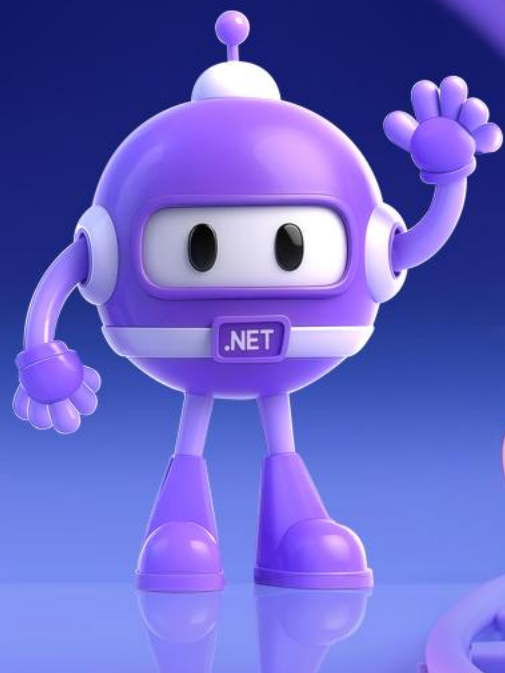


# .NET Conf China 2025

改变世界 改变自己

2025 年 11 月 30 日 | 中国 上海



.NET Conf China 2025

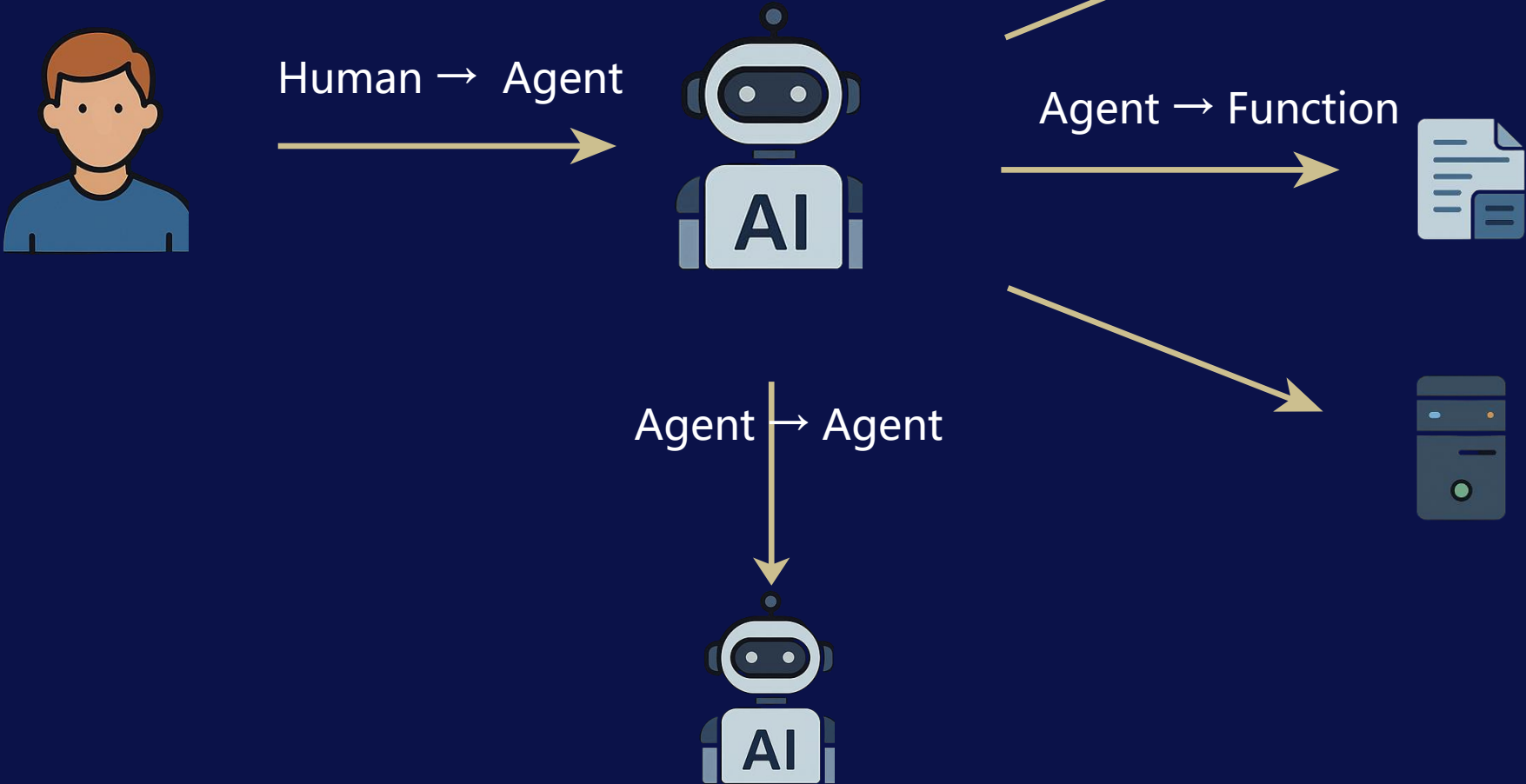
改变世界 改变自己

# 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



# 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。

RBAC  
基于角色的访问控制

使用“属性 (Attributes)”来决定是否授权。

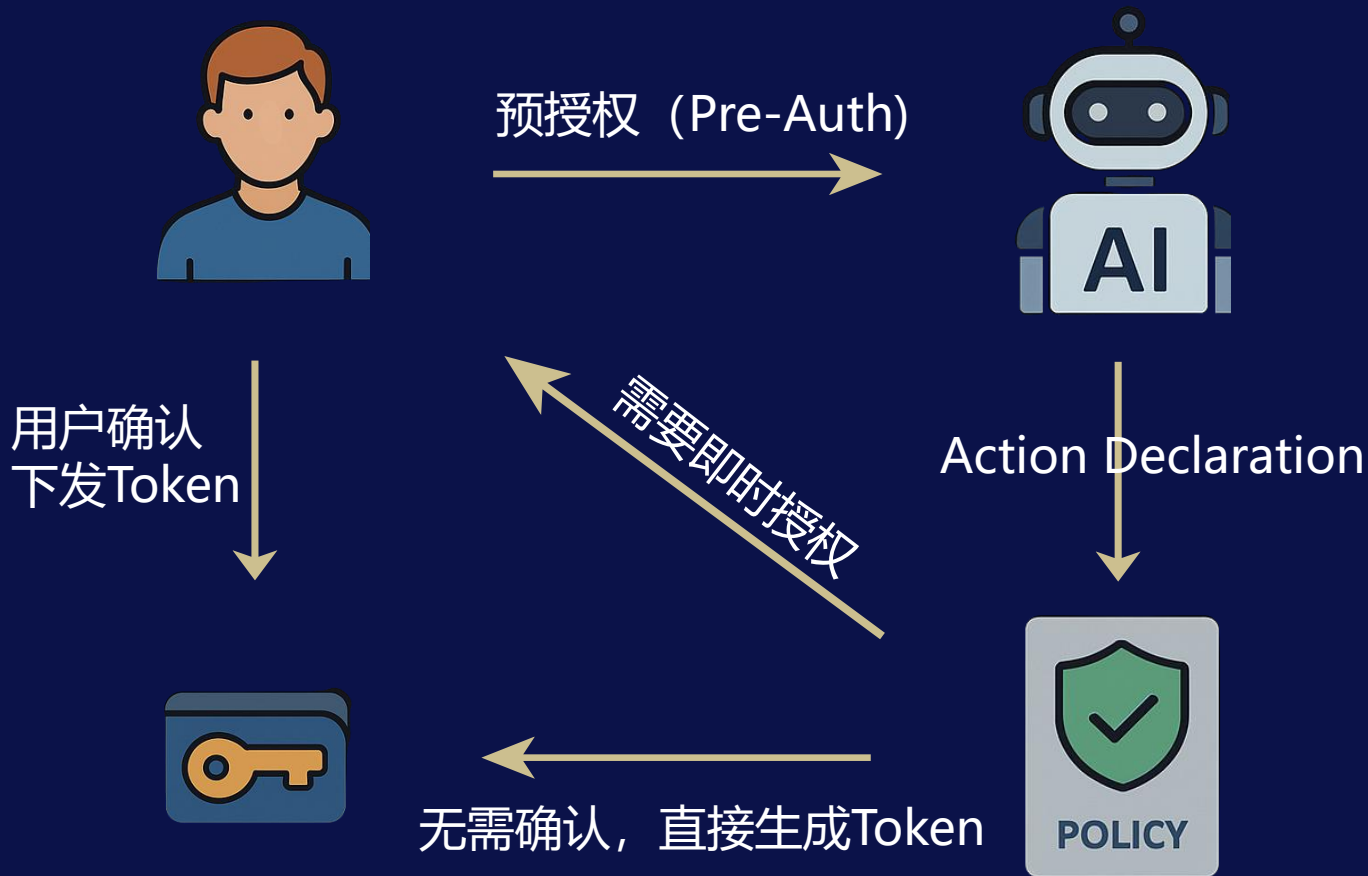
ABAC  
基于属性的访问控制

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。



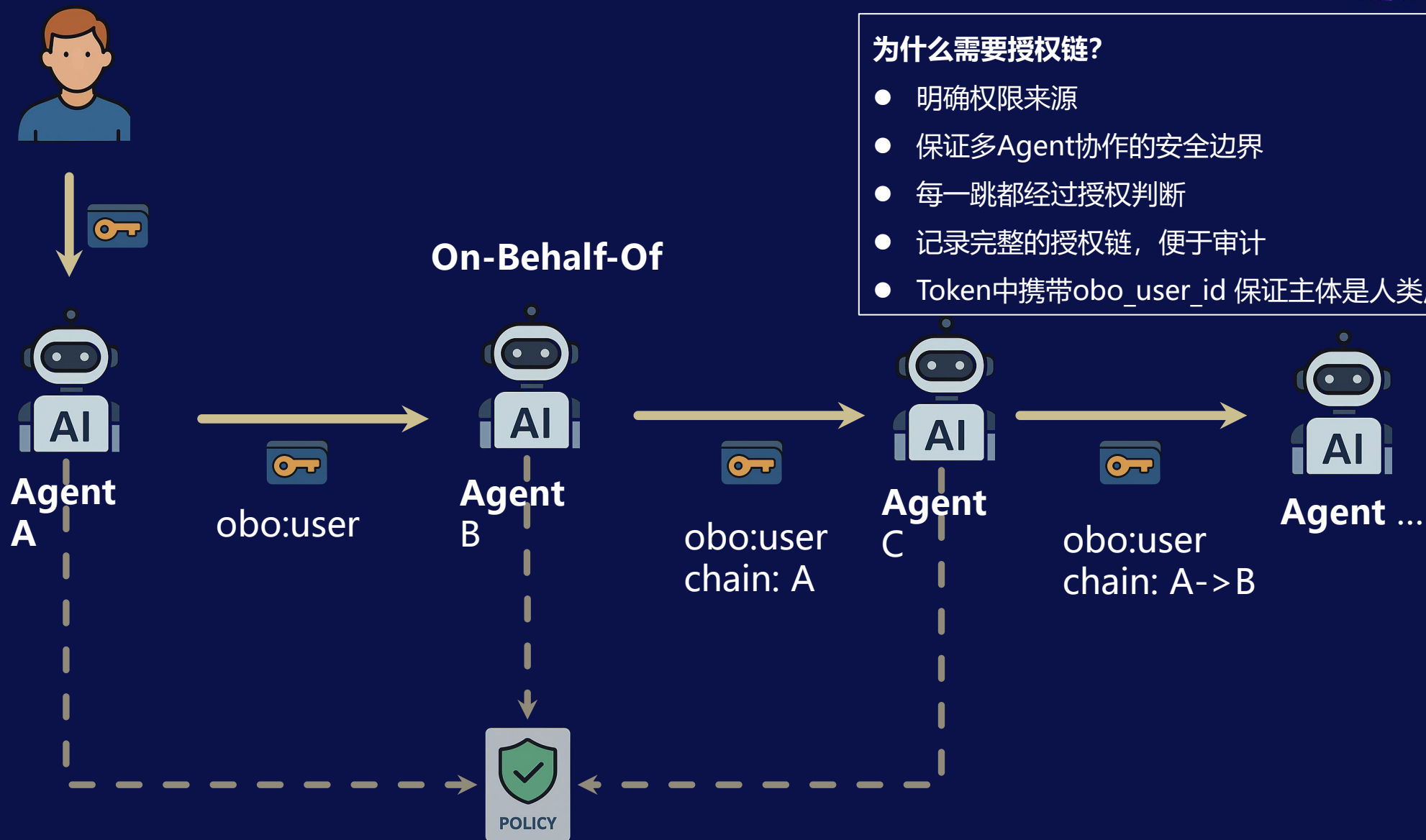
# 谁授权给谁?



- 检查预授权
- 评估action/reason
- 资源级别判断

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

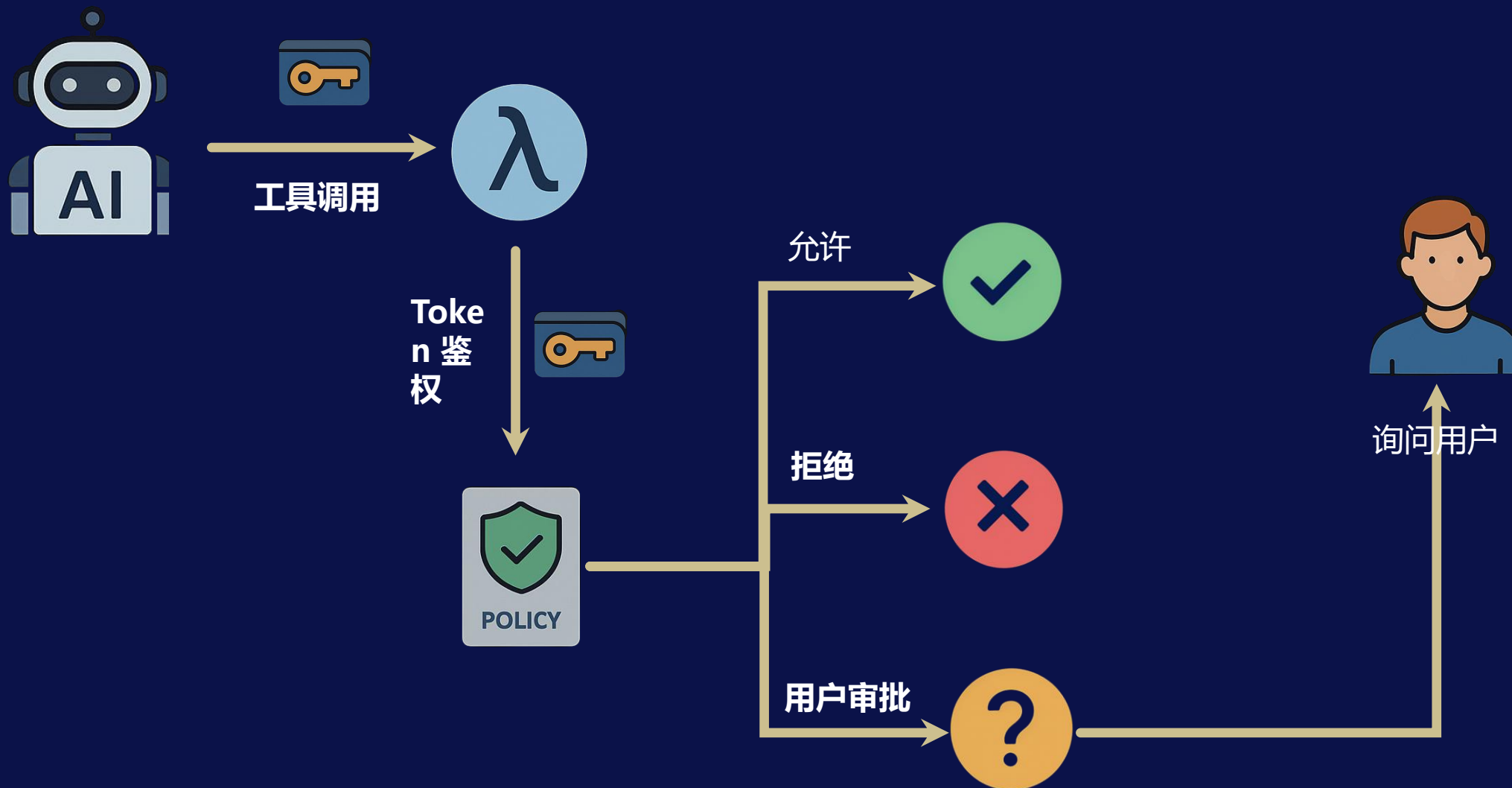
## 权限如何委托?



### 为什么需要授权链?






- 明确权限来源
- 保证多Agent协作的安全边界
- 每一跳都经过授权判断
- 记录完整的授权链, 便于审计
- Token中携带obo\_user\_id 保证主体是人类用户

## 工具调用如何管控?

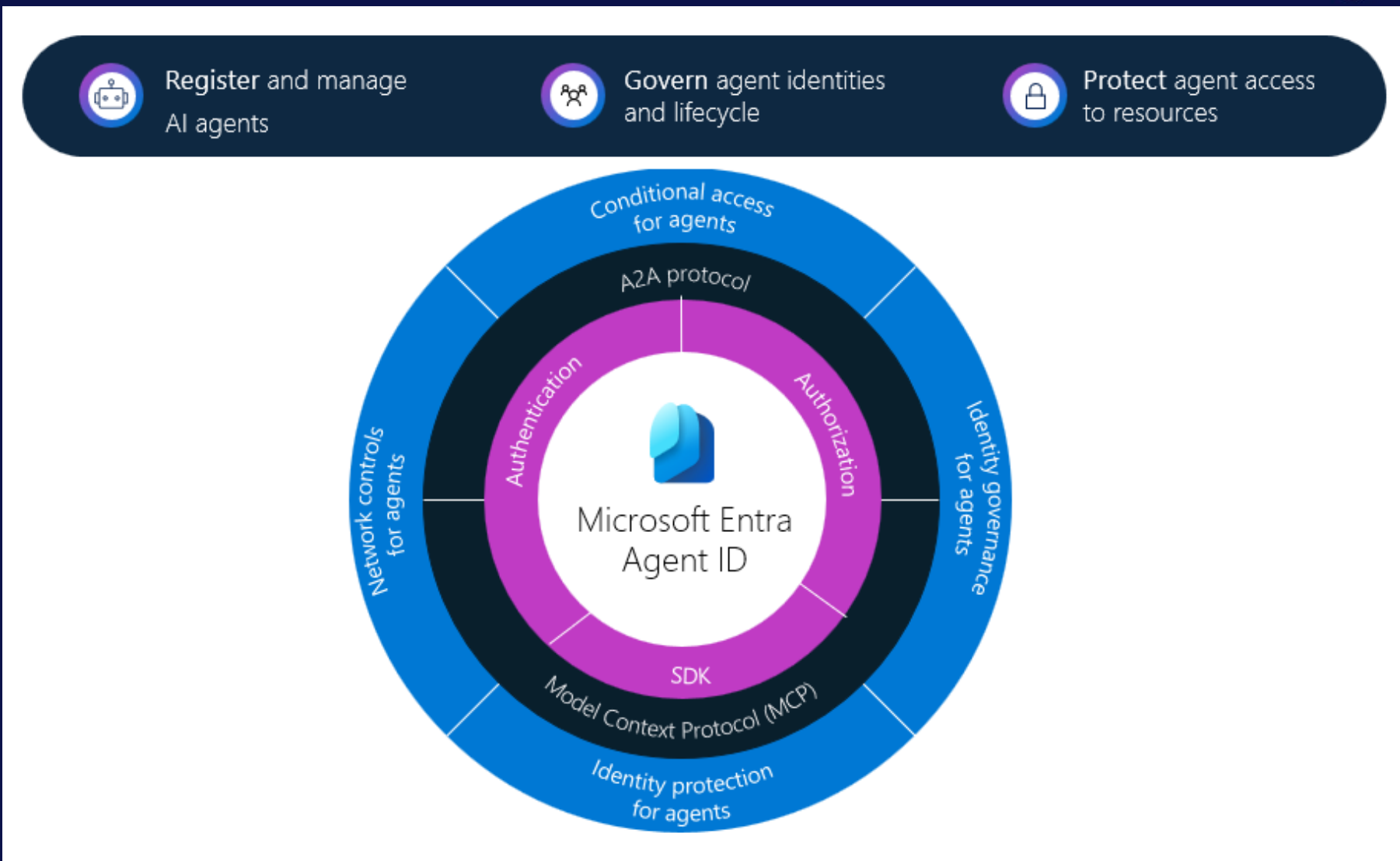


# 基于.NET 的 Agent 授权架构



<div><ul style="list-style-type: none"><li>• Agent Builder</li><li>• Context Builder</li><li>• FuncCall Middleware</li></ul></div> <div><ul style="list-style-type: none"><li>• MCP Client</li><li>• Prompt Template</li></ul></div>	Agent
<div><ul style="list-style-type: none"><li>• Policy Engine</li><li>• Tool Registry</li><li>• Delegation Store</li><li>• OpenIddict</li><li>• Audit Log</li></ul></div> <div></div>	Orchestrator
<div><ul style="list-style-type: none"><li>• MCP Server</li><li>• OpenAPI</li><li>• Native Plugin</li></ul></div>	Function

# Microsoft Entra Agent ID



**.NET Conf China 2025**

改变世界 改变自己



THANK YOU