

物联网设备密码机



A 产品概述



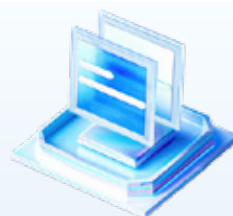
物联网设备密码机是以现代密码技术为核心，具有物理安全保护措施，具有完善密钥管理机制的硬件设备。物联网设备密码机为应用层密码设备，支持 SM1/SM2/SM3/SM4 国密算法，为业务系统提供安全的应用层密码服务，包括密钥管理、消息验证、数据加密、签名的产生和验证等，保证业务数据产生、传输、接收到处理整个过程的安全性、有效性、完整性、不可抵赖性。

A 产品功能



密码机管理功能

- 三层密钥体系
- 网络配置管理：密码机 IP 地址、子网掩码、网关、端口
- 权限管理：用户注册、登录、口令修改、注销；授权访问管理：增加 / 删除用户白名单



密码管理功能

- 密钥生成
- 密钥安全存储
- 密钥备份和恢复
- 密钥状态查询
- 密钥销毁



密码服务功能

- 数据加解密
- 签名、验证签名、会话密钥协商、数字信封
- 消息验证码 MAC 的产生、验证
- 消息杂凑
- 物理噪声源生成真随机数



服务接口

- 支持热备份、负载均衡
- 支持多操作系统：Sco Unix、AIX、HP-UNIX、Linux、Windows
- 支持 JAVA/C 程序语言
- 支持 JCE、PKCS#11、《公钥密码基础设施 密码设备应用接口》



密码算法

- 对称密码算法：SM1/SM4
- 非对称密码算法：SM2
- 杂凑算法：SM3

A 产品参数

产品参数					
SM1计算速率		800Mbps	物理特性	外形	2U标准机箱
SM2	签名速率	20000次/秒		体积尺寸	285 mm×145 mm× 38mm
	验证速率	18000次/秒		整机净重	12KG
RSA (2048bits)	密钥产生	30对/秒	电气特性	工作电源	交流220V± 10%，50± 1Hz，冗余电源（可选）
	签名速率	2000次/秒		功耗	260W
	验证速率	70000次/秒	环境指标	工作温度	0°C to +40°C
SM3计算速率		800Mbps		存储温度	-20°C to +55°C
SM4加解密速率		800Mbps		相对湿度	20%~80%
最大并发数		800	管理方式		控制台管理
MTBF		30000小时	网络接口		4个 10/100/1000M自适应
			工作协议		TCP/IP

* 规划中产品规格，具体当前可配置信息以详细产品手册为准。

- 物联网设备密码机采用防拆、防撬结构设计，利用全密封机壳、物理锁控制开启面板等技术为密钥的管理提供了强有力的保护。
- 密码机内置IP防火墙技术，提供IP包过滤，只有授权的用户才可以访问密码机，使用密码机的安全功能。
- 满足随意开关机的要求，可保证在出现意外掉电或人为随意关机的情况时，不会造成系统损坏，甚至崩溃等后果。

分层结构，逐层保护、密钥安全存储、密钥不可导出、支持人工密码机毁钥。

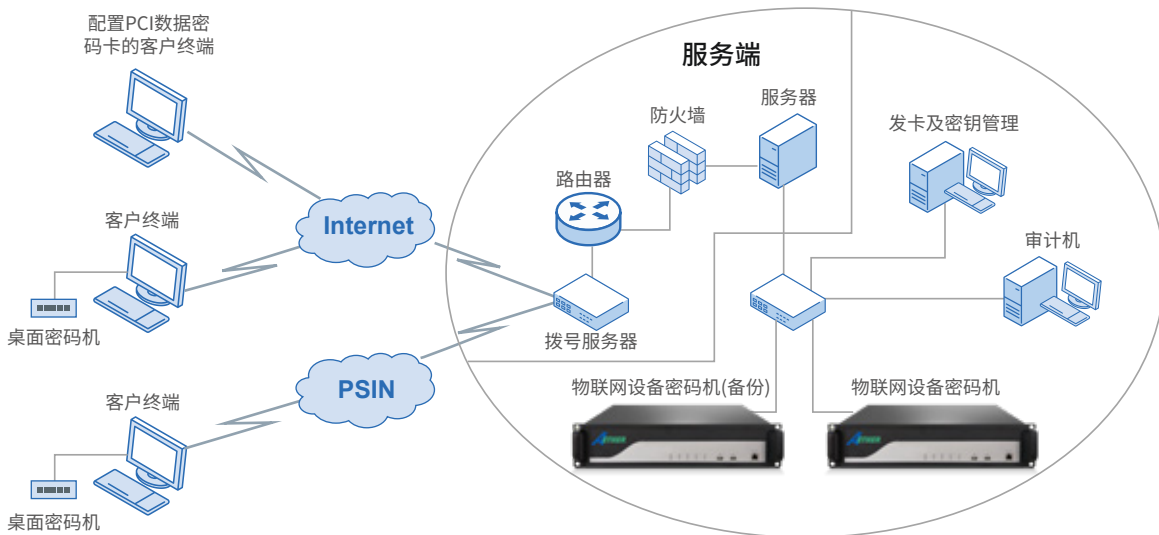


物联网设备密码机支持双机互备、多机负载均衡，同时支持故障自动切换、恢复。

服务器密码机全面支持国密算法SM1/SM2/SM3/SM4，提供支持Sco Unix、AIX、HP-UNIX、Linux、Windows等操作系统平台API，支持标准PKCS#11和JCE接口。

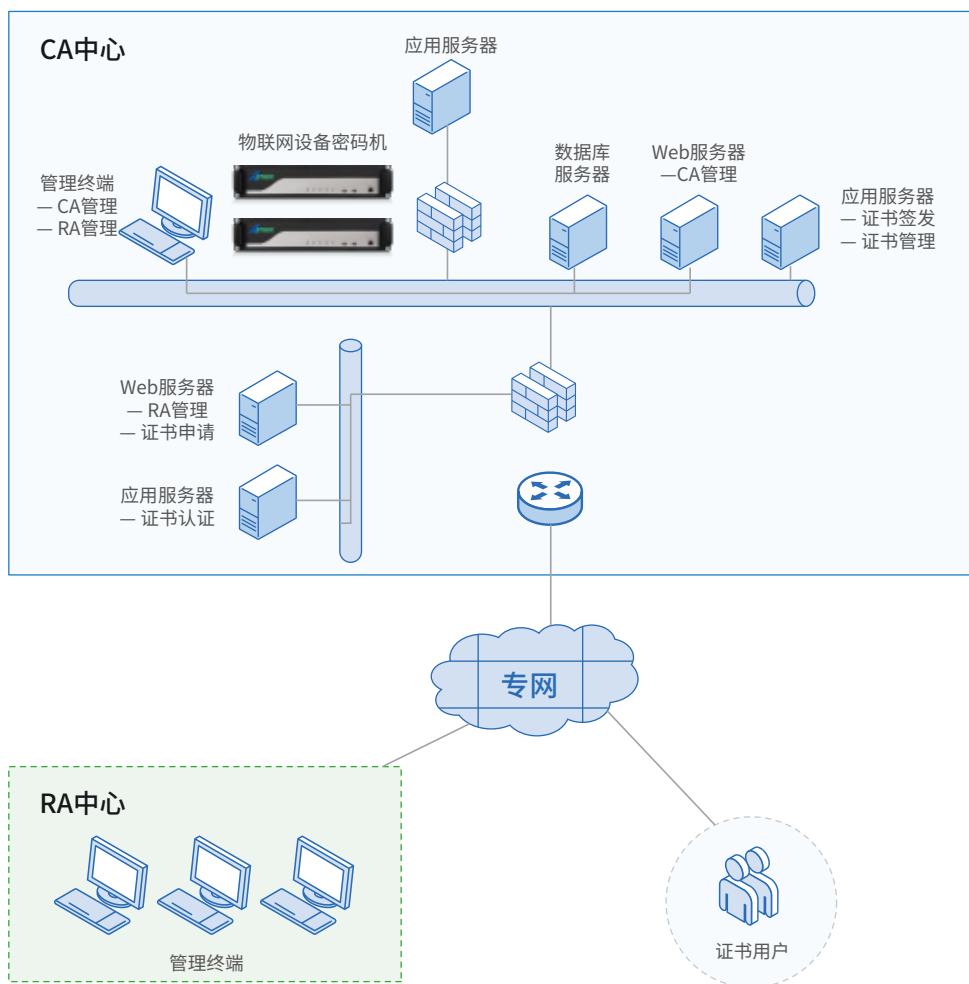
计算机安全模块系列应用

其典型配置如下：



基于安全模块系列的配置

在CA系统中的应用



CA应用部署图

本产品符合国家标准：

- GM/T 0030-2014 《服务器密码机技术规范》
- GM/T 0028-2014 《密码模块安全技术要求》
- GM/T 0002-2012 《SM4 分组密码算法》
- GM/T 0003-2012 《SM2 椭圆曲线公钥密码算法》
- GM/T 0004-2012 《SM3 密码杂凑算法》
- GM/T 0005-2021 《随机性检测规范》

深圳市永达电子信息股份有限公司
Shenzhen Y&D Electronics Information Co, Ltd.

★ 国家级高新技术企业 ★ 国家信息安全服务二级资质企业
★ ITSS二级资质企业 ★ 涉密信息系统集成甲级资质企业

地址：深圳市南山区科技北一路17号摩比天线大厦5楼

电话：0755-26727588 传真：0755-26727593

邮箱：sales@s-ec.com

官网：<http://www.s-ec.com>

版权所有 © 深圳市永达电子信息股份有限公司 保留一切权利。保留在没有任何通知或提示的情况下对本资料的内容进行修改的权利。



400-884-0006

