附件

服务类密码设备技术要求

1. 基本要求
应具备国家密码管理局批准的商用密码产品型号证书（在有效期内）
2. 算法要求
1、支持 1024 位 RSA、2048 位 RSA、SM2 非对称密钥密码算法 2、支持 SM1、SM4 对称密码算法 3、支持 SHA1、SM3 消息摘要算法
3. 功能要求
1、密钥生成与管理：支持生成 1024/2048 位 RSA 算法密钥对和 256 位 SM2 算法密钥对。 2、数据加密和解密：支持 1024/2048 位 RSA 算法、256 位 SM2 算法的数据加密、解密运算；支持 SM1 算法、SM4 算法数据加密和解密运算。 3、数据摘要的产生和验证：支持 SHA1、SM3 消息摘要算法计算消息摘要。 4、数字签名的产生和验证 :支持 1024/2048 位 RSA 算法、256 位 SM2 算法的数字签名、验证签名运算。 5、生成签名证书请求：支持按照 PKCS#10 标准生成证书请求并导出请求包。