
Open Autonomous programmable cloud appS & smart EdgE Sensors

# OASEES D6.3 Exploitation and standardization activities – Intermediate, Final

| | |
|---|---|
| Work package | WP6: Dissemination, Communication and Business Planning |
| Author | Enrique Areizaga – Tecnalia |
| Contributor | Charis Papatsarouchas – Adrestia R&D<br>Vasiliki Vlahodimitropoulou - OTE |
| Dissemination level | Public (PU) |
| Status | Draft |
| Due date | 30/04/2024 |
| Document date | 30/04/2024 |
| Version number | 1.0 |
|  | Funded by the European Union.<br>Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. |

| |
|---|
| Intermediate, Final |

## Revision and history chart

| Version | Date | Summary of changes |
|---|---|---|
| **0.1** | 31/01/2024 | First draft contents |
| **0.2** | 01/03/2024 | Draft with HSBooster inputs |
| **1.0** | 26/04/2024 | Final draft version |
| **1.1** | 30/04/2024 | Final Submitted Version |

| |
|---|
| Intermediate, Final |

## TABLE OF CONTENTS

| |
|---|
| Intermediate, Final |

## INDEX OF FIGURES



## INDEX OF TABLES

| |
|---|
| Intermediate, Final |

## GLOSSARY OF TERMS

CEN: European committee for Standardisation

CENELEC: European committee for Electrotechnical Standardisation

CEN BT STAIR: CEN-CENELECs group on research, innovation and education

Gaia-X: an initiative that develops, based on European values, a digital governance that can be applied to any existing cloud/ edge technology stack to obtain transparency, controllability, portability and interoperability across data and services.

IDSA: International Data Spaces Association, is on a mission to create the future of the global, digital economy with International Data Spaces (IDS), a secure, sovereign system of data sharing in which all participants can realize the full value of their data. IDS enables new ”smart services” and innovative business processes to work across companies and industries while ensuring that the self-determined control of data use (data sovereignty) remains in the hands of data providers.

SDO: A term that signifies any organisation developing standards, normally used for the industry or other specific organisations outside the formal organisations.

## LIST OF ABBREVIATIONS AND ACRONYMS

AI: Artificial Intelligence

BDVA: Big Data Value Association

CCMC: CEN-CENELEC Management Centre

CWA: CEN Workshop Agreement

DAO: Decentralized Autonomous Organization

D&C: Dissemination and Communications

DCM: Dissemination and Communication Manager

DSBA: Data Spaces Business Alliance

DSSC: Data Spaces support Centre

EAB: External Advisory Board

EAG: External Advisory Group (HSbooster.eu)

EC: European Commission

EISMEA: European Innovation Council and SMEs Executive Agency

Intermediate, Final

EPE: European Pool of Experts

ESO: European Standardisation Organisation (CEN. CENELEC, ETSI)

ETSI: European Telecommunications Standards Institute

EU: European Union

FP: Framework Programme

H2020: Horizon 2020

HE: Horizon Europe

HEI: Higher Education Institute

IEEE: Institute of Electrical and Electronics Engineers

IPR: Intellectual Property Rights

ISO: International Organization for Standardization

JRC: Joint Research Centre

KPIs: Key Performance Indicators

NC: National Committee (IEC/CENELEC)

NGO: Non-governmental Organization

NSB: National Standards Body (ISO/CEN)

PC: Project Coordinator

PoC: Proof of Concept

RDK: Rapid Development Kits

R&I: Research and Innovation

RO: Research Office

SoME: Social Media

SDO: Standardisation Developing Organisation

SME: Small and Medium Enterprises

SOP: Standard Operating Procedure

SOT: Standardisation Orientation Tool

| |
|---|
| Intermediate, Final |

SSI: Self Sovereign Identity

STAIR: Standards, Innovation & Research

TCG: The Trusted Computing Group

TM: Technical Manager

WP: Work Package

| |
|---|
| Intermediate, Final |

# INTRODUCTION

OASEES is a Research and Innovation project, funded by the European Union. Its goal is to create an open, decentralized, intelligent, programmable edge framework for Swarm architectures and applications, leveraging the Decentralized Autonomous Organization (DAO) paradigm and integrating Human-in-the-Loop (HITL) processes for efficient decision making. The OASEES vision is to provide the open tools and secure environments for swarm programming and orchestration for numerous fields, in a completely decentralized manner. An important aspect in this process is identification and identity management, in which OASEES targets the implementation of a portable and privacy-preserving ID federation system, for edge devices and services, with full compliance and compatibility to GAIA-X federation and IDSA trust directives and specifications. This situation solidifies the need for an integrated enabler framework tailored to the edge's extreme data processing demands, using different edge accelerators, i.e. GPU, NPU, SNN and Quantum.

OASEES' primary objectives are:

- Build rapid development kits (RDKs) for an open programmable framework across different smart edge nodes, while incorporating efficient cloud-to-edge continuum intelligence across heterogeneous target environments.
- Build a secure, trustworthy and decentralized edge ecosystem with native device support by integrating Self Sovereign Identity (SSI) for a portable digital identity that does not depend on any centralized authority. The OASEES decentralized device identity will be a new class of identifier that fulfils all four requirements: persistence, global resolvability, cryptographic verifiability, and decentralization
- Design a decentralized, agile and secure architecture for collaborative smart nodes at the edge, supporting heterogeneous device communication, backed by the Decentralized Autonomous Organization (DAO) paradigm integration
- Demonstrate the framework and programmability toolkit in a set of different vertical use cases and evaluate the benefits across different sectors
- Maximize the impact of the OASEES results via extensive communication, scientific dissemination, and exploitation activities. Foster the creation of an open-source community around the OASEES solution, engaging a diverse set of stakeholders

OASEES gathers a strong and complementary consortium of 21 different partners from 9 different European countries (Greece, Italy, Spain, France, Netherlands, Germany, Belgium, Romania and Luxemburg). The consortium gathers a wide range of companies, including SMEs, Academia, Research Institutes, and NGOs. OASEES will run from January 1st, 2023, to December 31st, 2025. A full list of the partners and their funding can be found at: https://cordis.europa.eu/project/id/101092702.

| |
|---|
| Intermediate, Final |

## PURPOSE AND SCOPE: COMPROMISE FROM GRANT AGREEMENT

Provide rationalised contributions to emerging and new standards, in Standards Developing Organizations and relevant pre-standardisation initiatives, such as:

- The Trusted Computing Group (TCG, https://trustedcomputinggroup.org/) in the Infrastructure and TPM Working Groups around the topic of attestation of the hardware and firmware (TEC).
- IEEE Future Network support the Edge Automation Platform (EAP) Task Force (ADRE).
- EENA enhance the usability of Next Generation 112 With the OASEES SDK concept (ADRE).
- PEMEA Consortium identify how OASEES can be incorporated in PUBLIC Safety networks (ADRE)
- ETSI contributions to related ISG WGs i.e., MEC and NFV (NCSRD).
- This activity will also include pre-standardisation activities through associations and industry groups such as the BDVA (IMEC, CEA), GAIA-X (TEC, IMEC, ALTRAN), ONF (NCSRD), Linux Foundation - LF Edge, (NCSRD), CNCF. SPH will focus on helping the other partners succeed in the various opensource.

KPIs for SDOs, Association and policy makers:

- More than “5” relevant SDOs (IEEE, IETF, ETSI, TCG, ENEA, PEMEA) with more than “5” contributions at YEAR 3 and more than “10” contributions at YEAR 5
- More than “10” relevant associations (BDVA, NGI, 6G IA, Networld Europe, ONF, FIWARE, GAIA-X, IDSA) with more than “5” contributions to Industry Associations at YEAR 3 and more than “10” at YEAR 5.

## STRUCTURE OF THE DELIVERABLE

This deliverable is organized into three distinct sections:

1. OASEES Strategy for Standardization: This section delineates the strategy devised by OASEES based on the outcomes derived from collaborative efforts with the HSBooster expert. It outlines the approach adopted by OASEES towards standardization initiatives.
2. OASEES Contribution to Relevant Standardization Developing Organizations: Here, the document highlights OASEES's active participation and contribution to pertinent Standardization Developing Organizations. It provides insights into the collaborative efforts aimed at shaping and influencing standardization processes.
3. Proof of Concept Definition and Process: This section elucidates the definition and procedural aspects of the Proof of Concept (PoC) undertaken by OASEES. It outlines the methodology employed and the key milestones associated with the PoC initiative.
4. OASEES Contribution to Relevant Pre-standardization Associations: Lastly, the document discusses OASEES's engagement and contribution to relevant Pre-standardization Associations. It underscores the proactive involvement of OASEES in shaping industry standards at an early stage of development.

| |
|---|
| Intermediate, Final |

## Relation to Other Work Packages and Tasks

This subsection will summarise the relationship of this deliverable with other deliverables of OASEES.

Table 1: Relation with other deliverables

| Deliverable | Lead Partner | PU/CO | Due Date |
|---|---|---|---|
| **D6.4 Exploitation and Standardization activities** | ADRE | Public | M36 |

| |
|---|
| Intermediate, Final |

## OASEES STANDARDS OUTCOMES

This section will provide the methodological framework that is followed in this deliverable.

### HORIZON STANDARDISATION BOOSTER

OASEES followed the process to become a project candidate for HSBooster service. After been accepted an expert was assigned and the Service started on November 2023 with the final meeting on February 22nd, 2024, according to the schedule depicted in the figure below:

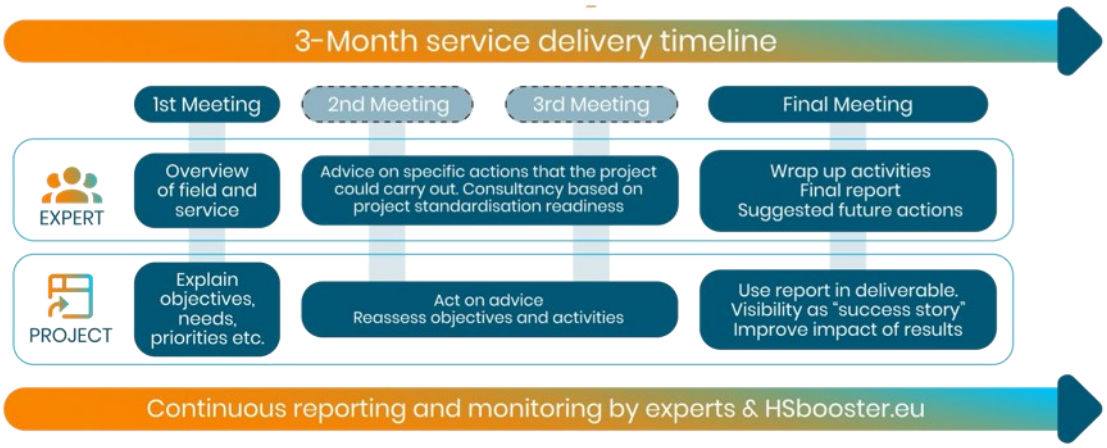


Figure 1: HSBooster service to OASEES

The OASEES partners previous experience with standards:

- The participation on behalf of OTE and MonB5G EU project in ETSI ZSM PoC 7 "Zero-touch closed-control security management of attacks detection and mitigation" - Demonstration of closed loop automation for mitigating against DDoS attacks from MTC (Machine Type Communication) devices on 5G Core Network (CN) components.
- Project Partner - NCSR Demokritos - member of the ISG MEC.
- CTN-UNE 71/SC 14 "Tecnologías Cuánticas"
- CEN/CLC/JTC 22- Quantum Technologies
- ISO/IEC JTC1/WG 14

**OASEES Priority Topics for Standardization**:

Recommendation to consider the European standards organization, as CEN (the European Committee for Standardization), CENELEC (European Committee for Electrotechnical Standardization and ETSI, the European Telecommunications Standards Institute), rather than ISO (International Organization for Standardization)

- Selected relevant standards:
  - CEN-CLC/JTC 21 - Artificial Intelligence
  - CEN/CLC/JTC 22 - Quantum Technologies
  - CEN-CLC/BTWG 6 – ICT standardization policy

    - CTN-UNE 71/SC 14 "Tecnologías cuánticas"
    - ISO/IEC JTC1/WG 14.
    - First identification by OASEES related to potential contribution to Standardization:
- Quantum Computing (Tecnalia and Fraunhofer from Munich)
- Cloud Accelerators / Orchestration – AI
- DAO – Digital Autonomous Organization – many areas within this, the main one.

**HSBooster Expert Recommendation for OASEES Regarding Potential Contribution to Standardisation**

In consideration of OASEES's potential contribution to standardisation, it is recommended to focus efforts on engagement with the following:

**ETSI ISG Working Groups (WGs):**

- Topic 3: Edge Infrastructure Sharing and Monetisation.

It is advised to convene a Proof of Concept (PoC) team consisting of representatives from NCSRD, IMEC, OTE, and other interested/relevant members of the consortium. This team should collaborate to draft and submit a proposal to the ETSI MEC ISG as an initial step towards contributing to standards development.

OASEES Consortium members will monitor and/or contribute to the standardisation bodies that align most closely with its interests, while ensuring that the OASEES framework remains consistent with the standards. The following is a description of the standardisation organisations that are relevant to the project.

**Proposed Standardisation Developing Organisations:**

**3GPP**

The 3rd Generation Partnership Project (3GPP) brings together seven telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC) and provides a stable environment for its members to produce the Technical Reports and Specifications that define 3GPP technologies. 3GPP includes three Technical Specification Groups (TSG), namely: Core Network & Terminals (CT), Services & Systems Aspects (SA), and Radio Access Networks (RAN). Including radio access, core network, and service capabilities, the project provides a comprehensive system description for mobile telecommunications cellular technologies.
3GPP TSG Service and System Aspects (SA) is responsible for the overall architecture and service capabilities of systems based on 3GPP specifications.

The 3GPP began working on edge computing in Release 15, with the initial versions of its 5G specifications defining the functionality for edge computing support. Work on improving 5G Core to enable edge computing and applications, as well as other critical areas like security, charging, and

management, began in Release 17. In Release 18, 3GPP continues to work on edge computing, including collaborating and alignment with external organisations. [1]

The **edge computing tasks** are allocated among three working groups of 3GPP. **3GPP SA2** working group is specifying aspects relevant to the 3GPP transport layer while SA5 and SA6 are in charge with defining the edge management and edge enabler layers, respectively. In the context of edge computing, 3GPP SA2 defines how user traffic is routed to the appropriate application servers in the edge clouds. It also provides the means for applications to provision traffic steering rules. Regarding edge computing, 3GPP SA5 is presently working on defining charging aspects for edge services and life-cycle management of application servers in the edge cloud. The architecture for enabling Edge Applications (EDGEAPP) is defined by 3GPP SA6, particularly by defining an enabling layer which allows communication between application clients and edge-deployed applications. Additionally, the architecture enables the use of the Common API Framework, or **CAPIF**, as a standardised method of offering and accessing APIs in the Edge Cloud.

**3GPP Radio Access Network (RAN)**

The 3GPP TSG Radio Access Network (RAN) is responsible for the technical co-ordination of the specification work done in the following Working Groups:

- **RAN1** – Radio Layer 1 (Physical layer)
- **RAN2** – Radio layer 2 and Radio layer 3 Radio Resource Control
- **RAN3** – UTRAN/E-UTRAN/NG-RAN architecture and related network interfaces
- **RAN4** – Radio Performance and Protocol Aspects
- **RAN5** – Mobile terminal conformance testing

3GPP initiated the development of a new radio-access technology known as NR (New Radio). By the end of 2017, the first version of the NR standards had been made available to satisfy industry demands for early 5G deployments in 2018. 5G NR is being deployed around the world to deliver faster data rates and unprecedented reliability to wireless communications. New base station types have emerged, defined according to the frequency range and the antenna configuration of the equipment

Support for reduced capability (RedCap) NR devices is introduced with 3GPP Rel-17 in order to accelerate industrial transformation and digitalization even further. The current NR specifications do not fully cover the use cases that these devices address. Some interesting use cases, such as industrial wireless sensors, video surveillance, and wearables, are made possible by the 3GPP RedCap NR feature, which simplifies UEs by reducing the number of RX/TX antennas, the amount of bandwidth and power used by UEs, the processing time and capability of UEs, and the data rates at which they operate.[2]

[1] https://www.3gpp.org/technologies/edge-computing

[2] https://www.3gpp.org/technologies/nr-redcap-glimpse

Intermediate, Final

**ETSI MEC ISG**

The Multi-access Edge Computing (MEC) initiative is an Industry Specification Group (ISG) within ETSI. According to the information provided on its official website[3] the purpose of the ISG is to create a standardized, open environment which will allow the efficient and seamless integration of applications from vendors, service providers, and third parties across multi-vendor Multi-access Edge Computing platforms.

The initiative aims to benefit several entities within the value chain, including mobile operators, application developers, Over the Top (OTT) players, Independent Software Vendors (ISVs), telecom equipment vendors, IT platform vendors, system integrators, and technology providers; all of these parties are interested in delivering services based on Multi-access Edge Computing concepts.

The work of the MEC initiative aims to unite the telco and IT-cloud worlds, providing IT and cloud-computing capabilities within the RAN (Radio Access Network). MEC also enables applications and services to be hosted 'on top' of the mobile network elements, i.e. above the network layer. These applications and services can benefit from being near the customer and from receiving local radio-network contextual information

MEC has the ability to enhance the experience of end-users by minimising service downtime, improving overall latency, ensuring security and data privacy, and introducing intelligent services at the edge. This is achieved by leveraging the most effective cloud service deployment strategies for applications, such as edge load balancing, secure messaging across multi-cloud, hybrid-cloud, and AI/ML services via distributed cloud.[4]

**ETSI NFV**

Network Functions Virtualization (NFV) has brought in a new era of software-based virtualized network functions (VNFs), displacing traditional physical (hardware) network equipment. It has also caused a dramatic shift in the telecom sector. NFV has overcome the technical challenges of software and hardware decoupling using general-purpose (commodity-off-the-shelf, or COTS) servers and the deployment of network services as software applications. Dedicated physical appliances have been replaced by distributed cloud infrastructure for network functions, which has completely changed how modern communications networks are designed, implemented, and operate.

After NFV has been around for a decade and has been the basis for significant investments and network deployments, now is an ideal time for considering about its potential for future evolution. To achieve this goal, one must be aware of, and respond to, the following requirements that telecom service providers address in their telco cloud:
1) unified network management

[3] https://www.etsi.org/technologies/multi-access-edge-computing

[4] ETSI GS MEC 002 V3.1.1 (2023-04) "Multi-access Edge Computing (MEC); Use Cases and Requirements", https://www.etsi.org/deliver/etsi_gs/MEC/001_099/002/03.01.01_60/gs_MEC002v030101p.pdf

2) use of latest cloud-native, IT, automation and Artificial Intelligence (AI) open-source software, and
3) multi-vendor interoperability and migration among different clouds.[5]

**ETSI PDL**

The ETSI Industry Specification Group on Permissioned Distributed Ledger (ISG PDL) analyses and provides the foundations for the operation of permissioned distributed ledgers, with the ultimate purpose of creating an open ecosystem of industrial solutions to be deployed by different sectors, fostering the application of these technologies, and therefore contributing to consolidate the trust and dependability on information technologies supported by global, open telecommunications networks.[6]

PDL technology can be widely adopted in various domains and layers of a mobile network system, including end users, RAN/core network, and service providers. The report on the use cases of Permissioned Distributed Ledgers (PDL) in 3GPP networks provides an analysis of their impact on architecture integration, highlighting key issues, challenges, and limitations. This analysis aims to identify the appropriate PDL solutions needed for the mobile network system. Additionally, it is analysed the impact of PDL on the architecture of the mobile network system, with reference to the 3GPP 5G architecture.[7]

**ISO/TC 307**

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. The objective of Technical Committee ISO/TC 307, *Blockchain and distributed ledger technologies* is to address the increasing demand for standardisation in the domains of blockchain and DLT by establishing globally accepted standards for enhancing security, privacy, scalability, and interoperability. In accomplishing that, it anticipates promoting the widespread adoption of the technology by fostering increased innovation, improved governance, and sustainable development. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.
The standardization work of ISO/TC 307 has been divided into six groups:

| | | |
|---|---|---|
| **WG** | **1** | Foundations |
| **WG** | **2** | Security, privacy and identity |

[5] ETSI White Paper No. 54 “Evolving NFV towards the next decade” https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP-54-Evolving_NFV_towards_the_next_decade.pdf

[6] ETSI White Paper No. 48 “An Introduction of Permissioned Distributed Ledger (PDL)” January 2022

[7] ETSI GR PDL 021 V1.1.1 “Permissioned Distributed Ledgers (PDL); Overview of use cases in 3GPP network and impact analysis on architecture integration” October 2023

| |
|---|
| Intermediate, Final |

**WG 3** Smart contracts and their applications
**SG 2** Use cases
**SG 6** Governance
**SG 7** Interoperability

Intermediate, Final

Table 2: Use Cases of PDL in 3GPP networks

| | **For Operator Use** | | | | | | **For 3rdparty Use** |
|---|---|---|---|---|---|---|---|
| General Use Cases | 1.Telecom Infrastructure Registry | 2. Operational Log Sharing | 3. Security/Privacy Enhancement | 4. Resource Sharing | 5. Trustworthy and Explainable Network-Native AI | 6. Smart Contract based Direct Inter operation | 7. Vertical Support |
| Sub-Use Cases | 1.1 Single domain Infrastructure Registry 1.2 Multidomain Infrastructure Registry | 2.1 Charging Bills 2.2 Service KPIs 2.3 UE Runtime Behaviours 2.4 Energy Consumption Measurement Data | 3.1 Decentralized Data Storage 3.2 Data Auditing 3.3 Decentralized Certificate 3.4 Decentralized Credential 3.5 Decentralized Identity | 4.1 Infrastructure Resource Sharing 4.2 Spectrum Resource Sharing 4.3 Digital Asset | 5.1 Training Data Collection 5.2 Distributed Learning 5.3 Model Verification | N/A | N/A |

**Associations:**

**GSMA**

The GSMA is an international organisation that unifies the mobile ecosystem to identify, develop, and spread innovation that is fundamental to societal transformation and positive business environments. GSMA's primary objective is to leverage the complete potential of connectivity to foster prosperity for individuals, industries, and society.[8]

**GSMA Operator Platform Group**

To facilitate the monetization of network capabilities, the Operator Platform aims to give a standard solution for operators to make those capabilities available to enterprise clients and developers. Through its federation features, the Operator Platform helps these business customers connect to a single platform and use all the features of all the networks that platform has joined. Subsequent versions of these specifications have covered network and network slicing as a service capability, while the original version concentrated on edge computing. An updated title reflects the broader scope of this revised set of criteria and architecture for the Operator Platform, which delves more into

[8] https://www.gsma.com/aboutus/

the charging architecture and requirements while also clarifying those related to security and the common data model.[9]

**6G Smart Networks and Services Industry Association (6G-IA)**

The 6G Smart Networks and Services Industry Association (6G-IA) represents European Industry and Research in the development of future networks and services. The main goal is to strengthen Europe's leadership in 5G technology, 5G advancement, and SNS/6G research.
The 6G-IA is the private sector representative in the 5G Public Private Partnership (5G-PPP) and the Smart Networks and Services Joint Undertaking (SNS JU). The European Commission represents the public side in the 5G-PPP and SNS JU.
The 6G-IA unites a worldwide industrial community consisting of telecommunications and digital organisations, including operators, manufacturers, research institutes, universities, verticals, SMEs, and ICT associations.
The 6G-IA is involved in several strategic activities such as standardisation, frequency spectrum management, R&D projects, technology expertise, collaboration with important vertical industrial sectors, especially for trial development, and international cooperation.[10]

**About ETSI MEC ISG**: The ETSI MEC ISG, or Mobile Edge Computing Industry Specification Group, is actively engaged in developing a standardized, open environment tailored for the efficient and seamless integration of applications. This integration spans across various stakeholders including vendors, service providers, and third parties. The focus lies on achieving interoperability across multi-vendor computing platforms situated at the edge of mobile networks.

[9] https://www.gsma.com/futurenetworks/operator-platform-hp/

[10] https://6g-ia.eu/

| |
|---|
| Intermediate, Final |

## OASEES Proof of Concept Proposal

The PoC explores deploying a drone swarm to efficiently inspect infrastructure, leveraging the capabilities of mobile edge computing (MEC) defined by ETSI MEC standards, and service management by ETSI ZSM guidelines. This integration aims to optimize the operational capabilities of drones within a regulated, efficient, and secure framework.

**MEC and ZSM Interfaces**: The integration of MEC and ZSM interfaces in this PoC brings numerous advantages, particularly in terms of operational efficiency, scalability, and security in drone operations:

Table 3: OASEES contribution to MEC/ZSM

| **MEC/ZSM enablers** | **Benefit to Drones Pilot** | **Contribution to MEC/ZSM** |
|---|---|---|
| **Service Continuity** | MEC ensures uninterrupted service delivery for drones, especially in areas of fluctuating network coverage, by providing edge-based processing and data storage. | Demonstrates the resilience and reliability of MEC deployments in maintaining service continuity for critical applications. |
| **Low-latency Services** | ZSM facilitates low-latency data processing, essential for real-time analytics and decision-making in drone surveillance and inspection tasks. | Validates ZSM's ability to manage and orchestrate low-latency edge applications efficiently. |
| **Resource Allocation** | MEC provides dynamic resource allocation which helps in optimal resource utilization based on the drone's computational needs and network conditions. | Highlights MEC's dynamic resource management capabilities, enhancing the practical deployment of resource-intensive applications. |
| **Scalability** | ZSM's service management architecture allows for scalable operations, supporting an increase in drone numbers or computational demand without loss of performance. | Provides real-world insights into the scalability of ZSM frameworks, bolstering its adaptability in diverse deployment scenarios. |
| **Security and Compliance** | MEC supports localized data processing, which reduces the risk of data breaches by minimizing data transit. ZSM ensures that all operations adhere to predefined security policies. | Showcases how MEC and ZSM can be leveraged to enhance security measures and ensure compliance with stringent regulatory requirements. |

Intermediate, Final

| Component | Description |
|---|---|
| Drones | A swarm of 3-5 drones, each outfitted with necessary sensors and computational tools. |
| Network Infrastructure | NCSRD 5G testbed with RedCap capabilities |
| Computational Hardware | Advanced devices integrated into drones for enhanced data processing. |

ETSI MEC standards define several interfaces that facilitate interactions between edge applications and the underlying mobile edge computing environment. For the drone PoC, the following specific interfaces from the ETSI MEC specifications are particularly relevant:

1. **Mp1 Interface**:
    - **Functionality**: Connects MEC applications to the MEC platform, enabling services such as location, radio network information, and bandwidth management.
    - **Benefit to Drones Pilot**: Allows drones to access real-time network-related information that can optimize their routing and operational efficiency based on current network conditions and availability.
2. **Mx2 Interface**:
    - **Functionality**: Facilitates inter-MEC system communication, enabling coordination between different MEC platforms.
    - **Benefit to Drones Pilot**: Ensures seamless service continuity and operational handover when drones move across different MEC platform boundaries, crucial for maintaining uninterrupted inspections over larger geographical areas.

**ETSI ZSM Interfaces:**

The ETSI Zero-touch network & Service Management (ZSM) framework provides interfaces that are crucial for automating the orchestration and management of network services and resources. For the drone PoC, consider these interfaces:

1. **Service Management Interface**:
    - **Functionality**: Manages the lifecycle of services, including deployment, scaling, updating, and termination.
    - **Benefit to Drones Pilot**: Automates the deployment and scaling of drone control applications, adapting to changing conditions and demands without human intervention.

2. **Orchestration Interface**:

    - **Functionality**: Provides orchestration capabilities across multiple domains and administrative boundaries, managing resources and services dynamically.

    - **Benefit to Drones Pilot**: Allows for dynamic resource allocation and real-time decision-making based on the current operational context and resource availability, which is essential for critical missions requiring high reliability and performance.

**Application of Interfaces in Drone PoC:**

- **Real-Time Data Processing and Decision Making**: Utilizing the Mp1 interface for accessing real-time network information enables drones to make on-the-fly decisions about flight paths and operations, optimizing routes for efficiency and safety based on live environmental data.

- **Cross-Domain Service Continuity**: The Mx2 interface ensures that drone operations are not disrupted when transitioning across different edge environments, which is vital for extensive infrastructure inspections spanning large areas.

- **Automated Service Management**: The Service Management interface from ZSM allows the drone fleet's control applications to be automatically managed, ensuring optimal performance and quick adaptation to new operational demands.

- **Resource Efficient Orchestration**: The Orchestration Interface facilitates efficient use of network and computational resources, crucial for maintaining the drones' operational capacity during long-duration missions or when processing large amounts of data.

By leveraging these specific MEC and ZSM interfaces, the OASEES drone PoC can achieve high levels of automation, efficiency, and reliability, which are essential for the advanced deployment of drones in infrastructure inspection scenarios. These interfaces not only enhance the operational capabilities of drones but also ensure that these operations are secure, compliant, and seamlessly integrated with existing and emerging network technologies.

This PoC is designed to showcase the integration of advanced technologies in a practical setting, highlighting the potential of mobile edge computing to revolutionize infrastructure inspections. By adhering to ETSI MEC and ETSI ZSM standards, the PoC not only meets high standards of mobile edge computing but also demonstrates the effectiveness of technological innovations in managing critical infrastructure. This project sets the stage for broader adoption and further innovations in automated and enhanced infrastructure monitoring.

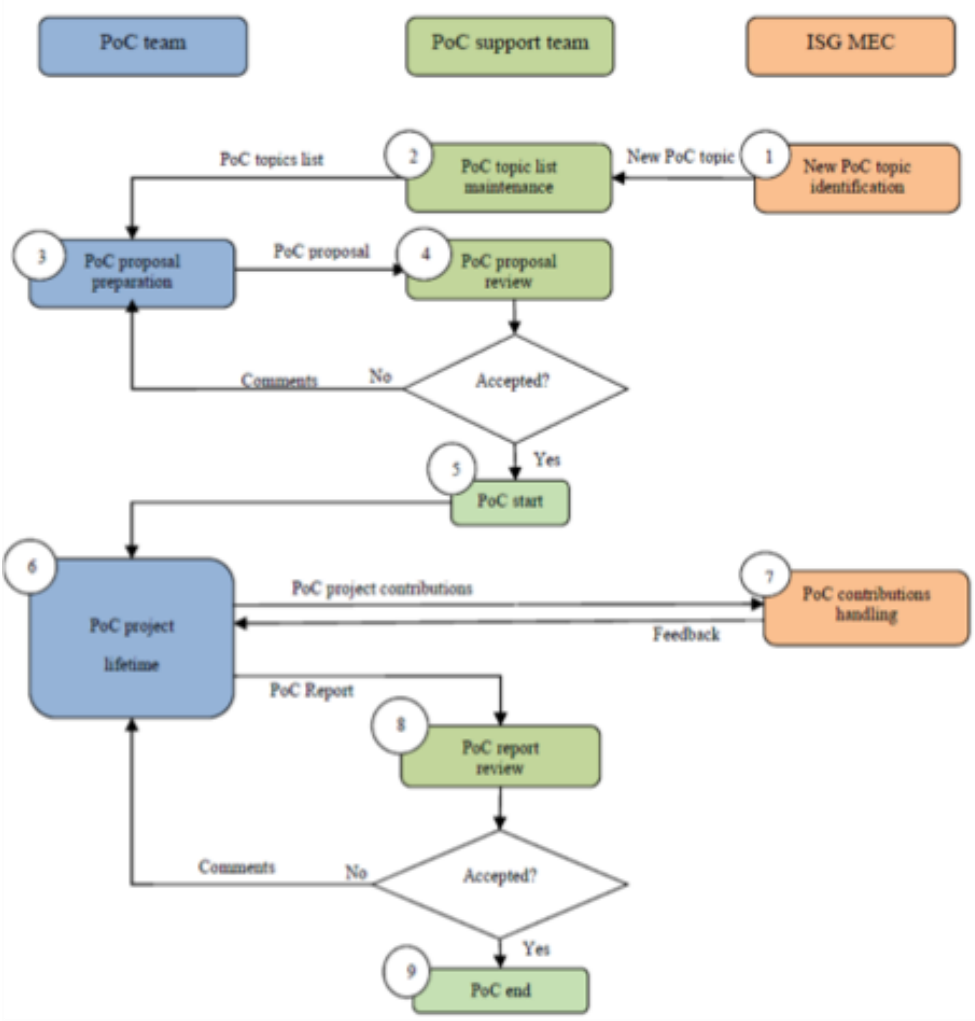


Figure 2: Proof of Concept process

| |
|---|
| Intermediate, Final |

## OASEES Publicly Available Specifications (PAS)

ETSI recognizes that other Standards Development Organizations (SDOs), fora and consortia can provide useful contributions to the work in areas of ICT standardization, and it is likely to be brought into ETSI´s work program.

ETSI offers to PAS submitters a speedy adoption, the reputation of high-quality specifications and a greater visibility in Europe and worldwide.

A PAS can be any publicly available technical specification or report developed by an ETSI Partner that is submitted to ETSI for adoption as an ETSI Technical Specification (TS) or Technical Report (TR).

Once published as an ETSI TS or ETSI TR it becomes an ETSI specification with a number of advantages.

More details in PAS[11].

## Further Suggestions from HSBooster expert

- Publicly Available Specifications (PAS)
- Different Standard Types[12]
- TCG, IEEE Future Network, EENA and PEMEA support procedure for standardization
- ETSI contributions to related ISG WGs and other way around
- Pre-standardisation activities through industry groups.

## Standardisation Training Material

- How to find the right Standards[13]
- How to participate in TCS or WGS[14]
- How Standards are developed within SDOs in Europe[15]
- How Standards are developed within SDOs internationally[16]

[11] https://www.etsi.org/images/files/Brochures/ETSI-Brochure-PAS.pdf

[12] https://www.etsi.org/standards/types-of-standards

[13] https://hsbooster.eu/sites/default/files/2023-06/I1%2001%20HOW%20TO%20FIND%20THE%20RIGHT%20STANDARD%20ver2_0.pdf

[14] https://hsbooster.eu/sites/default/files/2023-03/I1%2002%20HOW%20TO%20PARTICIPATE%20IN%20TCS%20OR%20WGS.pdf

[15] https://hsbooster.eu/sites/default/files/2023-10/I1%2003%20HOW%20STANDARDS%20ARE%20DEVELOPED%20WITHIN%20SDOS%20IN%20EUROPE%20%281%29.pdf

[16] https://hsbooster.eu/sites/default/files/2023-03/I1%2004%20HOW%20STANDARDS%20ARE%20DEVELOPED%20WITHIN%20SDOS%20INTERNATIONALLY.pdf

- Conformity Assessment Schemes and Systems[17]
- Consortia-based Standardisation[18]
- Legal Aspects of Standardisation[19]
- Introduction to Standard Essential Patents[20]

[17] https://hsbooster.eu/sites/default/files/2023-10/I105%20CONFORMITY%20ASSESSMENT%20SCHEMES%20AND%20SYSTEMS.pdf

[18] https://hsbooster.eu/sites/default/files/2023-03/B2%2001%20CONSORTIA-BASED%20STANDARDISATION.pdf

[19] https://hsbooster.eu/sites/default/files/2023-03/B1%2005%20LEGAL%20ASPECTS%20OF%20STANDARDISATION.pdf

[20] https://hsbooster.eu/sites/default/files/2023-03/B2%2003%20INTRODUCTION%20TO%20SEP.pdf

| |
|---|
| Intermediate, Final |

## PRE-STANDARDISATION ACTIVITIES: GAIA-X, IDSA

Contribution of OASEES to ISO Standards Adherence in IDSA and Gaia-x Initiatives

It is noted that both the IDSA and Gaia-x initiatives are currently in the process of seeking adherence to ISO standards, with an anticipated finalization date set for 2025. The participation and contribution from OASEES are expected to indirectly support the formulation of these standards.

**IDSA Protocol Adherence by OASES Members**

Within the framework of the IDSA, OASES members, represented notably by TECNALIA through its IDSA ambassador and other partners, are committed to ensuring that data generation and exchange adhere to the Data Spaces protocol. This adherence extends to compliance with related standards, with active contribution facilitated through collaborative partnerships and participation.

- Configuration of EDC connectors for Data Exchange and application of OASEES access and Usage policies.
- ISO/IEC AWI 20151: Cloud computing and distributed platforms, Dataspace concepts and characteristics was officially registered on January 2024 within the TC/SC work program at ISO/IEC JTC1 SC38. ISO/IEC AWI 20151 will guide industries and governments in implementing solutions for trusted data sharing.
- IDSA commits to forming the Standardization Working Group. This strategic move aims to harness expertise, foster collaboration, and effectively address the complex challenge of international standardization. ISO/IEC AWI 20151 shall be published during 2025 and OASEES Data Products will be aligned to it.

**Gaia-X Trust ecosystem Adherence by OASES Members**

Within the framework of Gaia-X, OASEES members are committed to participate in the design and implement a data sharing architecture that consists of common standards for data sharing, best practices, tools, and governance mechanisms. More precisely, TECNALIA has an active contribution to the OSS (Open-Source Software) and Data Exchange WG with inputs agreed in OASEES and collected in Deliverables D2.3 and D3.4.

- Definition on Data Products based on the requirements for DATA Federation in OASEES
- Contributing to the ISO when officially registered.

Current contribution to Gaia-x:

- Tech-X event 2023: The future of privacy-preserving computation under Gaia-X (Tecnalia) 3rd May 2023. Tech-X Agenda 2023 - Gaia-X: A Federated Secure Data Infrastructure
- Tech-X event 2024: How to make a Data Product for Gaia-X (Tecnalia). Accepted to be presented during the event in Luxemburg, Tuesday 23 May 2024. https://gaia-x.eu/tech-x-agenda-2024/

# CONCLUSIONS

To obtain a comprehensive comprehension of the potential contributions to various Standards Development Organizations (SDOs), OASEES has engaged with the HSBooster program. With the invaluable assistance of an HSBooster expert, the initial contribution to standardization has been formally ratified among the consortium partners. This contribution takes the form of a Proof of Concept meticulously tailored to align with one of the program's Use Cases.

Simultaneously, outreach efforts have been initiated with other SDOs, including PEMEA. However, given the current stage of the project, substantive engagement with these entities is anticipated to commence in Year 3. Nevertheless, this timeline does not hinder the attainment of Key Performance Indicators (KPIs), which include surpassing five contributions by that juncture. These contributions will be consolidated within Deliverable D6.4, scheduled for submission by the end of month 36.

The endeavours of OASEES in advancing pre-Standardization forums are progressing satisfactorily. The active involvement of our partners in initiatives such as Gaia-X, IDSA, and DSSC, among others, instils confidence that KPI targets will indeed be met by Year 3.