南京壹证通信息科技有限公司
Nanjing Eztoo Information Technology Co., Ltd.

南京壹证通信息科技有限公司成立于2016年8月18日，作为行业内领先的密码服务商，壹证通致力于推进中国可信身份生态建设，包含数字身份、国产密码、信息技术创新、平台服务、教育培训等方面的应用和发展，为互联网时代的新基建提供安全保障和可信身份服务。壹证通始终坚守“让信任更简单”的使命，打造绿色互联网身份生态圈。

解决方案名称：基于国产密码算法的密码服务平台金融证券业解决方案

提供单位：南京壹证通信息科技有限公司

产品/解决方案（实践案例项目）介绍：

案例背景：

目前，在我国大多数领域占主导地位的密码算法是国际商用密码算法，核心数据采用国外密码算法进行数字加密，这给我国金融证券业的信息安全带来很大风险隐患。因此，逐步推进金融证券领域国家密码算法的行业应用，增强金融证券业信息系统的自主可控能力显得尤为迫切。当前，随着信息技术的发展，密码技术在商业应用领域不断扩宽。商用密码技术已广泛应用于金融、科技、文化和社会生活的各个领域。在金融证券业，以网上交易、网上开户等业务为代表的互联网证券业务迅猛发展，方便了广大投资者通过互联网办理各类业务，促进了资本市场创新发展。然而，当前证券期货行业使用的各类商用密码应用，如数字加密、签名、验签等普遍采用的是国外的商用密码技术，各类支撑此类应用的安全设施、安全产品均构建于国外的基础算法和密码技术之上，摆脱不了受限、受制、受控于人的被动局面，这对于整个行业的自主可控、安全稳定发展构成巨大挑战。金融信息安全是国家信息安全的重要组成部分，密码的安全可靠和科学规范应用关系到我国的金融安全。

方案简介：

（1）有效的密码管理手段：密码服务中台将对密码设备接入集中管理，运维监控应用系统集中认证，密码使用统计密码资源使用态势感知，提前预警扩容密钥全生命周期安全可控。

（2）统一的密码服务入口：对外提供密码服务统一标准接口，对内兼容适配多硬件密码设备。

（3）可靠的CA证书兼容及业务连续性保障：对外提供证书业务统一标准接口，对内兼容适配多家CA发证业务接口，根据路由策略实现证书业务切换。

（4）功能融合扩展的支撑：密码技术严谨性与系统应用场景灵活性的融合，基于密码技术扩展密码应用场景与使用范围。

（5）整体安全服务的融合点：可选结合

其他密码产品，满足全方位密码安全需求一次建设，多应用场景使用。

方案优势：

（1）同时支持国际标准算法、国产标准算法，满足密码应用安全性评估（密评）要求，便于国密改造项目实施。

（2）实现密码资源的池化管理，即在实现密码设备集中管理的同时，将密码设备抽象为密码资源，由中台根据应用系统的密码业务需求，合理分配调度密码资源，实现密码资源最大化利用，同时也增强了密码应用的可靠性，保障支撑庞大的业务系统；基于微服务容器技术，便于密码资源的大规模快速部署，易管理，保障密码服务建设的多种虚拟化技术路线；

（3）基于云原生技术，支持云密码服务部署设计，可将密码中台部署在云上，即云密码服务中台，动态分配资源，充分利用云计算模型的工作负载，实现信息资源共享和按需使用。

（4）负载均衡综合管理。负载均衡综合管理为业务系统调用密码设备提供密码设备资源的统一调配，根据业务配置选择适配的负载算法及运算接口，并负责对密码请求的来源进行校验，将合法的请求均衡的发给各个运算节点进行计算。密码服务负载均衡支持轮询、最小连接、IP哈希、权重等常用负载均衡策略，同时，支持虚拟资源池的按权重分配，即通过为应用系统分配密码虚拟机资源个数的方式，来达到多个应用系统对密码运算资源的按需分配。

（5）支持多CA的数字证书综合管理。为了保障系统能相对透明的使用各种证书，密码安全服务平台设计了数字证书综合管理功能，主要对数字证书签发和使用，其中包括数字证书机构管理，存储介质的品牌、序列号、驱动、版本、证书生命周期提醒等进行统一管理，在用户使用过程中一方面减少操作步骤，一方面降低管理和运维成本。应用单位只需对接平台接口，就可以使用平台支持多家CA机构签发的证书。