C3安全峰会
CYBER | CLOUD | COMMUNICATION

从实时交易安全防护探讨数据资产的保护

陆光明
亚信安全

目录
CONTENTS

数据资产保护面临网络信息安全重大挑战

美国国家安全局陷入斯诺登之后最大泄密风波

NSA承包商哈罗德•马丁于2016年8月27日因窃取国安局数据被捕，马丁与曾揭露美国政府大规模监听行动的斯诺登受雇于同一家公司，马丁还被怀疑掌握了NSA的“源代码”，这些源代码通常被用来入侵俄罗斯、中国、伊朗等国的网络系统。调查人员在马丁家中和车内搜出美国政府高度机密文件的复印文本和数字文档，其中数字文档至少有几TB，还包括6份“敏感情报”。

12306密码泄露事件

2014年12月25日晨，很多旅客在12306网上购票，发现身份信息已被他人冒用。警方当晚将信息犯罪嫌疑人抓获。嫌疑人利用“撞库”攻击拿到10万旅客密码。

俄罗斯央行遭黑客攻击 3100万美元不翼而飞

2016年12月，俄罗斯中央银行官员瑟乔夫证实，该行电脑系统遭到了黑客入侵，犯罪分子从银行的代理账户中窃走了20亿卢布（约合3100万美元）的资金。瑟乔夫透露，黑客是通过伪造一名用户的证书进入的这些账户。

某大型银行支付用户存款遭窃

某大型银行电子支付是一种通过手机短信快速验证的转账服务。2015年6月-7月间，犯罪份子通过截获系列短信、获取储户信息，伪装身份转移资金。

企业数据资产保护从实时交易安全防护做起

企业数据资产泄露主要原因是黑客/黑产的攻击破坏和内部人员信息出售，最终体现于用户端的实时交易，如银行用户因信息劫持遭恶意转账，给企业信誉和个人财产造成重大损失。所以，做好实时交易安全防护是企业数据资产保护直接有效的方式。

实时交易安全分析-身份认证能力有待提升

银行在用户端实时交易的身份认证能力现状：

- **多因素认证的短信验证码方式应用广泛，但易遭劫持利用，如实施恶意转账**

  ----木马病毒，劫持短信验证码信息。

- **移动端生物识别技术成为应用趋势，但受限于终端普及、应用的可靠性、稳定性**

  ----终端的生物采集设备普及率受限；单一验证仍不可靠；复杂环境使用困难。

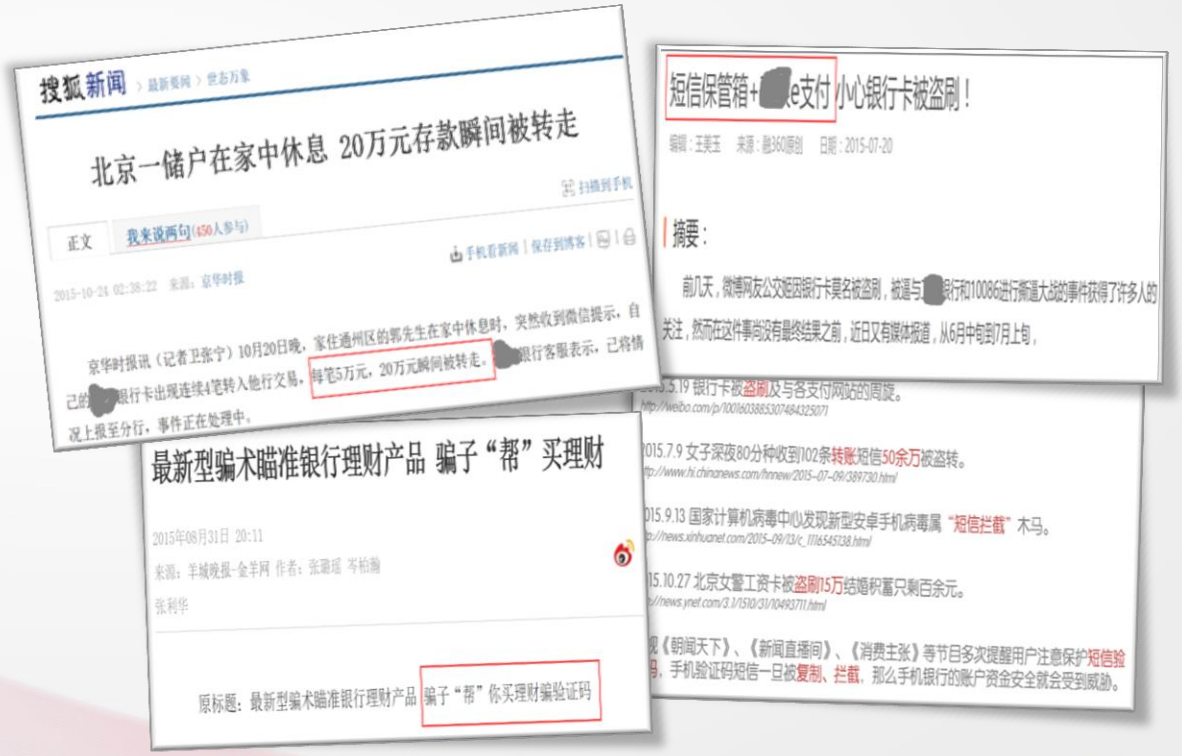
- **手机端的高级别安全（CA）需求与用户体验矛盾**

  ----一般需要外置设备，携带保管不方便。

- **-传统的身份证识别技术置换成本高，且不利于户外移动办公**

  ----传统“读卡设备+后端信息验证”在新一代身份证后需要大量设备替换；户外营销或上门服务携带不便。

媒体曝光了数起因“短信”劫持引起的财产损失安全事件



实时交易安全分析-反欺诈业务模型有待优化

薅羊毛给企业营销活动带来直接经济损失，让真正想参与活动的真实用户无法受益：

- 机器垃圾注册、猫池注册，造成大量虚假无效用户，参与大量活动套利

  ----大多企业风控模型（反欺诈与信用评估）是基于企业内部数据来做，或使用外部数据不够及时准确，无法更客观、精确的核实用户身份、参加活动真假。

薅羊毛给企业营销活动带来损失

实时交易安全解决思路

从用户交易过程与安全防护生命周期出发，建立“事前预防、事中防控、事后分析”的面向全渠道全客户全认证策略的安全防护管控模式，实现交易安全防护运营的自动化、智能化 。

风险预防：在已识别欺诈及风险点的基础上，调 整应对策略，预防欺诈

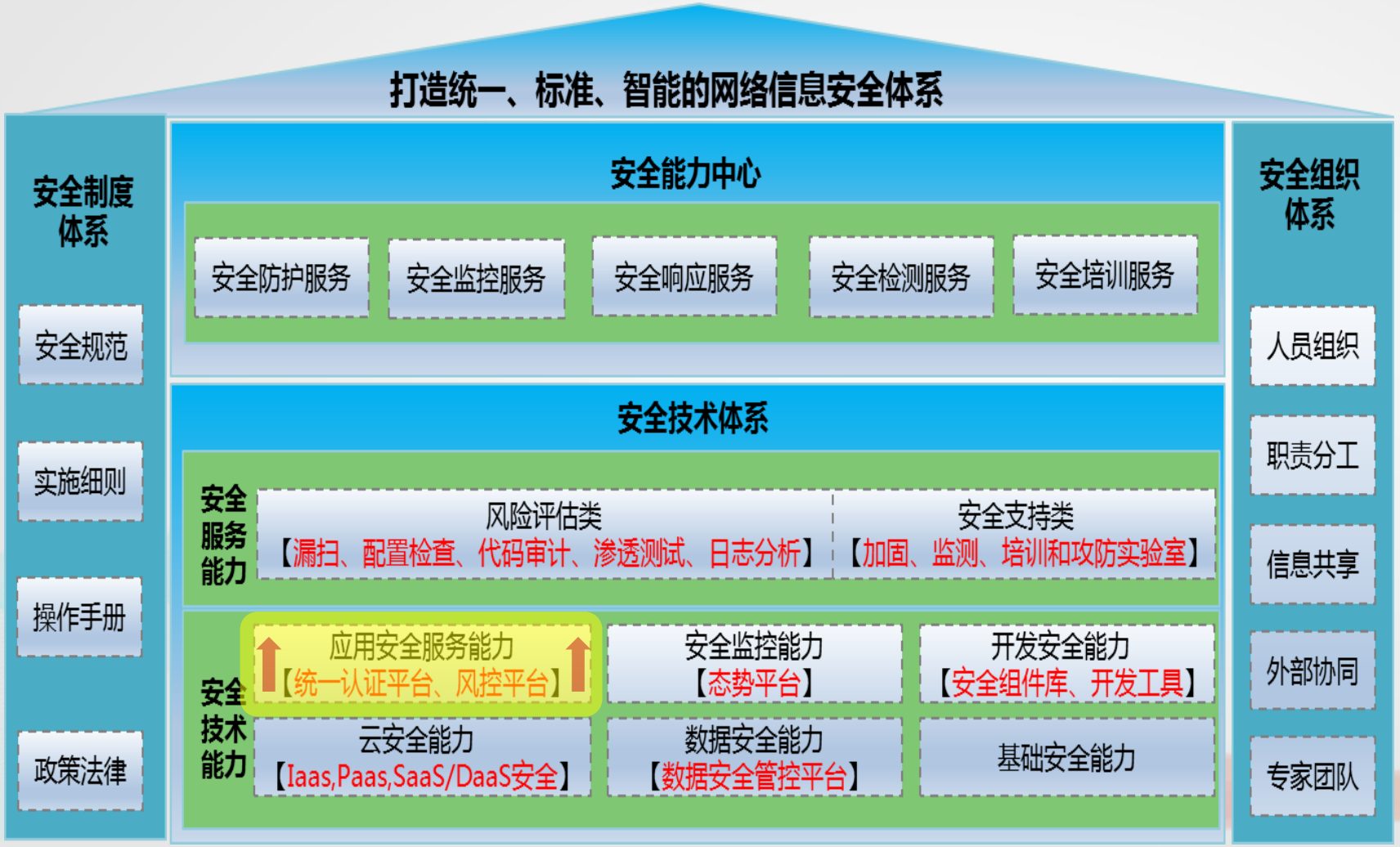
风险预测：发现可能存在的异常行为和可疑场景，并做定量和定性计算

风险处置：反馈风险等相关信息给安全中心和业务系统，进行确认并处理欺诈

风险分析：分析欺诈过程，发现交易实体、行为及管线，明确欺诈模式

事前预防　事中防控　事后分析

构建实时交易安全防护体系，保护数据资产



- 企业信息安全与用户端交易安全防护是系统工程，需要有网络信息安全体系的**顶层设计思维与全局产品观。**
- 交易安全实时防护重点探讨提升网络信息安全体系中的应用安全服务能力，体现为**身份认证能力、身份核实能力、全渠道识别欺诈行为能力**，解决交易中的信息劫持、身份冒充、欺诈与信用问题。

交易安全实时防护重点提升三个能力

提升身份认证能力

当前，用户端交易安全防护最为急迫且存在安全隐患的是身份认证技术需得到提升与加强防护，如短信验证码易遭劫持且应用广泛问题。可采用拨号认证替代方案，重点考虑**安全性、便捷性、成本优化**，让黑客/黑产即使窃取到用户相关资料也无法造成重大交易安全事件或极大增加破解成本与难度。

提升身份核实能力

引入**权威实时、海量多维、不涉及客户隐私**的外部数据与服务，优化业务风险控制的反欺诈、信用评估模型，让业务风险控制在核实用户身份能力上更加客观、多维且精确，防止欺诈行为与信用问题。

精确识别欺诈行为能力

交易安全实时防护的识别欺诈行为方面，重点以大数据实时防护分析为基础，结合面向**全渠道**跨系统的中央风控模式，通过**一客一策**动态认证策略，形成事前预防、事中防控、事后分析的主动、实时、智能防护能力，解决全渠道欺诈行为精确识别，同时无法协同工作问题。

实时交易业务安全解决方案

实时交易反欺诈解决方案

实时交易业务安全：大幅提升身份认证安全能力

SIM卡盾

解决手机端因硬件与携带原因，无法享受U盾高级别安全保障问题（可针对高端客户使用）

声纹认证

解决其生物识别在手机终端应用普及度和安全性与便捷性兼顾的矛盾

拨号认证

彻底解决目前短信验证码易被劫持、钓鱼诈骗、盗窃利用的安全风险

软U盾

解决手机端应用高级别安全与硬件置换成本和体验的矛盾

身份证云

解决企业在身份证识别业务上投入大量读取终端设备，后期身份证更新换代置换成本高昂的问题

隐私保护

解决业务联系方双因暴露真实号码带来的隐私与安全问题

数据服务

运营商级实名核验与征信数据，并整合工商、税务、法院、公安、电商、银联等外部数据，提供优化风控模型的数据服务

实时交易业务安全：拨号认证

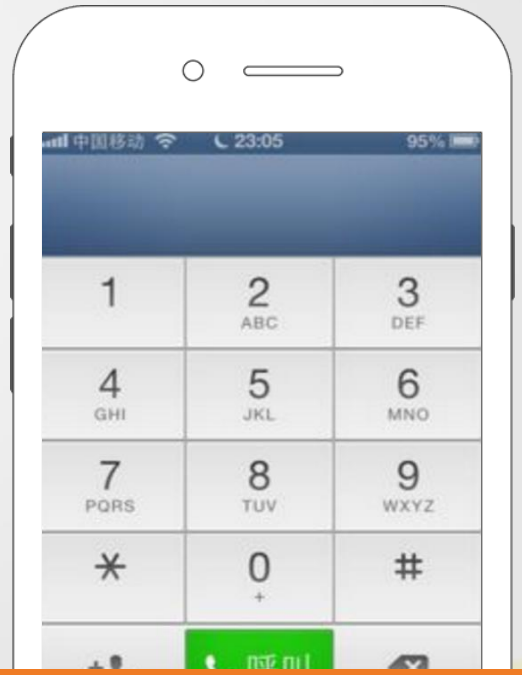
一触即发、秒级认证、用户体验无门槛！

短信验证升级版，通过终端用户主动拨打虚拟认证号码方式，借助通信运营商封闭网络识别能力，解决目前短信验证码易被劫持、钓鱼诈骗、盗窃利用的安全风险。

1. 手机号码为用户天然载体
2. 通信网的封闭性、高安全性
3. 从七号信令层识别本机或IP拨打
4. 拨通即验证，快捷高效，不存在延迟现象
5. 拨号方式符合大众操作习惯，无需再教育
6. 4种认证模式可选，轻松应对不同安全需求

短信验证码认证

拨打随机虚拟号认证



适用场景：高安全性与便捷性兼顾首选，如注册、登录、转账、支付、消费等。

实时交易业务安全：声纹认证

人声各异、拒绝模仿、芝麻开门的极致体验！

借助人体独特的声音特性，实现生物级安全认证，为多因素认证增加安全保障；同时借助声纹认证解决其生物识别在手机终端应用的安全性与复杂环境下使用便捷性的矛盾。

1. 声音采集设备为手机标配
2. 声纹识别+动态口令语音识别，双重验证
3. 防拼接与声纹自学习系统
4. 自如应对感冒、喝酒、方言
5. 多项国家技术专利
6. 国内声纹标准制定者

声纹预留

声纹验证

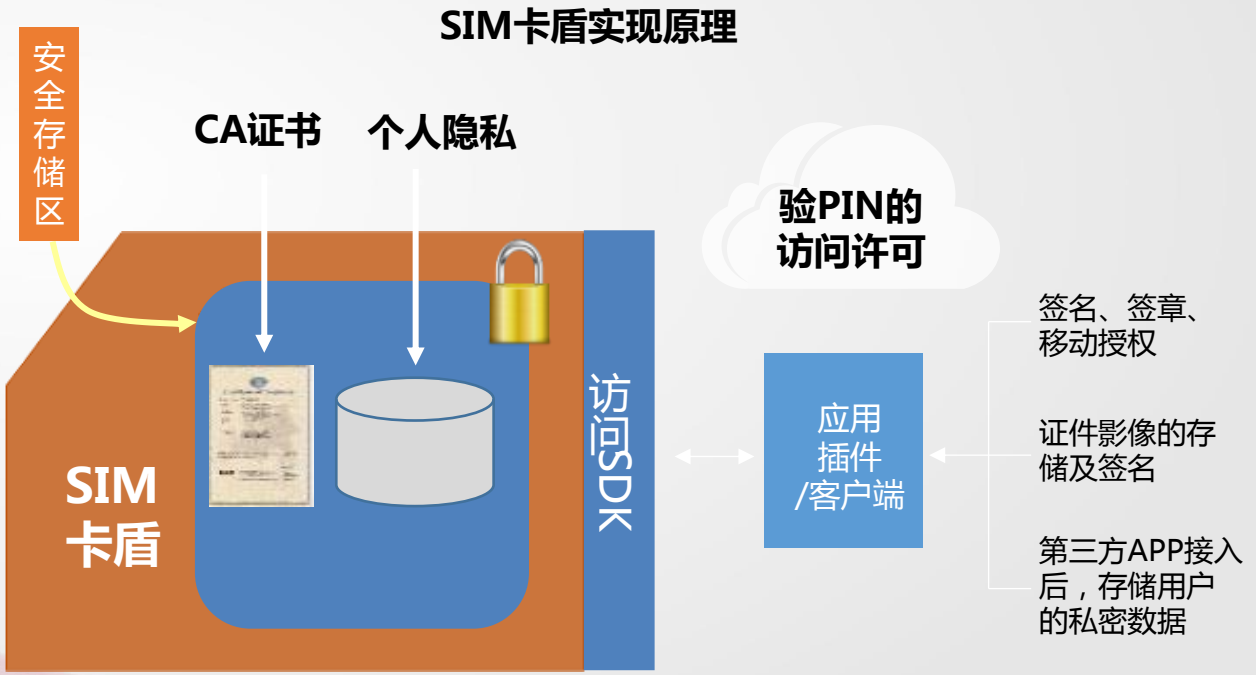
适用场景：便捷性兼安全性首选，高安全性辅助认证，如登录、转账、支付、消费多因素认证等。

实时交易业务安全： SIM卡盾

无需外带设备的手机U盾，尽享高级别移动安全服务！

将手机中的SIM卡作为U盾载体，实现硬件U盾安全保障，同时又通过SIM卡与移动应用的无缝衔接保障携带和使用的方便性。

1. 安全级别获得权威认证GSMA的最高等级Level4
2. 获得国家密码管理局的国密资质认证
3. SE资源访问权限严格控制，重要资源需PIN验证
4. 全程加密数字证书，将数字证书写入SIM卡内
5. 移动应用的全链路安全保障



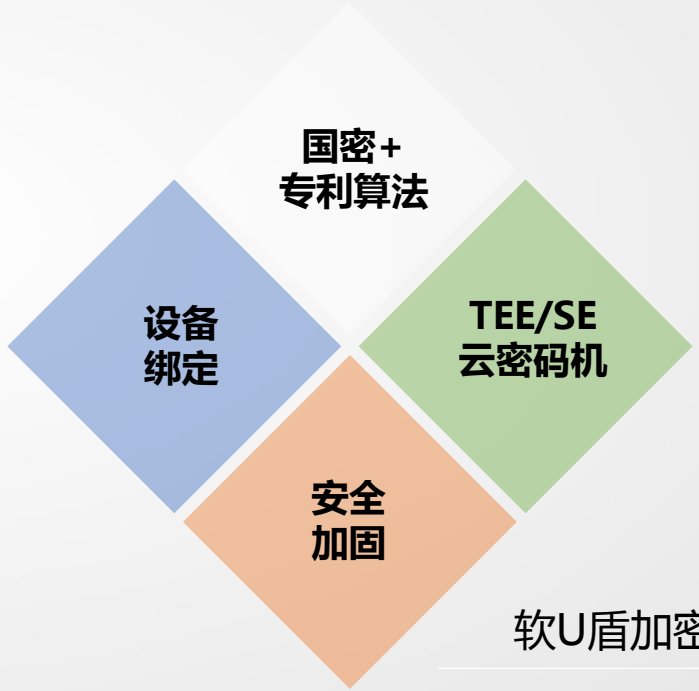
适用场景：手机端高级别安全与大客户首选，如大额转账、支付、消费等。

实时交易业务安全：软U盾

手机变U盾，轻松畅快体验高级别移动安全服务！

将手机做为令牌，综合运用密钥分割，协同计算等专利技术，采用可信计算环境和金融级国密算法，确保手机端高级安全认证实现。

1. “云+端”协同计算，密钥分割，SM2国密算法与专利算法
2. TEE、SE、云密码机等硬件级别保护
3. 捆绑手机设备，参与密钥计算，复制到其他手机无法解密
4. 节约投入成本，无终端设备购置成本、分发维护便捷高效
5. 用户可快速上手，系统灵活部署，可动态扩展



软U盾加密机制

适用场景：手机端高级别安全首选，如大额转账、支付、消费等。

实时交易业务安全：身份证云认证

安全不变、更多选择、移动营销好助手！

通过手机NFC、蓝牙或OTG等便捷接入方式，实现身份证的云端验证，方便移动营销服务；同时提升设备利用率，降低成本。

1. 获得公安部GA证书，内置SAM阅读器，安全可靠
2. 应用成本大幅降低：设备成本、置换成本、使用效率
3. 不同应用环境选择不同识别设备，灵活方便
4. 多样网络接入，满足不同应用场景需要
5. 方便业务集成，实现移动办公及实名认证一体化

身份证云认证实现原理

适用场景：新开网点、偏远地区、线下移动营销、线上客户自助服务。

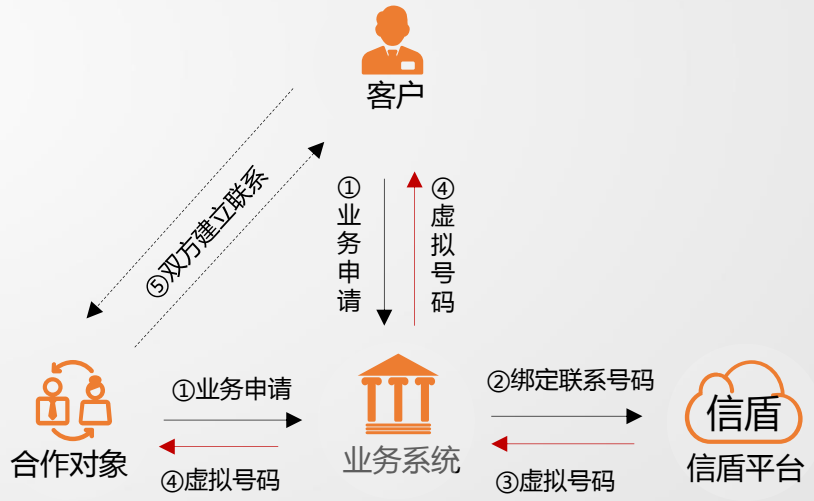
实时交易业务安全：隐私保护

保护隐私从号码做起：没有真实号码，一样能联系！

借助电信运营商虚拟小号能力，保护联系双方的真实电话号码，在业务完成期间或一定时间范围内虚拟号有效，达到联系双方隐私保护的目的。

1. 适用于三大电信运营商隐私保护，覆盖全网号码
2. 无需额外申请号码资源，开通即用
3. 业务双方通过虚拟号码联系，降低业务风险
4. 方便集成，快速落地应用

隐私保护服务



适用场景：企业供应链的合作对象需联系企业客户。

实时交易业务安全：数据服务

风险要从源头控起：让数据更有价值、让风控更加有效！

借助运营商的独特号码资源，帮助客户进行从名称、号码、身份证的实名核验，从源头识别客户；借助运营商的客户通信消费行为数据，让业务风险控制更加有效和准确。

1. 官方权威数据，与三大电信运营商等数据机构合作
2. 多维度海量价值数据（实名核验、征信数据等）
3. 动态实时数据接口，确保数据的精确度
4. 不涉及客户隐私数据，输出定性数据与比对结果，使用无法律风险

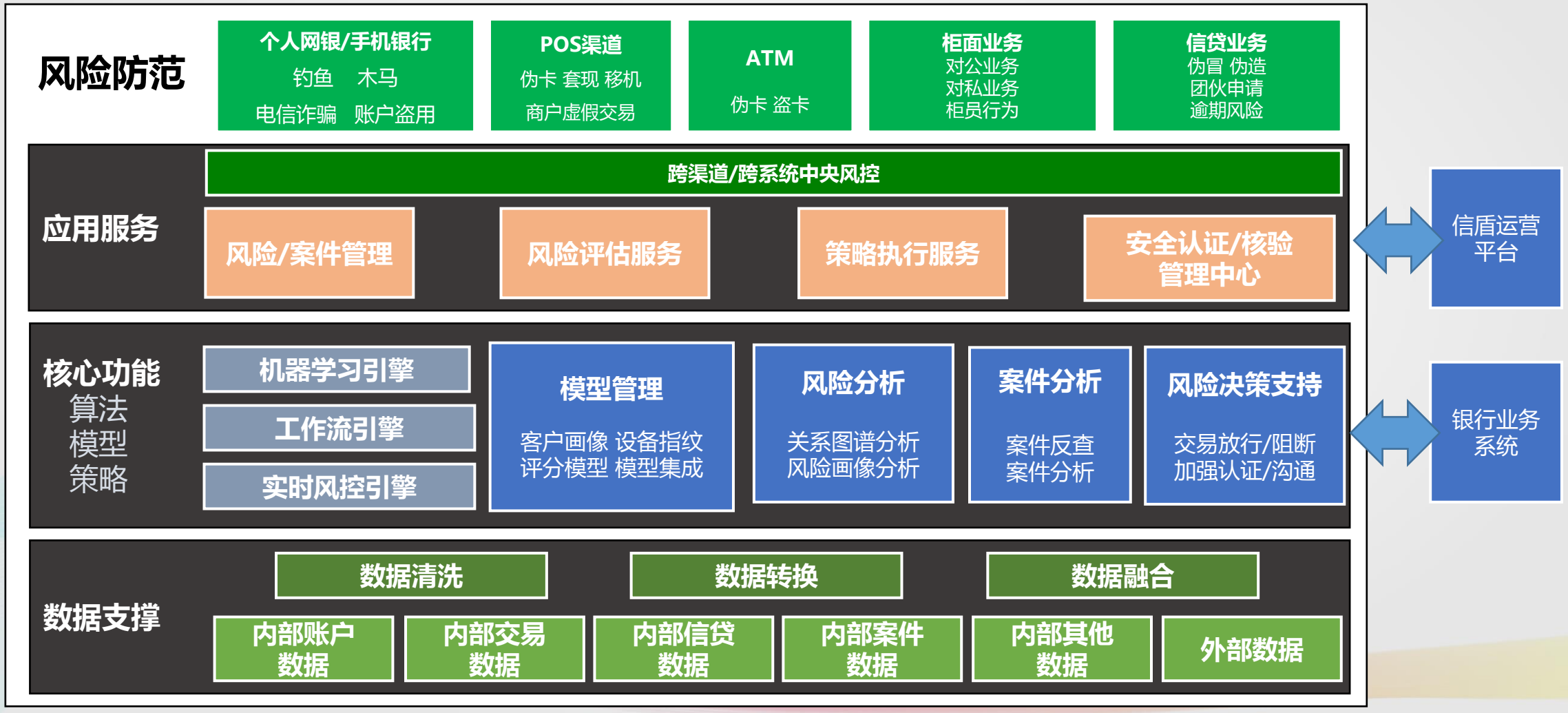
信盾数据服务目录

数据分类	序号	数据项目
公安部：身份证信息	1	身份证二要素（姓名+身份证号）
	2	身份证返网纹照片
	3	身份证返高清照片
	4	最新办证日期
电信运营商：风控信息	1	运营商三要素（姓名+身份证号+手机号码）
	2	手机号码当前用户状态
	3	手机号码在网时长
	4	手机号码归属地市
	5	ID已实名手机号码数量
	6	垃圾短信黑名单标识
	7	疑似养卡（异常使用号码）标识
	8	坏账用户标识
	9	移动星级
	10	M3账单总金额（元）
	11	M3通话总时长（分钟）
	12	M3流量使用情况（M）
	13	M3欠费停机频次
	14	M3使用的终端数量
	15	M3国内漫游通话标识
	16	M3国际漫游通话标识
其他行业：风控信息（互联网网贷/租车/公检法）	1	网贷黑名单信息查询
	2	被执行人信息查询
	3	失信被执行人信息查询
	4	个人不良记录查询
	5	个人疑似身份泄漏
	6	黑名单记信息查询
	7	租车行业黑名单
工商客户信息	1	个人工商信息
	2	企业工商信息
银联智慧反欺诈	1	银行信息认证（四要素）
	2	银行卡有效性验证
	3	交易活跃度检测
	4	交易地点统计
	5	疑似套现检测（个人）
	6	疑似套现检测（商户）
银联客户画像	1	银联用户画像
	2	银联商户画像
银联智慧报告	1	用户报告查询
	2	商户报告查询

数据服务目录

适用场景：企业在反欺诈与信用评估的业务风控模型优化方面。

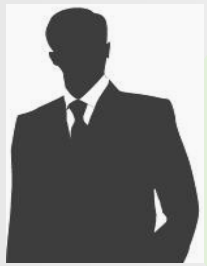
实时交易反欺诈：一客一策，全渠道协同反欺诈



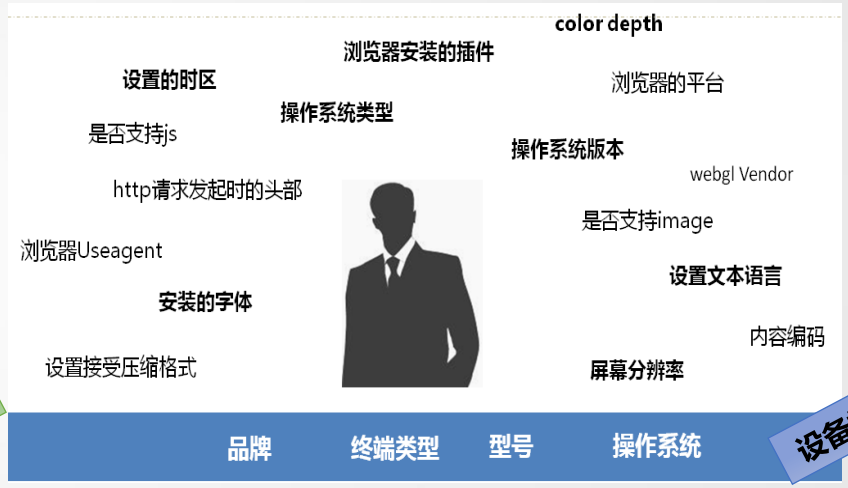
注：信盾运营平台即实时交易业务安全7大服务能力的产品名称

实时交易反欺诈：权威、多维、实时数据

突破传统风控的数据维度窄问题，基于企业内外数据，以丰富的维度、强相关和小颗粒度数据，结合强大的大数据实时分析能力提升风险管控水平。

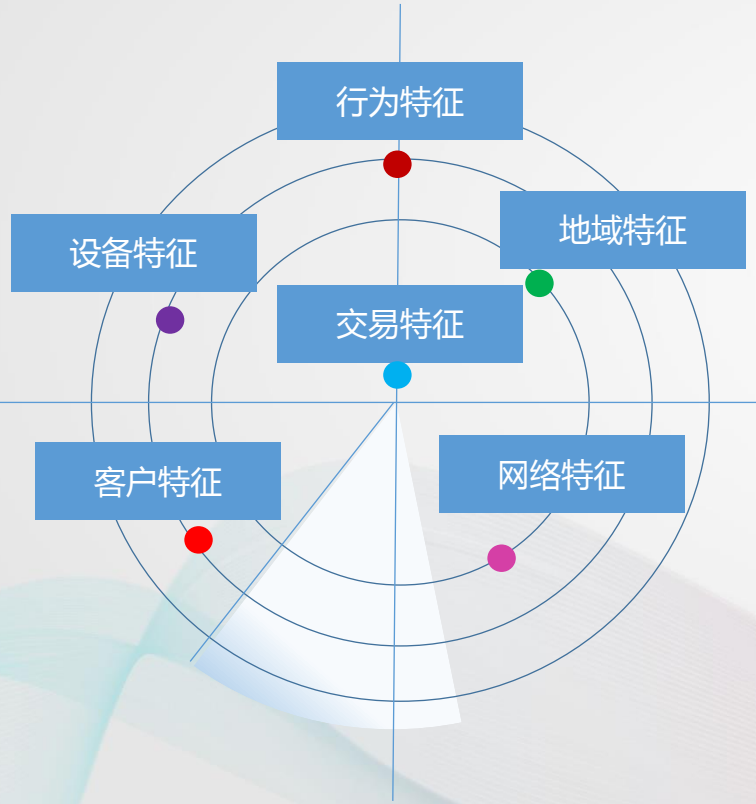


- •账户数据
- •业务数据
- **•设备数据**
- **•行为特征**
- •社交网络
- •偏好数据



- •逐步引入、打通跨行业数据
- •构建客户风险画像
- •通过多维度数据建立不同主体间的关联关系
- •提供设备指纹等关键技术能力

实时交易反欺诈：双重反欺诈引擎，精准识别欺诈行为



双重反欺诈引擎：

1 **线性规则模型**：基于专家经验的反欺诈规则引擎判定，快速应对突发风险事件。

优势

- 业务规则是来自对欺诈案件的事后总结，只对和已**发生欺诈类似的交易才有识别效果。**
- 规则模型在应对新的欺诈交易案件模式上具有**响应更新快**的特点

劣势

- 规则无论多复杂，都是对问题空间做线性区格，欺诈的小概率特性使得单纯使用业务规则会造成**非常高的误报率**
- 越来越复杂的规则和各规则变量之间类似矩阵组合关系使得规则的**管理复杂**

2 **非线性规则模型**：基于大数据的关联性分析基础上，针对每个客户的特征，构建“一客一策”的精准反欺诈模型。

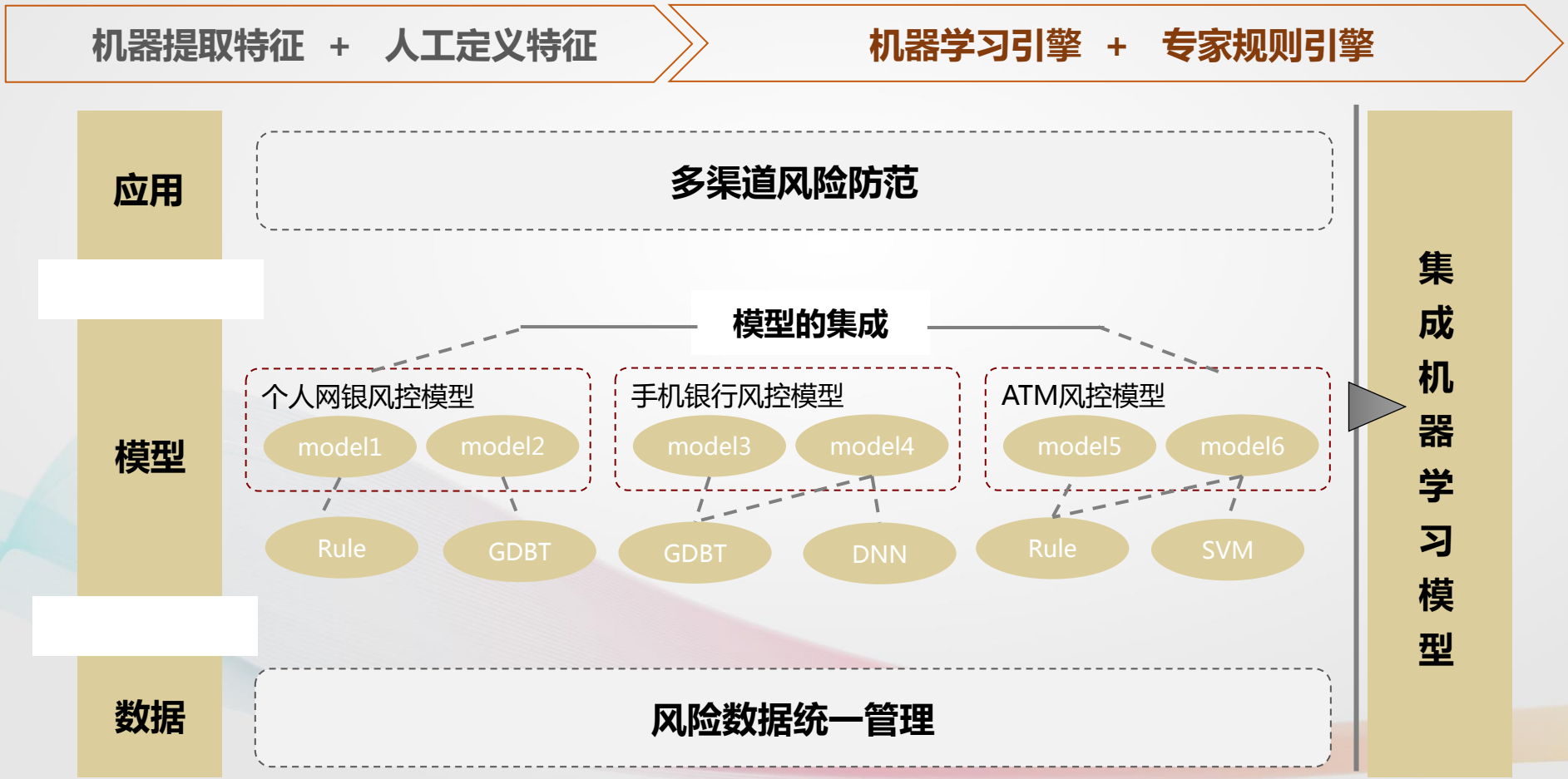
优势

- 对问题空间做非线性区格，在识别欺诈交易的同时**显著降低误报率**
- 洞察潜在的欺诈模式，具有一定的对未来发生的**新型欺诈的预测能力**
- 通过对欺诈数据和正常数据进行自学习自动进行更新，**显著减少风险监控人员的管理成本**

劣势

- 对明显或已知的欺诈判断缺少直接迅速的管理控制

实时交易反欺诈：双引擎风控，机器学习为主，专家规则为辅



实时交易反欺诈：实时计算能力，使欺诈行为无处遁藏

业务驱动

业务驱动风控手段的实时化

1. 如何在快速的交易业务中快速识别出欺诈客户？
2. 如何在海量业务数据中实现规则因子的快速匹配？
3. 如何能够识别日趋复杂的欺诈手段？

技术实现

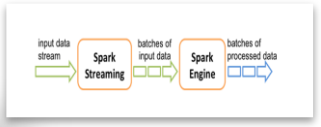
充分利用大数据相关技术，围绕数据，模型，分析为主要抓手，全面实现针对欺诈交易的事中识别和控制

1 数据采集实时化

通过Kafka、Flume等技术，实时抽取、聚合不同系统业务数据

2 数据分析实时化

基于流式计算的高速执行引擎，客户可以结合流式、批处理和交互式查询应用



3 事件识别实时化

通过Kafka、Flume等技术，实时抽取、聚合不同系统业务数据

4 模型的持续优化

人工更新与机器学习双管齐下，保持基于业务的模型规则的更新

价值提供

实时风控是对现有风控方式有效的补充

性能提升

与传统风控互为抓手，全面提升风控能力

性能指标支撑说明：

并发量（条）：百万级

系统响应时间：<200毫秒

战略实现

符合金融大数据发展要求

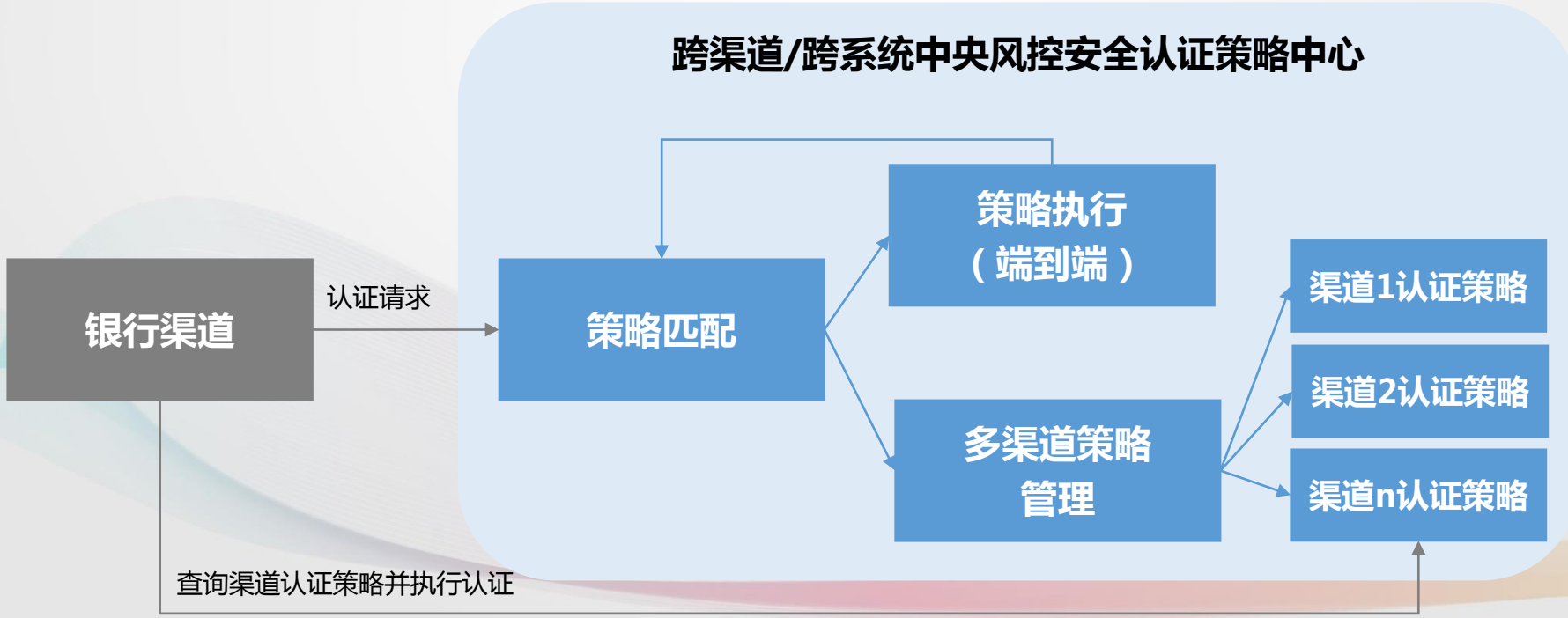
满意度提升

有效帮助客户减少损失，提升客户满意度

实时交易反欺诈：一客一策，实时动态认证防护

跨渠道/跨系统中央风控安全认证策略中心：

支持一客一策认证策略管控能力，实现对不同用户、不同渠道、不同场景、不同金额、不同认证策略的匹配、执行与端到端管控能力，加强对客户端交易异常行为的及时响应与处理。



C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank You