1.

主要方法有基于口令的认证，基于智能卡的认证，基于生物特征的认证。详细点则包括基于静态口令或动态口令的认证，基于USB Key的认证，基于指纹的认证。

2.

数字证书是由权威公正的第三方机构签发的，由用户的身份与其所持有的公钥相结合的计算机文件

基本功能：可对网络上传输的信息进行加密、解密、数字签名和签名验证，确保网上传递信息的机密性、完整性，以及交易实体身份的真实性，签名信息的不可否认性，从而保障网络的安全性。

3. X.509包含的信息：

①版本号 ②序列号 ③签名算法标识 ④签发者 ⑤有效期 ⑥证书主体名 ⑦证书主体的公钥信息 ⑧签发者惟一标识 ⑨证书主体惟一标识 ⑩扩展 ⑪签名

4. ①CA主要负责产生、分配并管理参与活动的所有实体所需的数字证书 ②CA管理公钥的整个生命周期，包括签发证书、规定证书的有效期限，何时需负责何时撤销证书、更新，归档等操作。

4. CA的主要职能

①制定并发布本地CA策略。但对本地策略总是对上级CA的补充，不能违背 ②对下属各成员的进行身份认证和鉴别 ③发布CA的证书，或代替上级CA发布证书 ④产生和管理下属成员的证书. ⑤ 证实RA的证书申请，返回证书制作的确认信息，或返回已制作的证书 ⑥ 接收和认证对所签发证书的撤消申请 ⑦ 产生和发布所签发证书和CRL ⑧ 保存证书、CRL信息、审计信息和所制定的策略。

5.

PKI信任模型

① 层次模型：CA之间有严格上下级关系，子CA证书为上级CA签发的

② 交叉模型：根CA之间能相互签发交叉认证证书

③ 混合模型：即层次模型与交叉模型混合

④ 桥CA模型：引入独立的桥CA中心，相当于虚拟的根CA。~~根CA与~~

⑤ 信任链模型：用户可拥有多个信任锚作为根CA链表