## 电子身份认证

电子身份认证也称为“电子身份验证”或“电子身份鉴别”，是指在计算机及计算机网络系统中确认操作者身份的过程，从而确定该用户是否具有对某种资源的访问和使用权限，进而使计算机和网络系统的访问策略能够可靠、有效地执行，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法利益。

基于PKI技术构建的可信电子身份认证体系、鉴权体系及行为追溯体系，采用数字证书的认证方式对用户进行强电子身份认证，实现信息系统可信、可控、可管理。

### 服务方式

在网络中部署认证网关，对用户进行电子身份认证。认证网关按部署模式分为三种：串联部署网关、并联部署网关和统一认证单点登录网关。

1. 串联部署

串联部署如图3-1所示。



外部用户

公网

防火墙

身份认证网关

内部用户

……

应用服务器

1

应用服务器

2

应用服务器

3

图3-1 串联模式部署图

串联模式的优点：

1. 安全性高：用户必须通过平台的认证加密后才能获取服务，同时平台将服务器与外界网络隔离，避免了对服务器的直接攻击。
2. 结构清晰：串联模式在物理部署和逻辑结构上都非常简单，容易理解。
3. 带宽利用率高：相对于并联模式，串联模式的效率及带宽利用率更高。

串联模式的缺点：

1. 需要对原有服务器进行网络改动及进行地址改变；
2. 对于网关的访问压力较大，需要平台具有较高的并发量。
3. 并联部署

并联部署如图3-2所示。

图4-2 并联模式部署图

图3-2 并联模式部署图

并联模式的优点：

1. 部署方便，应用无需改动原有的网络架构。
2. 减轻了平台的访问压力，用户在认证过后，直接与应用服务器进行数据传输。

并联模式的缺点：

1. 需要更高的安全手段保障：由于服务器和外界网络连接，存在绕开平台直接连接服务器和使用其它方式攻击服务器的可能性；同时，平台到服务器的数据需要进行加密处理，否则存在被窃听的安全隐患。
2. 性能较低：相对于串联模式，并联模式中用户到平台和平台到服务器的数据流量都通过一个网口进行，效率及带宽利用率相对较低。

（3）统一认证模式

统一认证单点登录部署如图3-3所示。

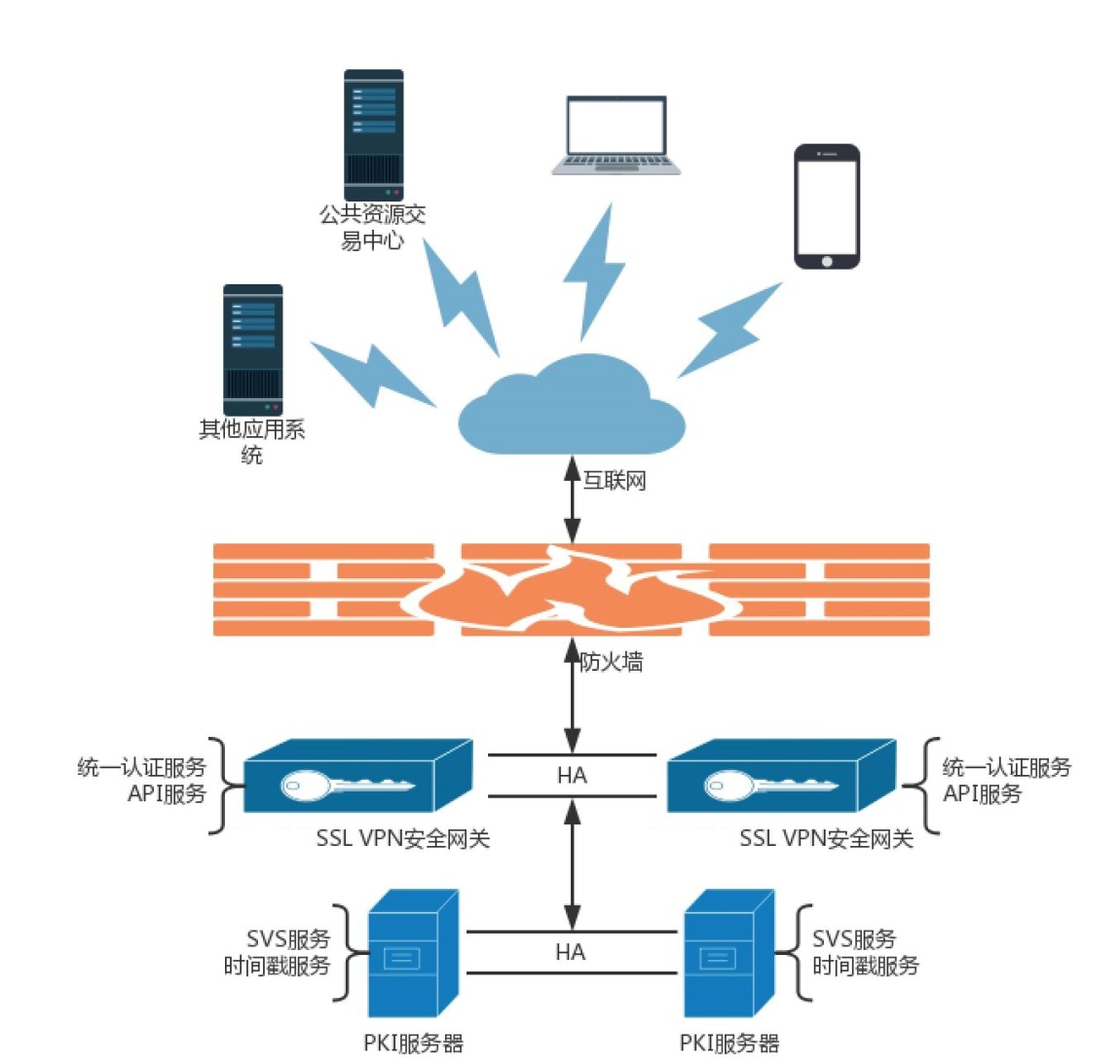


图3-3 统一认证单点登录部署图

统一认证模式开发改造简单，应用一次接入，支持多CA机构，可以根据意愿增加或减少支持的CA机构，无需再次修改应用。

### 工作原理

1. 串联模式

串联模式认证过程如图3-4所示。

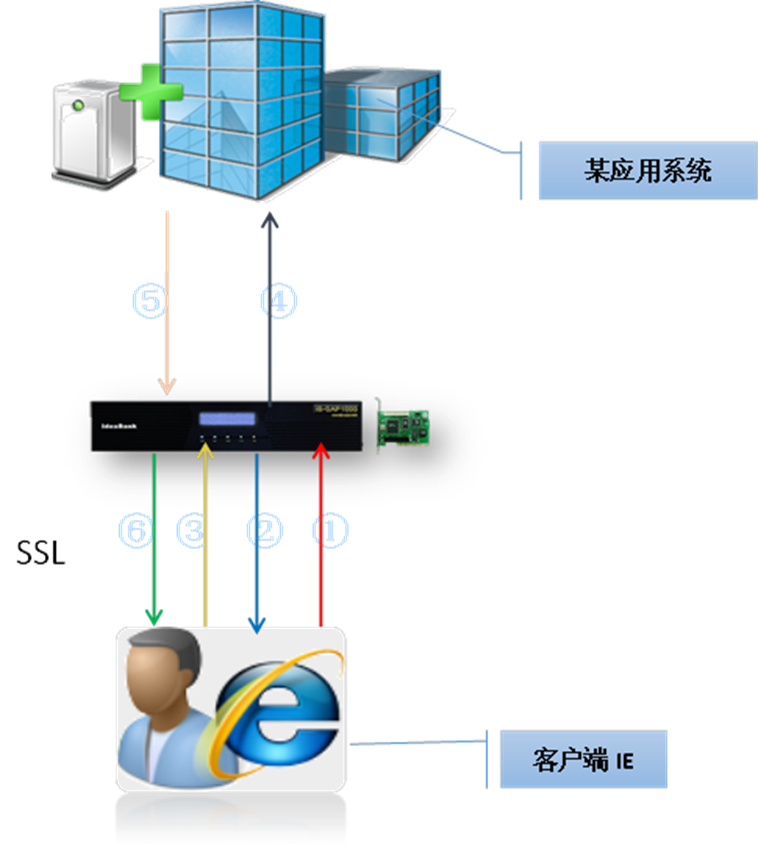


图3-4 串联模式认证过程图

认证过程描述如下：

1. 用户访问网关；
2. 平台验证用户身份合法性，不通过跳转到指定错误页面；
3. 用户身份合法性验证通过后并建立SSL隧道，平台根据用户权限提供可访问的应用资源；
4. 用户选择应用资源后，平台通过HTTP Header或HTTP Cookies等方式向后台应用传递用户信息；
5. 应用验证用户信息的合法性；
6. 用户正常访问应用资源。
7. 并联模式

并联模式认证过程如图3-5所示。

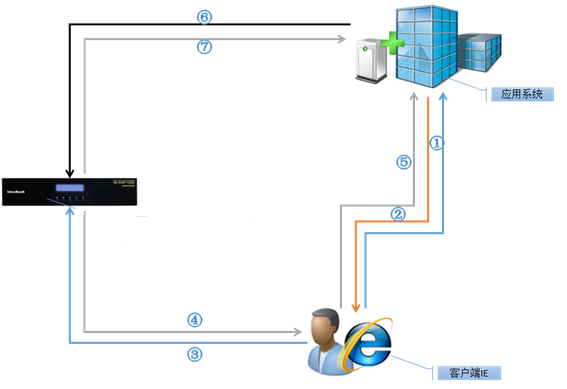


图3-5 并联模式认证过程图

认证过程描述如下：

1. 用户通过浏览器访问某应用系统；
2. 应用系统自动重定向至身份认证网关，请求统一身份认证；
3. 用户插入USBKey，浏览器通过HTTPS在身份认证网关进行双向身份认证；
4. 证书认证通过后，由平台对当前用户会话签名，返回客户端会话签名凭证；
5. 客户端浏览器自动重定向至应用系统，并提交会话签名凭证；
6. 应用系统后台在身份认证网关验证当前会话用户访问签名凭证是否正确以及应用系统接入的合法性；
7. 平台通过HTTP Header或HTTP Cookies等方式向后台应用传递用户信息。
8. 统一认证

统一认证认证过程如图3-6所示。

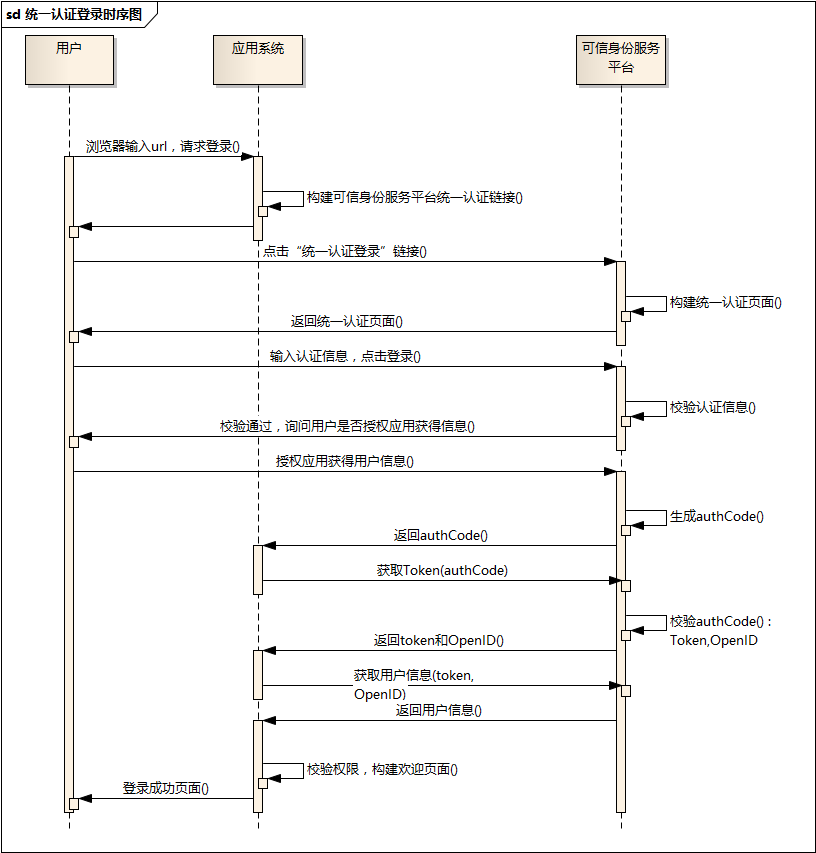


图3-6 统一认证过程图

认证过程描述如下：

1. 用户打开浏览器，输入应用系统URL，请求登录；
2. 应用系统构建可信身份服务平台统一认证链接；
3. 用户点击“统一认证登录”链接，跳转到可信身份服务平台；
4. 可信身份服务平台构建统一认证页面；
5. 用户输入认证信息（即使用数字证书认证），进行登录；
6. 可信身份服务平台校验认证信息（即校验数字证书合法性）；
7. 校验数字证书合法性通过后，询问用户是否授权应用系统获得用户信息；
8. 用户确认授权后，可信身份服务平台生成authCode，页面跳转到应用系统回调地址；
9. 应用系统根据authCode及自身身份标识到可信身份服务平台获取用户token；
10. 可信身份服务平台校验authCode，返回token和OpenID给应用系统；
11. 应用系统根据token和OpenID获取用户信息；
12. 可信身份服务平台返回应用系统其所要获得的用户信息；
13. 应用系统获得用户信息，校验用户在本身系统中的权限，构建欢迎页面；
14. 用户登录成功。

### 遵循的规范

* GM/T 0016-2012《智能密码钥匙密码应用接口规范》
* GM/T 0017-2012《智能密码钥匙密码应用接口数据格式规范》
* GM/T 0027-2014《智能密码钥匙技术规范》
* GM/T 0021-2012《动态口令密码应用技术规范》
* GM/T 0014-2012《数字证书认证系统密码协议规范》
* GM/T 0015-2012《基于SM2密码算法的数字证书格式规范》
* GM/T 0034-2014《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》
* GM/T 0037-2014《证书认证系统检测规范》
* GM/T 0043-2015《数字证书互操作检测规范》
* GM/T 0024-2014《SSL VPN技术规范》

GM/T 0025-2014《SSL VPN网关产品规范》