

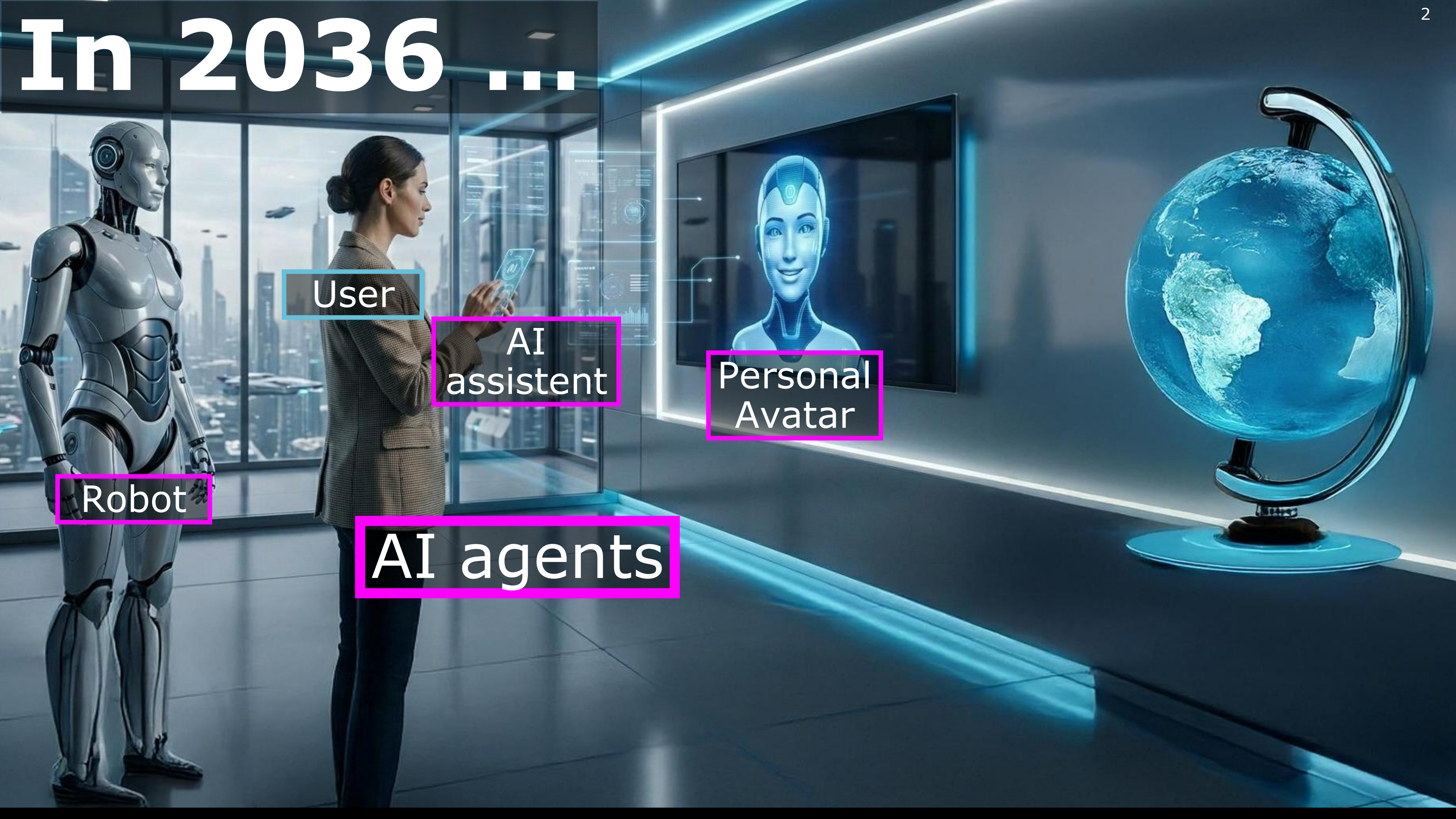
The MCP-I Standard

Pecha Kucha Presentation

Wiam Oulad Hadj Meftah, Eviden Digital Identity

In 2036 ...

2



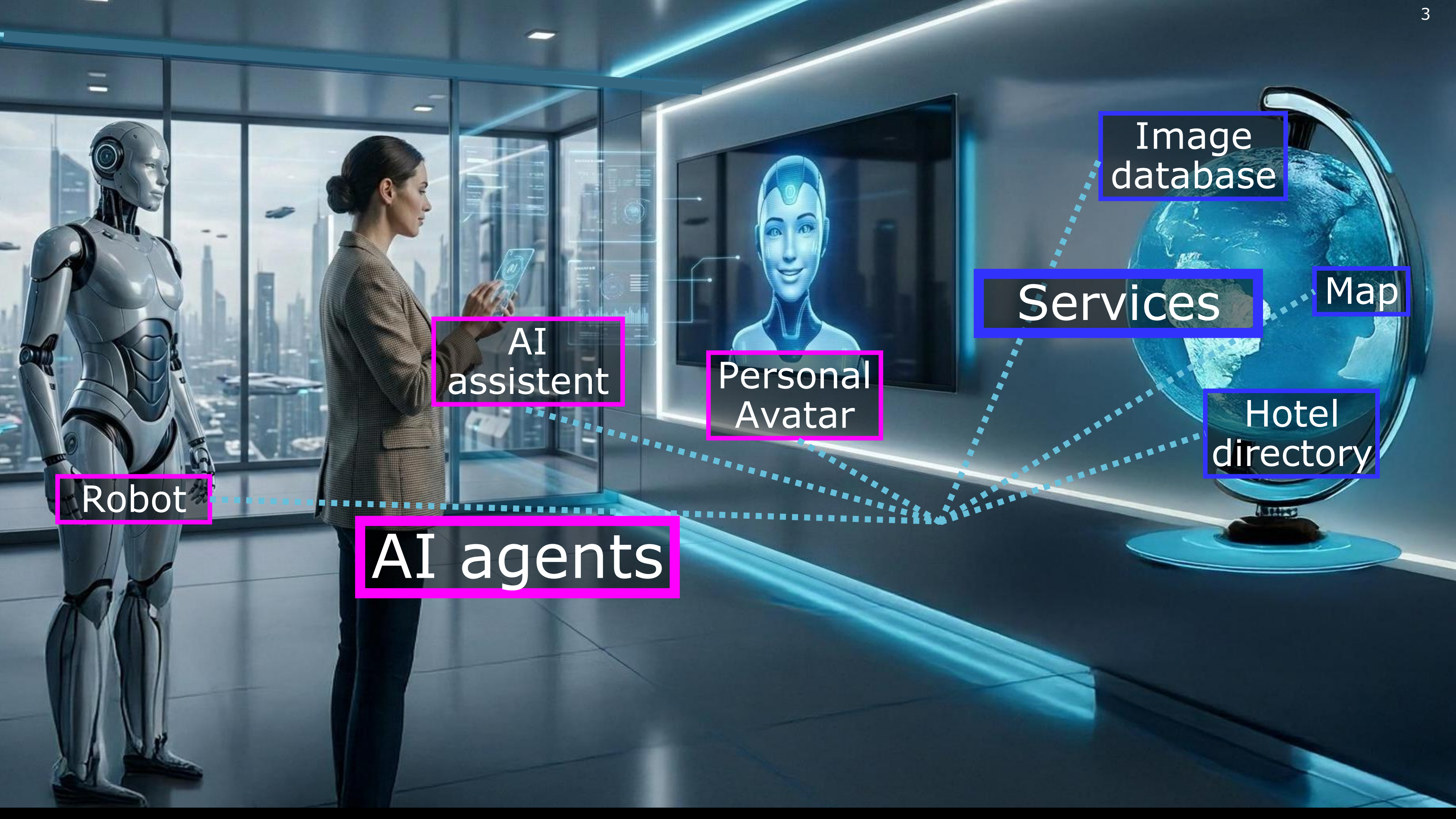
User

AI
assistant

Personal
Avatar

Robot

AI agents

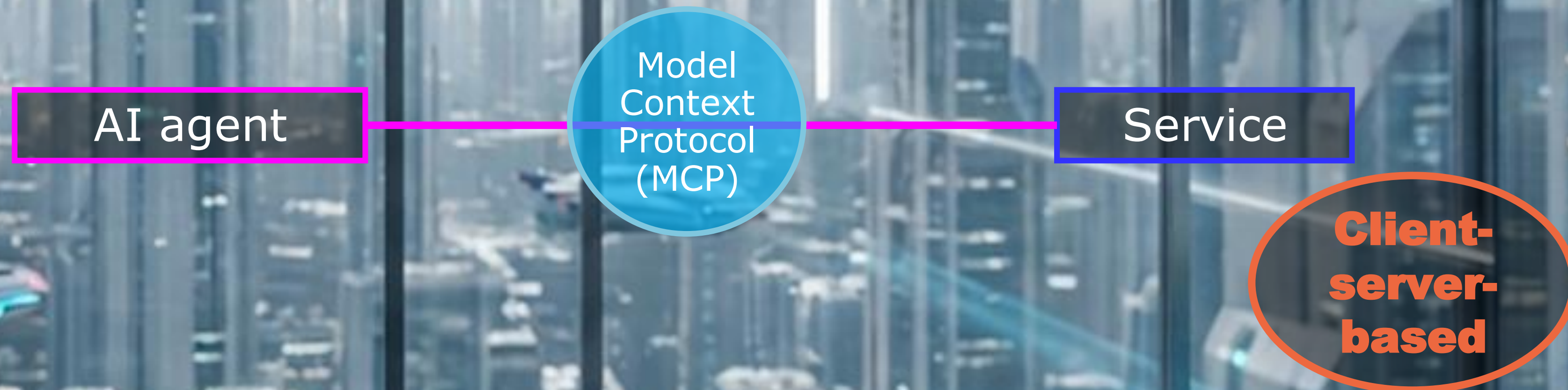




Model Context Protocol (MCP)

Introduced in 2024

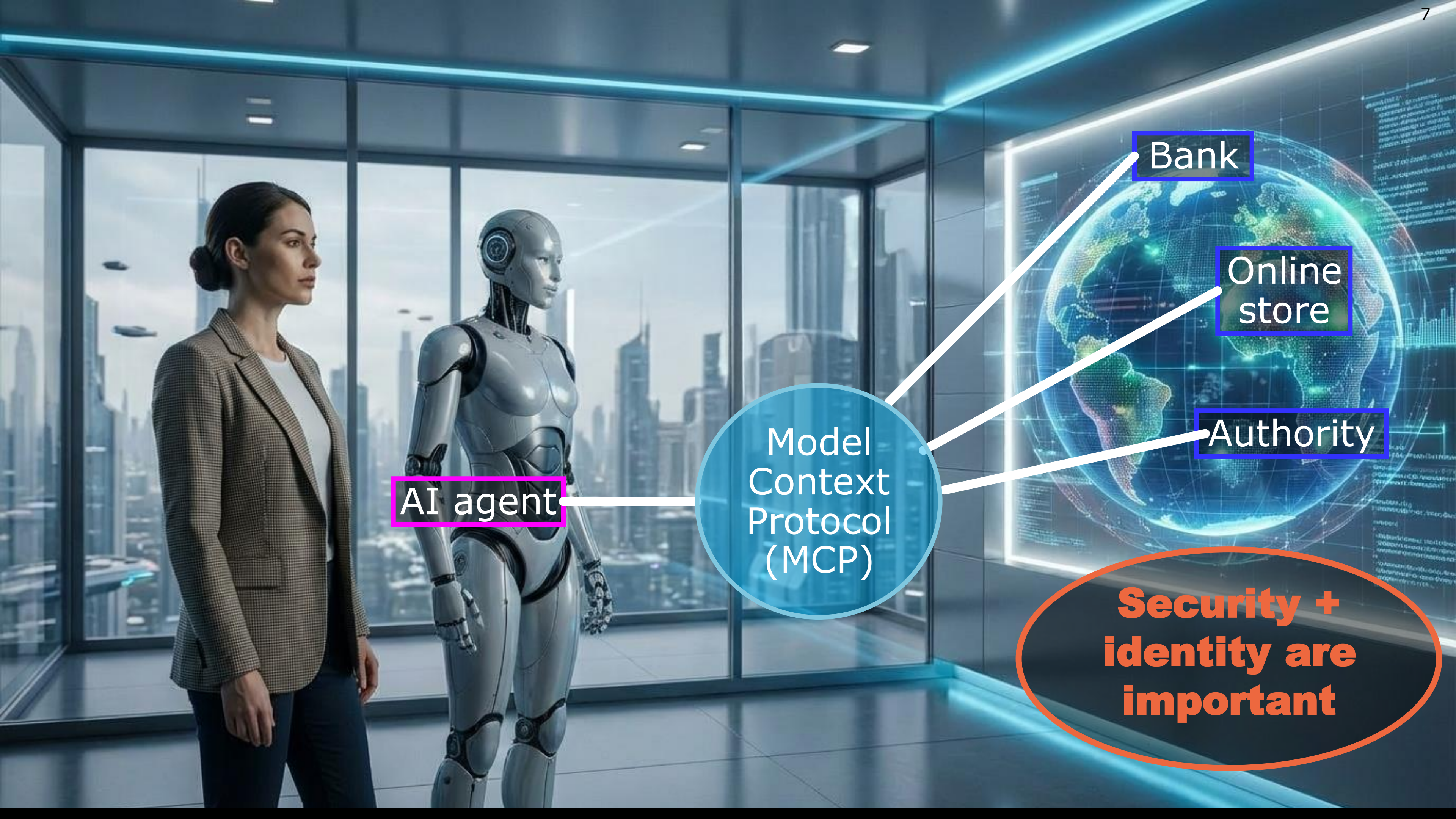
Standardizes communication between
AI agent and external service





**Security
Critical**

Avatar – Bank



Bank

Online
store

Authority

Model
Context
Protocol
(MCP)

AI agent

**Security +
identity are
important**

MCP-I

Model Context Protocol Identity

Extends MCP with cryptographic and other security mechanisms

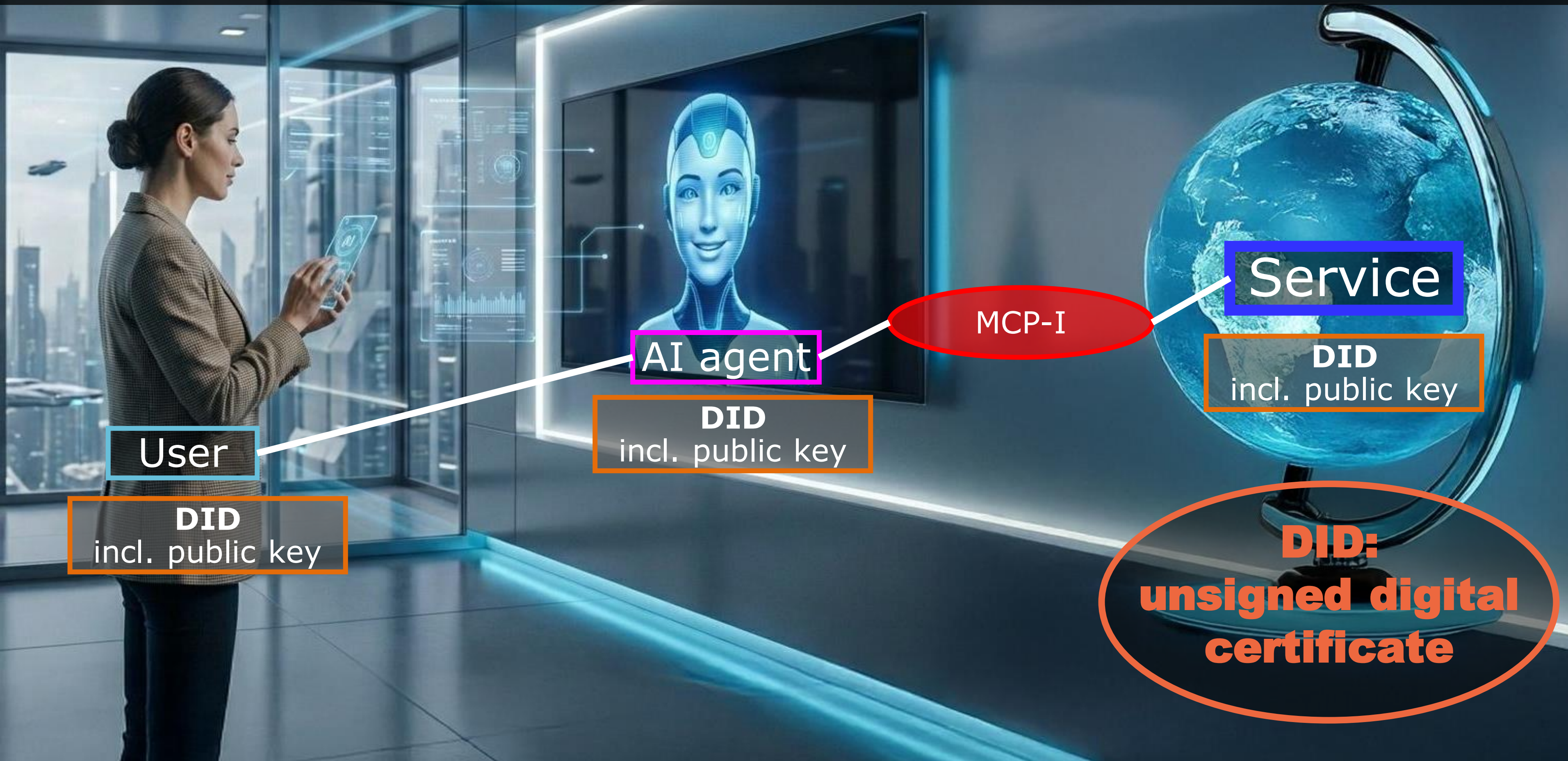
AI agent

MCP-I

Service

**Identity-
based**

Decentralized Identifier Document (DID)



Decentralized Identifier Document (DID) *Types*

DID:key *no trust anchor*

DID:web *Website as trust anchor*

DID:ion *Bitcoin as trust anchor*

DID:web

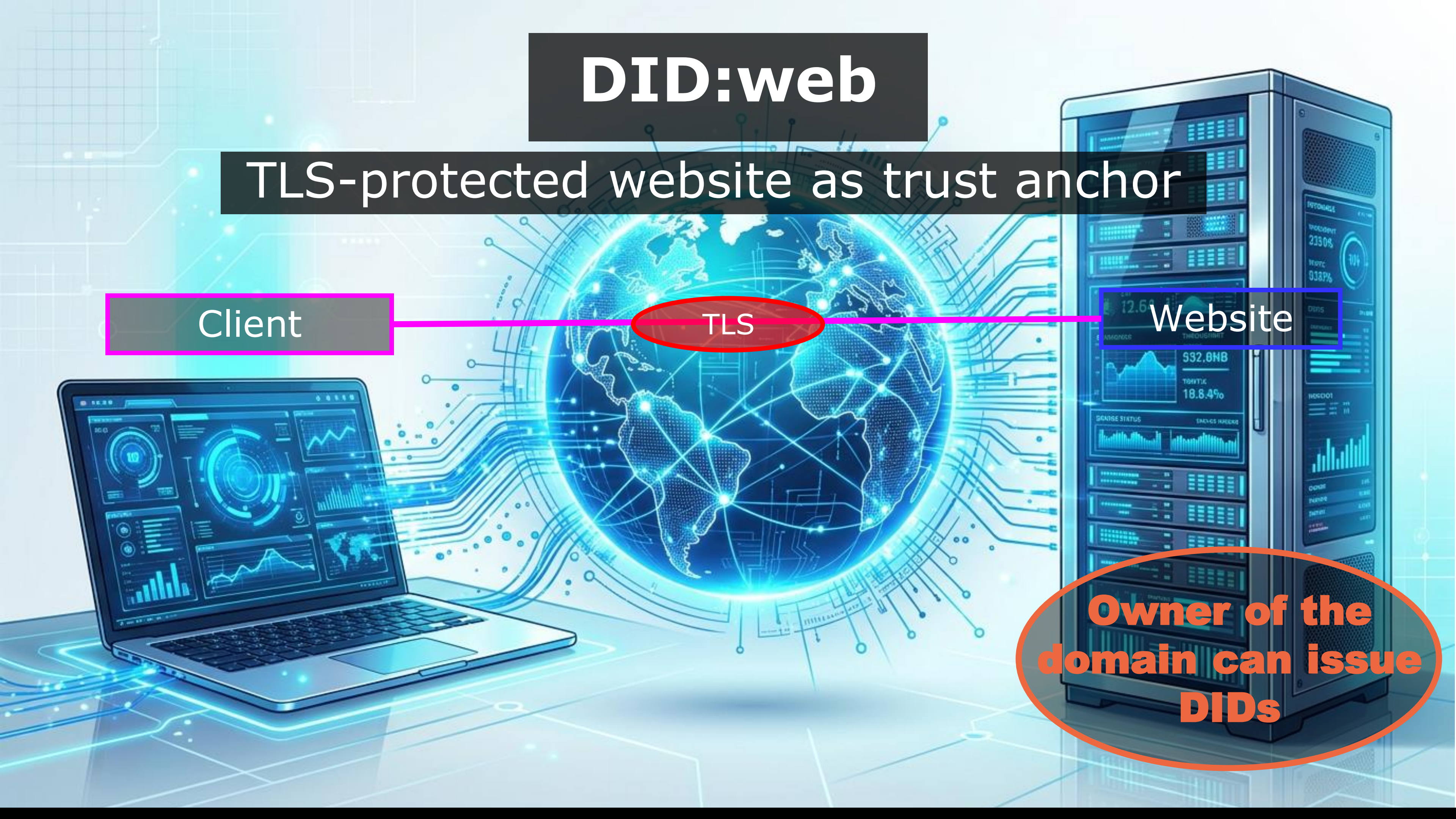
TLS-protected website as trust anchor

Client

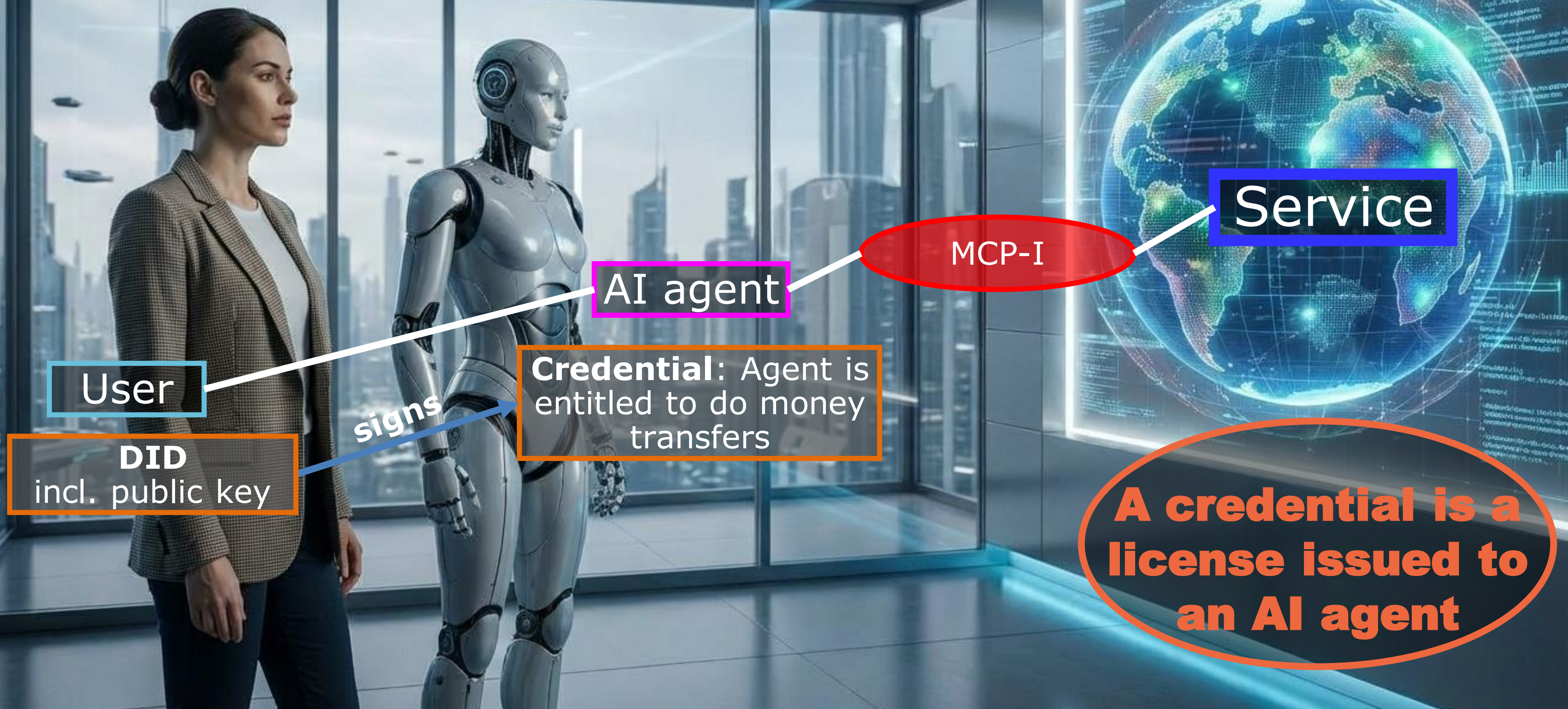
TLS

Website

**Owner of the
domain can issue
DIDs**



Credentials



Infrastructure Components

Delegation Service

Verifies credentials

DID Resolver

Resolves decentralized identifiers

Revocation Service

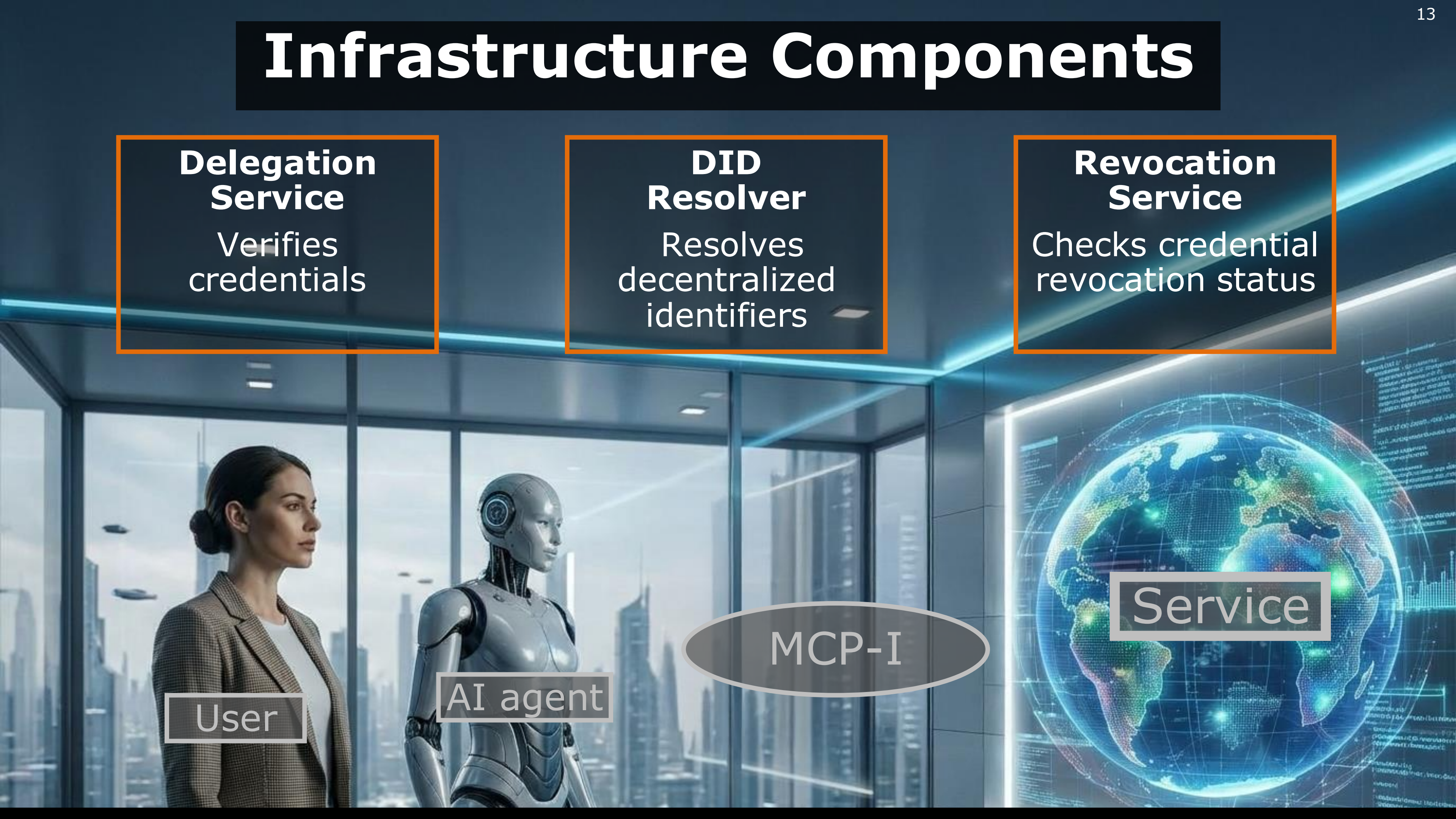
Checks credential revocation status

User

AI agent

MCP-I

Service



Non-crypto components

Reputation Service: Provides agent reputation information

Scoring based on:

- Conformance level
- Age of agent
- Number of past interactions
- Review scores and quantity

AI agent



Non-crypto components

Audit Service

Tracks identity, credential,
and delegation events



The role of PKI

User

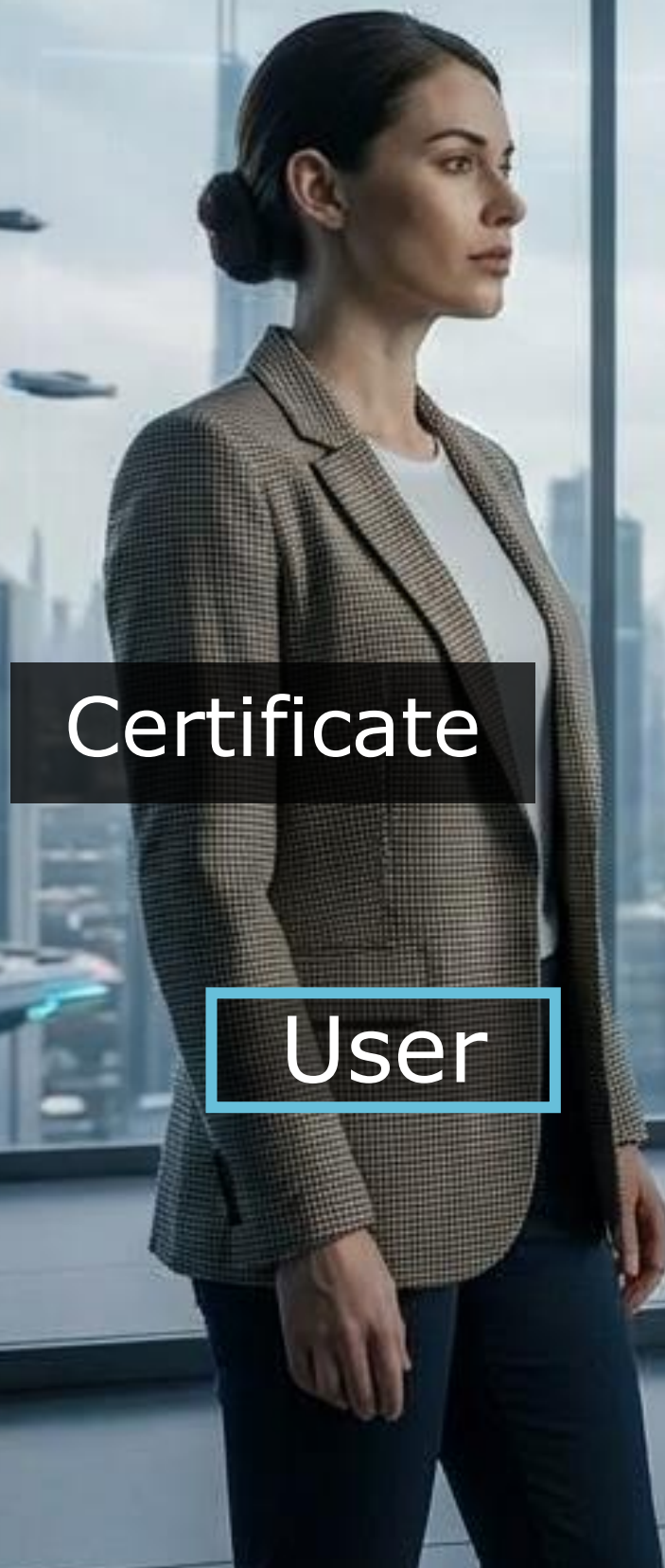
AI agent

MCP-I

Service

**Use of TLS 1.3 for
all communications
recommended**

The role of PKI



Certificate

User



Certificate

AI agent

MCP-I

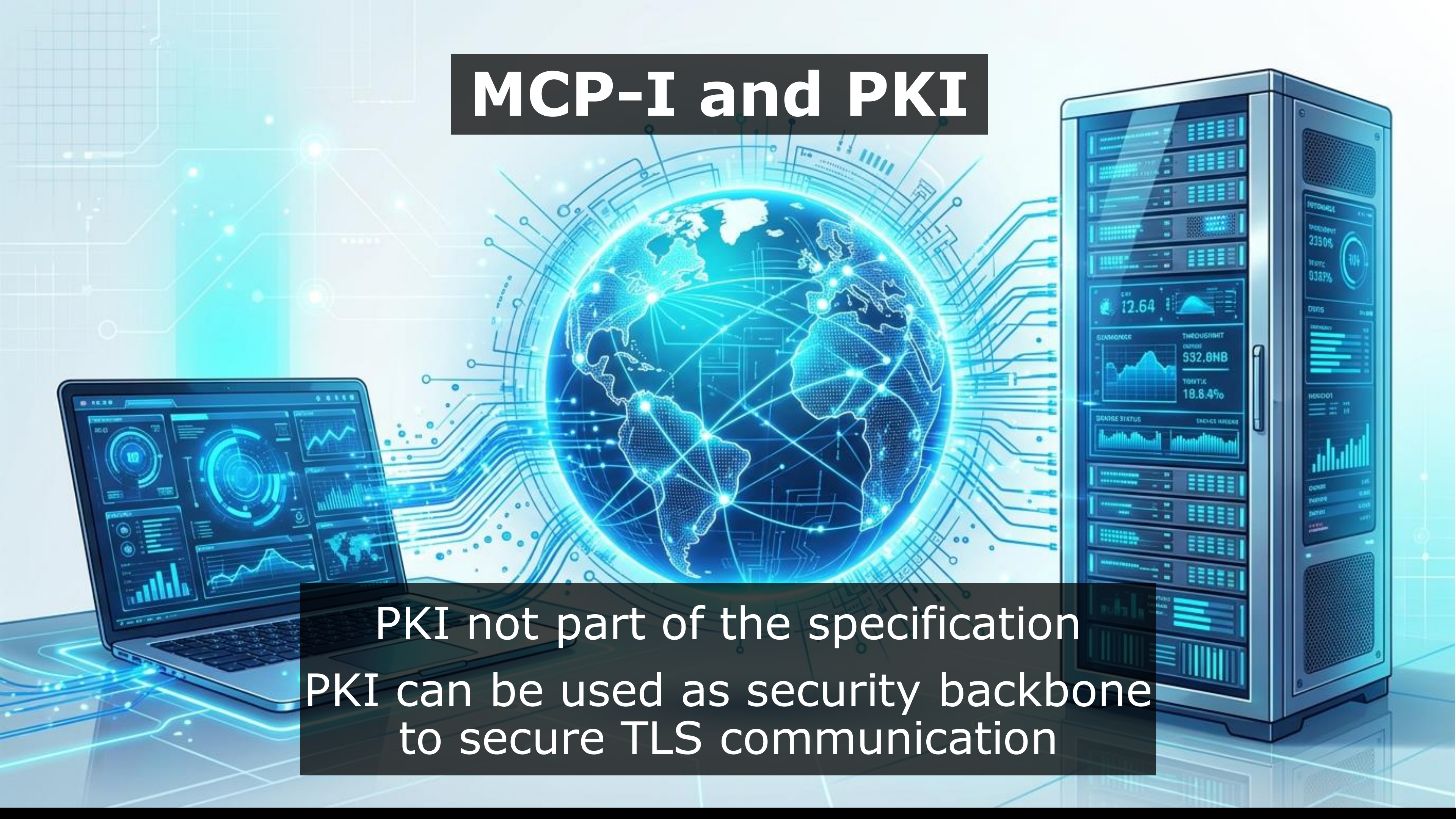
**Use of digital
certificates
recommended**



Service

Certificate

MCP-I and PKI



PKI not part of the specification
PKI can be used as security backbone
to secure TLS communication

Conclusion

MCP-I:

Framework for secure, identity-based communication in an AI-driven world

Combines crypto-based security with other security mechanisms

Conclusion

MCP-I:

PKI not part of the specification, but recommended to secure TLS communication

Conclusion

MCP-I:

Started in 2024

Still in an early stage

Might become important
in the near future

A futuristic scene set in a high-tech office with large windows overlooking a city. On the left, a sleek, silver humanoid robot stands. In the center, a woman in a brown blazer holds a transparent tablet displaying 'AI' and gestures with her other hand. On the right, a large, glowing digital globe features a woman's face and various data points. The word 'END' is prominently displayed in white over the globe.

END

Wiam Oulad Hadj Meftah, Eviden Digital Identity