跨境电子商务进口统一版信息化系统密码产品选型和使用指南

一、密码产品选型建议

跨境电子商务进口统一版信息化系统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	业务处理性能 （对报文进行签名运算的速度）	产品可靠性
IC 卡	≤12 票/分钟	低
USBKey	≤240 票/分钟	中
服务类密码设备	＞240 票/分钟（服务类密码设备厂商有不同性能配置的产品，较高性能的设备业务处理性能可以达到 100000 票/分钟以上，具体可咨询厂商）	高

二、密码产品使用指南

第一步：申请数字证书

用户如使用 IC 卡或 USBKey，可到当地电子口岸数据分中心按电子口岸入网企业流程办理(具体可咨询当地电子口岸数据分中心)。已办理 IC 卡或 USBKey 的用户可使用已有 IC 卡或 USBKey，无需重复办理。

用户如使用服务类密码设备，须按照《数据交换平台服务类密码设备技术要求》(见附件）自行选购服务器密码机、签

名验签服务器等服务类密码设备，并联系当地电子口岸数据分中心办理数字证书（具体可咨询当地电子口岸数据分中心）。服务类密码产品名录可在国家商用密码管理办公室网站“产品信息”栏目下查询《商用密码产品目录》（网址：http://www.oscca.gov.cn）。

第二步：开发集成

用户自行或选择第三方厂商按照《跨境电子商务进口统一版信息化系统企业对接报文规范（试行）》进行开发集成，实现跨境数据申报环节的数字签名和验签功能。

附件：《数据交换平台服务类密码设备技术要求》

附件

数据交换平台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。