07 量子安全服务平台系统 WF-QSPS

产品简介（WF-QSPS）

一、产品概述

量子安全服务平台系统代表了密码安全技术的下一代发展方向，通过量子技术与经典密码学的深度融合，为用户构建面向未来的、可持续演进的安全防护体系，是保障数字资产长期安全的关键基础设施。量子安全服务平台系统是面向未来网络安全威胁的前沿密码安全解决方案，集量子密钥分发技术与经典密码技术于一体，为核心业务系统、远程接入认证、物联网终端等场景提供抗量子计算攻击的安全保障。

二、核心架构

1. 一体化软硬件平台

- **硬件平台**：专用量子安全服务平台硬件服务器
- **软件平台**：全功能量子安全服务平台软件系统
  - 预烧写入硬件平台，实现软硬一体化交付
- **合规资质**：已完成国家规定的入网安全评估认证

三、核心技术特性

2. 算法与标准支持

- **国密算法全支持**：SM2（非对称加密）、SM3（哈希算法）、SM4（对称加密）
- **量子密钥集成**：专为量子专用密码设备产生的密钥设计管理框架

3. 量子密钥全生命周期管理

管理阶段	功能描述

管理阶段	功能描述
生成与获取	从量子密钥分发网络实时获取真随机量子密钥
分发与更新	支持在线分发、定期更新量子密钥至终端设备
存储与管理	支持 30 万用户密钥数据的安全存储与关联管理
注销与恢复	完整的密钥注销机制与安全恢复流程

4. **高性能运行指标**

- **密钥生成速率**：≥1000 个/秒，满足高并发业务需求
- **数据存储容量**：30 万用户密钥数据的安全存储能力

四、核心功能模块

1. 量子密钥分发与应用

- **在线量子密钥分发**：实时将量子密钥应用于：
  - 业务系统远程接入认证
  - 用户身份鉴别与授权
  - 安全通信会话建立
- **终端密钥更新**：在网络条件具备时，为适配终端自动分发/更新量子密钥

2. 设备集成管理

- **支持设备类型**：
  - 量子增强型 IPsec VPN 安全网关
  - 量子增强型安全认证物联终端
  - 量子密钥安全注入设备

- **设备信息管理**：完整的设备注册、状态监控、策略配置功能

3. **远程管理与服务**

- **远程密钥分发**：按需或定期远程分发量子密钥
- **设备在线管理**：远程设备注册、信息更新、策略下发
- **双因素认证**：UKey 硬件令牌结合口令的双因素身份验证

4. **密码服务功能**

- **基础密码服务**：加密、解密、数据 MAC 计算
- **高级密码操作**：转加密、密钥获取、密钥更新
- **随机数服务**：支持多种量子随机源设备接入，提供真随机数生成

5. **安全管理体系**

- **三位一体关联**：实现用户真实身份、量子密钥、数字证书三者的安全绑定
- **密钥生命周期管控**：从生成到注销的全流程安全监控

五、应用场景

1. **远程安全接入**

- 量子密钥强化的 VPN 远程访问
- 抗量子计算的移动办公安全接入

2. **物联网安全**

- 量子增强的物联网终端身份认证
- 物联网数据传输的量子加密保护

3. **关键基础设施保护**

- 政府、金融、能源等关键领域的量子安全通信
- 核心业务系统的抗量子攻击防护

4. **身份认证体系**

- 基于量子密钥的双因素/多因素认证
- 高安全等级的数字身份管理系统

六、产品价值

1. 安全性提升

- **抗量子计算攻击**：利用量子密钥分发技术，抵御未来量子计算机的密码破解
- **真随机性保障**：量子随机源提供不可预测的真随机数

2. 合规与标准

- **国密算法合规**：全面支持国家密码管理局认证算法
- **行业标准符合**：满足关键信息基础设施的安全要求

3. 高效与易用

- **高性能处理**：千级/秒的密钥生成能力
- **集中化管理**：统一平台管理多种量子安全设备
- **灵活部署**：支持云端、本地化多种部署模式

七、服务与支持

- 完整的系统部署与集成服务
- 量子密钥分发网络对接支持
- 定制化应用开发接口（API）
- 持续的安全更新与维护

关键性能和技术指标

序号	关键特性与内容		技术指标
1	软硬件平台	硬件平台	1. 量子安全服务平台硬件服务器

序号	关键特性与内容		技术指标
2		软件平台	1. 量子安全服务平台软件系统 2. 软件系统烧写到硬件平台中。
3		✧ 产品资质要求	1.完成入网安评。
4	产品技术指标	算法支持	支持国密 SM2、SM3、SM4 算法；
5		量子密钥管理	支持对量子专用密码设备产生的密钥进行管理；
6		量子密钥分发	实现量子密钥的在线分发，并运用到业务系统远程接入认证、用户身份鉴别等应用场景；
7		量子密钥在线更新	网络条件具备时，支持在线为适配的终端密码设备分发或更新量子密钥；
8		设备管理	支持量子增强型 IPsec VPN 安全网关、量子增强型安全认证安全物联终端等设备管理，支持量子密钥安全注入设备信息管理；
9		远程管理	支持远程管理，实现按需或定期分发量子密钥的功能，支持设备注册，实现在线分发量子密钥及更新设备信息的功能。
10		双因素身份认证	Ukey 结合口令实现双因素身份认证功能；
11		量子密钥获取	支持从量子密钥分发网络获取量子密钥的功能；
12		安全管理	支持对证书用户真实身份、量子密钥、证书三者进行有效关联和安全管理。

序号	关键特性与内容		技术指标
13		✧ 随机源设备接入	支持多种量子随机源随机数生成设备接入；
14		密钥生命周期管理	具有密钥的全生命周期管理功能，包括密钥生成、申请、更新、恢复、分发、注销等功能；
15		密码服务功能	提供加密、解密、转加密、获取密钥、密钥更新、计算数据 MAC 等密码服务功能
16		密钥生成速率	以数字证书为安全保障，可有与经典非对称应用高效对接；
17			每秒生成密钥速率 >=1000 个/秒；
18		密钥数据存储量	支持存储 30W 用户密钥数据。