ETSI GR ISC 004 V1.1.1 (2026-02)

GROUP REPORT

Integrated Sensing And Communications (ISAC); Security, Privacy, Trustworthiness and Sustainability

Disclaimer

The present document has been produced and approved by the Integrated Sensing And Communications (ISAC) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/ISC-004

Keywords
ISAC, privacy, security, sustainability, trustworthiness

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Integrated Sensing And Communications (ISAC).

Modal verbs terminology

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

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

Executive summary

The present document provides a comprehensive study on aspects related to security, privacy, trustworthiness, and sustainability within the context of Integrated Sensing and Communications (ISAC).

The present document identifies 19 key issues, of which 15 are related to privacy and security, and 4 related to sustainability. For each key issue, a detailed description is provided, together with potential technical and non-technical requirements. For the privacy and security key issues, the analysis is supported with a comprehensive set of threats per key issue.

In addition, the present document includes initial considerations on aspects related to trustworthiness and ownership of sensing data. The potential technical and non-technical requirements are analysed to identify consolidated requirements that future 6G systems should meet to deploy secure, privacy-preserving, trustworthy, and sustainable ISAC services.

Introduction

Interest in ISAC is growing worldwide among standardization bodies, industrial stakeholders, academia, and numerous collaborative projects. In this context, the present document provides a study on challenges related to security, privacy, trustworthiness, and sustainability for enablement of ISAC in a future 6G System.

1 Scope

The scope of the present document is to study security, privacy, trustworthiness, and sustainability in the context of ISAC in a future 6G System. This includes:

- An overview of existing definitions and characterizations of security, privacy, trustworthiness, and sustainability, and identification of related terms.
- Identification of key issues, description of relevant threats, and definition of potential requirement for security and privacy.
- Identification of key issues on sustainability.
- Consolidation of potential requirements corresponding to the key issues on security and privacy.
- Additional considerations regarding trustworthiness and data ownership.
- High-level objectives for sustainability.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

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

[i.1] ETSI GR ISC 001 (V1.1.1): "Integrated Sensing And Communications (ISAC);Use Cases and Deployment Scenarios".

[i.2] ISO/IEC 23643:2020: "Software and systems engineering — Capabilities of software safety and security verification tools".

[i.3] ISO/IEC TS 5723:2022(en): "Trustworthiness Vocabulary", 2025.

[i.4] ISO 20252:2019: "Market, opinion and social research, including insights and data analytics — Vocabulary and service requirements".

[i.5] ETSI TR 121 905 (V18.0.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Vocabulary for 3GPP Specifications (3GPP TR 21.905 version 18.0.0 Release 18)".

[i.6] ISO 7498-2:1989: "Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture".

[i.7] ISO/IEC 20000-10:2018: "Information technology - Service management - Part 10: Concepts and vocabulary".

[i.8] NIST SP 800-12: "An introduction to computer security: the NIST handbook", 1995.

[i.9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.10] ISO TS 27790:2009: "Health informatics — Document registry framework".

[i.11] ISO TS 14441:2013: "Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment".

[i.12] NIST SP 800-160v1r1: "Engineering Trustworthy Secure Systems".

[i.13] Gro Harlem Brundtland: "Report of the World Commission on Environment and Development: Our Common Future" 1987.

[i.14] ISO/IEC 29100:2020-03: "Information technology - Security techniques - Privacy framework".

[i.15] NIST SP 800-122 E. McCallister, T. Grance, K. Scarfone: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)".

[i.16] 3GPP TR 22.837 (V19.4.0): "Feasibility Study on Integrated Sensing and Communication (Release 19)".

[i.17] Nyangaresi, V.O., Abduljabbar, Z.A., Mutlaq, K.AA., Hussain, M.A., Hussien, Z.A.: "Forward and Backward Key Secrecy Preservation Scheme for Medical Internet of Things", 2023.

[i.18] Mozilla™ Foundation: "Immutable", 2025.

[i.19] Goetz et al.: "Java Concurrency in Practice; Section 3.4. Immutability", Addison Wesley Professional, 2006.

[i.20] P. Dass, S. Ujjwal, J. Novotny, Y. Zolotavkin, S. Köpsell: "Addressing privacy concerns in joint communication and sensing for 6G networks: challenges and prospects", Privacy Technologies.

[i.21] R. Becker et al.: "DAISY: A data information system for accountability under the general data protection regulation", GigaScience, 8(12), giz140.

[i.22] European Commission: "Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment".

[i.23] ETSI TR 128 908 (V18.0.0): "5G; Study on Artificial Intelligence/Machine Learning (AI/ ML) management (3GPP TR 28.908 version 18.0.0 Release 18)".

[i.24] European Commission: "Draft standardisation request as regards European Trusted Data Framework", 2024.

[i.25] ETSI TR 104 177: "Data Solutions (DATA); Landscape of Relevant Standards and Technologies for Data".

[i.26] ETSI TR 104 180: "Data Solutions (DATA); Development and identification of Data Quality Metrics".

[i.27] Draft CWA for comment CENELEC: "Trusted Data Transaction - Part 2: Trustworthiness requirements", 2025.

[i.28] Assaf Kasher, Yingxiang Sun: "Wifi-Sensing-Use-Cases", IEEE 802.11™ WLANs WG Group Mentor Public Documentation Portal, Group TGbf, DCN 1712, Rev 2, 2020.

[i.29] United Nations: "Sustainable Development Goals and the 2030 Agenda: Why Environmental Sustainability and Gender Equality are so important to Reducing Poverty and Inequalities - UNEP Perspectives Issue No. 17", 2015.

[i.30] ETSI GR ISC 003: "Integrated Sensing And Communications (ISAC); System and RAN Architectures".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
6GS	6th Generation System
AF	Application Function
AI	Artificial Intelligence
BLER	Block Error Rate
BS	Base Station
CEN	European Committee for Standardization
CN	Core Network
CPR	Consolidated Potential Requirement
CPU	Central Processing Unit
CWA	CEN Workshop Agreement
EC	European Commission
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
ISAC	Integrated Sensing and Communication
KPI	Key Performance Indicator
ML/AI	Machine Learning/ Artificial Intelligence
NF	Network Function
PII	Personally Identifiable Information
PR	Potential Requirement
PRR	Potential Regulatory Requirement
RAN	Radio Access Network
RF	Radio Frequency
RRC	Radio Resource Control
SA3	subcommittee on Security (3GPP)
SBA	Service Based Architecture
SIDP	Sensing Input Data Producer
SLA	Service Level Agreement
TC DATA	Technical Committee Data Solutions
TC	Technical Committee
TR	Technical Report
TSSA	Target Sensing Service Area
UAV	Unmanned Aerial Vehicle
UC	Use Case
UE	User Equipment
UN	United Nations
XR	Extended Reality

4 Definitions and foundations for security, privacy, trustworthiness, and sustainability

4.1 System terminology for ISAC-enabled 6G systems

For the purposes of the present document, the following terms as defined in ETSI GR ISC 003 [i.30] apply:

- **6GS Sensing Service Consumer (SSC):** a 6GS entity which can be authorized to request and consume 6G Sensing Service(s). SSC may include UEs, Access Nodes, and Core Network Functions.
- **3rd party Sensing Service Consumer (3-SSC):** an entity, not part of 6GS, which can be authorized to request and consume 6G Sensing Service(s).
- **Sensing signal:** is a transmitted signal from a sensing transmitter for the purpose of sensing. The signal can be 6G or non-6G.
- A **sensing transmitter:** is a 6G or non-6G entity that transmits a sensing signal.
- A **sensing receiver:** is a 6G or non-6G entity that receives a sensing signal and produces sensing data. A sensing receiver can be co-located with a sensing transmitter.
- **Sensing data:** is the 6G or non-6G data produced for sensing purposes.
- **A sensing entity:** is an entity referring to a sensing transmitter or to a sensing receiver.
- A **sensing service:** is a feature of the 6GS that is offered to service consumers. A sensing service provides sensing results based on communicated requirements and KPIs.
- **Sensing function:** indicates the logical function, which is involved to support a Sensing Service.

NOTE 1: The sensing function cannot be a sensing entity.

- A **sensing task:** is communicated from a sensing function to sensing entities and functions and consists of configuration information of the required sensing transmitter(s) and sensing receiver(s) (if applicable), the collection of sensing data, the processing of the sensing data and the exposure of the sensing results. Each sensing task fulfils a Sensing Service request.
- A **Target Sensing Service Area (TSSA):** is defined as a cartesian location area that needs to be sensed by deriving characteristics of the environment and/or objects within the environment with certain sensing service quality from the impacted (e.g. reflected, refracted, diffracted) 6G or non-6G sensing signals. This includes both indoor and outdoor environments.
- The **sensing results:** are processed or non-processed sensing data which may include characteristics of objects (e.g. type, distance, velocity, trajectory, size, shape, material), or other contextual information (e.g. time of generation, environmental information) about objects in the Target Sensing Service Area.

NOTE 2: It is not precluded that the sensing result exposed to an entity within 6GS or to a authorized third party may in some cases consist of the sensing data itself.

- **Sensing contextual information:** is information that is exposed with the sensing results which provides context to the conditions under which the sensing results were derived (e.g. time of generation, environmental information). This information does not contain sensing data or sensing results.
- **Fusion:** refers to a process to join two or more streams of sensing data or sensing results together to form one or more sensing data or sensing result stream(s). Fusion can take place at the origin of the sensing data, along the system entities of a 6GS. The fusion of sensing results can also take place along all 6GS system entities. Fusion can also take place in non-6GS entities.

4.2 Security

General definition: Security refers to the resistance to intentional, unauthorized action(s) intended to harm or compromise a system, see ISO/IEC 23643 [i.2]. This involves preserving the properties such as confidentiality, integrity and availability of information as defined in ISO 20252 [i.4] and ETSI TR 121 905 [i.5].

Confidentiality: This property ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes as defined in ISO 7498-2 [i.6].

Integrity: This property ensures that data has not been altered or destroyed in an unauthorized manner as defined in ISO 7498-2 [i.6] and ETSI TR 121 905 [i.5].

Availability: This property ensures that data is accessible and usable upon demand by an authorized entity, as defined in ISO 7498-2 [i.6]. It may further ensure the ability of a system to offer a service at an agreed time or over an agreed period of time, see ISO/IEC 20000-10 [i.7] and NIST SP 800-12 [i.8].

Based on the definitions in ISO/IEC 23643 [i.2], ISO 20252 [i.4], ETSI TR 121 905 [i.5], ISO 7498-2 [i.6], ISO/IEC 20000-10 [i.7] and NIST SP 800-12 [i.8].

Security in the context of ISAC refers to the resilience of integrated sensing and communication systems against intentional, unauthorized actions intended to harm or compromise system operations. This encompasses the preservation of confidentiality, integrity, and availability of both communication and sensing information, systems, and services such as sensing data, sensing entities, and sensing functions.

4.3 Personal Identifiable Information (PII)

As defined by EU GDPR [i.9], **Personally Identifiable Information** (PII) means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Even information that is not identifiable on its own can be considered **sensitive data**, if it may become identifiable when joined with other datasets.

4.4 Privacy

General definition: Privacy refers to the freedom to remain free from intrusions into one's personal life or affairs, particularly when such intrusions result from the improper or unlawful collection and use of personal data as defined in ISO TS 27790 [i.10]. Privacy covers the rights and obligations of individuals and organizations regarding the collection, use, storage, sharing, and disposal of PII, see ISO TS 14441 [i.11]. Privacy is always related to personal data or PII.

NOTE: While confidentiality focuses on preventing the disclosure of information to unauthorized actors, privacy specifically deals with the confidentiality of PII, including its management during collection, use, storage, sharing, and disposal. Therefore, privacy is not the same as confidentiality.

Based on the definitions in ISO TS 27790 [i.10] and information in ISO TS 14441 [i.11].

Privacy in the context of ISAC refers to the protection of individuals' personal information in integrated sensing and communication systems, focusing on the responsible collection, use, retention, disclosure, and disposal of PII, obtained through both communication and sensing activities. It ensures that individual data is handled ethically and transparently, safeguarding against illegal data gathering, usage, and inferences while respecting individual data protection rights and guidelines.

4.5 Trustworthiness

General definition: Trustworthiness as defined in ISO/IEC TS 5723 [i.3] refers the ability of the system to meet the expectations of the stakeholders in a measurable and verifiable way. Trustworthiness covers many different trustworthiness characteristics such as accountability, accuracy, authenticity, availability, integrity, privacy, quality, safety, security, sustainability, transparency and usability.

NOTE 1: Because of the broad nature of the term trustworthiness, it is not a synonym for privacy/security related aspects.

NOTE 2: While trustworthiness is objective and measurable, trust denotes just a belief that an entity meets certain expectations and can be relied upon. Therefore, trust may be granted to an entity whether the entity is trustworthy or not, as described in NIST SP 800-160 [i.12].

Based on the definitions in ISO/IEC TS 5723 [i.3] and NIST SP 800-160 [i.12],

Trustworthiness in the context of ISAC refers to the assurance that the integrated sensing and communication framework meets the expectations of the stakeholders in a measurable and verifiable way. This encompasses many different trustworthiness characteristics such as accountability, accuracy, authenticity, availability, integrity, privacy, quality, safety, security, sustainability, transparency, and usability.

4.6 Sensing policy, sensing consent and sensing transparency

4.6.1 Sensing policy

The sensing policies provide clear guidelines on what data is to be collected, which types of sensing objects are considered in each Target Sensing Service Area (TSSA), the purpose of collecting sensing data, and the entities involved in data collection, processing and exposure. They also outline where the sensing data is stored, who has access to raw and processed data, how the data is protected (in transit, in storage, or in use), and other obligations such as data retention and deletion.

4.6.2 Sensing consent

Sensing consent is a form of authorization, where appropriate, given with the knowledge of the data subject for the collection and processing of PII during sensing activities as defined in ISO/IEC 29100 [i.14] and NIST SP 800-122 [i.15]. In the context of ISAC systems, the data subjects include humans, with or without User Equipment (UE), involved in sensing activities, whose PII is being collected. The processing of the PII involves operations, such as collection, use, disclosure, storage, erasure, or transfer of the data. Additionally, sensing consent should also account for the confidentiality of private and sensitive infrastructures like military sites.

4.6.3 Sensing transparency

Sensing transparency is the principle of ensuring that individuals, whose PII is being collected, have clear and easily accessible information about the relevant sensing policies, procedures, and practices related to the processing of their PII during sensing activities, as defined in ISO/IEC 29100 [i.14] and NIST SP 800-122 [i.15]. Sensing transparency should also be considered for the sensing of private and sensitive infrastructures.

4.7 Sustainability

As defined by the United Nations General Assembly [i.13], sustainable development refers to development that meets the needs of the present without compromising the ability of future generations to meet their own needs.

NOTE: This definition does not limit the scope of sustainability to green technology or energy efficiency. The definition also includes social sustainability.

4.8 Types of Sensing Targets in ISAC-Enabled 6GS

Sensing targets in ISAC-enabled 6GS can be categorized based on whether they are human or non-human, fixed or stationary, and whether they are connected to the network or not. Different sensing target types are shown in Figure 1.

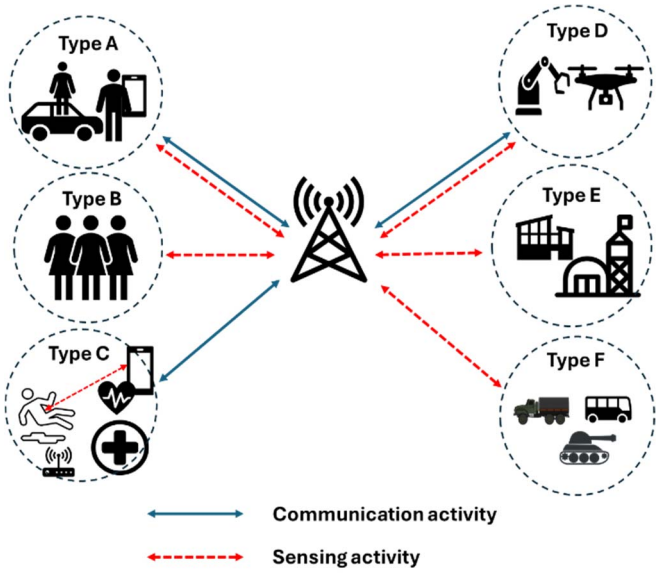

Figure 1: Types of sensing targets in an ISAC-enabled 6GS

Type A	Human with UE connected to the network (both communication and sensing), e.g. people with cell phone or vehicle connected to the network.
Type B	Human not connected to network (only sensing), e.g. people with or without cell phone not connected to the network.
Type C	Human connected to network (only for communication; applicable to use cases like human sleep monitoring and house monitoring according to ISO/IEC 29100 [i.14], where sensing performed by UEs and sensing data communicated to the network for processing).
Type D	Fixed or stationary non-human object connected to the network (communication and sensing), e.g. automated machines, UAVs, etc. with network connectivity.
Type E	Fixed non-human object not connected to the network, e.g. buildings, infrastructures, etc. (only sensing).
Type F	Stationary object not connected to the network (only sensing), e.g. vehicles without network connectivity.

NOTE: PII is involved only for sensing targets with human involvement (Types A, B, and C). While privacy requirements such as consent and transparency only apply to PII, confidentiality is also necessary to protect sensitive information, such as infrastructure details in military areas (Type E). Therefore, both security and privacy aspects should be considered when sensing target Types A, B, and C are involved. However, for sensing target Types D, E, and F, only security aspects are applicable.

5 Key issues on security and privacy

5.1 Key issue #1: Use of 6GS for unauthorized sensing

5.1.1 Key issue details

The issue in question is illustrated in Figure 2. A 6GS with unprotected sensing signals may offer the opportunity to unauthorized entities to do their own independent sensing of potentially sensitive information such as location, size, material, or other properties of a target, or environmental maps. The unauthorized sensor(s), further referred to as Pep, can be:

a) a cooperative UE that is a legitimate communication user but unauthorized for sensing;

b) a noncooperative or potentially malicious entity that exploits the sensing-optimized properties of the 6GS.

There can of course be communication users in the scene, that can be any entity with a UE. In all these cases the network is interested in providing security in the sense of protecting any entity within the sensing area from unauthorized sensing. The entity that is sensed without authorization can be a sensing user of the 6GS, or part of the environment.

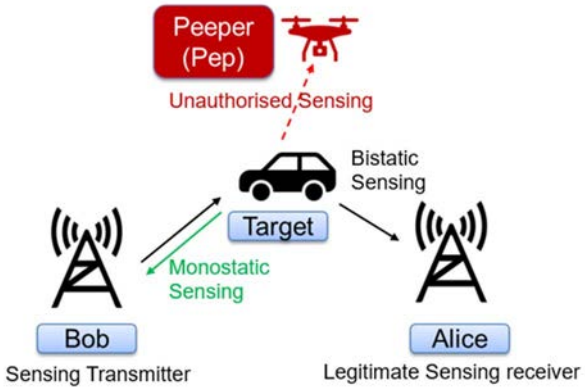

Figure 2: Illustrative scenario in sensing-security for ISAC transmission

5.1.2 Security, privacy, and trustworthiness threats

It is understood that sensing the environment by an unauthorized entity is a security-breaching activity that should be explicitly addressed and avoided correspondingly.

The uniqueness of the scenario in Figure 2, compared to other security scenarios (like the use case on Protection of Sensing Information in 3GPP TR 22.837 [i.16]), is the need to protect, not against data being eavesdropped or compromised, but against unauthorized use of the 6GS for sensing. The fact that the ISAC-enabled 6GS will be optimized for sensing (signals, resources, antennas, cooperation, etc.) may open up the opportunity to any unauthorized entity to collect sensing measurements of the environment with enhanced performance, potentially revealing sensitive environment information, such as the location of key infrastructures, UEs or people. This may further evade any charging functionality the operator has in place. Some sensitive scenarios, such as, e.g. military applications, critical energy infrastructures, biohazard waste management, etc. may pose requirements to provide security against unauthorized sensing of the environment.

Such scenarios imply that, aside to any application-dependent sensing / communication performance, the 6GS may need to provide protection against unauthorized sensing. This can apply to a number of network services such as connected cars sensing and communication, UAV monitoring, pedestrian localization and communication, among many others.

The requirement to provide protection against unauthorized sensing may imply that any unauthorized entity cannot leverage 6GS to obtain any sensing measurements or sensing data that could be used for localizing the target within the size of the cellular network scenario. In alternative scenarios this can mean that the unauthorized entity should not be able to leverage the 6GS to image the environment or specific objects beyond a certain resolution. Such requirements may be translated into numerical KPIs related to unauthorized sensing.

In this case there is no data link to encrypt, higher layer security solutions do not apply, and protecting against this potential breach requires security at the physical layer.

Within the TSSA, an unauthorized sensor (Pep) can carry out unauthorized sensing if they have a radar detection or imaging capability either with a UE or other device. Their eavesdropping can be active (including their own electromagnetic emissions) or passive.

The scenario can extend to monostatic or bistatic sensing or mixed, and to cooperative and non-cooperative communication and sensing. In all these cases the Pep has the opportunity to carry out unauthorized sensing, i.e. unauthorized use of the 6GS for sensing.

5.1.3 Potential requirements and metrics

Potential functional requirements for 6GS to cope with these threats are:

[PR 5.1-1] The 6GS needs to protect the target(s) against unauthorized sensing, with the same sensing signals that are being used to detect/estimate/localize the target(s), by ensuring that an unauthorized entity cannot obtain the required sensing accuracy to extract a meaningful result that could be used for localizing the target within the size of the cellular network scenario.

Some of the new KPI-related requirements for unauthorized sensing in this key issue are given in Table 1 for target localization and Table 2 for imaging.

Table 1: Performance Requirements for protection against unauthorized target localization

Scenario	Sensing service area	Confidence level [%]	Unauthorized sensing accuracy of positioning / velocity	Unauthorized sensing resolution for range / velocity	Unauthorized sensing Missed detection [%] / False alarm [%]	Gap between legitimate and unauthorized performance	Ratio of missed detection/false alarm of unauthorized sensing over legitimate sensing
Security against unauthorized target localization	Outdoor and Indoor	⩾ 95	[> X m] / [> X m/s] note 1	[> X m] / [> X m/s] note 1	[> 50] / [> 50]	[X m] / [> X m/s] / ≥ 10 note 2	Y
NOTE 1: X is to be determined by the specific scenario in place to ensure the unauthorized sensing does not offer meaningful information. NOTE 2: Y is given by the ratio of unauthorized to authorized Probability of Missed Detection or the ratio of unauthorized to authorized Probability of False Alarm, and is determined by the scenario in place.							

Table 2: Performance Requirements for protection against unauthorized target imaging/environment mapping

Scenario	Sensing service area	Confidence level [%]	Unauthorized sensing image resolution	Gap between legitimate and unauthorized imaging performance
Security against unauthorized target imaging / environment mapping	Outdoor and Indoor	≥ 95	[> X cm] note	[> X cm] note
NOTE: X is to be determined by the specific scenario in place to ensure the unauthorized sensing does not offer meaningful information.				

5.2 Key issue #2: Use of sensing signals by the target for data eavesdropping

5.2.1 Key issue details

The issue in question is illustrated in Figure 3. The sensing target(s) can be:

a) a cooperative target, e.g. a person or car that is part of the network and has subscribed for sensing services;

b) a noncooperative or passive entity that is being sensed by the sensing entity as part of mapping the environment or any other sensing application;

c) a potentially malicious entity that is looking to extract critical communication parameters with the aim to harm the service of the network in some way.

The communication users can be any entity with a UE. In cases with joint ISAC signalling with dual-use of communication data for sensing, the fact that the ISAC probing signal carries communication information to the targets in the environment opens up the opportunity to a target to act as an Eve and, directly or indirectly, extract information. Therefore, the network is interested in providing data confidentiality in the sense of protecting the communication users (UEs) from their payload data or other transmission parameters being eavesdropped by the adversary entity.

5.2.2 Security, confidentiality, and trustworthiness threats

The uniqueness of the scenario in Figure 3 compared to other security scenarios that need to protect against external eavesdroppers (Eves), is that the Eve is now a sensing target, which is illuminated by the ISAC-enabled 6GS to achieve the KPIs of the sensing task. This gives the target the opportunity to act as an eavesdropper and obtain payload data or L1-L3 parameters (e.g. the subcarrier spacing, carrier frequency, some RRC parameters, etc.) from the sensing signals. This motivates the need to provide enhanced confidentiality protection for communications.

The scenario implies that, in addition to any application-dependent sensing / communication performance, the 6GS needs to provide confidentiality guarantees against target eavesdropping.

Even if the payload data is encrypted using higher layer security approaches, the mere detection of an existing communication link between two entities can be private or critical information, for both civilian and defence applications. Therefore, protecting against this requires confidentiality at the Physical layer.

Within the sensing coverage area, a target can act as an Eve if they have a signalling or L1-L3 parameter detection capability either with a UE or other equipment. Their eavesdropping can be active (including some electromagnetic emissions) or passive.

The scenario can extend to monostatic or bistatic sensing or mixed, and to cooperative and non-cooperative communication and sensing. In all these cases a target has the opportunity to eavesdrop, potentially with high signal power.

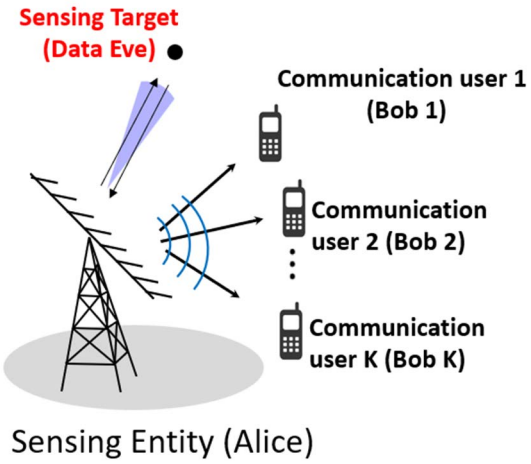

Figure 3: Illustrative scenario in data confidentiality for ISAC transmission

5.2.3 Potential requirements and metrics

Potential functional requirements for 6GS to cope with these threats are:

[PR 5.2-1] The 6GS should offer means to protect the payload data that is being transmitted and/or the L1-L3 parameters of the link to the UEs with the same sensing signals that is being used to detect/estimate/localize the target(s).

Some of the new KPI-related requirements for target eavesdropping in this key issue are given in Table 3. The explicit KPI values will depend on the scenario, the level of information accuracy required or eavesdropping tolerated for the application, and the likelihood for the eavesdropper to infer useful information, be that payload data or L1-L3 parameters. Secrecy rate shown below is defined as the difference in achievable payload data rate between the legitimate receiver and the eavesdropper, after a decoding attempt from the latter based on the obtained L1-L3 parameters. Probability of intercept defines the probability that the eavesdropper detects and exploits the legitimate transmission, to extract either the payload data itself or the link parameters. Eavesdropping Block Error Rate (BLER) defines the BLER with which the eavesdropper extracts payload data, once the legitimate data transmission is intercepted. In addition, the ratio of payload data BLER of eavesdropper over the legitimate receiver is defined for the cases where a significant margin in BLER performance is required by the service. Depending on the scenario, data confidentiality might implicate any individual KPI or combinations of these.

Table 3: Performance requirements for data confidentiality against unauthorized target eavesdropping

Scenario	Sensing service area	Probability of Intercept of L1-L3 parameters or payload data	Eavesdropper payload data Block Error Rate	Payload data Block Error Rate Ratio of Eavesdropper/User	Payload data Secrecy Rate
Data confidentiality against target eavesdropping	indoor and outdoor	[≤ A%] (note)	≥ B	≥ C	≥ D
NOTE: The explicit values of A, B, C and D will depend on the scenario, the level of information accuracy required or eavesdropping tolerated for the application, and the likelihood for the eavesdropper to infer useful information.					

5.3 Key issue #3: Over-the-air manipulation of 6G RF sensing signals

5.3.1 Key issue details

Sensing relies on the transmission and reception of sensing signals. These sensing signals are altered by the channel and the processing engine tries to extract that channel information. For some use cases, the sensing result may be used to trigger some action. One key attack scheme consists of a malicious entity that transmits signals to the sensing receiver to present a manipulated environment that could trigger some unintended action.

5.3.2 Security, privacy, and trustworthiness threats

Such an attack may correspond to multiple security threats, depending on the level of sophistication of the attacker. In case the sensing receiver is not able to extract any information from the sensing measurement, the threat may be characterized as a denial-of-service attack. This may be the case for jamming. For more advanced attacks, where the sensing result is manipulated, it may be characterized as tampering.

5.3.3 Potential requirements and metrics

[PR 5.3-1] The 6GS should provide a mechanism to identify potential attacks based on unauthorized transmissions.

[PR 5.3-1] The 6GS should provide mechanisms to secure 6G RF sensing signals from being tampered which may result in manipulated sensing data and sensing results.

5.4 Key issue #4: Secure handling of sensing data

5.4.1 Key issue details

As discussed in ETSI GR ISC 001 [i.1], various ISAC use cases require that both UEs and BSs are involved in a sensing task as sensing entities. For these use cases, the ISAC-enabled 6GS will potentially be designed to utilize network entities to transport, process, and store the sensing data and sensing results.

As a design decision, processing units may be located at the edge of the 6GS, close to the measurement generation, such as in RAN nodes, or in the CN. The processing and storage of data in the RAN can be advantageous for low latency applications that require a quick response upon a sensing result (e.g. sensing-assisted communication or digital twins for traffic control).

5.4.2 Security, privacy, and trustworthiness threats

Architectural considerations of a future 6GS may need to take into account the transport of sensing data over the network nodes to enable the collection of sensing data and its subsequent processing and storage in CN and RAN nodes. This implies that the data will be under the control of the RAN/CN infrastructure owners.

This raises concerns regarding security and privacy as sensing data can be analysed, modified and potentially compromised.

Furthermore, unauthorized parties could access the sensing data, thereby exposing current, future and previous sessions, see [i.17].

Additionally, storing sensing data in different nodes might require the use of storage server, which can be vulnerable to system disruptions and result in unreliable ISAC services, ultimately affecting the system's trustworthiness.

5.4.3 Potential requirements and metrics

[PR 5.4-1] The 6GS should guarantee that access to sensing data is restricted solely to intended RAN nodes and CN functions.

[PR 5.4-2] The 6GS should protect the integrity of sensing data during processing in RAN or/and CN.

[PR 5.4-3] The 6GS should provide resilience of data storage inside RAN/CN node to ensure its data remains available, intact, and secure.

[PR 5.4-4] The 6GS should incorporate cryptographic mechanisms that ensure forward and backward secrecy for sensing data transmission between RAN nodes and the CN.

[PR 5.4-5] The 6GS should incorporate comprehensive data retention policies that define clear guidelines for sensing data storage duration, ensuring compliance with privacy and regulatory requirements.

5.5 Key issue #5: Integrity of ISAC-enabled 6GS entities, and immutability of sensing data or sensing results

5.5.1 Key Issue details

Handling ISAC data will continuously leverage cloudified software system components across 6GS entities. For a 6GS to offer ISAC at scale, SBA and cloud continuum principles will be leveraged to scale Sensing services to fulfil high reliability requirements, on demand cloud resource allocations and ensuring failover scenarios to be handled seamlessly with a low impact on the sensing service availability. Ensuring integrity of ISAC-enabled 6GS entities is important in this scenario.

Immutability is defined as an object whose state cannot be changed once created, see [i.18] and [i.19]. For ISAC, immutability of sensing data or sensing results is the property that data once created cannot be altered. This includes the assurance of traceability of sensing data or sensing results inside a 6GS including the exposure of sensing data to (3-)SSCs.

5.5.2 Potential threats

For 6GS entities, CPU, storage or memory could be compromised, and software binaries being altered and/or accessed unauthorized resulting in compromised service requests from consumers or service responses from producers exposing critical authentication information (keys, credentials) or allow information to be injected to expose further sensitive information from 6GS entities. This is further aggravated for 6GS entities that may operate on third party infrastructure (cloud services).

Sensing data and sensing results can be potentially sensitive information and depending on the requested sensing service may contribute to mission critical services. If this data is altered with bad intentions along the way, wrong decision will be made inside the 6GS or by the SSC which operates based on the provided sensing results.

5.5.3 Potential requirements and metrics

[PR 5.5-1] The 6GS should have means and procedures for checking the integrity of ISAC-enabled 6GS entities.

[PR 5.5-2] The 6GS should have means and procedures for tracing the immutability of sensing data and sensing results.

5.6 Key issue #6: Sensing privacy, confidentiality, and consent in non-public spaces

5.6.1 Key issue details

There is a high likelihood of Sensing Services to be carried out in non-public spaces. Non-public spaces include critical infrastructure (power plants or governmental buildings) or private spaces with privacy restrictions (homes or schools). Sensing policies and consents need to be gathered and enforced by the ISAC-enabled 6GS for these non-public spaces. Furthermore, it is important to ensure the privacy and confidentiality of collected sensing data near non-public spaces including authorized exposure of sensing measurements in these scenarios.

5.6.2 Security, privacy, and trustworthiness threats

The issue has the following threats:

1) Unauthorized collection, storage and processing of sensing data from non-public spaces.

2) Gathering sensitive information about an environment without sufficient data protection mechanisms (e.g. number of children in a school, key components of a power plant).

5.6.3 Potential requirements and metrics

[PR 5.6-1] The 6GS should provide means of gathering policies and consent for collecting, processing and storing sensing data in non-public spaces.

[PR 5.6-2] The 6GS should provide means of choosing sensing receivers and sensing transmitters allowed to perform sensing in non-public spaces.

[PR 5.6-3] The 6GS should preserve the privacy of humans and preserve the confidentiality of information gathered in non-public spaces.

[PR 5.6-4] The 6GS should have means to provide private and confidential sensing results to only authorized and trusted applications.

5.7 Key issue #7: Privacy issues related to consent and transparency

5.7.1 Key issue details

The ISAC-enabled 6GS collects sensing data that often include PII of individuals in the TSSA. The processing of this sensing data may capture a wide range of sensitive information, such as a person's location, movement patterns, gestures, or even biometric data like gait, facial features, and heart rate, depending on the application and configuration [i.20].

In many use cases, sensing data collection and processing inherently involves human-related information, which may occur without direct human interaction with the 6GS or explicit awareness of the humans. This makes it challenging to ensure compliance with consent and transparency requirements defined under privacy regulations such as the GDPR, see Regulation (EU) 2016/679 [i.9], articles 13 and 14. For sensing data collection and processing that do not involve humans (e.g. sensing data of a military infrastructure), privacy requirements such as consent and transparency may not apply; however, confidentiality is still necessary to protect sensitive information, such as infrastructure details.

5.7.2 Security, privacy, and trustworthiness threats

If the 6GS fails to adhere to sensing policies, obtain sensing consent, and maintain sensing transparency, the following security and privacy threats can arise:

Unauthorized data collection and processing: Sensitive data and PII, such as location, movement patterns, or biometric data, etc. may be collected from the TSSA, (including sensing targets and the UEs involved in sensing) and processed without the knowledge or consent of individuals, violating privacy rights.

Unawareness of involvement: Without the UE owner's awareness, the hardware and software of UE may inadvertently participate in sensing data collection and processing.

Data misuse: The sensing data collected for one purpose could be repurposed for unauthorized applications that involve surveillance or profiling, without sensing consent and transparency.

Unintended disclosure: High-resolution sensing data and meta information obtained during the sensing process could inadvertently capture identifiable information (e.g. home addresses or personal activities) and expose it to unauthorized parties.

Lack of accountability: Without transparency, the individuals cannot track when their sensing data is being collected, how it is processed, stored, or shared, making it difficult to hold entities accountable for misuse.

Regulatory non-compliance: Without implementing sensing consent and transparency mechanisms, ISAC service providers may bypass privacy regulations like GDPR, potentially compromising the security and privacy of individuals' sensing data.

5.7.3 Potential new requirements

[PR 5.7-1] The 6GS should offer mechanisms to exercise choice and obtain consent from human involved in sensing activities and connected to the network, while also providing transparency information.

[PR 5.7-2] The 6GS should consider appropriate sensing consent and transparency guidelines for humans not connected to the network.

[PR 5.7-3] For non-human objects, whether fixed or stationary, and either connected or not connected to the network, where confidentiality is required, the 6GS should offer mechanisms or polices to ensure sensing consent and transparency.

[PR 5.7-4] To comply with sensing consent and transparency requirements, the 6GS should implement proper mechanisms within the core network.

[PR 5.7-5] The 6GSshould provide mechanisms for UEs involved in sensing tasks to manage sensing consent and transparency requirements effectively.

[PR 5.7-6] The 6GS should provide mechanisms to ensure that updated sensing policies are accessible to all entities involved in sensing activities.

[PR 5.7-7] The 6GS should provide mechanisms to ensure sensing consent and transparency at every stage of sensing data handling, including its collection, processing, storage, and sharing.

5.8 Key issue #8: Privacy-related aspects regarding sensing of humans that are not connected to the 6GS

5.8.1 Key issue details

Sensing of humans is generally considered an important use case category for wireless sensing. Unlike positioning and other features within provided by contemporary cellular systems, sensing does not require active collaboration of the sensed person or object. Thus, it is even possible to sense humans that are not connected to the 6GS. This feature has implications on privacy, since people can be sensed without knowing that they are sensed, by whom they are sensed, and for which purpose the sensing result is used.

5.8.2 Security, privacy, and trustworthiness threats

The issue translates to multiple privacy threats, but primarily to unawareness and unintervenability since sensed individuals are unaware of and cannot consent to or opt out of being sensed. Thus, there is a lack of control. Since the sensed humans are not connected to the 6GS, it is challenging to inform them of ongoing sensing sessions, making unawareness a key threat due to missing transparency.

5.8.3 Potential requirements and metrics

[PR 5.8-1] The 6GS should offer privacy-preserving sensing solutions for the case where explicit consent or notification is not possible.

5.8.4 Potential regulatory requirements

[PRR 5.8-1] Regulatory bodies should provide guidelines when a sensing operation includes sensing of humans that are not connected to the 6GS.

5.9 Key issue #9: Privacy-related aspects regarding sensing of humans that are connected to the 6GS

5.9.1 Key issue details

Sensing of humans is an important use case category for ISAC that was identified in ETSI GR ISC 001 [i.1].

Similar to key issue #8, RF sensing has the property that people can be sensed without knowing that they are sensed, by whom they are sensed, and for which purpose the sensing result is used. However, for sensing of humans that carry a UE that is connected to the 6G network, the situation differs slightly.

For individuals that carry a UE that is connected to the 6G network, there is room for potential solutions to communicate with these individuals that are sensed. Such interaction may be used to inform individuals or even to ask for consent on an individual basis. However, such interaction may result in additional threats to privacy since sensed humans in the TSSA may need to be identified to communicate with them.

While this issue includes use cases such as crowd monitoring that have the objective to sense humans, it also applies to use cases where humans are present in the sensed area but not part of the use case itself.

5.9.2 Security, privacy, and trustworthiness threats

The issue raises multiple privacy threats. Individuals may not be aware of whether they are being sensed, who is sensing them, and for which purpose the sensing result is used. This lack of awareness and intervenability can be a significant threat. Thus, there is a general lack of transparency and control in the sensing system. Additionally, sensed information may be linked to other data items, which may lead to privacy exposure beyond the sensing system and the potential identification of individuals.

5.9.3 Potential requirements and metrics

[PR 5.9-1] The 6GS should offer privacy-preserving sensing solutions including for the case when humans are present in the TSSA.

[PR 5.9-2] The 6GS should provide a means to inform users about active ongoing sensing operations.

[PR 5.9-3] The 6GS should protect privacy by offering suitable means to restrict linking of sensing results to other identifiable information.

5.9.4 Potential regulatory requirements

[PRR 5.9-1] Potential regulatory guidelines should consider the impact of sensing performance, deployment, and sensing environment on privacy and provide appropriate guidelines that may vary depending on the use case or deployment.

5.10 Key issue #10: Unauthorized passive 6G RF sensing

5.10.1 Key issue details

RF sensing utilizes electromagnetic waves to detect changes in the channel by measuring the mono-static or bi-static reflections of the sensing target. Passive sensing is a well-known technique that utilizes sensing signals that are transmitted for a different purpose for sensing in a bi-static or multi-static mode.

Some envisioned 6G use cases such as health monitoring (see ETSI GR ISC 001 [i.1], clause 5.8) require that the reflected sensing signals contain sensitive information about the sensed individual. If these reflected sensing signals can be received and used for sensing by unauthorized 3rd parties, such a 3rd party is able to extract the sensitive information about the sensed individual with the consequence that the privacy of the sensed person may be affected.

5.10.2 Security, privacy, and trustworthiness threats

The issue translates to multiple threats to privacy: Essentially, the passive listener can detect the signals and potentially even the intention. It may be possible to identify individuals, and the measurements may be linked to previous measurements to track and profile the user.

The sensing data may further be used for non-repudiation, e.g. to claim some behaviour of the individual, especially in combination with extensive storage of such data over time, leading to data disclosure. Finally, the individual is not aware of the passive listener.

5.10.3 Potential requirements and metrics

[PR 5.10-1] The 6GS should provide a means to prohibit passive sensing.

[PR 5.10-2] The 6GS should provide a means to classify vulnerability towards passive sensing for specific use cases, sensing modes, and deployments.

5.11 Key issue #11: Authorization of ISAC-enabled 6GS entities

5.11.1 Key Issue details

When executing a sensing task, 6GS entities (UEs, (R)AN, NFs, AFs) interact with each other to stay coordinated on which entity to perform sensing (transmitting and/or receiving Sensing Signals), collect, process, fuse, store and expose sensing data and sensing results. Such system activities may require authorization procedures with a high level of granularity, given the complex nature of executing a sensing task also when considering the different required data exchange requirements (latency, bandwidth, privacy) to support 6G and non-6G sensing.

5.11.2 Potential threats

Depending on the sensitivity of sensing data and sensing results, the system components accessing or providing sensing resources, sensing data or sensing results may not have the authorization to do so, resulting in undesired data leakages.

5.11.3 Potential requirements and metrics

[PR 5.11-1] The 6GS should enforce authorization of sensing entities and sensing functions to access or provide resources, specific to different sensing services.

5.12 Key issue #12: Privacy-related aspects regarding UE positioning in sensing

5.12.1 Key issue details

Certain sensing methodologies require the position of the involved sensing entities to accurately interpret the sensing results. For example, bistatic sensing typically computes range estimates based on the time difference of arrival between the direct line of sight path and the reflected path (from transmitter to target to receiver). This method necessitates precise positioning of both sensing entities to accurately determine the range from the time difference. Similar considerations arise in monostatic cooperative sensing, multistatic sensing, and simultaneous localization and mapping. When at least one of the sensing entities is a UE, this poses a privacy threat, as it enables the tracking of users participating in the sensing process.

In practice, positioning procedures are never exact, and the location of sensing entities can only be estimated. Consequently, errors in positioning procedures induce corresponding errors in sensing measurements. The positioning accuracy required for a sensing task is therefore determined by the application's specific localization requirements. In line with the GDPR principle that *"Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"*, GDPR [i.9], article 5c, the positioning accuracy should be no greater than what is necessary for the given application.

5.12.2 Security, privacy, and trustworthiness threats

The issue leads to multiple privacy and confidentiality threats, but primarily data misuse since involved users' or infrastructure's locations may be tracked despite the positioning's sole purpose being to assist in sensing. Other threats include unauthorized data collection (location tracked without explicit consent) and unintended disclosure (user may wish to assist in sensing without intending to reveal their location).

5.12.3 Potential requirements and metrics

[PR 5.12-1] The 6GS should obtain user consent for location information collection before utilizing their UE(s) for sensing operations.

[PR 5.12-2] The 6GS should delete UE location information collected for sensing after completing the corresponding sensing task.

[PR 5.12-3] The 6GS should ensure that positioning procedures provide only the level of accuracy strictly required for the sensing task and avoid collecting unnecessarily precise UE positions.

NOTE 1: The "level of accuracy strictly required" in PR3 does not necessarily correspond to ideal conditions. For example, the 6GS may collect positioning information with a sufficiently high level of accuracy to provide robustness against sensing entity dropout.

NOTE 2: All three PRs apply only to positioning procedures initiated to support a sensing task. They should not be interpreted as relating to general 6GS positioning procedures.

5.13 Key issue #13: Privacy risks from heterogeneous sensing capabilities

5.13.1 Key issue details

To fulfil a service request from an (3-)SSC in ISAC-enabled 6GS, entities such as UEs and BSs function as SIDPs, contributing to the collection of sensing data. However, these SIDPs may differ significantly in their sensing capabilities - some can only detect basic object categories, while others may capture fine-grained and potentially sensitive personal information, such as gender, behavioural patterns, or movement trajectories.

5.13.2 Security, privacy and trustworthiness threats

The disparity in sensing capabilities across SIDPs results in uneven privacy exposures, even when the (3-)SSC's requirements are limited to coarse-level information. Moreover, in ISAC scenarios, where sensing data from multiple SIDPs is fused or processed at the network or edge, additional privacy risks emerge. Sensitive information obtained by more capable SIDPs can be inadvertently propagated, inferred, or reconstructed during data fusion that can lead to unintended privacy leakages. This can occur even if each individual SIDP adheres to its own local privacy constraints. Therefore, there is a need for system-wide privacy enforcement mechanisms during both sensing and subsequent processing stages.

5.13.3 Potential new requirements

[PR 5.13-1] The 6GS should provide mechanisms to select and configure SIDPs with limited sensing capabilities based on use case-specific privacy constraints to prevent unintended capture of sensitive data.

[PR 5.13-1] The 6GS should provide privacy-preserving mechanism to remove or obfuscate sensitive information from sensing data and sensing results, when required.

5.14 Key issue #14: Privacy-related aspects of AI-based sensing data processing

5.14.1 Key issue details

AI plays a crucial role in sensing by enabling the processing, analysis and interpretation of vast amounts of data collected from various sensing entities. Through techniques like machine learning and deep learning, AI can identify patterns, make predictions, and facilitate real-time decision-making.

Training of AI models to process sensing data requires data collection which often involves gathering sensitive personal information, such as location, health metrics, or behavioural patterns, which raises concerns about consent and the potential for sensing data misuse. Users may not fully understand what training data is being collected or how it will be used, leading to issues related to lack of control [i.22].

5.14.2 Security, privacy, and trustworthiness threats

Trained AI models to process sensing data may leak private training data through model inversion or membership inference attacks, even when data is anonymized, compromising individual privacy. The reconstruction of sensitive inputs or identity might also be possible, where an attacker queries on the trained models on sensitive sensing measurements.

The potential lack of explainability of blackbox AI models may harm trustworthiness, as it can be difficult to ascertain how data is processed and how decisions are made based on that data. In addition to explainability, both fairness and robustness of the models should be considered to ensure the models used for data processing are trustworthy, see ETSI TR 128 908 [i.23].

Additionally, the storage and security of training data and AI models present challenges, as breaches can reveal personal information.

5.14.3 Potential requirements and metrics

[PR 5.14-1] The 6GS should restrict training data collection to information for which users have given consent, ensuring it is only used for the intended purpose.

[PR 5.14-2] The 6GS should implement techniques to anonymize or pseudonymize training data, ensuring that individuals cannot be readily identified from the data used for training or inference.

[PR 5.14-3] The 6GS should employ security protocols during storage and communication of the training data and AI models to protect against unauthorized access and breaches.

[PR 5.14-4] The 6GS should ensure that deployed AI models used for sensing data processing are trustworthy and transparent when possible, allowing users to understand how their data is being used and how decisions are made.

[PR 5.14-5] The 6GS should guarantee that AI models are trained in a privacy preserving way so that the parameters of the AI models cannot reveal any information about data used for training.

5.15 Key issue #15: Privacy challenges and malicious attacks in cooperative sensing

5.15.1 Key issue details

In cooperative sensing, UEs and BSs actively share both unprocessed data, processed data or sensing results across UEs or with the BS and core network, which can inadvertently lead to the disclosure of sensitive private information, including individuals' identities, locations and behaviours, to third parties or nearby devices. This interconnectedness, while enhancing the efficacy of sensing tasks, raises significant privacy and security concerns.

5.15.2 Security, privacy, and trustworthiness threats

One major issue is that correlating data from multiple cooperative sources can allow for the de-anonymization of individuals, even when each data source initially appears anonymized. This poses a risk of re-identifying individuals based on aggregated information, undermining the very purpose of anonymization. Additionally, in cooperative environments, the presence of malicious nodes poses a further threat, as these entities can inject false sensor data into the system. Such malicious activities can manifest as fabricated detections or spoofing, leading to inaccurate data interpretations and potentially harmful consequences. Therefore, while cooperative sensing can enhance data-driven insights, it is imperative to address these privacy and security challenges through robust security measures, data governance, and ethical considerations to protect individual privacy.

5.15.3 Potential requirements and metrics

[PR 5.15-1] The 6GS should protect the relationship between cooperating sensing entities as well as their identities.

[PR 5.15-2] The 6GS should apply data anonymization and pseudonymization techniques to protect the identities of users and sensed targets.

[PR 5.15-3] The 6GS should establish secure data sharing protocols that define how data can be shared among UEs and between the UEs and the BS as well as the core network while preserving the privacy of users associated with UEs and the sensing data or sensing results.

[PR 5.15-4] The 6GS should implement encryption protocols for stored and transmitted data. This ensures that sensitive information, during storage or collection between UEs, BSs, and the core network, remains secure from interception and unauthorized access.

[PR 5.15-5] The 6GS should ensure that any collected sensing data, sensing results, and sensing contextual information is not disclosed to unauthorized entities.

6 Considerations and consolidation for privacy, security, and trustworthiness

6.1 Considerations on sensing data ownership and accountability in ISAC System

In conventional data systems, the relationship between the data subject (the person the data is about), data processor (the entity which processes the data) and the data controller (the entity determining the purpose and means of the data processing) is generally well-defined, see [i.21]. However, in ISAC systems, determining ownership of the sensing data and who is responsible for its handling and protection becomes significantly more complex. Here, data ownership is considered in line with data protection principles as the rights and control of natural persons over data that identifies or can be linked to them.

ISAC enables the 6GS to sense the environment by collecting and processing sensing measurements, data, and results from base stations and UEs. This information pertains not only to users but also to any entity or individual within the TSSA, including bystanders or objects that never directly interact with the 6GS. As a result, data about non-users is constantly generated, which creates data ownership disputes, since these individuals are not explicit participants in the data generation or transmission process.

Furthermore, cooperative sensing among UEs or between UEs and base stations can involve joint signal processing and data analytics. This makes it difficult to trace any single piece of information back to a specific data subject, undermining the ability to assign clear data ownership. In such scenarios, it is challenging to find which participating entity is responsible for a specific outcome on sensing data.

Without clear information on data ownership, complying with regulatory requirements such as consent, data transparency, and usage limitation becomes difficult, as these require the involvement of the data owner. This creates risks of unauthorized data processing or unintended misuse of sensitive information.

Moreover, in the absence of well-defined governance frameworks and agreements that clearly allocate roles, responsibilities and liabilities, ensuring accountability among diverse stakeholders in ISAC systems remains a significant challenge, potentially leading to gaps in sensing data protection and misuse.

Based on the above considerations, the following potential approaches could be considered to address the data ownership and accountability concerns. For instance, the 6GS could log the roles and contributions of participating sensing entities in a verifiable and auditable manner, helping to clarify ownership of data collected during a sensing task and the responsibility in its use. The operators and UEs could establish Service Level Agreements (SLAs) that explicitly define conditions for data provenance, ensuring traceability and compliance with agreed data handling practices. In addition, the regulatory guidelines could specify designating a responsible authority or organization to uphold privacy principles such as consent, transparency, and the protection of non-user data subjects, thereby supporting both ownership and accountability.

6.2 Considerations for trustworthiness

In 2024, European Commission (EC) sent a standardization request to the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (Cenelec) and European Telecommunications Standards Institute (ETSI) to work on a European Trusted Data Framework, see [i.24]. The request specifically highlighted that the standardization bodies should work on trustworthiness and interoperability requirements for data sharing and highlighted key aspects that need standardization.

This led to the establishment of the Technical Committee (TC) Data Solutions (DATA). DATA recently brought forward new work item proposals around a landscape gap analytics (ETSI TR 104 177 [i.25]) and working on data quality assessment including trustworthiness (ETSI TR 104 180 [i.26]) in and across telecommunication systems. These work item proposals received strong support by both industry and academic institutions and the work conducted by TC DATA indicates the importance of studying trustworthiness.

Additionally, Cenelec has been working on a draft CWA on "Trusted Data Transaction - Part 2: Trustworthiness requirements" [i.27]. The draft CWA captures definitions and principles for trusted data transactions. It also discusses trustworthiness definition and requirements for trusted data transactions.

Based on these above on-going standardization works; it is imperative in ISAC to consider trustworthiness as a key study item, as it would need to conform to any European standards developed for data sharing (e.g. ISAC).

Trustworthiness can be use-case or scenario dependent and should be assessed as such. Trustworthiness was studied in the current 3GPP standards in ETSI TR 128 908 [i.23] specifically for AI/ML. The discussion is on trustworthiness metrics for AI/ML use-cases. Trustworthiness indicators discussed are explainability, fairness, robustness. Some identified issues include the relation between the trustworthiness indicators/metrics and the 3GPP management or network data, and how to support the consumer and the producer to have a consistent interpretation of the trustworthiness indicators/metrics.

The challenges of trustworthiness for ISAC may consider several aspects and characteristics as described in ISO/IEC TS 5723 [i.3]. Trustworthiness indicators/metrics may be applicable for sensing data/results generated by the 6GS. The data generated by the system entities can intentionally or unintentionally deviate from expected system behaviour. For example, a malicious entity injecting false data and causing intentional harm, or an unintentional degradation of data quality due to intrinsic or extrinsic factors need to be assessed and reported.

The trustworthiness for ISAC worth considering further starting from analysis of ISAC use-cases identified in ETSI GR ISC 001 [i.1] to identify and define if feasible trustworthiness metrics/indicators for sensing data/results.

6.3 Consolidated Potential Functional Requirements

The Consolidated Potential functional Requirements (CPR) are categorized into Tables 4 to 9:

Table 4: CPR for user consent in 6GS

CPR #	CPR	Original PR #
CPR 1-1	The 6GS should provide means of gathering policies and consent for collection, processing, storage of sensing data and location from humans connected to 6GS, covering both public and non-public spaces.	**PR 5.6-1** **PR 5.7-1** **PR 5.12-1**
CPR 1-2	The 6GS should provide means to ensure confidentiality for non-human objects.	**PR 5.7-3**
CPR 1-3	The 6GS should provide mechanisms to manage sensing consent and transparency requirements.	**PR 5.7-5** **PR 5.7-3** **PR 5.7-4**
CPR 1-4	The 6GS should restrict training and inference data collection to information for which users have given consent.	**PR 5.14-1**

Table 5: CPR for transparency in 6GS

CPR #	CPR	Original PR #
CPR 2-1	The 6GS should have means to inform users about active sensing operations.	**PR 5.9-2**
CPR 2-2	The 6GS should provide mechanisms to comply with transparency requirements for how data is handled at every stage including collection, processing, storage, and exposure.	**PR 5.7-1** **PR 5.7-7**

Table 6: CPR for privacy preservation in 6GS

CPR #	CPR	Original PR #
CPR 3-1	The 6GS should provide privacy-preserving sensing for all scenarios, including when consent is not possible.	**PR 5.6-3** **PR 5.8-1** **PR 5.9-1** **PR 5.13-1** **PR 5.13-2** **PR 5.14-5**
CPR 3-2	The 6GS should protect identities through anonymization and pseudonymization, preventing linking of sensing results to individuals and protecting relationships between cooperating sensing entities.	**PR 5.9-3** **PR 5.15-1** **PR 5.15-2** **PR 5.14-2**
CPR 3-3	The 6GS should ensure that positioning procedures provide only the level of accuracy strictly required for the sensing task and avoid collecting unnecessarily precise UE positions .and delete the information after completing the corresponding sensing task.	**PR 5.12-3** **PR 5.12-2**

Table 7: CPR for system security of 6GS

CPR #	CPR	Original PR #
CPR 4-1	The 6GS should verify the integrity of entities involved in the sensing task and protect data integrity during collection, processing and storage.	**PR 5.3-1** **PR 5.3-2** **PR 5.5-1** **PR 5.4-2**
CPR 4-2	The 6GS should restrict access to sensing data and sensing results to authorized entities.	**PR 5.15-5** **PR 5.4-1** **PR 5.6-4** **PR 5.11-1** **PR 5.6-3**
CPR 4-3	The 6GS should implement encryption protocols and ensure security of sensing data and sensing results during collection and storage.	**PR 5.15-3** **PR 5.15-4** **PR 5.14-3** **PR 5.4-4** **PR 5.2-1** **PR 5.4-3**
CPR 4-4	The 6GS should provide means and procedures for tracing the immutability of sensing data and sensing results.	**PR 5.5-2**
CPR 4-5	The 6GS should protect targets from unauthorized sensing by controlling which sensing receivers and transmitters can operate in non-public spaces, enforcing authorization for accessing sensing resources.	**PR 5.1-1** **PR 5.6-2** **PR 5.11-1**

Table 8: CPR for physical layer security of 6GS

CPR #	CPR	Original PR #
CPR 5-1	The 6GS should provide means to prohibit passive sensing and classify vulnerability levels for specific use cases, sensing modes, and deployments.	**PR 5.10-1** **PR 5.10-2**
CPR 5-2	The 6GS should provide means to detect unauthorized 6G sensing transmissions.	**PR 5.3-1** **PR 5.5-1**
CPR 5-3	The 6GS should provide mechanisms to secure 6G RF sensing signals from being tampered which may result in manipulated sensing data and sensing results.	**PR 5.3-2**

Table 9: Consolidated considerations towards regulatory bodies

CPR #	Consolidated Considerations	Original PR #
CC 6-1	Regulatory bodies should define transparency and data governance guidelines for sensing-enabled 6GS.	**PR 5.7-6** **PR 5.4-5**
CC 6-2	Regulatory bodies should provide operation guidelines for sensing of humans and infrastructure.	**PRR 5.8-1** **PRR 5.9-1** **PR 5.7-2**

7 Key issues on sustainability

7.1 Key issue #1: Power consumption of ISAC-enabled 6GS

7.1.1 Key issue details

As the telecommunications industry evolves from 5G to 6G, power efficiency emerges as a crucial sustainability goal in response to the increasing demand for continuous environment monitoring through ISAC and the need to mitigate environmental impacts. One key strategy in the design of energy efficient ISAC systems is to enable adaptive sensing and communication, which allows these systems to optimize when and how sensing occurs based on real-time conditions. Additionally, edge processing plays a crucial role in enhancing energy efficiency; by enabling on-device and edge processing or inference, ISAC systems can minimize the need to transmit all data to the cloud, thereby conserving energy and reducing latency. Moreover, through identification of edge processing, power limited devices can preserve energy through offloading compute processing to these edge compute processing, thereby enabling optimal energy configuration whilst preserving resilience of sensing tasks in obtaining sensing results for the sensing service request.

Moreover, ISAC can enable the 6GS to optimize power consumption through sensing-assisted communication allowing for adaptive communication strategies that adjust system parameters such as transmit power based on the specific conditions and requirements of the environment. An example is given in ETSI GR ISC 001 [i.1], suggesting that when devices are in close proximity, lower transmission power can be employed, significantly conserving energy while still ensuring effective communication.

In the context of energy-efficient smart buildings, ISAC can be leveraged to monitor occupancy in real-time and dynamically adjust heating, ventilation, air conditioning, and lighting systems as considered in IEEE 802.11bf [i.28]. By aligning sensing results with smart building systems to manage energy consumption with actual occupancy levels, ISAC can lower energy usage, contributing to more sustainable building operations. Overall, implementing energy-aware strategies using ISAC systems not only enhances operational efficiency but also supports broader sustainability goals.

To ensure ISAC systems meet the sustainability goal of energy efficiency, it is important to design and optimize the communication systems thoughtfully. By focusing on adaptive communication strategies, and more specifically on adjusting transmit power based on real-time conditions, ISAC systems can significantly reduce energy usage without compromising performance. Similarly, incorporating low-latency on-device and edge processing allows for data to be analysed locally, minimizing the need for extensive data transmission to centralized servers.

7.1.2 Potential requirements and metrics

Potential requirements to achieve and support the energy efficient ISAC systems design include the following:

[PR 7.1-1] The 6GS should utilize on-device and edge processing, to minimizing the need for extensive data transmission.

[PR 7.1-2] The 6GS should offer robust support for designing power-efficient communication systems, leveraging the sensing functionalities.

[PR 7.1-3] The 6GS should be designed to support ISAC in a power efficient way to accommodate the power consumption constraints of sensing task members and minimize the overall power consumption of sensing services.

7.2 Key issue #2: Utilization of spectrum resources in ISAC-enabled 6GS

7.2.1 Key issue details

Integrating sensing capabilities into the cellular communications system offers new services with the potential to enable numerous applications, coming at the cost of specific and significant needs for spectrum. Meanwhile, new communication services and applications towards IMT2030 and beyond may also require additional spectrum to account for the explosive mobile data traffic growth. Since both sensing and communication services in a 6G ISAC system should utilize the same spectral resources, this presents a significant challenge.

Although there are discussions to allocate new spectrum to 6G in the lower mid-band, spectrum is a precious resource that should be utilized smartly.

Without efficient sharing of spectrum between communication and sensing services, ISAC service may not be sustainable in terms of costs and, consequently, will have a negative social impact in terms of inclusivity.

In addition, the infrastructure required for communication and sensing, such as antenna panels and antenna towers, would need to increase if both functionalities operate in dedicated frequency bands, which will have a significant impact on the environment.

Finally, potential interference or inefficient utilization of spectrum such as static spectrum sharing between communication and sensing will necessitate complex algorithms. Such algorithms may increase the power consumption of the UE and infrastructure.

7.2.2 Potential requirements and metrics

[PR 7.2-1] The 6GS should enable efficient sharing of spectrum resources between communication and sensing functionality.

[PR 7.2-2] The 6GS should provide methods for efficient use of spectrum resources while meeting the sensing performance requirements.

7.3 Key issue #3: Overall environmental system footprint of ISAC-enabled 6GS

7.3.1 Key issue details

The United Nations Sustainability Goal 12 [i.29] on responsible consumption and production promotes a more sustainable lifestyle, by calling for responsible utilization of resources and a reduction of waste.

To quantify the impact, the environmental system footprint may be used that describes the impact of the 6G ISAC system on the environment in terms of energy consumption, carbon emissions, e-waste and resource utilization. This definition is broader than the ecological system footprint as a measure to quantify the biologically productive land and sea area required to support the consumption of resources and waste absorption of some entity.

Adding a new functionality to an existing system, as is the idea behind ISAC, usually comes with an increased environmental system footprint. The amount of resource utilization thereby depends on the complexity and capabilities of the newly introduced components in CN, RAN, and at the sensing entities itself. During operation, an optimized selection of sensing entities and sensing functions for a specific sensing task may support minimization of the environmental system footprint.

Leveraging the idea of integration with a high level of re-use of existing hardware may help to support the SDG12 by reducing the need for dedicated hardware and software components and wireless signal transmissions. That way, the additional environmental footprint of sensing can be kept small by choosing the optimal integration level.

In addition, the intelligent utilization of ISAC may further support the reduction of the overall environmental footprint of the 6GS by optimizing communication functionality, potentially resulting in reduced hardware requirements and reduced energy consumption due to the optimized communication functionality.

7.3.2 Potential requirements and metrics

The 6G ISAC system design should consider the resulting footprint during the entire development cycle and prefer options with smaller system footprint. Potential requirements could be formulated as follows:

[PR 7.3-1] The 6GS should have a means to quantify the contributions of system entities on the environmental system footprint.

[PR 7.3-2] The 6GS should minimize its environmental footprint when implementing ISAC.

[PR 7.3-3] The 6GS should support efficient sensing signal transmissions and measurement data transfer to processing entities.

[PR 7.3-4] The 6GS should support the selection of sensing entities and functions to ensure minimal environmental impact, if possible.

7.4 Key issue #4: Considerations on 'good health and well-being' with ISAC-enabled 6GS

7.4.1 Key issue details

The United Nations definition of sustainability [i.29] includes 'good health and well-being' as one of their 17 sustainability goals.

The impact on a potential 6GS is twofold: on the one hand, ISAC functionality may be leveraged to improve the health conditions of individuals in various ways directly and indirectly. On the other hand, it has to be guaranteed that the newly introduced ISAC functionality does not harm individuals in any way.

For the first category, ETSI GR ISC 001 [i.1], identified exemplary use cases. These include utilizing ISAC for real-time monitoring of health hazard and disaster risk, outdoor healthcare sensing and monitoring, and remotely controlled robots for senior citizen monitoring and care, that have a direct impact on the health status and well-being of individuals.

In addition, the health conditions of individuals may be increased indirectly through enhanced safety systems and personal support for individuals. Exemplary use cases for this category as identified in ETSI GR ISC 001 [i.1] include emergency vehicle route planning, throughput and safety on road intersections, and emergency search and rescue applications.

For the second category, the use case on body proximity sensor described in ETSI GR ISC 001 [i.1] addresses the goal to not introduce new threats to the health of individuals by leveraging ISAC to reduce exposure of individuals to electromagnetic waves.

In order to meet the sustainability goal for good health and well-being, it should furthermore be guaranteed that positive features are available to as many people as possible, to avoid violating the sustainability goal "reduced inequalities".

7.4.2 Potential requirements and metrics

Potential requirements to achieve and support the good health and well-being use case may include the following:

[PR 7.4-1] The 6GS should enable sensing features that support individuals in preserving or enhancing their personal health and well-being.

[PR 7.4-2] The 6GS should avoid increasing inequalities from its usage if sensing is supported.

8 Considerations and consolidation on sustainability

8.1 High-level objectives for sustainability

The development of sustainable ISAC-enabled 6GS requires a comprehensive approach addressing multiple interconnected dimensions. These high-level objectives are derived from the key issues on sustainability described in clause 7.

- **Power efficiency:** Leverage on-device and edge processing while supporting power-efficient designs for sensing tasks execution, see clause 7.1.
- **Spectrum resource utilization:** Enable intelligent spectrum sharing between communication and sensing functionalities within available bandwidth, see clause 7.2.
- **Environmental system footprint:** Minimize environmental impact through efficient signal transmission and strategic sensing entity selection, see clause 7.3.
- **Social equity:** Support health and well-being applications while ensuring equitable access without amplifying inequalities, see clause 7.4.

Together, these four objectives form an integrated sustainability framework essential for guiding ISAC-enabled 6GS to be sustainable and inclusive.

9 Conclusion

The scope of the present document is to identify 6G ISAC challenges on security, privacy, trustworthiness, and sustainability. To this end, relevant key issues and considerations are described that result in a comprehensive set of potential requirements a future 6G system should support to maximize the societal benefits of the newly introduced features.

The work is placed in a world-wide framework of efforts towards an ISAC-enabled 6G system. These range from research activities carried out by academia, industry, within collaborative projects, over specific stakeholder associations, and to early efforts within (pre-)standardization bodies.

The present document provides a comprehensive study of the security, privacy, trustworthiness, and sustainability aspects integral to the successful deployment of ISAC within future 6G systems. The present document has been dedicated to identifying key challenges and laying the groundwork for developing and deploying ISAC within future 6G systems.

During this first phase, a total of 19 key issues were identified and analysed, comprising 15 related to security and privacy, and 4 concerning sustainability. Additionally, the key issues on sustainability identify the UN sustainability development goals which can be impacted with an ISAC-enabled 6GS. The key issues identified are:

Key issues on security and privacy:

1) Use of 6GS for unauthorized sensing.

2) Use of sensing signals by the target for data eavesdropping.
3) Over-the-air manipulation of 6G RF sensing signals.
4) Secure handling of sensing data.
5) Integrity of ISAC-enabled 6GS entities, and immutability of sensing data or sensing results.
6) Sensing privacy, confidentiality, and consent in non-public spaces.
7) Privacy issues related to consent and transparency.
8) Privacy-related aspects regarding sensing of humans that are not connected to the 6GS.
9) Privacy-related aspects regarding sensing of humans that are connected to the 6GS.
10) Unauthorized passive 6G RF sensing.
11) Authorization of ISAC-enabled 6GS entities.
12) Privacy-related aspects regarding UE positioning in sensing.
13) Privacy risks from heterogeneous sensing capabilities.
14) Privacy-related aspects of AI-based sensing data processing.
15) Privacy challenges and malicious attacks in cooperative sensing.

Key issues on sustainability:

1) Power consumption of ISAC-enabled 6GS.
2) Utilization of spectrum resources in ISAC-enabled 6GS.
3) Overall environmental system footprint of ISAC-enabled 6GS.
4) Considerations on 'goal on good health and well-being' with ISAC-enabled 6GS.

For each of these issues, the present document provides a detailed description and derives a set of potential requirements that should be addressed in future standardization work. Additionally, a comprehensive set of potential threats is identified for the key issues on privacy and security.

Furthermore, the present document provides views on broader societal topics that are paramount for the acceptance of sensing services in a future 6G system. This includes considerations regarding the ownership of sensing data, exploring the complex interplay between data controllers, data processors, and data subjects, especially in the context of emerging privacy regulations. In addition, aspects related to trustworthiness in the context of ISAC are highlighted, with the conclusion that it should be an inherent characteristic of the system, encompassing reliability, integrity, and the explainability of outcomes.

The consolidation of these key issues and potential requirements provides a foundation for the subsequent normative work or any further studies and/or specifications work related to ISAC-enabled 6G systems. After the conclusion of this study phase, this ISG will now transition into its second phase, where it is suggested that the corresponding follow-up work should focus on developing concrete solutions to address the challenges identified within this present document.

In addition, it is recommended that the findings of the present document are proposed for consideration to the relevant standardization bodies (e.g. 3GPP SA3) to guide the development of secure, privacy-preserving, trustworthy, and sustainable ISAC services for future 6G Systems.

The foundational analysis that is presented within this present document may support the social benefit and technical feasibility of ISAC, which is crucial for successful deployments. It may help in guiding the design of a 6G system where ISAC is not only a powerful technological enabler but is also fundamentally secure, trustworthy, and aligned with societal and ethical values regarding user privacy and environmental sustainability.

Annex A:
Mapping of security and privacy key issues to use cases of ETSI GR ISC 001

This clause maps the security and privacy key issues identified in clause 5 of the present document to the use cases presented in ETSI GR ISC 001 [i.1], the mapping is provided in Table A.1. The intention of the mapping is to provide the reader an understanding of the context in which the identified key issues may be relevant.

The use case specifications in ETSI GR ISC 001 [i.1] provide insufficient detail for a direct, objective mapping; only five out of the eighteen use cases explicitly contain privacy or security requirements. Additionally, the few use cases which do mention such requirements, do not contain sufficient detail to distinguish among the key issues identified in clause 5. Therefore, the following mapping is derived from an interpretation of the ETSI GR ISC 001 [i.1] use case descriptions and their implicit needs as derived from the key issues defined in clause 5.

Consequently, the use case mapping should be considered preliminary, without the aspiration to be complete or absolute since the relevance may depend on the exact implementation of the use cases.

To make this interpretation-based mapping as transparent as possible, a set of conditions for each KI is provided. These conditions are intended to identify characteristics that make a use case susceptible to the corresponding key issue. The conditions are applied consistently across most use cases, with a few noted exceptions. For these exceptions, the specific use case is identified, and a justification is provided.

Table A.1: Mapping of key issues to use cases

	KI#1	KI#2	KI#3	KI#4	KI#5	KI#6	KI#7	KI#8	KI#9	KI# 10	KI# 11	KI# 12	KI# 13	KI# 14	KI# 15
UC#1	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
UC#2			x			x	x	x	x		x		x		
UC#3	x	x	x	x	x	x				x	x				x
UC#4	x	x	x	x	x	x	x	x	x	x	x	x	x		x
UC#5	x	x	x	x	x	x	x	x	x	x	x		x	x	x
UC#6	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
UC#7			x	x							x				x
UC#8	x	x	x	x	x	x	x	x	x	x	x		x	x	
UC#9			x	x	x	x	x	x	x		x		x		
UC#10			x	x	x	x					x				x
UC#11	x		x	x	x	x				x	x				x
UC#12			x	x	x	x					x				x
UC#13	x		x	x	x	x				x	x				
UC#14	x	x	x	x	x	x	x	x	x	x	x		x		x
UC#15	x	x	x	x	x	x				x	x				x
UC#16	x	x	x	x	x	x	x	x	x	x	x		x	x	
UC#17	x	x	x	x	x		x	x	x	x	x	x	x		x
UC#18	x	x	x	x	x	x	x	x	x	x	x	x	x		x

Key Issue #1 (Use of 6GS for unauthorized sensing):

- A use case is considered relevant to Key Issue #1 if it satisfies **both** of the following conditions:
  - The sensing signal is detectable by an unauthorized entity (this excludes use cases with weak transmit signals).
  - The sensing signal is transmitted in a public space.
- **Exception:** Use Case #7 is exempt as unauthorized sensing is not considered a primary concern within an emergency scenario.

Key Issue #2 (Use of sensing signals by the target for data eavesdropping):

- A use case is considered relevant to Key Issue #2 if it satisfies **at least one** of the following conditions:
  - The sensing target is a receiver.
  - The sensing target may carry a receiver.
  - The sensing target is in a public space.

Key Issue #3 (Over-the-air manipulation of 6G RF sensing signals):

- A use case is considered relevant to Key Issue #3 if it satisfies the following condition:
  - The use case involves sensing signals.

Key Issue #4 (Secure handling of sensing data):

- A use case is considered relevant to Key Issue #4 if it satisfies the following condition:
  - The use case leverages more than one sensing entity or sensing function for performing sensing measurements, processing sensing results, and/or storing sensing data within the RAN or core network.

Key Issue #5 (Integrity of ISAC-enabled 6GS entities, and immutability of sensing data or sensing results):

- A use case is considered relevant to Key Issue #5 if it satisfies the following condition:
  - The use case involves sensing data or sensing results shared with the RAN or core network.

Key Issue #6 (Sensing privacy, confidentiality, and consent in non-public spaces):

- A use case is considered relevant to Key Issue #6 if it satisfies at least one of the first two conditions AND at least one of the final two conditions:
  - The intended sensing targets are human.
  - Humans may be incidental sensing targets (i.e. subject to unintended disclosure).
  - The sensing task may collect information about critical infrastructure.
  - The sensing task occurs (at least partially) in non-public spaces.
- **Exception:** Use Case #7 is exempt. Although it may meet the conditions (e.g. targeting humans in a non-public space), privacy is not considered the primary concern in an emergency scenario.

Key Issue #7 (Privacy issues related to consent and transparency):

- A use case is considered relevant to Key Issue #7 if it satisfies **at least one** of the following conditions:
  - The intended sensing targets are human.
  - Humans may be incidental sensing targets (i.e. subject to unintended disclosure).
- **Exception:** Use Case #7 is exempt. In an emergency scenario, explicit consent and transparency are considered secondary concerns.

Key Issue #8 (Privacy-related aspects regarding sensing of humans that are not connected to the 6GS):

- The conditions for relevance are identical to those defined for Key Issue #7.

Key Issue #9 (Privacy-related aspects regarding sensing of humans that are connected to the 6GS):

- The conditions for relevance are identical to those defined for Key Issue #7.

Key Issue #10 (Unauthorized passive 6G RF sensing):

- The conditions for relevance are identical to those defined for Key Issue #1.

Key Issue #11 (Authorization of ISAC-enabled 6GS entities):

- All use cases are considered relevant to this key issue, as they all leverage 6G resources to perform sensing.

Key Issue #12 (Privacy-related aspects regarding UE positioning in sensing):

- A use case is considered relevant to Key Issue #12 if it satisfies **both** of the following conditions:
  - The sensing measurement involves at least one UE that is co-located with its owner (e.g. smartphone, smartwatch, XR headset/glasses, cars).
  - The sensing mode is bistatic, multistatic, or cooperative monostatic.
- **Exception:** Use Case #7 is exempt. In an emergency scenario, explicit consent and transparency are considered secondary concerns.

Key Issue #13 (Privacy risks from heterogeneous sensing capabilities):

- The conditions for relevance are identical to those defined for Key Issue #7.

Key Issue #14 (Privacy-related aspects of AI-based sensing data processing):

- A use case is considered relevant to Key Issue #14 if it satisfies the following condition:
  - The use case explicitly mentions ML/AI processing of sensing data.

Key Issue #15 (Privacy challenges and malicious attacks in cooperative sensing):

- A use case is considered relevant to Key Issue #15 if it satisfies the following condition:
  - The use case considers cooperation of multiple sensing entities.

NOTE: The mapping is based on the defined conditions and exceptions. However, if the potential requirements under the key issues are considered and the use cases are analysed in greater depth, additional mappings may also be justified.

Annex B:
Mapping of sustainability key issues to use cases of ETSI GR ISC 001

This clause maps the sustainability key issues identified in clause 7 of the present document to the use cases presented in ETSI GR ISC 001 [i.1], the mapping is provided in Table B.1. The intention of the mapping is to provide the reader an understanding of the context in which the identified key issues may be relevant.

The use cases described in ETSI GR ISC 001 [i.1] provide insufficient detail for a direct, objective mapping since sustainability is not covered. Therefore, the following mapping is derived from an interpretation of the ETSI GR ISC 001 [i.1] use case descriptions and their implicit needs as derived from the key issues defined in clause 7.

Consequently, the use case mapping should be considered preliminary, without the aspiration to be complete or absolute since the relevance may depend on the exact implementation of the use cases.

To make this interpretation-based mapping as transparent as possible, a set of conditions for each key issue is provided. These conditions are intended to identify characteristics that make a use case relevant for the corresponding key issue.

Table B.1: Mapping of sustainability key issues to use cases

	KI#1	KI#2	KI#3	KI#4
UC#1	x	x	x	x
UC#2	x	x	x	x
UC#3	x	x	x	
UC#4	x	x	x	
UC#5	x	x	x	x
UC#6	x	x	x	x
UC#7	x	x	x	x
UC#8	x	x	x	x
UC#9	x	x	x	x
UC#10	x	x	x	
UC#11	x	x	x	
UC#12	x	x	x	
UC#13	x	x	x	
UC#14	x	x	x	x
UC#15	x	x	x	
UC#16	x	x	x	
UC#17	x	x	x	x
UC#18	x	x	x	

Key Issue #1 (Power consumption of ISAC-enabled 6GS):

- A use case is considered relevant to Key Issue #1 if it satisfies **at least one** of the following conditions:
  - On-device processing is considered.
  - Edge processing is considered.
  - Data sharing is considered.
  - Sensing-assisted communications is considered.
  - 6GS provides a sensing service.

Key Issue #2 (Utilization of spectrum resources in ISAC-enabled 6GS):

- A use case is considered relevant to Key Issue #2 if it satisfies the following condition:
  - Sensing is performed over the same spectrum as communication services.

Key Issue #3 (Overall environmental system footprint of ISAC-enabled 6GS):

- A use case is considered relevant to Key Issue #3 if it satisfies the following condition:
  - The use case involves sensing with 6GS.

Key Issue #4 (Considerations on 'good health and well-being' with ISAC-enabled 6GS):

- A use case is considered relevant to Key Issue #4 if it satisfies **at least one** of the following conditions:
  - The use case involves functionality to improve the health conditions of individuals.
  - The use case involves functionality that can be used to harm individuals.

History

Version	Date	Status
V1.1.1	February 2026	Publication