Secure management of IoT devices lifecycle through identities, trust and distributed ledgers

D8.1: H - Requirement No. 1

Document Summary Information

<table>
<thead>
<tr>
<th>Grant Agreement No</th>
<th>Acronym</th>
<th>ERATOSTHENES</th>
</tr>
</thead>
<tbody>
<tr>
<td>101020416</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Full Title</th>
<th>Secure management of IoT devices lifecycle through identities, trust and distributed ledgers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Date</td>
<td>01/10/2021</td>
</tr>
<tr>
<td>Duration</td>
<td>42 months</td>
</tr>
<tr>
<td>Project URL</td>
<td><a href="http://www.eratosthenes-project.eu">www.eratosthenes-project.eu</a></td>
</tr>
<tr>
<td>Deliverable</td>
<td>H - Requirement No. 1</td>
</tr>
<tr>
<td>Work Package</td>
<td>WP8</td>
</tr>
<tr>
<td>Contractual due date</td>
<td>31/12/2021</td>
</tr>
<tr>
<td>Nature</td>
<td>Ethics</td>
</tr>
<tr>
<td>Dissemination Level</td>
<td>Public</td>
</tr>
<tr>
<td>Responsible author</td>
<td>DBC</td>
</tr>
<tr>
<td>Authors</td>
<td>George Athanasiou, Sara Nabaraoui (DBC)</td>
</tr>
<tr>
<td>Internal reviewers</td>
<td>Konstantinos Loupos (INLE)</td>
</tr>
</tbody>
</table>
**Revision history (including peer reviewing & quality control)**

<table>
<thead>
<tr>
<th>Version</th>
<th>Issue Date</th>
<th>% Complete</th>
<th>Changes</th>
<th>Contributor(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1</td>
<td>25/11/2021</td>
<td>40%</td>
<td>Initial Deliverable Structure &amp; Basic Processes</td>
<td>George Athanasiou, Sara Nabaraoui (DBC)</td>
</tr>
<tr>
<td>V2</td>
<td>30/11/2021</td>
<td>70%</td>
<td>Final content of sections 1-5, Circulation to consortium</td>
<td>George Athanasiou, Sara Nabaraoui (DBC)</td>
</tr>
<tr>
<td>V3</td>
<td>08/12/2021</td>
<td>100%</td>
<td>Final content of Sections 6-10</td>
<td>George Athanasiou, Sara Nabaraoui (DBC) Arnor Solberg (TELLU) Manel Rodriguez (IDIADA) Rohit Bohara (DWG)</td>
</tr>
<tr>
<td>V4</td>
<td>13/12/2021</td>
<td>100%</td>
<td>Internal review</td>
<td>Konstantinos Loupos (INLE)</td>
</tr>
<tr>
<td>V5</td>
<td>16/12/2021</td>
<td>100%</td>
<td>Final version approved by consortium</td>
<td>George Athanasiou (DBC) Konstantinos Loupos (INLE)</td>
</tr>
</tbody>
</table>

**Disclaimer**

The content of the publication herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the ERATOSTHENES consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the ERATOSTHENES Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the ERATOSTHENES Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

**Copyright message**

© ERATOSTHENES Consortium, 2020-2025. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

© ERATOSTHENES, 2021
# Table of Contents

1 Executive Summary .................................................................................................................. 4  
2 Introduction ............................................................................................................................. 5  
  2.1 Mapping ERATOSTHENES Outputs .................................................................................... 5  
  2.2 Deliverable Overview and Report Structure ....................................................................... 6  
3 Consent within ERATOSTHENES ............................................................................................. 7  
  3.1 Data collection activities ..................................................................................................... 7  
  3.2 Consent processes within ERATOSTHENES ................................................................. 7  
  3.3 Voluntary participation in pilots ......................................................................................... 7  
  3.4 Consent requirements for the ERATOSTHENES pilots ...................................................... 8  
  3.5 Data lifecycle ....................................................................................................................... 9  
4 Informed consent form for participation in research ............................................................... 10  
5 Elements of the information sheet for research participants ............................................... 11  
6 Information sheet for research participants of the 1st Pilot (Connected Vehicles) ............... 12  
7 Information sheet for research participants of the 2nd Pilot (Smart Health) ....................... 17  
8 Information sheet for research participants of the 3rd Pilot (Industry 4.0) ......................... 22  
9 Incidental findings policy ........................................................................................................ 27  
  9.1 Definition of incidental findings ....................................................................................... 27  
  9.2 Ethical concerns raised by incidental findings ................................................................... 27  
  9.3 The role of incidental findings risk assessment and the importance of relevant informed consent 28  
  9.4 Incidental findings policy in ERATOSTHENES ............................................................... 28  
10 Conclusions .......................................................................................................................... 29  

© ERATOSTHENES, 2021
1 Executive Summary

ERATOSTHENES H - Requirement No. 1 document responds to the first “ethics requirement” by the European Commission by analysing how consent and data collection will be handled within the project. This is regarded as work performed in WP8 (Ethics Requirements) and this report is the first deliverable on requirement No 1. In particular, the procedures and criteria that will be used to identify and recruit research participants followed by the informed consent procedures including personal data processing that will be implemented for the participation of humans, are presented. Templates of the informed consent/assent forms and information sheets for each pilot were proposed by the ERATOSTHENES pilot leaders and approved by the consortium. The deliverable also presents the procedures and criteria that will be used to identify/recruit research participants. Finally, an incidental findings policy is proposed.

As this report on the Ethics procedures is only the very first one, there will be three more deliverables that will follow this report with details on the opinions of the ethics and/or other competent authorities for the research with humans (requirement no. 2), POPD requirements (requirement no.3) on the DPOs and GDPR processes and finally the NEC report (requirement no. 5) on the materials imported/exported from the EU.
2 Introduction

2.1 Mapping ERATOSTHENES Outputs

The purpose of this section is to map ERATOSTHENES Grant Agreement (GA) commitments, both within the formal Deliverable and Task description, against the project’s respective outputs and work performed.

<table>
<thead>
<tr>
<th>ERATOSTHENES GA Component Title</th>
<th>ERATOSTHENES GA Component Outline</th>
<th>Respective Document Chapter(s)</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>DELIVERABLE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D8.1 H - Requirement No. 1</td>
<td>D7.1 will include:</td>
<td>Sections 3-9</td>
<td>The current report responds to the first 'ethics requirement' received from the European Commission.</td>
</tr>
<tr>
<td></td>
<td>• The procedures and criteria that will be used to identify/recruit research participants.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The informed consent procedures including personal data processing that will be implemented for the participation of humans.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Templates of the informed consent/assent forms and information sheets (in language and terms intelligible to the participants) including personal data processing.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Details on an incidental findings policy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WP/TASKS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WP8</td>
<td>This work package sets out the 'ethics requirements' that the project must comply with.</td>
<td>Sections 3-9</td>
<td>Chapters 3-6 include: the procedures and criteria that will be used to identify/recruit research participants; the informed consent procedures including personal data processing that will be implemented for the participation of humans; templates of the informed consent/assent forms and information sheets (in language and terms intelligible to the participants) including personal data processing details on an incidental findings policy. Incidental findings policy.</td>
</tr>
</tbody>
</table>
2.2 Deliverable Overview and Report Structure

The present report is structured around 8 Sections as follows:

- Section 1: Executive summary of the deliverable
- Section 2: Introduction and general overview of the requirements of the deliverable in comparison to what is mentioned in the Grant Agreement.
- Section 3: Detailed analysis on how consent and data collection is managed within ERATOSTHENES project.
- Section 4: Informed consent form (template) for participant is research.
- Section 5: Presentation of the components of the elements of the information sheet for research participants.
- Section 6: Information sheet for research participants of the 1st Pilot.
- Section 7: Information sheet for research participants of the 2nd Pilot.
- Section 8: Information sheet for research participants of the 3rd Pilot.
- Section 9: Incidental Findings Policy.
- Section 10: Conclusions.
3 Consent within ERATOSTHENES

3.1 Data collection activities

The data collection activities that will be performed within ERATOSTHENES events, will strictly adhere to EC regulation as well as the legislation of individual Member States and Associated Countries. The following specific cases for data collection are immediately identified:

- **The collection of personal, non-sensitive data within the ERATOSTHENES public events (workshops, pitstops etc.).** WP6 foresees the organization of the ERATOSTHENES advisory board workshops, demonstrations and public dissemination events, as a means to receive valuable stakeholder and end-user feedback within the project’s lifecycle. Should the collection of data via questionnaires or surveys be required within the ERATOSTHENES workshops, it will only entail the collection of personal, non-sensitive data. In such cases, participants will be presented with a consent form, available both in English and the local languages of the locations where each ERATOSTHENES event will be held. The data will be appropriately anonymised prior to any processing.

- **Written and Audio/Visual documentation of the ERATOSTHENES demos/pilots & dissemination events.** The ERATOSTHENES demos will be extensively documented by means of collecting written and photographic evidence, as well as audio/video capture. As previously stated, the participants of the project’s pilots will be debriefed and fully notified of all the pilot-related activities, including the documentation activities. Consent forms will be made available to the participants available both in English and the local language in the event location. Volunteers (in case that they will be invited to the pilots) will be able to withdraw from these activities at any given time.

ERATOSTHENES does not foresee the need to collect sensitive information of any kind. The consortium has also set in place a plan for ensuring the consent of every participant in the case of data collection activities.

3.2 Consent processes within ERATOSTHENES

The Consortium has already identified certain cases when consent of individual participants to project activities (that might require data collection) is needed. Four forms of consent are identified:

- When not expressly granted, **Implied Consent** can be inferred by participation to the ERATOSTHENES workshops and public events by persons that are willing observers, without their participation in data collection and feedback activities,

- **Express Consent** in written or verbal form will be required of participants to ERATOSTHENES workshops and events that participate in activities that require feedback and data collection through questionnaires etc. for the purposes of collecting User Requirements etc.,

- **Informed Consent** in written form will be required for participation in the ERATOSTHENES demos/pilots,

- **Unanimous Consent**, or general consent, by a group of several parties is consent given by all parties and is currently unforeseen.

Templates for Consent forms for audio/visual recording, participation in ERATOSTHENES pilots or feedback collection will be made available as part of T7.6. The involved partners, under the supervision of the Technical Coordinator, will be responsible to collect and anonymise the information prior to any processing, and the Project Coordinator will be in charge of maintaining an archive with the consent forms and documenting the related activities in the annual WP7 reports.

3.3 Voluntary participation in pilots

Participants for the ERATOSTHENES pilots will be identified and selected among:

- Project partners,
- Other employees from the partners organisations,
- End-user partner organizations (if required),
• Other invited end-user representatives (if required),
  • Research and Academia (if required).

The Consortium will not discriminate among volunteers on basis of their race, ethnicity, religious, or political beliefs etc. but will exercise caution in order to maintain demographic diversity in terms of age and gender balance among volunteers. Participants unable to give consent will be excluded from participating in the ERATOSTHENES pilots. Minors, the elderly, and persons that are mentally impaired (e.g. intoxicated, sleep-deprived, showing signs of high stress, etc.) are thus excluded. The Consortium also retains the right to exclude a volunteer from participation or interrupt her/his participation in case of conflict of interest (such as participation to other relevant studies). ERATOSTHENES states that there are no foreseeable risks to participants to project activities (physical or otherwise).

3.4 Consent requirements for the ERATOSTHENES pilots

Informed Consent requires three elements: (i) voluntary participation, (ii) competence and (iii) comprehension. In order to conform to the requirements, set in place by the Nuremberg Code1, the Declaration of Helsinki2, the APA Ethics Code3 and relevant EU legislation4, the Informed Consent forms need to include, at minimum, the following information:

• A statement that ERATOSTHENES involves research subjects and an explanation of the main purpose.
• The expected duration of the subject's participation in the pilot activity.
• A description of the procedures to be followed with focus on the experimental procedures.
• A statement that participation is voluntary.
• Information about who is organising and funding the research.
• A description of any reasonably foreseeable risk, discomfort or disadvantages. (First Aid and medical care will be available during the demonstration.)
• A description of any benefits to the subject or to others, which may reasonably be expected from the research, thus avoiding inappropriate expectations.
• A statement describing the procedures adopted for ensuring data protection/confidentiality/privacy including duration of storage of personal data and curation procedures.
• A description of handling of incidental findings.
• A reference to whom to contact for answers to pertinent questions about the research and research subjects' rights, and whom to contact in the event of a research-related injury to the subject.
• A statement offering the subject the opportunity to ask questions and to withdraw at any time from the research without consequences.
• An explanation of what will happen with the data or samples at the end of the research period and if the data/samples are retained or sent/sold to a third party for further research.
• Information about what will happen to the results of the research.

Finally, the participants will have to date, sign and initial the form, declaring that:

• They understand the purpose of the pilot,
• They have been given all the information that they have asked for,
• They agree to participate to the pilot,
• They understand that they reserve the right to ask for clarifications during the pilot and that they can withdraw at any given time.

Prior to the pilots, participants will be guided through the consent form and all pilot activities by qualified research staff.

---

3 https://www.apa.org/ethics/code
3.5 Data lifecycle

Furthermore, participants will be fully informed about information handling during all the stages of the data lifecycle, including:

- **Where and how this information it will be stored.** The partner responsible for the data collection and processing will also be responsible to ensure the security of the facilities and the confidentiality of the data, with support from the Project Coordinator and the Technical Coordinator.

- **Who will have access rights to it.** Qualified research personnel will have access to the data gathered from the participants after they have been anonymised. Consent forms will only be accessed by the Coordinator and/or the Data Protection Officer of the organisation collecting and processing data.

- **How long it will be stored.** Only during the project lifecycle. The related partner and the Coordinator will be responsible to delete and destroy data sets after the project’s conclusion.

- **How it will be anonymised and processed.** The Data Protection Officer of the partner involved in these activities, will be responsible to anonymise any collected data sets. Only the Coordinator or a certified Data Protection Officer will have access to non-anonymised sets, in order to facilitate the removal of a user’s data, should it be requested by the user. Any processing (automatic or manual) will be performed only on anonymised sets.

The signed consent statements will be held on archive by the Project Coordinator and the involved partner, and will be relayed to the Project Officer (all relevant documents will be part of the annual project management reports). Furthermore, **participants will be able to withdraw their consent forms and data at any given time.** Any partner involved in data collection and data processing will be required to **provide assurance that the data will not be mishandled or utilized outside the expected scope of the project**, along with the verification of their respective national Data Protection Authorities⁵, when deemed necessary.

---

4 Informed consent form for participation in research

[BEGINNING OF THE FORM]

I, undersigned [name] [date and place of birth – natural person] [contact details], hereby give my consent to take part in the research related to the pilot [name] carried out by the ERATOSTHENES Consortium.

1. I have been informed that the ERATOSTHENES project (Secure management of IoT devices lifecycle through identities, trust and distributed ledgers) is a research project currently run under the Horizon 2020 Framework Programme under the grant agreement no. 101020416. The coordinator of the project is Mr. Konstantinos Loupos, INLECOM INNOVATION (INLE) (konstantinos.loupos@inlecomsystems.com), who may be contacted with regard to any question regarding my participation.

2. I have been informed about the nature and the purposes of the project, including the duration and the possible risks and benefits of participation. I have read and understood the Information Sheet dated [DD/MM/YYYY], or it has been read to me. I have had all my questions answered to my satisfaction.

3. I understand that my participation in the research will include [describe briefly] as set out in the Information Sheet dated [DD/MM/YY].

4. I have been informed that I can also address any ethical questions or concerns arising from this research to the Ethical and Legal Manager of the project, Dr. George Athanasiou, DBC EUROPE SA (DBC) (gathanasiou@dbceurope.eu).

5. I understand [I will / I will not] be paid for my participation.

6. I give this consent fully informed, freely and voluntarily and I understand that I am free to withdraw my consent and discontinue my participation at any time without any negative consequences.

7. The relevant laws of [country] shall apply.

Done in two copies, of which one is for the ERATOSTHENES Consortium and one for the participant.

Name of the participant: __________________________________________

Place / date: ___________________________________________________

Signature: _______________________________________________________

[END OF THE FORM]
5 Elements of the information sheet for research participants

The elements listed below will be included in the information administered to potential participants of ERATOSTHENES pilots and/or other activities. It is the task of each pilot partner (or the partner organizing the relevant activity) to creatively tailor the information points or elements listed below to the concrete circumstances and capacities of the person concerned.

1. An overall description of the ERATOSTHENES project (including information about the financing of the project and possible conflict of interest);
2. An overall description in a comprehensive manner of the ERATOSTHENES system’s architecture;
3. The overall description of the ERATOSTHENES pilot where the research participant is engaged (date, place, aims, activities and tools applied in the pilot, participating partners);
4. The criteria and procedure to engage participants in the project (for end users – those working at the organizations of end-user partners and having expertise and skills for the type of pilot he/she participates; for volunteers – those who work at partners’ organizations or those who have been already engaged as a volunteer by end-user partner and when necessary have relevant skill for the specific pilot);
5. The pilot procedures, including the approximate number of participants in the pilot;
6. The participant’s role in the research project;
7. Safety measures to be taken during pilot;
8. Foreseeable risks, inconveniences and benefits, if any;
9. The free and voluntary nature of the participation;
10. The possibility to withdraw from the pilot at any time without consequences;
11. The responsibility of the participant and foreseeable circumstances and reasons where the participant’s involvement may be terminated;
12. Confidentiality of participant identity (if applicable);
13. Expected duration of the pilot and the participant’s specific participation;
14. The conditions of insurance;
15. Name and contact details of the ERATOSTHENES representative to enable the participant asking questions.
6 Information sheet for research participants of the 1st Pilot (Connected Vehicles)

1. An overall description of the ERATOSTHENES project

ERATOSTHENES project (Secure management of IoT devices lifecycle through identities, trust and distributed ledgers) is a research project currently run under the Horizon 2020 Framework Programme under the grant agreement no. 101020416. The EU-funded ERATOSTHENES project builds on recent challenges of Internet of Things (IoT) networks, including: lack of security visibility, lack of effective information sharing between organisations and availability of tools for CERTs/CSIRTs, heterogeneity of IoT devices, lack of a common trust enforcement mechanism and relevant standards, lack of a transparent identity and privacy frameworks and lacking security training and security protocols’ adoption for persons and devices. ERATOSTHENES will devise a novel distributed, automated, auditable, yet privacy-respectful, Trust and Identity Management Framework intended to dynamically and holistically manage the lifecycle of IoT devices, strengthening trust, identities, and resilience in the entire IoT ecosystem, supporting the enforcement of the NIS directive, GDPR and the Cybersecurity Act.

2. An overall description in a comprehensive manner of the ERATOSTHENES system’s architecture (draft version, the first version of the architecture will be delivered in D1.3 and the final one in D1.4)

The following figure presents a high-level overview of the envisioned architecture. The proposed solution addresses the lack of trust in large-scale networks consisting of various IoT devices and vendors in complex real-world scenarios. The solution will enhance trust in decentralized networks introducing end-to-end trust management with dynamic, self-deployment and recovery. ERATOSTHENES envisions to develop a decentralised and contextual Trust and Identity Management Framework for resource-restricted IoT environments well-suited for industrial applications following a Self-sovereign approach. The solution comprises of two major components, the Identity Manager (IdM), and Trust Manager and Broker (TMB), which relies either on the distributed network itself or on network coordinators (gateways) through the automated deployment of Trust Agents across the network.

The Trust Agent will be deployed and executed on the device as a containerized (TEE/TPM) or virtualized service (SμV), depending on the device’s processing capabilities. The device network enrolment will follow a context-based reputation approach, through which it will adopt its initial trust value score to ensure dynamic/automated deployment of the device in the distributed network. The TMB is needed to produce updated trust scores based on the real-time evaluation of device behaviours during established interactions in addition to feedback and recommendations gathered from other devices, based on three core trust computation algorithms and trust evaluation models (network experience, reputation, and contextual attributes). Their trust scores, along with the access policy and identities management for authentication purposes, will be securely stored and publicly shared through an inter-ledger implementation within the IoT network guaranteeing their transparency, integrity, authenticity, and authorization.
Furthermore, the solution will be based on a next-generation distributed inter-ledger approach with focus to self-aspects and collective threat intelligence in distributed networks of heterogeneous IoT devices. For these, authoritative consensus algorithms are usually deployed that rely on a centralized infrastructure to validate data; however, the validation speed is quite faster than the conventional algorithms (PoW, PoS). Such an algorithm would void the purpose of employing DLT technologies in IoT as the purpose of using DLT is to decentralize trust and enable sovereign-identity.

Thus, we envision the application of a **novel hybrid consensus model founded on the Proof-of-Importance algorithm.** Proof-of-Importance (PoI) algorithms work by judging the "importance" of a party in the operation of the overall DLT "network". If a party has multiple transactions in the network and provides a consistent "influx" of network utilization, the party is considered pivotal in the network’s evaluation. During the project, a PoI algorithm will be theorized, conscripted and applied in IoT by using the number of different devices an IoT device has exchanged data with as well as its volume based on the data production rate of the device and intermittent time between transmissions. This would be close to the real representation of the value an IoT device offers to a network, as the time it has been active on the network, the number of interactions it has had as well as the data volume it has exchanged all play a crucial role in its evaluation. A highly experimental initiative of the project as no previous attempt has been made at scientifically defining a PoI algorithm for the world of IoT.

By using a self-sovereign identity approach for the decentralised IdM, the authentication of the different IoT devices will be performed in a distributed manner, and thanks to the functionality associated with this approach, transmission channels will be encrypted and therefore secure based on **decentralised identifiers (DID) and Verifiable Credentials (VC).** Lastly, the overall framework to support secure lifecycle management (as the core project objective) will be accompanied by a system manager, which will host a series of required added-value services such as: i) Automated recovery after an attack based on a multi-layer approach ii) the aforementioned DLT implementation on network level, and iii) Blockchain-based (independent from the DLT implementation supporting the trust and identity management) cyberthreat information management.
3. The overall description of the ERATOSTHENES pilot where the research participant is engaged (date, place, aims, activities and tools applied in the pilot, participating partners)

**Date:** October 2022 (estimated)

**Place:** IDIADA’s facilities

**Aims:**
1. Support the transition from a bench deployment to the physical world for secure connected vehicle interactions
2. Become a key enabler of trustworthiness in vehicle to vehicle, vehicle to infrastructure or vehicle to cloud interaction.
3. Be a homogenous enabler within over the air software update mechanisms, a key issue for vehicle cyberattacks.

**Activities:**
First will be necessary to perform research on:
4. Identity management for over-the-air software updates and connected vehicles interactions
5. State of the art methods for secure and distributed asset identification for testing deployment
6. Distributed trust management in vehicle OBU and RSU deployments
7. Trust policies and recovery ability of trust agents. Integration of PUF for OBU authentication and authorization
8. Cyberthreats information sharing to CERTS/CSRTS interface
9. Monitor of suspicious and anomalous indicators in V2V communication
10. A setup and proof of concept of application and service architecture in an automotive testbed

After this activity is finalized and the concepts are clear the activities to perform the use cases validation will be arranged starting with the validation criteria definition for each functionality developed during the project. Continuing through the validation use cases activities and ending with the conclusions extraction from the results of the tests.

The validation process will have different loops previously defined at some points of the technology development process to move gradually the validation of the outputs of the project from a lab-test to production deployment.

**Tools:** IDAPT, RSU, server, vehicles, technological developments within ERATOSTHENES solution.

**Partners:** IDIADA (leader), ATOS, ENG, EUL will be the partners more involved in pilot 1. Other academic and industrial partners will be consulted during the Pilot activities.

4. The criteria and procedure to engage participants in the project (for end users – those working at the organizations of end-user partners and having expertise and skills for the type of pilot he/she participates; for volunteers – those who work at partners’ organizations or those who have been already engaged as a volunteer by end-user partner and when necessary have relevant skill for the specific pilot)

The main participants will be the project partners and the technical experts in charge of the validation activities.
5. The pilot procedures, including the approximate number of participants in the pilot

- Define requirements.
- Configure and program each actor in Pilot 1 to be able to carry out the interactions between them.
- Perform validation loops against the requirements previously defined.

6. The participant’s role in the research project

The participant’s roles include definition of the requirements that will be used to evaluate the pilot activities, a role that will be in charge of configuring and programming each actor of the validation field. Another technical role will be the one more involved in the development during the project solution giving support on the validation activities. Each role includes conducting research in order to carry out the pilot activities.

7. Safety measures to be taken during pilot

IDLADA has its own internal policies to check the vehicle safety before each validation/test.

If required, it can be defined more specific during the project.

8. Foreseeable risks, inconveniences and benefits, if any

Risks related with input tasks

1. The applications to be developed inside the scope of the project are not enough mature to be integrated in the OBU and validate it.
2. The applications development has delay, resulting in not having enough time to perform the validations on pilot.
3. Deliverables from previous WP differ from the expected outcome, resulting in a redefining of the validation plan.

Risk related with integration

1. The applications developed are not compatible with the OBU (IDAPT)
2. The applications developed are not compatible with the connectivity in the infrastructure

COVID risks:

1. Travels are limited due to pandemic restrictions

The expected benefits are the aims specified previously.

9. The free and voluntary nature of the participation.

You are not obliged to participate in project’s and pilot’s activities. The participation is free is and voluntary.
10. The possibility to withdraw from the pilot at any time without consequences

You are allowed to cease your participation in the pilot at any time without consequences.

11. The responsibility of the participant and foreseeable circumstances and reasons where the participant’s involvement may be terminated

The responsibility of the participant and foreseeable circumstances and reasons where the participant’s involvement may be terminated: end users are responsible for the professional handling of equipment, following standard procedure and orders from their superiors to avoid risks and harm to themselves and others.

12. Confidentiality of participant identity (if applicable)

Unless otherwise is required under the law or requested by you, your identity and the fact of participation in the pilot are available for ERATOSTHENES consortium. ERATOSTHENES consortium takes all the possible measures to respect your data protection and privacy rights and follows the principles of data minimization, purpose limitation and other applicable. ERATOSTHENES partners also pseudonymize and anonymize personal data whenever is feasible.

13. Expected duration of the pilot and the participant’s specific participation

Pilot 1 activities will be performed from month 12 to month 41 as it is specified in the gantt chart. This period includes previous tasks, for example the PoC evaluation. But the tasks that will provide outcomes of Pilot 1 technology validation activities will start at M19 until M41.

14. The conditions of insurance

The standard rules of insurance in organization you work for are applied.

15. Name and contact details of the ERATOSTHENES representative to enable the participant asking questions.

Alejandro Manilla

Alejandro.Manilla@idiada.com

Idiada
7 Information sheet for research participants of the 2nd Pilot (Smart Health)

1. An overall description of the ERATOSTHENES project

ERATOSTHENES project (Secure management of IoT devices lifecycle through identities, trust and distributed ledgers) is a research project currently run under the Horizon 2020 Framework Programme under the grant agreement no. 101020416. The EU-funded ERATOSTHENES project builds on recent challenges of Internet of Things (IoT) networks, including: lack of security visibility, lack of effective information sharing between organisations and availability of tools for CERTs/CSIRTs, heterogeneity of IoT devices, lack of a common trust enforcement mechanism and relevant standards, lack of a transparent identity and privacy frameworks and lacking security training and security protocols’ adoption for persons and devices. ERATOSTHENES will devise a novel distributed, automated, auditable, yet privacy-respectful, Trust and Identity Management Framework intended to dynamically and holistically manage the lifecycle of IoT devices, strengthening trust, identities, and resilience in the entire IoT ecosystem, supporting the enforcement of the NIS directive, GDPR and the Cybersecurity Act.

2. An overall description in a comprehensive manner of the ERATOSTHENES system’s architecture (draft version, the first version of the architecture will be delivered in D1.3 and the final one in D1.4)

The following figure presents a high-level overview of the envisioned architecture. The proposed solution addresses the lack of trust in large-scale networks consisting of various IoT devices and vendors in complex real-world scenarios. The solution will enhance trust in decentralised networks introducing end-to-end trust management with dynamic, self-deployment and recovery. ERATOSTHENES envisions to develop a decentralised and contextual Trust and Identity Management Framework for resource-restricted IoT environments well-suited for industrial applications following a Self-sovereign approach. The solution comprises of two major components, the Identity Manager (IdM), and Trust Manager and Broker (TMB), which relies either on the distributed network itself or on network coordinators (gateways) through the automated deployment of Trust Agents across the network.

The Trust Agent will be deployed and executed on the device as a containerized (TEE/TPM) or virtualized service (SuV), depending on the device’s processing capabilities. The device network enrolment will follow a context-based reputation approach, through which it will adopt its initial trust value score to ensure dynamic/automated deployment of the device in the distributed network. The TMB is needed to produce updated trust scores based on the real-time evaluation of device behaviours during established interactions in addition to feedback and recommendations gathered from other devices, based on three core trust computation algorithms and trust evaluation models (network experience, reputation, and contextual attributes). Their trust scores, along with the access policy and identities management for authentication purposes, will be securely stored and publicly shared through an inter-ledger implementation within the IoT network guaranteeing their transparency, integrity, authenticity, and authorization.
Furthermore, the solution will be based on a next-generation distributed inter-ledger approach with focus to self-aspects and collective threat intelligence in distributed networks of heterogeneous IoT devices. For these, authoritative consensus algorithms are usually deployed that rely on a centralized infrastructure to validate data; however, the validation speed is quite faster than the conventional algorithms (PoW, PoS). Such an algorithm would void the purpose of employing DLT technologies in IoT as the purpose of using DLT is to decentralize trust and enable sovereign-identity.

Thus, we envision the application of a novel hybrid consensus model founded on the Proof-of-Importance algorithm. Proof-of-Importance (PoI) algorithms work by judging the “importance” of a party in the operation of the overall DLT “network”. If a party has multiple transactions in the network and provides a consistent “influx” of network utilization, the party is considered pivotal in the network’s evaluation. During the project, a PoI algorithm will be theorized, conscripted and applied in IoT by using the number of different devices an IoT device has exchanged data with as well as its volume based on the data production rate of the device and intermittent time between transmissions. This would be close to the real representation of the value an IoT device offers to a network, as the time it has been active on the network, the number of interactions it has had as well as the data volume it has exchanged all play a crucial role in its evaluation. A highly experimental initiative of the project as no previous attempt has been made at scientifically defining a PoI algorithm for the world of IoT.

By using a self-sovereign identity approach for the decentralised IdM, the authentication of the different IoT devices will be performed in a distributed manner, and thanks to the functionality associated with this approach, transmission channels will be encrypted and therefore secure based on decentralised identifiers (DID) and Verifiable Credentials (VC). Lastly, the overall framework to support secure lifecycle management (as the core project objective) will be accompanied by a system manager, which will host a series of required added-value services such as: i) Automated recovery after an attack based on a multi-layer approach ii) the aforementioned DLT implementation on network level, and iii) Blockchain-based (independent from the DLT implementation supporting the trust and identity management) cyberthreat information management.
3. The overall description of the ERATOSTHENES pilot where the research participant is engaged (date, place, aims, activities and tools applied in the pilot, participating partners)

**Date:** February 2024 (estimated)

**Place:** Norway

**Aims:** The main aims of the pilot is to provide realistic requirements to the technical development performed in the project based on real application requirements in the eHealth domain, and to validate developments and technologies provided in the project.

**Activities:** Main activities is requirement specification and technology validation.

**Tools:** For the Development of the pilot, state of the art development tools such as github, IDEs, Jira, Jenkins, Maven, Helm, Ansible, docker, Kubernetes, Prometheus, Grafana etc will be applied. Moreover, tools developed and provided in the Eratosthenes project will be validated.

**Partners:** Both Technical providers and research partners will be involved. The exact list of partners remains to be defined, but Tellu will work closely with the research partner SINTEF for the pilot.

4. The criteria and procedure to engage participants in the project (for end users – those working at the organizations of end-user partners and having expertise and skills for the type of pilot he/she participates; for volunteers – those who work at partners’ organizations or those who have been already engaged as a volunteer by end-user partner and when necessary have relevant skill for the specific pilot)

As the main aims for the pilot is to identify requirements as input to the technical development in the project and validate innovative features and mechanisms, there is no need to recruit participants outside the project. Rather, we will engage participants in the project necessary to conduct the planned validation. Tellu, as the pilot owner, will develop the pilot. As the validation purely consider functional and non-functional aspects of the technical developments conducted in the project, the validation can be conducted applying test data (i.e., no real patient data is needed in the pilot).

5. The pilot procedures, including the approximate number of participants in the pilot

The main procedure include:

- Identify requirements
- Implement pilot
- Validate provided technologies against the requirements

In general the number of participants include 2-3 participants from Tellu (pilot development partner) and 1-2 participants from each technology provider.
6. The participant’s role in the research project

The roles include the pilot partner participant that are responsible for providing requirements, implementing the pilot and conduct the validation (in cooperation with the technical partner participants), and the technical partner investigating and realizing new technologies and tools that should be validated in the context of the pilots.

7. Safety measures to be taken during pilot

No particular safety measures need to be taken during pilot

8. Foreseeable risks, inconveniences and benefits, if any

In general, a main risk in R&D projects is that the proposed tools or technology do not meet the requirements. The inconvenience is that the challenges remains to be solved. For Tellu the potential benefit is in particular that Tellu can build a novel and advanced identity and trust management solution based on the project results.

9. The free and voluntary nature of the participation.

You are not obliged to participate in project’s and pilot’s activities. The participation is free is and voluntary.

10. The possibility to withdraw from the pilot at any time without consequences

You are allowed to cease your participation in the pilot at any time without consequences.

11. The responsibility of the participant and foreseeable circumstances and reasons where the participant’s involvement may be terminated

The responsibility of the participant and foreseeable circumstances and reasons where the participant’s involvement may be terminated. Participants are are responsible for the professional handling of equipment, following standard procedure and orders from their superiors to avoid risks and harm to themselves and others.

12. Confidentiality of participant identity (if applicable)

N/A for this pilot
13. Expected duration of the pilot and the participant’s specific participation

In general, the project follows an iterative and incremental approach. Moreover, since the pilot as mentioned before is concerning identification of requirements and validation of tools and mechanisms that is provided incrementally throughout the project, the pilot duration is considered to last from M28 to M42.

14. The conditions of insurance

The standard rules of insurance in organization you work for are applied.

15. Name and contact details of the ERATOSTHENES representative to enable the participant asking questions.

Arnor Solberg
arnor.solberg@tellu.no
Tellu
8 Information sheet for research participants of the 3rd Pilot (Industry 4.0)

1. An overall description of the ERATOSTHENES project

ERATOSTHENES project (Secure management of IoT devices lifecycle through identities, trust and distributed ledgers) is a research project currently run under the Horizon 2020 Framework Programme under the grant agreement no. 101020416. The EU-funded ERATOSTHENES project builds on recent challenges of Internet of Things (IoT) networks, including: lack of security visibility, lack of effective information sharing between organisations and availability of tools for CERTs/CSIRTs, heterogeneity of IoT devices, lack of a common trust enforcement mechanism and relevant standards, lack of a transparent identity and privacy frameworks and lacking security training and security protocols’ adoption for persons and devices. ERATOSTHENES will devise a novel distributed, automated, auditable, yet privacy-respectful, Trust and Identity Management Framework intended to dynamically and holistically manage the lifecycle of IoT devices, strengthening trust, identities, and resilience in the entire IoT ecosystem, supporting the enforcement of the NIS directive, GDPR and the Cybersecurity Act.

2. An overall description in a comprehensive manner of the ERATOSTHENES system’s architecture (draft version, the first version of the architecture will be delivered in D1.3 and the final one in D1.4)

The following figure presents a high-level overview of the envisioned architecture. The proposed solution addresses the lack of trust in large-scale networks consisting of various IoT devices and vendors in complex real-world scenarios. The solution will enhance trust in decentralized networks introducing end-to-end trust management with dynamic, self-deployment and recovery. ERATOSTHENES envisions to develop a decentralised and contextual Trust and Identity Management Framework for resource-restricted IoT environments well-suited for industrial applications following a Self-sovereign approach. The solution comprises of two major components, the Identity Manager (IdM), and Trust Manager and Broker (TMB), which relies either on the distributed network itself or on network coordinators (gateways) through the automated deployment of Trust Agents across the network.

The Trust Agent will be deployed and executed on the device as a containerized (TEE/TPM) or virtualized service ($\mu$V), depending on the device’s processing capabilities. The device network enrolment will follow a context-based reputation approach, through which it will adopt its initial trust value score to ensure dynamic automated deployment of the device in the distributed network. The TMB is needed to produce updated trust scores based on the real-time evaluation of device behaviours during established interactions in addition to feedback and recommendations gathered from other devices, based on three core trust computation algorithms and trust evaluation models (network experience, reputation, and contextual attributes). Their trust scores, along with the access policy and identities management for authentication purposes, will be securely stored and publicly shared through an inter-ledger implementation within the IoT network guaranteeing their transparency, integrity, authenticity, and authorization.
Furthermore, the solution will be based on a next-generation distributed inter-ledger approach with focus on self-aspects and collective threat intelligence in distributed networks of heterogeneous IoT devices. For these, authoritative consensus algorithms are usually deployed that rely on a centralized infrastructure to validate data; however, the validation speed is quite faster than the conventional algorithms (PoW, PoS). Such an algorithm would void the purpose of employing DLT technologies in IoT as the purpose of using DLT is to decentralize trust and enable sovereign-identity.

Thus, we envision the application of a **novel hybrid consensus model founded on the Proof-of-Importance algorithm**. Proof-of-Importance (PoI) algorithms work by judging the “importance” of a party in the operation of the overall DLT “network”. If a party has multiple transactions in the network and provides a consistent “influx” of network utilization, the party is considered pivotal in the network’s evaluation. During the project, a PoI algorithm will be theorized, conscripted and applied in IoT by using the number of different devices an IoT device has exchanged data with as well as its volume based on the data production rate of the device and intermittent time between transmissions. This would be close to the real representation of the value an IoT device offers to a network, as the time it has been active on the network, the number of interactions it has had as well as the data volume it has exchanged all play a crucial role in its evaluation. A highly experimental initiative of the project as no previous attempt has been made at scientifically defining a PoI algorithm for the world of IoT.

By using a self-sovereign identity approach for the decentralised IdM, the authentication of the different IoT devices will be performed in a distributed manner, and thanks to the functionality associated with this approach, transmission channels will be encrypted and therefore secure based on **decentralised identifiers (DID) and Verifiable Credentials (VC)**. Lastly, the overall framework to support secure lifecycle management (as the core project objective) will be accompanied by a system manager, which will host a series of required added-value services such as: i) Automated recovery after an attack based on a multi-layer approach ii) the aforementioned DLT implementation on network level, and iii) Blockchain-based (independent from the DLT implementation supporting the trust and identity management) cyberthreat information management.
3. The overall description of the ERATOSTHENES pilot where the research participant is engaged (date, place, aims, activities and tools applied in the pilot, participating partners)

**Date:** December 2024 (estimated)

**Place:** Germany

**Aims:** The pilot aims to increase the security by design in industrial IoT network and communication by introducing novel approaches on IoT Asset Identification and the use of disposable IDs to identify trustworthy entities in communication networks.

**Activities:** The activities involve investigating stakeholder requirements towards trust, reliability, security, performance, privacy and economic beneficial impacts, the involvement of industrial stakeholder in testbed implementation and testing, Implementation of a distributed service architecture for assets management and providing of disposable IDs. Setup and proof of concept of application and service architecture in an industrial testbed with heterogeneous IIoT

**Tools:** The cutting edge decentralized, and distributed technologies and advanced tools will be utilized for the design and development of the pilot. Additionally, the tools developed under the project will be used in the pilot.

**Partners:** DWG will be core partner in the pilot. Moreover, academic and industrial partners will be consulted and employed. DWG will adapt a collaborative approach.

4. The criteria and procedure to engage participants in the project (for end users – those working at the organizations of end-user partners and having expertise and skills for the type of pilot he/she participates; for volunteers – those who work at partners’ organizations or those who have been already engaged as a volunteer by end-user partner and when necessary have relevant skill for the specific pilot)

DWG will engage with all relevant partners in transparent manner. A detailed list of requirements and skills will be provided to the interested stakeholders. The work will be carried out with the participation of the project. An external organization or volunteer will be involved only if the work cannot be completed by DWG or the project partners.

5. The pilot procedures, including the approximate number of participants in the pilot

**The main procedures are:**

- Design solution architecture
- Develop Frontend and backend of the solution
- Prepare and program IoT devices
- Test scalability of the solution
Approximately 1 or 2 participants will be required to carry out each procedure.

6. The participant’s role in the research project

The participants’ role includes designing technical architecture for a secure and trusted identity management solution for IoT devices. This will involve deep understanding of embedded systems, real-time operating systems, communication protocols, and web application development.

7. Safety measures to be taken during pilot

There are no safety measures to be taken during the pilot.

8. Foreseeable risks, inconveniences and benefits, if any

Not able to find an industrial partner to test the solution.

9. The free and voluntary nature of the participation.

You are not obliged to participate in project’s and pilot’s activities. The participation is free and voluntary.

10. The possibility to withdraw from the pilot at any time without consequences

You are allowed to cease your participation in the pilot at any time without consequences.

11. The responsibility of the participant and foreseeable circumstances and reasons where the participant’s involvement may be terminated

The responsibility of the participant and foreseeable circumstances and reasons where the participant’s involvement may be terminated: end users are responsible for the professional handling of equipment, following standard procedure and orders from their superiors to avoid risks and harm to themselves and others.

12. Confidentiality of participant identity (if applicable)

Unless otherwise is required under the law or requested by you, your identity and the fact of participation in the pilot are available for ERATOSTHENES consortium. ERATOSTHENES consortium takes all the possible measures to respect your data protection and
privacy rights and follows the principles of data minimization, purpose limitation and other applicable. ERATOSTHENES partners also pseudonymize and anonymize personal data whenever is feasible.

Not applicable for the pilot.

13. Expected duration of the pilot and the participant’s specific participation

The pilot will be carried out from M19 to M41

14. The conditions of insurance

The standard rules of insurance in organization you work for are applied.

15. Name and contact details of the ERATOSTHENES representative to enable the participant asking questions.

Mirko Ross
m.ross@digital-worx.de
Digital Worx GmbH
9 Incidental findings policy

In general, ERATOSTHENES technologies and tasks will not involve personal data processing. Specifically, the pilot activities will mainly involve the inclusion of synthetic data (including the ‘smart health’ pilot). However, ERATOSTHENES project appreciates the importance of an incidental findings policy, i.e. a policy for the handling of findings that are outside the original purpose for which the research activity was conducted, that could be applied in cases that indeed personal data will be included in our activities (accidentally or by intention while the project developments evolve).

9.1 Definition of incidental findings

The notion of incidental findings originated among others, in medical research. In that context, definitions of incidental findings have a medical flavor, which might be also relevant in the context of ERATOSTHENES. For instance, a incidental findings are defined as:

“Findings concerning an individual research participant that has potential health or reproductive importance and is discovered in the course of conducting research but is beyond the aims of the study. This means that IFs may be on variables not directly under study and may not be anticipated in the research protocol.”

The Presidential Commission for the Study of Bioethical Issues (Bioethics Commission) has issued a report for researchers under the title incidental and secondary findings. According to this report incidental findings can be either “anticipatable” or “unanticipatable.”

An anticipatable incidental finding is one that is known to be associated with a test or procedure. Anticipatable incidental findings need not be common or even likely to occur. Their defining characteristic is that the possibility of finding them is known.

Unanticipatable incidental findings include findings that could not have been anticipated given the current state of scientific knowledge. Researchers cannot plan for these types of findings specifically. However, they can consider in advance what they might do if a particular kind of unexpected finding arises, for example, one that could be actionable or lifesaving.

9.2 Ethical concerns raised by incidental findings

The main ethical concern when incidental findings in research occur is how they should be handled if they arise and more specifically, whether or not, such findings should be disclosed to the research participants they relate to. This is a very complex matter as it entails additional (difficult) questions, such as who shall evaluate or assess potential risks and benefits of such disclosure and ultimately take the final decision of whether to communicate such findings or not, whether a medical expert should be involved and consent for this involvement be secured. The financial and psychological implications such findings may have on participants should be taken into consideration as shock may be caused by the discovery of a health problem and costly medical treatment may be necessary as a result. Perhaps, most importantly, the underlying question is what the research participant himself or herself would prefer, know or not to know about any such incidental findings. Most definitely, researchers have a duty to plan for incidental findings and they way to handle them as part of their indisputable general duty of protect participants against harm arising from research participation.

---


9.3  The role of incidental findings risk assessment and the importance of relevant informed consent

A risk assessment exercise is necessary in order researchers to minimise the risks of incidental findings. Researchers should evaluate beforehand the possibility of discovering incidental findings in the context of their research as well as the extent of such possibility, and as soon as these findings will be identified and listed, a further classification between anticiptable and unanticipatable may be merited. An, expert consultation, if needed, will be also important in order to assist researchers for incidental findings’ management, in particular their clinical significance, if any and the potential implications they may have to research participants.

Next step will be a disclosure or communication policy i.e. a detailed policy about the specific incidental findings, which will be communicated to researchers, the way of this communication or disclosure as well as the parties who will be responsible for this difficult task. Finally, a clear policy outlining what follow-up assistance will be provided will be also very important.

It is very important to note that informed consent is absolutely necessary in order to conduct research in an ethical and lawful manner. The European Commission\(^8\) provides some useful guidelines to participants in research on how to acquire a right and adequate informed consent from the research participants. More specifically, participants must be given an informed consent form and detailed information sheets that state what procedures will be implemented in the event of unexpected or incidental findings, specifically whether the participants have the right to know, or not to know, about any such findings. Incidental findings therefore need to be taken into consideration when researchers design their consent forms. More specifically, researchers should inform potential research participants in the informed consent process and forms that:

a. incidental findings may be found (i.e., of the existence of this possibility or risk);
b. the nature of such incidental findings (i.e., a short description);
c. the process by which incidental findings can be evaluated;
d. the circumstances under which they will be communicated to them, as well as of the disclosing process;
e. they can choose whether to receive such communication/disclosure or not.

9.4  Incidental findings policy in ERATOSTHENES

ERATOSTHENES has taken into account the aforementioned ethical considerations pertaining to incidental findings polices and has planned on the way any such findings are to be handled.

In brief, a possible discovery will immediately be reported by the relevant partner to the Project Consortium who in collaboration with the Ethics Committee will decide whether to inform the relevant research participant. The Ethics Committee may suggest the involvement of an expert to perform the assessment/evaluation of the significance of the incidental finding and to inform the research participant about the finding if the participant has opted to be informed.

The decision whether to communicate the incidental finding to the research participant concerned will depend on the choice that research participants have been asked to make in relation to incidental finding handling when they have consented to their participation in the project. In other words, it will depend on whether the research participant has opted to be informed of any such incidental findings regarding his or her health or not. The participants will have also the option to choose whether incidental findings will be disclosed to medical expert to evaluate them and to communicate them to the participant.

Furthermore, any incidental health finding will be anonymised or deleted immediately or immediately after research participant is informed in accordance with the rule stated above. Until anonymization or deletion, incidental findings are subject to the strict measures of data security applicable to the rest of the personal data involved in the project, including the use of reliable servers, authorizations and permissions for access as and encryption. A confidentiality agreement making explicit reference to incidental findings will also be signed by all of the consortium partners.

\(^8\) European Commission, How to complete your ethics self-assessment, 4 February 2019.
10 Conclusions

The present deliverable is the first document responding to the “ethics requirements” (relating to ERATOSTHENES WP8 activities) by the European Commission. We first presented how consent is managed within the ERATOSTHENES project and the way that the Pilot information sheets will be organized. Then we discussed the recruitment/selection of the research participants. The report was concluded with an incidental findings policy. In the following deliverables (D8.2-D8.4) we will have the chance to discuss the GDPR (data privacy) and in general the legal aspects of the ERATOSTHENES project.