1 每个人都可以创建CA中心，但是相比起大型CA中心，自建的CA中心的受信任度较低。每个CA中心都有自己的密钥对，且CA机构的root证书是所有人都可以自由获取的，这意味着所有人都可以轻易获取CA机构的公钥。

2 CA机构需负责对申请证书的用户进行身份验证，验证通过后再颁发签名后的证书。证书颁发后，CA机构需要管理已颁发的证书。

3 用户通过一些密钥生成工具，比如ssh-keygen等生成密钥对，然后将其中的公钥和用户身份信息等提交给CA认证中心，CA机构对用户身份进行认证后，**会用自己的公钥对用户身份信息和用户的公钥计算数字签名**，并将计算出的数字签名附着在数字证书的末尾颁发给用户。这样数字证书和用户保存的私钥就构成了用户的完整数字签名。

4 假设用户A向**深圳市CA机构**申请了数字证书，那么A将其数字证书发给B后，B如何验证该证书的有效性呢？

首先，B需要获取深圳市CA机构的root证书，从而拿到其公钥。然后用该公钥解码A传过来的数字签名，得到报文摘要，如果该报文摘要与A传过来的一样，那么数字证书验证通过，即**A确认该证书是深圳市CA机构颁发给B**的，因为A信任深圳市CA机构，而深圳市CA机构又信任B，从而形成了一条信任链，达到A信任B的效果。