www.ECLIPSE DIGITAL.eu

28 November 2025

D3.2 Specific Data Protection analysis

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. DIGITAL EUROPE Grant agreement N° 101158494.

Deliverable details

Title	WP	Version
D3.2 Specific Data Protection analysis	WP3	V1.0

Contractual delivery date	Actual delivery date	Delivery type*	Dissemination**
30/11/2025	30/11/2025	R	PU

* Delivery type: R: Document, report; DEM: Demonstrator, pilot, prototype; DEC: Websites, patent fillings, videos, etc; DMP: Data management plan.
** Dissemination Level: PU - Public; SEN – Sensitive, limited under the conditions of the Grant Agreement.

Author(s)	Organization
Dune Sebilleau, Diana Jimenez, Frédéric Mesureur, Guillaume Mockly, Estibaliz Arzoz Fernandez, Léo Cornec	Trialog

Version	Date	Person	Action	Status***
V0.1	May 2025	Dune Sebilleau	Creation of the structure	Draft
V0.2	June 2025	Frédéric Mesureur	Trustworthiness profiles methodology	Draft

V0.3	June 2025	Léo Cornec, Guillaume Mockly, Estibaliz Arzoz Fernandez	Internal Trialog review of the methodology	Draft
V0.4	July 2025	Dune Sebilleau	Preparation of the preliminary review	Preliminary review
V0.5	October 2025	Léo Cornec, Guillaume Mockly, Estibaliz Arzoz Fernandez, Workshops participants ****	Integration of workshops results	Draft
V0.6	October 2025	Dune Sebilleau	First version for review	Review
V0.7	November 2025	Lola Alacreu, Diego García-Casarrubios Gálvez, Alejandro Vicent Micó, Izabel Georgieva, Christos Constantinou	Reviews	Review
V1.0	30 November 2025	Dune Sebilleau	Integration of reviews	Final

***Status: Draft, Final, Approved, Submitted (to European Commission).

****Workshops participants: UPB: Andreea-Georgiana IANTOC, Mihaela Albu, Mihai Sanduleac; Voltalis: Aurore FOURCROY; Etra: Alejandro Vicent Micó, Diego García-Casarrubios Gálvez, Lola Alacreu Garcia, María Provecho Palacio; Ubitech: I. Zafeiropoulos, Katerina Drivakou, Katerina Drivakou; FHOOE: Jakob Kolmhofer, Kashyap Shievam; CEZ: Kůla Jan, Vostatek Martin, Tichý Luděk; RDN: Kamalanathan Ganesan, Mateo Cardenas,

Nuno Pinho da Silva; TD CEN: Biernot Krzysztof; EREDES: Sita Carvalho, Elektro Ljubljana: Uršula Krisper, Klemen Nagode; D4G: Witold KRASNY

KEYWORDS

Cybersecurity, privacy, trustworthiness, CERF, data protection, AI, data governance, GDPR, KPIs, workshops.

EXECUTIVE SUMMARY

This deliverable aims to present the data protection analysis performed in the ECLIPSE DIGITAL project. It presents the methodology of the analysis, that was performed on the five ECLIPSE DIGITAL High-level use-cases (HLUC) and its results.

The analysis was performed through the organisation of workshops involving pilots representing each of the HLUCs. First, the governance framework was defined, based on the following Legal and standardisation frameworks:

- Privacy and data protection: GDPR, AI Act, Data Act, Data Governance Act.
- Cybersecurity: NIS2 Directive, Cybersecurity Act, Cyber Resilience Act.
- Others: Digital Service Act.

Workshops on privacy and cybersecurity were then organised for each of the HLUC. Here are the main results for the five HLUCs:

HLUC 1: Personalised messages for consumer flexibility based on economic benefits

- Cybersecurity: All risks may be taken.
- Privacy: The following controls were identified:
    - Information access restriction.
    - Security in information transfer.
    - Protection and compliance related to PII and records.

HLUC2: PERSONALISED MESSAGES FOR CONSUMER FLEXIBILITY BASED ON NON-ECONOMIC INCENTIVES

- Cybersecurity: All risks may be taken.

- Privacy: The following controls were identified:
  - Data anonymization.
  - Implementation of authentication measures.
  - Consent management.
  - Employ encryption protocols.
  - Appropriate GDPR requests.

HLUC3: Personalised messages to consumers about energy efficiency potential

- Cybersecurity: The following risks must be reduced:
  - Bad/Falsified measurements from meters/HEMS propagate in prediction models leading to wrong predictions.
  - Tampered energy market price causing wrong advice.
- Privacy: The following controls were identified:
  - Structured identification of hardware assets involved in the pilot project.
  - User registration and authentication procedures.
  - Malware protection is implemented through a defence-in-depth approach.
  - Regular backup and time synchronisation.
  - Comprehensive event logging is enabled and logging services, recording all activities and providing an audit trail.
  - All operational software is managed through standardized processes.
  - AIIDA securisation data collection.
  - AIIDA Consent management opt-out.

HLUC4: Alerts for Extreme Grid Situations

- Cybersecurity: All risks may be taken.

- Privacy: No users data are used.

HLUC5: General Energy Efficiency Guidance

- Cybersecurity: The following risks must be reduced:
  - AIIDA interface flooded with data queries during peak load.
  - Aggregator injects biased flexibility signals to favour specific outcomes.
  - Data breach exposing household level consumption patterns.
- Privacy: The following controls were identified:
  - Planned information classification guideline.
  - Private Git repository, Data access/sharing based on requests, Access control for HLUC5 at the database level currently not supported.
  - Configuration for near real-time data services, Passwords in end customer application, User-centric authorisation.
  - Password management in the end user application.
  - Hash code for each user (planned), Apache Kafka and MQTT to secure communication.
  - Segregation of duties in HLUC 5.
  - Multi-Factor Authentication (MFA) planned.
  - Git development setting, Keycloak, Database.
  - Git - security checks in CI/CD pipelines.
  - Institutional control (FHOOE). Not applicable to HLUC5.
  - Securely develop, test and deploy HLUC 5 planned.
  - Security in HLUC 5 development, testing and deployment is currently not implemented – externally handled.
  - Institutional control (FHOOE).

AI trustworthiness was moreover studied in the context of the French pilot to provide methodologies and recommendations for the AI-based features implemented within the project.

In the last workshops, KPIs were finally defined to follow the progress of implementation results.

The results are then used to create trustworthiness profiles, that extend the interoperability profile in order to integrate the Common European Reference Framework (CERF).

COPYRIGHT STATEMENT

INDEX

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

This deliverable aims to present the analysis of the Cross-cutting characteristic plan (X-CCP) and its results. It reviews the privacy, cybersecurity and AI trustworthiness aspects of the CERF framework, and defines KPIs (Key Performance Indicators) for its implementation in the ECLIPSE DIGITAL project.

A series of trustworthiness profiles are then detailed to define the requirements for the trustworthiness of each profile.

This deliverable is divided into three main sections.

Section 2: The section presents the methodology of the X-CCP analysis. This includes the methodology, frameworks and standards used for the:

- Governance.
- Cybersecurity analysis.
- Privacy analysis.
- AI trustworthiness.
- KPIs.

The assessment methodology and organisation of the workshops are also included in this section.

Section 3: The results of the analysis are then presented in this section. This includes a common governance section, and, for of each High-Level Use Case (HLUC), the privacy and cybersecurity as well as KPIs. Finally, the AI trustworthiness is applied to the French pilot.

Section 4: Finally, the last section presents the methodology for trustworthiness profiles, and how they can be applied in the ECLIPSE DIGITAL project. This involved:

- The selection of trustworthiness objectives for the project.
- A taxonomy for the ECLIPSE DIGITAL profiles.
- A classification of the requirements.
- A common trustworthiness mechanism profile for all use cases.
- The example of its application to the HLUC 1.

2. METHODOLOGY FOR THE DATA PROTECTION ANALYSIS

2.1. PURPOSE OF THE ANALYSIS

The data protection analysis of the ECLIPSE DIGITAL project aims at ensuring the trustworthiness of the energy apps using the CERF framework. This will ensure the protection of the users' security and privacy. In particular, in the context of energy apps, a focus will be on the energy consumers, who will be the main users of these applications. An analysis of the AI systems is moreover included, to cover the specific risks related to AI, and to future-proof the CERF, as AI systems are expected to become increasingly present in the energy ecosystem. This analysis will follow the methodology of the cross-cutting characteristics plan (X-CCP), defined by Trialog.

2.2. FRAMEWORKS USED

The methodology for the cross-cutting characteristics plan (X-CCP) in ECLIPSE DIGITAL has been developed and applied by Trialog through the course of earlier projects, including the European projects MAESHA [1], Energica [2], Parmenides [3]. It is based on Trialog's expertise and knowledge on cybersecurity, privacy, AI trustworthiness frameworks as well as regulation and standardisation.

This one-shot analysis should enable the pilots and solution providers to get a deep understanding of cybersecurity and privacy principles, based on relevant reference architectures, ISO standards, IEC standards, NIST guidelines, and models and frameworks detailed in the tables below.

Moreover, the GDPR (General Data Protection Regulation) [4] was considered for all use-cases, as well as in the ECLIPSE DIGITAL Data Management Plan, which was established in deliverable 1.2 Data Management Plan [5].

The tables below list the main references on which the X-CCP methodology is built. The other references above are used to support the technical discussions and results.

Table 1: Main references used for the privacy method analysis

Reference	Description
ISO/IEC 29134 – Privacy Impact Assessment Guidelines [6]	This standard provides guidelines and recommendations for conducting a Privacy Impact Assessment (PIA), from understanding the benefits, objectives, and targets of a Data Privacy Impact Assessment (DPIA) to how to conduct the PIA process (e.g., risk assessment, risk treatment).
ISO/IEC 31000 – Risk management – Guidelines [7]	This standard provides guidelines supporting the risk management method used within the X-CCP.
LINDDUN methodology [8]	It is a PIA method that provides support to the elicitation and mitigation of privacy threats.

	LINDDUN: Linking, Identifying, Non-repudiation, Detecting, Data Disclosure, Unawareness, and Non-compliance.

Table 2: Main references used for the cybersecurity method analysis

Reference	Description
ISO/IEC 27005 – Information security risk management [9]	This standard provides the method and the structure for risk analysis.
ISO/IEC 27002 – Code practice for information security controls [10]	This standard provides a list of information security controls to be used during the risk analysis.
STRIDE method [11]	Methodology to analyse threats. It identifies and categorizes security threats that can lead to a cybersecurity breach of the target system.

Table 3: Main references used for the AI trustworthiness method analysis

Reference	**Description**
ISO/IEC JTC 1/SC 42 - ISO/IEC 42005 Information technology – Artificial intelligence – AI system.	This standard provides a methodology and a template for AI system impact assessment.

impact assessment [12], under development.	
ISO/IEC JTC 1/SC 42 - ISO/IEC TR 24028 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence [13], 2020.	This standard surveys: approaches to establish trust in AI systems. engineering pitfalls and associated threats and risks. approaches to assess trustworthiness characteristics.
Cen-Cenelec JTC21 – AI Trustworthiness framework [14], under development.	This harmonised standard provides the structure for AI trustworthiness analysis, and it is a standardisation request from the Commission to support the AI Act compliance.
ISO/IEC JTC 1/SC 42 - ISO/IEC 23894 Information technology — Artificial intelligence — Guidance on risk management [15], 2023.	This standard provides the methodology and structure for AI risk analysis.

Table 4: Main references used for the KPI assessment method analysis

Reference	Description
IEC 62443 series – Part 2-1: Security program requirements for IACS asset owners [16].	The KPIs methodology to assess security and maturity levels is described in this standard. series. Based on these two levels it defines the Security Program Rating (SPR) with a table.
IEC 62443 series - Part 2-2: IACS protection levels [16].	

2.3. CONTENTS OF THE ANALYSIS

2.3.1. GOVERNANCE

The governance analysis aims to define the main information about the systems participating in the analysis. The participants are defined, along with the responsibilities of each party.

2.3.2. CYBERSECURITY ANALYSIS

The security analysis begins with a description of the system, its interfaces, assets, stakeholders and use-cases. The analysis is applied to all systems developed and used in the project, including complex systems such as AI systems. The analysis parameters, including the likelihood, impact and risk scales, the risk map and treatment strategy can be defined.

The next step consists of identifying the threats, starting by defining the attacker profiles, and attaching them to the threats, along with the goal, assets involved, impact and target properties of each threat.

Attack paths are then investigated. The events are identified, describing their effect, the identification of Common Vulnerabilities and Exposures (CVE), the target properties and the likelihood of the event. They are linked to the attack paths that are defined afterwards, with the related threats, and the likelihood of each attack path.

From there, the global risk level is calculated by combining the likelihood and impact ratings of each risk. The risks are also linked to the attack paths.

Finally, the treatment plans are elaborated by defining the possible controls with their goals and implementation process, and attaching them to the risks, along with the strategy used to treat the risk, and the impact of the treatment.

2.3.3. PRIVACY ANALYSIS

The privacy analysis aims to support the solution providers in identifying and assessing the risks for privacy in the developed systems.

For a privacy analysis, there are 3 main steps:

I. Context for the Privacy analysis: it is a previous step before performing the analysis. In this step, the context of the system/asset/architecture/pilot is analysed in order to decide if it is needed a PIA (Privacy Impact Assessment). There is a threshold that provides the go/no-go for a PIA.
II. Privacy analysis itself: Once it has been analysed the context and the outcome is that a PIA is needed. Then, the PIA is conducted.
III. PIA report: A PIA report presents the results of the PIA/s in such a way that is clear: 1) why the PIA is needed, scope, context and outcome; 2)

the results of the PIA in terms of breaches, threats, impact and risk assessment, to finalize with the controls (mitigation measures to reduce the risks).

The second step, privacy analysis, is performed as follows:

I. Validation of the system/asset/pilot/architecture to analyse. It is discussed and clarified the asset to analyse and all the information that represent how it works, such as data flows (most important for a privacy analysis), architecture schemas or sequence diagrams.
II. Once it is clear the asset or system to assess, it is analysed based on the critical points from a privacy and data protection point of view. The PIIs (Personal Identifiable Information), are identified and listed.
III. The privacy breaches are identified and described.
IV. The threats (causes) that could provoke the breaches are elicited and categorized, following the LINDDUN categories [17]. Both, breaches and threats are linked (cause → event).
V. Once the breaches and threats are clear and linked, it is defined the level of impact and likelihood of the breaches to happen. This will produce the risk assessment. The impact is evaluated from two perspectives: the citizen privacy and the business/organisation (ISO/IEC 27550 and ISO/IEC 27552).
VI. Risk assessment (ISO/IEC 29134 Guidelines for PIA): depending on impact and likelihood levels, the breach relies on different areas that have from low to very-high risk level. Depending on this, the controls are defined and linked to reduce or avoid the higher risks.
VII. Controls: defined to reduce or avoid the high or very-high risks, it is used the ISO/IEC 27001/27002 to categorize them.

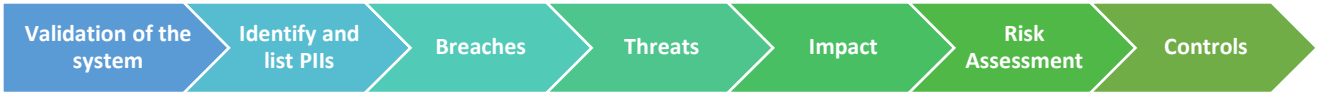


Figure 1: Privacy controls categories

2.3.4. AI TRUSTWORTHINESS

The AI Trustworthiness Plan is a practice developed in the project HEDGE-IoT [17] to support the assessment, development, management and maintenance of trustworthy AI systems throughout their life cycle. The practice is in the form of a training, an AI trustworthiness analysis, a workshop focused on AI risk analysis and the compilation of the results in a report. The AI trustworthiness questionnaire is based on the AI Act [18] and standards (published and in development). This document includes information about the AI context, scope, ecosystem, infrastructures, algorithm, model, data, trustworthiness characteristics, etc. It is in the form of a survey, or a framework divided into sections to progressively cover all the subjects.

For each AI system, a separate AI Trustworthiness Plan should be completed. It will cover subjects which are very specific to each AI system like data, model, uses, and risks.

In ECLIPSE DIGITAL, the practice is applied to three AI systems to raise awareness among the pilots, developers, managers and accountable people.

The plan is structured as follows:

1. Planning and AI system characterisation
    a. AI system plan info
    b. AI system information
2. Impact assessment

    a. AI Risk management
    b. Data, Algorithm and Model information
    c. Regulatory and standards compliance
    d. AI Trustworthiness
    e. AI Trustworthiness assurance
3. Continuous improvement
    a. Continuous improvement

Table 5 presents a more detailed structure of the survey with most of the key items available in each sub-section as well as the references used.

Table 5: Structure and references of the AI Trustworthiness Plan

Section	Sub-section	Key items	Associated standards and regulation
Plan and AI system characterisation	Plan information	• Generic information about the plan like version management, confidentiality and contacts.	[12]
	AI system characterisation	• ID information about the AI system like system purpose, life cycle stage, objectives, context, infrastructure, location, and accountability.	[14] [19] [18]
Impact assessment	AI risk management	• Relevant interested parties • Uses information • AI Risk management • Ethical, societal and environmental impact	[18] [12] [14] [20] [21] [22] [23] [24]
	Data, Algorithm and Model information	• Data information and quality • Algorithms and models information and quality	[25] [26] [14] [12]
	Regulatory and standards compliance	• Regulatory compliance • Standard Alignment	[12] [18] [20] [21] [22]
	AI Trustworthiness	• AI Cybersecurity (including logging functionalities) • AI privacy • AI Robustness, resilience and accuracy • AI Transparency (transparency, explainability, documentation)	[27] [18] [28] [27] [29] [30] [31] [32] [33] [34] [35] [36] [13] [37] [38]

		• AI management (governance, human oversight)	
	AI Trustworthiness assurance	• AI trustworthiness assurance expectations • AI trustworthiness process	[13]
Continuous improvement	Continuous improvement	• Continuous monitoring • Continuous maintenance • Continuous development	[12] [33] [32] [36]
Other items	Other items and complementary information	• Open section for additional information	[12]

2.3.5. KPIS

The goal of this assessment on security and privacy capabilities is to keep a follow-up on the progress of the implementations of the security and privacy measures during the project, and beyond the project. It aims to support the pilots' and systems' real-world implementation and scalability. Figure 2 shows the 3 main steps of the KPI management process. Firstly, an initial assessment is done to identify the current level of the pilot at security, maturity and global Security Program Rating (SPR) levels.

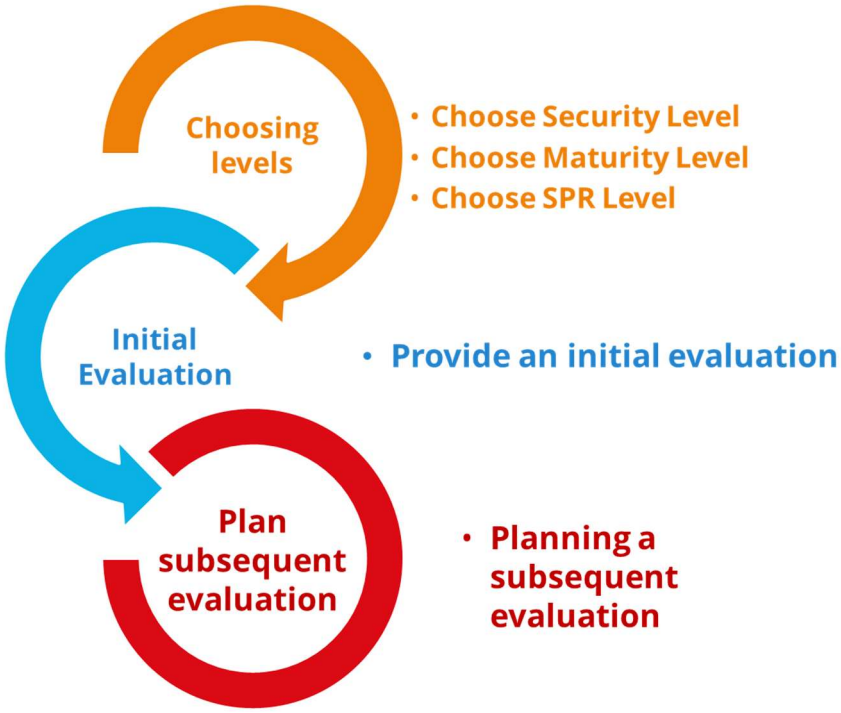


Figure 2: KPI management process - overview

A first KPIs evaluation is done before the start of the pilots and a second evaluation will be done one year later, almost at the end of the pilots and project. A partner or a pilot with a long-term approach could assess the KPIs regularly to monitor their progress.

2.4. ASSESSMENT METHODOLOGY

The assessment methodology is based on IEC 62443 [16]. It starts first with the selection of the Security Level (SL) (see Table 6) and secondly of the Maturity Level (ML) (see Table 7). Then, these two indicators are combined through a table (see Table 8), to identify the corresponding Security Program Rating (SPR). These 3 indicators are the KPIs and are defined together with the pilot team.

Table 6: List of the possible security level [16]

Security level	Description
SL0	• No or insufficient protection capability of the system of interest to reach SL1.
SL1	• Capability of the system of interest to protect against casual or coincidental violation.
SL2	• Capability of the system of interest to protect against intentional violation using simple means with low resources, generic skills and low motivation.
SL3	• Capability of the system of interest to protect against intentional violation using sophisticated means with moderate resources, domain specific skills and moderate motivation.
SL4	• Capability of the system of interest to protect against intentional violation using sophisticated means with extended resources, domain specific skills and high motivation.

Table 7: List of the possible maturity level [16]

Maturity level	Description
ML1 Initial	• Processes are performed in an ad-hoc and often undocumented (or not fully documented) manner. • Consistency across projects may not be able to be shown
ML2 Managed	• Documented process, not necessarily repeatable • Documentation exists that describes how to manage the delivery and performance of the capability. This documentation may be in the form of written procedures or written training programs for performing the capability
ML3 Defined/Practiced	• Documented process, repeatable and consistently followed. • The performance of a level 3 practice can be shown to be repeatable over time
ML4 Improving	• Documented process, repeatable and consistently followed, measured and steadily improved. • Using suitable process metrics, the effectiveness or performance improvements of the process or both, can be demonstrated. This results in a program that improves the process through technological, procedural, and management changes.

Table 8: SPR table [16]

ML4 Documented process, replicable, continuous follow-up, regular assessment and improvment	**SPR0**	**SPR1**	**SPR2**	**SPR3**	**SPR4**
ML3 Documented process, replicable, continuous follow-up	**SPR0**	**SPR1**	**SPR2**	**SPR3**	**SPR4**
ML2 Documented process, not needed replications	**SPR0**	**SPR1**	**SPR2**	**SPR2**	**SPR2**
ML1 Process ad hoc	**SPR0**	**SPR1**	**SPR1**	**SPR1**	**SPR1**
	SL0 No or insufficient protection capability to reach SL1	**SL1** Capability to protect against casual of coincidental violation	**SL2** Capability to protect against intentional violation using simpling means with low resources	**SL3** Capacibity to protect against intentional violation using sophisticated means with moderate resources	**SL4** Capability to protect against intentional violation using sophisitcated means with extended resources

2.5. WORKSHOPS ORGANISATION

A series of workshops have been organised by Trialog to define the Privacy and Security Plan for the ECLIPSE DIGITAL project. The workshops are based on the five ECLIPSE DIGITAL High-level use cases, each use case being represented by a pilot:

- HLUC1 on personalised Economic incentives: E-REDES (Portugal pilot).
- HLUC2 on personalised non-economic incentives: UPB (Romania pilot).
- HLUC3 on personalised recommendations on adoption of technologies: D4G (France, Estonia, Finland Denmark and Belgium pilots).
- HLUC4 on general alerts for critical events on the grid: CEZ (Czech Republic pilot).
- HLUC5 on general recommendations on energy efficiency: FHOO (Austria pilot).

The workshops gather Trialog's trustworthiness experts and selected pilot leaders. Other partners are moreover welcome to participate on a voluntary basis. These workshops enable to perform a focused security and privacy analysis for each pilot, for the five HLUCs developed in ECLIPSE DIGITAL. They allow to define the CERF trustworthiness profiles, as extensions of the interoperability profiles defined in D3.1.

The analysis has been divided into four phases

- The Kick-off to present the trustworthiness and its assessment to the participants.
- The training sessions, to introduce the concepts to the participants.
- The pilots' workshops, to collect all necessary information.

- The analysis of the results, done by Trialog and included in this deliverable.

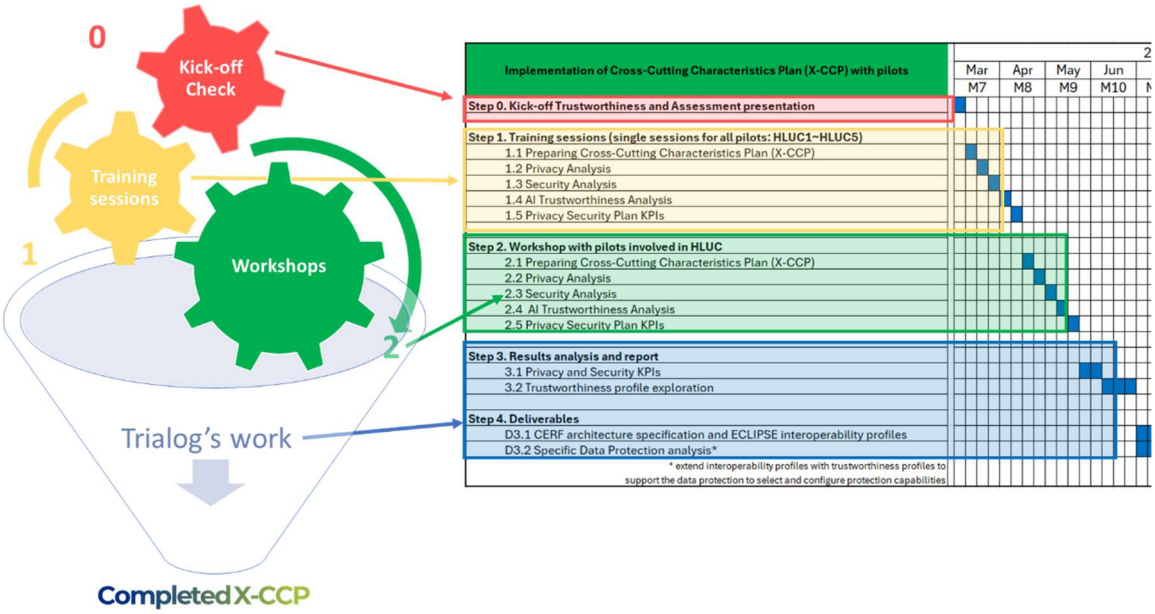


Figure 3: Organisation of the X-CCP work

The workshops used the X-CCP Assessment Dashboard provided by Trialog, which is a tool mainly made of a dashboard, providing an overview of the privacy and security activities and their progress status throughout the ECLIPSE DIGITAL project lifecycle. Activities are detailed to be carried out in separated screens of the dashboard to guide the project pilots in the analysis processes. It enables to collect, share and analyse the information about cybersecurity and privacy activities. It is moreover structured using the methodology developed by Trialog throughout several previous projects to assess the trustworthiness aspects of systems. This enables to structure the conversation and ensures that no aspects of the analysis are left behind.

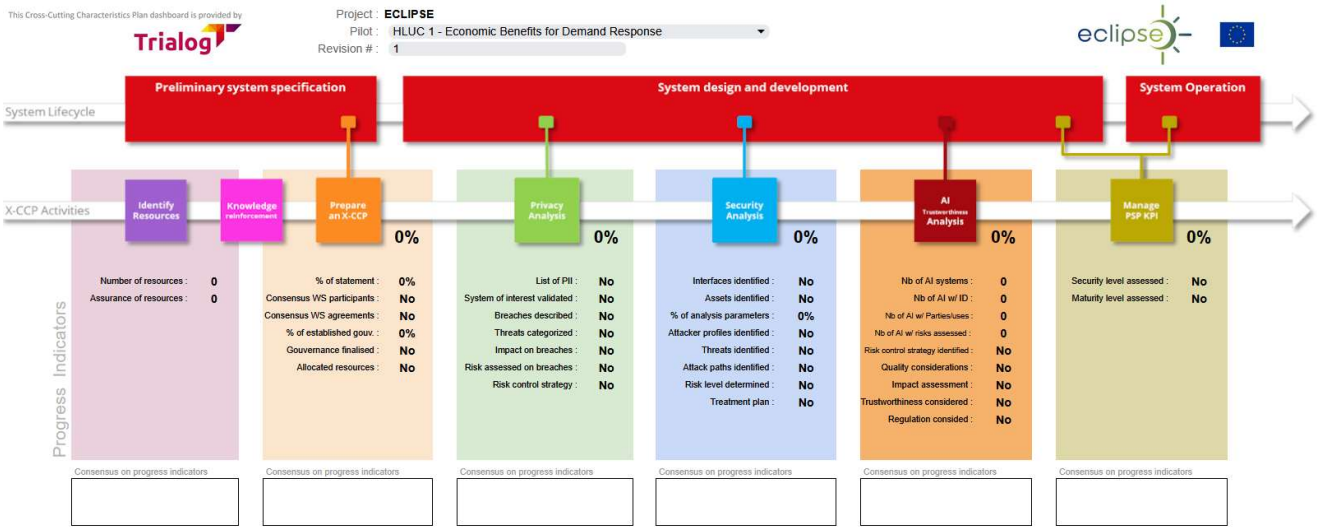


Figure 4: X-CCP assessment dashboard

3. RESULTS OF THE ANALYSIS

3.1. REMINDER OF THE ECLIPSE DIGITAL HIGH-LEVEL USE-CASES

3.1.1. HLUC 1: PERSONALISED MESSAGES FOR CONSUMER FLEXIBILITY BASED ON ECONOMIC BENEFITS

HLUC1 focuses on integrating smart devices and consumer participation into energy systems, leveraging real-time data, dynamic pricing, and flexibility mechanisms to optimize energy consumption, prevent grid congestion, and provide financial incentives for contributing to grid stability.

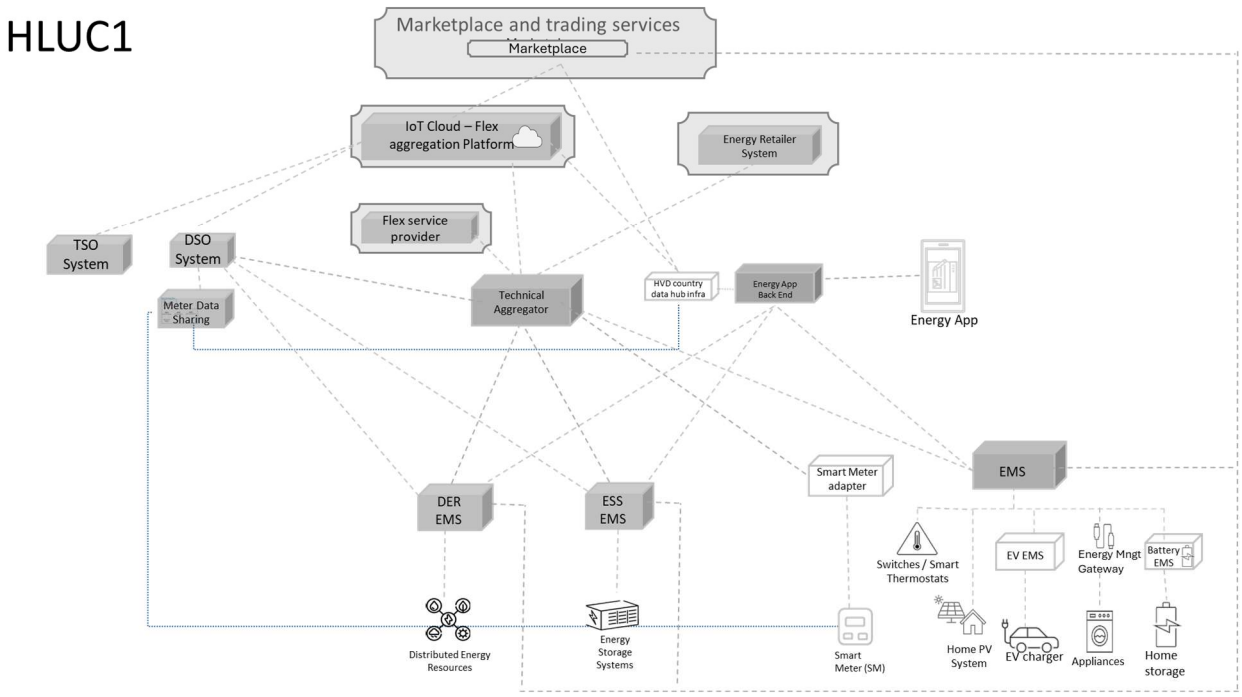


Figure 5: HLUC1 Generic SGAM architecture for ECLIPSE DIGITAL V1

3.1.2. HLUC 2: PERSONALISED MESSAGES FOR CONSUMER FLEXIBILITY BASED ON NON-ECONOMIC INCENTIVES

It focuses on leveraging real-time data, smart devices, and personalized or general information to optimise energy consumption, promote sustainability, and reduce carbon footprints by engaging users with actionable insights.

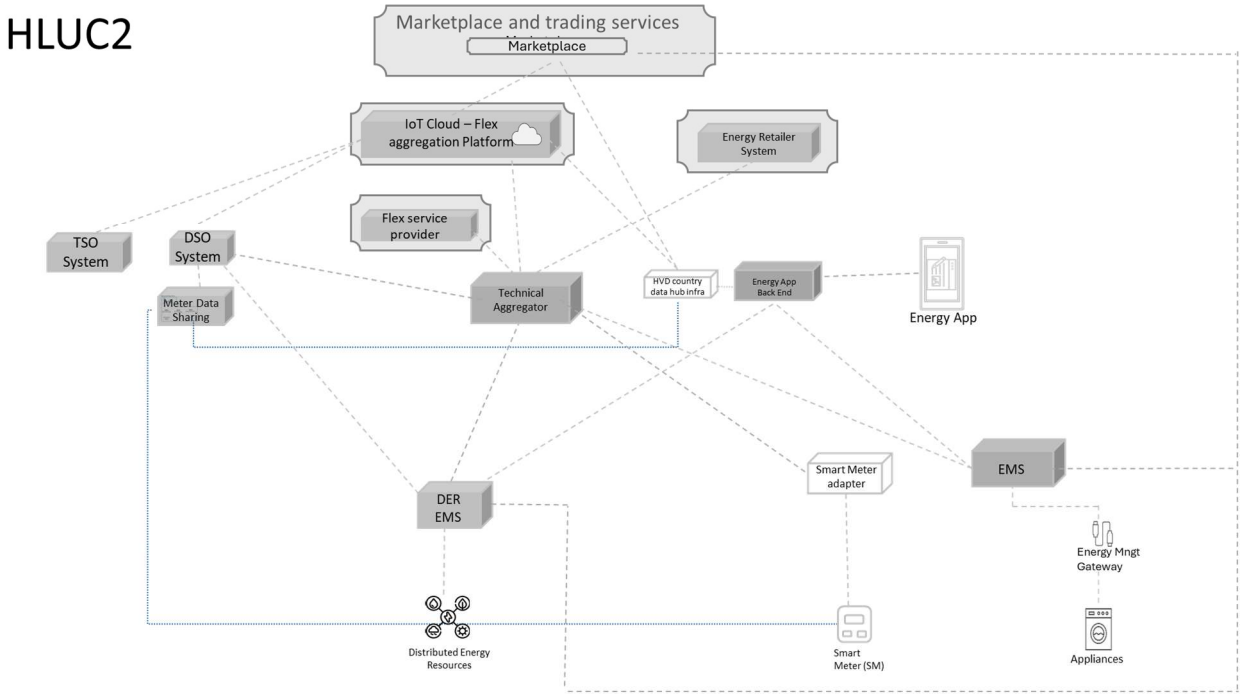


Figure 6: HLUC2 Generic SGAM architecture for ECLIPSE DIGITAL V1

3.1.3. HLUC 3: PERSONALISED MESSAGES TO CONSUMERS ABOUT ENERGY EFFICIENCY POTENTIAL

The system integrates real-time and historical data from diverse energy sources to provide personalized recommendations, notifications, and advisory services, enabling users to optimize their energy consumption, reduce costs, and align their energy usage with sustainability goals through the adoption of specific technologies.

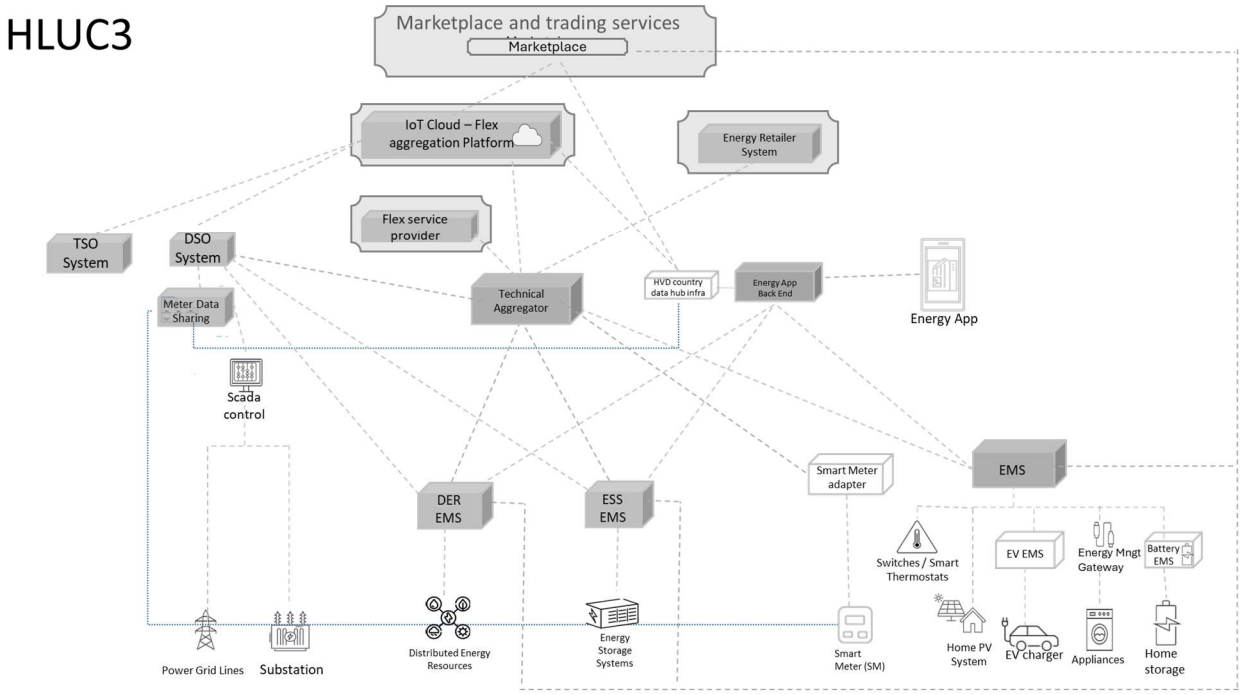


Figure 7: HLUC3 Generic SGAM architecture for ECLIPSE DIGITAL V1

3.1.4. HLUC 4: ALERTS FOR EXTREME GRID SITUATIONS

The system integrates real-time grid data from TSO and DSO to provide immediate alerts, personalized recommendations, and participation mechanisms for consumers and BSPs (Balancing Services Providers). It aims to enhance grid stability by encouraging energy-saving actions during critical events, leveraging demand response programs, standardized messaging, and simulations of extreme grid conditions.

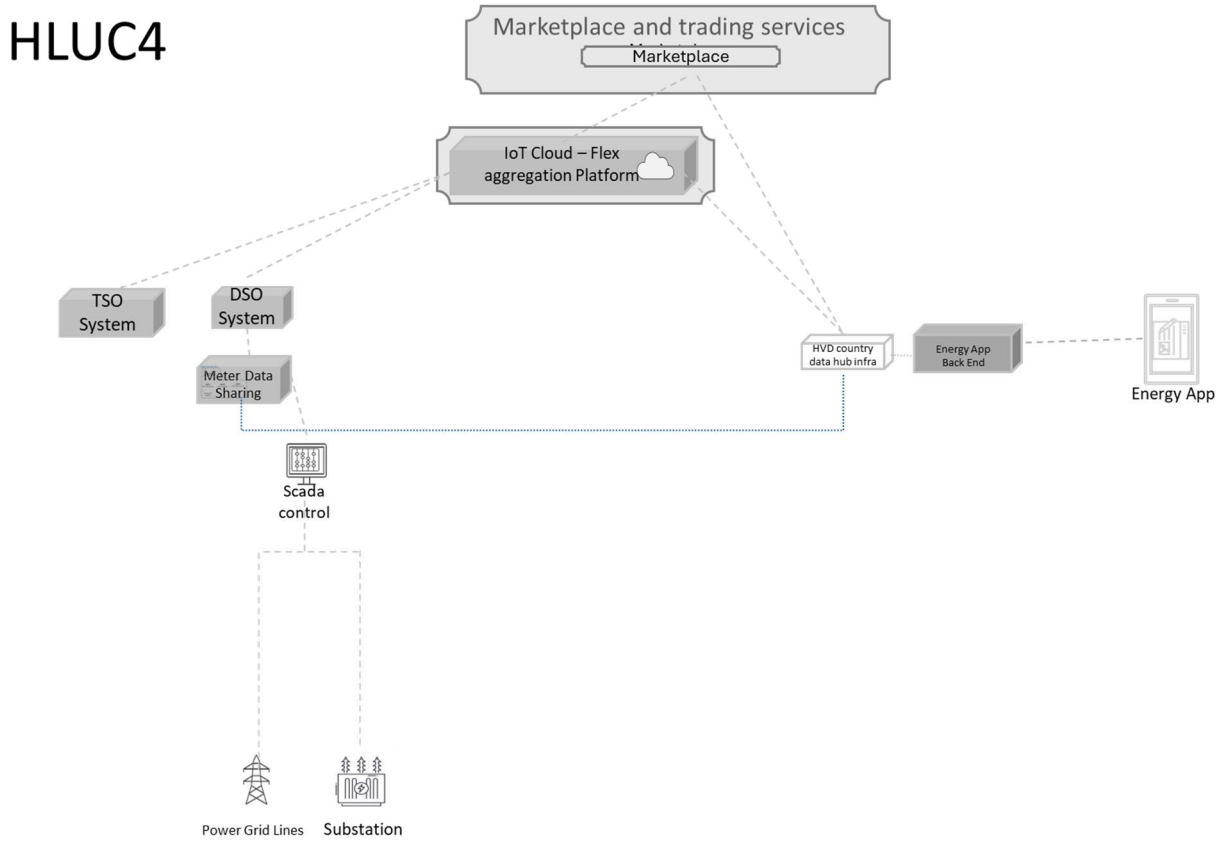


Figure 8: HLUC4 Generic SGAM architecture for ECLIPSE DIGITAL V1

3.1.5. HLUC 5: GENERAL ENERGY EFFICIENCY GUIDANCE

In HLUC 5, the app provides general recommendations, general tips, and educational content, promoting energy-efficient behaviours. It engages users through mobile apps, web pages, and gamification, catering to diverse audiences, from individual users to student residences and technical consumers.

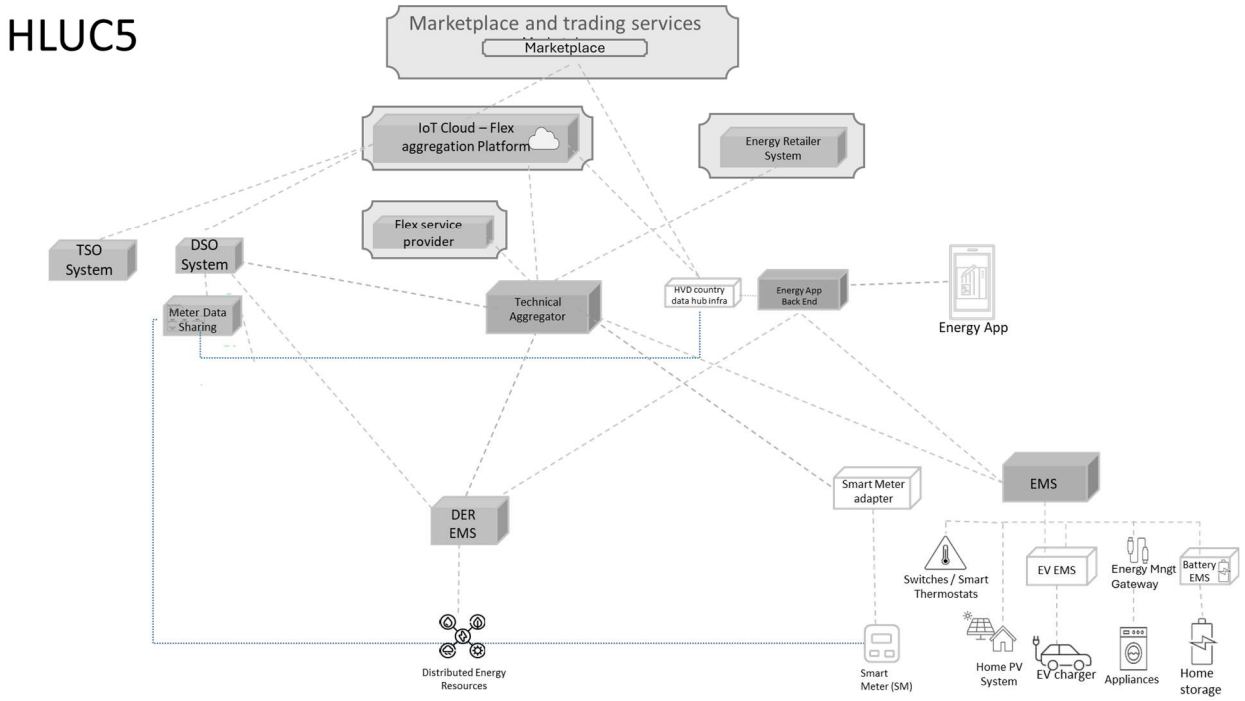


Figure 9: HLUC5 Generic SGAM architecture for ECLIPSE DIGITAL V1

3.2. GOVERNANCE ANALYSIS

The analysis of data in the X-CCP analysis is based on the data defined in the data management plan described in deliverable D2.1 “Analysis of existing energy monitoring applications and services in the market and of the legal framework” [40], and details defined in deliverable D3.1 “CERF architecture

specification and ECLIPSE interoperability profiles" [41] as well as D4.1 "ECLIPSE CERF for Energy Saving applications" [42] for the implementation details.

The Governance analysis presents three common main parts:

- Governance structure, operation.
- Legal and standardisation framework.
- Allocation of Resources.

Governance structure and operation:

In all HLUC, the governance schema presents a structure with:

- Pilot leader/manager.
- DSO.
- TSO (depending on the case).
- Aggregator or service/provider.

Depending on the use case, the TSO, DSO or Aggregator are present or not. The Governance board operates in the basis of periodical meetings (bi-weekly or monthly) to deal with pilot and HLUC actions and also cybersecurity and privacy controls update.

The data management across the ECLIPSE DIGITAL project is moreover supervised by the technical coordinator, with support from the Project coordinator, and with the advice from the Ethical external advisor. Each pilot leader then monitors the implementation of trustworthiness features their pilots, through the monitoring of the KPIs defined in each HLUC. The

timeline and responsible parties for the evaluation of the KPIs are defined at the end of each KPI table.

Legal and standardisation framework

The framework is exactly the same for all, which encompasses:

- Privacy and data protection: GDPR, AI Act, Data Act, Data Governance Act.
- Cybersecurity: NIS2 Directive, Cybersecurity Act, Cyber Resilience Act.
- Others: Digital Service Act.

Allocation of Resources:

None of the use cases and pilots need to allocate specific resources or budget for cybersecurity and privacy activities.

3.3. HIGH-LEVEL USE CASES ANALYSIS STRUCTURE

The use case analysis is divided into the cybersecurity analysis, the privacy analysis and the KPIs. The cybersecurity section analyses the threats, attack scenarios, and their links to conclude on the assessment of the risks. The privacy analysis defines the breaches and the threats, to evaluate the risk strategy and controls to be put in place. The KPIs section defines the KPIs that will be used to monitor the progress of security and cybersecurity.

3.4. PERSONALISED MESSAGES FOR CONSUMER FLEXIBILITY BASED ON ECONOMIC BENEFITS (HLUC1)

3.4.1. CYBERSECURITY ANALYSIS

Threats

Table 9: Cybersecurity threats for the HLUC 1 of ECLIPSE DIGITAL

	Threat description	Overall impact
T_HLUC1_1	End users apply falsified/incorrect directive which has adverse grid effects	Limited
T_HLUC1_2	End-users apply falsified/incorrect directive which has adverse financial effects	Limited
T_HLUC1_3	Impersonation of consumer or intermediary when negotiating agreement	Limited
T_HLUC1_4	Consumer or intermediary lying about application of incentives	Limited/Significant depending on how widespread it is
T_HLUC1_5	Leak of consumer private information	Limited/Significant

Attack Scenarios

Table 10: Cybersecurity attack scenarios for the HLUC 1 of ECLIPSE DIGITAL

STRIDE Category	Scenario ID	Scenario Description
Spoofing	**S_HLUC1_1**	Impersonating Price signal Engine to send falsified data
	S_HLUC1_2	Impersonating Consumer or Intermediary to sign an agreement
	S_HLUC1_3	Impersonating Energy App to send false messages
Tampering	**S_HLUC1_4**	Modify message from Price signal engine
	S_HLUC1_5	Modify message from Consumer or intermediary
	S_HLUC1_6	Modify message from Energy app
Repudiation	**S_HLUC1_7**	End users falsifying a record of engagement with an incentive
Information Disclosure	**S_HLUC1_8**	Accessing database containing private user information

Denial of Service	**S_HLUC1_9**	Prevent sending/receiving a message
Elevation of Privileges	**S_HLUC1_10**	Gain access to limited access features on the app

LINK Threat vs Attack Scenario

Table 11: Link between cybersecurity threats and attack scenarios for the HLUC 1 of ECLIPSE DIGITAL

	T_HLUC1_1	T_HLUC1_2	T_HLUC1_3	T_HLUC1_4	T_HLUC1_5
S_HLUC1_1	X	X			
S_HLUC1_2			X		
S_HLUC1_3	X	X			
S_HLUC1_4	X	X			
S_HLUC1_5			X		
S_HLUC1_6	X	X			
S_HLUC1_7				X	
S_HLUC1_8					X

S_HLUC1_9	X	X			
S_HLUC1_10			X	X	

Risk Assessment

Table 12: Cybersecurity risks assessment for the HLUC 1 of ECLIPSE DIGITAL

Threat	Impact	Likelihood	Overall Risk Assessment
T_HLUC1_1	Limited	Limited/Negligible	**May be taken**
T_HLUC1_2	Limited	Limited/Negligible	**May be taken**
T_HLUC1_3	Limited	Limited/Negligible	**May be taken**
T_HLUC1_4	Limited/Significant	Limited/Significant	**May be taken**
T_HLUC1_5	Limited/Significant	Limited/Negligible	**May be taken**

3.4.2. PRIVACY ANALYSIS

The HLUC1 has as main actors, the users and/or prosumers, the TSO and the DSO. There are specified, at least, 9-10 use cases to be tested in the different pilots from economic incentives, notifications of cost-effective consumption,

sandbox tariff program and tariff recommendation to request for flexibility services and participation in Service market.

The analysis of the architecture and data flows for privacy was performed. The main PIIs identified are:

- Energy consumption data.
- Production data (for prosumers).
- Id data (for each profile or user).
- Not preferences data about lifestyle and private life.

The results of the privacy impact assessment performed are the following.

Table 13: Privacy breaches for the HLUC 1 of ECLIPSE DIGITAL

Breach	Description	Overall impact
B1 - Integrity of data	Integrity of data (bids) – access to data, it could be modified	LIMITED
B2 - Confidentiality users' data	Confidentiality of the personal data of users.	SIGNIFICANT
B3 - GDPR users' rights violation	The rights defined in the law are not well addressed or respected by the data controller and processor.	SIGNIFICANT

The relation between threats and breaches:

Table 14: Privacy threats for the HLUC 1 of ECLIPSE DIGITAL

Threat	Category	B1	B2	B3
1 Identification from a CPE (connection point for electricity) to the user.	Identifiability		X	
2 Users denying they have given their Consent.	Non-repudiation			X
3 Unauthorized access to users' personal data	Disclosure of Information	X	X	
4 Unawareness of Consent for external user comparison	Unawareness and intervenability			X
5 Non-compliance with Regulation [Consent and privacy note] – wrong consent	Non-compliance			X

The different breaches, due to their level of impact and the likelihood, the risk assessment is the following, according to the Risk matrix (ISO/IEC 29134):

Figure 10: Privacy risk strategy for the HLUC 1 of ECLIPSE DIGITAL

The risk strategy is the following:

- For Breach 1, as the risk is in the green zone, it is assumed. There is no control to be taken for the risk.
- For Breach 2 and 3 as their risk is in the purple zone, measures are needed to reduce or avoid the risks.

CONTROLS

Table 15: Privacy controls for the HLUC 1 of ECLIPSE DIGITAL

Category	Subcategory	Control	Description
Access Control	System and application access control	Information access restriction	Information should only be accessed with proper authorisation and there should be different types of permissions to manage data
Communication security	Information transfer	Security in information transfer	Information transfer within the organisation must be carried out securely, adhering to the required policies and procedures.
Compliance	Compliance with legal and contractual requirements	Protection and compliance related to PII and records	Records should be protected from loss, destruction, falsification, unauthorized access and release in accordance with legislator, regulatory, contractual and business requirements. Protection and privacy of PII must be ensured and the consent statement must be clear and comply with applicable legislation and contractual requirements.

3.4.3. KPIS

This section defines the KPIs that will be used to monitor the implementation of cybersecurity and privacy measures in the ECLIPSE DIGITAL project.

Table 16: Privacy and cybersecurity KPIs for the HLUC 1 ECLIPSE DIGITAL

Levels	Rationale
SL2 Capability of the system of interest to protect against intentional violation using simple means with low resources, generic skills and low motivation.	Unauthorised access to users' personal data is prevented by the authorisation given by the project participants through the consent statement. According to this statement, the granted permissions can be revoked anytime during the project. Data aggregation and masking processes ensure that personal data is not shared with third parties and prevents participants' identification. The consent statement complies with the applicable legislation and is clear within the scope of data processing, nature of economic and non-economic benefits, participation requirements, partner entities and users' rights. Protection against falsification is also ensured through in-person/digital signatures along with validation of the identification of the participants.

ML2 Managed	In the scope of this project, there is documentation regarding the different control measures implemented but this documentation is not, at this point, repeatable.

SPR2

17 October 2025 E-Redes: Sita Carvalho and Ana Carolina.

Next evaluation of the KPIs (SL and ML): April – May 2026, before the analysis of the project results.

Responsible participants: Sita Carvalho and Ana Carolina (E-REDES).

3.5. PERSONALISED MESSAGES FOR CONSUMER FLEXIBILITY BASED ON NON-ECONOMIC INCENTIVES (HLUC2)

The use case analysis is divided into the cybersecurity analysis, the privacy analysis and the KPIs. The cybersecurity section analyses the threats, attack scenarios, and their links to conclude on the assessment of the risks. The privacy analysis defines the breaches and the threats, to evaluate the risk strategy and controls to be put in place. The KPIs section defines the KPIs that will be used to monitor the progress of security and cybersecurity.

3.5.1. CYBERSECURITY ANALYSIS

The cybersecurity analysis is identical for the HLUC 1 and HLUC 2. The results presented in section 3.4.1 are therefore relevant here.

3.5.2. PRIVACY ANALYSIS

The HLUC2 has a lot of similarities with HLUC1 and both architectures and data flows have most parts in common. This is the reason why the results are very similar, except for the non-economic incentives. The HLUC2 encompasses several use cases from personalized messages of non-economic incentives for benefits of the system, notification for sustainable energy decisions or environmental awareness or for sustainable consumer behaviour to flexibility participation of the consumers in system services producing energy savings. The main actors are the same as in HLUC1 except for the TSO that is not in the architecture scheme, but it is actor in some pilots.

From the analysis of the architecture and data flows, these are the PIIs identified:

- Energy consumption.
- Production data (for prosumers).
- Preferences on private and lifestyle.
- Information about savings (economic).

After the analysis of the HLUC2 architecture and data flow, these are the results: breaches, threats, impact and risk assessment and finally controls. Due to the similarity of both HLUCs (1 and 2) most of the breaches and threats are the same.

BREACHES

Table 17: Privacy breaches for the HLUC 2 of ECLIPSE DIGITAL

Breach	Description	Overall impact
B1 - Integrity of data	Integrity of data (bids) – access to data, it could be modified	LIMITED
B2 - Confidentiality users' data	Confidentiality of the personal data of users	SIGNIFICANT
B3 - GDPR users' rights violation	The rights defined in the law are not well addressed or respected by the data controller and processor	SIGNIFICANT
B4 - Flexibility data disclosed	Flexibility data disclosed without consent	LIMITED

The relation between the breaches and threats:

Table 18: Privacy threats for the HLUC 2 of ECLIPSE DIGITAL

Threat	Category	B1	B2	B3	B 4
1 Link the flexibility information to a user	Linking		X		
2 Detect the user through the personal data leak and anonymization failure	Detectability				X
3 Identification from a CPE to the user.	Identifiability		X		
4 Users claiming they did not provide consent.	Non-repudiation				X
5 Unauthorized access to users' personal data	Disclosure of Information	X			
6 Unawareness of Consent for external user comparison	Unawareness and intervenability			X	
7 Unawareness of Consent for energy data collection	Unawareness and intervenability			X	
8 Non-compliance with Regulation [Consent and privacy note] – wrong consent	Non-compliance			X	

The different breaches identified were assigned an impact and a likelihood level and this is risk assessment matrix outcome:

Figure 11: Privacy risk assessment for the HLUC 2 of ECLIPSE DIGITAL

The risk assessment matrix shows that breach 1 and 4 are in the green zone due to their impact and likelihood combination. For these reasons, the risk strategy is to assume those risks and no controls have been taken into account.

For the breach 2 and 3, both are in the purple zone, where the risk must be avoided or reduced. The following controls are considered to reduce the risk of these two breaches:

Table 19: Privacy controls for the HLUC 2 of ECLIPSE DIGITAL

Category	Subcategory	Control	Description	Threats
Asset management	Media handling	Data anonymization	Proper anonymization of customer data.	1, 3
Access control	User access management	Implementation of authentication measures	High level security implemented for user access (e.g. complex password, feedback for logins, etc).	5
Access control	User responsibilities	Consent management	Consent management measures to provide a clear and proper consent.	2, 4, 6, 7, 8
Communication security	Information transfer	Employ encryption protocols	Information transfer on a secure VPN network.	5
Compliance	Compliance with legal and contractual requirements	Appropriate GDPR requests	In depth development of GDPR legal requirements for each user.	6, 7, 8

3.5.3. KPIS

This section defines the KPIs that will be used to monitor the implementation of cybersecurity and privacy measures in the ECLIPSE DIGITAL project.

Table 20: Privacy and cybersecurity KPIs for the HLUC 2 of ECLIPSE DIGITAL

Levels	Rationale
SL1 Capability of the system of interest to protect against casual or coincidental violation.	Notifications are informative and cannot violate or intrude to other application in the environment of the end-user. Moreover, too frequent notifications may be cancelled by blocking or filtering according to rules which are also at the decision of the end user which receives such notifications. It should therefore consider a softer approach on the Security Level which will allow more flexibility while keeping low interactions with the server which sends the notifications.
ML2 Managed	As being a newly developed type of service, the emphasis is more on development of new features and adaptation through feedback of existing ones thus keeping a balance between documentation and development evolution.
SPR1 - 17.10.2025 UPB: Mihai Sanduleac, Ionut Damian	
Next date – March 2026 Responsible participants – Mihai Sanduleac, Ionut Damian	

3.6. PERSONALISED MESSAGES TO CONSUMERS ABOUT ENERGY EFFICIENCY POTENTIAL (HLUC3)

The use case analysis is divided into the cybersecurity analysis, the privacy analysis and the KPIs. The cybersecurity section analyses the threats, attack scenarios, and their links to conclude on the assessment of the risks. The privacy analysis defines the breaches and the threats, to evaluate the risk strategy and controls to be put in place. The KPIs section defines the KPIs that will be used to monitor the progress of security and cybersecurity.

3.6.1. CYBERSECURITY ANALYSIS

Threats

Table 21: Cybersecurity threats for the HLUC 3 of ECLIPSE DIGITAL

	Threat description	Overall impact
T_HLUC3_1	Bad/Falsified measurements from meters/HEMS propagate in prediction models leading to wrong predictions	Limited if not all measurements are falsified
T_HLUC3_2	Falsified messages coming from/to app	Negligible/Limited
T_HLUC3_3	Tampered energy market price causing wrong advice	Significant
T_HLUC3_4	Modification of prediction models	Significant

T_HLUC3_5	Leak of data related to consumer consumption patterns, personal details	Limited with negligible operational impact

Attack Scenarios

Table 22: Cybersecurity attack scenarios for the HLUC 3 of ECLIPSE DIGITAL

STRIDE Category	Scenario ID	Scenario Description
Spoofing	**S_HLUC3_1**	Impersonating a meter to send false measurements
	S_HLUC3_2	Impersonating Market operator to send false prices
	S_HLUC3_3	Impersonating energy app to send message
	S_HLUC3_4	Impersonating DERs to send wrong measurements
Tampering	**S_HLUC3_5**	Modifying message from a meter

	S_HLUC3_6	Modifying messages from the Market operator
	S_HLUC3_7	Modifying messages from the energy app
	S_HLUC3_8	Modifying message from a DER
	S_HLUC3_9	Modifying prediction model parameters
	S_HLUC3_10	Modifying consent information
	S_HLUC3_11	Modifying flexibility opt out parameters
Information Disclosure	**S_HLUC3_12**	Accessing historical data from consumers
	S_HLUC3_13	Accessing personal consumers details
Denial of Service	**S_HLUC3_14**	Overload digital services
	S_HLUC3_15	Prevent receiving price signal from Market operators

LINK Threat vs Attack Scenario

Table 23: Link between cybersecurity threats and attack scenarios for the HLUC 3 of ECLIPSE DIGITAL

	T_HLUC3_1	T_HLUC3_2	T_HLUC3_3	T_HLUC3_4	T_HLUC3_5
S_HLUC3_1	X				
S_HLUC3_2			X		
S_HLUC3_3		X			
S_HLUC3_4	X				
S_HLUC3_5	X				
S_HLUC3_6			X		
S_HLUC3_7		X			
S_HLUC3_8	X				
S_HLUC3_9				X	
S_HLUC3_10	X	X			
S_HLUC3_11	X	X			
S_HLUC3_12					X

S_HLUC3_13					X
S_HLUC3_14	X	X	X		
S_HLUC3_15			X		

Risk Assessment

Table 24: Cybersecurity risk assessment for the HLUC 3 of ECLIPSE DIGITAL

Threat	Impact	Likelihood	Overall Risk Assessment
T_HLUC3_1	Limited if not all measurements are falsified	Significant due to the diversity of DERs	**Must be reduced**
T_HLUC3_2	Negligible/Limited	Limited	**May be taken**
T_HLUC3_3	Significant	Limited	**Must be reduced**
T_HLUC3_4	Significant	Negligible/Limited	**May be taken**
T_HLUC3_5	Limited with negligible operational impact	Limited/Significant	**May be taken**

3.6.2. PRIVACY ANALYSIS

The HLUC3 is focused on efficiency and how the technology adoption can improve it. The use cases are in line with energy efficiency potential, notification of RES share, for consumer flexibility and sustainability but also tips for energy efficiency with PV panels and battery systems or prediction and consumption data notification. In this HLUC the main actor is the DSO and the consumers/prosumers. The DSO is the one that collects and process the data, which means that it is the data controller and processor. In this HLUC, there is an important capability, the pseudo anonymisation customer data that will be stored for years.

The analysis of the HLUC3 architecture and data flows, identified the main PIIs:

- Electricity consumption (heating/cooling devices)
- Energy production (PVs + Battery Home + EV charger)
- Metadata to characterise the customer (registration data provided from users).
- Other data:
  - Weather forecast
  - Network tariffs

From the analysis, these are the breaches considered:

Table 25: Privacy breaches for the HLUC 3 of ECLIPSE DIGITAL

Breach	Description	Impact
B1 - Personal data breach	Access to PIIs of users, so the data is compromised.	LIMITED

B2 - Illegitimate processing of personal data	Processing of personal data is not according to law and consent from users.	SIGNIFICANT
B3 - Violation of data subjects' rights	GDPR recognized users' rights are not well addressed by the Data Controllers and Processors.	SIGNIFICANT
B4 - Impossibility to use data (lack of quality data)	The data to be used has not enough quality	LIMITED
B5 - Anonymization process (for billing data storage 10 years) failed	The process of anonymization fails during these years.	SIGNIFICANT

The threats and breaches relation:

Table 26: Privacy threats for the HLUC 3 of ECLIPSE DIGITAL

Threat	Category	B1	B2	B3	B4	B5
1 Link to the user from the personal data leak and from failed anonymization process	Linkability	X	X	X		X
2 Identify the user from the personal data leak and from failed anonymization process	Identifiability	X		X		X

3 Users denying they have given consent	Non-repudiation		X	X		
4 Unauthorized information sharing and Access	Disclosure of information	X	X	X		X
5 Unclear the responsibilities for data processing	Unawareness and intervenability		X	X	X	
6 Unclear purposes of energy data collection	Unawareness and intervenability		X	X	X	
7 Implementation of the Consent process	Non-compliance		X	X		
8 Not enough ensured the process of Consent opt-out	Non-compliance		X	X		

The risk assessment matrix built from the breaches impact level and likelihood level assigned is the following:

Figure 12: Privacy risk assessment for the HLUC 3 of ECLIPSE DIGITAL

As it is depicted in the figure, there are different risks associated which required different risk strategies:

- Breach 1 risk is placed in the green area, so the risk strategy is to assume the risk identified with no additional controls.
- Breach 4 is placed in the yellow area, which requires to reduce the risk or even assume some part of the risk.
- Breach 2 and 3 are placed in the purple area, which requires a strategy with measures (controls) to reduce or avoid the risk.
- Breach 5, finally, is placed in the red area, which is really necessary and mandatory to transfer the risk to other areas with less risk level.

In summary, the controls implemented during HLUC3 are focused on reducing or avoiding breach 5, 2, 3 and reduce (if possible) breach 4, too.

CONTROLS

Table 27: Privacy controls for the HLUC 3 of ECLIPSE DIGITAL

Category	Subcategory	Control	Description	Threats
Asset management	Responsibility for assets	Structured identification of hardware assets involved in the pilot project	A structured listing of hardware assets involved in the use case, organized in a registry of "energy data sources"	1, 2, 4
Access control	User access management	User registration and authentication procedures	– Multi-Factor Authentication (MFA) – Secure login – Management of access rights – Session management and monitoring	1, 2, 4
Operation security	Protection from Malware	Malware protection is implemented through a defence-in-depth approach	– Container vulnerability scanning – Regular security updates – Network isolation – Access controls – Input validation – Intrusion prevention systems	1, 2, 4
Operation security	Backup	Regular backup and time synchronisation	– Regular backup of critical data, software and images. – Backup integrity is verified through automated restoration testing, and we maintain documented recovery procedures. All backup data is encrypted in transit and at rest.	1, 2, 4
Operation security	Logging and monitoring	Comprehensive event logging is enabled and logging services, recording all activities and providing an audit trail.	Logs are stored in object storage with versioning enabled and access controls preventing unauthorized modification. Administrative access is logged and monitored. Alerting is configured to notify administrators of critical events requiring action.	1, 2, 3, 4
Operation security	Controls of operational software	all operational software is managed through standardized processes		1, 2, 4

Communication security	Information transfer	AIIDA securisation data collection		1, 2, 3, 4, 5
Compliance	Compliance with legal and contractual requirements	AIIDA Consent management opt-out	comprehensive workflow to grant access to energy data with end user consent, specifying a duration of consent and revocation conditions.	3, 4, 5, 6, 7, 8

3.6.3. KPIS

This section defines the KPIs that will be used to monitor the implementation of cybersecurity and privacy measures in the ECLIPSE DIGITAL project.

Table 28: Privacy and cybersecurity KPIs for the HLUC 3 of ECLIPSE DIGITAL

Levels	Rationale
SL2: Capability of the system of interest to protect against intentional violation using simple means with low resources, generic skills and low motivation.	Taking the French pilot as representative of HLUC3, and considering Digital4Grids as a representative organization and technology provider contributing to the French pilot, the rationale of SL chosen is based on: • Baseline security & privacy services leveraged from infrastructure services related to its underlying cloud services, as well as custom services implemented such as registration and authentication, secure login, management of access rights, session monitoring, malware protection services… (non-exhaustive) • The latter being considered as a minimal capability of the system of interest to protect against intentional violation using simple means • Digital4Grids (as other French pilot contributors (DCBel, Voltalis)) categorize as SME-size company, providing the domain specific skills to protect against violation can be considered as generic, and motivation can be considered low to moderate

ML3 – Defined / Practices	Taking the French pilot as representative of HLUC3, and considering Digital4Grids as a representative organization and technology provider contributing to the French pilot, the rationale of ML chosen is based on: • Baseline security and privacy process documentation, such as the documented services provided by the EDDIE connector to data collection consent management and administration. This example process is designed to be harmonized across European environments and repeatable. • Concerning user data consent management, procedures and written and training exists to implement and use the service

SPR2 - 21.10.2025

Witold Krasny, D4G

3.7. ALERTS FOR EXTREME GRID SITUATIONS (HLUC4)

The use case analysis is divided into the cybersecurity analysis, the privacy analysis and the KPIs. The cybersecurity section analyses the threats, attack scenarios, and their links to conclude on the assessment of the risks. The privacy analysis defines the breaches and the threats, to evaluate the risk strategy and controls to be put in place. The KPIs section defines the KPIs that will be used to monitor the progress of security and cybersecurity.

3.7.1. CYBERSECURITY ANALYSIS

Threats

Table 29: Cybersecurity threats for the HLUC 4 of ECLIPSE DIGITAL

	Threat description	Overall impact
T_HLUC4_1	Incorrect message received by end users	Limited
T_HLUC4_2	Alert message not triggered or received	Limited

Attack Scenarios

Table 30: Cybersecurity attack scenarios for the HLUC 4 of ECLIPSE DIGITAL

STRIDE Category	Scenario ID	Scenario Description
Spoofing	**S_HLUC4_1**	Impersonating grid equipment to send false data
	S_HLUC4_2	Impersonating App to send false messages
Tampering	**S_HLUC4_3**	Modify message from App
	S_HLUC4_4	Modify message from grid equipment
Denial of Service	**S_HLUC4_5**	Prevent sending/receiving a message

LINK Threat vs Attack Scenario

Table 31: Link between cybersecurity threats and attack scenarios for the HLUC 4 of ECLIPSE DIGITAL

	T_HLUC1_1	T_HLUC1_2
S_HLUC4_1	X	
S_HLUC4_2	X	
S_HLUC4_3	X	
S_HLUC4_4	X	
S_HLUC4_5		X

Risk Assessment

Table 32: Cybersecurity risk assessment scenarios for the HLUC 4 of ECLIPSE DIGITAL

Threat	Impact	Likelihood	Overall Risk Assessment
T_HLUC4_1	Limited	Negligible	**May be taken**
T_HLUC4_2	Limited	Limited	**May be taken**

3.7.2. PRIVACY ANALYSIS

The HLUC4 is focused on grid data and use cases that do not use users' data. They do not collect specific personal or sensitive data from users. It uses a broadcast system to deliver the messages about relevant or catastrophic events.

Step 1 of the methodology (Context for the privacy analysis) was performed, and we concluded that there was not needed a Privacy Impact Assessment due to the lack of personal data collection and processing.

3.7.3. KPIS

This section defines the KPIs that will be used to monitor the implementation of cybersecurity and privacy measures in the ECLIPSE DIGITAL project.

Table 33: Cybersecurity and privacy KPIs scenarios for the HLUC 4 of ECLIPSE DIGITAL

Levels	Rationale
SL4: Capability of the system of interest to protect against intentional violation using sophisticated means with extended resources, domain specific skills and high motivation	Data messages concerning critical grid events are securely transmitted from the Dispatcher Management System (DMS) to the mobile application backend via a secured REST API. This API uses client credentials grant with tokens issued by our internal OAuth 2.0 / OpenID Connect (OIDC) identity provider, MEPAS, ensuring authenticated and authorized access. Notifications to mobile devices are delivered from mobile application backend using standard push notification services (e.g., Firebase Cloud Messaging), leveraging device tokens obtained from the mobile operating system during the user's sign-in process. The user authentication is handled via a secure authorization code flow through MEPAS, ensuring that device tokens are linked to authenticated sessions. All communication channels are encrypted using TLS, and token lifecycles are managed to minimize exposure and ensure secure access control.

ML3	Maturity level in case of HLUC 4 is set as defined and practiced in a way that the whole process is well described and repeatable in time. All messages from DMS are one-way, secured and encrypted, and the maturity of the documentation is quite high.

SPR4

3/11/2025

Martin Procházka, Jan Kůla, Anna Smičková

Next evaluation will be held after the full deployment of the app. (expected in 06/2026). Having a high level of security level at this moment, we do not expect any changes in the levels chosen

3.8. GENERAL ENERGY EFFICIENCY GUIDANCE (HLUC5)

The use case analysis is divided into the cybersecurity analysis, the privacy analysis and the KPIs. The cybersecurity section analyses the threats, attack scenarios, and their links to conclude on the assessment of the risks. The privacy analysis defines the breaches and the threats, to evaluate the risk strategy and controls to be put in place. The KPIs section defines the KPIs that will be used to monitor the progress of security and cybersecurity.

3.8.1. CYBERSECURITY ANALYSIS

Threats

Table 34: Cybersecurity threats for the HLUC 5 of ECLIPSE DIGITAL

	Threat description	Overall impact
T_HLUC5_1	Impersonated smart meter sends false energy data	Limited/Significant depending on scale
T_HLUC5_2	Malicious actor modifies historical data in transit in internal communication	Limited/Significant depending on scale
T_HLUC5_3	AIIDA interface flooded with data queries during peak load	Limited

T_HLUC5_4	IoT integration layer exploited to override home automation settings	Limited
T_HLUC5_5	Unintended access to admin features by frontend users	Significant
T_HLUC5_6	Aggregator injects biased flexibility signals to favour specific outcomes	Significant
T_HLUC5_7	Data breach exposing household-level consumption patterns	Significant

Attack Scenarios

Table 35: Cybersecurity attack scenarios for the HLUC 5 of ECLIPSE DIGITAL

STRIDE Category	Scenario ID	Scenario Description
Spoofing	**S_HLUC5_1**	Impersonated smart meter sends false energy data
Tampering	**S_HLUC5_2**	Malicious actor modifies historical data in transit

	S_HLUC5_3	Modify settings in the home automation system
	S_HLUC5_4	Aggregator injects biased flexibility signals to favour specific outcomes
Information Disclosure	**S_HLUC5_5**	Data breach exposing household-level consumption patterns
Denial of Service	**S_HLUC5_6**	AIIDA interface flooded with data queries during peak load
Elevation of Privileges	**S_HLUC5_7**	Unintended access to admin features by frontend users
	S_HLUC5_8	Flaw in the application (or its backend API) which exposes unauthorized settings

LINK Threat vs Attack Scenario

Table 36: Link between cybersecurity threats and attack scenarios for the HLUC 5 of ECLIPSE DIGITAL

	T_HLUC5_1	T_HLUC5_2	T_HLUC5_3	T_HLUC5_4	T_HLUC5_5	T_HLUC5_6	T_HLUC5_7

S_HLUC5_1	X						
S_HLUC5_2		X					
S_HLUC5_3				X			
S_HLUC5_4						X	
S_HLUC5_5							X
S_HLUC5_6			X				
S_HLUC5_7					X		
S_HLUC5_8				X			

Risk Assessment

Table 37: Cybersecurity risk assessment for the HLUC 5 of ECLIPSE DIGITAL

Threat	Impact	Likelihood	Overall Risk Assessment
T_HLUC5_1	Limited/Significant depending on scale	Limited	May be taken

T_HLUC5_2	Limited/Significant depending on scale	Limited	May be taken
T_HLUC5_3	Limited	Significant	Must be reduced
T_HLUC5_4	Limited	Limited	May be taken
T_HLUC5_5	Significant	Negligible	May be taken
T_HLUC5_6	Significant	Limited	Must be reduced
T_HLUC5_7	Significant	Limited	Must be reduced

3.8.2. PRIVACY ANALYSIS

The HLUC5 focuses on efficiency energy messages and the main actor is the DSO that collects data and process data, together with users or prosumers.

The use cases that the HLUC proposes go from general tips and guidance for energy efficiency to users' recommendations for energy management in residential buildings but also with the goal to educate in energy consumption habits for more energy efficiency.

The analysis of the HLUC architecture and data flows have identified the following PIIs:

- Historical validated Energy data (from the duration of the project).
- Near-real time energy data (from users' households).

The breaches identified are:

Table 38: Privacy breaches for the HLUC 5 of ECLIPSE DIGITAL

Breach	Description	Overall Impact
B1 - Violation of the data subject's rights	When the GDPR individuals' rights are not respected from the Data controller and processor.	SIGNIFICANT
B2 - Disclosure of PII from user's data	When the PIIs from the users is disclosed and the confidentiality of the data is compromised.	SIGNIFICANT
B3 - Illegitimate processing of personal data	If the data processing is not lawful and proportional according to GDPR statements.	LIMITED
B4 - Anonymization/ pseudo anonymization process failed	When the process to anonymised and minimized data is not well accomplished and finally, the data is not completely anonymised.	LIMITED-SIGNIFICANT

The threats and their relationship with the breaches:

Table 39: Privacy threats for the HLUC 5 of ECLIPSE DIGITAL

Threat	Category	B1	B2	B3	B4
1 Identification of a user from its energy consumption data.	Identifiability		X		X
2 Users denying they have given their consent.	Non-repudiation	X		X	

3 Disclosure of personal data from an unauthorized access.	Disclosure of information				X
4 Unawareness of the Consent requirements on purpose and processing.	Unawareness and intervenability	X		X	
5 Not enough clear purposes and processing in the Consent.	Non-compliance	X		X	

From the breaches' identification, the level of impact and likelihood chosen to provide the following risk assessment map:

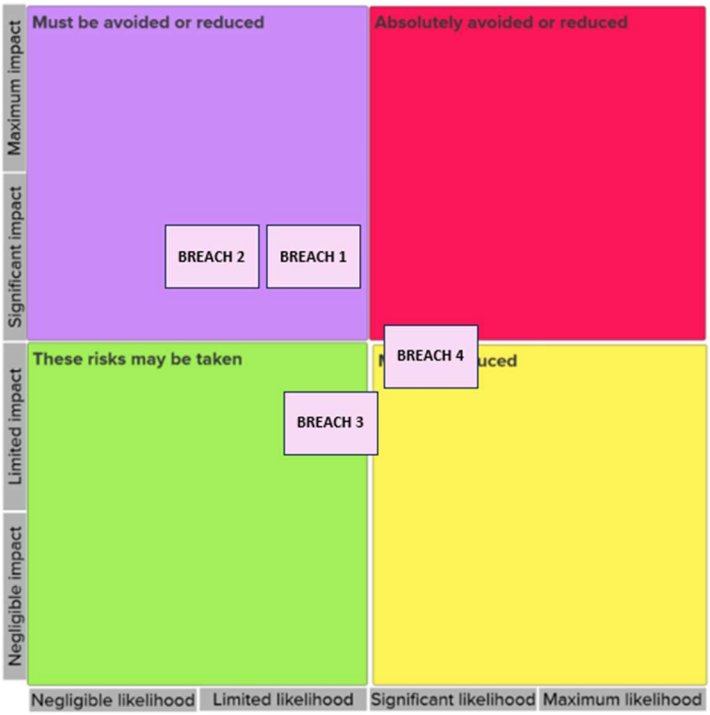


Figure 13: Privacy risk assessment for the HLUC 5 of ECLIPSE DIGITAL

From the risk assessment, the outcomes show:

- Breaches 1 and 2 are in the purple area, where the risk strategy is to avoid or reduce the risks.
- Breach 3 is in the green area where the risk is assumed, it is not needed to do anything else.
- Breach 4 is in the yellow zone mostly, so the strategy could be to assume or try to reduce the risk by implementing some controls.

In this case, the controls defined tackle the Breaches 1, 2 and 4.

CONTROLS

Table 40: Privacy controls the HLUC 5 of ECLIPSE DIGITAL

Category	Subcategory	Control	Description	Threats
Asset management	Information classification	Planned information classification guideline.	The guideline should distinguish between different classifications of data and user information and provide information on how each type of data should be secured.	1
Access control	Business requirements for access control	Private Git repository. Data access/sharing based on requests. Access control for HLUC5 at the database level currently not supported.	Currently, the project Git repository can be only accessed by the development team. Access requests are sent to users including which data requested by or shared with whom.	3, 4

			Permissions can be revoked by users or terminated by eligible parties. In the case of adding services requiring different privileges, access control at the level of tables, columns, etc. can be implemented.	
Access control	User responsibilities	Configuration for near real-time data services. Passwords in end customer application. User-centric authorization.	Users configure their own AIIDA instance for near real-time data. Users are responsible for safeguarding their authentication information. Users are involved in the authorization process to share their data or decide about access to requested data.	3
Access control	System and application access control	Password management in the end user application	In addition to password management in the end customer application, components used in ECLIPSE DIGITAL also	2, 3

			have their log on procedures (e.g., using Keycloak or through central authority).	
Cryptography	Cryptographic controls	Hash code for each user (planned). Apache Kafka and MQTT to secure communication.	Energy consumption data is not directly linked to users, but rather to unique hash code. Hence, the user cannot be identified from data and personal data will not be disclosed in case of unauthorized access. For communication, Apache Kafka and MQTT are used in HLUC5, which support encryption for data in transit (between clients and brokers) using TLS/SSL.	1, 2, 3
Operation security	Operational procedures and responsibilities	Segregation of duties in HLUC5	Separation of development, testing and operational environments. For example, developers do not have access to the live environment.	3

Operation security	Protection from Malware	Multi-Factor Authentication (MFA) planned.	In addition to regular updates and backup as well as practicing safe online habits, MFA can be enabled for extra layer of security.	3
Operation security	Logging and monitoring	Git development setting Keycloak Database	Git logs and Keycloak event logging are implemented in HLUC5. Concerning the database, logging every single access and command is supported.	2, 3
Operation security	Technical vulnerability management	Git - security checks in CI/CD pipelines.	Automated vulnerability scanning within CI/CD pipelines and GitHub workflows to detect and mitigate vulnerabilities during the development lifecycle.	2, 3
Communication security	Network Security management	Institutional control (FHOOE). Not applicable to HLUC5.	Since AIIDA takes care of problems related to impersonated smart meter, we consider this out of scope for HLUC5. However, this can be addressed by	2, 3, 4

			validating the received data (e.g., using validated historical data).	
System acquisition, development and maintenance	Security requirements of information systems	Securely develop, test and deploy HLUC5 planned.	We plan to implement different security guidelines for developers looking at aspects like input validation, secure usage of libraries, etc.	4, 5
System acquisition, development and maintenance	Security in development and support processes	Security in HLUC5 development, testing and deployment is currently not implemented – externally handled.	ECLIPSE DIGITAL uses different components which implement their own procedures and guidelines. For other development processes in ECLIPSE DIGITAL, we plan to implement secure development guidelines.	1
Compliance	Compliance with legal and contractual requirements	Institutional control (FHOOE).	FHOOE has an internal policy for complying with the Austrian laws and GDPR.	2, 4, 5

3.8.3. KPIS

This section defines the KPIs that will be used to monitor the implementation of cybersecurity and privacy measures in the ECLIPSE DIGITAL project.

Table 41: Cybersecurity and privacy KPIs for the HLUC 5 of ECLIPSE DIGITAL

Levels	Rationale
SL3 Capability of the system of interest to protect against intentional violation using sophisticated means with moderate resources, domain specific skills and moderate motivation	Unauthorized access to personal data is addressed by involving users in the authorization process to share their data or decide (accept/reject) about the permission to the requested data. The granted permissions can be revoked by users or terminated by eligible parties. Apache Kafka and MQTT are used in HLUC5 to secure communication, as encryption for data in transit (between clients and brokers) using TLS/SSL is supported. HLUC5 integrates Keycloak as a third-party identity and access management tool, which can be monitored through health status, API usage, and resource consumption. Segregation of duties is performed through separation of development, testing and operational environments. Since no third-party aggregators are involved in the scope of HLUC5, the threat due to aggregator injecting biased flexibility signals is not likely.

ML3 Defined/Practiced	– Upon reporting an incident or issue, a ticket of type bug is added to the HLUC5 internal repository backlog. Then, the ticket can be tracked by checking its status (e.g., in progress, review, etc.). After fixing the issue/bug and testing it, the ticket is marked as done and the fix is included in the next release. This process is consistently followed, even for documentation and enhancements.

SPR3

13.10.2025

FHOOE:

Aya Mohamed, CSO

We plan to perform the next evaluation of the KPIs upon having the prototype ready (Q1 2026), taking the current security and maturity levels into consideration. The responsible participant is the FHOOE team.

3.9. AI TRUSTWORTHINESS ANALYSIS RESULTS

3.9.1. INTRODUCTION

This activity was divided into 4 main steps:

1. Training and awareness: A session was held on the topics of trustworthiness, AI trustworthiness, associated regulation and standardisation, workshop preparation, and questionnaire preparation.

2. AI Impact assessment (for one AI system): This preparatory work takes the form of a guided questionnaire with the aim of:
    - provide initial analysis and basis for the workshop in the form of a high-level AI impact assessment,
    - allow the best possible workshop preparation for the participants by understanding the topics to be covered,
    - perform an impact assessment of their AI system guided by the predefined framework,
    - allow participants to find relevant information in advance, even if unknown to them, which is crucial for the workshop's success and
    - finally allow a more efficient workshop.

3. Workshop: This collaborative and guided workshop could be titled “AI system categorisation and risk/threats/controls analysis” and goes through the following steps:
    - review and validation of the AI system information based on the completed AI impact assessment.

- estimation, justification and agreement of the studied AI system risk category according to the AI Act.
- identification of the relevant risks or harms for the AI system studied.
- categorisation of identified risks by types of impact,
- For each identified risk:
    i. risk map completion considering likelihood and impact,
    ii. identification of threats or hazards that may lead to the risk,
    iii. identification of controls or mitigation manoeuvres possible to prevent, mitigate or avoid the risk
- identification of trustworthiness gaps.

4. Results summary report: This report summarises the activities performed, and results obtained.

The following elements are the main outputs of the AI trustworthiness-related activity:

- A recorded training session (to prepare the workshop) including a slide deck on the topic of AI trustworthiness (definitions, references, AI trustworthiness, AI regulation, AI Act, AI standardisation, AI Act harmonised standard, AI impact assessment methodology, AI trustworthiness analysis methodology, workshop preparation).
- One AI impact assessment by pilot on a selected AI system.
- One report by pilot summarising their workshop results and conclusion.

The AI Trustworthiness activity in the X-CPP used the following main references:

Table 42 Main references used for the ai trustworthiness analysis method

Reference	Description
ISO/IEC JTC 1/SC 42, - ISO/IEC 42005 Information technology – Artificial intelligence – AI system impact assessment [1], under development	This standard provides a methodology and a template for AI system impact assessment.
ISO/IEC JTC 1/SC 42 - ISO/IEC TR 24028 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence [2], 2020	This standard surveys: - approaches to establish trust in AI systems, - engineering pitfalls and associated threats and risks - approaches to assess trustworthiness characteristics
Cen-Cenelec JTC21 – AI Trustworthiness framework [3], under development	This standard provides the structure for AI trustworthiness analysis.
ISO/IEC JTC 1/SC 42 - ISO/IEC 23894 Information technology — Artificial intelligence — Guidance on risk management [23], 2023	This standard provides the methodology and structure for AI risk analysis.
THE ASSESSMENT LIST FOR TRUSTWORTHY ARTIFICIAL INTELLIGENCE (ALTAI) for self-assessment	This document presents a list of AI requirements to ensure Trustworthiness.
EU Grants. How to complete your ethics self-assessment	This document explains how to complete an Ethics Self-assessment and it tackles the AI topic in chapter 8.

Ethics By Design and Ethics of Use Approaches for Artificial Intelligence	This document explains how to create AI based solutions with Ethics by Design, including principles, requirements and practical steps.

The AI Trustworthiness activity is based on a multitude of standards and documents covering all AI Trustworthiness characteristics.

The AI Impact assessment was achieved following the structure of the table below:

Table 43: AI Trustworthiness questionnaire structure (based on ISO/IEC 42005)

Section	Sub-section	Key items
Plan and AI system characterisation	Plan information	• Generic information about the plan like version management, confidentiality and contacts
	AI system characterization	• ID information about the AI system like purpose, life cycle stage, objectives, context, infrastructure, location and accountability
Impact assessment	AI risk management	• Relevant interested parties • Uses information • AI risk management • Ethical, societal and environmental impact

	Data, algorithm and model information	• Data information and quality • Algorithms and models information and quality
	Regulatory and standards compliance	• Regulatory compliance • Standard alignment
	AI trustworthiness	• AI Cybersecurity (including logging functionalities) • AI privacy • AI robustness, resilience and accuracy • AI transparency (transparency, explainability, documentation) • AI management (governance, human oversight)
	AI trustworthiness assurance	• AI trustworthiness assurance expectations • AI trustworthiness process
Continuous improvement	Continuous improvement	• Continuous monitoring • Continuous maintenance • Continuous development
Other items	Other items and complementary information	• Open section for additional information

During the workshops, a collaborative online tool named Mural was used by all participants. Eight steps were followed throughout the session. The results were identified and approved during the session. They are summarised in this chapter.

Figure 14: Overview of the completed collaborative tool used for the workshop (MURAL)

3.9.2. AI TRUSTWORTHINESS ANALYSIS

For the AI trustworthiness analysis, 3 AI systems were selected based on resources for the task. Indeed, the French pilot was the only pilot with AI features that had resources in this task. The AI trustworthiness analysis reports for each pilot are available in annexes. This section presents some of the workshops' results.

3.9.2.1. CONSUMPTION AND PRODUCTION BASELINE CALCULATION - DIGITAL4GRIDS

The table below describes the AI system.

Table 44: AI system description

AI system name	Consumption/production baseline calculation
Life cycle stage	Design and development The data collection, as well as the exploration of the data analysis, has already started.
Organisation(s) in charge	Digital4Grids (French pilot)
Main objective	• This system calculates energy consumption forecasts for the coming 24 hours. • These forecasts are required to assess the "amount of flexibility" that a given device can offer at a given time.

AI system description	• Input: previous days' consumption values
	• Output: consumption forecast at a given time
	• Context:
	  ○ Energy - Flexibility domain
	  ○ Runs on-premise server, but in the future, it will be moved to the cloud
	  ○ Data located in the cloud
	  ○ To be used in the future on the EU market
	• AI system technical overview: As of now, the system is based on an X of Y principle. It calculates energy forecasts based on the consumption at the same time over the last few days.
	• Success criteria: quality of the forecast (can be measured through metrics like MAE and RMSE)

AI Act category estimation	High-risk • This AI system aims to operate in the energy domain and to provide automated inputs (forecast) to systems in charge of the management and operation of critical infrastructure and especially around flexibility. • Without controls, wrong predictions can have an impact on the grid, i.e., a critical infrastructure. • The trustworthiness of the critical infrastructure management system will have to trust or rely on this AI system.

AI act risk category requirements	High-risk category AI systems must respect AI trustworthiness principles. They are listed in the AI Act and detailed in the harmonised standard Cen-Cenelec AI Trustworthiness Framework. AI Act specifically mentions the following elements (non-exhaustive): • Risk management system (Article 9) • Data and data governance (Article 10) • Technical documentation (Article 11) • Record keeping (Article 12) • Transparency and provision of information to deployers (Article 13) • Human oversight (Article 14) • Cybersecurity (Article 15) • Accuracy (Article 15) • Robustness (Article 15) Additional requirements apply in Chapter 3 – Section 3. Here are some examples: • Quality management system (Article 17) • Documentation keeping (Article 18) • Keep automatically generated logs (Article 19) • Fundamental rights impact assessment Submission of a request of information upon the registration of high-risk AI systems. The list of requested documents is available in AI Act - Annexe 8 and 9.
Number of risks/harms identified (Feared events)	7

Number of threats/ hazards identified (for the risks)	38
Number of controls/ mitigation measures (for the risks)	33

Table 45: Categorisation of the identified risks by impact types

Impact type	Risk(s)
Security, Privacy and Safety	• Cybersecurity risks (e.g., Corrupted flex data transmission) • Incorrect prediction (e.g. due to bad quality data) that can lead to a harmful situation • Corrupted energy data transmission (i.e., data quality or cybersecurity attack) • Expose customer energy data / Personal data, or confidential data leakage
Operational and business	• Bad prediction (e.g. due to bad quality data) • No or reduced human control over AI Decisions
Ethical and societal	• Expose customer energy data / Personal data, or confidential data leakage • No or reduced human control over AI Decisions

3.9.2.2. SMART NOTIFICATIONS - VOLTALIS

The table below describes the AI system.

Table 46: AI system description

AI system name	Smart notifications
Life cycle stage	System inception (before design and development) • Data collection started? Yes • Exploratory data analysis? Yes
Organisation(s) in charge	Voltalis
Main objective	• The objective is to increase proactivity and offer a personalized service to users • Prediction of optimal notification sending times • Personalisation of optimisation advice based on consumption habits • Analysis of consumption patterns for preventive alerts • Adaptation of tone and frequency of notifications based on user engagement

AI system description	• Input:
	  ◦ Customer consumption habits/patterns collected by Voltalis assets
	  ◦ User preferences and interactions
	  ◦ Weather data
	• Output: Recommendations about relevant notification tone and frequency, optimisation advice, etc (see objectives section). This is to support Voltalis customer notification strategy and do automatic notifications.
	  ◦ Real-time consumption monitoring alerts
	  ◦ Programming reminders
	  ◦ Personalised optimisation advice
	  ◦ Important alerts
	• Context:
	  ◦ Energy - Flexibility domain
	  ◦ Runs on the cloud
	  ◦ The system depends on the MyVoltalis application and connected devices for data collection and the user interface
	  ◦ To be used in the future on the EU market
	• AI system technical overview:
	  ◦ AI type: Neural network
	  ◦ Algorithm type: Deep learning, decision trees
	• Success criteria:
	  ◦ Increase in heating savings

	○ Time spent on the application ○ Measurement of user engagement rate
AI Act category estimation	Limited risk • The AI system is a customer engagement and automatic notification tool operating in the energy domain without link to critical infrastructures. This AI system to support Voltalis customer notification strategy and do automatic notifications. AI system not used for functional or security purpose of the critical infrastructure (not a critical function). Not a system targeted by AI Act annexe III.
AI act risk category requirements	Limited risk category AI systems have to comply with transparency requirements listed in AI Act. • Clear disclosure to the user • AI content should be labelled (e.g. deepfake, automated notification) The goal of this transparency requirement is to balance innovation with user protection, ensuring people are not misled by AI while avoiding excessive regulation for lower-risk applications.
Number of risks/harms identified (Feared events)	7
Number of threats/hazards identified* (for the risks)	30

Number of controls/mitigation measures* (for the risks)	35

Table 47: Categorisation of the identified risks by impact types

Impact type	Risk(s)
Security, Privacy and safety	• Cybersecurity Risk • Personal data or confidential data leakage
Operational and business	• Lack of trust or explainability that leads to customer dissatisfaction • Incorrect recommendations /information /notification • Failure in edge/rare cases
Ethical and societal	• Personal data or confidential data leakage • Lack of trust or explainability that leads to customer dissatisfaction
Legal and regulatory	• Non-compliance with national or EU regulation (e.g., GDPR, AI Act, CRA) leads to lawsuits or penalties.
Environmental	• Environmental risks (e.g., electricity consumption, data storage)

3.9.2.3. TEMPERATURE MANAGEMENT- VOLTALIS

The table below describes the AI system.

Table 48: AI system description

AI system name	Temperature management
Life cycle stage	System inception (before design and development) • Data collection started? Yes • Exploratory data analysis? Yes
Organisation(s) in charge	Voltalis

Main objective **(long-term)**	• Improve user comfort while reducing energy consumption • Automatic management/adjustment of temperature • Suggestions of adjustments to balance comfort and energy savings • Learning users' thermal preferences • Automatic temperature optimisation based on multiple factors <u>Today's Voltalis vision</u>: • Today, the temperature is available in the MyVoltalis app but not prominently highlighted. With this redesign, Voltalis aims to make it a central element of the temperature control experience. • View of the home and its equipment directly from the main screen. • Ability to select predefined modes (e.g., comfort, eco, away, etc.). • Set the target (or setpoint) temperature with 0.5°C accuracy. • User can adjust the duration of an active command at any time. • Better detection of the radiator dial for manual adjustments.

AI system description	• Input: Customer thermal habits/patterns collected by Voltalis assets.
	• Output: Automatic management/adjustment of temperature.
	• Context:
	  ○ Energy – Smart appliance management for comfort thermal management
	  ○ Runs on the smartphone app
	  ○ To be used in the future on the EU market
	• Success criteria:
	  ○ User satisfaction with temperature control
	  ○ Energy savings achieved System reliability metrics
	  ○ User engagement rates
	  ○ Accuracy of temperature prediction

AI Act category estimation	Limited risk • The AI system is part of the energy ecosystem but is focused on thermal comfort management. • This AI system will be used in a first stage for residential buildings only (e.g., not hospitals, data centres, …). • There will be an automatic management of the residential building temperature. The AI system is not used for functional or security purposes of an energy-related critical infrastructure. It is not a system targeted by AI Act Annexe III, high-risk category.

AI act risk category requirements	Limited risk category AI systems have to comply with the transparency requirements listed in the AI Act. • Clear disclosure to the user • AI content should be labelled (e.g. deepfake, automated notification) The goal of these transparency requirements is to balance innovation with user protection, ensuring people are not misled by AI while avoiding excessive regulation for lower-risk applications.
Number of risks/harms identified (Feared events)	7
Number of threats/hazards identified* (for the risks)	41
Number of controls/mitigation measures* (for the risks)	38

Table 49: Categorisation of the identified risks by impact types

Impact type	Risk(s)
Security, Privacy and safety	• Cybersecurity Risk • Personal data or confidential data leakage • Incorrect output • Health and safety issue
Operational and business	• Incorrect output • Health and safety issue • Unexpected system behavior
Ethical and societal	• Health and safety issue • Personal data or confidential data leakage
Legal and regulatory	• Non-compliance with national or EU regulation (e.g., GDPR, AI Act, CRA) leads to lawsuits or penalties.
Environmental	• Environmental risks (e.g., energy consumption)

4. TRUSTWORTHINESS PROFILES

4.1. PROFILING METHODOLOGY

4.1.1. TRUSTWORTHINESS

4.1.1.1. INTRODUCTION

With the increase of functions of systems, their complexity also grows dramatically.

Such system may fail, cause harm, or expose Personal Identifiable Information (PII) (and worst, sensitive data) leading to serious consequences for individuals and undoubtedly a loss of confidence in the systems and/or organisations.

As a result, it is becoming vital as well as a challenge to build trustworthy systems.

> Trustworthiness is the "ability to meet stakeholders' expectations in a verifiable way" (*ISO/IEC TS 5723 - section 3.1.1* [39])
>
> Note: Depending on the context or sector, product or service, data, technology and process used, different characteristics apply and need verification to ensure stakeholders' expectations are met.
>
> Note: Trustworthiness is an attribute that can be applied to services, products, technology, data and information as well as to organizations.

There are two ways to look at trustworthiness:

1. contextualisation of high-level horizontal requirements in profiles that reference other standard documents which are the one assessed overall by the cross-cutting characteristics plan and

2. vertical trustworthiness profiles detailing for instance AI trustworthiness requirements throughout an AI system lifecycle which are the one assessed by the AI-Trustworthiness activity of the cross-cutting characteristics plan.

The cross-cutting characteristics plan provides a horizontal and vertical integration of the trustworthiness to address the challenge to build more trustworthy systems.

The list of trustworthiness cross-cutting characteristics can vary according to the level of expectation. For instance, Table 50 presents both a simple and an extended vision with additional characteristics.

Table 50: Example of different trustworthiness characteristics

Expectation Level	Trustworthiness cross-cutting characteristics
Simple vision	• Reliability • Resilience • Safety • Security • Privacy • Transparency

Extended vision	Simple vision characteristics: • Robustness • Availability • Integrity • Controllability • Quality • Authenticity • Usability • Accountability

Within ECLIPSE DIGITAL the trustworthiness characteristics to address constitute what the trustworthiness objectives to reach could be. A selection of these characteristics will be done to restrict the field of investigation for the project.

4.1.1.2. DEFINITION OF THE TRUSTWORTHINESS CHARACTERISTICS

IEC/ISO TS 5723 [39] defines the previously mentioned characteristics as follows:

- Accountability: "state of being accountable"
- Authenticity: "property that an entity is what it claims to be"
- Availability: "property of being accessible and usable on demand by an authorised entity"
- Controllability: "property of a system that a human or other external agent can intervene in the system's functioning"

- Information security: “preservation of confidentiality, integrity and availability of information”
- Security: “resistance to intentional, unauthorized act(s) designed to cause harm or damage to a system”
- Integrity: “<data> property whereby data have not been altered in an unauthorized manner since they were created, transmitted, or stored”
- Privacy: “freedom from intrusion into the private life or affairs of an individual”
- Quality: “<data> degree to which the characteristics of data satisfy stated and implied needs when used under specified conditions”
- Reliability: “<system> ability of an item to perform as required, without failure, for a given time interval, under given conditions”
- Resilience:
    - “<system> capability of a system to maintain its functions and structure in the face of internal and external change, and to degrade gracefully when this is necessary”
    - “<governance> ability to anticipate and adapt to, resist, or quickly recover from a potentially disruptive event, whether natural or man-made<governance> ability to anticipate and adapt to, resist, or quickly recover from a potentially disruptive event, whether natural or man-made”
- Robustness: “ability of a system to maintain its level of performance under a variety of circumstances”
- Safety: “property of a system such that it does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered”
- Transparency:

  - "<systems> property of a system or process to imply openness and accountability."
  - "<information> open, comprehensive, accessible, clear and understandable presentation of information"
- Usability: "extent to which a system product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use"

Each trustworthiness characteristic is covered by one or many standards and verification of trustworthiness can be achieved by an assurance plan.

4.1.1.3. MAIN TRUSTWORTHINESS STANDARDS

Published standards:

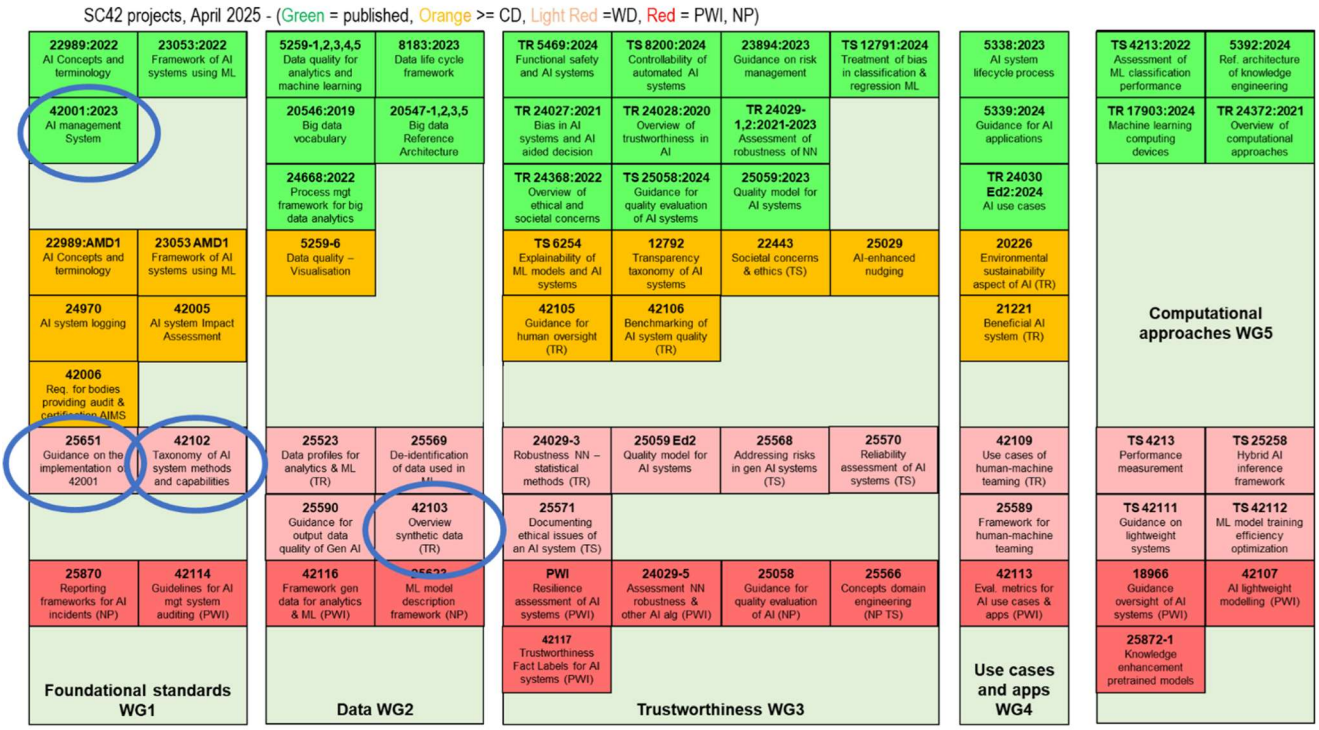
- ISO/IEC 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence
- ISO/IEC 30147:2021 Information technology — Internet of things — Methodology for trustworthiness of IoT system/service
- ISO/IEC TS 5723:2022 Trustworthiness — Vocabulary
- ISO/IEC TS 30149:2024 Internet of Things (IoT) — Trustworthiness principles
- ISO/IEC 30141:2024 IoT Internet of Things (IoT) — Reference architecture - Trustworthiness view
- ISO/IEC 24368:2022 Information technology — Artificial intelligence — Overview of ethical and societal concerns

Under development standards:

- ISO/IEC AWI 31303 Trustworthiness — Overview and concepts

- Cen-cenelec JTC21 AI Trustworthiness framework
- ISO/IEC JTC 1/SC 42 - ISO/IEC 42005 Information technology – Artificial intelligence – AI system impact assessment

It then relies on a wide range of standards to deep dive into each trustworthiness characteristic. For example, AI risk management is discussed in Trustworthiness standards and then relies partly on ISO/IEC 23894 information technology – Artificial intelligence – Guidance on risk management to go further. It shows how trustworthiness characteristics can be fragmented and consequently covered by many standards as depicted below.



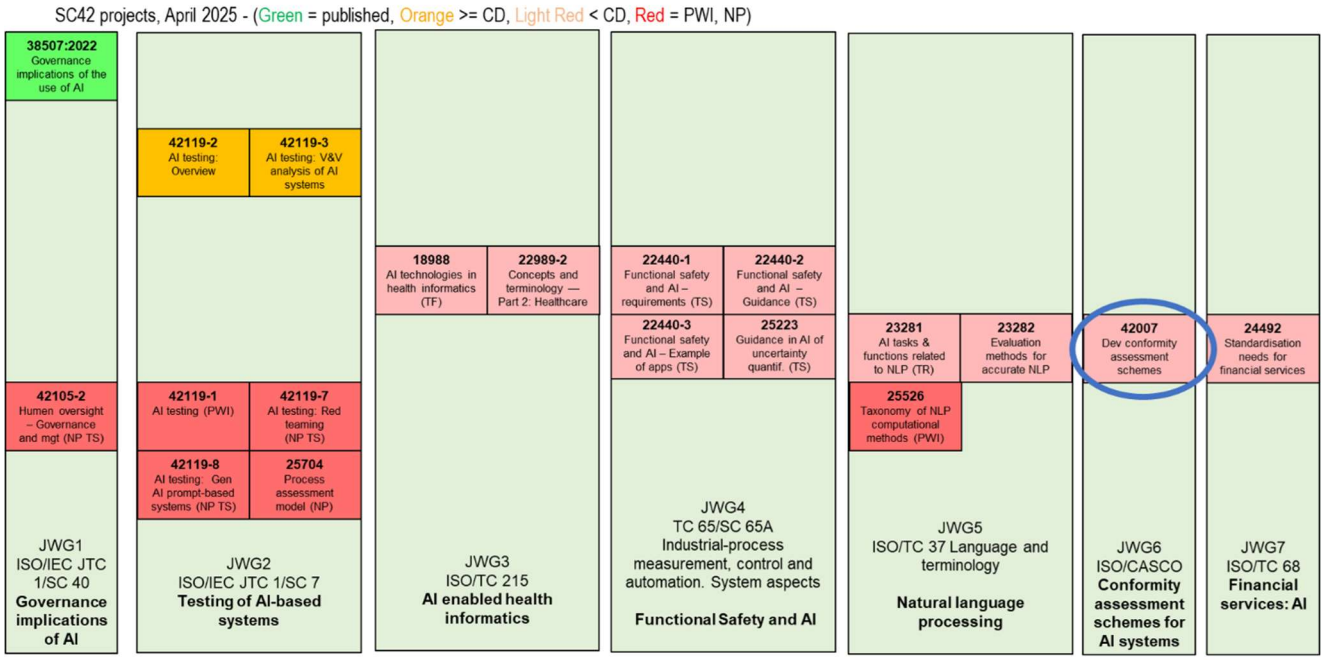


Figure 15: Standardisation perspective on AI

4.1.1.4. TRUSTWORTHINESS ASSURANCE

Trustworthiness assurance refers to the set of processes, practices, and measures designed to verify that a system is trustworthy. It aims to validation of the trustworthiness of a system.

The main challenge of trustworthiness assurance is: How to analyse the trustworthiness of a system during the design phase as well as after its realisation?

Assurance cases could be a solution.

From ISO/IEC/IEEE 15026-2 Systems and software engineering — Systems and software assurance [40] defines an assurance case as an "auditable artefact that provides a convincing and sound argument for a claim on the basis of tangible evidence under a given context" and an "assurance cases

are generally developed to support claims in areas such as safety, reliability, maintainability, human factors, operability, and security".

4.1.1.5. CONCEPTUAL MODEL FOR TRUSTWORTHINESS

The ISO/IEC TS 30149:2024 details a pathway from the selection of trustworthiness characteristics to address to the assurance requirements.

Once trustworthiness objectives have been defined, they can be used as the basis to validate the overall implementation of the system. There are several ways to accomplish this:

- apply a goal-orientation approach by designing capabilities,
- apply a risk-orientation approach through a risk analysis and the identification of measures and / or
- a combination of both.

The distinction between goal and risk is often of methodology or maturity origin:

- addressing a trustworthiness characteristic that is novel requires a risk-oriented approach, which involves the development of controls to treat identified risks and
- addressing a trustworthiness characteristic that has been treated in the past and is mature can sometimes involve a goal-oriented approach, which involves the development of capabilities to meet the goal.

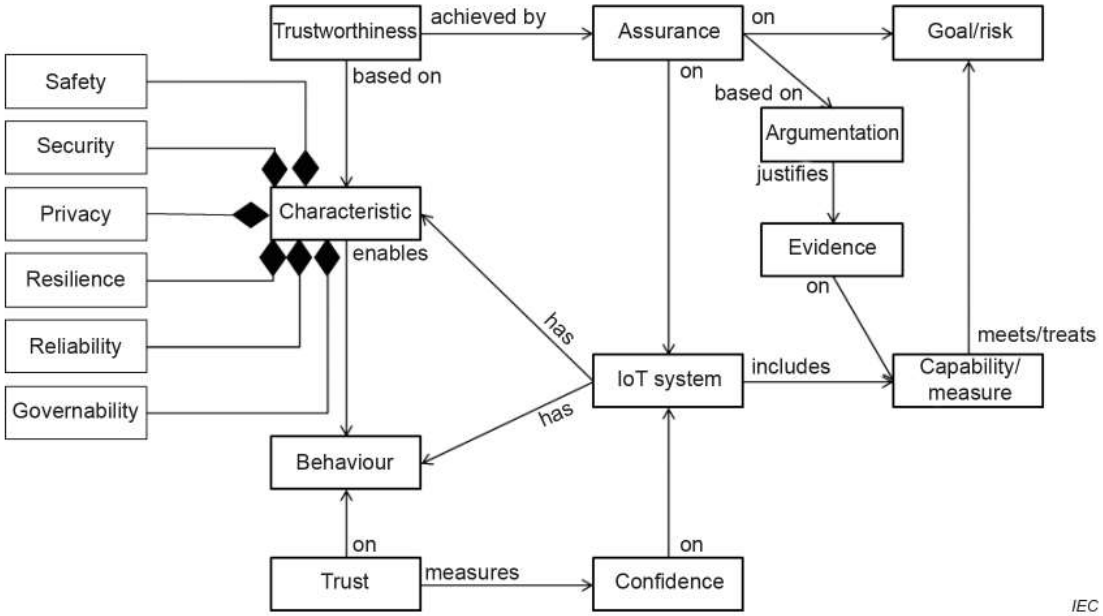


Figure 16: Conceptual model for trustworthiness

The conceptual model for trustworthiness depicted just above involves the following activities:

1. listing the characteristics and their dependencies,
2. identifying goals and related capabilities,
3. identifying risks and related treatments and
4. specifying assurance requirements in terms of claim, arguments and evidence.

4.1.2. PROFILES

4.1.2.1. DEFINITION

A profile is a standards writing concept defined in ISO/IEC TR 10000-1:1998.

In essence, a profile is a named set of requirements on an object of conformity assessment.

Profile definitions can be used to add structure to standards documents, making them easier to navigate, and also to create subsets or super-sets of the requirements in already-existing standards documents.

In other words, a profile is a viable list of requirements in a specific context.

ISO TR 10000-1 (Information technology — Framework and taxonomy of International Standardized Profiles - Part 1: General principles and documentation framework) provides guidance on profiles. The main concepts associated with the profile approach are as follow:

- Base standard: Refers to a standard that can be referenced in a profile.
- Profile: Set of base standards subsets, options, parameters.
- Taxonomy: Refers to a classification of profiles.

The construction of a profile follows a number of rules that are defined by the standardisation community. This consists of:

- a taxonomy of profiles,
    - Example: Level 1 lists verticals (e.g., health), level 2 lists a category of application in the domain
- a referencing scheme allowing profiles to point to specific text in base standards and
    - Example: Clause 5.1 of base standard A
- rules for the selection of the lists, subsets, options and parameters.
    - Example: Some base standards are mandatory
    - Example: Some base standards subsets are mandatory
    - Example: Some options are conditional

When defining the above rules, the following principles must be followed:

- a profile does not contradict requirements in base standards,

- a profile can contain conformance requirements which are more constraining and
- a profile can be the basis for the establishment of conformance test suites and testing methods.

4.1.2.2. APPLICATION TO ECLIPSE DIGITAL

The ECLIPSE-Digital profiles represent a consensus on the requirements that guide pilot implementations toward greater trustworthiness, effectively establishing a shared understanding of trust within the context of the project's use cases.

For ECLIPSE DIGITAL the profiles are sets of requirements to be defined for each cross-cutting characteristic and for each use-cases' context.

4.1.3. PROFILING PROCESS

The following diagram depicts the profile definition process with the final objective to initiate a Minimum Trustworthiness Mechanism Profiles repository in a post-ECLIPSE DIGITAL project activity guiding implementers on how to reach conformity and compliance to EU regulations. For now, ECLIPSE DIGITAL perimeter is highlighted with a red doted-line.

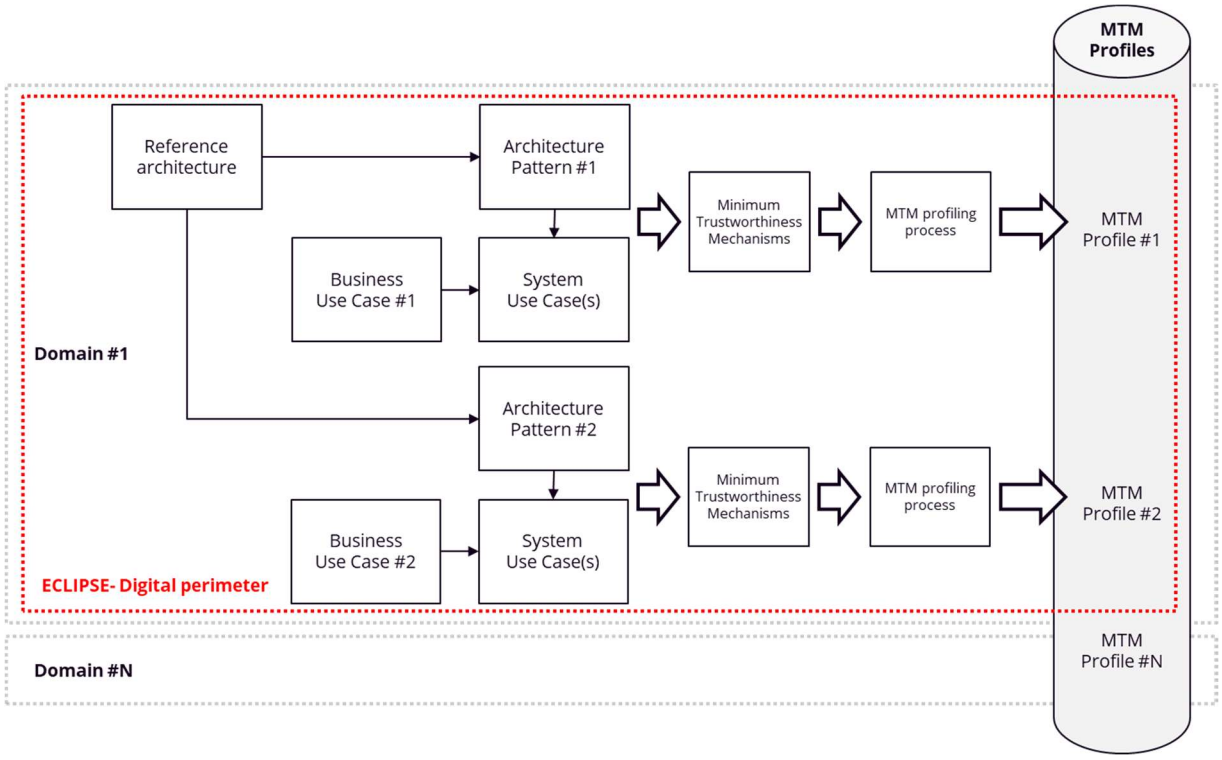


Figure 17: Profiling process

4.1.3.1. EXTRACTION OF MINIMUM TRUSTWORTHINESS MECHANISMS

From the goals and risks identified during the Trustworthiness characteristics analysis of the X-CCP, capabilities and measures have been defined constituting a set of Minimum Trustworthiness Mechanisms for ECLIPSE DIGITAL.

This minimum can be clustered in four categories to validate the implementations of the system:

- minimum capabilities to be implemented,
- minimum capabilities to be verified,
- minimum measures to be implemented and

- minimum measures to be verified.

In other words, a set of:

- Minimum Trustworthiness Mechanisms to be implemented and
- Minimum Trustworthiness Mechanisms to be verified.

The Minimum Trustworthiness Mechanisms extraction is illustrated in the following diagram:

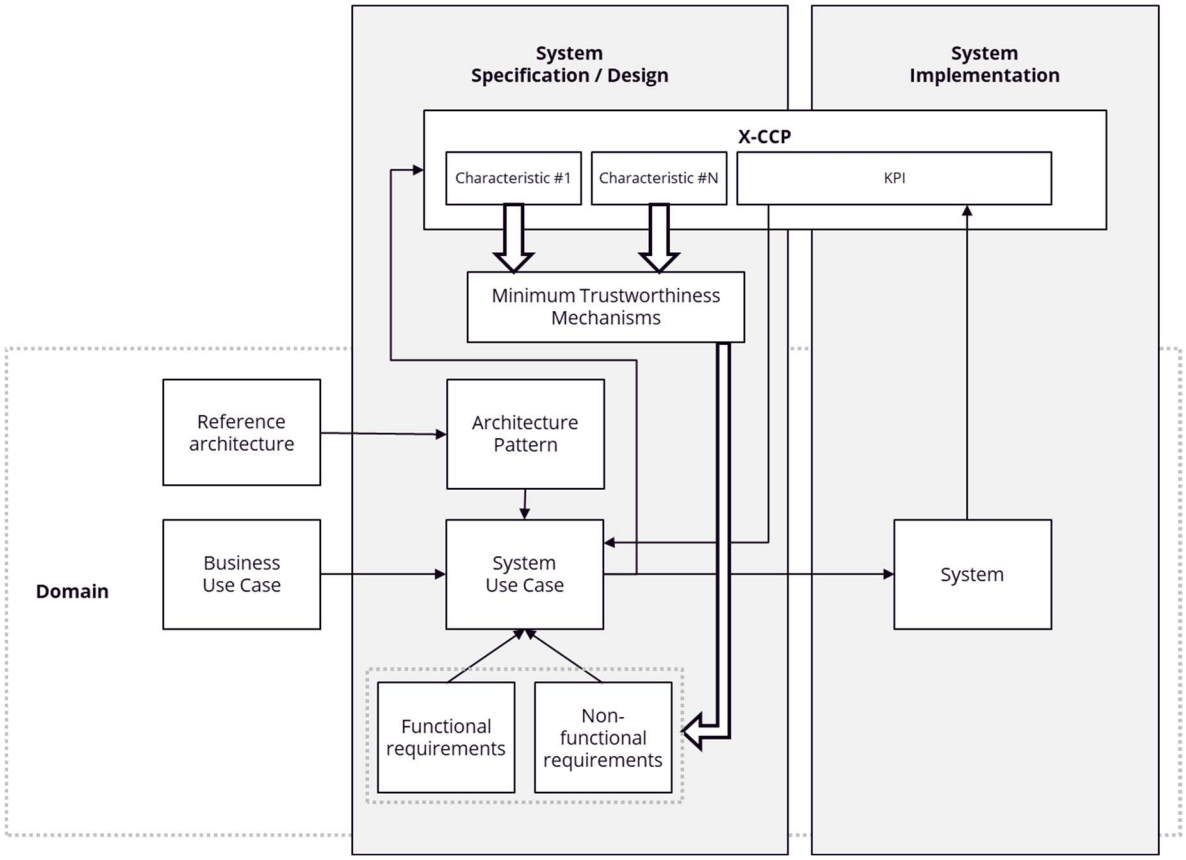


Figure 18: Minimum Trustworthiness Mechanisms extraction

Within the domain of ECLIPSE DIGITAL, use-cases have been implemented on patterns of architecture derived from the reference CERF architecture to answer to the stakeholders needs. Initial functional and non-functional requirements have been specified during the use-cases specification and design phase of the project.

Based on that the X-CCP process has been run through trustworthiness characteristics analysis to produce additional requirements, the trustworthiness mechanisms, to be integrated to the pilots' system implementations that will be finally monitored with KPIs.

4.1.3.2. CONSTRUCTION OF TRUSTWORTHINESS PROFILES

The trustworthiness profiles will be defined with mandatory fields of information within a specific context according to use-cases generalizable assumptions:

Table 51: Trustworthiness profiles fields

Field	Description
Context	The context is the one provided by the ECLIPSE DIGITAL project that is constituted by the reference architecture selected by the project on the one architecture patterns are identified to make the system use-cases alive based on the project high level use-cases.
Characteristic	Characteristics are the ones trustworthiness objectives have been identified. The identification of a Characteristic will be as follow: CH-CHn, CHn being the Characteristic_short_name.

Goal / Risk	The Goals / Risks are the ones identified during the X-CCP characteristics analysis to constitute the Minimum Trustworthiness Mechanisms. The identification of a Goal will be as follow: GL-GLn, GLn being the Goal_short_name. The identification of a Risk will be as follow: RK-RKn, RKn being the Risk_short_name.
Capability / Measure	The Capability / Measure are the ones selected / suggested to achieve the Goals or to reduce the Risks. The identification of a Capability will be as follow: CP-CPn, CPn being the Capability_short_name. The identification of a Measure will be as follow: MS-MSn, MSn being the Measure_short_name.
Requirement	Functional and non-functional requirements to achieve the Capabilities / Measures. Requirements include the "... shall ..." statement in the requirement sentence. The identification of a Requirement will be as follow: RQ-RQn, RQn being the Requirement_short_name.

Guidance	Recommendations on solutions to apply to bring to completion or reality the requirement. Requirements include the "… should …" statement in the recommendation sentence. A recommendations can also include justifications for applying or not previously defined requirements. The identification of a Recommendation will be as follow: RC-RCn, RCn being the Recommendation_short_name.
Description	A complete description of the recommendation including references to characteristics base standards and rules for the selection of the lists, subsets, options and parameters if needed.

Hence for reference, Capabilities and Measures identified during the X-CCP characteristics analysis will be summarized in a table for further usage within the requirements:

Table 52: Trustworthiness characteristics

Characteristic	Goal / Risk	Capability / Measure
CH-CH1	GL-GL1	CP-CP1 CP-CP2

	RK-RK1	MS-MS1
CH-Privacy	GL-Safety	CP-Protect_PII
…		

Requirements will use the following scheme with subsequent references to capabilities and / or measures using a full "path", e.g. for a capability CH-CH1.GL-GL1.CP-CP1, i.e. CH-Privacy.GL-Safety. CP-Protect_PII:

- RQ-RQ1
  - Description
    - … shall …
  - Reference to Capability / Measure
    - CH-CH1. GL-GL1.CP-CP1
    - CH-CH1. RK-RK1.MS-MS1
    - CH-CH1. RK-RK1.MS-MS2
    - …
  - Guidance
    - RC-RC1
      - Description
        - … should …
      - Example of evidence
        - …
      - Reference to base standard 1
        - …
        - Special application note
      - Reference to base standard 2
        - …

        - Special application note
            - …
    - RC-RC2
        - Description
            - …
    - …

Example of requirement:

- RQ-Governance_Scheme
    - Description
        - A governance scheme shall be established in systems including several organisations.
    - Reference to Capability / Measure
        - CH-Privacy.GL-Safety.CP-Protect_PII
    - Guidance
        - RC-Privacy_Plan
            - Description
                - A system privacy plan should be established.
            - Example of evidence
                - …
        - RC-Data_Management_Process
            - Description
                - A data management process should be established to ensure protection of PII.
            - Example of evidence
                - …
        - RC-Privacy_By_Design
            - Description

    - Engineering process to implement privacy-by-design should be established.
- Example of evidence
    - ...
- Reference to base standard
    - ...
- Special application note
    - ...

4.2. SELECTION OF TRUSTWORTHINESS OBJECTIVES FOR THE PROJECT

Within the ECLIPSE DIGITAL project the following characteristics as objectives for Trustworthiness have been selected and agreed:

- Governability,
- Privacy,
- Security and
- AI Trustworthiness.

These characteristics have been analysed for all the ECLIPSE DIGITAL use-cases and pilots and monitored with the X-CCP tool.

4.3. TAXONOMY FOR ECLIPSE DIGITAL PROFILES

This taxonomy provides a topic range of investigation to steer the Minimum Trustworthiness Mechanism Profiles definition for ECLIPSE DIGITAL. It includes the agreed trustworthiness objectives for the project.

Table 53: Taxonomy for the trustworthiness profiles

Category	Purpose	Taxonomy
Context identification	Identify components of the ecosystem including the system / complex-system itself and actors	• Business purposes • Actors including organisations • System / complex-system environment • Use-cases • Reference architecture • Targeted architecture pattern
System / complex-system lifecycle	List system / complex-system life-cycle phases	• System / complex-system specification • System / complex-system design • System / complex-system implementation • System / complex-system deployment • System / complex-system operation in real environment • System / complex-system retirement

Governability objective	Identify and define governance goals	• Ensure Trustworthiness Assurance of the system / complex-system
Privacy threats	Reference threats / risks to be considered in the privacy characteristic analysis	• Linking • Identifying • Non-repudiation • Detecting • Data disclosure • Unawareness & intervenability • Non-compliance
Security threats	Reference threats / risks to be considered in the security characteristic analysis	• Spoofing • Tampering • Repudiation • Information disclosure • Denial of service • Elevation of privilege
AI-Trustworthiness threats / hazards	Reference threats / hazards to be considered in the AI-Safety characteristic analysis	• Accountability • Bias • Explainability • Predictability • Resilience • Safety • Transparency

4.4. REQUIREMENTS' CLASSIFICATION

The statement of the requirements for a characteristic shall define the assurance requirements that the system needs to satisfy in order to meet the objectives for the system for this characteristic.

Assurance requirements are classified by characteristic:

- Governability,
- Privacy,
- Security,
- AI Trustworthiness

and classified by type:

- assurance requirements to be implemented and
- assurance requirements to be verified.

Assurance requirements in a context of a use-case will form a profile.

4.5. MINIMUM TRUSTWORTHINESS MECHANISM PROFILES FOR ECLIPSE DIGITAL

4.5.1. COMMON TRUSTWORTHINESS MECHANISM PROFILES TO ALL USE-CASES

4.5.1.1. CAPABILITIES / MEASURES REFERENCES

The following table content provides references to the Capabilities / Measures identified during the X-CCP analysis.

Table 54: Characteristics for the common trustworthiness mechanism profiles to all use-cases

Characteristic	Goal / Risk	Capability / Measure
CH-Governability	GL-Ensure_Trustworthiness_Governance	CP-Define_Trustworthiness_Governance

CH_Privacy	GL-GL1 Avoid unauthorized access to PIIs GL-GL2 Ensure confidentiality of Data GL-GL3 Avoid identification of users from CPE, energy consumption data GL-GL4 Ensure unlinking personal information (flexibility data) to a user GL-GL5 Ensure anonymization process for long data storage. GL-GL6 Keep data integrity (savings and bids) GL-GL7 Ensure regulation conformity (GDPR Users' Rights and data processing)	CP-CP1 Information access management. CP-CP2 Security in information transfer. CP-CP3 Data Protection compliance CP-CP4 Consent management process. CP-CP5 Data anonymization process.
CH_Security	N/A Note: Check "Trustworthiness mechanism profiles by use-case" section	N/A Note: Check "Trustworthiness mechanism profiles by use-case" section

CH_AI-Trustworthiness	GL-Ensure_AI_Trustworthiness	CP-AI_Act_alignement_High_Risk_category
		CP-AI_Act_alignement_Limited_Risk_category

4.5.1.2. GOVERNABILITY PROFILE

4.5.1.2.1. ASSURANCE REQUIREMENTS TO BE IMPLEMENTED

This section defines the assurance requirements to be implemented across the ECLIPSE DIGITAL project in order to comply to the common trustworthiness profile. For each requirement, relevant standards are listed with notes on the specific implementation details.

Table 55: Overview of Governability requirements and recommendations

Requirement	Recommendation
RQ-Define_and_institute_a_Trustworthiness_Governance	RC-Identify_entitled_participants_to_define_governance_structure
	RC-Define_governance_structure
	RC-Define_legal_ethical_and_compliance_framework

	RC-Define_governance_operations
	RC-Review_and_approve_governance_document

RQ-Define_and_institute_a_Trustworthiness_Governance

- Description
  - A Trustworthiness Governance shall be defined and instituted to ensure a proper steering of the Trustworthiness Assurance Plan of the system over its entire lifecycle. A governance structure, a framework and operations shall be defined and approved.
- Reference to Capability / Measure
  - CP-Define_Trustworthiness_Governance.
- Guidance
  - **RC-Identify_entitled_participants_to_define_governance_structure**
    - Description
      - Entitled participants should be identified for the governance structure definition of the Trustworthiness Assurance Plan to ensure that persons with right responsibilities agree on the governance structure in the ecosystem. A governance structure should be specific to a pilot.
      - Entitled actors should be the Trustworthiness Assurance Plan owner, the system owners, Data Protection Officers and Chief Security Officers.
    - Example of evidence

- Trustworthiness Assurance Plan owner: The pilot leader
- System owner: A partner operating the pilot.
- Data Protection Officer: A person from partners operating the pilot with a DPO role.
- Chief Security Officer: A person from partners operating the pilot with a CSO role.

- Reference to base standard
  - The following standards and methods may be used:
    - ISO/IEC 30145 series (Smart cities ICT reference framework) is used as an overall framework which provides a methodology for implementing and maintaining trustworthiness.
- Special application note
  - In particular "Technical management processes" recommend forming a trustworthiness team that should consist of multiple members with specific expertise related to trustworthiness characteristics but shall contain the chief responsible for the trustworthiness of the system.

- **RC-Define_governance_structure**
  - Description
    - A governance structure should be defined for the Trustworthiness Assurance Plan of a pilot. The structure should be made of a governance leadership (could be an agency, an organisation, an alliance…), involved organizations / relationships with other Trustworthiness Assurance Plan and resources for governance (could be persons, funds…).
  - Example of evidence

- Governance leadership: The pilot leader
- Involved organisations / relationships with other Trustworthiness Assurance Plan: The overall Trustworthiness Assurance Plan of the pilot associated. with partners specific Trustworthiness Assurance Plan
- Resources for governance: DPO and CSO of a partner that will provide support (e.g., legal) to the governance leadership.

- Reference to base standard
  - The following standards and methods may be used:
    - ISO/IEC 38500:2015 (Information technology — Governance of IT for the organization) is used by the governing body to govern the use of IT through three tasks: evaluate, direct and monitor.
    - ISO/IEC TS 38501 (Governance of IT – implementation guide) is used to support the implementation of the governance process, through a cycle of three activities: establish and sustain enabling environment, govern IT and continual review.
    - ISO/IEC TR 38502 (Governance of IT – Framework and model) is used to build a governance framework. It includes the following: principles for good governance, strategies and policies for the use of IT, business planning for IT, management systems for IT, the organization's use of IT, accountabilities and risk management.
- Special application note

- In particular ISO/IEC 38500:2015 provides recommendations on the governance structure and points out to source standards:
  - §5.7 - Stakeholder engagement - "The governing body should ensure that the organization's stakeholders are appropriately engaged, and their expectations considered.": ISO 37000:2021, 6.6.1.
  - §5.8 – Leadership - "The governing body should lead the organization ethically and effectively and ensure such leadership throughout the organization.": ISO 37000:2021, 6.7.1.

- **RC-Define_legal_ethical_and_compliance_framework**
  - Description
    - Legal, ethical and compliance policies should be defined including a data protection framework and officers, a security framework and officers, a citizen engagement framework and representatives and an incident management scheme.
  - Example of evidence
    - Data protection and sharing measures are defined and in place, monitored by a DPO and compliant with the GDPR.
    - Data security measures are defined and in place and monitored by a CSO.
    - Acting in a socially responsible way such as:
      - Ensure that the expectations of stakeholders are clearly understood.
      - Ensure that issues and opportunities affecting stakeholder expectations are identified.

        - Engage with all relevant stakeholders when establishing and reviewing governance policies.
        - Steer the Trustworthiness Plan such that its decision-making and activities are consistent with the organizational purpose, organizational values and governance policies.
    - An incident categorisation and actions are defined.
    - Evidence that the incident handling policy is in place and communicated to stakeholders.
    - Procedures for how to communicate any incident to relevant upper governance are defined.
- Reference to base standard
    - The following standards and methods may be used:
        - The data protection framework, and officers: GDPR, ISO 27701, ISO 31700.
        - The security framework, and officers: ISO 27001.
        - The citizen engagement framework, and representatives: ISO 27570.
        - Social responsibility: ISO/IEC 37000:2021.
        - The incident management scheme: The ISO/IEC 27035 series provide further guidance on incident management, check ISO/IEC 27035-1:2023 Information technology – Information security incident management – Part 1: Principles and process.
- Special application note
    - N/A

- **RC-Define_governance_operations**
    - Description

- Governance operations should be defined to be followed when the Trustworthiness Assurance Plan of a pilot will be in operation. Operations could be:
  - Collaboration agreement.
  - Officer nomination process.
  - Meeting organisation process.
  - Meeting reporting process.
  - Expected / consensual trustworthiness.
  - Publication process.
  - Trustworthiness Assurance Plan lifecycle process (continuous improvement).
  - Risk management process.

- Example of evidence
  - Collaboration agreement: Statement of an agreement signed by organisations involved in the pilot.
  - Officer nomination process: Approach to nominate responsible persons member of trustworthiness characteristics governance committee.
  - Meeting organisation process: One meeting every quarter to evaluate, direct and monitor the Trustworthiness Assurance Plan.
  - Meeting reporting process: Minutes template to be used
  - Agreement on the characteristics that should be part of the plan to ensure the expected / consensual Trustworthiness.
  - Publication process: Approval of trustworthiness characteristics governance committee, and publication within the pilot.

- Trustworthiness Assurance lifecycle process (continuous improvement): At the agenda every 6 months.
- Risk management process: How the management of risk is to be approached, ensure that when the governing body makes decisions, it assesses, treats, monitors, and communicates the nature and extent of the risks faced and oversee the organization's risk management activities.

- Reference to base standard
  - The following standards and methods may be used:
    - The implementation of the governance of the Trustworthiness Assurance Plan should be based on a cyclic approach considering the model presented in ISO/IEC 38500, see *Figure 19* depicted in the following application note. The first cycle of activities involves the establishment of the initial "implementation" or baseline, with subsequent cycles of the activities being used to support and enhance the governance of the Trustworthiness Assurance Plan implementation by means of continual improvement. The duration of cycles will be different for each organization, depending on a number of factors including the organization's size, its industry, as well as the maturity of the governance of the Trustworthiness Assurance Plan in the organization.
    - The implementation cycle comprises the following main activities which are expanded in the clauses below:

- Establish and sustain enabling environment: Starting by defining goals and strategies to steer the Trustworthiness Assurance Plan followed by establishing an enabling environment which ensures that all stakeholders are appropriately identified and made aware of their roles and responsibilities. Subsequent cycles will ensure that the enabling environment is sustained.
- Govern the Trustworthiness Assurance Plan: Progress to the evaluate, direct, and monitor activities to perform the governance of the Trustworthiness Assurance Plan.
- Continual review: Review the governance of the Trustworthiness Assurance Plan arrangements to determine whether desired outcomes are being achieved. If not, recommence the implementation cycle to effect the necessary changes, thereby ensuring continual improvement of the governance of the Trustworthiness Assurance Plan implementation.

- Special application note

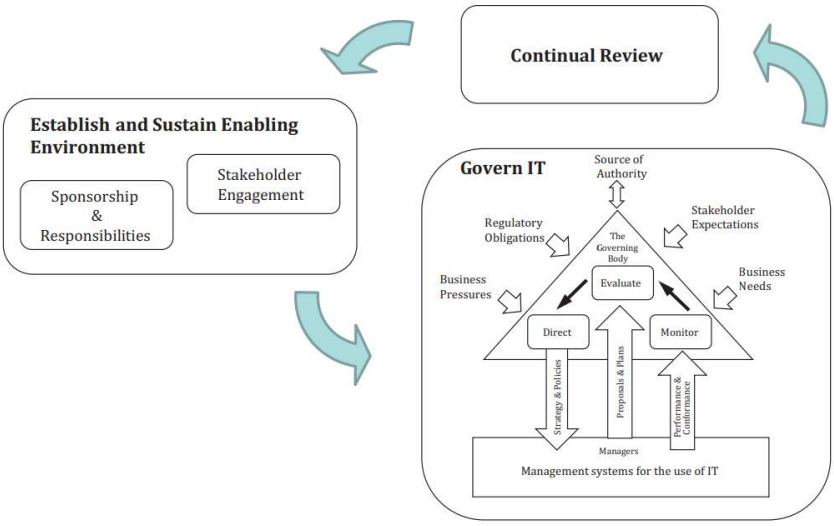


Figure 19: Trustworthiness Assurance Plan implementation approach (the "IT" as depicted) (incorporates ISO/IEC 38500)

- **RC-Review_and_approve_governance_document**
  - Description
    - The governance document should be reviewed and approved by the Trustworthiness Assurance Plan stakeholders to ensure the governance is established and actionable.
  - Example of evidence
    - The review should address the following recommendations:
      - RC-Identify_entitled_participants_to_define_governance_structure.
      - RC-Define_governance_structure.
      - RC-Define_legal_ethical_and_compliance_framework
      - RC-Define_governance_operations.

        - Approvals of the Trustworthiness Assurance Plan by the stakeholders.
    - The governance document should be checked and signed by all Trustworthiness Assurance Plan stakeholders.
- Reference to base standard
    - The following standards and methods may be used:
        - Establish governance policies: ISO 37000:2021
- Special application note
    - N/A

4.5.1.3. AI TRUSTWORTHINESS PROFILE

4.5.1.3.1. ASSURANCE REQUIREMENTS TO BE IMPLEMENTED

This section defines the assurance requirements for AI trustworthiness to be implemented across the ECLIPSE DIGITAL project in order to comply to the common trustworthiness profile. For each requirement, relevant standards for the implementation are listed.

Table 56: Overview of AI trustworthiness requirements and recommendations

Requirement	Recommendation
RQ-Align_with_AI_System_	RC-Clear, sufficient and regular impact assessment

with_obligations_of_IA_Act_High-Risk_Category	RC-Clear, sufficient and regular risk management
	RC-Clear, sufficient and regular quality management
	RC-Application of an AI system life cycle model
	RC-Clear, sufficient and regular fundamental rights impact assessment
	RC-Compliance with the regulatory framework
	RC-EU High-risk AI system registration and requirements
	RC-Clear governance and accountability (system and data)
	RC-Sufficient cybersecurity level
	RC-Sufficient privacy and data protection level
	RC-Clear and operational human oversight; sufficient controllability
	RC-Sufficient AI logging (automatic) and record keeping capabilities

	RC-Clear technical documentation and documentation keeping capability
	RC-Sufficient robustness and resilience
	RC-Sufficient safety
	RC-Sufficient accuracy and reliability
	RC-Sufficient transparency
	RC-Sufficient explainability
	RC-Sufficient data/algorithm quality and suitability
RQ-Align_with_AI_System_with_obligations_of_IA_Act_Limited_Risk_Category	RC-Sufficient transparency
	RC-Compliance with the regulatory framework

RQ-Align_with_AI_System_with_obligations_of_IA_Act_High-Risk_Category

- Description

- AI systems identified as high-risk following the AI Act requirements will have to comply with a trustworthy AI framework.

- Reference to Capability / Measure
  - CP-AI_Act_alignement_High_Risk_category.
- Guidance
  - **RC-Clear, sufficient and regular impact assessment**
    - Description
      - A clear, sufficient and regular impact assessment shall be defined and executed.
    - Example of evidence
      - Impact assessment document (could be by system or by version).
    - Reference to base standard
      - The following standards and methods may be used:
        - ISO/IEC JTC 1/SC42, ISO/IEC 42005 Information technology – Artificial intelligence – AI system impact assessment [12].
  - **RC-Clear, sufficient and regular risk management**
    - Description
      - A clear, sufficient and regular risk management shall be defined and executed.
    - Example of evidence
      - Risk management plan.
      - Risk management implementation monitoring document.
    - Reference to base standard
      - The following standards and methods may be used:

        - ISO/IEC JTC1/SC42 23894 Information technology — Artificial intelligence — Guidance on risk management [23].
        - ISO/IEC JTC1/SC42 42001 Information technology — Artificial intelligence — Management system [33].
- **RC-Clear, sufficient and regular quality management**
    - Description
        - A clear, sufficient and regular quality management shall be defined and executed.
    - Example of evidence
        - Quality process plan.
        - Quality process implementation monitoring.
    - Reference to base standard
        - The following standards and methods may be used:
            - ISO/IEC JTC1/SC42 25058 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guidance for quality evaluation of artificial intelligence (AI) systems [41].
            - ISO/IEC JTC1/SC42 42106 Information technology — Artificial intelligence — Overview of differentiated benchmarking of AI system quality characteristics [42].
            - ISO/IEC JTC1/SC42 5259-6 Artificial intelligence — Data quality for analytics and machine learning (ML) Part 6: Visualization framework for data quality [43].
- **RC-Application of an AI system life cycle process**
    - Description

- A sufficient AI system life cycle process shall be defined and executed.

- Example of evidence
  - Description of life cycle model use in implementation.
- Reference to base standard
  - The following standards and methods may be used:
    - ISO/IEC JTC 1/SC42 5338 information technology — Artificial intelligence — AI system life cycle processes [44].

- **RC-Clear, sufficient and regular fundamental rights impact assessment**
  - Description
    - A clear, sufficient and regular fundamental rights impact assessment shall be performed.
  - Example of evidence
    - Fundamental rights impact assessment (section of Impact assessment document).
  - Reference to base standard
    - The following standards and methods may be used:
      - ISO/IEC JTC1/SC42 42001 Information technology — Artificial intelligence — Management system [33].
      - ISO/IEC JTC1/SC42 24368 Information technology — Artificial intelligence — Overview of ethical and societal concerns [45].
      - ISO/IEC JTC1/SC42 22443 Information technology — Artificial intelligence — Guidance on addressing societal concerns and ethical considerations [46].
- **RC-Compliance with the regulatory framework**
  - Description

    - Compliance with the regulatory framework shall be ensured.
  - Example of evidence
    - Existence of this need in the company policy document
  - References
    - The following references may be used:
      - AI Act [18].
      - Cyber Resilience Act (CRA) [20].
      - Cybersecurity Act [47].
      - GDPR [21].
      - Data Governance Act [47].
      - ISO/IEC JTC 1/SC 42 42007 Information technology — Artificial intelligence — High-level framework and guidance for the development of conformity assessment schemes for AI systems [48].
- **RC-EU High-risk AI system registration and requirements**
  - Description
    - Every AI system categorised as high-risk should be registered on the European platform.
  - Example of evidence
    - Registration confirmation document.
  - Reference to base standard
    - The following standards and methods may be used:
      - Cen-Cenelec JTC 21 AI Trustworthiness framework [14].
- **RC-Clear governance and accountability (system and data)**
  - Description

        - A clear governance and accountability shall be defined for the AI system and the associated data (training, input and output).
    - Example of evidence
        - Organisation responsibility and role (in the company policy document).
    - Reference to base standard
        - The following standards and methods may be used:
            - ISO/IEC JTC1/SC42 42001 Information technology — Artificial intelligence — Management system [33].
- **RC-Sufficient cybersecurity level**
    - Description
        - A sufficient cybersecurity level shall be ensured.
    - Example of evidence
        - Impact assessment document (could be by system or by version).
    - Reference to base standard
        - The following standards and methods may be used:
            - ISO/IEC JTC1/SC27 27090 Cybersecurity — Artificial Intelligence — Guidance for addressing security threats to artificial intelligence systems [49].
            - ENISA Cybersecurity of AI and Standardisation [50].
- **RC-Sufficient privacy and data protection level**
    - Description
        - A sufficient privacy and data protection levels shall be ensured.
    - Example of evidence
        - Impact assessment document (could be by system or by version).

- Reference to base standard
  - The following standards and methods may be used:
    - ISO/IEC JTC1/SC27 27091 Cybersecurity and Privacy — Artificial Intelligence — Privacy protection [51].

- **RC-Clear and operational human oversight; sufficient controllability**
  - Description
    - A clear and operational human oversight shall be defined, as well as sufficient controllability of the AI system.
  - Example of evidence
    - System documentation.
    - Human oversight organisation document.
  - Reference to base standard
    - The following standards and methods may be used:
      - ISO/IEC JTC 1/SC 42 8200 Information technology — Artificial intelligence — Controllability of automated artificial intelligence systems [52].
      - ISO/IEC JTC 1/SC 42 42105 Information technology — Artificial intelligence — Guidance for human oversight of AI systems [53].
- **RC-Sufficient AI logging (automatic) and record-keeping capabilities**
  - Description
    - AI logging (automatic) and record-keeping capabilities shall be defined and implemented.
  - Example of evidence
    - System documentation.

    - Evidence that the AI logging and record-keeping systems are secure.
  - Reference to base standard
    - The following standards and methods may be used:
      - ISO/IEC JTC1/SC42 24970 Artificial intelligence — AI system logging [54].
- **RC-Clear technical documentation and documentation keeping capability**
  - Description
    - A clear technical documentation and documentation keeping capability shall be defined and implemented.
  - Example of evidence
    - System documentation.
    - Description of the organisation process for documentation management.
  - Reference to base standard
    - The following standards and methods may be used:
      - ISO/IEC JTC1/SC42 42001 Information technology — Artificial intelligence — Management system [33].
- **RC-Sufficient robustness and resilience**
  - Description
    - Sufficient robustness and resilience levels of the AI system shall be ensured and regularly assessed.
  - Example of evidence
    - Analysis and implemented measures for system robustness and resilience
  - Reference to base standard
    - The following standards and methods may be used:

        - ISO/IEC JTC1/SC42 42001 Information technology — Artificial intelligence — Management system [33]
        - ISO/IEC JTC1/SC42 5469 Artificial intelligence — Functional safety and AI systems [55]
        - ISO/IEC JTC1/SC42 24029-1:2021 Artificial Intelligence (AI) — Assessment of the robustness of neural networks –
            - Part 1: Overview [56].
            - Part 2: Methodology for the use of formal methods [57].
- **RC-Sufficient safety**
    - Description
        - A sufficient safety level of the AI system shall be ensured and regularly assessed.
    - Example of evidence
        - Analysis and implemented measures for system safety.
    - Reference to base standard
        - The following standards and methods may be used:
            - ISO/IEC JTC1/SC42 5469 Artificial intelligence — Functional safety and AI systems [55]
            - ISO/IEC JTC1/SC42 22440 Artificial intelligence — Functional safety and AI systems
                - Part 1: Requirements [58].
                - Part 2: Guidance [59].
                - Part 3: Requirements [60].
            - ISO/IEC JTC1/SC42 42119-2 Artificial intelligence — Testing of AI - Part 2: Overview of testing AI systems [61].
- **RC-Sufficient accuracy and reliability**

- Description
  - Sufficient accuracy and reliability levels shall be ensured and regularly assessed.
- Example of evidence
  - Analysis and implemented measures for system accuracy and reliability.
- Reference to base standard
  - The following standards and methods may be used:
    - ISO/IEC JTC1/SC42 25570 Information Technology — Artificial Intelligence — Reliability assessment of AI systems [62].

- **RC-Sufficient transparency**
  - Description
    - A sufficient transparency level shall be ensured.
    - The goal of these transparency requirements is to balance innovation with user protection, ensuring people are not misled by AI while avoiding excessive regulation for lower-risk applications.
  - Example of evidence
    - Analysed and implemented measures for system transparency.
  - Reference to base standard
    - The following standards and methods may be used:
      - ISO/IEC JTC1/SC42 42001 Information technology — Artificial intelligence — Management system [33].
      - ISO/IEC JTC1/SC42 12792 Information technology — Artificial intelligence — Transparency taxonomy of AI systems [63].
- **RC-Sufficient explainability**

- Description
  - A sufficient explainability level shall be ensured.
- Example of evidence
  - Analysis and implemented measures for system explainability.
- Reference to base standard
  - The following standards and methods may be used:
    - ISO/IEC JTC1/SC42 6254 Information technology — Artificial Intelligence — Objectives and approaches for explainability and interpretability of machine learning (ML) models and artificial intelligence (AI) systems [64].

- **RC-Sufficient data/algorithm quality and suitability**
  - Description
    - Sufficient data and algorithm quality and suitability levels should be ensured.
  - Example of evidence
    - Evidence that the system data and algorithm have a sufficient quality and suitability.
    - Analysis and implemented measures for system data/algorithm quality and suitability.
  - Reference to base standard
    - The following standards and methods may be used:
      - ISO/IEC JTC1/SC42 25058 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guidance for quality evaluation of artificial intelligence (AI) systems [41].

- ISO/IEC JTC1/SC42 24027 Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making [65]
- ISO/IEC JTC1/SC42 5259-6 Artificial intelligence — Data quality for analytics and machine learning (ML) Part 6: Visualization framework for data quality [43].
- ISO/IEC JTC1/SC42 42106 Information technology — Artificial intelligence — Overview of differentiated benchmarking of AI system quality characteristics [42].

- **RQ-Align_with_AI_System_with_obligations_of_IA_Act_Limited_Risk_Category**
  - Description
    - AI systems identified as limited risk following the AI Act categories will have to comply few requirements.
  - Reference to Capability / Measure
    - CP-AI_Act_alignement_Limited_category
  - Guidance
- **RC-Sufficient transparency**
  - Description
    - A sufficient transparency level shall be ensured.
    - The goal of these transparency requirements is to balance innovation with user protection, ensuring people are not misled by AI while avoiding excessive regulation for lower-risk applications.
  - Example of evidence
    - Evidence of the system transparency

        - Analysis and implemented measures for system transparency
    - Reference to base standard
        - The following standards and methods may be used :
            - ISO/IEC JTC1/SC42 42001 Information technology — Artificial intelligence — Management system
            - ISO/IEC JTC1/SC42 12792 Information technology — Artificial intelligence — Transparency taxonomy of AI systems
- **RC-Compliance with the regulatory framework**
    - Description
        - Compliance with the regulatory framework shall be ensured.
    - Example of evidence
        - Existence of this need in the company policy document
    - References
        - The following references may be used:
            - AI Act
            - Cyber Resilience Act (CRA)
            - Cybersecurity Act
            - GDPR,
            - Data Governance Act
            - ISO/IEC JTC 1/SC 42 42007 Information technology — Artificial intelligence — High-level framework and guidance for the development of conformity assessment schemes for AI systems

4.5.1.4. PRIVACY PROFILES

This section defines the privacy profiles to be implemented across the ECLIPSE DIGITAL project in order to comply to the common trustworthiness profile. This defines the main principles for privacy, and for each, specific requirements to be implemented.

4.5.1.4.1. ACCESS TO DATA

Table 57: Overview of Privacy - Access to data requirements and recommendations

Requirement	Recommendation
RQ-Information access restriction	RC- Implementation of authentication measures.
	RC- Access management procedures implementation.
	RC- Logs registers in the system.
RQ- Security in information transfer	RC-Internal information transfer must be secured, according to internal policies and procedures.
	RC- Use of secure networks, through VPNs.
	RC-Malware protection.

RQ- Information Access Restriction

- Description: The requirement encompasses the different procedures, recommendations and security measures to ensure that the access to PII (Personal Identifiable Information) is controlled.
- Capability reference:
  - CP-CP1 Information access management.
  - CP-CP2 Security in information transfer.
- Guidance:
  - RC- Implementation of authentication measures.
    - The recommendation encompasses different authentication measures that could be from physical address (biometric, badge) to enter data rooms or centres to digital measures to enter/log in systems.
    - Examples: Multi-factor authentication, user-centric authorization.
  - RC- Access management procedures implementation.
    - The access management policies, internal ones within organizations and projects are fundamental. The update in the rights of access (read, execute or write) enhance the access restriction and avoid unauthorized access.
    - Examples: access management policies of employees, project members.
  - RC- Logs registers in the system.
    - The registers of logs allow to have details on who has done something, when and what. A control over these logs can produce alarms to possible unauthorized access.
    - Examples: logs of activity, logs of system access.

4.5.1.4.2. LINKABILITY-DEIDENTIFICATION

Table 58: Overview of Privacy - Linkability-Deidentification requirements and recommendations

Requirement	Recommendation
RQ-Ensure processes to reduce linkability and de-identification risk.	RC-Data anonymization or pseudo anonymization.

RQ-Ensure processes to reduce linkability and de-identification risk.

- Description: The requirement prevents from de-identification risk and linkability risk. Different processes and procedures can be applied to reduce these risks.
- Capability reference:
  - CP-CP5 Data anonymization process.
- Guidance:
  - RC-Data anonymization or pseudo anonymization.
    - The recommendation applies to anonymize as much as possible PIIs, so that it is more difficult to link information to a user or an id. The goal is to reduce or avoid the risk of linkability and de-identification of the user.

4.5.1.4.3. DATA INTEGRITY

Table 59: Overview of Privacy – Data integrity requirements and recommendations

Requirement	Recommendation
RQ-Protection data records from loss, destruction, falsification, unauthorized access.	RC- Access management procedures to define and apply.
	RC- Control of actions within the data records (logs records).
	RC- Backup procedures implementation to protect data loss or destruction.
	RC- Control and alarm measures to detect alteration in the data (to prevent falsification or any unauthorized modification).
	RC- Ensure data transfers and communications.

RQ- Protection data records from loss, destruction, falsification, unauthorized access.

- Description: The requirement aims to prevent and keep the integrity of data, which means preventing form loss, destruction, falsification or modification of the data. The modification or loss of personal data can

affect strongly the system functioning and results but also the users' privacy and rights.

- Capability reference:
  - CP-CP3 Data Protection compliance
- Guidance:
  - RC- Access management procedures to define and apply.
    - This requirement is also applied in the Access to data profile. It should be defined a specific procedure or policy to access data in order to avoid not only unauthorised and unnecessary accesses to specific PIIs.
    - Example: restriction access for the team system, data controller and processors.
  - RC- Control of actions within the data records (logs records).
    - The requirement aims to monitor, somehow, the status of the data records. This could be done through logs records where it is stored the accesses and actions done with them.
  - RC- Backup procedures implementation to protect data loss or destruction.
    - The requirement tackles the data loss or destruction, with backups the risk is minimised, as the data can be restored.
  - RC- Control and alarm measures to detect alteration in the data (to prevent falsification or any unauthorised modification).
    - This is important as together with the logs, an implementation of scripts/software to check and monitor data records accesses and actions done in order to identify unusual activity or actions. It can launch alarms to detect possibly compromise of data.
  - RC- Ensure data transfers and communications.
    - Same as for Access to data.

4.5.1.4.4. REGULATION CONFORMITY

Table 60: Overview of Privacy – Regulation conformity requirements and recommendations

Requirement	Recommendation
RQ- Clarification of purpose for energy data collection and data processing.	RC- Assessment of data processing (proportionality and necessity)
	RC- Assessment of data subjects' rights compliance
	RC- Verify purpose and data processing information is explained in a clear way in the Consent.
RQ- Consent Compliance redaction	RC- Verify the Consent addresses GDPR users' rights
	RC- Verify the Consent explains clearly the roles of data Controller, Data Processor.
	RC- Verify the Consent explains, if the case, data transfers, specifically outside the EU.
	RC- Assessment of the data anonymisation process to be compliant with GDPR

RQ- Data anonymization process compliance	RC- Verify the Consent informs clearly about the data anonymisation process and data lifecycle.

RQ-Clarification of purpose for energy data collection and processing

- Description: The requirement aims to help and support the data controllers in order to be compliant with GDPR and data protection legislation. The purpose has to be clear, easy to explain and understandable for the users.
- Capability Reference:
  - CP-CP3 Data Protection compliance
  - CP-CP4 Consent management process.
- Guidance:
  - RC- Assessment of data processing (proportionality and necessity)
    - The recommendation helps to be compliant with GDPR in the data collection and data processing. The data processing must show clearly the necessity that it is not possible to achieve the results without doing this data processing. But also, the proportionality in data processing and data collection (data minimization strategy).
  - RC- Assessment of data subjects' rights compliance.
    - The recommendation is necessary to be compliant with the GDPR. The GDPR users' right such as Information (art. 12, 13 and 14), access and data portability (art. 15 and 20),

rectification and erasure (art. 16 and 17) or restriction to processing and withdraw (art. 18 and 21).

- RC- Verify purpose and data processing information is explained in a clear way in the Consent.
  - Check that the Consent gathers this information in a clear manner (get Consent (art. 7 and 8).

RQ- Consent Compliance redaction

- Description: This requirement is a key one as get the Consent (art. 7 and 8 from GDPR). The consent must be clear and understandable for the user and must include:
  - Purpose of data collection and data processing.
  - Explanation of data processing and its necessity and proportionality.
  - Data lifecycle (storage, deletion).
  - Users' rights reminder and available to execute them.
  - Information about data controllers, processors and data transfers outside the EU and/or third parties.
- Capability Reference:
  - CP-CP3 Data Protection compliance
  - CP-CP4 Consent management process.
- Guidance:
  - RC- Verify the Consent addresses GDPR users' rights
    - All the GDPR users' rights must be applicable, and the Consent must inform that they can exercise them.
  - RC- Verify the Consent explains clearly the roles of data Controller, Data Processor.
    - The information about who is collecting and storing the data and who processes the data on behalf of the controller

is essential. So, the user can ask for information or exercise his rights by contacting them.

- RC- Verify the Consent explains, if the case, data transfers, specifically outside the EU.
  - It is mandatory to explain if the users' data is transferred or shared with third parties in the data processing or for other reasons.

RQ- Data Anonymization process compliance

- Description: This requirement, related to profile Linkability-Deidentification, ensures that the data anonymization process is compliant with actual regulation.
- Capability Reference:
  - CP-CP3 Data Protection compliance
  - CP-CP4 Consent management process.
  - CP-CP5 Data anonymization process.
- Guidance:
  - RC- Assessment of the data anonymisation process to be compliant with GDPR
    - Check the data anonymisation process within the GDPR and standards (ISO/IEC 20889 Privacy enhancing data de-identification terminology and classification of techniques or ISO/IEC 27559 Privacy enhancing data de-identification framework.
  - RC- Verify the Consent informs clearly about the data anonymisation process and data lifecycle.
    - The data lifecycle (storage limit, data collection, deletion process) must be specified to the user in the Consent.

4.5.1.5. CYBERSECURITY PROFILES

4.5.1.5.1. REFERENCE LIST OF RECOMMENDATIONS

This section lists recommendations that can be applied across the ECLIPSE DIGITAL project in order to comply to the common trustworthiness profile.

- **RC-Secure channel**
  - Description:
    - A secure channel such as TLS (Transport Layer Security) or a VPN (Virtual private network) shall be used to establish communication
- **RC-Single Authentication**
  - Description:
    - If the sender is a TLS Client, an additional authentication method such as OAuth or client certificates shall be used to verify their identity
- **RC-Multiple Authentication**
  - Description:
    - If TLS is used, each participant shall be identified through an authentication method like OAuth
    - If a VPN is used, each participant is authenticated when getting access to the VPN
- **RC-Message signature**
  - Description:
    - To protect some fields in a message, the content of these fields should be hashed together and then signed with a private key

        - The associated public key should be securely distributed and authenticated, for example by a certificate
- **RC-Secure channel integrity**
    - Description:
        - A secure channel like TLS provides the necessary integrity protection
- **RC-Read access control**
    - Description:
        - Ensure that file system permissions are correctly set so that only the system users responsible for the data can read it
        - Additionally, enforce access control so that application users can only read data related to their account
- **RC-Nonce in message**
    - Description:
        - Another measure like a secure channel should be used to ensure message integrity
        - When used in a signed message, the nonce should be included in the field covered by the signature.
- **RC-Write access control**
    - Description:
        - Ensure that file system permissions are correctly set so that only the system users responsible for modifying the data can write to it
        - Additionally, enforce access control so that application users can only write data related to their account
- **RC-Multiple endpoints**
    - Description:

        - The system can be reached through at least 2 physical machines
- **RC-Multiple channels**
    - Description:
        - The system can send messages using at least 2 different channels
- **RC-API Credits**
    - Description:
        - Every user gets assigned a limited number of allowed requests credits
        - Requests are dropped when credits reach 0
        - New credits are added regularly up to a configured ceiling
- **RC-Hosting DDoS Filtering**
    - Description:
        - Choose a hosting provider implementing DDoS Filtering in their network
- **RC-Firewall**
    - Description:
        - Place servers behind a firewall configured to drop suspicious traffic
- **RC-Numeric Limits**
    - Description:
        - Ensure that the numbers processed, especially measurements, fit within reasonable limits
- **RC-Input monitoring**
    - Description:
        - Provide alerts when anomalous inputs are detected
- **RC-Automatic updates**
    - Description:

- If the device can automatically fetch and install updates, the functionality should be activated

4.5.2. TRUSTWORTHINESS MECHANISM PROFILES FOR "ECONOMIC BENEFITS FOR DEMAND RESPONSE" (HLUC1)

The trustworthiness profile for the High-level use case 1 has been established in this section to demonstrate how to apply a trustworthiness profile to a more specific use case. HLUC 1 was selected to illustrate the trustworthiness profile, as it presents the most complex structure among the HLUCs and therefore provides a representative example

4.5.2.1. CAPABILITIES / MEASURES REFERENCES

The following table content provides references to the Capabilities / Measures identified during the X-CCP analysis.

Table 61: Characteristics of the HLUC1 trustworthiness profile

Characteristic	Goal / Risk	Capability / Measure
CH-Governability	GL-Ensure_Trustworthiness_Governance	CP-Define_Trustworthiness_Governance

CH_Privacy	GL-GL1 Avoid unauthorized access to PIIs GL-GL2 Ensure confidentiality of Data GL-GL4 Ensure unlinking personal information (flexibility data) to a user GL-GL5 Ensure anonymization process for long data storage. GL-GL6 Keep data integrity (savings and bids)	CP-CP1 Information access management. CP-CP2 Security in information transfer. CP-CP5 Data anonymization process.
CH_Security	R_Tampered_Incentives_Report	M_Sender_Authentication
		M_Message_Integrity
	R_Negociation_spoofing	M_Sender_Authentication
	R_Tampered_directives	M_Message_Integrity
		M_Sender_Authentication
	R_private_data_leak	M_Data_Storage_Read_Protection

CH_AI-Trustworthiness	N/A Note: Check "Common Trustworthiness mechanism profiles to all use-cases" §	N/A Note: Check "Common Trustworthiness mechanism profiles to all use-cases" §

4.5.2.2. SECURITY PROFILE

4.5.2.2.1. ASSURANCE REQUIREMENTS TO BE IMPLEMENTED

- RQ_Report_Sender_Authentication
  - Description
    - The report sender shall be strongly authenticated
  - Reference to Capability/Measure
    - M_Sender_Authentication
  - Guidance
    - **RC-Secure channel**
    - **RC-Single Authentication**
- RQ_Report_Integrity
  - Description
    - The content of the report shall be authenticated and protected against modification by a signature
  - Reference to Capability/Measure
    - M_Message_Integrity
  - Guidance
    - **RC-Message signature**
- RQ_Negociation_Authentication
  - Description:
    - Negociation participants shall be strongly authenticated

        - The negociation protocol shall include digital signatures in messages to ensure the produced agreements are still authenticated when stored
    - Reference to Capability/Measure
        - M_Sender_Authentication
    - Guidance:
        - **RC-Secure channel**
        - **RC-Multiple Authentication**
- RQ_Directive_Integrity
    - Description:
        - The content of the directives shall be protected against modification on the wire
    - Reference to Capability/Measure
        - M_Message_Integrity
    - Guidance
        - **RC-Secure channel integrity**
- RQ_Directive_Authentication
    - Description:
        - The sender of a directive shall be authenticated by at least one of:
            - A secure channel providing authentication of the sender
            - A signature from the sender of the directive message
    - Reference to Capability/Measure
        - M_Sender_Authentication
    - Guidance
        - **RC-Single Authentication**
        - **RC-Message signature**
- RQ_User_Data_Storage_Read_Protection

- Description:
  - Read privileges for data related to user accounts shall be set appropriately according to the principle of least privileges
- Reference to Capability/Measure
  - M_Data_Storage_Read_Protection
- Guidance
  - **RC-Read access control**

4.6. REQUIREMENTS RATIONALE

The following table shows that every use-case is supported by requirements to be implemented and/or to be verified on each trustworthiness characteristic studied within ECLIPSE DIGITAL.

It also provides a commonality of requirements according to ECLIPSE DIGITAL use-cases.

Table 62: Requirements rationale for the HLUCs

Requirement	Use-cases				
	Economic Benefits for Demand Response (HLUC1)	Non-Economic Incentives for Voluntary Action (HLUC2)	Technology Adoption for Efficiency (HLUC3)	Alerts for Extreme Grid Situations (HLUC4)	General Energy Efficiency Guidance (HLUC5)

Requirements to be implemented					
RQ-Define_and_institute_a_Trustworthiness_Governance	X	X	X	X	X
RQ-Define_and_institute_a_Trustworthiness_Governance	X	X	X	X	X
RQ- Information Access Restriction	X	X	X		
RQ- Ensure processes to reduce linkability and de-identification risk	X				X
RQ- Protection data records from loss, destruction, falsification, unauthorized access.	X	X	X		

RQ- Clarification of purpose for energy data collection and data processing.	X	X	X		X
RQ- Consent Compliance redaction	X	X	X		X
RQ-Data anonymization process compliance			X		X
RQ- Report Sender Authentication					
RQ- Report Integrity					
RQ- Negotiation Authentication					
RQ- Directive Integrity					
RQ- Directive Authentication					
RQ- User data Storage Read Protection					

5. CONCLUSION

This deliverable aims to present the data protection analysis performed in the ECLIPSE DIGITAL project. It presents the methodology of the analysis, that was performed on the five ECLIPSE DIGITAL High-level use-cases and its results. This includes the governance, cybersecurity, privacy and AI trustworthiness of the energy-saving applications.

Here are the main results for the five HLUCs:

HLUC1: Personalised messages for consumer flexibility based on economic benefits

- Cybersecurity: All risks may be taken.
- Privacy: The following controls were identified:
  - Information access restriction.
  - Security in information transfer.
  - Protection and compliance related to PII and records.

HLUC2: PERSONALISED MESSAGES FOR CONSUMER FLEXIBILITY BASED ON NON-ECONOMIC INCENTIVES

- Cybersecurity: All risks may be taken.
- Privacy: The following controls were identified:
  - Data anonymization.
  - Implementation of authentication measures.
  - Consent management.
  - Employ encryption protocols.
  - Appropriate GDPR requests.

HLUC3: Personalised messages to consumers about energy efficiency potential

- Cybersecurity: The following risks must be reduced:
  - Bad/Falsified measurements from meters/HEMS propagate in prediction models leading to wrong predictions.
  - Tampered energy market price causing wrong advice.
- Privacy: The following controls were identified:
  - Structured identification of hardware assets involved in the pilot project.
  - User registration and authentication procedures.
  - Malware protection is implemented through a defence-in-depth approach.
  - Regular backup and time synchronisation.
  - Comprehensive event logging is enabled and logging services, recording all activities and providing an audit trail.
  - All operational software is managed through standardized processes.
  - AIIDA securisation data collection.
  - AIIDA Consent management opt-out.

HLUC4: Alerts for Extreme Grid Situations

- Cybersecurity: All risks may be taken.
- Privacy: No users data are used.

HLUC5: General Energy Efficiency Guidance

- Cybersecurity: The following risks must be reduced:
  - AIIDA interface flooded with data queries during peak load.

  - Aggregator injects biased flexibility signals to favour specific outcomes.
  - Data breach exposing household level consumption patterns.
- Privacy: The following controls were identified:
  - Planned information classification guideline.
  - Private Git repository, Data access/sharing based on requests, Access control for HLUC5 at the database level currently not supported.
  - Configuration for near real-time data services, Passwords in end customer application, User-centric authorisation.
  - Password management in the end user application.
  - Hash code for each user (planned), Apache Kafka and MQTT to secure communication.
  - Segregation of duties in HLUC 5.
  - Multi-Factor Authentication (MFA) planned.
  - Git development setting, Keycloak, Database
  - Git - security checks in CI/CD pipelines.
  - Institutional control (FHOOE). Not applicable to HLUC5.
  - Securely develop, test and deploy HLUC 5 planned.
  - Security in HLUC 5 development, testing and deployment is currently not implemented – externally handled.
  - Institutional control (FHOOE).

The results from this analysis should be used in the development and deployment phases of the project, in WP4 “Design and development of CERF and APIs” and WP5 “Preparation, coordination and monitoring of deployment and demonstration activities; as well as in any project using the CERF”.

KPIs are moreover defined to monitor the implementation of the defined cybersecurity, privacy, AI trustworthiness recommendations.

The results are then used to create trustworthiness profiles, that extend the interoperability profile in order to integrate the Common European Reference Framework (CERF) for energy applications.

6. ACRONYMS

Acronym	Definition
AI	Artificial Intelligence
AIIDA	Administrative Interface for In-house Data Access
API	Application Programming Interface
CERF	Common European Reference Framework
CH	Characteristics
CRA	Cyber Resilience Act
DDOS	Distributed Denial of Service
DMS	Dispatcher Management System
DPIA	Data Privacy Impact Assessment
DSO	Distribution System Operator
ENISA	European Union Agency for Cybersecurity
EU	European Union

GDPR	General Data Protection Regulation
GL	Goal
HEMS	Home Energy Management System
HLUC	High-Level Use Case
IACS	Industrial Automation Control System
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
KPI	Key Performance Indicators
LINDDUN	Linkability, Identifiability, Non-repudiation, Detectability, Disclosure, Unawareness, Non-compliance
MFA	Multi-Factor Authentication
ML	Maturity Level
MQTT	Message Queuing Telemetry Transport

MS	Measure
NIS 2	EU Directive on Network and Information Security (version 2)
NIST	National Institute of Standards and Technology
PIA	Privacy Impact Assessment
REST	Representational State Transfer
RC	Recommendation
RQ	Requirement
SGAM	Smart Grid Architecture Model
SL	Security Level
SPR	Security & Privacy Requirements
SSL	Secure Sockets Layer
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TSL	Transport Layer Security

TSO	Transmission System Operator
VPN	Virtual Private Network
X-CCP	Cross-cutting Characteristics Plan

7. REFERENCES

[1] European project Maesha (GA n°957843), “Deliverable D7.3: Security and privacy protection actions plan and results,” 2022.

[2] Energica European project Grant Agreement ID 0103742, “D1.7 Security and privacy protection action results,” 2021.

[3] Parmenides European project Grant Agreement n° 101096453, “Deliverable D5.2 Results of the application of the cybersecurity and privacy practice on the pilots,” 2024.

[4] EU, «General Data Protection Regulation (GDPR),» Intersoft consulting, 2016. [En ligne]. Available: https://gdpr-info.eu/. [Accès le 28 07 2023].

[5] ECLIPSE PROJECT, GA n°101158494, “Deliverable 1.2: Data Management Plan,” 2024.

[6] ISO, “ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment,” ISO, 2017. [Online]. Available: https://www.iso.org/standard/62289.html. [Accessed 06 01 2023].

[7] ISO, “ISO 31000:2018 (en) Risk management — Guidelines,” 2018. [Online]. Available: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en. [Accessed 06 01 2023].

[8] Lindunn, “LINDDUN privacy engineering,” 2020. [Online]. Available: https://www.linddun.org/. [Accessed 06 01 2023].

[9] ISO/IEC JTC 1/SC 27, «ISO/IEC 27005 – Information security risk management,» 2022.

[10] ISO/IEC JTC 1/SC 27, «ISO/IEC 27002 Information security, cybersecurity and privacy protection — Information security controls,» 2022.

[11] Microsoft, «STRIDE model».

[12] ISO/IEC JTC 1/SC 42, "ISO/IEC 42005 Information technology – Artificial intelligence – AI system impact assessment".

[13] ISO/IEC JTC 1/SC 42, «ISO/IEC TR 24028 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence,» 2020.

[14] Cen-Cenelec JTC21, «AI Trustworthiness framework».

[15] ISO, "Management system standards," ISO, [Online]. Available: https://www.iso.org/management-system-standards.html. [Accessed 06 01 2023].

[16] ISA, "ISA/IEC 62443 Series of Standards," 2022. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. [Accessed 06 01 2023].

[17] LINDDUN, "Privacy threat knowledge support," 2025. [Online]. Available: https://linddun.org/threats/. [Accessed 2025].

[18] HEDGE-IoT, «HEDGE-IoT - Holistic Approach towards Empowerment of the DiGitalization of the Energy Ecosystem through adoption of IoT solutions,» [En ligne]. Available: https://hedgeiot.eu/.

[19] European Commission, «AI ACT: REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL,» 2021.

[20] ISO/IEC JTC 1/SC 42, «ISO/IEC 8183 Information technology — Artificial intelligence — Data life cycle framework,» 2023.

[21] European Commission, «European Cyber Resilience Act (CRA),» 2024.

[22] European Parliament, «GDPR (General Data Protection Regulation): Regulation (EU) 2016/679».

[23] European Parliament, «NIS 2 Directive (Directive (EU) 2022/2555),» 2022.

[24] ISO/IEC JTC 1/SC 42, «ISO/IEC 23894 Information technology — Artificial intelligence — Guidance on risk management,» 2023.

[25] ISO/IEC JTC 1/SC 42, «ISO/IEC 24368 Information technology — Artificial intelligence — Overview of ethical and societal concerns,» 2022.

[26] ISO/IEC JTC 1/SC 42, «ISO/IEC 5259-1 Artificial intelligence — Data quality for analytics and machine learning (ML),» 2024.

[27] ISO/IEC JTC 1/SC 42, «ISO/IEC 5259-2 Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 2: Data quality measures learning (ML) - Part 2: Data quality measures,» Under development.

[28] ISO/IEC JTC 1/SC 27, «ISO/IEC CD 27090 Cybersecurity — Artificial Intelligence — Guidance for addressing security threats and failures in artificial intelligence systems».

[29] ISO/IEC JTC 1/SC 27, «ISO/IEC 27091.2 Cybersecurity and Privacy — Artificial Intelligence — Privacy protection».

[30] ISO/IEC JTC 1/SC 27, «ISO/IEC TR 27563 Security and privacy in artificial intelligence use cases — Best practices,» 2023.

[31] ISO/IEC JTC 1/SC 42, «ISO/IEC 12792 Information technology — Artificial intelligence — Transparency taxonomy of AI systems».

[32] ISO/IEC JTC 1/SC 42, «ISO/IEC 24029-1 Artificial Intelligence (AI) — Assessment of the robustness of neural networks,» 2021.

[33] ISO/IEC JTC 1/SC 42, «ISO/IEC 38507:2022 Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations,» 2022.

[34] ISO/IEC JTC 1/SC 42, «ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system,» 2023.

[35] ISO/IEC JTC 1/SC 42, «ISO/IEC 6254 Information technology 196 — Artificial intelligence — Objectives and approaches for explainability of ML models and AI systems,» 2024.

[36] ISO/IEC JTC 1/SC 42, «ISO/IEC AWI 24970 Artificial intelligence — AI system logging».

[37] ISO/IEC JTC 1/SC 42, «ISO/IEC AWI 42105 Guidance for human oversight».

[38] ISO/IEC JTC 1/SC 42, «SO/IEC 24029-2 Artificial intelligence (AI) — Assessment of the robustness of neural networks - Part 2: Methodology for the use of formal methods,» 2023.

[39] ISO/PC 317, «ISO 31700-1 Consumer protection — Privacy by design for consumer goods and services,» 2023.

[40] ECLIPSE DIGITAL project, Grant agreement N° 101158494, "D2.1 Data management plan," 2024.

[41] ECLIPSE DIGITAL project, Grant agreement N° 101158494, "D3.1 CERF architecture specification and ECLIPSE interoperability profile," 2025.

[42] ECLIPSE DIGITAL project, "D4.1 ECLIPSE CERF for Energy Saving applications," 2025.

[43] ISO/IEC JTC 1, «ISO/IEC TS 5723:2022 Trustworthiness — Vocabulary,» 2022.

[44] ISO/IEC JTC 1/SC 7, «ISO/IEC/IEEE 15026-2 Systems and software engineering — Systems and software assurance,» 2022.

[45] ISO/IEC JTC 1/SC 42, «ISO/IEC 25058 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guidance for quality evaluation of artificial intelligence (AI) systems».

[46] ISO/IEC JTC 1/SC 42, «ISO/IEC 42106 Information technology — Artificial intelligence — Overview of differentiated benchmarking of AI system quality characteristics».

[47] ISO/IEC JTC 1/SC 42, «ISO/IEC 5259-6 Artificial intelligence — Data quality for analytics and machine learning (ML)Part 6: Visualization framework for data quality».

[48] ISO/IEC JTC 1/SC 42, «ISO/IEC 5338 information technology — Artificial intelligence — AI system life cycle processes,» 2023.

[49] ISO/IEC JTC 1/SC 42, « 24368 Information technology — Artificial intelligence — Overview of ethical and societal concerns,» 2022.

[50] ISO/IEC JTC 1/SC 42, «ISO/IEC 22443 Information technology — Artificial intelligence — Guidance on addressing societal concerns and ethical considerations».

[51] European Commission, «Data Governance Act,» 2022. [En ligne].

[52] ISO/IEC JTC 1/SC 42, «ISO/IEC 42007 Information technology — Artificial intelligence — High-level framework and guidance for the development of conformity assessment schemes for AI systems».

[53] O/IEC JTC 1/SC 27, «ISO/IEC 27090 Cybersecurity — Artificial Intelligence — Guidance for addressing security threats to artificial intelligence systems».

[54] ENISA, «Cybersecurity of AI and Standardisation,» 2023.

[55] ISO/IEC JTC 1/SC 27, «ISO/IEC 27091 Cybersecurity and Privacy — Artificial Intelligence — Privacy protection».

[56] ISO/IEC JTC 1/SC 42, «ISO/IEC TS 8200:2024 Information technology — Artificial intelligence — Controllability of automated artificial intelligence systems,» 2024.

[57] ISO/IEC JTC 1/SC 42 , «ISO/IEC 42105 Information technology — Artificial intelligence — Guidance for human oversight of AI systems».

[58] ISO/IEC JTC 1/SC 42, «ISO/IEC 24970 Artificial intelligence — AI system logging».

[59] ISO/IEC JTC 1/SC 42, «ISO/IEC 5469:2024 Artificial intelligence — Functional safety and AI systems».

[60] ISO/IEC JTC 1/SC 42, « ISO/IEC 24029-1:2021 Artificial Intelligence (AI) — Assessment of the robustness of neural networks – Part 1: Overview,» 2021.

[61] ISO/IEC JTC 1/SC 42, «ISO/IEC 24029-2:2023 Artificial intelligence (AI) — Assessment of the robustness of neural networks – Part 2: Methodology for the use of formal methods».

[62] ISO/IEC JTC 1/SC 42, «ISO/IEC JTC 1/SC 42 22440 Artificial intelligence — Functional safety and AI systems - Part 1: Requirements».

[63] ISO/IEC JTC 1/SC 42, «ISO/IEC JTC 22440 Artificial intelligence — Functional safety and AI systems - Part 2: Guidance».

[64] ISO/IEC JTC 1/SC 42, «ISO/IEC JTC 22440 Artificial intelligence — Functional safety and AI systems - Part 3: Examples of application».

[65] ISO/IEC JTC 1/SC 42, «ISO/IEC 42119-2 Artificial intelligence — Testing of AIPart 2: Overview of testing AI systems».

[66] ISO/IEC JTC 1/SC 42, «ISO/IEC 25570 Information Technology — Artificial Intelligence — Reliability assessment of AI systems».

[67] ISO/IEC JTC 1/SC 42, «ISO/IEC 12792 Information technology — Artificial intelligence — Transparency taxonomy of AI systems».

[68] ISO/IEC JTC 1/SC 42, «ISO/IEC 6254 Information technology — Artificial intelligence — Objectives and approaches for explainability and interpretability of machine learning (ML) models and artificial intelligence (AI) systems».

[69] ISO/IEC JTC 1/SC 42 , «ISO/IEC 24027 Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making,» 2021.

[70] ISO, "ISO/IEC 20889:2018 Privacy enhancing data de-identification terminology and classification of techniques," 2018. [Online]. Available: https://www.iso.org/standard/69373.html. [Accessed 06 01 2023].

[71] ISO, "ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines," 2019. [Online]. Available: https://www.iso.org/standard/71670.html. [Accessed 06 01 2023].

[72] ISO, "ISO/IEC TS 27570:2021 Privacy protection — Privacy guidelines for smart cities," 2021. [Online]. Available: https://www.iso.org/standard/71678.html. [Accessed 06 01 2023].

[73] ISO, "ISO/IEC 27556:2022 Information security, cybersecurity and privacy protection — User-centric privacy preferences management framework," 2022. [Online]. Available: https://www.iso.org/standard/71674.html. [Accessed 06 01 2023].

[74] ISO, "ISO/IEC TR 27550:2019 Information technology — Security techniques — Privacy engineering for system life cycle processes," 2019. [Online]. Available: https://www.iso.org/standard/72024.html. [Accessed 06 01 2023].

[75] ISO, "ISO/IEC CD 27561.2 Information technology — Security techniques — Privacy operationalisation model and method for engineering (POMME)," ISO, [Online]. Available: https://www.iso.org/standard/80394.html. [Accessed 06 01 2023].

[76] ISO, "ISO/IEC 27400:2022 Cybersecurity — IoT security and privacy — Guidelines," 2022. [Online]. Available: https://www.iso.org/standard/44373.html. [Accessed 06 01 2023].

[77] ISO, "ISO/IEC 27559:2022 Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework," 2022. [Online]. Available: https://www.iso.org/standard/71677.html. [Accessed 06 01 2023].

[78] ISO, "ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework," 2011. [Online]. Available: https://www.iso.org/standard/45123.html. [Accessed 06 01 2023].

[79] ISO, "ISO 31700-1 Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements," 2023.

[Online]. Available: https://www.iso.org/standard/84977.html. [Accessed 06 01 2023].

[80] NIST, "NISTIR 7628 Rev. 1 Guidelines for Smart Grid Cybersecurity," 2014. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final. [Accessed 06 01 2023].

[81] NIST, "NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal System," NIST, 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf. [Accessed 06 01 2023].

[82] NIST, "Privacy Framework," 2022. [Online]. Available: https://www.nist.gov/privacy-framework. [Accessed 06 01 2023].

[83] CNIL, "Privacy impact assessment (PIA)," 02 2018. [Online]. Available: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf. [Accessed 06 01 2023].

[84] ISO, "Management system standards," ISO, [Online]. Available: https://www.iso.org/management-system-standards.html. [Accessed 06 01 2023].

[85] ISO, "ISO/IEC TS 27570:2021 Privacy protection — Privacy guidelines for smart cities," 2021. [Online]. Available: https://www.iso.org/standard/71678.html. [Accessed 06 01 2023].

[86] ISO, "ISO/IEC 27556:2022 Information security, cybersecurity and privacy protection — User-centric privacy preferences management

framework," 2022. [Online]. Available: https://www.iso.org/standard/71674.html. [Accessed 06 01 2023].

[87] ISO, "ISO/IEC CD 27561.2 Information technology — Security techniques — Privacy operationalisation model and method for engineering (POMME)," ISO, [Online]. Available: https://www.iso.org/standard/80394.html. [Accessed 06 01 2023].

[88] ISO, "ISO/IEC 27559:2022 Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework," 2022. [Online]. Available: https://www.iso.org/standard/71677.html. [Accessed 06 01 2023].

[89] ISO, "ISO 31700-1 Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements," 2023. [Online]. Available: https://www.iso.org/standard/84977.html. [Accessed 06 01 2023].

Thank You

If you have any questions, please get in touch with us.

www.ECLIPSE

info@ECLIPSE

@ECLIPSE

@ECLIPSE

@ECLIPSE