ETSI TR 104 027 V1.1.1 (2025-10)

TECHNICAL REPORT

User-Centric Approach in the digital ecosystem; The User Information System and Smart Customized Services; Concept, definition and services

Reference
DTR/USER-0055

Keywords
QoS, security, UIS, USER

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 6
3 Definition of terms, symbols and abbreviations 8
3.1 Terms 8
3.2 Symbols 9
3.3 Abbreviations 9
4 Smart Customized Services for UIS 10
4.1 Identification of the problem to be solved 10
4.2 Application of the ACIFO model in SCS 12
5 Use cases for User Information Systems 13
5.1 Introduction to use cases for UIC and their service composition 13
5.2 Urban mobility use case (Smart Urban Mobility Assistant) 14
5.3 Agriculture 16
5.4 Health 19
5.5 Assurance of Health and Safety in an IoT enabled construction environment 20
6 Regulatory and other constraints that may apply to UIS/SCS 21
6.1 Data governance 21
6.2 Privacy and data protection 22
6.3 Security 22
6.4 Data semantics and ontology 23
6.5 Accessibility 23
6.6 Ethics Considerations 23
7 Recommendations for further specification of ACIFO in SCS 25
7.1 General requirements for the Digital Ecosystem 25
7.1.1 Overview and introduction 25
7.1.2 The architectural dimension 26
7.1.3 The communication dimension 27
7.1.4 The Informational Dimension: 28
7.1.5 The functional Dimension 29
7.1.6 The Organizational Dimension 31
7.2 UIS/SCS requirements User side (userware) 31
7.2.1 Userware Interactions with the ecosystem components 31
7.2.2 User Centric Vision 33
Annex A: Assist-IoT project overview 34
Annex B: i-Tour project overview 35
Annex C: i-locate project overview 37
Annex D: Detail of regulatory factors to be considered in UIC/SCS 38
D.1 Privacy aspects 38
D.1.1 General overview 38
D.1.2 Identification of Data Controller 38
D.1.3 Identification of Data Processor 38
D.1.4 Identification of affected user (data subject) 38
D.1.5 Other privacy impacting aspects 39

D.2 Security....40
D.3 Data semantics and ontology....41
D.4 Data portability....41
D.5 Accessibility aspects....42
Annex E: Example of Application of ACIFO model to tomato cultivation (user side)....45
E.1 Overview....45
E.2 Functions and features....45
E.2.1 Real-time environmental (Sensors → UIS)....45
E.2.2 Anomaly detection (Userware)....46
E.2.3 Expert validation and AI model selection (Agronomy Expert)....46
E.2.4 AI-based anomaly analysis (AI Engine)....46
E.2.5 Corrective recommendations (Userware + Expert support)....46
E.2.6 Farmer decision-making and feedback (Farmer → Userware)....46
Annex F: Bibliography....47
History....48

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Special Committee User Group (USER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document presents an analysis of the user expectations, with respect to the study of data driven technologies (Artificial Intelligence (AI), deep learning, Machine Learning (ML)) to present the definition and concept of the User Information System (UIS), that enables Smart Customized Services (SCS) from both user and provider side. These services aim to provide personalization, adaptability, and intelligent decision support within the digital ecosystem.

NOTE: The UIS and SCS are designed to serve a broad spectrum of users. Their objective is to empower and protect all citizens. By integrating smart and assistive technologies, the system seeks to enhance participation in public, social, and economic activities, while also offering advanced users more autonomy and self-management capabilities.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI TR 103 438: "User Group; User centric approach in Digital Ecosystem".

[i.2] ETSI EG 203 602: "User Group; User Centric Approach: Guidance for users; Best practices to interact in the Digital Ecosystem".

[i.3] ETSI TR 103 603: "User Group; User Centric Approach; Guidance for providers and standardization makers".

[i.4] ETSI TR 103 604: "User Group; User centric approach; Qualification of the interaction with the digital ecosystem".

[i.5] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance).

[i.6] EN 301 549 (V3.2.1) (2021-03): "Accessibility requirements for ICT products and services".

[i.7] ISO 9241-210:2019: "Ergonomics of human-system interaction; Part 210: Human-centred design for interactive systems", Edition 2; 2019.

[i.8] Interaction Design Foundation: "Design for All".

[i.9] Centre for Excellence in Universal Design: "The 7 Principles".

[i.10] ETSI EG 202 116 (V1.2.2) (2009-03): "Human Factors (HF); Guidelines for ICT products and services; "Design for All"".

[i.11] ETSI TS 102 747 (V1.1.1) (2009-12): "Human Factors (HF); Personalization and User Profile Management; Architectural Framework".

[i.12] ETSI ES 202 746 (V1.1.1) (2010-02): "Human Factors (HF); Personalization and User Profile Management; User Profile Preferences and Information".

[i.13] University of East London: "Exploring the Ethical Implications of AI-Powered Personalization in Digital Marketing".

[i.14] EU TAi Guidelines.

[i.15] ETSI TR 104 221: "Securing Artificial Intelligence (SAI); Problem Statement".

[i.16] ETSI TS 104 224: "Securing Artificial Intelligence (SAI); Explicability and transparency of AI processing".

[i.17] ETSI TS 104 102: "Cyber Security (CYBER); Encrypted Traffic Integration (ETI); ZT-Kipling methodology".

[i.18] ETSI TR 103 477: "eHEALTH; Standardization use cases for eHealth".

[i.19] Assist-IoT project report D3.2: "Use Cases Manual & Requirements and Business Analysis - Initial".

[i.20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.21] The EU project i-Tour.

[i.22] Lazarotto, B.: "The right to data portability: A holistic analysis of GDPR, DMA and the Data Act".

[i.23] ETSI EN 303 760 (V1.1.1) (2024-10): "SmartM2M; SAREF Guidelines for IoT Semantic Interoperability; Develop, apply and evolve Smart Applications ontologies".

[i.24] ETSI TR 103 875-2: "User Centric approach in Digital Ecosystem; The Smart Interface; Part 2: Smart Identity: A Proof of Concept".

[i.25] ETSI TR 103 437: "USER; Quality of ICT services; New QoS approach in a digital ecosystem".

[i.26] OMG UML®: "OMG® Unified Modeling Language®", Version 2.5.1.

[i.27] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS).

[i.28] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS2).

[i.29] ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.30] Brandt Dainow: "Digital Alienation as the Foundation of Online Privacy Concerns".

[i.31] ETSI TR 119 476: "Electronic Signatures and Trust Infrastructures (ESI); Analysis of selective disclosure and zero-knowledge proofs applied to Electronic Attestation of Attributes".

[i.32] ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT".

[i.33] ISO/IEC 7498-1: "Information technology -- Open Systems Interconnection - Basic Reference Model: The Basic Model".

[i.34] Foureaux, Simon & Daum, Thomas (2025): ""But don't think it is a game": Agricultural videogames and "good farming"". Journal of Rural Studies. 117. 10.1016/j.jrurstud.2025.103686.

[i.35] ETSI Directives.

[i.36] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

[i.37] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (directive SRI 2).

[i.38] Sasan Rostambeik, Noemi Simoni, Antoine Boutignon: "Userware: A framework for next generation personalized services", Computer Communications, Volume 30, Issue 3, 2007, Pages 619-629, ISSN 0140-3664.

[i.39] "OGC City Geography Markup Language (CityGML); Part 1: Conceptual Model Standard".

[i.40] "OGC City Geography Markup Language (CityGML); Part 2: GML Encoding Standard".

[i.41] The EU project iLocate.

[i.42] The EU project Assist-IoT.

[i.43] Waze.

[i.44] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (EU Digital Markets Act (DMA)).

[i.45] ETSI TS 102 165-2: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

NOTE: An update is in preparation to a CYBER document at the time of preparation of the present document.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

Architecture Communication Information Function Organization (ACIFO) model: framework for interpreting and analysing complex systems whole through the five dimensions that characterize it

artificial intelligence: ability of a system to handle representations, both explicit and implicit, and procedures to perform tasks that would be considered intelligent if performed by a human

avatar: representation of the user in digital form

digital ecosystem: network of interconnected digital technologies, platforms, and services that interact with each other to create value for businesses and consumers and facilitate access to digital technology for everyone

machine learning: branch of artificial intelligence concerned with algorithms that learn how to perform tasks by analysing data, rather than explicitly programmed

reinforcement learning: form of machine learning where a policy defining how to act is learned by agents through experience to maximize their reward; and agents gain experience by interacting in an environment through state transitions

semi-supervised learning: form of machine learning where the data set is partially labelled. In this case, even the unlabelled data can be used to improve the quality of the model

supervised learning: form of machine learning where all the training data is labelled and the model can be trained to predict the output based on a new set of inputs

unsupervised learning: form of machine learning where the data set is unlabelled, and the model looks for structure in the data, including grouping and clustering

User Platform as a Service (UPaaS): userware developed according to the "aas" model

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

aaS	as a Service
ACIFO	Architecture Communication Information Function Organization
AI	Artificial Intelligence
API	Application Programming Interface
AR	Augmented Reality
DaaS	Device as a Service
DAC	Discretionary Access Control
DMA	Digital Market Act
DTP	Data Transfer Project
E2E	End-to-End
eIDAS	electronic IDentification, Authentication and trust Services
EUDI	EU Digital Identity Wallet
GDPR	General Data Protection Regulation
GIS	Geographic Information Systems
HMI	Human Machine Interface
IaC	Infrastructure as Code
ICT	Information & Communications Technology
IoT	Internet of Things
MAC	Mandatory Access Control
ML	Machine Learning
NaaS	Network as a Service
ODA	Open Distributed Architecture
OSH	Occupational Safety and Health
PaaS	Platform as a Service
PPE	Personal Protective Equipment
QoE	Quality of Experience
QoS	Quality of Service
SaaS	Software as a Service
SAREF	Smart Applications REFerence ontology
SCS	Smart Customized Service
SOA	Service-Oriented Architecture
SUMA	Smart Urban Mobility Assistant
UDR	User Digital Representation
UIS	User Information System
UML	Unified Modelling Language
UPaaS	User Platform as a Service

4 Smart Customized Services for UIS

4.1 Identification of the problem to be solved

Users of digital services have historically had limited ability to control the use of personal data by digital services and how a service shares that data with other services, nor is there usually fine-grained control of what is given in terms of personal data, rather there is often a "share all" approach to how data is released. Whilst users are protected by a number of legislative instruments (see clause 6 and Annex D, for a broad summary of these instruments), the control is often passed to the service provider and the user is often not directly involved in the way in which their data is used or how a service is composed from component services. Whilst there are a number of technical means to restrict the personal data given to a service, e.g. by selective disclosure as outlined for eIDAS [i.27], [i.28] and the EU Digital Identity Wallet (EUDI) in ETSI TR 119 476 [i.31], or by application of specific permutations of a user profile following the approach of ETSI TS 103 486 [i.32], there are wider implications and requirements that are considered in the present document that seek to empower the user's control of personal data.

NOTE 1: In the eIDAS2 regulation [i.28] it is stated in Recital 59 that "*Selective disclosure is a concept empowering the owner of data to disclose only certain parts of a larger data set, in order for the receiving entity to obtain only such information as is necessary for the provision of a service requested by a user. The European Digital Identity Wallet should technically enable the selective disclosure of attributes to relying parties. It should be technically possible for the user to selectively disclose attributes, including from multiple, distinct electronic attestations, and to combine and present them seamlessly to relying parties. This feature should become a basic design feature of European Digital Identity Wallets, thereby reinforcing convenience and the protection of personal data, including data minimization*".

Addressing only the user's data and its selective disclosure is not sufficient, rather the services that are offered to, or built by the user, also have to be cognizant of the problems that users face in having assurances of the protection of personal data, including data minimization whilst maximizing the conveniences of the digital ecosystem. To this end the present document expands the idea of user by considering the user as an information system (the User Information System (UIS)) in the context of Smart Customized Services (SCS). In this respect it is noted that the concept of user centric design is well established in many industries and describes an approach wherein products and services are explicitly developed around the user. This does not imply bespoke design and manufacture, rather it allows the user to choose aspects of the way the service is presented and accessed, particularly in the ICT domain by personalization of user interfaces. By allowing for greater control of how data is used and how services are constructed using the UIS/SCS model the user is afforded control of, and maintenance of, their personal autonomy. The userware (see [i.38]) is then a means of allowing the user to explicitly control their autonomy within the provision of services.

The role and purpose of SCS is to place the user at the centre of their own digital ecosystem as the UIS (i.e. allows users to have control of their autonomy), being a virtual representation of the user's preferences as an information element and active entity. The UIS in SCS is therefore a persistent digital object in the service domain, representing an intelligent agent of the user (i.e. as an AI-enabled avatar acting as the user).

SCS and UIS together extend and develop prior concepts of users being represented as information elements in order to allow users to maintain control over their data and more generally their own information system in the way that they present themselves to services and more generally online.

In order to support SCS/UIS a number of system pre-requisites have to be met. The primary pre-requisite is that service components are considered as always available and are able to semantically and contextually identify themselves. It is also expected that service components exhibit the following characteristics (these are expanded upon in clause 7 of the present document):

- **Statelessness:** Each service should be able to process requests without retaining any request-specific or contextual information. Operations should function independently of prior invocations.
- **Autonomy:** Services should execute their functionalities independently of each other.
- **Loose Coupling:** Connections between services should be flexible rather than rigid and not require functional dependency on any other service.
- **Cohesive:** Services should be logically coherent and self-contained (see also autonomy).

- **Abstract:** The internal service logic should remain abstracted from external environments (i.e. independent of).

NOTE 2: The term user in the present document is not intended to only refer to a human user but may include a service using other services.

NOTE 3: Services can have multiple characteristics, they may be information services or interactive services, and if a composition of services results in a new service then it is the composition that is referred to as the service.

In addition to the technical pre-requisites identified above there is an attestation in the present document that there is a consumer demand for more control of services (demand chain), and a matching willingness on the part of providers to meet that demand (supply chain).

The smart component is identified as an AI element and applies intelligence to ensure that services are configured and personalized only where the required data from UIS is appropriately acquired and curated (see ETSI TR 104 221 [i.15] for a wider examination of the role of data in machine learning).

The UIS model and its realization in the management of services with SCS expands the models from each of ETSI TS 102 747 [i.11] and ETSI ES 202 746 [i.12] to have a persistent user profile able to interact with multiple services. This is shown in Figure 1 as a Venn diagram where SCS lies at the intersection of these 3 technological design paradigms:

- User centric design:
  - Addressing Quality of Experience (QoE) aligned to Quality of Service (QoS).
- Societal digitization:
  - Addresses the increasingly important role of digital devices and their use to connect to services for business, entertainment and governance representing a digital ecosystem.
- Automation:
  - This includes the evolution of smart systems and the application of AI in various forms.

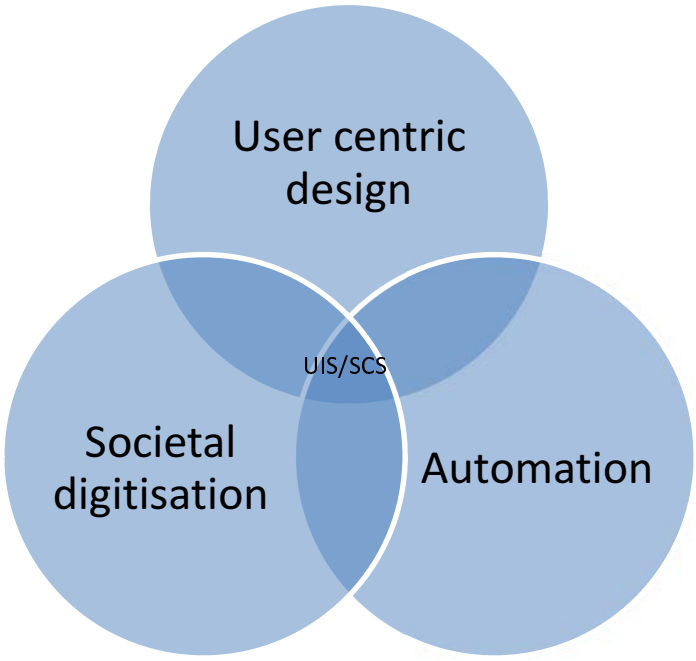

Figure 1: Intersection of domains that identifies the role of SCS

Whilst one outcome of loosely controlled release of personal data is that of digital alienation, it is also clear that current best practices such as for the EUDI [i.31] are not often as widely implemented as would be required to give the same quality of experience across all user interactions with the digital world with regards to the use of personal data that would mitigate threats such as those of digital alienation [i.30].

4.2 Application of the ACIFO model in SCS

The Venn diagram of Figure 1 is expanded first into the model given below in Figure 2 which illustrates the role of elements of each domain on SCS. In the context of Smart Customized Services (SCS), personalization is not limited to the adaptation of content or functionality to an individual. Analysis, through the ACIFO model, shows that it also results from organizational choices regarding data processing and governance, which dynamically adapt to the evolving user context and preferences. The layering that results is: Serviceware where the Platform as a service providers exist; Networkware that provides the necessary connectivity; and Userware where user-centric services exist (see Figure 2).

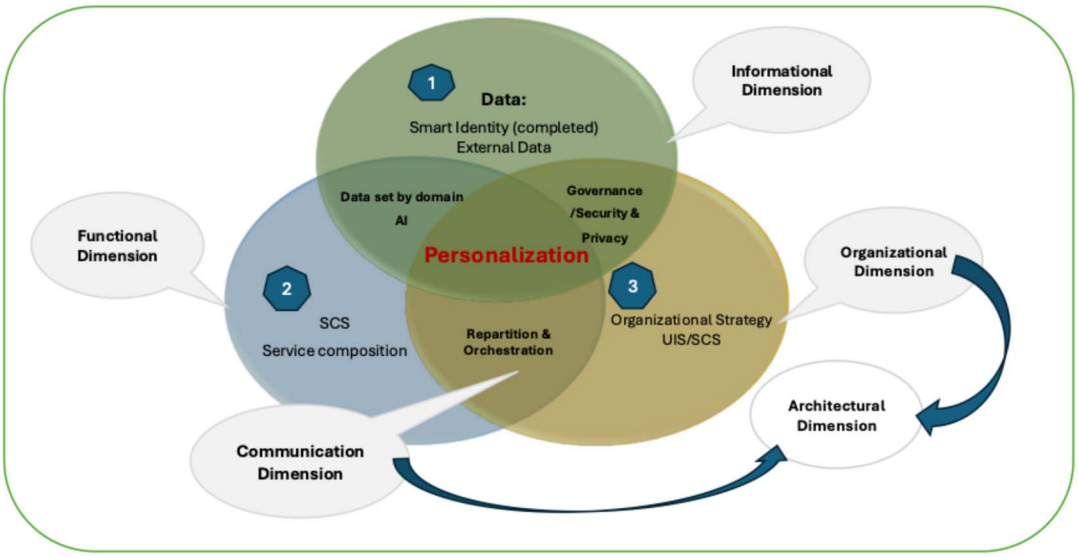

Figure 2: User Centric Approach: Personalization

SCS can be further developed using the 5-dimensions of Architecture, Communication, Information, Function, Organization (ACIFO) in the ACIFO model described in ETSI TR 103 438 [i.1], ETSI EG 203 602 [i.2], ETSI TR 103 603 [i.3], ETSI TR 103 604 [i.4]) examined in detail for the UIS/SCS environment in clause 7. In particular recommendations for application in a service centric environment are addressed in clause 7.1, and recommendations for application in a user centric environment (e.g. userware) are addressed in clause 7.2 of the present document:

- Architectural Model: defines the global structure, including semantics and is optimized for the stated objectives.
- Communication (Relational) Model: defines the exchange protocols, including HMIs (User) and APIs (provider) exchange and management protocols over three planes: (1) Management (Monitoring), (2) Control, and (3) Usage.
- Information Model: defines the different Profiles (User, device, service). The information covers the whole ecosystem (equipment, network, applications, services, HMIs, User, etc.) from the offer to the resource's availability for Users, Providers and any other partners. It is a knowledge data base representing the whole ecosystem.

EXAMPLE 1: In the present document the information model is the UIS, which includes all of the user preferences and contextual knowledge.

- Functional Model: defines services and service composition. The functionalities (the process) to compose any service based on "micro-service".

EXAMPLE 2: In the present document the functional model requires that functions are available using the "as a Service" model.

- Organization Model: defines the role of any actor and which actor is responsible of each action. ("Who is doing what?" in terms of responsibility for processing and data governance).

The particular use of ACIFO in the present documented is augmented by application of the ZT-Kipling criteria from ETSI TS 104 102 [i.17] which gathers knowledge of every interaction of the user (as UIS) with the system components (via the SCS) by requiring answers to the following questions on each use: What?, Why?, When?, How?, Where?, and Who? Whilst the application of [i.17] primarily impacts the Communication and Information elements of the ACIFO model, the consequence is that each of the other elements of the ACIFO model (i.e. the Architectural, Functional and Organizational elements) have to be designed in such a way that the ZT-Kipling criteria can be fulfilled.

NOTE: The ACIFO approach does not infer a specific order of addressing the dimensions but for the purposes of the present document are presented in the order of the acronym.

5 Use cases for User Information Systems

5.1 Introduction to use cases for UIC and their service composition

The present document adopts the model given in ETSI TR 103 477 [i.18] where it is stated that use cases are developed to examine problem statements that are a concise description of issues that need to be solved in the context of the use case. The purpose of the use case is to clearly describe:

- What the problem is.
- Who has that problem i.e. who will benefit when it is solved.
- What are the consequences of the problem.
- What a possible solution would be, this sets the expectations and the scope of the solution (is it a new process, an application, etc.).

In the context of standardization the problem is multi-fold but is primarily concerned with determination of interoperability. This may be at the application level where syntactic and semantic coherence is critical, or at any of the layers of the OSI stack (see ISO/IEC 7498-1 [i.33]). For communications interoperability the main concerns are to give assurance of connectivity, of routing (i.e. the ability of devices to connect in order to provide reliable transport of information from source to sink), and of mutuality of transfer rates (i.e. to ensure that data produced at a given rate can be consumed at the same rate). The purpose of the use cases given in the present document are to identify common requirements of UIS and SCS. The uses cases identify multiple functions to build relatively complex systems, although it is recognized that such systems (e.g. the urban mobility use case) are extensions of how users typically interact with the transport systems of their local environment, the potential of UIS/SCS to accelerate interventions and to act "in the loop" is identified by the use cases that follow. The use cases are presented to show how they impact different forms of user (in the form of actors in the use cases), and what information is required from and between actors to enable the use cases. It is noted that for most use cases there is a rational decomposition into multiple use cases.

Each use case identifies the actors in the use case, the principal interactions and the expected output in terms of the role of UIS and SCS. The use cases are drawn using the conventions of the Unified Modelling Language (UML) [i.26].

NOTE: The UIS/SCS is modelled as an UML Class for the present document but may be modelled in other ways.

The generalized use case model of UIS/SCS is given in Figure 3 where each actor manages their preference set as UIS, and creates SCSs which combine the data from the UIS of the actors with the microservices available.

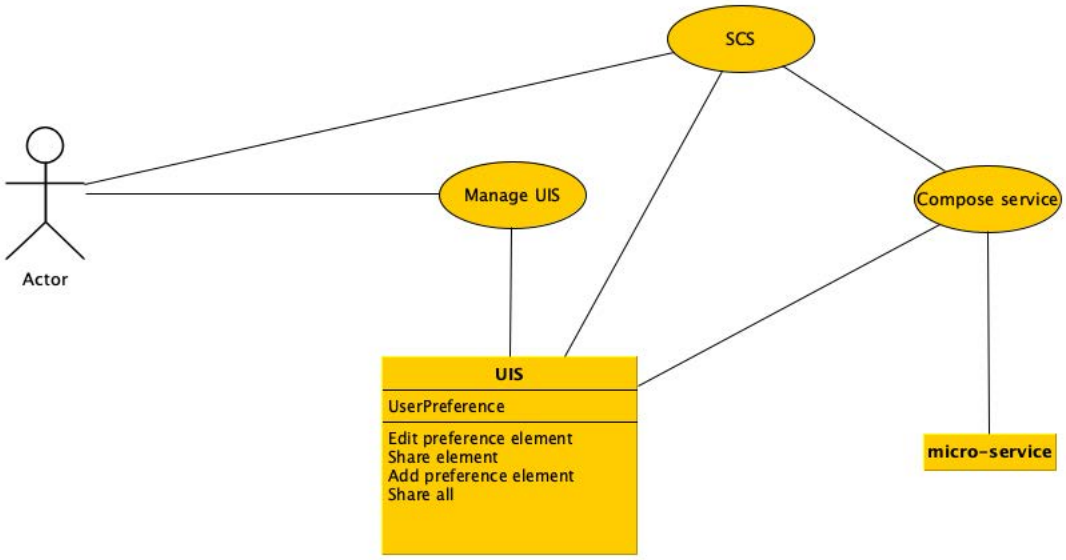

Figure 3: Generalized use case model of UIS/SCS

The services used in SCS via the Compose Service use-case are micro-services that have the characteristics outlined in clause 4.1 above.

In all cases it is assumed that the user controls which elements of the UIS are released, and that critically, the UIS has a means of selective disclosure available natively.

5.2 Urban mobility use case (Smart Urban Mobility Assistant)

Taking the general model suggested in clause 5.1 above the following outlines the role of SUMA.

- What is the problem that SUMA seeks to solve in the UIS/SCS context?
  - Existing methods of determining an optimized personal travel plan are deficient in addressing in-depth the personal preferences and context of the user. SUMA seeks to optimize the selection and integration of travel modes for each individual, in terms of time, cost, or environmental impact. It considers user preferences and the context: schedules, weather, traffic disruptions, etc. Thus SUMA facilitates user-optimized and personalized multi-modal urban travel (i.e. by the most effective mix of foot, bus, metro, car, or bike) whether for work, leisure, shopping, health, school, social relations, etc.
- Who has that problem i.e. who will benefit when it is solved.
  - The primary affected user is the person travelling. In addition having more knowledge of the real travel requirements and the preferences and contexts in which travel solutions are required may be of benefit to providers of travel solutions in optimizing their service composition and delivery.
- What are the consequences of the problem?
  - The primary consequence at the heart of SUMA is in data collection and processing. The following data is collected and processed:
    - **Personal data:** (taken from the UIS and augmented on request of the service). As not all personal data of the user is required the user consents to selective disclosure of only part of the UIS dataset (e.g. the user's calendar or diary, health information (where such data has a consequential impact on routing and accessibility (e.g. permanent or temporary disability), subscriptions to specific service providers in the context of SUMA).
    - **Transport offer data:** transport offer including prices and timetables.
    - **Cartographic data (GIS):** Geographic Information to enable route visualization and route calculation.

- **Contextual and environmental data:** weather, air pollution, connectivity…

- In addition to the data collection consequences of SUMA the following specific functionalities are embedded:
  - **Route calculation:** the route calculation finds and proposes a path depending on the availability of the transport offer, the user's preferences, and the environment (e.g. the user may set preferences for any of the fastest or shortest or least expensive routing taking into account the current context (i.e. things that impact the plan such as congestion, industrial action and so forth)).
  - **Notifications and alerts:** departure notification, guidance notification, recommendations, subscription renewal.
  - **guidance:** information regarding direction to take step by step.
  - **Recommendations on the way:** possibility of partnership with businesses or services present on the route and able to meet needs of the user identified in the agenda for example.
  - **Subscription management:** bus, metro, parking, self-service bike or vehicle…
  - **Statement: finance, health, environment:** a reporting in term of expense, health, impact environment.

- What a possible solution would be?
  - The wider deployment of user centric "as a service" components in the transport domain.

The user preferences for SUMA are taken from the UIS and SUMA as a whole represents an instantiation of the SCS model.

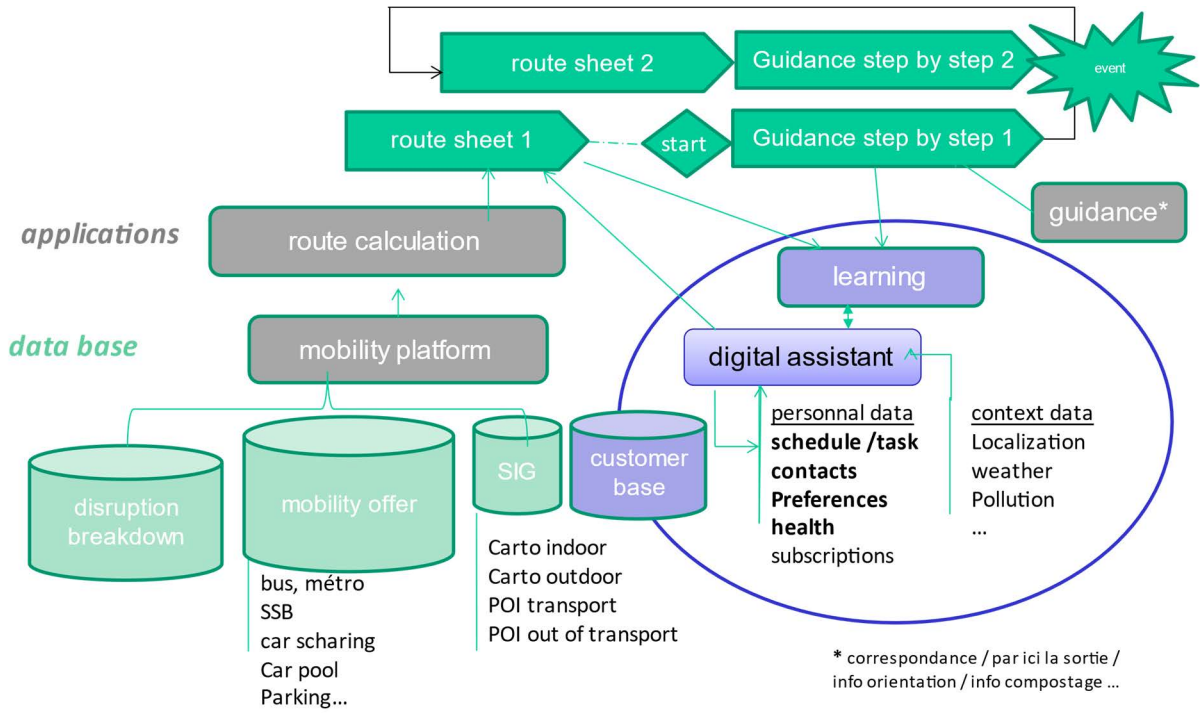

Figure 4: SUMA data and functional architecture

A specific example within the SUMA use case is given below.

EXAMPLE: The user has arranged a visit involving a flight from London's Heathrow airport, to Nice in order to attend a working meeting of an ETSI Technical Body. The public knowledge of this enables significant contextual information to be gathered, e.g. the meeting schedule, the airline schedule. In addition SUMA is aware of the starting point of the visit (the user's home), the user's preference for travel mode, and so forth. SUMA can then identify travel options at each point of the intended journey, suggest options for guard time (e.g. to change train platforms, or travel modes). SUMA can also ask for additional information, such as how much luggage the user is taking (that may assist in determining if public transport is viable for the pre- and post-flight travel).

From the available information SUMA recommends that the user is taken to a local London Underground station by a family member (SUMA has access to the shared family calendar and can request verification that this is reasonable) to take a combination of tube lines to Terminal 5 (from knowledge of which airline is being used SUMA can determine which airport terminal to use).

During the journey SUMA identifies a potential problem with the initially planned route and recommends a change of route and advises on the change in expected time of arrival, alongside the impact of remaining with the initially planned route. In this case the initially planned route is not viable so the user accepts SUMA's recommendation.

At all times SUMA monitors the overall travel progress, and if required can give feedback to friends and family - in this case to keep the user informed that the family member is safely home again after the drop off, and to also inform that same family member whenever a major phase of the journey is complete.

NOTE 1: The EU project i-Tour [i.21] addressed many of the core topics of the urban mobility use case as personalized multi-modal route planning and is summarized in Annex B.

NOTE 2: The i-Tour project [i.21] contains descriptions of a number of other, closely related, use cases.

NOTE 3: The use of Augmented Reality (AR) to assist in visualization of routing instructions in an urban environment, based on the wide availability of CityGML [i.39], [i.40] modelling of the built environment can be found in EU project i-Locate ([i.41]) and a summary can be found in Annex C.

5.3 Agriculture

Taking the general model suggested in clause 5.1 above the following outlines the role of UIS/SCS applied to an instance of an agricultural problem.

- What is the problem that UIS/SCS seeks to solve in the agricultural context?
  - Agriculture faces significant challenges, including climate change, resource depletion, water scarcity, and a rising global demand for food. To address these issues, the digitalized farm leverages real-time, data-driven decision-making to optimize crop yields, reduce risks associated with diseases and climatic hazards, support farmers in making precise and personalized decisions tailored to their specific conditions, and enable effective market integration to anticipate demand and plan harvests accordingly.
- Who has that problem? i.e. who will benefit when it is solved.
  - **Farmer:** Responsible for the daily use of the system, monitoring crop progress, checking alerts and recommendations, and implementing suggested actions. The farmer remains the final decision-maker and adjusts interventions according to their goals and constraints.
  - **Logistics provider (in both supply chain and demand chains):** Manages the supply chain for inputs (seeds, fertilizers, equipment) and the delivery of harvested crops to markets that are determined in advance by giving assurance of demand to encourage supply.

- What are the consequences of the problem?
  - Smart Customized Services (SCS) can dynamically compose and orchestrate features tailored to the specific needs of a user and their operational context. In agriculture, they enable solutions to be customized according to the specific characteristics of each farm, the farmer's preferences, and local environmental constraints. In order to operate successfully the following are added to the system:
    - **Connected sensors:** Continuously measure environmental and agronomic parameters (temperature, humidity, pH, light, nutrients).
    - **AI engine:** Analyses data, detects risks and opportunities, and generates forecasts.
    - **Digital farm (Digital Twin):** Virtual representation of the farm, integrating static and dynamic data.
    - **Smart interface:** Allows the farmer to visualize information, receive alerts, and interact with the system through the userware.
    - **Service Component Provider:** Supplies services that can be composed either by the Agronomist Expert or by the Farmer.
    - **Agronomist expert (E2E specialized service provider):** responsible for validating and optimizing AI models. It assesses prediction accuracy, adjusts algorithms if necessary, and ensures that recommendations provided to the farmer are reliable, relevant, and tailored to the context.
  - At present personalization (AI model & service composition) is carried out by the agronomist expert. Applying UIS/SCS will give the farmer more autonomy, allowing them to perform this service composition themselves by directly accessing the service provider's APIs.
- What a possible solution would be?
  - The digitalized farm implements a continuous cycle of data collection, analysis, and action to assist the farmer in the daily management of crops or livestock. Data from sensors is aggregated in the digital farm and analysed by an AI engine, which translates the results into targeted recommendations that the farmer can apply immediately. The actions taken, along with their observed effects, are then fed back into the Digital Twin, allowing future forecasts to be refined and recommendations to be continuously adapted to real field conditions:
    - Anomaly detection and identification of environmental trends.
    - Image analysis to assess tomato ripeness.
    - Automated diagnosis of leaf and fruit diseases.
    - Yield prediction based on historical and real-time data.
    - Visualization of results via interactive dashboards and visual indicators.
    - Agronomic recommendations for irrigation, harvesting, and plant protection treatments.
    - Issuance of intelligent alerts and notifications for optimal responsiveness.
  - In addition the UIS/SCS centred solution would be able to add the following:
    - **Preference management (UIS)**
      The farmer sets preferences in the UIS, such as humidity thresholds, yield objectives, and alert frequency. The farmer selects the corresponding IoT devices.
    - **Data collection & Analysis**
      Sensors continuously monitor temperature, humidity, soil pH, light intensity, and nutrient levels. The collected data is securely transmitted to the Digital Farm (via secure APIs), where it is analysed and processed to produce valuable and useful insight.

- **Analysis and detection (SCS + Serviceware)**
  The SCS orchestrate the available micro-services (humidity analysis, weather analysis, tomato maturity detection).
  The specialized service provider validates the AI models and provides advanced analyses, such as early disease detection and irrigation optimization.

- **Agronomic recommendations**
  The SCS translates the results into concrete recommendations—for example, irrigate more in the northern zone and plan the optimal harvest in five days. These recommendations are sent to the farmer via the intelligent interface.

- **Yield prediction**
  By combining historical and current data, the SCS estimates the total volume of tomatoes to be harvested.

- **Feedback and continuous learning**
  On the planned day, the farmer harvests the tomatoes. Yield and health data are fed back into the Digital Twin and SCS to improve the accuracy of future forecasts.

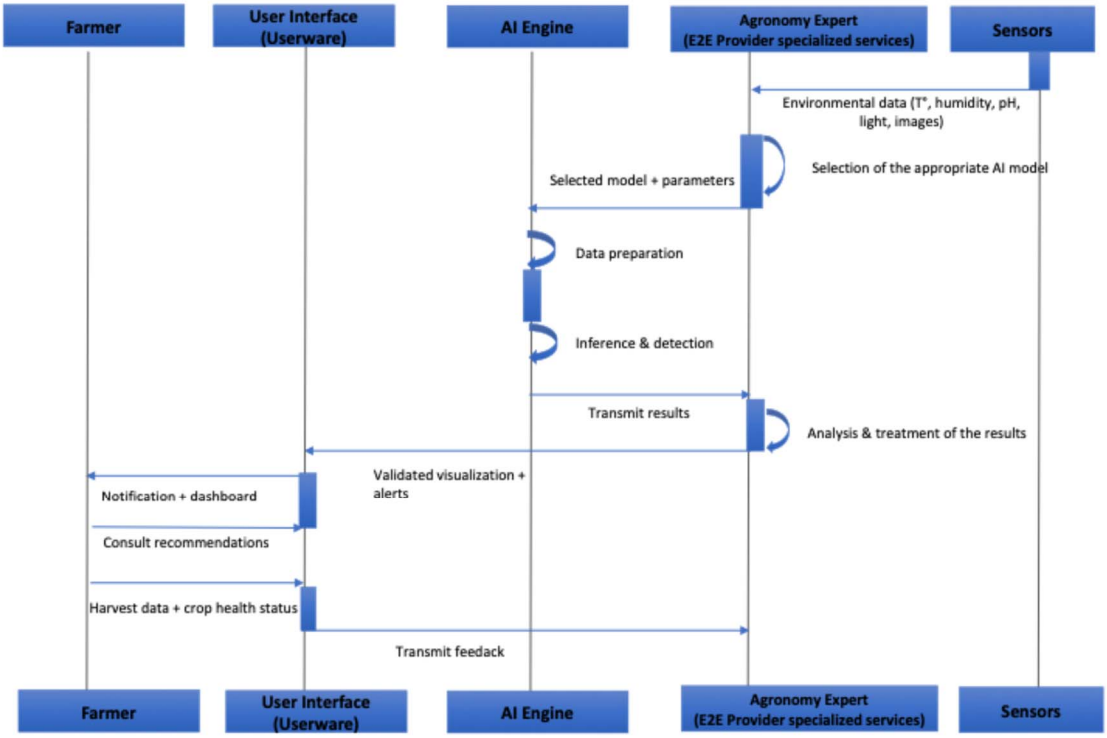

Figure 5: An example of UIS/SCS applied to tomato cultivation

In analysing the agriculture use case as above the role of personalization and autonomy identifies that in the current scenario, personalization (AI model & service composition) is carried out by the expert. To give the farmer more autonomy, they should be allowed to perform this service composition themselves by directly accessing the service provider's APIs and the text above relating to the consequences of the problem).

5.4 Health

ETSI TR 103 477 [i.18] identifies use cases and actors for each of diagnostic and therapeutic interventions. The present document extends the characterizations from [i.18] with many of the actors being present as persistent AI entities in the health system. Thus applying the use case purpose identified in [i.18] to the UIS/SCS enabled eHealth environment identifies the following:

- What the problem is.
  - The data relating to the health of an individual is not in the control of the individual and may not be readily available during triage, diagnosis, treatment and recovery. Without significant personal data used in a diagnosis the diagnosis and subsequent treatments may be invalid. Personalized healthcare is rare and often expensive even if the core data can be obtained at low cost (both financially and in terms of convenience). Without reasonable control of how data is shared the benefit of ICT enabled healthcare may not be realized.
- Who has that problem i.e. who will benefit when it is solved.
  - The healthcare support to a patient needs often deep and wide knowledge of a patient in order to make an accurate diagnosis. Whilst short term triage may fix an obvious problem it is not a full diagnosis. Thus whilst fixing the effect of a fall is good, it would be better to have access to health records that may identify an underlying problem that led to the fall.
  - The primary beneficiary is the patient but a wider community of beneficiaries include the healthcare providers, and society in general. Early access to health related data and its analysis may lead to early prevention of health and wellness issues.
- What are the consequences of the problem.
  - Increased digitization of health records with wider, controlled, access rules applied to assure user control as far as is possible.
- What a possible solution would be, this sets the expectations and the scope of the solution (is it a new process, an application, etc.).
  - In eHealth for much of the time the patient is represented by their health record which for the present document is considered as the root of the UIS, with the various diagnostic and therapeutic interventions acting as the SCS.

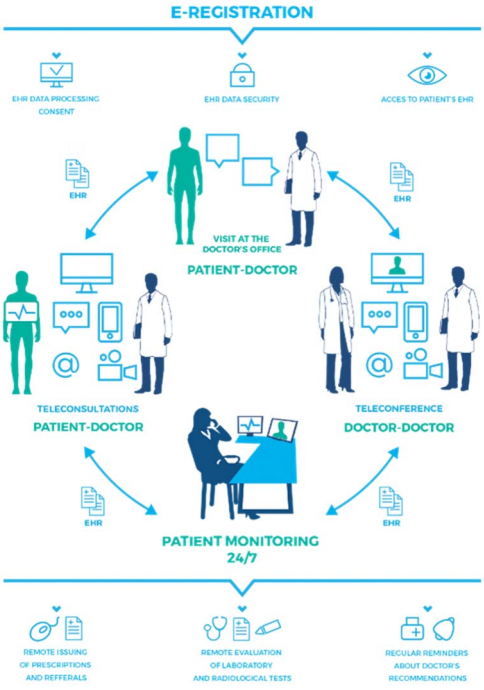

Figure 6: Electronic health record

5.5 Assurance of Health and Safety in an IoT enabled construction environment

NOTE 1: This use case has been derived from information contributed by the ASSIST-IoT project in their deliverable D3.2 [i.19].

NOTE 2: A summary of the ASSIST-IoT project [i.42] is given in Annex A of the present document.

Using the same schema outlines in clause 5.1 above the following is declared for this use case.

- What the problem is.
  - Within any building construction site, a large number of people with various levels of training and experience, from several subcontracted companies, are required to interact with each other, operate equipment or interface with heavy machinery.
  - It is necessary that all construction workers wear appropriate Personal Protective Equipment (PPE). The relevant PPE is risk assessed and is unlikely to be the same for all workers on a site. Verifying the correct use of PPE at each point in a site is difficult if the verification is dependent on only human verifiers, and may not be practical if the appropriate PPE for a remote work area is different from the PPE required at the inspection point.
  - All access points are securely locked and the construction workers and plant have been registered with the main contractor. Smart devices and wearables are paired together in order to monitor the construction worker's status, e.g. wearing all PPE or operating construction plant.
- Who has that problem i.e. who will benefit when it is solved.
  - The actors and their primary interactions are shown in Figure 7 and Figure 8 below.

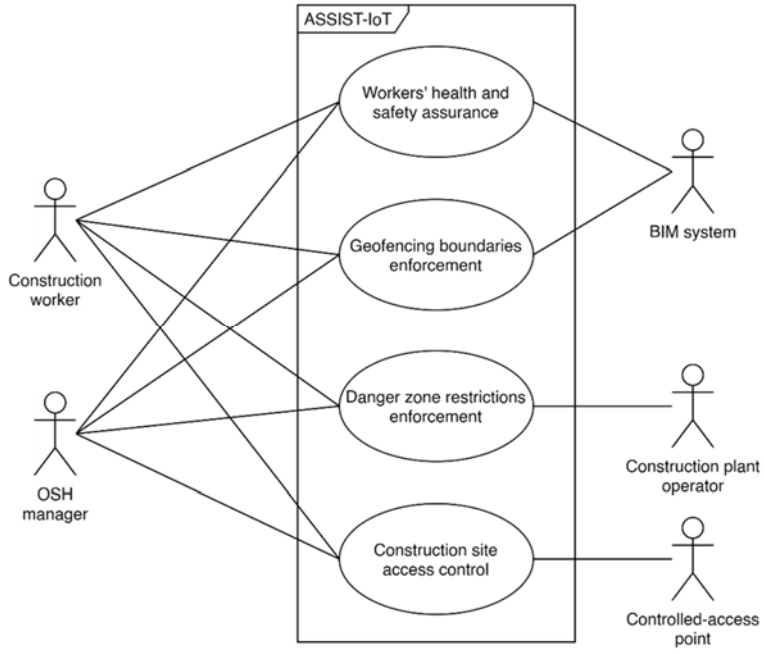

Figure 7: Illustration of occupation safety and health monitoring

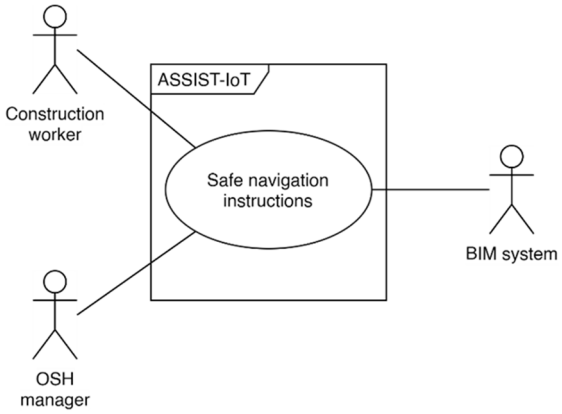

Figure 8: Illustration of safe navigation instructions

- What are the consequences of the problem.
  - The first responders are promptly notified about the occurrence, nature and location of an emergency and rescue the construction worker who is in danger.
  - The UIS/SCS platform needs in this instance to geo-aware and to have knowledge of the applicable Occupational Safety and Health (OSH) regulation.
- What a possible solution would be, this sets the expectations and the scope of the solution (is it a new process, an application, etc.).
  - Collecting reliable and relevant information in order to generate intelligent insights for the protection of all individuals present at any worksite within a large construction site can demonstrate the viability of UIS/SCS in gathering personal, industrial and contextual data to ensure that the user and any liable party is protected from inappropriate use of Personal Protective Equipment (PPE).

6 Regulatory and other constraints that may apply to UIS/SCS

6.1 Data governance

In giving user control, where the user is disassociated from the service by their persistent entity, their User Digital Representation (UDR), in the network, the user has to have assurance that the data gathered, exchanged and processed on their behalf is trustworthy.

There are many discussions of trust, and models of trust, that may apply to SCS. The concept of trust can be addressed by the application of methods such as those described in ETSI TS 104 102 [i.17] where based on the answers to a set of questions (who, what, where, when, why, how) knowledge is acquired of the entity that is to be trusted, and based on the answers and local policy a decision to trust or not can be made.

The definition of trust as "*confidence in the integrity of an entity for reliance on that entity to fulfil specific responsibilities*" and for the purpose of the present document this definition requires that each element in the SCS chain, and the services they provide has to be able to generate sufficient proofs or evidence to give assurance of that trust.

In some instances trust can be delegated to a third party as in the models used in eIDAS [i.27], [i.28] for Trusted Service Providers (see [i.29]). In all instances for SCS the primary requirement is to be able to satisfy the policy set by the user for the assignment of responsibility to a remote agent.

In order to build up the necessary context to give assurances of the trustworthiness of elements of SCS/UIS the requirements for transparency of explicability of AI processing defined in ETSI TS 104 224 [i.16] and by the application of the core questions from the ZT-Kipling method (ETSI TS 104 102 [i.17]) to the data and service. An example of the application of these approaches is given in Annex E.

6.2 Privacy and data protection

The UIS/SCS has to conform to societal expectations of privacy protection and to also conform to any legal restrictions. To achieve this some security capabilities are required (shown in more detail in clause 7.2 below), and it is expected that the overall system conforms to expectations of the GDPR [i.20] or equivalent national or regional legislation outside of the EU.

A further consideration of UIS/SCS is that it is assumed that there are multiple services and therefore the data subject is likely to be represented by a proxy (see also considerations for accessibility in clause 6.5.

A wider concern of applying existing data protection legislative frameworks to the UIS/SCS case is that consent may become unclear and therefore the UIS/SCS governance model has to accommodate the UIS/SCS acting somewhat independently of the user.

EXAMPLE: In the SUMA use case whilst a query may be anonymized for any particular phase of a journey, an observer, which may be the UIS/SCS itself, may be able to single out the user even if the UIS itself is a protected element of the system.

Article 20 of GDPR [i.20] in particular for the UIS/SCS context suggests a framework for the practice of the right to data portability, that data subjects have the right to receive data in a structured, commonly used and machine-readable format. It is not intended that the user should just receive an overview or summary of their data. The goal of portability is to be able to reuse personal data immediately (or later) by integrating it onto another platform or service.

The following general characteristics for machine readable data should therefore be applied to all UIS/SCS data and to the use of data in associated services:

- Reliability
- Authenticity
- Integrity
- Usability

The consequence of applying these characteristics is that, in addition to the appropriate semantic and contextual labelling (see clause 6.4 below), some attention is paid to data provenance.

Contrary to ad hoc downloads, APIs can enable continuous real-time data portability and thus the smooth interoperability of the different actors, their technologies and services. In addition, data holders can implement several restrictions via APIs to better control the use of their data, including by enabling access based on the identity of API users, and the scale and scope of the data used. Also, a dedicated API may reduce the perceived necessity of 'data scraping' which requires users to grant third parties access to their online account to extract the data from the online interface and, in some cases, to execute transactions on the customer's behalf. Such activities may violate data holders' terms of use or the IPRs of third parties. Data portability regimes that take advantage of APIs may in this way increase the security of, and trust underpinning, data transfers while minimizing the risk of copyright violations.

An example implementation of this data portability implementation is the Data Transfer Project (DTP) which is an open-source initiative which features data portability between multiple online platforms. [i.22] It provides a platform that allows individuals to move their online data between different platforms, without the need of downloading and re-uploading data. The ecosystem is achieved by extracting different files through various available APIs released by online platforms and translating such codes so that they are compatible with other platforms.

Further analysis of the impact of privacy regulations on UIS/SCS is given in Annex D of the present document.

6.3 Security

In regulatory terms there are a large number of instruments in place that serve to lower the risk to users of actions they take online. These include the Cyber Resilience Act [i.36], the Network Information Security Directive [i.37] and many of the other legislative instruments that address privacy and the content of data have an implicit, sometime explicit, set of security requirements. An analysis of the regulatory impact of security on UIS/SCS is given in Annex D.

6.4 Data semantics and ontology

The process of data portability, and of data interoperability, can be enabled by assuring that data is described semantically and to which a context can be attached, This requires that data has been structured to add meaning to it. In common practice an ontology is used to explicitly define the concepts and relationships within a domain, allowing machines to understand the data's semantic structure and to enable them to perform complex operations on it.

EXAMPLE: The Smart Applications REFerence ontology (SAREF) framework of ontologies for IoT that enables different parties to interoperate with each other at the semantic level [i.23] The common concept of SAREF is that all existing data models/protocols can be incorporated into an ontology (i.e. a common vocabulary). This captures the meaning of a concept (i.e. semantics) rather than the specific data format in which the concept is encoded for data exchange at the underlying communication layer. For this to work manufacturers and service providers should enable their data to be portable as it enables interoperability.

6.5 Accessibility

Any implementation of UIS/SCS should comply with the European Accessibility Act [i.5], a legal instrument that aims to improve the functioning of the internal market for accessible products and services by removing barriers created by divergent rules in Member States. A detailed review of the impact of [i.15] and related legislation on UIS/SCS is given in Annex D. The present clause highlights those actions applicable to UIS/SCS.

The SCS should conform to EN 301 549 [i.6], which can be applied to ICT-based products and services. Also applicable to the SCS is ISO 9241-210 [i.7], which provides requirements and recommendations for human-centred design principles and activities throughout the life cycle of computer-based interactive systems. It is intended to be used by those managing design processes and is concerned with ways in which both hardware and software components of interactive systems can enhance human-system interaction.

There are existing standards which provide for user profiles including:

- ETSI EG 202 116 [i.10] gives guidance to ICT product and service designers on Human Factors issues, good Human Factors design practices, and relevant international and national standards. The guidelines are intended to encourage a "Design for All" approach to making products and services accessible to as many people as possible, including elderly people and persons with disabilities, without the need for adaptation or specialized design.
- ETSI TS 102 747 [i.11] defines an architectural framework supporting the personalization and user profile management concepts.
- ETSI ES 202 746 [i.12] specifies a set of user profile preferences and information settings for deployment in ICT services and devices for use by ICT users and suppliers.

The concept of a user profile usually refers to a set of preferences, information and rules that are used by a device or service to deliver a customized version of capabilities to the user. In practice, most devices and services contain profiles specific to that product and unrelated to any other. This requires that, on change of service or device, the user has to re-educate themselves in how to personalize their services or devices and re-enter their information and preferences. This often results in variable success rates and user satisfaction.

6.6 Ethics Considerations

With SCS enabling highly personalized experiences for consumers the advent of AI-driven personalization presents opportunities to improve user engagement and experience. However, this gives rise to concerns and issues about the ethical use of AI, potential risks and hazards, and the need for suitable safeguards to protect the rights and well-being of consumers, although AI has a vast amount of promise (for example see [i.13]), the codification of such protection is addressed in the seven key requirements provided by the European Commission concerning the adoption of trustworthy artificial intelligence solutions (see the EU TAi Guidelines [i.14]). Table 1 below considers the alignment of each category with such requirements.

Whilst it is reasonable to suggest that any developer has to ensure that their product does not give rise to an ethical dilemma it is not reasonable to define ethical constraints in a standards environment. However in ETSI the wider requirements of [i.14] are addressed in the work programme of TC SAI [i.34].

NOTE: In ETSI a general decision has been made not to define any standards for ethics as ethical behaviours are not codifiable, rather many of the consequences of ethics are addressed in ensuring accessibility (see clause 6.5 above), and in ETSI's codes of conduct for members that are available in ETSI Directives [i.35].

Table 1: Concerns and Solutions in AI-Powered Personalization

Category from [i.14]	Main Contribution	Significance	Recommendations
Privacy and Data Security (Requirement #3)	Emphasizes the importance of protecting individuals' personal information when using AI for personalization. It addresses the risks of data breaches and unauthorized access, advocating for robust data protection measures and compliance with privacy regulations like GDPR.	Ensures that consumers' privacy rights are respected and their personal data is secure, fostering trust and preventing misuse.	Data Minimization Anonymization and Encryption Regular Audits Incident Response Plan Federated Learning
Algorithmic Bias (Requirement #5)	Highlights the potential for AI algorithms to perpetuate or amplify existing biases in the training data, leading to discriminatory outcomes. There are frameworks for identifying and mitigating these biases to ensure fair treatment of all consumer groups.	Promotes fairness and equality by preventing biased recommendations and exclusionary targeting, which can have adverse societal impacts.	Bias Detection Frameworks Human-in-the-loop Transparency Reports Bias Mitigation Techniques Diverse Training Data Federated Learning for Bias Reduction
Consumer Manipulation (Requirements #1, #3)	Examines the ethical concerns related to the potential manipulation of consumers through hyper-personalization. It is about how AI-driven personalization can exploit behavioural data and psychological insights to influence consumer behaviour.	Protects consumers' autonomy and agency by ensuring that personalized practices do not unduly influence or manipulate their decisions.	Ethical Design Principles for example informed consent User Feedback Mechanisms Behavioural Data Safeguards Transparency in Personalization for example using explain ability tools. Ethics Training for developers
Social Repercussions (Requirement #6)	Explores the broader societal impacts of AI-powered personalization. It emphasizes the need for supportive policies and programs to mitigate these risks.	Addresses the long-term societal implications of AI technologies.	Community Engagement Sustainability Initiatives Ethical AI Certifications
Transparency and Accountability (Requirements #2, #5)	Stresses the importance of transparency in AI systems to understand how decisions are made and to identify potential biases and errors. It calls for accountability mechanisms to assess the ethical implications of AI driven personalization.	Enhances trust and accountability by making AI decision-making processes more transparent, allowing for better oversight by users, policymakers, and regulators.	Explainable / Explicable AI Audit Trails Regulatory Compliance Third-Party Audits User Education for example explain how AI systems impact them

7 Recommendations for further specification of ACIFO in SCS

7.1 General requirements for the Digital Ecosystem

7.1.1 Overview and introduction

The digital ecosystem (see Figure 9), is given as a digital representation of "reality", independent of applications, and is built on the following characteristics:

- Core paradigms:
  - "softwarization/programmability" (software-defined infrastructure, APIs, IaC);
  - the "as-a-service" operating model (platform thinking with DaaS/NaaS/PaaS/SaaS); and
  - pervasive "virtualization" across E2E continuum.
- Autonomy by design (AI + IoT).
  - The combination of AI and IoT shifts the ecosystem from merely automated to autonomous: systems that sense, decide and act.
- Capability-driven governance (e.g. ODA).
  - Use a capability framework to describe what the organization should do to achieve desired outcomes.

Implication for the userware: the userware could be engineered as an autonomous, context-aware layer that orchestrates services on the user's behalf.

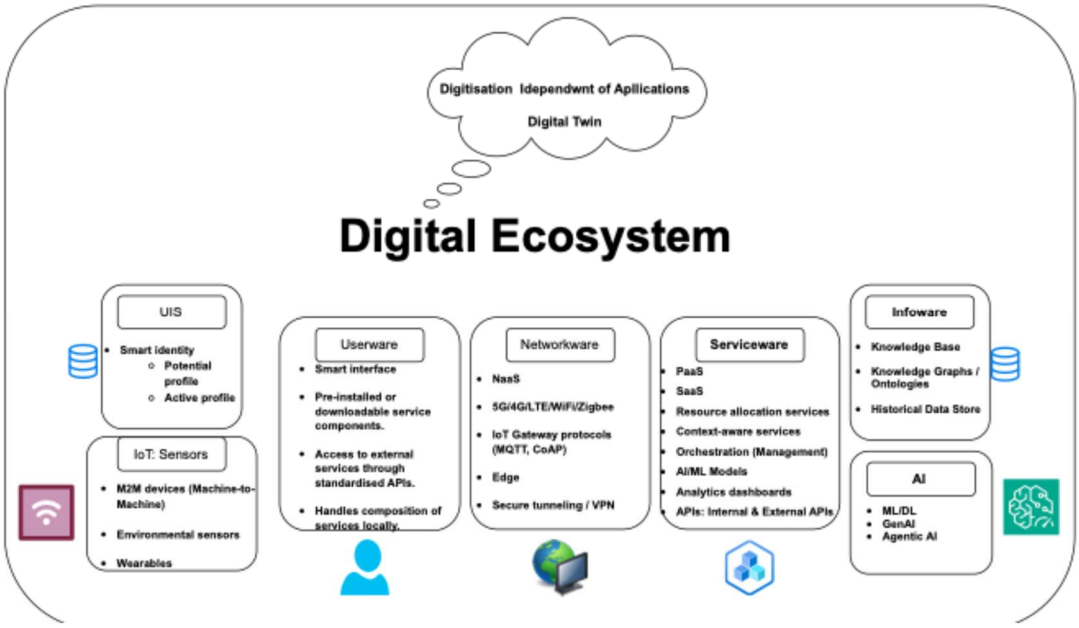

Figure 9: Generic Architectural Components of a digital ecosystem

The application of the fundamental questions of the ZT-Kipling method (ETSI TS 104 102 [i.17]) to the ACIFO dimensions are explained below.

Table 2: Application of ETSI TS 104 102 [i.17] in ACIFO Dimensions

ACIFO Dimension	ZT-Kipling questions (from [i.17])					
	What	**Why**	**How**	**Where**	**Who**	**When**
Architecture clause 7.1.2	What is the Overall Structure?	Why is this architecture designed this way?	How is the overall architecture structured?	Where does the ecosystem operate and its components reside?	Who are the key actors involved in the ecosystem?	When does the architecture's life-cycle occur?
Communication clause 7.1.3	What is the communication type?	What is the intent or purpose of the communication?	How are communication protocols and patterns implemented ?	Where do communications flow?	Who selects and manages the communication protocols?	When are communication protocols and parameters designed, implemented, and managed?
Information clause 7.1.4	What is the data?	Why is that data (in particular) chosen?	How is the data used?	Where is the data? (logically and geographically)?	Who owns and is liable for the data ?	When is that data meant to be available?
Function clause 7.1.5	What services and capabilities does the ecosystem provide?	Why is this function considered value added?	How are the services build and deliver ?	Where is the function activated?	Who activates, controls and manages every function?	When is the function activated?
Organization clause 7.1.6	What are administrative domains regulating the digital ecosystem?	Why this organization?	How do entities collaborate within this organization?	Where are the organizational entities of the ecosystem located?	Who does what (roles and responsibility)?	When does the organizational structure evolve?

7.1.2 The architectural dimension

The architectural dimension defines the overall structure designed to achieve predefined objectives. This structure is characterized by specific properties, and compliance with the architecture implies adherence to these properties, making any architecture inherently semantic.

The overall system architecture integrates both its logical components (i.e. software) and its physical infrastructure (i.e. Equipment, Topology) following the "as a service" model.

The digital ecosystem relies on components that provide:

- Transparency of Access: Users should be able to interact with local or remote components seamlessly and uniformly across the architecture.
- Transparency of Location: Users should not be required to be aware of the physical or logical placement of components within the architecture.
- Transparency of Concurrency: Components can be simultaneously shared or invoked by multiple users.
- Transparency of Scalability: The system can be expanded or reduced without disrupting user experience.
- Transparency of Faults: Users remain unaware of error-handling processes, with the system ensuring consistent service quality.

This approach to the architecture design inherently implies a distributed architecture in terms of both processing and data management.

- The logical architectural blocks of a digital ecosystem are organized into two primary views:
  - The User View; and
  - The Provider View.

- The User View represents all components that directly interact with the end-user. This includes:
  - Userware, UIS, IoT, Smart Interface, and their supporting components.
- The Provider View includes the components that deliver services and manage data on the backend:
  - Serviceware, Infoware, AI.

This approach to the architecture domain optimizes the structure and aligns to the strategic and business goals of the deployment (e.g. Green Computing, QoS-based, Privacy-based). This is then achieved by further adoption of an Open Distributed Architecture (ODA) to achieve goals of openness and distribution that in turn encompass the intended goals of transparency identified above.

The digital ecosystem's architecture is oriented toward a "user-centric" model, that pre-supposes that the services are always available irrespective of the format of the user's device and of the user's location. To achieve this, the architecture is expected to be able to transparently handle complexity, ensuring at minimum transparency in terms of access, location, concurrency, scalability, and fault tolerance.

Addressing the ZT-Kipling criteria [i.17] in more detail reveals the following for the architectural dimension:

- Where identifies a number of administrative domains for various forms of service provider: Platform as a Service (PaaS), Network as a Service (NaaS), Device as a Service (DaaS), Software as a Service (SaaS), User Platform as a Service (UPaaS), with the internal and external qualifier that conforms to the main actor. There is no strict limitation to the nature of the architecture within the digital ecosystem, thus each of dew, edge, fog, cloud are equally valid.
- Who considers the actors, stakeholders, and owners related to the digital ecosystem and is primarily defined in the logical view and the business context , as it deals with roles, responsibilities, and interactions.
- When can be understood in three key architectural contexts:
  - "Think" is the most strategic view of time, that acknowledges that Architecture is not static, rather it evolves and as a consequence requires anticipation and planning to enable that change and adapt in the future.
  - "Build" describes the timing related to how the ecosystem is built, deployed, and maintained.
  - "Run" describes the temporal constraints and behaviours of the ecosystem while it is running and is a fundamental part of the logical and physical views.

7.1.3 The communication dimension

The UIS/SCS is expected to be a persistent object in the system and to interact with the "conventional" APIs that represent any component service's configuration and personalization entity with the added consideration that the UIS adopts a common exchange protocol (i.e. there is an expectation that each component service's configuration and personalization entity is accessed by a common service level protocol (e.g. HTTP/S using JSON (self-defining) data structures).

The communication defines the different communication protocols and interactions of the service components. The UIS/SCS is expected to be a persistent object in the system and to interact with the "conventional" APIs that represent any component service's configuration and personalization entity with the added consideration that the UIS adopts a common exchange protocol (i.e. there is an expectation that each component service's configuration and personalization entity is accessed by a common service level protocol (e.g. HTTP/S using JSON (self-defining) data structures).

In the context of Smart Customized Services (SCS), personalization is not limited to the adaptation of content or functionality to an individual. Analysis, through the ACIFO model, shows that it also results from organizational choices regarding data processing and governance, which dynamically adapt to the evolving user context and preferences.

The communication dimension defines how information is exchanged between the architectural blocks of the digital ecosystem. It establishes the protocols and models that govern all interactions, ensuring a clear and purposeful flow of data across the system. The application of ZT-Kipling [i.17] considers this in more detail below:

- What is the communication type that allows determination of the communication protocols in the different layers of the ISO model in relation to the different architectural blocks of the ecosystem. This can be further characterized:
  - "Conventional" or Open API.
  - Open API/AI should facilitate a zero-contact approach (no human intervention, everything is automated).
  - A protocol which facilitates the composition of services and fosters a dynamic and collaborative ecosystem.
- Why allows for the determination of the purpose or reason for the connection/communication link. It clarifies the semantic meaning of the interaction and nature of process as either an interactive or an automated process:
  - Is it a Command (telling a service to do something); or
  - a Query (asking for information); or
  - an Event (notifying that something has happened).
- How allows determination of the concrete methods and technologies used to implement the communication patterns and seeks to explain how the protocols are selected and configured to satisfy the system's technological constraints and architectural drivers.
- Where addresses the concern regarding direction and scope of communications flows. It therefore identifies the communication between every architectural block, ensuring that transmission and reception occur end-to-end (i.e. at both endpoints).
- Who helps to identify the person, team or AI agent that selects communications flow based on the available topologies and the requirements of the application. And who manages them? Internal and external network administrators.
- When is then understood in three key architectural contexts Think, Build and Run, in accordance with the architectural blocks. The communication parameters management are particularly crucial during the "Run" phase.

7.1.4 The Informational Dimension:

At the foundation lies **data**, which serves as the informational backbone of personalization. This dimension integrates:

- **Smart Identity:** Complete representation of users, i.e. **their potential profile** where their preferences are found, behaviour patterns and knowledge.
- **External Data:** Environmental conditions, service-related metadata, domain-specific datasets, and AI-enriched information.

Data in this context is **complete, contextualized, and enriched** through AI-driven inference and domain expertise. It defines the scope of personalization possibilities and dictates how services can be adapted to the user.

This knowledge base (UIS) becomes reactive through the "active profile", i.e. following the "context awareness" which encompasses a rich set of contextual factors, including temporal information (time, day of the week), spatial data (location, environment), device characteristics (smartphone, wearable, computer), social interactions (alone, with friends, in a meeting) and ambient environmental conditions (weather, traffic, noise level). This ubiquitous awareness is the main factor enabling the provision of relevant, fast and non-intrusive proactive services that fit perfectly into the user's life.

The Information Dimension provides a complete blueprint for all data within the digital ecosystem independent of applications. This includes defining the types and value of information managed by the system, clarifying why it is collected to generate insights, enable services, and drive business decisions. It also establishes clear frameworks for data's entire lifecycle, from when it is created, to how it is secured and managed, and where it resides. Ultimately, this dimension assigns accountability by identifying who owns the data and is responsible for its integrity, ensuring information remains a trusted and valuable asset:

- What: It is the digital representation of reality, independent of applications. The data in a digital ecosystem refers to the collection of discrete or continuous values that convey information. All entities in the digital ecosystem are represented as an intelligent data object.
- Why: Data is chosen based on its relevance to a specific purpose or research question. It should have sufficient be capable of answering the posed questions. Ultimately, data is chosen to create value, provide insights, and drive business decisions.
- How: Data is used in a multitude of ways, from basic input for computational processes to a source of insights for advanced analytics. In a broader sense, data is the foundation for creating information, knowledge, and intelligence, enabling tasks like machine learning, predictive analytics, and process automation.
- Who: Data ownership is a formal role that establishes accountability and liability for data integrity and management.
- Where: Data is stored both logically and geographically. Logically, it can be organized in a hierarchy from bits and fields up to files and databases. Cloud providers allow for data to be stored across different geographical regions and availability zones and exposed via APIs (Data portability).
- When: Data is available based on its storage lifecycle, which can be either ephemeral or persistent.

7.1.5 The functional Dimension

To ensure a seamless and coherent user experience, the functional dimension relies on SCS. The application is constructed following an as-a-Service composition model (see ETSI TR 103 437 [i.25], page 13), enabling service components to be independently added, removed, or composed without compromising the global service architecture. This model ensures customization, flexibility in service composition, adaptability of offered services, and on-the-fly deployment. Essential properties for this model are:

- **Statelessness:** Each service consistently processes requests without retaining any request-specific or contextual information. Operations should function independently of prior invocations.
- **Autonomy:** Services should execute their functionalities independently, without requiring interaction with other services or human intervention, effectively serving as "black boxes".
- **Loose Coupling:** Connections between services should be flexible rather than rigid, eliminating functional dependencies and allowing for adaptable service compositions. Users can thus dynamically modify service combinations to suit their specific requirements.
- **Cohesion:** Services are logically coherent and self-contained, delivering meaningful and consistent functionality recognized by potential users. Internally, each service's logic is cohesive and self-sufficient.
- **Abstraction:** Beyond basic service descriptions in catalogues and SLAs, internal service logic should remain abstracted from external environments.

For software engineering, the properties of reuse and mutualization are expected to be present:

- **Reuse:** Facilitates the development of new services by leveraging generic interfaces (usage, control, management), promoting efficient software engineering practices.
- **Mutualization:** Services should support multi-tenancy, allowing simultaneous access by multiple users, thereby reinforcing the loose coupling principle fundamental to Service-Oriented Architecture (SOA).

To enable effective SCS management, the properties of exposition, auto-control, and ubiquity are essential:

- **Exposition:** Involves cohesive service descriptions and registration in service catalogues, detailing functional and non-functional aspects, including inherent QoS, thereby enabling third-party actors to select or assemble services based on specific competencies and profiles.
- **Auto-control:** Services should autonomously monitor and control their behaviours, particularly non-functional aspects, using autonomic management approaches, thereby quickly identifying and managing component-level issues.
- **Ubiquity:** Defined as functional equivalence across multiple service components, ubiquity groups similar services providing identical functionalities and QoS, irrespective of underlying implementation details. This facilitates scalability, enhanced availability, redundancy, and quality of service management.

Services can be offered by various providers located anywhere, including integration within IoT gateways. Users compose or link these services to build applications tailored to their needs. With the rapid increase of IoT services, complexity grows correspondingly, necessitating stringent control, particularly in critical applications. Effective application composition and structuring require controlled service components, with end-to-end QoS management.

Transparency regarding failures (a micro-service property) is assured through comprehensive QoS monitoring, allowing faulty components to be seamlessly replaced by equivalent community components.

Each service component is conceived as a self-contained and reusable building block, comparable to a "packaged business capability." The fundamental principle of SCS is that complex, value-added user experiences are not pre-built, but dynamically composed by combining services in innovative ways. This composable nature allows the system to be "personalized" and to adapt its functionality to the user's specific context in real time.

Indeed, intelligent personalized service marks a fundamental departure from traditional reactive service delivery models. It is conceptualized not as a static application, but as a dynamic and intelligent composition, designed to anticipate and proactively respond to user needs. SCS is designed to go beyond the traditional request-response cycle. Based on the "active profile," it actively offers services and makes suggestions based on a deep understanding of the user's predicted intentions and the current context. This involves implementing systems capable of "predictive assistance" and anticipating user needs before they are explicitly expressed.

NOTE: SCS integrates existing services to the UIS as the proxy of the user and the SCS entity may build new services from existing system capabilities that are orchestrated by the user's profile and preferences represented by the UIS.

The Functional View defines the core capabilities and services the ecosystem provides. It focuses on the processing logic and specific actions the system performs to fulfil its purpose, ultimately providing a clear understanding of the tangible value delivered to users and other systems. Applying the ZT-Kipling criteria [i.17] in more detail to the functional dimension reveals the following:

- What: The "What" is the service map, which represents the digital ecosystem's processing capabilities.
- Why: In a collaboration context, each provider offers specific aaS components (value-added), knowing that all the core services are reusable.
- How: Built with as-a-Service properties and exposed via APIs. Service delivery (all-inclusive) is a composition of services. DevOps practices or low-code platforms (within an agile approach) can accelerate service creation.
- Where: In a virtualized context, activation is location-agnostic.
- Who: Based on responsibilities and organization, there could either be: One Provider, or a collaboration of Providers or the user (see clause 7.2).
- When: It defines the workflows and triggers that initiate a function, a scheduled event, or a system event.

Functions are executed by Userware on user-side devices, by IoT devices on the network's edge, and by the provider's Serviceware within their data centres. This distribution allows for optimization based on factors like latency, scalability, and data proximity, reflecting the shared nature of execution in the digital ecosystem.

7.1.6 The Organizational Dimension

The organizational dimension determines data responsibility, where, and how data is processed and stored, spanning the dew, edge, fog, and cloud continuums. The key elements of this process are:

- Data Governance: Establishing control mechanisms to manage data integrity, access rights, and retention.
- Security and Privacy: Ensuring user data security, trust boundaries, and user consent policies (see clause 6).
- Strategic Resource Positioning: Determining the optimal processing location based on defined governance.

Applying the XT-Kipling criteria [i.17] assists in defining the role of any actor and clarifying which actor is responsible for which action:

- What: This describes the interconnected set of digital assets and services that form the ecosystem based on the strategy. Ways of working and governance: Identify the roles and responsibilities of each architectural block and all other entities within the digital ecosystem. Personalization (UIS/SCS) is the responsibility of serviceware or userware [i.38].
- How: How the entities collaborate within the Digital Ecosystem.
- Where: The location of the architectural organizational entities: "Where are entities (SCS) and enabling platforms located?". This defines the distribution of entities for all actors, including users and providers.
- Who: "Who is accountable and who enables delivery?" This identifies all the entities participating in the ecosystem. architectural blocks, Engineering leadership, platform leads, security/compliance, and community leads for standards and skills. Personalization could be achieved by serviceware or userware [i.38].
- When: "When is each of planning, monitoring, and auditing done?".
- Why: The organization model is chosen for effective management and to ensure that all stakeholders are considered. It answers the question "Why this organizational model matters ?" by providing the strategic rationale (personalization UIS/SCS). This model is designed to align strategy to execution, improve throughput and reliability, and scale delivery with predictable quality and controlled risk.

7.2 UIS/SCS requirements User side (userware)

7.2.1 Userware Interactions with the ecosystem components

To outline and highlight indicative requirements of UIS/SCS on the user-side within a digital ecosystem, the organizational model should define "who does what", according to the user's chosen autonomy level (see "the cursor" [i.25]).

The userware and its interface should make simple and explainable controls, exposing what actions are taken on the user's behalf while honouring consent and preferences. It should also ensure data control and sharing: users retain their data, grant purpose-bound access to providers at their discretion, and can review or revoke that access at any time.

This is essential because today's users carry an ubiquitous network (smartwatch, smartphones, tablets, etc.) nearly invisible yet requiring coordination and management, which the userware provides.

Finally, the model specifies collaborative service composition with providers clear roles, interfaces, and responsibilities so user policies and preferences are respected end-to-end.

To fulfil this role and this type of collaboration, all the services necessary for the user could be in the userware (see Table 3) with the properties of autonomy, simplicity, security and reliability.

Table 3:UIS/SCS Requirement in Userware

Ecosystem Components from the Userware perspective	UIS General Requirement	SCS General Requirement
UIS (Smart identity)	• Provide the creation, control and management of potential profiles ([i.24], clause 4.3). • Ensure data distribution and sharing with proper control and management.	• Enable secure integration of profiles into service workflows. • Ensure interoperability of user identity across services. • Enable clear visualization through the smart interface.
IoT Sensors (M2M, environmental, wearables)	• Guarantee transparent data collection (in real time) with user configuration. • Ensure data is transmitted to the user profile.	• Ensure Sensor Management (synchronize, Configuration, encryption, trust environment, etc.). • Enable secure transmission to provider. • Ensure service reliability from heterogeneous sensor inputs.
Userware (smart interface, service management)	• Ease of Use: Provides data (knowledge) to the smart interface to enable an intuitive user experience.	• Provide seamless service discovery, and execution. • Provide simple composition of services.
	Autonomy Based AI: • Enable user to configure how AI process data. • Provide different levels of autonomy over Data.	• Enable selection of AI functionalities. • Allow local handling of preferences and composition of services. • Adapt services dynamically to user's context.
	Security: Ensure the properties of availability, integrity, and confidentiality.	• Enable protection of personal data in services(Encryption, anonymization, fuzzification, etc.).
	Reliability: Enable the properties of QoS, robustness, fault tolerance.	• Enable redundancy, pertinence.
Networkware (4G/5G, edge, VPN)	• Ensure the properties of availability, integrity, and confidentiality. • Ensure availability of data for continuous connectivity.	• Ensure availability and continuity of connectivity for user operations. • Guarantee secure and reliable communication between distributed services. • Enable Quality of Service (QoS) monitoring.
Serviceware (PaaS, SaaS)	• Allow users to filter or control access to personal data. • Ensure timely and understandable feedback on actions taken.	• Ensure reliable service execution and orchestration. • Provide secure and context-aware services.
Infoware (knowledge base, ontologies)	• Guarantee privacy parameters. • Guarantee compliance with data governance and retention policies.	• Support knowledge-driven orchestration for personalized services. • Ensure semantic interoperability across services.

Ecosystem Components from the Userware perspective	UIS General Requirement	SCS General Requirement
AI (ML/DL, GenAI, Agentic AI)	• Allow user control over how AI-based recommendations are applied. • Ensure transparency about AI model use.	• Guarantee ethical, explainable, and reliable AI-driven decision-making. • Continuously improve services using feedback loops. • Integrate AI/ML models into workflows while protecting user data. • Ensure fairness, privacy, and accountability in AI operations.

7.2.2 User Centric Vision

According to user-centric vision, a connected ecosystem is designed to deliver seamless digital services through multiple interacting layers (Figure 10).

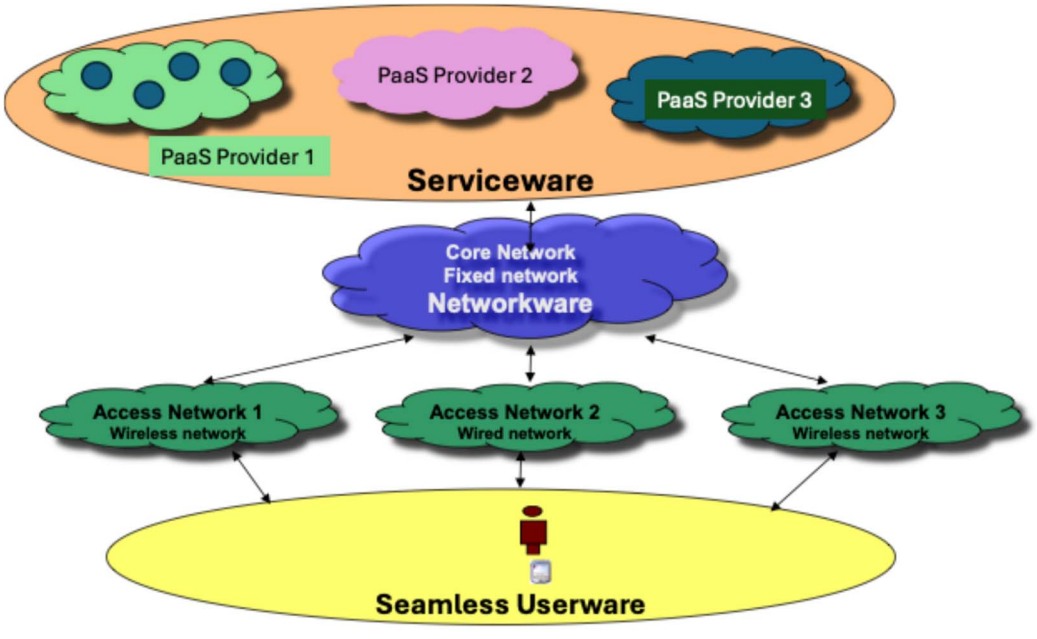

Figure 10: User vision of integrated ecosystem

Service providers offer digital services supported by an underlying network layer that ensures reliable connectivity. Access networks bridge users to these services, while the user layer enables personalization, real-time adaptation, and a smooth experience.

Annex A:
Assist-IoT project overview

NOTE: The description that follows is sourced from the Assist-IoT website [i.42] with additional editing to map aspects of the project to the requirements of UIS/SCS as outlined in the main body of the present document.

The ASSIST-IoT project addresses research for the design, implementation and validation of an open, decentralized reference architecture, associated enablers, services and tools, to assist human-centric applications in multiple verticals. ASSIST-IoT will design, implement and validate, in a realistic, measurable, and replicable way, a unified innovative multi-plane (semi-)autonomous decentralized edge-cloud reference architecture, supplemented by cross-cutting digital enablers. The architecture will support continuous integration and long-term sustainability of domain-agnostic, interoperable, capable, intelligent, distributed, scalable, secure and trustworthy IoT ecosystems.

Annex B:
i-Tour project overview

The i-Tour project of 2008/9 through to 2012 was predicated on the increasing success of navigation technologies, and the expected increase in the diffusion and acceptance of transportation services based on localization technologies. Widespread diffusion of novel info-mobility services promoting multi-modal transport were anticipated to have a profound impact on citizen's lives across EU, in terms of:

1) **Safety**, as 40 000+ people die on Europe roads each year with a cost for the European economy of approx. 200 B€ p.a.

2) **Efficiency**, as congestion costs an estimated in 1 % of EU total GDP or 100 B€ p.a.

3) **Environmental sustainability**, as transport accounts for 30 % of total energy consumption in the EU, with the vast majority being consumed by road transport.

At the time when i-Tour was proposed most of the relevant initiatives in multi-modal transport routing, whilst supporting routing through public transport networks, did not (could not) support personalization, in terms of user travel preferences, nor could they provide support of real-time information, nor did they promote an open approach based on common standards. Ideal route optimization has to take into account a complex set of conditions far beyond parameters such as travel times to include factors such as costs, preferred transport means, number of modality changes, pollution minimization, real-time public transport load (e.g. number of passengers currently on a given train), weather conditions (e.g. to suggest walking only in dry conditions). Further optimization at the travel information level has to take into account not only the current conditions but also the effects that the users of the system, as a community, infer on the traffic conditions themselves through new demand management strategies that account for the level of acceptance of the guiding system and adjust the overall system conditions accordingly.

The i-Tour project addressed the demand chain aspects identifying a need to support and promote sustainable and environmental-friendly travel preferences as essential. On the supply chain side the i-Tour project identified requirements to create ICT tools based on innovative strategies to promote clean transport based on rewarding mechanisms that can encourage sustainable travel choices. In addition the project identified that current (i.e. the year 2009 or so) data acquisition and distribution strategies, based on centralized authorities, needed to evolve towards distributed federated infrastructures whereby, through open architectures, providers can expose their services and benefit from those available within the infrastructure.

A large part of the i-Tour project thus addressed recommender systems as an early AI like approach to sharing experiences of the transport system (i.e. pre-dating more recent examples such as Waze [i.43]), and considered reward schemes to encourage use by consumers, and involvement of providers.

The i-Tour concept, although pre-dating UIS/SCS shares many of the characteristics:

- User as both consumer and provider of data.
- Recommender systems and other collaborative tools to share knowledge and experience.
- Micro-services composed into user services on demand.
- Strong support of open standards.

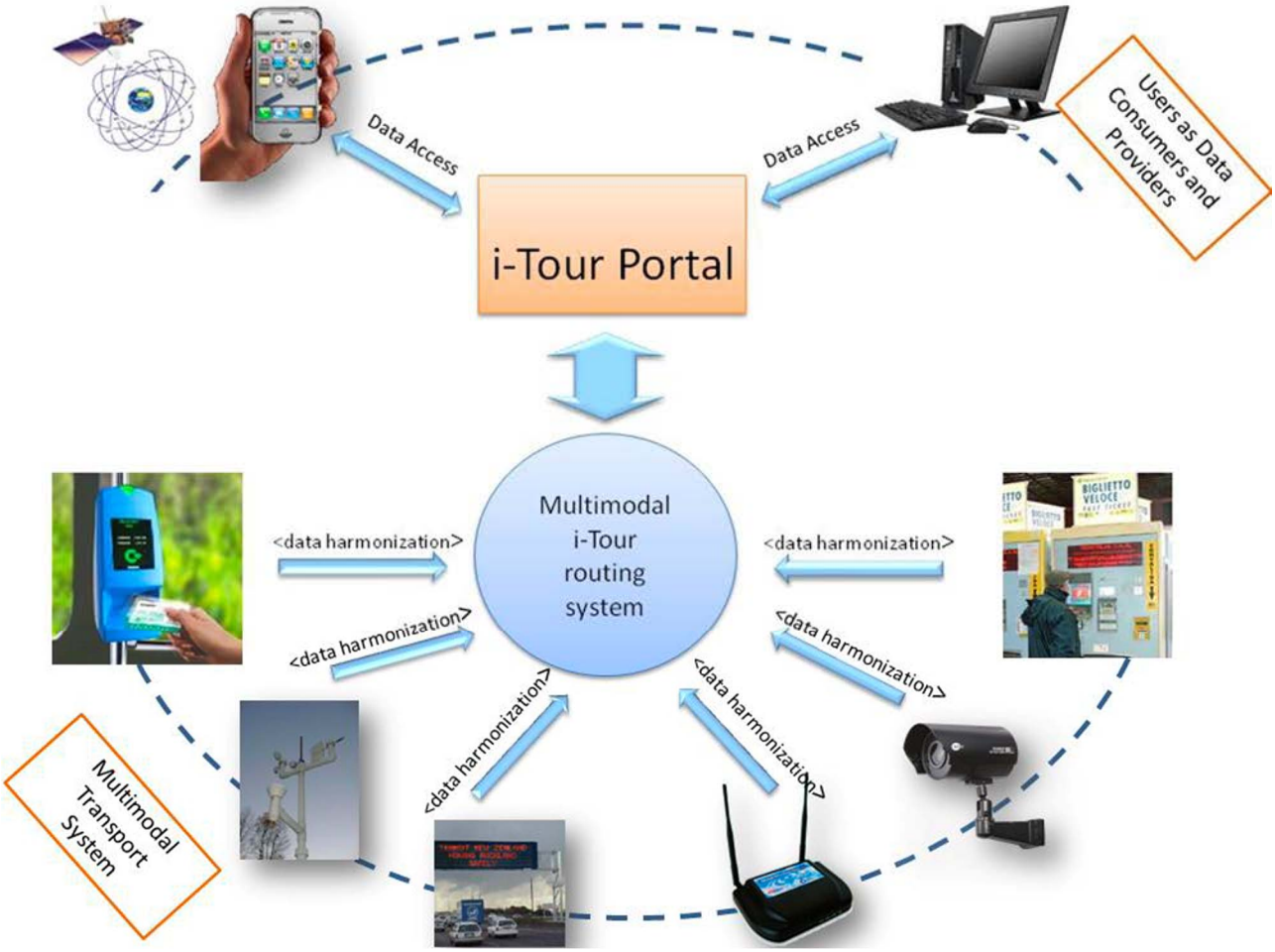

Figure B.1: Initial concept of i-Tour approach to the SUMA use case

Annex C:
i-locate project overview

The role of the i-locate project was to take advantage of the opportunities provided by increasingly accurate indoor localization technologies, for instance based on RFID (active or passive) or Wi-Fi®, to expand the scope of GIS to include indoor spaces (i.e. "indoor GIS"). The development of asset location and tracking technologies for integrated indoor and outdoor scenarios (the latter being typically GNSS-based, including Galileo), was seen as having the potential to be a key driver for innovation and business activities in several fields including -among others- logistics, facility management and retail. Improving location and tracking in the public health domain can bring to significant advantages in terms of improved quality of services and lower risks. A notable example of this can be found in Italy, where location of pharmaceutical products through labels, from production to sales at pharmacy, has allowed higher security and control well above average (0,1 % risk in Italy against 1 % in Europe and 6 - 7 % globally).

Modern hospitals and health care centres in fact are extremely complex systems of systems where efficient and accurate asset tracking and management is vital. The leading principles of today's integrated quality management procedures, predicate that each facet of a product or service provided is subject to continuous analysis and assessment. Ensuring open data access to asset information can be very beneficial to improve quality of services and reduce costs. It should be noted that, due to the sensitive nature of some of the data (e.g. personal health records) the open data nature of critical information only has to be limited to the boundaries of the health care systems.

Annex D:
Detail of regulatory factors to be considered in UIC/SCS

D.1 Privacy aspects

D.1.1 General overview

The UIS/SCS has to conform to societal expectations of privacy protection and to also conform to any legal restrictions. To achieve this some security capabilities are required (shown in more detail in clause D.2 below), and it is expected that the overall system conforms to expectations of the GDPR [i.21] or equivalent national or regional legislation outside of the EU. The UIS/SCS system has to be clear about the use of data particularly if the AI/ML model at the heart of UIS/SCS modifies the relative weighting of data elements. It is also shown that there are consequences of data export of anonymized data that may result in de-anonymized data if multiple datasets can be used by an AI/ML system to isolate characteristics of the data subject and to single out the data subject.

A further consideration of UIS/SCS is that it is assumed that there are multiple services and therefore the data subject is likely to be represented by a proxy (see also considerations for accessibility).

A wider concern of applying existing data protection legislative frameworks to the UIS/SCS case is that consent may become unclear and therefore the UIS/SCS governance model has to accommodate the UIS/SCS acting somewhat independently of the user.

EXAMPLE: In the SUMA use case whilst a query may be anonymized for any particular phase of a journey, an observer, which may be the UIS/SCS itself, may be able to single out the user even if the UIS itself is a protected element of the system.

D.1.2 Identification of Data Controller

The data controller in UIS/SCS is notionally the user as UIS/SCS acting for the user composes a service from micro-service elements, but the end user is not a formally recognized data controller in the meaning of GDPR. In UIS/SCS the data controller acts on behalf of the data subject.

NOTE 1: For SCS the user to data controller relationship is different from the conventional view as the user, through their representation as an AI-enabled proxy, is intended to be the lead determinant of data usage.

NOTE 2: There are aspects of liability for data misuse that apply to the data controller role and it is likely that entities offering micro-service components will have to address how they act in the context of UIS/SCS when subject to the legal requirements of GDPR.

D.1.3 Identification of Data Processor

The data processer acts on data as allowed by the data controller and the data policies of the data subject and is represented in UIS/SCS as the "as a service" entities that enable the user's service.

D.1.4 Identification of affected user (data subject)

The data subject is the entity on whose behalf the UIS/SCS acts.

D.1.5 Other privacy impacting aspects

Article 20 of GDPR [i.21], the "Rights to portability", gives the data subject (i.e. the affected user) the right to obtain and transfer their data to a different service, and the data controller should facilitate this transfer. This overlaps with Article 6(9) of the EU Digital Market Act (DMA) [i.44] and introduces a new data portability right which stipulates that gatekeepers have to provide end users and authorized third parties with "*effective portability of data provided by the end-user of generated through the activity of the end user*".

NOTE: Gatekeepers in the DMA are defined as having a significant impact on the internal market, providing a core platform service that is an important gateway for business users to reach end users, and enjoying an entrenched and durable position in its operations, or it is foreseeable that it will enjoy such a position in the near future.

While it does not adopt the term "right to data portability" the Data Act [i.18] instead, introduces a horizontal cross-sectoral data access right to consumers and businesses that encompasses "*data generated by the use of the product or related services*". This suggests that any AI manipulated data, or any augmented data is within its scope. It emphasizes the complementarity of this with the right to data portability in GDPR, including the right to receive personal data and to port data to other controllers. With regards to the scope of data covered, there is an overlap and some synchronism between the three Regulations: the GDPR regulates the processing of personal data, and the DMA and the Data Act include the processing of personal data and non-personal data by gatekeepers and IoT product manufacturers and services, respectively.

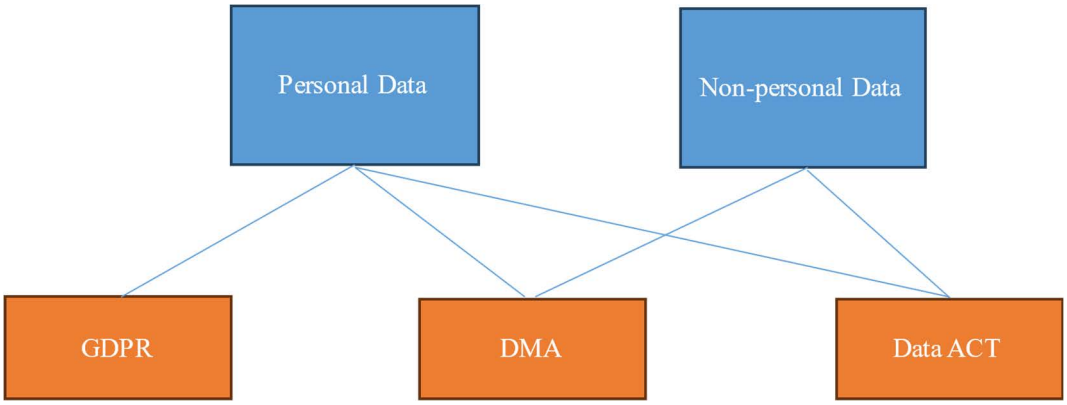

Figure D.1: GDPR, DMA and Data Act process personal and non-personal data

Focusing only on the right to data portability of personal data, the synchronized overlaps between the Regulations are modified. The GDPR has the smallest scope of the three Regulations since it is restricted to personal data that has been provided to a controller under the basis of consent or contract, whereas the DMA and the Data Act govern the processing of personal data independently of the lawful basis for processing, being cross-sectoral regulations that encompass different technologies, especially the Data Act, that has a broad scope of IoT technologies. Under the three Regulations, the GDPR covers all categories of personal data processors, and so has the broadest scope of the three. The DMA's scope is restricted to stakeholders who qualify as gatekeepers under the Act, and the Data Act's scope is restricted to IoT manufacturers and suppliers of related services, except for SMEs.

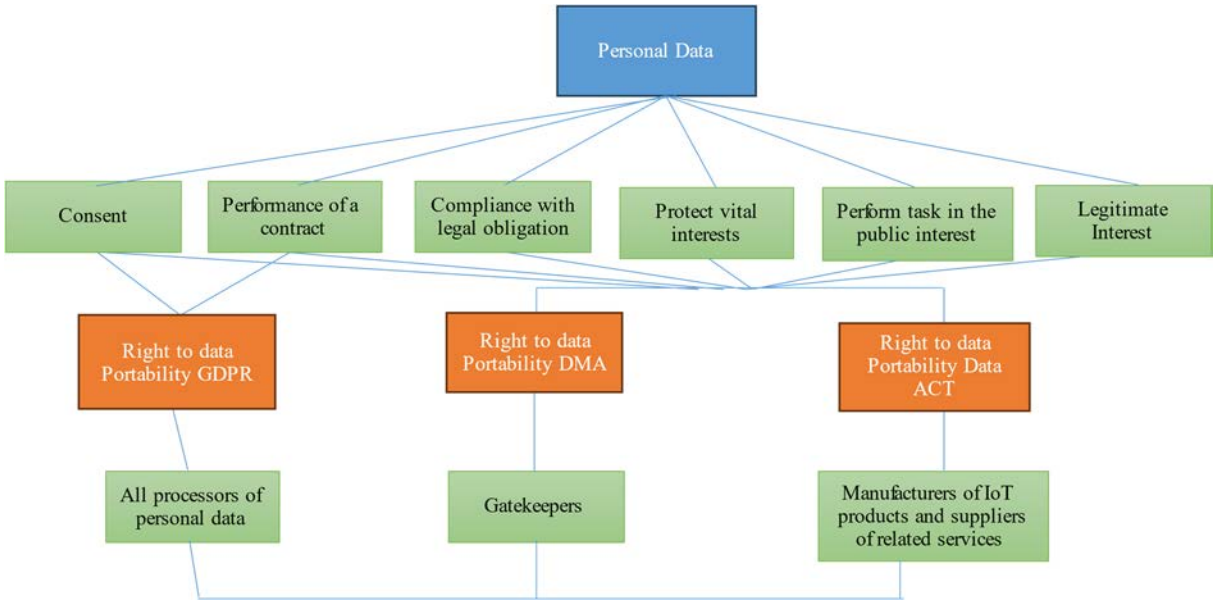

Figure D.2: Stakeholders affected by the different rights to data portability in the GDPR, DMA and Data Act

Within this multi-layered right to data portability, individual users potentially have more control over their data-both personal and non-personal-in the context of a multi-sectoral setting. This overlap is essential for UIS to function. Though at present there are a series of series of technical and legal interpretation-based obstacles that block its full implementation.

D.2 Security

In assessing the security requirement for SCS/UIS there are a small set of principles to be adhered to:

- Minimize the attack surface.
- Impose a principle of least privilege to allow the use of any asset.
- Impose a principle of least persistence for the use of any asset.

The general security provisions that apply to both privacy protection, and data protection, are those of least privilege and least persistence. In both cases the role of data minimization is critical. A number of approaches to this exist, and many require the detailed process of a privacy and data impact assessment exercise. This essentially requires that the technical design, and policy design, of a system determines the answer to a number of questions prior to, and in the execution of, a system.

NOTE 1: The principle of least privilege is one that has a very long history predating the ICT domain and embraces a number of concepts. The first of these is that an asset is of value and that things of value should not be shared to those not needing to have it, this then as a second concept introduces the idea that it is possible to determine who has the right to access, and this then extends to identifying the things that can be done with an asset and applying restricted rights to each of them. As an example, in the ICT domain a privilege may be one of read, edit, delete, or copy and a user may be granted one or more of these privileges. In summary least privilege access to a protected asset is to only allow those rights or privileges that are essential to perform the required task. In most access control systems that adopt least privilege the default is to deny (i.e. the least privilege is no privilege).

NOTE 2: Similarly to least privilege the concept of least persistence has a very long history that predates the ICT era. The concept of least persistence is that access to an asset is not granted forever, rather that access is granted for only sufficient time to perform the requested action. Least persistence is seen in most network systems where a resource is limited and shared (e.g. radio bandwidth, network capacity). Least persistence then ties into resource management as well as to security by taking steps to ensure that a resource is not hogged by any user.

In addition to the general principles of least persistence and least privilege the right to access data is further addressed by access control, for which a general model is given in clause 6 of ETSI TS 102 165-2 [i.45] addressing the technical means of achieving access control and the models of access control. In this there are two (2) primary models that are considered:

- Mandatory Access Control (MAC) - access to, and use of, the thing to which access is granted is wholly determined by the thing's owner.
- Discretionary Access Control (DAC) - the use of the thing to which access has been granted is at the discretion of the user and not addressed by the thing's owner.

In the UIS/SCS environment it should be assumed that the UIS base model is not changed without the knowledge and consent of the actual user it belongs to. Thus the relationship between the UIS and the services it enables through SCS is more likely to be of the MAC form than the DAC form in order to limit the release of personal data outside the controlled boundary.

NOTE 3: In some use cases, for example the Health use case given in clause 5.4, there are aspects of data held in the system that intersect with the core of UIS/SCS but are not persistent to the user view of UIS/SCS. In such cases access control requires a large degree of contextual awareness in order to ensure a service can be offered, particularly if withholding that service places the user at risk.

D.3 Data semantics and ontology

The process of data portability, and of data interoperability, can be enabled by assuring that data is described semantically and to which a context can be attached, This requires that data has been structured to add meaning to it. In common practice an ontology is used to explicitly define the concepts and relationships within a domain, allowing machines to understand the data's semantic structure and to enable them to perform complex operations on it.

EXAMPLE: The Smart Applications REFerence ontology (SAREF) framework of ontologies for IoT that enables different parties to interoperate with each other at the semantic level [i.23] The common concept of SAREF is that all existing data models/protocols can be incorporated into an ontology (i.e. a common vocabulary). This captures the meaning of a concept (i.e. semantics) rather than the specific data format in which the concept is encoded for data exchange at the underlying communication layer. For this to work manufacturers and service providers should enable their data to be portable as it enables interoperability.

D.4 Data portability

Article 20 of GDPR [i.20] suggests a framework for the practice of the right to data portability, that data subjects have the right to receive data in a structured, commonly used and machine-readable format.

Two transfer options are offered:

- Transfer of the data directly to the data subject; and
  - The user receives their data and is free to do what they want with it (c.f. discretionary access control (see clause D.2 above)).
- Transfer of the data from one controller to another.
  - The other service (that the user requested be sent the data) receives the data and can use it within their product.

The data controller has to make available to the user all the data that the user has provided either with their consent or through a contract and has to also include all the data resulting from their activity, in a machine-readable format, for example, a JSON, or RDF file. This is often done as ad-hoc downloads.

It is not intended that the user should just receive an overview or summary of their data. The goal of portability is to be able to reuse personal data immediately (or later) by integrating it onto another platform or service. So, for example, formats like PDF or XLSX files are not machine-readable data files, and they do not allow the transfer of the data to another platform or service as the file does not allow the user to reuse this data and is therefore in violation of their data portability rights.

NOTE: There is a distinction here between machine processable and machine readable, the latter requiring the data to have sufficient direct semantic and contextual labelling to assure correct processing.

The following general characteristics for machine readable data should be applied to all UIS/SCS data and to the use of data in associated services:

- Reliability
- Authenticity
- Integrity
- Usability

The consequence of applying these characteristics is that, in addition to the appropriate semantic and contextual labelling, some attention is paid to data provenance (see also clause D.3 above). For UIS real-time (continuous) data transfers between data holders should enable interoperability between the user-chosen digital services. This can be enabled by Application Programming Interface (APIs) which enable service providers to make their digital resources (e.g. data and software) available over the Internet [i.20].

Contrary to ad hoc downloads, APIs can enable continuous real-time data portability and thus the smooth interoperability of the different actors, their technologies and services. In addition, data holders can implement several restrictions via APIs to better control the use of their data, including by enabling access based on the identity of API users, and the scale and scope of the data used. Also, a dedicated API may reduce the perceived necessity of 'data scraping' which requires users to grant third parties access to their online account to extract the data from the online interface and, in some cases, to execute transactions on the customer's behalf. Such activities may violate data holders' terms of use or the IPRs of third parties. Data portability regimes that take advantage of APIs may in this way increase the security of, and trust underpinning, data transfers while minimizing the risk of copyright violations.

An example implementation of this data portability implementation is the Data Transfer Project (DTP) which is an open-source initiative which features data portability between multiple online platforms [i.22]. It provides a platform that allows individuals to move their online data between different platforms, without the need of downloading and re-uploading data. The ecosystem is achieved by extracting different files through various available APIs released by online platforms and translating such codes so that they are compatible with other platforms.

D.5 Accessibility aspects

Any implementation of UIS/SCS should comply with the European Accessibility Act [i.5], a legal instrument that aims to improve the functioning of the internal market for accessible products and services by removing barriers created by divergent rules in Member States.

These covered products and services include:

- computers and operating systems
- ATMs, ticketing and check-in machines
- smartphones
- TV equipment related to digital television services
- telephony services and related equipment
- access to audio-visual media services such as television broadcasts and related consumer equipment
- services related to air, bus, rail and waterborne passenger transport

- banking services
- e-books
- e-commerce

The SCS will include many of these products and services.

The SCS should conform to EN 301 549 [i.6], which can be applied to ICT-based products and services. This includes software (web pages, mobile applications, desktop applications, etc.), hardware (smartphones, personal computers, information kiosks, etc.), and any combination of hardware and software.

To that end, the requirements of the standard are self-scoping. This means they consist of two parts; the first part is a precondition for the second part, which holds the actual requirement. If a product or service meets the precondition, then the product or service has to conform to the second part of the requirement.

Also, applicable to the SCS is ISO 9241-210:2019 [i.7], which provides requirements and recommendations for human-centred design principles and activities throughout the life cycle of computer-based interactive systems. It is intended to be used by those managing design processes and is concerned with ways in which both hardware and software components of interactive systems can enhance human-system interaction.

It should also be noted that a designer can go beyond the requirements in EN 301 549 [i.6], these are design for all [i.8] and universal design principles [i.9]. This includes design principles such as:

- Provide the same means of use for all users: identical whenever possible; equivalent when not.
- Avoid segregating or stigmatizing any users.
- Provisions for privacy, security, and safety should be equally available to all users.
- Provide choice in methods of use.
- Eliminate unnecessary complexity.
- Provide compatibility with a variety of techniques or devices used by people with sensory limitations.

Design for all and universal design principles do go beyond what is required from current accessibility legalisation. They are ideal recommendations but not a requirement. Though they should be considered for the SCS for example if the user is colour blind, they should ideally need to only set one device or service to account for their colour blindness and any linked devices or services should copy or be able to access and use this setting.

There are existing standards which provide for user profiles including:

- ETSI EG 202 116 [i.10]. It gives guidance to ICT product and service designers on Human Factors issues, good Human Factors design practices, and relevant international and national standards. The guidelines are intended to encourage a "Design for All" approach to making products and services accessible to as many people as possible, including elderly people and persons with disabilities, without the need for adaptation or specialized design.
- ETSI TS 102 747 [i.11]. The document defines an architectural framework supporting the personalization and user profile management concepts.
- ETSI ES 202 746 [i.12]. It specifies a set of user profile preferences and information settings for deployment in ICT services and devices for use by ICT users and suppliers.

The concept of a user profile usually refers to a set of preferences, information and rules that are used by a device or service to deliver a customized version of capabilities to the user. In practice, most devices and services contain profiles specific to that product and unrelated to any other. This requires that, on change of service or device, the user has to re-educate themselves in how to personalize their services or devices and re-enter their information and preferences. This often results in variable success rates and user satisfaction.

There will be several user characteristics and preferences that will apply independently of any particular product (e.g. a user's preferred language or their need for enlarged text). A key objective is that users should not be required to provide this information more times than is necessary. Users move from one situation to another throughout the day (e.g. at home, driving, working). In each of these situations, users may have different needs for how they would like their ICT resources arranged. Generally, products provide the user with ways of tailoring their preferences to these different situations. Users should be able to specify their context-dependent needs in ways that require the minimum need to understand the individual products.

Annex E:
Example of Application of ACIFO model to tomato cultivation (user side)

E.1 Overview

To illustrate how UIS/SCS works in practice, the example of smart tomato cultivation (clause 5.3), seen entirely from the user side is considered. The farmer is surrounded by sensors that continuously monitor the environment - temperature, humidity, pH, light, even images of the crops. All of this information flows into the UIS. Here, the data is not just raw numbers but visualized and explained through service components and the interface, in a way the farmer can understand and act upon. The important point is that the farmer stays in control if he so desires. When an anomaly is detected, experts and AI models can step in to provide deeper analysis and recommendations, but the system always makes it clear what is happening and why. The farmer decides whether to follow a recommendation or adjusts it to their preferences, and provides feedback.

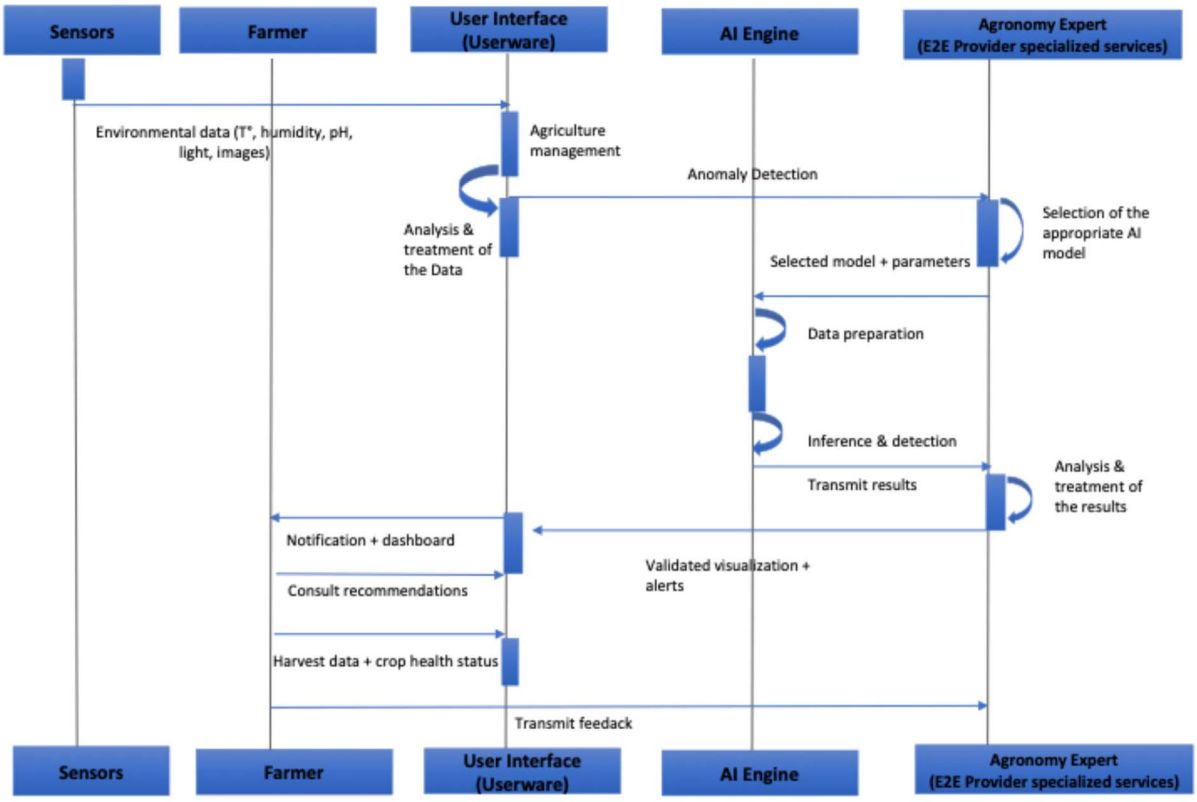

Figure E.1: Smart Tomato Cultivation (User Side)

E.2 Functions and features

E.2.1 Real-time environmental (Sensors → UIS)

It is important to note that the "SCS agriculture management" is in the Userware. It contains:

- Continuous comparison service for the incoming sensor data with predefined thresholds (e.g. for pH, humidity, or light levels).

- Synthesis and centralization service of all growth-related information for the tomatoes.
- Visualization service across the smart interface.
- Visual monitoring service of the crops by the cameras.

E.2.2 Anomaly detection (Userware)

The Userware constantly compares the incoming data with predefined thresholds (e.g. optimal humidity range, light exposure levels) and learned patterns. When irregularities are detected (e.g. early signs of water stress, unusual pH variation), the anomaly is flagged.

E.2.3 Expert validation and AI model selection (Agronomy Expert)

The anomaly report is sent to the Agronomy Expert, who evaluates the context and determines whether it requires advanced analysis. The expert selects the most appropriate AI model and configures its parameters.

E.2.4 AI-based anomaly analysis (AI Engine)

The AI Engine processes the anomaly data using the selected model.

E.2.5 Corrective recommendations (Userware + Expert support)

The processed results are returned to the Userware and validated by the Agronomy Expert.

The system generates precise, actionable recommendations for the farmer (e.g. "Increase watering in Zone A by 10 % over the next 3 days").

E.2.6 Farmer decision-making and feedback (Farmer → Userware)

The farmer receives real-time alerts and a dashboard with anomaly insights.

He consults recommendations, takes corrective actions, and then provides feedback (yield, treatment success, crop health status). This feedback is integrated into the system to continuously improve anomaly detection accuracy and model performance.

Annex F: Bibliography

- Exposito-Rosso, S., Cao, F.-X., et al.: "Research Report GDPR Data Portability: The Forgotten Right".
- Reimsbach-Kounatze, C., Molnar, A.: "The impact of data portability on user empowerment, innovation, and competition", Going Digital Toolkit Note, No. 25, 2024.
- "Data Transfer Project Overview and Fundamentals".
- ETSI TR 103 875-1: "User Centric Approach in Digital Ecosystem; The Smart Interface; Part 1: Smart Identity: user digital clone".
- ETSI TC SAI Work programme.

NOTE: Visible at https://www.etsi.org/technologies/artificial-intelligence and https://portal.etsi.org/tb.aspx?tbid=913&SubTB=913#/.

History

Document history		
V1.1.1	October 2025	Publication