MADITRACE

Guidelines and Recommendations for Security, Confidentiality and Privacy

Deliverable D3.7

Version N°1

Authors: Óscar Ansótegui Adarve (Funditec), Salomé Aida Sepúlveda Fontaine (Funditec)

Funded by
the European Union

Disclaimer

The content of this report reflects only the author's view. The European Commission is not responsible for any use that may be made of the information it contains.

Funded by
the European Union

Document information

Grant Agreement	n°101091502
Project Title	Material and digital traceability for the certification of critical raw materials
Project Acronym	MaDiTraCe
Project Coordinator	Daniel Monfort, BRGM
Project Duration	1 January 2023 – 30 Juin 2026 (42 months)
Related Work Package	WP3
Related Task(s)	T3.4
Lead Organisation	FUNDITEC
Contributing Partner(s)	CEA, SPHERITY
Due Date	30/06/2025
Submission Date	31/07/2025
Dissemination level	PU – Public

History

Date	Version	Submitted by	Reviewed by	Comments
29/07/2025	V1	Óscar Ansótegui Adarve (FUNDITEC)	Rouwaida Abdallah (CEA)	
30/07/2025	V1	Óscar Ansótegui Adarve (FUNDITEC)	Daniel Monfort (BRGM)	Final review after WP leader technical review
31/07/2025	V1	Óscar Ansótegui Adarve (FUNDITEC)	D. Monfort, L. Duivon, A. Paul	Final Version

Table of contents

1 Introduction 10
1.1 Background 10
1.2 Purpose and scope of the deliverable 10
1.3 Methodological approach 11
1.4 Relation with other tasks 11
2 Threat modelling and cybersecurity foundations *(based on Report 1)* 12
2.1 Relation with the preliminary threat modelling report 12
2.2 P.A.S.T.A. methodology 13
2.2.1 Overview and motivation 13
2.2.2 Description of the seven stages 13
2.2.3 Applicability to traceability architectures 14
2.3 Application of PASTA to MaDiTraCe 15
2.3.1 Asset identification 15
2.3.2 Threat agents and attack surface 17
2.3.3 Attack scenarios and abuse cases 20
2.4 Risk analysis 21
2.4.1 Risk prioritisation and classification 21
2.4.2 STRIDE and DREAD mapping 23
2.5 Cybersecurity recommendations 25
2.5.1 Securing the credential lifecycle 25
2.5.2 Preserving data integrity and authenticity 26
2.5.3 Ensuring system availability and resilience 26
2.5.4 Securing API exposure and partner integrations 27
2.6 Security tools, techniques and future implications 28
3 Blockchain evaluation and selection *(based on report 2)* 29
3.1 Relation with the Blockchain selection report 29
3.2 Relevance of blockchain in the DPP context 30
3.2.1 Key requirements of the Digital Product Passport 30
3.2.2 Evaluation of traditional vs distributed models 32
3.3 Blockchain selection methodology 34
3.3.1 Framework overview and taxonomy 34
3.3.2 Step-by-Step decision process 34
3.4 Comparative analysis of blockchain types 36
3.4.1 Comparison between Public, Private, Consortium and Hybrid blockchains 36

Funded by
the European Union

3.4.2 Governance, privacy and scalability trade-offs 37
3.5 Consensus mechanisms 37
3.6 Comparative assessment of candidate technologies 39
3.6.1 Strengths and weaknesses analysis of each technology 40
3.7 Final selection and justification 42
3.8 Conclusions and implementation planning 43
4 Notarization tool audit and Smart Contract security *(based on report 3)* 44
4.1 Relation with report 3 (Notarization Tool and Smart Contract Analysis)..................... 44
4.2 Notarization tool analysis..................... 45
4.2.1 Architecture and notarization process 45
4.2.2 Document verification on blockchain and server 45
4.2.3 Privacy and access considerations 46
4.3 Access control implementation 47
4.3.1 Definition of roles 47
4.3.2 Authentication methods and permissions..................... 47
4.3.3 Restricting access to individual notarizations..................... 48
4.4 Smart Contract analysis..................... 49
4.4.1 Security audit results with Slither 49
4.4.2 Identified vulnerabilities and improvements 50
4.4.3 Access control implementation with roles 50
4.5 Security recommendations 52
4.5.1 Enhancing privacy and data storage 52
4.5.2 Hash encryption implementation 52
4.5.3 Attack prevention and risk mitigation 53
4.6 Implementation roadmap and future enhancements..................... 53
5 Integrated guidelines for security and privacy..................... 54
5.1 Secure design principles 54
5.1.1 Authentication and authorisation 54
5.1.2 Encryption and hashing 55
5.1.3 Secure data flows and storage..................... 55
5.2 Confidentiality and GDPR compliance 56
5.2.1 Data minimisation and consent models 56
5.2.2 Pseudonymisation and user control..................... 57
5.3 Identity management and SSI considerations 57
5.3.1 Applicability and limitations..................... 58
5.3.2 Use of ZKP or delegated trust 58

Funded by
the European Union

6 Operational security and continuous risk management 59
6.1 Security governance for the traceability system 59
6.2 Monitoring, logging and incident response 59
6.3 Continuous threat modelling and update process 60
6.4 Auditing frameworks and compliance roadmap 60
6.5 Roles and responsibilities across stakeholders 61
6.6 Recommendations for future penetration testing 61
6.7 Supply chain threats and open risks 61
7 Conclusions and recommendations 62
7.1 Key security insights across workstreams 62
7.2 Recommendations for development and pilots 63
7.3 Strategic alignment with project goals 64
8 References 65
9 Annexes 66
9.1 Full Report 1 – Threat Modelling (PASTA) 66
9.1.1 Excel workbook - PASTA Methodology 66
9.2 Full Report 2 – Blockchain Selection 66
9.3 Full Report 3 – Notarization Tool and Smart Contract 66

List of tables

Table 1: Stages of P.A.S.T.A Methodology 14
Table 2: Asset Categorization 16
Table 3: Key Asset Classification 17
Table 4: Classification of Threat Agents in MaDiTraCe 18
Table 5: Main Attack Surface Categories in MaDiTraCe 19
Table 6: Key Attack Scenarios and Associated Abuse Cases 21
Table 7: Risk Prioritisation Matrix for Key Threats 23
Table 8: Mapping of Threats to STRIDE Categories 24
Table 9: DREAD Risk Scores for High-Priority Threats 25
Table 10: Mitigations by Domain and Component 27
Table 11: Blockchain Contributions to Key Requirements in the Digital Product Passport Context 31
Table 12 : Key Requirements for a Blockchain-Based Digital Product Passport 32
Table 13: Comparative Assessment of Centralised vs Distributed Models 33
Table 14: Blockchain selection steps applied to MaDiTraCe 35
Table 15: Comparative Overview of Blockchain Types 37
Table 16: Comparison of Consensus Mechanisms for Blockchain Networks 38
Table 17: Comparative Overview of Blockchain Candidates 40
Table 18: Blockchain Suitability Matrix 43
Table 19: Security Considerations in the Blockchain-Based Notarization Proces 45

Funded by
the European Union

Table 20: Proposed Enhancements for Secure and Private Notarization 47
Table 21: Authentication Methods for Access Control in Notarization Systems 48
Table 22: Overview of Secure Design Principles and Controls 54
Table 23: Recommended GDPR Compliance Controls 56
Table 24: Summary of SSI Considerations and Recommendations 58
Table 25: Roles and Responsibilities in the Security Governance Framework 61
Table 26: Operational Security Components and Recommended Practices 62
Table 27: Recommended Security Measures by Area and Priority 63

Summary

This deliverable (D3.7) provides a comprehensive set of guidelines and recommendations to ensure the security, confidentiality, and privacy of the MaDiTraCe architecture. Developed under Task 3.4 of Work Package 3, it supports the broader goal of enabling a secure and trustworthy digital product passport (DPP) for critical raw materials (CRMs) across global supply chains.

The document is structured around three main areas of focus:

- Secure system design, including threat modeling, architecture-level risk analysis, and the definition of access and control mechanisms.
- Data confidentiality and integrity, through the application of encryption strategies, secure storage, and blockchain-backed notarization processes.
- Risk management and mitigation, including vulnerability assessment, smart contract auditing, and guidelines for resilience and regulatory alignment.

In order to address these areas effectively, the work carried out in Task 3.4 was developed iteratively and modularly, producing three dedicated technical reports:

- A threat modeling report using the P.A.S.T.A. methodology to identify potential risks in the draft architecture.
- A blockchain selection report, evaluating and justifying the most suitable technology for the DPP.
- A smart contract and notarization tool assessment, analyzing privacy risks, verifying access control models, and auditing the associated smart contract.

This deliverable consolidates the findings from these reports into a single, integrated document that outlines actionable security guidelines and provides a clear roadmap for secure design and implementation in future phases. The outcomes and recommendations from this deliverable will be taken into account when refining the final architecture to be delivered in D3.6, ensuring alignment between threat modelling insights and system design decisions.

The referenced reports are included as annexes to support traceability and depth of analysis.

Keywords

Security, Privacy, Confidentiality, Risk Management, Threat Modeling, Blockchain, Digital Product Passport (DPP), Notarization, Smart Contracts, SSI (Self-Sovereign Identity), PASTA, Data Integrity, Access Control, GDPR Compliance, Slither, Merkle Tree, Encryption, Authentication, Cybersecurity Guidelines.

Funded by
the European Union

Abbreviations and acronyms

Acronym	Description
WP	Work Package
SSI	Self-Sovereign Identity
DPP	Digital Product Passport
PASTA	Process for Attack Simulation and Threat Analysis
RBAC	Role-Based Access Control
PoA	Proof of Authority
BFT	Byzantine Fault Tolerance
ZKP	Zero-Knowledge Proof
KMS	Key Management Service
HSM	Hardware Security Module
API	Application Programming Interface
MFA	Multi-Factor Authentication
EU	European Union
EBSI	European Blockchain Services Infrastructure
GDPR	General Data Protection Regulation
DoS	Denial of Service
PoC	Proof of Concept
HMAC	Hash-based Message Authentication Code

Funded by the European Union

1 Introduction

1.1 Background

The MaDiTraCe project aims to enhance transparency, reliability, and certification processes within critical raw material (CRM) supply chains. As part of this objective, Work Package 3 (WP3) focuses on the design and implementation of a secure and trustworthy digital product passport (DPP) that leverages digital technologies to ensure traceability, integrity, and compliance across multiple actors and jurisdictions.

In this context, Task 3.4 plays a key role by addressing the security, confidentiality, and privacy dimensions of the proposed traceability architecture. These aspects are not only technical requirements but also legal and ethical imperatives, particularly in light of regulations such as the General Data Protection Regulation (GDPR) and the increasing reliance on distributed systems and data exchange in cross-border supply chains.

The architectural choices made in Task 3.3, such as the use of blockchain technology, smart contracts, and potentially Self-Sovereign Identity (SSI), introduce new vectors of risk and require a structured and forward-looking security strategy. Task 3.4 was therefore designed to identify potential vulnerabilities, assess technological options, and provide a comprehensive set of recommendations to strengthen the resilience and trustworthiness of the DPP system.

This deliverable summarises the work carried out throughout Task 3.4 and supports subsequent implementation activities within WP3 and other technical work packages.

1.2 Purpose and scope of the deliverable

The purpose of this deliverable is to consolidate the outcomes of Task 3.4 and present a coherent set of guidelines and recommendations aimed at strengthening the security, confidentiality, and privacy of the MaDiTraCe traceability architecture. The deliverable addresses both strategic and technical aspects, offering actionable insights for implementation in subsequent development and integration tasks.

Its scope includes the following elements:

- Security analysis, including threat identification and mitigation strategies applied to the draft architecture.
- Evaluation of confidentiality and privacy requirements, with a focus on data protection mechanisms and alignment with relevant legal frameworks.
- Technical assessment of core components, such as the blockchain layer, the notarization tool, and the smart contract responsible for anchoring traceability data.
- Recommendations for access control, identity management, and secure design, with an emphasis on practical applicability in real-world industrial environments.

This deliverable serves as a bridge between the exploratory work conducted in Task 3.4. It provides the necessary security foundations to ensure that the MaDiTraCe digital product passport is robust, trustworthy, and compliant by design.

Funded by
the European Union

1.3 Methodological approach

Task 3.4 was carried out using a modular and iterative methodology, adapted to the evolving nature of the traceability architecture defined in Task 3.3. Given that key architectural decisions, such as the use of blockchain, smart contracts, and Self-Sovereign Identity (SSI), were progressively defined, the security analysis and recommendations had to remain flexible and responsive to changes.

To manage this dynamic environment, the task was structured around three complementary axes:

- Threat modelling and risk analysis, based on the P.A.S.T.A. (Process for Attack Simulation and Threat Analysis) methodology. This allowed for a structured identification of system assets, potential attackers, abuse cases, and risk mitigation strategies.
- Technology evaluation, focusing on blockchain selection criteria and the implications of different distributed ledger technologies (DLTs) for the MaDiTraCe digital product passport.
- Component-level assessment, centered on the analysis of the notarization tool, its associated smart contract (Store.sol), and the implementation of access control and data protection mechanisms.

Each of these axes led to the creation of an individual technical report, which served both as a foundation for internal validation and as source material for this deliverable. The approach allowed the project to maintain a clear audit trail while ensuring that the recommendations presented here are aligned with real architectural and operational choices.

The outputs of the three technical reports have been synthesised, integrated, and expanded in this document to provide a unified vision of the security, confidentiality, and privacy measures recommended for MaDiTraCe.

1.4 Relation with other tasks

This deliverable is directly linked to Task 3.3, which defines the architecture of the MaDiTraCe traceability system. The security, confidentiality, and privacy measures proposed in this document have been designed to complement and reinforce the architectural choices made in Task 3.3, ensuring that security is integrated from the early stages of system design rather than added as a separate layer.

In particular, the recommendations provided here support:

- The definition of the blockchain layer and data storage mechanisms analysed in Task 3.3, by identifying the most suitable technologies from a security and compliance perspective.
- The specification of smart contracts and notarization workflows, by providing guidelines for secure implementation and mitigation of known vulnerabilities.

- The integration or non-integration of Self-Sovereign Identity (SSI) components, by highlighting the implications for identity management, access control, and data minimisation.
- The design of data access and verification processes, by outlining principles for confidentiality, authentication, and auditability.

The outputs of Task 3.4 also provide a foundation for the technical development and validation activities, as well as contributing to the overall cybersecurity and compliance strategy of the project.

By maintaining consistency with the architectural, functional, and regulatory aspects of the project, this deliverable ensures that security, privacy, and data protection are treated as cross-cutting priorities within MaDiTraCe.

2 Threat modelling and cybersecurity foundations *(based on Report 1)*

2.1 Relation with the preliminary threat modelling report

The threat analysis presented in this chapter is the result of a structured assessment conducted under Task 3.4, and is extensively based on the technical document *Report 1 – Preliminary Threat Modeling Report: PASTA Analysis on Draft Architecture* developed by Funditec. This report constitutes the core output of the threat modelling activities and applies the PASTA (Process for Attack Simulation and Threat Analysis) methodology to the draft version of the MaDiTraCe architecture, as defined in Task 3.3.

At the time of the analysis, the architecture was still in a draft phase, with key elements such as the blockchain layer, data verification mechanisms, and identity systems under active discussion. Despite these evolving conditions, the application of PASTA provided a robust framework to model the attack surface, identify system-level risks, and recommend mitigation strategies that are valid across a range of plausible configurations.

To complement the report, a structured Excel-based threat modelling sheet was used to organise the identified threats, assets, actors, and mitigation actions. This spreadsheet acts as a dynamic reference point and allows for traceability and prioritisation of risks based on severity, likelihood, and impact. It also facilitates updates and iterations in response to architectural changes or new threat intelligence.

The integration of this report into the current deliverable (D3.7) ensures alignment between architectural design (Task 3.3), threat modelling (Task 3.4), and upcoming implementation. The approach also ensures scientific rigour, transparency in the analysis, and traceability of all identified cybersecurity concerns.

Whenever relevant, this chapter will explicitly reference specific sections or findings from the report and the accompanying spreadsheet to maintain coherence and verifiability. The full report is included as Annex 1 of this deliverable for in-depth consultation.

Funded by
the European Union

2.2 P.A.S.T.A. methodology

2.2.1 Overview and motivation

The application of the P.A.S.T.A. (Process for Attack Simulation and Threat Analysis) [1] methodology to the MaDiTraCe traceability system is driven by the need to proactively identify and mitigate cybersecurity threats that may compromise the integrity, confidentiality, or availability of traceability data. Unlike reactive approaches that address security concerns post-implementation, P.A.S.T.A. is designed to align threat modelling with business objectives from the outset of system design.

In the context of MaDiTraCe, this is particularly relevant due to the high regulatory sensitivity of critical raw material (CRM) traceability, the involvement of multiple stakeholders across jurisdictions, and the architectural reliance on emerging technologies such as blockchain and verifiable credentials. These technologies introduce not only significant benefits in terms of decentralisation and data immutability, but also new threat surfaces that traditional security frameworks may overlook.

By adopting a structured threat modelling methodology early in the design phase, Task 3.4 aimed to achieve the following [2]:

- Ensure security-by-design: Embedding threat identification and mitigation at the architectural level supports the design of inherently secure workflows, particularly in the digital product passport (DPP) infrastructure.
- Anticipate cross-cutting vulnerabilities: Given the layered nature of the system, combining blockchain, off-chain services, identity systems, and APIs, PASTA provides a holistic view of how threats may propagate across components.
- Support regulatory alignment: Threat modelling also informs the compliance strategy with GDPR and supply chain due diligence regulations, by revealing points where personal or sensitive data could be exposed or altered.
- Provide a traceable rationale for security decisions: The structured, seven-step approach of P.A.S.T.A. offers a repeatable and auditable process, allowing future updates to the architecture to be evaluated against previously identified risks.

The motivation for using P.A.S.T.A. in MaDiTraCe thus lies in its capacity to bridge technical threat analysis with strategic decision-making. It ensures that the traceability architecture is not only functional and scalable, but also trustworthy, resilient, and capable of resisting sophisticated adversarial behaviour from both internal and external actors.

2.2.2 Description of the seven stages

The P.A.S.T.A. methodology structures the threat modelling process into seven sequential stages [3], each contributing a specific layer of understanding to the system’s threat landscape. Applied to the MaDiTraCe architecture, these stages guided the identification of vulnerabilities and informed the definition of actionable countermeasures.

The following table summarises each stage and its relevance to MaDiTraCe [2]:

Funded by the European Union

Stage	Description	Application in MaDiTraCe
1. Define the Objectives (Business Impact Analysis)	Establish the business context and identify high-level security goals aligned with business priorities.	Ensuring traceability, regulatory compliance, and resistance to manipulation within CRM supply chains.
2. Define the Technical Scope	Identify technical assets, components, and boundaries of the system.	Draft architecture includes control and data planes, blockchain layer, SSI modules, and API endpoints.
3. Application Decomposition	Break the system into subcomponents to analyse their roles, interactions, and data sensitivities.	Components such as credential issuance, verifiable data manager, and monitoring services were decomposed and analysed.
4. Threat Analysis	Identify possible threats based on attacker profiles and known vulnerabilities.	Focused on credential forgery, DoS attacks, and data tampering in the Digital Twin and catalogue.
5. Vulnerability Analysis	Detect weaknesses and assign severity levels based on likelihood and impact.	Highlighted insufficient cryptographic controls, poor input validation, and limited monitoring capabilities.
6. Attack Modelling	Simulate realistic attack paths and their potential consequences.	Emulated DoS, Man-in-the-Middle (MitM), and insider attacks targeting critical trust components.
7. Risk and Impact Analysis	Prioritise risks and define tailored mitigation strategies.	Resulted in technical and organisational recommendations to address high-priority risks.

Table 1: Stages of P.A.S.T.A Methodology

This structured progression ensures that threat modelling is not a one-off task but an evolving process that can be revisited as the system architecture matures. It also enhances traceability of security decisions, since each mitigation strategy can be linked to a specific threat scenario and technical component.

The implementation of these stages during Task 3.4 helped identify weaknesses not only in individual modules but also in the overall interactions between subsystems, which is critical in complex, distributed architectures such as that of MaDiTraCe.

2.2.3 Applicability to traceability architectures

The P.A.S.T.A. methodology proves particularly suitable for traceability architectures such as MaDiTraCe, where multiple systems, actors, and technologies interact across organisational and jurisdictional boundaries [4]. The inherent complexity of digital product

Funded by the European Union

passports, especially when combined with decentralised components like blockchain and self-sovereign identity (SSI), demands a security framework that can accommodate both technical depth and systemic interdependence.

Several factors underline the applicability of P.A.S.T.A. to MaDiTraCe and similar traceability systems:

- **Multi-layered architecture**: Traceability systems typically comprise control planes (governance and issuance), data planes (sensors, digital twins, storage), and trust anchors (blockchain, credentials). P.A.S.T.A. accounts for this complexity by analysing each layer and the interactions between them.
- **Cross-organisational workflows**: In MaDiTraCe, actors include mining companies, certification bodies, manufacturers, and regulators. The P.A.S.T.A. model accommodates these varying roles by enabling the identification of threat agents with different motivations, privileges, and attack vectors.
- **Compliance-driven environments**: Regulations such as the EU Battery Regulation and Corporate Sustainability Due Diligence Directive impose strict requirements on data integrity, auditability, and confidentiality. P.A.S.T.A. explicitly links threats to business goals and legal obligations, making it easier to align security efforts with compliance strategies.
- **Evolving and modular systems**: As MaDiTraCe's architecture is expected to evolve over time, especially during the transition from proof of concept to large-scale deployment, the iterative nature of P.A.S.T.A. ensures that threat modelling can adapt to future updates, technology changes, or operational shifts.
- **Data authenticity as a cornerstone**: Since trust in the traceability system relies on the authenticity of data (e.g., origin, transformation steps, and environmental impact), P.A.S.T.A. helps evaluate the potential for credential forgery, data injection, and manipulation, which are key risks for distributed traceability infrastructures.

In conclusion, P.A.S.T.A. not only supports a granular and systemic threat analysis, but also reinforces the core objectives of traceability: verifiability, trust, and resilience. Its use in MaDiTraCe ensures that the foundations of the DPP are secured against both foreseeable and emerging risks, offering a robust baseline for subsequent implementation.

2.3 Application of PASTA to MaDiTraCe

2.3.1 Asset identification

Asset identification is a foundational step within the P.A.S.T.A. methodology, as it establishes a comprehensive inventory of the technical components, data assets, and functional services that constitute the MaDiTraCe traceability architecture. This inventory not only defines the technical scope of the system but also enables a precise mapping of threats to assets, facilitating effective risk mitigation.

In MaDiTraCe, the asset identification process was conducted during Stage 2 of the P.A.S.T.A. methodology and was refined iteratively throughout Task 3.4 as architectural details matured. The classification of assets considers both logical components (e.g., services, databases, APIs) and data objects (e.g., credentials, lifecycle records), aligned with the layered structure of the architecture.

Asset Categories

The assets were categorised into five main domains, as shown in the following table:

Asset Domain	Representative Assets	Security Properties at Risk
Digital Identity & SSI	- Legal Person Identifiers (LPIDs) - Credential Issuance Service (CO-008) - Credential Verification Engine (CO-018) - Root Credential Service (CO-022) - Identity Wallet (CO-011)	Authenticity, Integrity, Confidentiality
Data Storage & Catalogue	- Digital Twin Service (CO-005) - Data Catalogue Service (CO-006) - Verifiable Data Manager (CO-007)	Integrity, Availability
Network & Access	- API Gateway - Access Control Mechanisms - Interoperability Modules	Confidentiality, Availability, Integrity
Monitoring & Operations	- Logging and Monitoring System (CO-004) - Cloud Availability Manager (CO-013)	Integrity, Availability, Auditability
Data Exchange & Flow	- Data Plane (CO-002) - Schema Validation Engine (CO-017)	Availability, Integrity

Table 2: Asset Categorization

These assets were identified in close alignment with the architecture defined in Task 3.3 and represent the core enablers of traceability, compliance, and trust within the system. Each was further characterised in terms of its role, interfaces, dependencies, and threat exposure, as documented in the Threat Modelling Workbook (Annex 1).

Key Asset Attributes

Each asset is evaluated along three dimensions:

- **Criticality**: Impact of compromise on traceability, security, and compliance.
- **Sensitivity**: Degree to which the asset handles confidential, regulated, or integrity-sensitive information.

Funded by
the European Union

- **Exposure**: Likelihood of being targeted due to its network accessibility or centrality in workflows.

The table below illustrates examples of this classification for selected high-value assets:

Asset	Criticality	Sensitivity	Exposure	Rationale
Credential Issuance Service	High	High	Medium	Central to LPID creation. If compromised, attackers can forge identities and break trust model.
Digital Twin Service	High	Medium	Medium	Modifications can affect provenance and lifecycle visibility.
Cloud Availability Manager	Medium	Low	High	Ensures resilience; vital in DoS scenarios. High exposure due to continuous network interaction.
Logging & Monitoring System	High	Low	Medium	Key for detection and response. Failure to log or monitor reduces system visibility and auditability.
Verifiable Data Manager	High	High	Low	Responsible for embedding cryptographic proofs; low external exposure but high integrity impact.

Table 3: Key Asset Classification

Relationship with Threat Scenarios

The asset map enabled the structured assignment of threats and vulnerabilities in subsequent phases. For example:

- Threat TH-010 (Forged Enterprise Credentials) directly targets the Credential Issuance Service (CO-008) and Credential Verification Engine (CO-018).
- Threat TH-006 (Unauthorized Data Modification) affects the Digital Twin Service (CO-005) and Data Catalogue (CO-006).
- Threat TH-003 (DoS on Data Flow) endangers the Data Plane (CO-002) and Cloud Availability Manager (CO-013).

These mappings, detailed in the threat modelling Excel workbook, ensure that each mitigation strategy is explicitly traceable to the assets at risk.

2.3.2 Threat agents and attack surface

Following the identification of assets in the MaDiTraCe architecture, this section characterises the threat agents, the entities capable of initiating attacks, and delineates the attack surface, i.e., the vectors through which those agents can interact with or compromise the system [5].

Threat Agents: Profile and Capabilities

Threat agents in MaDiTraCe were categorised according to their origin, intent, and level of access. This classification helps estimate the likelihood and potential impact of attacks during risk analysis.

Threat Agent Type	**Description**	**Capabilities**	**Motivations**
External Attacker	Unaffiliated individuals/groups targeting public interfaces or open APIs.	Exploits in APIs, DoS, credential reuse	Disruption, sabotage, data theft
Malicious Insider	Legitimate users misusing privileged access (e.g., certifiers, operators).	Internal credential manipulation, data tampering	Financial gain, espionage, ideological reasons
Compromised Partner System	Third-party systems within the supply chain (e.g., issuer node compromised).	Forged credential issuance, injection via API	Exploitation of trust relationships
Automation/Botnets	Scripts or distributed bots targeting availability or brute-force entry.	High-volume API abuse, DoS, crawling sensitive data	Disruption, reconnaissance
Advanced Persistent Threats (APT)	Sophisticated actors using stealthy and persistent methods.	Multi-step compromise, evasion, targeted attacks	Long-term infiltration, IP theft, supply chain compromise

Table 4: Classification of Threat Agents in MaDiTraCe

This multi-layered profile helps align security measures with realistic threat scenarios, as different agents target different parts of the system (e.g., APTs on credential chains; botnets on APIs).

System Attack Surface

The attack surface encompasses the set of entry points where an adversary can interact with the system, whether to extract information, inject malicious data, or disrupt functionality. Based on the current architectural draft, the attack surface of MaDiTraCe can be grouped as follows:

Funded by
the European Union

Attack Surface Category	**Exposed Components**	**Relevant Threat Scenarios**
Credential Issuance and Validation APIs	CO-008, CO-018, CO-022 Identity Wallets and Verifiers	Forged credentials (TH-010), LPID injection (AT-028), trust chain bypass
Data Plane and Exchange Interfaces	CO-002, CO-005, CO-006	DoS attacks (TH-003), Data manipulation (TH-006), lifecycle falsification
Monitoring and Logging Interfaces	CO-004	Tampering with logs (insider), evasion of anomaly detection
Cloud and Availability Management APIs	CO-013	Denial-of-Service vectors, failover disruption
Schema and Input Validation Layers	CO-017	Data injection attacks (AT-008), malformed payloads
Inter-Organisational Integration Points	Off-chain API integrations (e.g., to Digital Twin providers or certifiers)	Compromised data sources, validation bypass from trusted third-parties

Table 5: Main Attack Surface Categories in MaDiTraCe

These entry points were identified through application decomposition and cross-referenced with the components listed in the Threat Modelling Workbook (Annex 9.1: Methodology_PASTA_Funditec.xlsm). Notably, the exposure is both vertical (user to database) and horizontal (between peer services), increasing the complexity of threat containment.

Key Observations

- SSI Components (CO-008, CO-018, CO-022) are highly privileged and particularly sensitive to compromise. Their exposure to both external and internal actors makes them critical attack vectors.
- The Data Plane (CO-002), due to its scale and throughput requirements, is highly vulnerable to resource exhaustion without appropriate throttling and redundancy mechanisms.
- Inter-organisational trust boundaries require special attention, as compromised partner nodes could operate under assumed legitimacy.

These findings guide the mitigation strategies proposed later in the deliverable (Section 2.5), particularly for reinforcing trust validation paths, securing APIs, and limiting propagation of injected or corrupted data.

Funded by
the European Union

2.3.3 Attack scenarios and abuse cases

Building on the identified threat agents and attack surface, this section presents the most relevant attack scenarios and abuse cases for the MaDiTraCe system. Each scenario represents a plausible chain of actions that an attacker might undertake to exploit vulnerabilities within the architecture, mapped directly to the components and threat agents previously analysed.

These scenarios were derived from the PASTA Stage 6 (Attack Modelling), where vulnerabilities were linked with feasible threat paths and consequences. They are documented in the Threat Modelling Workbook and summarised below.

Scenario ID	**Scenario Description**	**Involved Components**	**Abuse Case / Consequence**
AS-001	**Forged Credential Injection**: An attacker exploits weak issuance controls (VU-027) to inject a fake LPID into the system.	CO-008 (Credential Issuance Service), CO-022	Credential is treated as valid; attacker gains unauthorized access, simulates a legitimate entity, corrupts trust chain.
AS-002	**Unauthorized Data Modification**: An insider or external actor with escalated privileges modifies lifecycle data in the Digital Twin.	CO-005, CO-006, CO-007	Origin or certification data is altered, invalidating audit trails and leading to regulatory non-compliance.
AS-003	**DoS on Credential Verification**: A botnet floods the credential validation API, preventing legitimate participants from authenticating.	CO-018, CO-013	Service becomes unavailable, delaying transactions or halting traceability operations altogether.
AS-004	**Data Injection via Unvalidated Input**: A malformed or malicious payload is submitted to the Data Catalogue due to missing schema validation.	CO-006, CO-017	Corrupted data propagates through system; downstream analytics or reporting become inaccurate or unusable.
AS-005	**Credential Theft and Replay**: Attacker gains access to poorly protected credential storage and reuses tokens to impersonate a valid actor.	CO-011, CO-018	Session hijacking, unauthorized operations, and potential data exfiltration.

Funded by
the European Union

AS-006	**Trust Anchor Compromise**: The root authority (CO-022) is impersonated or compromised, allowing issuance of a cascade of fraudulent LPIDs.	CO-022, CO-008, CO-018	Entire trust model collapses, revocation and revalidation of large portions of the credential set may be needed.
AS-007	**Suppressed Monitoring**: An insider disables logging functions before performing unauthorized actions.	CO-004	Incident is not recorded; attack evades detection, complicating forensic analysis.
AS-008	**DoS on Data Plane**: Continuous data flow is interrupted by overloading the raw material transfer channel, exhausting system resources.	CO-002, CO-013	Service disruption affects material tracking in real time; trust in system performance degrades.

Table 6: Key Attack Scenarios and Associated Abuse Cases

Each scenario includes specific attacks (AT-xxx) and vulnerabilities (VU-xxx) as documented in the Report 1 annex 5.1 and 5.1.3 (Excel workbook Methodology_PASTA_Funditec.xlsm), all this can be found in annex 9.1 of this document . These are designed to be traceable and updatable in future threat assessments as the architecture evolves.

Implications for Risk Analysis

These abuse cases reinforce the need to:

- Harden the credential lifecycle, especially issuance and validation stages.
- Treat lifecycle data as highly sensitive and ensure robust validation pipelines.
- Prioritise availability and redundancy measures for high-traffic components (e.g., CO-002, CO-018).
- Maintain secure, immutable logs to support forensic traceability.

This catalogue of attack scenarios provides the operational basis for the risk prioritisation and STRIDE/DREAD mapping that follows in Section 2.4.

2.4 Risk analysis

2.4.1 Risk prioritisation and classification

The risk prioritisation process in Task 3.4 was designed to systematically evaluate and classify the threats identified through P.A.S.T.A. in terms of their likelihood, impact, and criticality. This assessment supports decision-making by focusing mitigation efforts on the most pressing vulnerabilities, particularly those affecting traceability integrity, credential trust, and operational continuity.

The prioritisation exercise used a qualitative scoring approach, integrating insights from the threat modelling workbook and expert judgement. Each threat was rated along two axes:

- **Impact**: The potential severity of a successful attack on system assets or business objectives.
- **Likelihood**: The estimated probability that the threat could be exploited, based on exposure, complexity, and attacker capabilities.

The resulting risk level is derived by combining both scores using a 3x3 matrix (Low / Medium / High). This provides a transparent and repeatable methodology to rank threats.

Threat ID	Threat Description	Impact	Likelihood	Risk Level	Justification
TH-010	Forged Enterprise Credentials	High	High	**High**	Compromise of credential trust enables impersonation and systemic data manipulation.
TH-006	Unauthorized Data Modification	High	Medium	**High**	Undermines traceability integrity, causing audit failures and legal non-compliance.
TH-003	DoS Attack Disrupting Data Flow	Medium	High	**High**	Affects system availability and causes critical delays in real-time material tracking.
TH-028	DoS on Credential Verification System	High	Medium	**High**	Prevents validation of entities, halting legitimate interactions and transactions.
TH-008	Data Injection Attacks	Medium	Medium	**Medium**	Leads to corrupted data in supply chain records; mitigated through schema validation if enforced.
TH-011	Unauthorized Access to Credential Storage	High	Low	**Medium**	Critical if exploited, but less likely with proper encryption and isolation.
TH-029	Issuance of Fraudulent Credentials	High	Low	**Medium**	Serious impact but mitigated through controlled credential

Funded by the European Union

					pipelines and trusted issuance flows.
TH-024	Unauthorized Access via Forged Credentials	High	Medium	**High**	Amplifies damage across services by leveraging invalid but accepted identities.

Table 7: Risk Prioritisation Matrix for Key Threats

These prioritised risks were directly linked to the attack scenarios listed in Section 2.3.3, ensuring consistency across the modelling process. All threats marked High are recommended for immediate mitigation (see Section 2.5).

Observations and Patterns

- Threats targeting the credential lifecycle (TH-010, TH-024, TH-029) consistently scored high, confirming that identity trust mechanisms are a critical security dependency in MaDiTraCe.
- Availability-related threats (TH-003, TH-028) are especially impactful due to the system's operational dependency on continuous data flows and credential validation.
- While data injection and storage access are serious concerns, their likelihood can be significantly reduced through technical safeguards already considered in the architecture (CO-017, CO-011).

This prioritisation feeds directly into the STRIDE and DREAD mapping (Section 2.4.2), helping align each threat with standardised threat categories and numerical scoring schemes.

2.4.2 STRIDE and DREAD mapping

To further systematise the threat modelling outcomes and enhance comparability with industry standards, each prioritised threat in MaDiTraCe has been mapped to the STRIDE [6], [7] model and evaluated using the DREAD [7] scoring system. This dual mapping allows for structured classification (via STRIDE) and semi-quantitative risk scoring (via DREAD), offering a more granular view of the risk landscape.

STRIDE Mapping

The STRIDE model categorises threats based on the type of security property they violate:

- **S**poofing identity
- **T**ampering with data
- **R**epudiation
- **I**nformation disclosure
- **D**enial of service
- **E**levation of privilege

Funded by the European Union

Threat ID	Threat Description	STRIDE Category	Violated Security Property
TH-010	Forged Enterprise Credentials	Spoofing, Elevation of Privilege	Authenticity, Access Control
TH-006	Unauthorized Data Modification	Tampering	Integrity
TH-003	DoS on Data Flow	Denial of Service	Availability
TH-028	DoS on Credential Verification	Denial of Service	Availability
TH-008	Data Injection	Tampering, Repudiation	Integrity, Auditability
TH-011	Credential Storage Access	Information Disclosure	Confidentiality
TH-024	Forged Credentials Bypassing Validation	Spoofing	Authenticity
TH-029	Fraudulent Credential Issuance	Spoofing, Tampering	Authenticity, Integrity

Table 8: Mapping of Threats to STRIDE Categories

DREAD Scoring

The DREAD model assigns scores to threats based on five criteria:

- **D**amage Potential (impact if exploited)
- **R**eproducibility (ease of repeating the attack)
- **E**xploitability (difficulty or ease of exploitation)
- **A**ffected Users (scope of impact)
- **D**iscoverability (likelihood of detection by attacker)

Each factor is scored on a scale from 1 (low) to 10 (high). The total average gives the DREAD risk score.

Threat ID	Threat Description	D	R	E	A	D	Avg Score	Risk Rating
TH-010	Forged Enterprise Credentials	9	8	7	9	6	**7.8**	High
TH-006	Unauthorized Data Modification	8	6	5	8	7	**6.8**	High
TH-003	DoS on Data Flow	7	8	8	7	5	**7.0**	High

Funded by
the European Union

TH-028	DoS on Credential Verification	8	7	7	7	5	**6.8**	High
TH-008	Data Injection	6	7	6	6	8	**6.6**	Medium
TH-011	Access to Credential Storage	9	5	4	7	3	**5.6**	Medium
TH-024	Forged Credentials Bypassing Validation	9	7	6	9	5	**7.2**	High
TH-029	Fraudulent Credential Issuance	9	5	4	8	4	**6.0**	Medium

Table 9: DREAD Risk Scores for High-Priority Threats

Insights and Utility

- STRIDE mapping reveals spoofing and tampering as the most prevalent threat categories, underscoring the need for robust identity verification and data validation mechanisms.
- DREAD scores reinforce prioritisation from Section 2.4.1, confirming that threats to credential integrity and system availability represent the highest risk concentrations.
- The combination of STRIDE and DREAD ensures that technical mitigations (Section 2.5) are properly aligned with the nature of the threat, not just its severity.

This mapping methodology can be re-applied iteratively as the MaDiTraCe architecture evolves, ensuring continuous alignment of threat modelling with system development.

2.5 Cybersecurity recommendations

Based on the risk prioritisation (Section 2.4), this section outlines the recommended mitigation strategies to address critical security concerns identified through the P.A.S.T.A. analysis. These recommendations span across three complementary layers:

- System-level architectural safeguards
- Technical control implementations
- Organisational and governance measures

Rather than treating these layers in isolation, this section integrates them per threat domain, to ensure coherence and avoid duplication.

2.5.1 Securing the credential lifecycle

The credential infrastructure is the backbone of the MaDiTraCe trust model. Threats such as credential forgery (TH-010), unauthorised access (TH-024), and fraudulent issuance (TH-029) demand reinforced controls across all layers.

Recommended measures:

- **Architectural:**
  - Isolate root credential issuance (CO-022) in a protected execution environment (e.g., HSM or secure enclave).
  - Define a dedicated trust chain validation pipeline in CO-018, including revocation and expiration checks.
- **Technical:**

- Use robust asymmetric cryptography (e.g., ECDSA over NIST P-256 or Ed25519) [8].
- Store credentials in encrypted form with MFA-enforced access via CO-011 (Identity Wallet) [9].
- Implement audit trails for all issuance and revocation actions (logged via CO-004).

- **Organisational:**
  - Define credential lifecycle policies (issuance, renewal, revocation).
  - Assign clear responsibility for trusted issuer governance and periodic review of root keys.

2.5.2 Preserving data integrity and authenticity

Traceability in MaDiTraCe relies on the verifiability of digital twin and catalogue data. Threats like data manipulation (TH-006), injection (TH-008), and silent corruption require structural and procedural countermeasures.

Recommended Measures:

- **Architectural:**
  - Embed the Verifiable Data Manager (CO-007) as a cryptographic integrity layer before data enters CO-005/CO-006.
  - Integrate the Schema Validation Engine (CO-017) in all input pipelines (API, partner integrations, internal services).
- **Technical:**
  - Enforce strict schema validation (JSON schema or similar) to detect malformed or malicious data inputs.
  - Embed hash-based proof-of-origin into every material record, using Merkle trees where appropriate.
- **Organisational:**
  - Limit write access via RBAC and segregate duties between data originators and validators.
  - Regularly test validation rules and schemas against new supply chain formats and edge cases.

2.5.3 Ensuring system availability and resilience

Denial-of-Service (DoS) threats such as TH-003 and TH-028 can disrupt traceability operations and credential validation. MaDiTraCe must be engineered with redundancy and self-protection mechanisms.

Recommended Measures:

- **Architectural:**
  - Deploy CO-013 (Cloud Availability Manager) with multi-zone redundancy and automated failover.
  - Isolate critical services (CO-002, CO-018) in dedicated resource pools to prevent cascading failure.
- **Technical:**
  - Apply per-endpoint and per-client rate limits at API Gateway level.
  - Use anomaly detection in CO-004 to identify traffic spikes, abuse patterns, or latency issues.
- **Organisational:**

Funded by
the European Union

  - Define incident response plans for service degradation events.
  - Establish SLAs and monitoring dashboards for availability metrics across partners.

2.5.4 Securing API exposure and partner integrations

Given the multi-stakeholder nature of MaDiTraCe, the system must assume that external interfaces and partners are potential threat vectors.

Recommended Measures:

- **Architectural:**
  - Introduce an API Gateway layer with consistent authentication, throttling, and logging across all exposed endpoints.
  - Enforce mutual Transport Layer Security (TLS) between services and with trusted partners.
- **Technical:**
  - Use OAuth 2.0 or similar for scoped access tokens between services.
  - Implement request signing and replay protection mechanisms (e.g., HMAC with nonce).
- **Organisational:**
  - Define an onboarding process for partner systems, including security reviews and credential provisioning.
  - Monitor third-party traffic for anomalies and revoke credentials on suspicious behaviour.

The following table summarises the key technical and architectural mitigation strategies applied across the main security domains identified in MaDiTraCe. Each domain is linked to the relevant system components and highlights the most effective safeguards implemented or recommended. This provides a concise overview of how security objectives are operationalised within the architecture.

Threat Domain	Key Components	Mitigation Highlights
Credential Management	CO-008, CO-011, CO-018, CO-022	Hardware Security Module (HSM)-backed issuance, revocation, encrypted storage, Multi-Factor Authentication (MFA), trust path validation
Data Integrity	CO-005, CO-006, CO-007, CO-017	Schema enforcement, cryptographic proofs, Role-Based Access Control (RBAC), audit logs
Availability (DoS resilience)	CO-002, CO-013, CO-018, CO-004	Rate limiting, auto-failover, anomaly alerts, traffic isolation
API Exposure	All exposed services via API Gateway	Open Authorization (OAuth) 2.0, Mutual Transport Layer Security (MTLS), signed requests, scoped access, partner onboarding controls

Table 10: Mitigations by Domain and Component

Funded by
the European Union

2.6 Security tools, techniques and future implications

The implementation of threat modelling in Task 3.4 has relied on a structured combination of manual analysis, semi-automated tracking, and standardised risk classification frameworks. These techniques have enabled a deep understanding of the MaDiTraCe architecture's attack surface and informed actionable mitigation strategies.

Summary of Tools and Techniques

- Manual Workshops were essential in the early stages to align threat modelling with business objectives and architectural decisions.
- A structured Excel Workbook was developed as a living tool to document components (CO-IDs), threats (TH-IDs), vulnerabilities (VU-IDs), and attack paths (AT-IDs). This supports traceability and alignment across future updates.
- STRIDE and DREAD frameworks were applied to classify and prioritise risks, balancing qualitative expert judgement with structured scoring.
- The documentation approach ensures that all identified threats are linked to specific system components and mitigation actions, enabling targeted improvements and auditability.
- Although automated tooling was not yet used due to the evolving nature of the architecture, its integration (e.g., IriusRisk, Threat Dragon) is recommended for future iterations once components stabilise.

Framework Complementarity: PASTA, STRIDE, and DREAD

To provide a comprehensive view of potential threats, the threat modelling approach integrates complementary frameworks, each addressing a different layer of analysis:

- PASTA (Process for Attack Simulation and Threat Analysis) focuses on the *why, how, and where* of potential attacks. It offers a risk-centric perspective aligned with business impact, helping identify likely threat scenarios from an attacker's viewpoint.
- STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) helps categorise the *types of attacks* that can occur against system components, based on known security properties.
- DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) is used to *prioritise threats* by evaluating their potential impact and likelihood, supporting the risk scoring and mitigation prioritisation process.

Together, these frameworks ensure that threats are not only identified but also well understood in terms of origin, nature, and impact, enabling effective and context-aware security planning.

Implications for Future Tasks

The outputs of Task 3.4 directly support and influence upcoming phases of the MaDiTraCe.

Funded by
the European Union

Furthermore, the threat modelling assets (particularly annex 5.13 in Report 1) should remain actively maintained throughout the project lifecycle. As MaDiTraCe transitions from draft to operational architecture, the threat model should be:

- Reviewed periodically (e.g., each major release or WP milestone).
- Updated upon architectural changes, new features, or integration of external systems.
- Reassessed after incidents or emerging vulnerabilities (e.g., new CVEs, supply chain threats).

By embedding security as an evolving process, rather than a one-off analysis, MaDiTraCe strengthens its commitment to secure, resilient, and compliant traceability systems. The outcomes and recommendations from this report will be taken into account when refining the final architecture to be delivered in D3.6, ensuring alignment between threat modelling insights and system design decisions.

3 Blockchain evaluation and selection *(based on report 2)*

3.1 Relation with the Blockchain selection report

The analysis presented in this chapter is based on the technical document *Report 2 – Blockchain Selection for MaDiTraCe*, developed by Funditec under Task 3.4. This report provides a comprehensive evaluation of blockchain technologies with the objective of supporting the design and deployment of a secure, scalable, and interoperable infrastructure for the Digital Product Passport (DPP).

While Task 3.4 included a broader threat modelling component, this section of the deliverable focuses specifically on the evaluation and selection of blockchain technologies capable of supporting traceability and trust across the critical raw materials (CRM) value chain. The decision-making process builds upon the requirements identified during Task 3.3 and incorporates criteria such as decentralisation level, governance models, privacy guarantees, regulatory compatibility (e.g. GDPR, eIDAS), and long-term maintainability.

The selection process was conducted using a structured multi-criteria evaluation methodology [10], as described in the report, including a comparative analysis of blockchain types (public, private, consortium), consensus mechanisms (e.g., PoW, PoA, PoS), and specific platforms such as EBSI [11], Hyperledger Besu, Ethereum, Polkadot, and Tezos. Particular attention was given to the alignment with the European Blockchain Services Infrastructure (EBSI), considering its relevance to the regulatory and technical ecosystem of MaDiTraCe.

The insights from this report directly inform the technical roadmap and implementation planning outlined in later sections of this deliverable (Section 3.7 and 3.8), and ensure that blockchain integration is not only technically sound but also strategically aligned with European initiatives and digital sovereignty principles.

Funded by the European Union

3.2 Relevance of blockchain in the DPP context

The integration of blockchain technology into the Digital Product Passport (DPP) framework is not a purely technical decision, but a strategic enabler of trust, auditability, and decentralised control across the lifecycle of critical raw materials. In the MaDiTraCe context, blockchain plays a foundational role in ensuring that the data attached to materials, such as origin, transformation, compliance certificates, and environmental footprint, can be shared and verified across actors without relying on a central authority [12].

This is particularly relevant in cross-border supply chains, where stakeholders (e.g., mining companies, manufacturers, auditors, regulators) operate under different jurisdictions and may not have pre-established trust relationships. By anchoring key DPP events (issuance, updates, verifications) to a distributed ledger, MaDiTraCe aims to create a shared, immutable audit trail that supports transparency, compliance, and resilience.

The Digital Product Passport (DPP) is a cornerstone of next-generation supply chain transparency and circular economy strategies. The concept is designed to:

Enhance traceability of products throughout their lifecycle.

Enable regulatory compliance by ensuring that stakeholders can verify sourcing, sustainability, and legal compliance.

Improve consumer and business trust by providing verifiable data on product origin and environmental impact.

Facilitate circular economy models by enabling recycling, reuse, and responsible disposal of materials.

For CRMs, a well-implemented DPP ensures that each batch of raw material, component, or finished product can be traced back to its source, mitigating risks of fraud, illegal mining, and unethical labor practices. However, implementing such a passport requires robust, tamper-proof, and scalable data infrastructure, which is where blockchain technology becomes relevant.

3.2.1 Key requirements of the Digital Product Passport

The Digital Product Passport (DPP) is envisioned as a shared, verifiable, and continuously updated data structure that tracks the identity, composition, origin, and lifecycle of a product, especially critical raw materials (CRM), as it moves through complex value chains [13]. In this context, blockchain is not merely an infrastructure choice, but a fundamental enabler of trust, traceability, and decentralised verification.

Traditional systems based on central databases are often siloed, prone to manipulation, and limited in their capacity to enforce cross-organisational integrity. In contrast, blockchain offers the following key properties that directly address the core challenges of DPP implementation:

Need in the DPP Context	Blockchain Contribution

Funded by
the European Union

Tamper-evident records: DPP data (e.g., origin, certifications) must be resistant to undetected changes	**Immutability**: Once anchored to the ledger, data cannot be altered without consensus or trace
Trust between disconnected actors: Stakeholders often lack direct trust relationships	**Decentralised trust model**: Eliminates reliance on a central authority or single point of failure
Regulatory compliance and auditability: DPPs must support transparency for regulators and auditors	**Transparent audit trails**: Native logging of all key actions, signatures and timestamps
Selective access and data privacy: Only relevant data should be visible to each actor	**Support for verifiable credentials and ZK-proofs**: Enables granular, privacy-preserving disclosures
Interoperability with EU infrastructure: Especially with initiatives like EBSI	**Alignment with EU-compliant protocols**: Including eIDAS, ESSIF, and DID standards
Future-proofing: The system must be adaptable and extensible as legislation evolves	**Smart contracts and modularity**: Programmable governance rules and scalable architecture

Table 1111: Blockchain Contributions to Key Requirements in the Digital Product Passport Context

Ultimately, blockchain offers the structural neutrality and resilience required for a system as ambitious as the DPP, where no single entity should unilaterally control product narratives, yet all must be able to verify them. For MaDiTraCe, this is especially relevant in complex global supply chains, where stakeholders must interact securely without depending on centralised intermediaries.

This alignment between technical affordances and regulatory goals justifies the central role of blockchain in the MaDiTraCe architecture.

Based on the architectural goals and regulatory landscape described in Task 3.3 and further detailed in Report 2, the blockchain layer in MaDiTraCe must satisfy the following key requirements:

Requirement	**Description**
Data integrity & immutability	Ensure that once DPP records (e.g., origin claims, certificates) are anchored, they cannot be altered.
Decentralised trust	Eliminate reliance on a single authority, enabling shared governance among diverse stakeholders.
Selective disclosure & privacy	Enable fine-grained control over which data is visible to whom, in line with GDPR and business needs.
Interoperability	Ensure compatibility with external systems and public initiatives such as EBSI.

Scalability & sustainability	Support a growing number of transactions and entities without incurring prohibitive costs or delays.
Auditability & compliance trace	Provide regulators with transparent access to provenance data for audits and due diligence.

Table 12 12: Key Requirements for a Blockchain-Based Digital Product Passport

These requirements shape both the design of the DPP infrastructure and the criteria used in the blockchain selection process.

3.2.2 Evaluation of traditional vs distributed models

The implementation of a Digital Product Passport (DPP) for critical raw materials requires a robust and verifiable infrastructure that supports data integrity, decentralised governance, and multi-stakeholder collaboration. In this context, two architectural paradigms were evaluated: traditional centralised systems and distributed ledger technologies (DLTs). This section provides a comparative evaluation of both approaches, highlighting their suitability in the context of traceability and compliance-driven environments.

Centralised Models

Traditional centralised architectures typically rely on a single authoritative entity that manages the data, infrastructure, and access control policies. While these systems may offer simplicity in deployment and integration, they suffer from several structural limitations when applied to complex, multi-actor supply chains such as those envisioned in MaDiTraCe:

- Single point of failure and control, increasing systemic risk and opportunities for data manipulation.
- Limited transparency and auditability, as data provenance often depends on internal records.
- Trust asymmetry, where actors must rely on the integrity of a central operator they may not know or control.
- Difficulties with interoperability, especially across jurisdictions or supply chain tiers.

Distributed Models (Blockchain)

In contrast, distributed ledger technologies provide a shared, tamper-evident infrastructure where records are replicated across multiple nodes and validated through consensus mechanisms. This aligns with the MaDiTraCe objective of ensuring that no single actor can unilaterally alter product data, while enabling verifiable traceability for regulators, certifiers, and end-users.

Key advantages of the distributed model include:

- Decentralised trust: No central authority controls the system; all participants validate and verify data collaboratively.

Funded by
the European Union

- Immutability and integrity: Once recorded, transactions are tamper-proof and auditable by design.
- Fine-grained access control: Coupled with SSI and verifiable credentials, blockchain enables selective disclosure and data minimisation.
- Regulatory alignment: Native support for audit trails, timestamping, and data origin is particularly relevant for GDPR, CSRD, and other EU regulations.

Evaluation Dimension	**Centralised Models**	**Distributed Models (Blockchain)**
Data Integrity	Vulnerable to internal tampering and unauthorised changes	Tamper-evident and cryptographically secured
Trust Model	Based on central authority	Based on consensus and decentralised validation
Auditability	Limited, internal-only logs	Transparent, verifiable, and public or semi-public audit trails
Resilience	Single point of failure risks	High availability through node redundancy
Cross-actor Collaboration	Difficult in multi-jurisdictional contexts	Designed for inter-organisational coordination
Scalability (governance)	Controlled by operator	Can be adapted through governance layers or consortium-led models
Compliance Readiness	Requires significant adaptation	Native support for data traceability and regulatory reporting

Table 1313: Comparative Assessment of Centralised vs Distributed Models

Analysis of the Comparison

Traditional databases are centralized and controlled by a single entity, making them vulnerable to data tampering and manipulation.

Blockchain provides tamper-resistant and decentralized storage, significantly reducing the risk of fraud and unauthorized modifications. However, it does not fully eliminate the possibility of fraud—particularly when data originates from off-chain sources, which may be compromised before being recorded on-chain.

Regulatory compliance can be automated using smart contracts, reducing administrative overhead.

Blockchain is more resilient, ensuring redundant storage and fault tolerance across a distributed network.

Given the requirements of the Digital Product Passport (DPP) outlined in Section 3.2.1 and the comparison between traditional databases and blockchain, it is clear that a blockchain-based solution is necessary. The need for multi-stakeholder transparency, immutable records, decentralized trust, and automated regulatory compliance makes blockchain the most suitable choice over centralized alternatives. However, not all blockchain architectures are equally suited for this use case. The next step is to determine which type of blockchain (public, private, hybrid, or consortium) best aligns with the technical and regulatory needs of MaDiTraCe.

In conclusion, while centralised systems may offer short-term implementation simplicity, they fall short in delivering the security, resilience, and transparency required by the DPP framework. Distributed models, particularly permissioned blockchains, represent a more future-proof and compliant foundation for building a traceability infrastructure capable of supporting regulatory and market expectations across the European Union.

3.3 Blockchain selection methodology

The selection of a suitable blockchain infrastructure for MaDiTraCe was conducted using a structured, multi-criteria methodology aimed at aligning the architectural, legal, and operational requirements of the Digital Product Passport (DPP) with the specific capabilities of available Distributed Ledger Technologies (DLTs). The methodology described in Report 2 ensures that the final decision is transparent, justifiable, and adaptable to the evolving regulatory and technological landscape of the European Union.

3.3.1 Framework overview and taxonomy

Selecting the right blockchain technology for the Digital Product Passport (DPP) in MaDiTraCe requires a structured decision-making approach that evaluates each potential option based on technical, regulatory, and business needs. To achieve this, we apply a blockchain taxonomy framework derived from the research paper "How to Choose a Blockchain Technology for an Innovation Project: Taxonomy and Use Cases " [10]

This framework organizes blockchain selection into a multi-stage decision process, ensuring that the chosen solution aligns with:

Regulatory compliance (EU laws, sustainability policies).

Technical efficiency (scalability, privacy, interoperability).

Operational feasibility (cost-effectiveness, ease of implementation).

The framework is inspired by literature and references to the existing work referenced in [10], in the paragraph above.

3.3.2 Step-by-Step decision process

The blockchain evaluation was conducted through the following step-by-step process:

Assessing the Need for Blockchain

- Do multiple stakeholders need to access shared records?
- Is data immutability essential?

Funded by
the European Union

- Is there a lack of trust among participants?
- Is auditability required for compliance?
- Would a centralized database be insufficient?

→ If "Yes" to most questions, blockchain is justified.

Determining the Type of Blockchain

- Should data be publicly accessible? (Choose Public)
- Should access be restricted to verified participants? (Choose Consortium / Hybrid)
- Should a single entity control access? (Choose Private)

→ The DPP requires a hybrid or consortium blockchain.

Choosing the Consensus Mechanism

- Prioritizing decentralization vs. efficiency
- Evaluating PoW, PoS, PoA, BFT (see Section 5)

Evaluating Blockchain Candidates

- Comparing leading technologies (EBSI, Hyperledger Fabric, Hyperledger Besu, Ethereum, Polkadot, Tezos)
- Assessing performance, security, costs, governance, and interoperability

Final Selection and Implementation Planning

- Deployment roadmap
- Integration with MaDiTraCe systems
- Smart contract development for regulatory compliance

This methodology ensured that the blockchain selection was not only technically sound but also strategically aligned with MaDiTraCe's goals of resilience, compliance, and European interoperability. Applying the decision-making framework to the MaDiTraCe DPP, we can outline the evaluation process:

Stage	**Decision Criteria**	**Outcome for MaDiTraCe**
Step 1: Is blockchain necessary?	Multi-stakeholder access, data immutability, compliance needs	Yes, blockchain is suitable
Step 2: Public vs. Private vs. Hybrid?	Need for transparency + privacy, regulatory oversight	Hybrid/Consortium blockchain
Step 3: Best consensus mechanism?	Balancing efficiency, security, decentralization	PoA or BFT
Step 4: Blockchain candidate comparison	Scalability, privacy, cost, governance	EBSI, Hyperledger Fabric, Hyperledger Besu
Step 5: Implementation Plan	PoC deployment, smart contract setup	PoC using EBSI

Table 14: Blockchain selection steps applied to MaDiTraCe

By following this systematic selection process, we ensure that the chosen blockchain technology is optimal for DPP requirements and fully aligned with the EU's sustainability and traceability policies.

Funded by the European Union

3.4 Comparative analysis of blockchain types

The choice of blockchain type, public, private, consortium, or hybrid [14], has major implications for the governance, trust model, scalability, and compliance of a digital traceability system such as MaDiTraCe. As part of the evaluation process, the characteristics of each type were compared against the specific functional and regulatory needs of the Digital Product Passport (DPP) infrastructure.

This section summarises the analysis conducted in Report 2, highlighting the trade-offs involved in selecting a blockchain governance model for a multi-stakeholder European project.

3.4.1 Comparison between Public, Private, Consortium and Hybrid blockchains

Each blockchain type presents distinct properties in terms of accessibility, control, performance, and transparency.

Property	**Public**	**Private**	**Consortium**	**Hybrid**
Access Control	Open to anyone	Fully restricted	Restricted to predefined members	Mixed: public for data access, private for validation
Consensus Participation	Permissionless	Single or few trusted validators	Multiple known parties share validation	Variable depending on component and function
Performance	Moderate to low (due to public validation)	High (centralised)	High to moderate	Balanced depending on design
Scalability	Challenging for high-throughput use cases	High	Moderate to high	High (if well-designed)
Governance	Community-driven, less controllable	Centralised	Joint governance among stakeholders	Context-dependent
Transparency	Full public visibility	Limited to internal participants	Visible among consortium members	Tunable; may combine both modes

Funded by the European Union

Security & Trust	Cryptographic + economic incentives	Depends on internal security practices	Relies on shared trust among members	Cryptographic + organisational trust
Suitability for DPP	Limited (GDPR, performance, access control)	Too centralised for trustless environments	Strong candidate: balances trust, compliance, and scalability	Promising for scenarios combining public verifiability and control

Table 1515: Comparative Overview of Blockchain Types

3.4.2 Governance, privacy and scalability trade-offs

The selection process revealed that public blockchains, while attractive for transparency and immutability, pose challenges related to privacy (e.g. GDPR compliance), performance bottlenecks, and lack of control over network governance. These issues are critical in regulated sectors involving sensitive supply chain data and personal information, such as in the CRM context.

Private blockchains, on the other hand, offer greater efficiency and control, but fail to deliver on decentralised trust, an essential feature for multi-party traceability infrastructures where no single actor should dominate decision-making or data integrity.

Consortium blockchains (e.g. Hyperledger Besu, Quorum) present a middle ground, enabling shared control among a predefined group of stakeholders. They support efficient validation, privacy-preserving mechanisms (e.g. permissioned data visibility), and can be designed to meet EU legal requirements, such as those related to GDPR and the CSRD. This makes them highly suitable for the DPP context.

Hybrid architectures also emerged as a flexible and promising option, especially where interoperability with public blockchains or the EBSI infrastructure is needed. For example, data hashes or credentials may be anchored in a public chain, while sensitive metadata is managed in a permissioned environment.

The evaluation concluded that a consortium or hybrid blockchain model offers the best alignment with MaDiTraCe's technical, legal, and operational needs, particularly in balancing trust distribution, performance, and regulatory compliance.

3.5 Consensus mechanisms

The choice of consensus mechanism is a core architectural decision that directly impacts the security, efficiency, and trust model of any blockchain-based system. In the context of MaDiTraCe, where traceability, regulatory alignment, and scalability are central, the evaluation of consensus protocols focused on identifying a mechanism that is energy-efficient, legally compatible, and operationally suitable for a European Digital Product Passport (DPP) infrastructure.

- Traditional consensus mechanisms like Proof of Work (PoW), while historically important, were quickly ruled out due to their high energy consumption, poor scalability, and misalignment with the EU's Green Deal objectives. Moreover, PoW does not offer the governance flexibility or identity verification controls required for permissioned traceability networks.
- Proof of Stake (PoS), particularly its modern variants (e.g. Nominated PoS, Delegated PoS), offers better energy profiles and performance. However, PoS remains heavily tied to economic incentives and token-based governance, which may be unsuitable or overly complex for consortia involving regulators, certification bodies, and non-commercial actors.
- In contrast, Proof of Authority (PoA) emerged as the most viable mechanism for MaDiTraCe. PoA is designed for permissioned networks, where validators are pre-approved entities rather than anonymous miners or stakers. Validators in PoA are typically known, legally bound organisations, such as consortium members or trusted institutions, making the model aligned with governance needs and auditable trust frameworks.

Consensus Mechanism	**How It Works**	**Decentralization**	**Scalability**	**Energy Efficiency**	**Security**	**Best Use Cases**
Proof of Work (PoW)	Miners solve cryptographic puzzles to validate transactions.	High	Low	Low (high energy consumption)	Very High	Cryptocurrencies (Bitcoin)
Proof of Stake (PoS)	Validators are chosen based on the number of tokens staked.	High	Medium	High	High	General blockchain applications
Proof of Authority (PoA)	Transactions are validated by pre-approved nodes (authorities).	Medium	High	Very High	High	Enterprise & regulated environments
Byzantine Fault Tolerance (BFT)	Nodes achieve consensus by reaching a majority agreement.	Medium	High	High	Very High	Permissioned networks (Hyperledger Fabric)

Table 1616: Comparison of Consensus Mechanisms for Blockchain Networks

For MaDiTraCe's consortium blockchain, the ideal consensus mechanism must meet the following criteria:

Energy efficiency: Avoid resource-intensive mechanisms like PoW.

Funded by the European Union

Scalability: Handle high transaction volumes efficiently.
Security: Ensure tamper-proof data integrity.
Regulatory compliance: Align with EU standards for traceability and governance.
Permissioned control: Allow selected trusted entities to validate transactions.
Based on these criteria, let's evaluate each mechanism:
Proof of Work (PoW): High energy consumption and low scalability make it inefficient for supply chain applications.
Proof of Stake (PoS): More efficient than PoW but primarily designed for public blockchains, making governance harder in a regulated supply chain ecosystem.
Proof of Authority (PoA): Efficient, scalable, and energy-friendly, making it a strong candidate for MaDiTraCe. Regulatory-aligned and used in government and enterprise settings (e.g., EBSI).
Byzantine Fault Tolerance (BFT): High security and efficiency, widely used in enterprise blockchains like Hyperledger Fabric or Besu. Works well for multi-stakeholder networks with controlled access.
Based on the evaluation, the two best options for MaDiTraCe are:
Proof of Authority (PoA) – Best for governance-aligned, energy-efficient networks like EBSI.
Byzantine Fault Tolerance (BFT) – Best for high-security, permissioned environments like Hyperledger Fabric.
For references in the paragraphs below please visit references in report 2.
Recommended Option: Proof of Authority (PoA) currently appears to be the most aligned consensus mechanism for MaDiTraCe, particularly given the potential integration with EBSI, which also adopts PoA. This mechanism offers advantages in terms of security, efficiency, and regulatory compliance. However, it is important to note that PoA has limitations, such as centralization concerns, and alternative consensus mechanisms may be considered depending on the final deployment context. A broader comparison is discussed in Deliverable D3.2.

3.6 Comparative assessment of candidate technologies

To identify the most suitable blockchain for the Digital Product Passport (DPP) in MaDiTraCe, six candidates were evaluated based on their technical and regulatory features: EBSI, Hyperledger Fabric, Hyperledger Besu, Ethereum, Polkadot, and Tezos. The criteria included scalability, privacy, governance, interoperability, transaction costs, and alignment with EU regulatory frameworks.

Blockchain	**Type**	**Consensus**	**Scalability**	**Privacy**	**Governance**	**Regulatory Compliance**	**Interoperability**	**Transaction Cost**	**Best Use Cases**
EBSI	Consortium	PoA	High	High	Medium – EU-led	High – EU-supported	High	Low	Government, supply chain, identity

Hyperledger Fabric	Consortium	BFT	High	High	Medium – Enterprise	High – Enterprise-grade	Medium	Low	Custom enterprise, traceability
Hyperledger Besu	Consortium	PoA / IBFT	High	High	High – configurable	Medium – Not EU-backed	High – Ethereum-compatible	Medium	Smart contracts with enterprise control
Ethereum	Public	PoS	Medium	Low	High – decentralized	Medium – No compliance focus	Medium	High	Decentralized apps, general use
Polkadot	Hybrid	NPoS	High	Medium	High – multichain	Medium – Not EU-focused	High	Medium	Cross-chain integrations
Tezos	Public	LPoS	Medium	Medium	High – self-amending	Medium – Low enterprise adoption	Medium	Medium	Niche smart contract deployments

Table 1717: Comparative Overview of Blockchain Candidates

The assessment revealed that EBSI, Hyperledger Fabric, and Hyperledger Besu were the top contenders. Each offers a different balance between regulatory alignment, privacy, scalability, and flexibility, which are all critical in the context of the MaDiTraCe ecosystem.

3.6.1 Strengths and weaknesses analysis of each technology

1. EBSI (European Blockchain Services Infrastructure)

Strengths:

- Developed by the European Union, making it highly compliant with regulations.
- Uses Proof of Authority (PoA), ensuring fast transactions and low costs.
- Supports traceability and identity verification, ideal for DPP and supply chains.

Weaknesses:

- Governance is EU-centric, which may limit flexibility.

Funded by
the European Union

- Not fully decentralized, as it relies on a consortium model.
- Best for: Government-regulated traceability systems, including DPP in MaDiTraCe.

2. Hyperledger Fabric

Strengths:

- Highly customizable with fine-grained access control.
- Can support Byzantine Fault Tolerance (BFT), providing strong security in a permissioned environment.
- No transaction fees (unlike Ethereum or Polkadot).

Weaknesses:

- More complex to deploy than EBSI.
- Not inherently interoperable with public blockchains.
- Best for: Enterprise applications with strict privacy and governance needs.

3. Ethereum

Strengths:

- Most widely adopted public blockchain with extensive developer support.
- Highly decentralized, ensuring strong security.
- Smart contract flexibility allows complex applications.

Weaknesses:

- High transaction fees make it costly for supply chain applications.
- Lower privacy, as all transactions are public by default.
- Not directly designed for enterprise traceability or regulatory frameworks.
- Best for: Decentralized applications, but not ideal for MaDiTraCe's compliance needs.

4. Hyperledger Besu

Strengths:

- Enterprise-grade Ethereum client, enabling interoperability with both public and private blockchains.
- Supports permissioned networks, allowing consortium governance while maintaining Ethereum compatibility.
- Uses Proof of Authority (PoA) or Istanbul Byzantine Fault Tolerance (IBFT), ensuring efficiency, security, and scalability.
- Smart contract compatibility with Ethereum, allowing seamless integration with Ethereum-based solutions.

Weaknesses:

- Higher complexity compared to private blockchains like Hyperledger Fabric, requiring Ethereum expertise for deployment.
- Transaction costs may arise if integrated with public Ethereum or other EVM-based networks.
- Not directly backed by EU regulatory bodies, unlike EBSI.
- Best for: Enterprise applications requiring Ethereum interoperability, smart contract flexibility, and permissioned governance models. A strong alternative if Ethereum compatibility is a key priority for MaDiTraCe.

Funded by the European Union

5. Polkadot

Strengths:
- Designed for interoperability, allowing integration with multiple chains.
- Scalability-friendly with parallel processing.

Weaknesses:
- Not specifically designed for regulatory compliance.
- Still maturing in terms of enterprise adoption.
- Best for: Cross-chain integrations, but not a strong candidate for MaDiTraCe.

6. Tezos

Strengths:
- Energy-efficient (LPoS), reducing operational costs.
- Self-amending governance, allowing upgrades without hard forks.

Weaknesses:
- Limited adoption in enterprise and regulatory projects.
- Not optimized for complex supply chain traceability.
- Best for: Niche applications, but not ideal for MaDiTraCe's DPP.

3.7 Final selection and justification

Based on the comparative analysis, EBSI (European Blockchain Services Infrastructure) is selected as the most suitable blockchain platform for MaDiTraCe's Digital Product Passport. This choice is supported by the following factors:
- Regulatory alignment: EBSI is developed under the European Commission, ensuring full compatibility with EU laws on traceability, digital identity, and sustainability.
- Efficient and low-cost: PoA consensus allows for fast transactions, low energy consumption, and minimal operational cost.
- Governance and privacy: A permissioned model enables multi-stakeholder governance with strong control over data visibility.
- Interoperability: EBSI is designed to work alongside other EU digital infrastructures and supports cross-border use cases.

Requirement	**EBSI**	**Hyperledger Fabric**	**Hyperledger Besu**
Regulatory Compliance	High – EU-backed	High – Enterprise-standard	Medium – Not EU-backed
Privacy & Data Control	High – Permissioned	High – Private network	High – Supports permissioned
Scalability	High – PoA Optimized	High – Enterprise-grade	High – IBFT consensus
Governance & Interoperability	Medium – EU-governed	Medium – Consortium-led	High – Ethereum compatibility

Funded by the European Union

Cost-Efficiency	Low – No gas fees	Low – No gas fees	Medium – EVM may introduce costs
Overall Suitability	**Good choice**	Good Alternative	Good Alternative

Table 1818: Blockchain Suitability Matrix

Alternatives such as Hyperledger Fabric and Besu remain valid if future technical or governance needs evolve:

- Hyperledger Fabric: Recommended for use cases requiring full internal control and complex governance structures.
- Hyperledger Besu: Suitable if Ethereum smart contract interoperability becomes a strategic priority.

3.8 Conclusions and implementation planning

This report has presented a structured, criteria-driven analysis for selecting a blockchain architecture suitable for implementing the Digital Product Passport (DPP) within the MaDiTraCe project. The evaluation was grounded in a taxonomy-based methodology, taking into account the functional requirements of the DPP, including data immutability, decentralized trust, regulatory alignment, and multi-stakeholder access.

Following the analysis of blockchain types, consensus mechanisms, and technology stacks, the assessment identified three blockchain frameworks as particularly relevant: EBSI, Hyperledger Fabric, and Hyperledger Besu. This selection is consistent with observations in Deliverable D3.2, where multiple blockchain configurations were recognized as viable for DPP use cases.

Each of the shortlisted options presents specific advantages:

EBSI (European Blockchain Services Infrastructure) demonstrates high alignment with EU regulatory frameworks and benefits from institutional governance and PoA-based efficiency. It is optimized for traceability, digital identity, and compliance with sustainability directives. Although based on Hyperledger Besu and technically compatible with EVM smart contracts, EBSI currently does not expose a general-purpose smart contract layer for unrestricted development.

Hyperledger Fabric offers high configurability, granular access control, and enterprise-grade privacy, making it well-suited for scenarios requiring strict governance and confidentiality within a consortium structure.

Hyperledger Besu combines Ethereum Virtual Machine (EVM) compatibility with support for permissioned networks via PoA or IBFT consensus, thus enabling advanced smart contract capabilities alongside enterprise interoperability.

Although EBSI emerges as the most suitable candidate from a regulatory and strategic standpoint within the EU context, it is important to note that the MaDiTraCe ecosystem may involve international stakeholders. In this sense, interoperability, cross-jurisdictional governance, and technical flexibility must also be considered during subsequent stages of development and deployment.

Therefore, it is recommended to initiate the implementation phase with a Proof of Concept (PoC) based on EBSI, while maintaining a modular system architecture that can accommodate alternative or complementary blockchain infrastructures (such as Hyperledger Fabric or Besu) should broader interoperability or governance requirements arise.

4 Notarization tool audit and Smart Contract security *(based on report 3)*

4.1 Relation with report 3 (Notarization Tool and Smart Contract Analysis)

This section integrates the insights derived from the detailed security assessment of the MaDiTraCe notarization tool and its associated smart contract (Store.sol), as presented in Report 3. The notarization tool leverages blockchain immutability and Merkle tree hashing techniques to provide a secure and efficient method for verifying document integrity without exposing the underlying files.

The analysis combines a threat modeling approach based on the P.A.S.T.A. methodology, a static smart contract audit [15] using Slither, and a comprehensive review of access control models and privacy mechanisms. These elements collectively identify key vulnerabilities and areas for improvement regarding data confidentiality, authentication, and contract robustness.

By grounding the security evaluation in established methodologies and automated tooling, this analysis ensures that the notarization system adheres to industry best practices while aligning with MaDiTraCe's goals of trustworthiness, compliance, and operational security.

The findings and recommendations from this chapter form a foundational input for future development iterations, particularly focusing on:

- Strengthening role-based access control (RBAC) and authentication mechanisms to restrict notarization and verification capabilities appropriately [16].
- Enhancing privacy through encryption of stored hashes and exploring zero-knowledge proof (ZKP) integration.
- Addressing smart contract weaknesses such as outdated Solidity versions, missing license identifiers, and access vulnerabilities.

This alignment between architectural design, code security, and privacy-by-design principles ensures that the notarization tool can effectively serve as a tamper-proof anchor within MaDiTraCe's digital traceability framework.

Funded by
the European Union

4.2 Notarization tool analysis

4.2.1 Architecture and notarization process

The notarization tool provides a secure and immutable method to verify the integrity of documents by computing their hashes and recording the Merkle root on the blockchain. This approach ensures tamper-proof notarization without exposing the original files.

Notarization Workflow:

1. File Selection: The user selects one or multiple files for notarization.
2. Hash Computation: The tool computes a cryptographic hash (e.g., SHA-256) for each file.
3. Merkle Tree Generation:
   - The computed hashes are structured into a Merkle tree.
   - A Merkle root is derived, representing the unique fingerprint of the entire dataset.
4. Storage:
   - The file hashes and Merkle root are stored on a centralized server.
   - The Merkle root is also recorded on the blockchain for immutability.
5. Notarization Confirmation: The user receives a proof of notarization, which allows verification at a later stage.

Key Security Considerations:

Security Aspect	**Description**
Privacy	Files remain on the user's device; only hashes are transmitted and stored, minimizing data exposure.
Immutability	Blockchain anchoring of the Merkle root ensures permanent, tamper-proof notarization evidence.
Efficiency	Merkle tree enables efficient verification without requiring all files, reducing computational and storage overhead.

Table 1919: Security Considerations in the Blockchain-Based Notarization Proces

4.2.2 Document verification on blockchain and server

The verification process ensures that previously notarized files remain unaltered. The tool supports two verification methods:

1. Partial File Verification (Server-Based)
   - Used when the user does not have all notarized files.
   - Steps:
     1. The user provides available files and selects the notarization index.
     2. The tool recomputes the hashes and checks them against the stored hashes on the server.
     3. If valid, the Merkle root is verified against the blockchain record.
2. Full File Verification (Blockchain-Based)
   - Used when the user has all notarized files.

- Steps:
    1. The tool recomputes all hashes and reconstructs the Merkle tree.
    2. The computed Merkle root is compared to the one stored on the blockchain.

3. Account-Based Verification: users can also retrieve their notarization history using:

- Server-Based Verification: Querying the server for notarized records associated with the user.
- Blockchain-Based Verification: Querying the blockchain for Merkle roots linked to the user's account.

4.2.3 Privacy and access considerations

Despite strong integrity guarantees, the system can benefit from further privacy and access control enhancements to mitigate potential metadata leakage and unauthorized access.

Identified Issues:

- Lack of Role-Based Access Control (RBAC): Currently, anyone can query the blockchain and verify a notarization. There is no restriction on who can access stored Merkle roots.
- No User Authentication in Verification:
    - The system allows anyone to verify a notarization if they have access to the blockchain.
    - The system lacks an authentication mechanism that allows the owner of a notarization to control who is authorized to verify it.
    - Although the original files are not stored, the absence of access controls may lead to indirect exposure risks. Hashes and Merkle roots recorded on the blockchain can still be correlated with external data sources, enabling potential metadata analysis or pattern inference.

Suggested Enhancements:

- Role-Based Access Control (RBAC):
    - Introduce notary, user, and administrator roles to restrict who can notarize and verify documents.
    - Only authorized users should be able to query specific notarized data.
- Authentication Layer for Verification: Require user authentication (e.g., wallet signature, API key) to prove ownership of a notarized file.
- Encrypted Hash Storage: Hashes should be encrypted before being stored on-chain, preventing unauthorized correlation attempts.

Enhancement	Description
RBAC Implementation	Define clear roles with specific permissions on notarization actions and data queries.
Authentication Layer	Enforce user authentication during verification to prove document ownership.

Funded by
the European Union

Encrypted Hash Storage	Encrypt notarized hashes before on-chain storage to protect privacy.

Table 2020: Proposed Enhancements for Secure and Private Notarization

4.3 Access control implementation

4.3.1 Definition of roles

The current notarization system does not enforce access control mechanisms, allowing unrestricted verification of notarized documents. To enhance security and privacy, a Role-Based Access Control (RBAC) model should be introduced, although is not critical because the verification of a notarization should mainly be public and those authorized who have the document and the index of the notarization may proceed to verify. However, three key roles are defined:

1. **Administrator (ADMIN_ROLE)**
   - Manages access control by assigning notary roles to authorized users.
   - Decides who have access to the system
   - Can audit notarized records but does not modify notarized data.
   - Oversees security policies, including authentication and permission management.
2. **Notary/ Owner of notarization**
   - Authorized notarize documents by submitting Merkle roots to the blockchain.
   - Owns the notarization hence decides who has access to verify his own notarization.
   - Can retrieve a list of notarized documents associated with their account.
   - Cannot access notarized records of other users unless explicitly permitted.
3. **Verifier**
   - Role authorized by the notary.
   - Can submit files for notarization through the system but does not directly interact with the blockchain.
   - Allowed to verify their own notarized documents.
   - Cannot access notarizations that do not belong to them. **to the owner who warrantees the access**

The RBAC model ensures decentralized access management so that notarization and verification actions are limited to authorized entities, reducing the risk of exposing unnecessary data, securing interactions within the supply chain.

4.3.2Authentication methods and permissions

To enhance access control, authentication mechanisms can be incorporated to verify users before allowing notarization or verification operations. The following authentication methods are recommended:

1. **Blockchain wallet authentication**
   - Users must sign a transaction with their Ethereum-compatible wallet (e.g., MetaMask) to verify their identity.
   - The smart contract checks if the sender has the correct role before allowing notarization or verification.

Funded by the European Union

   - This prevents unauthorized users from accessing notarized records.
2. **Off-Chain authentication with API Keys**
   - Users receive a unique API key upon registration, which must be included in notarization requests.
   - The API key is validated against a database before allowing access to stored hashes and Merkle roots.
   - This method is useful for server-based verification where blockchain interaction is not required.
3. **Multi-Factor authentication (MFA) for administrative actions**
   - Administrators should be required to use multi-factor authentication (MFA) when assigning roles or modifying permissions.
   - This adds an additional layer of security against unauthorized role modifications.

Authentication Method	**Description**	**Use Case**
Blockchain Wallet Authentication	Users must sign transactions with an Ethereum-compatible wallet (e.g., MetaMask).The smart contract checks if the sender has the correct role before permitting actions.This prevents unauthorized access to notarized records.	Authentication for blockchain-based notarization and verification.
Off-Chain Authentication with API Keys	Users receive a unique API key upon registration.API keys are validated against a database before allowing access.This method is useful for server-based verification where blockchain interaction is not required.	Server-based verification and access control.
Multi-Factor Authentication (MFA) for Administrative Actions	Administrators must use MFA when assigning roles or modifying permissions.This adds an extra security layer against unauthorized role changes.	Protection of sensitive administrative functions.

Table 2121: Authentication Methods for Access Control in Notarization Systems

4.3.3 Restricting access to individual notarizations

The current system lacks privacy controls, allowing anyone to verify notarized data if they have access to the blockchain. This exposes users to potential data correlation attacks, where adversaries can track notarization patterns.

Proposed Access Restriction Mechanisms:

1. **User-Specific Encryption of Notarized Data**

Funded by
the European Union

   - Instead of storing plaintext hashes on the blockchain, each user encrypts the hash before notarization.
   - The decryption key is only accessible to the owner, preventing unauthorized verification.
2. **Permissioned Smart Contract Queries**
   - Introduce a whitelisting mechanism in which only the original notary and the verifier explicitly authorized by the notary can query specific notarized records.
   - This ensures that notarization details cannot be accessed by unauthorized third parties, preserving privacy and alignment with predefined roles.
3. **Zero-Knowledge Proofs for Private Verification**
   - Implement zero-knowledge proofs (ZKP) to allow users to verify document authenticity without exposing the underlying Merkle root.
   - This ensures privacy while maintaining the integrity of the notarization process.

4.4 Smart Contract analysis

4.4.1 Security audit results with Slither

Steps to run Slither

To analyze the security of the Store.sol smart contract, Slither was used. Slither is a static analysis tool for Solidity that detects vulnerabilities, optimizes gas usage, and ensures best practices in smart contract development.

The following steps were performed:

1. Compile the smart contract to ensure it is free of syntax errors: npx hardhat compile

Output:

```
Warning: SPDX license identifier not provided in source file.
Compiled 1 Solidity file successfully (evm target: paris).
```

This warning indicates that the contract does not include an SPDX license identifier, which is a best practice for open-source compliance.

2. Run Slither on the contract to detect security vulnerabilities: slither contracts/Store.sol

Slither Output and Explanation

The following issues were identified:

1. Missing SPDX License Identifier

- **Issue:** The contract lacks an SPDX license identifier, which is recommended for compliance and clarity.
- **Solution:** Add the following line at the beginning of the contract:

```
// SPDX-License-Identifier: MIT
```

2. Solidity Version Contains Known Bugs

- **Issue:** The contract specifies pragma solidity ^0.8.0;, which includes several known **vulnerabilities** in earlier Solidity versions.

- **Solution:** Upgrade to a more recent Solidity version, such as:

```
pragma solidity ^0.8.19;
```

3. **Non-Standard Naming Conventions**

- **Issue:** Function parameters _root and _info do not follow Solidity's mixedCase naming convention.
- **Solution:** Update parameter names to root and info:

```
function addRoot(bytes32 root, string memory info) public { ... }
```

4.4.2 Identified vulnerabilities and improvements

Based on the analysis, the following vulnerabilities were detected, along with proposed improvements:

1. Lack of Access Control

- **Issue:** Any user can add and retrieve Merkle roots, leading to potential misuse.
- **Solution:** Implement Role-Based Access Control (RBAC) using OpenZeppelin's AccessControl. Only users with the Notary role should be allowed to notarize documents.

2. Public Data Exposure

- **Issue:** The contract allows anyone to read all notarized records. This could lead to metadata exposure and data correlation risks.
- **Solution:** Implement query restrictions, allowing only document owners or authorized users to retrieve their notarized data.

3. No Verification of Data Authenticity

- **Issue:** The contract does not verify if a user querying notarized data is the actual owner.
- **Solution:** Require users to authenticate their identity via wallet signatures before retrieving records.

4. Potential Denial-of-Service (DoS) Attacks

- Issue: There is no limit on how many notarized records a user can add, which could lead to blockchain storage abuse.
- Solution: Introduce gas fees or rate limits for notarization requests to prevent spam.

4.4.3 Access control implementation with roles

To mitigate the issues identified, a role-based access control system should be implemented. The following updates are proposed:

Funded by
the European Union

1. *Define Notary and Admin Roles*

Using OpenZeppelin's AccessControl, define two key roles:

```
bytes32 public constant NOTARY_ROLE = keccak256("NOTARY_ROLE");
bytes32 public constant ADMIN_ROLE = keccak256("ADMIN_ROLE");
```

- Admins can assign or revoke the Notary role.
- Notaries can notarize documents but cannot modify existing records.

2. *Restrict Access to Notarization Function*

Modify the addRoot function to enforce access control:

```
function addRoot(bytes32 root, string memory info) public onlyRole(NOTARY_ROLE) {
 indexToRootInfo[rootCount] = MerkleRootInfo({
 rootHash: root,
 additionalInfo: info,
 timestamp: block.timestamp,
 notarizer: msg.sender
 });
 userRoots[msg.sender].push(rootCount);
 emit RootAdded(rootCount, root, info, block.timestamp, msg.sender);
 rootCount++;
}
```

- This ensures only authorized notaries can add notarized records.

3. *Restrict Access to Notarization Data*

To preserve privacy and prevent unauthorized data exposure, retrieval functions must enforce ownership-based access control. The following implementation ensures that only the notary who submitted the record or an administrator can retrieve the corresponding notarized data:

```
function getRootByIndex(uint256 index) public view returns (bytes32, string memory,
uint256, address) {
 require(index < rootCount, "Index out of bounds.");
 MerkleRootInfo storage info = indexToRootInfo[index];
 require(info.notarizer == msg.sender || hasRole(ADMIN_ROLE, msg.sender), "Access denied.");

 return (info.rootHash, info.additionalInfo, info.timestamp, info.notarizer);

}
```

- This implementation restricts data access to the notary who submitted the record and system administrators. It avoids exposing notarized data to unauthorized users, thus reducing risks of metadata inference or misuse.

Note: The current version of the smart contract does not implement a verifier role or third-party access delegation. However, supporting controlled access for authorized verifiers (e.g., selected by the notary) could be a useful addition in future versions to accommodate broader use cases such as delegated validation.

4.5 Security recommendations

4.5.1 Enhancing privacy and data storage

While the notarization system ensures transparency and integrity, additional measures can further minimize data exposure risks without compromising verifiability:

1. **Encrypting Hashes Before Storage**
   - Apply lightweight encryption to hashes before recording them on the blockchain.
   - The decryption key should be accessible only to the document owner.
2. **Optimized On-Chain Storage**
   - Store only the **Merkle root** on-chain while keeping individual file hashes in a secure database.
   - This prevents potential inference of document details from blockchain data.
3. **Privacy-Preserving Verification**
   - Explore **Zero-Knowledge Proofs (ZKPs)** to enable validation without revealing sensitive information.

4.5.2 Hash encryption implementation

To prevent unauthorized access and enhance the protection of notarized data, the following measures are recommended:

1. **Hash Authentication with HMAC**
   - Use a **Hash-Based Message Authentication Code (HMAC)** with a secret key to strengthen data integrity.
   - Only users with the key can validate notarized records.
2. **Secure Off-Chain Storage**
   - Store individual hashes in an encrypted database using **AES-256**, with access managed through a Hardware Security Module (HSM) or Key Management Service (KMS).
3. **Asymmetric Encryption for Controlled Access**
   - Allow users to optionally encrypt their hashes with their public key, ensuring that only they can decrypt them.

4.5.3 Attack prevention and risk mitigation

To enhance security without compromising usability, the following measures are recommended:

1. Role-Based Access Control (RBAC)
   - Implement roles such as Notary, User, and Administrator to restrict functionalities within the contract.
   - Use OpenZeppelin's AccessControl to enforce permissions on notarization and verification functions.
2. Abuse and Load Protection
   - Limit the number of notarization requests to prevent excessive use.
   - Apply gas limits to mitigate potential spam transactions.
3. Wallet-Based Authentication
   - Require users to sign a transaction with their wallet before verifying notarized records.
   - This ensures that only legitimate owners can access their notarization details.
4. Secure Upgradeability
   - Implement a proxy upgrade pattern to allow future security updates without redeploying the contract.

4.6 Implementation roadmap and future enhancements

The security evaluation of the notarization tool and its smart contract (Store.sol) revealed key areas for improvement related to access control, data privacy, and attack mitigation. To ensure a robust and secure system, a phased implementation roadmap is proposed, prioritizing essential fixes while planning for future scalability and privacy enhancements.

Key Immediate Actions

- **Security and Code Quality:** Add SPDX license identifier, upgrade Solidity to ^0.8.19, and align naming conventions with best practices.

- **Access Control:** Implement Role-Based Access Control (RBAC) with Notary, User, and Administrator roles; enforce wallet-based authentication for critical operations.

- **Data Protection:** Encrypt hashes before on-chain storage and store individual hashes securely off-chain.

- **Attack Mitigation:** Introduce gas limits and rate limiting to prevent DoS and abuse attacks.

Planned Enhancements

- **Privacy Enhancements:** Explore zero-knowledge proofs (ZKPs) and user-controlled encryption for notarized data to strengthen confidentiality.

- **Scalability and Maintainability:** Develop proxy-based upgradeability mechanisms for the smart contract to allow seamless future updates.

- **Security Validation:** Schedule third-party audits and penetration tests; implement version control for contract updates.

This roadmap balances urgent security needs with long-term improvements to privacy, scalability, and usability. By following this structured approach, the notarization system will progressively achieve enhanced protection, compliance, and operational resilience without sacrificing efficiency or user experience.

5 Integrated guidelines for security and privacy

This section consolidates comprehensive guidelines and best practices to ensure robust security and privacy within the MaDiTraCe traceability system. It addresses secure design principles, GDPR compliance, identity management including SSI, and operational risk management aligned with state-of-the-art standards and regulatory requirements.

5.1 Secure design principles

Security by design is imperative to mitigate vulnerabilities at early stages, ensuring confidentiality, integrity, and availability of data and services.

Security Area	Implemented Controls	Purpose/Benefit
Authentication & Authorisation	Wallet-based signatures, RBAC, MFA, Delegated access	Enforce identity verification and granular permission control
Encryption & Hashing	AES-256, SHA-256/SHA-3, HMAC, Key lifecycle management	Protect confidentiality and integrity of data
Secure Data Flows & Storage	TLS 1.3, Network segmentation, Immutable logs, Encrypted off-chain storage	Prevent data leakage, tampering, and enable auditability

Table 2222: Overview of Secure Design Principles and Controls

5.1.1 Authentication and authorisation

Ensuring that only legitimate and authorized entities access MaDiTraCe services is a fundamental security requirement. Authentication and authorization mechanisms not only verify user identities but also strictly enforce access rights based on role definitions and operational context.

To achieve this, MaDiTraCe should implement:

- Decentralized Identity Verification via Wallet Signatures: Users authenticate transactions through digital signatures generated by their Ethereum-compatible wallets (e.g., MetaMask). This process ensures cryptographic proof of identity without exposing private keys, enhancing security and non-repudiation.
- Role-Based Access Control (RBAC): Access rights are assigned based on predefined roles such as Notary, User, and Administrator, enforcing the principle of least

Funded by
the European Union

privilege. This granular control restricts critical functions (e.g., notarization, data retrieval) to authorized parties only, minimizing the attack surface.

- Multi-Factor Authentication (MFA) for Administrative Functions: Elevated privileges, particularly administrative role assignments and security policy changes, require MFA to protect against credential theft or insider threats.
- Delegated Access Frameworks: The system supports delegation of limited access rights to trusted third parties via secure consent mechanisms. This facilitates regulatory audits and compliance checks without compromising user sovereignty.

5.1.2 Encryption and hashing

Data confidentiality and integrity are preserved through rigorous encryption and hashing techniques, which form the backbone of secure notarization and traceability.

The following controls should be employed:

- Transport and Storage Encryption: All data in transit are protected by TLS 1.3, ensuring confidentiality and integrity. At rest, sensitive information is encrypted using AES-256, both on off-chain databases and any on-chain encrypted payloads.
- Secure Cryptographic Hashing: Data objects are hashed using SHA-256 or SHA-3 to generate unique fingerprints, enabling tamper detection and Merkle tree constructions for scalable integrity proofs.
- Hash-Based Message Authentication Codes (HMAC): HMACs, utilizing secret keys, add an additional layer of authenticity and protection against replay and tampering attacks.
- Robust Key Management Practices: Cryptographic keys undergo lifecycle management encompassing secure generation, storage within HSMs or KMS, rotation, and revocation, accompanied by strict access controls and audit logging.

5.1.3 Secure data flows and storage

The design of data flows and storage infrastructure is critical to prevent unauthorized data access, modification, or leakage throughout the system lifecycle.

MaDiTraCe should integrate the following best practices:

- End-to-End Encryption: Data transmission between system components employs encrypted channels, ensuring confidentiality and resistance to interception or man-in-the-middle attacks.
- Network Segmentation and Defense-in-Depth: Infrastructure is segmented into security zones with tailored access controls and firewall rules, limiting lateral movement and containing potential breaches.
- Immutable, Tamper-Evident Audit Logging: System activities, including notarization events and access control changes, are logged immutably, supporting forensic investigations and compliance audits.

Funded by the European Union

- Off-Chain Storage with Controlled Access: Detailed notarized data and metadata are stored off-chain in encrypted databases with strict access controls, reducing blockchain bloat and preserving user privacy.
- Data Minimisation: Only minimal data, such as cryptographic proofs (Merkle roots), are stored on-chain, mitigating privacy risks and supporting GDPR compliance.

5.2 Confidentiality and GDPR compliance

In line with European regulations [17], [18] and best practices, systems managing sensitive data in supply chain traceability, such as the Digital Product Passport (DPP), should ensure strict confidentiality and compliance with the General Data Protection Regulation (GDPR). This section provides guidelines and recommendations to support the design, audit, and verification of such compliance within MaDiTraCe and similar architectures.

GDPR Principle	**Recommended Control**	**Purpose and Effectiveness**
Data Minimisation	Store only minimal proofs on-chain; pseudonymise data off-chain	Reduce privacy risks and data exposure
Consent Management	Explicit, granular, revocable user consents	Empower user control and meet regulatory demands
Pseudonymisation	Use DIDs and separate identity mappings	Protect personal identity while preserving functionality
Right to Erasure	Allow off-chain data deletion/anonymisation	Comply with user requests despite blockchain immutability
Transparency and Audit	Immutable logs of consents and accesses	Facilitate accountability and compliance demonstration

Table 2323: Recommended GDPR Compliance Controls

5.2.1 Data minimisation and consent models

One of the core GDPR principles is data minimisation, which requires collecting and processing only the data strictly necessary for defined purposes. To align with this principle, systems should:

- Limit on-chain data storage to essential proofs such as cryptographic hashes and Merkle roots, avoiding the storage of raw personal or sensitive data on public ledgers.
- Ensure pseudonymisation or anonymisation techniques are applied wherever possible to reduce identifiability of data subjects.
- Clearly define and document the specific purposes for which each data element is collected and processed, preventing unauthorized secondary use.

Funded by
the European Union

Regarding consent management, systems should:

- Implement mechanisms to obtain explicit, informed, and revocable consent from data subjects for processing their personal data, particularly for identity-related information.
- Provide fine-grained consent controls, enabling users to authorize or revoke consent for specific data categories or processing activities.
- Maintain audit logs of consent transactions to demonstrate compliance and accountability.
- Evaluate and document alternative lawful bases for processing (e.g., legitimate interest, contractual necessity) where consent is not the primary legal basis.

5.2.2 Pseudonymisation and user control

To enhance confidentiality and privacy, pseudonymisation techniques should be adopted. These may include:

- Using Decentralized Identifiers (DIDs) or similar pseudonymous identifiers to represent individuals or entities on-chain, thereby masking direct personal identifiers.
- Separating identity data storage, ensuring that mappings between pseudonyms and real identities are stored off-chain in secure, access-controlled environments.

For compliance with user rights under GDPR, systems should provide:

- Support for the right of access, allowing users to retrieve all data associated with their identity or pseudonym in a machine-readable format.
- Procedures enabling the right to erasure (or data anonymisation) of personal data stored off-chain, acknowledging blockchain immutability constraints.
- Mechanisms for withdrawal of consent, triggering cessation or limitation of processing activities as per user request.
- Transparent and immutable logging of data access and processing activities to demonstrate adherence to GDPR transparency and accountability requirements.

5.3 Identity management and SSI considerations

Decentralized Identity (DID) frameworks and Self-Sovereign Identity (SSI) paradigms are increasingly pivotal in enhancing privacy, security, and user autonomy within digital ecosystems. For projects como MaDiTraCe que involucran trazabilidad y notarización, it is strongly recommended to carefully assess and integrate SSI solutions to strengthen identity management while aligning with regulatory frameworks.

Funded by
the European Union

Aspect	Recommendation	Potential Impact
Applicability	Evaluate integration complexity and standard maturity	Ensure interoperability and operational feasibility
Usability	Design intuitive user identity workflows	Facilitate adoption and reduce user errors
Regulatory Compliance	Implement governance and consent aligned with GDPR	Maintain legal compliance and user trust
Privacy Enhancements	Employ ZKP for selective disclosure	Minimise data exposure during verifications
Scalability	Use Delegated Trust models for efficient verification	Improve system scalability and reduce overhead

Table 2424: Summary of SSI Considerations and Recommendations

5.3.1 Applicability and limitations

While SSI offers substantial advantages, such as user-controlled identities, reduced reliance on centralized identity providers, and enhanced privacy, projects should evaluate the practical applicability and current limitations in the context of their technical and operational requirements:

- Integration Complexity: SSI frameworks, especially those based on blockchain or distributed ledgers, may require considerable integration effort with existing legacy systems, supply chain actors, and regulatory bodies.
- Maturity and Standardization: Given the rapid evolution of SSI standards (e.g., W3C Verifiable Credentials), systems must ensure compatibility with stable, well-supported protocols to avoid interoperability issues.
- Usability Challenges: End-user adoption depends heavily on intuitive interfaces and education. It is essential to design identity workflows that minimize user friction while maintaining security guarantees.
- Regulatory Alignment: Although SSI enhances user control, organizations must still implement appropriate governance, consent management, and data protection measures to comply with GDPR and sector-specific regulations.

5.3.2 Use of ZKP or delegated trust

To further enhance privacy and scalability in identity verification, the deployment of Zero-Knowledge Proofs (ZKP) and Delegated Trust models is recommended where feasible:

- Zero-Knowledge Proofs: ZKPs allow proving possession or validity of credentials without disclosing the underlying data, aligning with data minimisation principles and enabling privacy-preserving verifications. This technology can be instrumental in scenarios where proof of compliance or certification is needed without exposing sensitive details.

Funded by
the European Union

- Delegated Trust: Implementing delegated trust frameworks enables selective disclosure and verification through trusted third parties, reducing verification overhead and enhancing scalability. This approach can be useful in multi-stakeholder environments, allowing interoperability among different actors while maintaining security.

6 Operational security and continuous risk management

Operational security is a critical pillar in the long-term success and resilience of the MaDiTraCe traceability system. Beyond secure design and development, continuous oversight, governance, and adaptive risk management processes are required to safeguard the integrity, confidentiality, and availability of the system throughout its lifecycle.

This section synthesizes essential practices and recommendations for establishing a robust operational security posture, ensuring ongoing compliance, and effectively managing evolving threats, including those originating from the supply chain.

6.1 Security governance for the traceability system

Effective governance provides the framework through which security policies, standards, and responsibilities are defined, communicated, and enforced across all stakeholders. Key governance considerations include:

- Establishing a Security Steering Committee: Composed of representatives from key partners (manufacturers, regulators, IT providers), this body should oversee security strategy, approve policies, and coordinate incident responses.
- Policy Development and Enforcement: Clear documentation of security policies covering access control, data protection, patching, and incident management must be maintained, with mechanisms for compliance verification.
- Risk Appetite Definition: Governance should articulate acceptable levels of risk, informing prioritization and resource allocation.
- Stakeholder Engagement: Regular security awareness and training programs should be instituted for all participants in the traceability ecosystem.

6.2 Monitoring, logging and incident response

Monitoring and Logging

Continuous monitoring is essential for early detection of anomalies, suspicious activities, and potential breaches. Recommended measures include:

- Comprehensive Logging: All access and transaction events across on-chain and off-chain components should be logged immutably and securely.

- Centralized Log Aggregation: Deploy Security Information and Event Management (SIEM) systems to aggregate logs from blockchain nodes, APIs, servers, and user interfaces for unified analysis.
- Anomaly Detection: Implement automated alerts triggered by patterns indicative of attacks (e.g., unusual transaction volumes, failed authentications).

Incident Response and Patch Management

Preparedness and agility in responding to security incidents minimize impact and recovery times:

- Incident Response Plan (IRP): Develop, test, and regularly update an IRP detailing roles, communication protocols, and containment procedures.
- Patch Management: Establish a process for timely application of security patches to blockchain clients, smart contracts, and supporting infrastructure, including procedures for emergency updates.
- Post-Incident Analysis: Conduct root cause analysis and incorporate lessons learned into security improvements.

6.3 Continuous threat modelling and update process

Security is not static; new vulnerabilities and threat actors emerge continuously. Therefore:

- Regular Threat Modelling: Repeat and update threat assessments periodically using structured methodologies such as P.A.S.T.A., adjusting to architectural changes and operational data.
- Integration with DevSecOps: Embed security testing, code analysis, and vulnerability scanning into continuous integration and deployment pipelines.
- Change Management: Ensure that updates to smart contracts or infrastructure undergo rigorous security review before deployment.

6.4 Auditing frameworks and compliance roadmap

To maintain transparency and trust, the traceability system should:

- Schedule Regular Audits: Engage independent third-party auditors for comprehensive security and privacy reviews, including smart contract audits and GDPR compliance assessments.
- Compliance Monitoring: Develop metrics and KPIs to monitor ongoing adherence to legal, regulatory, and contractual requirements.
- Reporting Mechanisms: Implement mechanisms for transparent reporting of audit results to governance bodies and, where applicable, public stakeholders.

Funded by
the European Union

6.5 Roles and responsibilities across stakeholders

Clear delineation of security roles enhances accountability:

Role	Responsibilities
Security Steering Committee	Strategic oversight, policy approval, incident coordination
System Administrators	Configuration management, patching, monitoring setup
Smart Contract Developers	Secure coding, testing, and deployment of smart contracts
Data Owners	Define access policies, consent management
End Users	Adhere to authentication protocols, report anomalies

Table 2525: Roles and Responsibilities in the Security Governance Framework

6.6 Recommendations for future penetration testing

To proactively identify weaknesses:

- Periodic Penetration Testing: Conduct internal and external penetration tests covering APIs, blockchain nodes, and smart contracts.
- Red Team Exercises: Simulate advanced, realistic attacks to assess incident response effectiveness and uncover hidden vulnerabilities.
- Bug Bounty Programs: Consider incentivizing external researchers to discover and responsibly disclose security flaws.

6.7 Supply chain threats and open risks

Recognizing that the supply chain itself can be a source of risk:

- Third-Party Risk Assessments: Evaluate the security posture of all external service providers, including blockchain infrastructure, identity providers, and cloud platforms.
- Secure Integration Practices: Adopt strict interface and data validation standards to prevent injection or manipulation attacks from compromised partners.
- Open Risks: Document known technical challenges such as scalability bottlenecks, cryptographic agility requirements, and emerging threat vectors (e.g., quantum computing impacts) to guide future research and mitigation planning.

Component	Recommended Practice	Purpose
Governance	Security steering committee and policy management	Align security efforts, clarify responsibilities

Monitoring & Logging	Centralized SIEM, anomaly detection, immutable logs	Early detection and forensic readiness
Incident Response	Tested IR plans, patch management, root cause analysis	Minimize impact, continuous improvement
Threat Modelling	Periodic updates with P.A.S.T.A. and integration in DevSecOps	Adapt to evolving threats, enforce secure updates
Auditing & Compliance	Independent audits, KPI monitoring, transparent reporting	Ensure accountability and trust
Roles & Responsibilities	Clearly defined roles for stakeholders	Foster ownership and coordination
Penetration Testing	Regular pentests, red teaming, bug bounties	Proactive vulnerability discovery
Supply Chain Security	Third-party risk assessment, secure integrations	Mitigate external attack vectors

Table 2626: Operational Security Components and Recommended Practices

This integrated operational security and continuous risk management framework provides a holistic approach to maintaining the security, privacy, and resilience of the MaDiTraCe traceability system throughout its lifecycle, aligning with European project expectations and industry best practices.

7 Conclusions and recommendations

7.1 Key security insights across workstreams

The security and privacy assessment of the MaDiTraCe project components, including the blockchain-based notarization tool, access control mechanisms, and data handling protocols, has highlighted several critical insights:

- Access Control is Paramount: Current designs without enforced Role-Based Access Control (RBAC) present significant risks of unauthorized access and data leakage. Strict enforcement of roles such as Notary, User, and Administrator is essential for secure operation.
- Data Privacy Must Be Reinforced: While blockchain immutability ensures integrity, the public nature of data on-chain raises privacy concerns. Employing encryption of hashes, off-chain storage of sensitive data, and advanced cryptographic methods such as Zero-Knowledge Proofs (ZKPs) are necessary to align with GDPR and ensure confidentiality.

- Smart Contract Security is Foundational: The Store.sol smart contract analysis revealed vulnerabilities typical of early Solidity versions and the absence of access restrictions. Upgrading Solidity versions, adding SPDX license identifiers, and implementing OpenZeppelin AccessControl modules are baseline requirements to mitigate risks.
- Operational Security and Continuous Risk Management are Vital: Beyond technical controls, the project requires ongoing governance structures, monitoring, auditing, and incident response plans to maintain resilience throughout the supply chain traceability lifecycle.

These findings align with the MaDiTraCe project's overarching goals of reinforcing the reliability and transparency of critical raw material supply chains through integrated digital and material science approaches.

7.2 Recommendations for development and pilots

To ensure secure, compliant, and resilient deployment of MaDiTraCe components in pilot environments, the following technical and organizational recommendations are prioritized:

Area	Recommendations	Priority
Access Control	Implement Role-Based Access Control (RBAC) with fine-grained permissions using standardized libraries.	High
Smart Contract Security	Upgrade Solidity compiler to latest stable version (^0.8.19), apply OpenZeppelin security patterns, and establish upgradeability proxies.	High
Data Privacy	Employ encryption for hashes on-chain, use secure off-chain storage for raw data and integrate Zero-Knowledge Proofs for private verifications.	High
Authentication	Enforce wallet-based authentication for blockchain interactions and multi-factor authentication (MFA) for administrators.	High
Monitoring and Incident Response	Deploy real-time logging and alerting systems; establish formal incident response and patch management workflows.	Medium
Compliance and Auditing	Integrate auditing frameworks aligned with GDPR and EU regulations; plan for third-party penetration tests and red teaming exercises.	Medium
Operational Governance	Define roles and responsibilities clearly across stakeholders; maintain continuous threat modeling and risk assessments.	Medium

Table 2727: Recommended Security Measures by Area and Priority

Pilot implementations should incorporate these measures early to validate their effectiveness under operational conditions. Feedback from pilots will refine these controls to balance security, usability, and scalability.

7.3 Strategic alignment with project goals

The security, confidentiality, and privacy recommendations outlined in this deliverable are tightly integrated with the overarching goals and specific objectives of the MaDiTraCe project, ensuring coherence and synergy across the consortium's efforts.

Alignment with General and Specific Objectives

- **General Objective:** To develop a trustworthy, scalable, and compliant digital product passport (DPP) infrastructure that enables transparent and reliable traceability of critical raw materials (CRMs) throughout their lifecycle. The security and privacy frameworks presented here directly support this by safeguarding data integrity, ensuring authorized access, and protecting sensitive information, thus establishing the trust necessary for broad stakeholder adoption.
- **Specific Objectives:**
    1. Design and implement robust cryptographic and blockchain-based notarization mechanisms that guarantee provenance and immutability of traceability data.
       This deliverable details the notarization tool's security architecture, smart contract hardening, and advanced cryptographic practices like zero-knowledge proofs, aligning with this objective.
    2. Develop and enforce privacy-preserving access control and identity management schemes compliant with GDPR and relevant EU regulations. Recommendations for Role-Based Access Control (RBAC), encrypted data storage, and wallet-based authentication form the foundation to meet these regulatory requirements.
    3. Establish operational security processes and continuous risk management practices that ensure system resilience in real-world conditions. The integration of monitoring, incident response, auditing, and governance frameworks ensures sustainable security management aligned with this objective.

Relationship with Other Work Packages

- **Mainly it has a relationship with WP4:** The secure traceability framework and notarization processes developed in WP3 feed directly into WP4's efforts to create credible certification mechanisms. The secure data provenance and privacy safeguards ensure that certification claims rest on trustworthy information foundations.

By ensuring that security and privacy measures are foundational rather than ancillary, this task enhances the project's ability to meet its goals effectively and sustainably. It facilitates trust across the value chain, accelerates adoption, and positions MaDiTraCe as a leading initiative in responsible digital traceability of critical raw materials.

Funded by the European Union

8 References

[1] "Process for Attack Simulation & Threat Analysis," https://4598121.fs1.hubspotusercontent-na1.net/hubfs/4598121/Ebooks/2022%20PASTA%20Ebook.pdf.

[2] T. Ucedavélez and M. M. Morana, *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. Wiley Blackwell, 2015. doi: 10.1002/9781118988374.

[3] "PASTA Threat Modeling - Threat-Modeling.com," https://threat-modeling.com/pasta-threat-modeling/.

[4] G. Bhusa and B. Shrestha, "The Role of PASTA in Addressing Future Trends in Regulatory Compliance: Emerging Cyber Threats," *International Journal of Innovative Science and Research Technology (IJISRT)*, pp. 110–115, Aug. 2024, doi: 10.38124/ijisrt/ijisrt24aug241.

[5] S. H. Mekala, Z. Baig, A. Anwar, and S. Zeadally, "Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions," Aug. 2023, *Elsevier B.V.* doi: 10.1016/j.comcom.2023.06.020.

[6] "A Comparative Risk Analysis on CyberShip System with STPA-Sec, STRIDE and CORAS," 2025, doi: 10.48550/arXiv.2212.10830Corpus.

[7] "STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery," https://onlinelibrary.wiley.com/doi/pdfdirect/10.4218/etrij.2021-0181.

[8] "Size, Speed, and Security: An Ed25519 Case Study," 2025, doi: 10.1007/978-3-030-91625-1_2Corpus.

[9] R. Nikam and M. Potey, "Cloud storage security using Multi-Factor Authentication," in *2016 International Conference on Recent Advances and Innovations in Engineering, ICRAIE 2016*, Institute of Electrical and Electronics Engineers Inc., 2016. doi: 10.1109/ICRAIE.2016.7939528.

[10] O. Ansotegui, "A Taxonomy of Blockchain Technologies: Principles of Identification and Classification," 2024, *University Library System, University of Pittsburgh*. doi: https://doi.org/10.1007/978-3-031-73122-8_13.

[11] "EBSI - European Blockchain Solutions Infrastructure," https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home.

[12] X. Ge *et al.*, "Blockchain and Green Certificates Based Market Structure and Transaction Mechanism of Direct Power-Purchase for Industrial Users," in *IEEE Transactions on Industry Applications*, Institute of Electrical and Electronics Engineers Inc., May 2023, pp. 2892–2903. doi: 10.1109/TIA.2023.3246966.

[13] C. Plociennik *et al.*, "Requirements for a Digital Product Passport to Boost the Circular Economy," in *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)*, Gesellschaft fur Informatik (GI), 2022, pp. 1485–1494. doi: 10.18420/inf2022_127.

[14] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," Jun. 2019, doi: 10.6028/NIST.IR.8202.

[15] C. Hanting, "A survey on smart contract vulnerabilities: Data sources, detection and repair," https://yanxiao6.github.io/papers/survey_on_smart_contract_vulnerabilities.pdf.

[16] "Access Control - OpenZeppelin Docs," https://docs.openzeppelin.com/contracts/4.x/access-control.

[17] "Circular economy action plan," https://environment.ec.europa.eu/strategy/circular-economy-action-plan_en.

[18] "Proposal for Ecodesign for Sustainable Products Regulation," https://environment.ec.europa.eu/publications/proposal-ecodesign-sustainable-products-regulation_en.

9 Annexes

9.1 Full Report 1 – Threat Modelling (PASTA)

Appendix A: check document *Preliminary Threat Modeling Report – PASTA Analysis on Draft Architecture.pdf*

9.1.1 Excel workbook - PASTA Methodology

Appendix B: Methodology_PASTA_Funditec.xlsm

9.2 Full Report 2 – Blockchain Selection

Appendix C: check document *Blockchain Selection for Maditrace.pdf*

9.3 Full Report 3 – Notarization Tool and Smart Contract

Appendix D: check document *Analysis of Notarization Tool and Smart Contract.pdf*

Funded by
the European Union