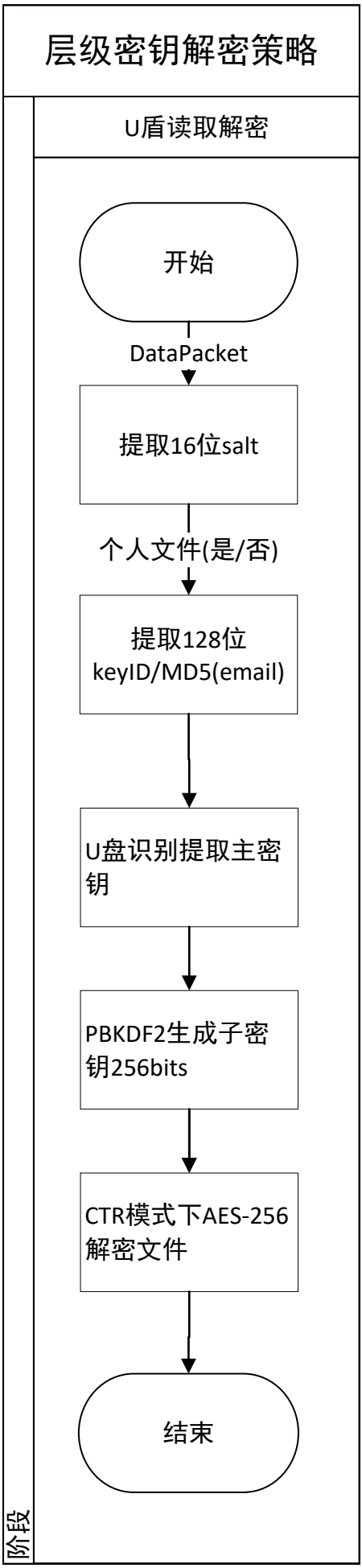
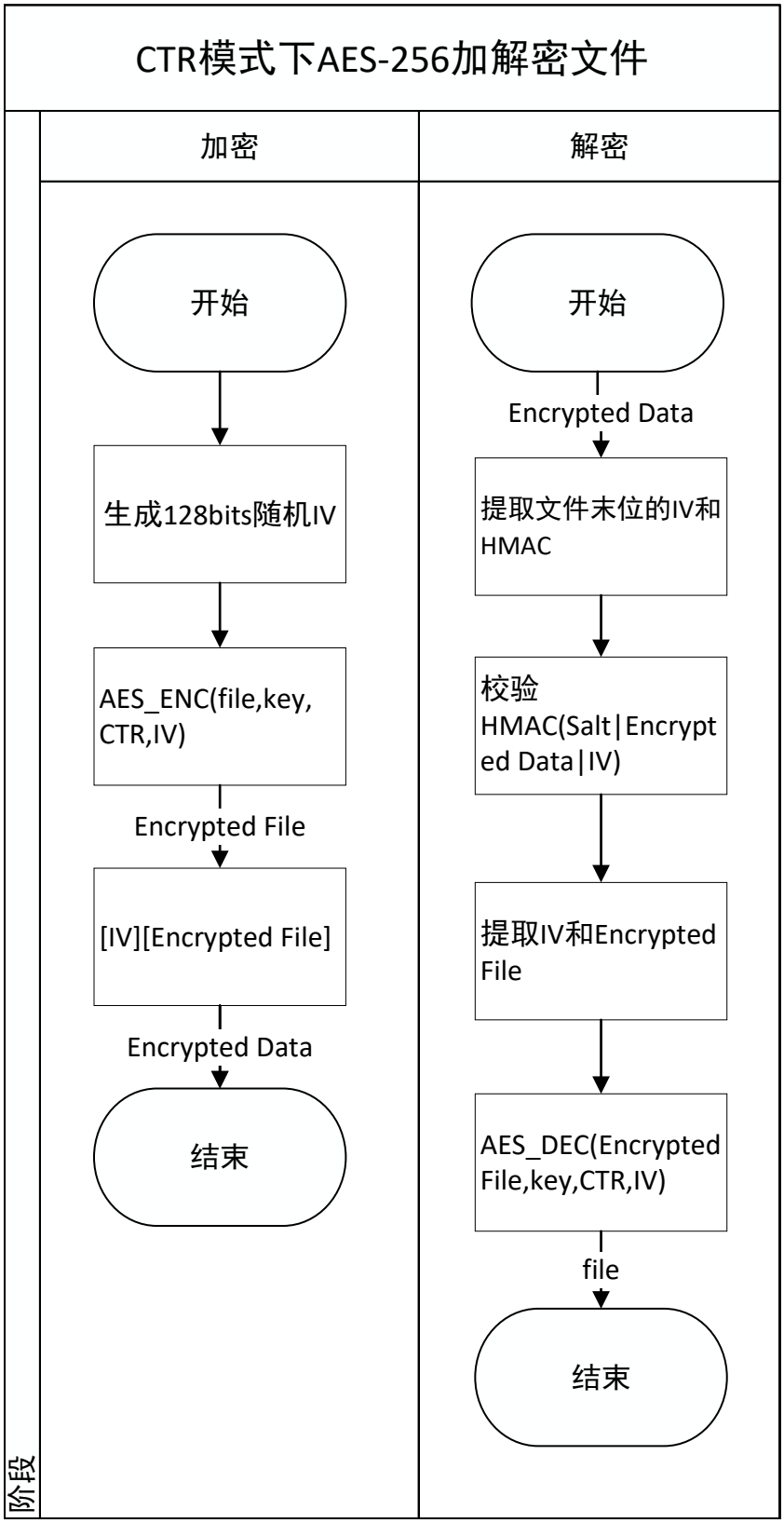
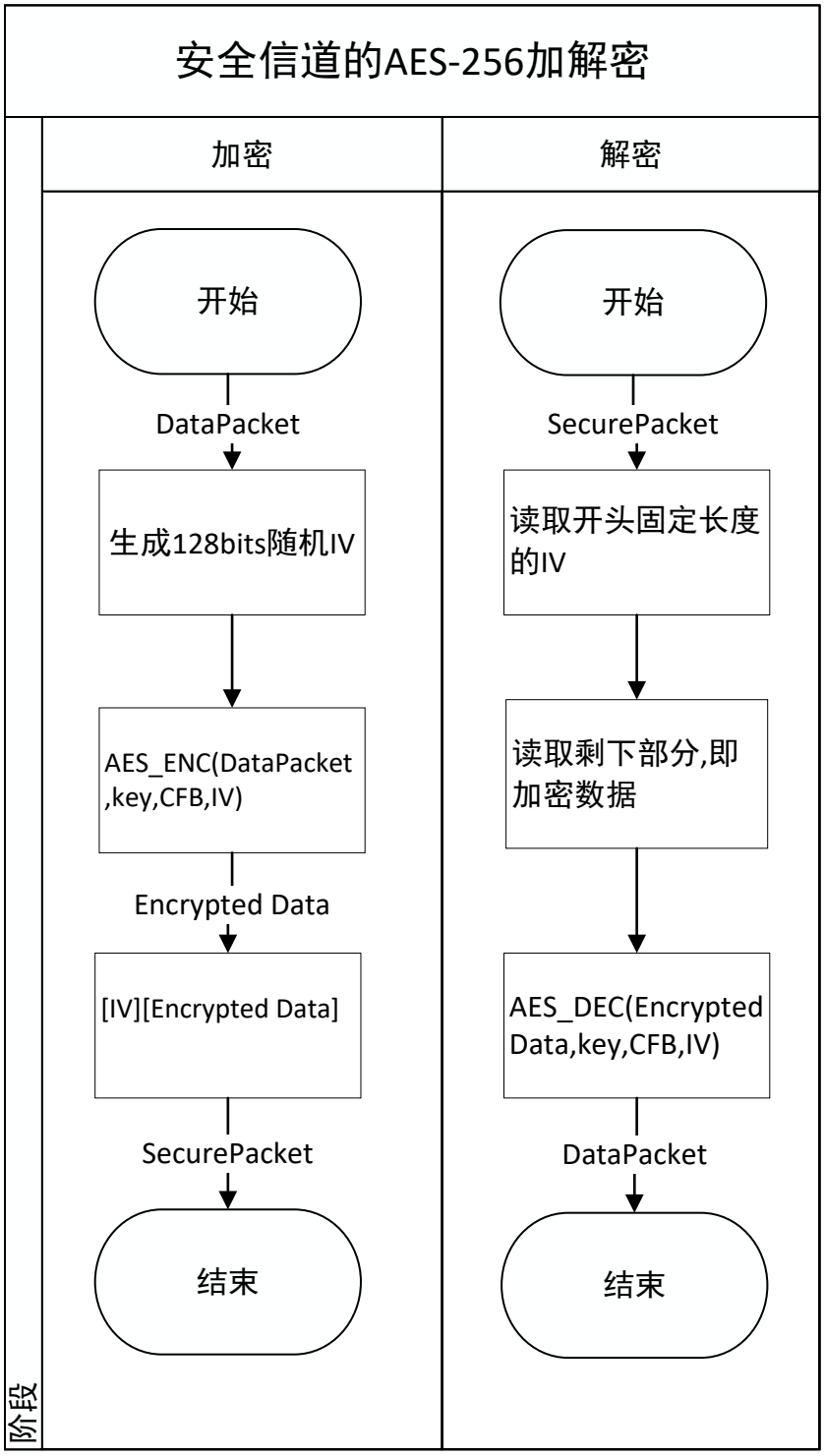
层级密钥加密协议

阶段

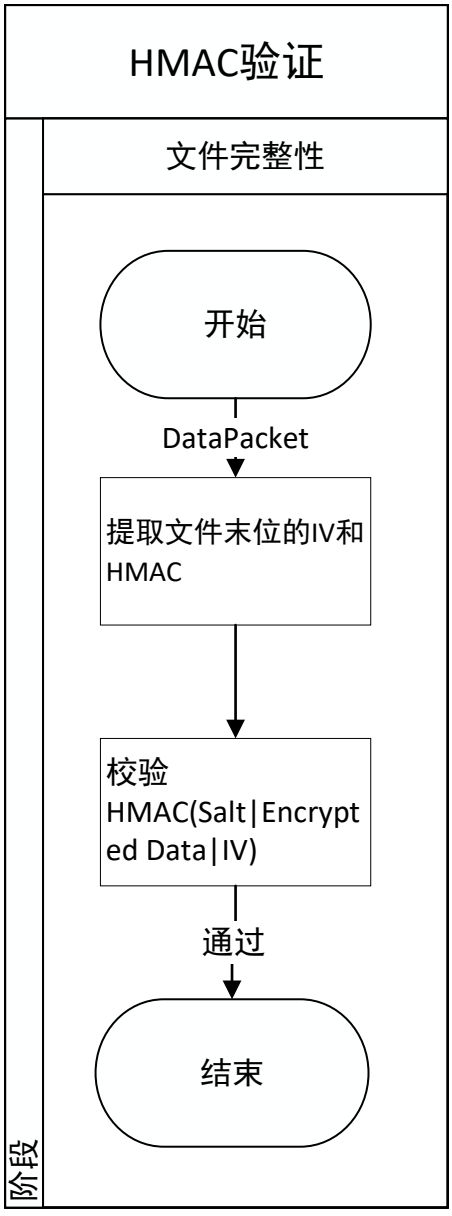
个人空间	用户组空间
开始	开始
随机生成主密钥256bits	随机生成主密钥256bits
主密钥文件名MD5(个人email)作为KeyID并存储U盘	生成128位随机数KeyID绑定主密钥并存储U盘
随机生成16位salt	选择用户共享主密钥
PBKDF2生成子密钥256bits	随机生成16位salt
CTR模式下AES-256加密文件	PBKDF2生成子密钥256bits
随机生成256位IV用于HMAC	CTR模式下AES-256加密文件
HMAC(Salt|Encrypted Data|IV)	随机生成256位IV用于HMAC
[Salt][[KeyID][Encrypted Data][IV][HMAC]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


层级密钥解密策略
U盾读取解密
开始
DataPacket
提取16位salt
个人文件(是/否)
提取128位
keyID/MD5(email)
U盘识别提取主密钥
PBKDF2生成子密钥256bits
CTR模式下AES-256解密文件
结束
阶段


CTR模式下AES-256加解密文件
加密
解密
开始
生成128bits随机IV
AES_ENC(file,key, CTR,IV)
Encrypted File
[IV][Encrypted File]
Encrypted Data
结束
开始
Encrypted Data
提取文件末位的IV和HMAC
校验HMAC(Salt|Encrypted Data|IV)
提取IV和Encrypted File
AES_DEC(Encrypted File,key,CTR,IV)
file
结束
阶段



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