基于信创化商用密码算法的证券网上交易数据安全体系研究

陶剑峰 | 中信建投证券信息技术部总监

目录

项目背景-公司简介

中信建投证券成立于2005年11月2日，是经中国证监会批准设立的全国性大型综合证券公司。主要股东有北京金融控股集团有限公司、中央汇金投资有限责任公司与中国中信集团有限公司。

20年	30个	300个	5家	1218万次
深耕证券交易	省、自治区和直辖市	证券分支机构	全资子公司	网上交易软件下载

2016年香港联交所上市，2018年在上海证券交易所主板上市。中信建投证券在为政府、企业、机构和个人投资者提供优质专业的金融服务过程中建立了良好的声誉，是国内证券行业首批6家并表监管试点企业之一，也是首批监管白名单企业之一。

项目背景-政策

国家战略

近年来金融数据安全上升到国家安全高度，国家相关部门和监管机构站在国家安全和长远战略的高度，提出了推动国产化实施，加强行业数据安全可控的要求。

政策法规

2020年《中华人民共和国密码法》，2021年工信部发布《“十四五”软件和信息技术服务业发展规划》进一步规范了信息技术创新和应用的要求。

行业监管

证监会根据《证券期货业密码应用工作规划》作出金融行业全面推行“国密”化改造，实现金融IT基础设施的国产化全面应用，保障证券行业的信息数据安全。

行业现状

证券行业沿用国际通用软硬件和密码算法体系，不符合国家信息安全战略和相关政策法规的要求，对证券行业的稳定发展造成潜在的信息数据安全风险。

项目背景-痛点

国外技术垄断

传统证券交易系统严重依赖国外IT基础软硬件（如Oracle/DB2数据库、VMware虚拟化、IBM/HP小型机）和底层技术，存在“卡脖子”的供应链断供和安全漏洞无法自主修复的巨大风险。

密码算法安全风险

原有信息系统普遍采用国际通用密码算法（如RSA、SHA-1等），存在潜在的安全后门风险，且不符合国家《密码法》、《网络安全法》以及金融行业监管机构（如证监会、中国人民银行）对核心系统使用国产密码算法（SM2/SM3/SM4等）的强制合规要求。

敏感数据全生命周期较弱

证券行业涉及海量高敏感数据（客户身份信息、资产数据、交易委托记录等），在传输、存储和处理过程中面临泄露、篡改和窃取风险。传统防护手段分散，未能形成基于国密算法的统一、高效的数据安全防护体系。

项目背景-推广意义

1

保护客户数据安全

密码安全技术保护交易数据的机密性、完整性和可用性，防止非法访问和篡改，确保客户资产的安全。

2

维护市场稳定

证券网上交易数据的泄露或篡改可能引发市场恐慌和不稳定，密码数据安全是维护市场秩序的重要保障。

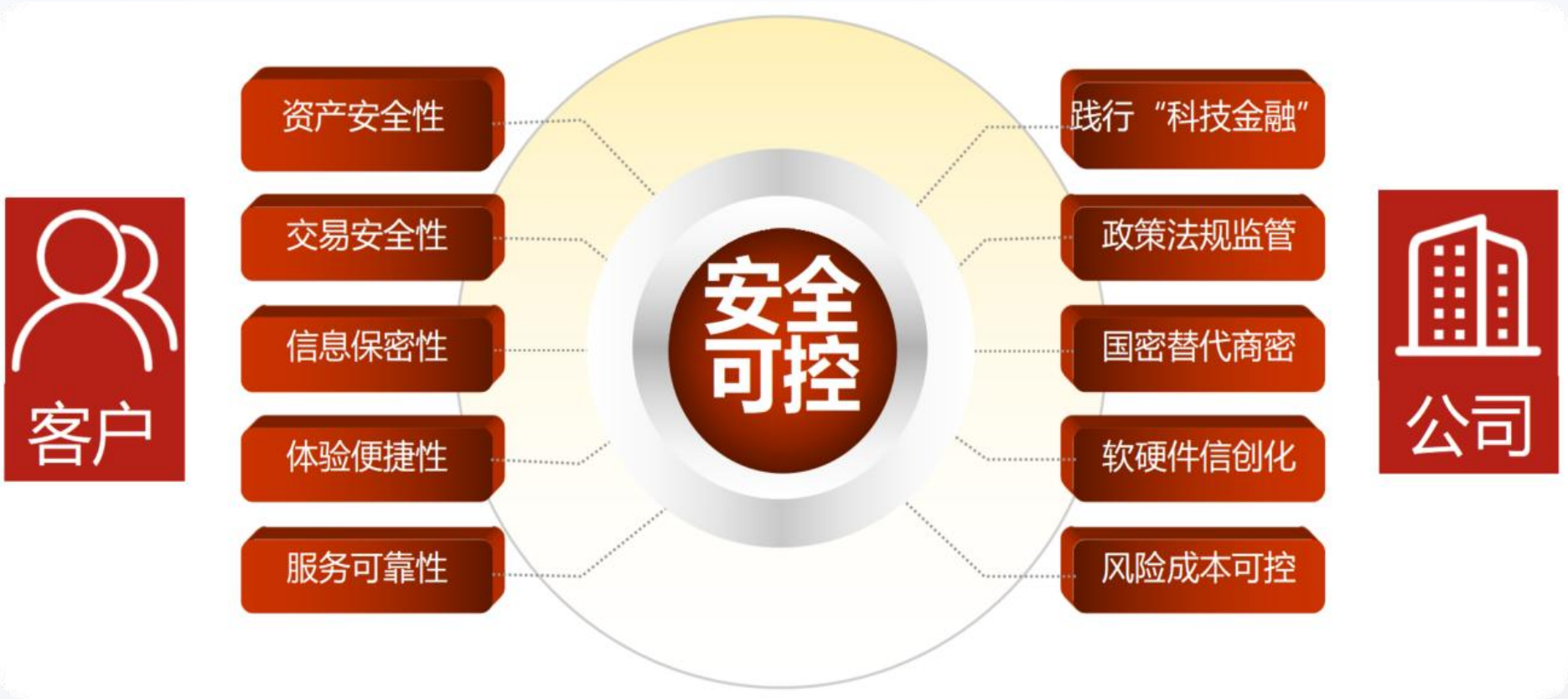
3

符合数据法规要求

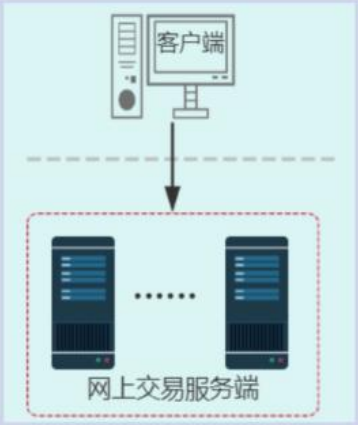
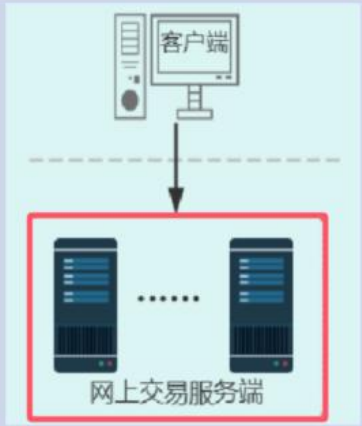
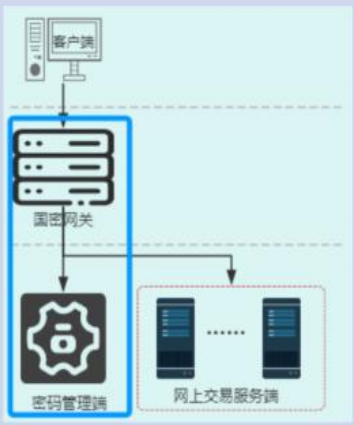
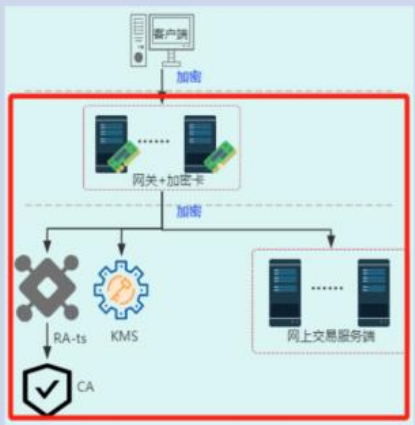
行业有严格的法律法规要求保护客户数据和交易数据的安全，密码数据安全技术是满足合规要求的重要手段。

目录

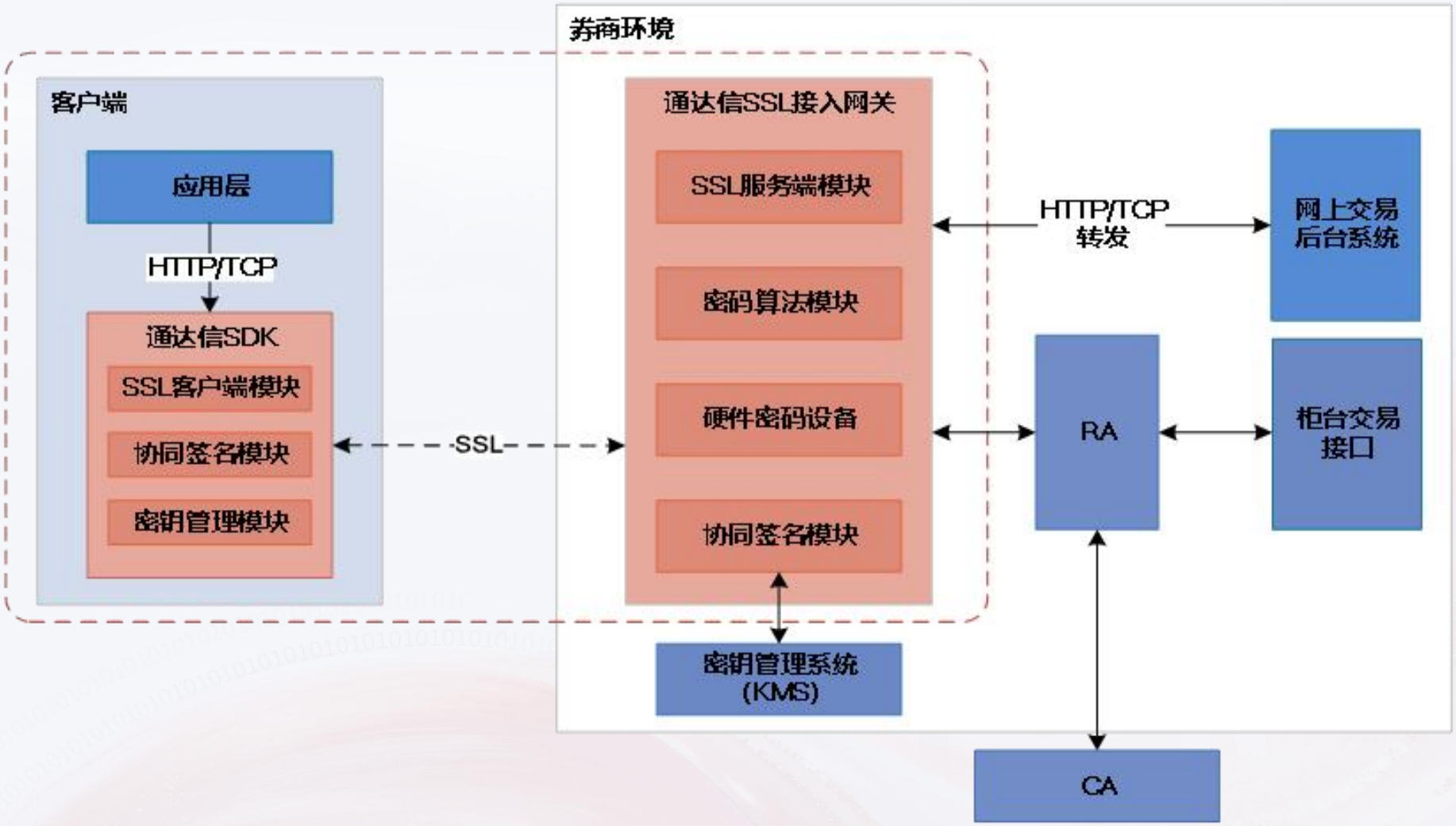
解决方案-目标


客户
资产安全性
交易安全性
信息保密性
体验便捷性
服务可靠性
安全可控
践行“科技金融”
政策法规监管
国密替代商密
软硬件信创化
风险成本可控
公司

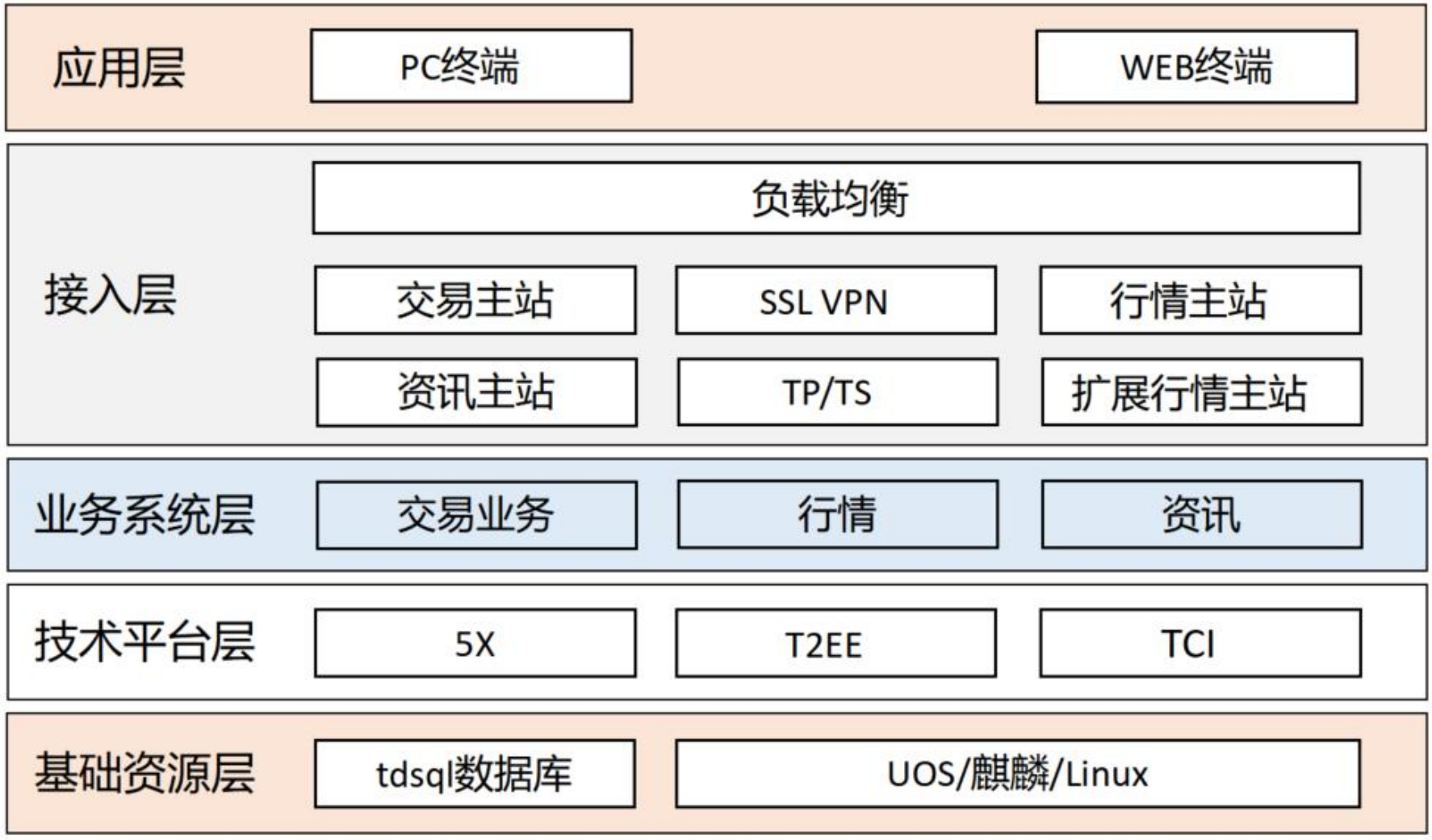
解决方案-对比

	改造前	信创改造	商密改国密	国密+信创
系统结构				
安全性	★	★★	★★★★	★★★★
可控性	★	★★★	★★★	★★★★★
		行业通用方案		中信建投方案

解决方案-国密

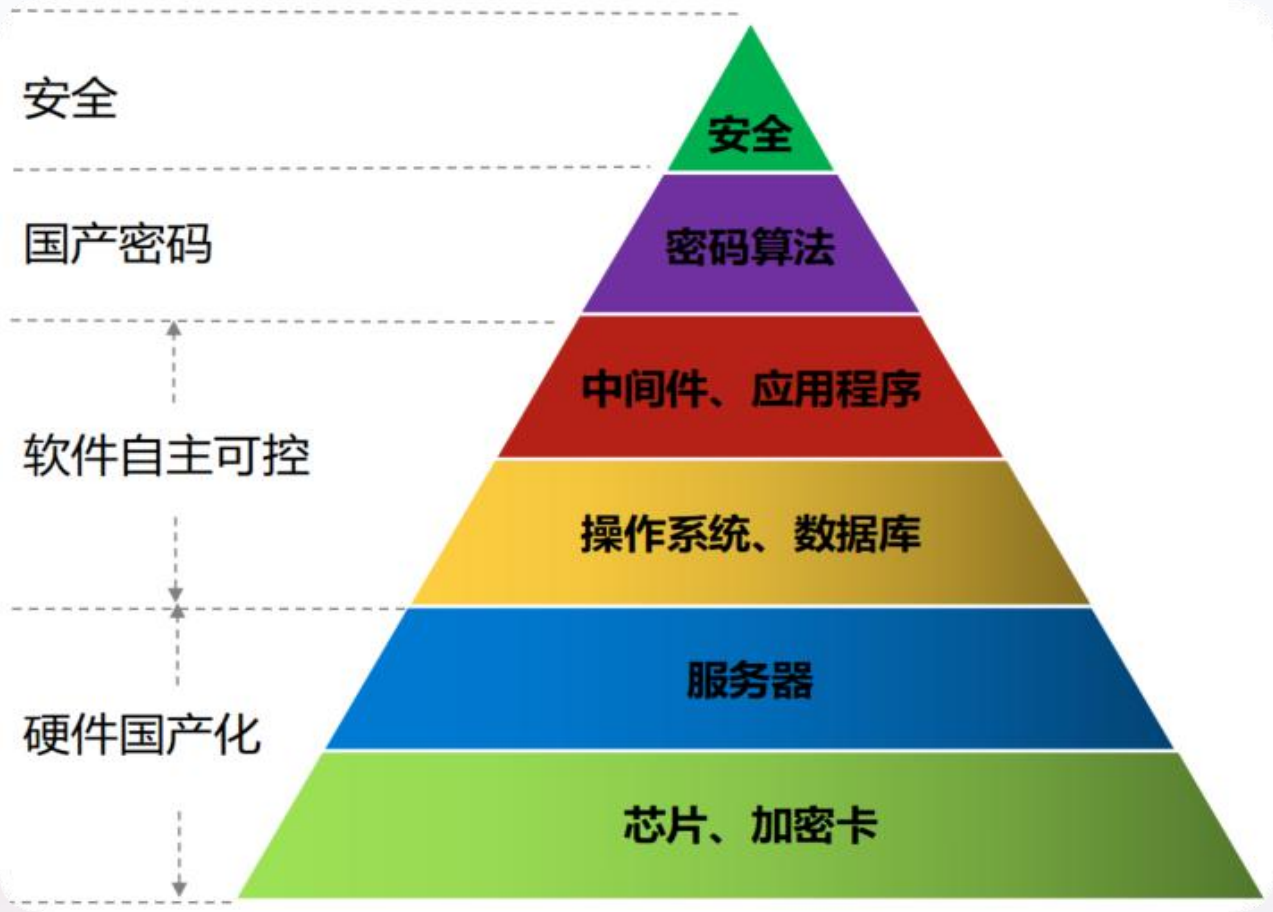

券商环境
客户端
应用层
HTTP/TCP
通达信SDK
SSL客户端模块
协同签名模块
密钥管理模块
SSL
通达信SSL接入网关
SSL服务端模块
密码算法模块
硬件密码设备
协同签名模块
密钥管理系统
(KMS)
HTTP/TCP
转发
网上交易
后台系统
RA
柜台交易
接口
CA

解决方案-信创


应用层
PC终端
WEB终端
接入层
负载均衡
交易主站
SSL VPN
行情主站
资讯主站
TP/TS
扩展行情主站
业务系统层
交易业务
行情
资讯
技术平台层
5X
T2EE
TCI
基础资源层
tdsql数据库
UOS/麒麟/Linux

解决方案-创新点

交易数据密码方案实现从硬件国产化、软件自主可控、国产密码算法改造保障数据安全可靠。



解决方案-创新点

国密加固

- 商用密码国产化替代
- CA体系的强身份认证
- 协同签名保障密钥安全
- 密码设备增强安全性

全栈信创

- 芯片、服务器、加密卡信创化
- 操作系统、中间件、数据库、应用程序信创适配

行业首例

- 证券行业首例国密+信创
- 为行业国产化替代提供参考

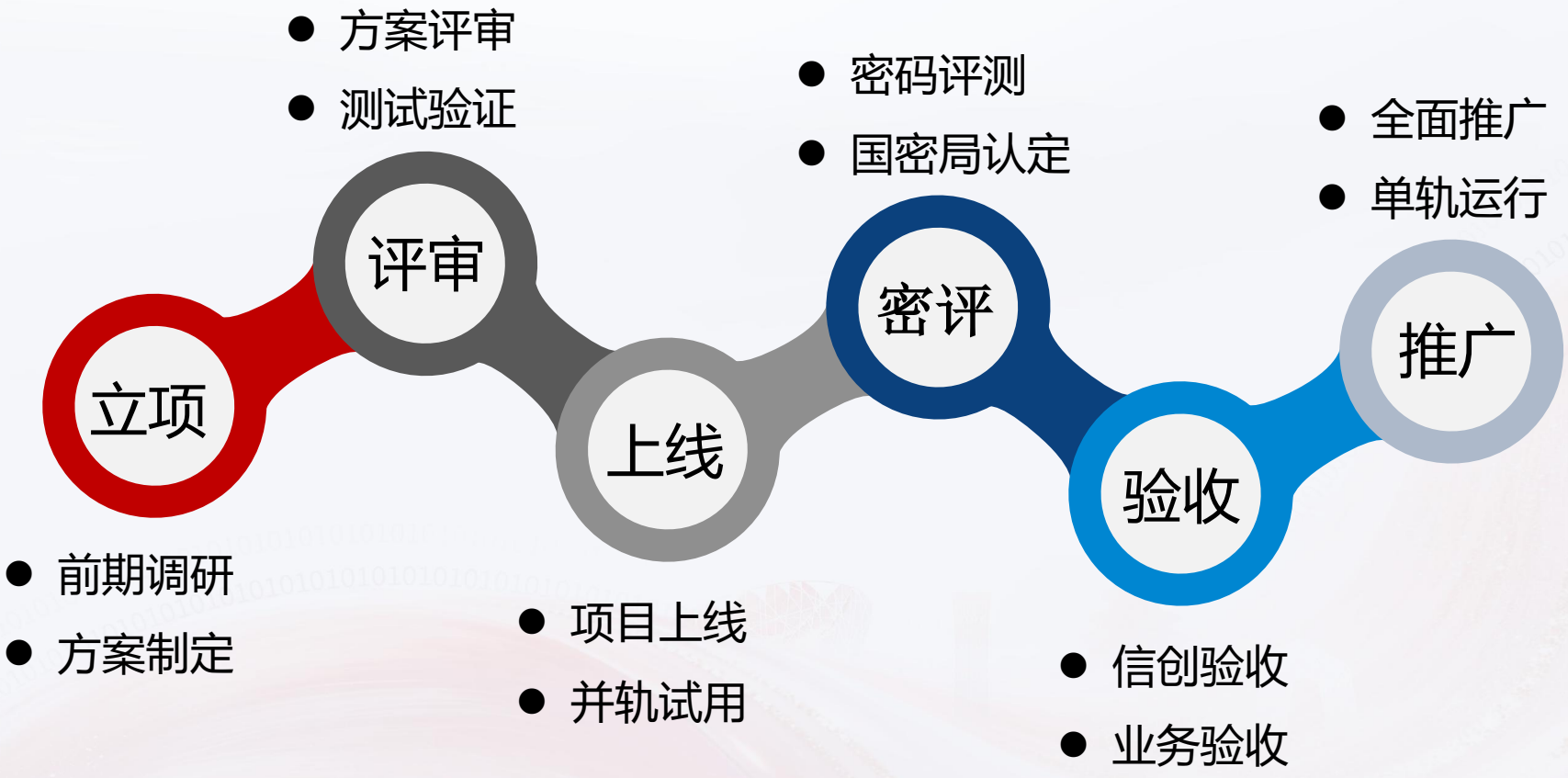
降本增效

- 节省软硬件、开发、人力资源
- 提升安全和自主可控

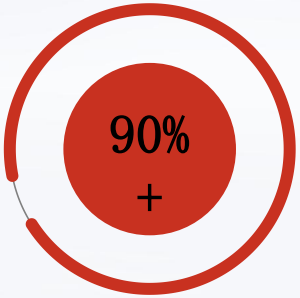
目录

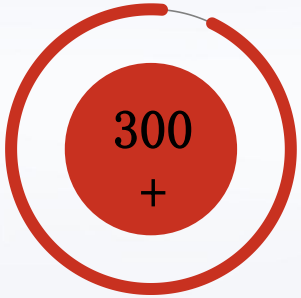
应用成效-历程

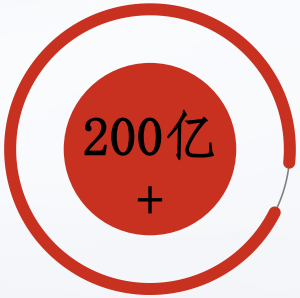
信创化商密改造历时3年

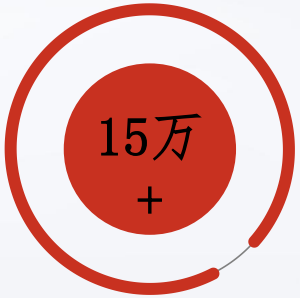


应用成效-效果









国密流量占比

国密流量占比超90%，排名行业第一

覆盖客户范围

覆盖全国300多家营业部客户

日均交易金额

日均交易金额超200亿元

日均用户数量

日均活跃用户数量超15万

沪深两市成交金额创历史最高记录的2024年10月8日，系统交易额达420亿元，运行平稳

应用成效-效益

解决行业核心痛点，构建数据密码安全体系

证券行业长期依赖国外密码算法（如RSA、AES）和基础设施，存在供应链“断供”风险，SM系列方案替代，可保障金融安全。

带动经济，多层次信创化安全防护

采用软硬件国产化，信创软硬件（加密卡、KMS）销售带动国产产业链增长，提高了市场规模，提高了系统的自主可控能力。

数据要素赋能，提升数据安全性

国密SSL协议降低数据泄露风险，渗透测试中拦截100%中间人攻击，SM4加密+国产数据库（Vastbase）使数据泄露修复成本降低70%。

应用成效-荣誉

行业奖项4项

- 中信集团第二届“绽放杯”银奖
- 第二届“金信通”金融科技创新应用“最具商业价值案例”
- 第二届云系统“稳定安全运行优秀案例”
- 证券业协会统一测试“最佳贡献单位”

行业文章4篇

- 金融电子化2篇-《证券公司交易数据密码安全体系研究》等
- 交易技术前沿2篇-《信创技术在证券交易中台的应用与研究》等

专利、著作权8项

- **专利：**《带自选股云同步图形用户界面的显示屏幕面板》、《一种智能证券交易系统、方法、设备及存储介质》、《一种适当性检测方法、系统、装置及电子设备》、《后量子密钥协商方法和设备》
- **软著：**《网上交易自选股云同步程序软件V1.0》、《风险评测V1.0》、《后量子协同签名系统V1.0》《NSAE应用安全网关V1.0》

目录

商业价值

行业示范价值

证券行业首次集成信创和商密的改造，方案已适配X86/ARM架构、麒麟/统信OS、Vastbase/达梦数据库，可快速复制至证券全行业，目前已经有10余家券商复制相同案例。

模式可持续性

国家密码数据算法赋能产业金融，提升产业链授信能力，以全栈国产化技术和数据要素安全流通机制为核心，形成金融信创领域“技术、标准、商业”三位一体的解决方案。

提升交易安全性与信任度

国产商用密码算法，能够有效保障数据机密性、完整性与可用性，防止交易数据被篡改或泄露，增强投资者对交易平台的信任。

满足国家法律法规要求

符合《网络安全法》、《数据安全法》、《个人信息保护法》、《密码法》以及证监会、证券业协会的一系列指引和规定。

目录

未来展望

证券行业推广

行业内证券、基金等友商进行技术与经验分享，同时也成为安全厂商推广信创国密方案的经典案例。

建立持续的安全评估和风险管理机制

随着信创和国密的深入推进，安全评估的审计和应急风险处理，需要建立持续的管理机制。

安全协议更加完善

未来，安全协议将更加完善，能够有效防止各种网络攻击和数据泄露，为证券交易数据的安全提供更加全面的保障。

未来展望

量子计算飞速发展、持续突破“量子优越性”

中国		美国		加拿大
 祖冲之三号 105量子比特 超导量子	 九章三号 255光子 光量子	 悬铃木 72量子比特	 Willow 105量子比特 超导量子	 北极光 219光子 光量子

2022年3月，麻省理工学院与阿布扎比技术创新研究所合作发布《从今天起，直面明天的量子黑客》

先存储、后破解风险（Steal Now Decrypt Later 攻击），现实威胁

美国长期从事信息收集工作，等待技术解密时刻的到来（史上最成功的“先存储后解密”行动之一：维诺那行动）

针对量子计算对传统密码体系的严峻挑战，物理学界和数学界分别提出两种密码技术体系：
基于物理特性的量子密钥分发技术 、基于数学难题的后量子密码技术 。

“物理”方法

量子密钥分发（QKD）

核心特点

- **物理安全**：量子特性确保真随机性，密钥分发过程“不可窃听”，能主动检测窃听行为
- **可长期免疫威胁**：安全性不依赖数学困难问题，仅由量子物理特性保障，无惧量子计算进步

局限性

- **传输距离有待提高**：长距离传输需依赖量子中继技术
- **功能性单一**：仅分发密钥，需搭配传统加密算法实现签名/认证等其他密码功能

“数学”方法

后量子密码（PQC）

核心特点

- **数学安全**：不满足绝对安全，安全性基于量子难以求解的数学困难问题
- **密码功能丰富**：PQC不仅抗量子，还能直接支持数字身份、签名验证等完整PKI密码体系

局限性

- **假设依赖性风险**：安全基于“量子无法破解数学难题”的假设，一旦这些基于数学问题的密码算法被新型量子计算突破，需再次进行全面的算法升级，升级工程化周期约十年
- **工程替换代价高**

QKD 和 PQC 各有长处、也各有盲区，谁也不能完全替代谁。与其“二选一”，不如“强强联合”！

谢谢观看