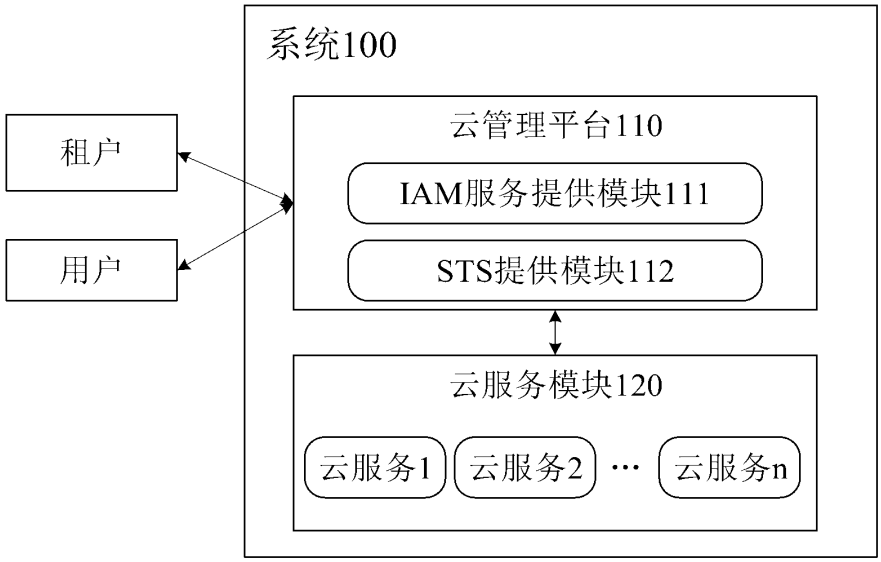

系统100
云管理平台110
IAM服务提供模块111
STS提供模块112
租户
用户
云服务模块120
云服务1
云服务2
…
云服务n

图 1

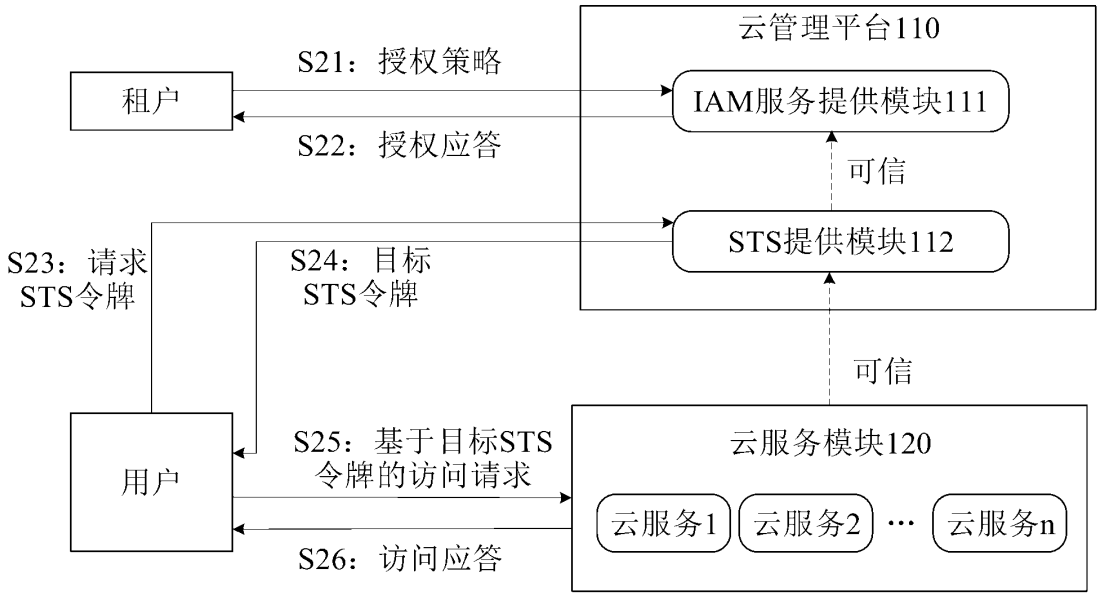

云管理平台110
S21：授权策略
租户
IAM服务提供模块111
S22：授权应答
可信
STS提供模块112
S23：请求
STS令牌
S24：目标
STS令牌
可信
用户
S25：基于目标STS
令牌的访问请求
云服务模块120
云服务1
云服务2
…
云服务n
S26：访问应答

图 2

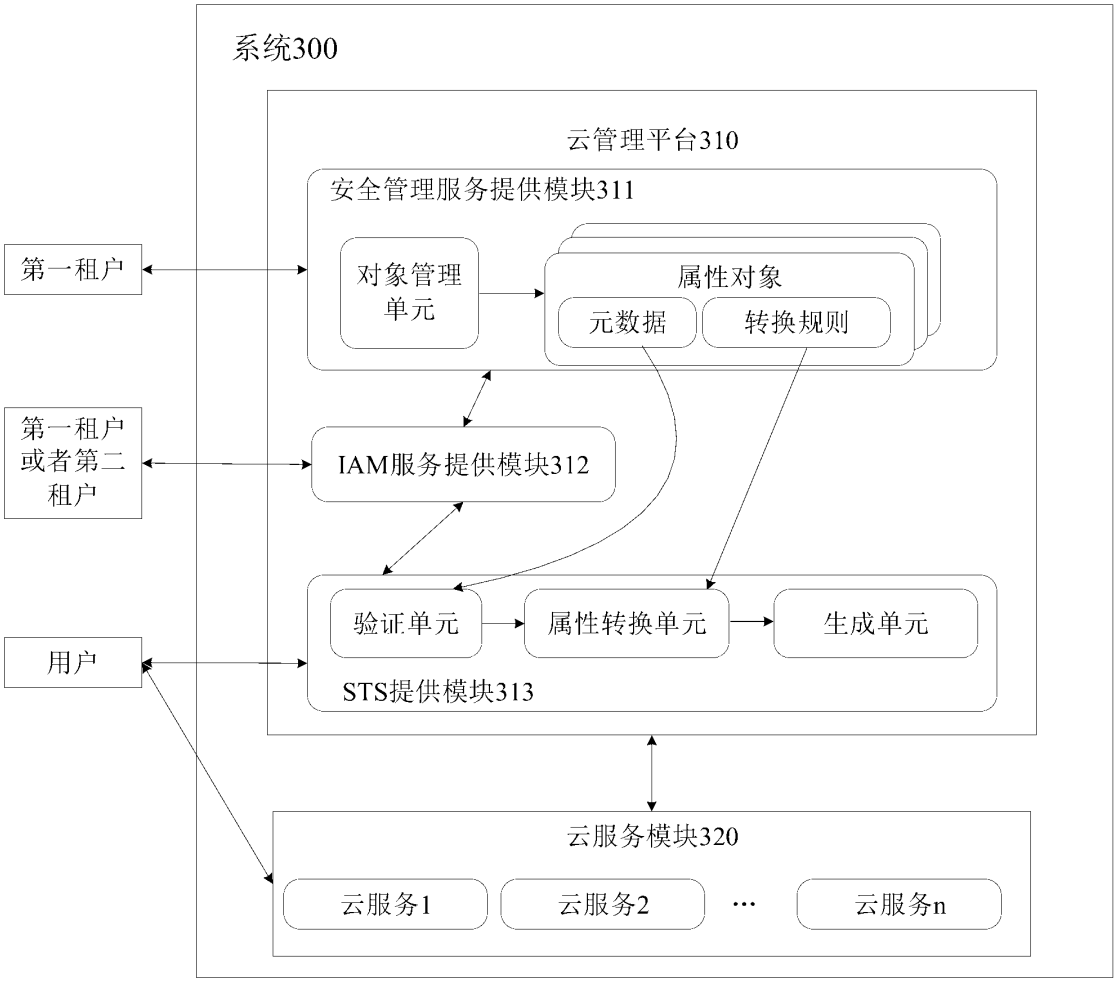

系统300
云管理平台310
安全管理服务提供模块311
对象管理单元
属性对象
元数据
转换规则
IAM服务提供模块312
验证单元
属性转换单元
生成单元
STS提供模块313
云服务模块320
云服务1
云服务2
…
云服务n
第一租户
第一租户或者第二租户
用户

图 3

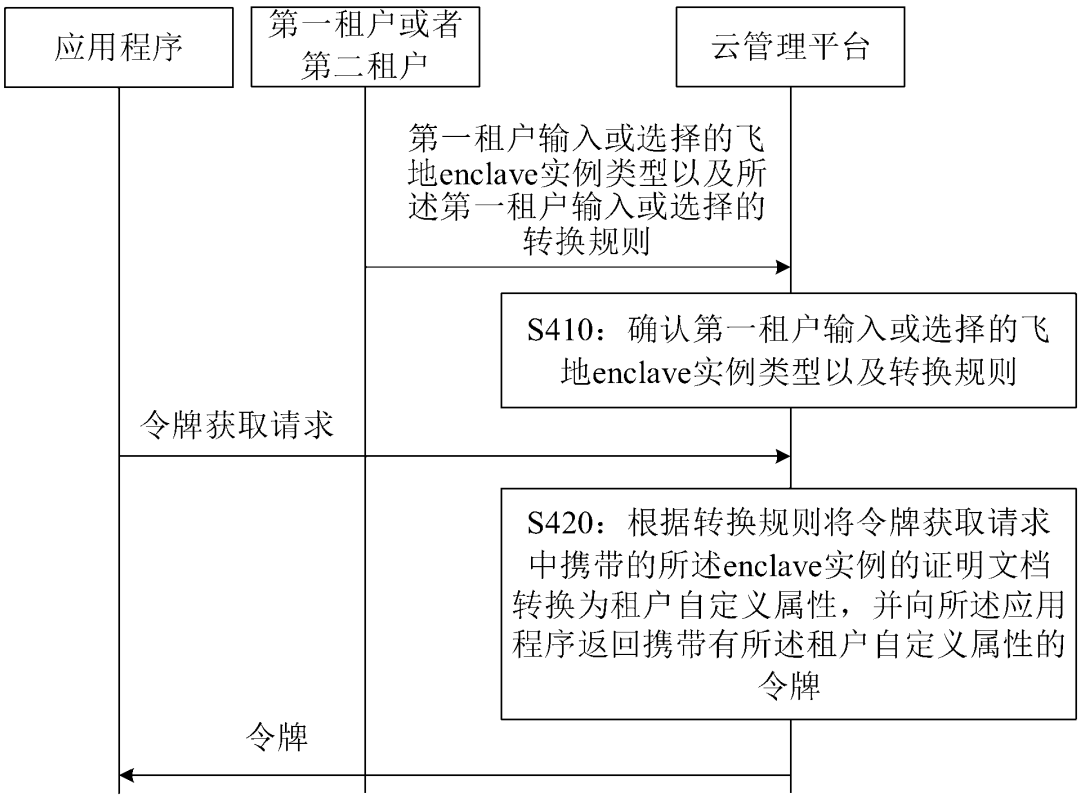

应用程序
第一租户或者第二租户
云管理平台
第一租户输入或选择的飞地enclave实例类型以及所述第一租户输入或选择的转换规则
S410：确认第一租户输入或选择的飞地enclave实例类型以及转换规则
令牌获取请求
S420：根据转换规则将令牌获取请求中携带的所述enclave实例的证明文档转换为租户自定义属性，并向所述应用程序返回携带有所述租户自定义属性的令牌
令牌

图 4

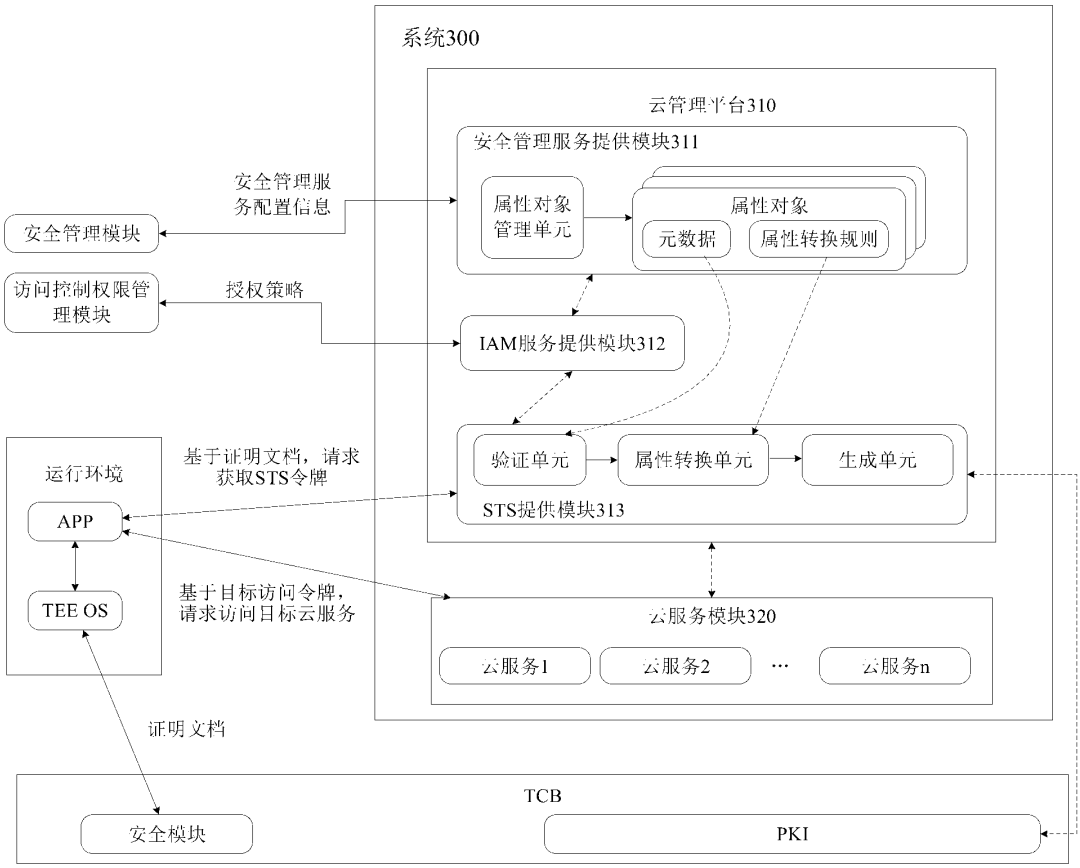

系统300
云管理平台310
安全管理服务提供模块311
安全管理服务配置信息
安全管理模块
属性对象管理单元
属性对象
元数据
属性转换规则
访问控制权限管理模块
授权策略
IAM服务提供模块312
验证单元
属性转换单元
生成单元
STS提供模块313
运行环境
基于证明文档，请求获取STS令牌
APP
TEE OS
基于目标访问令牌，请求访问目标云服务
云服务模块320
云服务1
云服务2
…
云服务n
证明文档
TCB
安全模块
PKI

图 5

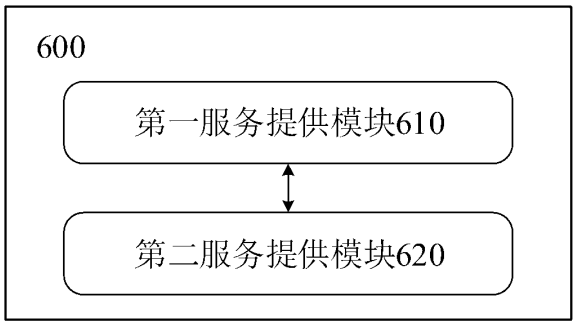

600
第一服务提供模块610
第二服务提供模块620

图 6

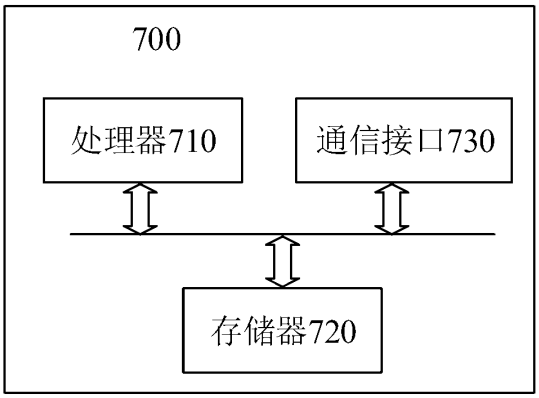


图 7