附件 3

海关跨境电商统一版系统

密码产品选型和使用指南（202205 版）

一、 密码产品选择建议

用户可根据实际业务量选择密码产品进行数字签名。

密码产品类型	数字签名运算参考性能
智能密码钥匙	约 250 票/分钟
服务类密码设备	性能高于智能密码钥匙，具体由设备配置高低决定

二、 密码产品使用指南

第一步：申请数字证书

（一）使用智能密码钥匙的用户

按电子口岸企业入网流程办理数字证书（具体可咨询当地数据分中心）。

（二）使用服务类密码设备的用户

选择符合《服务类密码设备技术要求》（见下表）的服务器密码机、签名验签服务器等服务类密码设备，联系当地数据分中心办理数字证书。

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（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 256 位 SM2 密码算法密钥对。 3.2 数据加密和解密：支持 256 位 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 256 位 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《信息安全技术 SM2 密码算法使用规范》（GB/T 35276-2017）“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）

第二步：开发集成

用户按照相关报文规范进行开发集成，实现业务数据的数字签名功能。

2022 年 5 月