一、挑战-应答认证方法是通过对一轮应答实现验证者对证明者的认证，利用一次性随机数实现防重放攻击



三、何一个使用证书的第三方在验证证书有效性的时候，要执行以下验证操作：

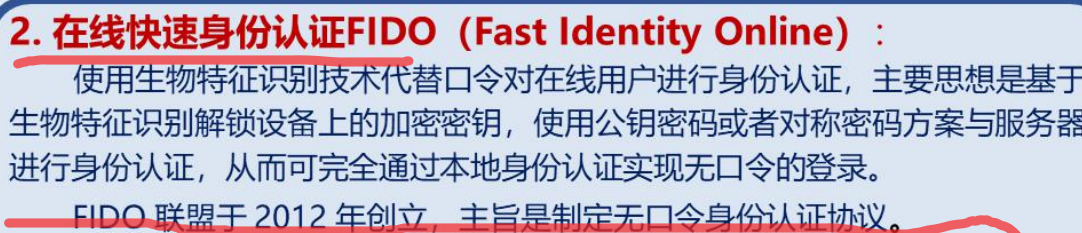
证书颁发机构是否是其信任的机构。

证书是否在有效期内。

证书是否在证书撤销列表当中。

证书的数字签名是否有效。

所有上述验证通过以后，用户就可以从证书获得证书持有人的公钥，并信任这个公钥。

1. 

UAF认证的主要流程是使用者发起申请，APP要求进行认证。使用者在终端基于存储特征进行认证。

1. 虚拟化的实现主要有两种方式：

全虚拟化和硬件支持的虚拟化，对于IO虚拟化来说，还有第三种，那就是半虚拟化。

虚拟化面临的安全威胁：

1. 虚拟机逃逸2.边信道攻击3.网络隔离4.镜像和快照的安全

八、区块链的数据结构是由包含交易信息的区块按照从远及近的顺序有序链接起来的。区块被从远及近有序地链接在这个链条里，每个区块都指向前一个区块。

区块链通过密码学哈希函数和非对称加密保证其不可篡改。

十、