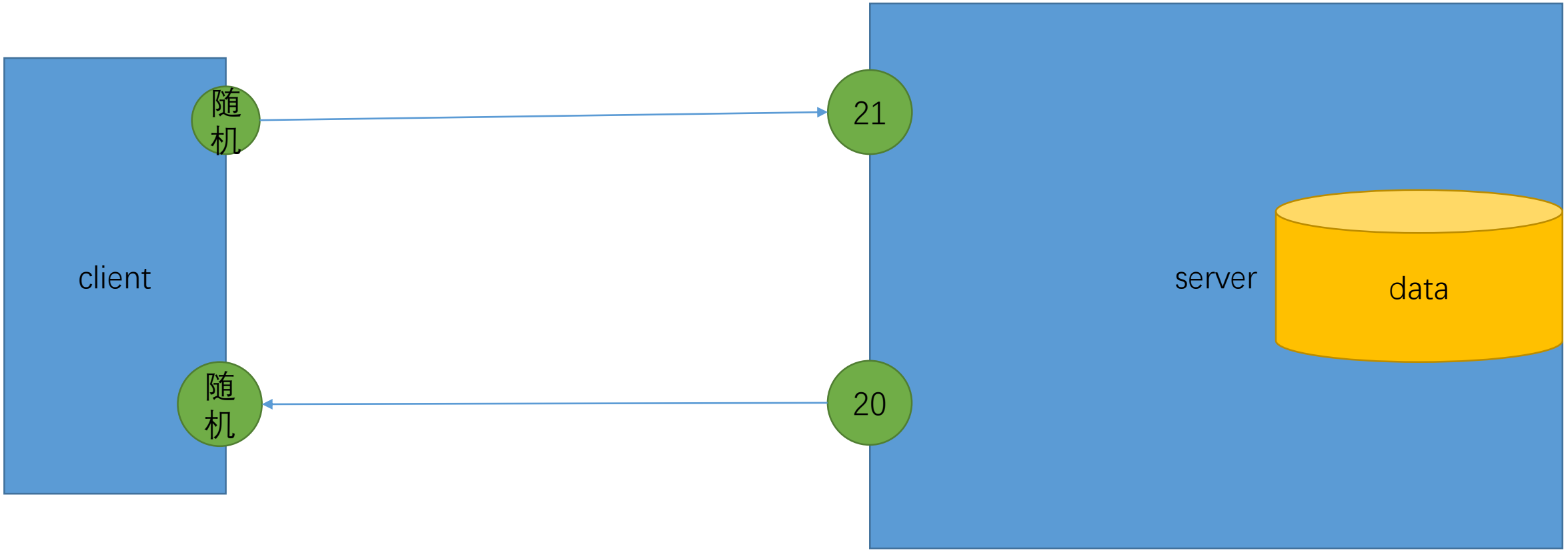
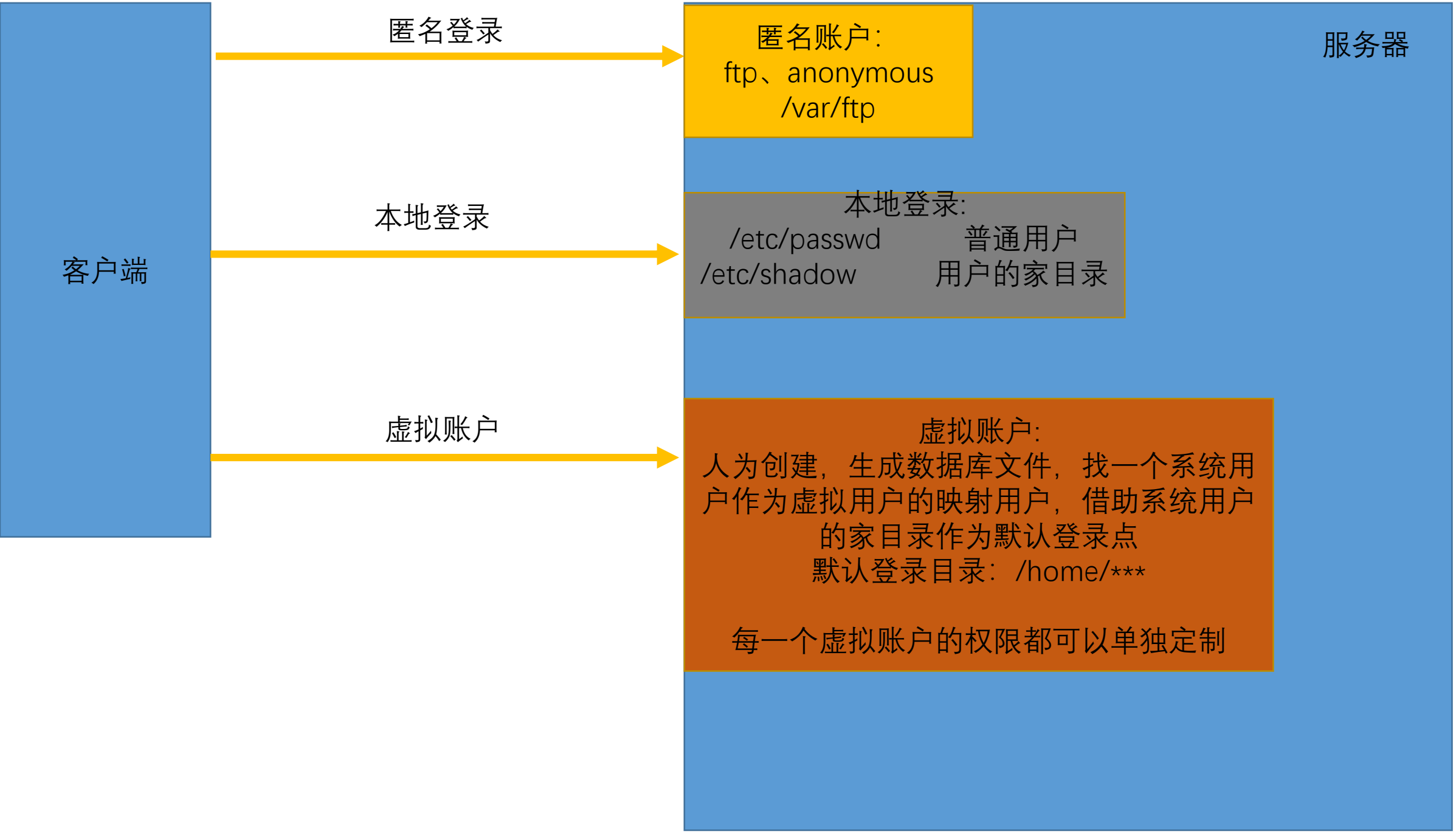
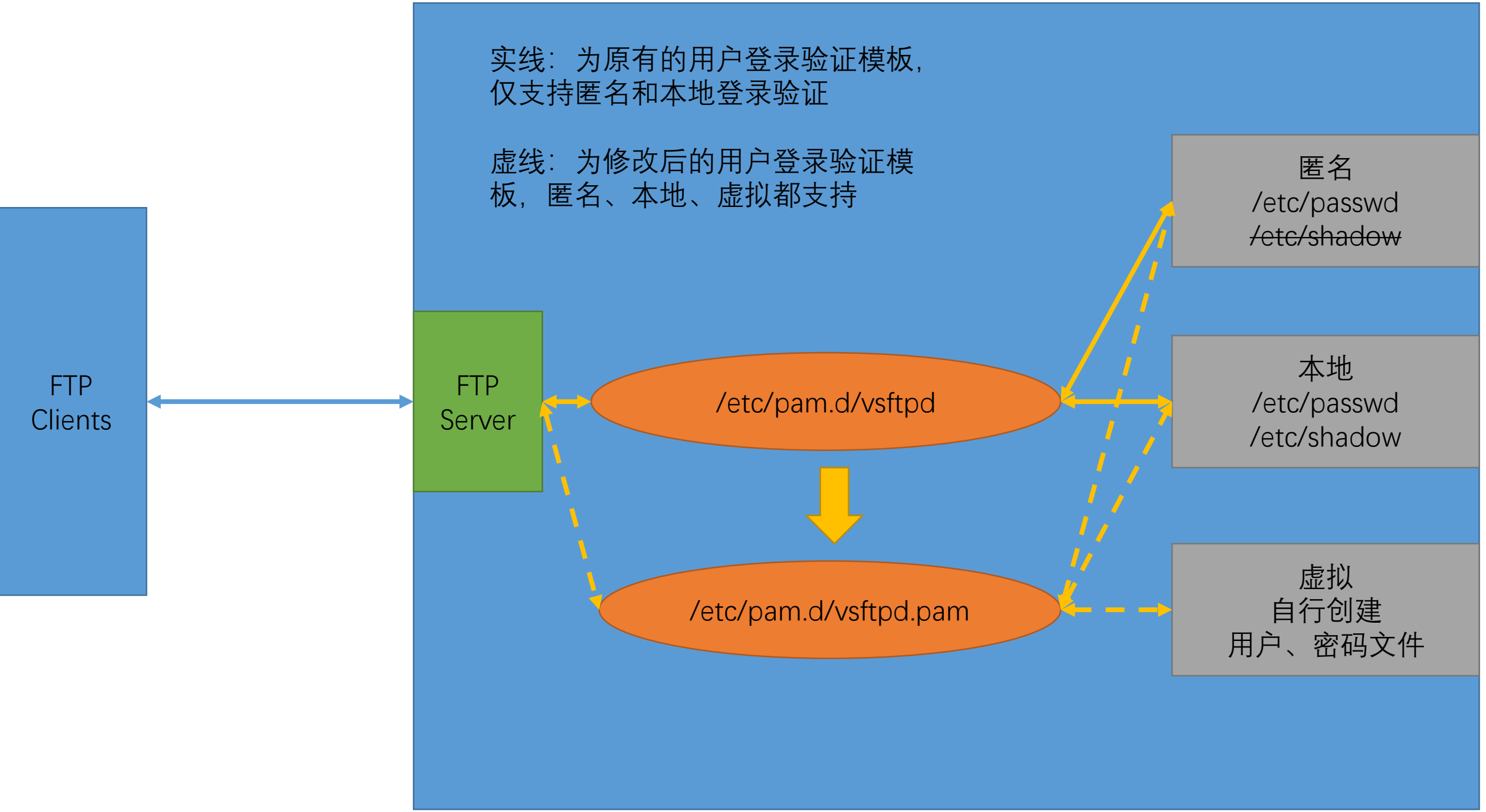
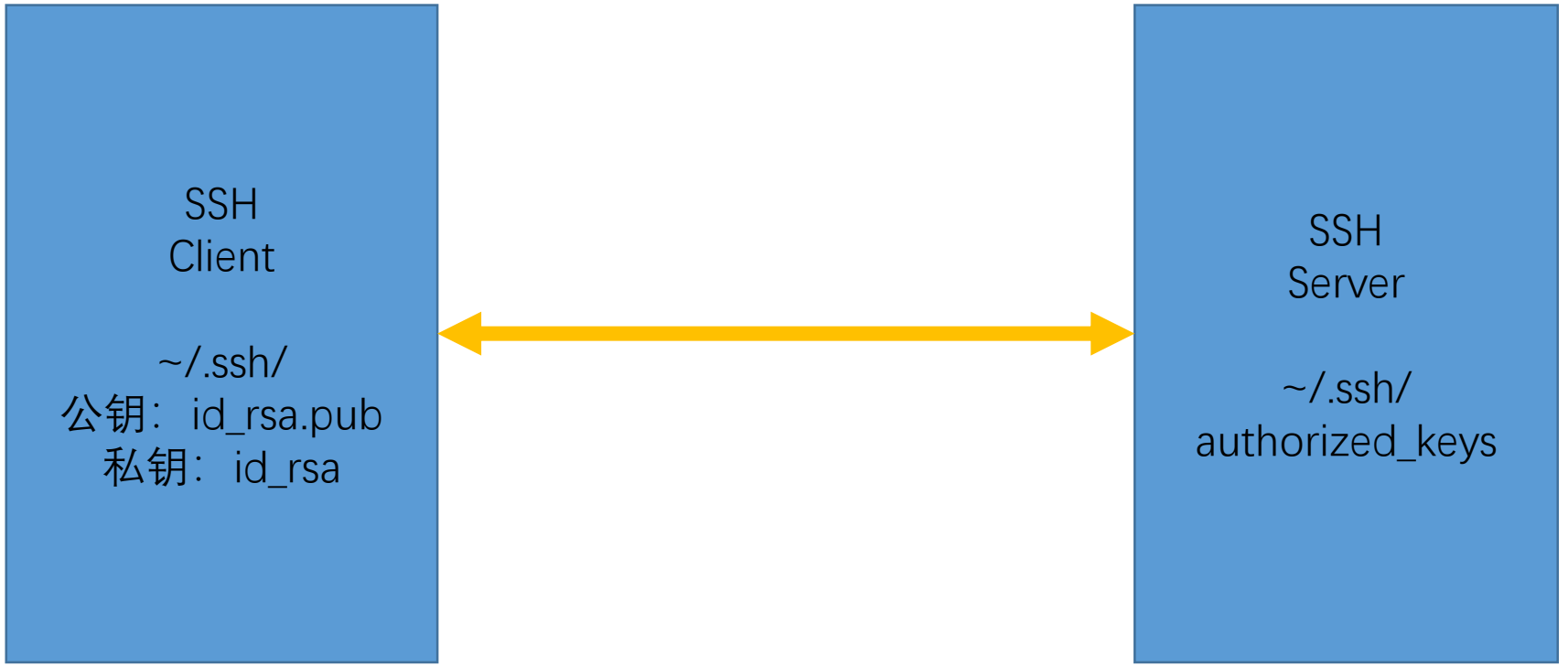

随机
client
随机
21
20
server
data


客户端
匿名登录
本地登录
虚拟账户
匿名账户:
ftp、anonymous
/var/ftp
服务器
本地登录:
/etc/passwd
/etc/shadow
普通用户
用户的家目录
虚拟账户:
人为创建，生成数据库文件，找一个系统用户作为虚拟用户的映射用户，借助系统用户的家目录作为默认登录点
默认登录目录：/home/***
每一个虚拟账户的权限都可以单独定制


实线：为原有的用户登录验证模板，
仅支持匿名和本地登录验证
虚线：为修改后的用户登录验证模
板，匿名、本地、虚拟都支持
FTP
Clients
FTP
Server
/etc/pam.d/vsftpd
/etc/pam.d/vsftpd.pam
匿名
/etc/passwd
~~/etc/shadow~~
本地
/etc/passwd
/etc/shadow
虚拟
自行创建
用户、密码文件



注：sshd服务的配置文件中，注释掉的是默认生效的

1. 由客户端生成密钥对文件，并将公钥文件上传到服务器的指定目录下，修改指定名称：ssh-keygen –t rsa –b 1024 & ssh-copy-id user@ip

2. 需要在服务器端开启密钥对登录认证模式（默认是开启的）

秘钥：解密加密的数据包
证书：提供加密所需的功能{加密类型、加密长度}

因为数据包是从客户端发向服务器端的，所以需要将证书给客户端使用，客户端使用证书将要发送的数据包加密，然后再进行传输
服务器端接收到客户端发送的加密数据包后，拿着秘钥文件进行解析，得到明文

CA 证书服务器
秘钥：*.key
证书：*.csr
签字后的证书：*.crt

客户端所使用的证书是，CA服务器签名后的证书。

签名后的证书：
1. 有一定有效期
2. 有加密类型
3. 有加密长度
.....