

SecurePacket

安全信道	IV1	Encrypted Data
	AES-256下 128bits的随机向量	AES_ENC(DataPacket, key,CFB,IV1)

Encrypted Data

IV2	Encrypted File
AES-256下 128bits的随机向量	AES_ENC(file,key, CTR,IV2)

DataPacket

文件加密	Salt	KeyID	Encrypted Data
	16位随机数	128位随机数	[IV][AES_ENC(file,key, CTR,IV2)]
	IV3		HMAC
	256位随机数		SHA-256下运行HMAC(Salt Encrypted Data)生成256bitsHMAC