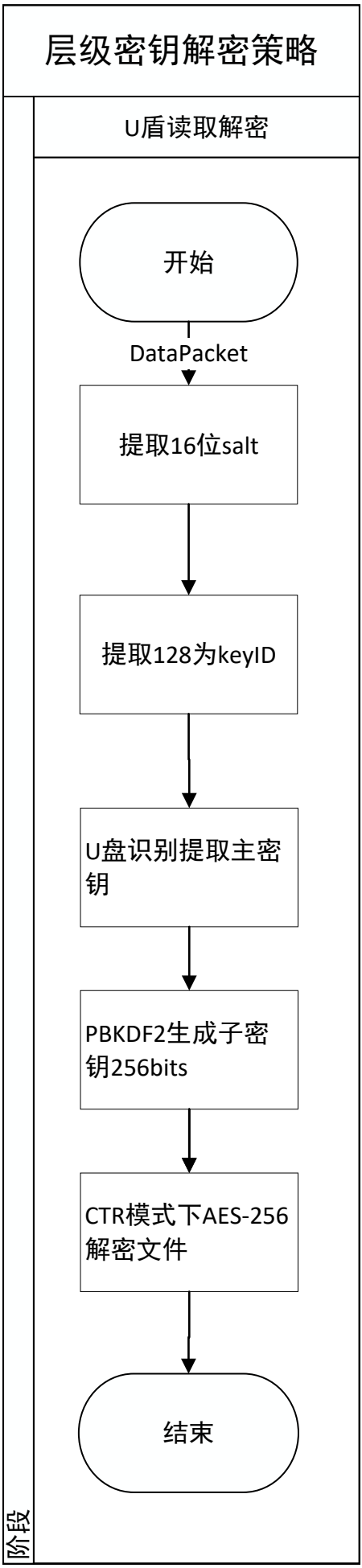
层级密钥加密策略

注:用安全的随机数生成算法

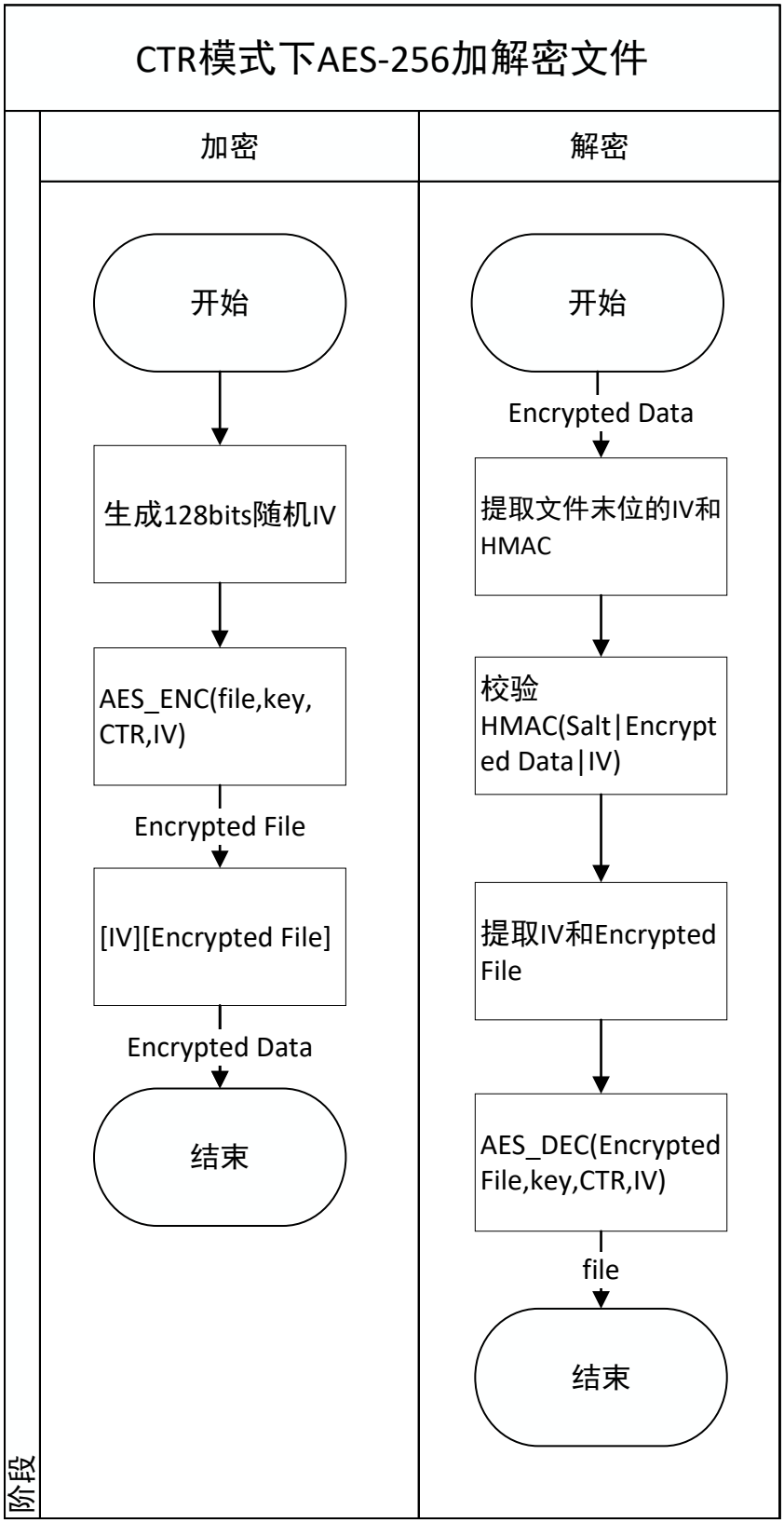
阶段

个人空间	用户组空间
开始	开始
随机生成主密钥256bits	随机生成主密钥256bits
主密钥文件名:MD5(个人email) → 生成128位随机数KeyID	生成128位随机数KeyID绑定主密钥,并存储U盘 ← 主密钥文件名:KeyID
随机生成16位salt	选择用户共享主密钥
PBKDF2生成子密钥256bits	随机生成16位salt
CTR模式下AES-256加密文件	PBKDF2生成子密钥256bits
随机生成256位IV用于HMAC	CTR模式下AES-256加密文件
HMAC(Salt|Encrypted Data|IV)	随机生成256位IV用于HMAC
[Salt][[KeyID][Encrypted Data][IV][HMAC]	HMAC(Salt|Encrypted Data|IV)
安全信道	[Salt][[KeyID][Encrypted Data][IV][HMAC]
服务器	安全信道
结束	服务器
	结束

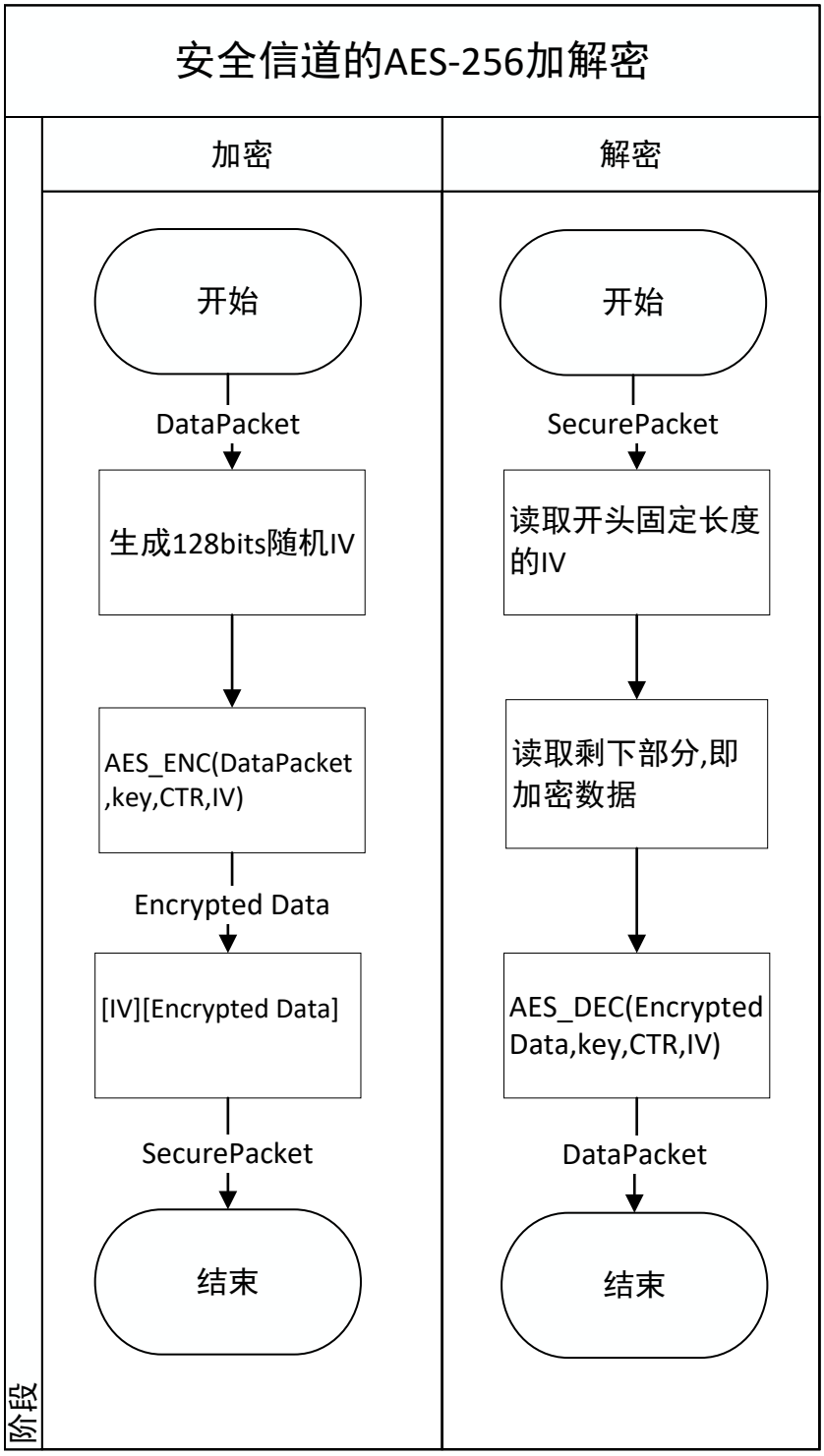
注:HMAC验证对象增加了



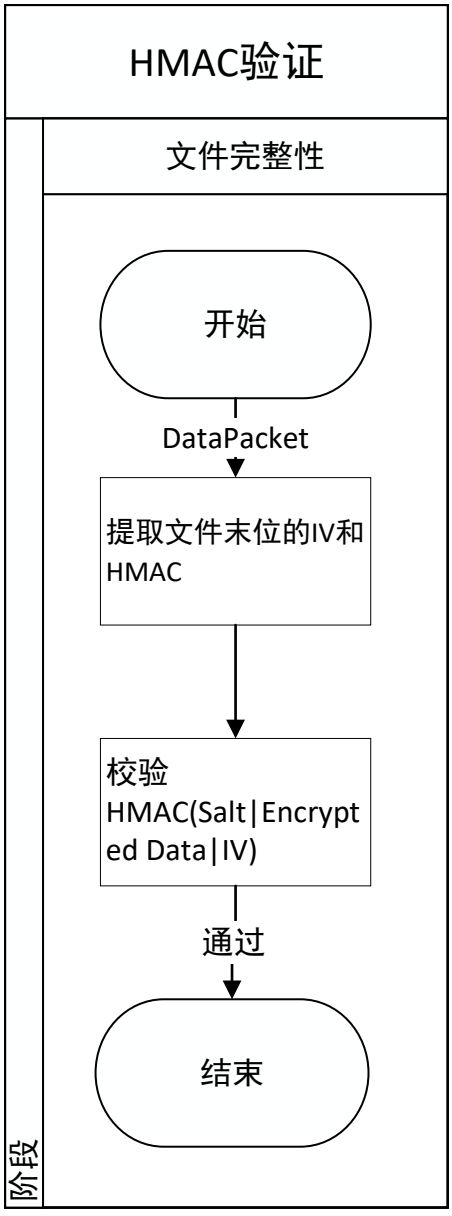
注:用安全的随机数生成算法



注:用安全的随机数生成算法



注:key是DH协商的会话密钥


HMAC验证
文件完整性
开始
DataPacket
提取文件末位的IV和HMAC
校验HMAC(Salt|Encrypted Data|IV)
通过
结束
阶段

注:这个接口可复用