ETSI TC SAI

Securing Artificial Intelligence

Artificial Intelligence (AI) is transforming every aspect of our digital lives – from predictive text on smartphones to smart manufacturing and cloud systems. However, the rapid growth of AI also brings **significant security risks.**

To address these, ETSI established the **Technical Committee on Securing Artificial Intelligence (TC SAI),** focused on creating **high-quality technical standards** that secure AI technologies from new and evolving threats.

Key Activities & Responsibilities

Improving the security of AI by developing technical standards that:

- **Protect AI systems** from being exploited
- **Mitigate the misuse** of AI by malicious actors
- Leverage AI to **enhance cybersecurity defenses**
- Address **societal and safety impacts** of AI deployment

ETSI Technical Committee Securing Artificial Intelligence (TC SAI) brings together:

- **Network operators**
- **Technology manufacturers**
- **End users**
- **Governments & regulators**

CASE STUDY:
Baseline Cyber Security Requirements for AI Models and Systems

ETSI TC SAI has introduced a specification for baseline cyber security requirements for AI models and systems, which defines principles for secure design, secure development, secure deployment, secure maintenance and secure end of life. This publication is currently in the approval process to become a European Standard.

Collaboration

TC SAI collaborates closely with other ETSI committees such as TC CYBER and TC DATA on topics including:

- Use of AI in cybersecurity
- Privacy and security of data in AI systems
- Adherence to data protection legislation

Standards & Specifications

TC SAI maintains a comprehensive, publicly available library of standards covering:

- **Securing AI** – Defending AI components within broader systems
- **Mitigating Malicious AI** – Addressing threats where AI is used as the attack vector
- **AI for Security** – Applying AI to strengthen existing security solutions
- **Societal Security & Safety** – Ensuring safe, ethical deployment of AI systems

Contact ETSI TC SAI

SAIsupport@etsi.org

TC SAI Portal:
https://portal.etsi.org/SAI

Mr Scott Cadzow, ETSI TC SAI Chair
Scott Cadzow

Dr Georges Sharkov, ETSI TC SAI Vice-Chair
George Sharkov

Mr Alec Brusilovsky, ETSI TC SAI Vice-Chair
Alec Brusilovsky

Dr Li Tieyan, ETSI TC SAI Vice-Chair
Li Tieyan

Mr Kim Nordström, ETSI SAI Technical Officer
Kim Nordström

About ETSI

ETSI is one of only three bodies officially recognised by the European Union as a European Standards Organisation (ESO). It is an independent, not-for-profit body dedicated to ICT standardisation. With over 900 member organisations from more than 60 countries across five continents, ETSI offers an open and inclusive environment for members representing large and small private companies, research institutions, academia, governments, and public organisations. ETSI supports the timely development, ratification, and testing of globally applicable standards for ICT-enabled systems, applications, and services across all sectors of industry and society.

ETSI
The Standards People