ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

Remote Attestation Challenges for AI Agents

FG-TIDA

Remote attestation for AI agents

What to attest · How to attest · When to attest?

ABSTRACT

Note

[Author: write a short abstract — what this document analyses (remote attestation challenges for AI agents) and what a reader will take away.]

This document examines the challenges of remote attestation (RA) for AI agents, organised around three questions: what to attest, how to attest, and when to attest. It surveys the current RA landscape, states the problem for agentic AI, identifies the core challenges and research/standardization gaps, and maps existing standards building blocks to the needs of AI-agent attestation.

HISTORY

Version	Document	Approval	Focus Group	Working Group
0.1	Remote Attestation Challenges for AI Agents	<date>	TIDA	RA-AAI

To access this Document as a PDF, open the published documentation site in your web browser and click the PDF download link, or navigate directly to https://fg-tida.github.io/wg1-ra-aai/specification.pdf.

AUTHORS

Name	Affiliation	Contact
<Jane Doe>	<Organization / Company>	<jane.doe@example.com>
<John Smith>	<Organization / Company>	<john.smith@example.com>

KEYWORDS

Remote attestation, AI agents, agentic AI, trust, RATS, TCG, trusted computing.

PREFACE

> **Note**
>
> *[Author: write the preface — the motivation for this document, its scope, and its intended audience.]*

FOREWORD

Agentic AI systems now act as autonomous entities capable of reasoning, planning, and executing tasks across services, infrastructures, and organizational boundaries. This fundamentally changes the nature of identity in digital systems: identity is no longer limited to human users and static machine instances but must also encompass autonomous, dynamic, and goal-oriented agents. And identity alone is insufficient — the core question extends beyond "what an entity is" to "whether, and under what conditions, that entity should be trusted to act".

The Focus Group on Trust and Identity for humans and agentic AI (FG-TIDA) addresses trust management and interoperable digital identity infrastructure for humans and for agentic AI, supporting the development of secure, trustworthy digital ecosystems in which humans and agentic AI can safely interact and collaborate.

FG-TIDA was established under Recommendation ITU-T A.7 (Focus groups: Establishment and working procedures), with ITU-T Study Group 17 as its parent group. Further details are available in the group's terms of reference.

For more news and updates about the TIDA Community, including its supporter organizations, please refer to the community's published resources.

CONTENTS

RA Landscape: Industry Analysis . . . 1
0.0.1 Market & Actors Map . . . 1
0.0.2 RA Ecosystem . . . 1
0.1 Problem Statement . . . 1
0.1.1 Security and Privacy Vulnerabilities of AI Agents and Agentic Networks . . . 1
0.1.2 Core Problem . . . 1
0.1.3 Gap . . . 1
0.2 RA Core Challenges . . . 1
0.3 Three Fundamental Questions . . . 2
0.3.1 What to Attest? . . . 2
0.3.2 How to Attest? . . . 2
0.3.3 When to Attest? . . . 2
0.3.4 Research Gaps . . . 2
0.3.5 Standardization Gaps . . . 2
0.4 Standards' Existing Building Blocks . . . 2
0.4.1 IETF Landscape and Mapping to Agent RA . . . 2
0.4.2 TCG Landscape and Mapping to Agent RA . . . 2
0.5 Future Directions . . . 3
0.6 References . . . 3

RA Landscape: Industry Analysis

> **Note**
>
> *[Author: introduce this chapter — the current state of the remote attestation (RA) industry as it relates to AI agents.]*

0.0.1 Market & Actors Map

[Author: map the market and the key actors in the remote attestation space — who provides RA technology, who consumes it, and how AI-agent vendors fit in.]

0.0.2 RA Ecosystem

[Author: describe the remote attestation ecosystem — the components, relationships, and existing deployment patterns relevant to AI agents.]

0.1 Problem Statement

> **Note**
>
> *[Author: frame the problem this document addresses.]*

0.1.1 Security and Privacy Vulnerabilities of AI Agents and Agentic Networks

[Author: describe the major security and privacy vulnerabilities introduced by AI agents and agentic networks.]

0.1.2 Core Problem

[Author: state the core problem in remote attestation for AI agents.]

0.1.3 Gap

[Author: identify the gap between what current remote attestation approaches provide and what AI agents require.]

0.2 RA Core Challenges

> **Note**
>
> *[Author: introduce and describe the core challenges of remote attestation for AI agents.]*

0.3 Three Fundamental Questions

Note

[Author: introduce the three fundamental questions that structure remote attestation for AI agents.]

0.3.1 What to Attest?

[Author: discuss what should be attested for an AI agent — identity, code, configuration, model, runtime state, behaviour, and so on.]

0.3.2 How to Attest?

[Author: discuss the mechanisms and protocols for attesting an AI agent.]

0.3.3 When to Attest?

[Author: discuss the timing and triggers for attestation — at load, at runtime, per interaction, continuously.]

0.3.4 Research Gaps

[Author: summarise the open research gaps across the three questions.]

0.3.5 Standardization Gaps

[Author: summarise the standardization gaps across the three questions.]

0.4 Standards' Existing Building Blocks

Note

[Author: introduce the existing standards that can serve as building blocks for AI-agent remote attestation.]

0.4.1 IETF Landscape and Mapping to Agent RA

[Author: survey the relevant IETF work (e.g. RATS architecture, EAT, and related drafts) and map it to AI-agent remote attestation.]

0.4.2 TCG Landscape and Mapping to Agent RA

[Author: survey the relevant Trusted Computing Group (TCG) work and map it to AI-agent remote attestation.]

0.5 Future Directions

Note

[Author: outline future directions — recommended next steps, proposed work items, and opportunities for standardization.]

0.6 References

Note

[Author: list the normative and informative references cited in this document. Below are examples of the format — replace them with the actual IETF, TCG, and other sources you cite.]

[RATS-Architecture]
IETF RFC 9334, *Remote ATtestation procedureS (RATS) Architecture*,

https://datatracker.ietf.org/doc/html/rfc9334

[EAT]
IETF, *Entity Attestation Token (EAT)*,

https://datatracker.ietf.org/doc/html/draft-ietf-rats-eat

[TCG]
Trusted Computing Group, *specifications*,

https://trustedcomputinggroup.org/

LIST OF TABLES

LIST OF FIGURES