**商用密码出口管制清单**

**1．系统、设备和部件**

1.1 安全芯片

部分或全部实现了密码运算、密钥管理、随机数生成等功能的集成电路芯片，且具有以下特征之一：

1. 含有专门用于电力、税务、公安、金融等领域的64位以上密钥长度的对称密码算法、768位以上密钥长度的基于整数因子分解的非对称密码算法或128位以上密钥长度基于椭圆曲线的非对称密码算法；

2. 含有64位以上密钥长度的对称密码算法、768位以上密钥长度的基于整数因子分解的非对称密码算法或128位以上密钥长度基于椭圆曲线的非对称密码算法，且对称密码算法加解密速率10Gbps以上或非对称密码算法签名速率50000次/秒以上。

1.2密码机（密码卡）

以实现密码运算为主要功能的设备（包括密码卡），且具有以下两种特征：

1. 含有64位以上密钥长度的对称密码算法、768位以上密钥长度的基于整数因子分解的非对称密码算法或128位以上密钥长度基于椭圆曲线的非对称密码算法；
2. 对称密码算法加解密速率10Gbps以上或非对称密码算法签名速率50000次/秒以上。

1.3 加密VPN设备

以IPSec/SSL VPN为主要功能的设备，且具有以下两种特征：

1. 含有64位以上密钥长度的对称密码算法、768位以上密钥长度的基于整数因子分解的非对称密码算法或128位以上密钥长度基于椭圆曲线的非对称密码算法；
2. 加密通信速率10Gbps以上。

1.4 密钥管理产品

用于对称密钥或非对称密钥的生成、分发、存储等管理功能的服务端设备，且具有以下两种特征：

1. 含有64位以上密钥长度的对称密码算法、768位以上密钥长度的基于整数因子分解的非对称密码算法或128位以上密钥长度基于椭圆曲线的非对称密码算法；
2. 支持管理对象数量10000以上。

1.5 专用密码设备

含有专门用于电力、税务、公安、金融等领域的64位

以上密钥长度的对称密码算法、768位以上密钥长度的

基于整数因子分解的非对称密码算法或128位以上密钥

长度基于椭圆曲线的非对称密码算法的设备。

1.6 量子密码设备

以量子力学和密码学为基础，利用量子技术实现密码功能的设备。

1.7 密码分析设备

用于破解、弱化或绕过密码技术、产品或系统的分析设备。

**2． 测试、检查和生产设备**

2.1 密码研制生产设备

专门设计用于研制或生产1.1项至1.7项的设备。

2.2 密码测试验证设备

专门设计用于测量、测试、评估、验证1.1项至1.7项的设备。

**3． 软件**

专门设计或改进用于研制、生产或使用1.1项至2.2项的软件。

**4． 技术**

专门设计或改进用于研制、生产或使用1.1项至3项的技术。