LOCARD

DELIVERABLE

D2.2 SELP Compliance Report

Project Acronym:	LOCARD	
Project title:	Lawful evidence collecting and continuity platform development	
Grant Agreement No.	832735	
Website:	http://locard.eu/	
Contact:	info@locard.eu	
Version:	101	
Date:	23 November 2019	
Responsible Partner:	EEMA	
Contributing Partners:	ARC, VUB, Others	
Reviewers:	Constantinos Patsakis (ARC) Miltiadis Anastasiadis (MOT)	
Clasification	Public	U
Length		
Dissemination List:	Public	X

This project has received financial support from the European Union Horizon 2020 Programme under grant agreement no. 832735.

1 Revision History

Revision	Date	Author	Organization	Description
0.1	15/10/2019	Jon Shamah	EEMA	Initial draft
0.2	21/10/2019	Jon Shamah	EEMA	2nd draft
0.3	22/10/2019	Jon Shamah	EEMA	3rd draft
0.4	27/10/2019	Istvan Borocz	EEMA	Internal WP2 review
0.5	27/10/2019	Jon Shamah	EEMA	Fine tuning and summary text
0.6	28/10/2019	Jon Shamah / Lorraine Spector	EEMA	Fine tuning
0.7	28/10/2019	Jon Shamah	EEMA	For external review
0.8	21/11/2019	Jon Shamah	EEMA	Lay-out fine tuning
1.0	23/11/2019	Jon Shamah	EEMA	Final

2 Contents

2.1 List of Tables

2.2 List of Figures

3 Glossary

Terms Specific to LOCARD

LEA	Law Enforcement Agency
Local Node	The access point to the LOCARD platform in a particular jurisdiction
Local Node Authority	The authority responsible for the Local Node, especially access policies
Smart Contract	An automated series of code which accompanies each entry onto the LOCARD platform and enforces the policies and conditions determined by the entry originator

Technical Terms

API	Application programming interface
Artefact	Object to be tested. In the case of LOCARD: reference architecture; first Implementation; demonstrators and use cases; final release.
Blockchain	An immutable storage method utilised by LOCARD
eIDAS	eIDentity Assurance and trust Services regulation (EU 910/2014)
GDPR	General Data Protection Regulations (Directive 95/46/EC)
GUI	Graphic User Interface
IDMS	Identity Management Interface
MoSCoW	Descriptive method to describe Must have / Shall have / Could have /Won't have conditions
SELP	Socio, Ethical, Legal and Privacy

Data Protection Terms

Consent of the data subject	It should be a statement or clear affirmative action which is freely given, specific, informed and unambiguous and imitate the wishes of the data subject whereby he/she agrees to the processing of personal data relating to him or her. It can be withdrawn by the data subject anytime; Assessment of free consent can be done via the care of the performance of a contract, provisions of the service agreement.
Data breach	Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Data Controller	A natural or legal person who, alone or jointly, determines the purposes and means of processing is called data controller
Data Processor	A natural or legal person who processes personal data on behalf on the controller is called data processor.
Pseudonymization	Pseudonymization is a kind of processing of personal data in a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information

Detailed descriptions of all terms can be found in LOCARD Deliverable D2.1

4 Executive Summary

Digital evidence is currently an integral part of criminal investigations, and not confined to pure cybercrime cases. The very ubiquity of digital devices, e.g. smartphones, in modern society makes digital evidence extremely relevant for investigations about all kinds of criminal behaviour like murder, contraband activities, and people smuggling, to name a few. LOCARD aims to provide a holistic platform for chain of custody assurance along the forensic workflow, a trusted distributed platform allowing the storage of digital evidence metadata in a blockchain.

For LOCARD, the transparency and immutability that Distributed Ledger Technologies offer brings benefits that may not be able to be achieved in any other way. However, with Distributed Ledger Technologies comes a requirement for robust access control and identity management processes.

These qualities bring a measure of flexibility in the design and attributes of LOCARD that must be monitored and assessed in order to ensure that it meets the obligations to the users and that the robustness of the solution can be maintained in varying circumstances and environments.

Because of the very distributed nature of LOCARD, the various restrictions, conditions and policies that need to be adhered to, must be maintained in a Master Policy which maintains confidence and trust across the entire platform.

This enables clear and consistent auditing and unambiguous 'Rules of the Game' for all users.

In this deliverable D2.2, the LOCARD architecture will be briefly described at high level for contextual reference, the LOCARD Master Policies will be described, and then the elements of that policy will be mapped to the architecture and how they will be applied will be described.

Finally, the requirements as described in D2.1 will be listed, together with the other related parameters, and a brief description of how the status of compliance to those requirements will be collected. This will constitute the basis of the compliance auditing that will take place periodically during the project and into operations.

This deliverable is purposed to be a practical contextual implementation of D2.1 in respect to the LOCARD Platform. It is meant to be understandable to the non-specialist reader, and while it will concentrate on the Societal, Ethical, Legal and Privacy policies, as well as EU Policies components of the Master Policy, it will also explain their context within the greater set of policies applicable to LOCARD and will analyse the compliance to SELP and other policy components of the architecture, rather than offering architecture suggestions, which are the responsibility of Work Package 3.

This deliverable is also intended to be utilised as part of the briefing documentation for onboarding new participants to LOCARD, and also as part of a concept guide for use at the end of the funded project.

5 Introduction

LOCARD project aims to provide a holistic platform for chain of custody assurance along the forensic workflow, i.e. a trusted distributed platform allowing the storage of digital evidence metadata in a blockchain. Each node of LOCARD will be able to independently set its own permission policies and to selectively share access to digital evidence with other nodes when deemed necessary and upon proper authorization through fine-grained policies. LOCARD's modularity will also allow diverse actors to tailor the platform to their specific needs and role in the digital forensic workflow, from preparation and readiness, to collection, analysis and reporting.

LOCARD provides dedicated components for the proactive collection of digital data as well as management of the chain of custody.

LOCARD increases the trust in the handling and processing of digital evidence and the management of chain of custody by providing transparency, using immutable storage to store the chain of custody and using end-to-end security through Trusted Environment Execution. To this end, LOCARD will strive to provide a collaborative and distributed platform that will assist in (see Fig. 1):

1. Collecting digital evidence (online and offline).
2. Processing the stored data to realize the full extent of the related incident (e.g. by finding previously unknown correlations related to possible parallel running/finished investigations).
3. Providing the necessary reports.
4. Handling the data for the court (exports).
5. Allowing citizens to report online incidents.
6. Bind the transactions between clients, investigators, companies etc. through Smart Contracts allowing for integrity, authenticity, traceability and auditability of digital evidence along with digital evidence – related actions.
7. Allow tagging of events and alerts once specific criteria are met on stream data.

Even the best maintained documentation will be useless and might be disputed in a court of law should it not be accompanied by a proper chain of custody which is proven to be intact. This means that, upon acquisition of digital evidence, the evidence must be tagged, numbered and catalogued in an append only registry. The use of blockchain from LOCARD guarantees that the immutability of this and consequently the integrity and authenticity of the underlying evidence.

On the other hand, GDPR[1] mandates compromised organisations as data controllers to report personal data breaches within 72 hours. Due to the heavy fines that the organisations might face, it is important for them to have a clear and continuous insight of how their incident is being processed/investigated. The use of blockchain technology from LOCARD and its reports will enable them to monitor this process as the investigators push the acquired digital evidence to the blockchain. This will allow them to evaluate the case individually from their side.

In order to bring digital evidences in the court of law it is necessary to follow the national standards, laws and methodologies regarding the chain of custody (investigation, acquisition, preservation, transfer, storage, etc.) to ensure that the evidences have not been tampered with. LOCARD will store digital evidences in an immutable distributed storage while at the same time it will employ Smart Contracts in order to keep record of who is using the evidence and the exact actions taken throughout the analysis process. Thus, all the evidence as well as the chain of custody will be court-proof eliminating any doubts.

[1] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en

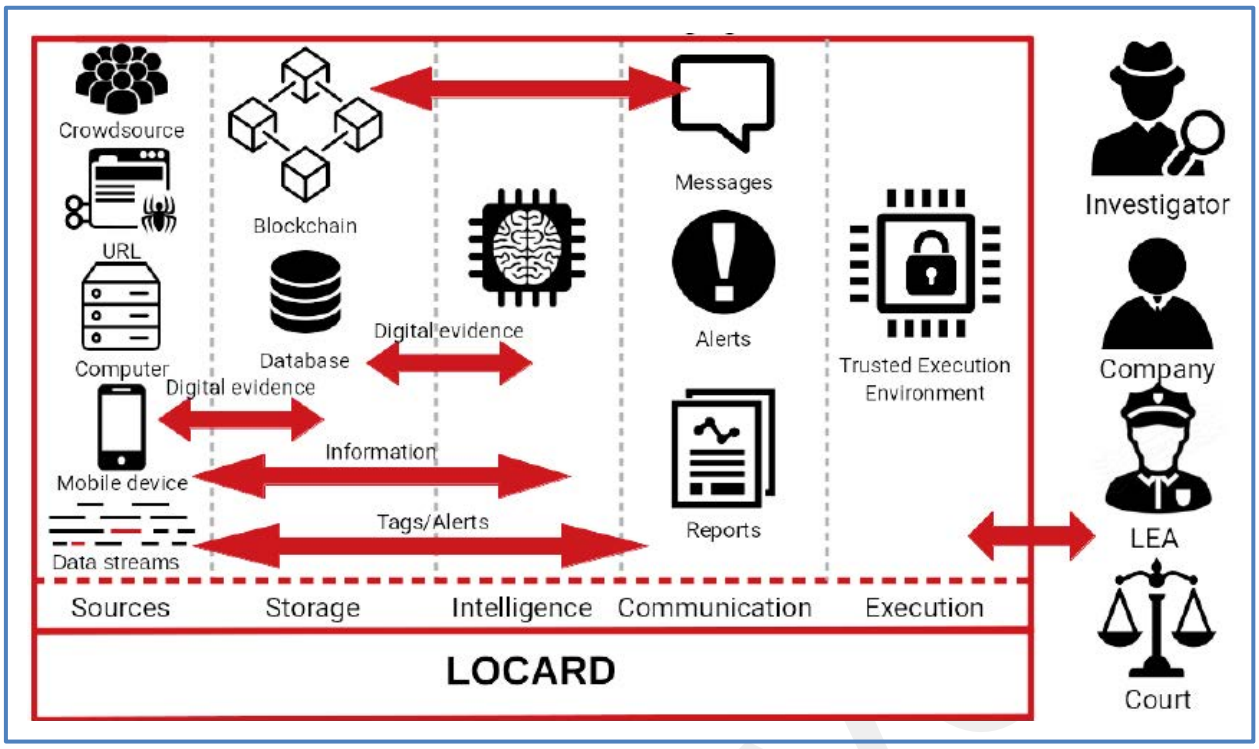

Figure: 1 LOCARD distributed platform

Figure 1 shows the range of components that interact in the workflows and chain of custody domain. These range from data collection of real-time sources (on the left of figure 1) to the end users (on the right of figure 1).

The key goal of chain of custody management is to ensure that all evidence, digital evidence included, has to be stored in a manner that cannot be disputed in a court of law, thus it must be proved beyond ”any reasonable doubt” that the evidence has not been tampered with and that lawful procedures have been followed in every step related to the relevant case (e.g. acquisition, storage, investigation, etc.). It is argued that in order to achieve that, an immutable storage is needed where all the acquired digital evidences are stored and all the transactions are monitored. The above matches ideally to the concept of blockchain, which have been applied successfully in the scope of supply chain management. Indeed, blockchain technologies among other features offer immutability, transparency, robustness, auditability, integrity, authenticity and security.

LOCARD is a unique project that must support scalability and efficiency for storing and sharing vast amounts of data by storing data in an easier to use off-chain mechanism. The latter is expected to significantly improve the provided functionality and improve its scalability. Moreover, LOCARD must consider, within its policy, ways to guarantee that only specific sets of users would be able to access the content, allowing for legal admissibility and compliance. Subsequently LOCARD has to consider a number of factors in its access policy to be successful. These requirements include:

- Technology
- Legal
- Ethics
- Privacy
- Societal
- EU Regulations
- International Conventions

In particular the access to the LOCARD blockchain, which is responsible for maintaining storage for the chain of custody data needs to consider:

- Access Levels
- Roles
- Users
- Actors

These requirements might be either global or local and need to be considered as “Upward Driven” i.e. allowing each Member State and User Organisation of the platform to define its own users, roles, access levels and policies, but still controlled within a common set of policies and governance.

In this document, the LOCARD architecture will be briefly described at high level, the LOCARD Master set of policies will be described, and then the elements of that policy will be mapped to the architecture and how they will be applied will be described. Real-time data collection components to be developed by LOCARD will be treated as other digital evidence, considering their special handling requirements.

Finally, the requirements as described in D2.1 will be listed, together with the other related parameters. The method of collection for monitoring of compliance that will take place periodically during the project and into operations, is also described.

It should be noted that whilst LOCARD endeavours to present a practical platform for use in cross-border digital Chain of Custody, there will be, at the end of the funded period, a series of recommendations for LEAs and other bodies towards harmonisation.

6 LOCARD Contextual Architecture

6.1 LOCARD as a global and flexible technology

The LOCARD concept is based on two principles:

1) The processes that underly the platform itself are transparent, clearly understood and trusted.
2) The data that is stored on the LOCARD platform (the audit trail of criminal evidence), AND the details of the processes in which they were collected should be restricted to those that are entitled to and agreed by the originator of the stored data.

These principles, when combined, present challenges in design and operation, especially when operating across multiple jurisdictions, whilst respecting EU-wide regulations.

Operational considerations need to be considered such as: the right to privacy, and the right to the protection of personal Data must be respected, as well as the operational needs such as pseudonymisation (and anonymisation) within audit records, the restriction of data according to jurisdictional conditions, and the rules that govern LEAs and other bodies and actors within the action itself.

LOCARD needs to accommodate these needs to establish the required trust across all participants and users in order to be a success.

6.2 LOCARD Components

In order to understand how these considerations outlined in D2.1 can be realised, it is first important to understand at practical conceptual level, how LOCARD will be implemented.

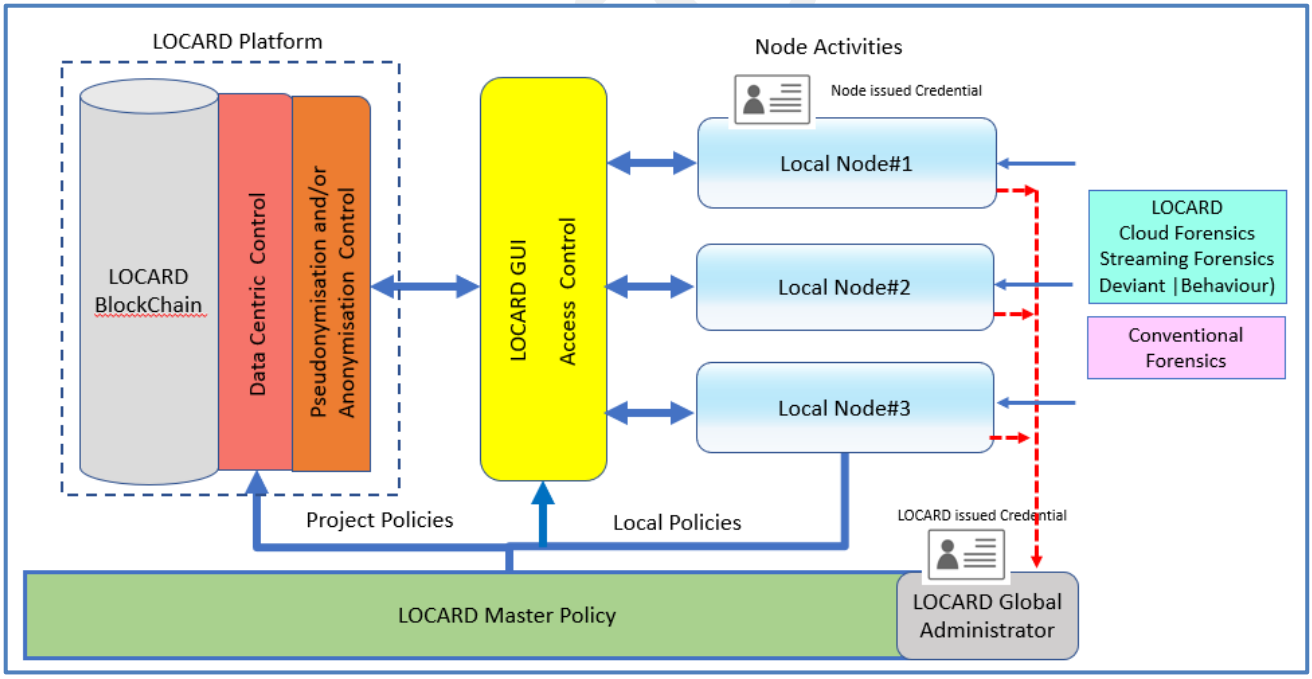

Figure: 2 Conceptual LOCARD Implementation

Figure 2 describes the overall design of the interplay between the components in LOCARD.

The LOCARD Platform consists:

6.3 Local Node(s)

There is one Local Node per Member State or jurisdiction. There may be multiple jurisdictions per Member State.

Each Local Node may act as an access point to the LOCARD Platform and may be used by many local actors and users. These could include LEAs, Forensics Laboratories, legal representatives, and other entities that are authorised to access the LOCARD Chain of Custody records (the stored data).

The rules for determining authorisations, the issuance of access credentials, and the rules for each individual piece of stored data will be determined by the contributor of that evidence record into LOCARD, and so trust must be propagated along the entire LOCARD platform. For this reason, the issuance of credentials, and the maintenance and setting of these rules must be conducted centrally per each Local Node.

In each jurisdiction, it is expected that only one entity, **the Local Node Authority**, will have overall authority to determine these matters and access privileges for the Local Node. The type of authority may vary between jurisdictions, and it may be usual that different levels of actors will be responsible in different jurisdictions.

Local Nodes will also act as the conduit for real-time digital data in each jurisdiction, providing a consistent and common approach to automated data collection audition and integrity maintenance.

Task 3.1 is responsible for determining the workflows for the LOCARD Pilot use cases and the authorities to control each Local Node.

In longer-term operational use, the LOCARD Platform may be connected to the Local Node by way of Application Programming Interface (API), in which case the use of the Local Node as a gateway will be pivotal. However, during the LOCARD pilot phase, it is unreasonable to expect the LEAs to expose their operational systems to a test system, especially as LOCARD will only be tested with dummy data. In this interim case, LOCARD will be accessed via a web-based GUI.

6.4 Access Control and Graphical User Interface

This provides the 'gatekeeping' to ensure access and use is restricted to authorised users.

When in full use, the Local Node will be connected directly to the LOCARD Access Control component via an Application Programming Interface (API). However, as discussed above, during the pilot phase of LOCARD, a separate Graphic User Interface (GUI) will be used to access the LOCARD Platform, and this will be incorporated as part of the Access Control component.

The Access Control component is designed to maintain the rules and conditions pertaining to the individual Local Node. This component will be located within the Member State.

The Access Control Component will also determine the enforcement of the smart contract to be associated with the data record to be applied to the LOCARD Platform. As previously stated, the LOCARD Platform utilises Blockchain, and with it, smart contracts, to enforce control over the data records.

The advantage of maintaining the Access Control components, at the Local Node, and within control of the central managing entity of the node, is that there is an opportunity to maintain any pseudonymity independently of the LOCARD platform and in the local jurisdiction if required.

6.5 Pseudonymisation and/or Anonymisation Control

In many circumstances, persons may need to have their names anonymised or pseudonymised in order to maintain security or to comply with SELP concerns outlined in deliverable D2.1. It should be noted that often, the very fact that an individual or detail is mentioned in an audit log may result in the unwitting revelation of pertinent information. This is especially so when the audit trail contained by LOCARD may be examined lawfully by third parties.

These personal names, (or in fact locations or other details) can be hidden using different methods as follows:

1) Anonymisation

In the case of anonymisation, the detail that needs to be hidden is cryptographically obfuscated so that it can never be reverse engineered to the original. Additionally, each time this is conducted for the same detail, a different outcome will be generated. In the most part, this option is not compatible with the concept of an audit in chain of custody.

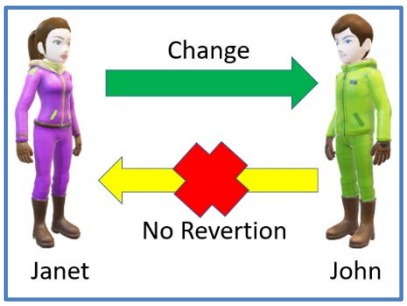

Figure: 3 Anonymisation

2) Pseudonymisation

In the case of pseudonymisation, the detail that needs to be hidden is cryptographically obfuscated but under special circumstances and with permissions may be cryptographically reverse engineered back to the original. Additionally, each time this is conducted for the same detail, a different outcome will be generated, but will always be reverse engineered to the same. This option is compatible with the concept of a chain of custody, where the ability to determine the actual name or detail is in the control of the originating authority and reversion can be executed if agreed. This is less secure than anonymisation but can be compatible with the concept of audit in chain of custody.

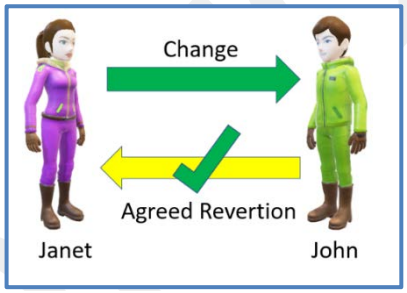

Figure: 4 Pseudonymisation

3) Derived (nickname)

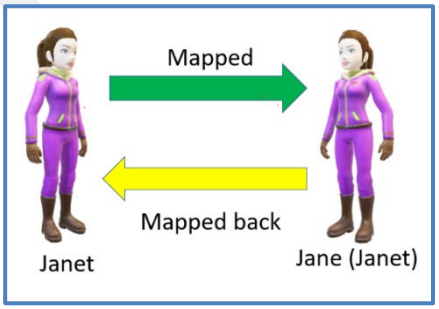

Figure: 5 Derived Identity

In the case of a derived identity, the detail that needs to be hidden is simply replaced by another and while it is not identical, it is mapped and is not cryptographically protected. Each time this is conducted for the same detail, an identical outcome will be generated. This could be the case if the obfuscation was conducted at the Local Node, but outside of the LOCARD Platform User Control. This is the least secure but the most transparent.

This will determine which users will be identifiable directly or with a 'nickname', identified by (a recoverable) pseudonym, or maintain complete anonymity.

Summarising the characteristics as follows:

Type of Obfuscation	Robustness	General Auditable	Repeatable
Anonymity	Cryptographically Strong	No	No
Pseudonymity	Cryptographically Strong	Yes	No
Derivation	No Cryptographically derived	Yes	Yes

Table 1 Comparison of data obfuscation

In most cases the obfuscation is likely to be the responsibility of the Local Node authority.

Where the application of the anonymisation layer will take place will be decided in Work Package 3. A non-exhaustive summary of consequences is outlined in table 3 below:

Location of Anonymisation layer	Visibility of LOCARD user	Consequence
LOCARD Blockchain Platform	LOCARD knows the end user explicitly	LOCARD can audit activity, but the end user is exposed beyond the node's internal domain. LOCARD cannot associate activities across the chain of custody. The node cannot associate activities across the chain of custody.
Local node	LOCARD does not know the end user explicitly	LOCARD cannot audit activity
LOCARD Blockchain Platform and Local Node	LOCARD does not know the end user explicitly	LOCARD cannot audit activity

Table 2 Consequences of Anonymisation

In each of the cases above, the subject of the criminal evidence data is protected by the LOCARD Blockchain Manager.

6.5.1.1 Consequences of Pseudonymisation on LOCARD

Where the application of a Pseudonymisation layer takes place will be decided in Work Package 3. A non-exhaustive summary of consequences is outlined in table 4 below:

Location of Pseudonymisation layer	Visibility of LOCARD user	Consequence

LOCARD Blockchain Platform	LOCARD knows the end user explicitly	LOCARD can audit activity, the end user is not explicitly exposed in the audit, but is identifiable if permitted, as per LOCARD Master policy. LOCARD can associate activities across the chain of custody.
Local Node	LOCARD does not know the end user explicitly	LOCARD can audit activity, but the end user is only identifiable if permitted by the node, as per its own internal rules. LOCARD can associate activities across the chain of custody. The node can associate activities across the chain of custody.
LOCARD Blockchain Platform and Local Node	LOCARD does not know the end user explicitly	LOCARD can audit activity, but the end user is only identifiable if permitted by the local node, as per its own internal rules. LOCARD can associate activities across the chain of custody. The node cannot associate activities across the chain of custody.

Table 3 Consequences of Pseudonymisation

It should be noted that these consequences are for guidance only and will vary depending on the method of application of anonymisation and/or pseudonymisation.

6.6 Data Centric Control

This component determines how the data record to be stored on LOCARD and will be accessible and is often an integral part of the blockchain solution. It is often referred to as the 'smart contract'. The control will be granular in that each data record stored on LOCARD can have its own set of rules controlled by the executed smart contract when it was applied to the LOCARD Platform. (See D4.3). A smart contract is a computer code that can be built into the blockchain to facilitate, verify, or negotiate a 'contract' agreement. Smart contracts operate under a set of conditions that users agree to in order to access the data. When those conditions are met, the terms of the agreement are automatically carried out, and the data is made available in the predetermined manner and with the predetermined restrictions.

Examples of data centric control can be:

1) "This data entry can only be viewed by a user with level 'Inspector' or higher."
2) "This data entry must be anonymised in all cases, when viewed outside of the originating jurisdiction"
3) "This data entry must not be viewed in XYZ Member States"

These controls can be complex or simple and form the basis of the smart contract. It is likely that there will be standard schemas established to make it as easy as possible to store a data record on LOCARD.

6.7 LOCARD Blockchain

The LOCARD Blockchain is the primary storage mechanism (See D4.3) for all LOCARD data records. Blockchain technology was chosen as it is highly distributed and by design, has multiple copies of the records stored and updated at each 'node', thus ensuring that a copy of the data is maintained in each jurisdiction.

LOCARD will use a Private Permissioned model meaning that it will only be accessible to specified users with specified authorisations and is likely to be on a private secured network.

The usage characteristics of each data record is managed by the smart contract which performs Data Centric Control.

When entering data onto the LOCARD blockchain the workflow rules in the smart contract, including who is trusted to verify them, (see "Trust Lists" section below) are set by the originating local node and its user as in figure 6.

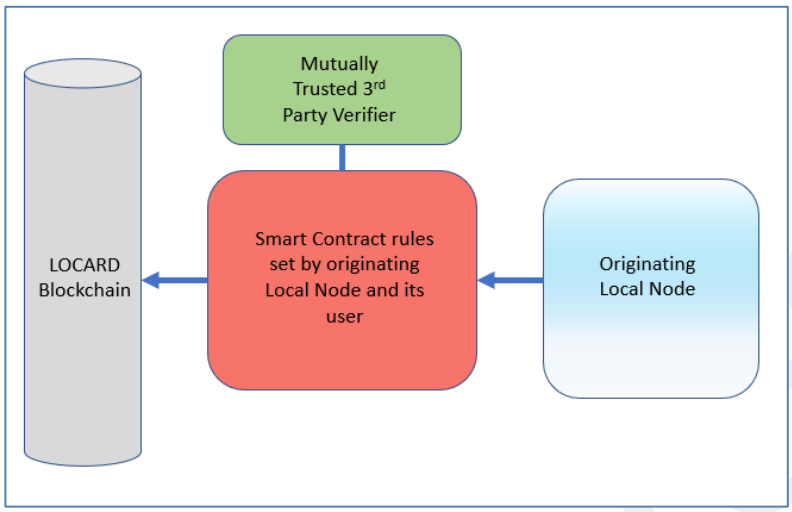

Figure: 6 workflow for entering data onto LOCARD Blockchain

Similarly, when viewing data on the blockchain (or copying data for further forensic manipulation) the workflow rules are enforced by the Smart Contract and verified by a Trusted 3rd Party Verifier as per Figure 7.

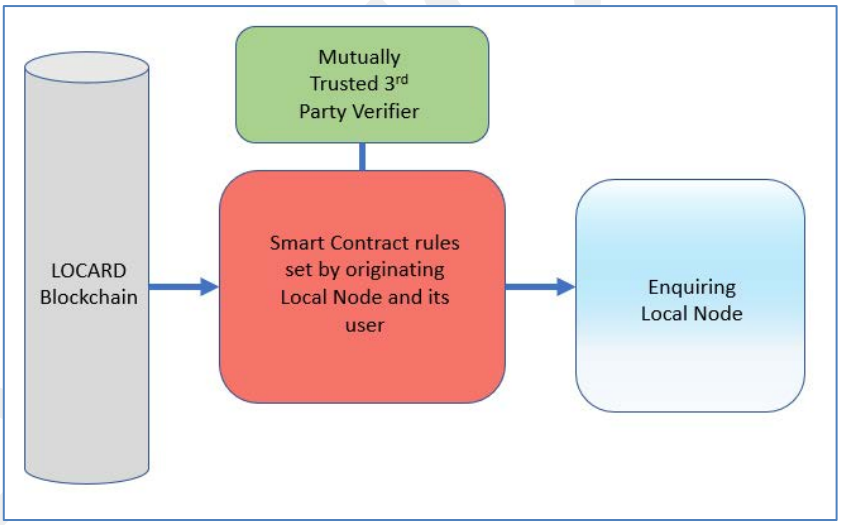

Figure: 7 workflow for viewing data onto LOCARD Blockchain

6.8 LOCARD Master Policy

This lists the 'Rules of the Game' for LOCARD, as described below. It comprises the global LOCARD Platform that will be maintained for all data entries and additionally specific entry by entry conditions set by Local Nodes.

The LOCARD Master Policy ensures that Trust in LOCARD is maintained throughout its use and provides that assurance that LOCARD meets the SELP and regulatory requirements for operating in the EU and other jurisdictions when they become appropriate.

The LOCARD Master policy can be enforced at the Local Node itself, the Access Control component, and on the LOCARD blockchain itself, where it is enforced by the smart contract.

6.9 LOCARD Global Administrator

Depending on the final architecture, this will be the overall authority in control of LOCARD that will be responsible for the global aspects of the platform, its operations and governance. The LOCARD Global Administrator would determine issues such as the composition of Schemas for Smart Contracts, the approval of the authorities that are needed to confirm (verify) that smart contract conditions have been fulfilled, and control trust in operational decisions on the use of the LOCARD Platform etc.

The Administration function itself would be subject to high level governance, which may derive from an international body or EU appointed entity, agreed by all stakeholders.

In the development stages of LOCARD the role of Global Administrator will be taken up by the Coordinator (ARC) or a delegated partner.

6.10 The Use of Trust Lists

As stated, the LOCARD Global Administrator provides approval for verification authorities, essential in the use of Smart Contracts.

In Europe, it is common practice to use “Trust Lists” to manage large numbers of entries from multiple sources. This is similar to how Trust Lists work in the eIDAS Regulation (EC) No 910/2014/EU.

Trusted Lists have a constitutive effect. In other words, a trust service provider (in the LOCARD case that is the Smart Contract Verifier) and the verifications it provides will be trusted only if it appears in the Trusted Lists. Consequently, LOCARD users can only confidently establish a Smart Contract using the legal effect associated with a given trusted verifier, if the latter is listed (as trusted) in the Trusted Lists.

There is an obligation for each LOCAL Node’s Authority to establish, maintain and publish trusted lists, pertaining to the trusted Verifiers within their jurisdiction, together with information related to the verification services provided by them.

Trusted Lists are therefore essential in ensuring certainty and building trust among LOCARD users, as they indicate the status of the Smart Contract verifiers to be used.

The “List of Lists”, listing all the Trust Lists used in LOCARD, will be held and distributed by the LOCARD Global Administrator.

In LOCARD, they could work like this:

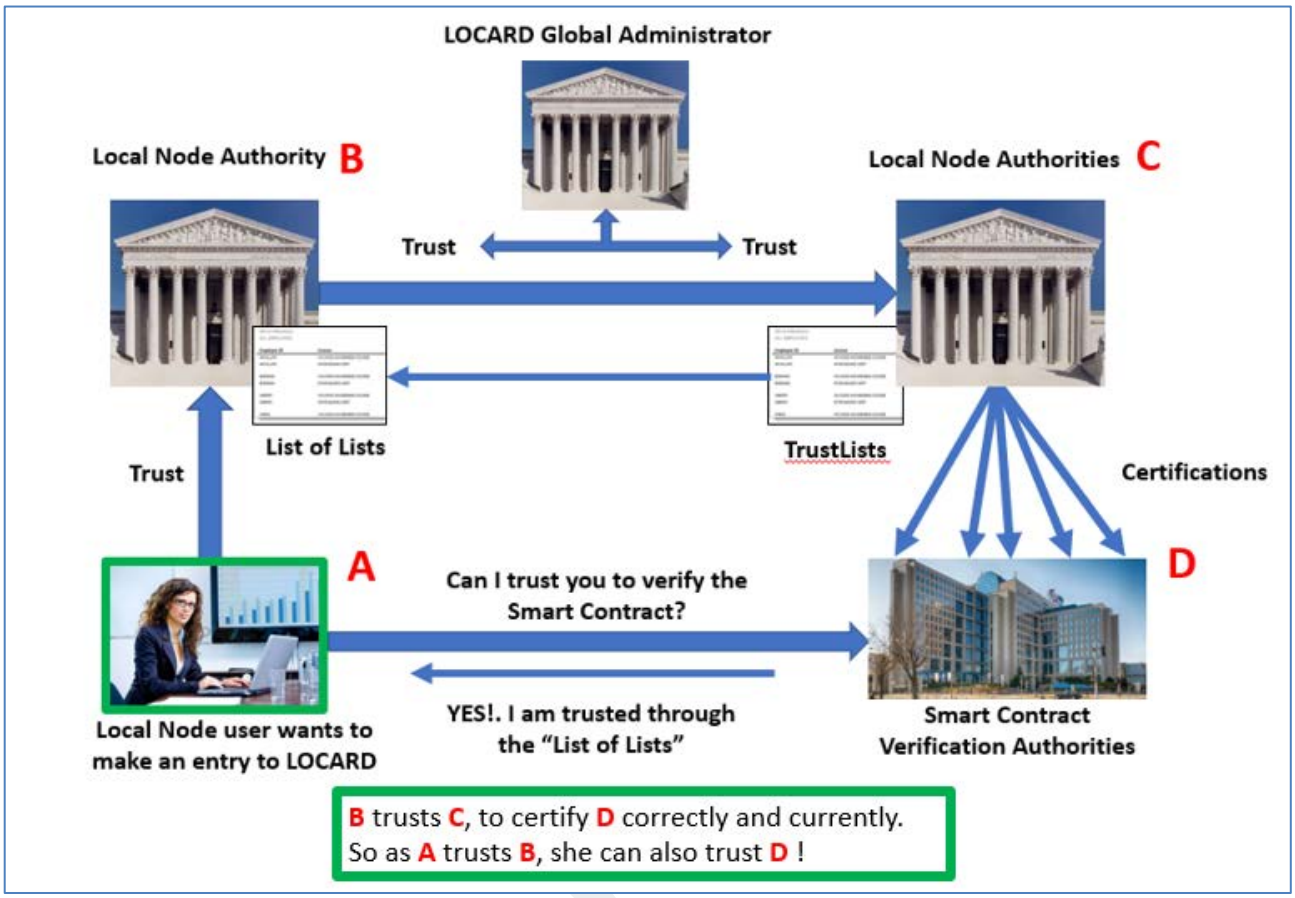

Figure: 8 LOCARD Trust List Relationships

In the Figure 6, the LOCARD Global Administrator distributes a signed "List of Lists" is distributed to all Local Node Authorities ("B" and "C"). When making an entry of a data record on LOCARD using the Smart Contract, the verifiers of the smart contract will be checked against the relevent Trust Lists (approved by the List of Lists). *Figure 6 is illustrative of the trust flows only.*

So the originating Local Node user can specify which verifiers can be used to verify that the smart contract has been correctly and faithfully executed in the knowledge that they can be trusted.

Alternatively a single aggregated Trust List could be used, but this would require continuing effort by the LOCARD Global Administrator to monitor and maintain that list in all jurisdictions.

This mechanism will be hidden toi users of LOCARD through pre-designed Smart Contract schemas (workflows) that will only use verifiers that are on the an approved Trust List.

7 LOCARD Master Policy Overview

The LOCARD Master Policy comprises the 'Rules of the Game' that all participants in LOCARD must obey ('Project Policies'), coupled with specific rules imposed by Member States ('Local Policies'). These interplay between components of the policies are illustrated below in Figure 3.

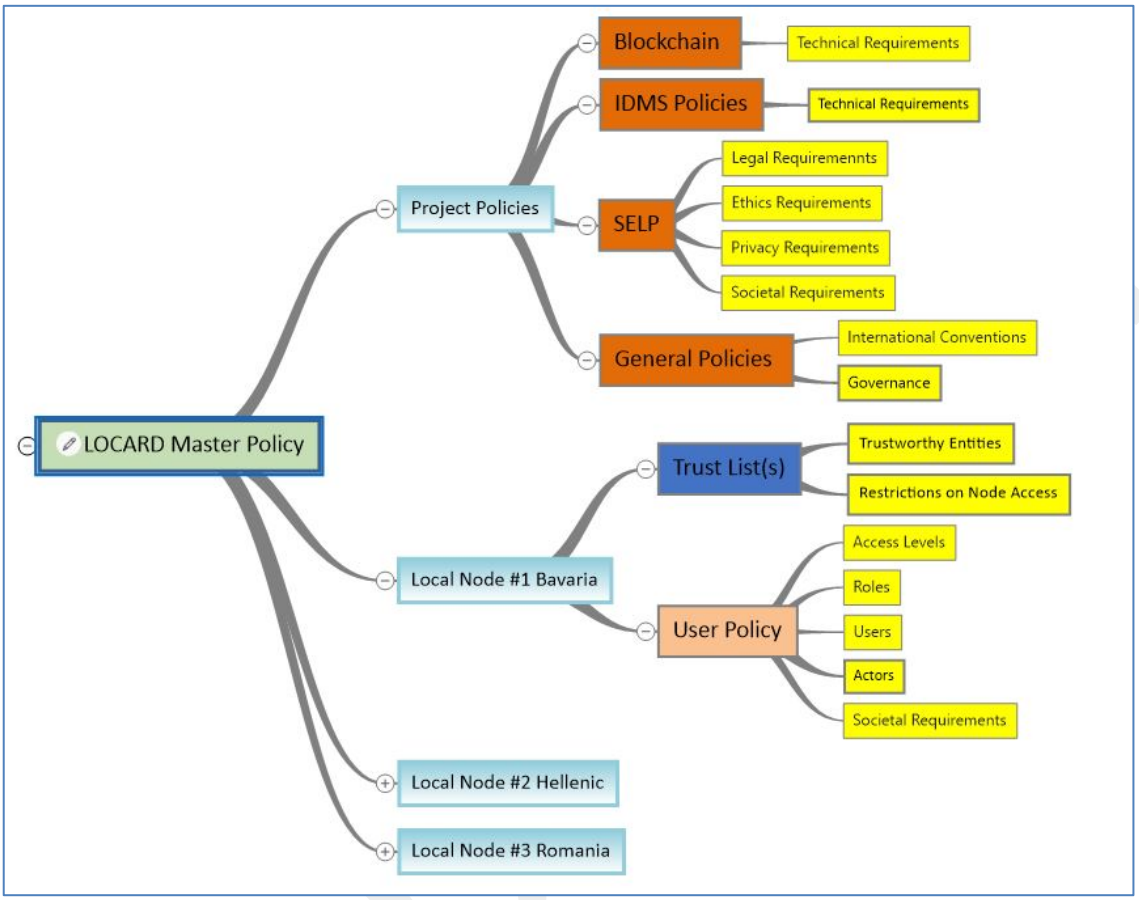

Figure: 9 LOCARD Master Policy

The LOCARD Master Policy will be derived from the following requirements as listed previously and with the following responsibilities for their *descriptions*

Policy Component	Responsible Work Package
Blockchain and IDMS Technical	3/4
Societal, Ethical, Legal and Privacy	2
General Policies	2/4
Local Node Policies	3

Table 4 LOCARD Policy Components

The goal is to ensure that the policies and rules of all participants are respected. This ensures trust and continual usage of LOCARD, with new participants joining over time.

As per figure 6 and table 4, there are multiple elements to the Master Policy, and each may be enforced within various LOCARD components (such as the smart contract) or at the Local Nodes themselves.

7.1 Project-Wide Policies – Blockchain & IDMS

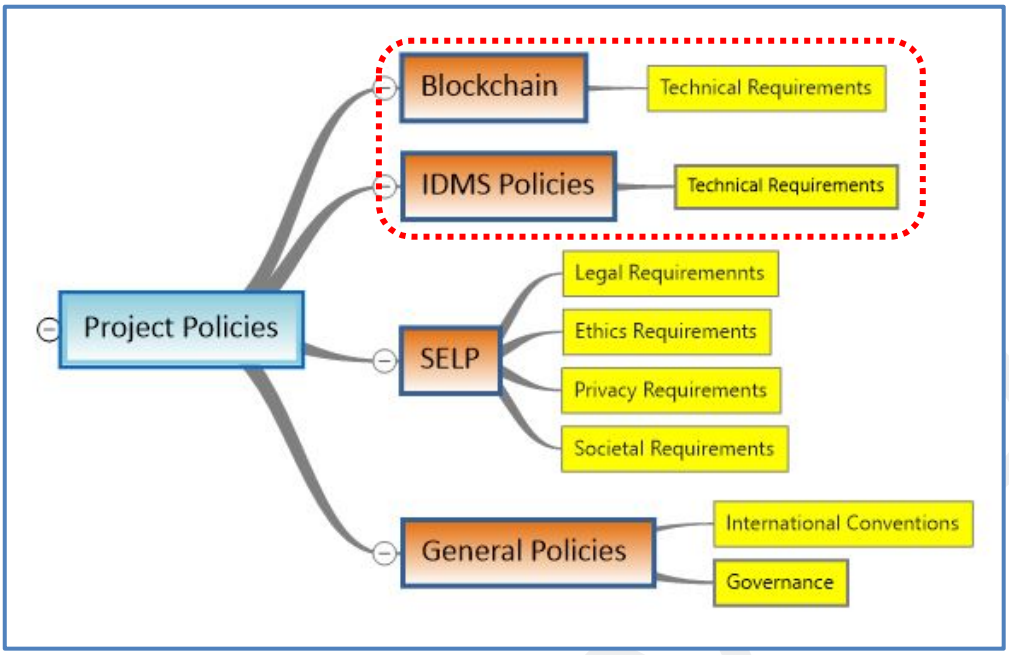

Figure: 10 Project-Wide Policies - Technical

It should be noted that EU policies (eIDAS, GDPR, Privacy) are discussed within IDMS and SELP sections due to the nature of their influence across the entire LOCARD Master Policy.

7.1.1 Blockchain Technical Policy Components

The use of blockchain technology in LOCARD may determine several technical and security requirements that extend across all components of LOCARD. These will depend on the final architecture, but will include:

1. Agreement to trust a list of verifiers of smart contract events in each jurisdiction
2. Agreement to provide a performance and availability of Local Nodes as part of a Service Level Agreement

These may also encompass minimum security requirements, protocols, schemas, In Operation, these are likely to be the responsibility of the LOCARD Global Administrator and may be upheld through multilateral agreement rather than technology.

7.1.2 Identity Technical Policy Components

The use of identity obfuscation has been discussed previously. However, there must be minimum standards regarding the use of identities across the entire platform.

It should be clear that LOCARD, primarily being targeted to EU Member States, must comply with the eIDAS Trust Regulation (See D4.4) where appropriate. This will be summarised below. However, other Standards Developing Organisations (SDOs) produce relevant associated standards and these will be described as well in the later section. These regulations will need to be enforced or verified by the LOCARD platform.

The eIDAS Regulation specifies three assurance levels of 'trust':

Low	
	limited degree of confidence in the claimed or asserted identity of a Person
	reference to technical specifications, standards and procedures, including technical controls, the

	purpose of which is to decrease the risk of misuse or alteration of the identity
Substantial	
	substantial degree of confidence in the claimed or asserted identity of a Person
	reference to technical specifications, standards and procedures, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity
High	
	higher degree of confidence in the claimed or asserted identity of a Person
	reference to technical specifications, standards and procedures, including technical controls, the purpose of which is to prevent misuse or alteration of the identity

Table 5 Levels of Assurance for identities

Level 3 (High) is the appropriate level for LOCARD activities.

Each of these addition services ('Trust Services') will also be required to ensure that data is to be trusted:

Ensuring Level 3 (High) digital signatures are used:	
	Qualified certificate delivery for electronic signatures
	Qualified certificate delivery for electronic seals
	Qualified certificate delivery for website authentication
Standardising the date and time when using LOCARD:	
	Qualified time stamping
Verifying digital signatures are valid at time of use:	
	Qualified validation of qualified electronic signatures
	Qualified validation of qualified electronic seals
	Qualified preservation of qualified electronic signatures
	Qualified preservation of qualified electronic seals

Table 6 Additional Trust Services required

Both Assurance Levels and Trusted services are EU Regulations and are described in EU 910/2014 with further implementation acts as outlined in D4.4.

It is expected that LEAs and other entities will conform to these regulations regarding identification, digital signatures and their supporting actions.

It should be noted that the compliance to eIDAS is listed here as part of IDMS policy rather than separately.

7.2 Project-Wide Policies – SELP

7.2.1 Legal Policy Requirements

7.2.2 Ethics / Privacy and Social Policy (SELP) Requirements

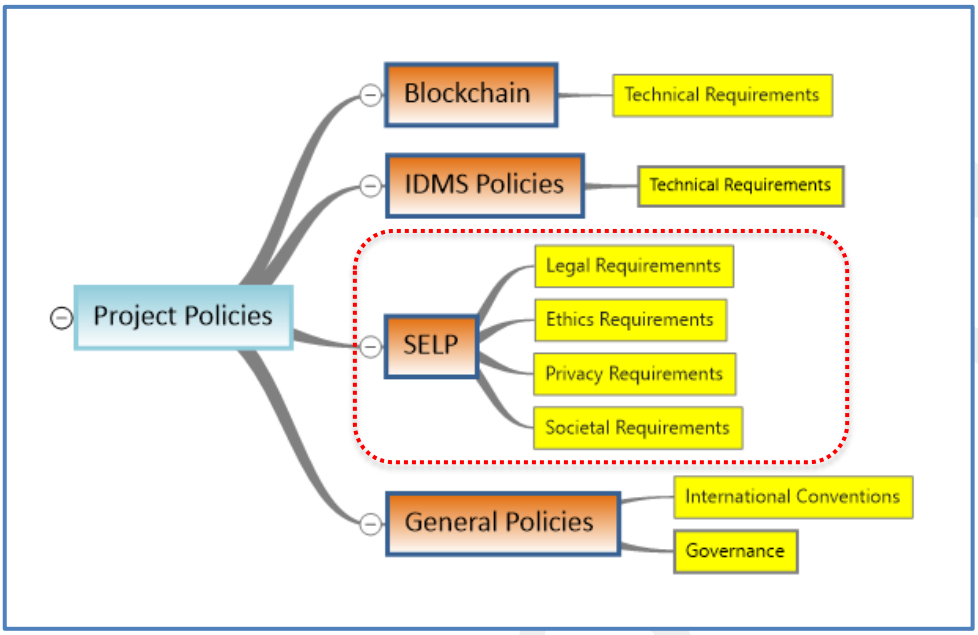

Figure: 11 Project-Wide Policies - SELP

The SELP requirements cover the following and are discussed in detail in deliverable D2.1:

- The ethical requirements incumbent upon first responders, investigators, and analysts and the use of data envisaged by LOCARD within the foreseen contexts;
- The data protection framework including (but not limited to) the General Data Protection Regulation (the GDPR) Regulation 2016/679/EU[2] and the 2016/680 Data Protection Directive[3] that pertains in particular, to data protection in the context of criminal investigations.
- Human Rights: The European Court of Human Rights has important case law relating to the privacy of the individual; and
- Legal possibilities and restraints found within national law for the use and sharing of data in emergency contexts such as public emergencies, natural disasters and terrorist attacks. The LOCARD project will, in terms of Member State law, look at the examples of Greece, Romania, and Germany which will be used as trial sites during the project.

It should be noted that this deliverable and the corresponding tasks in Work Package 2 test the compliance to SELP and other policy components of the architecture, rather than the overall design.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

7.3 General Policies

Due to overlap, general policies such as eIDAS, GDPR and Privacy are generally covered by the SELP and IDMS requirements and described above. However, in certain circumstances, such as interoperability with other jurisdictions outside of the EU, these may extend beyond the foreseen SELP requirements.

International Conventions

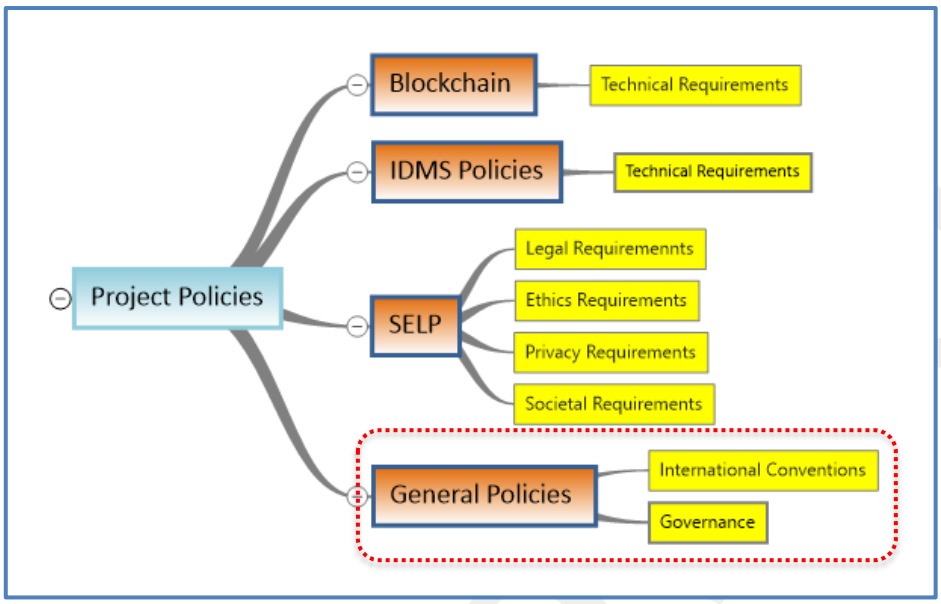

Figure: 12 Project-Wide Policies - General

Extra-territorial requirements, such as those due to international conventions may need to be applied to the LOCARD platform and these should be within the responsibility of the LOCARD Global Administrator to ensure compliance, as they will apply to all users and all Local Nodes.

Governance

LOCARD wide policies and decisions regarding the governance of the LOCARD platform itself must be the responsibility of the LOCARD Global Administrator, as discussed above. Adherence to the terms and conditions of use of the LOCARD Platform, whether by convention or multilateral agreement, must be part of any smart contract to ensure trust between all parties.

7.4 Local Node Policies

7.4.1 Trust Lists

Trust Lists at the Local Node represent the restrictions that are placed upon the data being sent to the LOCARD platform that are either general rules. For example: “Never make record data visible to XYZ entity” or “Flag any record data from XYZ entity as being untrustworthy”.

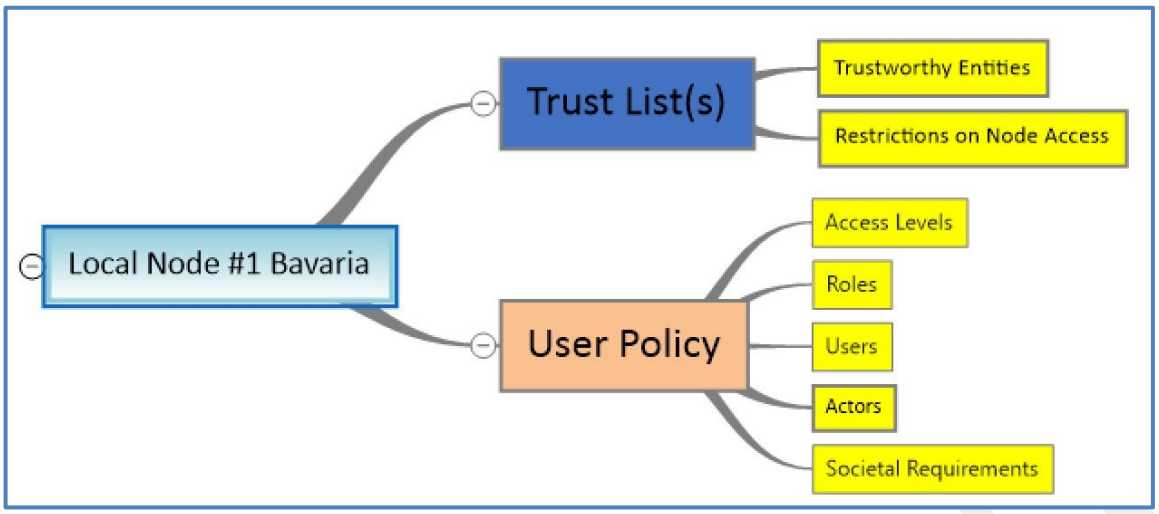

Figure: 13 Local Node Policies

In operation, these rules should be implemented at the Local Node, and should be in sole control of the Local Node Authority.

Trustworthy Entities

These restrictions may be legally derived or the result of policy decisions by the Local Node authority. Traditionally stored in the form of 'white' or 'black' lists of specific entities, they can be used to enforce political or trust policies either between users in from a single local node or between local nodes.

Restrictions on Node Access

Often, there may be protocols in place at the Local Node to restrict the access to the LOCARD platform by particular entities dependant on the type of evidence or case that is being recorded and investigated. For example: "If this is a XXX crime, only permit access LOCARD to this YYY agency".

7.4.2 User Policy

User Policies determine how to provision identities to users, while managing authentication, authorization, and data sharing. This is the traditional Identity and Access Control portion of LOCARD at the local node. It is the responsibility of the Local Node Authority to define the access rules.

Each node of LOCARD will be able to independently set its own permission policies and to selectively share access to digital evidence with other nodes when deemed necessary and upon proper authorization through fine-grained policies. LOCARD's modularity will also allow diverse actors to tailor the platform to their specific needs and role in the digital forensic workflow, from preparation and readiness, to collection, analysis and reporting. Please see LOCARD Deliverable D4.4. for a broader background on Identity Management.

As discussed earlier, in section 7.1.2, the issuance of credentials should be conformant with the eIDAS Trust Services regulations regarding levels of assurance.

During the funded project, credentials will be issued specifically for access to the LOCARD Access Control GUI. Authorisations will then be determined manually per credential and stored in the LOCARD Access Control GUI itself.

However, in full operation, that GUI may be replaced by direct access to the LOCARD platform via an API. In this case there will be access to many individual entities, so a common credential should be used. It is suggested that "eIDAS Notified" National eID cards be used as the basic trusted credential, being uniformly Level of Assurance 3-HIGH. Authorisations will then be determined in the Local Node for each credential.

Determination of roles, users, and actors will need to be standardised across each Local Node, otherwise there can be no guarantee that a particular attribute restriction can be enforced across each Local Node.

During the funded project, agreement between participants to utilise standardised descriptions will be required. This should be based on ISO/IEC 27037:2012.

However, in full operation, there should be a migration to use ISO/IEC 27037:2037 which defines types of 'Actors' and roles. If this is not possible, the Local Node should be able to map the local terms into this standard description.

8 SELP Compliance for LOCARD

8.1 Monitoring and maintaining Compliance

This monitoring forms part of LOCARD tasks T2.2 and T2.3

During the design and build, periodic monitoring will take place to ensure compliance with the Master Policy and requirements outlined in D2.1. and to feed into D2.3 the SELP impact assessment.

As part of this monitoring, the responsibility for each of the supporting assets should be assigned not only for a guide to a compliant design, but also as a part of any operational guide for the use of LOCARD Platform and design of the smart contract template:

Policy Component	Design and build responsibility	Operational Responsible for component
Blockchain Technical	WP5	LOCARD Global Administrator
IDMS Technical	WP5	LOCARD Global Administrator
Societal, Ethical, Legal and Privacy	WP5	Smart contract (on LOCARD Platform)
General Policies	WP5	Smart contract (on LOCARD Platform)
Trust List	WP3	Local Node Authority
User Policies (including identity obfuscation)	WP3	Local Node Authority and/or smart contract

Table 7 Policy components and responsibilities

8.2 Evaluation Approach to SELP Compliance Requirements

The LOCARD evaluation approach will examine three differing artefacts; The LOCARD Reference Architecture (WP3), Initial implementation (WP5), and Demonstrators (WP6).

LOCARD will use a simple evaluation process into three easy steps. First, we identify each of the Artefacts, which in their case are three use cases, a reference architecture, and implementation. Second, we clarify the SELP requirements and expectations for each of the artefacts (See Section 9 in this document, developed from deliverable D2.1).

Lastly, we evaluate, which is when each artefact identified is tested against the SELP requirements. The results of this will assist in D2.3 (Impact Assessments). The three artefacts are then re-evaluated during the project (if appropriate for the reference architecture artefact) and reported in deliverables D2.4 (Month 24) and D2.5 (Month 25).

It is important that the requirements are an unambiguous as possible. For this reason, the MoSCoW method is used. Being outcome-focused, the method provides a clear and measurable set of specifications, which can, over time, be continually monitored for compliance. The method labels each specific requirement, making it easier to prioritise.

The MoSCoW Method is an acronym made up of the first letters. (The two Os have been added to make the word ‘moscow’ readable; they don’t have any meaning themselves) The M stands for ‘Must haves‘, S for ‘Should haves‘, C for ‘Could haves‘ and W for ‘Won’t haves‘. Each requirement is assigned one MoSCoW label, by which it can be measured.

In order to monitor the progress of the evaluations over the timeline of the funded project, a series of visualisations will be used.

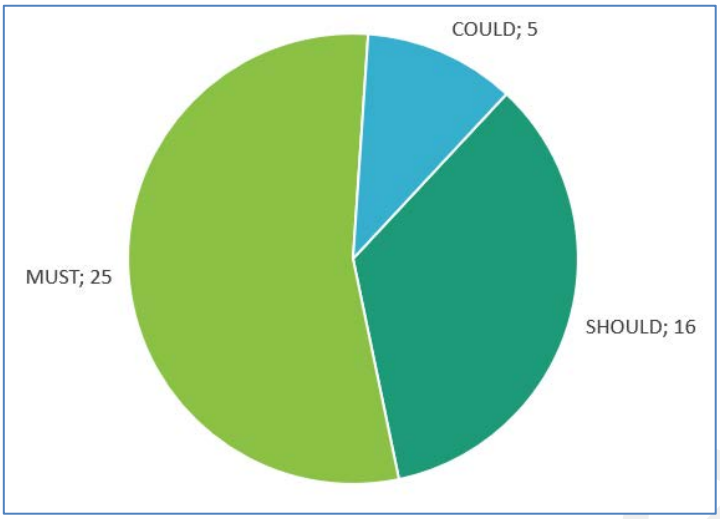

Figure: 14 Initial Classification and MoSCoW labelling of SELP Requirements

It is recognised that the requirements may evolve over the period of the project and will vary when examining each artefact. The current initial levels (figure 12) are applicable to the implementation architecture artefact.

8.3 Measurement of status of compliance

For each requirement it is necessary to determine the state of compliance, together with other meaningful data in order to track the progress of each requirement and to compare improvements or rectifications.

The information collected will also gather how the test was conducted, and should it not pass mitigations to resolve the issue, and any anticipated knock-on impacts to other requirements

Theme	Description of Response
Organisational Information	
	Version (or identifier of tested revision of test software)
	Date of assessment
	Task responsible for implementation of requirement
	Task responsible for implementation of any mitigation
Compliance	
	Status of compliance (Pass /Neutral/Fail)
	Measured how? (manual/measurement:detail)
	Description of primary and supporting assets of the system to the requirement
	If Pass, Neutral or fail, description of reason for score
	If Neutral or fail, possible mitigation actions
	If Neutral or fail, impacts on other components of the mitigation that will in turn require mitigation
Application	

	Compatibility of the applicable use cases to the requirement, and any deviations (Pass /Neutral/Fail)
	If Pass, Neutral or fail, description of reason for score
	If Neutral or fail, possible mitigation actions
	If Neutral or fail, impacts on other components of the mitigation that will in turn require mitigation

Table 8 Status Information Collection

8.4 Method of gathering compliance data

Because of the large amount of data that will need to be collected, a digital survey tool will be completed by the partners involved in the development of each artefact.

This will be developed for use using either the EU Survey Tool[4] or commercial equivalent approved by the Security Advisory Board (SAB) if required. The language used will be English, but it is anticipated that alternate languages may be used in the future.

This will enable direct comparisons between artefacts and frequent monitoring of progress regarding compliance. Additionally, this may be extended beyond the SELP requirements to other aspects of the Master policy which require monitoring.

8.5 Timelines for Compliance

The following is a suggested timeline for the process for compliance testing until the end of the LOCARD funded project:

Artefact	Compliance Start	Compliance Completion	Related Deliverables
Reference Architecture	M10	M12	D3.4 System Requirements D3.5 Reference Architecture
Rectification and Mitigation	M13	M20	Continuing to work collaboratively the WPs to improve outcomes and rectify deficiencies as the occur
Initial Implementation	M21	M24	D5.7 Integration of demonstrator Applications - iteration 1 (Note: Consortium Confidential)
Rectification and Mitigation	M25	M30	Continuing to work collaboratively the WPs to improve outcomes and rectify deficiencies as the occur
Demonstrators / Use Cases	M31	M34	D6.3 LOCARD deployment and validation report

Table 9 Process for SELP compliance testing

Note that these dates may be subject to agreed change between the relevant work packages and WP2.

[4] https://ec.europa.eu/eusurvey/home/welcome

9 LOCARD SELP Requirements

This section is a distillation of the D2.1 determination and reflects the SELP requirements for LOCARD. It provides an indicative list of criteria to be met by the consortium in connection with the project and should be considered provisional. Where appropriate, technical implementation will be assigned as above to individual WPs. It must be emphasised that this is only a provisional list and its content is subject to change in light of the development processes in the project. However, this list will be used as part of the SELP section of the compliance questionnaire.

9.1 Consent

For law enforcement purposes, the rights of data subjects are limited. However, during the period of the funded research project, the goals of the data processing may vary, and may be open to interpretation. This will be determined when these requirements are tested and may be marked as "Not Applicable in this artefact"

As per recital 32 of the GDPR "Consent should be given by a clear affirmative act establishing a **freely given, specific, informed and unambiguous** indication of the data subject's agreement to the processing of personal data relating to him or her…"

9.2 SELP requirements in tabular format

Compliance Reference	D2.1 Reference	Condition	Classification on Architecture
SELP: 001	4.2	The identification of the affected dimensions of privacy by LOCARD **COULD** facilitate a better designing process.	COULD
SELP: 002	4.2	The harm, caused to the right to privacy, **MUST** be necessary to pursue other benefits (i.e. preference of other rights).	MUST
SELP: 003	4.2	The harm caused to the right to privacy **MUST** be proportionate to other benefits (i.e. preference of other rights).	MUST
SELP: 004	4.2-4.3	Fair balance between the competing private and public interests (e.g. public safety and right to access to personal data which is used as an evidence) **SHOULD** be preserved.	SHOULD
SELP: 005	4.3.2	The LOCARD project **MUST** protect any personal data it collects or processes according to the definition of personal data in the GDPR.	MUST
SELP: 006	4.3.13.1	Any data controllers of such personal data within LOCARD, **MUST,** both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, which are designed to implement data-protection principles in an effective manner, and to integrate the necessary safeguards into	MUST

		the processing in order to meet the requirements of GDPR and protect the rights of data subjects.	
SELP: 007	5.2.1	PR.002 provisions **SHOULD** bear in mind the provisions in GDPR for the use of data in criminal justice, anti-fraud and counter terrorism purposes.	SHOULD
SELP: 008	4.3.5-4.3.6	It **MUST** be clarified which types of personal data will be processed by the LOCARD platform.	MUST
SELP: 009	4.3.6	It **MUST** be clarified whether sensitive data will be processed by the LOCARD platform and if yes which types.	MUST
SELP: 010	4.3.22.1.4	The processed data by the LOCARD platform must be relevant and accurate.	MUST
SELP: 011	4.3.12	The data controller (and data processor(s)) as well as the recipients of personal data **MUST** be identified prior to the processing of personal data.	MUST
SELP: 012	4.3.19	It **SHOULD** be made clear, whether personal data will be transferred to third countries and if yes, whether the third country provide adequate protection.	SHOULD
SELP: 013	4.3.13.1	Data controller in LOCARD **MUST** be able to demonstrate compliance with data protection law	MUST
SELP: 014	4.3.13.1	Data subjects **MUST** be informed about the intended data processing operation during the duration of the LOCARD project.	MUST
SELP: 015	4.3.13.1	The legal ground and the purpose of the data processing **MUST** be defined.	MUST
SELP: 016	4.3.10	If the processing of personal data will be based on the consent of the data subject, it **MUST** be informed, specific and freely given.	MUST
SELP: 017	4.3.13.1	The end date of the processing **SHOULD** be determined, and it **SHOULD** be made clear, what will happen with the personal data afterwards.	SHOULD
SELP: 018	4.3.13.1	The security of data **MUST** be ensured	MUST
SELP: 019	4.3.13.1	The rules of access to personal data (with special attention to its conditions, mode, and limits) **MUST** be clearly defined	MUST
SELP: 020	4.3.13.1	The processing operations **MUST** be documented.	MUST
SELP: 021	4.3.12	The exercise of the rights of the data subjects **MUST** be ensured.	MUST
SELP: 022	4.3.12	Information **SHOULD** be provided to the data subject about the processing operation within LOCARD?	SHOULD
SELP: 023	4.3.13	If the LOCARD platform will be applied and used without informing the data subjects the safeguards and security measures **MUST** be clarified beforehand.	MUST

SELP: 024	4.3.13	Unused personal data **SHOULD** be deleted automatically.	SHOULD
SELP: 025	4.3.13	The processed data **MUST** be relevant and accurate for the purposes of data processing. The LOCARD system should record and work with only those types of data which are necessary to reach the goal of the processing.	MUST
SELP: 026	4.3.13	The processing of personal data **MUST** be based on a legitimate legal ground and shall have specified purposes	MUST
SELP: 027	4.2	The engagement of data subjects to the development phase **COULD** provide additional information regarding potential risks, furthermore it **COULD** provide assurance of the outcome of the risk management and increase of the mutual understanding among data subjects and the LOCARD project.	COULD
SELP: 028	4.3.13	Appropriate technical and organisational measures **MUST** be applied to ensure a level of security appropriate to the potential risk.	MUST
SELP: 029	4.3.13	To determine the level of adequacy of the applied security measures, every determining factor **SHOULD** be taken into consideration whereas the means of communication is a pivotal element.	SHOULD
SELP: 030	4.3.10	Consent **MUST** only be given by the data subject, if the age of the same is over the age of 16 years;	MUST
SELP: 031	4.3.10	Consent on behalf of a child, a person below 16 years, **MUST** be given by his/her legal or lawful guardian;	MUST
SELP: 032	4.3.10	The data controller **MUST** verify whether the consent given by the child's parental guardian is the same or not;	MUST
SELP: 033	4.3.10	Consent **MUST** be freely given, specific, informed and unambiguous;	MUST
SELP: 034	4.3.10	Consent **SHOULD** be given by way of a statement or clear affirmative action;	SHOULD
SELP: 035	4.3.10	Consent **MUST** imitate the wishes of the data subject whereby he/she agrees to the processing of personal data relating to him or her;	MUST
SELP: 036	4.3.10	Consent **COULD** be withdrawn by the data subject anytime;	COULD
SELP: 037	4.3.10	Withdrawal and giving of consent **SHOULD** be easy and can be done in the same manner;	SHOULD
SELP: 038	4.3.10	Assessment of free consent **COULD** be done via the care of the performance of a contract, provisions of the service agreement.	COULD
SELP: 039	4.3.23	The ecosystem of LOCARD **SHOULD** accommodate the different levels of skills of its users.	SHOULD

SELP: 040	4.3.23	The main benefits LOCARD (either a specific component of it or the system as a whole), thus the potential reasons of choosing this platform, **SHOULD** be identified.	SHOULD
SELP: 041	4.3.23	The principle of equality **SHOULD** be considered.	SHOULD
SELP: 042	4.3.23	Clear benefits **COULD** enhance the acceptability and involvement of cutting-edge technologies in law enforcement	COULD
SELP: 043	4.3.23	The system **SHOULD** be prepared for atypical scenarios	SHOULD
SELP: 044	4.3.23	Every possible outcome **SHOULD** be taken into consideration and affect the development of the system	SHOULD
SELP: 045	4.3.23	The extent of the involvement of data subjects as research participants to the development processes **SHOULD** be defined.	SHOULD
SELP: 046	4.3.23	The views and feedbacks of stakeholders **SHOULD** be collected	SHOULD

Table 10 SELP conditions to be met

10 Project Description

Digital evidence is currently an integral part of criminal investigations, and not confined to pure cybercrime cases. Criminal behaviours like financial frauds, intellectual property theft, industrial espionage, and terrorist networks leverage the Internet and cyberspace. The very ubiquity of digital devices, e.g. smartphones, in modern society makes digital evidence extremely relevant for investigations about all kinds of criminal behaviour like murder, contraband activities, and people smuggling, to name a few. Due to its nature, the use of digital evidence in a court of law has always been challenging. It is critical that it should be accompanied by a proper chain of custody, guaranteeing its source and integrity. LOCARD aims to provide a holistic platform for chain of custody assurance along the forensic workflow, a trusted distributed platform allowing the storage of digital evidence metadata in a blockchain. Each node of LOCARD will be able to independently set its own permission policies and to selectively share access to digital evidence with other nodes when deemed necessary and upon proper authorization through fine-grained policies. LOCARD's modularity will also allow diverse actors to tailor the platform to their specific needs and role in the digital forensic workflow, from preparation and readiness, to collection, to analysis and reporting. LOCARD will have a crowdsource module to collect citizen reports of selected violations, a crawler to detect and correlate online deviant behaviour, and a toolkit for investigators that will assist them in collecting online and offline evidence. This will be powered by an immutable storage and an identity management system that will protect privacy and handle access to evidence data using a Trusted Execution Environment. Blockchain technology will not only guarantee that information about the evidence cannot be tampered with but allow interoperability without the need for a trusted third party.

Participant Legal Names

- Athina-Erevnitiko Kentro Kainotomias Stis Technologies
- StAG
- Fundacion Apwg, European Union Foundation
- Motivian Eood
- Imc Diachirisi Pliroforion Kai Epikinonion Anonymos Etairia
- Universita Degli Studi Di Padova
- Telefonica Investigacion Y Desarrollo Sa
- European Electronic Messaging Association Aisbl
- Neurosoft Cyprus Limited
- Vrije Universiteit Brussel
- Vlaamse Ict Organisatie
- Infotrend Innovations Co Ltd
- Universita Ta Malta
- Kentro Meleton Asfaleias
- Technische Universitat Berlin
- Norges Teknisk-Naturvitenskapelige Universitet Ntnu
- Hellenic Police
- Inspectoratul General Al Politiei Romane