THALES
Building a future we can all trust

Defining the layered identity management model for agentic AI

ITU-T Workshop
March 2026

www.thalesgroup.com

About me

Debora Comparin
ITU-T SG17 WP1 Chair

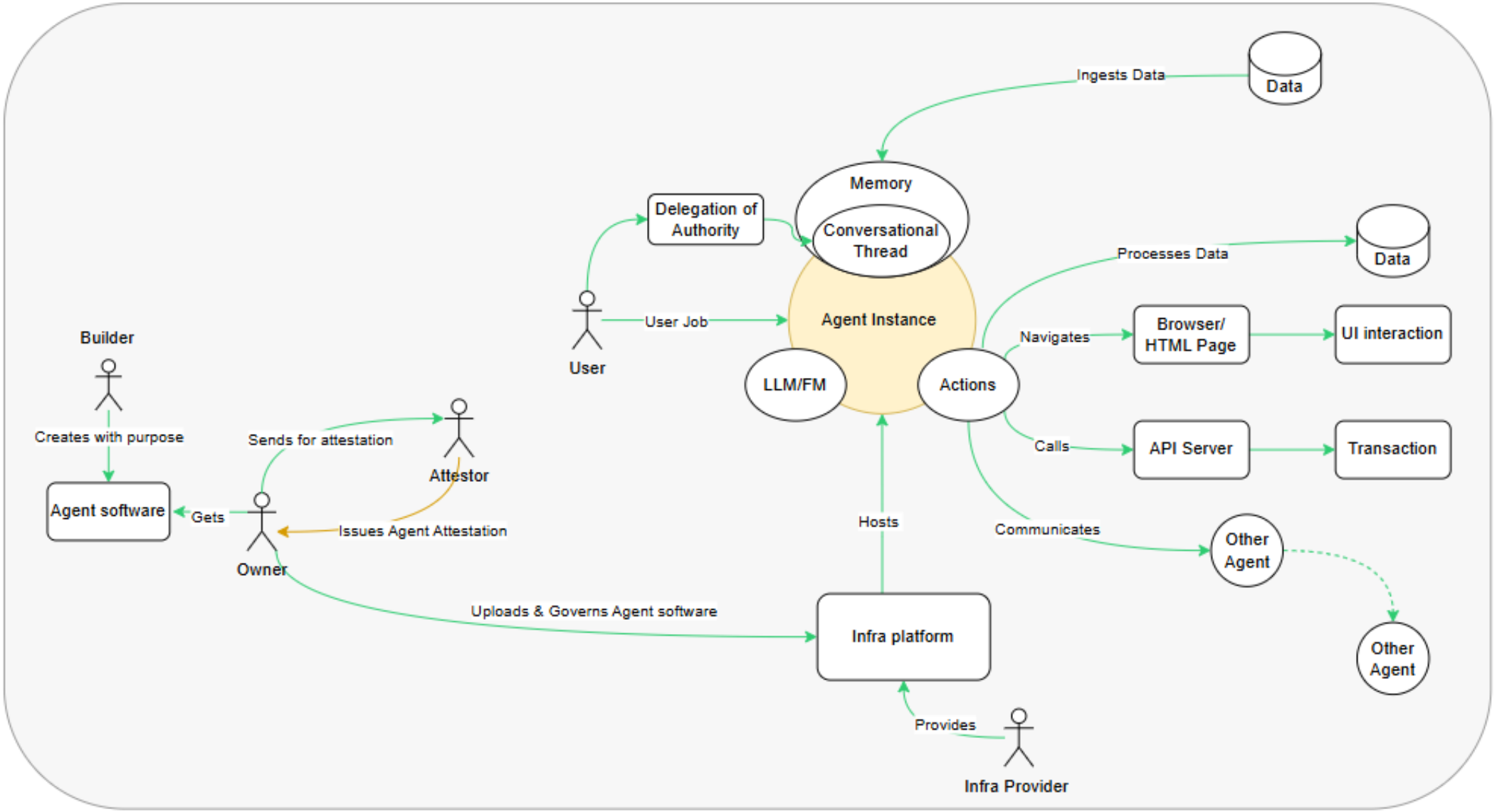
Proposed Definition for Agentic AI (at least for today's discussion)

An Agentic AI or AI Agent or Agent is an autonomous software entity that interprets goals, formulates intent, and executes actions, often by invoking external tools, APIs, or other agents to achieve outcomes on behalf of users.

Its behaviour is driven by model-based reasoning, typically relying on Large Language Models (LLMs) or other Foundation Models (FMs) to analyze context, generate plans, and adapt its actions dynamically.

Hot debate: is an agent a workload?

The Agentic AI Ecosystem



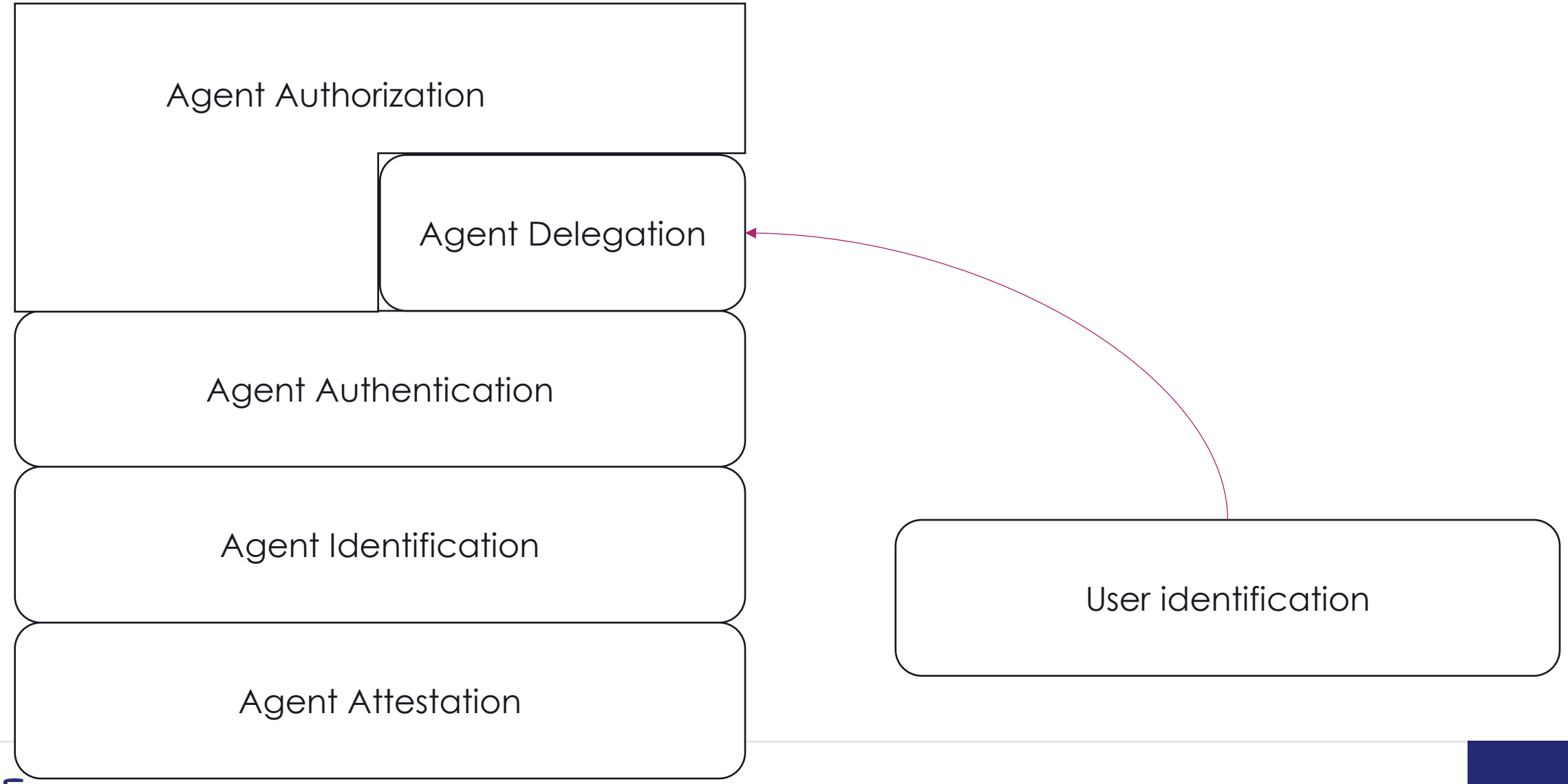
Why does an Agent need identity?

AI agent needs an identifier and credentials so it can be authenticated by the Tools, Services, other agents, LargeLanguage Model, System and the User (via the underlying operating system or platform, similar to existing applications and services).

Once authenticated, these parties determine if the AI Agent is authorized to access the requested LargeLanguage Model, Tools, Services or Resources.

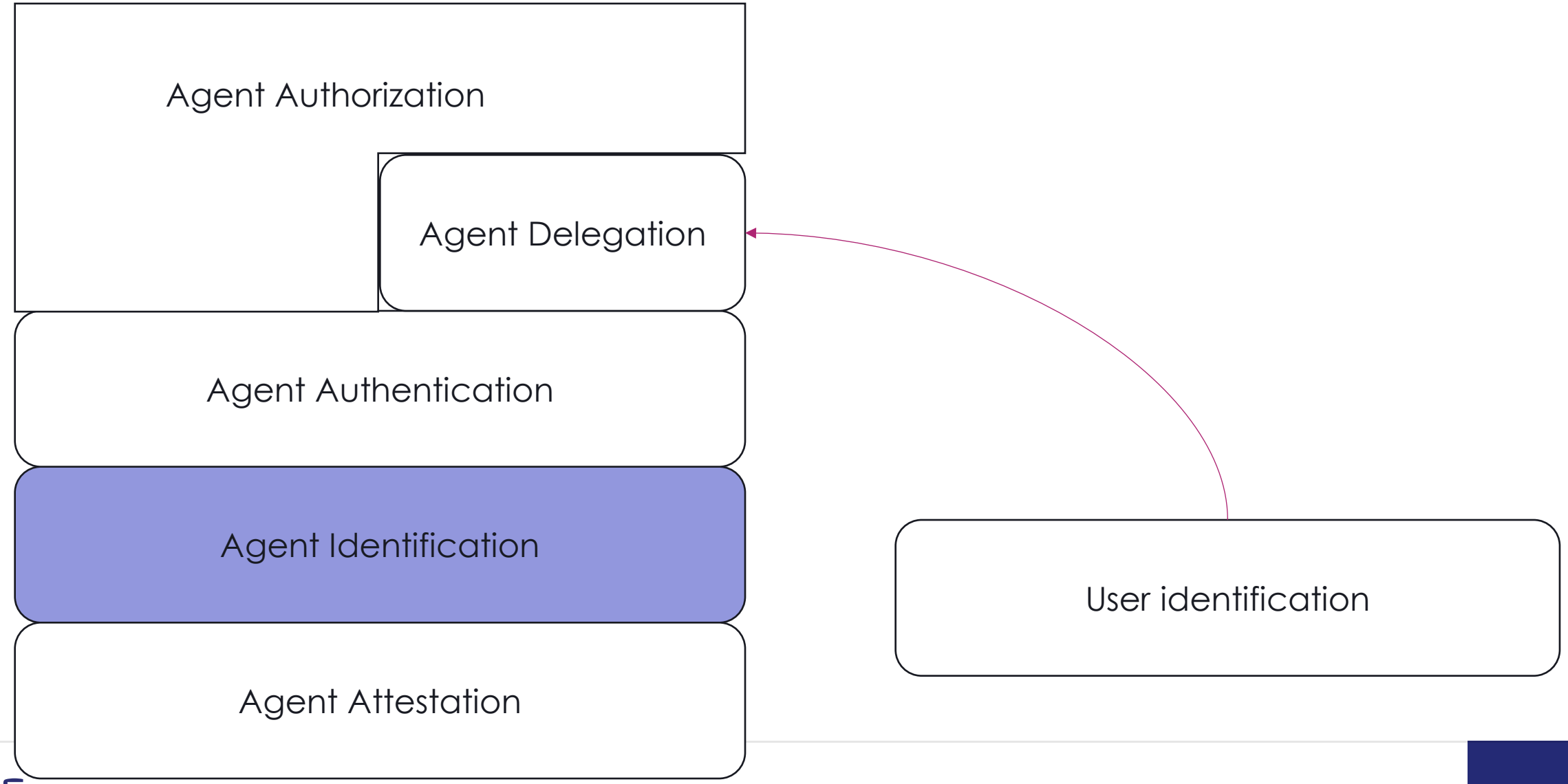
If the AI Agent is acting on behalf of a User or System, the User or System needs to delegate authority to the AI Agent, and the User or System context is preserved and used as input to authorization decisions and recorded in audit trails.

Proposed Agent ID stack



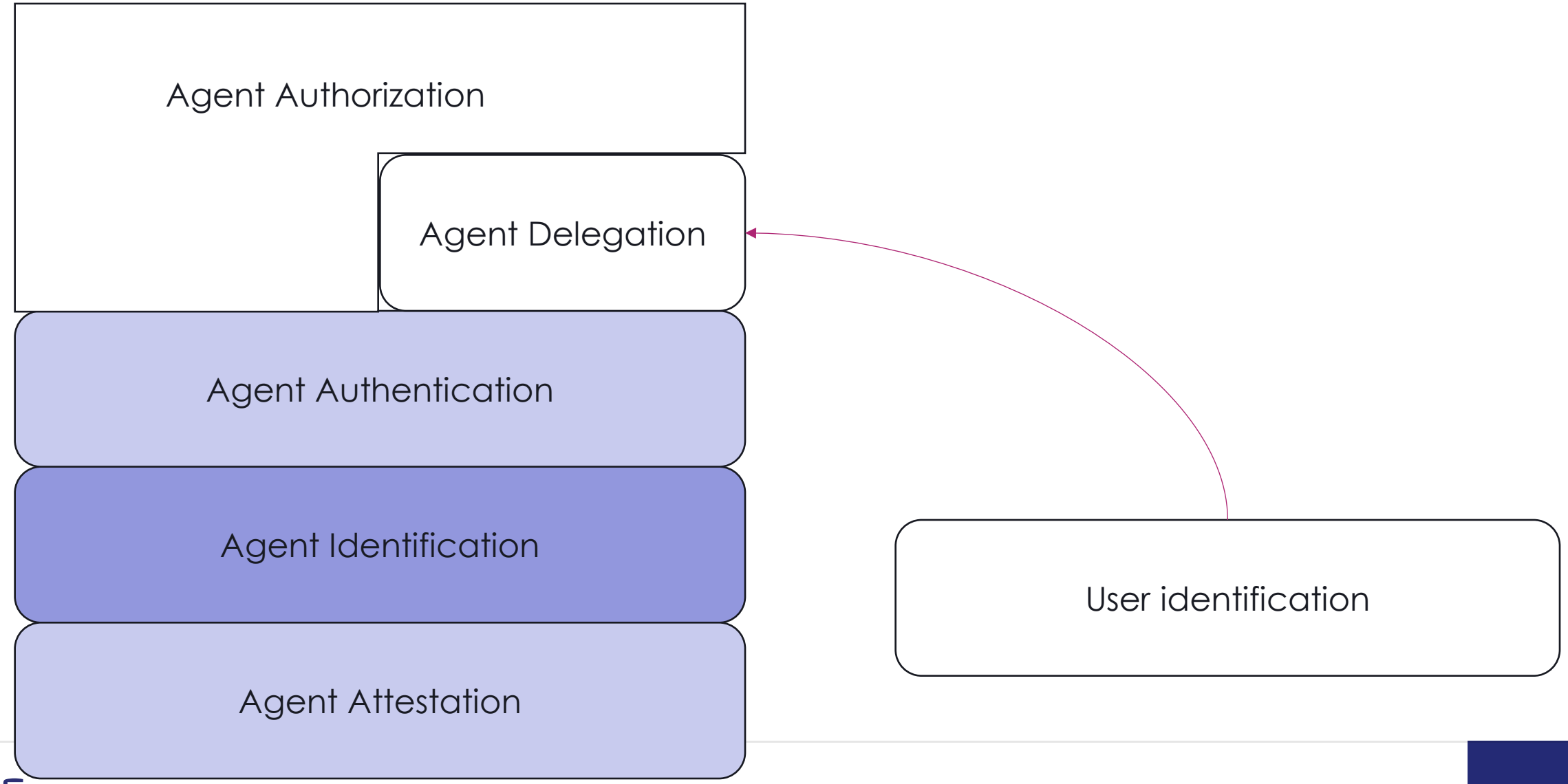
REF xxxxxxxxxxxx rev xxx – date Name of the company / Template: 87211168-DOC-GRP-EN-007

Focus of this panel



REF xxxxxxxxxxxx rev xxx – date Name of the company / Template: 87211168-DOC-GRP-EN-007

Focus of this panel



REF xxxxxxxxxxxx rev xxx – date Name of the company / Template: 87211168-DOC-GRP-EN-007

Which Agent identity?
A proposed mental model for a layered ID of Agents

Accountability?

Protocol Identity	oAuth ClientID etc.	Represent a software client meaningful n the context of a given protocol
Logical Identity	ANS	Represents the software as a persistent, conceptual entity, independent of where or how it is deployed
Service Identity	DNS	Represents a network-reachable service endpoint e.g. api.example.com. A service endpoint MAY represent multiple deployments and hence multiple workloads
Workload Identity	WIMSE, SPIFFE	Represent a specific workload instance, or a logical workload consisting of multiple instances that share the same identity within a given trust domain

Which Agent identity?
A proposed mental model for a layered ID of Agents

Accountability?

Protocol Identity	oAuth ClientID etc.	Represent a software client meaningful n the context of a given protocol
Logical Identity	ANS	sistent, of where
Service Identity	DNS	service A service
Workload Identity	WIMSE, SPIFFI	stance, or a logical workload consisting of multiple instances that share the same identity within a given trust domain

Each one with a specific identifier, credential(s), issuer, authentication mechanisms

REF xxxxxxxxxxx rev xxx – date Name of the company / Template: 87211168-DOC-GRP-EN-007

Example of Workload Identity with WIMSE

Property	WIMSE
Identifier	URI identifying a workload within a trust domain `wimse://<trust-domain>/<path>`
Credential	– Workload Identity Token (WIT): JWT binding a public key to the WIMSE identifier – Workload Identity Certificate (WIC): X.509 certificate binding a public key to the WIMSE identifier
Issuer	Trust Domain Authority (WIMSE issuer / identity provider)
Authentication	**Transport layer** mTLS using WIC
	Application layer – WIT + WPT (JWT proof of possession) – WIT + HTTP Message Signatures The WIT is targeted for application-level protocols. The WIC is targeted for transport-level protocols. This does not preclude the use of the WIT in transport-level protocols or the WIC in application-level protocols, but these are the primary intended uses.
	Protocol layer

Table 4: WIMSE workload identity

If this mental model works, can you help building a complete picture?

Authentication Layer	Protocol Identity	Logical Identity	Service Identity	Workload Identity
Transport Layer				• mTLS using WIC
Application Layer				• WIT + WPT (JWT proof of possession) • WIT + HTTP Message Signatures
Protocol Layer				

REF xxxxxxxxxxxx rev xxx – date Name of the company / Template: 87211168-DOC-GRP-EN-007

THALES
Building a future we can all trust

Thank you

www.thalesgroup.com