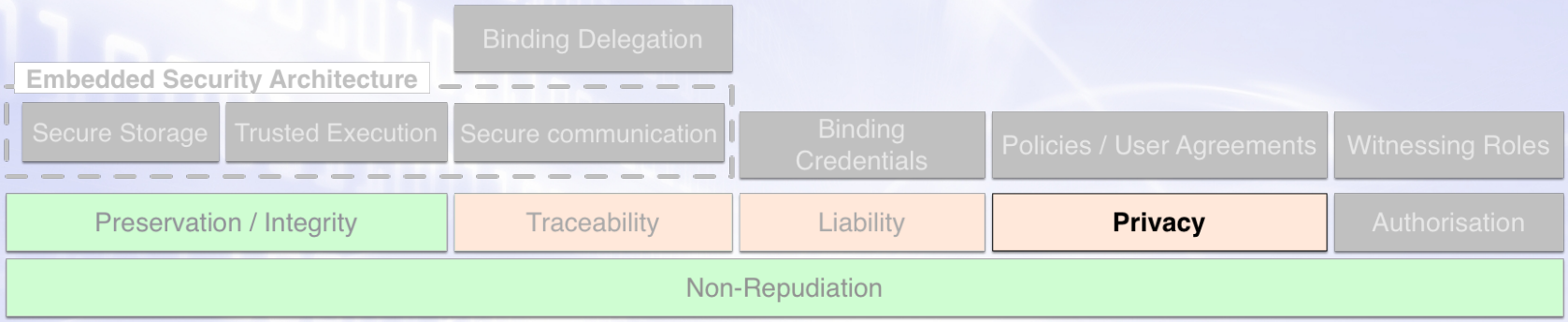
Requirements - Liability



"can mean something that is a hindrance or puts an individual or group at a disadvantage, or something someone is responsible for, or something that increases the chance of something occurring (i.e., it is a cause)."

- A digital witness is a powerful tool for obtaining digital evidence, and how and why it is being used has to be controlled.
- Liability in this sense is focused on the responsibility of using the digital witness properly.
- Liability is also applied to obtain proofs that can help to clarify the source of an offence or attack.

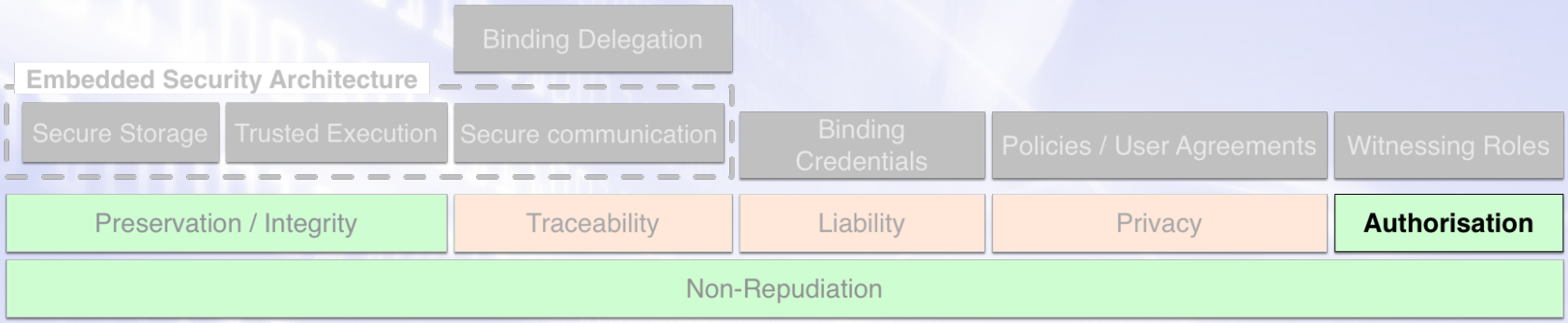
Requirements - Privacy



"Is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively."

- The user's privacy will be ensured according to the policies accepted or not by the user.
- Certain policies can define the granularity of a user's data based on the type of object and the context.

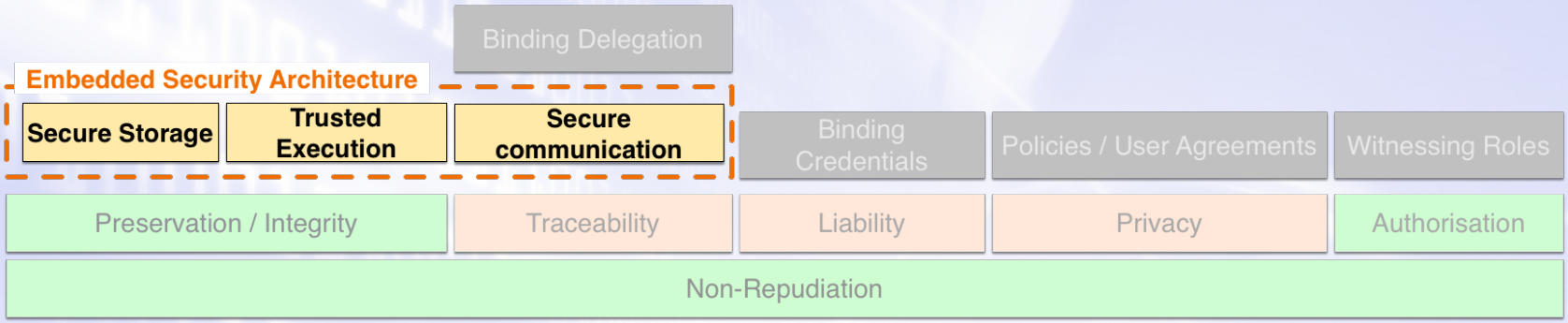
Requirements - Authorisation



"Is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular. "

- The access to the information of the user is defined by the user's policies.
- The access to the digital evidence is controlled by the binding delegation process.
- The access to the digital evidence in the OCPs can be controlled using traditional mechanisms to maintain the Chain of Custody.

Requirements - Embedded Security



Digital witnesses are defined considering embedded security architectures to make use of a core-of-trust to:

- *Implement Trusted Execution Environments.*
- *Store and Protect, with anti-tampering hardware-based solutions, the proof of* integrity *of the digital evidence.*

- The cryptographic facilities that these security chips integrate allows in many cases to deploy a secure communication.
- A digital witness is defined to be collaborative, to allow the independence of a major network as in the case of DCoC approaches.

Requirements - Embedded Security

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 2. Security features of chips embedded in personal devices.

- The IoT devices with security characteristics are from vehicles to wearables.

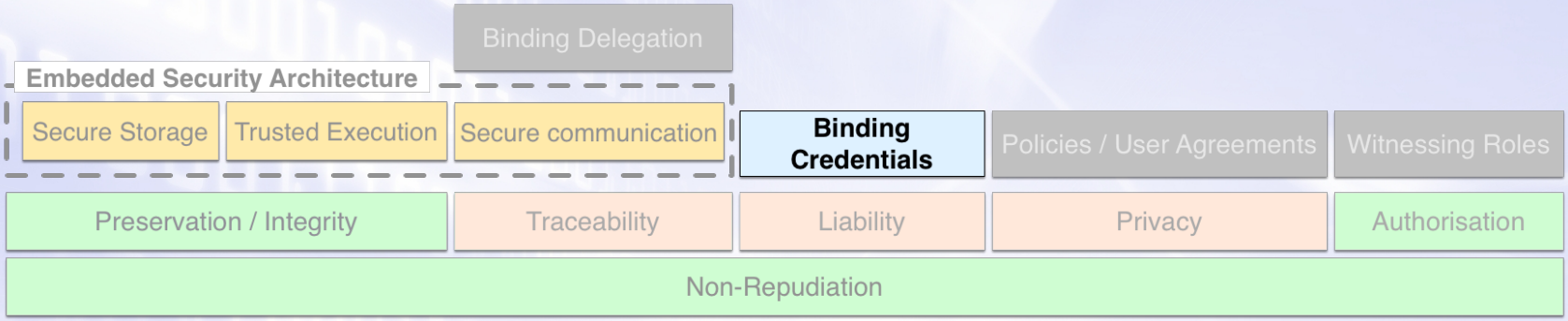
Requirements - Embedded Security

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

TABLE 3. Other features of chips embedded in personal devices.

- A serious limitation to these security devices is their limited storage capacity.
- The digital evidence stored in the chips must be delegated to an entity with the necessary authority to process the digital evidence as soon as possible.

Requirements - Binding Credentials

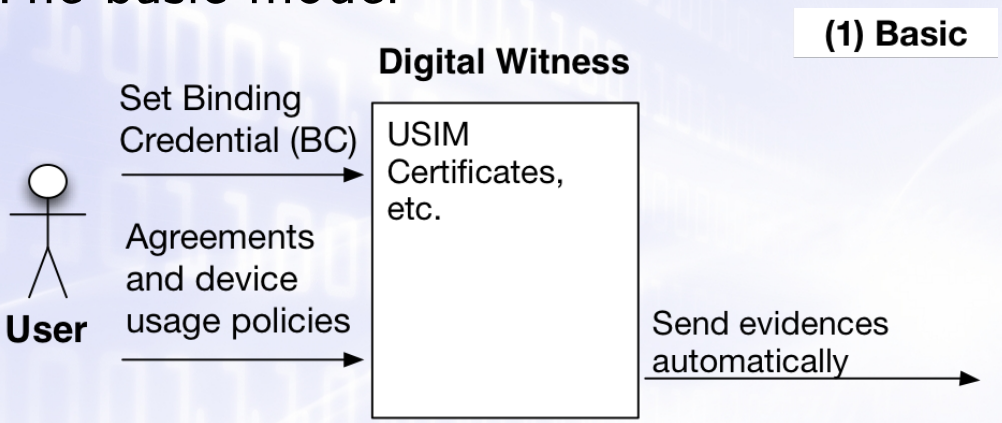


Unbreakable link between a digital evidence and the owner of the device which acquire it.

- Link between a user and the information generated by his/her devices.
- A digital witness acts in behalf of his/her user.
- A possible solution: *proxy signatures*.
- Biometrics to ensure the presence of the user.

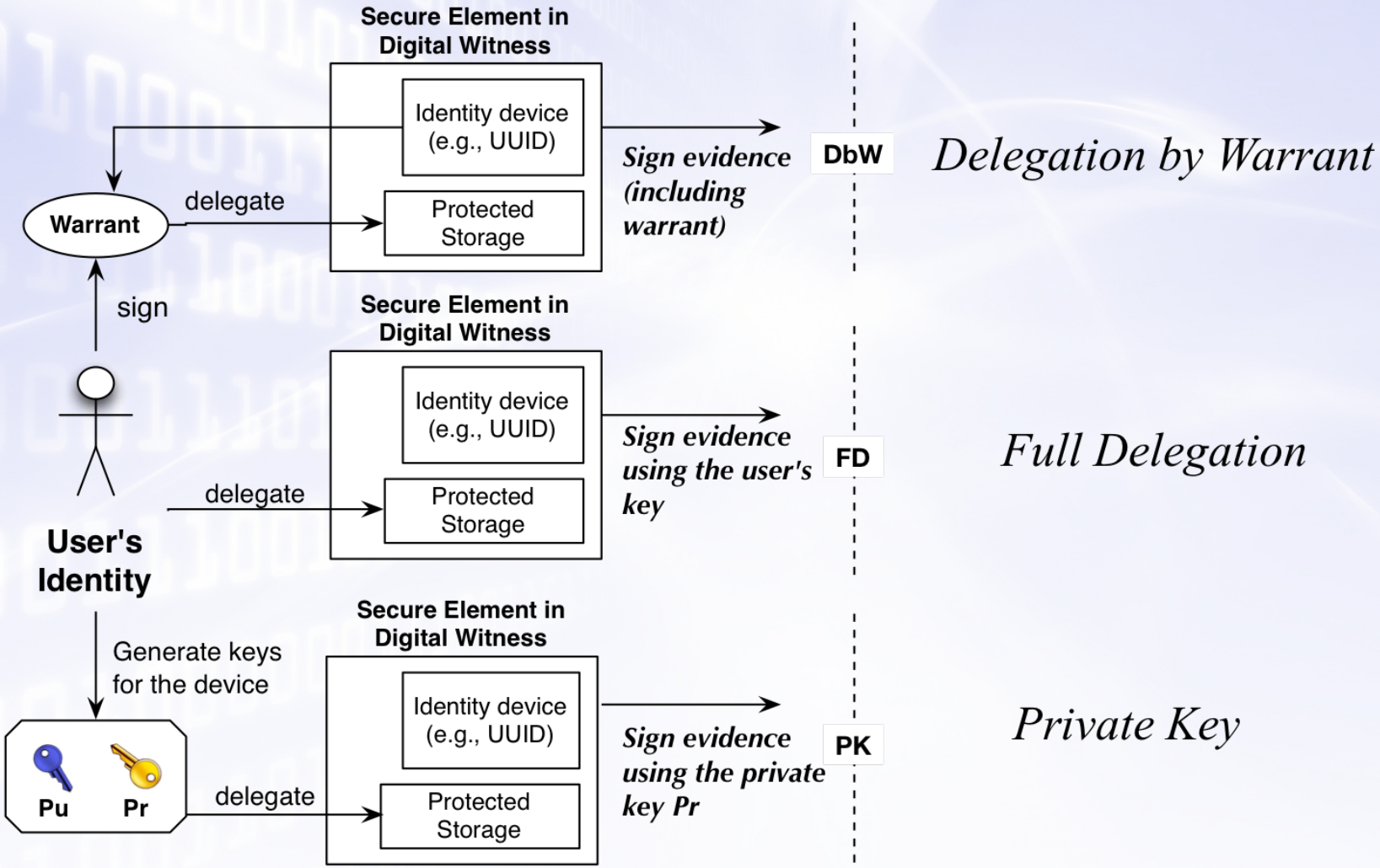
Requirements - Binding Credentials

The basic mode:



1. The user choose a solution implementing binding credentials.
2. The user agrees with the terms of the service and configure the digital witness according to the recommendations.
3. The digital witness stores all relevant information.
4. The evidences are sent automatically in behalf of the user.

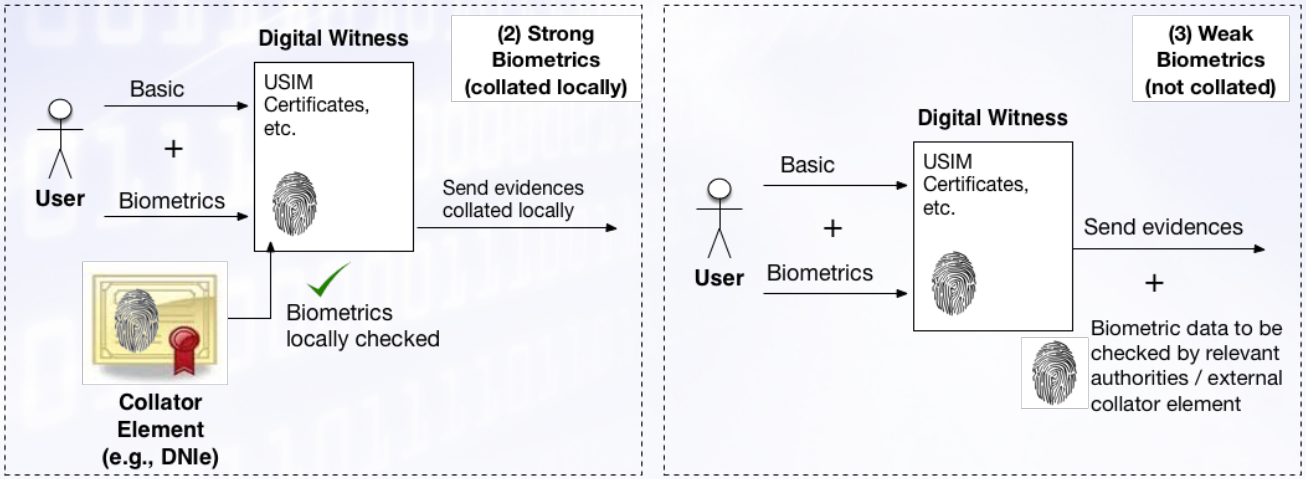
Requirements - BCs - Proxy signatures



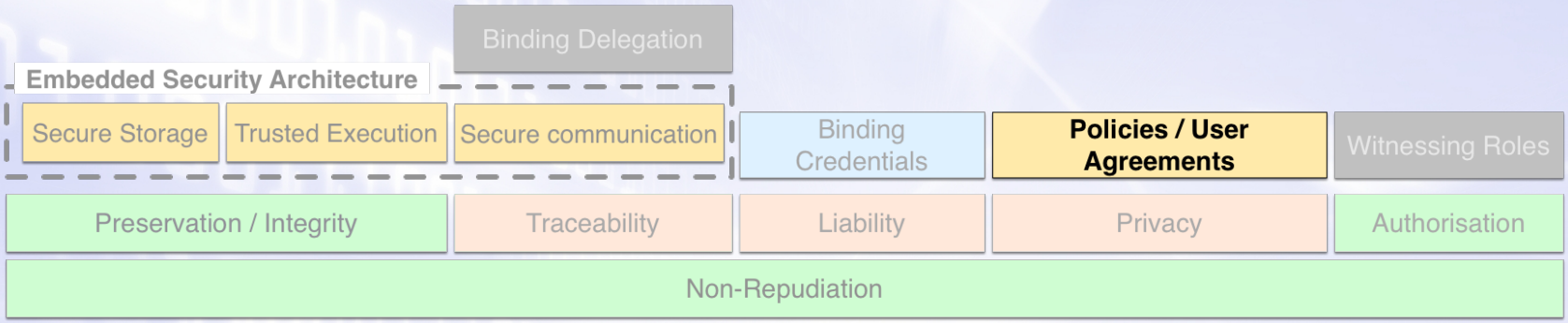
Requirements - BCs - Biometrics

The basic mode can be enhanced using biometrics to ensure the user's presence in some points during the digital evidence management cycle.

- Validation at source (e.g., using powerful identity cards).
- Validation at destination (e.g., contrasted with an official database).



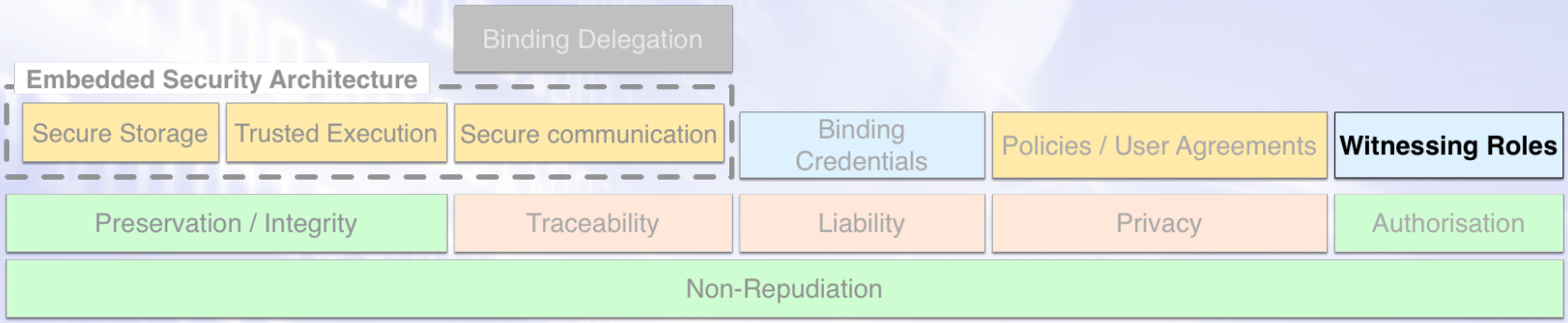
Requirements - Policies / User agreements



A DW cannot operate if the user does not accept the terms and policies of the digital witness. Furthermore, the user can configure its digital witness within a set of acceptable parameters.

- The configuration of the digital witness could affect to the admissibility of the digital evidence in a court of law.
- A *contract manager* can help to the user to understand the policies given a context.

Requirements - Witnessing Roles

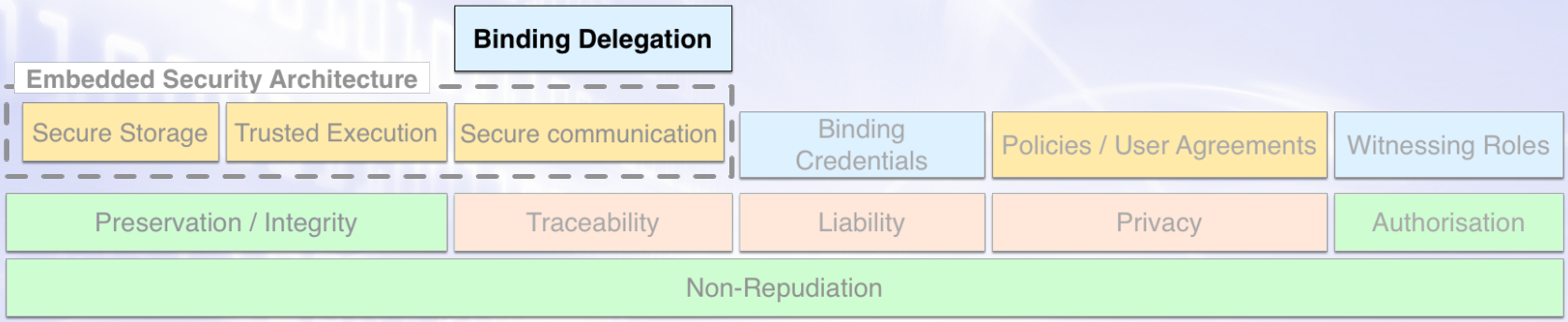


The digital witness approach defines different user and device profiles. The delegation procedure must consider the different users and profile of devices during the DCoC-IoT.

Table: Preliminary roles in a Digital Witness approach

General Rol	Specific Role	Brief Description	Resources	Level
Digital Witness	Citizen	Digital Witness which belongs to a citizen	Low	1
Digital Custodian	Custodian	DW which belongs to a Legal Enforcement Agency (LEA)	Low	2
	Mobile Custodian	Vehicle which belongs to a LEA	Medium	3
	Fixed Custodian	Fixed infrastructure (e.g., Official Collection Point)	Not limited	4

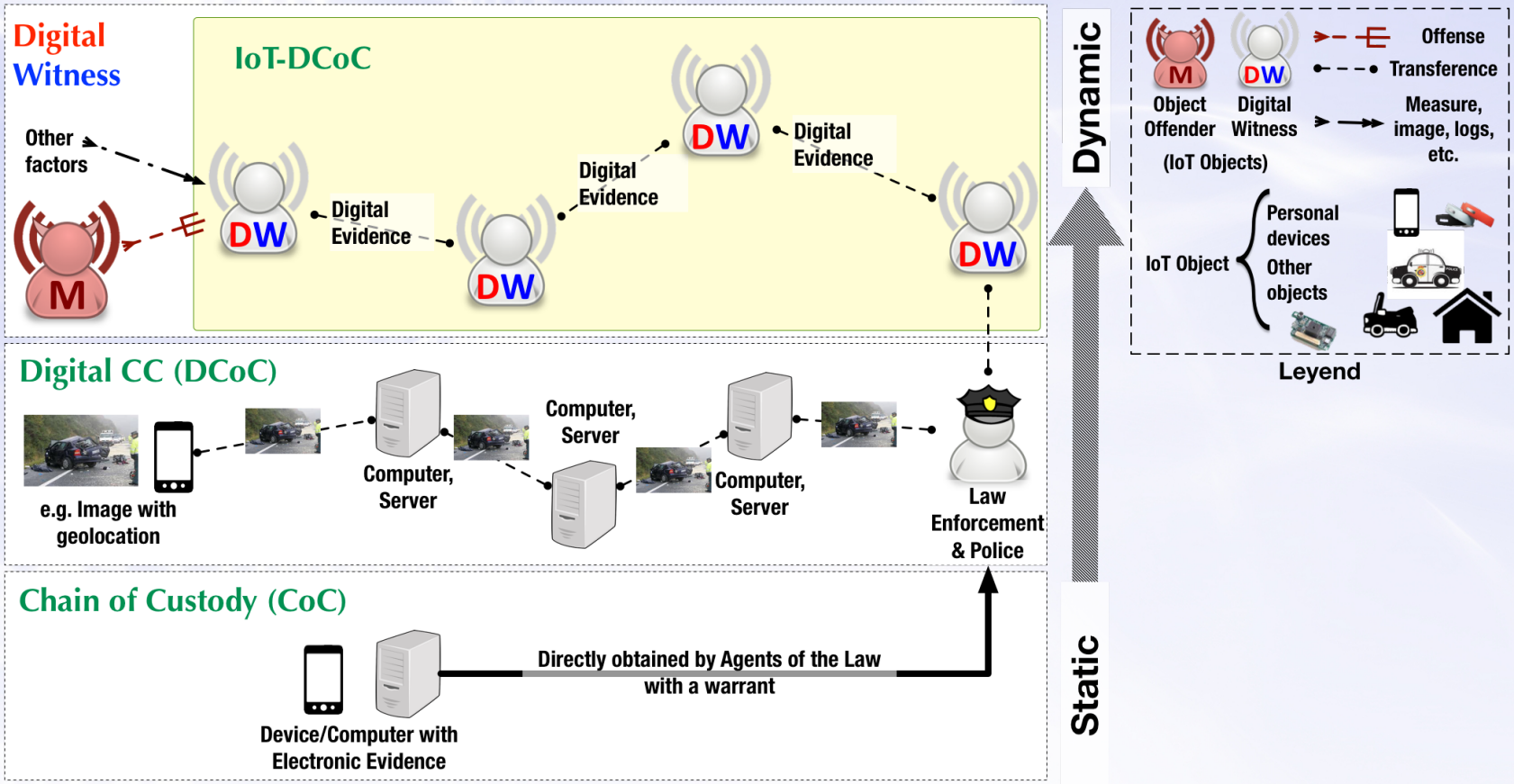
Requirements - Binding Delegation



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.

- Delegate digital evidence between the digital witness in a Digital Chain of Custody (DCoC).
- Uses binding credentials to ensure the traceability of the digital evidence.

Requirements - Binding Delegation



The main purpose of the *binding delegation* is to deploy a Digital Chain of Custody in IoT (DCoC-IoT).

Requirements - Binding Delegation

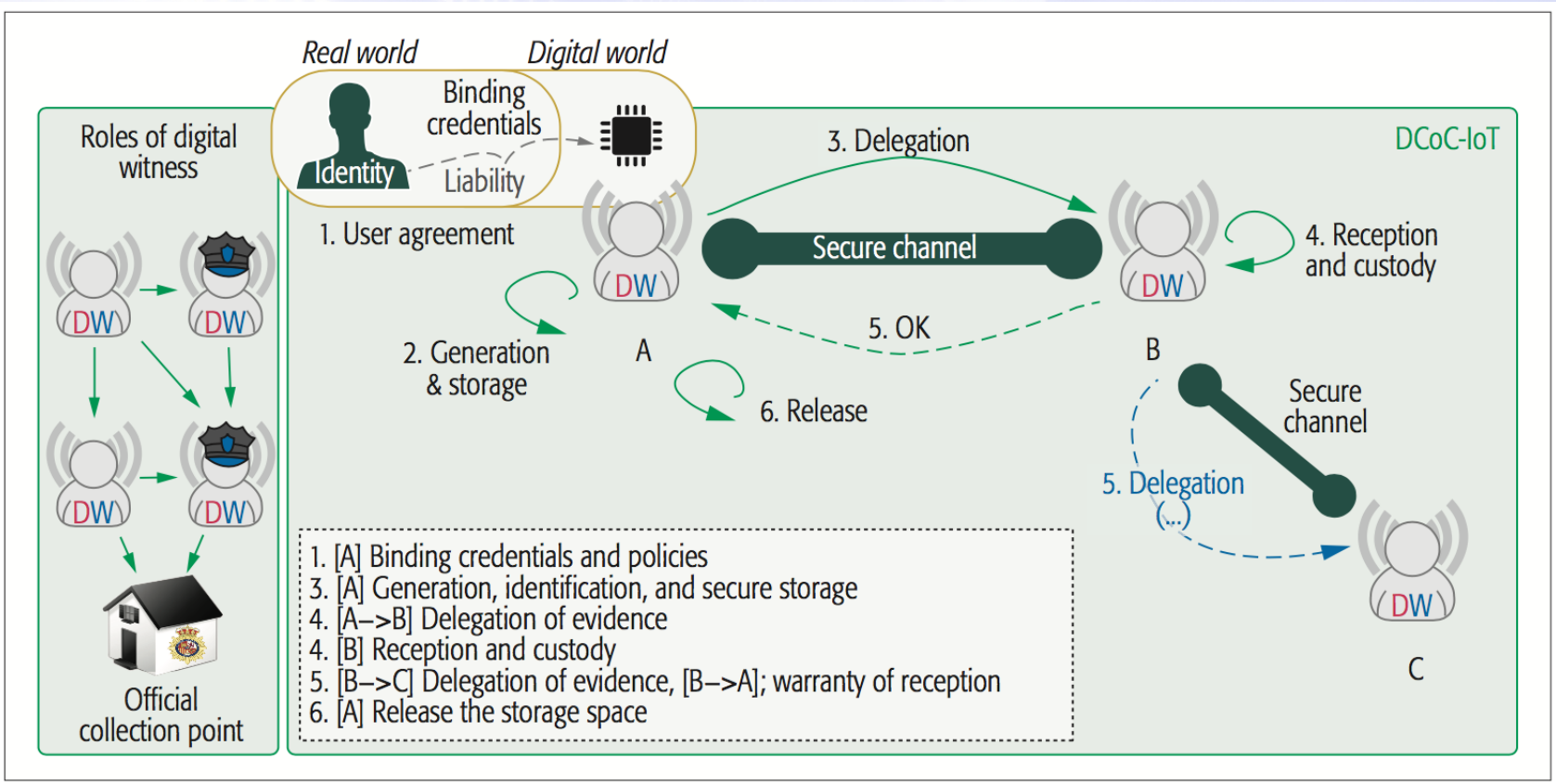
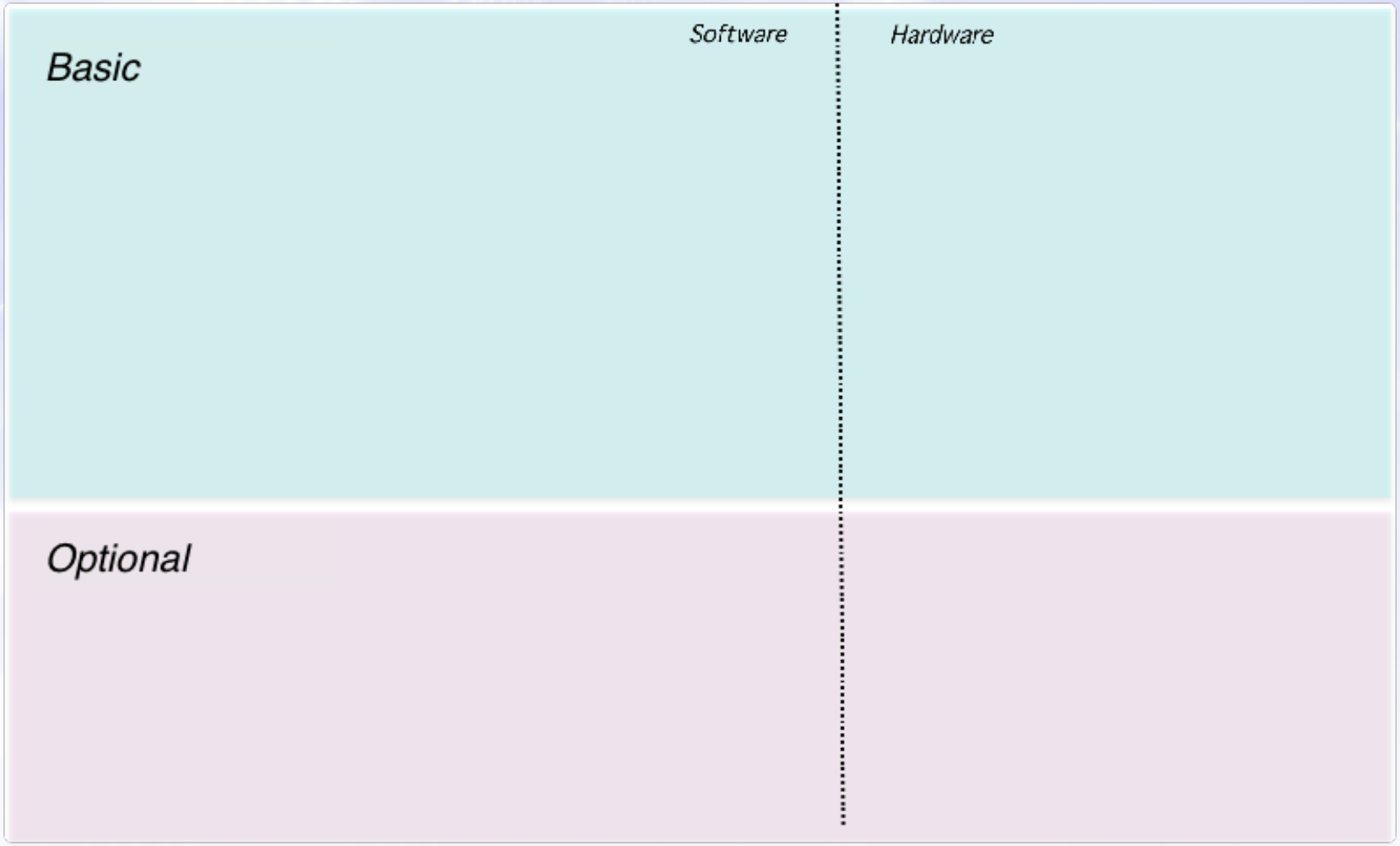


FIGURE 2. Binding delegation.

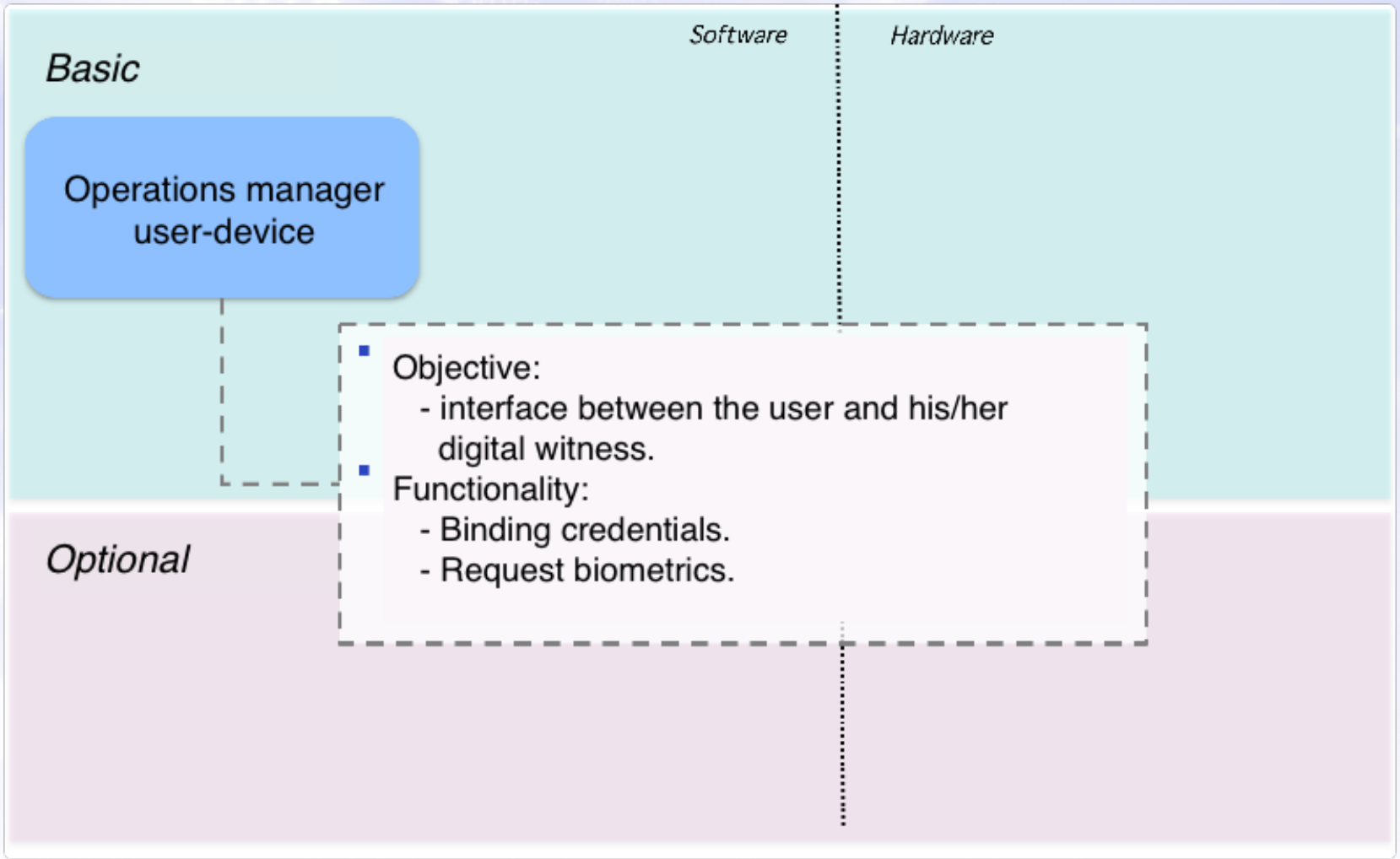
The space to store the digital evidence is released according to the policies defined by the user.

Plan

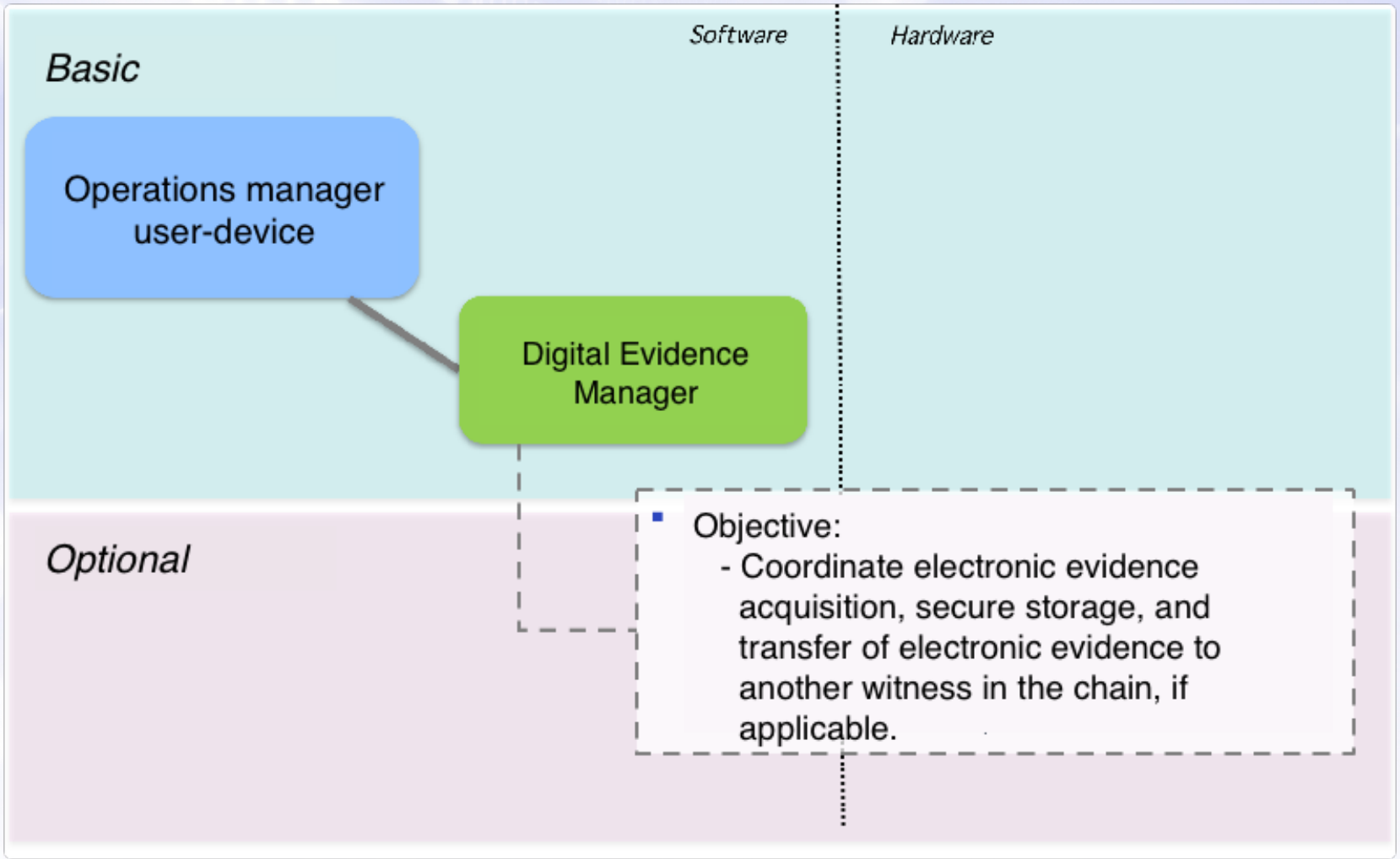
Components



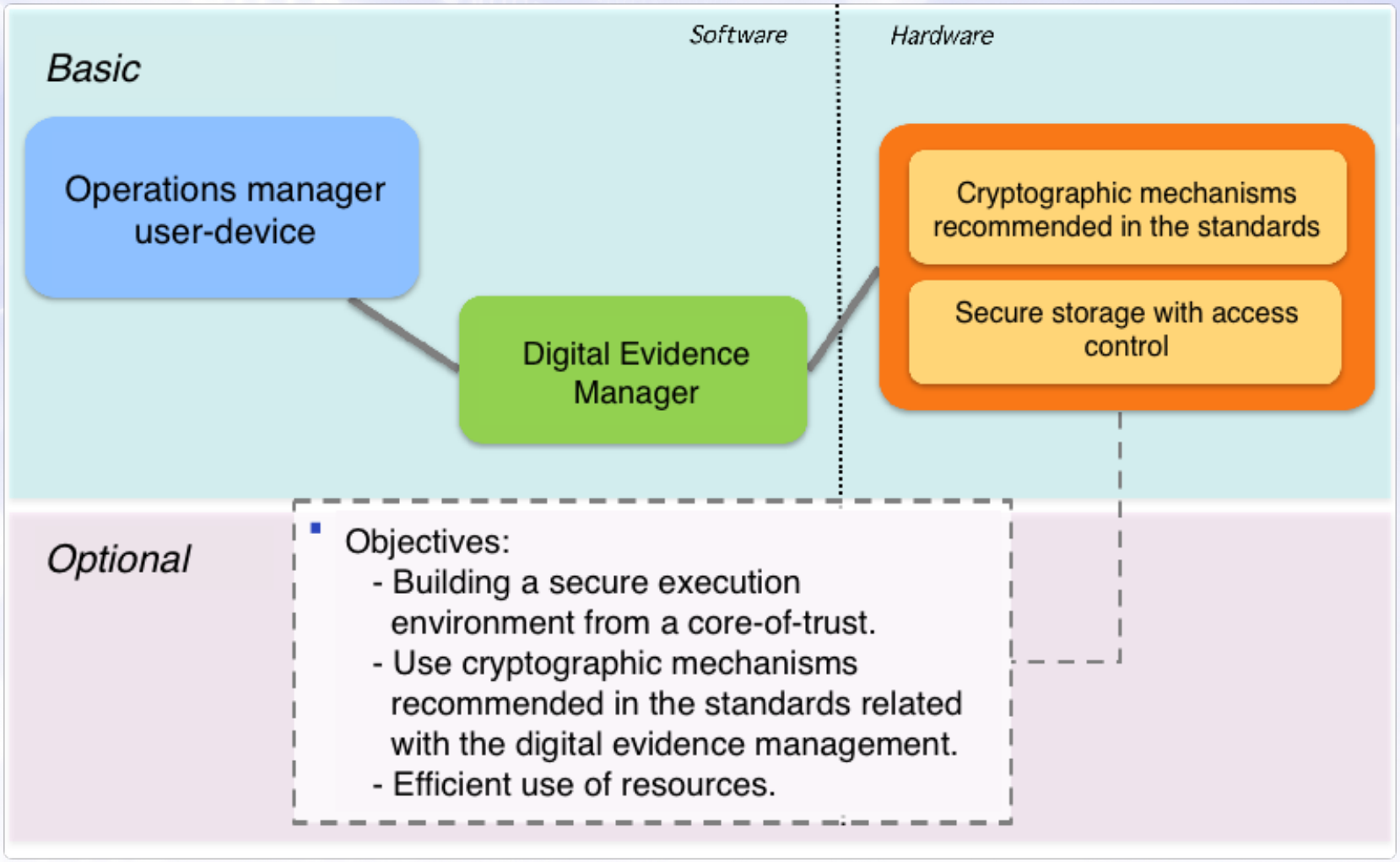
Components


Software
Hardware
Basic
Operations manager user-device
Objective:
- interface between the user and his/her digital witness.
Functionality:
- Binding credentials.
- Request biometrics.
Optional

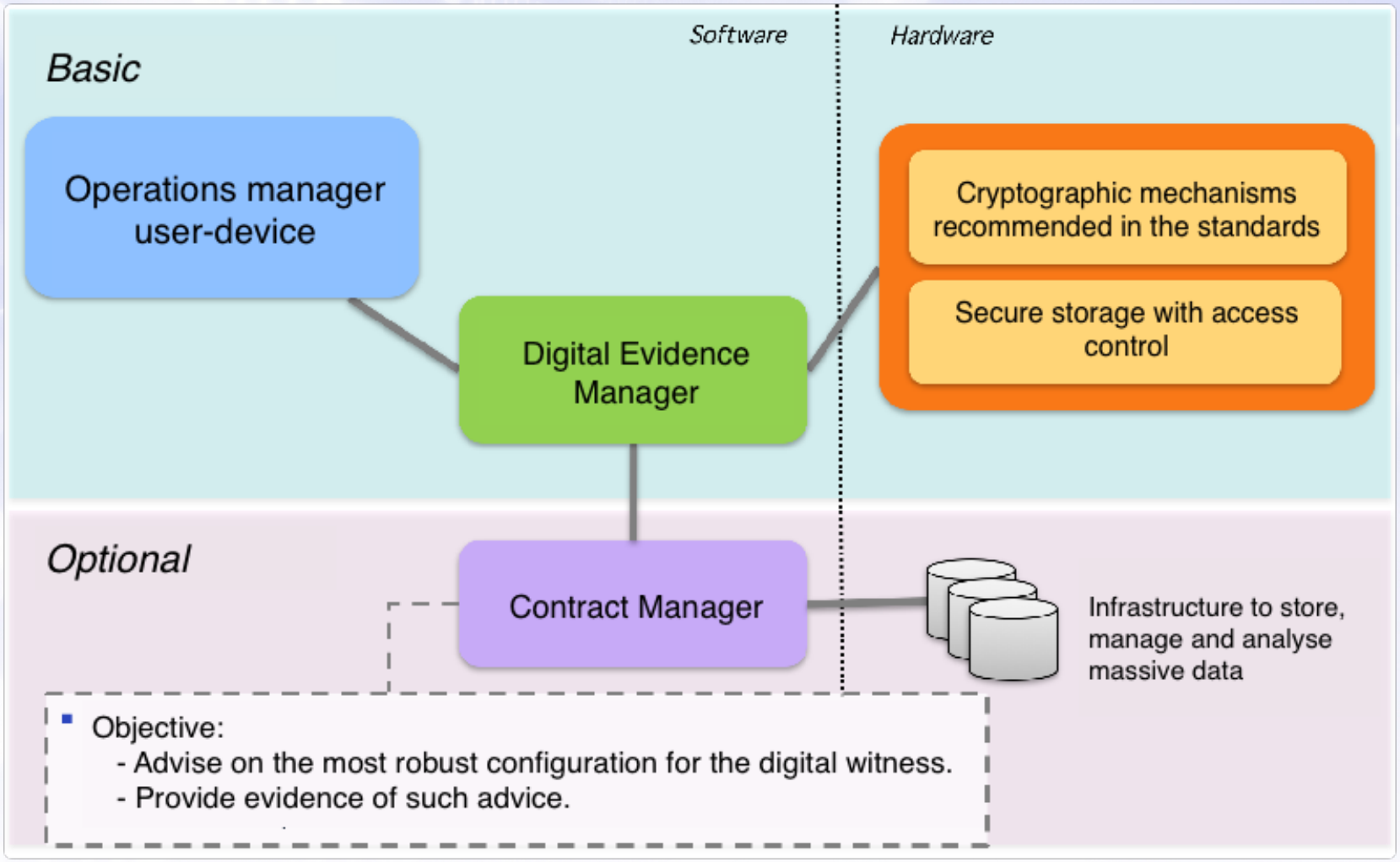
Components


Software
Hardware
Basic
Operations manager user-device
Digital Evidence Manager
Optional
Objective:
- Coordinate electronic evidence acquisition, secure storage, and transfer of electronic evidence to another witness in the chain, if applicable.

Components


Software
Hardware
Basic
Operations manager user-device
Digital Evidence Manager
Cryptographic mechanisms recommended in the standards
Secure storage with access control
Optional
Objectives:
- Building a secure execution environment from a core-of-trust.
- Use cryptographic mechanisms recommended in the standards related with the digital evidence management.
- Efficient use of resources.

Components


Software
Hardware
Basic
Operations manager user-device
Digital Evidence Manager
Cryptographic mechanisms recommended in the standards
Secure storage with access control
Optional
Contract Manager
Infrastructure to store, manage and analyse massive data
Objective:
- Advise on the most robust configuration for the digital witness.
- Provide evidence of such advice.

Components (complete)

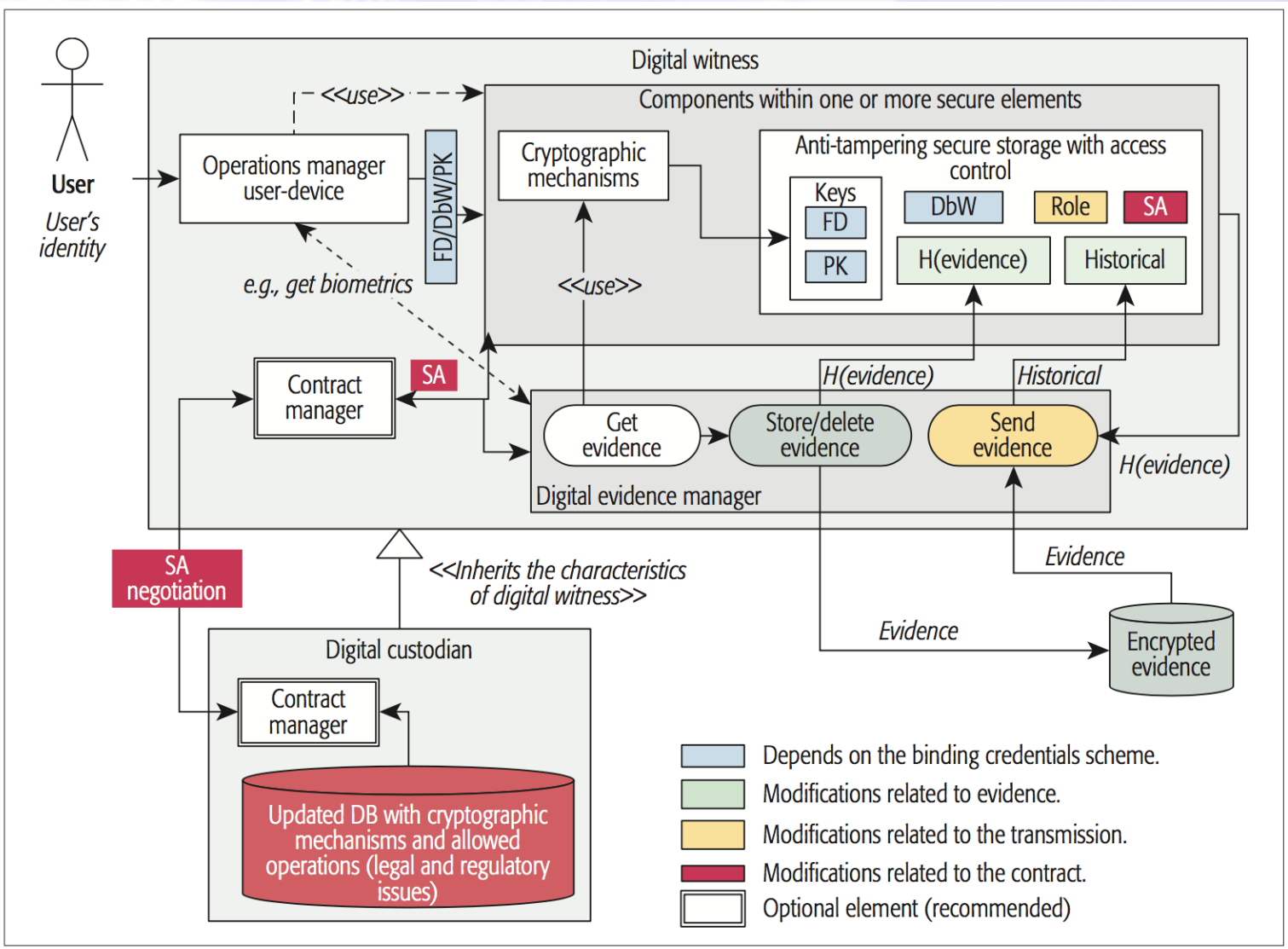


FIGURE 3. Functional requirements for digital witness based on binding credentials).

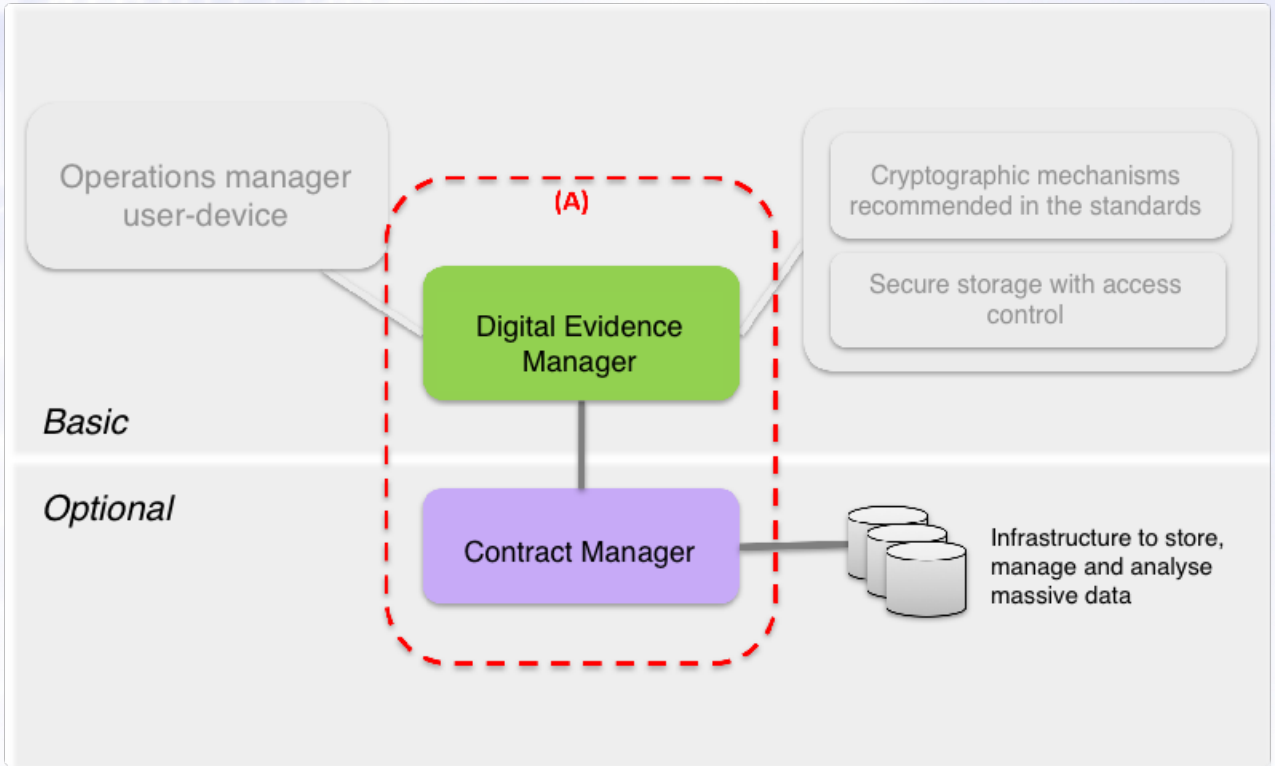
Relationship between the components

Three basic use-cases:

(A) Establishment of **action policies** for the use of digital witnesses.

(B) Creation of **binding credentials (BCs).**

(C) Digital evidence management with BCs.



Relationship between the components

Three basic use-cases:

(A) Establishment of **action policies** for the use of digital witnesses.

(B) Creation of **binding credentials (BCs)**.

(C) Digital evidence management with BCs.

Group policies:

- *Group Policy 1* (GP1)- Defines policies relating the user to the device.
- *Group Policy 2* (GP2)- Contains the policies used by the Digital Evidence Manager.
  - P1 Acquisition of digital evidence.
  - P2 Transmission of evidences.
  - P3 Storage of evidence.
  - P4 Digital evidence Erasure.

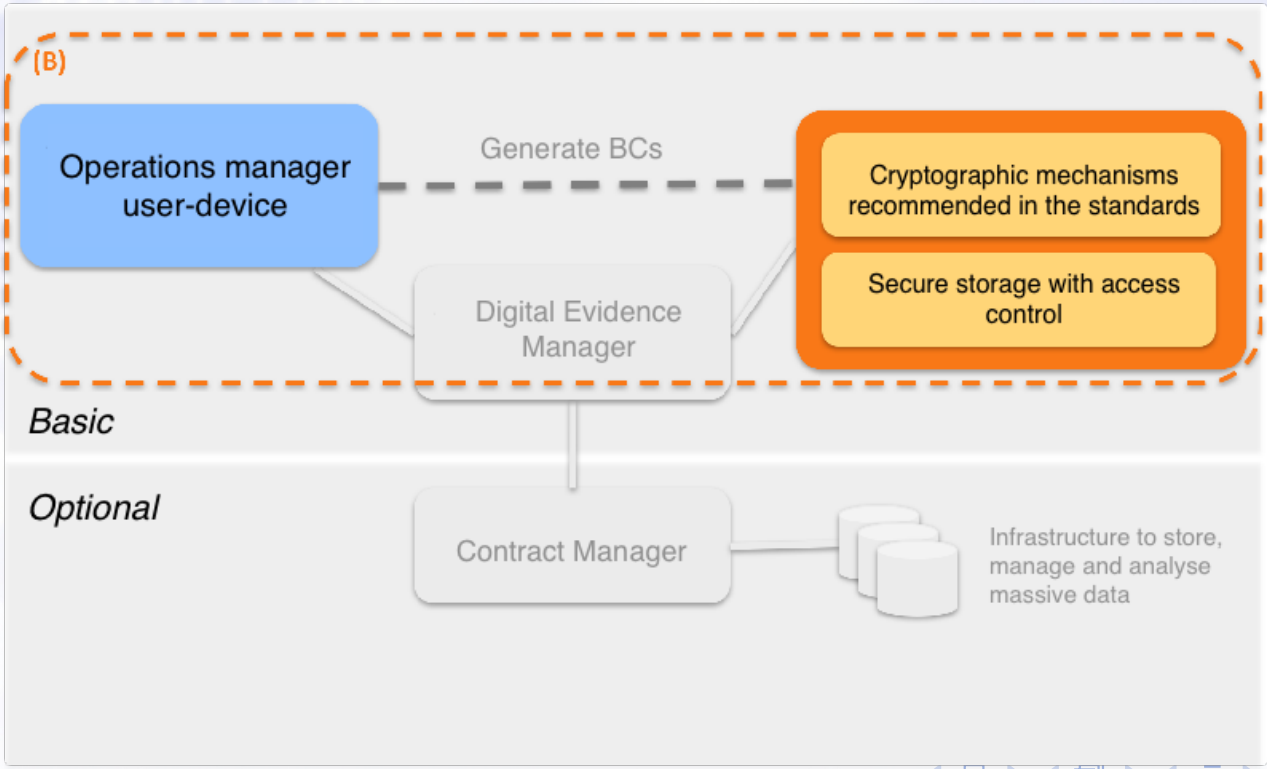
Relationship between the components

Three basic use-cases:

(A) Establishment of **action policies** for the use of digital witnesses.

(B) Creation of **binding credentials (BCs).**

(C) Digital evidence management with BCs.



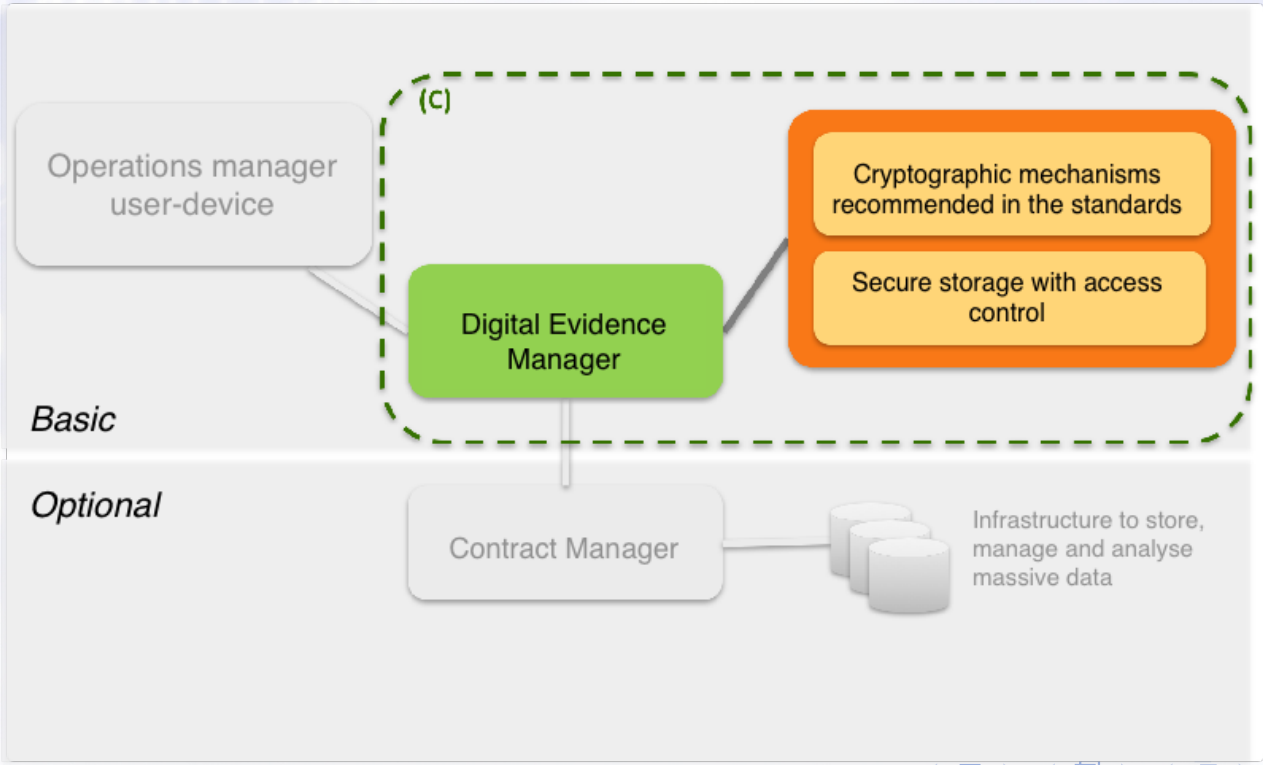
Relationship between the components

Three basic use-cases:

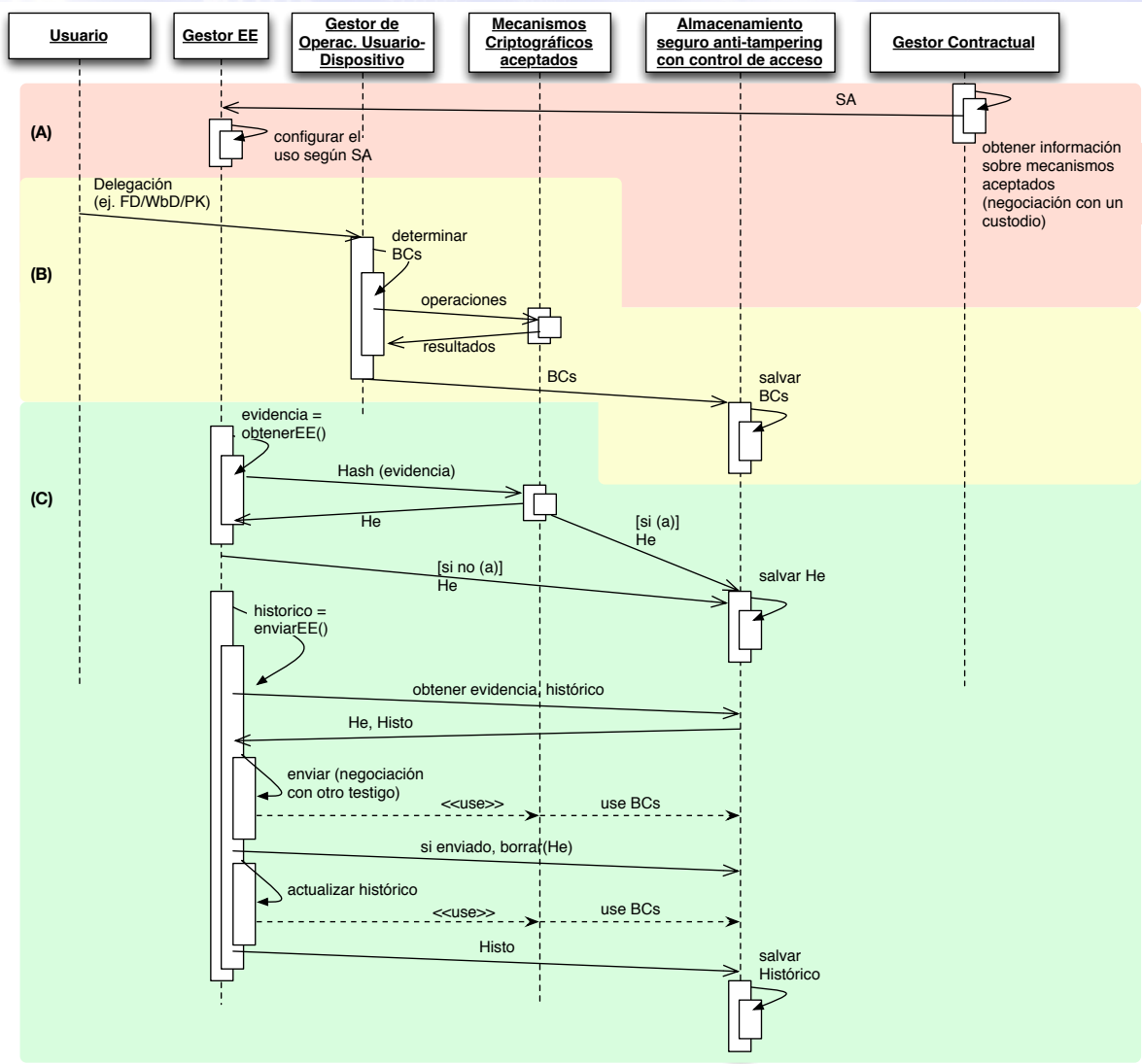
(A) Establishment of **action policies** for the use of digital witnesses.

(B) Creation of **binding credentials (BCs).**

(C) Digital evidence management with BCs.



Sequence diagram



(a): Soporte de escritura directa de resultados de hashes en almacenamiento seguro.

Plan

Digital Witness and Privacy

Why should privacy requirements be considered in digital witnessing?

Digital Witness and Privacy

In general:

- Ensuring fundamental rights.
- Responsibility factor: the user knows and consents to the use of the digital witness and how his data will be handled, given a specific purpose.

Digital Witness and Privacy

In general:

- Ensuring fundamental rights.
- Responsibility factor: the user knows and consents to the use of the digital witness and how his data will be handled, given a specific purpose.

In the case of the digital witness...

- Personal devices - users should give their **explicit consent**, but, also...
- It may be asked **more than ever** how this approach (and other future approaches devised to IoT-forensics) affects the privacy of other users who may be directly or indirectly affected.

A collaborative approach as the digital witness depends greatly on the willingness of the user **to be accepted**.

Questions to analyse Privacy in DW

Questions for the Investigative Process:

- Who is the victim/offended party?
- Who was present?
- Where did the event occur? When? For how long?
- Where others affected?

Questions for the Admissibility of the digital evidence:

- Where is the data from?
- Who has had access to the data during the DCoC-IoT? Which participant and what type of access?
- Did the digital witness act in accordance with the legal framework and respecting ethical principles?

Questions to analyse Privacy in DW

Questions for the Investigative Process:

- Who is the victim/offended party?
- Who was present?
- Where did the event occur? When? For how long?
- Where others affected?

Questions for the Admissibility of the digital evidence:

- Where is the data from?
- Who has had access to the data during the DCoC-IoT? Which participant and what type of access?
- Did the digital witness act in accordance with the legal framework and respecting ethical principles?

Synthesis: approachable privacy requirements

TABLE I: Relationship between DW Properties, Privacy Requirements and Mitigation Methods proposed

Property DW	Capillary Network			Official Collection Points		
	Purpose	Privacy Required	Mitigation Method	Purpose	Privacy Required	Mitigation Method
Anti-tampering Behaviour	Trustworthy links in the DCoC-IoT Preservation	Status Confidentiality Privacy Attestation	Direct anonymous attestation Opt-out / Silent	Trustworthy device	Users data in OCP	Users registered in one OCP - users consent
Binding Credentials	Responsability Access Control	Anonymity	Anonymous DW: Crowd-like Group signature	Responsability	Anonymity	Multi-Party Declaration
Binding Delegation (DCoC-IoT)	Traceability Preservation Provenance	Anonymity, Unlinkability, Unobservability, Undetectability, Location Privacy, Tansactional Privacy	Privacy-based route discovery Blockchain Smart Contracts	Traceability Correlation (different sources) Provenance	Data collection (multiple sources) Location privacy re-identification	Key group shared with OCP
ISO/IEC 27050:2016	Final acceptance (well known and accepted procedures)	Disposal (link data)	Consents (others) Proof of secure erasure	Final acceptance (well known and accepted procedures)	Disposal (stored data)	Proof of secure erasure

Summary

The DW approach allows *other devices* in the environment - and not only the OCP and authorised digital witnesses - to obtain information about users who were not even directly related to the offence, or deduce information which is not relevant to the investigation.

Mitigation Methods

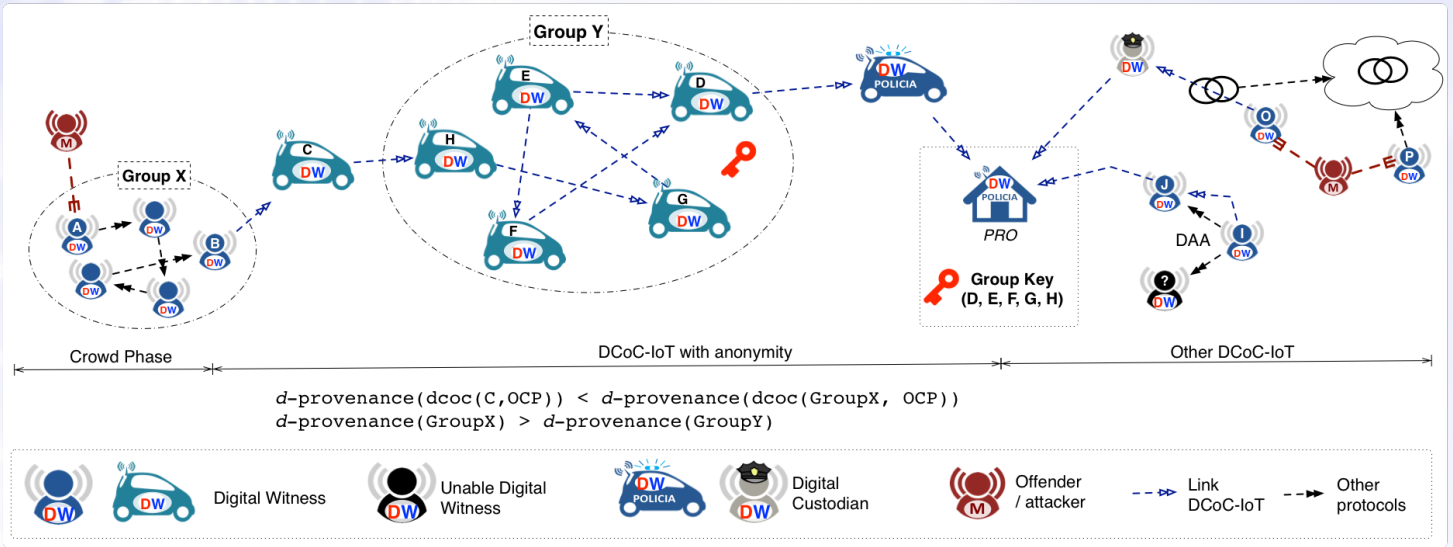
- While the link between the user's identity and his/her device is a key piece in the definition of the digital witness approach, mitigation mechanisms should be proposed that allow balancing this solution to protect personal data that...
  - Are not relevant to an investigation or
  - Are not necessary for the primary purpose of the digital witness - that is, to delegate the digital evidence to the OCP without risking its admissibility.

Mitigation Methods

- While the link between the user's identity and his/her device is a key piece in the definition of the digital witness approach, mitigation mechanisms should be proposed that allow balancing this solution to protect personal data that...
  - Are not relevant to an investigation or
  - Are not necessary for the primary purpose of the digital witness - that is, to delegate the digital evidence to the OCP without risking its admissibility.
- Mitigation methods are conditioned by:
  - Limitations / restrictions of the digital witness - the scheme does not allow anonymous witnessing to maintain the *traceability*.
  - Implementations of the concept - to be considered during the implementation of the digital witness but do not affect to the definition of digital witness.

Mitigation - Anonymity in DCoC-IoT

- Affects to the definition of digital witness.
- We *relax* the definition of DW to allow the anonymous digital witnessing.
- An example of implementation: *Crowd* in the origin of the digital evidence, and a *group key* that can be shared with the *OCP* to the intermediary links once the DCoC-IoT has been deployed.



d-provenance: distortion in the digital evidence provenance due to the inclusion of privacy mechanisms.

Mitigation - Digital Witness Implementation

To be considered during the implementation of a digital witness, but do not affect to the definition.

- Attestation.
  - Risk. Devices nearby may know when a digital witness has been disabled from its duties.
  - Solution. Direct Anonymous Attestation (DAA) allows a verifier to check whether a user is using a platform with a certified hardware security module.

Mitigation - Digital Witness Implementation

To be considered during the implementation of a digital witness, but do not affect to the definition.

- Links discovery.
  - Risk. The identity of those involved in the discovery process is exposed.
  - Solution. Adapting anonymous routing protocols, such as AASR, to digital witness.

Mitigation - Digital Witness Implementation

To be considered during the implementation of a digital witness, but do not affect to the definition.

- Time-stamping.
  - Need. Corroborate the acquisition of electronic evidence of the environment, without the signer (e.g., a more powerful digital witness) knowing the contents of the evidence (e.g., multi-party declaration).
  - Solution. Blind signature mechanisms + signature chaining.

Mitigation - Digital Witness Implementation

To be considered during the implementation of a digital witness, but do not affect to the definition.

- Blockchain Smart Contracts.
  - Risk. Secure and decentralised transactions preserving privacy.
  - Solution. Hawk - a solution for transactional privacy using block chain and a TTP that can be instantiated to a *trusted computing hardware*.
  - Additional. Check whether an incident has already been reported.

Mitigation - Digital Witness Implementation

To be considered during the implementation of a digital witness, but do not affect to the definition.

- Multi-party Declaration.
  - Need. Some of the witnesses may be reluctant to share their own version of the incident with other participants.
  - Solution. Homomorphic encryption or secure computation - The witnesses can collaboratively share and operate the statements of each of the participants without learning the content of the declarations.

Mitigation - Digital Witness Implementation

To be considered during the implementation of a digital witness, but do not affect to the definition.

- Disposal Guarantees.
  - Risk. The information provided by a collaborator (digital witness) should be used only to resolve the case in question and will not be used for other purposes.
  - Solution. Proof of secure erasure, by which means a verifier can check whether or not a prover has erased its memory.
  - Who? This verification would only involve the OCP and digital witnesses who store information about other digital witnesses not considered in the DCoC-IoT.
  - A digital witness in a DCoC-IoT already define mechanisms to eliminate the data transmitted in teh deployment of the DCoC.

Expanding the problem to IoT-Forensics

Why should privacy requirements be considered in IoT-forensics?

Privacy in IoT-Forensics

- The IoT is not *only* about billions of heterogenous devices connected to the Internet.
- The user also plays a fundamental role in this paradigm and obviating it is a terrible mistake.
- Collecting evidence from IoT devices may have implications for individual privacy and thus tackling this problem is critical in IoT-forensics.

Privacy in IoT-Forensics

- The IoT is not *only* about billions of heterogenous devices connected to the Internet.
- The user also plays a fundamental role in this paradigm and obviating it is a terrible mistake.
- Collecting evidence from IoT devices may have implications for individual privacy and thus tackling this problem is critical in IoT-forensics.

Related works in this field:

- Privacy for honest users. Diferenciar usuarios honestos de deshonestos antes de aplicar mecanismos forenses que puedan vulnerar su privacidad dentro de una red corporativa.
- Use of forensic mechanisms to evaluate privacy in mobile platforms.
- Papers related to IoT-Forensics highlight the relevance of privacy, but without considering cooperative scenarios or the role of the witness. Traditional computer forensics but the evidences are collected from new IoT devices.

PRoFIT: a tentative solution

The *Privacy-aware Forensic model for the IoT* (PRoFIT) defines six phases through the combination of a traditional forensic model and ISO/IEC 29100:2011 (Privacy principles).

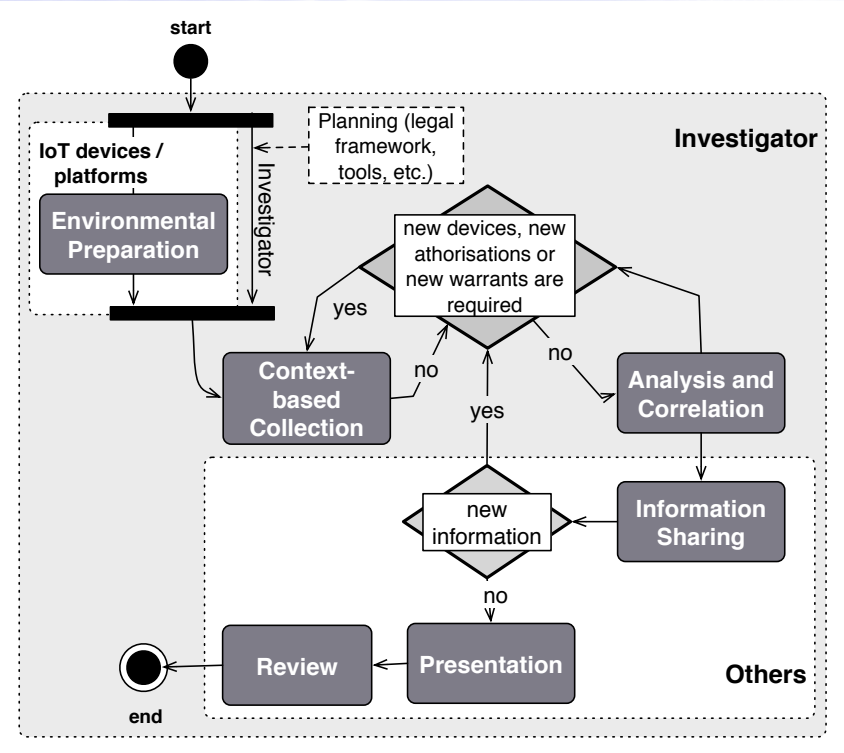
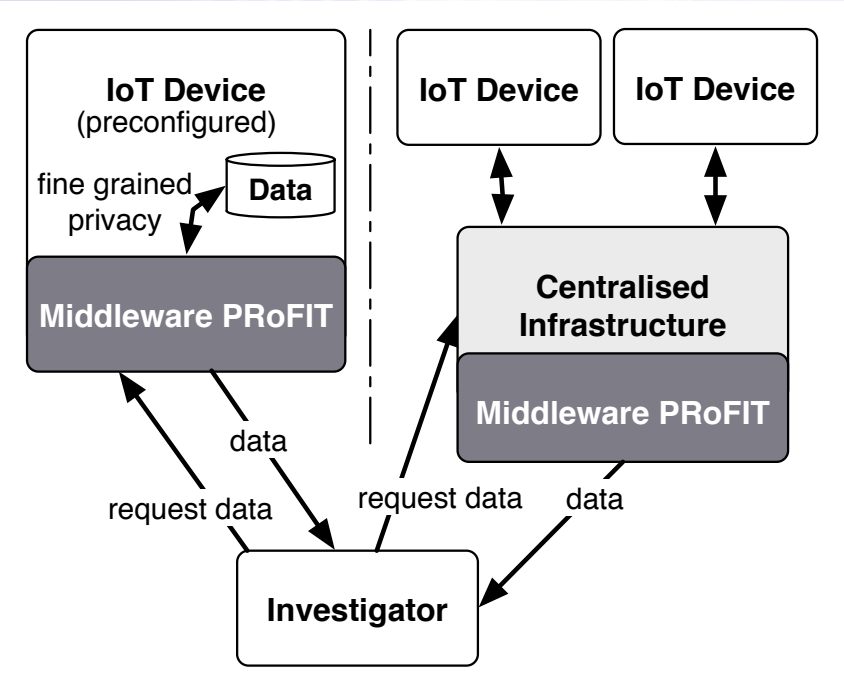


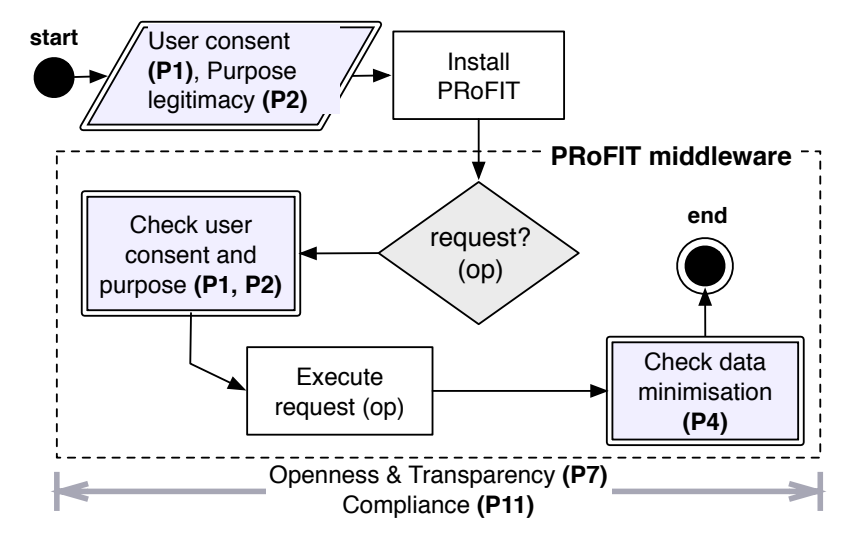
TABLE II: Privacy Requirements in PRoFIT phases

PRoFIT phase	ISO/IEC 29100					
Preparation	P1	P2	P4	P7		P11
Context-based collection	P1	P2	P3	P6	P8	
Data analysis and correlation	P9	P10				
Information sharing	P1	P2	P10			
Presentation	P4	P6				
Review	P5	P7				

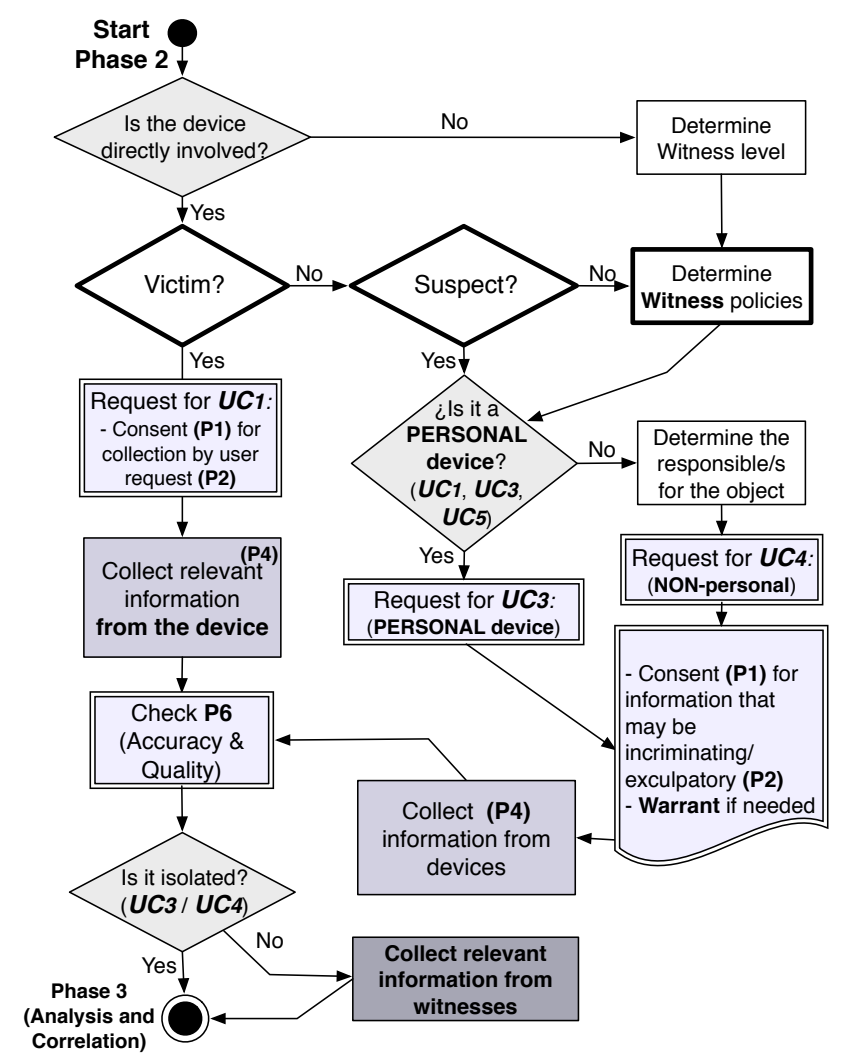
P1. Consent and choice, P2. Purpose legitimacy and specification, P3. Collection limitation, P4. Data minimization, P5. Use, retention and disclosure limitation, P6. Accuracy and quality, P7. Openness, transparency and notice, P8. Individual participation and access, P9. Accountability, P10. Information security controls, P11. Compliance

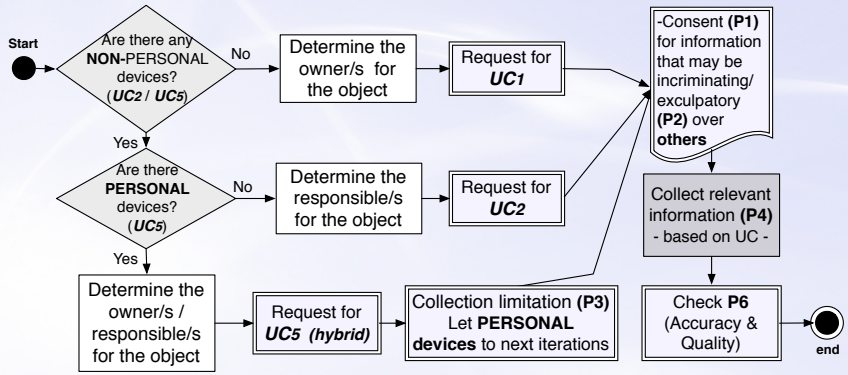
Phase 1 - Environmental Preparation

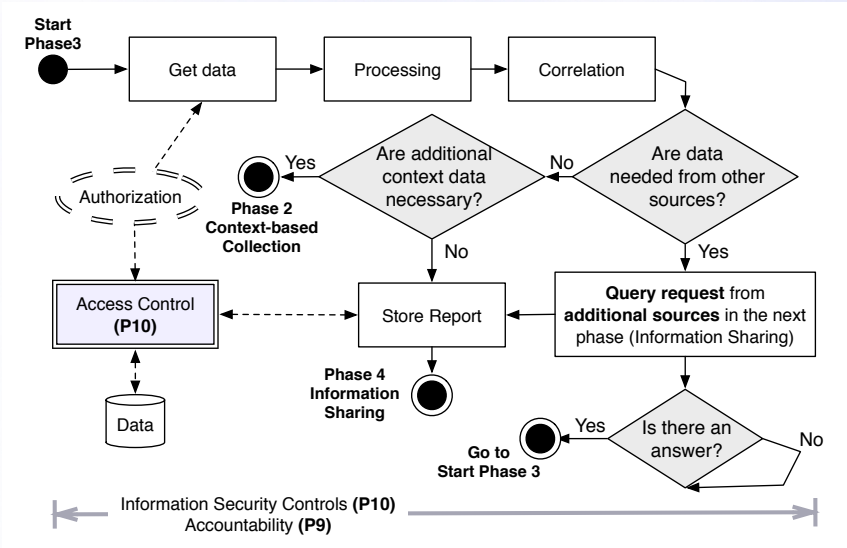




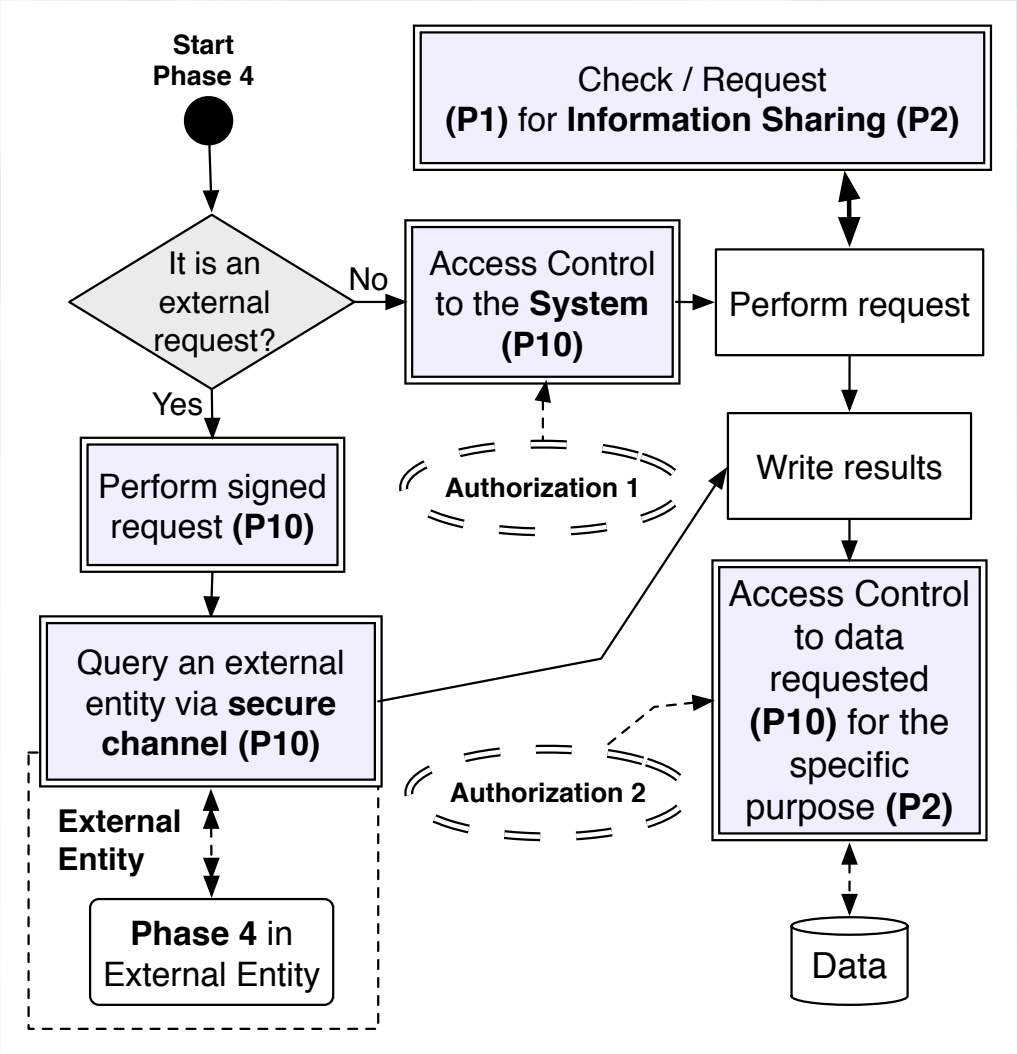
Phases 2-3: Forensic Investigation



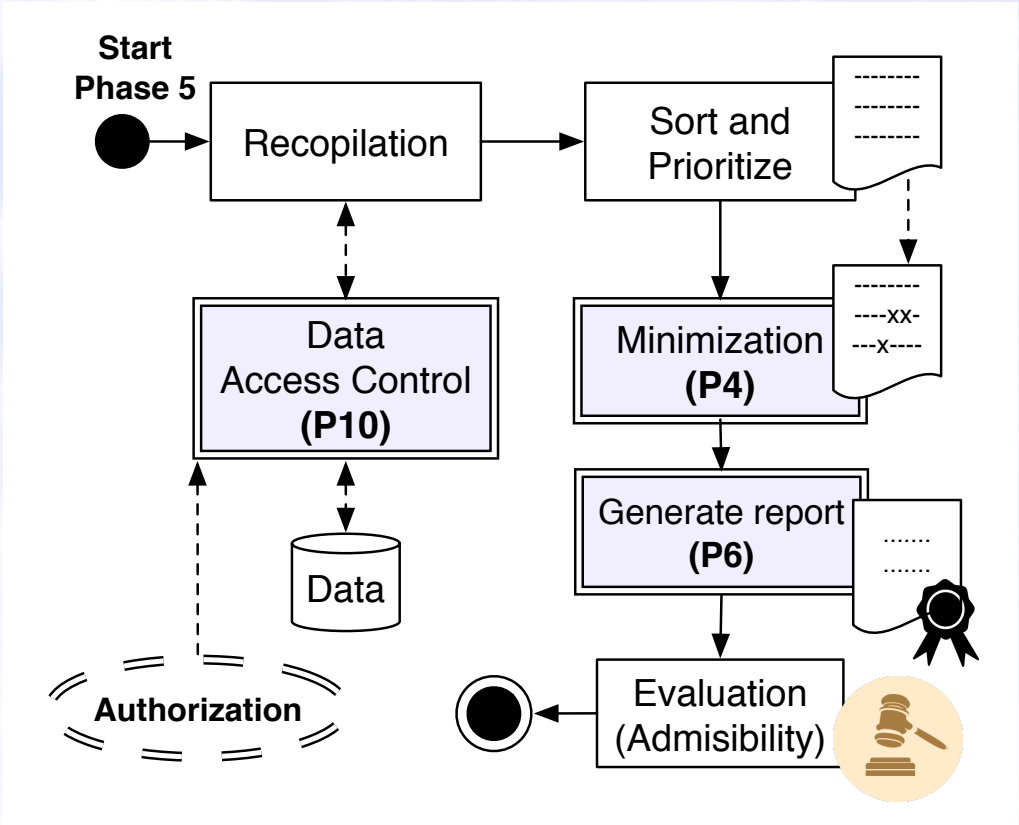




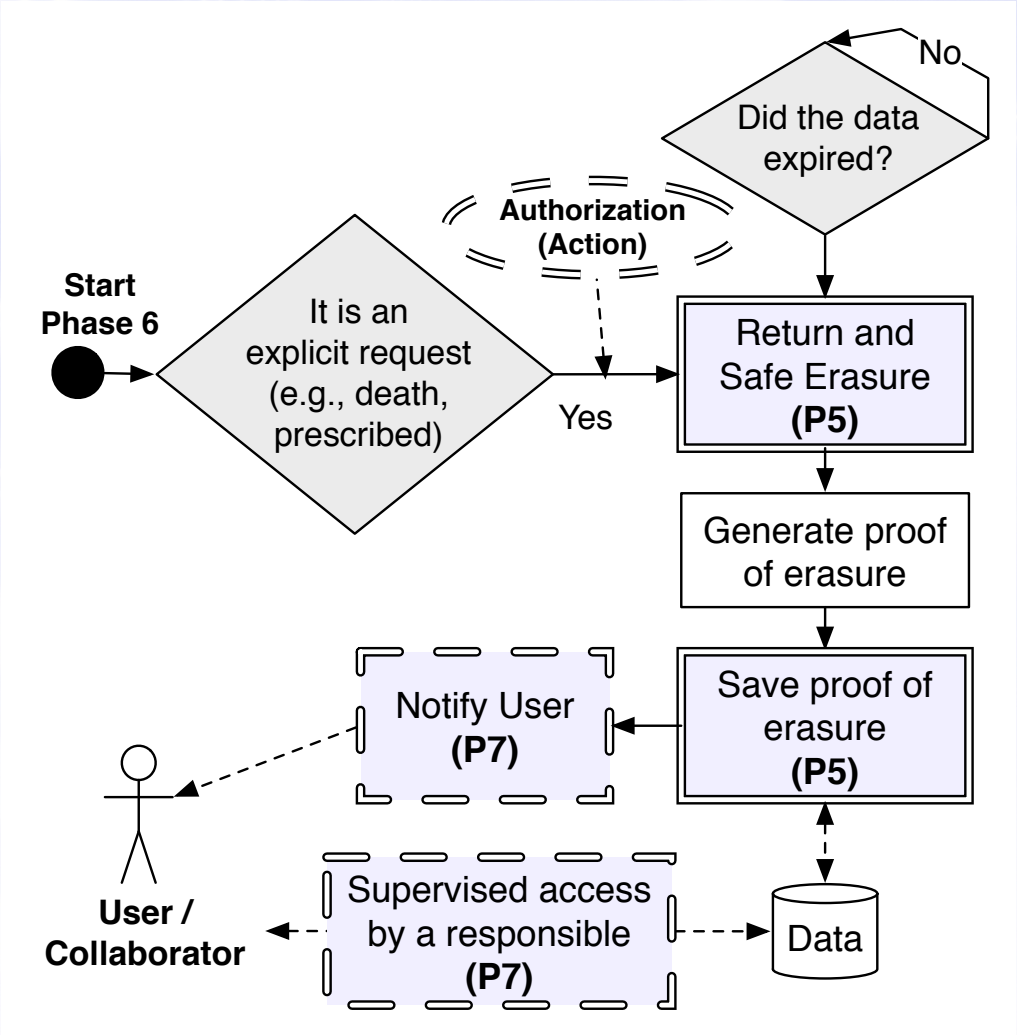
Phase 4 - Information Sharing



Phase 5 - Presentation



Phase 6 - Review



Use cases: applying PRoFIT to Digital Witness

Social Malware - *The Coffee Shop*

Bob has a smartphone with a PRoFIT-compliant software installed (phase 1). He walks into a coffee shop, where there are several IoT devices, both personal and non-personal.

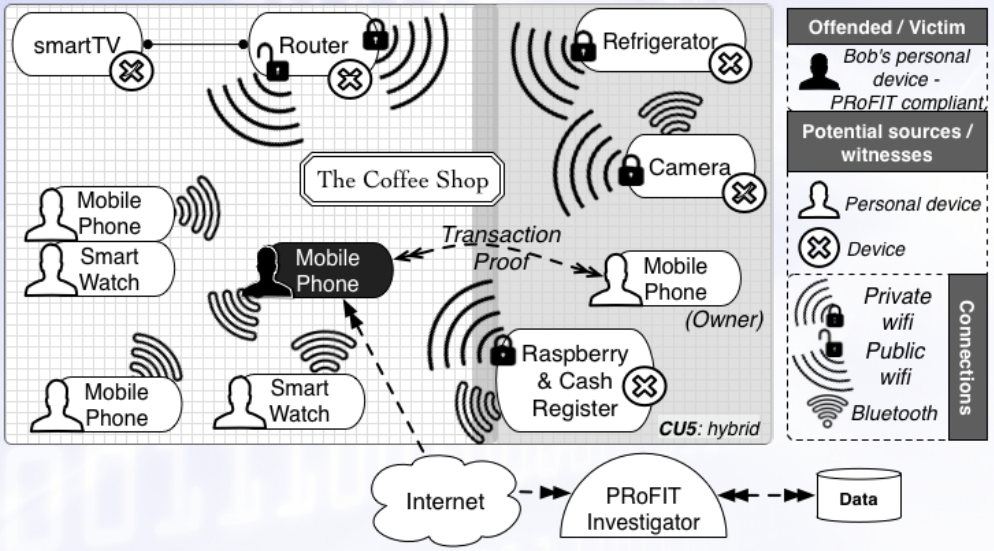
Warehouse Registration

Max is a police officer. He has to register in a warehouse where there are several IoT devices (e.g. cameras, sensors and actuators, etc.). It is suspected that some of the devices store digital evidence that may be key to resolving an investigation.

- Both use cases are fictitious.
- The steps of PRoFIT are different considering that in the second scenario (context) the main actor is a police officer performing a register with a search warrant digitalized and stored in his digital witness - that is a digital custodian.

The Coffee Shop I

While Bob is in the coffee shop, PRoFIT detects an attempted attack from some of the devices in its vicinity.



A device nearby is trying to propagate a worm, exploiting a vulnerability in the *meetMe* application which works using Bluetooth.

Phase 2 Bob decides to request the start of an investigation by sending the evidence stored in his device to the PRoFIT system (phase 2).

- The remote system request the PRoFIT agent installed in Bob's device to collect new evidence from any devices nearby willing to collaborate (back to phase 2).

The Coffee Shop II

- First, non-personal devices are asked for any information they can offer. The owner of the coffee shop agrees to collaborate and allows the devices (e.g., the cash register) to send information to the investigator using the PRoFIT agent installed in Bob's device as the gateway.
- This information is encrypted and signed. After reception by the investigator, the device receives a proof of correct reception that can be checked by its owner.
- This proof can be used by the owner of the coffee shop to ask the investigator to (i) check the correctness of the data provided, and (ii) to recant and request the erasure of the statement.

Phase 3 Based on the new information, the results of the investigation indicate that the malware is latent in a non-personal device, the Raspberry Pi, and the infection was received from outside the network, as indicated by the logs of the router.

The Coffee Shop III

Phase 4 Since it has not been possible to identify the source of the problem with the information collected, Bob gives his consent to the investigator to **share his information** with other agencies but only for the purpose of the investigation (phase 4).

- After some time has passed, an improved version of the same malware affects new IoT devices. Since the PRoFIT system keep information regarding the initial attack, it is possible to correlate these data with new evidence taken from various sources and discover the source of the attack and a potential suspect.

Phase 5 The data provided by Bob and other devices are finally used to elaborate a final report (phase 5), which is admitted in the trial.

Phase 6 Some time after the court ruling, the owner of the coffee shop is notified that the **data he provided has been removed** from the system. A proof of deletion is provided to him (phase 6).

Warehouse Registration I

Phase 1 Max uses a digital custodian that stores a signed search warrant, and that is pre-configured to gather evidence relevant to the case.

Phase 2 During registration, Max is the specialist in charge of storing volatile digital evidence using his digital custodian. To do this, his device scans the network of the store and saves the state of the connections.

- It also receives memory dumps and other data that Max decides to store on the device. All these steps are made obviating the requests and consents of users because they have a court order to carry out the procedures that Max's device is carrying out.

Warehouse Registration II

Phase 3 Once in the laboratory, during the analysis (phase 3) the data collected are processed and extracted the relevant electronic evidence for the investigation.

Phase 4 In this particular case, no external database queries are required (phase 4).

Phase 5 The final reports are written (phase 5).

Phase 6 The evidence is accepted for its view and, after a time, the objects collected during the registration, from which the evidence was extracted, are returned to the owner (phase 6).

Plan

Closing remarks

- Computer Forensics has changed a lot in just twenty years, and it has yet to change much more.
- IoT-Forensics is much more than only new devices to be analysed. Is a new paradigm where to understand the context of the devices will be fundamental for the prosecution of the cybercriminals.
- The digital witness can contribute to capture digital evidence of attacks that have so far gone unnoticed by us.
- It is necessary to find a balance between IoT-Forensics and Privacy, since the relevance in IoT scenarios will depend greatly on the context.
- Both use cases are fictitious. However, it is reasonable to think that this type of attack is occurring (or will occur) without the user even noticing it.

Bibliography

R1 B.Nelson, A. Phillips and C. Steuart."A Brief History of Computer Forensics", Guide to Computer Forensics and Investigations, 4th edition.

R2 E.Casey (2011). "Digital evidence and computer crime: Forensic science, computers, and the internet". Academic press.

R3 "Information technology - Security techniques - Electronic discovery - Part 1: Overview and concepts". ISO/IEC JTC 1/SC 27.

R4 A. Nieto, R. Roman, and J. Lopez. "Digital Witness: Safeguarding Digital Evidence by using Secure Architectures in Personal Devices", In IEEE Network, IEEE ComSoc. ISSN: 0890-8044.

R5 A. Nieto, R. Rios and J. Lopez, "Digital Witness and Privacy in IoT: Anonymous Witnessing Approach", In the 16th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom 2017), IEEE, 08/2017 (In Press).

R6 A. Nieto, R. Rios and J. Lopez, "A Methodology for Privacy-Aware IoT-Forensics", In the 16th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom 2017), IEEE, 08/2017 (In Press).

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

Thank you very much for your attention

Ana Nieto

nieto@lcc.uma.es

Network, Information and Computer Security Lab

NICS
Network, Information and Computer Security Lab

22 May 2017