网络安全接入移动解决方案预研

# 任务要求

关于安全认证网关的移动端设计，分别从2个方案设计方向（身份和链路）调研移动app和小程序实现时的优缺点及技术路线，给出相关建议

身份方向：APP 登录身份 ，比如 登录身份的有效性 短信验证 、指纹验证 、人脸 、事件证书 、标识身份IBC 等。小程序授权登录 等等

链路方向：移动终端程序 + 移动网关接入 + 网关服务端

# 任务调研

## 安全认证网关移动端可能的功能需求

安全认证网关移动端的功能需求大致上可分为两个方向，一是完整的vpn移动客户端，具有桌面版的vpn客户端的所有功能，支持手机接入vpn网关服务器，与vpn服务端建立虚拟专用通道，实现手机端对内网的安全访问。二是将移动端程序看做是一个辅助vpn桌面客户端登录的工具，为vpn桌面客户端提供更多的登录认证方式，如扫码登录等

### **完整的vpn移动客户端**

完整的VPN移动客户端功能类似领导建议的链路方向方案，即移动端程序（界面） + 移动网关接入（内核） + 网关服务端。在此种模式下需开发一个移动端界面操作程序，一个移动端网关接入内核，移动端界面操作程序通过控制移动端网关接入内核与网关服务端建立链接。

### **辅助vpn桌面客户端登录的工具**

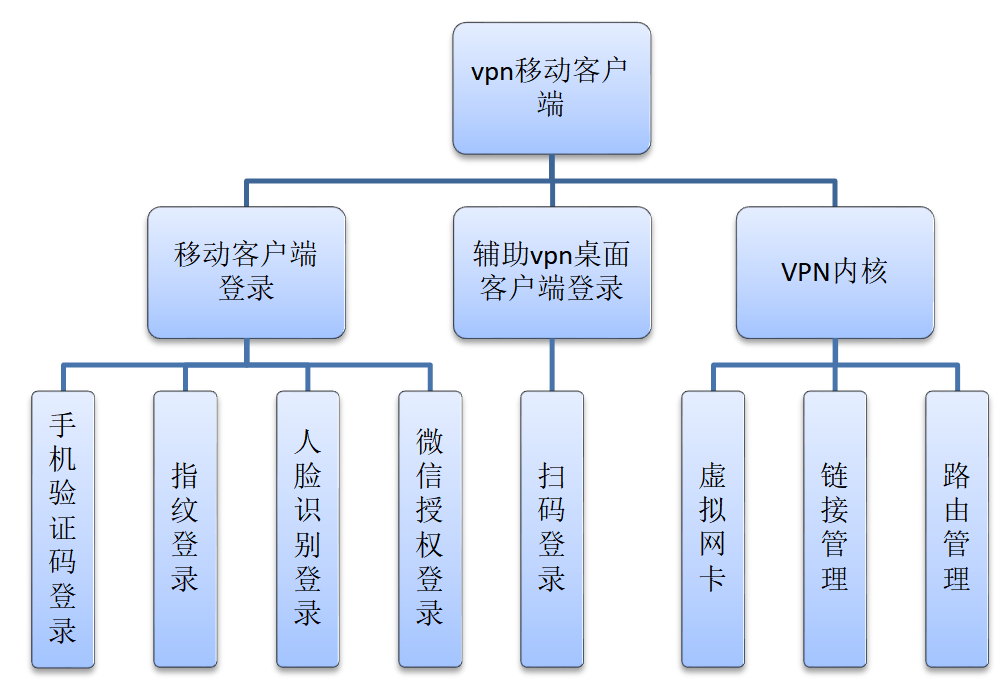
辅助vpn桌面客户端登录的工具功能，首先该工具先登录，登录方式可采用领导所说的身份方向，如登录身份的有效性 短信验证 、指纹验证 、人脸 、事件证书 、标识身份IBC ，小程序授权登录，该工具登录后通过扫描vpn桌面客户端展示出的二维码信息进行相关处理后，与vpn桌面客户端进行通信，使vpn桌面客户端登录用户vpn账户，连接vpn服务端，进而在桌面电脑上访问vpn业务内网。该模式下，手机端仅具备辅助登录功能，不具备建立vpn链接，访问业务内网的功能。

### **功能确认**

经确认，选择完整的vpn移动客户端功能，以下简称为vpn移动客户端。

同时，Vpn移动客户端可同时支持辅助vpn桌面客户端登录的功能。

至于领导说的身份方向，可在vpn移动客户端登录时，或者辅助vpn桌面客户端登录时与openvpn登录账号进行关联，作为一种身份识别方式。



## App和小程序实现比较

就既定需求而言，只能选择app。

复杂的应用程序不适合小程序，因为小程序代码不能超过1MB，所以不能做太复杂的应用

对需要大量计算的功能类应用，小程序无法满足

小程序是与微信一同占用手机空间，内存较小

App可以实现完整功能，灵活性强；小程序仅限微信提供的接口功能

小程序低频、非刚需、轻量级、功能单一，高频刚需还是要靠APP

小程序在很多功能、用户体验等方面还是比不上APP

小程序只能在腾讯开发的Java框架内开发。

微信小程序不能在支持web应用的浏览器上运行

## 身份方向--移动端客户登录

Vpn移动客户端的登录方式，同时需与openvpn账号采用某种协议进行关联。

可选方式有：

1. 手机验证码登录----Mob、xutils
2. 指纹登录
3. 人脸识别登录 （可做可不做，建议不做了）
4. 事件证书（建议不做了）
5. 标识身份IBC （建议不做了）
6. 微信授权登录

这部分要做的工作如下

1. 确定各个登录方式的实现方法、实现技术以及该技术是否能使用国密算法
2. vpn服务端的配置管理工具如何管理这些登录方式
3. 实现app自身的vpn功能，设计协议，确定各登录模式如何与openvpn账号关联
4. 设计协议，vpn桌面客户端如何生成二维码，二维码的生成格式，与app客户端的协议关联等

## 链路方向--vpn内核

链路方向即vpn内核的实现计划在基于openvpn开源android源码上进行，同时结合Android VPNService，实现如下功能：

1. 首先，搭建环境，跑通原有设计
2. 其次，研究源码和相关android技术，实现国密的改造，打通国密ssl链路
3. 最后，实现各种登录方式与openvpn账号的关联，以实现身份方向的各种登录方式下的openvpn链接

# 调研结论

使用app开发，链路方向实现主要vpn内核功能，身份方向实现app的登录验证及app与openvpn账号的绑定。

在实现上，先实现链路，后实现方向，方向可实现可不实现，不影响主体功能，实现更高大上点。