Work outside the IETF

Suresh Krishnan

Relevant work outside the IETF

THE LINUX FOUNDATION

Agentic AI Foundation

Model Context Protocol

Agent2Agent (A2A) Protocol

AGNTCY

CONFIDENTIAL COMPUTING CONSORTIUM

Attestation SIG

Proposed security analysis of agentic AI

IEEE

P3394

Standard for LLM Agent Interface

ISO

SC42

Artificial intelligence

Global Alliance for Genomics & Health

Collaborate. Innovate. Accelerate.

AI Agent Protocol

Community Group

ITU

ITU-T Study Group 17

Agentic AI Security

3GPP A GLOBAL INITIATIVE

TR 22.870

6G Use Cases and Service Requirements

TR 23.801-01

Study on Architecture for 6G System

Additional Info and Links

With inputs from: Arnaud Taddei, Zaheduzzaman Sarker, Muhammad Usama Sardar

Linux Foundation (LF)

- Agentic AI Foundation: https://aaif.io
  - Model Context Protocol (MCP) https://modelcontextprotocol.io
  - Agent2Agent (A2A) Protocol https://a2a-protocol.org
  - AGNTCY project https://agntcy.org
  - LF AI & Data https://lfaidata.foundation/
- Confidential Computing Consortium (CCC)
  - Attestation SIG: https://github.com/CCC-Attestation
  - Proposal on security analysis of Confidential Agentic AI Systems: https://github.com/ccc-attestation/governance/issues/20
    - Pre-handshake attestation results in replay [ref] and diversion [ref] attacks.
    - Intra-handshake attestation is vulnerable to diversion [ref] and relay [ref] attacks.
    - Post-handshake attestation is unavoidable for agentic AI. Intra-handshake attestation only adds unnecessary complexity which is avoidable.

AI in 3GPP – 6G perspective

Very high-level view

- Two main streams of the topics : **AI for 6G architecture** and **6G network for AI**.
- **AI for 6G architecture** concentrates on -
  - How AI-capable entities in the 6G Core Network can handle requests with or without intent, enable modular procedures, support closed-loop learning
  - AI/ML-enabled network functions, performance monitoring, operator control, roaming, and interoperability with 5G
- **6G network for AI** emphasizes on -
  - Methods to enable communication amongst AI agents on different UEs via discovery, identifying and authorising the agents in the UEs
  - Enhanced network capability exposure functionalities to the AI agent on the Application Functions in the data networks (e.g. on the Internet)
- **Current progress status in 3GPP**
  - Significant momentum with 6G study progress since 6G workshop in 2025
  - SA1 is finalizing the study phase on 6G use cases and requirements, use cases will be part of TR 22.870.
  - SA2 moved forward with identifying and summarizing solution variants for Key Issues (KI18 and KI19, see TR: 23.801-01) and expected to conclude on 6G Study by March 2027.
  - SA3 will discuss the security threats and potential security solutions based on the outcome of SA2.

Global Alliance for Genomics and Health

- Trusted Research Environment (TRE) Open Suite https://www.ga4gh.org/what-we-do/ga4gh-implementation-forum/gif-projects/tre-open-suite/

ITU-T SG17 Status on Agentic AI Security and Trust

A strategy, A new structure, First work items, A roadmap, A schedule

In general a LOT of work since December 2024 at high cadence

- ITU-T SG17 grew to 400 participants and 57 member states as per strong modernization program
- One new member per month mostly western industry (Thales, Cognizant, Google, Vodafone, etc.)
- First workshop Challenging the status quo on AI Security 11th of July 2025 (LS 2077)
- AI Strategy available to IETF (LS 2106)

Leads to

Restructuring (to be fully approved beginning April)

- Creation of new Question 16 for AI Security including Agentic AI with a carve out for no overlap with IETF!
- Merge of Question 3 and Question for Agentic AI Digital Identity Amendment of Question 7 for Agentic AI

Leads to

Leads to

New Q10 work items

Out of 40 work items on AI security 7 are related to Agentic AI (+20 in draft!)

- X.LLMCC Guidelines for large language model data security based on confidential computing, already sent to IETF per liaison 2108
- X.S-AIA Security requirements and guidelines for Artificial Intelligence agent
- XSTR.sem-AIA Security evaluation methods for Artificial Intelligence agent
- X.sr-taimas Security requirements for terminal-based artificial intelligence multi-agent system
- X.dpidm-aAI Terminology and design guidelines for Agentic AI identity management
- XSTR.gidi Globally interoperable digital identity (including humans/enterprise/non-humans i.e. Agentic AI) Even the European Union contributes!
- XSTR.ltf-AAI Landscape of trust framework for agentic AI

Supports / is supported by

A specific scheduled roadmap through Workshops opened to everyone and SG17 meetings

- **1st Workshop** 30-31st of March - ITU Workshop on "Trustable and Interoperable Digital Identities for Human and Agentic AI"
  - First SG17 Content Week 30th of March - 2nd of April
- **2nd Workshop** 2nd of June - Workshop on globally interoperable digital identity
  - Fifth SG17 Plenary 1-10th of June
- **3rd Workshop** 10th of July - Designing Trust Management for Agentic AI
  - AI for Good 6-10th of July

Leads to

Leads to