

产品概述

天融信密钥管理系统是一款采用硬件安全模块保护密钥安全的高可用、可扩展的企业级密码产品。支持包括对称密钥、非对称密钥、数字证书等多种加密对象的统一管理。通过对加密对象的统一管理,可简化密钥管理操作,使加密变得更易于配置和管理,减少了密钥管理系统的维护成本,满足企业多应用多业务场景的密钥管理需求。



产品功能

加密对象全生命周期管理

提供对称密钥、非对称密钥、数字证书等加密对象的状态管理和属性管理。完成对加密对象的生成、存储、激活、分发、更新、注销、销毁和删除等全生命周期管理操作及加密属性的获取、添加、修改和删除等操作。

多种算法密钥管理

支持SM1、SM4、AES、3DES等对称算法密钥的生成与管理;支持SM2、RSA、ECDSA等非对称算法密钥的生成与管理;支持HMAC-SM3、HMAC-SHA512等密钥的生成与管理。

密钥安全生成

密钥管理系统密钥采用由国家密码管理局批准使用的物理噪声源产生器芯片生成的随机数,密钥生成后由硬件密码模块中的系统保护密钥加密后存储。

密钥安全下发

客户端业务系统密钥获取操作支持SSL数字证书、密钥用户名和口令及wrapping key等多种认证及加密方式,几种方式可灵活组合配置。保证敏感信息在经过网络传输过程中的安全性,避免接口通信信息泄露、中间人攻击、重放攻击等可能性。

典型应用

密码技术作为保障金融信息安全的核心技术,在金融领域得到广泛应用。中国证券监督管理委员会提出逐步在网上证券、网上期货、网上基金等业务中规范密码应用,推广使用合规有效的密码算法和密码产品。

通过提供密钥管理系统及密码卡等密码产品,完成接入客户端数字身份认证,确保登录身份信息的合规合法。

