Net-Zero self-adaptive activation of distributed self-resilient augmented services

D7.5 - Impact to standardisation bodies, consortiums, and Alliances.r1

Lead beneficiary	NOVA	**Lead authors**	Ioannis Markopoulos, Angelos Lampropoulos
Reviewers	Francesco Paolucci (CNIT), Gürkan Gür (ZHAW)		
Type	R	**Dissemination**	PU
Document version	V1.0	**Due date**	31/12/2025

Co-funded by
the European Union

6GSNS

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
**State Secretariat for Education,
Research and Innovation SERI**

UK Research
and Innovation

Project information

Project title	Net-Zero self-adaptive activation of distributed self-resilient augmented services
Project acronym	NATWORK
Grant Agreement No	101139285
Type of action	HORIZON JU Research and Innovation Actions
Call	HORIZON-JU-SNS-2023
Topic	HORIZON-JU-SNS-2023-STREAM-B-01-04 Reliable Services and Smart Security
Start date	01/01/2024
Duration	36months

Document information

Associated WP	WP7
Associated task(s)	T7.4
Main Author(s)	Ioannis Markopoulos (NOVA), Angelos Lampropoulos (NOVA)
Author(s)	Antonios Lalas, Vangelis V. Kopsacheilis, Anastasios Drosou (CERTH), Kostas Pournaras, Didoe Prevedourou (PNET), Nasim Nezhadsistani (UZH), Edgardo Montes de Oca, Ana Cavalli (MONT), Sergio Zapata Caparrós (GRAD), Mohammed Alshawki (ELTE), Maria Safianowska (ISRD), Gürkan Gür (ZHAW), Vincent Lefebvre (TSS), Mays AL-Naday (UESSEX)
Reviewers	Francesco Paolucci (CNIT), Gürkan Gür (ZHAW)
Type	R – Document, Report
Dissemination level	PU – Public
Due date	M24 (31/12/2025)
Submission date	31/12/2025

Document version history

Version	Date	Changes	Contributor (s)
v0.1	17/09/2025	Draft initial document for ToC validation	Ioannis Markopoulos, Angelos Lampropoulos (NOVA), Antonios Lalas (CERTH), All authors
v0.2	29/10/2025	25% of the content completed	All authors
v0.3	12/11/2025	65% of the content completed	All authors
v0.4	18/11/2025	90% of the content completed	All authors
v0.5	25/11/2025	Deliver final draft	Ioannis Markopoulos, Angelos Lampropoulos (NOVA), All authors
v0.6	09/12/2025	Review of document completed	Francesco Paolucci (CNIT), Gürkan Gür (ZHAW)
v0.7	12/12/2025	Review comments implemented	All authors
v0.8	16/12/2025	Quality review completed	Leonardo Padial (HES-SO)
v0.9	23/12/2025	Final review and refinements	Antonios Lalas, Vangelis V. Kopsacheilis (CERTH), All authors
v1.0	31/12/2025	Document ready for submission	Antonios Lalas (CERTH)

Disclaimer

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or 6G-SNS. Neither the European Union nor the granting authority can be held responsible for them. The European Commission is not responsible for any use that may be made of the information it contains.

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

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

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

Copyright message

Contents

List of acronyms and abbreviations

Abbreviation	Description
3GPP	3rd Generation Partnership Program
5G	Fifth generation
6G	Sixth generation
6G-IA	6G Smart Networks and Services Industry Association
AI	Artificial Intelligence
AIEE	American Institute of Electrical Engineers
AIOTI	Alliance for AI, IoT and Edge Continuum Innovation
ATIS	The Alliance for Telecommunications Industry Solutions
BSI	British Standards Institution
CCSDS	Consultative Committee for Space Data Systems
CI/CD	Continuous Integration / Continuous Deployment
CR	Change Request
CRA	Cyber Resilience Act
CT	Core Network and Terminals
DLT	Distributed Ledger Technology
ECSS	European Cooperation for Space Standardization
ENI	Experiential Networked Intelligence
ENISA	European Union Agency for Cybersecurity
ETP	European Technology Platform
ETSI	European Telecommunications Standards Institute
EUSR	European Union Standardisation Requests
FGs	Focus Groups
GSMA	Global System for Mobile Association
KVIs	Key Value Indicators
ICT	Information and communications technologies
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IRE	Institute of Radio Engineers
ISG	Industry Specification Group
ISO	Organization for Standardization
IT	Information Technology
ITU-R	International Telecommunication Union – Radiocommunication Sector
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
LTE	Long Term Evolution
NIST	National Institute of Standards and Technology
NFV	Network Functions Virtualization

Abbreviation	Description
nGRG	Next Generation Research Group
O-RAN	Open Radio Access Network
OARC	OpenAR Cloud Association
OASIS	Organization for the Advancement of Structured Information Standards
OSL	OpenSLice
PLS	Physical Layer Security
RAN	Radio Access Network
RFCs	Request for Comments
RIS	Reflective Intelligent Surfaces
SA	Service and System Aspects
SCoDIHNet	Smart Connectivity Digital Innovation Hub Network
SDG	Software Development Group
SDG OSL	Software Development Group for OpenSlice
SDG OOP	Software Development Group OpenOP
SDOs	Standards Developing Organizations
SME	Small and Medium-sized Enterprise
SNS JU	Smart Networks and Services Joint Undertaking
SRIA	Strategic Research Innovation Agenda
TB	Technology Board
TIP	Telecom Infra Project
TRL	Technology Readiness Level
TSC	Technical Steering Committee
TSG	Technical Specification Group
TTC	Telecommunication Technology Committee
UMTS	Universal Mobile Telecommunications System
V2V	Vehicle-to-vehicle communications
WGs	Working Groups
WiTaR	Women in Telecommunication and Research
ZSM	Zero touch network & Service Management

List of tables

Executive summary

This report, namely Deliverable D7.5 “Impact to standardisation bodies, consortiums, and Alliances.r1” focuses on the standardisation activities in which NATWORK partners are engaged and the active involvement of NATWORK partners in Working Groups (WGs) associated with 5G and 6G networking matters, as well as cybersecurity. Over the deliverable, a thorough account of the engagement between NATWORK and the related Standards Developing Organizations (SDOs) is also presented.

The relation between NATWORK partners and the SDOs related to cybersecurity and networking is presented through the current deliverable. Standardisation bodies have an active role in shaping industry landscapes by setting rules that define product compatibility, quality, and safety. Several partners have extensive engagement with standardization bodies, on which a direct or indirect relation to NATWORK exists. An introduction to these SDOs is presented within this report. Information on the SDOs and the relation between the SDO and the related partner(s) is presented.

The initial Technology Readiness Level (TRL) of NATWORK components and/or services is low (initial values TRL1-2), expected to rise to TRL3-4 towards the end of the project. Taking that into account, standardisation activities by NATWORK partners are outlined in the current report. NATWORK partners have ongoing communication with the related standardization bodies. Initial results of NATWORK have been shared with these groups. Furthermore, dissemination and exploitation of these outcomes from a standardization perspective is under development.

Another topic on which D7.5 engages is the interaction of the NATWORK project with the related Working Groups (WGs) associated with 5G and 6G networking and cybersecurity domains. There are three (3) types of WGs in which partners are engaged, namely 6G Smart Networks and Services Industry Association (6G-IA), Smart Networks and Services Joint Undertaking (SNS JU), and NetworldEurope. Through the current deliverable, constructive communication and cooperation from the representatives of partners towards these entities are outlined.

Moreover, the NATWORK Policy Brief #1: Transparency in 6G Security, Resilience & Trust is presented, that was formulated to facilitate the EU policy discussions related to connectivity. Although it is not a direct contribution to standards, it can have an indirect impact to standardization activities, thus it is reported as a preliminary outcome of the relevant discussions.

The current report, D7.5, is the first report on “Impact to standardisation bodies, consortiums, and Alliances”. The second report will further determine the engagement of NATWORK partners with the three types of WGs, namely, 6G-IA, SNS JU and NetworldEurope. Moreover, the second report will assess the standardization activities of NATWORK partners with SDOs. The second deliverable will be submitted at M36, December 2026.

1. Introduction

During task T7.4 “Standardisation Activities & Policy Recommendations” the identification of relevant standards and the contribution to key standardisation bodies to support 6G standardisation, particularly in the security-related domain, has been initiated. This process will continue throughout the timeline of the NATWORK project so that this two-way interaction between SDOs and NATWORK will be strengthened and enhanced. Moreover, studies on 6G standardisation and pre-standardisation conducted by several SDOs are being monitored by NATWORK partners. These activities are presented through the current report, D7.5 “Impact to standardisation bodies, consortiums, and alliances.r1”.

Standardisation is a key element that transforms the results of a project – in this case, the NATWORK project – into actual standards. The standardisation process advances the safety, competitiveness, and interoperability of these results throughout the EU. Standardisation bodies play a crucial role in identifying the rules governing each industry, specifically in the areas of cybersecurity and 5G & 6G networking. Throughout this report, these activities are explained in detail.

The present deliverable is the first version that depicts the standardisation activities of NATWORK. The interaction between NATWORK partners and the Standards Developing Organizations (SDOs) related to cybersecurity and 6G networking is introduced. Furthermore, the engagement between NATWORK and 6G-IA, SNS-JU, and NetworldEurope WGs is also illustrated. Initial policy recommendations are also formulated and introduced. The second version of this report will be submitted at M36. It will include a more comprehensive review of standardization activities towards SDOs, as well as a thorough revision of the related interaction between NATWORK partners with the WGs mentioned above.

1.1. Purpose and structure of the document

D7.5 “Impact to standardisation bodies, consortiums, and Alliances.r1” concentrates on the relevant standards to cybersecurity and 5G & 6G networks, the related SDOs associated with these standards, as well as the standardisation activities of the NATWORK project, along with the interaction between the NATWORK partners and the 6G-IA, SNS-JU, and NetworldEurope associated Working Groups, as well as policy recommendations.

Following the Introduction, which defines the purpose, audience, and interrelations within the project framework, the sections of the report at hand can be summarized as follows:

- **Section 2 – Standardisation**: Section 2 highlights the importance of standardisation in general and through European Framework Programmes in particular, through a series of benefits. Moreover, this section describes Standards Developing Organizations (SDOs) related to the NATWORK project.
- **Section 3** – **Standardisation Activities**: This section illustrates NATWORK's involvement in ongoing standardisation activities and the relationship between SDOs and the NATWORK partners.
- **Section 4** – **6G-IA, SNS JU and NetworldEurope Working Groups Engagement**: Section 4 pinpoints the NATWORK engagement to Working Groups from 6G Smart Networks and Services Industry Association, Smart Networks and Services Joint Undertaking, and NetworldEurope formal bodies.
- **Section 5** – **Policy Recommendations:** This section presents the NATWORK Policy Brief #1: Transparency in 6G Security, Resilience & Trust, that was formulated to facilitate the EU policy discussions related to connectivity. Although it is not a direct contribution to standards, it can have an indirect impact to standardization activities, thus it is reported as a preliminary outcome of the relevant discussions.
- **Section 6** – **Conclusions**: This section addresses the key aspects of this deliverable, including the importance of standardisation in European Framework Programmes and the related SDOs for NATWORK, as well as the standardisation activities that NATWORK partners are focusing on. In addition, the engagement of NATWORK partners with specific WGs is also presented.

1.2. Intended Audience

The NATWORK Project's D7.5 "Impact to standardisation bodies, consortiums, and Alliances.r1" is devised for public use in the context of standardization activities of the NATWORK consortium, comprising members, project partners, and affiliated stakeholders. The deliverable focuses on the standardization bodies related to the NATWORK project and the standardization activities on which NATWORK partners investigate thoroughly. These activities advance the safety, competitiveness, and interoperability of EU products and services in a systematic manner. Furthermore, the present report demonstrates the engagement by NATWORK partners with WGs that focus on 5G/6G networks and cybersecurity. The deliverable D7.5 can be reviewed by any audience interested in cybersecurity and/or networking. It provides a reasonable basis for these themes and can be further assessed through projects on similar subjects.

1.3. Interrelations

The NATWORK consortium integrates a multidisciplinary spectrum of competencies and resources from academia, industry, and research sectors, focusing on user-centric service development, robust economic and business models, cutting-edge cybersecurity, seamless interoperability, and comprehensive on-demand services. The project integrates a collaboration of fifteen partners from ten EU member states and associated countries (UK and CH), ensuring a broad representation for addressing security requirements of emerging 6G Smart Networks and Services in Europe and beyond.

NATWORK is categorized as a "Research Innovation Action - RIA" project and is methodically segmented into 7 WPs, further subdivided into tasks. With partners contributing to multiple activities across various WPs, the structure ensures clarity in responsibilities and optimizes communication amongst the consortium's partners, boards, and committees. The interrelation framework within NATWORK facilitates smooth operation and collaborative innovation across the consortium, ensuring the interconnection of diverse expertise from various entities (i.e., Research Institutes, Universities, SMEs, and Large Industries), enabling scientific, technological, and security advancements in the realm of 6G.

D7.5 "Impact to standardisation bodies, consortiums, and Alliances.r1" is correlated with T7.4 "Standardisation Activities & Policy Recommendations". Through D7.5, the standards relevant to NATWORK, along with the related mappings that link these standards to the corresponding NATWORK components and services are presented. A direct connection between standards and WP2, where the requirements of NATWORK were established, as well as WP3, WP4, and WP5 – the technical Work Packages that the NATWORK components were structured – is achieved. Furthermore, D7.5 pinpoints the interaction of the NATWORK project with WGs related to the NATWORK themes (5G/6G networking). These themes are associated with WP7 "Dissemination of Results, Exploitation & Standardization" and are reported in the current deliverable.

2. Standardisation

This section examines the significance of the standardisation process through which products and services are safe, interoperable, and of high quality. The benefits of standardisation are described. Additionally, several SDOs relevant to the NATWORK project are portrayed. These standardisation bodies are connected to NATWORK partners explicitly or implicitly.

2.1. Benefits of standardisation

Standardisation is a critical process that promotes the safety, competitiveness and interoperability of products and services throughout the EU. Fostering the standardisation process can identify ways in which project results can be pushed into standards. Through standardization, the most relevant standards activities are being assessed in terms of monitoring and impact. By being active through standards, one addresses the complex landscape of digital technologies and the directions in which direct and uninterrupted responses are needed.

By being active in standardization practices, several benefits arise. More specifically, the benefits of standardisation are summarized as follows [1]:

- **Bridge the gap between research and market**: Through standardisation, the project results are accepted by the market in a uniform and consistent manner.
- **Foster innovation**: Through standardization, a common basis on which technical assessment is performed through formal processes can ensure interoperability and drive innovation.
- **Project results up-to-date with industry standards**: Through standardization, the results of R&D projects can be validated by emerging technologies.
- **Improve product quality**: Standardization helps ensure that products and services are of a consistent quality, which can increase customer satisfaction and reduce the risk of product recalls or defects as the TRL levels of the project components increase.
- **Reduce risks & costs**: Mitigating risks and ensuring dependable performance by using new technologies, for instance, reassures customers and consumers.
- **Reduce time & resources**: Using standardization can help develop, produce and distribute products and services by reducing time and resources used.
- **Share information throughout key stakeholders**: Standardisation enables networking between various stakeholders, including but not limited to scientific and commercial associates at different levels.
- **Additional benefits**: Easier access to public procurement markets is enabled, technical barriers are diminished and technology transfer is facilitated.

2.2. Standardisation Development Organisations related to NATWORK

SDOs are bodies that focus on developing, coordinating, and maintaining technical standards. These standards ensure safety, quality, and interoperability over industries and sectors in a consistent way. Partners from Horizon Projects – including universities, research centres, SMEs, and large corporations – engage with standardisation bodies to establish common procedures and participate in the standards development process.

Specifically for NATWORK partners, there is direct or indirect engagement with specific SDOs. In the table below, the association between NATWORK partners and the SDOs is illustrated:

Table 1: SDO-NATWORK partner co-operation

NATWORK Partner	SDO	WG	Additional information
CERTH	ETSI	TC-CYBER, NFV, ISG RIS	CERTH is an active member of ETSI, participating in several events organised by ETSI, and supporting its activities also through CERTH members that hold vice-director positions and responsibilities within the SDO.
ZHAW	IEEE	1920.2 Vehicle to Vehicle Communications for Unmanned Aircraft Systems Standardisation WG	Dr. Gür (ZHAW) is a core member of this WG. However, the standard is currently under review and in the voting phase at IEEE for approval since 2025. Therefore, a direct impact on the current standard is unlikely. However, NATWORK can have an impact on future versions. So, engagement is ongoing.
ZHAW	IEEE	IEEE P3349 - Space System Cybersecurity Design Standard WG	This WG is relevant from the secure NTN in 6G and secure systems engineering aspects.
IMEC	ETSI	EN 304 635 Virtualisation and Container Execution Systems	IMEC is actively contributing to this EUSR standard, translating expertise gained from NATWORK into essential cybersecurity requirements for CRA compliance.

NATWORK Partner	SDO	WG	Additional information
IMEC	IETF		Indirect connection between NATWORK and IETF technical documentation (Request for Comments), including the classification of edge devices and the concepts (RFC 7228) and definitions for intent-based networking (RFC 9315).
IMEC	OASIS		OASIS focuses on the areas of cybersecurity, supply chain, blockchain, IoT and artificial intelligence. IMEC is a member but not actively contributing. Contributions to OASIS can be further assessed throughout the timeline of NATWORK.
ISRD	Open RAN Alliance		ISRD is a member not actively contributing as of now. ISRD has experience in contributing to WG1 (Use cases and Architecture), WG3 (Near-RT RIC), WG11 (Security)
ISRD	3GPP		3GPP focuses on areas on which NATWORK is associated with, including Radio Access Network (RAN), Core Network and 5G. ISRD is a member not actively contributing as of now, however potential engagements with this SDO will be assessed.
ISRD	TIP		TIP operates as a collaborative ecosystem that brings together network operators, vendors, research institutions, and system integrators to develop practical, implementation-driven solutions. ISRD is a member not actively contributing as of now.
PNET	Open AR Cloud Association (applied) (OARC)		PNET joined the OpenAR Cloud Association in 2024, actively contributing to key working groups by sharing innovations and bringing project results back to the OARC community.
PNET	ETSI	OSL	Used in support of NATWORK Use Cases. The SDG OSL is developing an open-source Operations Support System (OSS) intending to revolutionize

NATWORK Partner	SDO	WG	Additional information
			the delivery of Network Slice as a Service (NSaaS). Video: link
UZH	ITU-T	SG13 - Future networks and emerging network technologies	UZH has a connection with ITU-T Study Group 13 (Future Networks). No dedicated plans for standardization, however UZH can help through ITU-T
MONT	ENISA *	Enterprise Security	Mainly dedicated to raising awareness

(*): It should be noted regarding ENISA that although it is not an SDO, it has a direct link to SDOs; this is accomplished by contributing to the SDOs' standardisation work at the strategic and tactical levels.

In the following sub-sections information for each SDO related to NATWORK project is presented.

2.2.1. ETSI

The European Telecommunications Standards Institute [1] (ETSI) is a leading international standards organization responsible for developing globally applicable standards for information and communications technologies (ICT). Founded in 1988 and recognized by the European Union, ETSI brings together industry, government, academic, and research stakeholders to support interoperability, innovation, and technological harmonization across global markets. With thousands of members from over 60 countries, ETSI plays a pivotal role in shaping key technologies, including mobile communications, cybersecurity, IoT, broadcast, and emerging network architectures, and serves as a central hub for technical collaboration, standardization, and policy alignment within the ICT ecosystem. In the context of NATWORK, this is reflected in the role of the OpenSlice Software Development Group (SDG OSL), which advances open-source implementations aligned with ETSI NFV, TM Forum, GSMA, and ZSM specifications, providing a relevant reference point for orchestration concepts and interoperability practices. Moreover, NATWORK has investigated participation in several WGs, such as TC-CYBER, NFV, ISG RIS, and SDG OpenOP (SDG OOP).

2.2.2. IEEE

IEEE [2] is the world's largest technical professional organization for the advancement of technology. Established in 1963 through the merger of the American Institute of Electrical

[1] https://www.etsi.org/

[2] https://www.ieee.org/

Engineers (AIEE) and the Institute of Radio Engineers (IRE), IEEE serves engineers, scientists, and other professionals in electronics, electrical engineering, computer science, telecommunications, and related areas. With over 400,000 members in more than 160 countries, IEEE has a significant impact on advancing technology worldwide. It acts as a hub for technical authorship, standardization, and professional collaboration, influencing industries, academia, and governmental technology policy.

The IEEE 1920.2 standard for Vehicle-to-Vehicle (V2V) Communications for Unmanned Aircraft Systems (UAS) is developed based on five use cases suggested by the Radio Technical Commission for Aeronautics (RTCA), one of the standards organizations. This standard also includes the message formats and the protocol for V2V communications for UAS.

The IEEE 3349 Standard for Space System Cybersecurity proposes a security-centric, component-based specification designed to underpin the development of future space missions from their inception. It emphasizes the incorporation of robust security principles that are effective against a broad spectrum of threats, including those posed by existing, hypothetical and potential future adversaries. By prioritizing a foundational approach to security, this standard aims to ensure that space missions are designed with inherent resilience against cyber threats, aligning with the evolving landscape of space cybersecurity. It does not seek to replace other standards; instead, where possible, we aim to point to and reference existing work by bodies such as British Standards Institution (BSI), European Cooperation for Space Standardization (EECS), National Institute of Standards and Technology (NIST), and Consultative Committee for Space Data Systems (CCSDS) when their standards granularity suits the required bottom-up secure-by-design approach.

2.2.3. IETF

The Internet Engineering Task Force[3] (IETF) was founded in 1986 and is the premier SDO for Internet and network-related technologies. The IETF provides voluntary standards that are often adopted by Internet users, network operators, and equipment vendors, helping to shape the development and trajectory of Internet technology. Furthermore, many of these standards are continually updated as new challenges appear.

According to their mission statement[4], the goal of IETF is:

"To produce high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better.

[3] https://www.ietf.org/

[4] https://www.rfc-editor.org/info/rfc3935

These documents include protocol standards, best current practices, and informational documents of various kinds."

IETF has produced over 9000 Request for Comments (RFCs) which allow for community input to standardize technologies and practices, including technologies such as IPv4 and the Transmission Control Protocol, which form the foundations of the Internet. Although many RFCs are informational and not officially endorsed by the standards development process[5], they may still be used as guidelines. Of more specific interest to the NATWORK project, example RFCs include the classification of edge devices (or microcontrollers, RFC 7228), and concepts and definitions for intent-based networking (RFC 9315). IETF standards can be considered throughout the development of NATWORK components.

2.2.4. OASIS

The Organization for the Advancement of Structured Information Standards (OASIS) is a consortium allowing individuals, organizations, and industry to collaborate on open solutions and technical standards[6]. Their stated goal is "*to advance the fair, transparent development of open-source software and standards through the power of global collaboration and community*".

OASIS has a long-standing history, being founded in 1993 as SGML Open, a collaboration of industry vendors, changing to OASIS in 1998 as its scope expanded to include other topics such as artificial intelligence, cybersecurity, supply chain, blockchain, and IoT.

The organization offers three key programs to support projects and aid in standardization:

- **Technical Committees** develop specifications through an open, lightweight process with a path to recognition in international policy and procurement, achieving both integrity and rapid progress.
- **Open Projects** provides collaborative communities with foundation-level support, IP and license management, stakeholder governance, an open process, etc. With Open Projects, communities can develop what they choose: code, APIs, standards, reference implementations, all under open-source licenses.
- **Technical Advisory Groups to ISO** represent the interests of American organizations and enable the US to have a voice in the global standards produced by the International Organization for Standardization (ISO).

[5] https://datatracker.ietf.org/doc/rfc2026/

[6] https://www.oasis-open.org/

2.2.5. Open RAN Alliance

The O-RAN Alliance[7] is a global community of over 300 mobile operators, vendors, and research/academic institutions in the RAN industry. Its mission is to develop architectures, specifications, and initiatives that promote open standards, software-based functions, microservices, and white-box hardware for radio access networks. The Alliance aims to drive the commercial success of mobile broadband, fostering investment, innovation, and the adoption of services that benefit both end-users and the broader mobile ecosystem. Participation is open to members and participants (contributors and academic contributors), while stakeholders that could harm the Alliance's objectives are excluded.

Within the O-RAN Alliance, work is organized through several types of groups that guide the development and evolution of open and intelligent RAN architectures. Working Groups (WGs) develop technical specifications and define network architectures to ensure interoperability, while Focus Groups (FGs) address cross-cutting strategic topics, providing guidance, recommendations, and coordination across WGs. The Technical Steering Committee (TSC) oversees technical matters, approves specifications before Board review, and includes Member and Participant delegates as well as WG and FG co-chairs, with each WG/FG having operator (Member) and vendor (Participant) co-chairs. The TSC, together with the Board, also supervises the Next Generation Research Group (nGRG), which explores open and intelligent RAN concepts beyond 5G, producing research reports, requirements, and testbed evaluations for 6G and future networks [2].

2.2.6. 3GPP

The 3rd Generation Partnership Project (3GPP) is a global collaboration of telecommunication standards organizations responsible for developing technical specifications for mobile communication systems[8]. Established in 1998, 3GPP brings together seven regional Standards Development Organizations (SDOs) such as ETSI, ATIS, and TTC, as well as hundreds of industry members, including network operators, equipment vendors, chipset manufacturers, and research institutions. Its scope has evolved significantly over time: while it initially focused on 3G (UMTS), it later expanded to define the complete ecosystems of 4G LTE, 5G, and ongoing 6G technologies.

3GPP operates through a structured framework divided into Technical Specification Groups (TSGs), each responsible for specific domains. The key groups— Radio Access Network (RAN),

[7] https://www.o-ran.org/

[8] https://www.3gpp.org/about-us

Service and System Aspects (SA), and Core Network and Terminals (CT)—work in parallel to develop harmonized standards that ensure interoperability, performance, and scalability across global mobile networks. The output of these groups is organized into "Releases," each representing a stable set of features and enhancements. For instance, Release 15 defined the first phase of 5G New Radio, while subsequent releases introduced advanced capabilities such as network slicing, ultra-reliable low-latency communication, and integrated non-terrestrial networks.

By enabling a common technical foundation, 3GPP is crucial for global compatibility, vendor interoperability, and predictable evolution of mobile technologies. For technical projects, alignment with 3GPP standards ensures that system designs remain future-proof, compliant with industry expectations, and capable of integrating seamlessly into the broader telecommunications ecosystem.

2.2.7. TIP

The Telecom Infra Project (TIP) is a global industry initiative founded in 2016 to accelerate the development and deployment of open, disaggregated, and interoperable telecommunications infrastructure[9]. Unlike traditional standards bodies, TIP operates as a collaborative ecosystem that brings together network operators, vendors, research institutions, and system integrators to develop practical, implementation-driven solutions. Its mission is to reshape the telecom supply chain by promoting openness and flexibility, reducing vendor lock-in, and enabling faster innovation cycles.

TIP organizes its work into Project Groups, each focused on specific segments of the telecom network—such as OpenRAN, Optical & IP, and Edge Computing. These groups work on reference designs, test plans, and validated blueprints rather than formal standards. Through TIP's community labs and trial environments, technologies are tested in real-world conditions, ensuring that proposed architectures are robust, interoperable, and commercially viable. This hands-on, deployment-oriented approach complements formal standardization efforts from organizations like 3GPP by translating high-level specifications into practical, multi-vendor solutions.

A crucial outcome of TIP's work is the TIP Exchange, a marketplace where operators can evaluate compliant products and solutions tested against TIP-defined requirements. By fostering openness and collaboration, TIP plays a significant role in driving diversification of the telecom ecosystem and accelerating innovation in areas such as Open RAN, transport networks, and

[9] https://telecominfraproject.com/who-we-are/

cloud-native architectures. For technical projects, engagement with TIP frameworks and solutions helps ensure alignment with emerging industry trends and supports the adoption of flexible, future-ready network architectures.

2.2.8. Open AR Cloud Association

The OpenAR Cloud Association (OARC)[10] was founded in 2018 in the US and the European arm in 2022 with a mission "to drive the development of open and interoperable AR Cloud technology, data and standards to connect the physical and digital worlds for the benefit of all". This is a growing association of more than 50 companies, institutions and standards organizations focusing on the creation of an Open Spatial Computing Platform.

The OARC Working Groups (WG) are the primary method by which members tackle the challenges facing the successful achievement of real-world spatial computing usage every day and for the benefit of all of humanity. The WGs of the OARC are shown below.

1. Spatial Indexing & GeoPose
2. Reality Modeling/Mapping (Spatial Data Creation)
3. Content Delivery, Browsing & Ownership
4. Privacy
5. Edge-Computing, IoT, and 5G for AR-Cloud
6. Security
7. Compliance, Regulations, and Legal
8. User Experience, Accessibility, and Safety
9. Open Source, Open Data and Open R&D
10. Organization and Community
11. Distributed Ledger Technology (DLT) and decentralized apps for AR-Cloud

PNET joined the OpenAR Cloud Association in 2024 and has been an active member in selected working groups. PNET's participation is focused on bringing new developments and learnings to relevant projects and at the same time, disseminate projects' results to the OARC community.

2.2.9. ITU-T

The ITU Telecommunication Standardization Sector[11] (ITU-T) is the UN body that sets standards for global telecommunications and ICT. It develops "Recommendations" that are agreed upon

[10] https://www.openarcloud.org

[11] https://www.itu.int/en/ITU-T/Pages/default.aspx

internationally to ensure that fixed, mobile, satellite, and emerging digital infrastructures can all work together.

UZH has a documented history of involvement in ITU-T Study Group 13 (Future Networks). The tussle-analysis method for assessing the socio-economic effects of future networks was incorporated into Recommendation Y.3013 [3], and UZH's Communication Systems Group reported its role in that work. This enables the examination of trade-offs between the interests of different stakeholders when deploying machine learning-driven network control or large-scale IoT platforms. As a result, there is a clear connection between UZH's past influence on ITU-T Recommendations and its current work on AI-based network intelligence and IoT ecosystems [4][5][6].

2.2.10. ENISA

ENISA[12], the European Union Agency for Cybersecurity, is the EU's dedicated cybersecurity hub, working to achieve a high, common level of digital security across Europe by providing expertise, developing certification schemes, building capacity, and fostering cooperation between member states and EU bodies to tackle cyber threats and ensure a secure digital future. Established in 2004 and strengthened by the EU Cybersecurity Act, ENISA supports EU cyber policy, boosts trust in digital products, and helps prepare for future cyber challenges through knowledge sharing and capacity building.

MONT participated in the ENISA AdHoc Working Group (WG) on Enterprise Security. It presented and provided tools for improving the user awareness of cyberthreats and phishing attacks. This working group has now completed its planned lifespan.

[12] https://www.enisa.europa.eu/

3. Standardisation Activities

In the period leading up to this deliverable, NATWORK partners have been involved in various engagements with different standardization organizations. They have communicated the preliminary NATWORK results to those groups and worked to disseminate and exploit these outcomes from a standardization perspective.

3.1. ETSI Software Development Group for OpenSlice

PNET has been actively contributing to the ETSI Software Development Group for OpenSlice (SDG OSL), where its Technical Director, Dr. Christos Tranoris, also serves as the Chair of the group. This close involvement enables a continuous exchange of insights between NATWORK and OSL, particularly regarding orchestration concepts and open-source implementation practices. While OSL is not directly integrated into NATWORK developments, its principles and tooling serve as a reference framework for guided orchestration patterns within the project. Similarly, the experience and technical outcomes from NATWORK may inform future OSL discussions and enhancements where relevant.

In this context, PNET has contributed to the following activities within ETSI SDG OSL:

- Definitions and implementation of Kubernetes operator to deploy new Kubernetes clusters on top of OpenStack.
- Definitions and implementation of Kubernetes operator to deploy open source 5G systems (Open5GS) in a Kubernetes cluster.
- Implementation of CI/CD deployment cycles on ETSI SDG OSL GitLab repository.
- Support for deploying HELMs in a Kubernetes system, which involves enabling OSL to easily manage HELM charts installations via Service Orders and allowing them to install HELM-chart-based applications in end-to-end complex services.

Through these actions, PNET ensures that NATWORK remains aligned with the latest developments in service orchestration and standardisation practices, while maintaining a realistic, forward-looking connection with the ETSI SDG OSL community.

3.2. IEEE

ZHAW contributed to IEEE 1920.2 and IEEE 3349 standardization activities related to secure and trustworthy networks from the perspective of aerial and space networks. In this regard, the outcomes of the NATWORK project were communicated to the members of IEEE 1920.2 Working Group in respective meetings. Dr. Gür (ZHAW) is a core member of this WG. However, the standard is currently under review and in the voting phase at IEEE for approval since 2025. Therefore, a direct impact on the current standard is unlikely. However, NATWORK can have an impact on future versions. So, engagement is ongoing.

Moreover, the secure systems engineering approach developed in the IEEE P3349 Working Group was adopted as an alternative for T5.1 activities and evaluated in D5.1. Therefore, the interaction between the NATWORK project and these IEEE Working Groups was two ways.

3.3. O-RAN WG11 xApp Remote Attestation

ISRD, together with TSS, prepared initial technical input on the remote attestation of ISRD's produced xApps with TSS runtime integrity technology, which is developed under T3.4. TSS performed a state-of-the-art analysis of the O-RAN Alliance Specifications and Technical reports, concluding that the O-RAN Alliance places great emphasis on specifying xApp security. It was identified that WG11 calls out for remote attestation of the complete O-Cloud software stack (including applications). In addition, in O-RAN.WG11.TR.AppLCM-Security-R004-v04. 00, it calls for runtime integrity verification, but without delivering a solution. It is worth noting that it also notices performance challenges, which the TSS's solution developed in the NATWORK project addresses. Thus, this field will be the most suitable for proposing the NATWORK xApp remote attestation solution to be included as a standardized procedure. The next step, after finalizing the internal approval from both partners, is to bring it as a Change Request (CR) to the O-RAN Security Requirements and Controls Specifications 13.0 (as a requirement) by Dr. Maria Safianowska (ISRD).

3.4. ETSI EUSR

IMEC has been contributing to the ETSI European Union Standardisation Requests (EUSR) vertical standard for *"Virtualisation and Container Execution Systems"*. This work is a collaboration with the CRACY[13] project to translate the expertise gained in NATWORK about container and virtual

[13] https://cra-cy.eu

machine security into a CRA compliance framework of cybersecurity requirements for products with digital elements.

IMEC is an active participant in the regular “VES/CES CRA Vertical Standard” meetings and has proposed several additions to the standard, such as a new framework for applying security requirements to different hypervisor architectures, and modifications to the requirements for container runtime systems.

Through these actions, IMEC ensures that the CRA requirements for hypervisors and container systems are aligned with the best practices and cybersecurity research insights.

3.5. ETSI Software Development Group for OpenOP

Starting in the first quarter of 2026, CERTH will take the necessary steps to join the activities of the ETSI Software Development Group OpenOP (SDG OOP). Initial discussions have already started during December 2025. This group aims to deliver an Open-Source Operator Platform enabling operator network and testbed federation, along with standardized capability exposure APIs. The NATWORK consortium plans to conduct targeted harmonisation and standardisation work within the SDG OOP along with sibling projects with analogous outcomes.

4. 6G-IA, SNS JU and NetworldEurope Working Groups Engagement

This section outlines the engagement of the NATWORK project with the associated working groups (WGs) that have been formed to address specific issues related to 5G and 6G networking. The WGs that the NATWORK project is engaged with are governed by the following formal entities:

- 6G Smart Networks and Services Industry Association
- Smart Networks and Services Joint Undertaking
- NetworldEurope

NATWORK project, through T7.4 "Standardisation Activities & Policy Recommendations", appointed explicitly representatives to the WGs that are related to NATWORK activities. Nine (9) partners have representatives in these WGs. These representatives commit to constructive communication and cooperation with these entities. In the table below, the relevant WGs, the partner or partners that are engaged with the WG, and the actual representative per partner are depicted:

Table 2: Association between NATWORK partners, representatives and 6G-IA, SNS JU and NetworldEurope WGs

Type	Working Group	NATWORK Partner(s)	Representative
6G-IA	Vision	1. UESSEX	Mays AL-Naday
6G-IA	Pre-Standardisation	1. PNET	Vaia Kalokidou
6G-IA	5G/6G for Connected and Automated Mobility (CAM)	1. CERTH	Antonios Lalas & Vangelis V. Kopsacheilis
6G-IA	Spectrum	1. GRADIANT	Joaquín Escudero
6G-IA	Security	1. CERTH 2. GRADIANT 3. UEssex 4. ZHAW 5. TSS 6. ELTE 7. MONT	1. Antonios Lalas 2. Joaquín Escudero 3. Mays AL-Naday 4. Gürkan Gür 5. Vincent Lefebvre 6. Mohammed Alshawki 7. Edgardo Montes de Oca
6G-IA	Women in Telecommunication and Research (WiTaR)	1. GRADIANT 2. CERTH 3. p-NET	1. Aurora Paz Perez 2. Ioanna Kapetanidou 3. Dr. Vaia Kalokidou & Didoe Prevedourou

Type	Working Group	NATWORK Partner(s)	Representative
SNS JU	6G Architecture	1. CERTH 2. ISRD	1. Antonios Lalas 2. Md Arifur Rahman
SNS JU	Reliable Software Networks	1. ELTE 2. ISRD 3. CERTH	1. Sándor Laki 2. Adam Flizikowski 3. Antonios Lalas & Vangelis V. Kopsacheilis
SNS JU	Technology Board Member	1. CERTH 2. PNET	1. Antonios Lalas 2. Dr. Christos Tranoris
SNS JU	Sustainability	1. UESSEX	Dr. Mays AL-Naday
NetworldEurope	SME	1. PNET 2. MONT 3. ISRD 4. TSS	1. Didoe Prevedourou & Roula Ioannou 2. Edgardo Montes de Oca 3. Adam Flizikowski 4. Vincent Lefebvre
NetworldEurope	Enabling Technologies for Future Vertical Ecosystem Transformation	1. CERTH	Antonios Lalas

In the following sub-sections, NATWORK engagement with SNS-JU, 6G-IA, and NetworldEurope Working Groups is described in detail.

4.1. 6G-IA Working Groups

This section presents the 6G-IA WGs in relation to the NATWORK project. These WGs are open to 6G-IA members and representatives of ongoing SNS JU projects (NATWORK is part of SNS JU projects). Through ongoing engagement with 6G-IA WGs, collective views on 5G and 6G areas are discussed and related context is published through white papers. The engagement with 6G-IA WGs is active and several representatives participate in WG meetings regularly. Furthermore, NATWORK contributions towards the 6G-IA WGs are depicted in the following sub-sections.

One can find additional information on 6G-IA WGs in the following link: https://6g-ia.eu/6g-ia-working-groups

4.1.1. Vision

UESSEX has been an active member of the Vision WG in 6G-IA, regularly attended WG meetings since 2022 and continued throughout the NATWORK project so far. Within this engagement, UESSEX has contributed into a number of activities and outputs including:

- Co-author and co-edit the white paper (where NATWORK innovation is cited): SUSTAINABILITY OF 6G: WAYS TO REDUCE ENERGY CONSUMPTION[14]
- Contributed to the Sustainability workshop organised alongside EUCNC 2025
- Contributed to an industry-driven panel on sustainability, alongside CSCN 2025

4.1.2. Pre-Standardisation

PNET is an active member of the 6G-IA Pre-Standardisation group and has been sustaining a close relationship with ongoing standardization efforts (3GPP, O-RAN Alliance, ETSI, ITU-R) and focuses its efforts in having a more active role in the influencing and roadmap development of standardisation and monitor all recent advancements closely.

PNET attended the Pre-Standardisation Working Group meeting on October 15th, 2025, maintaining its active engagement in standardisation-related activities. During the meeting, it followed key updates from 3GPP plenaries, particularly on Release 19 and 20 developments, as well as presentations on Reflective Intelligent Surfaces (RIS), recent ETSI ISG ENI work, and the operationalization of Key Value Indicators (KVIs).

PNET also attended the meeting of November 19th, where a presentation (from Alliance for AI, IoT and Edge Continuum Innovation (AIOTI)) on the INSTAR project was made, followed by discussions on potential collaboration opportunities with Pre-STD WG. Then, there was a debrief from Techritory 2025, a joint WiTaR-Pre-Std workshop “Advancing research and pre-standardisation synergies in emerging technologies”. A conversation was initiated on a special potential session proposal for EUCNC 2026, collaborating with ITU-T AI native network focus group.

PNET attends the group’s monthly meetings, during which events (such as TECHNOTRON) engagement activities are planned, and important ongoing standardization developments are discussed.

[14] https://6g-ia.eu/wp-content/uploads/2025/01/sustainability_of_6g-path_forward_v1.2.2.pdf

4.1.3. 5G/6G for Connected and Automated Mobility WG (CAM)

CERTH is a member of the 6G-IA 5G/6G for Connected and Automated Mobility Working Group. CERTH represents the NATWORK consortium in this Working Group (WG) since October 2025. The WG meets on a regular basis every two weeks. So far, CERTH has participated in discussions regarding two main expected outcomes of the group over the following months.

The first refers to an envisioned White Paper. The WG put efforts to finalise the structure (ToC) of a White Paper entitled: “6G for Connected and Automated Mobility (CAM) – Current Status and EU Vision for 2030+”. The Working Group is aiming to complete the writing of the document in time so it will be ready for distribution in the same period with the realization of the EuCNC 2026 event.

In addition, since October 2025, CERTH has participated in the Working Group efforts to elaborate and prepare a Webinar entitled “Overview of SNS CAM Ecosystem”. This followed the format of an online workshop and realised successfully on December 12, 2025. The goal of this action was to provide a comprehensive overview of the current status in research, CEF projects, standards, policy/regulation, and related initiatives (5GAA, CCAM Partnership, OEMs). Also, to support the development of a white paper and recommendations for FP10 topics within SNS JU and Cluster 5. In the above concept, CERTH provided to the WG structured information on NATWORK that will cover key aspects such as the project-id, the use cases, lessons learned and research outcomes, market-oriented insights, expected impact standardisation, regulation and deployment, as well as future challenges that may influence FP10 and 6G strategy.

4.1.4. Spectrum

GRAD is a member of the 6G-IA Spectrum Working Group and has regularly attended its meetings. This WG focuses on the regulatory and technical aspects of the radio spectrum for beyond 5G and future 6G systems. GRAD follows discussions about the progress of 6G spectrum across the regions. Many candidate bands still face uncertainty and require further study. Europe is taking a cautious approach, and global alignment remains a challenge.

4.1.5. Security

CERTH is a member of the 6G-IA Security Working Group and attends meetings. CERTH has contributed to the “Innovative Approaches for 6G Security” White Paper in 2025, leveraging its NATWORK outcomes regarding an AI-driven framework for Physical Layer Security (PLS). CERTH also presented the project status in the WG meeting (January 2025), with emphasis on the concepts, the objectives and challenges and also implementation aspects such as the architecture and the pilot cases, while it participated in the security workshop organized during EuCNC & 6G Summit 2025.

GRAD is a member of the 6G-IA Security Working Group and regularly attends meetings. GRAD has contributed to the “Innovative Approaches for 6G Security” White Paper in 2025, leveraging its NATWORK outcomes regarding an AI-driven framework for Physical Layer Security (PLS). Additionally, GRAD has presented the poster “Machine Learning-Enhanced Physical Layer Key Generation in OFDM Sub-THz Systems” at the EuCNC & 6G Summit 2025.

ZHAW is a member of the 6G-IA Security Working Group. It is an active member and attends regular working group meetings. ZHAW has also contributed to the 2025 Edition of the 6G-IA Security Work Group White Paper with its NATWORK outcomes regarding AI-powered Moving Target Defense (MTD).

MONT is participating in the 6G-IA Security WG and will present work accomplished concerning the security of 6G networking resulting from NATWORK.

ELTE is a member of 6G-IA Security Working Group, represented by Dr. Alshawki, who is a participating member and attends the regular monthly meetings of the work group. Additionally, ELTE has partially participated in the editing of the 2025 Edition whitepaper regarding the security of federated learning, to be continued by the next edition with further results.

TSS is a member of the 6G-IA Security Working Group, represented by Vincent Lefebvre, who is a participating member and regularly attends the monthly meetings of the working group. Additionally, TSS contributed to the preparation of the new edition of the security white paper (submitted at the end of November 2025), notably highlighting our work on WebAssembly (WASM) module runtime integrity verification. We will also contribute to the 2026 edition, with ongoing work focused on bringing confidentiality to WASM modules and, separately, to containers, along with a fully automated, zero-touch integrity verification process orchestrated by blockchain technology.

4.1.6. Women in Telecommunication and Research (WiTaR)

PNET (Didoe Prevedourou and Vaia Kalokidou), **GRAD** (Aurora Paz Pérez) and **CERTH** (Ioanna Kapetanidou) are active members of the 6G-IA WiTaR working group. Their participation in WiTaR is driven by a strong commitment to support an initiative that promotes women in engineering and technology, highlighting their achievements and engagement in leadership positions, and fosters inclusivity and diversity in the wider community, with the vision to influence the policies that should be implemented in the direction of closing the gender gap. PNET attends the group’s monthly meetings, during which event engagement activities are discussed and planned. GRAD has facilitated communication among working group members at events such as IEEE ICMLCN and MWC, both of which were held in Barcelona. WiTaR meetings, held periodically, take the form of round-table discussions and revolve around topics such as upcoming events attended by members, organizing talks and panel discussions, and fostering networking opportunities among different organizations.

4.2. SNS JU Working Groups

SNS JU WGs assess the inter-project cooperation of SNS JU projects. Through the WG activities, project partners examine the technical areas on which the projects are based. The goal of these interactions is to foster constructive synergies between partners and / or projects. The outcome of these discussions is circulated through white papers. In the following subsections, the NATWORK activities related to SNS JU WGs are illustrated.

Additional information can be found under https://smart-networks.europa.eu/sns-ju-working-groups/

4.2.1. 6G Architecture

CERTH is a member of the 6G Architecture Working Group and regularly attends meetings, participating in relevant discussions. CERTH also presented the NATWORK project status in the WG meeting (April 2025) with emphasis on the concepts, the objectives and challenges and also implementation aspects such as the architecture and the pilot cases.

ISRD regularly takes part in the workgroup meetings and follows the discussions. This Working Group aims to provide a shared platform for SNS JU projects to exchange and align on the development and validation of architectural concepts and components, ultimately forming a unified European vision of the 6G architecture. Results from the SNS JU Architecture Working Group will be disseminated via white papers, international conferences and workshops, as well as targeted bilateral and multilateral workshops with global stakeholders. ISRD is prepared to report the relevant developments of NATWORK.

4.2.2. Reliable Software Networks

CERTH, ELTE and **ISRD** take part in the work of SNS JU Reliable Software Networks working group and have attended most of the meetings. The second-phase projects, including NATWORK, were presented in the working group meetings this year. ELTE contributed to the WG as a section editor of the whitepaper “Network & Service Management Advancements - Key frameworks and Interfaces towards open, Intelligent and reliable 6G networks” and to the Special Session “Software-based evolution towards the 6G era in telecommunications” at EUCNC 2025. NATWORK was introduced in May 2025 by means of a project overview distributed to the group. On 22 May 2025 CERTH gave a presentation of the project with emphasis on the concepts, the objectives and challenges and also implementation aspects such as the architecture and the pilot cases.

In the upcoming period, ELTE plans to present the project's software solutions in mini-workshops or in new whitepapers initiated by the WG. In addition, starting in January 2026, CERTH will contribute to the authoring of a new White Paper entitled “AI/ML Frameworks for smart networks and services”, a joint effort of projects participating in the Working Groups under the coordination of the WG chairman. The white paper is expected to be completed and revised before EUCNC 2026, so it can be presented and discussed in the frame of the event. Furthermore, CERTH with the participation of other consortium partners will put efforts in the standardisation domain under the frame of joint activities between ITU-T and 6G-IA. The ITU has issued a Liaison Statement to the 6G-IA concerning the ITU-T Focus Group on AI-Native Telecommunication Networks (FG-AINN). FG-AINN invites contributions on use cases, gap analyses, architectures, and proof-of-concepts, while 6G-IA seeks broad consensus aligned with the priorities of the SNS JU community. The Focus Group scheduled the composition of five (5) technical reports and specification documents. The targeted delivery dates of the five expected documents span over the period June to September 2026.

4.2.3. Sustainability

UESSEX has been active member of the Sustainability WG of SNS JU, since joining in June 2025. Activities included:

- Attending WG meeting over September – December 2025,
- Presenting NATWORK innovation and progress on sustainability in the WG meeting on 21st Nov 2025, including presentation of one of NATWORK demonstrators
- Contribution (co-authorship) to a sustainability white paper, currently being drafted by the WG. Particularly focusing on the interplay between cybersecurity and sustainability of 6G ecosystems and how different SNS projects approach the trade-offs posed by the different requirements.

4.2.4. Technology Board

CERTH is a member of the SNS JU (Smart Networks and Services Joint Undertaking) Technology Board (TB) and regularly attends meetings, participating in relevant discussions. Dr. Antonios Lalas, the deputy-coordinator and technical manager of NATWORK represents the project. CERTH reinforces its relationships with other stakeholders involved in Europe's 6G research and innovation framework, while communicates important aspects of research and innovation activities of the project. CERTH will host the next SNS JU TB meeting to be held in Thessaloniki on the 21st of May 2026, thus further enhancing the collaboration under the SNS JU with relevant stakeholders.

PNET's Technical Director, Dr. Christos Tranoris, is also a member of the SNS JU Technology Board, representing the company within the broader 6G ecosystem. Through this role, PNET attends meetings and follows discussions on the technological priorities and ongoing initiatives of the SNS programme. Through this engagement, PNET is able to reinforce its relationships with other stakeholders involved in Europe's 6G research and innovation framework, stay informed of strategic developments and maintain awareness of emerging directions in the European 6G landscape.

4.3. NetworldEurope Working Groups

NetworldEurope is the European Technology Platform (ETP) focusing on communications networks and services. ETP follows the European changing policies as stated in the Horizon Europe programme. An objective for ETP is to cooperate with any kind of research discipline, technology, or geographical area. Engagement in NetworldEurope is throughout the Horizon Europe participants, including universities, research centres, SMEs, and large corporations. This section describes the activities undertaken by NATWORK partners towards the NetworldEurope WGs.

More information can be found at https://www.networldeurope.eu/vision-mission/

4.3.1. SME

PNET is active member of the NetworldEurope SME Working Group. They attend all group meetings, provide material for the "Find your SME" web page, and the SME brochure annually, make presentations and promote the group's work.

PNET took part in the NetworldEurope SME Working Group meetings on September 9th and October 30th, 2025. This shows its ongoing involvement with the SME community. PNET contributed updated profile information and success stories for the upcoming SME brochure. It also noted the launch of the ENVELOPE Program's second call and other Working Group initiatives, highlighting its commitment to following collaborative opportunities. In the October meeting, PNET participated in discussions about improving SME visibility and engagement and stayed updated on news from the SNS 2025 call, Strategic Research and Innovation Agenda (SRIA) development, and SCoDIHNet activities. By actively attending and contributing, PNET remains a visible and engaged part of the NetworldEurope SME ecosystem.

MONT participates in the WG meetings, contributed to the brochure by providing its company profile and success stories, and is participating in the task force elaborating the SME position paper.

4.3.2. Enabling Technologies for Future Vertical Ecosystem Transformation

CERTH is a full member of NetworldEurope. Members of the NATWORK consortium have attended the Special Session "Unlocking 5G-Advanced and 6G for Verticals Through Service Based Architecture, Network Exposure and Network APIs", an event organised by the Enabling Technologies for Future Vertical Ecosystem Transformation working group in the frame of EUCNC & 6G Summit, held on 5 June 2025 at Poznan, Poland.

NetworldEurope is the European Technology Platform for communications networks, uniting industry, SMEs, and academia to shape Europe's digital future. It develops research agendas, produces strategic papers, and supports EU policy for 5G/6G. The platform fosters collaboration, strengthens innovation, and guides European research priorities in next-generation communication technologies.

The NetworldEurope Enabling Technologies for Future Vertical Ecosystem Transformation working group, focuses on aligning core communication technologies with the needs of diverse vertical industries, especially in the transition toward 6G. It fosters collaboration between telecom and sector stakeholders to share long-term roadmaps, define functional requirements, and explore architectural integration and transformation opportunities beyond 5G/6G. Its work spans technological and economic dimensions, addressing business model evolution and collaboration across sectors, initially focusing on manufacturing, automotive, healthcare, transportation, robotics, and energy. The working group also develops white papers and hosts sessions to support research, standardization, and innovation in transforming vertical ecosystems.

5. Policy Recommendations

Europe stands at a pivotal juncture in the evolution of connectivity. The transition from 5G and beyond into 6G (or "beyond-5G/6G") is not just a technological advance but also a strategic enabler for industrial competitiveness, secure digital infrastructure, and societal transformation. The European Union is approaching 6G as both a strategic industrial policy and a societal/digital policy priority. Policy action combines research funding (notably the Smart Networks and Services Joint Undertaking — SNS JU), spectrum planning, security rules and standardisation coordination, and longer-term ecosystem building (research-industry-state alignment). The EU's SNS JU is the central governance and funding vehicle for pre-commercial 6G R&I in Europe. It pools EU funds with industry contributions (large-scale co-investment) and issues competitive calls to drive targeted research streams. The SNS JU also aims to align member states and industrial stakeholders to create a coherent European 6G ecosystem.

This section presents the NATWORK Policy Brief #1: Transparency in 6G Security, Resilience & Trust, that was formulated in order to facilitate the EU policy discussions related to connectivity. Although it is not a direct contribution to standards, it can have an indirect impact to standardization activities, thus it isreported as a preliminary outcome of the relevant discussions.

5.1. EU policy key priorities

1. **Security-by-design and trustworthy connectivity.** EU policy places high importance on secure-by-design networks (reflecting past concerns like the 5G toolbox and the EU's cyber agenda). Recent calls show that the Commission wants 6G R&I to bake in confidentiality, integrity, availability and resilience from the architecture level upward.
2. **Industrial sovereignty and ecosystem building.** Europe seeks a competitive domestic 6G ecosystem — from chips and photonics to system software and testbeds — via co-funding models that bind industry to public research. This is intended to reduce strategic dependencies and secure supply chains for critical communications. The SNS JU mechanism and associated SRIA (Strategic Research & Innovation Agenda) steer investments to fill industrial gaps.
3. **Spectrum policy and timing.** Allocation of mid-band and upper mid/low-high bands (including the contentious upper 6 GHz) is a policy lever that directly affects 6G feasibility and competitiveness. In 2025 debates, regulators, operators and industry groups clashed over whether to reserve parts of the upper 6 GHz for mobile (future 6G) vs. unlicensed Wi-Fi use — a battle that will shape Europe's capacity to deliver wide-area, high-capacity

6G services. National regulators, the Radio Spectrum Policy Group (RSPG) and CEPT are central actors here.

4. **Transatlantic and global alignment.** The EU is coordinating roadmaps and joint positions with international partners (notably the U.S.) to align research agendas, interoperability and standardisation priorities. Joint roadmap papers and 6G-IA stakeholder outputs demonstrate a pragmatic approach: collaborate where possible (research, testbeds, standards) while protecting strategic national interests.
5. **From research to experimentation to deployment.** The SNS JU model explicitly funds a progression: research → pan-EU federated testbeds → trials → pre-commercial deployments. Funding streams (STREAM-B for technology/security, STREAM-C for experimental infra) reflect policy intent to support not only theoretical advances but also federated, real-world validation across member states.

5.2. Trends in EU policymaking

- **Mission-oriented, industry-co-funded programmes.** The SNS JU exemplifies the EU's preference for public-private joint undertakings (co-investment, shared governance) rather than purely grant-driven research. This encourages uptake and faster industrialisation of research outputs.
- **Security and resilience elevated to first-class goals.** Security is no longer an afterthought; rules, call texts and work programmes demand measurable reliability and security properties for network elements and services. This will likely lead to EU-specific certification/regulatory instruments alongside international standards.
- **Spectrum diplomacy is policy-critical.** Europe's ability to secure spectrum suitable for 6G is being contested domestically and internationally — and policy outcomes will materially affect Europe's 6G competitiveness. Expect policies combining technical studies, stakeholder consultations and RSPG/CEPT recommendations (Radio Spectrum Policy Group and the European Conference of Postal and Telecommunications Administrations.
- **Coordination with broader tech policy (AI, cyber, semiconductors).** 6G policy is intersecting with policies on AI safety, chip sovereignty (chips for radios/AI at the edge) and cybersecurity frameworks — leading to cross-policy initiatives and combined funding instruments (e.g., microelectronics and secure edge compute).

5.3. NATWORK project overview

NATWORK is a three-year research project launched on 1st January 2024, funded by the EU under

Topic HORIZON-JU-SNS-2023-STREAM-B-01-04. The ambition of the project is to set the foundations and deploy the very first economically realistic, energy efficient and viable bio-inspired AI-based 6G cybersecurity and resilience framework for intelligent networking and services, taking a holistic approach and considering all elements in a cross-sector business environment to address the diverse requirements and challenges that arise. The NATWORK project aims to develop a novel AI-leveraged self-adaptive security mechanism for 6G networks based on resilient bio-mimicry principles. It also progresses a blockchain-based remote attestation which establishes continuous service and software component trust, without depending on hardware or system dependency or inducing performance overhead. The goal is to improve the malleability and the self-resilience of future 6G network ecosystems to offer augmented and secure services at the lowest energy costs. The principle premise is to empower various entities of 6G ecosystems with the ability to self-regulate their conditions to provide service continuity in compliance with service SLAs. The Secure Federated Learning architecture of NATWORK is based on decentralized defensive AI models embedded in disaggregated 6G network physical layer, smart Edge Network Interface Cards and RAN devices with P4-based programmable data plane and advanced DPU acceleration, with local feature extraction at wire-speed and AI model training. Among the key 6G security challenges that NATWORK aims to alleviate are Moving Target Defence and adaptive response to incidents. Also the employment of Net Zero AI and energy-efficient security for sustainable networks, the detection of new attack types and establishing end-to-end security for deploying payloads, enabling secure migration of in-network operations and distributed computations.

5.4. NATWORK insights

The project is currently at the end of its 2nd year. During the project evolution so far, its results and experimentation allowed the consortium to reach a spectrum of insights that may have potential interest for policymaking in the near future. The project achieved so far the following results:

- **Architecture & Orchestration:** Defined a modular 6G architecture with federated slice orchestration across edge, RAN and core networks. Developed intent-based security management**,** blockchain-based integrity verification, and in-network AI for threat detection.
- **AI for Security:** Delivered a federated AI framework (AI-as-a-Security-Service) with explainable AI components, runtime attestation, and secure orchestration across containers, VMs and WASM environments.

- **Physical-Layer Defence:** Created models and testbeds for anti-jamming**,** Reconfigurable Intelligent Surface (RIS)-based protection, and energy-efficient, net-zero ML algorithms for green and secure networks.
- **Software CIA (Confidentiality, Integrity, Availability) SECaaS:** enabling secure deployment anywhere and without overhead.
- **Testbeds & Evaluation:** Integrated 11 distributed testbeds and 34 components across 16 use cases, providing a basis for pan-EU experimental validation.
- **Standardisation & Exploitation:** Engaged with ETSI, 3GPP and 6G-IA; developed dissemination, exploitation, and innovation strategies linked to EU certification and standardisation efforts.

During project lifetime, the consortium identified the following persisting policy gaps and emerging needs:

1. Lack of integrated certification schemes for 6G orchestration and AI security components.
2. Fragmented spectrum and regulatory approaches delaying testing of secure 6G services across borders.
3. Limited guidance on AI explainability and accountability within telecom environments.
4. Insufficient integration between 6G, AI Act, Cybersecurity Act, and Data Act frameworks.
5. Underdeveloped sustainability standards linking energy efficiency and network security performance.
6. Shortage of specialised skills in AI-driven network orchestration and programmable security.

5.5. Policy recommendations

Based on the convergence of NATWORK outcomes and the EU's strategic priorities for 6G, we may suggest the following proposals for EU policy making in the forthcoming period:

1. Foster the development of **European infrastructure-agnostic CIA-hardening for networking and service software**, without dependency on processor technology or on cloud vendor lock-in.
2. Establish a **6G Trust & Resilience Certification Scheme**, building on NATWORK's secure-by-design SLAs and federated orchestration frameworks.
3. Publish an EU **6G Security & Trust Standards Roadmap** aligning project outputs with ETSI, 3GPP, and ITU workstreams.
4. Expand NATWORK's testbed network into a **Federated Pan-EU 6G Security Testbed Infrastructure** to validate interoperability, AI-security and physical-layer resilience.
5. Launch **6G Security Uptake Pilots** with vertical industries to test certified solutions in pre-commercial environments.

6. Incentivise **secure and sustainable 6G chip and component design**, aligned to the EU Chips Act.
7. Establish a **6G Security & Orchestration Skills Programme** (via Erasmus+/Digital Europe) for network engineers, AI-security experts, and programmable-network specialists.
8. Integrate **security and orchestration requirements into 6G spectrum licences** (upper 6 GHz and beyond).
9. Develop **regulatory guidance for programmable networks**, covering runtime attestation, workload portability and federated learning security.
10. Mandate **net-zero and energy-efficiency KPIs** in all 6G security projects.
11. Promote **user-centric transparency** through explainable AI, SLA trust dashboards, and auditable orchestration logs.

5.6. Policy impact

The NATWORK project has demonstrated that **Europe's 6G vision can achieve reliability, security, and sustainability simultaneously**, provided that policymaking evolves alongside technological innovation. Implementing the above policy actions will deliver measurable benefits:

- **Strategic Autonomy:** Strengthened EU control over 6G security technologies, standards, and supply chains.
- **Openness:** Foster open security solutions, removing vendor lock-ins and dependencies
- **Regulatory Coherence:** Alignment across the Cybersecurity Act, AI Act, Data Act, and upcoming telecom reforms.
- **Innovation Acceleration:** Seamless transition from research to market through certified, interoperable components.
- **Economic Growth:** New opportunities for European SMEs in AI security, orchestration software, and network hardware.
- **Sustainability:** Integration of net-zero targets and energy-efficient AI into 6G systems.
- **Societal Trust:** Transparent, explainable, and privacy-preserving networks enhancing user confidence and digital inclusion.

6. Conclusions

Deliverable D7.5 “Impact to standardisation bodies, consortiums, and Alliances.r1” is the first of two reports that identifies the interconnection between NATWORK partners and the related SDOs in networking and Information Technology (IT) security. The importance of the standardisation procedure throughout a European Project, as well as the benefits of applying standardisation within the European context were also depicted in the present deliverable.

Within this report, the initial interconnections through SDOs and NATWORK partners were demonstrated. A description of several SDOs was presented through the report, while a direct or indirect connection between NATWORK partners was also reported. Moreover, standardisation activities, including the communication of preliminary results of NATWORK and the related dissemination and exploitation of these results were illustrated.

Additionally, NATWORK partners actively participate in Working Groups related to 5G and 6G networking. These working groups are of three categories: the 6G Smart Networks and Services Industry Association (6G-IA), Smart Networks and Services Joint Undertaking (SNS JU) and NetworldEurope. Through the 1st Reporting Period representative(s) per NATWORK partner were identified in every individual WG. Each representative reported the engagement for WG that was assigned. The engagement with each WG was illustrated in the current deliverable.

Finally, the NATWORK Policy Brief #1: Transparency in 6G Security, Resilience & Trust was presented to facilitate the EU policy discussions related to connectivity. Although it is not a direct contribution to standards, it can have an indirect impact to standardization activities, thus it was reported as a preliminary outcome of the relevant discussions.

6.1. Next steps

The current deliverable depicts the initial interaction between partners and the associated standardization bodies. Currently, communication towards these SDOs focuses on preliminary NATWORK results. As time passes and NATWORK results mature, contributions to SDOs can become more impactful. Also, dissemination and exploitation activities will be more targeted in terms of standardization.

Moreover, further development of the interactions between 6G-IA, SNS JU, ITU-T and NetworldEurope WGs and the NATWORK partners will be established. This engagement will grow as NATWORK results will be more targeted. Additional engagement with meetings and webinars on the affiliated WGs will be performed. Contribution to white papers and reports will be enhanced and reported in the second version of "Impact to standardisation bodies, consortiums, and Alliances".

Based on the above analysis detailed in the previous sections, we could identify and list the consortium's next steps regarding standardisation:

- Mature NATWORK technical results and translate them into concrete, high-impact standardisation contributions.
- Increase formal submissions (e.g., Change Requests, inputs, reports) to relevant SDOs such as ETSI, O-RAN Alliance, IEEE, and ITU-T.
- Propose NATWORK-developed solutions (e.g., xApp remote attestation) for inclusion in existing or upcoming specifications.
- Actively contribute to future revisions of standards where current versions are already in voting or frozen phases.
- Strengthen engagement with 6G-IA, SNS JU, ITU-T and NetworldEurope Working Groups as results become more targeted.
- Participate more intensively in WG meetings, webinars, workshops, and joint standardisation events.
- Contribute to and co-author white papers, technical reports, and policy recommendations aligned with 5G/6G roadmaps.
- Support joint ITU-T and 6G-IA activities, including contributions to FG-AINN reports on AI-native networks.
- Align NATWORK outcomes with EU policy, Cyber Resilience Act (CRA) compliance, and cybersecurity frameworks via ETSI and ENISA-linked activities.
- Enhance dissemination and exploitation strategies with a clear focus on standardisation impact.
- Monitor evolving standardisation landscapes (3GPP Releases, O-RAN specs, ETSI ISGs) to identify new contribution opportunities.

The current document is the first version of the "Impact to standardisation bodies, consortiums, and Alliances" report. The outcomes of the above-mentioned activities scheduled for the forthcoming months, will be reported in the deliverable's second version, a report to compile all related NATWORK activities, expected upon completion of the NATWORK project at M36.

References

[1] Research Consortium Bridge. (2020). Addressing research and innovation in European standardization activities and deliverables. https://www.cencenelec.eu/media/Guides/CEN-CLC/cenclcguide23.pdf

[2] O-RAN Alliance. (n.d.). About us. Retrieved December 9, 2025, from https://www.o-ran.org/about

[3] International Telecommunication Union. (2014). Socio-economic assessment of future networks by tussle analysis (ITU-T Recommendation Y.3013). https://www.itu.int/rec/T-REC-Y.3013/en

[4] International Telecommunication Union. (2019). Architectural framework for machine learning in future networks including IMT-2020 (ITU-T Recommendation Y.3172). https://www.itu.int/rec/T-REC-Y.3172/en

[5] International Telecommunication Union. (2020). Framework for evaluating intelligence levels of future networks including IMT-2020 (ITU-T Recommendation Y.3173). https://www.itu.int/rec/T-REC-Y.3173/en

[6] International Telecommunication Union. (2012). Overview of the Internet of Things (IoT) (ITU-T Recommendation Y.4000/Y.2060). https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060