ETSI TR 104 067 V1.1.1 (2024-04)

Securing Artificial Intelligence (SAI);
Proofs of Concepts Framework

Reference
DTR/SAI-0017

Keywords
artificial intelligence, cyber security,
proof of concept, testing

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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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.

1 Scope

The present document provides information about the "lightweight" framework to be used by ETSI TC SAI to create multi-partner Proofs of Concepts (PoCs).

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 are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR SAI 004 (V1.1.1): "Securing Artificial Intelligence (SAI); Problem Statement".

NOTE: ETSI GR SAI 004 is in the process of conversion to ETSI TC SAI deliverable as ETSI TR 104 221 and the latest published document applies.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

PoC project: activity oriented to perform a PoC

NOTE: According to the framework described in the present document.

PoC proposal: initial description of a PoC Project, submitted as a contribution for review and acceptance

NOTE: See clause 4.2.

PoC report: detailed description of the results and findings of a PoC Project, submitted once the PoC Project has finished

PoC review team: entity in charge of administering the PoC activity process

NOTE: For now TC SAI acts as the PoC review team.

PoC team: organizations actively contributing to a PoC Project

NOTE: See clause 4.3.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR SAI 004 [i.1] and the following apply:

AI	Artificial Intelligence
PoC	Proof of Concept
SAI	Securing Artificial Intelligence
TC	Technical Committee
TR	Technical Report
WI	Work Item

4 ETSI SAI PoC framework

4.1 Rationale

AI-based solutions are being implemented in various systems, fulfilling critical functions related to data analysis, infrastructure management and (cyber)security, just to name a few. In theory, an AI-based system can become a target on its own, and detecting of these type of attacks can pose a significant challenge. However, real-world examples of such attacks are less common. Understanding of the practical aspects to - on one hand, conduct an impactful attack against an AI-based system, and on the other, to defend against and respond to such a threat, is still limited.

Proofs of Concepts are vital tools to demonstrate that the problems TC SAI focuses on are of great practical importance, showing both the applicability of ideas and technology. Multi-party PoCs strengthen collaboration between TC SAI members and participants and can bring new partners to the group. The results help to put TC SAI's work into perspective, as well as create external visibility and build awareness of AI security problems.

4.2 Process

TC SAI calls for PoCs during the life of the TC. The process is intended to be lightweight and 'bottom-up', i.e. originating from the members and participants of the TC SAI community:

1) The interested organizations form the PoC Team, which consists of at least two organizations, and at least one of them is the TC SAI member or participant.

2) The PoC Team prepares the PoC Proposal, which should relate to current or proposed TC SAI WIs, use cases, test cases, problems, etc., considered therein.

3) The PoC Team sends the PoC Proposal in the format specified in clause 4.3 to the SAI@LIST.ETSI.ORG mailing list to inform the community and gather feedback.

4) Based on the community feedback and the criteria mentioned above in bullets 1) to 3), if the consensus is reached, the TC SAI approves the PoC Proposal and the SAI officials assign it a number.

5) The PoC Team updates the TC SAI about the progress and presents the results during TC SAI meetings. If possible, the PoC Team also presents the results in public venues (conferences, exhibitions) and promotes the PoC in (social) media.

6) Once an PoC Project is concluded, a PoC Report with the final results is expected to be provided to TC SAI as a contribution to a TC SAI face to face meeting or be announced on the SAI@LIST.ETSI.ORG mailing list. A PoC Wiki section of the ETSI portal via a link on the TC SAI home page will also indicate the present document.

7) PoC team members who are participants of a PoC Project may bring technical proposals based on PoC results to TC SAI as regular contributions.

4.3 PoC proposal format

PoC title: <title_here>				
Abstract: <abstract_here, incl. topics, goals>				
Related WIs: <WIs>				
PoC Team members				
#	**Organization name**	**Envisioned role**	**TC SAI member/ participant (yes/no)**	**Contact (name; email)**
1				
2				
3				
…				

History

Document history		
V1.1.1	April 2024	Publication