服务类密码设备技术要求

1. 基本要求
应获得商用密码产品认证证书（证书在有效期内）
2. 算法要求
2.1 支持 SM2 密码算法 2.2 支持 SM1、SM4 密码算法 2.3 支持 SM3 消息摘要算法
3. 功能要求
3.1 密钥生成与管理：支持生成 SM2 密码算法密钥对。 3.2 数据加密和解密：支持 SM2 密码算法的数据加密、解密运算；支持 SM1、SM4 密码算法数据加密和解密运算。 3.3 数据摘要的产生和验证：支持 SM3 消息摘要算法计算消息摘要。 3.4 数字签名的产生和验证：支持 SM2 算法的数字签名、验证签名运算。 3.5 生成签名证书请求：支持按照《基于 SM2 算法的证书申请语法规范》（GM/T 0092-2020）生成证书申请并导出证书申请数据包。 3.6 加密密钥对导入：支持按照《SM2 密码算法使用规范》（GM/T 0009-2023）“7.4 密钥对保护数据格式”导入生成的加密密钥对。（此项为预留功能，当业务应用有数据加密需求时，需使用该功能）