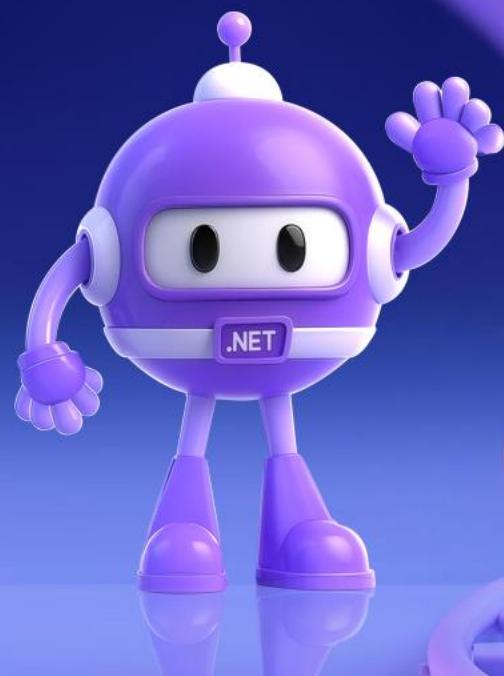


.NET Conf China 2025

改变世界 改变自己

2025 年 11 月 30 日 | 中国 上海



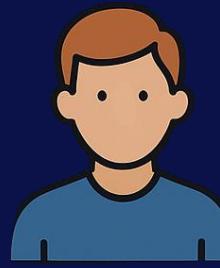
基于 .NET 的 AI Agent 授权体系



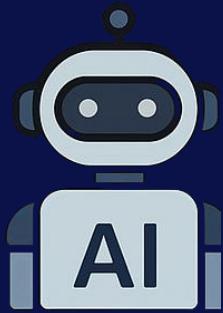
郭 强
Custouch 技术研发经理



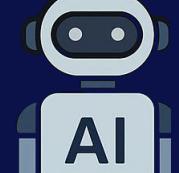
这是一个大问题



Human → Agent



Agent → Agent



Agent → Function



整体设计原则和架构



Zero Trust

默认不信任任何请求，所有访问都必须“重新证明自己”。

Context-aware

授权时，不只看“你是谁”，还看“你现在在什么环境下、在干什么”。

Least Privilege

只给完成当前任务所必需的最少权限，不多给一丝一毫。

权限模型怎么选

通过“角色”来管理权限。用户属于角色，角色拥有权限。

使用“属性（Attributes）”来决定是否授权。

RBAC
基于角色的访问控制

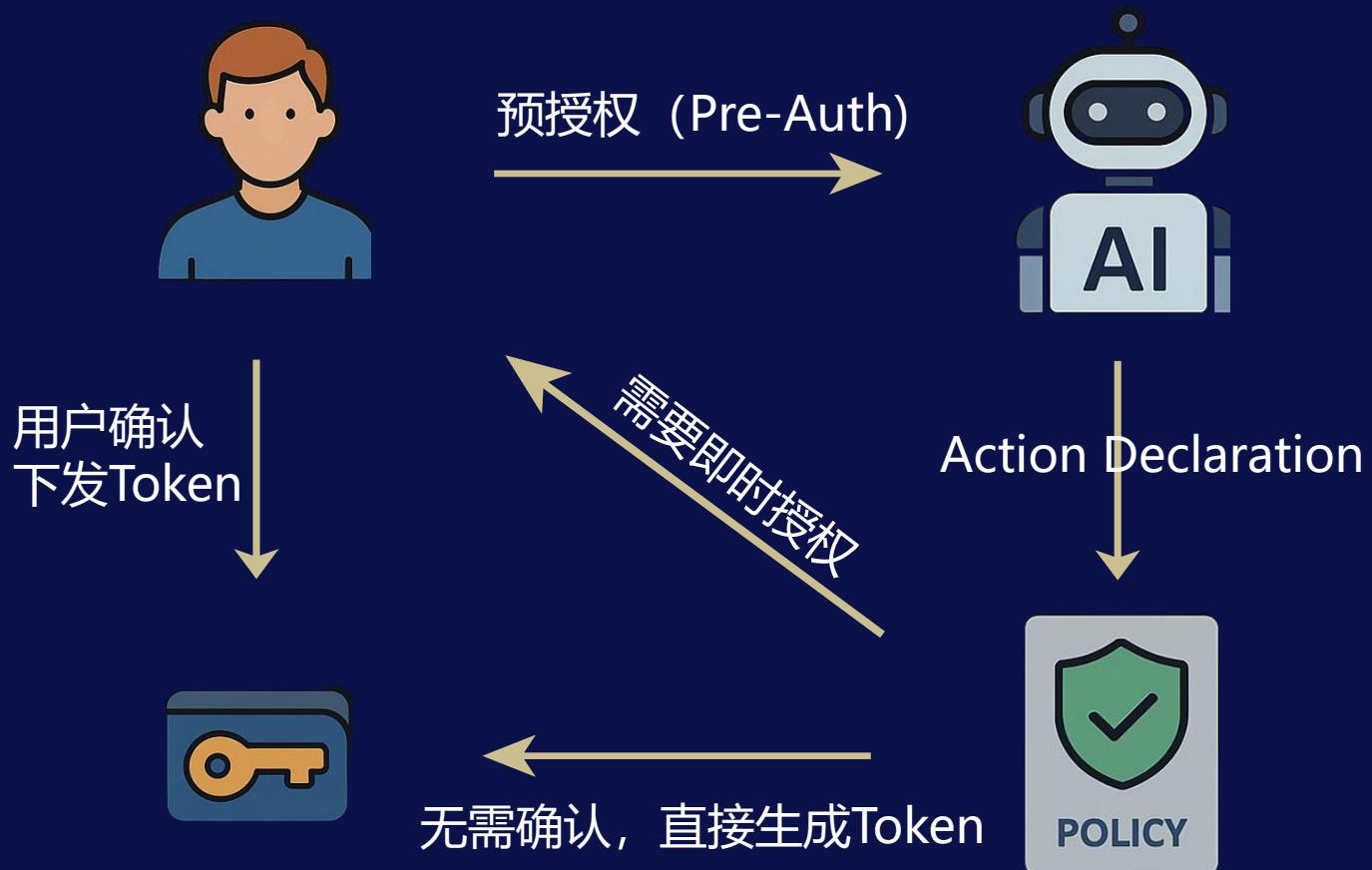
ABAC
基于属性的访问控制

PBAC
基于策略的访问控制



利用统一的策略（Policy）引擎，根据请求上下文做出动态授权决策。

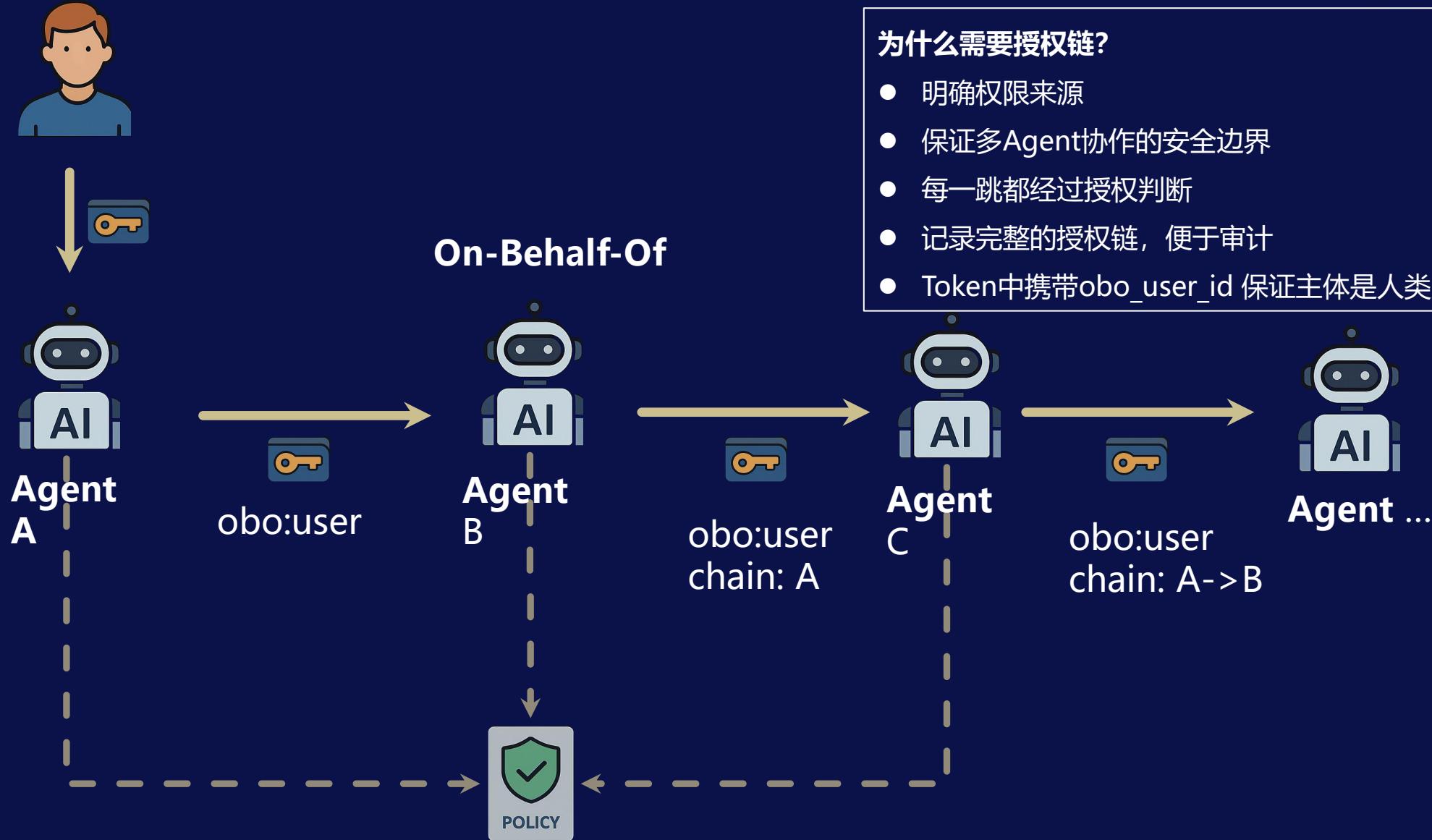
谁授权给谁?



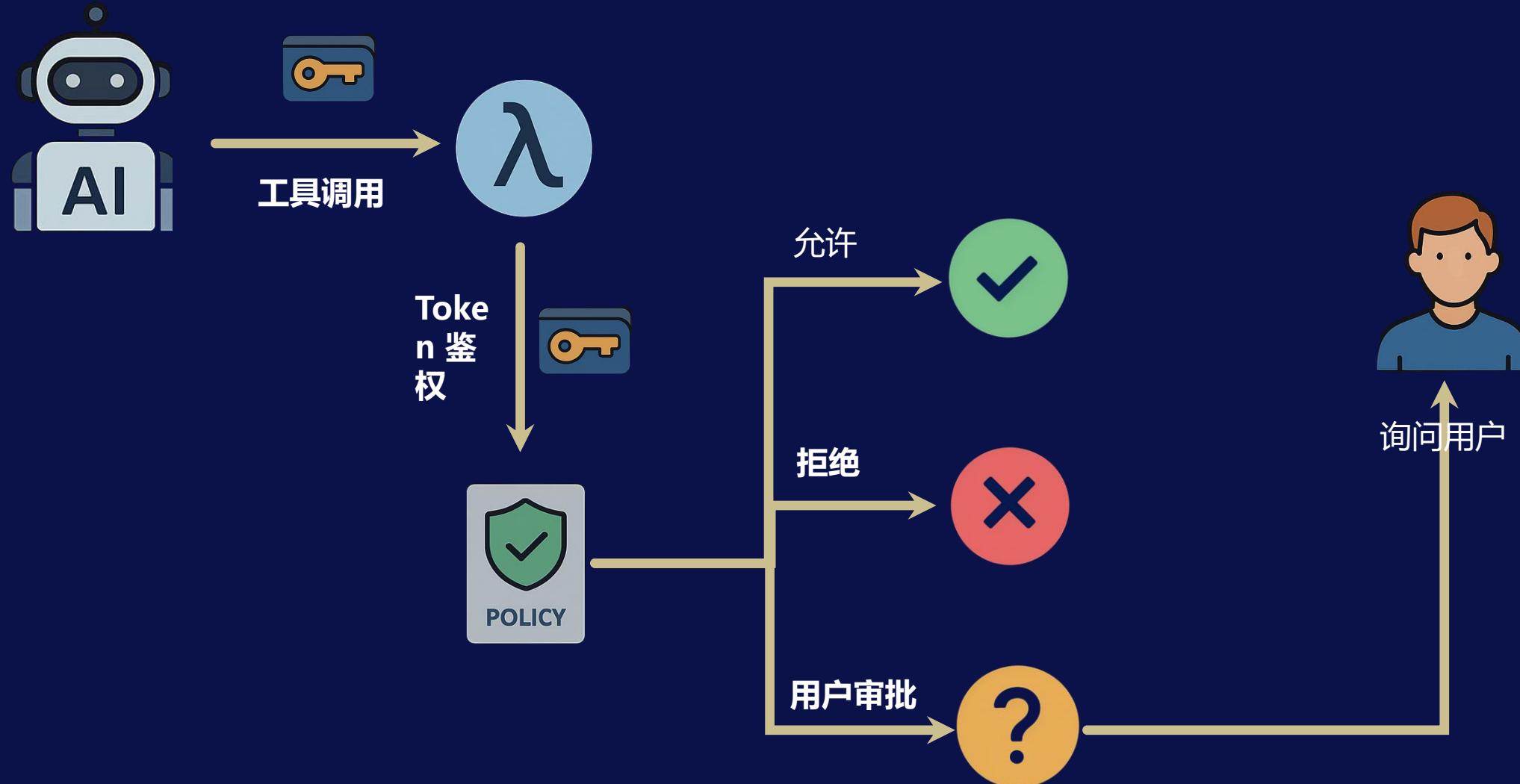
预授权 (Pre-Auth)	即时授权 (Just In Time)
长期有效, 直至撤销	实时询问、逐次确认
定义Agent的能力边界	高风险动作必须用户确认 (审批/授权)
适用于低风险动作	用于高风险动作

- 检查预授权
- 评估action/reason
- 资源级别判断

权限如何委托?

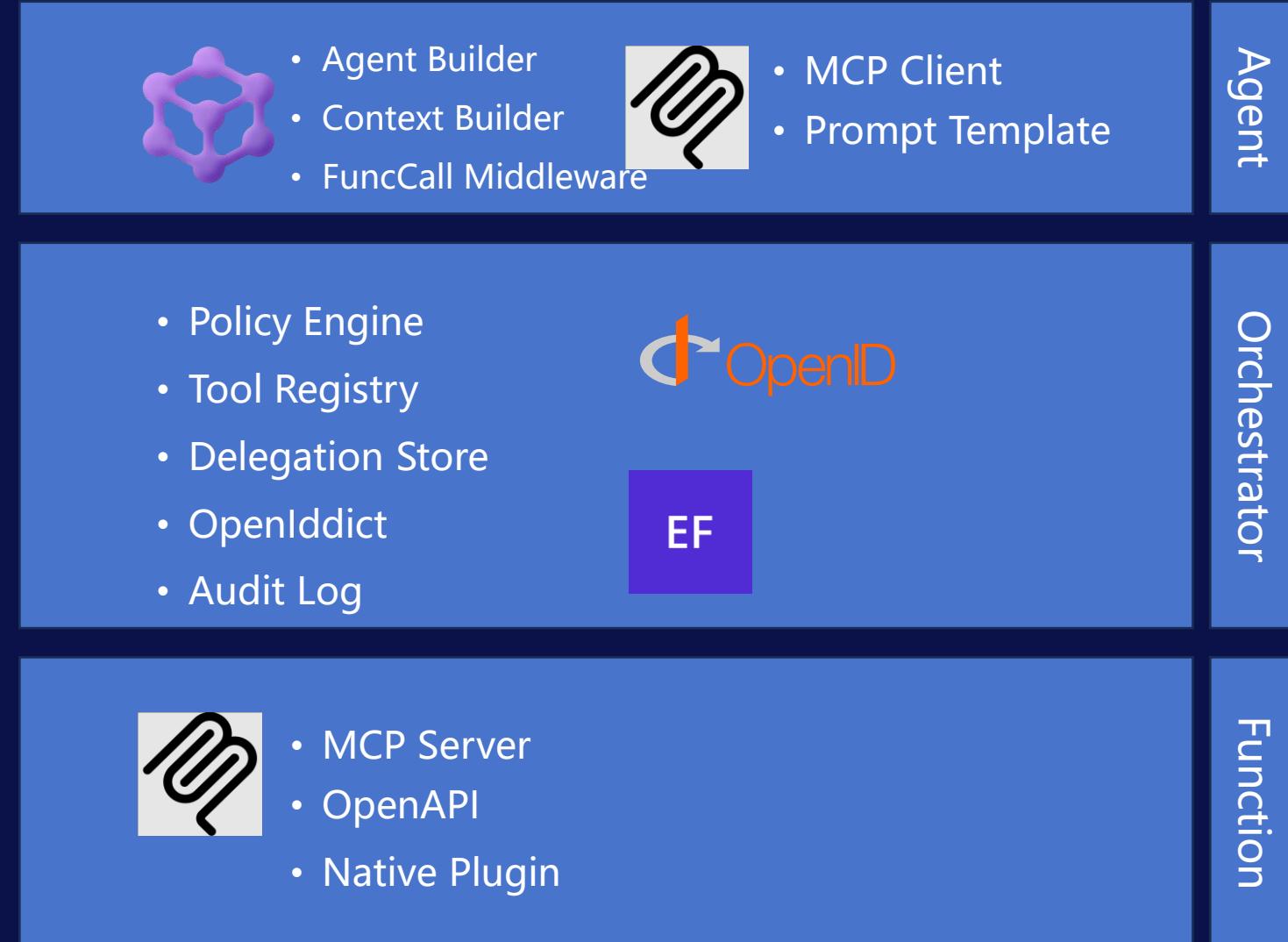


工具调用如何管控?

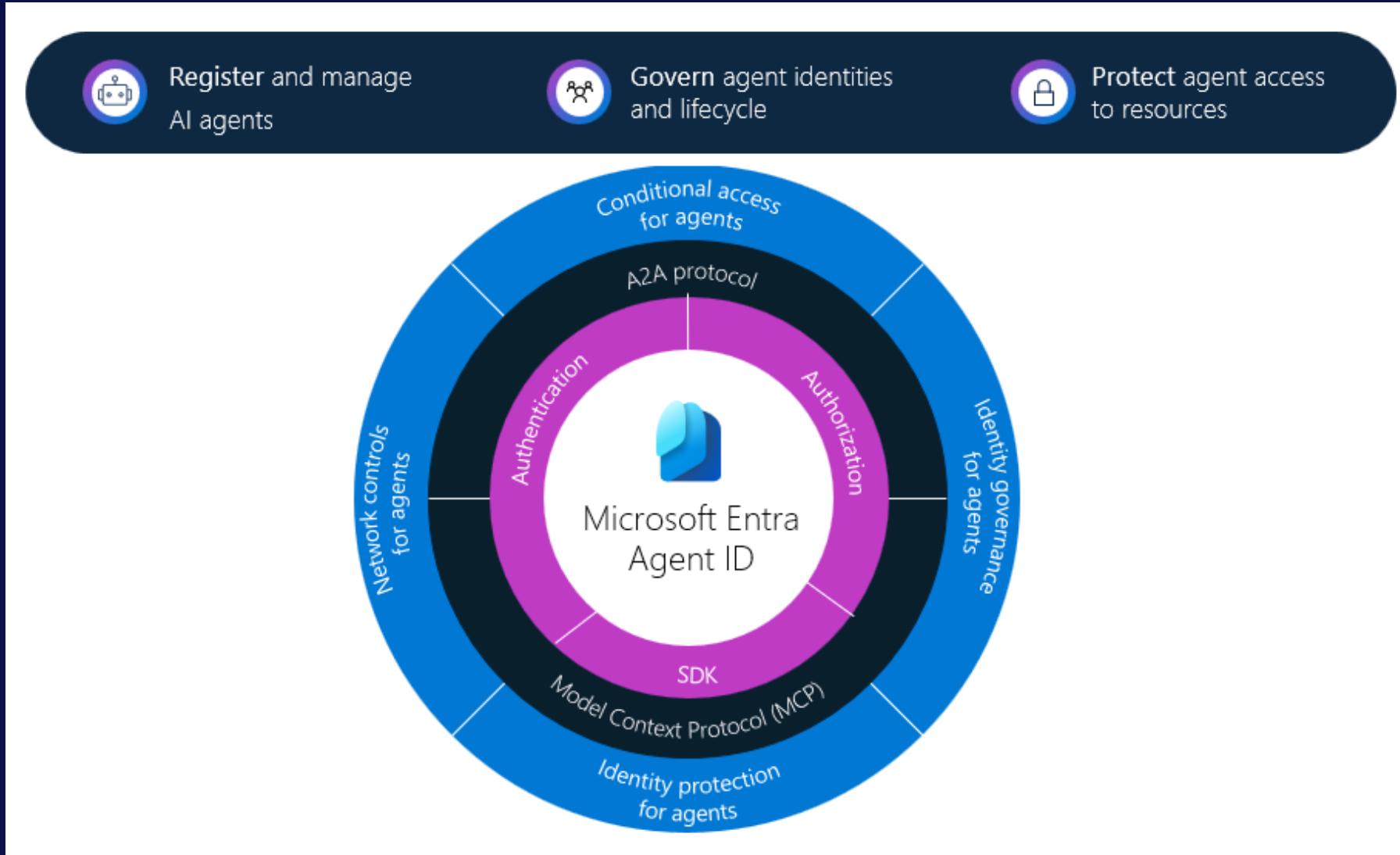




基于.NET 的 Agent 授权架构



Microsoft Entra Agent ID



THANK YOU