EUROPEAN HEALTH AND DIGITAL EXECUTIVE AGENCY (HADEA)

HADEA.B – Digital, Industry and Space
B.2 – Digital

AMENDMENT No AMD-101102743-7

Project: 101102743 — TRACE4EU

The parties agree to amend the Agreement as follows ('**Amendment**'):

1 . Addition of a new beneficiary

The following new beneficiary is added as from:

- VALUNODE OU (VALUNODE): 1 April 2024

This implies the **following changes** to the Agreement:

- The new beneficiary and the entry date are added to the list of participants in the **Data Sheet**.
- The new beneficiary is added to the **Preamble**:
  - 36. **VALUNODE OU (VALUNODE),** PIC 879963922, established in TATARI TN 1, TALLINN 10116, Estonia

2 . Beneficiary termination

The participation of the following beneficiary is terminated as from:

- DIGICITI NETWORKS OU (DIGICITI):
  - end of work date (‘exit date’): 31 March 2024
  - termination date: 31 March 2024 or the date of entry into force of this Amendment (whichever is the latest)

This implies the **following changes** to the Agreement:

- The beneficiary is deleted from the **Preamble**.
  - ~~14. DIGICITI NETWORKS OU (DIGICITI), PIC 892686345, established in TELLISKIVI TN 60/2, TALLINN 10412, Estonia,~~

  and the exit date is added to the list of participants in the **Data Sheet**.

In accordance with Article 32 of the Agreement, the beneficiary’s obligations continue to apply after termination.

If the termination leads to an amendment of the estimated budget (Annex 2), the maximum amount for joint and several liability of the terminated beneficiary is that of the estimated budget *before* this Amendment.

3 . Change of Annex 1

Annex 1 is changed and replaced by the Annex 1 attached to this Amendment.

4. Change of Annex 2

The estimated budget in **Annex 2** is changed.

This implies the **following changes** to the Agreement:

- **Annex 2** is changed and replaced by the Annex 2 attached to this Amendment.
- The table on maximum grant amount and total estimated eligible costs and contributions in the **Data Sheet** is updated.

All other provisions of the Agreement and its Annexes remain unchanged.

This Amendment **enters into force** on the day of the last signature.

This Amendment **takes effect** on the date(s) mentioned in the amendment clause(s) (or — if no date was chosen — on the same date the Amendment enters into force).

Please inform the other members of your consortium (if any) of this Amendment.

SIGNATURES

For the coordinator

[redacted] with ECAS id n006fqk1 signed in the Participant Portal on 06/05/2024 at 12:45:13 (transaction id SigId-62897-8P7D5bEp6rTlXTzt374daZHoWc2NLzKYqn6POHnSzlNckaZdDglyJmqHy7BNkH6CgDLEvUxHaPg2L7hVYwFESiW-yntOf97TTHq8GZt5aBGF4O-jnJHRR7767zOrAlaNSb3w4ncZwsLUfnJM9WPH8kL8nRheZaeEIREU7bac2WzemhgjfHCrmvARMftzdfldjYkvZW). Timestamp by third party at 2024.05.06 12:45:54 CEST

For the granting authority

Signed by J[redacted] with ECAS id jungeje as an authorised representative on 22-05-2024 15:19:01 (transaction id SigId-10001-Z1iSzxVpeNcBVOj77tyW9qjk4Hsv1bJN2GP2gImIV5DoqX4huQKgYN454rGBIJ90cIY1yv393QCbXA6VLTIzpe-yntOf97TTHqoPPtGMdHyoy-1RokPnEWLkNMig6TpvwoZCzSifJ23bDWBwzrg2c3hEZOycBX4S93GkozdSNjomhWdWrfxkzpZXtw4VXCI4CaSzk) 2024.05.22 15:19:05 CEST

Done in English

Enclosures: Grant Agreement Data Sheet
Grant Agreement Annex 1
Grant Agreement Annex 2

ANNEX 1

Digital Europe Programme (DIGITAL)

Description of the action (DoA)

Part A

Part B

DESCRIPTION OF THE ACTION (PART A)

COVER PAGE

Part A of the Description of the Action (DoA) must be completed directly on the Portal Grant Preparation screens.

PROJECT *Grant Preparation (General Information screen) — Enter the info.*	
Project number:	101102743
Project name:	Traceability Reference Architecture Conformant EBSI for European Union
Project acronym:	TRACE4EU
Call:	DIGITAL-2022-DEPLOY-02
Topic:	DIGITAL-2022-DEPLOY-02-EBSI-SERVICES
Type of action:	DIGITAL-SIMPLE
Service:	HADEA/B/02
Project starting date:	1 June 2023
Project duration:	27 months

TABLE OF CONTENTS

Project summary 3
List of participants 3
List of work packages 5
Staff effort 12
List of deliverables 14
List of milestones (outputs/outcomes) 23
List of critical risks 24

PROJECT SUMMARY

Project summary

Grant Preparation (General Information screen) — Provide an overall description of your project (including context and overall objectives, planned activities and main achievements, and expected results and impacts (on target groups, change procedures, capacities, innovation etc)). This summary should give readers a clear idea of what your project is about.

Use the project summary from your proposal.

The traceability of data, documents, and physical goods are essential in many fields. Therefore, the traceability use case was one of the first developed by the EBP (from 2018 on). Traceability use cases and applications enable EBSI and other blockchain-based electronic ledgers to be used and applied in many domains. The general objective of this project is to create an "umbrella architecture" based on existing EBSI services. The architecture builds the basis for the realization of traceability application scenarios. Furthermore, TRACE4EU focuses on engagement with pan-European stakeholders and promotion of recommendations for further development of the EBSI eco-system. As a result, TRACE4EU can significantly influence traditional industries and contribute to their transition to more efficient, productive, competitive, and resilient ones. It will also strengthen transparency in the European area for citizens, who can better and proactively track the flow of commodities and data through future traceability implementations. The umbrella architecture will be derived from the work on multiple scenarios, including analyzing requirements for traceability applications of tangible and intangible assets that work in local and cross-border settings.

LIST OF PARTICIPANTS

PARTICIPANTS

Grant Preparation (Beneficiaries screen) — Enter the info.

Number	Role	Short name	Legal name	Country	PIC
1	COO	Intesi	INTESI GROUP SPA	IT	886542171
2	BEN	GovPart	GOVPART GMBH	DE	888107654
3	BEN	msg	MSG SYSTEMS AG	DE	886714249
4	BEN	TU Berlin	TECHNISCHE UNIVERSITAT BERLIN	DE	999986678
5	BEN	INFOCERT	INFOCERT SPA	IT	990330037
6	BEN	VALIDATED ID SL	VALIDATED ID SL	ES	937979040
7	BEN	LIST	LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY	LU	934320200
8	BEN	ARCHIPELS	ARCHIPELS	FR	891545140
9	BEN	HAW HAMBURG	HOCHSCHULE FUR ANGEWANDTE WISSENSCHAFTEN HAMBURG	DE	999876680
10	BEN	DANUBE TECH	DANUBE TECH GMBH	AT	919243975
11	BEN	Spherity GmbH	SPHERITY GMBH	DE	904225271
12	BEN	UNIPD	UNIVERSITA DEGLI STUDI DI PADOVA	IT	999995602
13	BEN	TalTech	TALLINNA TEHNIKAÜLIKOOL	EE	999842536
14	BEN	DIGICITI	DIGICITI NETWORKS OU	EE	892686345

PARTICIPANTS

Grant Preparation (Beneficiaries screen) — Enter the info.

Number	Role	Short name	Legal name	Country	PIC
15	BEN	Neumann	NEUMANN JANOS NONPROFIT KOZHASZNU KORLATOLT FELELOSSEGU TARSASAG	HU	998453593
16	BEN	RBI	RUDER BOSKOVIC INSTITUTE	HR	999875031
17	BEN	GOLDMAN	AC GOLDMAN SOLUTIONS&SERVICES GSS LTD	CY	917565390
18	BEN	MGTŠ	MINISTRSTVO ZA GOSPODARSTVO, TURIZEM IN SPORT	SI	998818895
19	BEN	NTNU	NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET NTNU	NO	999977851
20	BEN	UNISOT	UNISOT AS	NO	892058949
21	BEN	NDF	FISKERIDIREKTORATET	NO	890176470
22	BEN	GRNET S.A.	NATIONAL INFRASTRUCTURES FOR RESEARCH AND TECHNOLOGY	EL	999937887
23	BEN	Excid	INTERNET IDENTITY SECURITY ANDPRIVACY SOLUTIONS I.K.E.	EL	885501167
24	BEN	Maritech AS	MARITECH AS	NO	885423082
25	BEN	HASHNET	HASHNET DISTRIBUIRANE TEHNOLOGIJE DOO	SI	900883621
26	AP	MINECHAIN	Minechain GmbH	DE	890417418
27	AP	FNDMT	FABRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA	ES	912199059
28	AP	NDA	DIGITALISERINGSDIREKTORATET	NO	998942667
29	AP	INFRACHAIN ASBL	INFRACHAIN ASBL	LU	907230428
30	AP	SDURDD	Central State Office for the Development of Digital Society	HR	894141442
31	AP	INCM	IMPRENSA NACIONAL - CASA DA MOEDA, S. A.	PT	911351958
32	AP	NArch	Arkivverket The National Archives of Norway	NO	890829086
33	AP	DFO	Direktoratet for forvaltning og økonomistyring	NO	892580809
34	AP	UVMB	ALLATORVOSTUDOMANYI EGYETEM	HU	917811673
35	AP	Talao	WEB3 DIGITAL WALLET,	FR	885481088
36	BEN	VALUNODE	VALUNODE OU	EE	879963922

LIST OF WORK PACKAGES

Work packages

Grant Preparation (Work Packages screen) — Enter the info.

Work Package No	Work Package name	Lead Beneficiary	Effort (Person-Months)	Start Month	End Month	Deliverables
WP1	Project Management and Coordination	1 - Intesi	60.47	1	27	D1.1 – Project Management Handbook D1.2 – Quality Assurance Plan (QAP) D1.3 – Risk Management Plan and Reports D1.4 – Final project reports D1.5 – Interim report D1.6 – Final report D1.7 – Ethics Check
WP2	Technology, interoperability, and cybersecurity	4 - TU Berlin	317.50	1	27	D2.1 – Architectural equirements D2.2 – Initial architecture D2.3 – Umbrella Architecture Components D2.4 – Finalization of conformance tests D2.5 – Support of chosen protocols and platforms D2.6 – Exploitation and dissemination
WP3	Utilization, Rollout, Scalability, and Communication	3 - msg	115.00	1	27	D3.1 – Overview on Stakeholders D3.2 – Assessed EBSI results D3.3 – Distribution Strategy and Rollout plan D3.4 – Implemented ecosystem
WP4	Products and Materials traceability pillar	11 - Spherity GmbH	193.00	1	27	D4.1 – Products & Materials traceability scenarios and requirements D4.2 – Product & Materials traceability demonstrators D4.3 – WP4: Piloting reports and recommendations

Work packages

Grant Preparation (Work Packages screen) — Enter the info.

Work Package No	Work Package name	Lead Beneficiary	Effort (Person-Months)	Start Month	End Month	Deliverables
WP5	Data and documents traceability pillar	5 - INFOCERT	224.50	1	27	D5.1 – Document traceability scenarios and requirements D5.2 – Document traceability demonstrators D5.3 – WP5: Piloting reports and recommendations

Work package WP1 – Project Management and Coordination

Work Package Number	WP1	Lead Beneficiary	1 - Intesi
Work Package Name	Project Management and Coordination		
Start Month	1	End Month	27

Objectives
The key objectives of the Project Management & Coordination Work Package are: • To ensure implementation of the projects in line with the guidelines from the European Commission, the Grand Agreement and the CA applying the project governance principles and mechanisms, • To perform overall scientific and technical coordination of the project • To ensure Ethics, Security, GDPR and Gender Management procedures and manage all types of the project data upon FAIR and Ethical principles • To monitor and assess risks and opportunities encountered during project implementation • To take appropriate steps to safeguard existing and future legal, copyright and IPR issues. Ensure that the project meets its objectives in a timely, cost effective and high-quality manner.

Description
The Project Coordinator will assume responsibility for contacting the Project Officer, formulating propositions for possible modifications of the work plan, supervising contacts with all external organisations, delivering all types of deliverables. An important key for project success will be ensuring effective collaboration and easy communication between partners and towards external entities. The Project Coordinator prefers to delegate this important Work Package to msg as Beneficiary experienced in large-scale IT project management. The WP1 includes following Tasks: Task 1.1 Project Management & Financial Administration The task groups all the activities to be carried out by the Project Coordinator and includes: (a) maintaining contractual documents; (b) issue of internal and contractual periodic reports; (c) organising project launch (establishing procedures, project management methods and tools, organising project kick-off meeting) and follow-up (periodic project boards meetings, progress review, and conflict resolution); (d) co-ordinating the timely production of deliverables and reports and maintaining the project archive; (e) coordination of financial and administrative issues: (f) KPI monitoring Task 1.2 Quality Assurance and Risk Management This task aims at planning, managing, and controlling the quality of project activities and deliverables. The quality methodologies and procedures applied will be in line with the most common standards suitable for the needs of a research project. This task includes the internal and external deliverable review, internal review of the results, tracking of the “lessons learned”. Task 1.3 Innovation and technical management The task groups all the activities to be carried out by the Technical Manager and includes: (A) Monitoring of the general scientific and technological evolution; (B) Monitoring of the progress of innovation and technological developments carried out in digital identity framework; (C) Identification and troubleshooting of technical problems; (D) Liaison with related projects, standardisation bodies and networks of excellence. The task includes also review and approval of technical reports and deliverables. Task 1.4 Assessment, testing, and development feedback of large-scale pilots (Pilot Coordination) This task will perform a continuous monitoring and assessment of the status and progress of the pilots across WP2 and WP3, aiming to ensure that they are operated smoothly and in line with their stated goals. Furthermore, this task will be checking whether, when and how the conformance and interoperability requirements are met by the pilots and to what degree the ambition level of being "as close to real life as possible" is achieved. Feedback and alignment mechanisms with the coordinators or WP2 and WP3 pilot as well as the testing and infrastructure tasks in WP4 will be established in order to implement this task.

Work package WP2 – Technology, interoperability, and cybersecurity

Work Package Number	WP2	Lead Beneficiary	4 - TU Berlin
Work Package Name	Technology, interoperability, and cybersecurity		

Start Month	1	End Month	27

Objectives
• Creation of an umbrella architecture that can foster traceability use cases • Development of architectural components on the top of EBSI • Testing goal: Conformance testing with APIs and vocabularies • Identify and mitigate potential risks of the umbrella architecture • Creation of conformance with the EU regulation such as GDPR • Alignment of the technology stack with existing frameworks such as eSSIF to enable interoperability

Description
The WP2 includes following Tasks: Task 2.1 Architecture Design The goal of this task is to create an actionable detailed architecture from the high-level architecture provided in this proposal. The detailed architecture will contain the mapping of system components to existing EBSI services and new components such as preservation services that are not a part of EBSI yet. Task 2.2 Implementation This task covers the implementation activities related to the umbrella architecture of TRACE4EU. In particular, components that have been defined during the architecture design and do not exist yet will be implemented as well as components, protocols and tools that are needed to achieve the goals of TRACE4EU. Task 2.3 Testing In this task, we will develop test suites that can be run against the components developed in T2.2. This will be modelled after other test suites that have been used successfully e.g. in the W3C to test compliance of DID and VC implementations. Task 2.4 Cybersecurity & Privacy Analysis and Mitigation The goal of this task is to identify potential cybersecurity and privacy risks (e.g. attack surface and vulnerabilities) of the new system that is developed in T2.1 and T2.2 with its umbrella use case, especially at the interface to the EBSI/DLT infrastructure. A focus is put on the integrity of data, authenticity of communication partner or data, confidentiality of data, availability of services, and how non-repudiation as well as privacy is achieved. Task 2.5 Legislation Conformity Analysis Task 2.5 substantiates the data protection environment of the architectural components in terms of the GDPR and analyses the basic legal potential of the application of the use cases to be developed. On the basis of this analysis de lege lata, the second step will be to elaborate the legal design of the architecture to be created, from which recommendations for legislative reforms can be derived. Task 2.6 Interoperability Interoperability will be investigated in two directions. First, the interoperability of the architecture developed in this project with the existing EBSI services and building blocks. Second, interoperability between private sector platforms. The interoperability with the EBSI will include the core services, chain and storage, and infrastructure layers.

Work package WP3 – Utilization, Rollout, Scalability, and Communication

Work Package Number	WP3	Lead Beneficiary	3 - msg
Work Package Name	Utilization, Rollout, Scalability, and Communication		
Start Month	1	End Month	27

Objectives
• Utilization, scalability, rollout, and communication of developed services and software. • Coordination of the development activities with the EBSI core team and other external projects and networks. • Creation of a strategy to collect competencies for the rollout of the application scenarios in a scalable manner across multiple EBP countries

Description
WP3 includes following Tasks:

Task 3.1 Coordination with other external projects and networks
Technical coordination and alignment with related external projects and networks relevant stakeholders (EC, EBSI, Standardization Committees etc.) especially those ones working with EBSI and other DLT in coordination with other WP coordination on: Regulation in EU, EFTA and relevant member states, standardization, integration of use cases, infrastructure, interoperability, operations, maintenance, cybersecurity & privacy, periodical meetings
Task 3.2 Coordination with the EBSI Core Team
Main content is observation and assessment of ongoing European political, regulative, strategic, technical initiatives related to the projects (e.g. eIDAS,GDPR, EBSI, related ESI projects like Diplomas etc.) including the information exchange and adoption for TRACE4EU use cases and coordination with related WP 2 . A permanent exchange with WP 4 & 5 will be established including assessment of cross-border implementation there ensure implementation and utilization of TRACE4EU Application Scenarios in the participating member states as well as cross-border.
Task 3.3 Strategy development for further distribution of the use case among other EU countries
The main task is to define a strategy for rollout scalable cross-industry / cross-border use cases from WP 4 and 5. A collaboration with EBSI adopter programme and other external projects identified in T 3.1 and T3.22.
Task 3.4 Scalability, rollout and ecosystem building across Europe and Application Scenarios
Development and implementation of rollout strategy from T 3.3 across Europe by one example.
Task 3.5 Overall User Engagement and Communication
All use cases of TRACE4EU will attain their full real-life usability with involvement of users outside this project. The organization an execution will be done by WP 3 in close collaboration with WP4 and 5. This task is provided to promote and widen the engagement of future users, by dissemination, communication and appropriate campaigning.

Work package WP4 – Products and Materials traceability pillar

Work Package Number	WP4	**Lead Beneficiary**	11 - Spherity GmbH
Work Package Name	Products and Materials traceability pillar		
Start Month	1	**End Month**	27

Objectives

• Application of the EBSI-based umbrella architecture to four Products and Materials Use Cases with different requirements and European regional interests in order to test the interoperability among countries, use cases, and requirements
• Demonstration of the technological interoperability of the developed umbrella architecture between the Products & Materials Traceability pillar and Document/data Traceability pillar
• Motivation of the European public authorities, research institutions, universities and private sector actors to use the EBSI architecture through demonstrating itsit's applicability to politically, socially and economically relevant Use Cases
• Best practices definition for the transfer of the EBSI-based umbrella architecture to other EU countries, similar Use Cases and various requirements
• Definition of the cooperation methods with other Use Case-related and EBSI-related previous, ongoing and future projects for mutual benefits and project interconnection

Description

WP4 Includes following Tasks:
Task 4.1 Implementation and piloting of Seafood Tracing Application Scenario
This task will design, implement, and pilot the scenario for seafood tracing. We will first identify requirements through collaboration with authorities and stakeholders in the seafood supply chain in Norway and the EU and identify the EBSI and stakeholders' infrastructure, which will be fed to WP2. We will then set up the piloting environment based on the architectural deliverables provided by WP2 and on additional components which we will develop or reuse from UNISOT's infrastructure. Continuous evaluation and improvement of our prototype will be performed with the help of a panel of selected stakeholders and end-users.
Task 4.2 Implementation and piloting of the Agrifood Tracing Application Scenario
This task will design, implement, and pilot the scenario for short supply chain agri-food tracing. We will first identify requirements through collaboration with food business operators (producers, retailers and the HoReCa sector), authorities and other stakeholders in three agri-food short supply chains (potato, egg and pork meat) in Hungary. Then we will identify the EBSI and stakeholders' infrastructure, which will be fed to WP2. We will then set up the piloting environment

based on the architectural deliverables provided by WP2 and on additional components which we will develop or reuse from UNISOT's infrastructure. Continuous evaluation and improvement of our prototype will be performed with the help of a panel of selected food business operators, stakeholders and also consumers as end users.
Task 4.3 Implementation and piloting of Materials Tracing Application Scenario
In this Use Case we will show the traceability of materials such as metals (potentially wood).
Participants involved are those who use metals (or wood) in their products, such as in Batteries (or Buildings) which have to comply to the new Battery Regulation and the EU Ecodesign for Sustainable Products Regulation, ESG requirements, child labour standards, responsible mining or other regulations and standards. The solution will be beneficial for numerous actors in the metal (and wood) value chain who will have less effort to declare product information and comply with existing regulations.
Task 4.4 Implementation and piloting of Halloumi Cheese (PDO)Tracing Application Scenario
EU geographical indication schemes protect specific knowhow, authenticity and agro-environmental conditions. The EC registered Halloumi as a protected designation of origin (PDO), protecting the valuable name against imitation and misuse across the EU. Only Χαλλούμι/Halloumi/Hellim produced in Cyprus according to the product specification is now allowed to use the registered name. The implementation of this application scenario will be based on the use of EBSI capabilities and APIs (current and new/enhanced), utilising case-agnostic data schemas. The Halloumi-model successful application will demonstrate that EBSI technology can provide an effective, trusted, digitalised and automated service/solution, to safeguard PDO and, in extension, PGI registered EU products.
Task 4.5 Lessons learned from products/materials traceability piloting
By the end of the project we would like to assess the feasibility of an EBSI-based agri-food traceability system in real-life environment (including applicability for tracing, quality assurance, safety assurance, and further data analysis), and also identify the further improvement and development needs regarding the data and metadata content, and the validity of these.
Task 4.6 Overall User Engagement and Communication
Regarding the fact that all WP4 use cases will attain their full real-life usability with involvement of users outside this project, this task is provided to promote and widen the engagement of future users, by dissemination, communication and appropriate campaigning.

Work package WP5 – Data and documents traceability pillar

Work Package Number	WP5	**Lead Beneficiary**	5 - INFOCERT
Work Package Name	Data and documents traceability pillar		
Start Month	1	**End Month**	27

Objectives
• Demonstrate how real use cases on document traceability can benefit from EBSI • Identify requirements for document traceability which are not yet part of EBSI and that may lead to the implementation of ancillary support services (in WP2) • Contribute to the EBSI adopter program with feedbacks and open components

Description
WP5 includes following Tasks: Task 5.1 Implementation and piloting of Open Rights Data Exchange application Valunode’s Open Rights Declaration Exchange requires the identification and authentication of rights holders and declarers. The execution of the use case will add authentication by the Self-Sovereign Identity application. Then, the Declaration Application takes a fingerprint of the related digital asset, immutably binds rights holders' identities with content identification, and stores this identifier binding in a shared DLT-based infrastructure. The execution of the use case will use the pluggable Ethereum protocol for the shared infrastructure initiated by Valunode. Task 5.2 Implementation and piloting of resume credentials application Resume credentials are credentials that persons carry with themselves throughout their professional life. Some of these credentials are given by public institutions such as high schools and upper secondary school diplomas. Mostly, they consist of credentials issued by companies. Depending on the county and state, there are preservation requirements for those documents for between two to fifty years (in Germany). One focus of resume credentials is the traceability, long-term preservation, and cross-border showcase of credentials given to persons by public institutions.

Task 5.3 Implementation and piloting of Democratizing Academic Publishing application
The DAP platform aims to create a democratic and reliable, trustworthy and efficient infrastructure for Open-Access scientific publishing (communication and dissemination), to strengthen the European Research Area (ERA) and the Digital European Program (DEP), and to support advanced global knowledge transfer. Since knowledge and information are strategic power, DAP aims to return this power to authors, researchers, scientists and the public, to improve good and trustworthy research practices, and to prevent violations of research integrity, as seen e.g. by the proliferation of "predatory publishers of Open-Access.
Task 5.4 Implementation and piloting of Electronic registered delivery application
This task will initially design the piloting scenario for electronic registered delivery, identifying infrastructural requirements which will be fed to WP2. It will subsequently setup the piloting environment based on the architectural deliverables provided by WP2 and possibly on additional components which will be developed specifically in this task. It will eventually execute the pilot with the help of a panel of selected users.
Task 5.5 Implementation and piloting of Know Your Customer application (KYC tool)
The KYC tool will allow an EU citizen to securely and digitally submit his personal documents to e.g. a bank, which will validate them and then store them encrypted on a preservation storage. The bank will also store the encryption key on EBSI. The citizen will then be able to make his KYC docs available to any other bank or institution by sharing with them the encryption key via the EBSI network.
Task 5.6 Lessons learned from data/document traceability piloting
This task will collect reports, statistics, remarks form the use cases one they have been tested on pilot users. It will then summarize the findings and recommend future actions on that basis.

STAFF EFFORT

Staff effort per participant

Grant Preparation (Work packages - Effort screen) — Enter the info.

Participant	WP1	WP2	WP3	WP4	WP5	Total Person-Months
1 - Intesi	26.00	14.50	5.00			45.50
2 - GovPart					10.00	10.00
3 - msg	32.00	23.00	41.00	5.00	20.00	121.00
4 - TU Berlin		54.00			36.00	90.00
5 - INFOCERT		12.00	6.00		34.00	52.00
6 - VALIDATED ID SL		47.00	16.00		9.00	72.00
7 - LIST		12.00		5.00	7.00	24.00
8 - ARCHIPELS		10.00				10.00
9 - HAW HAMBURG		14.00				14.00
10 - DANUBE TECH		31.00			8.00	39.00
11 - Spherity GmbH		16.00	6.00	37.00		59.00
12 - UNIPD		10.00			5.00	15.00
13 - TalTech		6.00				6.00
14 - DIGICITI	0.91				3.71	4.62
15 - Neumann			26.00	48.00		74.00
16 - RBI		17.00	7.00	3.00	34.00	61.00
17 - GOLDMAN		1.00	8.00	35.00	33.00	77.00
19 - NTNU		6.00		21.00		27.00
20 - UNISOT		6.00		14.00		20.00

Staff effort per participant

Grant Preparation (Work packages - Effort screen) — Enter the info.

Participant	WP1	WP2	WP3	WP4	WP5	Total Person-Months
21 - NDF				2.00		2.00
22 - GRNET S.A.		18.00				18.00
23 - Excid		18.00				18.00
24 - Maritech AS				23.00		23.00
25 - HASHNET		2.00			15.00	17.00
36 - VALUNODE	1.56				9.79	11.35
Total Person-Months	60.47	317.50	115.00	193.00	224.50	910.47

LIST OF DELIVERABLES

Deliverables

Grant Preparation (Deliverables screen) — Enter the info.

The labels used mean:

Public — fully open (⚠ automatically posted online)
Sensitive — limited under the conditions of the Grant Agreement
EU classified —RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision 2015/444

Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
D1.1	Project Management Handbook	WP1	3 - msg	R — Document, report	SEN - Sensitive	6
D1.2	Quality Assurance Plan (QAP)	WP1	3 - msg	R — Document, report	SEN - Sensitive	6
D1.3	Risk Management Plan and Reports	WP1	3 - msg	R — Document, report	SEN - Sensitive	6
D1.4	Final project reports	WP1	3 - msg	R — Document, report	PU - Public	27
D1.5	Interim report	WP1	1 - Intesi	R — Document, report	PU - Public	12
D1.6	Final report	WP1	1 - Intesi	R — Document, report	PU - Public	27
D1.7	Ethics Check	WP1	14 - DIGICITI	R — Document, report	PU - Public	6
D2.1	Architectural equirements	WP2	4 - TU Berlin	R — Document, report	SEN - Sensitive	12
D2.2	Initial architecture	WP2	4 - TU Berlin	R — Document, report	SEN - Sensitive	8
D2.3	Umbrella Architecture Components	WP2	6 - VALIDATED ID SL	R — Document, report	PU - Public	27
D2.4	Finalization of conformance tests	WP2	10 - DANUBE TECH	R — Document, report	PU - Public	27
D2.5	Support of chosen protocols and platforms	WP2	10 - DANUBE TECH	DEM — Demonstrator, pilot, prototype	PU - Public	27
D2.6	Exploitation and dissemination	WP2	4 - TU Berlin	R — Document, report	PU - Public	8
D3.1	Overview on Stakeholders	WP3	3 - msg	R — Document, report	SEN - Sensitive	6

Deliverables

Grant Preparation (Deliverables screen) — Enter the info.

The labels used mean:

Public — fully open (⚠ automatically posted online)
Sensitive — limited under the conditions of the Grant Agreement
EU classified —RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision 2015/444

Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
D3.2	Assessed EBSI results	WP3	3 - msg	R — Document, report	SEN - Sensitive	6
D3.3	Distribution Strategy and Rollout plan	WP3	3 - msg	R — Document, report	PU - Public	6
D3.4	Implemented ecosystem	WP3	3 - msg	DEM — Demonstrator, pilot, prototype	PU - Public	27
D4.1	Products & Materials traceability scenarios and requirements	WP4	11 - Spherity GmbH	R — Document, report	PU - Public	8
D4.2	Product & Materials traceability demonstrators	WP4	11 - Spherity GmbH	DEM — Demonstrator, pilot, prototype	SEN - Sensitive	18
D4.3	WP4: Piloting reports and recommendations	WP4	11 - Spherity GmbH	R — Document, report	PU - Public	27
D5.1	Document traceability scenarios and requirements	WP5	5 - INFOCERT	R — Document, report	PU - Public	8
D5.2	Document traceability demonstrators	WP5	5 - INFOCERT	DEM — Demonstrator, pilot, prototype	SEN - Sensitive	18
D5.3	WP5: Piloting reports and recommendations	WP5	5 - INFOCERT	R — Document, report	PU - Public	27

Deliverable D1.1 – Project Management Handbook

Deliverable Number	D1.1	**Lead Beneficiary**	3 - msg
Deliverable Name	Project Management Handbook		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	6	**Work Package No**	WP1

Description
D1.1 details the project management procedures, tools and assigned responsibilities, communication, meeting and reporting requirements and quality plan. Document, English

Deliverable D1.2 – Quality Assurance Plan (QAP)

Deliverable Number	D1.2	**Lead Beneficiary**	3 - msg
Deliverable Name	Quality Assurance Plan (QAP)		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	6	**Work Package No**	WP1

Description
D1.2 Outlines the quality management plan, including tracking by KPI. Document, English

Deliverable D1.3 – Risk Management Plan and Reports

Deliverable Number	D1.3	**Lead Beneficiary**	3 - msg
Deliverable Name	Risk Management Plan and Reports		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	6	**Work Package No**	WP1

Description
D1.3 outlines the risk analysis and mitigation framework. Document, English

Deliverable D1.4 – Final project reports

Deliverable Number	D1.4	**Lead Beneficiary**	3 - msg
Deliverable Name	Final project reports		
Type	R — Document, report	**Dissemination Level**	PU - Public
Due Date (month)	27	**Work Package No**	WP1

Description
D1.4 is the final report to be uploaded online and become publicly. available (if not indicated differently by EC). Document, English

Deliverable D1.5 – Interim report

Deliverable Number	D1.5	Lead Beneficiary	1 - Intesi
Deliverable Name	Interim report		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	12	Work Package No	WP1

Description
Interim report according to the Grant Agreement and Call for Proposals. Includes: • The engagement with stakeholders and their relevance for the EBSI take-up; • Legal, technical and organisational challenges, including security and data protection considerations and future standardisation needs. Appropriate follow up should be identified; • Recommendations for the further development of the EBSI eco-system; • Specific organisational structure and governance procedures; • Deliverables and achievements; • Synergies with other actions; • Updated KPIs; • Information on how dissemination and exploitation plans were implemented.

Deliverable D1.6 – Final report

Deliverable Number	D1.6	Lead Beneficiary	1 - Intesi
Deliverable Name	Final report		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	27	Work Package No	WP1

Description
Final Report according to the Grant Agreement and Call for Proposals. Includes: • The engagement with stakeholders and their relevance for the EBSI take-up; • Legal, technical and organisational challenges, including security and data protection considerations and future standardisation needs. Appropriate follow up should be identified; • Recommendations for the further development of the EBSI eco-system; • Specific organisational structure and governance procedures; • Deliverables and achievements; • Synergies with other actions; • Updated KPIs; • Information on how dissemination and exploitation plans were implemented. This report will also include the final Ethics report.

Deliverable D1.7 – Ethics Check

Deliverable Number	D1.7	Lead Beneficiary	14 - DIGICITI
Deliverable Name	Ethics Check		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	6	Work Package No	WP1

Description

Contains an assessment as requested by the Ethics Summary Report provided.

Deliverable D2.1 – Architectural equirements

Deliverable Number	D2.1	**Lead Beneficiary**	4 - TU Berlin
Deliverable Name	Architectural equirements		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	12	**Work Package No**	WP2

Description
Finalized requirements for improving the umbrella architecture.

Deliverable D2.2 – Initial architecture

Deliverable Number	D2.2	**Lead Beneficiary**	4 - TU Berlin
Deliverable Name	Initial architecture		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	8	**Work Package No**	WP2

Description
Creation of the initial architecture to start developing the required components and integrate with existing EBSI services

Deliverable D2.3 – Umbrella Architecture Components

Deliverable Number	D2.3	**Lead Beneficiary**	6 - VALIDATED ID SL
Deliverable Name	Umbrella Architecture Components		
Type	R — Document, report	**Dissemination Level**	PU - Public
Due Date (month)	27	**Work Package No**	WP2

Description
This deliverable details the components developed for the umbrella architecture of TRACE4EU. It includes a list of developed components including detailed information such as interfaces, etc.

Deliverable D2.4 – Finalization of conformance tests

Deliverable Number	D2.4	**Lead Beneficiary**	10 - DANUBE TECH
Deliverable Name	Finalization of conformance tests		
Type	R — Document, report	**Dissemination Level**	PU - Public
Due Date (month)	27	**Work Package No**	WP2

Description

Delivery of the final report for the conformance tests with defined platforms

Deliverable D2.5 – Support of chosen protocols and platforms

Deliverable Number	D2.5	**Lead Beneficiary**	10 - DANUBE TECH
Deliverable Name	Support of chosen protocols and platforms		
Type	DEM — Demonstrator, pilot, prototype	**Dissemination Level**	PU - Public
Due Date (month)	27	**Work Package No**	WP2

Description
Interoperability demonstration with chosen private and public sector platforms and protocols

Deliverable D2.6 – Exploitation and dissemination

Deliverable Number	D2.6	**Lead Beneficiary**	4 - TU Berlin
Deliverable Name	Exploitation and dissemination		
Type	R — Document, report	**Dissemination Level**	PU - Public
Due Date (month)	8	**Work Package No**	WP2

Description
TRACE4EU will achieve the third outcome by producing documentation and reports on all development phases. Deliverables of the third outcome will be used for recommendations for further development, piloting, and operational exploitation of the EBP priority use cases. This is an initial report with the first project results.

Deliverable D3.1 – Overview on Stakeholders

Deliverable Number	D3.1	**Lead Beneficiary**	3 - msg
Deliverable Name	Overview on Stakeholders		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	6	**Work Package No**	WP3

Description
PDF, ENG

Deliverable D3.2 – Assessed EBSI results

Deliverable Number	D3.2	**Lead Beneficiary**	3 - msg
Deliverable Name	Assessed EBSI results		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	6	**Work Package No**	WP3

Description
PDF, ENG

Deliverable D3.3 – Distribution Strategy and Rollout plan

Deliverable Number	D3.3	**Lead Beneficiary**	3 - msg
Deliverable Name	Distribution Strategy and Rollout plan		
Type	R — Document, report	**Dissemination Level**	PU - Public
Due Date (month)	6	**Work Package No**	WP3

Description
PDF, ENG

Deliverable D3.4 – Implemented ecosystem

Deliverable Number	D3.4	**Lead Beneficiary**	3 - msg
Deliverable Name	Implemented ecosystem		
Type	DEM — Demonstrator, pilot, prototype	**Dissemination Level**	PU - Public
Due Date (month)	27	**Work Package No**	WP3

Description
PDF, ENG Number of strategic building blocks for large-scale implementation/rollout of cross-border use cases.

Deliverable D4.1 – Products & Materials traceability scenarios and requirements

Deliverable Number	D4.1	**Lead Beneficiary**	11 - Spherity GmbH
Deliverable Name	Products & Materials traceability scenarios and requirements		
Type	R — Document, report	**Dissemination Level**	PU - Public
Due Date (month)	8	**Work Package No**	WP4

Description
Specification of requirements and scenarios for all document traceability pilots

Deliverable D4.2 – Product & Materials traceability demonstrators

Deliverable Number	D4.2	**Lead Beneficiary**	11 - Spherity GmbH
Deliverable Name	Product & Materials traceability demonstrators		
Type	DEM — Demonstrator, pilot, prototype	**Dissemination Level**	SEN - Sensitive
Due Date (month)	18	**Work Package No**	WP4

Description
Release of software (github repos) and complete working environments for pilots

Deliverable D4.3 – WP4: Piloting reports and recommendations

Deliverable Number	D4.3	**Lead Beneficiary**	11 - Spherity GmbH
Deliverable Name	WP4: Piloting reports and recommendations		
Type	R — Document, report	**Dissemination Level**	PU - Public
Due Date (month)	27	**Work Package No**	WP4

Description
Report of piloting activities (number of users, issues, etc.) and lessons learned

Deliverable D5.1 – Document traceability scenarios and requirements

Deliverable Number	D5.1	**Lead Beneficiary**	5 - INFOCERT
Deliverable Name	Document traceability scenarios and requirements		
Type	R — Document, report	**Dissemination Level**	PU - Public
Due Date (month)	8	**Work Package No**	WP5

Description
specification of requirements and scenarios for all document traceability pilots

Deliverable D5.2 – Document traceability demonstrators

Deliverable Number	D5.2	**Lead Beneficiary**	5 - INFOCERT
Deliverable Name	Document traceability demonstrators		
Type	DEM — Demonstrator, pilot, prototype	**Dissemination Level**	SEN - Sensitive
Due Date (month)	18	**Work Package No**	WP5

Description
Release of software (github repos) and complete working environments for pilots

Deliverable D5.3 – WP5: Piloting reports and recommendations

Deliverable Number	D5.3	**Lead Beneficiary**	5 - INFOCERT
Deliverable Name	WP5: Piloting reports and recommendations		
Type	R — Document, report	**Dissemination Level**	PU - Public
Due Date (month)	27	**Work Package No**	WP5

Description
Report of piloting activities (number of users, issues, etc.) and lessons learned

LIST OF MILESTONES

Milestones

Grant Preparation (Milestones screen) — Enter the info.

Milestone No	Milestone Name	Work Package No	Lead Beneficiary	Means of Verification	Due Date (month)
1	Basic project documentation is set up	WP1	3 - msg	The Deliverables D1.1-D1.3 are submitted	6
2	Mid-project review	WP1	3 - msg	The KPI, project budget, list of current participants are compared with those planned in MS1 and analysed for differences.	12
3	Project finalized	WP1	3 - msg	D1.4 as Deliverable is completed, D1.7 is completed.	27
4	Milestone 1 for WP2	WP2	4 - TU Berlin	Demonstrating a middle maturity of the technical architecture, clear vision of the project and clear technical specifications. Means of verification: D2.1, D2.2, D2.3, D2.4, D2.8, D2.10, D2.12, D2.14, and D.2.15	12
5	Milestone 2 for WP2	WP2	4 - TU Berlin	Providing final release, clear documentation and final demonstrator. Means of verification: D2.5, D2.6, D2.7, D2.9, D2.11, D2.13, and D2.17	27
6	List of external stakeholders	WP3	3 - msg	Deliverable D3.1	6
7	EBSI results assessed	WP3	3 - msg	Deliverable D3.2	6
8	Distribution strategy and Rollout Plan	WP3	3 - msg	Deliverable D3.3	6
9	Rollout pilot (Application Scenarios)	WP3	3 - msg	Deliverable D3.4	27
10	WP4: Definition of scenarios completed	WP4	11 - Spherity GmbH	Deliverable D4.1 released	8
11	WP4: Piloting environment ready	WP4	11 - Spherity GmbH	D4.2 delivered and components deployed in execution environments	18
12	WP4: Piloting concluded	WP4	11 - Spherity GmbH	Deliverable D4.3 released	27

Milestones

Grant Preparation (Milestones screen) — Enter the info.

Milestone No	Milestone Name	Work Package No	Lead Beneficiary	Means of Verification	Due Date (month)
13	WP5: Definition of scenarios completed	WP5	5 - INFOCERT	Deliverable D5.1 released	8
14	WP5: piloting environment ready	WP5	5 - INFOCERT	Deliverable D5.2 delivered and components deployed in execution environments	18
15	WP5: Piloting concluded	WP5	5 - INFOCERT	Deliverable D5.3 released	27

LIST OF CRITICAL RISKS

Critical risks & risk management strategy

Grant Preparation (Critical Risks screen) — Enter the info.

Risk number	Description	Work Package No(s)	Proposed Mitigation Measures
1	Coordination and communication issues Likelihood: Medium; Impact: Low; This risk can lead to missed deadlines, not clear priorities, and goals, etc.	WP1	The mitigation strategies for this risk included setting up clear communication channel, establishing roles and responsibilities for each partner that are clearly defined, and hold regular meetings to address issues immediately before they are becoming a bigger issue.
2	Partner does not deliver work they have committed Likelihood: Medium Impact: Medium This risk can occur because a partner is not able to deliver the appropriate work which was committed due to several reasons such as overcommitment.	WP1	This risk is mitigated by having a process in place that handles cases like this together by having backup plans. Task 1.2 is responsible for addressing this risk.
3	Conflicting priorities and goals Likelihood: Medium; Impact: Medium; When this risk occurs, it can lead to missed deadlines, objectives and goals of the project.	WP1	This risk is mitigated by defining the project's objectives already in an early stage and involving all partners in this process. This way, it is ensured that all partners are aligned with the project goals and priorities.

Critical risks & risk management strategy

Grant Preparation (Critical Risks screen) — Enter the info.

Risk number	Description	Work Package No(s)	Proposed Mitigation Measures
4	Budget overrun Likelihood: Low; Impact: Medium; This risk can lead to financing troubles of the involved partners. Developing use cases based on new technologies are less predictable than "business as usual" regarding costs. And the 50% funding rate means that partners may find themselves financially overwhelmed if they have to invest (co-fund) over the anticipated amounts.	WP1	This risk is mitigated by paying special attention to accurate budget reporting, control, and budget forecasting, throughout the project entire project execution.
5	Change of legislative environment in the EU Likelihood: Medium; Impact: Medium; This risk can lead to unconformity of the developed services with the changed legislative environment.	WP2	Task 2.5 is dedicated to analysis the legislation conformity. Therefore, even if a change in the legislative environment occurs, the project has dedicated resources and experts focusing on this aspect.
6	Cybersecurity related vulnerability Likelihood: Medium; Impact: Low; This risk leads to security issues that can be exploited. Nevertheless, vulnerabilities in services and software libraries are a common risk for all software products.	WP3, WP1, WP5, WP4, WP2	This risk is mitigated by having a process in place which monitors emerging vulnerabilities together with patch/update strategy. Task 2.4 tackles this risk. The likelihood for this risk is medium with a low impact on the project.
7	Uncertain requirements Likelihood: Medium; Impact: Medium; This risk can lead to missed deadlines or a product that cannot be used as planned. TRACE4EU aims to integrate with EBSI which could also create uncertain requirements.	WP5, WP4, WP2	This risk is mitigated by defining the project requirements within the related WPs in a thorough process for identifying all requirements involving all stakeholders. In case of EBSI, TRACE4EU will maintain close contact to EBSI core team in order to be aware of new requirements.
8	Software quality issues Likelihood: Medium; Impact: Low; This risk could lead to software bugs, system failures, or integration issues.	WP5, WP4, WP2	This risk is mitigated by performing thorough testing processes together with quality assurance processes. In particular, this risk is addressed in task 1.2.
9	Missing dependencies Likelihood: Medium; Impact: Medium; This risk could put the project deadlines in danger.	WP5, WP4, WP2	This risk is mitigated by identifying the needed dependencies in an early stage as well as my maintaining a contingency plan, and ensure a strategy that allows the project of having multiple options for critical dependencies. Also we are using an integrated approach in the project addressing missing dependencies.

Critical risks & risk management strategy

Grant Preparation (Critical Risks screen) — Enter the info.

Risk number	Description	Work Package No(s)	Proposed Mitigation Measures
10	Stigmatization of the blockchain technology Likelihood: Low Impact: Low This risk could decrease its interest as well as the number of parties that are willing to use this technology.	WP3	This risk is mitigated through creating awareness of TRACE4EU, its technologies, EBSI, its objectives, and results. Awareness is created in WP3 through trainings and workshops and the TRACE4EU website. The likelihood for this risk is low with a low impact on the project.
11	Resistance to change processes and fear of new technologies Likelihood: Medium Impact: Low This risk could make hit harder to add innovative process must be applied across a product manufacturing, distribution, and supply chain, involving farmers, truck drivers, manufacturers, and points of sale and consumers.	WP4	This risk is mitigated by defining well-planned communication and training activities. Early involvement of key stakeholders/actors and influencers across the product chain creates a robust chain of “ambassadors” and supporters. establishment of adequate support team and process. Also training the users to become familiar with the technology as such.
12	Competitive market Likelihood: Low; Impact: Low; This risk leads to the fact that competitive market solutions are available that hinder the establishment of the in this project developed solutions.	WP5, WP4	This risk is mitigated by performing market research, which should be an ongoing activity, and results should be reported to the consortium. Additionally, within TRACE4EU, new solutions are being developed based on cutting-edge technologies. Therefore, not many competitors will be available.
13	Low level of digitalization in product and materials supply chain Likelihood: Medium; Impact: Low; This risk could lead to the fact that the product and materials supply chain is comparatively low and additionally there might be fear of applying new technologies such as blockchains.	WP4	This risk is mitigated by selecting agri-food actors that are aware of the project goals together with closely cooperating with them and providing support in the form of workshops that also highlight the benefits for the agri-food industry and products.



Digital Europe Programme (DIGITAL)

Description of the action (DoA)

Part B

TECHNICAL DESCRIPTION (PART B)

COVER PAGE

Part B of the Application Form must be downloaded from the Portal Submission System, completed and then assembled and re-uploaded as PDF in the system.
Note: *Please read carefully the conditions set out in the Call document (for open calls: published on the Portal). Pay particular attention to the award criteria; they explain how the application will be evaluated.*

PROJECT	
Project name:	(T)raceability (R)eference (A)pplication (or (A)rchitecture) (C)onformant (E)BSI for European Union
Project acronym:	TRACE4EU
Coordinator contact:	[redacted]Intesi Group SpA

HISTORY OF CHANGES		
VERSION	**PUBLICATION DATE**	**CHANGE**
1.0	**01.11.2021**	Initial version (new MFF).
2.0	**13.02.2023**	1. Page 6 – adding more information on “Furthermore, coordination with EBSI core team is envisioned, but it is not clear how this will be achieved. In addition, cooperation with the European Commission is not elaborated in sufficient detail Please elaborate.” 2. Page 13 – adding more information on “6. The distribution of nodes at country level is not clear. Please explain.” 3. Pages 16-17 – adding more information on “4. Some use cases (e.g. digital twins for products and materials) are not sufficiently discussed, and it is not clear how they can generate valid outputs in a real scenario. Please elaborate.” 4. Page 24 – adding more information on “3. It is not sufficiently clear how advanced the projects itself is on the proposed implementation. For example, it is not clear which parts of the use case are contributed by the project and which parts already exist. Please explain.” 5. Page 33-34 – adding more information on “1. Some of the project specific objectives and activities are not described with sufficient detail. For example, while the provision of support services is considered, it is not very clear what these services will entail. Can you please provide a better description?” 6. Page 36 – adding more information on “Deliverables: The mandatory deliverables from the call text should be included in the Deliverables list”

		7. Page 38 – adding more information on "7. Project specific details and concrete measures are not clearly provided (e.g. scientific channel is mentioned as an emphasis, although no conferences or scientific journals have been explicitly identified as targets). Please elaborate." 8. Deliverables WP1: We kindly ask for shifting the manual-like deliverables by 2 months to ensure an effective project start
3.0	**15.03.2023**	Page 17 – specify the role of the associated partner UVMB Page 19 - specify the role of the associated partner SDURDD Page 22 – specify the role of the associated partners MINECHAIN, AltMe, FNDMT and INCM Section 4.4 – Subcontracting correction in form of a more detailed explanation Section 6 – Purchase costs correction in form of a more detailed explanation
4.0	**03.04.2023**	Page 24 - minor corrections to align with the Part A were made Section 4.4 – Subcontracting correction in form of a more detailed explanation Section 6 – Purchase costs correction in form of a more detailed explanation All missing partner information have been added
Final	**19.04.2023**	Subcontracting for MGTS has been adjusted, the new distribution of costs for MGTS: HR costs (reduced to): 51.940 EUR Subcontracting (increased to): 58.455,60 (which is 40.200 +18.255,60 EUR - from reduced labour cost) Travel and subsistence: unchanged =3.000 Indirect costs (calculated automatically): 7.938,00 EUR The overall Subcontracting for the project on the page 35 has been adjusted respectively to 313.455,60 EUR. DFO&Digdir descriptions have been added/changed as requested.
Amendment	**28.09.2023**	- change coordinator from MGTS to Intesi Group - change all references and responsibilities from MGTS to Intesi Group - Change subcontracting budget from MGTS to funding (personal costs) of Intesi Group - change timelines for deliverables (postponement due to change coordinator) - change responsible partner for D 3.1 and D 3.2 from TalTech to msg - extension project duration - shift budget and effort (13 PM) from NDF to Maritech which is related to Tasks 4.1, 4.2, 4.5, 4.6

		- change Budget from ExcID from category a1 to a3 - add Associated Partner Talao - Delete Task 5.7 in WP 5 and moved it into new Task 3.4 in WP 3 - Change in Project plan acc. new project duration (27 month) - adjusted deliverable references in Part B acc. actual Part A - Change of Intesi group Bank account
Amendment	**27.03.2024**	Terminating Digiciti's role per 31 March 2024 Adding Valunode's role from 1 April 2024

TABLE OF CONTENTS

TECHNICAL DESCRIPTION (PART B) **2**
COVER PAGE **2**
PROJECT SUMMARY **6**
1. RELEVANCE **6**
1.1 Objectives and activities 6
1.1.1 Project Overview 6
1.1.2 Alignment with the objectives and activities of the call 7
1.1.3 Contribution to the objectives of the Digital Europe Programme 8
1.2 Contribution to long-term policy objectives, policies and strategies — Synergies 8
1.3 Digital technology supply chain 10
1.4 Financial obstacles 10
2. IMPLEMENTATION **10**
2.1 Maturity 10
2.1.1 Maturity of EBSI Traceability Use Case 11
2.1.2 TRACE4EU Value Proposition 12
2.1.3 Maturity of the TRACE4EU Project Partners 14
2.2 Implementation plan and efficient use of resources 15
2.2.1 High-level Architecture 16
2.2.2 TRACE4EU Application Scenarios 17
2.2.3 Alignment with and Extension of EBSI services 20
2.2.4 Project Structure 21
2.2.5 Additional Technologies 23
2.3 Capacity to carry out the proposed work 26
3. IMPACT **37**
3.1 Expected outcomes and deliverables — Dissemination and communication 37
3.2 Competitiveness and benefits for society 42
3.3 Environmental sustainability and contribution to European Green Deal goals 44
4. WORK PLAN, WORK PACKAGES, TIMING AND SUBCONTRACTING **45**
4.3 Timetable 45
4.4 Subcontracting (n/a for prefixed Lump Sum Grants) 50
5. OTHER **52**
5.1 Ethics 52
5.2 Security 52
6. DECLARATIONS **52**
Purchases and equipment *52*
ANNEXES **54**

PROJECT SUMMARY

Project summary
See Abstract (Application Form Part A).

1. RELEVANCE

1.1 Objectives and activities

Objectives and activities

Describe how the project is aligned with the objectives and activities as described in the Call document.

How does the project address the general objectives and themes and priorities of the call? What is the project's contribution to the overall Digital Europe Programme objectives?

The European Union has set itself the goal of strengthening its member states' economic and social cohesion. Achieving the EU's goal requires a digital transformation and creating many digital services that function across borders and operate openly, transparently, and securely. One technical candidate for achieving these goals is using Blockchains and Distributed Ledger Technologies (DLT). Here, multiple distributed servers hold the same data, and a consensus mechanism decides which additional data will be added. Data updates are grouped into blocks, and each block references the state of the previous block, which means that no data can usually be manipulated after the write operation.
The European Commission (EC), EU Member States, Norway, and Liechtenstein have recognized the potential of this technology. They have jointly established the European Blockchain Partnership (EBP), developing and operating the European Blockchain Services Infrastructure (EBSI). The goal of EBSI is to enable the development of digital trusted services based on DLT technology for cooperation across national borders. As part of the "Digital Europe Programme (DIGITAL)," the EU promotes using and implementing digital technologies. This project, **TRACE4EU**, will address and investigate several application scenarios for **document traceability** and implement them with the help of EBSI services. In this context, it will extend, improve and mature the architecture of EBSI to promote its useability as a production environment.

1.1.1 Project Overview

The traceability of data, documents, and physical goods are essential in many fields. Therefore, the traceability use case was one of the first developed by the EBP (from 2018 on). Traceability use cases and applications enable EBSI and other blockchain-based electronic ledgers to be used and applied in many domains. The general objective of this project is to create an "umbrella architecture" based on existing EBSI services. The architecture builds the basis for the realization of traceability application scenarios. Furthermore, TRACE4EU focuses on engagement with pan-European stakeholders and promotion of recommendations for further development of the EBSI eco-system. As a result, TRACE4EU can significantly influence traditional industries and contribute to their transition to more efficient, productive, competitive, and resilient ones. It will also strengthen transparency in the European area for citizens, who can better and proactively track the flow of commodities and data through future traceability implementations. The umbrella architecture will be derived from the work on multiple scenarios, including analyzing requirements for traceability applications of tangible and intangible assets that work in local and cross-border settings. One of the project goals is to identify existing EBSI services and develop additional traceability services strongly connected with EBSI services. To connect existing EBSI services and new traceability services, the TRACE4EU partners will implement, evaluate and demonstrate developed scenarios by using and extending the EBSI services. To enable the necessary flexibility of the resulting architecture, each partner will also consider the local specifics for traceability in each country or region. A corresponding country-specific government supports each application scenario of this proposal. Furthermore, the governments provide local requirements for applying the umbrella architecture.

Figure 1 shows the TRACE4EU consortium comprising **24 partners and 10 associated partners** from **14 countries** to best meet the calls' objectives. As a result, all scenarios could optimally consider the cross-border requirements of EBSI.

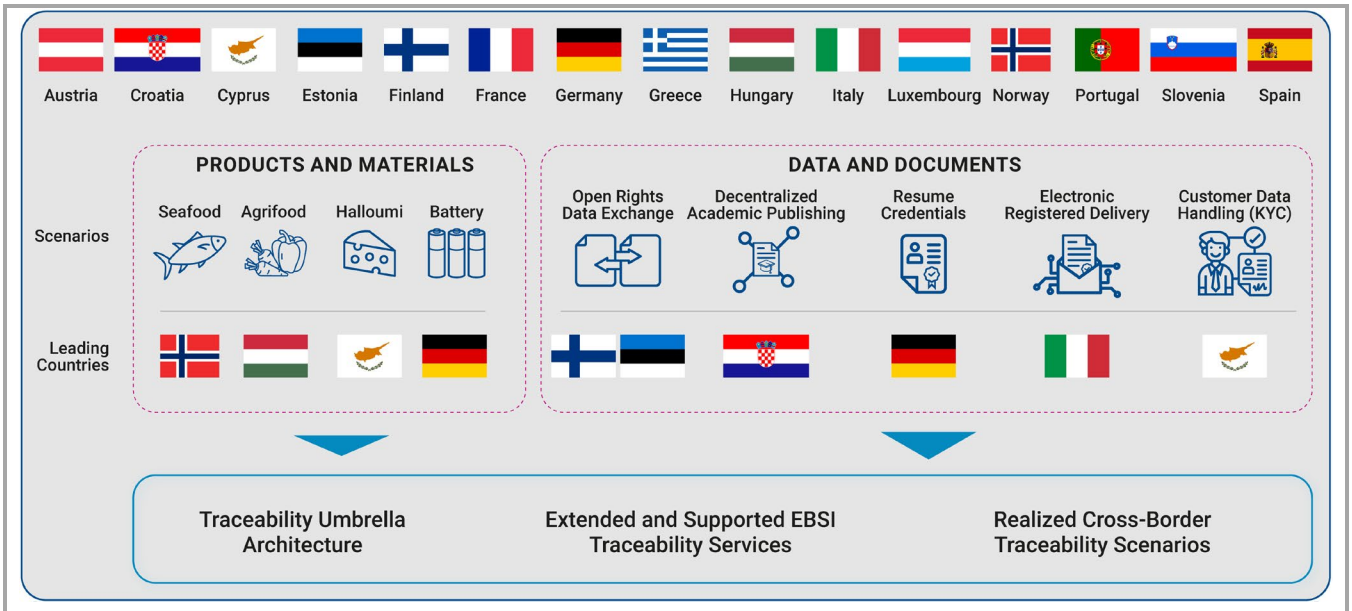


Figure 1 The TRACE4EU consortium consists of 24 partners and 10 associated partners from 15 EU countries

The partners are from 9 research institutions, 15 small and medium-sized enterprises, and six government bodies. Most of the partners have experience with EBSI because of the participation of early adopters in waves one and two. Furthermore, TRACE4EU has experienced EBSI node providers. The TRACE4EU partners are continuously in contact with EBP members, the EBSI core team, and pilot projects. The connection of TRACE4EU partners to EBSI, EBP, and pilot projects will be leveraged in this project proposal to advance the EBSI capabilities for traceability in a collaborative and coordinated manner. TRACE4EU consortium includes domain experts in traceability, manufacturing and supply chain professionals, legislators, scientists, and technicians.

TRACE4EU consortium divides traceability use case into two application scenarios:

- Traceability of Data and Documents
- Traceability of Products and Materials

Products and Materials respond to the need to be able to view the components of products transparently. However, transparency in product provenance can increase citizens' awareness to buy more local products. It is also helpful for companies and governments, which must check and prove the materials used. Building traceable supply chains with proof, certificates, and data lead to more openness and transparency for society and business. The TRACE4EU project will work on four application scenarios:

- Food production from agricultural products (led by Hungary)
- Seafood lifecycle (led by Norway)
- Trademarked sale of halloumi (led by Cyprus)
- Traceability of metals for battery production (led by Germany).

Data and Documents address the traceability of digital information. Verifying digital information for correctness, integrity, and/or validity is a significant challenge because multiple actors or non-trusted third parties often play a role in issuing or retrieving the data. The goal is to extend EBSIs' traceability services to solve these problems. To do this, TRACE4EU will work on the following application scenarios:

- Open exchange of rights data related to digital assets (led by Finland and Estonia)
- Resumé credentials for citizens (led by Germany)
- Decentralized academic publishing, DAP (led by Croatia)
- Electronic delivery of verified messages (led by Italy)
- Customer data retrieval for identification, KYC (led by Cyprus).

The application scenarios offer real added value for the citizens of the European Union and can influence other activities as flagship projects. Working on the application scenarios will lead to a holistic, generalized architecture from the scenarios' requirements. The results of the application scenarios and the TRACE4EU project, in general, will promote the development of future traceability projects of EBSI. The following sections describe the listed application scenarios in more detail.

1.1.2 Alignment with the objectives and activities of the call

The TRACE4EU project will expand and **reinforce the EBSI and EBP use case "Traceability."** For this purpose, several application scenarios have been selected, which will be implemented in real life by multiple

European partners together. The application scenarios offer a broad spectrum from traceability of raw materials to purchase or consumption of products by consumers. All scenarios will be tested by project members and the community, resulting in **beneficial and valid cross-border applications.** For the implementation of this project proposal, **TRACE4EU consortium members** provide and share extensive experience on best practices in distributed ledgers and EBSI. They also **operate EBSI nodes, can engage users, and provide support services** to strengthen national and international adoption of EBSI. The experience of TRACE4EU members will lead to useful traceability applications that benefit EU citizens and businesses.
The development of application scenarios will be intensively **coordinated with the EBSI core team** and the European Commission to **leverage existing EBSI services.** Wherever necessary, **proposals** and implementations will contribute **to the further development of the EBSI ecosystem**. These innovations will become visible through the processing of our scenarios. For example, we have determined areas of improvement in EBSI's storage capabilities. These and other aspects will be discussed in detail in TRACE4EU and ultimately result in a recommendation for a traceability umbrella architecture. Coordination with the EBSI core team is ensured by providing regular reports on TRACE4EU progress at the quarterly EBSI meetings, in which members of the TRACE4EU consortium representatives participate. On behalf of the European Commission, Policy Officer for Digital Innovation and Blockchain at the European Commission Pierre Marro is aware of TRACE4EU, and the project's progress will be regularly communicated to him as well. These measures will enable TRACE4EU to remain steadily compliant with the most recent EBSI-related developments and policies by both the European Blockchain Partnership and the European Commission.

1.1.3 Contribution to the objectives of the Digital Europe Programme

"Reinforce EU critical digital capacities by focusing on the key areas of artificial intelligence (AI), cybersecurity, advanced computing, data infrastructure, governance, and processing."
With its ideas, scenarios, and implementations, TRACE4EU will work on data infrastructure, governance, and processing. In cooperation with many governmental organizations, an umbrella architecture will be created, EBSI services will be extended, and traceability applications will be developed.

"best use for critical sectors like energy, climate change, and environment, manufacturing, agriculture, and health"
TRACE4EU has defined nine application scenarios to be worked on. Four of them can be assigned to the areas of energy, environment, agriculture, and manufacturing (see Section 2 and 3).

"upskilling to provide a workforce"
The TRACE4EU consortium will conduct several workshops and publish academic papers during the project period (see Section 3.2). It will provide resources to familiarize with traceability projects. Furthermore, higher education institutions are involved in the consortium to transfer the EBSI topics to students and teachers.

"digital transformation for private sector, small and medium-sized enterprises (SMEs), and public administration"
The TRACE4EU consortium consists of SMEs, government agencies, and universities. By participating in the project, the digital transformation of these partners is driven forward, and the implemented scenarios have the potential to change entire industries. In addition, an important goal is that others can implement their digital transformation based on the developed services and results.

"support to the Green Deal to SMEs and public authorities in their digital transformation"
Sections 1.2 and 3.4 show that the TRACE4EU project supports the Green Deal through energy efficiency and paper reduction. And it enables traceability applications to comply with sustainable production processes.

1.2 Contribution to long-term policy objectives, policies and strategies — Synergies

Contribution to long-term policy objectives, policies and strategies — Synergies

Describe how the project contributes to long-term policy objectives of the call's domain/area and to the relevant policies and strategies, and how it is based on a sound needs analysis in line with the activities at European and national level.

What challenge does the project aim to address?

The objectives should be specific, measurable, achievable, relevant and time-bound within the duration of the project.

TRACE4EU contributes to the following long-term policy objectives:

1. **Building public services for the digital transformation of the EU industrial ecosystems:** Through pan-European EBP use cases based on fully EBSI-compliant application scenarios, TRACE4EU contributes to the Digital Europe Programme by supporting the digital transformation of the industrial

ecosystem. The challenges for developing pan-European application scenarios are elaboration of business, functional and technical requirements considering country-specific policies. TRACE4EU addresses these challenges as authorities, companies, and universities from many European countries contribute with their experience and knowledge, especially in blockchain and distributed ledger technology.

2. **Realization of European regulations and legal certainty:** TRACE4EU consortium will design, implement and test application scenarios for trustworthy and privacy-preserving interactions between citizens, organizations, and public authorities. The developed solutions and processes will comply with the Single Digital Gateway Regulation (SDGR) and the underlying Once-Only Principle (OOP), ensuring that businesses and citizens in contact with public administrations must only provide data once. To fulfill SDGR and OOP, TRACE4EU will develop application scenarios including business, functional and technical requirements, exploiting existing EBSI capabilities. Addressing SDGR and OOP also includes strong alignment with eIDAS and GDPR. To meet the challenges of EU regulations and legal certainty, participants of TRACE4EU contribute with years of experience in decentralized ledger technologies, Self-Sovereign Identity, and international research projects.
3. **Increasing synergies with European and national activities:** TRACE4EU aims to build a robust and decentralized ecosystem utilizing gained knowledge from different initiatives, projects, and organizations. Consortial partners are active in the Horizon program, CHAISE, INATBA, and Gaia-X. The domain expertise, coupled with strong collaboration with World Wide Web Consortium (W3C), Decentralized Identity Foundation (DIF), and Trust-over-IP Foundation (ToIP), will significantly increase the quality of (research) results of the TRACE4EU project. Furthermore, TRACE4EU partners bring more detailed knowledge of EBSI through participation in previous early adopters waves one and two. Some consortium partners have already worked on blockchain research projects and built networks. Therefore, TRACE4EU guarantees openness to other stakeholders and further extension of the use case to other EBP countries.
4. **Promoting blockchain for sustainability:** The TRACE4EU project uses the EBSI services, which exclusively use blockchains that aims to lower computationally intensive of consensus algorithm to minimize power consumption. Furthermore, one goal is the pre-production implementation of digitization projects that will transform existing traceability practices for which paper and pen is often still used. Thus, the project contributes to paper reduction. Another aspect is that traceability applications generally enable the verification of products, materials, projects, and documents. This makes the TRACE4EU project sustainable and allows it to create a more sustainable future.
5. **Supporting interoperability and standards**: TRACE4EU focuses on cross-border verification of the authenticity of qualified signatures and certificates issued by qualified trust service providers. The implementations will orient to an open ecosystem, interoperable usable, and aligned to existing standards. TRACE4EU uses existing standards wherever possible to ensure that the interaction between the individual actors and the integration of future partners functions smoothly. The project consortium has a strong background and contacts in establishing and writing new standards. TRACE4EU project will be strongly aligned with eIDAS regulation[1]. Furthermore, standards and committees such as ISO/TC 307/JWG 04 "Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG, ETSI Electronic Signature Initiative (ESI) committee; ETSI Industry Specification Group on Permissioned Distributed Ledger (ISG PDL); CEN/CLC/JTC 019/WG 01 "Decentralized identity management" will be considered.
6. **Reinforcing and exploiting EBSI:** One of EBSI's primary objectives is to provide blockchain services and capabilities to the EU member states for them to realize their blockchain projects without having to deal with setting up their blockchain network. Nevertheless, many EU organizations are unaware of EBSI's capabilities, and even member states lack knowledge in this regard. TRACE4EU aims to, on the one hand, enhance existing EBSI nodes and extend the existing network by deploying new nodes. And on the other hand, TRACE4EU will host trainings that focus on national and sectoral levels for educational purposes, including complementing activities undertaken by the EBSI core team. Most importantly, TRACE4EU will pilot the traceability use case for several scenarios, in a cross-border setup, by involving 30 partners. This way, the exploitation effort will affect all partners, including many potential customers and clients.
7. **Supporting blockchain skills development:** Blockchain is still a relatively new technology, where rare experts are needed to build blockchain solutions, use cases, and realize projects. EBSI provides blockchain services to the European information technology landscape but still lacks awareness within Europe. TRACE4EU consists of 30 partners and will build large-scale pilots of the traceability use case for various scenarios utilizing EBSI's capabilities. This way, TRACE4EU supports the development of blockchain skills by introducing and involving EBSI capabilities and further developing, deploying, and

[1] eIDAS regulation: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

designing new services and functionalities. At the end of the project, all involved partners will have increased know-how of blockchain technology, including EBSI's services.

8. **Interacting with the community:** TRACE4EU involves many existing and new EBSI community partners. All work will provide the most open access to information possible and actively coordinate with the community. A project goal is the broad acceptance and openness of our results.

TRACE4EUs' proposal provides legal certainty to all involved stakeholders. The legal experience and background of some partners are more than 20 years of dedication to the legal aspects of electronic signature and digital identity technologies. Furthermore, within the consortium, at a corporate level, qualified trust service providers are involved, with a high level of knowledge and commitment to the trust service provision model defined by eIDAS.

Digital identity is an essential part of Europe's global digital transformation strategy. Europe is a world leader and showcase for digital identity, e-signatures, and privacy regulatory aspects. TRACE4EU aims to respond to the new digital identity paradigm promoted by the Commission with the latest draft of the eIDAS regulation. The eIDAS regulation originates from the previous work carried out by most of the consortium members. Furthermore, the eIDAS Bridge [2]allows the world of decentralized identities to be united with the current eIDAS regulation by using qualified certificates and seals. Also notable is the participation in developing the ESSIF framework[3], whose development has always considered regulatory compliance aspects.

Finally, some TRACE4EU participants are members of the ETSI standardization body, which is currently developing a large part of the technical regulations of eIDAS 2.

The main challenges the project addresses:

- Practical and private sector-oriented real-world application scenarios
- Pre-production to production
- Long-term preservation services with up to 50 years of preservation

1.3 Digital technology supply chain

Digital technology supply chain

Explain to what extent the project would reinforce and secure the digital technology supply chain in the EU.

⚠ *This criterion might not be applicable to all topics — for details refer to the Call document.*

Not applicable

1.4 Financial obstacles

Financial obstacles

Describe to what extent the project can overcome financial obstacles such as the lack of market finance.

⚠ *This criterion might not be applicable to all topics — for details refer to the Call document.*

Not applicable

2. IMPLEMENTATION

2.1 Maturity

Maturity

Explain the maturity of the project, i.e. the state of preparation and the readiness to start the implementation of the proposed activities.

TRACE4EU is designed with a mature technology stack, standardized by organizations such as W3C and ETSI, and utilized by organizations such as EBSI. The core components of TRACE4EU are exploiting the EBSI services. On the one hand, TRACE4EU utilizes the self-sovereign identity (SSI) approach. SSI emerged as a philosophy in 2016, and until now, it has seen numerous implementations across public and private sector platforms and projects. The eSSIF, Alastria, and IDunion are Europe's most significant SSI projects running while creating infrastructure for public and private sector use cases. The components related to SSI are either standardized or in the standardization process across organizations such as W3C, DIF, and the OpenID Foundation. On the other hand, TRACE4EU adds components for creating the requirements set by the regulatory framework to enable the long-term preservation of digital signatures and documents by ETSI TS 119 511. With these components, TRACE4EU completes the existing EBSI services to comply with European long-term preservation requirements according to eIDAS fully.

[2] eIDAS Bridge: https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about
[3] ESSIF Framework: https://decentralized-id.com/government/europe/eSSIF/

In the following, we will first evaluate the maturity of the used technologies, then discuss the maturity of the EBSI traceability use case and the added value of the TRACE4EU project proposal. We then finalize the project's maturity by presenting the partners' competencies and previous related work.

DIDs and DID Documents: DIDs are a new type of globally unique identifier like ISBN specified by the W3C. DIDs allow users to generate their identifiers using systems they trust. In addition, DIDs enable users to prove control over them through cryptographic proofs such as digital signatures. A DID contains no additional information but resolves into a DID document, which includes public information such as public keys used to, e.g., prove the DIDs ownership. The DID document contains the DID subject's DID (user/identity). In addition, it defines the cryptographic verification material required by entities interacting with the DID subject for various purposes. For example, cryptographic verification is used to verify digital signatures as needed for verifying issued credentials, authentication, or exchanging confidential messages. The added value of DIDs and DID documents lies in storing this information in tamper-proof and highly available verifiable data registries (VDR). VDRs can be governed in a decentralized manner by multiple parties. Examples of such VDRs are distributed-ledger technologies (DLT) such as Hyperledger Fabric or Besu. This type of VDR enables participants to have an accepted trust anchor that is not governed by a centralized entity. Such a value proposal is quite powerful as it also aligns with the governance of the EU. Thus, EBSI offers such VDRs as core services. Four years after their introduction, decentralized identifiers are a W3C recommendation and mature enough to be used in implementations for real applications in production environments.

Verifiable Credentials & Presentations: The Verifiable Credentials (VC) Data Model 2.0, defined by the W3C, is a data format for describing credentials (e.g., IDs or certificates) in the context of self-sovereign identity. The data model is a container for content that can be preserved in a tamper-proof, privacy-friendly, machine-verifiable manner and whose origin can be cryptographically verified. In this context, VCs use digital signatures or other cryptographic technologies such as zero-knowledge proofs (ZKP) to derive a so-called verifiable presentation (VP) from VCs, which contains all or partial contents of the VC and a proof. In addition, the VP includes proof that the VC is bound to the identity subject. The contents of the displayed VP can be cryptographically verified for authenticity and integrity. To ensure that VCs are interpreted correctly and that the issuing body and the verifying body use the same terminology, a context must be defined for the VC, specifying the respective VC's attributes and structure. A VC can be modeled with JSON or JSON-LD. The verifiable credential data model is in the Editor's draft status. There are changes to be expected until it becomes a W3C recommendation, but the specification is mature enough to be used in implementations.

Long-term Preservation: In 2014, the European Commission introduced the regulation on electronic identification and trust services (eIDAS) for electronic transactions in the EU internal market. The qualified electronic signatures, seals, and timestamps shall be preserved with a qualified preservation service to comply with the regulation (see eIDAS Article 33 and 40). eIDAS recital 61 describes the necessity of long-term preservation as the following: "This Regulation should ensure the long-term preservation of information, to ensure the legal validity of electronic signatures and electronic seals over extended periods and guarantee that they can be validated irrespective of future technological changes." ETSI standardized the long-term preservation of digital signatures. Since then, Member States have created technical specifications and implementation based on the regulatory requirements from the eIDAS and the specification from ETSI TS 119 511. Among those specifications and implementations are TR-03125 by the German Federal Office for Information Security and several compliant commercial solutions (18 mentioned in EU trust list). Therefore, the maturity of long-term preservation specifications and implementations are high and can also be implemented so that they can either be exploited by other EBSI services or integrated as EBSI core services to the EBSI architecture.

2.1.1 Maturity of EBSI Traceability Use Case

Currently, the EBSI architecture contains components required to have document traceability. EBSI utilizes blockchain technology to prove the integrity of documents. Integrity in this context means that the document has not been modified and represents precisely what the initial author has created. For this purpose, the hash of the document is stored on-chain. The integrity of the presented document is validated by checking the signature's hash against the document's hash stored on-chain. If both match, it means that the presented document is in the state the author created.Furthermore, to prove whether a signature is correct, the document must be signed with a private key of a public/private key pair, where the public key is known to the validating party. In the case of EBSI, the public key can be stored in an X.509 certificate or a DID document. Generally, if the traced documents are JPEGs or PDFs, the public key related to the signing private key is stored in an X.509 certificate. The trust in the public key in the X.509 certificate can be achieved via a certificate chain up to a trusted root certificate or trust anchor. For the self-sovereign identity use cases (Diploma, Identity, and Social Security), the public key related to the signing key is found in a DID document. In this case, a JSON document in the format of a verifiable credential according to the W3C Editor's Draft is created by the author.

The EBSI core services offer registration of DIDs and the creation of DID documents by the author. The trust in the public key in the DID document can be achieved with the EBSI acting as an on-chain verifiable data registry

and trust anchor. Trust is anchored to the EBSI ledger because the history of the key data cannot be manipulated without re-hashing. The underlying public key via DID and DID document is also validated during the document validation. Furthermore, the correctness of the intended purpose of the X.509 certificates must be validated: For the validity and correctness of a certificate, it is checked whether the signature or seal set by the issuer of the certificate is valid, whether certificate extensions in accordance with [eIDAS Regulation], Article 38 No. 3 and the intended purpose of the certificate have been set correctly and whether a certificate path to a trusted root certificate or trust anchor can be formed and whether the certificate has not been revoked. In the case of DIDs and DID documents, EBSI offers a Trusted Issuer Registry and other core services to validate the correctness of the intended purpose of the DID documents.

The final building block of document traceability is timestamping service. According to the eIDAS Regulation, Article 3 No. 33, an "electronic time stamp" means data in electronic form which binds other data in the electronic form to a particular time establishing evidence that the latter data existed at that time." A timestamp is required to ensure that the document has been created at a specific time. EBSI core services offer timestamping services. Furthermore, in the case of traceability use cases, the timestamps for document hashes are also stored on-chain. Figure 2 illustrates how TRACE4EU leverages EBSI to implement cross-border verification of product certificates and history, document integrity, and verifiable credentials related to Identity, Diploma, Product, and Document. Through EBSI, a verifier can verify a verifiable credential issued by a different country. For instance, cheese produced in Cyprus is verifiable by a customer in Germany, or a seafood company in Norway can verify the origin of olive oil produced in Italy.

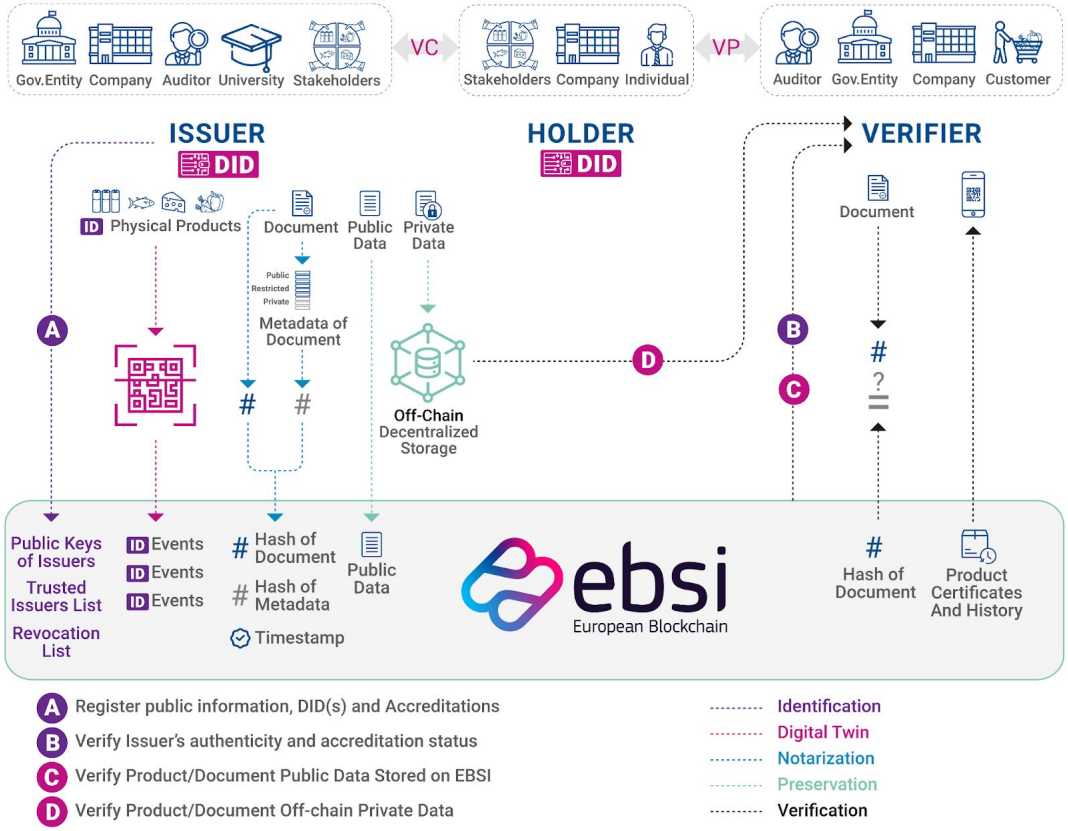


Figure 2 High-level architecture of the TRACE4EU traceability use case

2.1.2 TRACE4EU Value Proposition

TRACE4EU project is exploiting the existing EBSI services while also bringing additional components to enable preservation services that fulfill the long-term preservation requirement between two to thirty years[4] in the EU member states. The project aims to achieve this by creating an umbrella architecture and deploying services that will serve multiple application scenarios for the traceability use case, including the existing EBSI use cases such as Diplomas. To this extent, TRACE4EU is completing the current EBSI services to enable traceability use cases in regulated domains such as legal documents and electronic identification. With this extension, it will be possible

[4] EC Document management and archival policy: https://ec.europa.eu/info/about-european-commission/service-standards-and-principles/transparency/freedom-information/access-documents/information-and-document-management/archival-policy/document-management-and-archival-policy_en

to use verifiable credentials or ERC-721 for legal documents and transactions between citizens, businesses, and public authorities.
The utilization of verifiable credentials and ERC-721 tokens with the combination of preservation services opens a wide variety of application scenarios. In addition to the umbrella architecture and deployment of additional services, the TRACE4EU project is proposing to implement nine application scenarios categorized in two application domains:
a) ***Traceability of Products and Materials*** addresses the traceability requirements of physical products. Physical (pre-)products and materials are shipped and processed in factories and manufacturing plants until the end products reach the consumer. The traceability of products and materials application scenarios enables tracking products of each step in the supply chain.
As a first step, all actors in the supply chain need to apply for an identity credential from a trusted identity provider such as the GS1 or the Global Legal Entity Identity Foundation (GLEIF). Identity credentials are stored in the company wallet as verifiable credentials. Then various supply chain actors are inspected by Auditors for compliance, e.g., mines are checked on ESG/Responsible Mining criteria, or companies that process Norwegian fish outside of Norway need to be checked to receive a 'Seafood from Norway' certification. Auditors then issue the corresponding certifications as verifiable credentials to the mine or the fish processor, which keep those in their wallet. A holder can present verifiable credentials to comply with a ministry or verify the end customers' proof of origin. Such product and material certifications must be preserved for a specific time, different for each product category. Figure 3 presents the application domain of traceability of products and materials on a high level.

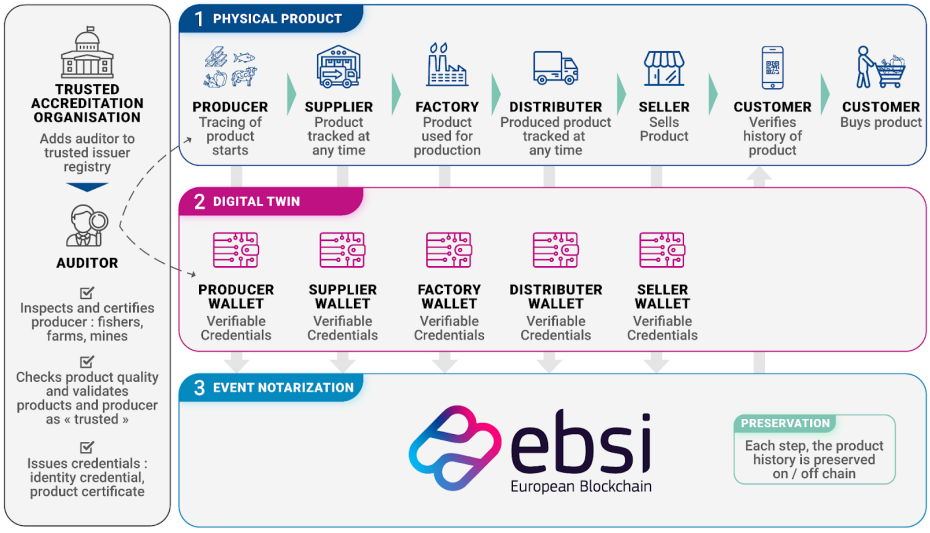


Figure 3 Application domain - Traceability of Products and Materials

b) ***Traceability of Data and Documents*** addresses the traceability requirements of physical and digital-native documents. These documents are bound to a physical person or a legal entity. For instance, digital documents can be certifications and credentials a person collects over time or digital rights belonging to organizations. The *traceability of data and documents* domain enables required conditions for archiving up to thirty years after the creation by the issuing parties. Figure 4 depicts the t*raceability of data and documents* domain on a high level.

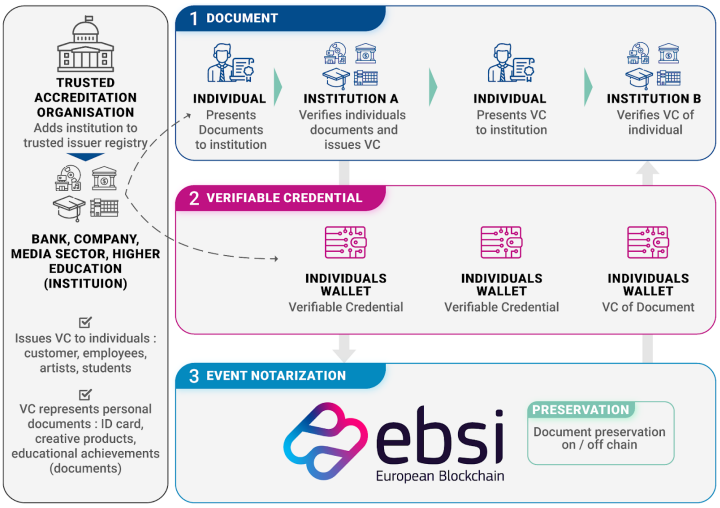


Figure 4 Application domain - Traceability of Documents

The presented application scenarios will be tested for conformity with existing regulations and standards such as eIDAS and TS 119 511. They are also to be tested with legal entities, natural persons, and end users in a cross-border environment to ensure there is no fragmentation and it complies with the requirements of participating EBP countries. Moreover, EBP representatives of the countries' trusted accredited organizations and trust service providers participating in the TRACE4EU project will support the application domains to foster in their corresponding countries, thus, enabling the rollout and scaling of the traceability use case across the participating countries. Each of the Application Scenarios will use the same layers to apply the developed umbrella architecture, which initial state has been determined by the consortium as follows (a subject to change during the requirements analysis and project execution).
The following information and requirements will be collected from each application scenario:

- Type of data
- Metadata
- Protocol used
- Interoperability required
- DID
- APIs and integration
- Scenario-specific requirements
- Piloting country-specific requirements

To collect the relevant information and requirements, TRACE4EU, directly through participation or indirectly through a Letter of Support, secured all relevant public bodies responsible for and interested in shaping the respective scenarios. As a result, each application scenario has a similar structure, size, and potential for a larger rollout and EU-wide applicability. Furthermore, the application scenarios will be interoperable and cross-border useable.

2.1.3 Maturity of the TRACE4EU Project Partners

TRACE4EU consortium comprises 34 companies and organizations from both public and private sectors from 13 EBP countries. Some companies and organizations have participated in EBSI early adopters waves 1 and 2 since 2018. Moreover, a part of the consortium has participated in both EBSI early adopters wave one and wave two programs, where they worked on creating and deploying EBSI conformant wallets and implementing cross-border diplomas use cases. Germany-NRW, CY-EBSI, EBSILUX, UniCert, and EBSI4Austria are the projects that the TRACE4EU partners have contributed to in the early adopter programs. Moreover, founding partners of eSSIF are also a part of the TRACE4EU consortium.
TRACE4EU partners also bring relevant experience outside the EBSI and eSSIF programs. For instance, TRACE4EU partners have participated in NGI eSSIF-Lab and DAPSI open call projects. In addition, several Horizon Europe projects, such as the KRAKEN data marketplace for personal data, and IMPULSE improvement of electronic identities with blockchain and artificial intelligence, are personal data-related projects that our project partners participate in or have participated in. TRACE4EU consortium brings know-how and competence in (blockchain-based) traceability of products and materials from Horizon Europe projects. For instance, one partner is engaged in the Horizon project FARM2FORK, a holistic approach for tackling food systems and risks and national projects in the digitization of meat production.
The technical competencies of the TRACE4EU project partners are also diverse. The consortium comprises companies that bring competencies in copyright management, blockchain in media & entertainment, legal transactions in digital environments, trusted services for electronic identification and digital transactions, agricultural and seafood, and electronic components such as batteries. Moreover, companies and organizations in the TRACE4EU project bring decades of combined experience in the self-sovereign identity paradigm in national and international European projects. Lastly, our partners specialize in the interoperability of self-sovereign identities and digital certificates, where they contribute to the standardization of the SSI technology stack and preservation services.
The TRACE4EU consortium brings project management and steering competencies to ensure that the proposed project will be executed and appropriately finalized. Furthermore, the implementation of the proposed project is secured by the competencies in software development and deployment with CI/CD and agile approaches of the project partners. Finally, our project partners bring competencies in the deployment, rollout, and scalability of products and services in multi-national parallel deployment environments. With this technological know-how and competencies in required fields to achieve successful project execution and rollout, as well as the technology readiness level of the deployed technology and the current status of EBSI, TRACE4EU is ready to execute the project and start implementing the proposed activities.

2.2 Implementation plan and efficient use of resources

Implementation plan

Show that the implementation work plan is sound by explaining the rationale behind the proposed work packages and how they contribute to achieve the objectives of the project.

Explain the coherence between the objectives, activities, planned resources and project management processes.

Show how the project integrates, builds on and follows up on any pre-existing work or EU funded projects. Provide details (including architecture and deliverables) about pre-existing technical solutions.

Standardized and open infrastructure is crucial for incentivizing parties to participate and build their solutions based on it. For this purpose, European Blockchain Services Infrastructure (EBSI) has been created in Europe. The EBSI is a blockchain network of distributed nodes across the EBP countries to provide support for vital applications. Online exchange of documents is de facto challenging to verify the integrity of the documents[5].
The availability of following nodes is currently planned for the TRACE4EU project:

- Germany − 2 nodes (HAW and one new node)
- Norway − 1 node
- Croatia – 1 node
- Slovenia – 1 node
- Estonia – 1 node
- Hungary – 1 node
- Luxembourg – 1 node
- Cyprus – 1 node
- Greece – 2 nodes (GRNET and CERTH)

To reduce the cost and time of validation of documents, the EBSI was developed by 29 countries in 2018[6]. EBSI currently supports cross-border services for four use cases:

- Identity (SSI)
- Diploma
- Social Security
- Document Traceability

Document traceability use case is the backbone of the other EBSI use cases. All other EBSI use cases depend on trusted digital audit trails, automated compliance, and certificate checks to prove data integrity[7] that comes with traceability. TRACE4EU will enhance the document traceability use case of EBSI with a tailored umbrella architecture. The umbrella architecture will be aligned with existing EBSI components, enabling additional (new) traceability components and services. TRACE4EU develops components and services based on defined application scenarios.
Furthermore, TRACE4EU results will be open-source and have no vendor lock-in mechanisms. Therefore, the traceability architecture is available for any interested party. The TRACE4EU consortium includes EBP members who will demonstrate future results of the application scenarios throughout Europe. With the demonstration of application scenarios, TRACE4EU aims to attract other interested parties from EBP countries to adopt the solution during and after project execution. Another focus of TRACE4EU is the interoperability of the umbrella architecture, as it is the most important requirement for traceability across European countries. Table 1 presents the requirements and corresponding descriptions to achieve the mentioned goals.

Table 1 TRACE4EU project requirements and corresponding description

Requirement	Description
Integrity	Documents need to be checked for integrity. Integrity is the first requirement for the traceability use case. Math and cryptography methods ensure that documents have not been tampered with after initial creation with the issuers' signature.
Persistence	Documents and material traceability data (data) should be persistent and validatable for decades. Depending on the use case and regulation, up to thirty years of validating ability is reasonable to expect. For this reason, a service that utilizes the building stones of EBSI shall be necessary to preserve the data and make it available over extended periods.

[5] What is EBSI: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi
[6] EBSI: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home
[7] EBSI Use Cases: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Use+cases#anchor-ebsi-use cases

Avoidance of Vendor Lock-In	The architecture shall avoid using technology that locks other providers and end users to specific software.
Interoperability	The architecture components not part of EBSI will be created and designed interoperable.
Portability	Data shall be stored in the medium of choice of the data owner. Furthermore, data should be portable to any other medium of choice of the data owner if required. This requirement is essential for the traceability of documents where data belongs to an end user who might change the storage medium (i.e., smartphone) every couple of years.
Verifiability	The origins of data shall be verifiable. Therefore, issuer instances shall be traceable to a trust anchor. Furthermore, the authorization of the issuer instance shall be verifiable as well. For example, Issuer A issues a resume credential. Not only must the data be cryptographically verifiable, but there shall also be a trace to the issuer's authorization for issuing resume credentials.
Tracking of events	The occurrence of the event of data creation shall be traceable (notarization) through an accepted and verifiable trust anchor. Verifiability of the events can be achieved only via a tamper-proof trust anchor.
Cybersecurity	The architecture and the interactions between the entities shall fulfill some of the information security properties. Issuer and Holder authentication: The Issuer and Holder shall be authenticated by cryptographic and optionally legal means.
Message privacy	The exchanged data shall not be publicly available, only to the sender and recipient.
Proof privacy	Proofs of data shall not be publicly available to the sender and recipient.

2.2.1 High-level Architecture

The requirements from the various application domains of traceability results in the High-level architecture of TRACE4EU, as shown in Figure 5. The architecture consists of four building blocks and also indicates the traceability flow. The sorted blocks of Figure 5 represent the traceability process steps beginning with the lowest block Identification. The first traceability process is *identification*, and the last is *preservation*. The blocks consist of the required components for the process step of traceability.

Identification: Identifying issuers, persons, and things is essential. Hence, the first building block of the TRACE4EU architecture contains the components required for identifying entities.
Identification is essential for the following reasons:

- Strengthen trust between the issuer, holder, and verifier. Identification enables cryptographically secure communication channels between entities, such as DIDComm or SIOP. Through such channels, entities can securely exchange information while fulfilling information security properties such as authenticity, integrity, and confidentiality.
- Enable adding an identity to a certificate.

Identification of an entity can be bound to a verifiable credential (certificate). In the case of traceable documents and materials, the roles of the issuer, holder, and verifier are called trusted parties in this chapter. Depending on the application scenario, trusted parties either add value or provide goods and services to the product in the value chain. Parties require trust in identification and authorization to each other. Trust between parties is an essential requirement for authentic credentials. Trust to verifiable credentials is necessary to address whether another party is authentic related to issued and presented credentials.

Digital Twin: Digital twin categories are as follows:

- The digital twin of products and materials: Digital product passports for batteries (battery passports), textiles, buildings, and electronics that contain product components, materials, certifications, and proof of products' origin are examples of this digital twin category.
- The digital twin of entities: Entities getting certified claims, such as credentials about related attributes, also known as the traceability of data and documents. The creation of a digital twin involves a third party issuing verifiable documents that contain claims about a subject, such as natural persons or legal entities. It can affect the creation of a digital copy of a physical document such as upper secondary school diplomas, or it can be a digital-native document such as e-Learning certificates.

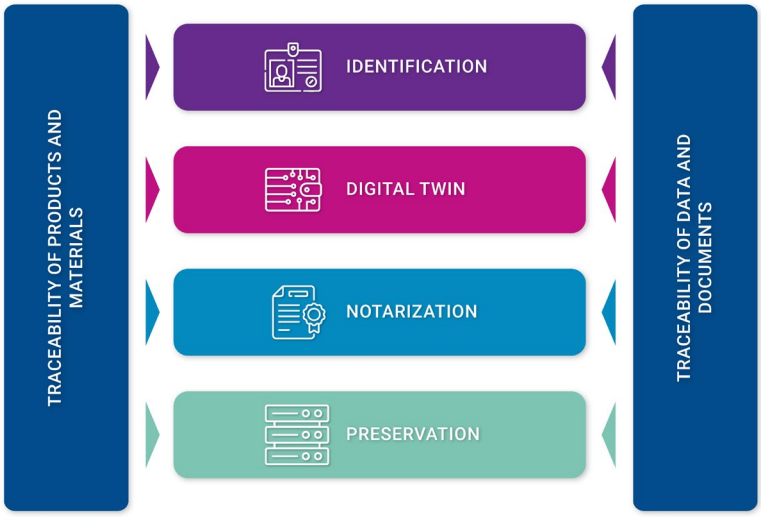


Figure 5 High-level architecture of TRACE4EU

An authorized and identified issuer will create a digital, verifiable credential in both mentioned categories. Verifiable credentials are cryptographically verifiable and tamper-resistant. Furthermore, the holder decides the medium of choice to store a digital twin. The holder can be an owner of materials and goods or documents.

Notarization: TRACE4EU addresses notarization as the verifiable tracking of events. Notarization in TRACE4EU is not about a trusted third-party notarizing documents for broader acceptance and higher assurance. The architecture of TRACE4EU provides the creation timestamp used to notarize digital twins. Digital twins will be verifiable through cryptography and an accepted source of truth. Each time a digital twin will be created or modified; a notarization is carried out to the EBSI ledger. Notarization events will be noted in the credential so the relying party can check when the creation event happened.

Preservation: Traceability of products and documents can have high demand on how long the data shall be validatable. For instance, depending on the state, an upper secondary school diploma must be validatable between 30 to 50 years in Germany. Furthermore, parts for the automotive industry (i.e., car batteries) also have high demands. Therefore, long-term validation ability is equally important for the traceability of products. For this purpose, a long-term preservation service is required to fulfil the traceability requirements of specific use cases.

2.2.2 TRACE4EU Application Scenarios

The following **nine application scenarios** describe the planned cross-border implementations of TRACE4EU:

Seafood: The Seafood scenario enables global traceability of seafood products. It allows the creation, holding, and verifying of digital twins for all actors in a supply chain. Digital twins represent claims of any seafood asset. Claims of a digital twin could be the location or the timestamp of caught fish. A public blockchain allows proving the processes and environments of the seafood asset, traveling throughout the supply chain.
The Seafood scenario fulfills and extends the following supply chain requirements:

- Traceability – Optimizing transparency of origin and transport of seafood products
- Sustainability – Improvement of ecological (transport) processes and food safety
- Circular economy - Development and expansion of recirculation of packaging and biomaterials.

Unique value proposition: Norway exported 3.1 million tonnes of seafood worth NOK 120.8 billion in 2021. Many of the seafood is exported to EU member states. Many stakeholders are involved in seafood catching or farming, processing, transportation, and trading. Currently, the seafood supply chain stakeholders do not share data often, a specific industry with data silo issues. Without sufficient traceability of the supply chain and data transparency, it is challenging for authorities to monitor the responsible production and processing in the seafood supply chain, which may lead to food safety issues. Without traceability of the seafood supply chain, addressing illegal fishing and cheating in seafood trading is challenging.

Positive impact: Full traceability will help authorities monitor and manage the seafood supply chain, ensure consumers' food safety, and regulate and encourage all stakeholders to perform responsible seafood production and processing.

Relevance to all European countries: The use case is relevant to many EU countries, such as Spain, The Netherlands, and Sweden (Iceland EAA), producing and exporting seafood to other EU countries worldwide. The use case is also relevant to all EU citizens. Full traceability of the seafood will provide them with better information about the quality of the food to ensure food safety and fair price.

In order to support the Seafood Use Case on the regulatory and implementation level, several partners from Norwegian side will be participating in the respective Use Case, specifically in the Work Package 4. The NArch (The National Archives of Norway), DFO and NDA will be covering the data delivery, data validation, regulatory topics in the Associated Partner role.

Agri-food: The Agri-food scenario aims to create blockchain-based tracking of data exchange between food producers and raw food material processors.
The Agri-food scenario emerges from two real challenges in Hungary:

- Insufficient amount data about the exact. Verifiable information about the amount, quality, and precise details of the location of the original harvest is almost non-existent.
- Complex planning for kindergarten and school catering.

Blockchain-based solutions for traceability will enable better supply chains and better consumer information about food quality. Hungary will have a use case pilot environment with the producers' digital market.

Unique value proposition: Creating blockchain-based tracking of data exchange between food producers and raw food material processors will result in more secure and valid data, enabling better supply chains and better consumer information.

Positive impact: The use case outcomes will impact consumer confidence, increasing the production of healthy food of high nutritional value raw materials. Validated data can be processed by artificial intelligence or machine learning or be a data-trading subject.

Relevance to all European countries: Short food supply chains are operational in every Member State, and assisting these with blockchain technology could improve both quality and safety. Food-chain safety is a highly harmonized area in the EU.

UVMB will support the consortium as Associated Partner and contribute to the WP4, specifically to the Agri-food Use Case, during the proejct lifetime, with its' extensive knowledge and previous project experience in the field.

Battery: The Battery scenario covers the tracing of metals to fulfill the "new Battery Regulation" requirements for responsible mining of battery raw materials. Mining companies need mining certificates such as IRMA or TüV (Cera 4in1). In the battery scenario, verifiable credentials represent digital mining certificates. Trusted Organizations issue verifiable credentials to mining companies' digital identity wallets. A certificate in the form of a verifiable credential allows mining companies to present trustworthy, digital mining certificates to institutions, such as governments. Institutions verify digital mining certificates with cryptographic algorithms and EBSI. Such "proof or origin use cases" are a general requirement of the digital product passport that is now also regulated in

the Ecodesign for Sustainable products directive for other product categories, such as buildings, electronics, and textiles.
For the most part, batteries consist of critical raw materials, such as cobalt, graphite, gold, and lithium. Critical raw materials are often subject to a negative environmental and social impact. For European companies it is thus essential that their raw material is traced from the origin to the final product, so that they can comply with ESG requirements (stated by various EU regulations, such as the new Battery Regulation, the Supply Chain Due Diligence Act, and the upcoming Critical Raw Materials Act. In the project we will work with actors along the raw materials supply chain, to establish a chain of custody from the origin to the manufactured product. Supply chain actors will provide evidence about their custody of the material, such as invoices, bills of delivery, etc. Those documents will be issued as verifiable credentials and create the basis for a closed-loop material traceability.

Halloumi: EU geographical indication schemes protect specific know-how, authenticity, and agro-environmental conditions. The European Commission approved the protection of Halloumi as a protected designation of origin (PDO), covering the valuable name against imitation and misuse across the EU. Only Χαλλούμι/Halloumi/Hellim produced in Cyprus according to the product specification is now allowed to use the registered name. The implementation of the Halloumi will be based on using EBSI capabilities and APIs (current and new/enhanced), utilizing case-agnostic data schemas. The Halloumi scenario will demonstrate EBSIs' ability to provide effectively, trusted, digitalized, and automated services to safeguard PDO and PGI registered EU products.

Unique value proposition: The Halloumi model's successful application will demonstrate that EBSI technology can provide an effective, trusted, digitalized, and automated service/solution to safeguard PDO and PGI registered EU products. EU geographical indication schemes protect specific know-how, authenticity, and agro-environmental conditions. The EC registered Halloumi as a protected designation of origin (PDO), protecting the valuable name against imitation and misuse across the EU. Only Χαλλούμι/Halloumi/Hellim produced in Cyprus according to the product specification is now allowed to use the registered name. The implementation of this Use Case application scenario will be based on using EBSI capabilities and APIs (current and new/enhanced), utilizing case-agnostic data schemas.

Positive impact: The main objective is to provide a digital mechanism that provides trusted means to (a) the professionals associated with the Halloumi production and supply chain for verification, monitoring, and tracing, and (b) the consumer who, being the end-user, would be able to identify/verify that what he/she gets from the market shelf is what he wants and pays for, i.e. a genuine PDO Halloumi cheese. Once implemented, this will protect both the Producer's investment (the industry) and the consumer's interest and rights across the EU. Halloumi export accounts for EUR 220m (the year 2020) while the local consumption in Cyprus reaches EUR 120m (2020), projecting several consumers above 3 million EU citizens. Consequently, the market potential of this application/system is significant, considering all EU PDO/PGI products that may adopt and capitalize on this solution.

Relevance to all European countries: Because of the globalization of the food supply chain and the free movement of goods, interest in detecting adulteration in food has increased. For authentication, a combination of analytical methods is mainly used in detecting minor differences in the botanical/ geographical origin and adulteration in sample traces. The Application development aims to directly address the harmonization of a trusted authenticity tracing digital mechanism applicable for any European PDO products by engaging blockchain/DLT (EBSI) technologies. This will be demonstrated via the Halloumi PDO Application Scenario. The Application will be developed based on a product-agnostic design structure; its backbone will have an adaptable and generic core structure, customizable to any EU PDO and PGI registered products.

Open Rights Data Exchange: The Open Rights Data Exchange scenario, led by DIGICITI and VALUNODE, enables the monetization of digital assets through trusted rights data. VALUNODE is building an Open Rights Data Exchange, a data intermediation service regulated by the Data Governance Act.
The unique value propositions of services to holders (rights holders):

- Easy and incentivized attestation of machine-readable rights data, as well as curation, deduplication, and matching of rights data.
- Real-time access to reliable, exhaustive, current, and interoperable rights data, as well as auditable provenance and authenticity of rights data.

The Open Rights Data Exchange scenario and VALUNODE are opting for decentralized storage of rights data and storing immutable bindings between contents and declarers on EBSI. Digital bindings point to public metadata stored on IPFS, the latter addressing private metadata stored locally.

Résumé Credentials: The Résumé credentials scenario aims to establish and improve verifiable credentials of professional experiences using EBSI. Citizens must ask employees to issue an employer reference and keep paper records of their (professional) experience. Companies face the challenge of verifying the authenticity of applicants' professional experiences as manual verification is time-consuming. Furthermore, information from

applicants about professional experience could be fraudulent. The résumé credentials scenario covers cross-border and interoperable applications for governments, companies, and citizens. Additionally, the developing phase considers the long-term preservation of credentials. Résumé credentials such as upper secondary school diplomas require up to 50 years of long-term preservation. Talao will support Resume Credential through their wallet and technology which is close to eIDAS 2.0 and ARF but also EBSI and so supports legally compliant resume credentials for TRACE4EU.

Decentralized Academic Publishing: The Decentralized Academic Publishing scenario covers Open science with increasing numbers and timely publications.
The requirements for academic publications to modern platforms are:

- Secure publication of scientific papers.
- Trustworthy publication processes
- Fast transactions between author and platform

The Decentralized Academic Publishing scenario aims to enrich and extend EBSI services for sharing, storing, and securing transactions in the academic publishing process. Further goals of the Decentralized Academic Publishing scenario are to increase the quality of peer review involving academic integrity, publication bias, and fraud from increased pressure to publish while building a decentralized ecosystem for publishing and reviewing scientific papers.

SDURDD from the Croatian side will contribute as Associared Partner to the WP5 with the overall governmental support and necessary information on the current legislation to provide the interoperability of the solution for Croatia and thus supporting it's successful rollout.

Electronic Registered Delivery: The electronically registered delivery scenario covers digital processes for paper-based registered mail. The scenario is based on the use case of receipts of sending. The project proposes an implementation able to notarize receipts on EBSI. Furthermore, the design aligns with ISO/AWI 19636-3 "Processes, data elements, and documents in commerce, industry, and administrations." Trusted communication platforms for electronic documents - Part 3: blockchain-based implementation guidelines (work in progress) and discussed in ETSI.

KYC Tool: The KYC Tool scenatio covers EU citizens submitting their KYC (Know Your Customer) documents to banks and other institutions. The scenario considers any EU country that requires identifying customers. KYC processes are constantly repeating. A new customer opens an account or requests new financial services. Maintaining personal details is necessary every 2-3 years. The KYC Tool scenario will simplify the KYC process and reduce customer time-consuming and cost-intense identification. New services for KYC processes will extend the EBSI, and services will be integrated and extended. The proposed KYC scenario aligns with GDPR requirements.

2.2.3 Alignment with and Extension of EBSI services

TRACE4EUs' architecture defines nine application scenarios that utilize four building blocks.
The first building block **identification** of legal entities, things, and persons uses DIDs and DID documents. Therefore, the identification building block consists of the existing EBSI core services such as DID Authentication and Wallet Libraries and DID Registry, Ledger, Authorization, and User Onboarding APIs. These APIs interact with the lower EBSI layers and the components such as DID registry in the Ethereum Smart Contract cluster. In addition to the existing services, Moreover, depending on the requirement analysis and the initial architectural design, TRACE4EU will deploy additional services for supporting fungible and non-fungible token contracts and oracle services. The second step of the traceability use case consists of creating verifiable credentials for a **digital twin**. Digital twins are verifiable credentials of a product, material, data, or document. EBSI core services such as Verifiable Credential and the Wallet Libraries will be utilized by developed services. TRACE4EU will bring EBSI to conform wallets to store the issued verifiable credentials off-chain with the product's owner (holder), material, data, or document. The EBSI is complete for verifying verifiable credentials, including the exchange protocols and message envelope. Missing services will be designed and developed. Creating a digital twin triggers notarization events on the EBSI ledger by storing the hash of the verifiable credential with a timestamp. The timestamping services of the EBSI serve as **notarization** services. In the creation process of digital twins, an issuer signs a verifiable credential containing a claim of creation timestamp. A timestamp is noted through the event notarization to a verifiable credential. Timestamping of credentials enables the verifier to prove the authenticity of credentials by verifying the timestamp at a time in a trustful manner. The tamper-resistance property of EBSI increases the trust of digital twins. Furthermore, the event entry cannot be tampered with unless a rehashing of the event. The notarization building block exploits the timestamp API of the EBSI core services.

The final step of the traceability use case is **preservation**. Depending on the application scenario and the EBP country's preservation regulations, the following requirements arise:

- Long-term preservation of product credentials, materials, data, or documents for up to thirty years. EBSI is a long-term trust anchor as the stored data is available in a distributed manner.
- Stopping nodes need to notify all other nodes, as all nodes contain the exact copy of the data.
- Preservation and availability of data. Issuing and verifying of credentials, even when signature algorithms changed over time.
- Post-quantum security. Current DLT are not post-quantum secure (cf. DIN/TS 31648) as it requires additional steps such as re-hashing the stored information with a post-quantum secure hashing algorithm.

TRACE4EU proposes long-term preservation services conforming with the eIDAS regulation and the specifications and guidelines such as DIN/TS 31648 and ETSI TS 119 511. TRACE4EU designs, implements, and coordinates new preservation services with the EBSI core team. TRACE4EU preservation services will be integrated into the EBSI core or as additional services. Figure 6 visualizes the architecture of TRACE4EU and its building blocks mapped to the existing EBSI architecture. Figure 6 also shows the added application scenarios and services by TRACE4EU.

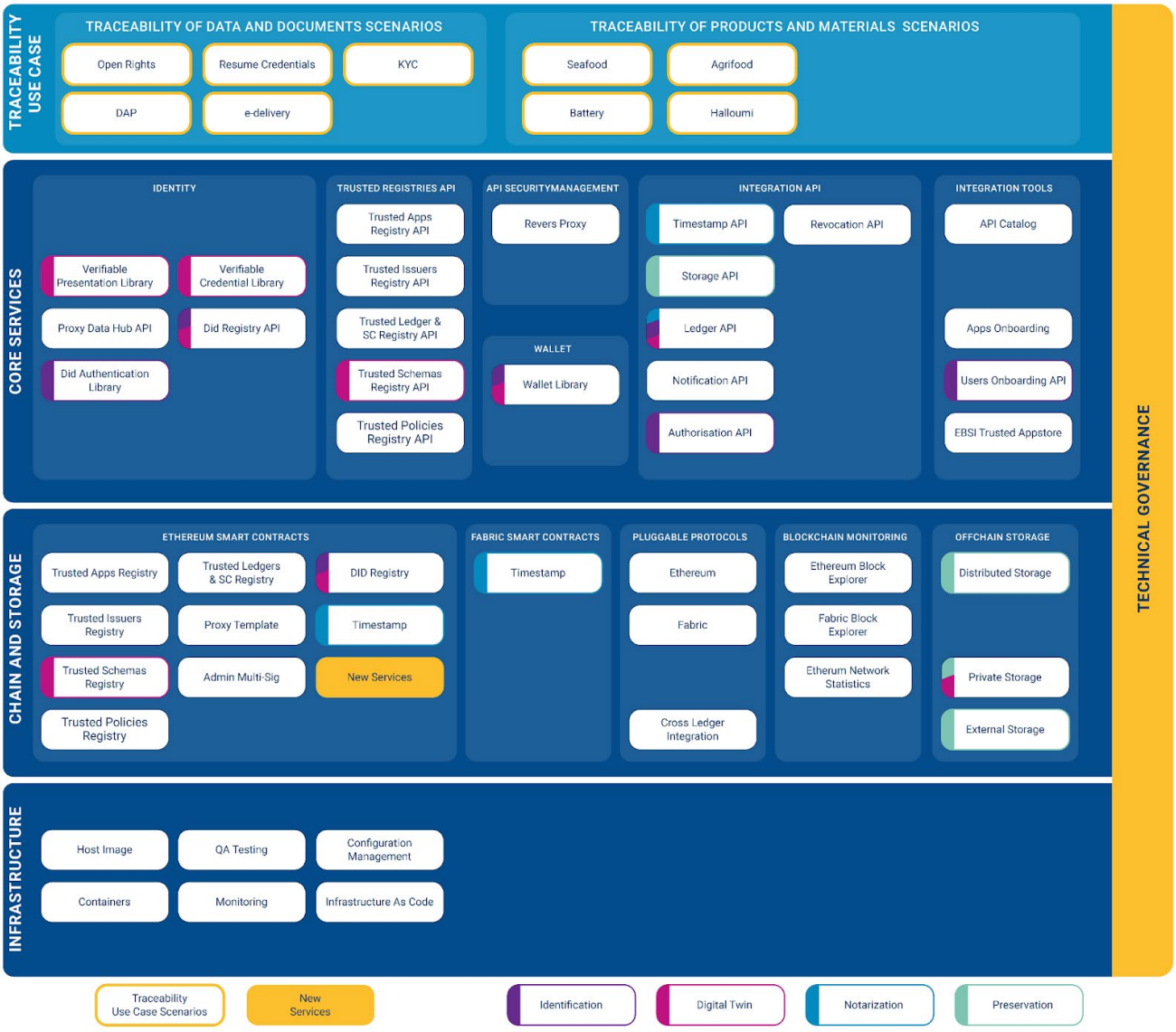


Figure 6 TRACE4EU architecture and application scenarios

2.2.4 Project Structure

TRACE4EU is based on a Work Breakdown Structure (WBS) to reach the objectives and deliverables. Figure 7 shows the evolved WBS in cooperation with the project partners. Deliverables of the working packages are described in the milestones of the WPs in this proposal.

Description of WBS, presented in Figure 7, beginning at the top:

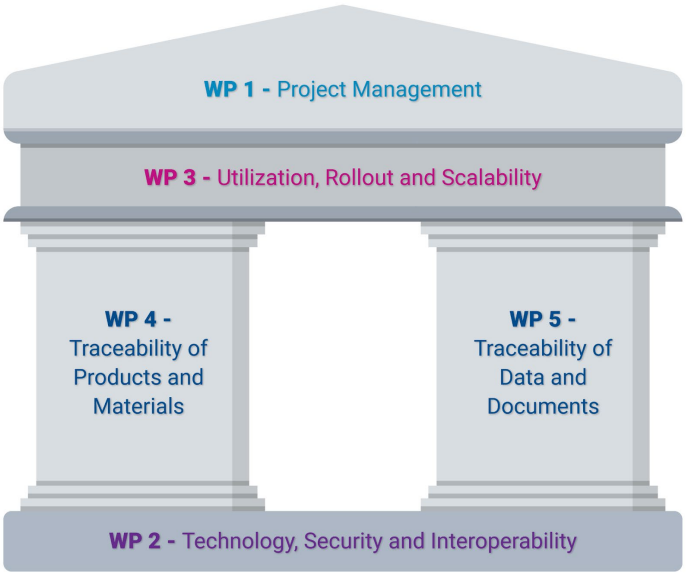


Figure 7 TRACE4EU working package structure

WP1 covers the general TRACE4EU project coordination at the governance and project level. Furthermore, it describes tasks coordinating application scenarios.

WP3 focuses on the utilization, scalability, rollout, and communication of the developed services and software. WP3 coordinates the development activities with the EBSI core team and other external projects and networks. Furthermore, the partners in the WP3 bring their competencies to create a strategy for the rollout of the application scenarios in a scalable manner across multiple EBP countries simultaneously.

WP4 and WP5 represent the two pillars of TRACE4EU containing all relevant tasks for traceability of products and materials and data and documents. In WP4 and WP5, the partners will work on the piloting, implementation, user engagement, and user communication for each application scenario of the TRACE4EU project.

WP2 covers the foundations of the project: The design of an umbrella architecture to foster the traceability use case and its application domains and scenarios. WP2 covers implementing and testing activities, including utilizing existing EBSI services and deploying new ones. Moreover, WP2 will analyze the legislation conformity, cybersecurity, and privacy to improve the overall architecture and implementation.

Analyzing: The legislation, cybersecurity, and privacy analysis results are equally relevant and essential. The legislation conformity analysis's initial results will influence the architecture and implementation of TRACE4EU. TRACE4EU considers legislative changes of the EU during project runtime, such as the introduction of eIDAS 2.0. Regulation changes by the EU imply modification of TRACE4EU architectural design. Furthermore, the TRACE4EU architecture design includes cybersecurity and privacy aspects of services and software.

Developing: TRACE4EU follows a customer-centric approach to developing the architecture, services, and software. The first and foremost part of this approach is understanding the customers, designing a user journey that will fit the customers, and improving the offered services by continuous and iterative development. Throughout the development period, constant user feedback via interviews and testing will flow back to the TRACE4EU software and services development roadmap. All WPs will consider user feedback for recommendations for further developments of EBSI services. The development of the umbrella architecture and implementation starts with the definition of target user groups that potentially uses the TRACE4EU services and software. TRACE4EU partners will interview users of the target groups to understand the requirements of those user groups. Based on retrieved users' feedback, user journeys will be created and specified as epics. Defined epics will be distributed to suitable WPs. Within the WPs, epics will result in user stories containing tasks, acceptance criteria, and functional requirements. Finally, the development teams will work on actualizing the user stories and implementing functional requirements in iterative releases throughout the project runtime (Release 1, 2, 3, and commercial release).

Testing: In parallel to the tasks related to architecture design and implementation, TRACE4EU strongly focuses on testing. The partners will build on their experience working in standardization communities such as W3C and DIF. W3C and DIF provide numerous tests for building blocks such as DIDs and VCs.

In general, TRACE4EU work according to the following two principles for testing:

- Implementations developed by TRACE4EU will be tested for conformance with a specification and interoperability with other implementations.
- Learnings and insights from the testing process flow into the specification and technical architecture work.

To comply with the principles, all WPs interact closely with testing implementations and processes. Furthermore, benchmarks and plugfest will support the testing efforts of TRACE4EU.

Deployment of new Services: In addition to exploiting the existing EBSI services, TRACE4EU will deploy new services supporting long-term preservation compliant with eIDAS. Furthermore, TRACE4EU will enable an interoperable environment with Trust Service Providers (TSPs). For specific scenarios, the integration of TSP,

such as Infocert, promotes regulated use cases such as qualified electronic signatures and seals for legal documents based on EBSI core services and aligned with EU regulations, such as eIDAS.
Deployment of Verifiable Credentials with Qualified Electronic Signatures and Seals: The main challenges with Qualified Electronic Signatures and Seals are currently the lack of regulatory bindingness of the Verifiable Data Models model with DID, the Verifiable Credentials, and the digital signatures used. These do not meet the requirements of the eIDAS Regulation. The eIDAS Regulation only recognizes PAdES (for PDF), CAdES (for CMS), and XAdES (for XML) as qualified electronic signatures and seals. The EU is solving this challenge through the eIDAS Bridge, whereby digital proofs provide (qualified) electronic signatures or seals by eIDAS and the three advanced electronic signature specifications mentioned above. The foreseeable eIDAS 2.0 could result in changes in this context and recognize JAdES as a specification conforming to a qualified electronic signature or seal. TRACE4EU consortium considers a legislative conformance analysis by designing the umbrella architecture.
Deployment of Wallets: Verifiable credentials containing qualified electronic signatures and seals require an additional signature generation and validation utilizing the eIDAS Bridge during the issuance and verification. The extra steps for using the eIDAS Bridge need off-chain storage options that conform with EBSI. TRACE4EU will deploy wallets that fulfill off-chain storage and eIDAS bridge integration for the product, material, data, and document owners.
Deployment of Issuer and Verifier Agents: The realization of scenarios depends on covering each phase of the credential life-cycle. In the first phase, a credential is issued to the product owner. Issuing a credential requires the deployment of an issuer agent capable of communicating with the owners' wallet and new or existing EBSI services. The exact requirements count for the verifier. Verifier needs an agent to verify the authenticity of presented credentials from a credential owner. TRACE4EU will showcase the scenarios in cross-border environments.
Interoperability: Interoperability with non-EBSI platforms and systems is an essential factor for the adoption and success of the proposed project. Furthermore, it might be necessary to support additional protocols and services such as qualified Time Stamp Authorities to generate qualified electronic timestamps. Therefore, TRACE4EU focuses on interoperability with private sector platforms, protocols, and services. The results will flow back to the TRACE4EU architecture design and service development for EU-wide adoption.

In order to deliver the technological, but also the regulatory interoperability, TRACE4EU has included partners with innovative technological solutions like MINECHAIN and AltMe, participating as Associated Partners with limited capacities in WP2, but also governmental organizations like FNDMT and INCM which will secure the project results' interoperability with regulatory expectations and contribute mostly in the WP3.

2.2.5 Additional Technologies

Advanced Robust Hashes: Actions of end users of EBSI services should be non-repudiation to achieve security. Therefore, assuring personal data privacy is crucial. Preference measures for users' privacy concerns are implemented in technical research under the keyword of k-anonymity. The trade-off between privacy and system functionality covers differential privacy, which allows precise information about shared data sets without limiting privacy. TRACE4EU uses advanced robust hashes to study the feasibility of the trade-off.
Zero-knowledge Proofs: Zero-knowledge Proofs ensure the privacy of holders' data for verifiable presentations. TRACE4EU will study if Zero-knowledge Proofs increase the privacy and security of EBSI services in the projects' application scenarios. An overview and comparison of proof algorithms that are complete, reliable, performant, and easy to implement will be created.

Project management, quality assurance and monitoring and evaluation strategy

Describe the measures planned to ensure that the project implementation is of high quality and completed in time.

Describe the methods to ensure good quality of monitoring, planning and control activities.

Describe the evaluation methods and indicators (quantitative and qualitative) to monitor and verify the outreach and coverage of the activities and results. The indicators proposed to measure progress should be specific, measurable, achievable, relevant and time-bound.

Project management: The project management in TRACE4EU follows the PRINCE2 Agile Methodology with all advantages of combining classic project management with agile elements. TRACE4EU uses modern communication and project management tools like Slack and Asana. The tools ensure optimal digital cooperation and transparent and continuous information flows between participants about the projects' current state. Furthermore, Git and Confluence enable high flexibility of iterative development processes. Both user feedback and the reference application of the Wallet will impact the iterative development and influence the project management model.
Reporting: The project reports will provide information on the scope, strategies, plans, schedule, effort/cost, and quality, as well as information related to the status of risks, issues, initiation requests, charters, checklists, progress, project changes, and outsourcing with the appropriate level of detail. Project reports will also be

recorded in the Project Management Plan. Project steering comprises representatives from various horizontal services to use, adapt and enhance applications during a set of large-scale pilots, procurement, and legal.
Project report elements are as follows:

- Project Management Plan
- Project Handbook
- Project Work Plan
- Communications Management Plan
- Project Logs
- Project Checklists
- Outputs of the Monitor Project Performance activity

Measures planned to ensure that the project implementation is of high quality: This section describes the quality controls and assurance measures to ensure the quality of developed services. Quality controls include activities needed to maintain a desired level of excellence. TRACE4EU considers quality planning, quality assurance, control, and improvement throughout the project until the closing phase and the final acceptance of the project. The objectives, approach, requirements, activities, metrics, and responsibilities are clearly defined and documented.
Monitor Project Performance: TRACE4EU collects information about the state of the project's progress and overall health. The essential information TRACE4EU records the following information of project dimensions: The scope, schedule, cost, quality, risk, issues, and project change. Furthermore, forecasting the evaluation to report the overall project progress is foreseen.
TRACE4EU utilizes a dashboard to monitor project performance. The dashboard complies with the PM² Methodology and consists of the following blocks:

- Control schedule
- Manage quality of information supplied to the contracting authority
- Manage deliverables acceptance
- Manage requirements
- Manage project changes
- Manage risk
- Manage issues and decisions

The TRACE4EU consortium sets **specific, measurable, achievable, and timebound KPIs** relevant to this call, covering both obligatory KPIs set by the European Commission and own KPIs relevant to the project for even more effective measurement of the project outcomes. It is essential to indicate that the KPIs do not represent the maximum for the project lifetime. TRACE4EU calculates the appropriate **minimum** amount for the project, and the consortium aims to increase the number during the project lifetime even further. Achieving each KPI is a direct responsibility of the respective WP Lead and is to be reported to the Consortium Lead and WP1, concentrating on the Project Coordination. Table 2 shows an excerpt of TRACE4EU deliverables with description and corresponding KPI. Table 3 shows KPIs for the application scenarios.

Table 2 Excerpt of TRACE4EU deliverables with description and corresponding KPI

Deliverables	Description	KPI
Nodes supporting the project	-	11
EBSI trainings	5 Partners do 2 trainings per year	20
Project presentations	-	15
Project-related publications	6 HEIs do 3-5 publications per year	10
Participating Member states in traceability use case	-	15
Application Scenarios	-	9
Estimated new EBSI-Nodes	-	10

Table 3 Application scenarios of TRACE4EU and corresponding KPI

Application Scenario	KPI: Organizations (End Users)
Seafood	4
Agri-food	6
Halloumi	20 (plus customer)
Batteries	6 (plus customer)
Open Rights Data Exchange	10
Resumé Credentials	10 (plus citizens)
Decentralized Academic Publishing	6 (plus further HEIs)
Electronic Registered Delivery	10
Know Your Customer	5 (plus customer)

Cost effectiveness and financial management *(n/a for prefixed Lump Sum Grants)*

Describe the measures adopted to ensure that the proposed results and objectives will be achieved in the most cost-effective way.

Indicate the arrangements adopted for the financial management of the project and, in particular, how the financial resources will be allocated and managed within the consortium.

⚠ *Do NOT compare and justify the costs of each work package, but summarize briefly why your budget is cost effective.*

Project resources have been budgeted based on the foreseen role and contribution for each participant and the necessary competencies. TRACE4EU is committed to cost-efficiency as it maximizes the project impact by using the established project budget.
The project is planned for 24 months, its total budget is 7,024.031,05 €. The total estimated effort is 896 person/month distributed in the 5 Work Packages. The major cost item in the project is the personnel costs. All partners have committed appropriate personnel resources from existing staff as well as additional staff to be recruited to undertake the project. The total personnel cost has been calculated based on person-months agreed to be allocated to the project by the partners and the corresponding average person-month rates for each of the partners.
The focus and priorities of the TRACE4EU project are reflected in the budget distribution for the different WP's. the largest part of the budget is allocated in the WP2 which will develop the overall architectural solution (WP1 4,7%, WP 2 35,8%, WP3 11,8%, WP4 23,3%, WP5: 24,4%).
Before the submission, the project cost effectiveness has been optimized in 2 steps: by Work Package Leads and by the Consortium Management. Throughout the project lifetime, the costs submitted by each participant will be regularly controlled in the same way: by the Work Package Lead and then by the Consortium Management on the quarterly basis. All request for budget changes will undergo the same vertical, offering a stable and transparent financial management strategy.

Critical risks and risk management strategy

Describe critical risks, uncertainties or difficulties related to the implementation of your project, and your measures/strategy for addressing them.

Indicate for each risk (in the description) the impact and the likelihood that the risk will materialise (high, medium, low), even after taking into account the mitigating measures.

Note: *Uncertainties and unexpected events occur in all organisations, even if very well-run. The risk analysis will help you to predict issues that could delay or hinder project activities. A good risk management strategy is essential for good project management.*

Risk No	Description	Work package No	Proposed risk-mitigation measures
R2.1	Change of legislative environment in the EU	2	WP 2.5 is the mitigation to this risk: Close observation and due diligence regarding the legislation and agile approach to adapt to the changes.
R2.2	Cybersecurity-related vulnerability	2	WP 2.4 mitigation, changing the architecture/implementation accordingly
R3.1	Further stigmatization of the blockchain technology	3	Sensibilization of the public with producing info material about what blockchain is and what it can or cannot do. Separating the valid projects from the hype projects.
R2.3	CYP(1) - Resistance to change and techno-fear, mainly when a new and radical process must be applied across a product manufacturing, distribution, and supply chain, involving farmers, truck drivers, manufacturers, and points of sale and consumers. Communication, Training, and spotless Support will be primary challenges and effort-intensive activities.	4	Well-planned Communication and Training activities. Early involvement of key stakeholders/actors and influencers across the product chain creates a robust chain of "ambassadors" and supporters. Establishment of adequate support team and process.

R2.4	CYP(2) - Competitive market solutions. Impact on the interests of private companies (possibly large-influential) who expect to profit by selling their similar proprietary solutions.	4 & 5	Take seriously market awareness and sensitivities. Market research ("espionage") should be an ongoing activity, feeding information to the project to maintain the balance, avoiding the development of danger to the project conflicts. Capitalization on Governmental and EU support.
R2.5	CYP(3) - Budget overrun: developing application use cases based on new technologies could be less predictable than "business as usual" development cycles. 50% funding means the partners may find themselves financially uncomfortable if they have to invest (co-fund) over the anticipated amounts.	All WPs	Special attention to accurate budget reporting, control and forecasting, throughout the project execution.
R3.2	HUN - The low digitalization level of the agri-food systems and the willingness to apply blockchain-based technologies might be critical challenges to tackle. Also, the (lack of) validity (trueness) of data introduced might be a high risk, which should be mitigated through careful planning and thorough assessment of the incentive system of the agri-food business operators.	3	Close cooperation with agri-food actors, sectoral workshops, highlighting benefits for agri-food products.

2.3 Capacity to carry out the proposed work

Consortium cooperation and division of roles (if applicable)

Describe the participants (Beneficiaries, Affiliated Entities and Associated Partners, if any) and explain how they will work together to implement the project. How will they bring together the necessary expertise? How will they complement each other?

In what way does each of the participants contribute to the project? Show that each has a valid role and adequate resources to fulfil that role.

***Note:** When building your consortium you should think of organisations that can help you reach objectives and solve problems.*

The TRACE4EU consortium is composed according to the requirements of the call and project deliverables. The ambition to bring the traceability use case into production has determined the selection of the most relevant and competent partners. The consortium partners define and design the requirements of the use cases and implement and test these in different countries and cross-border. A core group of European Blockchain Partnership policy representatives supported the consortium building process based on the DEP-call objectives.
The strength of the consortium is the variety of policy, business, research, technical, and implementation expertise. TRACE4EU partners contribute domain expertise in EBSI, Self-Sovereign Identity, traceability, supply chain, preservation, and education. With 13 countries involved in the consortium, we will have a large-scale implementation throughout the European ecosystem to meet the DEP ambitions.
The TRACE4EU consortium is led and managed by the Intesi Group and msg. Intesi Group and msg drive the success of cross-border solutions, making their leadership invaluable to the project.
TRACE4EU partners have made significant progress utilizing the European Blockchain Services Infrastructure (EBSI) API to implement a variety of European use cases. For instance, a cross border diploma use case between TU Berlin and WU Vienna.
All partners are actively working to develop and deploy cross-border solutions that leverage the EBSI's capabilities, with a strong focus on digital identity, digital signature, and secure data exchange.
TRACE4EU partners possess extensive expertise in EBSI, including early experience with ESSIF and EBSI documentation and APIs. Additionally, our partners have strong expertise in related fields such as blockchain technology, IT security, digital signatures, and project management. The careful selection of partners results from many collaborative jour fixes. Knowledge and experience are strategically aligned for optimal project outcomes.

All TRACE4EU partners are crucial in driving the advancement of the project. DANUBE TECH and Spherity GmbH are two partners with a strong track record in EBSI, SSI technology, and standardization efforts. Danube

Tech is a leader in community and standardization efforts, such as W3C and DIF. Markus Sabadello, a co-author of DID Core and Resolution specs at W3C, brings valuable technical architect experience with EBSI and ESSIF infrastructures.

ITA | Intesi Group S.p.A. (Intesi)

Intesi developed a market-leading product in the field of digital signature and is a Qualified Trust Service Provider for services that cover digital signature, time stamping, eDelivery, digital identity, and onboarding. Intesi is an established partner of Public Administrations and companies in Banking, Financial, Insurance, Pharmaceutical, Telecoms, and Energy. Furthermore, IG holds certifications for ISO 9001, 27001, and ETSI EN 319 401 (eIDAS QTSP). IG followed the birth and evolution of blockchain technologies from the beginning with R&D activities. In 2020 IG published an internet-draft that allows the integration of any distributed ledger (like EBSI) within qualified time stamps by ensuring compliance with the eIDAS regulation and combining the benefits of distributed ledgers with full legal validity.

AUT | Danube Tech GmbH (DANUBE TECH)

DANUBE TECH is a pioneer in SSI technologies and has been deeply involved in various community and standardization efforts, e.g., at the World Wide Web Consortium (W3C), Decentralized Identity Foundation (DIF), Trust-over-IP Foundation (ToIP), IDunion, INATBA, and other organizations. We co-authored the DID Core and DID Resolution specifications at W3C. We have also worked directly on EBSIv1 and EBSIv2 infrastructure in the role of a technical architect, and we have successfully conducted projects building on EBSI, such as "EBSI4Austria" and "Transatlantic SSI Interop." We have also collaborated with several consortium members in the last few years.

CYP | AC Goldman Solutions &Services GSS Ltd (GOLDMAN)

GOLDMAN is an SME offering high-quality services in Information Communication Technologies, with main operating areas/focus on Software Development, Network, Security & Infrastructure Services, and Project management. Goldman participated in more than five EU-funded and CEF projects, including eDelivery, EuroLogin/eIDAS, CSIRT, and EBSI. Goldman strives to develop competencies and skills in innovative technologies and applications, recently demonstrated through the successful development of the Diploma Use Case for Cyprus (entire journey – License to Practice) as part of the EBSI Early Adopters program (Wave 2), showcasing “Success Story #5” in EBSI’s Demo Days. Also participating in EA EBSI Wave3, as well as aspiring to play a significant role through Consortium partnerships within DEP’s current EBSI deployment projects. In addition to hands-on familiarization with EBSI capabilities, Goldman recently developed a private blockchain setup (as a Proof of Concept) using Hyper-Ledger Fabric (HLF), successfully demonstrating its ability and variety of skills in Blockchain/DLT design and development. A new corporate strategic objective has been set towards leading involvement and contribution to the further development, piloting, and operational exploitation of the EBP priority use cases. **DEU | GOVPART GmbH (GovPart)**

GovPart was founded with the idea of driving innovative projects on behalf of customers and being able to draw on a large network of experts. GovPart can also contribute its expertise and experience in projects where it is necessary to bring together many players and integrate new technologies into existing or newly established processes. The CEO of GovPart, Mr. Helmut Nehrenheim - an employee in a German / North Rhine-Westphalian ministry - has been an expert in e-government for many years. In this role, he is a Founding-Father of ESSIF and a participant in the EBSI Early Adopter Program. GovPart runs one EBSI Node in the piloting environment and can run up to 10 depending on the EBSI policy.

DEU | Spherity GmbH

Sperity GmbH is a cloud wallet provider, expert for decentralized technologies, and implementation partner for the Federation Services of Gaia-X. Spherity GmbH is a consortial partner of the three-year Horizon project” MaDiTraCe,” which implements material and digital traceability for certifying critical raw materials. Spherity GmbH will drive the technical implementation of the digitalization of responsible mining certification according to the CERA4in1 standard. Spherity GmbH will guarantee the exchange around technical standardization, process design, ecosystem work, and overall governance. Furthermore, Spherity GmbH is a supporting partner of the “Battery Pass” Project, funded by the Federal German Ministry of Economic Affairs and Climate Action. It will define the first standards and implement a technical prototype of the digital battery passport, which includes traceability information of various materials such as Cobalt, Lithium, Aluminium, and Copper. The results of this project will influence the work of TRACE4EU. Finally, Spherity is also a Member of the Global Battery Alliance, as an active participant of its “Track & Trace Working Group and will adopt the GBA standards for the material traceability pillar of TRACE4EU, for example the ESG standards and the GHG rule books defined by the GBA.

DEU | Technical University of Berlin (TU Berlin)

TU Berlin participated in the EBSI early adopters wave 2 (ea2), focusing on exchanging and verifying digital education credentials. During the participation, TU Berlin implemented EBSI-compliant applications to sign, issue, hold and verify educational credentials. TU Berlin has technical expertise in the evolving EBSI tech stack and collaborates with DANUBE TECH, TU Graz, and WU Vienna on educational cross-border use cases. TU Berlin research also includes collaboration with LIST (EBSILUX) in professional experience credentials.

Furthermore, TU Berlin has been working on SSI-related projects since 2018 and brings expertise in the interoperability of self-sovereign identities.

DEU | University of Applied Sciences Hamburg (HAW HAMBURG)

Prof. Skwarek's Research and Transfer Center for Digital Business Processes at HAW HAMBURG specializes in the secure connection of cyber-physical systems to the decentralized, semantic Internet 4.0, focusing on decentralized identities. HAW HAMBURG can draw on technical and conceptual preparatory work for decentralized identity management in the field of Industry 4.0 (DigitaP - BMWi), energy trading (Peak - BMWK), research data (KI2GISAXS - KAI), and Smart Mobility (STEREO - BMWi). HAW HAMBURG is involved in ISO/TC 307 and CEN/CLC/JTC 19 and gained much experience by setting up and operating the 33rd EBSI node.

ESP | VALIDATED ID SL

Validated ID SL is a European Qualified Trust Service Provider that offers services for qualified electronic signatures and seals, certificates, and timestamps with more than ten years of experience in digital signatures and digital identities. In 2018, Validated ID SL started working with Self-Sovereign Identities and participated in initiatives such as DIF, INATBA, and more. Recently, Validated ID SL became a member of the standardization body ETSI. Currently, Validated ID SL provides state-of-the-art and beyond SSI services, including an identity wallet, which is EBSI compliant. It is worth mentioning that Validated ID SL put research and innovation effort into further evolving their SSI services and contributing to standardizations such as the OpenID Connect standard. Validated ID SL was also part of EBSI's core development team, focusing on implementing EBSI core functionality.

EST | Tallinn University of Technology (TalTech)

Founded in 1918, TalTech is the only technological university in Estonia and is Estonias' most international university. At TalTech, Tallinn Law School (TLS) is an international research institution focusing on a broad spectrum of law and technology issues. Recent research projects at TLS usually have been connected to the EU Digital Single Market, Estonian novel ICT-solutions (the most innovative of them being e-residency), national e-governance architectures, cyber security issues, smart contracts, and blockchain technology, as well as automated vehicles. The volume of our institutes' successfully granted projects (mainly EU/EC) during the last eight years is at ca. 5 million EUR. TLS's three research groups comprise, among other things, experts from Germany, Italy, Spain, Estonia, the Netherlands, India, Georgia, and Ukraine and follow the mission to contribute to responsible, ethical research and innovation, reaching out to the European legal space worldwide.

EST | Digiciti Networks OÜ (DIGICITI)

The DIGICITI team has decades of experience in rights data working with the creative industries, online platforms, standardization bodies, and the European Commission. They have defined the Open Rights Data Framework in the study Copyright and New Technologies published by the Commission in 2022. They are industry associates of the Centre for Blockchain Technologies at University College London and the inventors of the blockchain-ready International Standard Content Code. They deployed a rights and royalties management system on the enterprise blockchain platform MultiChain in 2019 and a first Open Rights Data Exchange on Ethereum/ Polygon in 2022.

EST | Valunode OÜ (VALUNODE)

The VALUNODE team has decades of experience in rights data working with the creative industries, online platforms, standardization bodies, and the European Commission. They have defined the Open Rights Data Framework in the study Copyright and New Technologies published by the Commission in 2022. They are industry associates of the Centre for Blockchain Technologies at University College London. They are tracing rights data from music makers to filmmakers and rights users in the 2022-24 project Musika Peripherika co-funded by the Innovation Lab of the Creative Europe Programme, where they contribute to the IP management use case of the EBSI pre-commercial procurement.

FRA | Archipels SAS (ARCHIPELS)

ARCHIPELS is a Blockchain consortium initiated in France by La Caisse des Depots et Consignations, La Poste, EDF, and Engie, which aims to deliver services around Organizations' and Individuals' identities, to enable trust and prevent fraud. Via Archipels Connect, a decentralized identity management solution based on Blockchain technology, they allow the development of Self-Sovereign Identity projects, from the design of your use case to the product launch. They operate in the production of an Ethereum-based blockchain private network that handles over 15 million attributes certifications per month, among which are proof of residency and payslip documents for French citizens. They have developed a Blockchain Layer-2 mechanism to enable GDPR compliance and scalability of Blockchain infrastructures. Also, ARCHIPELS has strong expertise in tackling privacy challenges in decentralized ecosystems, particularly leveraging zero-knowledge-proof technologies.

GRC | National Infrastructures for Research and Technology (GRNET S.A.)

GRNET S.A., under the auspices of the Ministry of Digital Governance, has developed and deployed the gov.gr government services portal, servicing millions of citizens. It is the National Research and Education Network (NREN) of Greece and has participated in numerous European projects. GRNET S.A. has pervasive experience in developing and delivering critical production applications. It operates its data centers in the country and offers networking and cloud services to Greek academia. GRNET S.A. has followed EBSI from the beginning and

operates EBSI nodes in Athens, Greece, funded by the ELEDGER EU CEF Telecom project. Among other projects, it has also participated in PRIViLEDGE (Privacy-Enhancing Cryptography in Distributed Ledgers) and eSSIF-Lab (European Self-Sovereign Identity Framework Lab).

GRC | Internet Identity, Security and Privacy Solutions P.C. (ExcID)

The team at ExcID, a spinoff of the Athens University of Economics and Business, has implemented the NGI eSSIF (European Self-Sovereign Identity Framework) lab project "Enabling Zero Trust architectures using OAuth2.0 and Verifiable Credentials". ExcID designed, implemented, and demonstrated an access control solution based on widely used W3C, DIF, and IETF standards, composed of a VC issuer and a VC verifier, that enables strong authentication and authorization of every access request in Zero Trust Architectures (ZTAs). Additionally, within the EU Horizon 2020 project SOFIE: Secure Open Federation for Internet Everywhere and NGI DAPSI project SelectShare, ExcID has implemented and demonstrated interoperable and scalable identity, provenance, and traceability solutions in the food supply-chain, mobile gaming, and energy sectors.

HRV | Ruđer Bošković Institute (RBI)

Ruđer Bošković Institute **(**RBI) is the largest scientific institution in Croatia, with extensive experience in EU framework projects. It coordinates the National Blockchain Partnership (NBP) and establishes the National Blockchain Service Infrastructure (CroBSI). The 70th EBSI node (pilot) is installed at RBI. RBI is developing generic use cases for EBSI, such as Democratisation of Academic Publishing - DAP (T5.3). Together with the Central State Office for the Digitization of Society, RBI works on developing a Blockchain platform to establish a service for joining public or private networks using open source blockchain solutions. These solutions align with EBSI recommendations and result in a multi-tenant DLT platform for application development. The developed multi-tenant platform will be connected to the Croatian Interoperability System. It will enable connection to the EBSI projects planned by the European Union, as well as the promotion of investments and projects in this area - digital identity, digital mail, digital diploma, digital notary, trusted data exchange, and democratization of academic publishing.

HUN | Neumann János Nonprofit Public Benefit Limited Liability Company (Neumann)

Neumann is a publicly owned organization bearing the full support and oversight of the Ministry of Technology & Industry of Hungary, working to raise the digitalization level of Hungary. To this end, it supports and implements key projects in several digital transformation fields and the Hungarian Government's flagship projects, including blockchain and fintech. Neumann– through its affiliate company – is the founder of the Blockchain Coalition in Hungary, operating and coordinating the forum and the platform for the entire relevant ecosystem of the country (market and public actors, decision-makers, professional organizations) with the goal of international cooperation. The organization has been participating in EBSI policy and tech forums since 2019, participated in the installation of the first Hungarian official EBSI node, and has extensive connections with other node operators and Hungarian blockchain organizations.

ITA | University of Padova (UNIPD)

UNIPD had the scientific coordination of NGI Project Truth Seeker Chain (https://www.trublo.eu/truth-seekers-chain/) for traceability of information to cull fake news. UNIPD founded in 1222, is one of the oldest universities in Europe and one of the largest in Italy. UNIPD has 32 departments and 8 Schools operating in almost all the teaching disciplines and research areas. It hosts about 60,000 students, 2,100 professors, researchers, 1,500 Ph.D. students, and 900 postdocs. The Department of Information Engineering, one of the biggest, is a leading center for education, research, and technological development in information and communication technologies. It has more than 100 Professors and Researchers, 44 administrative and technical staff, about 100 Ph.D. students, and more than 60 postdocs. The Department has recently gained the excellence award in the latest Italian research assessment (aka VQR) for its research area, i.e., ICT.

ITA | InfoCert S.p.A. (INFOCERT)

With a registered capital of 17,704,890 € and a group turnover in 2021 of about 100 M€, INFOCERT is the most prominent Certification Authority in Europe and one of the foremost Qualified Trust Service Providers (QTSP). INFOCERT is an accredited company providing services that cover digitalization, eDelivery, digital onboarding & identity, digital signature, digital document archiving, and electronic invoicing to customers. The domains covered are Financial, Insurance, Pharmaceutical, Manufacturing, Telecoms, Energy, Utilities, Distribution, Health, Public Administration, and Professional and Trade Associations. INFOCERT owns patents in remote recognition, geo-referenced signature, and certified chat. INFOCERT holds ISO 9001, 27001, 20000, and SOC2 certifications and ISO 14001 and ETSI EN 319 401. INFOCERT is a Founding Steward of Sovrin (the first Identity specific distributed ledger) and the leading promoter of Dizme, which implements an SSI ecosystem bound to eIDAS services.

LUX | Luxembourg Institute of Science and Technology (LIST)

LIST is a partner of the EBSILUX project that aims to create an MVP implementing the EBSI Diploma use case. The Ministry of Digitalisation Luxembourg coordinates the EBSILUX projects that will end in Feb 2023. LIST has been working for several years on using Blockchain to improve the traceability of dangerous goods transport using Hyperledger Fabric and Ethereum. The Luxembourg Government finances the participation of LIST in

TRACE4EU. LIST is also a partner in the Housing+ project funded by the EU (Erasmus+), providing blockchain training content for the real estate market.

NOR | Norwegian University of Science and Technology (NTNU)

NTNU is leading a project PaaSforChain (Platform as Service Technologies for High-performance Blockchain-based Supply Chain Management Systems, https://www.ntnu.edu/paasforchain). The project uses blockchain technologies to trace the seafood supply chain and seafood exportation from Norway to China. The project is financed by the Research Council of Norway and the Ministry of Science and Technology of the People's Republic of China via the Chinese-Norwegian Collaborative Projects on Digitalisation. The project duration is 2020 to 2022.

NOR | UNISOT

UNISOT is a Norwegian Web3 Supply Chain Sustainability PaaS company. We provide solutions to global supply chain actors to be more sustainable and empower them to prove that to their customers and consumers. Our 360° Global Interoperability enables our customers to produce verifiable sustainability reporting and verifiable Scope 3 (End-to-End GHG) reporting. Our primary focus is to provide solutions to all actors in global supply chains to be more sustainable by being more efficient. Furthermore, we aim to provide tools that enable proving product Quality, Ingredients, Provenance, and Sustainability in a Digital Product Passport. All functions are becoming mandatory with the new regulations such as EU/FDA Supply Chain Traceability laws, EU Taxonomy for Sustainability, CBAM, and EPA Scope 1,2,3. Our unique B2B2C solutions are based on Scalable, Stable, Cost-efficient, and Energy-efficient Public Blockchain technology.

NOR | The Norwegian Digitalisation Agency (Digdir)

Digdir develops and operates essential national shared solutions and ensures the strategic coordination of digitalization in the sector. Digdirs' target groups are central and local government authorities, the business and voluntary sectors, and the general public. Digdir represents Norway in the EBP and is committed to supporting the development and uptake of EBSI. To this end, Digdir is involved in several blockchain initiatives where EBSI is relevant. Example: Collaboration with the Brønnøysund Register Center on "Aksjeeierbok" (shareholder Cap Table); ref. https://www.digdir.no/media/1623/download and https://symfoni.github.io/brreg-docs/#introduction. Up until 2022, Digdir has hosted an EBSI node in pre-production. In the future, Digdir will support the University of Oslo as a Node Operator, providing funding through the EBSINE consortium (also DIGITAL call 2).

NOR | Direktoratet for forvaltning og økonomistyring (DFO)

The unit for public procurement (ANS) at the Norwegian Agency for public and financial management (DFO) offers support and guidance to Norwegian public procurers. As well as giving general guidance, facilitate digital platforms for tendering processes, procurement catalogues, ANS offer guidance on sustainable procurement and innovation. According to the Norwegian public procurement directive, risks for human rights violations, in supply with high risks of human rights breaches, need to be considered. Contracting authorities are obliged to have processes and routines for safeguarding responsible supply chain management in accordance to the OECD due diligence guidance on responsible business conduct and the Transparency Act, when procuring so called high risk products. The process of tracking high risks products along the supply chain requires a lot of resources and time. There are always risks of false certifications and documents in all tiers of the supply chain. Blockchain technology will therefore be looked into in 2023 for enabling the process of tracking high risks products along the tiers of the supply chain – from final product assembly down to outtake of raw materials.

NOR | Maritech AS

For more than 40 years, Maritech AS has been one of the seafood industry's leading suppliers of software solutions. Many of the world's largest companies within aquaculture and fisheries benefit from our products and services. Their software solutions provide control and traceability throughout our customers' value chain.

DEU | msg group (msg)

As an international group of companies, msg is creating added value in the digitized world by giving top priority to people, whether customers, employees or users of our solutions. To achieve that, msg build on 40 years of industry expertise and the creative and solution-driven entrepreneurial spirit that has always been our hallmark. With over 9,000 experts in 28 countries, msg is represented in the world's most important markets. Long-term partnerships strengthen our pulling-power and ensure sustainable success. msg provides solutions for trustworthy digital ecosystem based on DLT focused on regulated industries. The msg-experts aree leading in security and compliance and take part in various R&D-projects e.g. GAIA-X, ID Union and standardization initiatives or lead standardization projects on DLT at ISO, ETSI, CEN or DIN. The solutions from msg contain operations of DLT-networks, platforms as well as connectors to legacy IT e.g. SAP with main focus on rollout across Europe.

CRO | SDURDD

SDURDD-The State Central Office for the Development of the Digital Society (SDRDD) is a state administrative organization whose mission is to monitor and improve the development of the digital society and bring it into compliance with European Union directives and regulations in the field of digital society and economy. It provides professional support to the Government of the Republic of Croatia in the development of a secure digital infrastructure and public digital services, as well as in the dissemination of the development of the digital society

in all spheres of life and activity of Croatian citizens, business and the public sector. Towards a developed, secure and inclusive digital society realized through the synergy of business, public administration, science, research and education. The Croatian NPOO Plan 2021-2026 envisages a program to establish a blockchain platform under the project C2.3.R3-1L to develop the distributed service center with EBSI nodes for Digital Identity, Digital Post, Digital Diploma, Digital Notary i Trusted Data Sharing in Publishing. It is intended to establish a national federated component in the EBSI network for DLT service aplications. In this context, SDURDD will provide a computer component for the nodes and aditional technical staff.

ESP | FNMT

FNMT-RCM, or the Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (National Mint and Stamp Factory - Royal Mint), is a Spanish public body that, in its more traditional role, is responsible for producing coins, banknotes, stamps, and a wide range of security documents that are fundamental in the life of citizens, like those that vouch for their identity and recognize their aptitudes and rights (National Identity Card, Spanish Passport, EU Residence Permit, Driving Licensce etc.). Additionally, FNMT also acts as a Trust Service Provider (TSP) in accordance with the eIDAS Regulation, offering a wide range of services intended to ensure a high level of security and trust in electronic transactions, including electronic signatures, electronic seals, time stamping, and website authentication. In terms of research, FNMT has a dedicated team focused on developing new technologies and, particularly, improving the security features of a wide range of physical or digital products, either its own or someone else's. Among these features, traceability plays a key part in many of the solutions currently being offered or explored, which range from schemes based on particular kinds of text/image codes, to solutions that leverage smart technologies -such as RFID and NFC-, or even blockchain. One particularly relevant example of a traceability project in which the FNMT has been recently involved came with the publication of Spanish Order HAC/1365/2018, whereby the traceability and security of tobacco products was regulated, and FNMT was designated as the provider of the traceability system for tobacco stamps used to seal cigarette packs, track their movement in the supply chain, and detect any illicit trade.

POR | INCM

INCM is the result of the merger of two of the oldest industrial establishments in the country, Imprensa Nacional, created in 1768, and Casa da Moeda, with more than 700 years of history. Currently, technological innovation, developed in partnership with some of the main universities and national research centers, is one of the strategic pillars of INCM, whose mission is to create, produce and supply goods and services that require high safety and security standards, focused on the customer and innovative solutions. Participating in TRACE4EU Project is in line with our mission and will help us fulfill our vision to be recognized, nationally and internationally, as a leader in security products and services essential to society.

HUN | UVMB

UVMB is the only veterinary university in Hungary, established in 1787. The University plays a leading and pivotal role in the education and research connected to animal health and food chain safety. The University has a wide network of stakeholders (feed producers, farmers, veterinary drug producers, food producers, etc.) acting as a consultation and also as a dissemination forum. As the only veterinary higher education institution in Hungary, the University has a key role in keeping animal health, veterinary public health, and food safety trainings up to date with continuous development. Recent research projects of the UVMB mainly connect to the safety and sustainability of the food systems, and to digital and data oriented solutions of the agri-food industry. UVMB has a wide international network as well, linking academia to policy making (member state food safety authorities, the Heads of European Food Safety Agencies) and to the risk assessment community (member state food safety risk assessment institutions and the European Food Safety Authority (EFSA)).

SLO | Hashnet

Hashnet d.o.o. is a Slovenian distributed ledger technology infrastructure provider. We have developed the Hashnet Distrubuted Ledger Technology infrastructure implemented with Proof-of-Stake with master nodes or Proof-of-Authority consensus algorithms. Hashnet DLT protocol is in the process of evaluation by European Blockchain Partnership to become one of the pilot protocols for European Blockchain Service Infrastructure. Overall strategy of Hashnet is based on development of world-leading public and private green DLT infrastructure and enabling cost efficient transition from unsustainable (high energy consuming) and centralized infrastructure used today to a green infrastructure powered by the environmentally friendly Hashnet consensus protocol.

NOR | The Norwegian Directorate of Fisheries (NDF)

NDF is a Norwegian government agency subject to the Ministry of Trade, Industry and Fisheries. NDF is the authorities' leading advisory and executive body within fisheries administration and management in Norway. The

Directorate's main task is to promote profitable economic activity through sustainable and user-oriented management of marine resources and the marine environment. NDF has supreme responsibility of conducting monitor, control and surveilance (MCS) management of fisheries conducted in areas under Norwegian jurisdiction and by Norwegian vessels. To strengthen the MCS management of the the future, NDF launched the CatchID-program (https://www.fiskeridir.no/Yrkesfiske/fangstid) In 2021, with the aim to support the development of new technological solutions for automated catch registration on-board fishing vessels. This approach will increase transparency, traceability and trust throughout the value chain, where EBSI and other DLT are very relevatan technologies. NDF are currently partners in severeal projects working with different approaches for traceability of seafood.

NOR | Arkivverket Norway (NArch)

The National Archives Services of Norway (Arkivverket) is an independent government authority under the Ministry of Culture. The authority of the Director General and The National Archives Services of Norway is vested in the Archival Act of 1992. The tasks of The National Archives Services of Norway are: to preserve archive material from state institutions, to make this material available for use to the public, to control the work on records administration within the ministries, regional and county authorities, to contribute to the preservation of private archives. Arkivverket will contribute to the TRACE4EU project with the following subjects: Supporting clarification on regulatory issues. Archiving by design. The Norwegian Archives Act and the Norwegian Public Access to Information Act. Supplying regulatory and technical requirements for compliance with the Archives Act. The National Archives Services of Norway (Arkivverket) is an independent government authority under the Ministry of Culture. The tasks of The National Archives Services of Norway are: to preserve archive material from state institutions, to make this material available for use to the public, to control the work on records administration within the ministries, regional and county authorities, to contribute to the preservation of private archives. Arkivverket will contribute to the TRACE4EU project with the following subjects: Supporting clarification on regulatory issues. Archiving by design. The Norwegian Archives Act and the Norwegian Public Access to Information Act. Supplying regulatory and technical requirements for compliance with the Archives Act.

LUX | Infrachain

Infrachain is a privately driven non-profit organization with public sector support created by the emerging Blockchain-industry. We are a cross-industry effort aiming to push the adoption curve of blockchain by sharing expertise, participating in blockchain projects, disseminating information on operational blockchain use cases and creating an international ecosystem. We are a Blockchain community and focus on issues allowing Blockchain applications to become operational in the current regulatory environment. It's efforts are concentrated on adoption curve of blockchain by creating a compliant-ready community and permissioned node blockchain infrastructure, providing disintermediation services to all aspects of the economy (Fintech, Healthcare, Public services, Supply chain management, etc.) as well as creating a vibrant European community of blockchain professionals driving and shaping the future blockchain industry.

DEU | Minechain

Minechain accelerates the green hydrogen value chain by providing a centralized, digital hub for managing and coordinating various aspects of the green hydrogen production and distribution process. The solution includes tracking the production and transportation of green hydrogen, monitoring and optimizing the performance of green hydrogen production facilities, and facilitating the trading and purchasing of green hydrogen between different parties in the value chain.Table 4 presents TRACE4EUs' nine application scenarios, corresponding leads, and governmental bodies.

Table 4 TRACE4EU application scenarios mapped to corresponding leads and governmental bodies

Scenario	Scenario Lead	Country Lead	Governmental Bodies providing requirements
Seafood	NTNU	NOR	Directorate of Fisheries, DFO, The National Archives of Norway, LU Ministry Of Agriculture
Agrifood	Neumann	HUN	HU Ministry of Technology and Industry
Batteries	Spherity GmbH	DEU	Federal German Ministry of Economic Affairs and Climate Action

Halloumi	GOLDMAN	CYP	Cyprus Government -Deputy Ministry of Research Innovation and Digital Policy(DMRID), Ministry of Agriculture and Rural Development (MARDE).
Open Rights Data Exchange	DIGICITI, VALUNODE	EST and FIN	EE Ministry of Economic Affairs and Communications and FI Ministry of Education and Culture
Resume Credentials	TU Berlin	DEU	Federal Ministry of Education and Research
Decentralized Academic Publishing	RBI	HUN	Central State Office for the Development of the Digital Society in Croatia
Electronic Registered Delivery	INFOCERT	ITA	L'Agenzia per l'Italia Digitale (AgID) è l'Agenzia della Presidenza del Consiglio dei Ministri
Know Your Customer (KYC)	GOLDMAN	CYP	Cyprus Government -Deputy Ministry of Research Innovation and Digital Policy (DMRID)

Project teams and staff

Describe the project teams and how they will work together to implement the project.

List the staff included in the project budget (budget category A) by function/profile (e.g. project manager, senior expert/advisor/researcher, junior expert/advisor/researcher, trainers/teachers, technical personnel, administrative personnel etc. and describe briefly their tasks.

Name and function	Organisation	Role/tasks/professional profile and expertise
[redacted]pen Technologies Director	DIGICITI	Research & Development lead/Implementation and piloting of Open Rights Data Exchange application/Inventor of the International Standard Content Code, Titusz promotes open software helping individuals and organizations better manage digital content./ https://www.linkedin.com/in/titusz/
[redacted] CEO, Research & Innovation Director	DIGICITI, VALUNODE	Task management/Implementation and piloting of Open Rights Data Exchange application/30+ years of experience in systems engineering, working at the crossroad of digital rights, policies and technologies, Philippe is also an industry associate of the UCL Center for Blockchain Technologies. https://www.linkedin.com/in/philipperixhon/
[redacted]	UNIPD	Professor of Distributed Systems Engineering and Cybersecurity
[redacted]	UNIPD	Post-Doctoral Researcher for DLT, SSI and Cybersecurity
[redacted]	GovPart	Founding-Father of ESSIF and participant in the EBSI Early Adopter Program.
[redacted] senior expert	Neumann	Lead expert in fintech and blockchain. Support and coordination of the fintech and blockchain ecosystem and the provision of relevant regulatory support. Demonstrated experience in the design and preparation of blockchain projects and its related usage in public administration in Hungary.
[redacted]hD	UVMB	Chair of the European Food Safety Authority (EFSA) Advisory Group on Data. Member of the Heads of European

		Food Safety Agencies (HoA) Network on Food chain analysis tools. Demonstrated experience in the field of food safety and traceability.
[redacted]	GOLDMAN	CY-EBSI Business development and Technical PM. Holder of an Electrical and Electronics Engineering (BEng-Hons) Degree and an Information Systems Engineering Postgraduate Diploma, started his career as a Software engineer/designer for Ericsson Telecommunication Systems in UK and Sweden, then moved to the Banking industry (IT sector, Cyprus and Romania). Nearly 30 years later, having participated /managed a considerable number of major IT business services and infrastructure projects in the Telecoms and Financial sectors, he successfully ran Goldman's participation in CY-EBSI as a technical PM for the development of the Diplomas Use Case as part of EBSI's Early Adopters program.
[redacted]	GOLDMAN	CY-EBSI Architect and Development Lead. Holder of a BSc degree in Economics and two MSc degrees in Computer Science, from Queen Mary University of London. He has 29 years of experience as a developer, IT security and network engineer. He has worked as a front-end and back-end developer on several projects funded by the EU, the last one being the development of the Diploma verifiable credentials application based on EBSI.
[redacted]	Tal Technology	Tenured Assistant Professor of Private Law at the Department of Law at TalTech, Tallinn. [redacted]research focuses on comparative private law, here especially in insolvency law, private international law, contracts in digital environments and consumer law. He provided comprehensive research on Estonian, German and international law to various stakeholders within numerous EC tenders. [redacted]eeps track with forensic issues by serving as Of Counsel for the law firm bnt Attorneys in CEE in their Tallinn office. A list of his publications is available at <http://bit.ly/1fz4RkT>.
[redacted]	INFOCERT	Innovation manager, with core competences on trust services, identity management, distributed ledgers, security. Acting as subject expert in many digital transformation projects at national and international levels. Member of the EU Blockchain Observatory expert group, ISO TC 307, ETSI ESI. Contract professor of software engineering at the University of Padova. PhD in Mathematics.
[redacted]	msg	[redacted] is Principal with long term experience in regulation, technology and innovations on DLT, Digital Identity and Trust, compliance and information security. He`s Standardization Expert and Convenor in Working Groups at ISO Tc 46 Sc11, ISO Tc 307, CEN JTC 19, ETSI ESI and taking part in various R & D- and implementation Projects on DLT such as GAIA-X, ID Union, B3i or CDBC. Steffen Schwalm will lead WP 3.
[redacted]	TU Berlin	Subject matter expert in self-sovereign identity based educational credentials. Contributed to EBSI EA2 via UniCert project.

[redacted]	ExcID	Design and evaluation of SSI and DLT technologies in the IoT, remote services, Zero Trust Architectures, and content dissemination. Professor of Informatics at the Athens University of Economics and Business. Co-Owner of the SME ExcID (INTERNET IDENTITY SECURITY AND PRIVACY SOLUTIONS I.K.E.), which is a spin-off of the Athens University of Economics and Business. His participation in project TRACE4EU will be according to Section 6.2 (Specific eligibility conditions for each budget category), A. Personnel costs, A.4-The work of SME owners for the action of the Grant Agreement.
[redacted]	ExcID	Design of solutions and management of projects on the application and interoperability of SSI and DLT technologies and digital identity in the IoT, and the supply chain and energy verticals.Professor of Informatics at the Athens University of Economics and Business. Co-owner of the SME ExcID (INTERNET IDENTITY SECURITY AND PRIVACY SOLUTIONS I.K.E.), which is a spin-off of the Athens University of Economics and Business. His participation in project TRACE4EU will be according to Section 6.2 (Specific eligibility conditions for each budget category), A. Personnel costs, A.4-The work of SME owners for the action of the Grant Agreement.
[redacted]	ExcID	Design and implementation of SSI technologies for access control, privacy, and selective disclosure in the IoT, the energy domain, and Zero Trust Architectures.Contributions to standardization groups and events such as DIF DIFCon, OAuth Security Workshop, IIW, W3C WoT and Credentials Community Group WGs, IETF's Web Authorization WG.
[redacted]	VALIDATED ID SL	CTO and co-founder of Validated ID. His professional career is specialized in cryptography, digital identity and digital signature services. He is currently in charge of the technical evolution of Validated ID's digital signature service VIDsigner and the construction of our digital identity service (SSI), VIDchain. He also participates in forums related to sovereign identity, such as DIF and RWOT.
[redacted]	VALIDATED ID SL	Project manager, with expertise in identity and access management, SSI, blockchain, cryptography and security and privcy. He is also the Austrian representative in the ESSIF use case group of EBSI. Recently, he became an ETSI member and focuses on the electronic signatures and infrastructure working group (ESI). He performed research in the SSI and realted fields availabel on google scholar page (Andreas Abraham - Google Scholar).
[redacted]	HAW HAMBURG	P[redacted]is head of the research and transfer centre focusing on security of distributed systems, holds several patents, has published more than 30 peer-reviewed articles and is co-author of 2 books. He is part of several reviewing boards of international blockchain and distributed ledger journals. P[redacted]k is also the holder of 4 national and international awards for research and teaching. In addition, he is very active in the national and international standardisation of blockchain and distributed ledger systems.

[redacted]	NTNU	[redacted] has more than 100 scientific publications and has many years of industrial and academic experience in software engineering, software security and blockchain. He is a technical committee member of the IEEE International conference on Blockchain and Cryptocurrency (ICBC). He is leading a research project using blockchain to trace Norway's seafood supply chain.
[redacted]	LIST	[redacted] is a senior researcher at the Luxembourg Institute of Science and Technology LIST. Uwe Roth worked as the senior researcher and head of the Interoperability Laboratory for Security in AdHoc Networks of the University of Luxembourg. Starting 2008 at the Public Research Center Henri Tudor (which is now LIST). He is now doing research in the Security and Privacy Group of the Trusted Service Systems Team of LIST. [redacted] current focus lies on privacy related questions in the DLT domain. He filed a patent at the end of 2016 that uses a blockchain as a core element to trace the access of files in a network. He is or was involved in several projects that use a blockchain in the context of different use cases.
[redacted]	LIST	[redacted] is an engineer at the Luxembourg Institute of Science and Technology LIST. He is doing research in the Security and Privacy Group of the Trusted Service Systems Team of LIST and is working on applied privacy and cybersecurity. [redacted] current focus lies on Blockchain, SSI and Internet of Things applications. He filed a patent at the end of 2017 concerning the privacy of network users. [redacted] completed his Engineer degree in 1996 and a master in Information Security Management in 2013. He worked almost 20 years in the IT sector as system administrator, software developer and consultant. https://www.linkedin.com/in/thierrygrandjean/

Outside resources (subcontracting, seconded staff, etc)

If you do not have all skills/resources in-house, describe how you intend to get them (contributions of members, partner organisations, subcontracting, etc.) and for which role/tasks/professional profile/expertise

If there is subcontracting, please also complete the table in section 4.

The Subcontracting is limited to 313.455,60EUR of the project total budget, and will be used only for contract services requiring very highly specialized experts, which are not available within the entity and data sets. Further explanations are available in the Subcontracting section.

Consortium management and decision-making risk(if applicable)

Explain the management structures and decision-making mechanisms within the consortium. Describe how decisions will be taken and how regular and effective communication will be ensured. Describe methods to ensure planning and control.

***Note:** The concept (including organisational structure and decision-making mechanisms) must be adapted to the complexity and scale of the project.*

The TRACE4EU consortium has a 5-level structure for decision-oriented roles:

Executive Committee consisting of the Project Leader and most relevant participants (Beneficiaries and Associated Partners like larger R&D networks included) – takes decisions on choosing and accepting new Relying Parties, consortium budget, consortium structure and any arising issues

WP Lead – holds responsibility for the overall WP success and is main representative of the WP at the Executive Committee
WP Co-Lead – supports WP coordination and substitutes the WP Lead if the WP Lead is not available
Task Lead – holds responsibility for a specific Task within the respective WP
Participant – contributes to various tasks and escalates any arising issues to the Task Lead and/or WP Lead

Each issue will be escalated bottom-up up to the WP Leads, and each WP Lead may escalate the issue to the Executive Committee. In case the Executive Committee is not able to make a decision, the Project Coordinator will have the final say.

In addition to the decision-oriented roles, there are several operational roles important for the project execution and not specifically bound to a certain WP:

Financial Coordinator (FC) will be solving any issues regarding the budget re-distribution, budget monitoring and financials
Project Management Coordinator (PMC) will be responsible for the overall coordination of project activities, KPI tracking, ASANA fulfilment and similar
Technical Coordinator (TC) will be responsible for the day-by-day coordination of the technical work of the project and monitoring of its technical achievements
Ethics Mentor (EM) ensures that all ethics issues related to activities in the grant are addressed in compliance with ethical principles, the applicable international and national law, and the provisions set out in the Grant Agreement.
Dissemination & Communication Manager (DCM) will be responsible for raising project awareness in the target audiences to foster wide adoption of the project results
User Experience and User Feedback Manager (UXM) will be responsible for User Feedback collection, analysis and integration across WPs

3. IMPACT

3.1 Expected outcomes and deliverables — Dissemination and communication

Expected outcomes and deliverables

Define and explain the extent to which the project will achieve the expected impacts listed in Call document.

TRACE4EU will realize the expected outcomes of the call "DIGITAL-2022-DEPLOY-02-EBSI-SERVICES - EBSI - Deployment of services, other use cases". The project will provide optimal technical and business case outcomes according to the requirements to continue and extend EBSI services. Furthermore, TRACE4EU aims to deliver enhanced services for citizens, governments, and businesses.
This section describes the expected outcomes and the associated work packages (WPs) to which they belong. The impact of TRACE4EU project outcomes is described below with the related impact measurements (KPIs). The deliverables of each WP and corresponding KPIs provide measurable benefits demonstrating how TRACE4EU contributes to the impacts listed in the call document.

Specific objective outcome
TRACE4EU partners will use their knowledge of distributed ledgers and EBSI to increase the use of EBSI in the EU. They will create a traceability architecture that improves cross-border government-driven processes and benefits EU citizens and businesses. TRACE4EU's application scenarios focus on traceability of raw materials and documents. These scenarios will be tested to ensure authenticity and origin of raw materials, such as fish and cheese. The traceability of digital certificates and credentials will be tested to ensure their validity and integrity. The proposed outcome of the TRACE4EU project is to improve EU citizens' experience in various digital, governmental, and economic needs.
Traceability umbrella architecture
The TRACE4EU consortium will develop a recommendation for a traceability umbrella architecture. The implementation of TRACE4EUs' umbrella-architecture will be coordinated with the EBSI core team and the European Commission to ensure seamless integration and maximum benefit for EU citizens and businesses.

Support Services
The TRACE4EU consortium will provide support services to assist stakeholders, including the European Commission and TRACE4EU consortial partners. TRACE4EU support services include technical support, training, documentation, knowledge management, and communication through applications such as Atlassian Confluence. Support services provide comprehensive support for the operation of developed solutions and ensure stakeholders have access to the latest information and best practices. Support services may evolve as the project progresses and the needs of the stakeholders change.

Specific objective data storage
The TRACE4EU consortium will focus on identifying and addressing areas of improvement in the EBSI infrastructure, specifically in storage capabilities. Through analysis and testing of real-world scenarios, project partners can pinpoint regions where EBSI's storage capabilities can be enhanced.

Testing
TRACE4EU will test its implementation on EBSI with real-world use-cases. Testing will evaluate the performance and functionality of developed applications, and identify areas for improvement. Testing is crucial for ensuring the success and adoption of TRACE4EU solutions in the EU.

Outcome 1: Reinforcing the EBSI and progressing the deployment and the extension of the EBP use cases

The TRACE4EU consortium will implement application scenarios in products and materials and document traceability defined by EBP. Implementations, experience, and knowledge of TRACE4EU is used in further EU cross-border information and data exchange activities. Table 5 shows the relation of WPs and deliverables to measurable KPIs to achieve the first outcome: Reinforce the EBSI and progress the deployment and the extension of the EBP use cases.

Table 5 TRACE4EU WPs, deliverables and corresponding KPIs to achieve Outcome 1

Associated WP	Deliverables	KPI
Architectural components WP2	D2.1	Number of gathered business, functional, and technical requirements.
	D2.2	Number of exploited EBSI core services.
	D2.3	Number of defined and implemented architectural components.
	D2.4	Number of deployed architectural components.
	D2.5, D2.6	Number of additional components integrated into the EBSI.
	D2.4, D2.6	Number of released and tested EBSI services, considering the involvement of significant stakeholders.
	D2.4, D2.5, D2.6	Number of privacy- and security measures and legislation considerations.
	D2.4, D2.5, D2.6	Number of developed architectural components that are interoperable with private- and public sector platforms.
Application Scenarios WP4 Products and Materials, WP5 Intangible assets	D4.1, D5.1	Number of developed traceability applications cross-border functional.

Outcome 2 - Increasing the engagement with stakeholders and their relevance for the EBSI take-up

Increasing the engagement with stakeholders and their relevance for the EBSI take-up will increase project awareness among key stakeholders by using tailored tools and channels for each type of audience. Citizens (holders) will improve trust in digital services, and public administrations and businesses (issuers, verifies) will understand their use. Support will be given during development by fostering cross-country initiatives and reflecting each member state's legal and political context. Furthermore, TRACE4EU partners will offer knowledge transfer and support about the (technical) use of EBSI services and developed services by TRACE4EU online and offline channels. Table 6 shows the WPs associated with TRACE4EUs' second outcome.

Table 6 TRACE4EU WPs, deliverables and corresponding KPIs to achieve Outcome 2

Associated WP	Deliverables	KPIs
WP3	D3.1	Number of coordinators communicating with the EBSI core team and the European Commission.

	D3.2	Number of cooperations with other stakeholders for future extension of developed applications to other EBP countries.
	D3.3, D3.4	Number of strategic building blocks for large-scale implementation/rollout of cross-border use cases.
WP4, WP5	D4.2, D5.2	Number of document traceability demonstrators. Number of EBSI trainings based on the demonstrators.

Outcome 3 - Provide recommendations for the further development of the EBSI eco-system

TRACE4EU will achieve the third outcome by producing documentation and reports on all development phases. Deliverables of the third outcome will be used for recommendations for further development, piloting, and operational exploitation of the EBP priority use cases. The consortium will use different tools, such as Confluence, and wikis, to provide documentation and information on the deliverables. Table 7 shows the corresponding WPs and deliverables for reaching outcome 3.

Table 7 TRACE4EU WPs, deliverables and corresponding KPIs to achieve Outcome 3

Associated WP	Deliverables	KPI
WP2, WP4, WP5	D2.5, D2.6, D4.3, D5.3	Number of reports and recommendations for further development, piloting, and operational exploitation of the EBP priority use cases.

Outcome 4 – Dissemination, communication, interim and final reports

See hereunder “Dissemination and communication of the project and its results” whereby an additional deliverable on dissemination and exploitation, part of D1.1, will be submitted in the first six months of the project

The reports will address among others:

- The engagement with stakeholders and their relevance for the EBSI take-up;
- Legal, technical and organisational challenges, including security and data protection considerations and future standardisation needs. Appropriate follow up should be identified;
- Recommendations for the further development of the EBSI eco-system;
- Specific organisational structure and governance procedures;
- Deliverables and achievements;
- Synergies with other actions;
- Updated KPIs;
- Information on how dissemination and exploitation plans were implemented.

Table 8 TRACE4EU WPs, deliverables and corresponding KPIs to achieve Outcome 3

Associated WP	Deliverables	KPI
WP1, WP3, WP4, WP5	D1.1, D3.3, D3.4, D4.3, D5.3	To be submitted in the first six months of the project
WP1	D1.4, D1.5	Number of delivered reports

Dissemination and communication of the project and its results

If relevant, describe the communication and dissemination activities, activities (target groups, main messages, tools, and channels) which are planned in order to promote the activities/results and maximise the impact. The aim is to inform and reach out to society and show the activities performed, and the use and the benefits the project will have for citizens

Clarify how you will reach the target groups, relevant stakeholders, policymakers and the general public and explain the choice of the dissemination channels.

Describe how the visibility of EU funding will be ensured.

⚠ *In case your proposal is selected for funding, you will have to provide a more detailed plan for these activities (dissemination and communication plan), within 6 months after grant signature. This plan will have to be periodically updated; in line with the project progress.*

The dissemination of the project results and the exploitation of the project achievements are the critical elements for the success of the main activities to maximize the expected impacts. Dissemination and exploitation of results are grounded in linkages to private stakeholders, security and law enforcement organizations, universities, standardization bodies, insurance companies, policymakers, and end-users in the field.

Dissemination of results: To maximize the impact and achieve the project objectives, TRACE4EU develops a detailed plan for dissemination and exploitation. The main objective of the dissemination effort is to reach the most significant possible number of stakeholders identified by the project. Another objective is to generate an adequate flow of information and publicity about the project results, the contribution made to European knowledge and scientific excellence, the value of collaboration on a Europe-wide scale, and the benefits to EU citizens in general. To realize this objective, project partners will define and implement an integrated dissemination strategy from the project's' early stages to capture the project concept, approach, and outputs and design a detailed communication plan. TRACE4EUs' approach is to create a strategy that will shift from event-based activities and material production to campaign-based activities, targeting a broader range of stakeholders and the international public and using quantifiable objectives (success indicators) to assess activities' impact during the project. The TRACE4EU dissemination activities will focus on target groups directly concerned and influenced by the project results, as stated in Table 9.

Table 8 TRACE4EUs' target groups for dissemination

Stakeholders	Impacts and benefits
Academic institutions, Industry, organizations & SMEs	Ensure that the project approach supports that document traceability is an integrated part of the management model in the relevant organisations, taking due consideration of regulatory frameworks.
EU CERTs/CSIRTs	EU CERTs/CSIRTs EU CERTs/CSIRTs will widen their cyber incidents experience. They will improve their security awareness training and general incident handling activities. Furthermore, they will exploit TRACE4EU results to strengthen public cyber security awareness.
Scientific Community (research centres, universities & RTOs)	Research Centres can benefit from the innovative knowledge and technical know-how stemming from the project's journal publications in the following significant ways: (a) Expand their research agenda, in the area of document traceability, (b) Incorporate the knowledge that will be derived from the TRACE4EU project on their scientific research areas, improving their research achievements and experimental results and (c) Exploit TRACE4EU knowledge in their educational capacities (Pre/Post graduate courses, summer schools, PhD fellowships, internship programs etc.), which stand to gain important knowledge.
Policy makers (EC, European Parliament, Governments, Standardisation Organisations)	The continuous change in threat environment, technology development and end-user needs require a regulatory framework with inherent dynamic ability.

Dissemination and communication activities: *In the early phases of the project, dissemination and communication activities start and will continue during the project runtime with a continuous engagement of internal and external audiences. The dissemination activities will have their targets and objectives established from the beginning and are divided into three primary campaigns:*

- Launch campaign
- Execution campaign
- Final campaign

Launch campaign (M1 to M6): The objective is to publicize the start of the project and the envisaged goals utilizing the project's website, visual identity, and dissemination & communication materials. The website will be updated regularly during the project lifetime and will be maintained for five years after the project ends. TRACE4EU aims to build a community of identified stakeholders through press releases. Press releases inform the public and relevant audience of the project launch, specific objectives and challenges, involved partners, and project plans. Dissemination material, including the TRACE4EU logo, flier, brochures, templates for project documents, and presentations, will be prepared for subsequent use in the project.

Execution campaign (M6 to M24): As soon as the TRACE4EU project runs and has not finished, the pilot system will be presented, and discussions will be initiated with specialized audiences from the scientific community, as well as relevant stakeholders and policymakers to determine the stakeholders' needs and expectations.

Emphasis will be put on conferences, scientific workshops, academic papers, and scientific magazines. The commercial dissemination will focus on shorter, more generic but driven communication items (web coverage, flyers, press releases, whitepapers, exhibition stands, magazines, and websites focused on smart home operators and stakeholders). TRACE4EU will adhere to the EU's guide to successful communications to disseminate the project's results in the best possible way.
TRACE4EU will launch the following initiatives to raise public participation and awareness:

- ***Creation, elaboration, and provision of dissemination materia***l: The consortium will focus on producing the marketing material consisting of leaflets, posters, and brochures. The marketing material is used to promote the project's achievements and primary outcomes in dissemination and networking events (e.g., Privacy & Data Protection, Smart Cities/Homes, and ICT events) to be attended throughout the project's life.
- ***Newsletters, press releases, presentations, leaflets, brochures, and videos*** will be updated (or newly created) as soon as the main project objectives are achieved to keep informed the widest audience possible and increase interest. Submission of papers to renowned peer-reviewed conferences and journals: Some indicative conferences and journals have already been identified as useful for TRACE4EU dissemination. A list of relevant conferences and journals will be included in the dissemination reports.
- **Conferences and Workshops**: Conferences and Workshops will be organized during the project to disseminate the TRACE4EU initiative, goal, and results to the broadest audience possible. Conferences and workshops will increase interest, promote the discussion on TRACE4EU topics and provide feedback. The project plans to organize at least two workshops to be collocated with significant events to promote the results, recommendations, and tools and receive feedback from the participants.
- ***Social Media & Blog***: Social media (Twitter/LinkedIn) and the relevant blog communities will be frequently posted with TRACE4EU news and information material to keep the information flow upright and increase the interest of multiple audiences.

Additionally, participants plan to share their experience with TRACE4EU in following conferences:
Scientific conferences aligned to the European commission and EBSI Topics

1. IEEE European Symposium on Security and Privacy (EuroS&P)
2. ACM Conference on Computer and Communications Security (CCS)
3. IEEE International Conference on Blockchain and Cryptocurrency (ICBC)
4. European Identity & Cloud Conference (EIC)
5. ACM International Conference on Distributed Event-Based Systems (DEBS)

Blockchain

1. ACM Conference on Computer and Communications Security (CCS)
2. IEEE International Conference on Blockchain (Blockchain)
3. ACM International Conference on Distributed Computing Systems (ICDCS)
4. International Conference on Financial Cryptography and Data Security (FC)

TRACE4EU will also target the following journals and conferences to publish its scientific results.
• Journals: "Elsevier Blockchain: Research and Applications", "Elsevier Computers & Security", "IEEE Access", "IEEE Communications Standards", "IEEE Transactions on Dependable and Secure Computing", "MDPI Future Internet", "ACM Distributed Ledger Technologies: Research and Practice".
• Conferences/workshops: "Open Identity Summit", "IEEE International Conference on Blockchain", "Blockchain Research and Applications for Innovative Networks and Services", "IEEE Symposium on Security and Privacy", "IEEE Conference on Standards for Communications and Networking", "Global Information Infrastructure and Networking Symposium", "MyData Global", "International Conference on Ubiquitous Computing and Ambient Intelligence", "International Conference on Advanced Information Networking and Applications", "International Conference on Availability, Reliability and Security".
Furthermore, target industrial and standardization events for presenting TRACE4EU's results will include the following: European Blockchain Convention, DIF (Decentralized Identity Foundation) DIFCon, Internet Identity Workshop (IIW), W3C Credentials Community Group, in addition to events organized by the EU Blockchain Observatory & Forum, the European Blockchain Association (EBA), the International Association for Trusted Blockchain Applications (INATBA), and the IEEE Blockchain Initiative.
Final Campaign: Project results will be presented in different fora using the dissemination above channels during the final campaign. TRACE4EU will prepare final presentations, videos, newsletters, and press releases to promote achievements, results, and measured KPIs. TRACE4EU aims to continue its efforts toward disseminating and communicating the derived results even after the termination of the project. In particular, TRACE4EU partners will maintain both the website and the social media pages. The blog will be open for discussions on TRACE4EU's activities and transport-related topics in general. Finally, open-access research papers can be accessed through IEEE Xplore, ACM, Digital Library, Springer, and Elsevier, reminding

TRACE4EU's achievements. The final TRACE4EU workshop will be held after the project focusing on the exploitation of results. TRACE4EU partners consider the dissemination strategy as a preliminary activity towards the commercialization and exploitation of results to sustain the activity beyond the end of the project.

3.2 Competitiveness and benefits for society

Competitiveness and benefits for the society

Describe the extent to which the project will strengthen competitiveness and bring important benefits for society

The TRACE4EU aims not only for the theoretical development of the EBSI Traceability Use Case and enriching the EBSI infrastructure through new elements as well as technical support by operating a helpdesk by HAW but also for the practical application of EBSI in several economic scenarios. Each scenario is unique and offers a range of values to society.

Seafood Application Scenario

Unique value proposition: Norway exported 3.1 million tonnes of seafood worth NOK 120.8 billion in 2021. Many of the seafood is exported to EU member states. Many stakeholders are involved in seafood catching or farming, processing, transportation, and trading. Currently, the seafood supply chain stakeholders do not share data often, a specific industry with data silo issues. Without sufficient traceability of the supply chain and data transparency, it is challenging for authorities to monitor the responsible production and processing in the seafood supply chain, which may lead to food safety issues. Without traceability of the seafood supply chain, addressing illegal fishing and cheating in seafood trading is challenging.

Positive impact: Full traceability will help authorities monitor and manage the seafood supply chain, ensure consumers' food safety, and regulate and encourage all stakeholders to perform responsible seafood production and processing.

Relevance to all European countries: The use case is relevant to many EU countries, such as Spain, The Netherlands, and Sweden (Iceland EAA), producing and exporting seafood to other EU countries worldwide. The use case is also relevant to all EU citizens. Full traceability of the seafood will provide them with better information about the quality of the food to ensure food safety and fair price.

Agri-food Application Scenario

Unique value proposition: Creating blockchain-based tracking of data exchange between food producers and raw food material processors will result in more secure and valid data, enabling better supply chains and better consumer information.

Positive impact: The use case outcomes will impact consumer confidence, increasing the production of healthy food of high nutritional value raw materials. Validated data can be processed by artificial intelligence or machine learning or be a data-trading subject.

Relevance to all European countries: Short food supply chains are operational in every Member State, and assisting these with blockchain technology could improve both quality and safety. Food-chain safety is a highly harmonized area in the EU. UNIVET is also involved in several European Food Safety Authority (EFSA) professional networks.

Batteries Application Scenario

Unique value proposition: By tracking ESG, CO2 Footprint (GHG emissions), and other digitally verifiable information, the battery supply chain becomes more secure and verifiable.

Positive impact: Battery traceability solutions ensure battery components' reuse, repair, and recycling. The motivation of the activities, also in the Projects of GBA, CatenaX, and Battery Pass (made with Germany, MaDiTraCE, and CirPass is to provide a compliance solution for the "new Battery Regulation."

Relevance to all European countries: As developed in this project, Umbrella technologies will help to enable the circular economy of products and materials. The developed technologies will help to build compliance solutions for the various product categories (buildings, textiles, electronics) of the Ecodesign of Sustainable Products. Furthermore, TRACE4EU considers EU regulations, Supply Chain Acts, and other areas of supply chain digitization, such as Farm 2 Fork initiatives for food products.

Halloumi Application Scenario

Unique value proposition: The Halloumi model's successful Application will demonstrate that EBSI technology can provide an effective, trusted, digitalized, and automated service/solution to safeguard PDO and PGI registered EU products. EU geographical indication schemes protect specific know-how, authenticity, and agro-environmental conditions. The EC registered Halloumi as a protected designation of origin (PDO), protecting the valuable name against imitation and misuse across the EU. Only Χαλλούμι/Halloumi/Hellim produced in Cyprus according to the product specification is now allowed to use the registered name. The implementation of this Use Case application scenario will be based on using EBSI capabilities and APIs (current and new/enhanced), utilizing case-agnostic data schemas.

Positive impact: The main objective is to provide a digital mechanism that provides trusted means to (a) the professionals associated with the Halloumi production and supply chain for verification, monitoring, and tracing,

and (b) the consumer who, being the end-user, would be able to identify/verify that what he/she gets from the market shelf is what he wants and pays for, i.e. a genuine PDO Halloumi cheese. Once implemented, this will protect both the Producer's investment (the industry) and the consumer's interest and rights across the EU. Halloumi export accounts for EUR 220m (the year 2020) while the local consumption in Cyprus reaches EUR 120m (2020), projecting several consumers above 3 million EU citizens. Consequently, the market potential of this application/system is significant, considering all EU PDO/PGI products that may adopt and capitalize on this solution.

Relevance to all European countries: Because of the globalization of the food supply chain and the free movement of goods, interest in detecting adulteration in food has increased. For authentication, a combination of analytical methods is mainly used in detecting minor differences in the botanical/ geographical origin and adulteration in sample traces. The Application development aims to directly address the harmonization of a trusted authenticity tracing digital mechanism applicable for any European PDO products by engaging blockchain/DLT (EBSI) technologies. This will be demonstrated via the Halloumi PDO Application Scenario. The Application will be developed based on a product-agnostic design structure; its backbone will have an adaptable and generic core structure, customizable to any EU PDO and PGI registered products.

Open Rights Data Exchange Application Scenario

Unique value proposition: Open Rights Data Exchange Application Scenario enables easy and incentivized attestation of machine-readable rights data for rights users. Furthermore, the scenario promotes real-time access to reliable, exhaustive, current, and interoperable rights data.

Positive impact: accurate, simple, speedy, and affordable remuneration of creators of digital media.

Relevance to all European countries: directly relevant to 12,000,000 professionals and 220,000,000 users and 5 to 6% of GDP depending on the Member State.

Resume Credentials Application Scenario

Unique value proposition: (i) Employees can digitally verify their professional experience skills and prove them when needed (application). (ii) Employers can become trusted issuers for professional experience credentials and automatically verify applicants' professional experience for authenticity.

Positive impact: Less fraudulent applications, faster application processes, and possibly less biased application candidate selection by evaluating only verifiable digital experiences.

Relevance to all European countries: Resume credentials could be used by 156.9 million full-time workers in the EU (Statista). Even if only 10% of all EU employees used resume credentials, the range would be around 15 million citizens. According to the EU Commission, in 28 EU member states, there are nearly 23 million micro, small and medium-sized enterprises. Digital resume credentials would lower application costs for employers by fastening the processes and making it much easier for EU citizens to apply for a job cross-border.

Decentralized Academic Publishing Application Scenario

Unique value proposition: The unique value proposition manifests itself in applying and integrating DLT technology in publishing. The current platform is enhanced by increasing security, speed, and efficiency in transmitting scientific information in compliance with the EU regulation on an Open access platform for research publications.

Positive impact: A decentralized publishing platform allows for: low entry costs for all members of the ecosystem; a decentralized regulatory framework (all decisions are based on consensus among the different actors in the system, preventing monopolies); decentralized archiving of articles and reviews (to prevent censorship); anonymity on request; privacy (blind reviews); and decentralized reviews (assignment and submission of reviews, peer review), as well as the possibility of direct publication.

Relevance to all European countries: The proposed publishing model is independent of the journal, meaning peer review and publication can occur without a traditional publisher. Improving scientific communication leads to faster and better development of society. The 22 billion euros in budgetary funds that today go to private publishers (currently the most profitable industry) as processing costs for open scientific publications are retained by the scientific community for cross-fertilization in science. A DAP has the potential for a breakthrough innovation that can significantly impact research, society, and the economy in the EU and broader.

Electronic Registered Delivery Application Scenario

Unique value proposition: Benefits of Electronic Registered Delivery (ERD) are well known they increase trust in electronic communication by giving proof of sending/receiving messages. This is paramount in many transactions where legal certainty has to be established. The unique value proposition of this proposal is twofold: i) the improvement of the ERD model by providing immutable storage and notarization of sending/receiving evidence. ii) the capability of using a general-purpose authentication means (EBSI-based id wallet) for access to the ERD services.

Positive impact: Immutable storage and notarization provide an essential step forward in communication management and long-term legal enforcement. It will also help enforce interoperability between diverse ERD systems. A standard authentication tool provided increased usability and simplified access, fostering usage.

Relevance to all European countries: Many EU countries already have in place ERD systems, some of which have a significant user base (e.g.. 12M users in Italy). Such systems offer limited usability and almost no cross-

system interoperability. This proposal provides the perspective for enhanced usability and interoperability, which would foster service usage (and, consequently, trusted digital communication) across the EU.

KYC-Tool Application Scenario

Unique value proposition: KYC documents will be submitted once and be accessible by any requesting entity (e.g., Bank) authorized by the documents' owner, in full compliance with GDPR. The Know your Customer (KYC-tool) EBSI use case scenario enables a seamless exchange of customer information amongst financial institutions. It promotes real-time compliance processing, enabling digital customer onboarding while empowering customers with digital identity and document management in a secure manner. Currently, there is a manual process to gather customer information and collect all the KYC documents. The sharing of this information with 3rd party validation agencies is also cumbersome. Each of the divisions performs KYC in a siloed manner, and hence there is duplication of effort. With the implementation of the KYC tool, customers will be able to share documents in a secure, controlled, and trustworthy manner, in full compliance with GDPR.

Positive impact: Banks and other institutions in any EU country that must identify their customers as part of the service provisioning process will benefit from the proposed KYC-tool use case application. The KYC application scenario will simplify the KYC process, reduce effort and minimize admin costs for both customers and institutions. Only new (first-time) customers without KYC will go through the KYC process. The key benefits are: (i) Better customer experience, easy, secure, and controlled data sharing, (ii) Cost-time savings for all involved parties, (iii) Automated compliance: increased transparency provides auditors with easy and fast verification of KYC activity transactions.

Relevance to all European countries: AML/KYC regulatory framework applies to all EU member states and citizens having to submit KYC-related personal documents to a Banking or Financial services (or any other) institution.

3.3 Environmental sustainability and contribution to European Green Deal goals

Environmental sustainability and contribution to European Green Deal goals

Describe the extent to which the project will contribute to environmental sustainability and in particular to European Green Deal goals

⚠ *This might not be applicable to all topics — for details refer to the Call document.*

TRACE4EU exploits the existing EBSI services. The underlying DLT of EBSI is the Hyperledger Besu (Ethereum fork, public-permissioned ledger) and Fabric (private-permissioned ledger). Both ledgers utilize consensus algorithms that do not require high computation, such as the Proof of Work algorithm. Therefore, using existing EBSI services is environmentally sustainable: the new services and software that come with TRACE4EU use and rely on EBSI. Hence, no wasted energy consumption comes with the TRACE4EU software and services.

Moreover, TRACE4EU and the recognition of credentials for products, materials, data, and documents with a higher level of assurance with qualified electronic signatures, seals, and timestamps will reduce the necessity of creating such documents in physical format significantly. The reduction in paper consumption also influences the energy used for paper production. Therefore, the TRACE4EU project proposes an environmentally sustainable alternative for legal documents in digital form and contributes to the European Green Deal goals such as climate neutrality of the EU by 2050.

Lastly, certain application scenarios such as traceability of seafood, agrifood, and batteries ultimately aim to help efficiently use resources. Efficient use of resources will be achieved by clean and disambiguous traceability of the materials and products that improve effective recycling of waste products into the circular economy. In addition, the implementations of traceability applications enable proof of origin for raw material and the auditability of the production conditions, such as Child Labor and Wastewater Treatment.

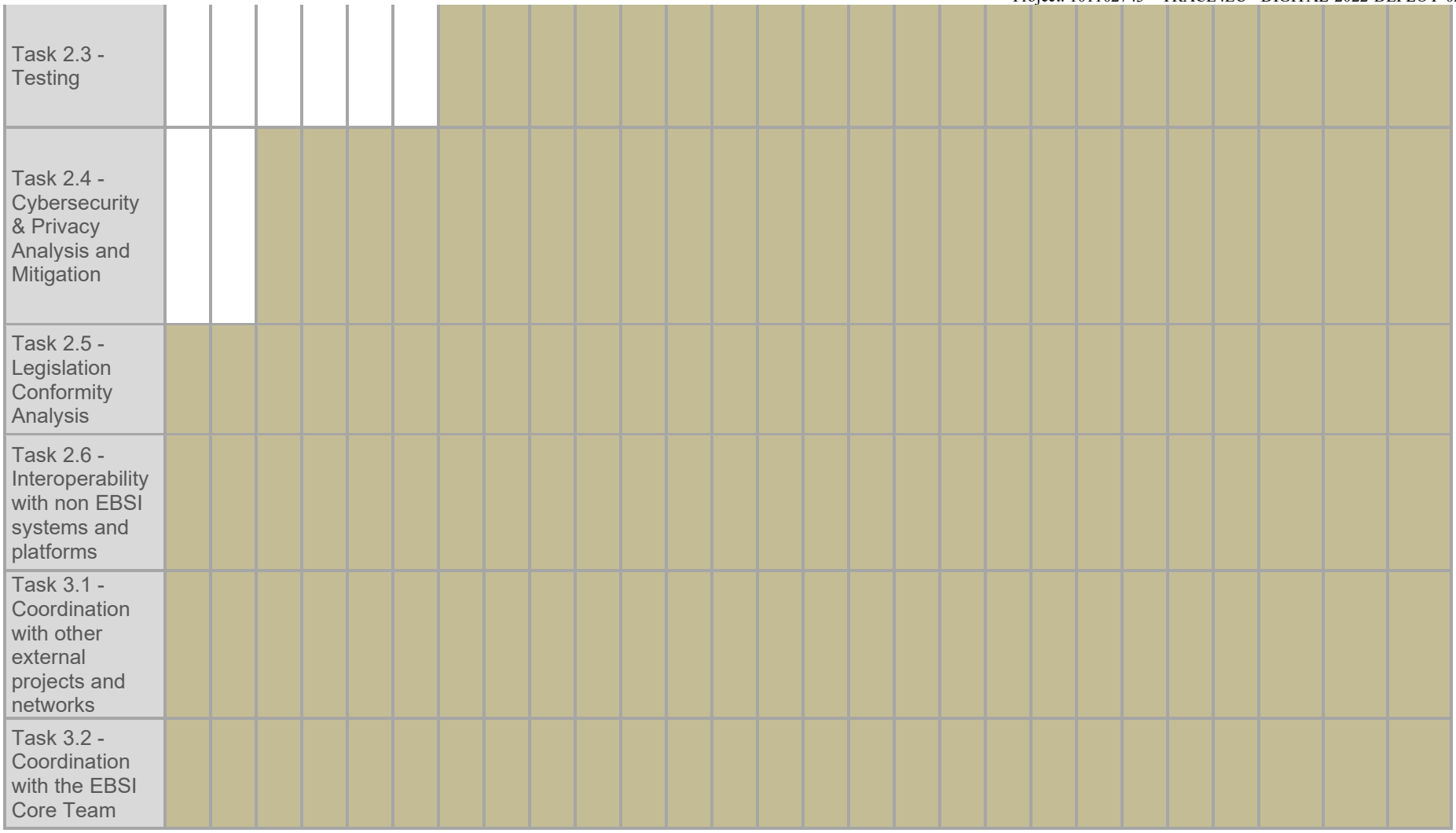
4. WORK PLAN, WORK PACKAGES, TIMING AND SUBCONTRACTING

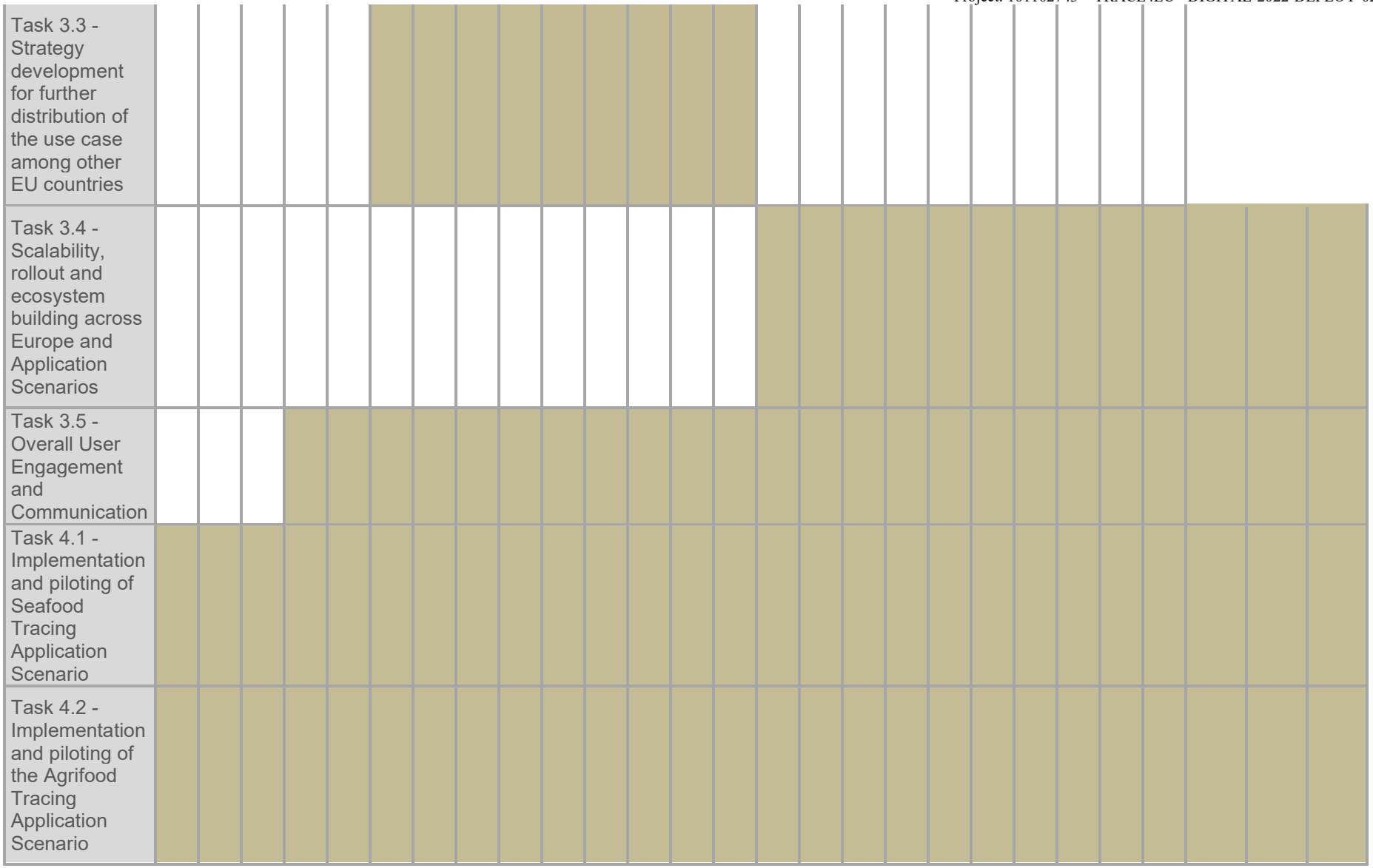
4.3 Timetable

Fill in cells in beige to show the duration of activities. Repeat lines/columns as necessary.

Note: *Use the project month numbers instead of calendar months. Month 1 marks always the start of the project. In the timeline you should indicate the timing of each activity per WP.*

ACTIVITY	MONTHS																										
	M 1	M 2	M 3	M 4	M 5	M 6	M 7	M 8	M 9	M 10	M 11	M 12	M 13	M 14	M 15	M 16	M 17	M 18	M 19	M 20	M 21	M 22	M 23	M 24	M25	M26	M27
Task 1.1 - Coordination of Application Scenario piloting																											
Task 1.2 - General coordination at the governmental level																											
Task 1.3 - General coordination at the project level																											
Task 2.1 - Umbrella architectural design																											
Task 2.2 - Continuous implementation and deployment																											


Task 2.3 - Testing
Task 2.4 - Cybersecurity & Privacy Analysis and Mitigation
Task 2.5 - Legislation Conformity Analysis
Task 2.6 - Interoperability with non EBSI systems and platforms
Task 3.1 - Coordination with other external projects and networks
Task 3.2 - Coordination with the EBSI Core Team


Task 3.3 - Strategy development for further distribution of the use case among other EU countries
Task 3.4 - Scalability, rollout and ecosystem building across Europe and Application Scenarios
Task 3.5 - Overall User Engagement and Communication
Task 4.1 - Implementation and piloting of Seafood Tracing Application Scenario
Task 4.2 - Implementation and piloting of the Agrifood Tracing Application Scenario

Task 4.3 - Implementation and piloting of Batteries Tracing Application Scenario																											
Task 4.4 - Implementation and piloting of Halloumi Cheese Tracing Application Scenario																											
Task 4.5 - Lessons learned from products & materials traceability piloting																											
Task 4.6 - Overall User Engagement and Communication																											
Task 5.1 - Implementation and piloting of Open Rights Data Exchange Tracing Application Scenario																											

Task 5.2 - Implementation and piloting of Resume Credentials Tracing Application																											
Task 5.3 - Implementation and piloting of Decentralized Academic Publishing Tracing Application Scenario																											
Task 5.4 - Implementation and piloting of Electronic Registered Delivery Tracing Application Scenario																											
Task 5.5 - Implementation and piloting of KYC Tracing Application Scenario																											
Task 5.6 - Lessons learned from data/document traceability piloting																											

Task 5.7 - Overall User Engagement and Communication																															

4.4 Subcontracting (n/a for prefixed Lump Sum Grants)

Subcontracting

Give details on subcontracted project tasks (if any) and explain the reasons why (as opposed to direct implementation by the Beneficiaries/Affiliated Entities).

Subcontracting — Subcontracting means the implementation of 'action tasks', i.e. specific tasks which are part of the EU grant and are described in Annex 1 of the Grant Agreement.

***Note:** Subcontracting concerns the outsourcing of a part of the project to a party outside the consortium. It is not simply about purchasing goods or services. We normally expect that the participants have sufficient operational capacity to implement the project activities themselves. Subcontracting should therefore be exceptional.*

Include only subcontracts that comply with the rules (i.e. best value for money and no conflict of interest; no subcontracting of coordinator tasks).

Work Package No	Subcontract No (continuous numbering linked to WP)	Subcontract Name (subcontracted action tasks)	Description (including task number and BEN to which it is linked)	Estimated Costs (EUR)	Justification (Why is subcontracting necessary?)	Best-Value-for-Money (How do you intend to ensure it?)
WP4	S4.1	Connecting Digital Producer's Market to blockchain - Compliance with Hungary's Digital Agricultural Strategy under Task 4.2	Neumann plans to use a subcontractor for implementing action Task 4.2. A dedicated team of experts from an organization specialized in the Hungarian supply chain regulations and procedures will be needed to optimize the TRACE4EU impact on the Hungarian case.	235,000	The Digital Producers' Market Nonprofit Ltd. started the development of the system based on the governmental regulation already in 2020. At present,the blockchain-related tasks have to be launched. Neumann Nltd. will subcontract this task due to the lack of expertise in house.	3 Offers, best value-for-money according to the EU and national procurement law
WP5	S5.1	Academic Publishing under Task 5.3	External subcontracting for RBI will be needed for: ➢ Implementation and piloting of Decentralized Academic Publishing Application platform ➢ Consulting, design and SW development of smart contracts for the DAP platform system (in particular ERC20 and ERC721 contracts) ➢ Support in setting up a test environment.	20.000	As highly specialized expertise will be needed, the RBI is seeking support from experts who developed the HeshNet consensus algorithm (Moon Code d.o.o.) and intend to use and leverage expertise for optimal performance of the DAP platform.	3 Offers, best value-for-money according to the EU and national procurement law

Other issues: *If subcontracting <u>for the entire project</u> goes beyond 30% of the total eligible costs, give specific reasons.*			Insert text			

5. OTHER

5.1 Ethics

Ethics
If the Call document contains a section on ethics, the ethics issues and measures you intend to take to solve/avoid them must be described in the annexed Ethics issues table .
See annex

5.2 Security

Security
Describe security issues that may arise during the project implementation in the annexed Security issues table. *Indicate if there is need for EU classification of information (Decision 2015/444) or any other specific security measures.* ***Note:** Beneficiaries must ensure that their projects are not subject to national/third country security requirements that could affect the implementation or put into question the award of the grant (e.g. technology restrictions, national security classification, etc).*
See annex

6. DECLARATIONS

Double funding	
Information concerning other EU grants for this project ⚠ *Please note that there is a strict prohibition of double funding from the EU budget (except under EU Synergies actions).*	**YES/NO**
We confirm that to our best knowledge neither the project as a whole nor any parts of it have benefitted from any other EU grant *(including EU funding managed by authorities in EU Member States or other funding bodies, e.g. Erasmus, EU Regional Funds, EU Agricultural Funds, European Investment Bank, etc)*. If NO, explain and provide details.	YES
We confirm that to our best knowledge neither the project as a whole nor any parts of it are (nor will be) submitted for any other EU grant *(including EU funding managed by authorities in EU Member States or other funding bodies, e.g. Erasmus, EU Regional Funds, EU Agricultural Funds, European Investment Bank, etc)*. If NO, explain and provide details.	YES

Financial support to third parties (if applicable)
If in your project the maximum amount per third party will be more than the threshold amount set in the Call document, justify and explain why the higher amount is necessary in order to fulfil your project's objectives.
Not applicable

Purchases and equipment

Purchase costs (travel and subsistence, equipment and other goods works and services) *Details for major cost items (needed if costs declared under 'purchase costs' are higher than 15% of the claimed personnel costs).* *Start with the most expensive cost items, down to the 15% threshold.*				
Participant 1:	GovPart GmbH			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)

C.1 Travel and subsistence	*[*Travel and Subsistence*]*	WP5	Travel and subsistence costs related to project meetings and visits 1 meeting in Brussels, 2 meetings in another EU city = 3 person-travels 1 person per WP-meeting (2 WP-Meetings - One at the beginning and one at the end of WP 5) = 2 person travels Total: 5 person-travels	3,000.00
C2. Equipment	*[*Equipment*]*	WP 5	Hosting costs for server infrastructure and high-quality hardware equipment	40,000.00
			Total	43,000 EUR
			Total purchase costs > 15% (all participants)	31,750 EUR
			Remaining purchase costs < 15% (all participants)	164,122 EUR
			Total purchase costs (all participants)	195,872 EUR

ANNEXES

LIST OF ANNEXES

Standard
Detailed budget table/Calculator (annex 1 to Part B) — *not applicable*
CVs (annex 2 to Part B) — *not applicable*
Annual activity reports (annex 3 to Part B) — *not applicable*
List of previous projects (annex 4 to Part B) — *mandatory, if required in the Call document*

Special
Other annexes (annex 5 to Part B) — *mandatory, if required in the Call document*

ANNEX 2

ESTIMATED BUDGET FOR THE ACTION

Forms of funding	Estimated eligible[1] costs (per budget category)										Estimated EU contribution[2]			
	Direct costs								Indirect costs	Total costs	EU contribution to eligible costs			Maximum grant amount[6]
	A. Personnel costs			B. Subcontracting costs	C. Purchase costs			D. Other cost categories	E. Indirect costs[3]		Funding rate %[4]	Maximum EU contribution[5]	Requested EU contribution	
	A.1 Employees (or equivalent) A.2 Natural persons under direct contract A.3 Seconded persons		A.4 SME owners and natural person beneficiaries	B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties	D.2 Internally invoiced goods and services	E. Indirect costs				
	Actual costs	Unit costs (usual accounting practices)	Unit costs[7]	Actual costs	Actual costs	Actual costs	Actual costs	Actual costs	Unit costs (usual accounting practices)	Flat-rate costs[8]				
	a1	a2	a3	b	c1	c2	c3	d1	d2	e = flat-rate * (a1 + a2 + a3 + b + c1 + c2 + c3 + d1 + d2)	f = a + b + c + d + e	U	g = f * U%	h	m
1 - Intesi	371 300.00	0.00	0.00	0.00	3 000.00	0.00	0.00	0.00	0.00	26 201.00	400 501.00	50	200 250.50	200 250.50	200 250.50
2 - GovPart	75 000.00	0.00	0.00	0.00	3 000.00	0.00	40 000.00	0.00	0.00	8 260.00	126 260.00	50	63 130.00	63 130.00	63 130.00
3 - msg	887 500.00	0.00	0.00	0.00	6 000.00	0.00	2 111.42	0.00	0.00	62 692.80	958 304.22	50	479 152.11	479 152.11	479 152.11
4 - TU Berlin	578 728.00	0.00	0.00	0.00	6 000.00	0.00	41 760.00	0.00	0.00	43 854.16	670 342.16	50	335 171.08	335 171.08	335 171.08
5 - INFOCERT	316 400.00	0.00	0.00	0.00	6 000.00	0.00	0.00	0.00	0.00	22 568.00	344 968.00	50	172 484.00	172 484.00	172 484.00
6 - VALIDATED ID SL	525 000.00	0.00	0.00	0.00	6 000.00	0.00	0.00	0.00	0.00	37 170.00	568 170.00	50	284 085.00	284 085.00	284 085.00
7 - LIST	0.00	203 211.00	0.00	0.00	6 000.00	0.00	0.00	0.00	0.00	14 644.77	223 855.77	50	111 927.89	111 927.89	111 927.89
8 - ARCHIPELS	84 500.00	0.00	0.00	0.00	3 000.00	0.00	0.00	0.00	0.00	6 125.00	93 625.00	50	46 812.50	46 812.50	46 812.50
9 - HAW HAMBURG	77 000.00	0.00	0.00	0.00	3 000.00	0.00	0.00	0.00	0.00	5 600.00	85 600.00	50	42 800.00	42 800.00	42 800.00
10 - DANUBE TECH	312 000.00	0.00	0.00	0.00	3 000.00	0.00	0.00	0.00	0.00	22 050.00	337 050.00	50	168 525.00	168 525.00	168 525.00
11 - Spherity GmbH	413 000.00	0.00	0.00	0.00	3 000.00	0.00	0.00	0.00	0.00	29 120.00	445 120.00	50	222 560.00	222 560.00	222 560.00
12 - UNIPD	107 250.00	0.00	0.00	0.00	6 000.00	0.00	0.00	0.00	0.00	7 927.50	121 177.50	50	60 588.75	60 588.75	60 588.75
13 - TalTech	48 000.00	0.00	0.00	0.00	3 000.00	0.00	0.00	0.00	0.00	3 570.00	54 570.00	50	27 285.00	27 285.00	27 285.00
14 - DIGICITI	37 440.00	0.00	0.00	0.00	1 131.08	0.00	0.00	0.00	0.00	2 699.98	41 271.06	50	20 635.53	20 635.53	20 635.53
15 - Neumann	236 800.00	0.00	0.00	235 000.00	3 000.00	0.00	0.00	0.00	0.00	33 236.00	508 036.00	50	254 018.00	254 018.00	254 018.00
16 - RBI	292 800.00	0.00	0.00	20 000.00	3 000.00	0.00	0.00	0.00	0.00	22 106.00	337 906.00	50	168 953.00	168 953.00	168 953.00
17 - GOLDMAN	462 543.00	0.00	0.00	0.00	16 000.00	0.00	0.00	0.00	0.00	33 498.01	512 041.01	50	256 020.51	256 020.51	256 020.51
18 - MGTŠ	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	50	0.00	0.00	0.00
19 - NTNU	197 851.00	0.00	0.00	0.00	6 000.00	0.00	0.00	0.00	0.00	14 269.57	218 120.57	50	109 060.29	109 060.29	109 060.29
20 - UNISOT	300 000.00	0.00	0.00	0.00	6 000.00	0.00	0.00	0.00	0.00	21 420.00	327 420.00	50	163 710.00	163 710.00	163 710.00
21 - NDF	15 000.00	0.00	0.00	0.00	3 000.00	0.00	0.00	0.00	0.00	1 260.00	19 260.00	50	9 630.00	9 630.00	9 630.00
22 - GRNET S.A.	100 800.00	0.00	0.00	0.00	3 000.00	0.00	0.00	0.00	0.00	7 266.00	111 066.00	50	55 533.00	55 533.00	55 533.00
23 - Excid	0.00	0.00	74 610.00	0.00	3 000.00	0.00	0.00	0.00	0.00	5 432.70	83 042.70	50	41 521.35	41 521.35	41 521.35
24 - Maritech AS	180 500.00	0.00	0.00	0.00	3 000.00	0.00	0.00	0.00	0.00	12 845.00	196 345.00	50	98 172.50	98 172.50	98 172.50
25 - HASHNET	127 500.00	0.00	0.00	0.00	3 000.00	0.00	0.00	0.00	0.00	9 135.00	139 635.00	50	69 817.50	69 817.50	69 817.50
26 - MINECHAIN															
27 - FNDMT															
28 - NDA															
29 - INFRACHAIN ASBL															

	Estimated eligible[1] costs (per budget category)											Estimated EU contribution[2]			
	Direct costs									Indirect costs	Total costs	EU contribution to eligible costs			Maximum grant amount[6]
	A. Personnel costs			B. Subcontracting costs	C. Purchase costs			D. Other cost categories		E. Indirect costs[3]		Funding rate %[4]	Maximum EU contribution[5]	Requested EU contribution	
	A.1 Employees (or equivalent) A.2 Natural persons under direct contract A.3 Seconded persons		A.4 SME owners and natural person beneficiaries	B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties	D.2 Internally invoiced goods and services	E. Indirect costs					
Forms of funding	Actual costs	Unit costs (usual accounting practices)	Unit costs[7]	Actual costs	Actual costs	Actual costs	Actual costs	Actual costs	Unit costs (usual accounting practices)	Flat-rate costs[8]					
	a1	a2	a3	b	c1	c2	c3	d1	d2	e = flat-rate * (a1 + a2 + a3 + b + c1 + c2 + c3 + d1 + d2)	f = a + b + c + d + e	U	g = f * U%	h	m
30 - SDURDD															
31 - INCM															
32 - NArch															
33 - DFO															
34 - UVMB															
35 - Talao															
36 - VALUNODE	91 910.00	0.00	0.00	0.00	1 868.92	0.00	0.00	0.00	0.00	6 564.52	100 343.44	50	50 171.72	50 171.72	50 171.72
Σ consortium	5 838 822.00	203 211.00	74 610.00	255 000.00	109 000.00	0.00	83 871.42	0.00	0.00	459 516.01	7 024 030.43		3 512 015.23	3 512 015.23	3 512 015.23

[1] See Article 6 for the eligibility conditions. All amounts must be expressed in EUR (see Article 21 for the conversion rules).
[2] The consortium remains free to decide on a different internal distribution of the EU funding (via the consortium agreement; see Article 7).
[3] Indirect costs already covered by an operating grant (received under any EU funding programme) are ineligible (see Article 6.3). Therefore, a beneficiary/affiliated entity that receives an operating grant during the action duration cannot declare indirect costs for the year(s)/reporting period(s) covered by the operating grant, unless they can demonstrate that the operating grant does not cover any costs of the action. This requires specific accounting tools. Please immediately contact us via the EU Funding & Tenders Portal for details.
[4] See Data Sheet for the funding rate(s).
[5] This is the theoretical amount of the EU contribution to costs, if the reimbursement rate is applied to all the budgeted costs. This theoretical amount is then capped by the 'maximum grant amount'.
[6] The 'maximum grant amount' is the maximum grant amount decided by the EU. It normally corresponds to the requested grant, but may be lower.
[7] See Annex 2a 'Additional information on the estimated budget' for the details (units, cost per unit).
[8] See Data Sheet for the flat-rate.

DATA SHEET

1. General data

Project summary:

Project summary
The traceability of data, documents, and physical goods are essential in many fields. Therefore, the traceability use case was one of the first developed by the EBP (from 2018 on). Traceability use cases and applications enable EBSI and other blockchain-based electronic ledgers to be used and applied in many domains. The general objective of this project is to create an "umbrella architecture" based on existing EBSI services. The architecture builds the basis for the realization of traceability application scenarios. Furthermore, TRACE4EU focuses on engagement with pan-European stakeholders and promotion of recommendations for further development of the EBSI eco-system. As a result, TRACE4EU can significantly influence traditional industries and contribute to their transition to more efficient, productive, competitive, and resilient ones. It will also strengthen transparency in the European area for citizens, who can better and proactively track the flow of commodities and data through future traceability implementations. The umbrella architecture will be derived from the work on multiple scenarios, including analyzing requirements for traceability applications of tangible and intangible assets that work in local and cross-border settings.

Keywords:

- Blockchain and Distributed Ledger Technology (DLT)
- traceability document data product materials

Project number: 101102743

Project name: Traceability Reference Architecture Conformant EBSI for European Union

Project acronym: TRACE4EU

Call: DIGITAL-2022-DEPLOY-02

Topic: DIGITAL-2022-DEPLOY-02-EBSI-SERVICES

Type of action: DIGITAL Simple Grants

Granting authority: European Health and Digital Executive Agency

Grant managed through EU Funding & Tenders Portal: Yes (eGrants)

Project starting date:1 June 2023

Project end date: 31 August 2025

Project duration: 27 months

Consortium agreement: Yes

2. Participants

List of participants:

N°	Role	Short name	Legal name	Ctry	PIC	Total eligible costs (BEN and AE)	Max grant amount	Entry date	Exit date
1	COO	Intesi	INTESI GROUP SPA	IT	886542171	400 501.00	200 250.50		
2	BEN	GovPart	GOVPART GMBH	DE	888107654	126 260.00	63 130.00		
3	BEN	msg	MSG SYSTEMS AG	DE	886714249	958 304.22	479 152.11		
4	BEN	TU Berlin	TECHNISCHE UNIVERSITAT BERLIN	DE	999986678	670 342.16	335 171.08		
5	BEN	INFOCERT	INFOCERT SPA	IT	990330037	344 968.00	172 484.00		

N°	Role	Short name	Legal name	Ctry	PIC	Total eligible costs (BEN and AE)	Max grant amount	Entry date	Exit date
6	BEN	VALIDATED ID SL	VALIDATED ID SL	ES	937979040	568 170.00	284 085.00		
7	BEN	LIST	LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY	LU	934320200	223 855.77	111 927.89		
8	BEN	ARCHIPELS	ARCHIPELS	FR	891545140	93 625.00	46 812.50		
9	BEN	HAW HAMBURG	HOCHSCHULE FUR ANGEWANDTE WISSENSCHAFTEN HAMBURG	DE	999876680	85 600.00	42 800.00		
10	BEN	DANUBE TECH	DANUBE TECH GMBH	AT	919243975	337 050.00	168 525.00		
11	BEN	Spherity GmbH	SPHERITY GMBH	DE	904225271	445 120.00	222 560.00		
12	BEN	UNIPD	UNIVERSITA DEGLI STUDI DI PADOVA	IT	999995602	121 177.50	60 588.75		
13	BEN	TalTech	TALLINNA TEHNIKAÜLIKOOL	EE	999842536	54 570.00	27 285.00		
14	BEN	DIGICITI	DIGICITI NETWORKS OU	EE	892686345	41 271.06	20 635.53		31/3/2024
15	BEN	Neumann	NEUMANN JANOS NONPROFIT KOZHASZNU KORLATOLT FELELOSSEGU TARSASAG	HU	998453593	508 036.00	254 018.00		
16	BEN	RBI	RUDER BOSKOVIC INSTITUTE	HR	999875031	337 906.00	168 953.00		
17	BEN	GOLDMAN	AC GOLDMAN SOLUTIONS&SERVICES GSS LTD	CY	917565390	512 041.01	256 020.51		
18	BEN	MGTŠ	MINISTRSTVO ZA GOSPODARSTVO, TURIZEM IN SPORT	SI	998818895	0.00	0.00		17/12/2023
19	BEN	NTNU	NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET NTNU	NO	999977851	218 120.57	109 060.29		
20	BEN	UNISOT	UNISOT AS	NO	892058949	327 420.00	163 710.00		
21	BEN	NDF	FISKERIDIREKTORATET	NO	890176470	19 260.00	9 630.00		
22	BEN	GRNET S.A.	NATIONAL INFRASTRUCTURES FOR RESEARCH AND TECHNOLOGY	EL	999937887	111 066.00	55 533.00		
23	BEN	Excid	INTERNET IDENTITY SECURITY ANDPRIVACY SOLUTIONS I.K.E.	EL	885501167	83 042.70	41 521.35		
24	BEN	Maritech AS	MARITECH AS	NO	885423082	196 345.00	98 172.50		
25	BEN	HASHNET	HASHNET DISTRIBUIRANE TEHNOLOGIJE DOO	SI	900883621	139 635.00	69 817.50		
26	AP	MINECHAIN	Minechain GmbH	DE	890417418	0.00	0.00		
27	AP	FNDMT	FABRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA	ES	912199059	0.00	0.00		
28	AP	NDA	DIGITALISERINGSDIREKTORATET	NO	998942667	0.00	0.00		
29	AP	INFRACHAIN ASBL	INFRACHAIN ASBL	LU	907230428	0.00	0.00		
30	AP	SDURDD	Central State Office for the Development of Digital Society	HR	894141442	0.00	0.00		
31	AP	INCM	IMPRENSA NACIONAL - CASA DA MOEDA, S. A.	PT	911351958	0.00	0.00		
32	AP	NArch	Arkivverket The National Archives of Norway	NO	890829086	0.00	0.00		
33	AP	DFO	Direktoratet for forvaltning og økonomistyring	NO	892580809	0.00	0.00		
34	AP	UVMB	ALLATORVOSTUDOMANYI EGYETEM	HU	917811673	0.00	0.00		
35	AP	Talao	WEB3 DIGITAL WALLET,	FR	885481088	0.00	0.00	18/12/2023	
36	BEN	VALUNODE	VALUNODE OU	EE	879963922	100 343.44	50 171.72	1/4/2024	
Total						7 024 030.43	3 512 015.23		

Coordinator:

– INTESI GROUP SPA (Intesi): from 18 December 2023 to present

– MINISTRSTVO ZA GOSPODARSTVO, TURIZEM IN SPORT (MGTŠ): from 10 May 2023 to 17 December 2023

3. Grant

Maximum grant amount, total estimated eligible costs and contributions and funding rate:

Total eligible costs (BEN and AE)	Funding rate (%)	Maximum grant amount (Annex 2)	Maximum grant amount (award decision)
7 024 030.43	50	3 512 015.23	3 512 015.23

Grant form: Budget-based

Grant mode: Action grant

Budget categories/activity types:

- A. Personnel costs
  - A.1 Employees, A.2 Natural persons under direct contract, A.3 Seconded persons
  - A.4 SME owners and natural person beneficiaries
- B. Subcontracting costs
- C. Purchase costs
  - C.1 Travel and subsistence
  - C.2 Equipment
  - C.3 Other goods, works and services
- D. Other cost categories
  - D.1 Financial support to third parties
  - D.2 Internally invoiced goods and services
- E. Indirect costs

Cost eligibility options:

- Standard supplementary payments
- Average personnel costs (unit cost according to usual cost accounting practices)
- Limitation for subcontracting
- Travel and subsistence:
  - Travel: Actual costs
  - Accommodation: Actual costs
  - Subsistence: Actual costs
- Equipment: depreciation only
- Costs for providing financial support to third parties (actual cost; max amount for each recipient: EUR 60 000.00)
- Indirect cost flat-rate: 7% of the eligible direct costs (categories A-D, except volunteers costs and exempted specific cost categories, if any)
- VAT: Yes
- Other ineligible costs

Budget flexibility: Yes (no flexibility cap)

4. Reporting, payments and recoveries

4.1 Continuous reporting (art 21)

Deliverables: see Funding & Tenders Portal Continuous Reporting tool

4.2 Periodic reporting and payments

Reporting and payment schedule (art 21, 22):

Reporting					Payments	
Reporting periods			Type	Deadline	Type	Deadline (time to pay)
RP No	Month from	Month to				
					Initial prefinancing	30 days from entry into force/10 days before starting date/ financial guarantee (if required) – whichever is the latest
1	1	12	Periodic report	60 days after end of reporting period	Interim payment	90 days from receiving periodic report
2	13	27	Periodic report	60 days after end of reporting period	Final payment	90 days from receiving periodic report

Prefinancing payments and guarantees:

Prefinancing payment		Prefinancing guarantee		
Type	Amount	Guarantee amount	Division per participant	
Prefinancing 1 (initial)	1 756 007.62	n/a	1 - Intesi	n/a
			2 - GovPart	n/a
			3 - msg	n/a
			4 - TU Berlin	n/a
			5 - INFOCERT	n/a
			6 - VALIDATED ID SL	n/a
			7 - LIST	n/a
			8 - ARCHIPELS	n/a
			9 - HAW HAMBURG	n/a
			10 - DANUBE TECH	n/a
			11 - Spherity GmbH	n/a
			12 - UNIPD	n/a
			13 - TalTech	n/a
			14 - DIGICITI	n/a
			15 - Neumann	n/a
			16 - RBI	n/a
			17 - GOLDMAN	n/a
			18 - MGTŠ	n/a

Prefinancing payment		Prefinancing guarantee		
Type	Amount	Guarantee amount	Division per participant	
			19 - NTNU	n/a
			20 - UNISOT	n/a
			21 - NDF	n/a
			22 - GRNET S.A.	n/a
			23 - Excid	n/a
			24 - Maritech AS	n/a
			25 - HASHNET	n/a
			36 - VALUNODE	n/a

Reporting and payment modalities (art 21, 22):

Mutual Insurance Mechanism (MIM): No

Restrictions on distribution of initial prefinancing: The prefinancing may be distributed only if the minimum number of beneficiaries set out in the call condititions (if any) have acceded to the Agreement and only to beneficiaries that have acceded.

Interim payment ceiling (if any): 90% of the maximum grant amount

No-profit rule: Yes

Late payment interest: ECB + 3.5%

Bank account for payments:

[redacted]

Conversion into euros: Double conversion

Reporting language: Language of the Agreement

4.3 Certificates (art 24):

Certificates on the financial statements (CFS):

Conditions:

Schedule: only at final payment, if threshold is reached

Standard threshold (beneficiary-level):

- financial statement: requested EU contribution to costs ≥ EUR 325 000.00

4.4 Recoveries (art 22)

First-line liability for recoveries:

Beneficiary termination: Beneficiary concerned

Final payment: Coordinator

After final payment: Beneficiary concerned

Joint and several liability for enforced recoveries (in case of non-payment):

Limited joint and several liability of other beneficiaries — up to the maximum grant amount of the beneficiary

Joint and several liability of affiliated entities — n/a

5. Consequences of non-compliance, applicable law & dispute settlement forum

Applicable law (art 43):

Standard applicable law regime: EU law + law of Belgium

Dispute settlement forum (art 43):

Standard dispute settlement forum:

EU beneficiaries: EU General Court + EU Court of Justice (on appeal)

Non-EU beneficiaries: Courts of Brussels, Belgium (unless an international agreement provides for the enforceability of EU court judgements)

6. Other

Specific rules (Annex 5): Yes

Standard time-limits after project end:

Confidentiality (for X years after final payment): 5

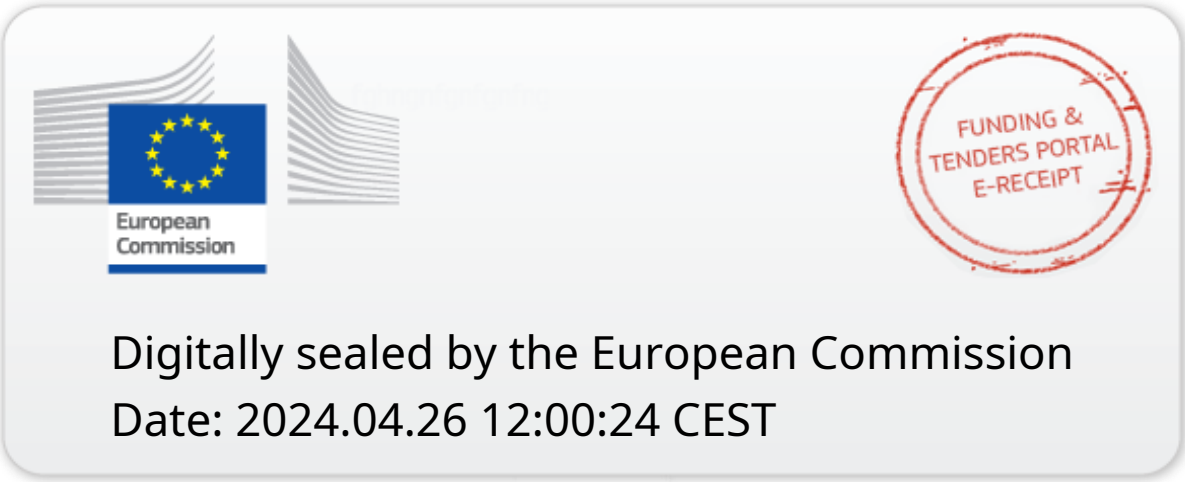
Record-keeping (for X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

Reviews (up to X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

Audits (up to X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

Extension of findings from other grants to this grant (no later than X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

Impact evaluation (up to X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)



This electronic receipt is a digitally signed version of the document submitted by your organisation. Both the content of the document and a set of metadata have been digitally sealed.

This digital signature mechanism, using a public-private key pair mechanism, uniquely binds this eReceipt to the modules of the Funding & Tenders Portal of the European Commission, to the transaction for which it was generated and ensures its full integrity. Therefore a complete digitally signed trail of the transaction is available both for your organisation and for the issuer of the eReceipt.

Any attempt to modify the content will lead to a break of the integrity of the electronic signature, which can be verified at any time by clicking on the eReceipt validation symbol.

More info about eReceipts can be found in the FAQ page of the Funding & Tenders Portal.

(https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq)