ETSI TS 104 033 V1.1.1 (2026-05)

TECHNICAL SPECIFICATION

Securing Artificial Intelligence (SAI); Security requirements for an Artificial Intelligence Computing Platform

Reference
DTS/SAI-006

Keywords
artificial intelligence, security

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Securing Artificial Intelligence (SAI).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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 specifies the requirements for a security framework of an AI computing platform. It further defines the security functions to be provided by the platform, the components to be implemented in the platform and their interfaces.

The present document is intended for use by designers of AI computing platforms.

The present document extends from the conclusions presented in ETSI GR SAI 009 [i.1].

NOTE: The present document applies to AI computing platforms that are deployed in data centres or edge computing environments. Other forms of computing platform, e.g. mobile phones or embedded devices capable of executing AI functionality, may also refer to this security framework adapted to specific conditions, resource constraints and security requirements.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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 necessary for the application of the present document.

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

2.2 Informative references

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

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

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

[i.1] ETSI GR SAI 009: "Securing Artificial Intelligence (SAI); Artificial Intelligence Computing Platform Security Framework".

[i.2] OWASP: "CycloneDX v1.7".

[i.3] ETSI TR 104 048: "Securing Artificial Intelligence (SAI); Data Supply Chain Security".

[i.4] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[i.5] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[i.6] ISO/IEC 24970: "Artificial intelligence — AI system logging".

[i.7] ETSI EN 304 223: "Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

AI application: software program that use AI techniques to perform specific tasks

AI computing platform: computing platform intended to host AI applications

AI model: computer program that has been trained on a set of data to recognize certain patterns or make certain decisions without further human intervention

execution environment: context in which computer code can execute (run)

3.2 Symbols

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

{*Security component*} delimits a "security component" described in Annex B that is involved in the interactive procedures

EXAMPLE: {Security management module}, {Host HMEE security function}.

<*Service-based interface*> delimits a "Service-based interface" described in Annex B that is used to deliver relevant information or data between the AI computing platform and platform users

EXAMPLE: <N4>, <S1>.

3.3 Abbreviations

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

AES	Advanced Encryption Standard
AI	Artificial Intelligence
BMC	Baseboard Management Controller
BoM	Bill of Materials
CPU	Central Processing Unit
DoS	Denial of Service
GCM	Galios Counter Mode
GPU	Graphics Processing Unit
HBRT	Hardware Based Root of Trust
HMEE	Hardware-Mediated Execution Enclave
HSM	Hardware Security Module
HUK	Hardware Unique Key
JTAG	Joint Test Action Group
LLM	Large Language Model
NIC	Network Interface Card
NPU	Network Processing Unit
OS	Operating System
RPO	Recovery Point Objective
RTR	Root of Trust for Reporting
RTS	Root of Trust for Storage
SDK	Software Development Kit
SE	Secure Enclave
SoC	System on Chip

TCG	Trusted Computing Group
TLS	Transport Layer Security
TPM	Trusted Platform Module
UI	User Interface
VM	Virtual Machine

4 Overview

The AI computing platform is a platform that is optimized to provide an execution environment and related resources to an AI system as shown in Figure 1 with a detailed view of the AI computing platform given in Figure 2.

The baseline requirements from ETSI EN 303 645 [i.4] apply (and shown in Table 1 below) in addition to specific requirements identified in the present document. Refer to Annex A for details.

Table 1: Baseline provision from ETSI EN 303 645 [i.4] mapped to the AI Computing platform requirement

Requirement in ETSI EN 303 645 [i.4]	Equivalent or extended provision in the present document
5.1 No universal default passwords	n/a
5.2 Implement a means to manage reports of vulnerabilities	
5.3 Keep software updated	
5.4 Securely store sensitive security parameters	Addressed in clause 5.1.4.2
5.5 Communicate securely	Addressed in clause 5.1.4.1
5.6 Minimize exposed attack surfaces	
5.7 Ensure software integrity	
5.8 Ensure that personal data is secure	
5.9 Make systems resilient to outages	
5.10 Examine system telemetry data	
5.11 Make it easy for users to delete user data	
5.12 Make installation and maintenance of devices easy	
5.13 Validate input data	
6 Data protection provisions for consumer IoT	

The AI Computing platform shall make provision to support the requirements for transparency and explicability of AI processing defined in ETSI TS 104 224 [1], and should support the baseline security requirements for AI models and systems in ETSI EN 304 223 [i.7]. Refer to Annex F for details. The platform also should respect the recommendations for data supply chain security outlined in ETSI TR 104 048 [i.3].

The AI computing platform is decomposed into three (3) distinct layers:

- Hardware layer, composed of elements to give assurance of hardware enabled secure storage, networking hardware and specialist computing hardware in support of AI functions (e.g. AI Accelerator elements).
- Basic software layer, is an interface to provide the hardware layer capabilities to AI application providers and users and is composed of operating system, chip-level SDK, virtualization component for VM or containers, etc.
- (AI) Application enabling layer, is the AI application facing element of the platform and is composed of different types of deep learning framework, application-level SDK, management module, etc.

NOTE: As the AI Computing platform defined in the present document is intended for deployment primarily in data centres or edge computing environments the elements of a computing platform that would be present for a desktop or UI-centric environment (e.g. graphics processing) are not considered.

The further decomposition of each of the three (3) distinct layers are given in Annex B.

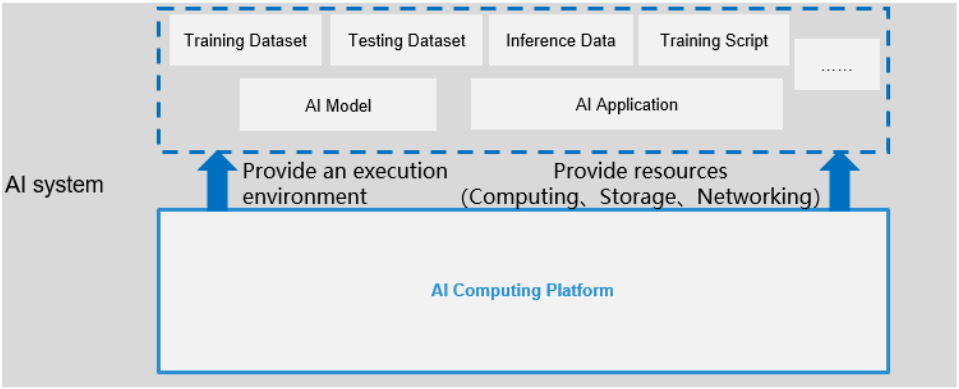

Figure 1: AI computing platform overview

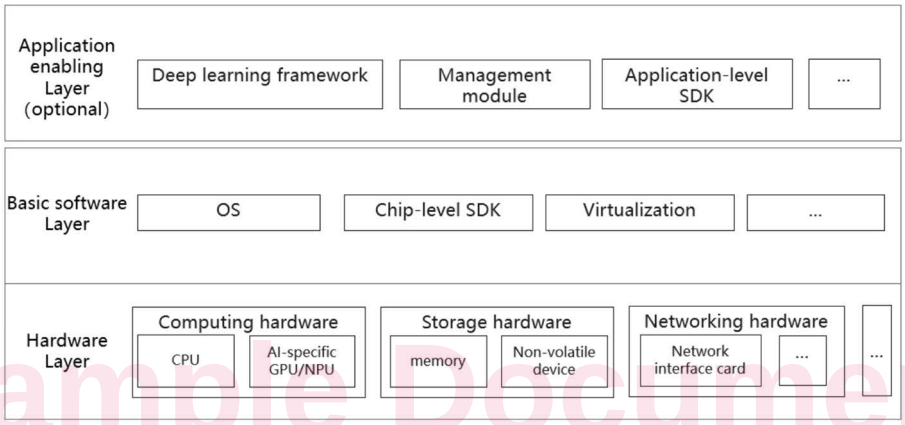

Figure 2: De-composition of a typical AI computing platform

The platform provides resources required for the AI model and associated AI application including (see also ETSI GR SAI 009 [i.1]):

- Computing execution environment (in particular, one or more AI accelerated processors are included), the execution environment includes the fundamental software framework, various kinds of libraries and different hardware drivers.
- Storage to give secure and reliable support of assets including training dataset, testing dataset, inference data and training script, etc.
- Networking.

In ETSI GR SAI 009 [i.1], Table 1 and Table 2, threats to the AI computing platform are summarized and analysed. The threat analysis from ETSI GR SAI 009 [i.1] is adopted without change for the present document. From the security threat analysis provided in ETSI GR SAI 009 [i.1] the following security services are identified and specified in detail in the present document:

- Protection of AI assets in transmission and storage.
- Protection of AI assets during processing.
- AI accelerator resource isolation service.
- Model training recovery service.
- Inference attack detection service.
- AI related log protection.
- Model BoM service.

In addition, the AI Computing platform shall support the following more general services in support of the AI Computing platform specific services listed above:

- Identity management and access control (see clause 5.1.2).
- Integrity protection (see clause 5.1.3):
  - Protection of integrity of system startup data.
  - Protection of integrity of AI model data.
- Data protection (see clause 5.1.4):
  - Data in transit.
  - Data at rest.
- Secure audit (see clause 5.1.5).
- Secure response (see clause 5.1.6).
- Resilience (see clause 5.1.7).

5 Security requirements and security functions of the framework

5.1 Security requirements for the AI computing platform

5.1.1 Overview

The security requirements for the AI computing platform are defined in order to mitigate threats against itself.

The baseline security requirements are grouped as shown in Figure 3 in order to protect the AI Computing platform.

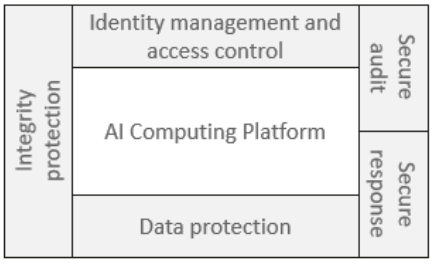

Figure 3: Overview of baseline security requirements of the AI computing platform

NOTE 1: Unless otherwise specified, all security requirements are applicable to the AI computing platform in data centre and edge computing scenarios.

NOTE 2: The implementation reference for security mechanism of the AI computing platform based on clause 5 is provided in Annex D.

5.1.2 Identity management and access control

The AI computing platform shall implement the principle of least privilege where the following requirements on identity management and access control apply:

- External physical interfaces of the AI computing platform, e.g. JTAG ports, shall be disabled after manufacture.

NOTE 1: This is consistent with the principles outlined in clause 5.6 of ETSI EN 303 645 [i.4], particularly provisions 5.6-3 and 5.6-4, to minimize the attack surface.

- Access control shall be implemented to allow only authorized access to the platform via the physical interface.
- Remote access of an account with root privilege shall be prohibited.

NOTE 2: Root privilege violates the principle of least privilege and is consistent with provision 5.6-7 of ETSI EN 303 645 [i.4].

- Only identified and authenticated parties, where authorization to access has been verified, shall be able to access resources on an AI computing platform.

5.1.3 Integrity protection

5.1.3.1 Protection of integrity of system startup data

The following requirements on integrity protection of system startup data apply:

- An AI computing platform shall support and implement a secure boot mechanism.

EXAMPLE: An AI computing platform can meet this requirement by support of solutions including those from the Trusted Computing Group (TCG) which have the capability to cooperate with hardware security modules such as a Trusted Platform Module (TPM) hardware root of trust, a Hardware Security Module (HSM) or Secure Enclave (SE) to facilitate the mechanisms including proactive integrity measurement and remote attestation.

5.1.3.2 Protection of integrity of AI model data

- The following requirements on integrity of AI model data apply: An AI computing platform should support for verifying integrity of AI model before performing inference task.

5.1.4 Data protection

5.1.4.1 Data in transit

NOTE: For the present clause data refers to AI specific data.

The following requirements on protection of data in transit apply:

- The AI computing platform shall protect data transmitted to and from the platform from unauthorized exposure.
- The AI computing platform shall protect data transmitted to and from the platform by only allowing transmission to or from identified, authenticated and authorized entities.

EXAMPLE: Known protocols such as TLSv1.3 [i.5] with appropriate selection and application of cryptographic primitives can be used to satisfy these requirements, e.g. TLS_AES_128_GCM_SHA256 (identifying TLS using AES-128 in Galois Counter Mode for encryption with SHA256 for hashing operations).

5.1.4.2 Data at rest

The following requirements on protection of data at rest apply:

- The AI computing platform shall have the ability to backup, and recover, system configuration parameters and other data that may be required for system recovery.

NOTE: This is consistent with provisions given in clauses 5.7 and 5.11 of ETSI EN 303 645 [i.4].