

AI Agent Authentication and Authorization

draft-klrc-aiagent-auth-00

Pieter Kasselmann
Defakto Security

Jeff Lombardo
AWS

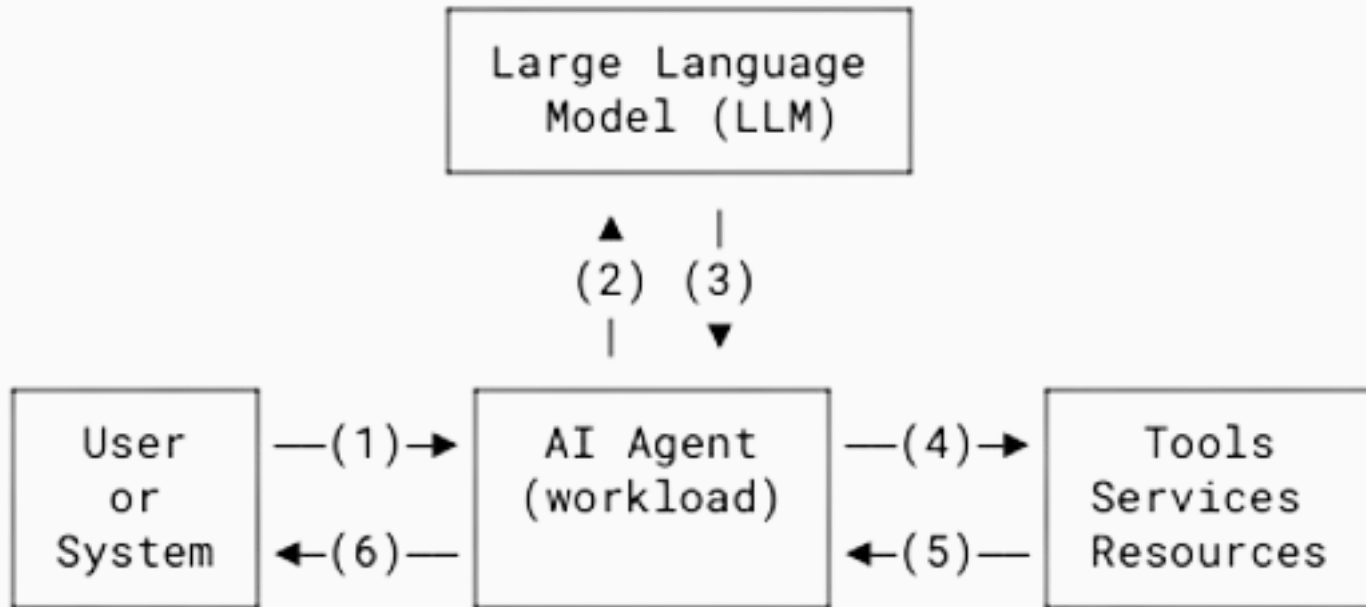
Yaroslav Rosomakho*
Zscaler

Brian Campbell*
Ping Identity

AI is exploding. We need guardrails as soon as possible!

- There is a tendency to invent new “AI” protocols
- We **MUST** leverage the learnings and exiting standards of several decades of identity, authentication, and authorization
- There is a wide spectrum of standards involved, but there is no single framework guiding implementers to the right places
- We **MAY** locate missing pieces in existing standards to surgically address them

Background: Agents are workloads



Background: What is this draft?

Informational draft to map existing (mainly IETF) technologies to
Agentic communications auth

- Identifiers
- Credential Format
- Attestation
- Provisioning
- Authentication
- Authorization
- Monitoring and Observability

Policy	Monitoring, Observability & Remediation	Compliance
	Authorization	
	Authentication	
	Provisioning	
	Attestation	
	Credentials	
	Identifier	

Background: Key building blocks

- WIMSE identifier for agentic AI identity
- WIMSE credentials and authentication for AI authentication
- OAuth 2.0 for authorization and delegation
- SSF/CAEP for monitoring and observability

Hoped dispatching outcome

- AD-Sponsored
- Existing WG (OAuth, WIMSE)
- Some new WG?