TC SAI Terms of Reference

Presented during Board#144 and approved by correspondence

Scope

The aim of Technical Committee Securing Artificial Intelligence (TC SAI) is to develop technical specifications that mitigate against threats arising from the deployment of AI, and threats to AI systems, from both other AIs, and from conventional sources. Whilst in the short to medium term the focus of TC SAI will be on the application of Machine Learning (ML) the group shall also give guidance and evaluation reports to ETSI and its stakeholders on the wider developments of AI.

NOTE: The term AI is used to include variants and siblings of AI including ML.

As AI becomes an increasing element of the ICT world it is essential that it is made secure, safe and societally responsible. The word "securing" in the name of TC SAI is thus intended to address all of those aspects. Artificial Intelligence has to be secure but it cannot only be secure - it has to be safe, it has to be societal, it has to be suitable. Thus the “S” in SAI is implicitly expanded to have all of these meanings. Whilst the boundaries of AI are uncertain, and what is secure is also uncertain, TC SAI will work to ensure that it addresses the end-role of AI by working on security of AI respecting the roles of safety, suitability and society in using AI. The underlying rationale for TC SAI is that autonomous mechanical and computing entities may make decisions that act against the relying parties either by design or as a result of malicious intent. The conventional cycle of risk analysis and countermeasure deployment represented by the Identify-Protect-Detect-Respond cycle needs to be re-assessed when an autonomous machine is involved.

TC SAI addresses 4 main aspects of AI security standardisation:

1. Securing AI from attack e.g. where AI is a component in the system that needs defending.
2. Mitigating against AI e.g. where AI is the ‘problem’ (or used to improve and enhance other more conventional attack vectors),
3. Using AI to enhance security measures against attack from other things e.g. AI is part of the ‘solution’ (or used to improve and enhance more conventional countermeasures),
4. Societal security and safety aspects of the use and application of AI.

Achieving a common understanding of the duality of attack and defence is key to the successful development of guidance and specifications from the TC. The purpose of TC SAI is to develop the technical knowledge in the form of ETSI deliverables that act as a baseline in ensuring that AI is secure, safe, societally relevant and suitable. The stakeholders impacted by the activity of the TC include all the member groups represented in ETSI and some of the wider societal environments that AIs will be deployed in. This includes end users, manufacturers, operators and governments The activity of TC SAI will include gathering concerns of each stakeholder group to ensure that ETSI and the output of TC SAI correctly address all of those concerns.

In addressing the societal aspects of the work TC SAI shall address protection of at risk populations (e.g. those who may be targeted by AI generated content) and to ensure that SMEs are included in the development, and consideration, of the work.

Areas of Activity

TC SAI will produce both informative documents (Technical Reports (including Special Reports and ETSI Guides)) and normative documents (Technical Specifications (including ENs and if requested hENs)). In addition TC SAI will inherit and maintain the work done under the auspices of ISG SAI. In addressing secure AI with the broad interpretation of security to include safety and societal aspects as above TC SAI will engage with EU and other regulatory bodies to ensure that the output supports relevant global, regional and national requirements.

The following deliverable forms will be produced by TC SAI:

- Report(s) describing the challenges related to securing AI enhanced infrastructures
- Specification(s) of the end-to-end security mitigations for AI systems
- Specification(s) of the functional architecture and solutions for the provision of a secure interconnection of AIs
- Specification(s) including interfaces/APIs/protocols and information / data models to secure the target infrastructures,
- Report(s) describing the challenges related to securing infrastructures against AI/ML amplified threats,
- Specification(s) of the key use cases and related security requirements in relation to AI/ML threats,
- Specification(s) on test methodologies used to validate that threats can be mitigated in the target use cases.
- Report(s) describing the opportunities offered by AI/ML security technologies
- Specification(s) including interfaces/APIs/protocols and information / data models to produce robust, effective AI/ML security products
- Report(s) providing a descriptive Proof of Concept (PoC) framework with minimum requirements, templates, process description,
- Report(s) providing gap analysis of the work done in existing standards and open source groups in relation to the agreed AI use cases,
- Specification(s) of the business use cases and related requirements including those developed by other ETSI Technical Bodies.

The detailed TC SAI work plan may be modified as the work and project priorities evolve and will be maintained and made available on the ETSI portal.

Throughout its activity TC SAI will engage with and provide recommendations across ETSI and partner SDOs when impacts on their specifications are foreseen.

Collaboration with other bodies

Close collaboration and coordination with other standard groups is required to ensure that all the organizations together provide complementary solutions. It will also be necessary to identify and agree the roles of the corresponding standardization bodies in filling any identified gaps in standardisation.

TC SAI will set-up the appropriate communication channels to the following groups both within and outside of ETSI.

ETSI groups

TC SAI shall establish relationships with the following ETSI groups:

- ETSI OCG AI
- ETSI PP 3GPP
- ETSI PP oneM2M
- ETSI TC SmartM2M
- ETSI TC SmartBAN
- ETSI TC CYBER (and associated groups including ISG ETI, WG QSC, SAGE)
- ETSI ISG CIM
- ETSI ISG ENI
- ETSI ISG NFV

- ETSI ISG ZSM
- ETSI TC eHEALTH

and others as identified during the progression of the work.

External groups

The TC SAI also intends to cooperate with a number of external organizations including:

- ENISA
- JRC
- CEN / CENELEC
- IETF
- ITU-T
- ISO/IEC JTC1
- NIST

and others as identified during the progression of the work.