

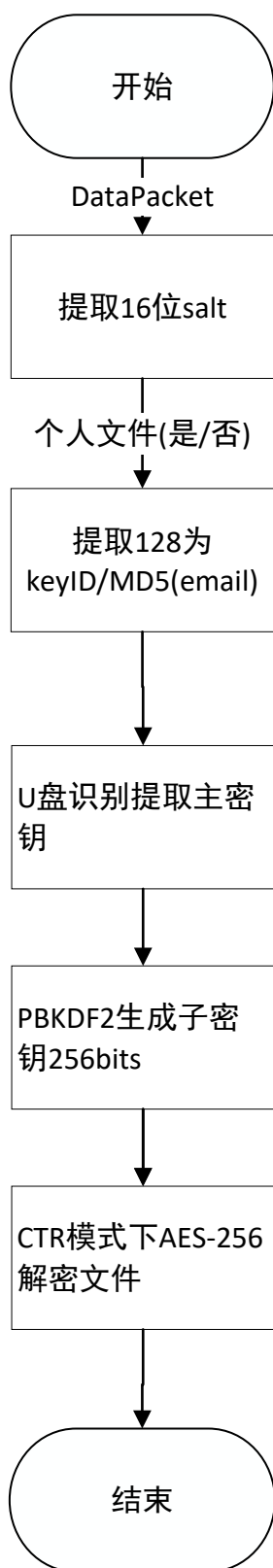
主 密 钥 文 件
名 : M D 5 (个 人
email)

主密钥文件名:KeyID

注:HMAC验证对象增加了

层级密钥解密策略

U盾读取解密

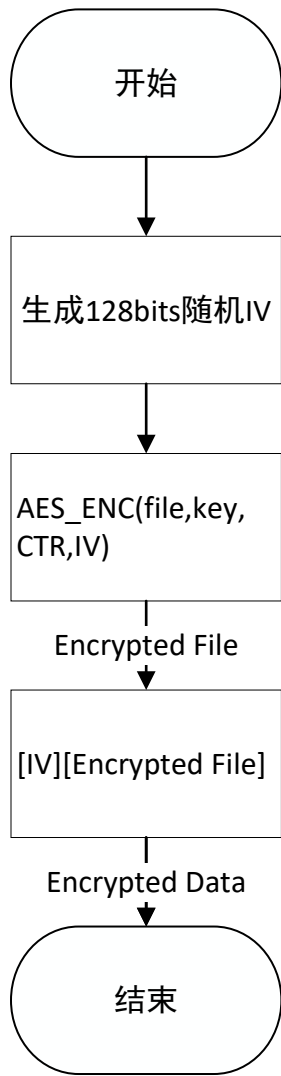


CTR模式下AES-256加解密文件

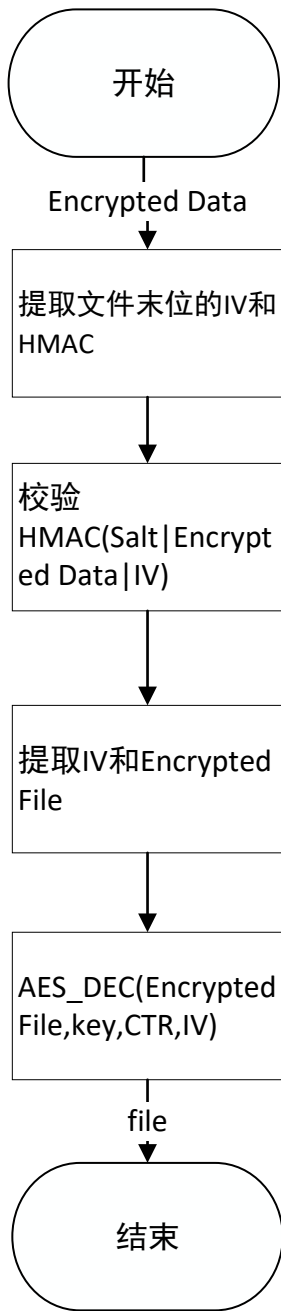
注:用安全的随机数生成算法

阶段

加密



解密



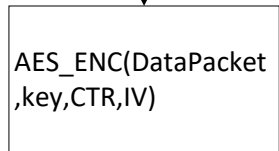
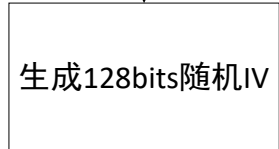
安全信道的AES-256加解密

加密

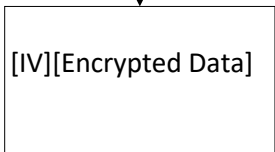
解密



DataPacket



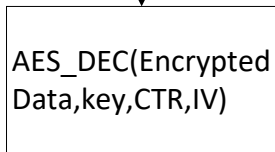
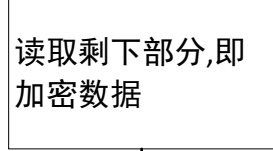
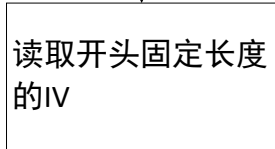
Encrypted Data



SecurePacket



SecurePacket

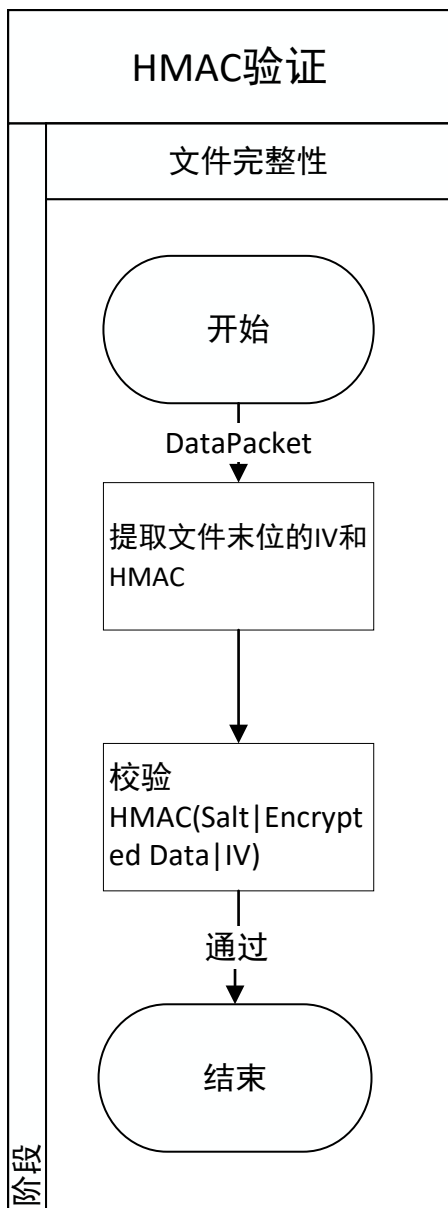


DataPacket



注:key是DH协商的会话密钥

阶段



注:这个接口可复用