**CA证书服务实现方案**

# 1、功能描述

实现节点之间的通信认证以及对网络节点的新增退出等管理操作。

CA证书服务分为客户端与服务器端，客户端主要功能是用来生成公私钥密钥对，私钥不上传服务器由用户自己保存。服务端主要功能是签发客户端的证书请求创建节点证书，对节点动态变更的管理，节点用户登陆的管理。+

证书

公钥



# 2、客户端功能实现

客户端使用命令行工具创建公私钥对，私钥本地留存。用户使用账户/密码的方式登陆服务端的管理界面。



填入节点的相关信息（机构、域名、邮箱等），导入公钥提交到服务端，由服务端完成对客户端证书的签名生成证书

# 3、服务端功能实现

## 3.1证书签发

服务端收到客户端发送的证书请求后，用CA的私钥签名证书请求，生成证书文件，下发给客户端。

证书

证书生成请求

公钥

机构

域名

…

公钥

机构

域名

…

签名

私钥

公钥

## 3.2证书管理

实现证书的分发，网络中各节点证书的同步。使用管理员账户登陆管理界面，可实现对节点证书的撤销操作。

公钥



证书



证书



证书



证书



## 3.3节点管理

使用管理账户可以在网络节点中增加新节点、退出网络中的某个节点

## 3.4用户管理

给用户授权一些账户密码，每个账号密码可以对应多个节点，以便于客户端登陆管理自己的证书相关，也便于服务器表示节点信息