

THALES

CYBERSECURITY

AI Agents Need a New Trust Model

Ward Duchamps

Director of Strategy & Innovation
Thales

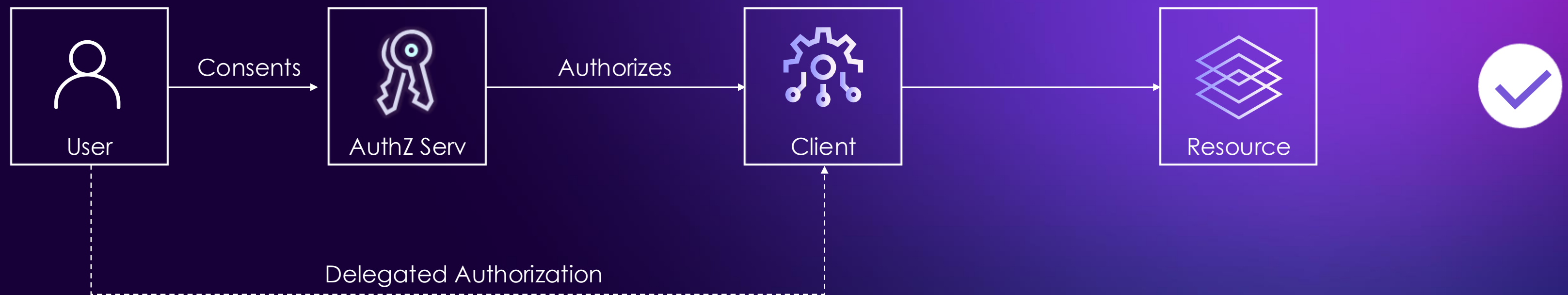
March 31st 2026, Geneva, Switzerland



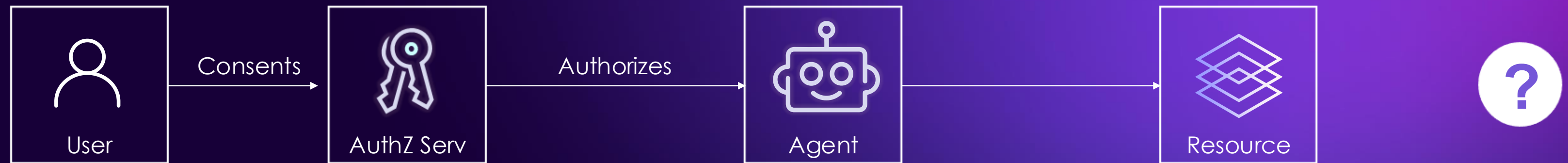
Designing for Autonomy Not for Assistance

From “Agentish” to Agentic.
Shifting from human-in-the-loop
to intent-driven execution.

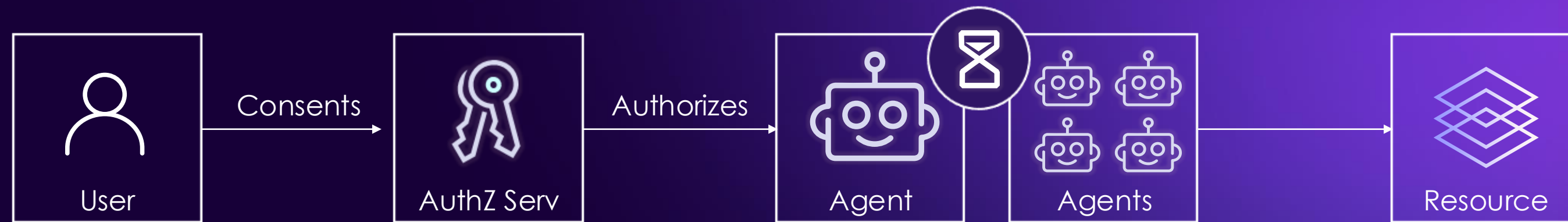
OAuth relies on user consent to delegate authorization to a centralized Authorization Server



Can this delegated authorization model hold in an agentic, autonomous world?



Three fundamental gaps make OAuth-style delegation impractical for highly autonomous systems

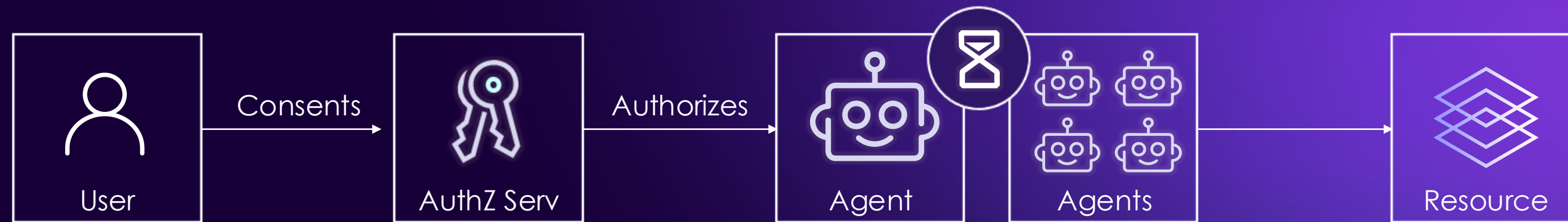


Time mismatch: sessions vs. intent

OAuth uses short-lived tokens.

But Agent tasks, and user intent,
may span hours or days.

Three fundamental gaps make OAuth-style delegation impractical for highly autonomous systems



Intent ≠ resource aware

OAuth assumes the user understands and approves specific resources and scopes.

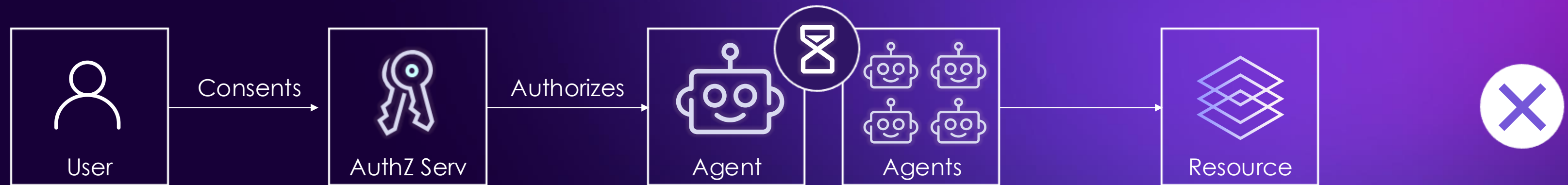
But in Agentic models, the user defines *what*, and the Agent decides *how*.

Time mismatch: sessions vs. intent

OAuth uses short-lived tokens.

But Agent tasks, and user intent, may span hours or days.

Three fundamental gaps make OAuth-style delegation impractical for highly autonomous systems



Intent $\neq$ resource aware

OAuth assumes the user understands and approves specific resources and scopes.

But in Agentic models, the user defines *what*, and the Agent decides *how*.

Time mismatch: sessions vs. intent

OAuth uses short-lived tokens.

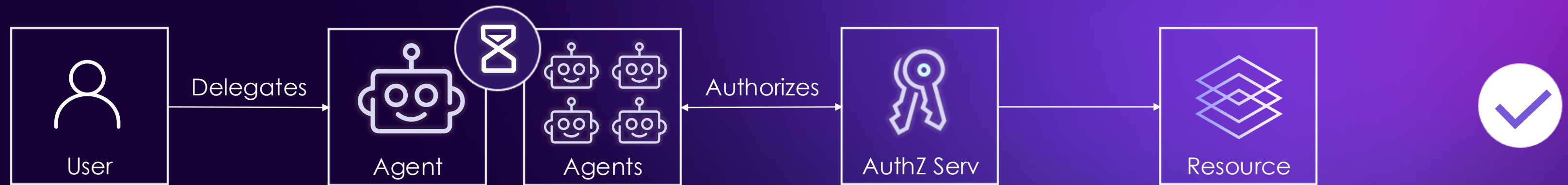
But Agent tasks, and user intent, may span hours or days.

Dynamic execution paths

OAuth assumes fixed scopes and known resources.

But Agents decide the path at runtime, requiring new, unforeseen data access.

A new model: users delegate intent to agents before agents obtain resource authorization



User delegates intent to the agent.

Agents determine execution while preserving that intent end-to-end.

Agent actions are authorized in alignment with the original human intent.



Delegated Intent

What the Parent Specifies

Goal

Deliver passenger to UC Berkeley

Constraint

Safety is non-negotiable

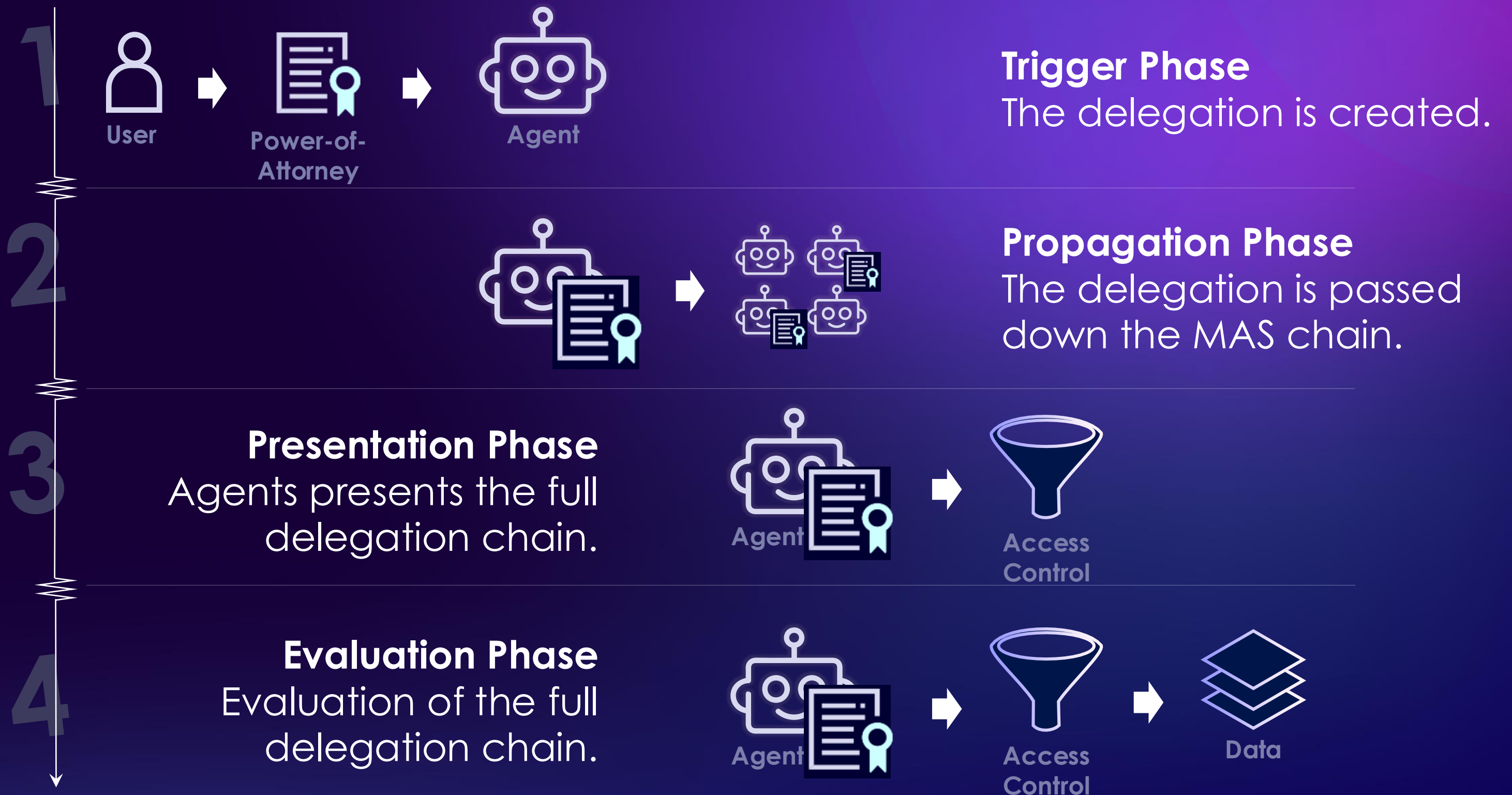
Delegation

Provide verifiable proof to obtain temporary campus access

Autonomy

System determines route and execution in real time

Binding end-user intent to data access policies



Trusted Agent Access

×

+

←

→

↻

f0faa4bda7574bf3ad3f03b579ac8aa8

☆

↓

Incognito (2)

⋮

L'Oréal

AI Agent

New chat

My agent

Chat history

PoA dashboard

Mark Chan

COO

Hello Chief Operations Officer. Instead of helping you drafting reports, I suggest to handle some of your regular tasks more autonomously. I can update stock projections based on sales forecast, so operations teams can anticipate demand and avoid shortages. Would you like me to take care of this for you?

11:51

Ask your question

AI agents can make mistakes. Verify important information.

Trusted Agent Access

×

+

←

→

↺

f0faa4bda7574bf3ad3f03b579ac8aa8

☆

↓

Incognito (2)

⋮

L'Oréal

AI Agent

New chat

My agent

Chat history

PoA dashboard

Mark Chan

COO

Hello Chief Operations Officer. Instead of helping you drafting reports, I suggest to handle some of your regular tasks more autonomously. I can update stock projections based on sales forecast, so operations teams can anticipate demand and avoid shortages. Would you like me to take care of this for you?

12:11

Yes, that sounds like a great plan. Please do.

12:11

MC

Ask your question

AI agents can make mistakes. Verify important information.

Trusted Agent Access

×

+

←

→

↺

f0faa4bda7574bf3ad3f03b579ac8aa8

☆

↓

Incognito (2)

⋮

L'Oréal

AI Agent

+

New chat

My agent

↺

Chat history

PoA dashboard

Mark Chan

COO

you like me to take care of this for you.

12:14

Yes, that sounds like a great plan. Please do.

12:14

MC

✦

Here is the proposed digital power of attorney.

12:14

📄

Power of Attorney Document

Optimize stock by updating inventory forecast based on sales forecast, so that operational teams can anticipate demand and avoid stockouts.

• Frequency of update: Twice a month

• Tolerance in stock: 3%

• Sales pipeline maturity: 7-10

12:14

Ask your question

User Config

AI agents can make mistakes. Verify important information.

Trusted Agent Access

×

+

←

→

↺

f0faa4bda7574bf3ad3f03b579ac8aa8

☆

↓

Incognito (2)

⋮

L'Oréal

AI Agent

+

New chat

My agent

Chat history

PoA dashboard

User Config

Mark Chan

COO



12:18

Here is the proposed digital power of attorney.

12:18

Power of Attorney Document

Optimize stock by updating inventory forecast based on sales forecast, so that operational teams can anticipate demand and avoid stockouts.

• Frequency of update: Twice a month

• Tolerance in stock: 3%

• Sales pipeline maturity: 7-10

12:18

Make it once a month.

12:18

MC

Ask your question

AI agents can make mistakes. Verify important information.

Trusted Agent Access

×

+

←

→

↺

f0faa4bda7574bf3ad3f03b579ac8aa8-

☆

↓

Incognito (2)

⋮

L'Oréal

AI Agent

+

New chat

My agent

↺

Chat history

PoA dashboard

Mark Chan

COO



• Sales pipeline maturity: 7-10

12:21

Make it once a month.

12:21

Here is the updated proposed digital power of attorney.

12:21

Power of Attorney Document

Optimize stock by updating inventory forecast based on sales forecast, so that operational teams can anticipate demand and avoid stockouts.

• Frequency of update: Once a month

• Tolerance in stock: 3%

• Sales pipeline maturity: 7-10

12:21

Ask your question

AI agents can make mistakes. Verify important information.

Trusted Agent Access

×

+

←

→

↺

f0faa4bda7574bf3ad3f03b579ac8aa8

☆

↓

Incognito (2)

⋮

L'Oréal

AI Agent

+

New chat

My agent

🕒

Chat history

📁

PoA dashboard

Mark Chan

COO



12:24

Power of Attorney Document

Optimize stock by updating inventory forecast based on sales forecast, so that operational teams can anticipate demand and avoid stockouts.

• Frequency of update: Once a month

• Tolerance in stock: 3%

• Sales pipeline maturity: 7-10

12:24

Perfect. Okay for this mandate.

12:24

MC

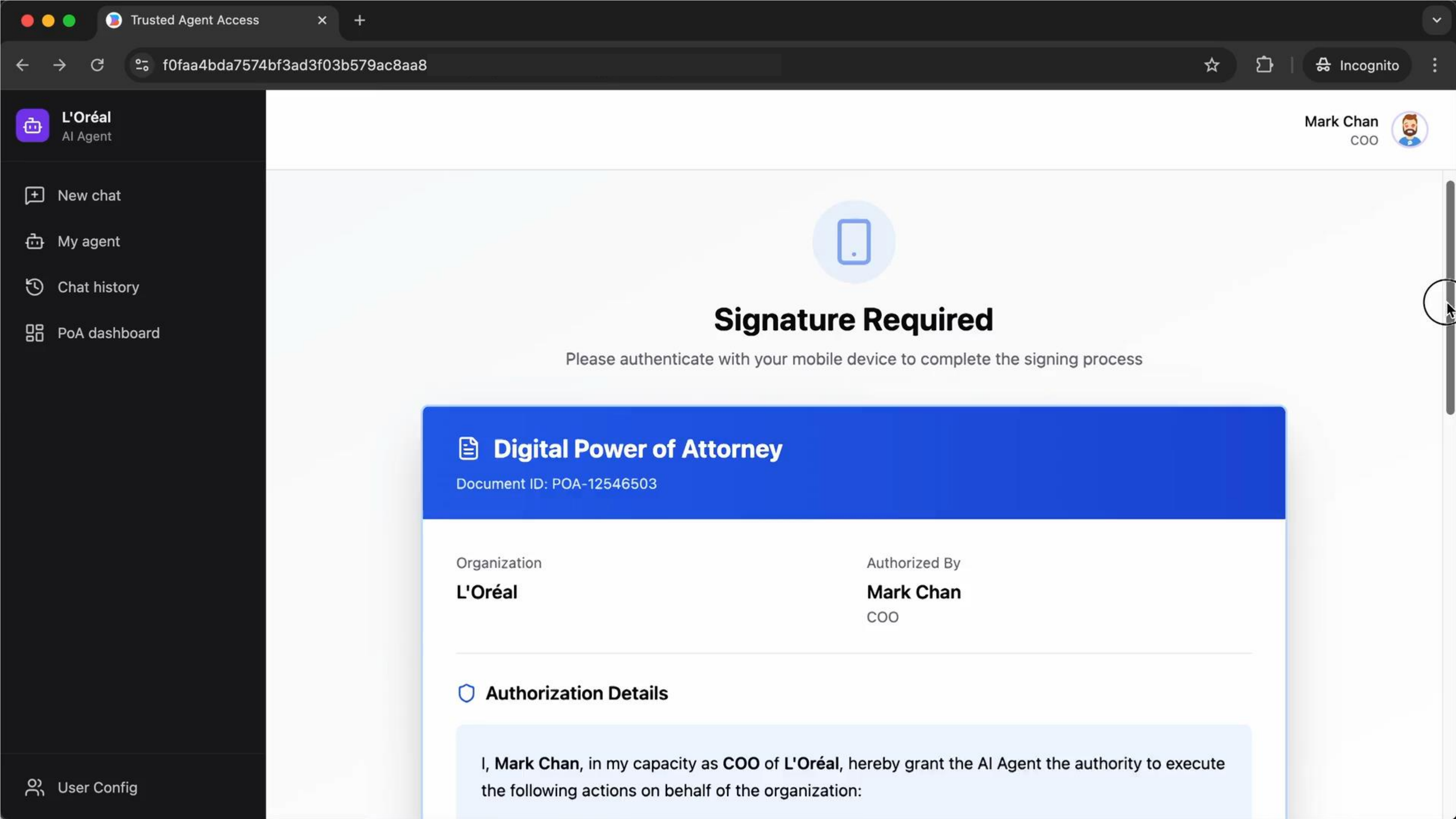
✦

Please follow the instructions in the next step.

12:24

Prepare this mandate for my digital signature

AI agents can make mistakes. Verify important information.



L'Oréal
AI Agent



New chat



My agent



Chat history



PoA dashboard



User Config

Mark Chan
COO



Signature Required

Please authenticate with your mobile device to complete the signing process



Digital Power of Attorney

Document ID: POA-12546503

Organization

L'Oréal

Authorized By

Mark Chan

COO



Authorization Details

I, Mark Chan, in my capacity as COO of L'Oréal, hereby grant the AI Agent the authority to execute the following actions on behalf of the organization:

Scan QR Code

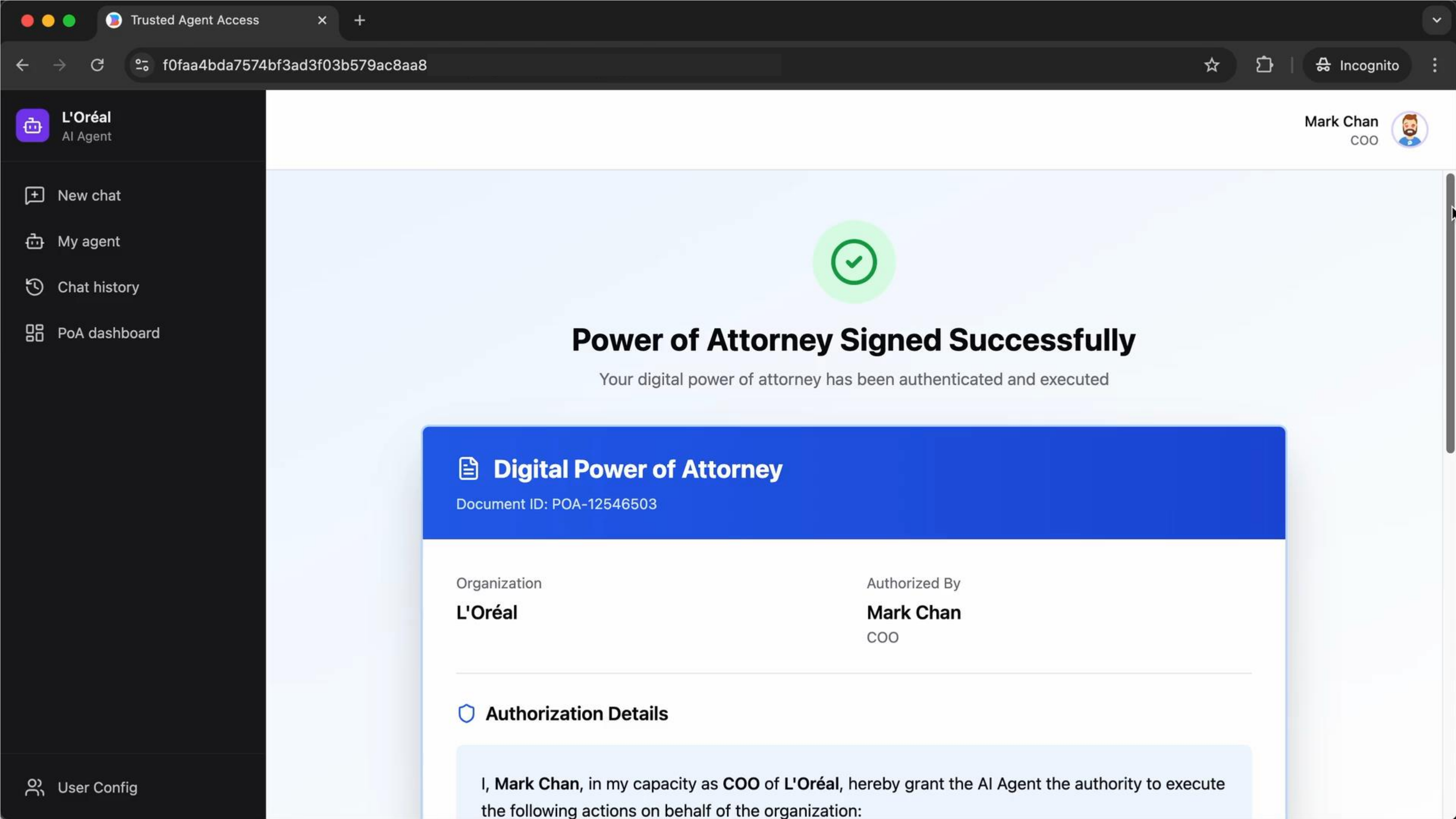
Position the QR code within the frame



 Tap to Scan

Scan the QR code to verify your identity

 Mark Chan 



L'Oréal
AI Agent



New chat



My agent



Chat history



PoA dashboard



User Config

Mark Chan
COO



Power of Attorney Signed Successfully

Your digital power of attorney has been authenticated and executed



Digital Power of Attorney

Document ID: POA-12546503

Organization

L'Oréal

Authorized By

Mark Chan

COO

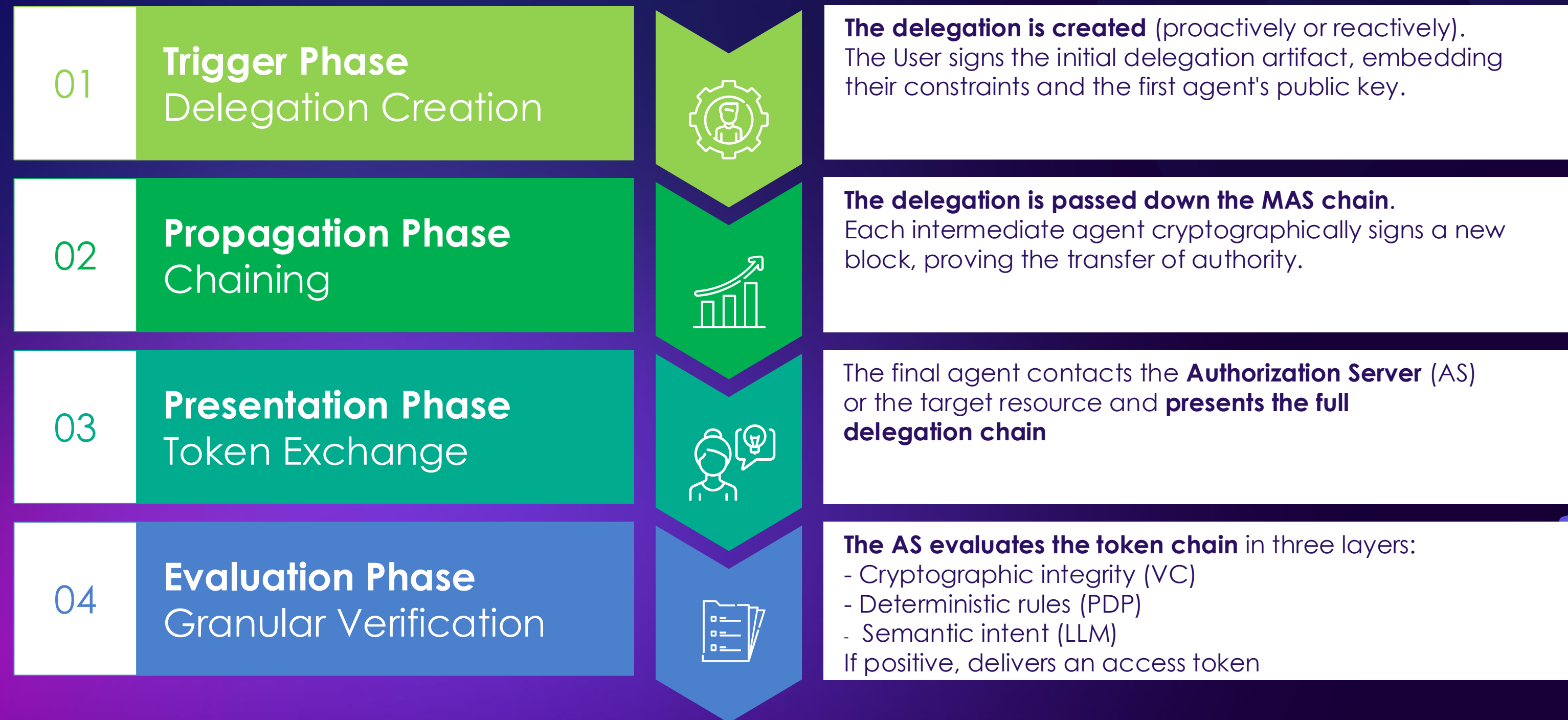


Authorization Details

I, **Mark Chan**, in my capacity as **COO** of **L'Oréal**, hereby grant the AI Agent the authority to execute the following actions on behalf of the organization:

Our Flow Proposal

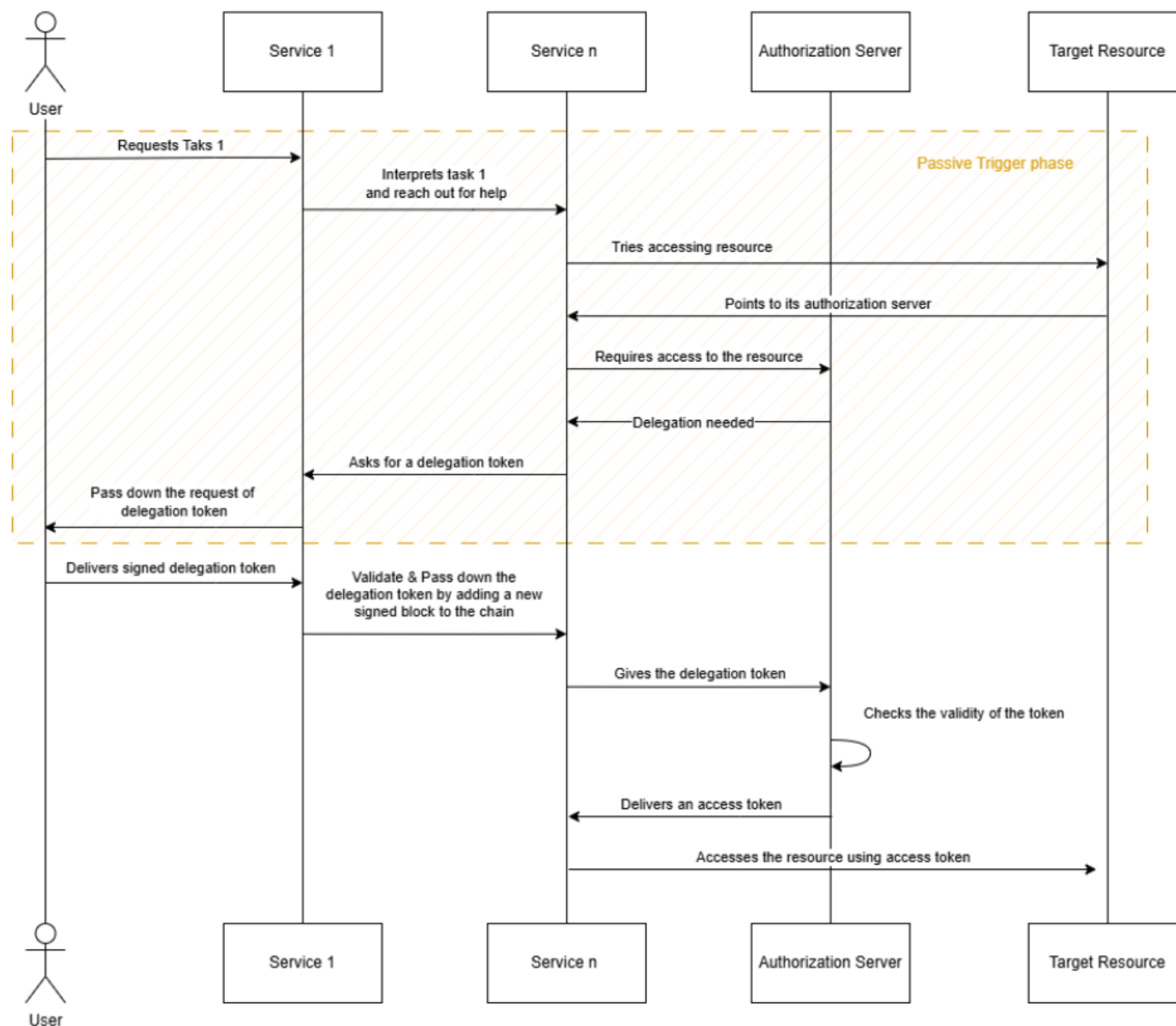
A New Protocol for The End-to-End Delegation Flow: From Trigger to Presentation



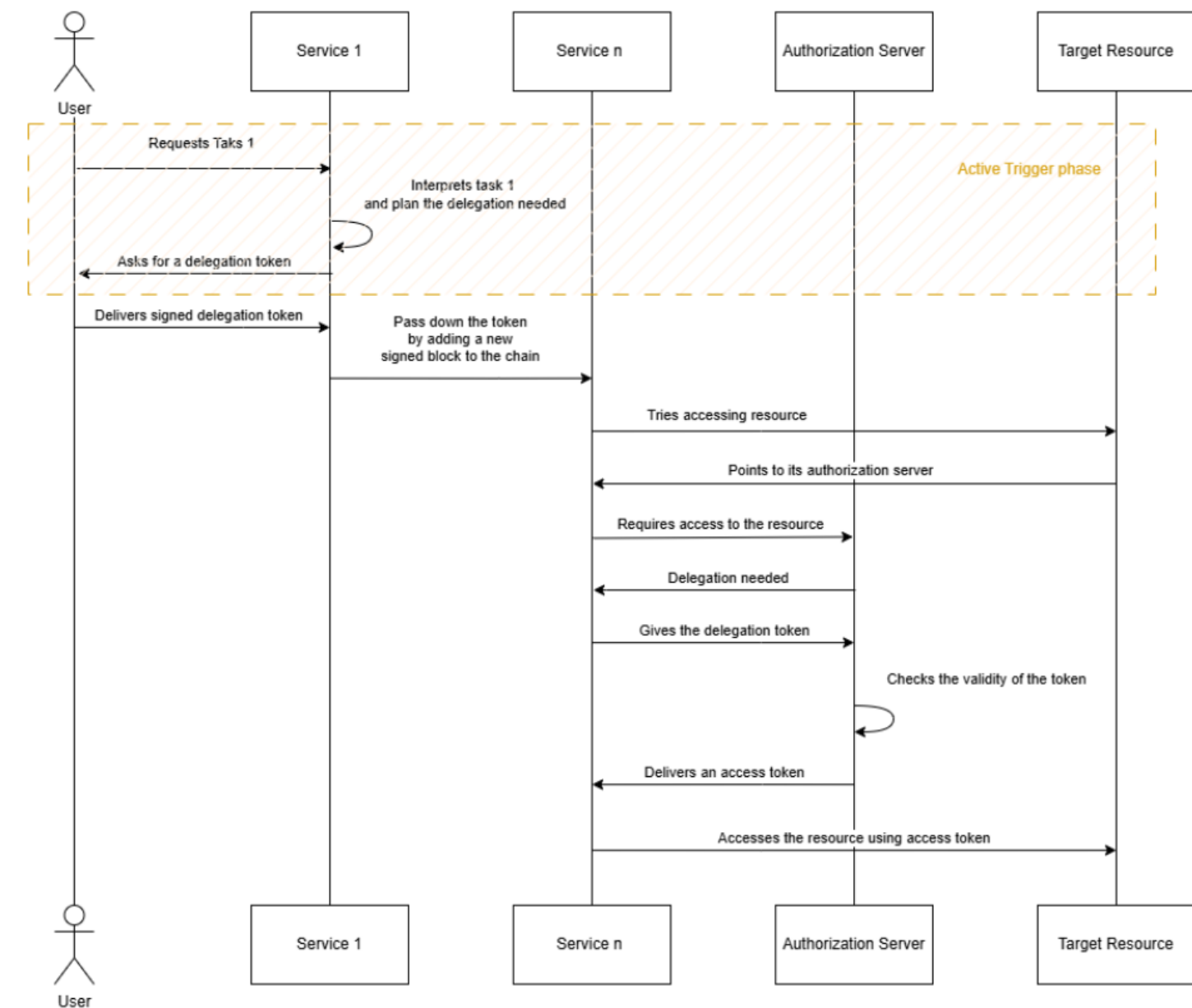
Delegation Triggers: Passive vs. Active Models

Downstream-initiated vs. upstream-anticipated authorization

Passive Trigger



Active Trigger



Autonomy Changes Everything



User defines *what*,
agent chooses *how*



Time delay between
intent and execution



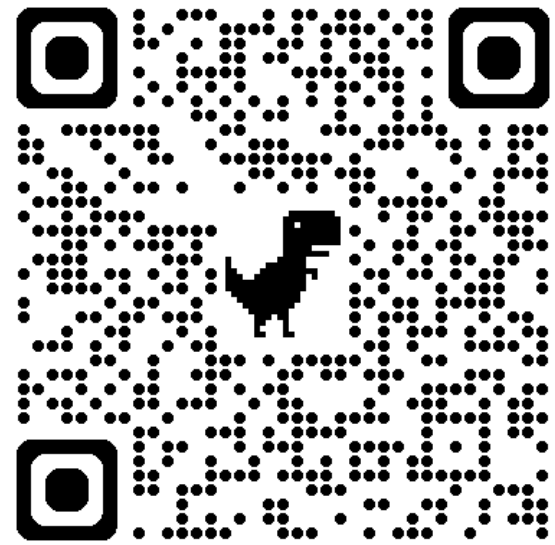
Agent defines
data access paths

Human intent is the anchor for trust



Contribute to the Paper

A New Protocol for The Delegation of
Human Intent in Agentic



<https://www.overleaf.com/project/698b05cf2a3cff501f939234>

Reach out and Share



ward.duchamps@thalesgroup.com

[linkedin.com/in/wardduchamps](https://www.linkedin.com/in/wardduchamps)

Let's Work
Together



Thank you



Ward Duchamps

ward.duchamps@thalesgroup.com

[linkedin.com/in/wardduchamps](https://www.linkedin.com/in/wardduchamps)