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

D5.6 – Interim Report of Piloting Activities and Impact Assessment

Document Summary Information

<table>
<thead>
<tr>
<th>Grant Agreement No</th>
<th>101020416</th>
<th>Acronym</th>
<th>ERATOSTHENES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Title</td>
<td>Secure management of IoT devices lifecycle through identities, trust and distributed ledgers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start Date</td>
<td>01/10/2021</td>
<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>
<td></td>
<td></td>
</tr>
<tr>
<td>Deliverable</td>
<td>D5.6 Interim Report of Piloting Activities and Impact Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work Package</td>
<td>WP5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contractual due date</td>
<td>M26</td>
<td>Actual submission date</td>
<td>30/11/2023</td>
</tr>
<tr>
<td>Nature</td>
<td>R</td>
<td>Dissemination Level</td>
<td>PU</td>
</tr>
<tr>
<td>Responsible author</td>
<td>Rohit Bohara</td>
<td>Lead Beneficiary</td>
<td>DWG</td>
</tr>
<tr>
<td>Authors</td>
<td>Rohit Bohara <a href="mailto:r.bohara@digital-worx.de">r.bohara@digital-worx.de</a> (DWG)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rosella Omana Mancilla <a href="mailto:RosellaOmana.Mancilla@eng.it">RosellaOmana.Mancilla@eng.it</a> (ENG)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cristina Timón López <a href="mailto:mariacristina.timon@um.es">mariacristina.timon@um.es</a> (UMU)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manel Rodriguez <a href="mailto:manel.rodriguez@idiada.com">manel.rodriguez@idiada.com</a> (IDIADA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Utkarsh Goyal <a href="mailto:utkarsh.goyal@tellu.no">utkarsh.goyal@tellu.no</a> (TELLU)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>John Savill &lt; <a href="mailto:john.savill@idiada.com">john.savill@idiada.com</a>&gt; (IDIADA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Arnor Solberg <a href="mailto:arnor.solberg@tellu.no">arnor.solberg@tellu.no</a> (TELLU)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© ERATOSTHENES, 2020
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interval reviewers</strong></td>
<td>Rustem Dautov <a href="mailto:rustem.dautov@sintef.no">rustem.dautov@sintef.no</a> (SINTEF)</td>
</tr>
<tr>
<td></td>
<td>Shukun Tokas <a href="mailto:shukun.tokas@sintef.no">shukun.tokas@sintef.no</a> (SINTEF)</td>
</tr>
<tr>
<td></td>
<td>Hui Song <a href="mailto:hui.song@sintef.no">hui.song@sintef.no</a> (SINTEF)</td>
</tr>
<tr>
<td></td>
<td>Christos Xenakis <a href="mailto:xenakis@unipi.gr">xenakis@unipi.gr</a> (UPRC)</td>
</tr>
</tbody>
</table>

Christos Xenakis <xenakis@unipi.gr> (UPRC)
Jesus Garcia Rodriguez <jesus.garcia15@um.es> (UMU)
D5.6 – Interim Report of Piloting Activities and Impact Assessment

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>v0.1</td>
<td>25/07/2023</td>
<td>1</td>
<td>Initial Deliverable Structure</td>
<td>DWG</td>
</tr>
<tr>
<td>v0.2</td>
<td>15/08/2023</td>
<td>10</td>
<td>Validation and evaluation KPIs and scenario</td>
<td>ENG</td>
</tr>
<tr>
<td>v0.3</td>
<td>24/08/2023</td>
<td>12</td>
<td>Assigned contribution to responsible partner</td>
<td>DWG, ENG</td>
</tr>
<tr>
<td>v0.4</td>
<td>07/09/2023</td>
<td>20</td>
<td>Added executive summary and section 2</td>
<td>DWG</td>
</tr>
<tr>
<td>v0.5</td>
<td>15/09/2023</td>
<td>22</td>
<td>Added Pilot 3 introduction, activities and timeline</td>
<td>DWG</td>
</tr>
<tr>
<td>v0.6</td>
<td>20/09/2023</td>
<td>25</td>
<td>Added test and deployment plan, conclusion</td>
<td>DWG</td>
</tr>
<tr>
<td>v0.7</td>
<td>02/10/2023</td>
<td>95</td>
<td>Pilot 1 and Pilot 2 details, DPIA, SIA, evaluation strategy</td>
<td>DWG, UMU, TELU, IDIADA, UPRC</td>
</tr>
<tr>
<td>v0.8</td>
<td>10/11/2023</td>
<td>96</td>
<td>Review comments</td>
<td>ENG, INLECOM</td>
</tr>
<tr>
<td>v0.9</td>
<td>21/11/2023</td>
<td>99</td>
<td>Address the comments</td>
<td>DWG</td>
</tr>
<tr>
<td>v1.0</td>
<td>27/11/2023</td>
<td>100</td>
<td>Internal review and final version</td>
<td>SINTEF, UPRC, DWG</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.
# Table of Contents

1. Executive Summary ........................................................................................................... 9
2. Introduction ......................................................................................................................... 10
   2.1 Mapping ERATOSTHENES Outputs .............................................................................. 10
   2.2 Deliverable Overview and Report Structure ............................................................... 11
   2.3 Inputs from Other deliverables .................................................................................... 11
   2.4 Progress Since the First Deliverable Version ............................................................... 12
3. Piloting Activities ............................................................................................................... 13
   3.1 Testing Framework ....................................................................................................... 13
   3.2 Deployment Strategy ................................................................................................... 14
   3.3 Evaluation Strategy and Structure .............................................................................. 14
      3.3.1 Requirements and KPIs ......................................................................................... 16
   3.4 Pilot 1: Connected Vehicles ......................................................................................... 17
      3.4.1 Use Cases ............................................................................................................ 18
      3.4.2 Instantiation ......................................................................................................... 20
   3.5 Pilot 2: Smart Health .................................................................................................... 24
      3.5.1 Use Cases ............................................................................................................ 25
      3.5.2 Instantiation ......................................................................................................... 27
   3.6 Pilot 3: Disposable IDs in Industry 4.0 ....................................................................... 33
      3.6.1 Use Cases ............................................................................................................ 35
      3.6.2 Instantiation ......................................................................................................... 36
4. Social Impact Assessment .................................................................................................... 43
   4.1 Pilot 1 SIA ..................................................................................................................... 44
   4.2 Pilot 2 SIA ..................................................................................................................... 44
   4.3 Pilot 3 SIA ..................................................................................................................... 45
5. Data Protection Impact Assessment .................................................................................... 46
   5.0 The ERATOSTHENES Architecture and the Pilots ....................................................... 47
   5.1 Prior Considerations: The Qualification of Personal Data ............................................. 48
      5.1.1 Legal Notions on Personal Data ............................................................................. 48
      5.1.2 ERATOSTHENES: Are Device Identifiers Personal Data? .................................. 49
   5.2 Scope of the Data Protection Impact Assessment .......................................................... 51
   5.3 Data Protection Considerations .................................................................................... 51
      5.3.1 Data Protection Implications-Connected Vehicles ................................................ 52
      5.3.2 Data Protection Implications-Smart Health .......................................................... 53
      5.3.3 Data Protection Implications-Disposable IDs in Industry 4.0 ............................... 56

© ERATOSTHENES, 2020
List of Tables
Table 1: Adherence to ERATOSTHENES Deliverable & Tasks Descriptions ............................................ 10
Table 2: Technical Components included in pilots ............................................................................. 14
Table 3: Pilots’ Functional Requirements and validation means .......................................................... 16
Table 4: Pilots’ External requirements and validation means ............................................................... 16
Table 5: User satisfaction template .................................................................................................. 16
Table 6. Pilot 1 Activities and Timeline since D5.2 ......................................................................... 18
Table 7: Pilot 2 Activities and Timeline since D5.2 ......................................................................... 24
Table 8. Pilot 3 Activities and Timeline since D5.2 ......................................................................... 34
Table 9: Social Impact Assessment Categories .................................................................................. 43
Table 10: Social Impact Assessment Metrics and Values ................................................................... 43
Table 11: Pilot 1 Social Impact Assessment ......................................................................................... 44
Table 12: Pilot 2 Social Impact Assessment ......................................................................................... 45
Table 13: Pilot 3 Social Impact Assessment ......................................................................................... 45
Table 14: Privacy risk scale of Spanish Data Protection Agency ......................................................... 47
Table 15: Privacy Threats identified using DPIA in Pilot 1 normal scenario ..................................... 52
Table 16: Privacy Threats identified using DPIA in Pilot 1 use cases ............................................... 53
Table 17: Traceability threats identified using DPIA in Pilot 1 normal scenario ............................... 53
Table 18: Traceability threats identified using DPIA in Pilot 1 use cases ........................................ 53
Table 19: Privacy threats identified using DPIA in Pilot 2 normal scenario .................................... 55
Table 20: Privacy threats identified using DPIA in Pilot 2 use cases .............................................. 55
Table 21: Privacy threats identified using DPIA in Pilot 3 normal scenario .................................... 56
Table 22: Privacy threats identified using DPIA in Pilot 3 use cases .............................................. 56

List of Figures
Figure 1: Testing and Deployment framework .................................................................................. 13
Figure 2: Pilot 1 architecture diagram ................................................................. 17
Figure 3: Pilot 1 V2I Communication ................................................................. 19
Figure 4: Pilot 1 V2V Communication ................................................................. 19
Figure 5: Pilot 1 Remote Software update ......................................................... 20
Figure 6: MQTT broker deployment logs ......................................................... 20
Figure 7: DTA and IDS/IPS Git repository cloning form central ERATOSOTHENES GitLab ................................................................. 21
Figure 8: Docker list and sizes after running the IDS/IPS module ..................... 22
Figure 9: SSI demo deployment ........................................................................ 23
Figure 10: PUF deployment verification ......................................................... 23
Figure 11: Pilot 2 Architecture Diagram ............................................................ 24
Figure 12: Pilot 2 Gateway Authentication ..................................................... 26
Figure 13: Pilot 2 External Gateway authentication ............................................ 26
Figure 14: Pilot 2 External Service Authentication ............................................ 27
Figure 15: Pilot 2 Trust management of devices and services ......................... 27
Figure 16: Showing the specification of the VM hosted on AWS ...................... 28
Figure 17: PUF enrolment status of the Tellu Gateway .................................... 28
Figure 18: SSI component containers on the server ........................................... 29
Figure 19: TMB Deployment and container logs .............................................. 29
Figure 20: Mongo-Express GUI ..................................................................... 30
Figure 21: TMB Containers in Docker Desktop GUI ....................................... 30
Figure 22: trust-agent and mosquito containers logs ....................................... 31
Figure 23: A simplified digital twin of an RPM gateway ................................... 32
Figure 24: DLT component deployment on the server ...................................... 33
Figure 25: Pilot 3 architecture diagram ............................................................. 33
Figure 26: Pilot 3 Use case 1 and 2 illustration ................................................ 35
Figure 27: Pilot 3 authorization using Disposable ID ........................................ 36
Figure 28: Basic Docker commands ................................................................. 36
Figure 29: Pilot3 deployment script help documentation .................................. 36
Figure 30: git sub-module commands ............................................................... 37
Figure 31: git submodule add example ............................................................ 37
Figure 32: Status of git submodules in pilot3 repository ................................... 37
Figure 33: OS Details of the deployment server .............................................. 38
Figure 34: DLT deployment logs .................................................................... 38
Figure 35: SSI deployment logs ...................................................................... 39
Figure 36: DID generation using curl .............................................................. 39
Glossary of terms and abbreviations used

<table>
<thead>
<tr>
<th>Abbreviation / Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADP</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>CAN</td>
<td>Controller Area Network</td>
</tr>
<tr>
<td>CI/CD</td>
<td>Continuous Integration / Continuous Delivery</td>
</tr>
<tr>
<td>COPD</td>
<td>Chronic Obstructive Pulmonary Disease</td>
</tr>
<tr>
<td>CTI</td>
<td>Cyber Threat Intelligence</td>
</tr>
<tr>
<td>DID</td>
<td>Decentralized Identifier</td>
</tr>
<tr>
<td>DLT</td>
<td>Distributed Ledger Technology</td>
</tr>
<tr>
<td>DMP</td>
<td>Data Management Plan</td>
</tr>
<tr>
<td>DPIA</td>
<td>Data Protection Impact Assessment</td>
</tr>
<tr>
<td>DTA</td>
<td>Deployer of Trust Agents</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Union Agency for Cybersecurity</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GRPC</td>
<td>Google Remote Procedure Calls</td>
</tr>
<tr>
<td>GUID</td>
<td>Globally Unique Identifier</td>
</tr>
<tr>
<td>IdM</td>
<td>Identity Management</td>
</tr>
<tr>
<td>IDS/IPS</td>
<td>Intrusion Detection System / Intrusion Prevention System</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IPC</td>
<td>Inter-Process Communication</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Performance Indicator</td>
</tr>
<tr>
<td>MQTT</td>
<td>MQ Telemetry Transport</td>
</tr>
<tr>
<td>MUD</td>
<td>Manufacturer Usage Description</td>
</tr>
<tr>
<td>MVP</td>
<td>Minimum Viable Product</td>
</tr>
<tr>
<td>PoC</td>
<td>Proof of Concept</td>
</tr>
<tr>
<td>PUF</td>
<td>Physical Unclonable Function</td>
</tr>
<tr>
<td>SecaaS</td>
<td>Security as a Service</td>
</tr>
<tr>
<td>SIA</td>
<td>Social Impact Assessment</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSI</td>
<td>Self-sovereign Identity</td>
</tr>
<tr>
<td>TA</td>
<td>Trust Agent</td>
</tr>
<tr>
<td>TMB</td>
<td>Trust Manager and Broker</td>
</tr>
<tr>
<td>TMRA</td>
<td>Threat Modelling &amp; Risk Assessment</td>
</tr>
<tr>
<td>UUID</td>
<td>Universally Unique Identifier</td>
</tr>
<tr>
<td>V2I</td>
<td>Vehicle to Infrastructure</td>
</tr>
<tr>
<td>V2V</td>
<td>Vehicle to Vehicle</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WiFi</td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
</tbody>
</table>
1 Executive Summary

The deliverable D5.6: Interim Report of Piloting Activities and Impact Assessment describes the activities carried out and planned in the Task 5.2 namely, Pilots Management and Impact Assessment which is part of the work package 5: Framework integration, real-world pilots and cybersecurity exercises. The deliverable reports the initial outcomes of the piloting activities performed by the 3 pilots in the ERATOSTHENES project. These pilots are namely, Pilot 1: Connected Vehicles, Pilot 2: Smart Health, and Pilot 3: Disposable IDs in Industry 4.0. The pilots have their own recipe to integrate, validate and deploy the core technical components developed in the technical work packages 2, 3 and 4.

The core focus of the document is impact assessment of all 3 pilots. It includes social impact assessment and data protection impact assessment. It has been performed for each pilot project separately as they deal with different types of data and target fields. Another important topic covered in this deliverable is tools and pilot evaluation & validation.
2 Introduction

This section outlines fundamental information of the deliverable, task and work packages. It begins by mapping the results of D5.6 with the T5.2 and WP5. Thereafter, the overall structure of the deliverable document is presented with a brief summary of each chapter. Section 2.3 describes the relationship of D5.6 with other deliverables. It also gives details of content that is referred from other deliverables for introduction and painting the full picture. This section would help readers to get the bird eye view of the deliverable D5.6.

2.1 Mapping ERATOSTHENES Outputs

The deliverable is the outcome of the piloting activities performed in the T5.2 and is completely aligned with the objective of WP5 defined in the ERATOSTHENES Grant Agreement document. Purpose of this section is to map ERATOSTHENES Grand Agreement commitments, both within the formal Deliverable and Task description, against the project’s respective outputs and work performed. It is outlined in Table 1.

<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><strong>DELIVERABLE</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D5.6 Interim Report of Piloting Activities and Impact Assessment</td>
<td>Report on the first outcomes of the piloting activities. This deliverable will also and will provide a PIA/DPIA evaluation based on the GDPR.</td>
<td>Chapter 3-5</td>
<td>Chapter 3 describes pilots, their use case, testing, validation and deployment activities. Chapter 4 and 5 are dedicated to data impact assessment and social impact assessment for each pilot.</td>
</tr>
<tr>
<td><strong>TASKS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 5.2 Pilots Management and Impact Assessment</td>
<td>This task will start from the preparation of a detailed Pilot Deployment Plan that will structure all piloting and validation activities, and the preparatory activities for the framework deployment in IoT devices, validation baselines (KPIs) and final evaluation. This task will complement Task 5.1 focusing on the controlled testing and validation of ERATOSTHENES framework. Building upon the CI/CD environment of T5.1, it will provide the functional and non-functional verification of the framework and its sub-components. An automated testing framework will be selected/deployed. Unit</td>
<td>Chapter 3 to 5</td>
<td>Chapter 3 describes piloting activities and Chapter 4, and 5 gives details on impact assessment.</td>
</tr>
</tbody>
</table>
tests will be collected from the development tasks of WP2 to WP4 while integration tests, based upon requirements defined in WP1 will be developed in T5.2. This will also include details on which technology will be validated in each Pilot, and the means for ensuring technical and operational viability. This task will also monitor the above baselines as well as the deployment/validation activities, active throughout the whole WP5 duration, and will provide feedback from the piloting activities to the technical WPs for improvements and technological adaptations/alignment. Lastly, Social Impact Assessment and Data Protection Impact Assessment will be performed for each pilot to ensure alignment with legal requirements and produce exploitation guidelines. Despite the pilots not raising ethics considerations, this task will perform ethics screening when needed. Results will be a planning report (D5.2), an interim management report (D5.6) and a final evaluation report (D5.13) that will consolidate the technological evaluation and benchmarking of the overall system.

2.2 Deliverable Overview and Report Structure

Impact assessment, piloting activities and pilot validation are the themes of this deliverable. They are defined in lengths in the deliverable documents. The deliverable is structured in different chapters which outline specific topics such as social impact assessment, pilot architecture etc. Furthermore, each chapter has sections and sub-sections to provide more details on the topic addressed. The document is structured as follow:

- Chapter 1 gives an overview of the deliverable with an executive summary.
- Chapter 2 outlines the structure and objective of the deliverable and its mapping with other tasks and work packages of the ERATOSTHENES project.
- Chapter 3 describes the piloting activities of each pilot.
- Chapter 4 documents social impact assessment.
- Chapter 5 gives details on data protection impact assessment.
- Chapter 6 sums up the deliverable and gives insights on future activities.

2.3 Inputs from Other deliverables

The deliverable D5.6 is the successor of the D5.2. In D5.2, preparatory activities of pilots and introduction of the impact assessment were given. These topics have been extended in the D5.6 with more details. In the WP5, each pilot has its own task assigned. The pilot development, integration and deployment activities are performed in T5.3, T5.4 and T5.5. And these tasks are overseen by the T5.2. Therefore, the D5.6 contains some outcomes of these tasks which set the platform for D5.7, D5.8 and D5.9. The deliverable has also referenced some previous work from other deliverables for better mapping with other ERATOSTHENES components. Therefore, we have considered referenced deliverables to be input to deliverable D5.6.

- ERATOSTHENES architecture diagram form D1.3 - Preliminary ERATOSTHENES Architecture
2.4 Progress Since the First Deliverable Version

The deliverable D5.6 is the successor of the D5.2. In D5.2, preparatory activities of pilots and introduction of the impact assessment were given. These topics have been extended in the D5.6 with more details. In the WP5, each pilot has its own task assigned. The pilot development, integration and deployment activities are performed in T5.3, T5.4 and T5.5. And these tasks are overseen by the T5.2. Therefore, the D5.6 contains some outcomes of these tasks which set the platform for D5.7, D5.8 and D5.9. The deliverable has also referenced some previous work from other deliverables for better mapping with other ERATOSTHENES components. Therefore, we have considered referenced deliverables to be input to deliverable D5.6.

- ERATOSTHENES architecture diagram form D1.3 - Preliminary ERATOSTHENES Architecture
- Deployment and validation inputs from D5.1- First System integration and Proof of Concept
- Pilot description, KPIs from D1.2 - Use cases, requirements, and methodological Framework
3 Piloting Activities

In the ERATOSTHENES project, various core technical components will be designed and developed to improve cybersecurity of IoT devices throughout their lifecycle e.g., design, implementation, bootstrapping, operation and maintenance phases. These core components are validated, integrated and deployed using various recipes in the 3 pilots. It will make the ERATOSTHENES components for the real-world deployment. The pilots cover use cases from transport, health and industry 4.0.

The pilots will be developed in tasks T5.3, T5.4 and T5.5 respectively. The task T5.2 oversees all 3 pilots and is responsible for the collaboration among them. In this section, brief description of the pilots and their activities are defined. More detailed information about pilots will be given in the deliverables D5.7, D5.8 and D5.9 respectively in month M29.

3.1 Testing Framework

The quality of the technical components and processes designed and developed in the ERATOSTHENES project is of prime importance. It is ensured using multi-facet rigorous testing. It will include unit testing, integration testing and system testing. Various tools used in the testing frameworks are Postman, GitLab\(^1\) source control, Jenkins\(^2\) pipeline, Nexus Repository\(^3\), and containerization tools as shown in Figure 1.

---

\(^1\) GitLab, a DevOps software package which can develop, secure, and operate software. https://ci-cysec.eng.it/gitlab.

\(^2\) Jenkins is an open-source automation server. It helps automate the parts of software development related to building, testing, and deploying, facilitating continuous integration, and continuous delivery. https://ci-cysec.eng.it/jenkins

\(^3\) Nexus Repository OSS is an open-source repository that supports many artifact formats, including Docker, Java™, and npm. https://ci-cysec.eng.it/nexus.

**Figure 1: Testing and Deployment framework**
The planned multi-level testing strategy will ensure that bugs and vulnerabilities in the technical components are detected and fixed at the earliest. In the project, we will do unit, integration and system level testing at the component level and integration and system testing at the pilot level. The testing will involve the following steps.

- Component owner writes and stores unit, integration and system tests for component level in component repository.
- Pilot owner writes and stores integration and system tests for pilot level in pilot repository.
- Jenkins pipeline is used to run tests and collect test results.

More technical details on the test methodology and test results will be given by pilots in the deliverables D5.7, D5.8 and D5.9.

### 3.2 Deployment Strategy

In the ERATOSTHENES project, the pilots will demonstrate the technical components developed in the WP2-4. Each pilot has its own list of technical components and configuration parameters which are driven by the specific use cases of the pilots. Each use case demands a specific set of functionalities and processes.

A deployment server will be set up and maintained by each pilot and they will have their own instances of the technical components. It will allow the pilots to configure the components for specific use cases. For the deployment, we will use the existing CI/CD framework. It includes GitLab, Jenkins pipeline, Nexus Repository and containerization tools as shown in Figure 1.

Multiple tools and technologies are used to automatically deployed the technical components in the pilot environment. There are multiple steps involved in the deployment. They are listed below.

- Technical components partners commit code to the specific GitLab repository of the component.
- Jenkinsfile is added to the component repository by DWG or ENG. It contains the configuration of building docker images and pushing them to the Nexus Registry.
- DWG or ENG configure the pipelines on the Jenkins server.
- For each commit, the Jenkins pipeline is triggered, the docker image is built and pushed to the Nexus Repository.
- Pilot partners define component integration configurations in the specific GitLab repository of the pilot. It includes environment variables, docker compose files, Kubernetes files and scripts.
- Pilot specific deployment server pulls the pilot configurations from the GitLab and docker images from the Nexus Repository and spins off container applications.

More technical details on the deployment strategy will be given by pilots in the deliverables D5.7, D5.8 and D5.9.

### 3.3 Evaluation Strategy and Structure

Evaluation is the process of checking whether the outcomes of the development function as expected, it is about answering “Are we building the right solution”? It helps to determine software’s overall quality, effectiveness, and suitability for a specific purpose or use case. It involves a systematic examination of various aspects of the software, including its functionality, performance, usability, security, and compliance with requirements or standards. In the ERATOSTHENES project, we will utilize the pilots to evaluate and validate the technical components. We will perform the evaluation in 2 phases. The technical components integrated by pilots in phase 1 are listed in Table 2.

<table>
<thead>
<tr>
<th>Module/Framework</th>
<th>Pilot 1</th>
<th>Pilot 2</th>
<th>Pilot 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Manager and the Broker</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

© ERATOSTHENES, 2020
The key aspects that we will look for are functionality, performance, usability, security, reliability and user feedback. Here are some benefits of the evaluation.

- Identify failures which might have been missed at the time of verification.
- A misunderstood requirement specification may have been developed and integrated into the solution/product - this can be understood when differences between actual and expected results come under the scanner.
- Through evaluation bugs and vulnerabilities can be addressed early in the development cycle. This leads to higher-quality software.
- Collecting feedback from end users on usability results in user satisfaction.
- It ensures that developed technical components comply with the industry standards, regulations and legal requirements.
- It leads to continuous improvement.

Each phase will involve multiple steps as listed below.

1. Identify solutions to be validated from ERATOSTHENES tools
2. Identify ERATOSTHENES performance to be validated
3. Identify relevant KPIs, related to the scenarios and tools
4. Define Evaluation questionnaire based on the previously collected data
5. Refine Evaluation questionnaire based on pilots and technical partners
6. Pilots’ demonstration
7. Pilots’ validation and evaluation
8. Collection of results into pilots’ reports
Steps 5 to 9 will be repeated for the second evaluation process.

### 3.3.1 Requirements and KPIs

The requirements and key performance indicators of each pilot are defined in the deliverable D5.2. They will play major in the evaluation process. It will involve looking at the requirements and their KPIs and asking a question which determines if the requirement is fulfilled or not. An example is shown in Table 3.

#### Table 3: Pilots’ Functional Requirements and validation means

<table>
<thead>
<tr>
<th>Req.</th>
<th>Validation Means</th>
<th>Measurable Success criteria (KPI)</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2_OR_01</td>
<td>Privacy of personal identifiable information is ensured according to ISO27701 requirements</td>
<td>Compliance with ISO27701</td>
<td>Do you think that Privacy of personal identifiable information is ensured according to ISO27701?</td>
</tr>
<tr>
<td>PX_OR_02</td>
<td>Privacy of personal identifiable information is ensured according to GDPR requirements</td>
<td>GDPR compliance</td>
<td>Are the deployed modules in line with the privacy regulations (GDPR)?</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

A similar exercise will be performed from the technical partners’ perspective as well. For each technical component, its requirements will be mapped to KPIs, and clear questions will be used during the evaluation process. An example is shown in Table 4.

#### Table 4: Pilots’ External requirements and validation means

<table>
<thead>
<tr>
<th>Req. num.</th>
<th>Validation Means</th>
<th>Measurable Success criteria (KPI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXT_FR_01</td>
<td>Establish a monitoring scenario where CTI reports will be generated</td>
<td>CTI reports following interoperable formats are generated after events are detected by IDS</td>
</tr>
<tr>
<td>P1_FR_07</td>
<td>80% of attacks are detected, logged, and shared via CTI</td>
<td>80% of the detected attacks are detected logged</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

From the requirements in D2.1, grouped in the previous chapter, the validation means, and Measurable Success Criteria are translated into two types of evaluation:

- **Performance Evaluation** – with this type of questionnaire the functionality of each module is analysed from the Pilots’ perspective
- **KPI Validation** – technical personnel (from tech. partners and pilots) verify the achievement of each KPI

Moreover, for each pilot and component user satisfaction will be created as shown in Table 5.

#### Table 5: User satisfaction template

<table>
<thead>
<tr>
<th>Are the interfaces user-friendly?</th>
<th>Totally disagree</th>
<th>Somewhat disagree</th>
<th>Neutral</th>
<th>Somewhat agree</th>
<th>Totally agree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
### 3.4 Pilot 1: Connected Vehicles

In the automotive world the number of IoT devices involved has increased drastically in the latest years due to the evolution of the environment to a smarter one. In this new smart environment, all the actors are interacting between themselves and making decisions by themselves. Due to this tendency, increasing the cybersecurity in this field is a requirement. In pilot 1 there will be two use cases to be validated, the first one is about the interaction with the infrastructure and the second one wants to cover a key topic in the automotive world, a software update of the vehicle units. Until now the main efforts in Pilot 1 task (T5.3) were focused on the development of the use case 1 as it will be the one evaluated in the first testing loop. It will validate the interaction between a vehicle and a smart traffic light through V2X communications. **Figure 2** shows the ERATOSTHENES components involved in the first use case.

![Pilot 1 architecture diagram](image)

**Figure 2: Pilot 1 architecture diagram**

In **Figure 2**, it can be appreciated which components will be deployed and demonstrated during validation activities of the use case 1 and which other actors are present in the execution. On the right side it can be seen the vehicle, which, thanks to ERATOSTHENES will be able to validate and get access to the service provided by the traffic light (left side) in order give speed advise, following the GLOSA logic, to the person who is driving the car.

This pilot is designed to explore the potential applicability of the ERATOSTHENES security architecture within the automotive industry. Specifically, it tests the prospective benefits for connected vehicles that interact not only with other vehicles but also with external roadside elements, such as smart traffic lights. These vehicles need to ascertain the trustworthiness of these elements,
This pilot envisages two different use cases.

- **Use Case 1- Secure Connections**

The objective of this use case is to enhance security during the establishment of connections between vehicles and either external roadside elements or other vehicles. To achieve this, it is crucial to determine the trustworthiness of these external elements for which the ERATOSTHENES architecture is employed. Two communication possibilities are considered.
A) Vehicle to Infrastructure

In this scenario, as presented in Figure 3, a vehicle, using its On-Board Unit (OBU), forms a connection with a smart traffic light. This interaction enables the vehicle, for example, to assess if it should proceed at its current speed or decelerate.

B) Vehicle to Vehicle

In this scenario, as presented in Figure 4, one vehicle seeks to establish communication with another, aiming to enhance traffic management, such as providing information on congestion, or boost safety by alerting about potential accidents.

- Use Case 2- Remote Software Updates

This second use case, as presented in Figure 5, is formulated within the context of a major challenge in the automotive industry. Ensuring that smart vehicle software is appropriately updated is vital, yet these updates can potentially open gateways for malicious attacks, leading to privacy violations or even actual accidents. To mitigate this risk, it is key to guarantee that the software updates are securely sourced from a trusted repository.
3.4.2 Instantiation

Docker containers will be used to deploy and run all the necessary modules for Pilot 1. In the ATOS provided server the domain modules, along with a MQTT broker for communication between the containers, will be installed. In the vehicle IOT devices (IDAPT) the client-side modules will be installed. The technical partners have provided linked docker containers to download via a central nexus repository. The PUF and SSI client are installed on the client IOT device.

For both Pilot 1 use cases, and the deployment verification, the domain modules will be installed in an ATOS provided server. This means a VPN is required to communicate with the client-side modules on the IOT devices in Spain and the UK. The deployment server is a x86 Ubuntu server with 128 GB of storage space for modules and log files.

Currently the installed modules are the CTI sharing agent, the DLT, the FedLPY attack detection, the MUD manager, the Trust management broker and the TMRA module.

The deployment for most of the modules follows the same simple process that was explained during the module trainings, led by the module leaders. The module is cloned onto the server, the .env file is configured then it can be started using the “docker compose up” command. The order the modules are started does matter and is specified in the docker container dependencies spreadsheet. Following subsections give details on deployment of technical components involved in Pilot 1.

- MQTT Broker and MONGO database

A Mosquito MQTT broker has been downloaded and installed on the server. It is an open-source broker that will disperse the messages between the docker containers running the individual modules. It is being run from the Eclipse-Mosquitto docker container.

A database is required, and MongoDB is an open-source database platform that can be used from a docker container. Both images are pulled from the central docker hub to the domain server. Figure 6 shows deployment logs of the component.
• **TMB**

The TMB git repository was cloned into the domain server. To pull the docker image and start the container the docker-compose command is used. Figure 7 shows some modules being cloned onto the server.

```
pratosthenes@eratosthenes:~$ git submodule add https://CI-CySec.eng.it/gitlab/ERATOSTHENES/dta.git dta
Cloning into '/home/eratosthenes/dta'...
Remote: Counting objects: 100% (2662/2662), done.
Remote: Compressing objects: 100% (128/128), done.
Remote: Total 2662 (delta 79), reused 0 (delta 0), pack-reused 2532
Receiving objects: 100% (2662/2662), 40.20 MB | 5.48 MB/s, done.
Resolving deltas: 100% (779/779), done.
pratosthenes@eratosthenes:~$
```

```
pratosthenes@eratosthenes:~$ git submodule add https://CI-CySec.eng.it/gitlab/ERATOSTHENES/wp4/ids-ips.git IDSIPS
Cloning into '/home/eratosthenes/IDSIPS'...
Remote: Counting objects: 100% (354/354), done.
Remote: Compressing objects: 100% (354/354), done.
Remote: Total 354 (delta 48), reused 0 (delta 0), pack-reused 269
Receiving objects: 100% (354/354), 15.51 MB | 5.97 MB/s, done.
Resolving deltas: 100% (348/348), done.
pratosthenes@eratosthenes:~$
```

**Figure 7:** DTA and IDS/IPS Git repository cloning form central ERATOSTHENES GitLab

In the Pilot 1 use cases, the TMB is used to share the data received from the Trust Agent to all the submodules that will assess the trustworthiness of devices. The Trust Agent in this case is the IDAPT device on the vehicle or in the infrastructure and the Agent data is stored in the MongoDB and the TMRA will assess the risk score. The MUD manager is also connected to the broker and will manage the manufacturer-supplied identifier for the IDAPT devices. The trust manager is deployed and started in the domain. The agent is deployed and started in the IDAPT device.

• **TMRA**

The TMRA git repository was cloned into the domain server. To pull the docker image and start the container the docker-compose command is used. The TMRA also works with the TMB module. It works by creating a digital twin threat model and outputting risk scores for each device and threat type. Any time there is an event, such as a new vehicle being added to the network, a new risk score is generated and passed to the TMB.

• **MUD**

The MUD management git repository was cloned into the domain server. To pull the docker image and start the container the docker-compose command is used. The MUD management works with the TMB and controls the retrieval and translation of the MUD files from the IDAPT device. The MUD management lite version is used for this initial deployment, using the command "`docker-compose -f docker-compose-lite.yml up -d`"

• **CTI**

The CTI sharing agent git repository was cloned into the domain server. To pull the docker image and start the container the docker-compose command is used. The CTI is another module that will be used in this pilot that works with the TMB to share threat intelligence within the domain and externally to other domains.

• **FedLPy**

The FedLPy attack detection git repository was cloned into the domain server. To pull the docker image and start the container the docker-compose command is used.

The FedLPy will interact with the intrusion detection system to inform of detected attacks. With this initial deployment test there are no attacks involved. The module client itself can be run with the initial attack detection model that has been built from generated traffic data from IDIADA.
• **DLT**

The DLT management git repository was cloned into the domain server. To pull the docker image and start the container the docker-compose command is used. The DLT docker container can be started when the ERATOSTHENES network is up.

The DLT, in the Pilot 1 use cases, will use blockchain technologies to store information that is used by the modules in the ERATOSTHENES network. Everything stored in this solution can be verified by members of the network but cannot be modified. Specifically in the Pilot 1 use case it will store the trust score for each IDAPT, generated by the TMRA and shared by the TMB.

• **IDS/IPS**

The IDS/IPS management git repository was cloned into the domain server. To pull the docker image and start the container the docker-compose command is used as shown in Figure 8.

The intrusion detection and intrusion prevention system work with the TMB. There won’t be any intrusion to detect with this initial deployment but in the final scenario, developed by IDIADA, there will be an attack attempt. The monitoring IDS module will include an alert GUI to alert when there is an intrusion detected in the vehicle communication channel. There is still the initial implementation of the anomaly detection and the CTI sharing.

![Figure 8: Docker list and sizes after running the IDS/IPS module](image)

• **DTA**

The DTA management git repository was cloned into the domain server. To pull the docker image and start the container the docker-compose command is used.

In this deployment instance the DTA will deploy the Trust agents to the required devices.

• **SSI**

The SSI component has modules that will be deployed on both the server and the client device. On the server the ledger repository is cloned, and the demonstration containers used for the 5.6 integration are deployed using a Makefile, as shown in the Figure 9.
When the TMB, DLT and SSI modules are started, a test can be run using Potman Collections which are a number of saved requests. The integration demonstration goes through the process from creating a public DID to issuing credentials and presenting proof.

- **PUF**

  The PUF has been installed on the client-side IoT device as shown in Figure 10. With the help of members from Eulambia, connecting via a secure ZeroTier VPN, the module has been cloned onto the IDAPT. There is complete integration with the device, and the module has been installed despite the end-of-life and unsupported Ubuntu kernel used on the IDAPT. It requires the installation of the ADP.

The PUF client is the root of the trust authentication for the IDAPT device.
The Trust agent is the device-side part of the TMB module. It holds the IoT trust agent data which is shared to the TMB in the domain when registering the IDAPT device. This includes the device ID, operating system specifications, hardware specifications and the MUD URL. The TMB module that contains the initial version of the TA is cloned and deployed on the IDAPT device.

3.5 Pilot 2: Smart Health

The Smart Health pilot is a Remote patient monitoring system. It facilitates remote assistance and follow up on patients suffering from chronic diseases such as diabetes, COPD or other diseases where patients at least partly can stay at home such as COVID-19. In general, the eHealth use case enables patients to stay home during treatment and care and foster self-care. It includes a Personal Health Gateway, which is deployed in every patient’s home, that is responsible for collecting data from various medical sensors and sending them to the back-end Cloud services. The services provide data to health personnel allowing for remote patient monitoring, data is recorded in the patient’s electronic health journal, and it normalizes data according to standard eHealth ontologies to allow for performing various data analysis. The architecture diagram in Figure 11 shows the different components which we will test in this pilot and improve the security in the e-health sector.

![Pilot 2 Architecture Diagram](image)

Initially, we started with the deployment of several components on our gateway. In phase 1 of the demo, we will show the onboarding of our own gateway into our own service. Following that, we will collect several metrics using the Trust Agent for the continuous monitoring of our gateway. Table 7 describes the performed activities in the context of Pilot 2 since the D5.2.

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Timeline</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Prepared pilot deployment, validation and impact plans and delivered in the D5.2</td>
<td>M15</td>
</tr>
<tr>
<td></td>
<td>Activity Description</td>
<td>Timeframe</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>2</td>
<td>Attended regularly pilot collaboration meetings under T5.2</td>
<td>M15-M26</td>
</tr>
<tr>
<td>3</td>
<td>Presented pilot 2 in the review and plenary meeting</td>
<td>M18</td>
</tr>
<tr>
<td>4</td>
<td>Updated the pilot 2 architecture diagram based on inputs of plenary meeting</td>
<td>M19</td>
</tr>
<tr>
<td>5</td>
<td>Had meetings with SINTEF regarding the discussion of the metrics that can be collected by the Trust Agent to calculate the Trust Score</td>
<td>M20-M21</td>
</tr>
<tr>
<td>6</td>
<td>Setup deployment server</td>
<td>M22</td>
</tr>
<tr>
<td>7</td>
<td>Presented pilot 2 architecture, use cases, demonstration plan in plenary meeting and had open discussion</td>
<td>M23</td>
</tr>
<tr>
<td>8</td>
<td>Analysed the pilot outcomes and carried out social impact assessment for pilot 3</td>
<td>M24-M25</td>
</tr>
<tr>
<td>9</td>
<td>Had regular meetings with UMU to prepare data impact assessment for pilot 3</td>
<td>M24-M25</td>
</tr>
<tr>
<td>10</td>
<td>Had meeting with SINTEF regarding the Trust Agent deployment. Followed by meeting with UPRC for the calculation of Trust Score based on the metrics collected by Trust Agent</td>
<td>M25</td>
</tr>
<tr>
<td>10</td>
<td>Have meeting with the Eulambia regarding the deployment of PUF component</td>
<td>M25-M26</td>
</tr>
<tr>
<td>11</td>
<td>Created pilot introduction video for dissemination</td>
<td>M26</td>
</tr>
<tr>
<td>12</td>
<td>Provided content for D5.6</td>
<td>M26</td>
</tr>
<tr>
<td>13</td>
<td>Start validating and deploying core components</td>
<td>M26</td>
</tr>
</tbody>
</table>

### 3.5.1 Use Cases

- **Use Case 1- Device Authentication and Authorization**

  **A) Authenticate our own Gateway in our System**

  Tellu offers a suite of devices delivered to each patient as part of their business operations. Each suite of devices needs to be connected with a single gateway (Tellu Personal Health Gateway). Until now, the enrollment process was cumbersome and demanded manual intervention, making it difficult to scale. However, with the implementation of ERATOSTHENES, these various devices can be connected automatically by authenticating the gateway and leveraging the trust functionalities offered by the ERATOSTHENES architecture as shown in **Figure 12**.
B) Authenticate External Gateway/Device in our own System

The objective of this use case is to facilitate the integration of a third-party device (or gateway) (e.g., an Apple Wallet) into Tellu's platform. In alignment with the process delineated in the first use case, the third-party device would need to complete a prior enrollment in the ERATOSTHENES architecture. This enrollment enables the generation of a corresponding identifier that aids in securely incorporating the device into the platform as illustrated in Figure 13. Thus, it ensures a seamless and secure user experience while broadening the scope of devices compatible with Tellu's system.

C) Authenticate External Services to Access our own Gateway/Devices

The primary objective of this use case is to strengthen security measures. It is of major importance considering the sensitive nature of data these devices might handle, such as health information. The authentication of external services can be leveraged in multiple scenarios. In general, when a third-party service provider interacts with these devices or the gateway itself, it is crucial to verify their trustworthiness. This is enabled through their prior enrollment in the ERATOSTHENES architecture, which assigns and records a level of trust for each third party.

A specific scenario that necessitates access to Tellu's gateway is the case of emergency services. An explanatory scenario is when firefighters need to access a sensor during a fire outbreak. To facilitate this, the emergency service should have previously registered with the ERATOSTHENES system. Upon registration, they are assigned a unique identifier and a trust score. When emergency access is required, the gateway can quickly consult this trust score and, if appropriate, grant immediate access as shown in Figure 14.
• **Use Case 2 - Trust Management of Devices/Services**

There are two scenarios, but for systematic reasons, we have grouped them into one. This use case builds upon the previous one. Once a device/gateway is enrolled and considered operational, the ERATOSTHENES features are utilized to sustain trust over time as shown in Figure 15. This is achieved using specific trust metrics that assist towards the detection of unusual behavior.

• **Use Case 3 - Prove Compliance**

Building on the previous use case, the described objective for this use case is to monitor privacy measures using specific metrics tailored for that purpose. Relevant examples include ensuring data encryption, preventing the sharing of encryption keys between gateways, and setting up the network to block any unwanted connections with gateways. This can be related to compliance controllers that are implemented and these can be monitored accordingly to check compliance.

### 3.5.2 Instantiation

Because most of the components in the ERATOSTHENES project are built as docker containers. As a result, in Pilot 2, we deployed the docker setup in both our IoT device and the server, allowing docker containers to be simply deployed. In Pilot 2, we have a Raspberry Pi 3 with a Debian image installed as our gateway. As a result, all client-side components will be put on the Raspberry Pi, together with an MQTT server capable of sending data to the server. We
have so far installed SSI, PUF, TMB, TA, DTA, and DLT components. All deployment screenshots for various components are available below.

For the deployment server we have launched a Virtual Machine (VM) on AWS. The VM is the Linux machine that supports all the Ubuntu commands, and it has around 30 GB of space. The details of the server are shown in Figure 16.

![VM Details](image)

Figure 16: Showing the specification of the VM hosted on AWS

- **PUF**

PUF technology created a unique identification for the device based on the device characteristics that will be used in the ERATOSTHENES project. In Pilot 2, we have our gateway/ Raspberry Pi that needs to be onboarded on the ERATOSTHENES architecture for the deployment of the PUF component. For deployment purposes, our gateway must be on the same network as Eulambia, which oversees the PUF component. We used the Zerotier VPN for this reason and made our gateway available on the same network ID as provided by Eulambia. As a result, Eulambia can SSH into our gateway and generate a token, as shown in the screenshot below, which can be used for many purposes in the ERATOSTHENES architecture, such as authentication and authorization. The PUF enrolment status of the Tellu gateway is shown in Figure 17.

![PUF Enrollment Status](image)

Figure 17: PUF enrolment status of the Tellu Gateway

- **SSI**

The SSI (Self-Sovereign Identity) component is used for onboarding the Tellu gateway on the server. Moreover, it will also be utilized for the verification of the third-party components as well as allowing the third-party services to access the Tellu gateway. The SSI component have two modules one of the modules has been deployed on the IoT device and the other module is deployed on the server. Figure 18 shows the deployment of the SSI module.
• **TMB/TMRA**

The deployment of the TMB/TMRA component was completed successfully, as presented in Figure 19. The TMB component was delivered in the form of three different docker components that can be composed using a single command. The first container contains the Trust Manager Broker (TMB), while the second consists of the MongoDB Database. The last container comes with `mongo-express`\(^4\) that allows administrators to access the attached MongoDB Database using a web-based GUI. All those elements were deployed locally and are confirmed to be accessible for further development in the subsequent part of the project. In a fully developed version of the project, TMB component will be deployed server-side and will be responsible for managing, collecting data from, and assessing the trustworthiness of gateways connected to the network.

\(^4\) *Mongo-express*, A web-based MongoDB admin interface written with Node.js, Express, and Bootstrap3, [https://github.com/mongo-express/mongo-express](https://github.com/mongo-express/mongo-express)
Figure 20: Mongo-Express GUI

This interface can be deployed in a selected manner and accessed through the browser (default address: localhost:8081).

Figure 21: TMB Containers in Docker Desktop GUI

As shown in Figure 21, the TMB component is technically made from three different docker containers, each storing a different part of it.

- **Trust Agent**

The Trust Agent is one of the central components that, along with the Trust Manager Broker, ensures the appropriate resilience of the network. As the central assumption underlying the Pilot 2 use scenario was that different IoT devices serving as gateways might join the network at any given time (not necessarily possessing the latest available specification and configuration), the proper communication of the Trust Agent (TA) with the TMB is crucial for achieving an operational level of the project. At this stage of the development, a container with TA was deployed on the experimental gateway, and its ability to collect and dispatch information was tested locally (the collected data has not yet been sent to an external server). Figure 22 shows the deployment and container logs.
- **Deployer of Trust Agents**

  The Deployer of Trust Agents (DTA) is responsible for managing the lifecycle of the TAs deployed on RPM gateways within the ERATOSTHENES framework, including the initial deployment, as well as further updates, rollbacks, and recovery. To this end, the DTA collects various contextual information from managed devices at run-time, as well as propagates down software management commands (e.g., deploy, update, roll-back, recovery). At the same time, the DTA also keeps track of available TAs to assign them to target devices based on their multi-dimensional context. The DTA component has been designed and implemented in a modular, loosely coupled manner with MQTT being the main transportation/communication layer across these components. More specifically, the three main functional components of the DTA are the following:

  - **Device-side monitoring agents** collect contextual information and receive TA management commands.
  - **DTA back-end** builds upon and extends the default functionality of the existing digital twin platform Eclipse Ditto.\(^5\)
  - **DTA front-end** offers the TA management features through a graphical user interface.

For convenience, these three components are packaged as Docker images and can be easily deployed using standard tools, either as stand-alone containers or as part of a larger docker-compose configuration. Once up and running, the monitoring agents send contextual run-time information from the devices, the backend receives this information and updates the corresponding digital twins, and the front-end displays the live status of managed devices and receives management commands. At the core of the DTA’s operation is the live representation of the managed devices, i.e., its digital twin (a simplified example focusing on the TA management is depicted in **Figure 23**). The twin includes both static (i.e., attributes) and dynamic (i.e., features) information about the coupled devices.

---

\(^5\) [https://github.com/eclipse-ditto/ditto](https://github.com/eclipse-ditto/ditto)
The actual management of TAs is facilitated using the continuous comparison of the reported and the desired status of the TAs (i.e., so-called the ‘Desired-Reported Property’ pattern). Any differences between the two will trigger a corresponding action to be taken. For example, if the reported properties include a deployed TA, but not started, whilst the desired properties include a running trust agent, the DTA will send a corresponding instruction to the device-side agent to launch the TA. This comparison process continues until both the reported and the desired properties are eventually in sync.

- **DLT**

  DLT utilizes blockchain technology to provide a decentralized solution for the transparent and immutable storage of the information that will be used by the ERATOSTHENES and its components. Basically, it is a distributed storage that is immutable and cannot be altered and everything which is stored in this space like identity management or the trust score information is verifiable by the peers in the network.

  In Pilot 2, DLT will be used for storing the DID created during the process of onboarding of Tellu gateway. It will also be used for storing the Trust score by the TMB/TMRA component. The DLT component needs to be deployed only once, all other components of ERATOSTHENES can integrate with the DLT on their own. **Figure 24** shows the deployment of the DLT component on the server side.
3.6 Pilot 3: Disposable IDs in Industry 4.0

The industry 4.0 revolution has accelerated the rise of usage of IoT devices for controlling, managing, monitoring and optimizing industrial processes. On one hand, it has improved the processes and on the other hand, it has increased the attack surface, such as the introduction of introduced new attack vectors. The security of IoT devices is of prime importance. In pilot 3, we have identified that secure identification of IoT devices is the first step towards IoT security. Once the identification is done securely, the authentication and authorization can be performed.

Figure 25: Pilot 3 architecture diagram
Currently, static identifiers are used for IoT devices which are attached to them lifelong. It is a security loophole. In the pilot 3, we have designed a solution to generate disposable identities based on self-sovereign identity (SSI) framework (defined in deliverable D3.1). The disposable identities have limited scope and life. They can be utilized for authorization of IoT devices. The disposable identities have the following characteristics.

- created as unique IDs for an assigned process or communication
- can be limited on the way and lifetime of usage
- have a cryptographic child relation to certain entity/asset ID
- is built on quantum safe cryptographic methods
- can be revoked at any time by the parent ID owner
- can’t be cloned or faked by cryptographic mechanisms
- can be processed on distributed networks
- compliant to GDPR and European Self Sovereign ID strategy

In pilot 3, the core technical components developed in WP2-4 will be integrated, validated and deployed. These technical components align with various security aspects e.g., bootstrapping, threat monitoring, and trust generation, to strengthen the security of IoT devices. The technical components are shown in Figure 25.

Since the last deliverable, D5.2, various activities have been performed in the pilot 3. Task T5.5: Pilot 3 - Industry 4.0: Execution and Validation started in M19 which is dedicated to pilot 3. The piloting activities for the pilot 3 are listed in Table 8.

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Timeline</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Prepared pilot deployment, validation and impact plans and delivered in the D5.2</td>
<td>M15</td>
</tr>
<tr>
<td>2</td>
<td>Attended regularly pilot collaboration meetings under T5.2</td>
<td>M15-M26</td>
</tr>
<tr>
<td>3</td>
<td>Presented pilot 3 in the review and plenary meeting</td>
<td>M18</td>
</tr>
<tr>
<td>4</td>
<td>Updated the pilot 3 architecture diagram based on inputs from the plenary meeting</td>
<td>M19</td>
</tr>
<tr>
<td>5</td>
<td>Kickoff of task T5.5</td>
<td>M19</td>
</tr>
<tr>
<td>6</td>
<td>Had a series of meetings with ATOS on the topic of disposable identity and updated the disposable identity generation sequence diagram</td>
<td>M20-M21</td>
</tr>
<tr>
<td>7</td>
<td>Setup deployment server</td>
<td>M22</td>
</tr>
<tr>
<td>8</td>
<td>Presented pilot 3 architecture, use cases, demonstration plan in plenary meeting and had open discussion</td>
<td>M23</td>
</tr>
<tr>
<td>9</td>
<td>Analysed the pilot outcomes and carried out social impact assessment for pilot 2</td>
<td>M24-M25</td>
</tr>
<tr>
<td>10</td>
<td>Had regular meetings with UMU for preparing data impact assessment for pilot 2</td>
<td>M24-M25</td>
</tr>
<tr>
<td>11</td>
<td>Created pilot introduction video for dissemination</td>
<td>M25</td>
</tr>
</tbody>
</table>
3.6.1 Use Cases

The diverse functionalities are represented through five use cases. For systematic clarity, we limit the analysis to the use cases pertinent to data protection, merging use cases 1 and 2 because of their similarities.

- **Use Cases 1 and 2 - Disposable IDs**

  The aim of this use case is to facilitate the creation of disposable IDs for devices enrolled in the ERATOSTHENES architecture. These disposable IDs prove to be beneficial when temporary access to a service is required. Upon request, the service can verify the continued existence of the ID and, if relevant, its associated trust score with the ERATOSTHENES architecture as shown in Figure 26.

- **Use Case 3 - Trust and Permission Service**

  This use case is a progression from the previous one, permitting a device with an associated disposable ID to execute specific actions or access particular resources. The procedural flows mirror those of the earlier use case but with the added step of verifying permissions or authorizations linked to the disposable ID as shown in Figure 27.

---

6 The original names of the use cases are: “Implementation of resilient and secure asset identification” and “Distributed Disposable IDs”.

© ERATOSTHENES, 2020
3.6.2 Instantiation

The pilot 3 utilizes containerization technology for deploying the various technical components. Each ERATOSTHENES technical component is packaged as a docker image which can be spun off in a silo with container orchestration tools such as Docker\(^7\), Kubernetes. It has multiple benefits e.g., consistency, isolation, portability, scalability, and CI/CD to name a few. In Pilot 3, the Compose\(^8\) plugin of the Docker is used to manage containers. Some of the useful commands are illustrated in Figure 28.

![Figure 28: Basic Docker commands](image)

We have written a Bash script to automate the component deployment process. It provides functionalities to start, stop, pause and resume container services for different components. The sub-commands and options of the script are shown in Figure 29.

![Figure 29: Pilot3 deployment script help documentation](image)

Each core technical component has its own git repository. We have created a pilot instantiation repository in which the repositories of technical components are added as git submodule\(^9\). It helps us to keep the source code consistent.

---

\(^7\) Docker is a set of platform as a service products that use OS-level virtualization to deliver software in packages called containers. https://www.docker.com

\(^8\) Compose is a tool for defining and running multi-container Docker applications. https://docs.docker.com/compose/

and removes the need to maintain multiple copies for different pilots. We use git CLI to add, initialize, clone and push submodules. The commands are illustrated in Figure 30.

![Figure 30: git sub-module commands](image)

An example of adding Ledger Platform as a submodule is shown in Figure 31.

![Figure 31: git submodule add example](image)

So far, we have added Ledger Platform, SSI Framework, Trust Manager and Broker and Intrusion Detection Prevention System engine (IDS-IPS) repositories as submodules. The details are shown in Figure 32.

![Figure 32: Status of git submodules in pilot3 repository](image)

A deployment server is used to host the technical components. In the Pilot3, we have used Ubuntu Server hosted on our private Proxmox server. It is a container powered by the Linux Container (LXC) runtime. It run Ubuntu 20.04 as illustrated in Figure 33.

![Figure 33](image)

---

10 Proxmox Virtual Environment is a hyper-converged infrastructure open-source software. It is a hosted hypervisor that can run operating systems including Linux and Windows on x86-64 hardware. https://www.proxmox.com/en/.

11 LXC is a well-known Linux container runtime that consists of tools, templates, and library and language bindings. https://linuxcontainers.org/lxc/introduction/.
The objective of the DLT is to provide both single-domain and inter-domain domains with immutable and auditable support for advanced identity management, trusted data sharing and discovery. It does this by leveraging smart contract support so that entities can interact with DLTs both locally and inter-domain. It plays a key role in the context of the ERATOSTHENES architecture. Specifically, the Ledger Platform component supports the secure storage, retrieval and exchange of data related to:

- cyber-security information
- trust-related data such as context parameters, device reputation and trust scores
- identity-related data deployment

The ledger platform leverages Hyperledger Fabric, which is an open-source enterprise-grade permissioned Distributed Ledger Technology (DLT) platform, designed for use in enterprise contexts, that delivers some key differentiating capabilities over other popular distributed ledger or blockchain platforms. The Hyperledger Fabric deployment involves multiple peers, orderers, and databases as shown in Figure 34.

A fundamental element of a Hyperledger Fabric blockchain network is the set of peer nodes (or, simply, peers). They manage ledgers and smart contracts. An orderer does transaction ordering in the fabric network, which along with other orderer nodes forms an ordering service. Because Fabric’s design relies on deterministic consensus algorithms, any block validated by the peer is guaranteed to be final and correct. In Hyperledger Fabric, a ledger consists of two distinct, though related, parts – a world state and a blockchain. The world state is a database that holds the current values of a set of ledger states. In the ERATOSTHENES, we use the CouchDB database to store the world state. Each peer in the fabric network maintains copy of blockchain.

**Self-Sovereign Identity**

Self-Sovereign Identity (SSI) framework is composed of server-side and device-side modules. The Ledger uSelf Broker component is deployed on the server side and the Ledger uSelf IoT component runs on the IoT device side. These components provide Authentication and Authorization services following a Self-Sovereign Identity approach and
complying with Decentralized Identifiers (DID) and Verifiable Credentials standards, both by the W3C. The deployment using pilot3.sh script is shown in Figure 35.

![Figure 35: SSI deployment logs]

Figure 35: SSI deployment logs

In Pilot 3, we have used Ledge uSelf to generate decentralized identifier and verifiable credentials. The API required to create DID is shown in Figure 36.

![Figure 36: DID generation using curl]

Figure 36: DID generation using curl

- **PUF**

PUF technology is used in the ERATOSTHENES to generate unique keys based on the device characteristics. In Pilot 3, PUF with SSI and DLT is utilized to generate disposable identity. The PUF security ecosystem development comprises of:

- A web service for PUF key validation
- A production intranet service for enrolling devices automatically
- An internet service for device authentication
- A dedicated counterpart application for automatic enrolment of the device.
- An authentication client
- Three software protocols (authentication, enrolment, validation)
- One optical PUF hardware device (strong PUF)
- One electronic PUF hardware device (weak PUF)

Nowadays the need for a technology which can provide true random keys without collision is of a major concern for all network security providers. The use of PUF technology-based devices can provide strong key authentication based on randomly disordered physical mediums which cannot be replicated or cloned.

In the Pilot 3, we have used a Raspberry Pi Model 4B as an IoT device. We have created a secure private network powered by ZeroTier\(^\text{12}\) to facilitate communication between IoT devices and PUF server. A ZeroTier client is installed on the Raspberry Pi. Basic commands are shown Figure 37.

\(^{12}\) ZeroTier lets you build modern, secure multi-point virtualized networks of almost any type. [https://www.zerotier.com/](https://www.zerotier.com/)
The device was enrolled on Eulambia server using the ZeroTier network. The device status is shown in Figure 38.

![ZeroTier installation](image)

**Figure 37: ZeroTier installation**

![PUF enrolment status](image)

**Figure 38: PUF enrolment status**

- **Trust Manager & Broker**

  The Trust Manager & Broker component is virtually the heart of the ERATOSTHENES architecture. It facilitates interactions between components on the domain side (e.g., Threat Modelling & Risk Assessment, DLT, Intrusion Detection Prevention System, MUD Server) and IoT devices. The ability to facilitate the establishment of trust between entities in an IoT ecosystem is the most significant industrial/business issue that the Trust Manager and Broker component addresses in Pilot3. In the context of IoT networks, trust refers to the expectation that an IoT device will provide, correct, truthful, and reliable service to another entity upon the latter's request. A score of numerical value shows the degree of a device's trustworthiness. Also, the first goal of the TMB component is to generate and provide evidence regarding the level of trustworthiness of an IoT device as well as to maintain and update Trust Records for every IoT network device. Additionally, Pilot 3, interacts with the IDS-IPS component to generate insights on incident detection and protection. **Figure 39** shows the deployment logs of the TMB component.

![TMB Deployment logs](image)

**Figure 39: TMB Deployment logs**

- **Intrusion Detection System and Intrusion Protection System**

  An open-source-based intrusion detection system that focuses on the identification of anomalies in a restricted, IoT-based network environment. **Figure 40** shows the containers started for the IDS-IPS component.
It utilizes Elasticsearch tool as a distributed, multitenant-capable full-text search engine. For the Pilot 3, it runs on port 9200. The status of Elasticsearch can be checked using calling a HTTP API as shown in Figure 41.

Moreover, Elasticsearch facilitates an HTTP-powered web interface and schema-free JSON documents. Users can create a dashboard and customize it to visualize various logs and metrics as shown in Figure 42. It helps to visualize different data generated in the Pilot 3.
The ADI module of IDS-IPS provides RESTful APIs. They are written in Python using FastAPI\(^\text{14}\). The documentation of the APIs written using OpenAPI\(^\text{15}\) is illustrated in Figure 43.

\[\text{Figure 43: AD OpenAPI documentation}\]

\(^{14}\) FastAPI is a modern, fast (high-performance), web framework for building APIs with Python 3.8+ based on standard Python type hints. [https://fastapi.tiangolo.com/](https://fastapi.tiangolo.com/)

\(^{15}\) The OpenAPI Specification is a specification language for HTTP APIs that provides a standardized means to define your API to others. [https://www.openapis.org/](https://www.openapis.org/)
4 Social Impact Assessment

In the ERATOSTHENES project, there is a feedback loop between technical work packages and pilots. The work packages are responsible for designing and developing core technical components. The pilots are given the task of integrating and validating the components for various use cases and give feedback on the readiness level, performance and quality to the work packages. The pilots will demonstrate the technical capabilities of the ERATOSTHENES project which is both a major contribution of the project and it can provide far-reaching impacts after the project completion.

We have analysed the pilots’ impact in two broad verticals. It includes Social Impact Assessment (SIA) and Data Protection Impact Assessment (DPIA). In the SIA, we identified various categories e.g., security, awareness, and described the impacts of each pilot as defined in Table 9.

<table>
<thead>
<tr>
<th>#</th>
<th>Category Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Technology Advancement</td>
<td>Innovative technology comes out of the pilots, IP</td>
</tr>
<tr>
<td>2</td>
<td>Standardization Changes</td>
<td>Technical architecture, components, algorithms could add something to existing standards or could introduce new standards</td>
</tr>
<tr>
<td>3</td>
<td>Policy &amp; Regulations Changes</td>
<td>Use cases of pilots could make a good case for changes/new policies/regulations</td>
</tr>
<tr>
<td>4</td>
<td>Open-Source Community Resources</td>
<td>Technical architecture, components, algorithms could be made public for open-source dev community, which can adapt them</td>
</tr>
<tr>
<td>5</td>
<td>SME Space</td>
<td>Pilot could be developed as product to sell to integrate with existing new product</td>
</tr>
<tr>
<td>6</td>
<td>Security and Privacy</td>
<td>Data collected, generated and processed by pilots and the processes developed.</td>
</tr>
<tr>
<td>7</td>
<td>Exploitability and marketization</td>
<td>Exploit the pilot solutions, integrate with other solutions, e.g., emergency services in pilot2</td>
</tr>
<tr>
<td>8</td>
<td>Awareness &amp; Training</td>
<td>About security, privacy, regulations, training</td>
</tr>
</tbody>
</table>

For each identified category, all pilots did the analysis which included a description of the impact, impact type, level of impact etc as defined in Table 10.

<table>
<thead>
<tr>
<th>#</th>
<th>SIA Metric</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Category of Impact</td>
<td>Defined in Table XX</td>
</tr>
<tr>
<td>2</td>
<td>Description of Impact</td>
<td>It has descriptive text.</td>
</tr>
</tbody>
</table>
### 3. Type of Impact
- Positive
- Negative

### 4. Level of Impact
- Low
- Mid
- High

### 5. Nature of Impact
- Permanent
- Reversible

### 6. Level of Certainty
- Absolutely
- Probably
- Unsure

### 7. Project Stage
- Planning
- Development
- Operation
- Dissemination
- Completion

## 4.1 Pilot 1 SIA

The Social Impact Assessments of Pilot 1 are illustrated in Table 11.

### Table 11: Pilot 1 Social Impact Assessment

<table>
<thead>
<tr>
<th>Index</th>
<th>Category of Impact</th>
<th>Description of Impact</th>
<th>Is Impact Positive or Negative</th>
<th>Level of Impact</th>
<th>Is Impact Reversible or Permanent</th>
<th>Level of Certainty About the Impact</th>
<th>Project Stage where Impact will Happen</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Technology Advancement</td>
<td>In Pilot 1, the Institute will develop a VoIP communication channel that will allow for secure voice communication without the need for dialing.</td>
<td>Positive</td>
<td>Mid</td>
<td>Reversible</td>
<td>Probably</td>
<td>Completion</td>
</tr>
<tr>
<td>2</td>
<td>Technology Advancement</td>
<td>Novel attack detection using behavioral learning is developed that detects and acts upon abnormal network traffic.</td>
<td>Positive</td>
<td>Mid</td>
<td>Reversible</td>
<td>Probably</td>
<td>Completion</td>
</tr>
<tr>
<td>3</td>
<td>Technology Advancement</td>
<td>The trust management software and agent enables the management of IoT devices to be securely verified. The software detects and acts upon abnormalities in the software and provides guidance for the manufacturer.</td>
<td>Positive</td>
<td>Mid</td>
<td>Reversible</td>
<td>Probably</td>
<td>Completion</td>
</tr>
<tr>
<td>4</td>
<td>Standardization Changes</td>
<td>The Trust Management Framework (TMF) must be adopted to ensure the TMF data that is shared with the IoT devices that are supported by the manufacturer.</td>
<td>Positive</td>
<td>High</td>
<td>Reversible</td>
<td>Probably</td>
<td>Completion</td>
</tr>
<tr>
<td>5</td>
<td>Standardization Changes</td>
<td>Trust management software and agent will require software to be installed on the server and trust requirements on manufacturer.</td>
<td>Positive</td>
<td>Mid</td>
<td>Reversible</td>
<td>Probably</td>
<td>Completion</td>
</tr>
<tr>
<td>6</td>
<td>Policy &amp; Regulations Changes</td>
<td>Security and Privacy</td>
<td>Positive</td>
<td>High</td>
<td>Reversible</td>
<td>Probably</td>
<td>Completion</td>
</tr>
</tbody>
</table>

## 4.2 Pilot 2 SIA

The Social Impact Assessments of Pilot 2 is illustrated in Table 12.
4.3 Pilot 3 SIA

The Social Impact Assessments of Pilot 3 is illustrated in Table 13.

Table 13: Pilot 3 Social Impact Assessment

<table>
<thead>
<tr>
<th>Index</th>
<th>Category of Impact</th>
<th>Description of Impact</th>
<th>Is Impact Positive or Negative</th>
<th>Level of Impact</th>
<th>Is Impact Reversible or Permanent</th>
<th>Level of Certainty About the Impact</th>
<th>Project Stage where Impact will Happen</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Technology Advancement</td>
<td>In Pilot 3, new technical solutions will be developed.</td>
<td>Negative</td>
<td>Low</td>
<td>Reversible</td>
<td>Unlikely</td>
<td>Completion</td>
</tr>
<tr>
<td>2</td>
<td>Technology Advancement</td>
<td>In Pilot 3, new technical solutions will be developed.</td>
<td>Negative</td>
<td>Low</td>
<td>Reversible</td>
<td>Unlikely</td>
<td>Completion</td>
</tr>
<tr>
<td>3</td>
<td>Standardization Changes</td>
<td>The way the authentication and authorization of the devices in the IoT space using NIF and other Eratosthenes components will be validated in the Pilot 2.</td>
<td>Negative</td>
<td>Low</td>
<td>Reversible</td>
<td>Unlikely</td>
<td>Completion</td>
</tr>
<tr>
<td>4</td>
<td>Policy &amp; Regulations Changes</td>
<td>To give access of patient-level data to the emergency medical services in case of emergency.</td>
<td>Negative</td>
<td>Low</td>
<td>Reversible</td>
<td>Unlikely</td>
<td>Completion</td>
</tr>
<tr>
<td>5</td>
<td>Security &amp; Privacy</td>
<td>As using the Eratosthenes architecture will enhance the security of the third-party devices as well as sharing the data to the third-party services, this will give the opportunity to exploit the large market penetration of our services.</td>
<td>Negative</td>
<td>Low</td>
<td>Reversible</td>
<td>Unlikely</td>
<td>Completion</td>
</tr>
</tbody>
</table>

© ERATOSTHENES, 2020
5 Data Protection Impact Assessment

Pursuant to Regulation (EU) 2016/679 (GDPR), all data controllers and processors are obliged to apply data protection methodologies by design and by default (Article 25 GDPR). This necessarily implies the application of several complementary and successive methodologies:

- Analysis of the risks involved in the processing, from the perspective not only from data security but also for the rights and freedoms of individuals.
- Identification of the necessary measures for the processing to eliminate and mitigate risk and be developed under the requirements of privacy by design in order to: a) Limit the volume and category of personal data necessary for the purposes of the processing and b) Adopt functional and appropriate safety measures for the processing.

The Data Protection Impact Assessment (DPIA) is an obligation under the GDPR. The aim of the rule is to improve compliance with the Regulation, especially in situations "likely to result in a high risk to the rights and freedoms of natural persons", as stipulated by Recital 84 of the GDPR. In this regard, there are certain obligatory circumstances dictating when a DPIA should be conducted. Article 35 of GDPR specifically mandates the execution of this assessment

“where a type of processing, in particular using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data” [9].

While the examined scenarios do not pose a significant risk to the rights and freedoms of natural persons, the implementation of new technologies necessitates a DPIA. This is crucial to guarantee that the design of the pilots adheres to the utmost standards of privacy and data protection for potentially involved users. Furthermore, a DPIA at design stage (i.e., prior specific plans of implementation) can provide valuable guidelines for possible future deployment of these technologies in real-world scenarios within the context of the proposed pilots.

It is important to note that the primary objective of ERATOSTHENES is to enhance privacy and security in digital processes. This is accomplished by mitigating risks through the creation of an architecture that establishes and maintains trust with participants on a continuously monitored basis, thereby minimizing the potential for malicious attacks and the subsequent impact on users' rights and freedoms. Additionally, the ERATOSTHENES architecture is tailored for IoT technologies and primarily focuses on the processing of non-personal data. However, considering that these ecosystems might not be entirely independent and could require the participation of natural persons to a certain extent, any direct or indirect implications on personal data must be evaluated within the framework of a DPIA.

This section aims to fulfil the requirements laid out in Article 35 of the GDPR. However, given the unique context of a research project, we propose an adaptation of the traditional methodology. We begin by suggesting a section that delineates the terms and criteria to be used in qualifying data as either personal or non-personal. This is followed by an examination of the various data flows in each pilot, along with an overview of any potential processing of personal data, associated risks, and risk treatment plan.

The primary purpose of the DPIA is to keep specific stakeholders informed and to identify potential privacy and data protection risks at an early stage, ensuring that further deployments in real scenarios are conducted with due respect for user rights and freedoms. To evaluate the privacy risks presented, we use the scale provided by the Spanish Data Protection Agency\textsuperscript{16} (Likelihood x Impact=Risk) as shown in Table 14.

---

\textsuperscript{16} Spanish Data Protection Agency: “Guía práctica para las evaluaciones de Impacto en la protección de los datos sujetas al RGPD” V.2018.
### Table 14: Privacy risk scale of Spanish Data Protection Agency

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very likely</td>
<td>4</td>
</tr>
<tr>
<td>Relevant</td>
<td>3</td>
</tr>
<tr>
<td>Limited</td>
<td>2</td>
</tr>
<tr>
<td>Unlikely</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level of impact</th>
<th>Description</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Significant</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Limited</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Negligible</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

The potential results (Likelihood x Impact) are adapted to the categories and levels of privacy affectation provided by PILAR17.

### 5.0 The ERATOSTHENES Architecture and the Pilots

ERATOSTHENES proposes an architecture for the secure and privacy-respectful management of interconnected devices. The main purpose of the architecture is to increase trust, which consequently enhances security and privacy. This is made possible through device identification and the continuous monitoring of trust scores, enabling the determination of a device's trustworthiness. This not only facilitates improved user experience in certain cases but also

---


© ERATOSTHENES, 2020
allows these devices to interoperate securely. As a result, it provides the highest safeguards when personal data sharing does occur.

This architecture adheres to the Zero Trust principle of "Never Trust, Always Verify". It falls under the sphere of Zero Trust Architectures, which signifies not only advancements in securing environments but also enhanced protection of users' personal data.

Without delving into the technical details outlined in the various deliverables of the project, ERATOSTHENES architecture components enable the evaluation of a device's trust level. This is achieved through a sequence of algorithmic checks and the calculation of a "trust score" at the point of enrollment and during subsequent periods via routine security checks. These checks continuously monitor for any anomalous activity that may trigger the "trust detector". Furthermore, additional components maintain black-or-white lists of authorized actions for a specific device, which are crucial in determining a device's trust level.

These components collaborate with a single domain Distributed Ledger Technology (DLT) to record "trust levels" as well as any related updates or security events. Simultaneously, the architecture allows for operations beyond a single-domain DLT, extending to an inter-domain DLT, thus facilitating the expansion of trust beyond a single entity or legal person. In addition, the traceability feature of the DLT enables not only the potential inquiry of trust levels but also ensures complete traceability of all events.

To make it possible, interconnected devices must be equipped with a series of modules, particularly for the generation of a partial trust algorithm (Trust Agent) and a unique identifier or digital fingerprint (Physical Unclonable Function or PUF). Further components are provided, including an advanced data protector for secure and encrypted data storage.

Moreover, ERATOSTHENES can provide additional services, especially identity management (IdM) services. By interfacing with this component, devices can manage identities and issue credentials (privacy-preserving Attribute-based Credentials) that can be stored on the device. This component also collaborates with the DLT within a single domain to record specific events (such as the issuance of a credential).

The ERATOSTHENES project has envisaged three different pilots, each exploring varied use cases detailed in this document. The first pilot focuses on the automotive industry, investigating the potential interactions between connected vehicles and external roadside infrastructure. This includes vehicle-to-vehicle communication and interactions with other external components, such as smart traffic lights. The second pilot delves into the utility of ERATOSTHENES' trust architecture for authenticating smart devices with a single gateway. This pilot aims to deliver a seamless user experience while simultaneously ensuring data security when interactions with external parties occur. Lastly, the third pilot probes into the architecture's possibilities within industry applications, particularly the generation of temporary, disposable IDs. These IDs could authorize specific actions within a given ecosystem, further augmenting system security and control.

The three pilots take a different approach to the ERATOSTHENES architecture that will be the subject of study in the subsequent sections.

5.1 Prior Considerations: The Qualification of Personal Data

5.1.1 Legal Notions on Personal Data

Personal data, as defined in Article 4 (1) of the GDPR, means

“Any information relating to an identified or identifiable individual. An identifiable natural person is one who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number,
location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” [9].

Hence, personal data is the information that directly or indirectly relates to an identified or identifiable natural person. Conversely, when data does not relate to an identified or identifiable natural person, data must be considered anonymous, which according to what is stated in Recital 26 of the GDPR, does not fall under the scope of principles of data protection.

Determining the anonymity of data presents significant challenges due to the diverse interpretations provided by the GDPR and the Article 29 Data Protection Working Party (A29 WP) [9]. According to Recital 26 of the GDPR, which adopts a risk-based approach, data can be considered anonymous if it is reasonably improbable to associate it with an identified or identifiable individual.

When assessing the identifiability of an individual, it is crucial to consider all potential means, those that could be utilized by either the data controller or any other party, to indirectly or directly identify the person in question. To evaluate the likelihood of these means being employed, several objective factors must be weighed, such as associated costs, time, and the technology available.

In contrast, the A29 WP Opinion on Anonymization Techniques asserts that there should be no residual risk of identification, defining anonymization as the process of modifying personal data in such a way that identification becomes irreversibly impossible. As per the A29 WP, anonymization should render identification permanently impossible, given the current state of technology. Furthermore, the A29 WP offers three criteria to discern whether data can be considered anonymous:

1. Singling Out: this pertains to the potential to isolate certain records or all records that identify an individual within the dataset.
2. Linkability: this represents the risk that arises when a minimum of two datasets contains information concerning the same individual.
3. Inference: this refers to the ability to deduce, with a significant degree of probability, the value of a particular attribute based on the values of a separate set of attributes.

Furthermore, there has existed divergence on the topic of before which parties the data shall be anonymous. Two approaches have been given:

a) Relative approach: data must be anonymous from the perspective of the controller and consider realistic chances of combining data in order to identify the individual.
b) Absolute approach: data must also be anonymous from the perspective of third parties. It takes into account all possibilities and chances in which the data controller, or any other party, would be able to identify the data subject individually.

For the purpose of ensuring a higher degree of compliance, we suggest taking a stricter approach and analyzing the processed data according to the A29 criteria to determine if the data are anonymous.

### 5.1.2 ERATOSTHENES: Are Device Identifiers Personal Data?

The ERATOSTHENES project, as outlined in the initial section, does not directly deal with the identities of natural persons. Instead, its primary focus is on identifying objects and forming potential connections to the identities of legal entities.

An identity describes an entity within a specific scope. The International Telecommunication Union (ITU, 2018, p.4) defines identity as a “representation of an entity in the form of one or more attributes that allow the entity or entities
to be sufficiently distinguished within context”. At the same time, identity refers to an entity. An entity is a real-world thing (Clarke, 2009) which includes and, at the same time, distinguishes between natural or legal persons and objects. All of these can be considered entities and, therefore, have an identity. However, the content will differ depending on the specific entity it pertains to, as well as the unique characteristics of the digital medium.

When applying the concept of identity to objects, factors to consider could be whether these objects allow interconnection, have Internet access, or are subject to specific regimes that justify their traceability. Secondly, the specific purposes could be logistics, commerce, fraud prevention, or traceability during the lifecycle, among many others. The digital identity of objects is usually managed through identification, which at the same time can refer to different techniques such as identifiers (e.g., GUID4 or UUID5), codes, radio-identification…

Within the framework of the ERATOSTHENES project, several identification technologies have been proposed. Specifically, these include a physical unclonable function (PUF) and the assignment of decentralized identifiers (DIDs), which facilitate the identification of devices within DLTs. While DIDs have been suggested for identifying natural persons, there are concerns about potential issues arising from their association with blockchain technologies, particularly the potential conflicts with the right to be forgotten. To circumvent this issue, the project aims to exclusively associate DIDs with the identities of devices. Detailed information can be found in ERATOSTHENES Deliverable D3.1.

However, it is crucial to examine whether identifying objects (or, in this case, devices) could identify or make natural persons identifiable. To evaluate this, we propose considering two key elements when enrolling a device in the ERATOSTHENES architecture:

- **Device Identifier**: this is assigned through various technologies. The PUF, for instance, acts as a digital fingerprint for devices. Moreover, within the context of DLT, these devices are given a DID.
- **Introducer’s Certificate**: this refers to the entity that enrolls the device in ERATOSTHENES. Although this certificate could potentially refer to a natural person, the primary goal within the ERATOSTHENES framework is to limit it to data pertaining to a legal entity. In exceptional cases, for security control purposes, the certificate could contain personal data if it becomes necessary to reidentify the specific person within an organization who enrolled a device within a certain legal entity.

The point of departure we take is that, in principle, a device’s identifier, by itself, will not be qualified as personal data. It will require studying the specific design of the identifier (e.g., Mark’s iPhone could easily identify the owner of the device) and the context in which it is used (e.g., if other data are collected or could potentially be accessed and could ease identification).

In the ERATOSTHENES architecture, the introducer’s certificate plays a crucial role. This certificate should ideally be limited to identifying the legal entity (e.g., indicating that a specific smart thermometer belongs to the University of Murcia). However, it could also contain personal data, leading to two possible scenarios:

- **The owner and the introducer are not the same person**, but it becomes necessary to reidentify the specific individual within an organization who has enrolled the device (e.g., Mark, a manager at Company X, has enrolled Device Y).
- **The owner and the introducer of the device are the same person**. The individual who enrolls the device is also its owner (e.g., Mark has enrolled his own iPhone).

In both scenarios, the processing of personal data will require the implementation of suitable safeguards. However, the implications are more significant in the second scenario, as identifying the owner of a device could lead to traceability of all actions performed by a specific individual using that device. Conversely, in the first scenario, the data processing would primarily pertain to the security measures and controls that are implemented within data governance policies.

© ERATOSTHENES, 2020
Consequently, the conclusion should be simple: in the context of ERATOSTHENES a device's identifier should not be qualified as personal data, provided certain conditions are met. We propose using the A29 WP criteria to identify these conditions:

- The device's identifier does not single out, or allow singling out, data that could potentially identify the user. This implies that a device's identifier, such as Mark's UMU iPhone, is not used. Moreover, no additional data that could allow identification is collected. Furthermore, the use of anonymity techniques is suggested (e.g., a MAC address is not collected directly, but it goes through a process of anonymization/pseudonymization).
- The device's identifier does not enable one to infer that two data sets contain information about the same individual. For instance, from the device identifier XYZ used for workout purposes, we cannot associate it with the user's height.
- The device's identifier does not permit deducing, with a high probability, the value of other attributes. For example, from the device identifier XYZ, one cannot deduce that the owner is 28 years old.

Moreover, within the framework of ERATOSTHENES:

- The introducer's certificate does not identify a natural person. Particularly, it does not identify the owner of the device.

In conclusion, a device identifier does not necessarily entail the processing of personal data. However, this qualification will need to be obtained in a specific scenario once the concrete data to be processed is determined and the different criteria reassessed. Within the project's scope, the target objective is to design scenarios where the context in which the device identifier is processed is not considered personal data. Consequently, while interconnected devices could potentially share personal data among themselves, this data sharing is beyond the scope of the ERATOSTHENES architecture, whose primary function is to facilitate trust, placing significant importance on ensuring that devices, assigned a certain trust score, are not associated with a natural person.

However, exploring potential avenues, such as the reputation of a specific natural person, to establish trust in a certain device could be interesting. Yet, such considerations exceed the project's scope.

5.2 Scope of the Data Protection Impact Assessment

This DPIA aims to evaluate the potential data protection implications of selected pilots and their respective use cases within the ERATOSTHENES project's scope. Therefore, analyzing the general architecture goes beyond the objective of this task. However, it was still necessary to address specific aspects as these could ultimately influence the proposed use cases, which embody the implementation of the architecture in specific scenarios.

It should be noted, however, that all the data used in the pilots' testing phase will be synthetic. Therefore, our analysis aims to extend beyond this controlled scenario to understand the potential data protection implications in a real-world deployment situation. The description of pilots, their use cases and data flow are described in Section 3.

5.3 Data Protection Considerations

This section is designed to analyze the data protection and privacy implications associated with the use cases outlined earlier. Considering the particular nature of this study, which does not primarily focus on an architecture designed for processing personal data, we have structured this section to address two fundamental questions:

1. Does the design of the pilot’s use cases directly affect privacy and data protection?

---

20 If it does identify the user of the device, it would be impossible to consider it as anonymous data.

21 But instead, are only associated with legal entities.
2. Does the pilot signify any indirect enhancements or challenges from the standpoint of privacy and data protection?

The references made throughout this section are envisaged in the context of a potential future real implementation of the use cases described within the three pilots.

5.3.1 Data Protection Implications-Connected Vehicles

In response to the first question, the pilot does not present any direct implications, as identifiers are assigned only to vehicles, not individuals. One might ponder whether these vehicle identifiers could potentially be linked to the respective owners or drivers of the vehicles. However, the design of the identifier in this particular use case should be constructed in such a way that it precludes this possibility.

Nevertheless, as previously outlined in the introduction, we must evaluate whether the data meets the criteria to be considered anonymous. As such:

- The device identifier is specifically designed to avoid singling out individuals. These identifiers should ideally comprise a random combination of numbers and letters and do not include personal identifiers such as names or surnames.
- The vehicle identifier does not facilitate the identification of other data sets belonging to the same individuals. Given the random mix of numbers and letters, it would be impossible to determine if other potential data sets belong to the same person.
- The vehicle identifier does not permit the inference of additional data.

In this context, data such as vehicle registration plates are not used, as this type of information could easily become personal data when combined with other data sets. Moreover, no additional data is being collected (any potential personal data remains within the device and is not processed through the ERATOSTHENES architecture) that could potentially render the individual identifiable. Additionally, it is crucial to emphasize that these vehicle identifiers are in no way connected to an ERATOSTHENES user account and that the entity responsible for enrolling the vehicle in ERATOSTHENES is the manufacturer (hence, a legal entity) prior to being owned by an individual. Furthermore, the type of data that could typically be processed within the ERATOSTHENES framework, particularly for IdM purposes, might be restricted to the type of vehicle. For instance, whether it is an emergency vehicle.

Concerning the second question, from an indirect standpoint, this use case can indeed represent an enhancement for privacy and personal data protection. In this context, the ERATOSTHENES functionality evaluated within the scope of the pilot introduces an additional layer of security to interconnected vehicles. Specifically, the capability to verify and assign a trust score safeguards against malicious entities intercepting the vehicle, which could potentially lead to a privacy and data breach through the transmission of malware, phishing attempts, or other forms of cyberattacks.

ERATOSTHENES prevents such possibilities, thereby effectively reducing privacy risks. We outline the following potential privacy risks in these scenarios:

- **Unlawful access to personal data.** This risk could emerge in both use cases, during connection to an external element or during a software update. ERATOSTHENES’ monitoring and assignment of trust levels significantly mitigate the chances of such an attack occurring. Privacy threats in normal scenario and pilot use cases are listed in Table 15 and Table 16.

Normal Scenario

Table 15: Privacy Threats identified using DPIA in Pilot 1 normal scenario

<table>
<thead>
<tr>
<th>Threat</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
</table>

22 Therefore, the vehicle will be enrolled in the ERATOSTHENES prior to be owned by an individual.

© ERATOSTHENES, 2020
Pilot Use Cases

Table 16: Privacy Threats identified using DPIA in Pilot 1 use cases

<table>
<thead>
<tr>
<th>Threat</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlawful access to personal data</td>
<td>Unlikely</td>
<td>Significant</td>
<td>Low</td>
</tr>
</tbody>
</table>

- **User Traceability.** This type of attack could potentially occur following a data breach. The OBU may be synchronized with a specific user account. An attacker could exploit the identification of the natural person for traceability purposes. As with the previous risk, the added layer of security in this particular use case significantly diminishes the likelihood of such a cyberattack taking place. Traceability threats in normal scenario and pilot use cases are listed in Table 17 and Table 18.

Normal Scenario

Table 17: Traceability threats identified using DPIA in Pilot 1 normal scenario

<table>
<thead>
<tr>
<th>Threat</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Traceability</td>
<td>Relevant</td>
<td>Significant</td>
<td>High</td>
</tr>
</tbody>
</table>

Pilot Use Cases

Table 18: Traceability threats identified using DPIA in Pilot 1 use cases

<table>
<thead>
<tr>
<th>Threat</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Traceability</td>
<td>Unlikely</td>
<td>Significant</td>
<td>Low</td>
</tr>
</tbody>
</table>

No new vulnerabilities have been identified in the implementation of the ERATOSTHENES architecture. Therefore, the key factor is the proper anonymization of the vehicle identifier for the purpose of:

- Minimize processing when it is neither necessary nor proportional.
- Avoid creating new opportunities for potential attackers who might target the ERATOSTHENES architecture with the aim of obtaining personal data, which could potentially lead to subsequent cyberattacks.

### 5.3.2 Data Protection Implications-Smart Health

The second pilot may present more complexities from the perspective of data protection, given that an association occurs between the device's identifier and the user account. However, this association is managed outside of the ERATOSTHENES architecture. It falls under the scope of Tellu's services, which are solely aware of the link between the device identifier and the user's account. Furthermore, it is important to emphasize that the pilot will not use any personal data. Any references made in this section pertain to hypothetical future scenarios of real implementation.
In our opinion, in a scenario where all the processes are managed by Tellu (acting as data controller), that is to say, it deploys the ERATOSTHENES architecture, it is very unlikely that device identifiers are considered anonymous data insofar as there is an association. Still, it will have to be determined in the scenario of real implementation the specific data collected by Tellu that could potentially render the device identifier as anonymous proved that the possibility of establishing this association is highly unlikely and, therefore, could potentially be considered as anonymous data following the relative approach.

The classification as personal data implies the application of the GDPR, necessitating compliance with its principles. Tellu is deeply conscious of these principles and obligations. They ensure the utmost in privacy and data protection, given how crucial it is to their business model. However, we will revisit some of these measures in this section.

The legal basis for the processing of personal data in a hypothetical real implementation of the use cases described within the pilot could be user consent or the performance of a contract, pursuant to Article 6.1(a) and (b) of the GDPR, depending on the manner in which Tellu’s services are acquired. In any case, the user enrollment and creation of the user’s account occurs in a prior stage, during which certain personal data is typically processed. This requires adherence to data protection safeguards. This step, however, is assumed to have been previously addressed by Tellu's service. Within the specific context of the pilot, and only in a scenario of real implementation, it would be necessary to obtain consent for processing the device identifier or at least make the user aware of the association with their account. Moreover, Tellu must ensure the user's right to withdraw consent or opt out of its services.

Other principles that warrant consideration include data minimization. This principle has a unique manifestation within the scope of this project, specifically the limitation on data retention terms. Data minimization is not solely about collecting the bare minimum data necessary for the purposes but also restricting its storage to the time strictly required. This becomes relevant within the scope of a DLT, which means that no personal data should be stored in a DLT to ensure compliance with the data minimization principles as well as with the right to be forgotten.

From the perspective of proportionality, it is necessary to evaluate if the objective sought through data processing can be achieved by other means posing lower risks. Following the guidelines of the Spanish Data Protection Agency, there is a need to scrutinize each data processing operation in line with the proportionality requirements, entailing three successive assessments:

1. **Suitability Criteria**: Assessing if the measure can achieve the proposed objective.
2. **Necessity Criteria**: Evaluating whether the measure is necessary means there is not a more moderate alternative available to attain the same level of effectiveness.
3. **Strict Proportionality Criteria**: Determining if the measure is balanced (i.e., the benefits to the general interest outweigh the potential damage to other conflicting assets or values).

While the processes described in the pilot could technically operate without linking to a user's account, within the context of Tellu's service, this association is essential. This is due to the nature of services provided by Tellu, specifically an e-health platform that tailors healthcare to individual patient needs.

Furthermore, other principles will apply, such as data accuracy and transparency of processing (Article 5.1 (d) and (a), respectively, of the GDPR). Transparency in processing entails that, on the one hand, the user has the right to access their own data at any time without needing to provide special justification, ensuring that they are aware of the information being processed. On the other hand, data processing should be transparent to facilitate auditing by law enforcement authorities and to help identify potential unlawful activities.

Data confidentiality is also a critical requirement, though its application is more pronounced outside the scope of the pilot. While the device identifiers should be kept confidential, the main privacy risk in this scenario arises from the

---

23 We claim that it is very unlikely because, in our opinion, it is not impossible. It depends on the specific data collected by Tellu. It is possible to use this type of platform in an anonymous way, but it is very unlikely. In addition, data relating to the physical appearance or condition is generally collected.

24 As per Article 7 of the GDPR, the controller, in this case, Tellu, must demonstrate that the data subject has consented to the processing. This necessitates the presentation of clear and distinguishable consent information.
Disclosure of sensitive data captured by the device. The methods these devices use to capture data, as well as their transmission to Tellu's platform, fall outside the scope of the ERATOSTHENES architecture.

The possibility of pseudonymizing the data related to the user and devices should also be considered to mitigate potential privacy risks. However, given the nature of their services, Tellu will normally know which user owns which device. Therefore, even if the device identifier undergoes anonymization techniques, it will still retain the classification of personal data.

In the context of this pilot, the pivotal element is ensuring that the link between the device's identifier and the user's account is not permanent. This link must be destructible, rendering the device's identifier, which can be stored on the DLT through the generation of a DID, as anonymous. By doing so, it upholds compatibility with the right to be forgotten. Practically, this is achieved in the specific use case by physically and logically separating the user's account from the device's identifier.

Furthermore, similar to the first pilot, we believe that implementing the ERATOSTHENES architecture in these scenarios could represent a significant enhancement in terms of privacy and data protection. The main privacy risk that emerges in the context of this pilot is:

- **Unlawful access to personal data.** This risk is aggravated by the fact that health data, considered as special categories of personal data under Article 9 of the GDPR, are being processed by these devices. While the pilot focuses on accessing or sharing sensor data, our analysis also considers the potential sharing of health data if necessary. Privacy threats in normal scenario and pilot use cases are listed in Table 19 and Table 20.

### Normal Scenario

<table>
<thead>
<tr>
<th>Threat</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlawful access to personal data</td>
<td>Relevant</td>
<td>Maximum</td>
<td>Very critical</td>
</tr>
</tbody>
</table>

### Pilot Use Cases

<table>
<thead>
<tr>
<th>Threat</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlawful access to personal data</td>
<td>Unlikely</td>
<td>Maximum</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Notably, the pilot, through its various use cases, facilitates crucial improvements that, despite materializing in the same privacy risk, impact three distinct dimensions:

a) **Data Sharing.** It enables an evaluation of devices and users to ascertain whether it is safe to share certain data with third parties.

---

25 It does not necessarily imply that Tellu knows the name and surname of the patient. It might be possible that the patient decides not to use their real name. However, this scenario is unlikely in the described scope and Tellu will be aware of certain personal data. For instance, it is likely that it will be aware of an email address, as well as other personal data, such as gender, age, height, etc.

26 Unless both, the user and the device identifier go through a process of anonymization.

27 The analysis limited to sensor data will be very similar, with the difference that the impact would be limited, materializing in a risk low risk for normal scenario and almost negligible for pilot use cases.
b) **Device Behavior Control.** It controls and monitors the behavior of external private devices, preventing malicious activities that might otherwise go unnoticed by the user.

c) **Emergency Services Access.** It allows access by emergency services to sensor data by doing so with enhanced assurances and respect for privacy and data protection rights.

As a result, the potential real implementation of this pilot could involve personal data. However, it is important to distinguish that the handling of health data would occur outside the ERATOSTHENES architecture, as it forms part of Tellu's core business. The unique value added by the pilot lies in the identification of devices through ERATOSTHENES. We conclude that while this pilot can bring important benefits, the presence of a DLT in the architecture necessitates caution. Any form of personal data recording on the DLT should be avoided, particularly any record of the association between devices and user accounts.

### 5.3.3 Data Protection Implications-Disposable IDs in Industry 4.0

The third pilot could potentially have the least direct implications on personal data processing, given its focus on the industrial domain. The purpose of this pilot is to explore the benefits of ERATOSTHENES in the context of industrial applications, which usually do not involve natural persons.

Therefore, the situation is similar to that described in the first pilot. In this scenario, we have a device that enrolls within the architecture. However, instead of obtaining a permanent identifier, the device gets a sort of temporary identifier valid for a specified period of time.

The significant distinction, however, is that this identifier does not refer to a natural person, nor can a natural person be indirectly identified through this identifier, as it refers to a device used within the industrial context. Therefore, this identifier would not be qualified as personal data.

From the perspective of indirect implications, as with the other pilots, there is a potential improvement in privacy and data protection derived from robust mechanisms for authorizing access to personal data. This comes into play when an identity is verified, but more particularly, the permissions and authorizations associated with that identifier. This is especially relevant in scenarios where infrastructures are constantly interconnected and, therefore, sharing information. While the authentication/authorization flow occurs at every access point, it is enhanced in the pilot by:

- The temporary nature of the identifier. Once it is invalid, the associated permissions become null and void.
- The trust score is assigned within the ERATOSTHENES architecture.

Consequently, the primary privacy risk associated with this use case is again:

- **Unlawful access to personal data.** This could occur if a malicious industrial device gains access to specific data domains that are restricted, thereby committing potential subsequent cybercrimes. Privacy threats in normal scenario and pilot use cases are listed in **Table 21** and **Table 22**.

#### Normal Scenario

**Table 21:** Privacy threats identified using DPIA in Pilot 3 normal scenario

<table>
<thead>
<tr>
<th>Threat</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlawful access to personal data</td>
<td>Relevant</td>
<td>Significant</td>
<td>High</td>
</tr>
</tbody>
</table>

#### Pilot Use Cases

**Table 22:** Privacy threats identified using DPIA in Pilot 3 use cases

<table>
<thead>
<tr>
<th>Threat</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
</table>
Unlawful access to personal data | Unlikely | Significant | Low

By mitigating this risk, other potential types of cyberattacks, such as identity theft, are also deterred. For instance, a flaw in the industrial chain could allow a malicious device to access my consumer data, which could then potentially be used for impersonation purposes.

Therefore, the impact of this pilot on privacy and data protection is minimal, given its specific application scope. However, this conclusion is context dependent. Implementing the same functionalities in a different scenario would necessitate a separate analysis.

5.4 Risk Treatment Plan

The outcome of this DPIA reveals that no significant risks pertaining to privacy and data protection have been detected. The design framework of the pilots, coupled with the particularities of the architecture (specifically designed for IoT contexts) and its application in scenarios that are not significantly associated with natural persons, efficiently minimizes potential risks to privacy and data protection.

However, it is recommended that certain precautionary measures are put in place. These measures vary in nature; some are more generic and hence universally applicable across all pilots, while others are tailored more specifically toward individual pilots. Yet, it should be highlighted that these measures refer to scenarios of potential real implementation of the pilots, insofar as in the testing within the ERATOSTHENES project, no personal data is involved.

5.4.1 Basic Safeguards

Each pilot will need to implement the following measures:

A) Actions to guarantee the anonymization of device identifiers:

- The introducer's certificate should not contain any device’s owner information or personal data whenever possible and should be restricted to the identification of legal entities (e.g., that a certain device belongs to the University of Murcia).
- Device identifiers should be anonymized through techniques such as randomization, encryption, the addition of noise…
- No additional data that is not strictly needed for the service is collected.
- Strict access control measures should be put in place so that only authorized personnel can view or modify device identifiers. This can be accomplished through the implementation of two-factor authentication solutions or monitoring of access and changes to device identifiers.
- Regular audits should be conducted to avoid issues like duplicated device identifiers.
- The promotion of security education, with ongoing training and awareness sessions for staff members, should be prioritized.
- There should be defined protocols for the recycling of device identifiers.
- A secure backup system for identifiers should be established to prevent loss or corruption of these identifiers.

B) Measures to ensure the privacy and data protection of various participants:

- Adhere to a privacy policy for the provision of their services that is fully compliant with all GDPR principles, particularly the principle of data minimization, by not requesting any additional personal data beyond what is necessary for the provision of their services.
- Implement a policy for communicating incidents that impact device identifiers or other potential personal data.
- Develop a plan for regular vulnerability scanning, setting up intrusion alerts, and managing access to information.
- Maintain an inventory of all software and hardware.
- Establish procedures for detecting software vulnerabilities and coordinating responses.
• Develop a comprehensive policy for handling all types of incidents to limit the impact or consequences of successful attacks and devise procedures for incident management.

5.4.2 Specific Safeguards

In terms of the specific risks for each pilot, we have identified a set of additional measures.

• **Connected Vehicles**

Given that the processing of personal data is not identified, risk mitigation measures should focus on preserving the anonymity of vehicle identifiers. This can be achieved by:

  • Utilizing techniques such as randomization to ensure the anonymity of the vehicle identifier so it cannot be linked to an owner or driver (as would be the case with vehicle registration plates).\(^{28}\)
  • Refraining from collecting any additional data that could cause the vehicle identifier to be classified as personal data.
  • Monitoring the operation of the architecture to prevent the emergence of potential backdoors that could extract personal data from the vehicle.

• **Smart Health**

In this pilot, we have identified the potential processing of personal data, thus necessitating the adoption of GDPR safeguards:

  • Considering the possible nature of the identifier as personal data, it will be essential to obtain the user's informed consent, or if the legal basis applicable for the processing is a contractual obligation, at least make the user aware of the association between their Tellu's account and the devices.
  • Additionally, the association between the user's account and the devices should be established in such a way that it is impossible for third parties to make this association. Beyond physical separation, this could potentially be achieved through techniques such as anonymization, encryption, or hashing.
  • The user must have the option to exercise their rights, withdraw their consent, and request their data to be deleted. This means that the pilot should be designed in a way that enables data erasure. Therefore, no personal data should be stored on the DLT, and by deleting data such as the user account, the device's identifier (which might have an associated DID registered in the DLT) becomes anonymous data.
  • Tellu should maintain a record of all processing activities and avoid the device-user account association in all instances where it is not necessary.

• **Disposable IDs in Industry 4.0**

The processing of personal data is not identified, and given the industrial deployment of these use cases, there is not an immediate need to preserve the anonymity of the device identifier. However, it is still advisable to consider the following measures:

  • Adoption of policies regarding the lifespan of disposable IDs.
  • Implementation of token-based authentication instead of transmitting the identifier directly.
  • Consistent monitoring of the system architecture to preempt the emergence of potential vulnerabilities that could lead to unauthorized extraction of personal data from industrial domains.

\(^{28}\) In principle this should not happen in the specific scope of the pilot studied insofar as the enrollment takes place by the manufacturer, prior to be owned by a specific user.
5.5 Exploitation Guidelines

It is important to insist on the fact that all pilot testing in the scope of this project will exclusively use synthetic data. This approach effectively mitigates any potential concerns related to privacy and data protection.

However, the primary objective of this study was to understand the potential implications of the use cases comprehended in the pilots within a real-world implementation scenario. Our findings suggest that, with the exception of pilot 2, the impacts are generally limited due to the specific scope of deployment (i.e., strict IoT scenarios). Nevertheless, the ultimate goal is to transition these pilots into real-world scenarios, necessitating the implementation of safeguards.

In light of this, and in addition to the recommendations provided in the previous section, we advise the following, considering the current tension between GDPR and blockchain technology:

- As much as possible, avoid linking users to device identifiers. Certain factors, such as a user's reputation contributing to the trust level of a device, may need to stay within academic discussions and be explored at a later stage once there is clear guidance on the compatibility between GDPR and blockchain.
- If such associations cannot be avoided or if personal data must be processed:
  a) Consider the use of current experimental techniques to facilitate compatibility with data erasure. These techniques may include homomorphic encryption, hash functions (particularly chameleon hashes), the addition of noise, pruning, and others. However, given the uncertainty surrounding the effectiveness of these techniques in anonymizing data, we recommend adopting a cautious approach. Nonetheless, if certain data must be stored on the blockchain, it is preferable to employ these techniques.
  b) Opt for off-chain data storage and reconsider the necessity of a DLT. In some instances, the DLT may not be required as the same functions can be achieved using a traditional database, at least until the legal uncertainties surrounding blockchain are clarified. Choose off-chain data storage methods that allow for data erasure and can anonymize the device's identifier.
  c) Acknowledge that if a user chooses to exercise their right to data erasure, it may necessitate restarting the blockchain. However, this option is generally not feasible from a business perspective.

At present, there is no official clarification on the intersection of blockchain technologies and the right to be forgotten. It is anticipated that data protection authorities, such as the European Data Protection Supervisor or the Article 29 WP, will eventually issue guidelines on this matter, clarifying the legal text's content. However, until such time, it is advisable to employ the technology in real use cases, primarily in contexts where interaction with natural persons is minimal. In cases like pilot 2, it is crucial to adopt all necessary measures to protect privacy and data protection. This means that users must be informed and give their consent during the enrollment of their device within the ERATOSTHENES framework, as the association with the user's account will potentially categorize the device's identifier as personal data. In addition, as it has been repeatedly noted, it is crucial to ensure that the association is not stored in any form of a DLT of the type blockchain, as it would (at least for the moment) directly contravene the GDPR.

This study is conducted within the context of a research project. The use cases necessitate a second analysis in a real-world implementation context, where the specific scope of implementation is clearly defined. Nevertheless, the reasoning and safeguards proposed in this study should be considered in the final design of the pilots.

5.6 Conclusion of the DPIA

The ERATOSTHENES architecture offers enhanced security and privacy features. While this DPIA is specifically tailored for a research project, it provides preliminary insights into the architecture's implications for privacy and data protection.

In broad terms, the ERATOSTHENES architecture signifies a notable enhancement in privacy and data protection. While its primary focus is on bolstering security in IoT contexts, this enhanced security directly contributes to improved privacy. Moreover, it addresses a pivotal challenge in today's digital societies. In an era where communication capabilities have expanded exponentially, trust is at an all-time low. A growing segment of the population believes that
technology presents more risks than benefits, resulting in their exclusion. This sentiment can sometimes even bar them from accessing certain services or using specific technologies.

ERATOSTHENES addresses this exact concern by designing an architecture that allows for control, not just at the beginning but continuously monitored throughout its entire lifecycle. This capability marks a notable advancement in the social dimension, with enhanced privacy and data protection being a prime example.

The primary challenge concerning privacy and data protection posed by ERATOSTHENES is the use of blockchain technology. Given the current ambiguity around the compatibility of GDPR with blockchain, it is challenging to establish definitive guidelines on this matter. For the time being, it is advisable to limit its use and avoid storing any personal data on the blockchain. However, it is worth noting the evolving landscape. A prime example is the ambitious project led by the European Commission in collaboration with Member States to establish the European Blockchain Service Infrastructure (EBSI).

It is reasonable to anticipate that a harmonious relationship between blockchain and the GDPR will eventually be established. Given the specific nature of its use cases, the ERATOSTHENES project does not pose significant concerns in this context, largely due to its limited application scope. However, the second use case could potentially present more issues. Yet, as long as personal data is not stored on the blockchain, we believe that data processing in this scenario should be treated like any other personal data processing. This requires adopting the necessary safeguards. Moreover, it is worth highlighting that Tellu is well-acquainted with the privacy and data protection demands pertinent to its specific use case.

Although the pilots described do not anticipate storing personal data within ERATOSTHENES, such a scenario remains a potential occurrence. To address this, ERATOSTHENES is equipped with mechanisms like the advanced data protector, which ensures encryption and secure storage of the data.

In conclusion, the context in which the ERATOSTHENES architecture is introduced does not raise significant concerns regarding privacy and data protection. Its implementation can be viewed positively, especially given the enhanced security it provides, which consequently leads to improved privacy and data protection. We have also considered the possibility of leveraging the ERATOSTHENES architecture with more direct involvement of natural persons, potentially assigning trust scores to them. As long as these individuals are not permanently identifiable on a blockchain, this approach would be acceptable, provided the necessary GDPR safeguards are in place. Additionally, we recommend delving into further use cases for this technology and revisiting its potential once the debate surrounding blockchain technology and the right to be forgotten reaches clarity.
6 Conclusions

Deliverable D5.6 documents the outcomes of T5.2 from M15 to M26. It gives the details on the first deployment of all ERATOSTHENES technical components in the three pilots as well as the social impact analysis, data protection impact analysis and piloting activities of each pilot. The social impact analysis describes the impact of each pilot in different categories e.g., SME, technical, security. The impacts of pilots have characteristics such as level of impact, certainty of impact, timeline of impact, nature of impact etc. In the data protection impact analysis, the focus was on data that will be generated by the pilots. The analysis makes sure that the pilots are compatible with the GDPR. Moreover, the summary of piloting activities performed under T5.2 for each pilot has been also given in the deliverable.

As described in sections 7 and 8, the consortium has defined a well-elaborated and detailed working plan for the validation of all components (assets) of the project in the three pilots. The first deployment of the respective components per pilot has been completed and the actual validation of them has started.

The deliverable also sheds light on the testing and deployment (including validation) plans of the pilots. Each pilot will validate the required technical components and deploy them on their private deployment server. In the D5.7, D5.8 and D5.9 in M29, pilots will provide detailed technical descriptions of the test, validation and deployment processes and tools.