ETSI TR 104 065 V1.1.1 (2025-05)

TECHNICAL REPORT

Securing Artificial Intelligence (SAI); AI Act mapping and gap analysis to ETSI workplan

Reference

DTR/SAI-0013

Keywords

artificial intelligence, regulation

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

Important notice

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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 Technical Report (TR) has been produced by ETSI Technical Committee Securing Artificial Intelligence (SAI).

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.

Introduction

The present document has been developed to give a summary of the role of ETSI's standards, and those in associated SDOs, that support the mandates and recommendations found in the EU's AI Act [i.1]. The content is indicative and as such there may be standards that have been overlooked and therefore not considered in the mapping.

1 Scope

The present document provides an analysis of the standardization requirements of the AI Act [i.1] against the workplan of ETSI (across all TBs) in order to identify gaps and the means to fill them.

NOTE: The present document is a Technical Report and contains no requirements, however the text does contain quotes from the AI Act [i.1] where mandates are stated, but where quoted these have no normative effect.

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] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[i.2] ETSI TR 104 029: "Securing Artificial Intelligence (SAI); Global Ecosystem".

[i.3] ETSI White Paper 52: "ETSI Activities in the field of Artificial Intelligence Preparing the implementation of the European AI Act".

[i.4] ETSI White Paper 61: "ETSI Technology Radar".

[i.5] Lisbon Treaty: "Consolidated Versions Of The Treaty On European Union And The Treaty On The Functioning Of The European Union".

[i.6] European Union: "Charter of Fundamental Rights of the European Union".

[i.7] ETSI Directives.

[i.8] ETSI FORGE.

[i.9] ETSI SAREF source files.

[i.10] ETSI GR SAI 001 (V1.1.1): "Securing Artificial Intelligence (SAI); AI Threat Ontology".

NOTE: Updated by ETSI TS 104 050 [i.20].

[i.11] ETSI GR SAI 006 (V1.1.1): "Securing Artificial Intelligence (SAI); The role of hardware in security of AI".

[i.12] ETSI GR SAI 009 (V1.1.1): "Securing Artificial Intelligence (SAI); Artificial Intelligence Computing Platform Security Framework".

[i.13] ETSI GR SAI 002 (V1.1.1): "Securing Artificial Intelligence (SAI); Data Supply Chain Security".

NOTE: Updated by ETSI TR 104 048 [i.25].

[i.14] ETSI GR SAI 007 (V1.1.1): "Securing Artificial Intelligence (SAI); Explicability and transparency of AI processing".

NOTE: Updated by ETSI TS 104 224 [i.23].

[i.15] ETSI GR SAI 013 (V1.1.1): "Securing Artificial Intelligence (SAI); Proofs of Concepts Framework".

NOTE: Updated by ETSI TR 104 067 [i.19].

[i.16] ETSI GR SAI 005 (V1.1.1): "Securing Artificial Intelligence (SAI); Mitigation Strategy Report".

NOTE: Updated by ETSI TR 104 222 [i.28].

[i.17] ETSI GR SAI 004 (V1.1.1): "Securing Artificial Intelligence (SAI); Problem Statement".

NOTE: Updated by ETSI TR 104 221 [i.27].

[i.18] ETSI GR SAI 011 (V1.1.1): "Securing Artificial Intelligence (SAI); Automated Manipulation of Multimedia Identity Representations".

NOTE: Updated by ETSI TR 104 062 [i.29].

[i.19] ETSI TR 104 067 (V1.1.1): "Securing Artificial Intelligence (SAI); Proofs of Concepts Framework".

[i.20] ETSI TS 104 050 (V1.1.1): "Securing Artificial Intelligence (SAI); AI Threat Ontology and definitions".

[i.21] ETSI TR 104 225 (V1.1.1): "Securing Artificial Intelligence TC (SAI); Privacy aspects of AI/ML systems".

[i.22] ETSI TR 104 031 (V1.1.1): "Securing Artificial Intelligence (SAI); Collaborative Artificial Intelligence".

[i.23] ETSI TS 104 224 (V1.1.1): "Securing Artificial Intelligence (SAI); Explicability and transparency of AI processing".

[i.24] ETSI TR 104 032 (V1.1.1): "Securing Artificial Intelligence (SAI); Traceability of AI Models".

[i.25] ETSI TR 104 048 (V1.1.1): "Securing Artificial Intelligence (SAI); Data Supply Chain Security".

[i.26] ETSI TR 104 030 (V1.1.1): "Securing Artificial Intelligence (SAI); Critical Security Controls for Effective Cyber Defence; Artificial Intelligence Sector".

[i.27] ETSI TR 104 221 (V1.1.1): "Securing Artificial Intelligence (SAI); Problem Statement".

[i.28] ETSI TR 104 222 (V1.2.1): "Securing Artificial Intelligence; Mitigation Strategy Report".

[i.29] ETSI TR 104 062 (V1.2.1): "Securing Artificial Intelligence; Automated Manipulation of Multimedia Identity Representations".

[i.30] ETSI TR 104 066 (V1.1.1): "Securing Artificial Intelligence (SAI); Security Testing of AI".

[i.31] ETSI Member Portal.

[i.32] ETSI standards search and download.

[i.33] ETSI Writing world class standards guidance.

[i.34] ETSI TR 103 935: "Cyber Security (CYBER); Assessment of cyber risk based on products' properties to support market placement".

[i.35] ETSI TS 104 223: "Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems".

[i.36] ETSI TR 103 305 (all parts): "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence".

[i.37] ETSI TS 102 165-1: "Cyber Security (CYBER); Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.38] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in the AI Act [i.1] and the following apply:

AI system: machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments

dactyloscopic: identification by comparison of fingerprints

deep fake: AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful

general-purpose AI model: AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are released on the market

informed consent: subject's freely given, specific, unambiguous and voluntary expression of his or her willingness to participate in a particular testing in real-world conditions, after having been informed of all aspects of the testing that are relevant to the subject's decision to participate

input data: data provided to or directly acquired by an AI system on the basis of which the system produces an output

intended purpose: use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation

risk: combination of the probability of an occurrence of harm and the severity of that harm

substantial modification: change to an AI system after its placing on the market or putting into service which is not foreseen or planned in the initial conformity assessment carried out by the provider

testing data: data used for providing an independent evaluation of the AI system in order to confirm the expected performance of that system before its placing on the market or putting into service

training data: data used for training an AI system through fitting its learnable parameters

validation data: data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and its learning process in order, inter alia, to prevent underfitting or overfitting

validation data set: separate data set or part of the training data set, either as a fixed or variable split

3.2 Symbols

Void.

3.3 Abbreviations

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

AI	Artificial Intelligence
AICIE	AI Common Incident Expression
EN	European Norm
hEN	Harmonised European Norm
OJEU	Official Journal of the European Union
PoC	Proof of Concept
SDO	Standards Development Organisation
TB	Technical Body
UCYBEX	Universal Cybersecurity Information Exchange Framework

4 Summary of provisions of the AI Act

4.1 Purpose of the act

The purpose of the AI Act [i.1] is identified in recital 1 of the agreed text as follows:

QUOTE: "*To improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union, in accordance with Union values, to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of fundamental rights of the European Union (the 'Charter'), including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union, and to support innovation. This Regulation ensures the free movement, cross-border, of AI-based goods and services, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.*"

The definition of what the AI act [i.1] covers is addressed in some detail in Articles 1 (Subject Matter), 2 (Scope) and 3 (Definitions) of the act. For the purposes of the present document some of the definitions given in Article 3 have been transposed to an ETSI style in clause 3.1 above and presented as terms.

NOTE: Definitions given in Article 3 of the AI Act [i.1] are usually considered as normative whereas the terms given in the present document are not.

4.2 References to the role of standards in the act

An arbitrary search of the text of the act for the word standard finds 109 occurrences many of which can be summarily dismissed with respect to the activity of ETSI or any other SDO. Recital 117 does introduce the role of Harmonised Standards and the role of the AI Office in their management. Therefore the purpose of conformance to Harmonised Standards as giving a presumption of conformity to the provisions of the act is consistent with other EU regulation. This does suggest that the SDOs should work to develop such hENs but also requires awareness that an SDO cannot simply choose to publish an hEN, rather an hEN has to be written against specific actions of the EU.

NOTE 1: An hEN is the product of a specific standardization request and has a citation in the Official Journal of the European Union (OJEU).

In Recital 121 of the Act [i.1] the means of elaboration of a technical standard are addressed and cites the importance of wide stakeholder involvement. It can be fairly stated that ETSI's representation satisfies the conditions underpinning the text of Recital 121.

NOTE 2: There are support schemes available to bolster SME attendance to ETSI that further enhance ETSI's ability to satisfy the stakeholder diversity criteria (noting too that ETSI's global reach enhances its cultural diversity).

NOTE 3: The voting of different forms of ETSI deliverable are defined in the ETSI Directives [i.7]. However with the exception of ENs where the National Voting process is invoked, the general model in ETSI Technical Bodies (TBs) is to work to achieve consensus and to not determine acceptability of the content from a member weighted vote.

NOTE 4: Recent updates to the ETSI Directives [i.7] address voting and participation exemptions for activity in ETSI taken in response to an EU Standardisation Request.

NOTE 5: When registering to meetings of ETSI's TBs delegates register as representatives of their member organizations and not as either individuals or national representatives (unless their member organization is explicitly the national representative).

There is some mention of energy efficiency of AI (see Article 40(2), Article 59(1)(a)(iii), Article 95(2)(b), and is a requirement of the technical documentation addressed in Article 53(1)(a) of [i.1]). In ETSI the TB Environmental Engineering (EE) does address some of the issues arising. However at a slightly deeper level the silicon architectures contribute here and without particular input from SDOs most of the major manufacturers of silicon processors are addressing power efficiency, and specialized processor models, that will continuously improve the environmental footprint of AI. This is obviously deep rooted and has concerns over how data is stored and accessed, the transfer of data and so forth.

RECOMMENDATION:
TC EE and similar bodies in ETSI (and partner SDOs) should take note of the energy efficiency requirements from [i.1] and give advice to ensure that stakeholders can comply with the intent of the regulation.

Article 31(12) of [i.1] is itself partly addressed by the widespread availability of the present document during its development and post publication. To quote: "*Notified bodies shall participate in coordination activities as referred to in Article 38. They shall also take part directly, or be represented in, European standardisation organisations, or ensure that they are aware and up to date in respect of relevant standards.*" There is no restriction of membership of ETSI that would prevent the cited notified bodies from engaging in the ETSI standardization process. Furthermore as the notified bodies are explicitly mandated to participate in the standardization process ETSI cannot be seen to inhibit them.

NOTE 6: The calendar of meetings of ETSI's TBs is visible to all through the ETSI Portal [i.31] and ETSI's members and counsellors have access to all meetings and documents. In addition all of ETSI's published output is available without charge from ETSI's website [i.32].

In Article 40(2) there is a general statement regarding standards quality (to quote "*When issuing a standardisation request to European standardisation organisations, the Commission shall specify that standards have to be clear, consistent, including with the standards developed in the various sectors for products covered by the existing Union harmonisation legislation listed in Annex I, and aiming to ensure that AI systems or AI models placed on the market or put into service in the Union meet the relevant requirements laid down in this Regulation*") that is fully met by ETSI's quality control processes, by the ETSI Writing World Class Standards guidance [i.33], and by ETSI Directives [i.7].

It is further indicated in Article 40(3) that, to quote (emphasis added for the purposes of the present document), "*The participants in the standardisation process shall seek to promote investment and innovation in AI, including through increasing legal certainty, as well as the competitiveness and growth of the Union market, and shall contribute to strengthening global cooperation on standardisation and* ***taking into account existing international standards in the field of AI*** *that are consistent with Union values, fundamental rights and interests, and shall enhance multi-stakeholder governance ensuring a balanced representation of interests and the effective participation of all relevant stakeholders*". The reference here to existing international standards could be taken, for the present document, to mean that the output from TC SAI and prior output from ISG SAI, as well as output from other ETSI TBs and SDOs (e.g. ITU-T, IETF, IEEE), can be used in support of the Act [i.1]. However, the definition of international standards that has been adopted in Europe is quite restrictive, limiting international standards to those adopted by the recognized International Standardization Organizations ISO, IEC and ITU. For the purposes of the present document however the wider aim is to have European standards adopted globally, thus reinforcing the implicit model of ETSI to bring global stakeholders together to develop standards in ETSI that are then adopted globally.

Reflecting on the requirement in Article 40(3) that standards developed, and the development process, is "*consistent with Union values*, *fundamental rights and interests*" it is recognized that the EU's values are laid out in Article 2 of the Lisbon Treaty [i.5] and the EU Charter of Fundamental Rights [i.6] and can be summarized in the following headings:

- Human dignity
- Freedom
- Democracy
- Equality
- Rule of law
- Human rights

ETSI addresses these in the Code of Conduct for ETSI Members found in the ETSI Directives [i.7] and in the ETSI Values statements also in the ETSI Directives [i.7].

4.3 Mandates for standards/standards content in the act

There are significant numbers of mandates in the act as evidenced by a simple search for the term "shall" for which there are 888 instances. Few of those are directed to technical standardization but rather to actions of member states and the offices of the EU. Therefore based on a crude filtering the number of mandates that require action by SDOs results in the smaller set considered below.

Article 4 (AI Literacy) may be met in part by the general purpose reports prepared by ETSI TC SAI. This includes the technical reports that address the AI Problem Statement [i.27], the AI Data Supply Chain [i.25], the AI Ontology [i.20], and others. Whilst it is mandated to improve AI literacy and places responsibility on providers and deployers the general analysis provided by ETSI can be seen as making provision for building that literacy.

NOTE: As a technology becomes more pervasive there is often a movement to address its role across all levels of education. This has been observed across all of human history and it is reasonably expected that knowledge and expertise in AI will become an endemic element of education in coming years.

ETSI has expanded on its activity in education in partnership with other SDOs in the form of a project under the Digital Europe banner addressing ESOs collaboration on education material for standards. A summary of the project is given in Annex A of the present document.

In Article 5 (prohibited AI practices) the mandate is framed as what cannot be done, whereas for standardization it has to be framed somewhat differently. This means what measures can be provided that, when followed, prevent the prohibited practices being placed in the market. This is explored in more detail later in the present document.

Some of the mandates allow techniques to be applied only in very particular contexts. This may not be a standards issue unless the AI facility is sufficiently autonomous to be able to select its functionality based on context.

In Article 12 (Recording-Keeping), the mandate is to automate recording of events over the duration of the lifetime of the system. While technical specifications for the security framework of AI computing platform prepared by ETSI TC SAI can support the mechanism of recording keeping by protect the integrity of the logs collected to guarantee the procedure for transparency and provision of information to deployers described in Article 13 there are additional safeguards that may need to be applied. This is addressed in part in ETSI TS 104 224 [i.23] where clause 6.4.1 states: "*An AI/ML system can make decisions at a rate that, if a detailed evidential record was to be created, and retained securely, has potential to overload the system. Rather than take a detailed evidential record for every decision the goal of explicability and transparency is to ensure that the rationale for a decision is clear*". Thus [i.23] advises care in recording events in order to ensure the system functionality is balanced with accountability.

Article 15 (Accuracy, Robustness and Cybersecurity) may be met by the reports/specifications prepared by ETSI TC SAI. This includes the technical reports that introduce the mitigation strategy for AI security issues (see [i.28]) and the hardware role in AI security (see [i.11]), and technical specifications on the security for the underlying AI computing platform of AI systems and relevant cyber security requirements for systems.

4.4 Relationship to open source projects

As much of the AI Act [i.1] is about ensuring Union values and such there is a useful diversion in Recital 89 of the act that appears to distinguish liability and the role of open source. To quote "*Third parties making accessible to the public tools, services, processes, or AI components other than general-purpose AI models, shall not be mandated to comply with requirements targeting the responsibilities along the AI value chain, in particular towards the provider that has used or integrated them, when those tools, services, processes, or AI components are made accessible under a free and open licence*". Whilst SDOs do not often make tools, services or components they often do make the standards that underpin them accessible under free and open licences, and most SDOs have an open IPR policy that grants access under FRAND terms for any protected IPR contained in, and essential to the application of, the standard. Or in other words a body such as ETSI does not control how a standard is applied, nor does it make any conditions on open source, only that IPR is offered on FRAND terms (which may include an open source licence model).

It is also useful to note that many standards from multiple SDOs are executable in one form or another. Many of these code elements from ETSI are provided as an element of the standard and often are made public with an open source form of licence. It is also noted that most SDOs are attempting to move to models that allow more open access to standards both during development and once published, which may blur some of the points outlined in Recital 89.

EXAMPLE 1: ETSI's FORGE [i.8] resource contains libraries of data definitions (e.g. ASN.1 source files), and for linked data (e.g. for NSGSI-LD).

EXAMPLE 2: ETSI makes available semantic data in the form of ontologies (e.g. SAREF [i.9]).

Whilst not made clear in the quote from Recital 89 of [i.1], and further in Recitals 102, 103 and 104, the main issue of the use of open source is addressed in Article 2(12) which states "*This Regulation does not apply to AI systems released under free and open-source licences, unless they are placed on the market or put into service as high-risk AI systems or as an AI system that falls under Article 5 or 50*". The definition of AI System given in clause 3.1 of the present document, and the one given in Article 3 of [i.1] from which it is quoted, make reference to "*a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*". Many machine-based systems will, over time, include AI elements, some of which will have roots in open-source, thus the classification under Articles 5 or 50 should take precedence as stated in Article 12. However, the requirements and observations identified in ETSI TR 104 048 [i.25] relating to security of the supply chain are applicable irrespective of the nature of the supply chain components.

In the ETSI domain there is considerable support of open source. Thus the wording of the cited recitals and of Article 2(12) may have an impact, in particular, on ETSI's family of Open Source TBs (i.e. OCF, OSL, OSM, TFS) where AI models may form part of their output.

5 ETSI's AI standards

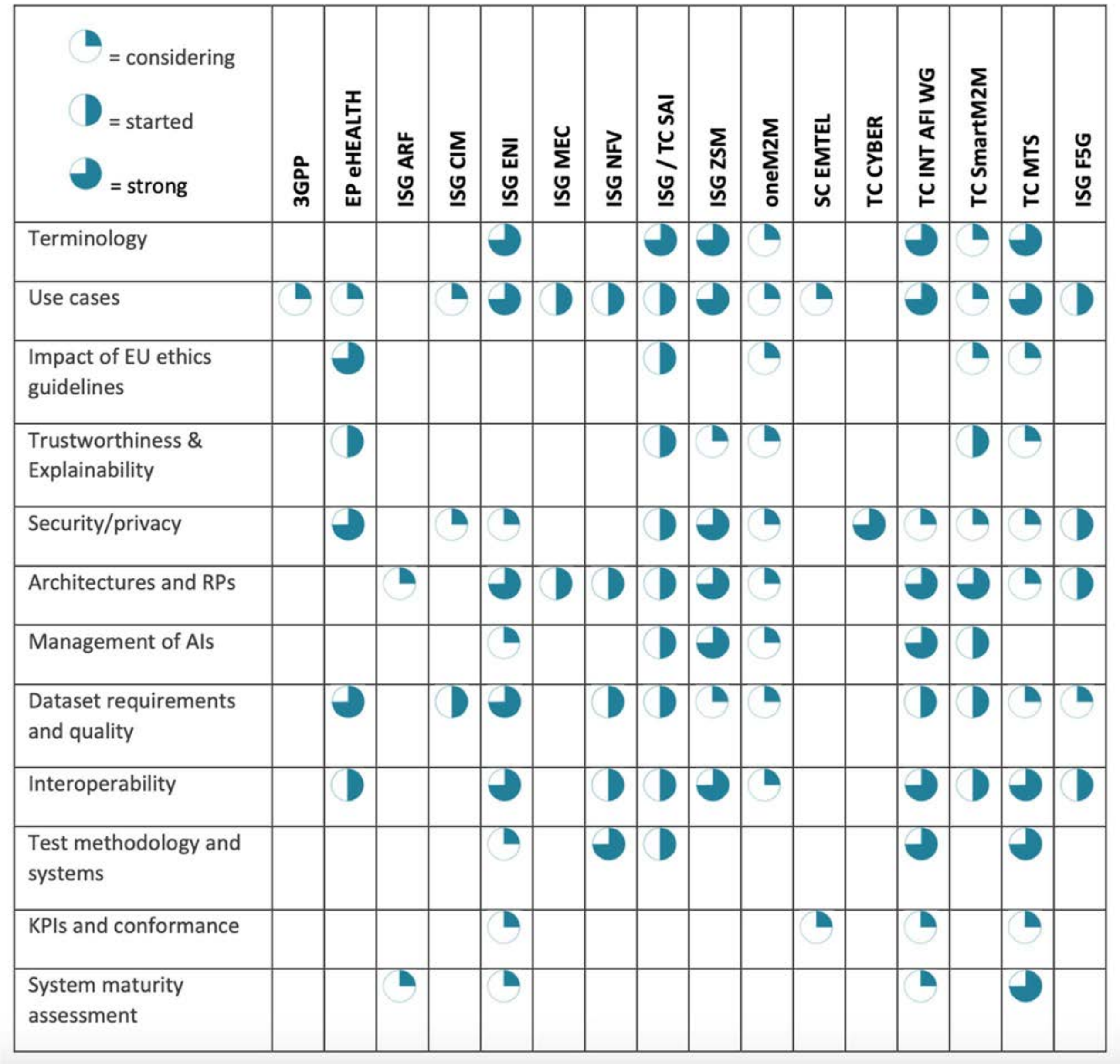
5.1 Overview of ETSI's AI standards

ETSI has a long history of involvement in AI, even if the term AI has not been explicit in work items and deliverables. The Experiential Networked Intelligence (ENI) group uses data from multiple sources to learn, the Zero-touch network and Service Management (ZSM) group similarly gathers data to make autonomous network provisioning and management decisions. In the F5G group the role of Digital Twins as AI driven entities is explored. In Intelligent Transport Systems (ITS) there is an implicit acceptance of AI/ML processing of data in vehicle and traffic management.

In more AI explicit groups there again is a lot of activity across ETSI. This includes TC SAI, OCG AI (a coordination body pulling together expertise from almost all of ETSI's technical bodies), TC MTS AI looking at the testing of AI (and the role of AI in testing). In the security domain in addition to TC SAI there is activity in TC CYBER to ensure that core processes and methods for risk analysis, for countermeasures and for evaluation, all take AI and ML into account either as an attack vector, or as an analysis accelerator.

The recent white paper from ETSI gives a good summary of ETSI's historic and planned AI activity [i.3].

Additionally ETSI's Technology Radar white paper from late 2023 [i.4] identifies 16 ETSI TBs active in AI across 12 dimensions as documented in Table 1 of the white paper copied below.



◔ = considering ◑ = started ◕ = strong	3GPP	EP eHEALTH	ISG ARF	ISG CIM	ISG ENI	ISG MEC	ISG NFV	ISG / TC SAI	ISG ZSM	oneM2M	SC EMTEL	TC CYBER	TC INT AFI WG	TC SmartM2M	TC MTS	ISG F5G
Terminology					◕			◕	◕	◔			◕	◔	◕	
Use cases	◔	◔		◔	◕	◑	◑	◑	◕	◔	◔		◕	◔	◕	◑
Impact of EU ethics guidelines		◕						◑		◔				◔	◔	
Trustworthiness & Explainability		◑						◑	◔	◔				◑	◔	
Security/privacy		◕		◔	◔			◑	◕	◔		◕	◔	◔	◔	◑
Architectures and RPs			◔		◕	◑	◑	◑	◕	◔			◕	◕	◔	◑
Management of AIs					◔			◑	◕	◔			◕	◑		
Dataset requirements and quality		◕		◑	◕		◑	◑	◔	◔			◑	◑	◔	◔
Interoperability		◑			◕		◑	◑	◕	◔			◕	◑	◕	◑
Test methodology and systems					◔		◕	◑					◕		◕	
KPIs and conformance					◔						◔		◔		◔	
System maturity assessment			◔		◔								◔		◕	

Figure 1: ETSI Activity in AI

The 12 dimensions listed in Figure 1 are all present in some form in the text of the AI Act [i.1] and it is therefore clear from this level of analysis that with the exception of "Trustworthiness and Explainability", and "KPIs and conformance" that even in mid-2023 that ETSI can claim to be strongly involved in 10 of the 12 dimensions. The situation is changed since the time of these white papers as ISG SAI published ETSI GR SAI 007 [i.14] on Explicability and Transparency which has been further updated in ETSI TS 104 224 [i.23] (see clause 5.3 below) into a full Technical Specification (TS), and ETSI's TC MTS is moving ahead in addressing testing (particularly conformance testing) in addition to the activity in TC SAI (see clause 5.3 below). Since preparing the picture given in Figure 1 it is obvious that ISG Electronic Signature and Trust Infrastructures (ESI) are extremely active in the domain "KPIs and conformance", and that TC SAI and TC MTS together address the "Trustworthiness and Explainability" dimension. It is therefore asserted that ETSI has technical activity across of 12 of the dimensions. Further, as suggested in clause 4.3 as AI becomes increasingly endemic so SDOs and the population as a whole will be engaged across all of the AI dimensions indicated in Figure 1.

In addition as AI becomes increasingly more pervasive it can be reasonably anticipated that TBs across ETSI will, at least, ask questions regarding the role of AI the context of their TBs. As ETSI standards/deliverables are driven by contributions of the members who are inevitably going to question if there is a role for AI in their domain, hence the list of ETSI TBs active in AI is more likely to grow than shrink.

5.2 Relationship to other SDO activity

ETSI is not the only body in standards for AI. In addressing this role ETSI TC SAI maintains a "roadmap" of activity that identifies key concerns and maps from those concerns to standards activity. In addition the work item for ETSI TR 104 029 [i.2] identifies in some detail the global ecosystem.

NOTE 1: The text of ETSI TR 104 029 [i.2] is made public as a rolling update after every meeting of TC SAI and linked from the front matter of SAI's entry on the ETSI Portal (see marked up screenshot in Figure 2 below).

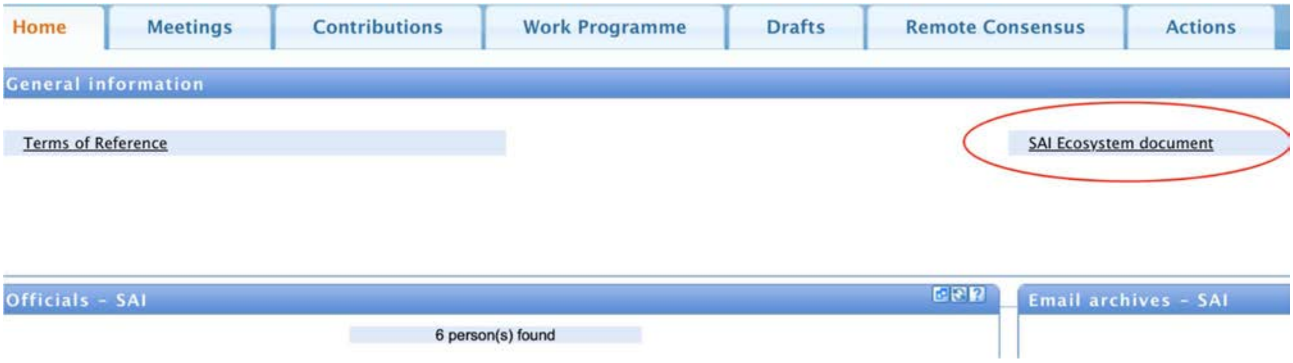


Figure 2: Persistent availability of SAI Ecosystem document from ETSI Portal (SAI)

NOTE 2: As stated in clause 4.2 the definition of standards body, and international standards body, addressed by ETSI, and seen in the context of ETSI TR 104 029 [i.2], is much wider than the definition of each that is used in the AI Act [i.1].

5.3 Catalogue of ETSI TC SAI work items

With the exception of the present document ETSI TC SAI has not raised work items specifically against the text of the AI Act [i.1], and in particular has not raised or developed any work items specifically to address the text of the Standardisation Request (SR) that was addressed to CEN/CENELEC and being directly addressed by JTC21 (where security aspects are addressed in WG5). However ETSI is clearly active in topics that intersect with the AI Act [i.1] and with the associated SR, and has a mode-4 agreement in place that allows experts from ETSI to be nominated to attend related meetings of JTC21 and vice-versa. The cooperation between ETSI and JTC21, and the public availability of ETSI's deliverables, particularly any TSs, should not inhibit their citation from deliverables of JTC21. In this regard the activity of ETSI is maintained to be consistent with the aims of the AI Act [i.1], the SR, and the work programme of JTC21.

Once published, as with all ETSI deliverables, the PDF format document is made available for download without charge (the hyperlinks for the published version are to the PDF file). The editable word file of the published deliverable is also available to all ETSI members.

The full catalogue of ETSI TC SAI work items is given in Annex B of the present document, and mapped to the AI Act [i.1] in detail in clause 6.2.

5.4 Framing the content of standards

As noted in clause 4.3 above, Article 5 of the AI Act [i.1] (prohibited AI practices) is framed as what cannot be done, whereas for standardization it has to be framed somewhat differently. This means what measures can be provided that, when followed, prevent the placement on the market of AI solutions that enable the prohibited practices.

The concern here is that some of the prohibited practices build on allowed practices. The primary answer offered to date is to adopt principles of transparency and explicability (the term explainability is used by some other SDOs) as required by Article 13. In determining the application and risk associated to the application of AI the general guidance of risk awareness has been addressed in ETSI across a number of TBs. It is noted that Article 9 requires that "*a risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems*" which requires that a preliminary assessment has been made to properly identify the system as a high-risk AI system. Whilst the general definition of a high-risk AI system given in Article 6 is quite broad the approach in ETSI is to perform a quantitative risk analysis, using the ETSI TS 102 165-1 [i.37] method that, for any attack surface identifies the overall risk. In addition ETSI publishes a set of Cyber Security Controls and have applied those to AI in ETSI TR 104 030 [i.26]. Here where AI is involved there is a broad understanding that few systems will be AI for AI's sake, rather that AI is used in support of another process such as facial recognition. The primary purpose is then facial recognition and not AI. The text in the AI act [i.1] in Article 5 therefore is not interpreted to prevent the development of AI for biometric recognition but rather to restrict its use in certain circumstances. The standards developed in ETSI to give assurance of the security of AI thus ensure that the data, its processing, and its interpretation, are clear. In doing so it is intended that any deployment of the system can clearly demonstrate if the deployment is allowed under the restrictions set by Article 5.

The rules and requirements for identifying the purpose of AI in a system are defined in ETSI TS 104 224 [i.23]. In particular the intent (as per Article 13 of the AI Act [i.1]) is to ensure that the statement of purpose of a system allows a layperson to clearly understand the purpose of the system and to explicitly identify the role of AI in achieving that purpose. The particular way in which this is framed in ETSI TS 104 224 [i.23] is copied below (see Table 1).

Table 1: System documentation elements in static explicability analysis identified in ETSI TS 104 224 [i.23]

Documentation Element	Element	Mandatory	Short description
1	Statement of system purpose	Yes	This element of the system documentation is intended to allow a layperson to clearly understand the purpose of the system and to explicitly identify the role of AI in achieving that purpose.
2a	Identification of data source(s)	Yes	Where the data comes from and how the authenticity of the data source is verified.
2b	Purpose of data source(s) (in support of system purpose)	Yes	The role of the particular data source in the system (e.g. training data containing images of dogs to train the system in recognizing a dog from an image).
2c	Method(s) used to determine data quality	Strongly recommended	Methods and processes used in determining if the input data is a fair and accurate representation of the desired input. This should address how bias or preference is identified and corrected in the data input.
3	Identity of liable party	Yes	For each processing or data element a means to identify liability for correction of errors or for maintenance of the element.

In addition the ETSI Writing world class standards guidance [i.33] makes clear the purpose of the "Scope" statement of the content as follows: "*The aim of the Scope clause is to provide readers with a succinct, factual statement of the purpose of the document. This may include the subject of the standard, the area of applicability, the type of product or service and other relevant information such as the relationship of the standard to other standards - as long as such details clarify the Scope of your document.*" When properly addressed this supports the "statement of system purpose" element seen in Table 1 (the latter refers to the product, the former to the standard that may be used in developing the product).

6 Article by article mapping of AI Act to ETSI Standardization programme

6.1 Mapping AI act to ETSI

Table 2: Article by article mapping to ETSI standards work

Article	Heading	Summary of Primary text	ETSI mapping
Chapter I, General provisions			
1	Subject matter	The purpose of this Regulation is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy Artificial Intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation.	This is addressed by ETSI's Directives and by the establishment of ETSI as an ESO under Regulation 1025/2012 [i.38] and subsequent revisions.
2	Scope	Identifies who is addressed by the regulation.	Not of direct relevance to ETSI as ETSI produces standards in order to allow those addressed by the scope to meet their obligations set by the regulation.
3	Definitions	Defines terms used in the document.	Mapped across ETSI's deliverables into a format that meets ETSI's drafting rules. Definitions in ETSI deliverables are not normative. All of the published terms used in ETSI's documents are listed on ETSI's TEDDI tool (https://webapp.etsi.org/Teddi/).
4	AI literacy	Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.	This is addressed in part in Annex A of the present document. The text in clause 4.3 of the present document also applies wherein it is identified that many of the general purpose reports prepared by ETSI can be seen as making provision for building that literacy.
Chapter II: Prohibited AI practices			
5	Prohibited AI practices	Lists practices that are prohibited.	As noted in clause 4.3 the mandate is framed as what cannot be done, whereas for standardization it has to be framed somewhat differently. This means what measures can be provided that, when followed, prevent the prohibited practices being placed in the market. Some of the mandates allow techniques to be applied only in very particular contexts. This may not be a standards issue unless the AI facility is sufficiently autonomous to be able to select its functionality based on context.

Article	Heading	Summary of Primary text	ETSI mapping
Chapter III: High Risk AI Systems			
SECTION 1: Classification of AI systems as high-risk			
6	Classification rules for high-risk AI systems	Rules for classifying and therefore determining if a system is high-risk.	As noted in clause 5.4 of the present document the scope statement of a standard, and the statement of purpose of a product (as defined in ETSI TS 104 224 [i.23]), will allow some indication of the likelihood of the resultant system being defined as high-risk.
7	Amendments to Annex III		As above.
SECTION 2: Requirements for high-risk AI systems			
8	Compliance with the requirements	States that all other parts of the section are mandatory and proof of compliance is required.	Not required.
9	Risk management system	A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems. The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating.	ETSI produces a number of documents aimed at containing risk. The application of the Cyber Security Controls series of ETSI TR 103 305 [i.36] (a multipart standard) to systems addresses all the lifecycle aspects requested and has applied those to AI in ETSI TR 104 030 [i.26]. At the more detailed technical assessment of risk the ETSI TS 102 165-1 [i.37] approach applies. The specific assessment of risk as applied to market placement of a product identified in ETSI TR 103 935 [i.34] may also apply.
10	Data and data governance	High-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5 whenever such data sets are used.	In part this is addressed by the transparency and explicability obligations in ETSI TS 104 224 [i.23], and in the actions identified in the supply chain report (ETSI TR 104 048 [i.25]) and also by the traceability actions given in ETSI TR 104 032 [i.24].
11	Technical documentation	The elements required are defined in Annex IV and has to include a DoC as defined by Article 47.	This requires best practice of auditing of design and of the supply chain. Several standards exist that address this and are classified in ETSI TR 104 029 [i.2].
12	Record-keeping	Allow for the automatic recording of events over the lifetime of the system.	As stated in clause 4.3 of the present document the mandate is to automate recording of events over the duration of the lifetime of the system. While technical specifications for the security framework of AI computing platform prepared by ETSI TC SAI can support the mechanism of recording keeping by protect the integrity of the logs collected to guarantee the procedure for transparency and provision of information to deployers described in Article 13.
13	Transparency and provision of information to deployers	High-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately.	The requirements stated in ETSI TS 104 224 [i.23] apply to both static and runtime transparency and explicability.

Article	Heading	Summary of Primary text	ETSI mapping
14	Human oversight	High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use.	It is noted that Article 14 may inhibit the placement on the market of some autonomous systems and particularly of Agentic-AI systems. The discipline of Functional Safety (FS) applied to such systems may allow their deployment without direct involvement of "human in the loop" but rather allow for reasonable oversight by natural persons. The adoption of FS approaches in AI is an item of open study in ETSI.
15	Accuracy, robustness and cybersecurity	High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle.	The topic of metrics for accuracy, robustness and cybersecurity is a topic gaining interest in ETSI and other SDOs. An initial requirement for this is provided as part of the transparency and explicability document, ETSI TS 104 224 [i.23].
SECTION 3: Obligations of providers and deployers of high-risk AI systems and other parties			
16	Obligations of providers of high-risk AI systems	As per the title.	Addressed across all of ETSI's AI output.
17	Quality management system	Providers of high-risk AI systems shall put a quality management system in place that shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions.	This is consistent with the guidance given for application of the Critical Security Controls of ETSI TR 103 305 [i.36] and ETSI TR 104 030 [i.26].
18	Documentation keeping	Requires records to be maintained for 10 years after placement on the market.	Not covered specifically in ETSI's AI portfolio but the general controls of ETSI TR 103 305 [i.36] apply.
19	Automatically generated logs	In each case the article title is deemed self-describing.	See clause 5.4 of the present document.
20	Corrective actions and duty of information		New work items establishing the AI Common Incident Expression (AICIE) alongside the development of the Universal Cybersecurity Information Exchange Framework (UCYBEX) apply.
21	Cooperation with competent authorities		Not applicable.
22	Authorised representatives of providers of high-risk AI systems		In ETSI TS 104 224 [i.23] (see also clause 5.4 of the present document) it is mandated that the liable party is identifiable across the supply chain.
23	Obligations of importers		Not an obvious domain for technical standards.
24	Obligations of distributors		
25	Responsibilities along the AI value chain		This is covered to an extent by each of ETSI TR 104 032 [i.24] and ETSI TR 104 048 [i.25]. It is also addressed in part in the transparency and explicability document ETSI TS 104 224 [i.23] in ensuring understanding of the value chain.
26	Obligations of deployers of high-risk AI systems		Not directly applicable.
27	Fundamental rights impact assessment for high-risk AI systems		The risk analysis methods developed in ETSI (e.g. ETSI TS 102 165-1 [i.37]) address harm in abstract terms and encourage assessment of rights of the stakeholders.

Article	Heading	Summary of Primary text	ETSI mapping
SECTION 4: Notifying authorities and notified bodies			
28 to 39	Various	Identifies specific actions of notifying authorities and notified bodies.	Not particularly of concern to SDOs but of particular interest to the process of making products and services available to the market. The SDO activity in this is addressed in Section 5 of the Act.
SECTION 5: Standards, conformity assessment, certificates, registration			
40	Harmonised standards and standardisation deliverables	Reinforces the role of hENs giving presumption of conformity.	As stated in clause 4.2 above "*an SDO cannot simply choose to publish an hEN, rather an hEN has to be written against specific actions of the EU*" , therefore ETSI at the time of preparation of the present document is not active in preparing hENs but will give assistance to relevant ESOs as stated in clause 5.2 above.
41	Common specifications	The Commission may adopt, implementing acts establishing common specifications for the requirements set out in Section 2 of this Chapter (Requirements for high-risk AI systems).	No current action (no implementing acts).
42	Presumption of conformity with certain requirements	Describes the normal process associated to presumption of conformity.	No specific actions or mapping at this time.
43	Conformity assessment		
44	Certificates		
45	Information obligations of notified bodies		
46	Derogation from conformity assessment procedure		
47	EU declaration of conformity		
48	CE marking		
49	Registration		
CHAPTER IV **TRANSPARENCY OBLIGATIONS FOR PROVIDERS AND DEPLOYERS OF CERTAIN AI SYSTEMS**			
50	Transparency obligations for providers and deployers of certain AI systems	Providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use.	This is addressed by ETSI TS 104 224 [i.23] (see also clause 5.4 of the present document) for both static and run time conditions of the AI system.

Article	Heading	Summary of Primary text	ETSI mapping
CHAPTER V **GENERAL-PURPOSE AI MODELS**			
51	Classification of general-purpose AI models as general-purpose AI models with systemic risk	Various (applies much of prior chapters to models that are not specifically identified as high risk).	As for mappings in prior chapters.
52	Procedure		
53	Obligations for providers of general-purpose AI models		
54	Authorised representatives of providers of general-purpose AI models		
55	Obligations of providers of general-purpose AI models with systemic risk		
56	Codes of practice	The AI Office shall encourage and facilitate the drawing up of codes of practice at Union level in order to contribute to the proper application of this Regulation, taking into account international approaches.	ETSI has recently completed ETSI TS 104 223 [i.35] that has been developed from the UK Code of Practice after a public consultation involving many EU and global stakeholders.
CHAPTER VI **MEASURES IN SUPPORT OF INNOVATION**			
57 through 63	Various	The measures support a regulatory sandbox to allow stakeholders to develop and innovate in a controlled environment where regulators can facilitate testing whilst optimising regulatory oversight.	Not directly applicable but may be used in collaboration with the "proofs of concept" sandbox outlined in ETSI TR 104 067 [i.19].
CHAPTER VII **GOVERNANCE**			
64 to 69	Various	Establishes the AI Office and associated bodies.	No direct standards action expected, however ETSI may wish to ensure that communication from the AI Office and associated bodies is communicated to ETSI members.
CHAPTER VIII **EU DATABASE FOR HIGH-RISK AI SYSTEMS**			
71	EU database for high-risk AI systems listed in Annex III	The Commission shall, in collaboration with the Member States, set up and maintain an EU database containing information relating to the registration of high-risk AI systems.	No specific ETSI activity is foreseen.
CHAPTER IX **POST-MARKET MONITORING, INFORMATION SHARING AND MARKET SURVEILLANCE**			
72	Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems		This is being addressed by the creation of new work items in both TC SAI and in TC CYBER to report and share vulnerability information, misbehaviour, and other risk factors. This work will specify the AI Common Incident Expression (AICIE) and work alongside the development of the Universal Cybersecurity Information Exchange Framework (UCYBEX).
73	Reporting of serious incidents		
74 to 94	Various	Addresses the organisation of market surveillance and how it interacts with other stakeholders.	

Article	Heading	Summary of Primary text	ETSI mapping
CHAPTER X **CODES OF CONDUCT AND GUIDELINES**			
95	Codes of conduct for voluntary application of specific requirements	The AI Office and the Member States shall encourage and facilitate the drawing up of codes of conduct, including related governance mechanisms, intended to foster the voluntary application to AI systems.	ETSI has recently completed ETSI TS 104 223 [i.35] that has been developed from the UK Code of Practice after a public consultation involving many EU and global stakeholders that may be instrumental in achieving the objectives of this article.
96	Guidelines from the Commission on the implementation of this Regulation	The Commission shall develop guidelines on the practical implementation of this Regulation [i.1].	As above.
CHAPTER XI **DELEGATION OF POWER AND COMMITTEE PROCEDURE**			
97	Exercise of the delegation	Addressed to EU.	Not applicable to ETSI.
98	Committee procedure		
CHAPTER XII **PENALTIES**			
99-101	Various	Identifies the penalties if a provider fails to comply to the requirements set out by the legislation.	Not strictly relevant to SDOs. Whilst SDO members may be subject to the identified penalties the role of the SDO here is to offer technical means that limit the risk of being subject to penalties.
CHAPTER XIII **FINAL PROVISIONS**			
102 - 110	Amendments to existing regulations	Identifies where existing regulation is directly impacted by the AI Act [i.1].	This will be further evaluated by TC SAI and OCG AI and actions given to relevant ETSI TBs where required.
111	AI systems already placed on the market or put into service and general-purpose AI models already placed on the marked	Large-scale IT systems that have been placed on the market or put into service before 2 August 2027 shall be brought into compliance with this Regulation by 31 December 2030.	No specific action from ETSI.
112	Evaluation and review	The Commission shall assess the need for amendment of the list set out in Annex III and of the list of prohibited AI practices laid down in Article 5, once a year following the entry into force of this Regulation.	No specific action from ETSI.
113	Entry into force and application	Applies from 2nd August 2026 with some exceptions: Articles 1 through 5 apply from 2nd February 2025 (i.e. in force now) Chapter III section 4 and others apply from 2nd August 2025. Article 6(1) applies from 2nd August 2027.	No specific action from ETSI. The harmonised standards required (see clause 5.2 of the present document) have to take account of these dates as hENs should be available to give presumption of conformity prior to the relevant in force dates.

6.2 Mapping ETSI TC SAI and ISG AI output to AI act

Table 2 can be presented in a different way that looks at some specific output of ETSI, in this instance from TC SAI, and mapping from the output back to specific articles of the AI Act [i.1]. Prior to this a summary of the security principles for AI, defined in ETSI TS 104 223 [i.35], is given. The intent of ETSI TS 104 223 [i.35] as indicated by its title is to define "Baseline Cyber Security Requirements for AI Models and Systems" and thus is intended to ensure, in addition to security of the AI model and system, that users of ETSI TS 104 223 [i.35] are able to prepare their products and services to be placed on the market and to conform to any applicable regulation including the AI Act [i.1].

Table 3: AI Security Principles and Provisions from ETSI TS 104 223 [i.35] mapped to AI Act [i.1] Articles

Principle	Article from AI Act
Secure Design	
Principle 1: Raise awareness of AI security threats and risks	Article 4 (primarily). The principle and its sub-principles while applying mainly to System Operators, Developers, and Data Custodians all aim to increase awareness and by default improve the AI literacy of those involved.
Principle 2: Design the AI system for security as well as functionality and performance	Article 15. The principle and its sub-principles are much more detailed in defining and mandating actions of System Operators and Developers than the act.
Principle 3: Evaluate the threats and manage the risks to the AI system	Article 9 (primarily).
Principle 4: Enable human responsibility for AI systems	Article 14.
Secure Development	
Principle 5: Identify, track and protect the assets	Articles 9 and 10.
Principle 6: Secure the infrastructure	Articles 9, 10 and 15.
Principle 7: Secure the supply chain	Articles 10 and 15.
Principle 8: Document data, models and prompts	Articles 9, 10, 14 and 15.
Principle 9: Conduct appropriate testing and evaluation	Articles 9, 10, 15.
Secure Deployment	
Principle 10: Communication and processes associated with End users and Affected Entities	Article 72, Article 14, Article 50, others.
Secure Maintenance	
Principle 11: Maintain regular security updates, patches and mitigations	Article 72.
Principle 12: Monitor the system's behaviour	Article 72 and all of Articles 9, 10, 14 and 15.
Secure End of Life	
Principle 13: Ensure proper data and model disposal	Articles 9, 10 and 15.

In Table 4 below an indicative mapping of ETSI TC SAI deliverables to the AI Act [i.1] is given. It should be noted that in some cases a specific mapping is not possible as a document may be used to address a very specific technical concern that is not addressed at the same level of granularity in the AI Act [i.1]. Thus in some instances whilst a mapping is shown it is not to be interpreted as conformance to the identified specification given complete assurance of conformance to the intent of the article in the AI Act [i.1].

Table 4: Indicative mapping from ETSI deliverables to AI Act [i.1] articles

ETSI deliverable	Title	Applicable parts of the AI Act
ETSI GR SAI 001 V1.1.1 (2022-01) [i.10]	Securing Artificial Intelligence (SAI); AI Threat Ontology	Superseded by ETSI TS 104 050 [i.20]
ETSI GR SAI 006 V1.1.1 (2022-03) [i.11]	Securing Artificial Intelligence (SAI); The role of hardware in security of AI	All. The AI Act [i.1] does not place specific requirements on the hardware platform which this GR does address.
ETSI GR SAI 009 V1.1.1 (2023-02) [i.12]	Securing Artificial Intelligence (SAI); Artificial Intelligence Computing Platform Security Framework	All. As above.
ETSI GR SAI 002 V1.1.1 (2021-08) [i.13]	Securing Artificial Intelligence (SAI); Data Supply Chain Security	Superseded by ETSI TR 104 048 [i.25].
ETSI GR SAI 007 V1.1.1 (2023-03) [i.14]	Securing Artificial Intelligence (SAI); Explicability and transparency of AI processing	Superseded by ETSI TS 104 224 [i.23].
ETSI GR SAI 013 V1.1.1 (2023-03) [i.15]	Securing Artificial Intelligence (SAI); Proofs of Concepts Framework	Superseded by ETSI TR 104 067 [i.19].
ETSI GR SAI 005 V1.1.1 (2021-03) [i.16]	Securing Artificial Intelligence (SAI); Mitigation Strategy Report	Superseded by ETSI TR 104 222 [i.28].
ETSI GR SAI 004 V1.1.1 (2020-12) [i.17]	Securing Artificial Intelligence (SAI); Problem Statement	Superseded by ETSI TR 104 221 [i.27].
ETSI GR SAI 011 V1.1.1 (2023-06) [i.18]	Securing Artificial Intelligence (SAI); Automated Manipulation of Multimedia Identity Representations	Superseded by ETSI TR 104 062 [i.29].

ETSI deliverable	Title	Applicable parts of the AI Act
ETSI TR 104 067 V1.1.1 (2024-04) [i.19]	Securing Artificial Intelligence (SAI); Proofs of Concepts Framework	Articles 57 through 63 (as in Table 2).
ETSI TS 104 050 V1.1.1 (2025-03) [i.20]	Securing Artificial Intelligence (SAI); AI Threat Ontology and definitions	Article 3 and throughout the Act. The purpose of the ontology is to express definitions in an active manner (so consistent with Article 3 and also with Articles 9, 10, 14 and 15).
ETSI TR 104 225 V1.1.1 (2024-04) [i.21]	Securing Artificial Intelligence TC (SAI); Privacy aspects of AI/ML systems	Articles 13 and 15.
ETSI TR 104 031 V1.1.1 (2024-01) [i.22]	Securing Artificial Intelligence (SAI); Collaborative Artificial Intelligence	All. This work item addresses a mode of applying AI where multiple AI agents are pervasively distributed in different places but interact with each other to work on the same or different AI tasks.
ETSI TS 104 224 V1.1.1 (2025-03) [i.23]	Securing Artificial Intelligence (SAI); Explicability and transparency of AI processing	Articles 13 and 14. Whilst primarily mapping to Article 13 this specification addresses many other aspects of how to design an AI system including 14 for allowing oversight and the data supply chain.
ETSI TR 104 032 V1.1.1 (2024-02) [i.24]	Securing Artificial Intelligence (SAI); Traceability of AI Models	This extends and builds on core concepts from ETSI TS 104 224 [i.23] and applies to similar parts of the AI Act [i.1].
ETSI TR 104 048 V1.1.1 (2025-01) [i.25]	Securing Artificial Intelligence (SAI); Data Supply Chain Security	Article 10.
ETSI TR 104 030 V1.1.1 (2025-03) [i.26]	Securing Artificial Intelligence (SAI); Critical Security Controls for Effective Cyber Defence; Artificial Intelligence Sector	All. ETSI TR 104 030 [i.26] extends from the ETSI TR 103 305 [i.36] series (TC CYBER). The security controls apply to all aspects of effective development, deployment and governance of systems including those with AI/ML components.
ETSI TR 104 221 V1.1.1 (2025-01) [i.27]	Securing Artificial Intelligence (SAI); Problem Statement	All. The purpose of the problem statement is to identify the problems in AI/ML that give rise to cybersecurity and societal risk. This is therefore consistent with the recitals of the AI Act [i.1] and with the resulting provisions given by the articles of the AI Act [i.1].
ETSI TR 104 222 V1.2.1 (2024-07) [i.28]	Securing Artificial Intelligence; Mitigation Strategy Report	All. As for the problem statement the purpose of this report is to identify and advise on mitigation strategies that apply across the AI/ML domain.
ETSI TR 104 062 V1.2.1 (2024-07) [i.29]	Securing Artificial Intelligence; Automated Manipulation of Multimedia Identity Representations	All. This builds on both the problem statement and the mitigation strategy report to concentrate on one particular form of attack and its mitigation.
ETSI TR 104 066 V1.1.1 (2024-07) [i.30]	Securing Artificial Intelligence; Security Testing of AI	All. In engineering the role of testing is central to success and this report identifies both the challenges of AI testing means to overcome those challenges.
ETSI TS 104 223 V1.1.1 (2025-04) [i.35]	Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems	See Table 3 above.

Annex A: Summary of ETSI's involvement in the DIGITALEUROPE - ESOs collaboration on education material for standards

Whilst the overall programme is addressed in the DIGITALEUROPE (DE) programme the following key points where ETSI's members will be involved as contributors are highlighted.

Phase 3 of the project addresses content development to be led by DE with support from the ESOs. This will identify the overall content and in particular Identify key components of the AI Act [i.1] and harmonised standards to be addressed, which is in part the rationale of the present document. This is to be followed by a phase 4 of technical development to be led by the ESOs (ETSI is named first in the list).

The 4th phase will develop tools for risk assessment, logging, traceability, and compliance validation. This is in part addressed by a number of the deliverables of TC SAI and supported by deliverables from other bodies in ETSI, in particular TC CYBER.

ETSI has developed an education and reachout group whose role began in 2018 and seen in the public facing webpages at https://www.etsi.org/education. Further information on the ETSI Education about Standardization activities can be requested by contacting the ETSI team at education@etsi.org.

Annex B:
Catalogue of ETSI TC SAI and ISG SAI deliverables

ETSI deliverable	Title	Scope
ETSI GR SAI 001 V1.1.1 (2022-01) [i.10]	Securing Artificial Intelligence (SAI); AI Threat Ontology	The purpose of this work item is to define what would be considered an AI threat and how it might differ from threats to traditional systems. The starting point that offers the rationale for this work is that currently, there is no common understanding of what constitutes an attack on AI and how it might be created, hosted and propagated. The AI Threat Ontology deliverable will seek to align terminology across the different stakeholders and multiple industries. This document will define what is meant by these terms in the context of cyber and physical security and with an accompanying narrative that should be readily accessible by both experts and less informed audiences across the multiple industries. Note that this threat ontology will address AI as system, an adversarial attacker, and as a system defender.
ETSI GR SAI 006 V1.1.1 (2022-03) [i.11]	Securing Artificial Intelligence (SAI); The role of hardware in security of AI	To prepare a report that identifies the role of hardware, both specialized and general-purpose, in the security of AI. This will address the mitigations available in hardware to prevent attacks (as identified in ETSI GR SAI 005 [i.16]) and also address the general requirements on hardware to support SAI (expanding from ETSI GR SAI 004 [i.17], ETSI GR SAI 002 [i.13], and ETSI TR 104 066 [i.30]). In addition this report will address possible strategies to use AI for protection of hardware. The report will also provide a summary of academic and industrial experience in hardware security for AI. In addition, the report will address vulnerabilities or weaknesses introduced by hardware that may amplify attack vectors on AI.
ETSI GR SAI 009 V1.1.1 (2023-02) [i.12]	Securing Artificial Intelligence (SAI); Artificial Intelligence Computing Platform Security Framework	This work item aims to specify a security framework of AI computing platform containing hardware and basic software to protect valuable assets like models and data deployed on AI computing platform when they are used in runtime or stored at rest. The security framework consists of security components in AI computing platform and security mechanisms executed by security components in the platform. By specifying the security framework, AI computing platform can be consolidated against the relevant attack and able to provide security capabilities to facilitate the stakeholders in AI systems to better protect the valuable assets(model/data) on AI computing platform. The study will use ETSI GR SAI 006 [i.11] as a start point for hardware aspects and avoid overlap with ETSI GR SAI 006 [i.11].

ETSI deliverable	Title	Scope
ETSI GR SAI 002 V1.1.1 (2021-08) [i.13]	Securing Artificial Intelligence (SAI); Data Supply Chain Security	Data is a critical component in the development of AI systems. This includes raw data as well as information and feedback from other systems and humans in the loop, all of which can be used to change the function of the system by training and retraining the AI. However, access to suitable data is often limited causing a need to resort to less suitable sources of data. Compromising the integrity of training data has been demonstrated to be a viable attack vector against an AI system. This means that securing the supply chain of the data is an important step in securing the AI. This report will summarize the methods currently used to source data for training AI along with the regulations, standards and protocols that can control the handling and sharing of that data. It will then provide gap analysis on this information to scope possible requirements for standards for ensuring traceability and integrity in the data, associated attributes, information and feedback, as well as the confidentiality of these.
ETSI GR SAI 007 V1.1.1 (2023-03) [i.14]	Securing Artificial Intelligence (SAI); Explicability and transparency of AI processing	The intent of this work item is to extend from the published work of SAI to address the issues of design of AI platforms (data, algorithms, frameworks) that are able to give assurance of explainability and transparency of decisions. This is intended in part to also consider the impact of issues arising from regulation of AI to address ethics and misuse and to allow independent determination of bias (a light touch). The report will address both intrinsic and post-hoc analysis of AI systems.
ETSI GR SAI 013 V1.1.1 (2023-03) [i.15]	Securing Artificial Intelligence (SAI); Proofs of Concepts Framework	The document provides information about the 'lightweight' framework to be used by ETSI ISG SAI to create multi-partner Proofs of Concepts (PoCs).
ETSI GR SAI 005 V1.1.1 (2021-03) [i.16]	Securing Artificial Intelligence (SAI); Mitigation Strategy Report	This work item aims to summarize and analyse existing and potential mitigation against threats for AI-based systems. The goal is to have guidelines for mitigating against threats introduced by adopting AI into systems. These guidelines will shed light baselines of securing AI-based systems by mitigating against known or potential security threats. They also address security capabilities, challenges, and limitations when adopting mitigation for AI-based systems in certain potential use cases.
ETSI GR SAI 004 V1.1.1 (2020-12) [i.17]	Securing Artificial Intelligence (SAI); Problem Statement	This work item describes the challenges of securing AI-based systems and solutions, including challenges relating to data, algorithms and models in both training and implementation environments. The focus will be on challenges which are specific to AI-based systems, including poisoning and evasion.
ETSI GR SAI 011 V1.1.1 (2023-06) [i.18]	Securing Artificial Intelligence (SAI); Automated Manipulation of Multimedia Identity Representations	This work item covers AI-based techniques for automatically manipulating identity data represented in different media formats, such as audio, video and text (deepfakes). The work item describes the different technical approaches and analyses the threats posed by deepfakes in different attack scenarios. It then provides technical and organizational measures to mitigate these threats and discusses their effectiveness and limitations.
ETSI TR 104 067 V1.1.1 (2024-04) [i.19]	Securing Artificial Intelligence (SAI); Proofs of Concepts Framework	The document provides information about the 'lightweight' framework to be used by ETSI TC SAI to create multi-partner Proofs of Concepts (PoCs).

ETSI deliverable	Title	Scope
ETSI TS 104 050 V1.1.1 (2025-03) [i.20]	Securing Artificial Intelligence (SAI); AI Threat Ontology and definitions	The purpose of this work item is to define what would be considered an AI threat and how it might differ from threats to traditional systems. The WI defines a common terminology for AI (aligned to CEN/ISO). The starting point that offers the rationale for this work is that currently, there is no common understanding of what constitutes an attack on AI and how it might be created, hosted and propagated. The AI Threat Ontology deliverable will seek to align terminology across the different stakeholders and multiple industries. This document will define what is meant by these terms in the context of cyber and physical security and with an accompanying narrative that should be readily accessible by both experts and less informed audiences across multiple industries. Note that this threat ontology will address AI as a system, an adversarial attacker, and a system defender.
ETSI TR 104 225 V1.1.1 (2024-04) [i.21]	Securing Artificial Intelligence TC (SAI); Privacy aspects of AI/ML systems	The purpose of this work item is to identify the role of privacy as one of the components of the Security of AI and proceed with the attempt to define Privacy in the context of AI that covers both, safeguarding models and protecting data, as well as the role of privacy-sensitive data in AI solutions. It investigates and addresses the attacks and their associated remediations where applicable, considering the existence of multiple levels of trust affecting the lifecycle of data. Appropriate means to label/protect/anonymize privacy-sensitive data elements during data collection and processing are studied aiming to protect privacy-sensitive data, while limiting AI performance impact. The investigated attack mitigations include Non-AI-Specific (traditional Security/Privacy redresses), AI/ML-specific remedies, pre-emptive remediations ("left of the boom"), and reactive responses to an adversarial activity ("right of the boom"). In addition, the anticipated delivery document will seek to align terminology with existing ETSI SAI ISG documents and studies, and will reference previously-studied privacy attacks and remediations (see ETSI GR SAI 004 [i.17], ETSI GR SAI 002 [i.13]). The anticipated delivery document will also provide a summary of academic and industrial experience in privacy protection for AI.
ETSI TR 104 031 V1.1.1 (2024-01) [i.22]	Securing Artificial Intelligence (SAI); Collaborative Artificial Intelligence	This work item covers security aspects of pervasive and collaborative Artificial Intelligence (AI) (e.g. federated learning, transfer learning, distributed reinforcement learning, decentralized machine learning), where multiple AI agents are pervasively distributed in different places but interact with each other to work on the same or different AI tasks. These AI agents exchange AI models and/or inferred knowledge. The work item investigates use cases of security for pervasive and collaborative AI, and analyses potential security concerns such as trust and communications among those AI agents. Then the work item provides technical recommendations on approaches to mitigate these issues including their limitations.

ETSI deliverable	Title	Scope
ETSI TS 104 224 V1.1.1 (2025-03) [i.23]	Securing Artificial Intelligence (SAI); Explicability and transparency of AI processing	The intent of this work item is to extend from the published work of SAI to address the issues of design of AI platforms (data, algorithms, frameworks) that are able to give support to claims of explainability and transparency of decisions. This is intended in part to also consider the impact of issues arising from regulation of AI to address ethics and misuse and to allow independent determination of bias (a light touch). The report will address both intrinsic and post-hoc analysis of AI systems.
ETSI TR 104 032 V1.1.1 (2024-02) [i.24]	Securing Artificial Intelligence (SAI); Traceability of AI Models	The NWI will study the role of traceability in the challenge of Securing AI and explore issues related to sharing and re-using models across tasks and industries. The scope includes threats, and their associated remediations where applicable, to ownership rights of AI creators as well as to verification of models origin, integrity or purpose. Mitigations can be non-AI-Specific (Digital Right Management applicable to AI) and AI-specific techniques (e.g. watermarking) from prevention and detection phases. They can be both model-agnostic or model enhancement techniques. Threats and mitigations specific to the collaborative learning setting, implying multiple data and model owners, could be also explored. The NWI will align terminology with existing ETSI ISG SAI documents and studies, and reference/complement previously studied attacks and remediations (ETSI GR SAI 004 [i.17], ETSI GR SAI 005 [i.16]). It will also gather industrial and academic feedback on traceability and ownership rights protection and model verification (including integrity of model metadata) in the context of AI.
ETSI TR 104 048 V1.1.1 (2025-01) [i.25]	Securing Artificial Intelligence (SAI); Data Supply Chain Security	Data is a critical component in the development of AI systems. This includes raw data as well as information and feedback from other systems and humans in the loop, all of which can be used to change the function of the system by training and retraining the AI. However, access to suitable data is often limited causing a need to resort to less suitable sources of data. Compromising the integrity of training data has been demonstrated to be a viable attack vector against an AI system. This means that securing the supply chain of the data is an important step in securing the AI. This report will summarize the methods currently used to source data for training AI along with the regulations, standards and protocols that can control the handling and sharing of that data. It will then provide gap analysis on this information to scope possible requirements for standards for ensuring traceability and integrity in the data, associated attributes, information and feedback, as well as the confidentiality of these.
ETSI TR 104 030 V1.1.1 (2025-03) [i.26]	Securing Artificial Intelligence (SAI); Critical Security Controls for Effective Cyber Defence; Artificial Intelligence Sector	Applies the latest version of the Critical Security Controls and facilitation mechanisms for effective risk control and enhanced resilience of AI sector products and services.
ETSI TR 104 221 V1.1.1 (2025-01) [i.27]	Securing Artificial Intelligence (SAI); Problem Statement	This work item describes the challenges of securing AI-based systems and solutions, including challenges relating to data, algorithms and models in both training and implementation environments. The focus will be on challenges which are specific to AI-based systems, including poisoning and evasion.

ETSI deliverable	Title	Scope
ETSI TR 104 222 V1.2.1 (2024-07) [i.28]	Securing Artificial Intelligence; Mitigation Strategy Report	This work item aims to summarize and analyse existing and potential mitigation against threats for AI-based systems. The goal is to have guidelines for mitigating against threats introduced by adopting AI into systems. These guidelines will shed light baselines of securing AI-based systems by mitigating against known or potential security threats. They also address security capabilities, challenges, and limitations when adopting mitigation for AI-based systems in certain potential use cases.
ETSI TR 104 062 V1.2.1 (2024-07) [i.29]	Securing Artificial Intelligence; Automated Manipulation of Multimedia Identity Representations	This work item covers AI-based techniques for automatically manipulating identity data represented in different media formats, such as audio, video and text (deepfakes). The work item describes the different technical approaches and analyses the threats posed by deepfakes in different attack scenarios. It then provides technical and organizational measures to mitigate these threats and discusses their effectiveness and limitations.
ETSI TR 104 066 V1.1.1 (2024-07) [i.30]	Securing Artificial Intelligence; Security Testing of AI	The purpose of this work item is to identify methods and techniques that are appropriate for security testing of AI-based components including to show that the requirements for explicability and transparency are met by the test objectives. Security testing of AI has some commonalities with security testing of traditional systems but provides new challenges and requires different approaches, due to (a) significant differences between subsymbolic AI and traditional systems that have strong implications on their security and on how to test their security properties, (b) non-determinism since AI-based systems may evolve over time (self-learning systems) and security properties may degrade, (c) test oracle problem, assigning a test verdict is different and more difficult for AI-based systems since not all expected results are known a priori, and (d) data-driven algorithms: in contrast to traditional systems, (training) data forms the behaviour of subsymbolic AI. The scope of this work item is to cover the following topics: • security testing approaches for AI; • security test oracles for AI; • definition of test adequacy criteria for security testing of AI.
ETSI TS 104 223 V1.1.1 (2025-04) [i.35]	Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems	The present document defines baseline security requirements for AI models and systems. This includes systems that incorporate deep neural networks, such as generative AI. For consistency, the term "AI systems" throughout the present document when framing the scope of provisions and "AI security" which is considered a subset of cyber security. The present document is not designed for academics who are creating and testing AI systems only for research purposes (AI systems which are not going to be deployed). The present document separates principles and requirements into five phases. These are secure design, secure development, secure deployment, secure maintenance and secure end of life. Relevant standards and publications are signposted at the start of each principle to highlight links between the various documents and the present document. This is not an exhaustive list.

Annex C: Bibliography

- Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

- 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).

History

Document history		
V1.1.1	May 2025	Publication