# 硬件加密机 HSM 加密机 加密卡 PCIE加密卡

| | |
|---|---|
| 产品名称 | 硬件加密机 HSM 加密机 加密卡 PCIE加密卡 |
| 公司名称 | 上海安当技术有限公司 |
| 价格 | 80000.00/台 |
| 规格参数 | |
| 公司地址 | 上海市松江区泗泾镇赵非公路51号18幢1层116 |
| 联系电话 | 15830600995 |

# 产品详情

目前有两款
服务器加密机，分别为通用型服务器加密机和信创加密机(采用国产兆芯处理器和国产操作系统)，产品符合国 家商用密码管理和密码行业标准，经过了商密检测认证。加密机支持SM1算法、SM2算法、SM3算法、SM4算法以及RSA 算法、ECC算法和SHA-256杂凑算法，具有数字签名/验证、身份认证、数据加/解密、消息完整性验证、物理噪声源真随 机数生成等密码功能，同时提供安全的密钥管理机制和完善的设备管理机制。适用于电子商务、电子政务、CA认证、网上 银行等各类密码安全应用系统。

产品功能

配置管理

采用管理终端软件进行配置管理，配置管理命令的处理在加密机内进行。配置管理用于设置密钥、配置参数等工作，涉及一些敏感的信息，采用专线连接，信息只在专线上进行传输，大大减小了泄漏的可能性

多机并行

服务器加密机支持密码机群的多级并行工作、负载平衡和互为热备份，以适应系统性能的扩展，提高密码机群的可靠性和可用性。

实时监控

对加密机的运行状态进行实时监控。加密机的“ 看门狗 ”功能可在加密机软件系统死机时自动复位加密机，加密机的状态监控进程定期对主要硬件进行检查，如果发现错误就报警提示或者停止密码服务。

密码算法

数据加密：支持国产SM1、SM4分组密码算法；数字签名/验证:支持SM2、ECC以及RSA公钥密码算法；杂凑算法：支持SM3、SHA-256杂凑算法。

密码服务

按照《GM/T0018-2012密码设备应用接口规范》通过以太网接口对外提供密码服务：密钥生成与管理功能，加/解密功能；签名/验证功能；杂凑算法功能；数字信封；随机数生成功能，密码算法及密钥防护功能。

开机自检

加密机开机时会进行算法正确性检查、随机数随机性检查和密钥完整性检查。

产品优势

安全的密钥存储技术

加密机采用安全芯片与低功耗静态存储器相结合的方式实现密钥的安全存储。外部电源断开时，低功耗静态存储器改由内部锂电池供电，以维持密钥不丢失。需要销毁密钥时，用密钥销毁钥匙将密钥销毁锁旋转到销毁位置，密钥销毁电路会自动清除低功耗静态存储器中的所有密钥。

Linux操作系统定制

加密机采用的是定制的Linux操作系统。操作系统是从源代码开始构建的，构建过程遵循了小功能集原则，去除了所有不需要的组件、协议和服务，只保留了必须的功能。定制的操作系统具有很高的运行效率和安全性。

国产密码算法硬件实现

加密机采用PCI-E接口与FPGA算法卡连接实现高速的国产密码算法。FPGA芯片主要实现PCI-E控制器、加密机与各个算法芯片的数据转发、随机数采集及缓存等功能。这种方式实现国密算法具有高可靠性、低成本、高速度、微功耗以及保密性强等优点。

高效能绿色环保设计

在硬件层面，利用新的工艺和电路技术以及关键的电路和体系结构创新来降低功耗，同时实现佳性能，例如采用低功耗的嵌入式处理和便于低功耗设计的器件，降低系统的静态功耗；在软件层面，在了解每条指令所产生的功耗基础上，选择正确的编译方法，通过编译优化和指令排序等方法降低动态功耗。

### 高集成度设计

该加密机是基于本单位自行研制的主板和算法卡，具有集成度高、性能高、处理能力强、可靠性高、功耗低、功能强劲等特点。这种高集成度设计有效减少了组成系统的元器件和连线数量，提高了系统的稳定性和可靠性。

### 多机并行负载动态均衡技术

支持加密机群的多机并行工作、负载平衡和互为热备份，以适应系统性能的扩展，提高加密机群的可靠性和可用性。构成加密机集群时，通过采用集成在加密机API上的负载均衡技术，可以实现加密机自动负载动态均衡，使得加密机集群内每一台加密机都能得到充分利用，能够发挥佳的使用效率。