

天融信协同签名系统

www.topsec.com.cn

产品概述

天融信协同签名系统(简称:TopCSS),采用先进的分布式密钥管理技术、国产化SM2算法,和国密标准的随机数发生器。协同签名系统摆脱智能密码钥匙等硬件存储介质的束缚,将用户终端设备(如手机、平板电脑、专用手持智能终端、PC等)作为客户端,通过在服务端和客户端分别存储部分密钥,实现密钥安全的协同生成、协同签名、协同解密,可以为政务、金融、医疗健康、电子证照、移动办公等多个领域,提供多场景的、安全可靠的跨平台协同签名服务。

产品功能

基于国产密码算法

支持SM1/SM2/SM3/SM4国产密码算法,确保签名过程的安全性和数据的机密性。

支持丰富的协同应用

- a. 协同扫码服务:支持使用协同签名客户端进行安全可靠的移动扫码签名、移动扫码登录等操作;
- b. 协同签章服务:支持使用协同签名客户端进行安全可靠的移动电子签章操作。

GM/T 0105 随机数发生器

客户端提供符合GM/T 0105标准的软件随机数发生器,确保数字签名和认证过程中生成的随机数具备高度的随机性和不可预测性。

协同密钥策略配置

支持多样化的协同密钥生成策略配置,支持设置密钥生存周期,支持对协同密钥的创建数量进行限制与管理。

数据备份与恢复

提供基于(3,5)门限机制的数据备份恢复服务,可对协同密钥、系统配置、应用信息等重要数据进行备份和恢复。支持定时备份、导入导出备份文件。

丰富的密码运算服务

支持协同签名、协同解密,同时支持非协同对称加解密、签名验签等功能,满足用户多样化安全需求。



产品特点

高安全性

- a. 协同密钥安全性:系统采用密钥分割技术,将传统的单一密钥分割为客户端密钥和服务端密钥两部分,分别密文存储在服务端和客户端上,保障协同密钥的安全性。
- b. 通信链路安全性:在协同签名客户端与服务端间,建立基于国密SSL协议的安全通信链路,确保协同签名客户端到服务端的数据传输的机密性和完整性。

全面兼容信创平台

支持Android、iOS、鸿蒙、Windows、Mac、Linux、国产信创操作系统等主流客户端操作系统,支持全部国产信创硬件平台,可以在不同的平台上使用统一的协同签名机制,实现跨平台的身份认证和签名验签服务。

多CA适配

支持内置CA以及第三方CA的适配。满足组织机构内部统一便捷的证书管理需求,同时支持灵活对接外部认证体系,适配多种业务场景与安全策略。

易用性

基于协同签名技术,在移动端和桌面端无需智能密码钥匙等硬件介质的参与,即可进行私钥相关的操作,避免了硬件介质携带的不便性,以及易丢失、易损坏等问题。

产品资质

《商用密码产品认证证书》