2023

开放银行数据保护与合规实践案例报告

中国银联技术管理委员会开放银行工作组

2023-5 发布

中国银联技术管理委员会

开放银行工作组研究成果

版权声明

编写委员会

委员会组长单位：中国工商银行

委员会成员单位：中国银联、中国农业银行、中国银行、中国建设银行、交通银行、中国邮政储蓄银行、华夏银行、民生银行、招商银行、上海浦东发展银行、山东城商联盟、罗思（上海）咨询有限公司、北京市路盛律师事务所

编委会成员：

刘承岩	傅宜生	李树尉	朱　军	郭汉利
郭志军	胡军锋	卢科兵	虞　刚	尤堂成
万　化	郑述庆			

课题组成员：（排名不分先后）

组长单位：	夏知渊	徐琳玲	魏博言	
成员单位：				
欧阳琛	周锦佳	林　宁	许冬燕	张高磊
李　楠	叶　涛	廖旺胜	庄思瀚	王秋卉
苏　晨	方鹤鸣	邵雪峰	宋　宁	陆绍益
肖　昊	焦伟哲	竺铁生	李　东	战　扬
傅　杰	葛明嵩	曹　祥	周　磊	慈春秀
田艳阳				

特别鸣谢（排名不分先后）

张　弛	周雍恺	侯陈达	谢世杰	张少敏
钱　江	李盛群	张　婧	李晓敦	冯吉禹
陈　鹏	廖静雅	严青伟	秦旭果	刘书洪
王广驰	单传强	袁　捷		

感谢以上专家参与以编写本报告为目的的调研访谈及评审。

目录

开放银行数据保护与合规实践案例报告

一、背景与目标

2021 年 11 月，中国银联技术管理委员会开放银行工作组发布了《开放银行数据保护与合规研究报告（2021）》（以下称 2021 年报告）。自 2021 年报告发布以来，多家银行的开放银行服务都进行了业务场景的拓展与技术方案的更迭。基于此，我们推出了本报告作为 2021 年报告的续篇，通过大量详实的案例分析讨论开放银行落地所需的技术和实现方式。

开放银行（Open Banking）指银行通过共享数据、业务服务等形式开展与业态的业务连接和场景合作，实现金融服务能力与客户生产生活、政务商务等服务贯通融合的金融服务方式。其主旨和核心在于数据和服务的开放共享[1]，是商业银行数字化转型的重要组成部分。开放银行业态涉及作为数据主体的客户、银行、第三方、技术信息转接机构等参与方[2]。自 2012 年以来，国有大行、股份制银行等相继推出开放银行平台以拓宽业务渠道。随着中国《数据安全法》以及《个人信息保护法》等法律的出台，我国对于数据安全的监管力度逐步加大。2022 年 12 月，《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》（简称“数据二十条”）对外发布，从数据产权、流通交易、收益分配、安全治理等方面提出了 20 条政策举措，进一步奠定了未来数据要素合规高效流通使用的整体基调。因此，以数据和服务开放共享为基础，深入应用于各类生活场景的开放银行，其所涉及的数据保护及合规实现问题受到了日益增多的关注。

此外，自 2021 年报告发布以来，也有其他机构陆续发布了开放银行相关的报告。比如，2021 年 11 月，中国光大银行联合普华永道发布《商业银行数据战略白皮书》[3]，指出商业银行制定数据战略有四大驱动力，分别是“国家战略的重要使命”，“监管合规的明确要求”，“商业银行发展的关键机遇”和“业务发展的必然诉求”。该白皮书还总结出“一个愿景”、“两点聚焦”、“四大赋能”、“六大支柱”的商业银行数据战略地图，并分享了光大银行数据战略重点案例。

2022 年 6 月，浦发银行、IBM 和中国信通院联合发布《商业银行数据资产管理体系建设实践报告》[4]，该报告指出我们正在进入一个新时代，数字经济将有望成为国民经济新引擎，作为数字经济的核心生产要素——数据要素，更是数字经济发展的“助推器”。数据资产化是商业银行数据价值持续释放的必经之路，该报告还展望未来数据变现将催生银行业务新模式。

---

[1] 中国银联技术管理委员会开放银行工作组：《开放银行数据保护与合规研究报告》，第 5 页

[2] 中国银联技术管理委员会开放银行工作组：《开放银行数据保护与合规研究报告》，第 11 页

[3] https://www.pwccn.com/zh/banking/commercial-bank-data-strategy-nov2021.pdf

[4] https://www.ibm.com/downloads/cas/VZYOA3BB

2022 年 7 月，平安银行与 IDC 联合编写并发布了《中国开放银行白皮书 2022》[5]，该白皮书指出开放银行已成为推动我国数字经济与实体经济融合发展的新力量，开放银行在赋能实体经济发展过程中遇到了一系列的问题和挑战：诸如对实体经济行业用户的业务模式、金融需求理解程度不够，缺乏基于开放银行的成功实践与运营经验等。而破局之道在于探索出一套政策引领、模式创新、根植场景、共建生态的成功实践，未来对实体经济的赋能方式必将从“单点化”走向“体系化”。该白皮书还分享了平安星云开放联盟实践的典型案例。

2022 年 12 月，民生银行、中国金融认证中心和中国电子银行网联合发布《2022 开放银行生态金融白皮书》[6]，从开放银行赋能普惠金融的路径、政策引导、创新模式着手，选择包含代理记账在内的 10 个行业解决方案进行深度剖析，系统地阐述开放银行在不同行业场景下助推中小微企业数字化发展的服务模式。

本报告主要是对各银行当前开放银行落地实践案例进行收集和汇编，并基于 2021 年报告中所梳理的数据保护策略与数据合规要求，对案例中的数据保护要点进行分析，目的是在当前数据安全管理趋严的形式下，为开放银行的数据保护方案、流程提供易于参考和实践的指引。

二、开放银行数据保护合规要求概述

为了更好的发挥开放银行落地案例的指引作用，本章将基于 2021 年报告以及报告发布之后的重点法规更新，对数据报告策略和合规要求进行总体性回顾和系统梳理。

（一）总体原则

开放银行的数据处理基本原则指的是数据处理者在数据生命周期的各阶段进行各种数据处理时均应遵循的根本准则，是指导监管机构制定规范、进行管理以及开放银行进行具体数据处理行为的纲领。根据《民法典》《个人信息保护法》《数据安全法》《网络安全法》等法律规范，开放银行数据处理者需遵循合法性，公开明示，知情同意，最小够用，数据安全与可问责性，准确性六大原则[7]。

2022 年 12 月，中国银行保险监督管理委员会发布《银行保险机构消费者权益保护管理办法》，明确银行保险机构处理消费者个人信息，应当坚持合法、正当、必要、诚信原则，切实保护消费者信息安全权，整体上符合上述六大原则。

（二）数据收集合规

信息收集指获得信息的控制权的行为。根据《个人信息保护法》《个人金融信息技术保护规范》《网上银行系统信息安全通用规范》等法律法规，信息收集者应制定并公开收集规则，保证个人信息主体对收集的知情和同意，对特殊信息的收集采取特殊收

[5] https://openbank.pingan.com/corporate/extended/whitePaper

[6] https://www.cebnet.com.cn/upload/resources/file/2022/12/07/199023.pdf

[7] 中国银联技术管理委员会开放银行工作组：《开放银行数据保护与合规研究报告》，第 14 页

集方式、遵守特殊规定。具体来说，首先，在收集规则方面，在规则中明确收集目的，方式及范围[8]，收集需合理且限于实现目的的最小范围，一般情况下，最小范围指“直接关联、最低频率和最小数量”。其次，在获得信息主体同意方面，应以信息主体能理解的语言告知其收集者的身份、联系方式、收集目的、收集方式等内容。对于个人敏感信息[9]，除上述告知内容外，还应当向个人告知收集敏感信息的必要性，并获得个人的单独同意。对于不满 14 周岁的自然人信息，除应取得其监护人同意，还应制定专门的个人信息处理规则。再次，在收集方式方面，一般原则是收集个人信息应采用对个人权益影响最小的方式，并保证收集个人信息过程的安全性。特殊信息的收集则应遵守特别规定，例如对于 C3 类别信息，要使用加密等技术措施保证数据的保密性，防止其被未授权的第三方获取。最后，在停止收集方面，在用户不再使用某服务，或当个人信息控制者停止运营其产品或服务时应当停止收集。

（三）数据使用合规

根据《个人金融信息技术保护规范》，数据使用是指对个人金融信息进行展示、共享和转让、公开披露、委托处理、加工处理等操作的过程。根据《个人金融信息技术保护规范》等要求，数据使用前要对数据进行甄别，征得个人信息主体同意，对数据进行脱敏处理，以共享形式使用数据的数据控制者还应建立相应安全制度体系。具体来说，在数据使用前，应先对数据是否能够进行使用进行甄别，剔除如动态口令等敏感级别较高的信息。在使用个人金融信息时，要征得个人金融信息主体明示同意，履行告知义务，并且采用去标识化等手段对数据进行脱敏处理，不使用未经处理的原始数据。此外，进行数据使用的个人金融信息控制者应建立安全制度体系，如个人金融信息控制者向第三方共享个人金融信息的，应对第三方对数据的使用情况、数据保护能力等进行审查与评估。对于委托处理，即金融业机构因金融产品或服务的需要，将收集的个人金融信息委托给第三方机构（包含外包服务机构与外部合作机构）处理时，需注意委托行为不应超出已征得个人金融信息主体授权同意的范围，并准确记录和保存委托处理个人金融信息的情况。对于 C3 以及 C2 类别信息中的用户鉴别辅助信息，不应委托给第三方机构进行处理。对第三方机构进行监督的方式包括但不限于签署合同规定第三方的责任和义务，对第三方展开安全检查、评估和审计，对第三方嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包等）开展技术检测等。[10]

（四）数据传输合规

数据传输指按照一定的规程，通过一条或者多条数据链路，将数据从数据源传输到数据终端。根据《个人信息保护法》，《个人金融信息技术保护规范》，《信息安全技术 数据安全能力成熟度模型》等要求，对于境内数据传输，金融机构使用公共网络传输 C2、C3 类信息时应使用加密通道或数据加密的方式进行传输，作为网络运营者的

[8] 《信息安全技术 个人信息安全规范》第 5.4 条

[9] 《个人金融信息保护技术规范》第 4.2 条将个人金融信息按敏感程度分为 C1、C2、C3 三个类别，C3 类别敏感程度最高

[10] 《个人金融信息保护技术规范》第 6.1.4.4 条

金融机构应对网络进行可用性管理，保证网络稳定运行。向境外传输数据则需要满足更高的合规要求，例如需要向个人信息主体披露境外接收方的情况并获得单独同意，向网信部门申报数据出境安全评估和网络安全审查，或者按照网信部门的规定进行个人信息保护认证，或者根据《个人信息出境标准合同办法》与境外接收方订立合同等。

对于数据跨境传输，个人金融信息如果确需向境外提供的应当获得个人金融信息主体明示同意，开展个人金融信息出境安全评估等。

2021 年 12 月，国家互联网信息办公室等发布《网络安全审查办法（2021）》（《审查办法》），规定了应当向网络安全审查办公室申报网络安全审查的情形，申报网络安全审查应提交的材料，审查中重点评估的风险因素等。2022 年 7 月，国家互联网信息办公室发布《数据出境安全评估办法》（《评估办法》），规定了应当申报数据出境安全评估的情形，包括数据处理者向境外提供重要数据、关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息、自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息以及国家网信部门规定的其他需要申报数据出境安全评估的情形。《评估办法》提出了数据出境安全评估的具体要求，规定数据处理者在申报数据出境安全评估前应当开展数据出境风险自评估并明确了重点评估事项。规定数据处理者在与境外接收方订立的法律文件中明确约定数据安全保护责任义务，在数据出境安全评估有效期内发生影响数据出境安全的情形应当重新申报评估。此外，还明确了数据出境安全评估程序、监督管理制度、法律责任以及合规整改要求等。

2022 年 6 月，全国信息安全标准化技术委员会发布了《网络安全标准实践指南—个人信息跨境处理活动安全认证规范》，在 2022 年 12 月发布了《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》，为个人信息保护认证制度提供了法律依据，明确了适格的申请认证主体，认证申请的具体要求，个人信息主体的权利以及相关方的责任义务等。2022 年 11 月，国家市场监督管理总局，国家互联网信息办公室发布《个人信息保护认证实施规则》，指出认证采取“技术验证+现场审核+获证后监督”模式。

2023 年 2 月，国家网信办发布《个人信息出境标准合同办法》（《合同办法》），自 2023 年 6 月 1 日起施行，适用于个人信息处理者通过与境外接收方订立个人信息出境标准合同的方式向中华人民共和国境外提供个人信息的情形。《合同办法》对订立标准合同的个人信息处理者的主体要求、个人信息保护影响评估、标准合同的格式和条款、标准合同生效后的备案、标准合同的补充或重新订立、网信办及其工作人员的职责等进行了规定。此外，《合同办法》还公布了《个人信息出境标准合同》，对标准合同的内容和具体条款进行明确，除签订合同的双方主体信息外，还包括相关概念的定义、个人信息处理者的义务、境外接受方的义务、境外接收方所在国家或者地区个人信息保护政策和法规对合同履行的影响、个人信息主体的权利、救济、合同解除、违约责任以及其他共九条内容。《合同办法》明确，个人信息处理者可以与境外接收方约定其他条款，但不得与标准合同相冲突。

（五）数据存储合规

数据存储指银行在提供金融产品和服务、开展经营管理等活动中，将数据进行持久化保存的过程，包括但不限于云存储服务、网络存储设备等载体存储数据。根据《个人信息保护法》《网络安全法》《信息安全技术 个人信息安全规范》等法律法规，数据储存首先应保证数据安全，满足所储存数据的“保密性、完整性、可用性”。此外，个人金融信息存储还应满足“本地化”[11]存储要求，数据分类分级存储要求，存储期限最小化要求和去标识化后存储要求。

对于金融行业的云计算数据，还提出了云计算数据中心物理隔离[12]，云服务商以资源控制范围定责原则（由金融机构先承担网络安全等责任，如相关云服务商对云计算环境安全有责任的，金融机构可追偿），对金融行业关键信息基础设施重要系统和数据库进行容灾备份的监管要求。

（六）其他最新法律法规

为更好的保护个人信息，并促进数据合规安全高效流通，在 2021 年报告发布之后的一年多时间里，国家部委、全国金融标准化技术委员会等密集出台了很多数据相关法律法规、行业标准等。

2021 年 11 月，国家互联网信息办公室发布《网络数据安全管理条例（征求意见稿）》，从一般规定、个人信息保护、重要数据安全、数据跨境安全管理、互联网平台运营者义务等方面对网络数据安全参与者进行规范。《征求意见稿》拟建立数据分类分级保护制度，数据分为一般数据、重要数据、核心数据，不同级别的数据采取不同的保护措施。对个人信息和重要数据进行重点保护，对核心数据实行严格保护。《征求意见稿》还提出数据处理者应当建立数据安全应急处置机制，发生数据安全事件时及时启动应急响应机制，发生重要数据或者十万人以上个人信息泄露、毁损、丢失等数据安全事件时，数据处理者应当在八小时内向设区的市级网信部门和有关主管部门报告。

2021 年 12 月，全国金融标准化技术委员会发布关于征求《金融数据安全 数据安全评估规范（征求意见稿）》，以 JR/T 0197-2020《金融数据安全 数据安全分级指南》、JR/T 0223-2021《金融数据安全 数据生命周期安全规范》为金融数据安全评估的主要内容，从金融数据的安全管理评估、安全保护评估、安全运维评估三个方面对评估结果的判定原则和判定方式等进行说明。

2022 年 4 月，国家发展改革委办公厅银保监会办公厅发布《关于加强信用信息共享应用推进融资信用服务平台网络建设的通知》，并指出各银保监局要发挥监管部门了解银行的优势，及时收集并反映银行服务中小微企业的实际需求，推动各地更加精准、

[11] 根据《个人信息保护法》第四十条和《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知 》要求，境内收集和产生的个人信息存储在境内。

[12] 中国人民银行 JR/T0167-2020《云计算技术金融应用规范 安全技术要求》6.1（a）。物理隔离，即服务金融行业的云计算数据中心在基础设施层面与其他行业进行隔离，对物理服务器、网络接入设施等均实现隔离。

更加全面地归集共享信息，优化数据交换方式，提升信用信息的可用性，为银行提高中小微企业服务能力做好数据支撑。各银行业金融机构要积极对接各级平台，把握好信用信息共享深化的有利时机，强化自身数据能力建设，充分利用信用信息资源和银行内部金融数据，综合运用大数据等金融科技手段，扎实推进小微企业、涉农贷款业务的数字化转型，提高授信审批、风险预警管理的能力，创新信贷产品。

2022 年 12 月，中共中央国务院发布《关于构建数据基础制度更好发挥数据要素作用的意见》（简称“数据二十条”），从数据产权、流通交易、收益分配、安全治理等方面构建数据基础制度，提出二十条政策举措，指出要建立健全个人信息数据确权授权机制。对承载个人信息的数据，推动数据处理者按照个人授权范围依法依规采集、持有、托管和使用数据，规范对个人信息的处理活动，不得采取“一揽子授权”、强制同意等方式过度收集个人信息，促进个人信息合理利用。金融行业作为天然依赖数据的行业，数据已经逐步成为金融机构数字化经营的核心资产。在数据产权方面，数据二十条提出的数据产权结构性分置制度对于金融机构的数据管理具有重大意义，包括合法保障多方权益、释放推动数据要素流通的积极信号，打破数据资源的单一垄断，和奠定数据收益分配的基础；在流通交易方面，对于金融机构而言，数据二十条的发布将大幅提升数据交易市场的活跃度，金融机构在数据的交易与流通中不再仅限于传统的“数据需求方”角色，而是在此基础上进一步衍生出“数据供给方”及“数据生态服务方”的职能，以三方角色融入数据交易生态圈，深度参与数据要素市场建设；在收益分配方面，数据二十条明确了“谁投入、谁贡献、谁受益”原则，金融机构需要以差异化的视角思考各参与主体间的收益分配关系；在安全治理方面，数据二十条明确守住数据安全是数据要素流通交易的红线和底线，只有建立健全数据要素安全体系，才能保障数据能够更加有效地运转和流通，金融机构应加强数据安全治理中的责任落实，建立完备的数据安全治理体系，共同维护以安全合规为基础的数据要素市场环境，积极推动数据的有效流通，充分发挥金融机构数据的责任和义务。[13]

三、开放银行数据保护及合规落地案例

开放银行通过 API（应用程序接口）与 TSP（第三方服务提供商）等技术将银行服务与产品直接嵌入合作平台，实现了银行与第三方之间的数据信息共享与融合。开放银行模式实现银行传统线下金融业务数字化，通过和业态合作拓展业务可以让银行获取场景数据，实现穿透式管理，更好地帮助银行精准构建用户画像，提供细致的金融服务。本章主要是银行开放银行落地实践案例的汇总，在每个案例中，都会基于第二章梳理的数据合规要求，说明其中的数据保护要点，以期望为开放银行的数据保护方案、流程提供易于参考和实践的指引。

（一）开放平台的多平台 SDK 方案

案例关键字：加解密；SDK；多平台

[13] 《数启新篇，智赢未来——“数据二十条”对金融行业的影响与启示》，普华永道，上海数据交易所

案例提供方：华夏银行

1. 合规概况介绍

该技术方案主要体现了数据传输合规，《个人金融信息保护技术规范》要求金融机构在使用公共网络传输时需对 C2、C3 类信息进行加密传输。该方案采用在管理台配置的方式，设定各平台数据传输所使用的加解密技术，包括对称加密和非对称加密的国密算法等，并将各平台数据传输的加解密方式进行封装进 SDK，统一管控了加解密技术标准，并简化了日常项目开发的周期和成本，是数据传输合规较成熟的落地实践方案。

2. 背景

开放平台多平台 SDK 方案为接入方提供了封装的认证授权算法、加解密算法、国密算法支持、证书管理、token 管理、服务调用、结果解析等功能。通过提供支持服务器端、移动端、H5 端，多平台的 SDK 方案，既实现开放平台的安全接入、数据保护的统一管控的标准化方案，又大大简化了接入方的开发周期和成本，实现了对业务的快速相应和强力支撑。

3. 方案

该方案支持多种加密算法包括多种国密算法，都可以通过平台进行配置，以下示例以常见的算法 AES256 等为例。

(1) Java SDK

Java SDK 封装的应用方服务器与服务提供方服务器直接交互的模式下，流程图如下：

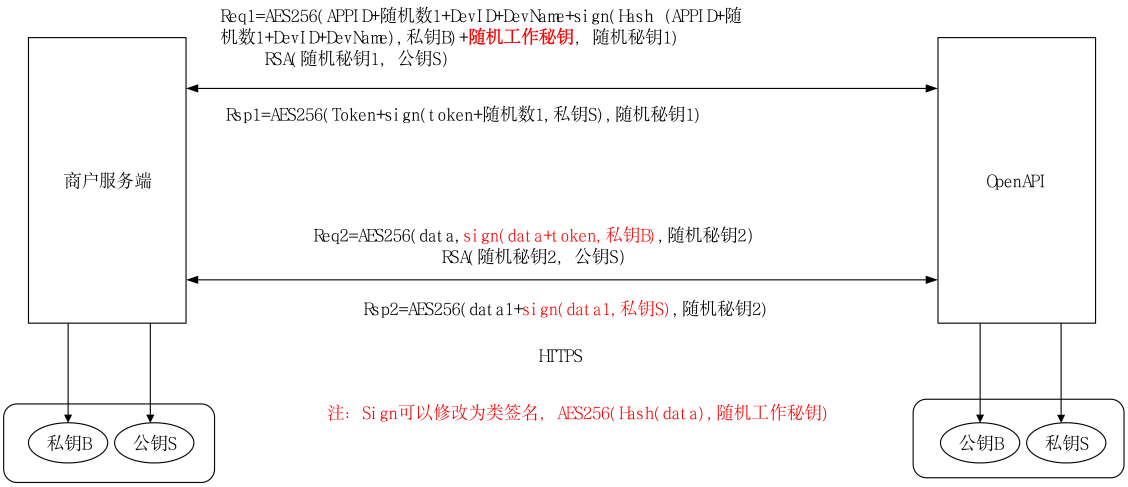

图 1 Java SDK 加密通讯机制

应用服务器使用摘要算法对 APPID、随机数、设备标识等进行合并并生成摘要，使用密钥对摘要做签名；然后再对报文内容、签名、随机工作密钥等进行 AES256 加密，生成数据密文；再使用非对称加密算法对随机密钥进行加密，生成密钥密文；将数据密文和密钥密文通过 HTTPS 方式发送到服务提供方。

服务提供方使用私钥解密密钥密文，获取随机密钥；然后随机密钥对数据密文进行 AES256 解密， 并对签名字段做验签运算；成功后，生成 token。使用服务方私钥对 token 和随机数进行签名运算，生成签名，并使用随机密钥对 token 和签名进行加密，将密文返回应用方。

应用方使用随机密钥解密密文，然后使用 token 和随机数进行验签，成功后后续交易，在有效期内，基于 token 做安全通讯。

(2) 移动端 SDK

移动端主要指分为 Android 和 iOS 的场景，使用移动端 SDK，封装的相关流程如下：

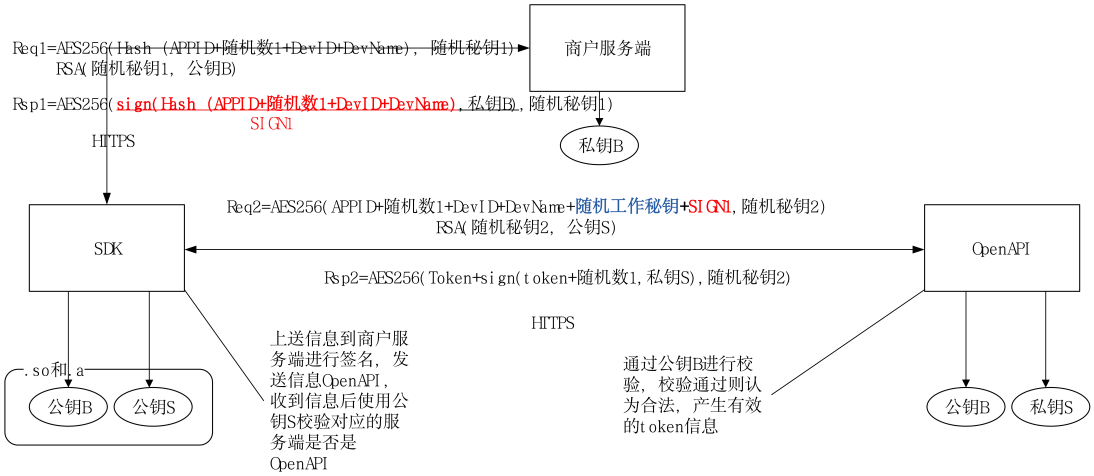

图 2 移动端 SDK 加密通讯机制

移动端 SDK 对 APPID、随机数、设备标识等进行摘要计算，并使用随机密钥对数据摘要进行 AES256 加密，生成数据密文；然后对随机密钥进行非对称加密，生成密钥密文；将数据密文和密钥密文以 HTTPS 方式发送到应用方服务器。

应用方服务器端对密钥密文进行解密，获取随机密钥；然后使用随机密钥对数据密文进行解密，获取数据摘要；然后再对数据摘要进行签名，并对签名进行 AES256 加密，将签名密文返回给移动端 SDK。

移动端 SDK 对签名密文解密，获取签名；然后使用新的随机密钥对 APPID、随机数、设备标识、随机工作密钥、签名等进行加密，生产密文数据；并对随机密钥进行非对称加密，生成密文密钥；将密文数据和密文密钥通过 HTTPS 的方式发送到服务提供方。

服务提供方对密文密钥进行解密，获取随机密钥；使用随机密钥解密密文数据，获取明文；然后使用 APPID、随机数、设备标识进行摘要运算，最后对摘要和签名进行验签运算；验签成功后生成 token。将 token 和随机数，进行签名，然后用随机密钥对 token 和签名进行 AES256 加密，将密文返回移动端 SDK。

移动端 SDK 使用随机密钥进行解密，并对随机数和 token 进行验签；成功后，则获取的 token 有效。后续所有交易，在有效期内，基于 token 来做安全通讯。

(3) JS SDK

JS SDK 是基于浏览器客户端请求，H5 客户端不具备保存密钥的条件，流程图如下：

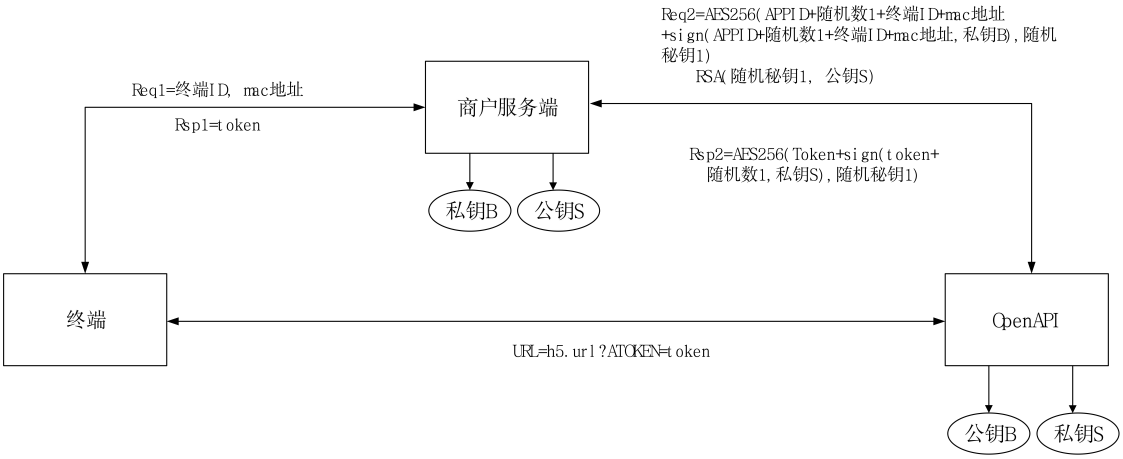

图 3 JS SDK 加密通讯机制

JS SDK 以 HTTPS 的方式传送设备标识到应用方服务器。

应用方服务器使用对 APPID、随机数、设备标识进行签名，然后使用随机密钥将 APPID、随机数、设备标识、签名进行 AES256 加密，生成数据密文；并对随机密钥进行非对称加密，生成密钥密文；将数据密文和密钥密文以 HTTPS 方式发送到服务提供方。

服务提供方解密密钥密文，获取随机密钥；然后使用随机密钥对数据密文进行 AES256 解密，获取数据明文；然后对 APPID、随机数、设备标识进行验签，成功后，生成 token。然后对 token 和随机数进行签名；将签名和 token 使用随机密钥进行 AES256 加密，生成密文；返回给应用方服务器。

应用方服务器解密获得对 token 和随机数，并进行验签，通过后，证明 token 安全可用，将 token 返回给 JS SDK。

JS SDK 收到 token 后，在有效期内，基于 token 做有安全通讯。

4. 数据保护及合规情况梳理

该方案主要关注于数据传输阶段的数据安全的保护，通过上述的算法进行加密传输。

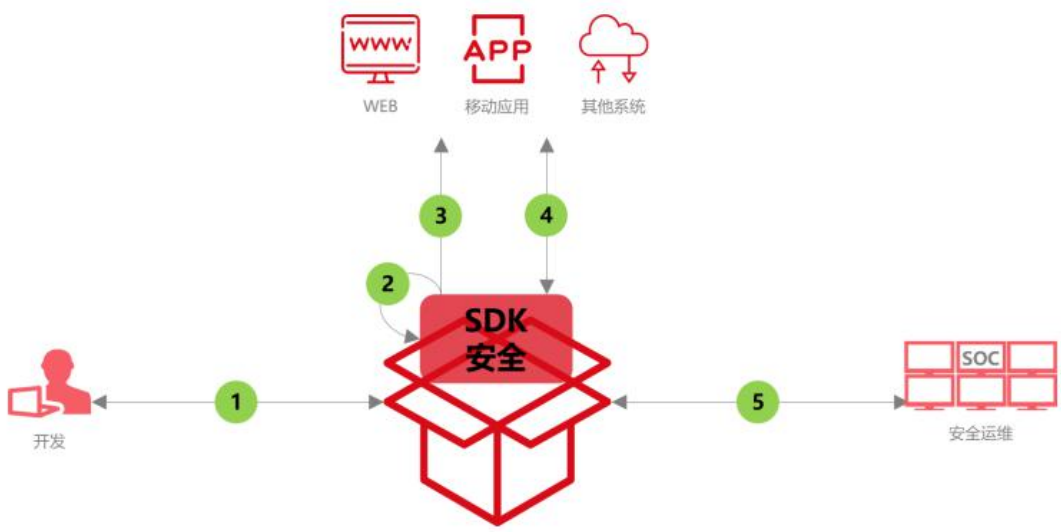

图 4 SDK 安全管理机制

并且针对 SDK 本身的安全，进行规范化管理。确保 SDK 自身的安全性，SDK 的使用模式导致其自身的安全问题会产生放大效应。需要在 SDK 的开发、使用、监测等全生命周期执行严格的安全标准，减少安全漏洞的产生，及时发现安全漏洞并立即修补，提升 SDK 的安全性。

(1) 开发阶段

安全检测：首先需要参考安全基线，对外发 SDK 展开自动化测评和渗透测试，解决 SDK 所面临的安全问题，如泄漏用户数据、自身存在安全漏洞、业务逻辑不完整、攻击面过多、第三方组件漏洞、不符合等保规范等。

(2) 发布前

安全保护：外发的 SDK 可能会包含登录、支付、统计、监测、通讯、推送、验证等众多业务逻辑，可能被外部逆向破解，以分析、调试其中的业务逻辑。

因此需要比对安全检测的结果，对 SDK 实施安全加固等主动防护操作，保护其核心算法、密钥、后台 API 接口、业务逻辑等关键内容，增强 SDK 安全性、降低被攻击的可能。

(3) 对外发布

安全管理：对需要集成调用的 SDK 登记应用包名、签名等信息，在 SDK 调用过程中验证宿主 App 的包名、签名等信息，防止被非授权第三方非法集成和调用等问题的发生。同时通过接入管理，对存在重大安全隐患（安全威胁大、应用安全防护措施低、用户投诉多等）的 App 进行接入封禁，确保 SDK 的接入安全。

(4) 运行过程中

运行监控：SDK 的运行环境具有不可控性，因此需要对 SDK 实施主动安全监控，实现对 SDK 威胁的感知、对宿主应用所在环境威胁的感知（如 SDK 的宿主 App 运行环境是否真实、安全；是否存在恶意攻击 SDK、通过 SDK 窃取敏感信息、扰乱正常的业务交易等风险问题），在风险发生时或发生前做到预警、阻断，在风险发生后可以进行追溯。

(5) 面临风险时

安全响应：对 SDK 运行过程中遇到的各种安全威胁，需要借助 SDK 威胁态势感知检测、SDK 渠道监测结果，分析各种安全威胁，通过业务控制、技术对抗及法律方法等，对安全风险及时的进行响应处理。

SDK 对个人信息及数据的收集和处理应符合国家法律、标准的规定。SDK 在嵌入 APP 应用使用后，APP 以间接方式访问开放银行系统的接口服务，API 安全的内容也适用于 SDK 安全。

（二）数据访问控制安全平台

案例关键字：数据访问控制；基于属性(ABAC)的上下文模型

案例提供方：中国建设银行

1. 合规概况介绍

在数据使用方面，为满足数据使用的“最小化”原则，建成全行企业级的数据安全访问控制平台，提供业务过程中细粒度的数据安全访问控制，着力于解决个人信息保护与业务场景相融合的难题。

2. 背景

中国建设银行在进行数字化转型过程中，明确数据是企业重要的战略资产，是驱动线上业务快速发展、完成战略转型的核心力量。而伴随着数据的高度集中，广泛使用，数据泄露风险也日益加剧，而传统数据安全更偏向 IT 与技术手段，难以满足需要与具体业务场景融合的个人信息保护需求，存在以下痛点：一是个人信息查询问题的涉及面极广，几乎涉及到了企业所有业务系统中的每一项业务、每一支交易接口；二是发起个人信息查询业务的场景极其复杂。通常访问控制策略需要对业务场景，访问者的身份属性，访问的环境属性，以及所访问的数据属性进行判断，根据属性信息动态的执行访问控制，才是将访问控制落实到具体业务，且最小化内部人员数据权限的有效数据安全措施。

传统的解决方案，数据权限与访问控制策略逻辑只能由每一个业务系统的开发人员硬编码到业务系统代码中，需要企业投入大量时间成本、人力成本和资金成本对现有系统功能改造。如果未来新的业务功能涉及个人信息查询问题，或者监管要求的调整，必然增加额外的资源投入，延缓新业务功能的发布速度。同时，业务逻辑中混入的数据访问控制策略代码难以维护与灵活调整，很难应对未来的政策要求。

随着相关数据安全法规和制度逐渐完善，监管要求日趋严格，数据安全防范需求尤为紧迫，亟需通过相关信息系统和技术框架体系的建设，规范员工数据使用行为，保护客户隐私。为此，建行于 2020 年启动了数据访问控制安全平台项目，经过近两年的落地验证，已建成全行企业级的数据安全访问控制平台，为数百个系统提供了业务过程中细粒度的数据安全访问控制，充分保护了客户的金融个人信息，着力于解决个人信息保护与业务场景相融合的难题，从业务系统数据资产梳理、到由业务需求出发制定访问控制策略、再到自动同步个人信息查询业务相关属性数据执行访问控制，平台为个人信息保护的每个关键环节提供了良好的技术支持，至此个人信息保护得以落实，数据安全治理得以完善，很好的适配了相关法规对个人信息保护的各项要求。

3. 方案

(1) 解决思路

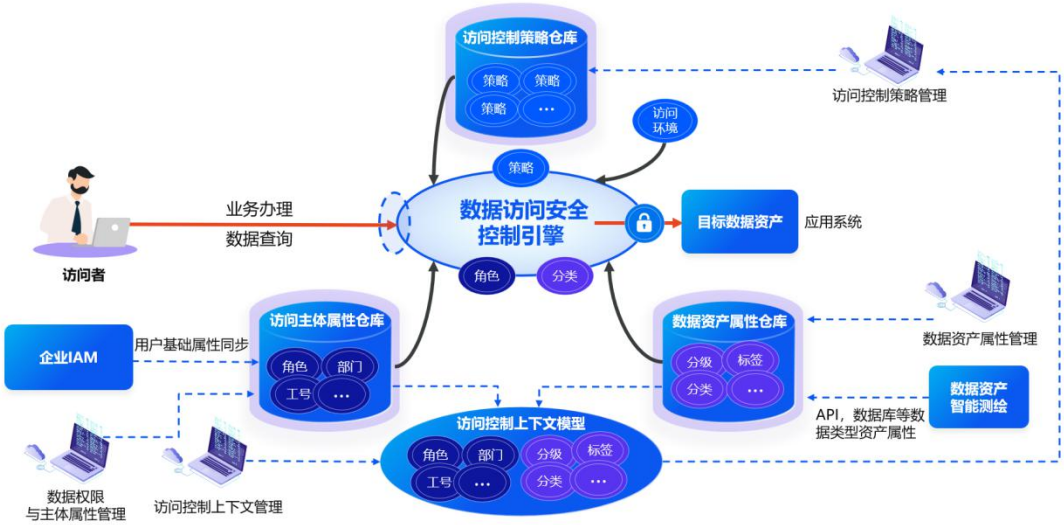

图 5 系统整体架构

要根除个人信息查询管理混乱的问题，建设易于实施、可持续使用、为企业降本增效的数据访问控制安全平台，以下是能触达目标的三个关键步骤：

1、全局掌握业务过程中涉及个人信息查询的数据接口

应用系统的 API 接口是个人信息输出的重要关口，将数据访问控制点设在应用接口返回用户数据时，是实现数据访问控制的最理想途径。应用 API 接口都由什么业务在调用，每个接口都在输出些什么类型的数据，接口输出的数据是否包含个人敏感信息，厘清这些信息，是建立企业级 API 数据访问控制关键的一步。

2、整体评估业务过程中个人信息的访问控制策略

业务办理过程中的个人信息保护不能简单地一刀切。如果对所有个人信息都进行脱敏屏蔽，将导致很多需要核实个人信息的业务无法办理。企业需要在不影响业务正常执行的前提下，最小化用户对个人信息的查询权限，解决查询权限混乱与查询业务操作不规范的问题。

3、通过平台实现数据访问控制统一管理

全面的数据接口测绘与数据风险评估是解决个人信息查询问题的必要过程，但要真正解决个人信息查询的数据安全问题，最终必需要在每一支交易中实现访问控制。

(2) 解决方案

图 6 数据访问控制安全平台解决方案

1、全面盘点应用 API 资产，并赋予 API 业务属性

要建立企业级数据访问控制平台，在应用接口返回用户数据时实现访问控制，需要先对企业应用数据接口进行全面的数据资产治理，梳理清楚应用系统所有的 API 接口，接口数据包含的字段，以及数据的个人敏感信息情况，才能有的放矢，将访问控制落实到具体业务接口的具体敏感数据字段。

2、构建基于属性（ABAC）的访问控制上下文模型，自动同步访问控制所需的属性数据

基于属性(ABAC)的上下文模型是从发起访问的用户、账号、应用，被访问的数据、应用、接口，以及访问发生时环境的属性出发，构建由访问主体，访问客体，访问环境属性组成的结构模型。接口数据访问发生时，系统自动同步“运行时”上下文属性数据，并与策略条件设置的值或范围进行匹配，执行与条件相符的输出。在整个接口数据访问控制闭环里， ABAC 构建的是一种动态数据访问控制模型，基于属性和环境条件授予访问权限，具有即时生效的特点，策略改变/属性改变后访问控制的结果即时生

效，这种特性为应用系统提供了更大的灵活性，同时平台提供低代码窗口扩展上下文模型属性，管理员可根据业务需求自定义属性类型，扩展属性与内置属性共同构建更加完善的上下文模型，满足各种应用不同业务的访问控制需求。

3、可视化制定多层级影响范围的访问控制策略

平台以访问控制上下文模型和 ABAC 策略方法为基础，为用户提供可视化，低代码的访问控制策略编辑工具。用户可通过拖拉拽的方式将策略元素放置到策略编辑栏中，并以流程编排模式编辑访问控制执行逻辑，可使用上下文中的任意属性，组合各种逻辑作为访问控制条件，为各个逻辑分支配置或保留、或脱敏、或移除的数据输出结果。

4、从业务需求出发的接口数据整体评估

业务是数据的直接使用方，什么数据是在办理业务时需要看到的，什么数据是高度敏感不可完全显示的，以及哪些数据是业务不需要的多余数据，业务人员对这些信息的掌握最为准确。平台提供从业务出发对接口数据访问控制需求进行评估的通道，评估人员可通过接口数据模型，对已识别的敏感数据字段进行业务评估。策略配置人员参考评估结果，制定准确、有效的访问控制策略。

4. 成效及价值

(1) 技术成效

通过构建企业级平台，系统性解决业务过程中的数据访问安全问题是数据安全领域的一个难题。与传统的数据安全相比较，其复杂程度高、未知问题多、不具参考性，往往解决了一个难题，另外一个难题又接踵而至。解决此难题，需要全面的技术创新，在平台建设过程中两项具有代表性的技术创新过程如下：

1、运行时交易报文的动态结构测绘：业务过程中的数据由应用系统运行时产生，它们不像数据库中存储的数据，看得见摸得着。要对运行时数据进行安全访问控制，就必须先准确测绘出每一支交易的报文结构、字段分级分类、补充所需的各种元数据。面对此项挑战，通过埋点技术手段采集运行时数据，结合人工智能技术识别数据字段的分级分类，创新了分支特征算法、分支识别算法、分支合并算法等专门用于交易接口业务分支测绘的一系列算法。

2、访问控制执行方式与 SDK：业务办理过程中的数据访问控制技术与普通的数据脱敏技术不是一个概念，这里通过两个显著特性说明其技术创新性：一、普通的数据脱敏只需要提供数据脱敏算法与一些数据批处理能力，而业务办理过程中的访问控制需要由整个业务上下文决定：是否对某个字段进行脱敏需要根据正在执行什么业务，访问者的岗位、角色、所属机构，被访问的是什么数据，访问发生的时间、客户端所属的网络环境等要素进行综合判决。二、访问控制的执行点需要嵌入到应用系统的业务逻辑中，这里又面临了多重技术挑战：SDK 的集成不能对现有应用产生较大的侵入性，集成需要快速、简便；SDK 需要能够动态收集判决所需的业务上下文信息；SDK 需要有极高的执行性能、稳定性与容错能力，以建设银行自身的实践为例，访问控制 SDK 集成在建设银行日均交易量数亿的业务系统中，每一笔交易数百上千个字段，全部都

经过了访问控制引擎。访问控制 SDK 无论在策略解析、策略缓存、报文解析、访问控制执行等各环节上均采用了多种创新技术，在不增加计算硬件资源的条件下提供了全行业务过程中的数据安全访问控制服务。

(2) 业务成效

经过近两年的落地验证，中国建设银行已建成全行企业级的数据安全访问控制平台，统一访问控制策略，为行内员工渠道上数百个系统提供了业务过程中细粒度的数据安全访问控制，日均处理交易请求近 3 亿条，充分保护了客户的金融个人信息安全。

（三）敏感信息标记化输出

案例关键字：授权机制；敏感信息标记化处理

案例提供方：民生银行

1. 合规概况介绍

《开放银行数据保护与合规研究报告》对数据共享使用合规性要求、操作流程和技术支持方案等进行了归纳总结，在共享个人金融信息时，要征得个人金融信息主体同意，履行告知义务。《个人金融信息保护规范》(JR-T 0171-2020)规定，在共享个人金融信息时，支付账号及其等效信息在共享和转让时，除法律法规和行业主管部门另有规定外，应使用支付标记化（按照 JR/T 0149-2016）技术进行脱敏处理（因业务需要无法使用支付标记化技术时，应进行加密），防范信息泄露风险。

2. 背景

2020 年新冠疫情的影响下，灵活用工市场规模出现了显著增长。灵活用工可以满足企业阶段性用工需求，降低企业用工成本和用工风险，提升企业的用工弹性，企业更倾向于雇佣灵活的工作人员来应对业务需求的波动和不确定性。同时，随着数字技术的发展，各种共享经济平台的出现也为灵活用工提供了更多机会和便利，推动了灵活用工市场的发展。

通过开放银行向具有委托代征资质的共享经济平台输出薪福通、借记卡申卡接口，通过公私联动的一体化解决方案，为共享经济平台提供完善的金融服务。

为确保个人客户账户数据信息传输的合规性，在提供数据查询服务前，引导个人客户进行授权，取得客户明示同意，并针对输出的敏感信息进行标记化处理，实现在识别个人用户真实意愿的前提下保证共享经济平台机构和民生银行数据信息传输安全。

3. 方案

业务方案方面，民生银行薪福通作为对公结算类产品，为平台提供资金分账管理和劳务报酬发放能力，不同用工单位支付的用工款项，可以支付到对应的子账簿中，账务清晰明了。借记卡为平台上的个体劳动者提供用于接收劳务报酬的银行个人账户。

业务流程方面，个体劳动者在平台上可以申请借记卡，银行根据申请记录为个体劳动者寄发卡片，在个体劳动者进行临柜卡片激活后，引导个体劳动者选择是否授权平台获取其卡号信息用于劳动报酬的发放。若客户授权，则将标记化的卡号提供给平台，平台在为个体劳动者发放劳动报酬时，将标记化卡号提供给开放银行，开放银行对标记化卡号进行还原后，推送至薪福通产品系统进行后续业务处理。

(1) 授权机制

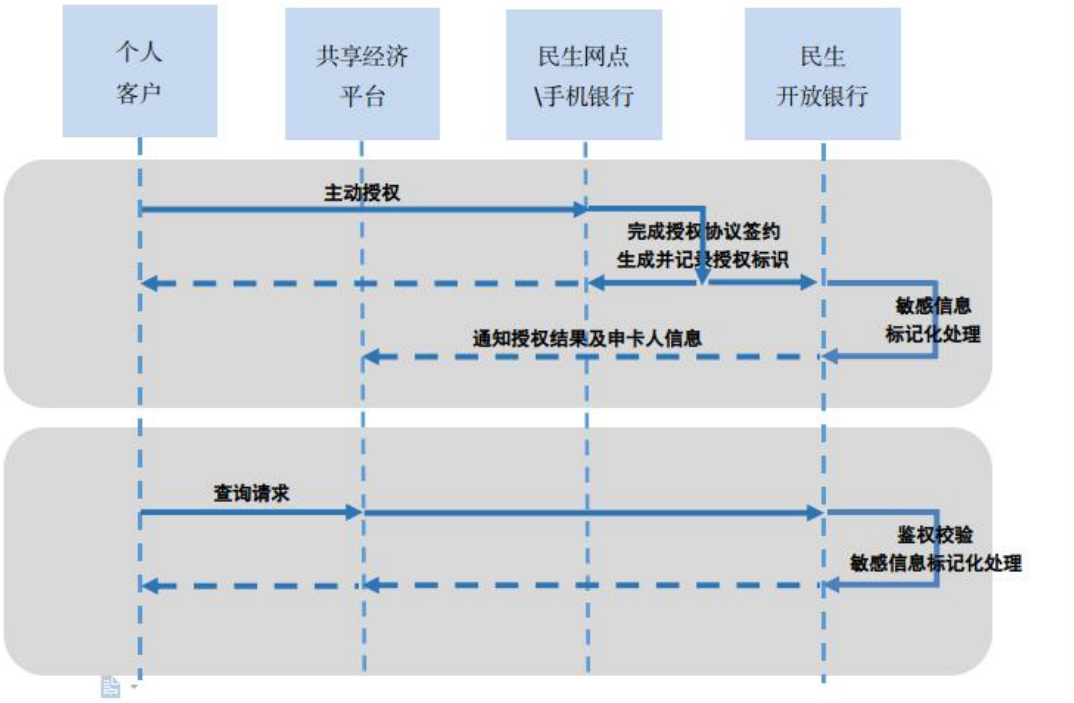

图 7 个人客户授权机制

1、个人客户开卡后，引导客户在民生银行线上或线下渠道选择是否授权平台获取卡号信息，民生银行存储授权标识。

2、民生银行判断该客户是否已完成授权，确定已完成授权后，通知共享经济平台该用户的标记化卡号信息。

3、共享经济平台端发起个人客户卡信息查询，民生银行通过授权标识鉴权，鉴权通过同步返回标记化卡号信息。

(2) 敏感信息标记化处理

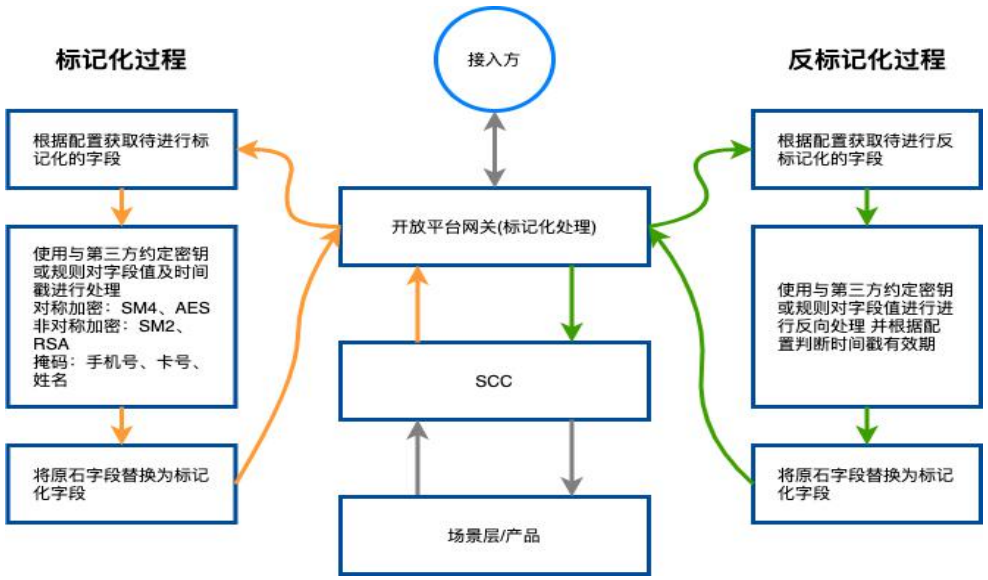

图 8 标记化处理过程

敏感信息标记化由开放平台网关根据预定规则统一处理，对手机号、卡号、姓名等个人敏感信息进行掩码处理，对重要敏感字段采用加密处理，确保开放银行与接入方之间无敏感信息明文传输。

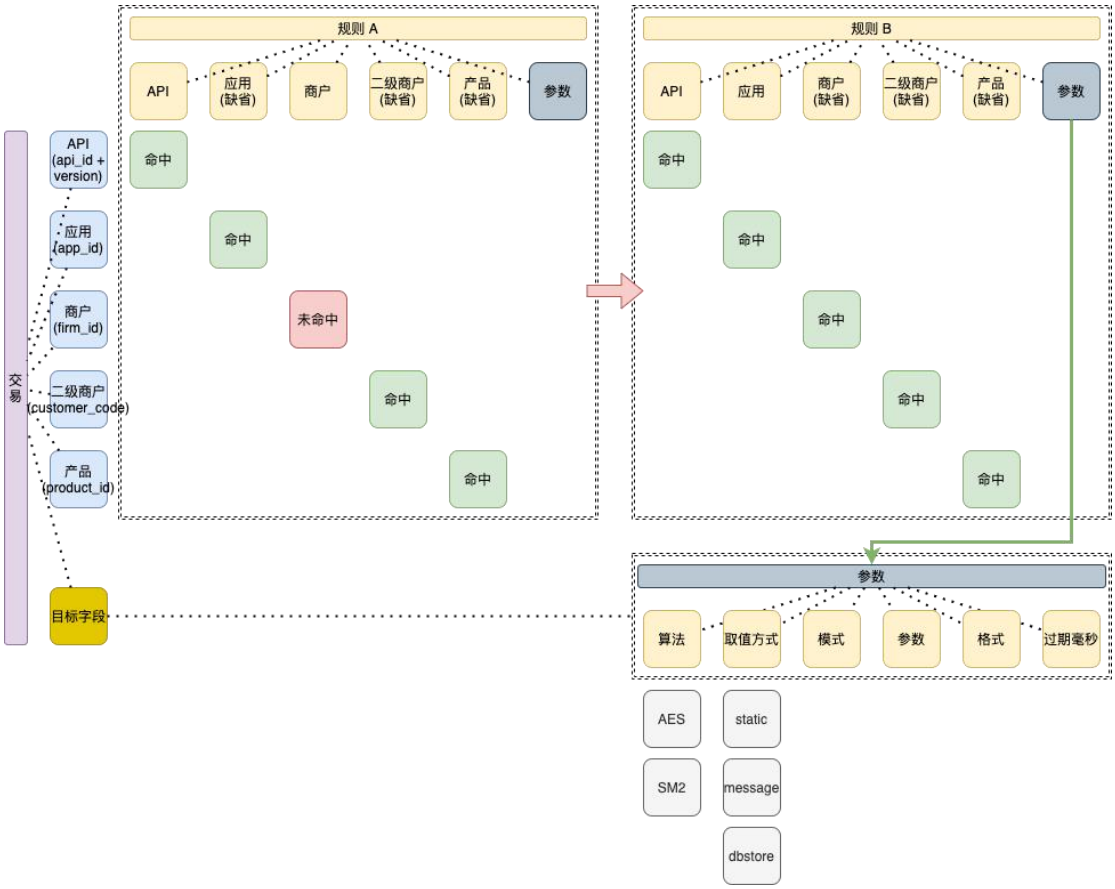

图 9 标记化处理逻辑

1、算法：

（1）提供国际和国密多种算法支持，哈希、掩码、加密等。

（2）基于统一的密码服务平台安保系统提供的远程调用，支持多种加密算法的组合使用，包括但不限于 AES、RSA、SM2、SM4 等算法。

2、过期毫秒：

（1）加密时，将当前时间拼接在目标字段的值后参与运算。

（2）解密时，如果存在过期校验，在反标记化中根据时间做比较。

4. 成效及价值

（1）技术成效

在本案例中授权机制及敏感信息的标记化处理，有效的保障了数据安全和用户隐私，满足了现有数据传输安全相关政策的要求。同时，在整体与共享经济平台交互和结果传递过程中均为报文加密传递，有效防止了共享平台和民生银行其他数据资产的泄露。在满足监管要求的前提下，实现了便捷、高效、安全的数据传输，实现了数据的高价值应用和流转。

（2）业务成效

精确应用授权机制及敏感信息标记化服务，为民生银行在共享经济领域提供了有力的支撑和赋能，帮助民生银行实现更便捷更高效更安全的用户体验。通过与持证机构合作，通过公私联动的方式，提高 B 端结算规模的同时，又可以开展 C 端批量获客。

（四）基于责任链的开放银行数据保护及合规实践

案例关键字：责任链模型；数据保护

案例提供方：中国农业银行

1. 合规概况介绍

数据收集合规方面，开放银行在提供用户信息相关服务时，若涉及收集用户信息将以签署授权协议的方式获取用户授权;数据共享使用方面，第三方在调用获取、使用、变更客户信息、账户、资金等接口时，需先取得客户明示同意，同时开放银行依据最少够用原则，采用了报文非必要字段过滤及关键字脱敏的方式；数据传输合规方面，通道层基于 TLS1.2 及以上版本安全通道进行通信，应用层支持标准国际国密算法加密，为保证与第三方之间数据传输的完整性与不可抵赖性，采用数字签名技术，为合作方应用一对一颁发证书，后续通过证书来验证第三方合法身份；数据存储合规方面，平台不存储业务类数据，业务数据从后台关联系统获取，技术类数据则入库大数据平台永久保存，对于交易日志，在完成去标识化处理后上送运维平台展示，并依据标准脱敏规则，对邮箱、身份证号、手机号等信息进行脱敏处理。

2. 背景

开放银行作为金融机构开放数据的载体，通过与第三方机构合作，实现了银行与第三方间数据服务的开放共享，将银行服务嵌入到用户生活的方方面面。在数据的共享和流转过程中，如何保障数据安全和用户隐私则显得尤为重要。为此，农业银行开放银行提出了一种基于责任链模型的开放银行数据保护解决方案。该方案基于 ZuulFilter 责任链模式构建了开放银行认证授权及数据保护体系，由一系列紧密配合工作的 Filter 按照预设的 FilterOrder 实现，Filter 间不直接通信，通过 RequestContext 共享状态。

3. 方案

(1) 开放银行数据保护责任链模型

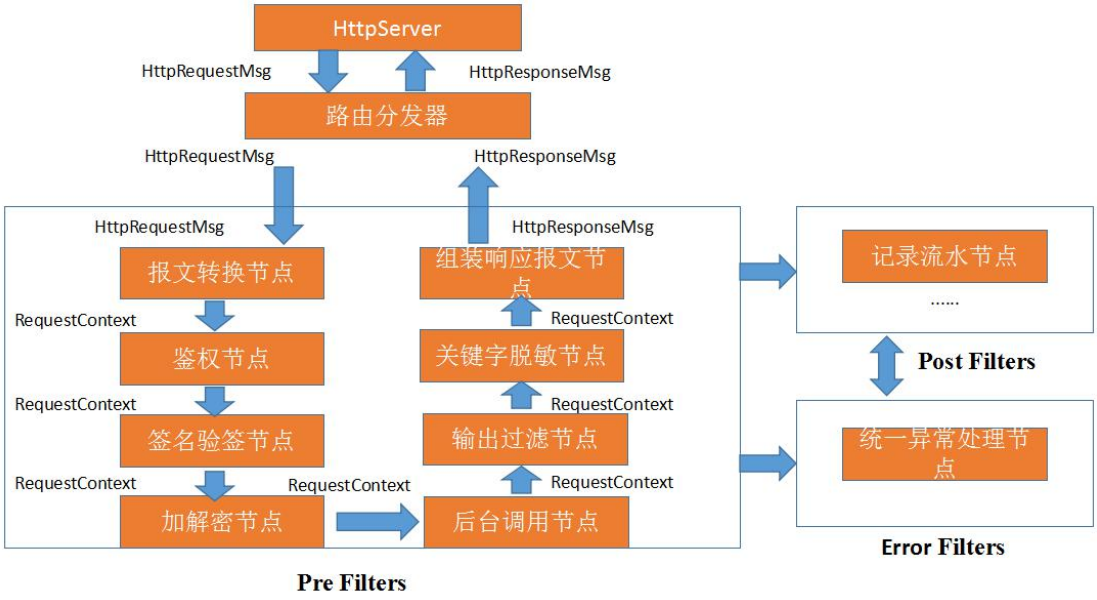

图 10 开放银行数据保护责任链模型

开放银行数据保护责任链模型主要包括三部分：Pre Filters、Error Filters 和 Post Filters。Error Filters 和 Post Filters 分别负责进行统一异常处理和事后流水记录，Pre Filters 是模型的重点，包含了一系列的数据处理节点，上图重点列出了一部分。

其中，报文转换节点用于校验合作方报文格式是否符合 HTTP 规范以及是否满足开放银行标准；鉴权节点用于鉴别合作方是否具有开放银行接口访问权限；签名验签节点通过验证合作方数字证书的有效性以确认合作方身份真实性；加解密节点在应用层面采用密钥加密手段保护数据安全；后台调用节点负责链接我行多样的开放金融产品服务；输出过滤节点可根据实际需求过滤掉报文中的非必要字段，保证了信息的最小集输出原则；关键字脱敏节点可按预设脱敏规则对响应报文的敏感信息进行脱敏处理，保护用户隐私；组装响应报文节点在完成前面所有节点处理后将组装后的响应数据共享给合作方。

责任链模型中各个处理节点形成了先后的层级关系，但各个节点间互不影响，耦合度较低，仅通过 RequestContext 共享状态。Pre Filters 执行过程中失败则会由 Error Filters 接手处理，执行完毕后进入 Post Filters 记录流水日志。只有链条上所有节点均正常执行完毕后，才会视为请求处理成功。

4. 成效及价值

(1) 技术成效

本案例中所提出的开放银行数据保护责任链模型包含了一系列的安全控制节点，有效保障了数据安全和用户隐私，符合目前数据安全相关政策要求。同时，在数据的收集、使用、传输和存储阶段，提出了对应的解决方案。责任链模型中众多的安全节点，犹如一道道关卡，在数据的生命周期管理中，起到了较好的保护作用，从而实现了同第三方机构之间便捷、高效、安全的数据共享。

(2) 业务成效

本模型已广泛应用在农业银行开放银行的开放服务中，包括但不限于电子账户、数字钱包等产品，涉及社保、教育、出行等多方面领域。截至 2022 年底，已在 400 余个总分行接口、2500 余个合作方应用中得到了可靠的实践。

(五) 服务开放平台数据安全管控

案例关键字：数据安全、服务开放

案例提供方：邮政储蓄银行

1. 合规概况介绍

在数据收集方面，服务开放平台在接口投产前对接口的数据收集合规性进行评估，并制定统一的数据收集授权机制和隐私协议，提示并获得用户主动授权同意。在数据传输方面，服务开放平台和合作伙伴间利用 SM2 和 SM4 算法实现私钥加密和报文加密，保障数据传输的保密性，并对合作伙伴的 API 请求做签名验签，保障通信过程的完整性和真实性。在数据存储方面，将客户个人信息等隐私数据上传至行内客户信息平台进行统一管控，身份鉴别类和密钥等数据由专门渠道系统、生物特征系统和密钥管理平台等系统全程加密存储，实现重要数据的分区分域存储管理。数据使用方面，提供统一的数据访问、数据共享、数据脱敏展示等策略，在服务端控制用户对敏感数据的使用，禁止所有接口提供批量打印或导出敏感数据服务，保障数据使用安全。数据删除方面，服务开放平台对已注销客户和平台已下线服务涉及的客户进行状态标记，并通过状态标记结果，限制服务开放平台对相关客户数据的在线访问和使用，保障用户合法权益。

2. 背景

在当前金融科技环境下，不仅互联网公司布局服务开放平台，拓展业务领域，扩大业务范围，覆盖更多客户；各大、中银行基于自身特点分别推出金融开放平台，提供对外服务接口，将金融服务融入不同的平台及产业链，提供全覆盖的金融服务。

近年邮储银行在集团合作、供应链服务领域都有较大的提升，通过各种渠道提供各项金融服务。为了避免各系统各自为政，独立开发，造成各种“竖井”式的前置系统，对外接口不统一，对内产生较多的功能重复接口，增加系统运维及推广的难度，邮储银行整合现有的金融服务和业务能力，规划建设了对外发布 API、H5、SDK 等多种形式的接口服务开放平台，为应用方提供“能力开放、开发工具和运行环境”于一体的一站式服务平台。

为确保服务开放平台在对外服务过程中数据交互安全合规性，邮储银行通过建立服务开放平台管理办法、服务开放接口安全规范、数据安全评估办法等安全管理制度以及内部数据合规评估、研发安全管控机制，并同时引入专业第三方 API 安全、数据安全评估服务，共同保障服务开放平台数据安全。

3. 方案

(1) 安全管控制度建设

针对服务开放平台面临的复杂的内外部环境，邮储银行通过完善的制度规范对服务平台建设、接口建设、合作流程管理、应用方管理、数据安全管理等进行规范管理。服务开放平台数据安全管控制度建设情况如下图所示。

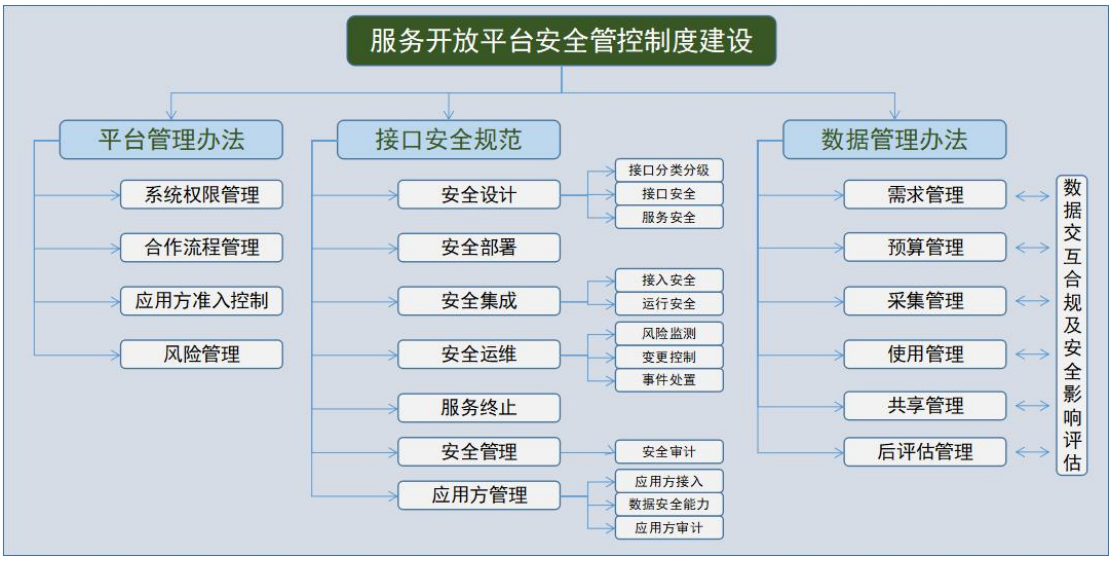

图 11 服务开放平台数据安全管控制度建设示意图

(2) 安全管控策略

针对服务开放平台的数据安全管控，邮储银行综合利用内部安全团队和外部第三方安全厂商等内外部安全能力，扬长避短，分别从研发安全管控、系统安全运维、数据安

全管理、接口与数据交互安全评估、数据安全合规评估等多个维度同步开展，共同为服务开放平台数据安全提供保障。

研发安全管控方面，邮储银行研发安全团队建立软件研发全生命周期安全管控流程，将安全左移，从业务需求分析、系统设计、系统研发和安全投产验收等各个环节，充分识别系统面临的安全威胁，建立集网络、主机、应用、数据和场景等安全闭环管控流程。

系统安全运维方面，邮储银行运维安全团队提供全面的运维监控、服务监控、流量监控、入侵检测、态势感知、数据备份与恢复等安全能力，充分保障系统安全运行。

数据安全管理方面，邮储银行数据安全管理团队建立外部数据交付安全评估管理流程，在服务开放平台业务服务接入前开展数据安全评估，识别服务开放平台在外提供服务时数据控制情况，评估数据在出行、入行以及各应用场景下的安全风险，形成数据安全影响评估报告。

在 API 接口与数据交互安全评估方面，邮储银行定期对行内为外部第三方合作机构提供服务的系统开展接口与数据交互安全评估工作，根据金融行业最新发布的接口安全和数据安全标准，利用安全渗透测试、人员访谈、文件调阅等手段充分系统所面临的监管合规风险和技术风险。

在数据安全合规评估方面，邮储银行每年邀请专业的数据安全评估机构，对邮储银行数据安全管理的制度流程和组织架构、系统数据生命周期管理情况、系统安全漏洞等进行全面评估。

邮储银行服务开放平台数据安全管控策略如下图所示：

图 12 服务开放平台数据安全管控策略示意图

(3) 安全管控技术实现

邮储银行服务开放平台是通过互联网和专线两种接入模式，为第三方合作伙伴以及总、分行等应用方提供 API、H5、SDK 等多种形式的一站式接口服务平台。

服务开放平台是一个多层次的、多业务的、跨平台的业务处理系统，内部与邮储银行目前运营的多个关联系统有连接，外部对接产业应用平台及消费平台各种生态系统。因此系统的安全需求体现在多个层面上，这些层面的安全目标各不相同但互相关联。

邮储银行服务开放平台通过 IaaS 云平台、行内各关联系统和平台自身的安全组件为平台提供通用的安全服务能力，形成一个集硬件与软件于一体的安全服务网关。服务开放平台技术框架如下图所示。

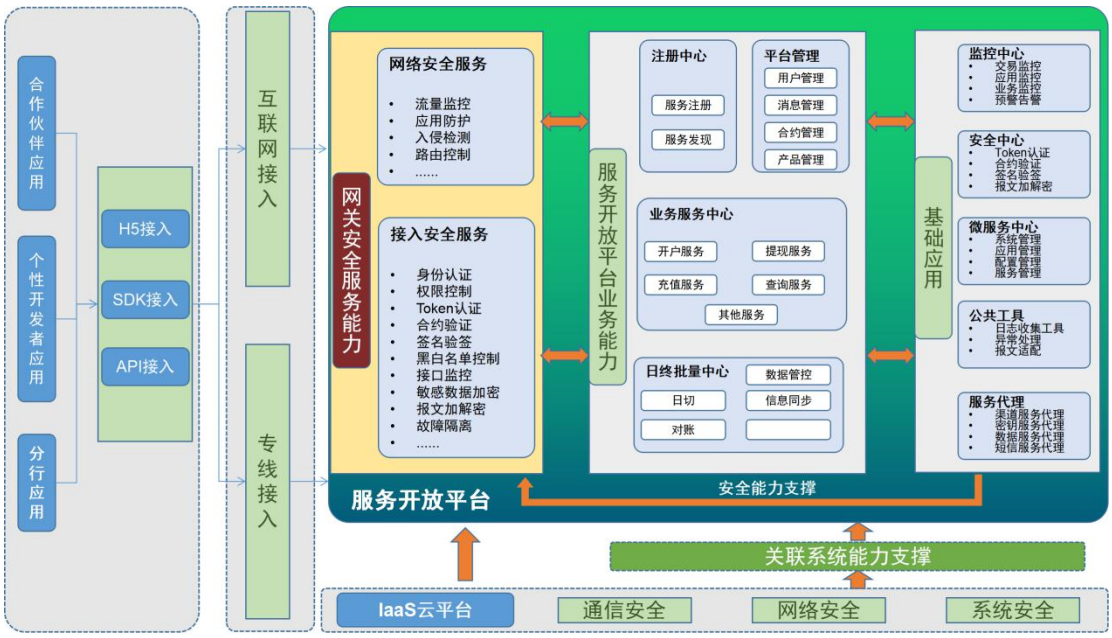

图 13 服务开放平台技术框架图

当服务开放平台在与合作方进行数据交互时，利用报文加解密和签名验签技术，保障报文数据传输的安全性和真实性。服务开放平台数据交互安全技术设计如下图所示：

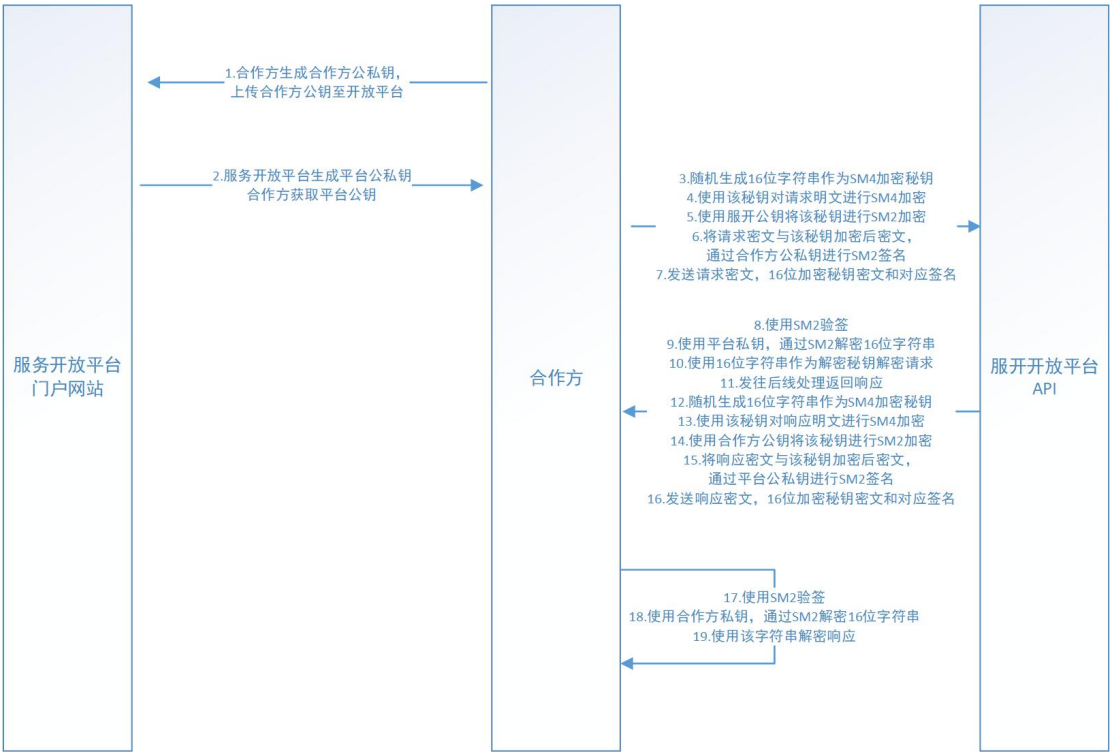

图 14 服务开放平台数据交互安全技术设计图

密钥交换规则：1.合作伙伴根据服务开放平台提供的密钥生成工具，生成公私钥。2.合作伙伴将公钥 public key 1 上传给服务开放平台，保留私钥 private key1。3.合作伙伴下载服务开放平台分配给合作伙伴的公钥 public key 2 和签名密钥 security key 1，服务开放平台持有平台私钥 private key2。

报文加密规则：1.合作伙伴发起 API 调用时，随机生成一个 key，并使用这个 key 对请求报文做 SM4 对称加密。然后使用 public key 2 对这个 key 进行 SM2 非对称加密。2.服务开放平台收到合作伙伴的请求报文后，使用 private key2 对加密过的 key 进行解密，并使用解密后的 key 对请求报文解密。

签名验签过程：1.利用报文加密过程的密钥交换规则生成加解密密钥并实现密钥安全交换。2.合作伙伴对使用 SM4 加密过的报文+合作伙伴签名密钥 security key1 组成的字符串取 SM3 的值，使用 public key 2 进行 SM2 加密后作为签名。3.服务开放平台使用 private key 2 对签名进行解密，得到合作伙伴的签名值。然后对请求报文密文+合作伙伴签名密钥 security key1 组成的字符串做 SM3 得到服务端计算的报文签名值。通过对比合作伙伴签名值和服务端计算的报文签名值是否一致实现验签，判断报文是否被篡改。

4. 成效及价值

依据《数据安全法》、《个人信息保护法》以及相关行业标准规范，从安全制度体系建设、安全管控策略和安全管控技术三个层面，建立了完善的服务开放平台数据安全管理体系，并通过了 ISO27001 信息安全管理体系认证。具备覆盖系统全生命周期的数据安全保护流程，在业务需求阶段，建立了合作方数据安全准入机制，对我行与合作方进行数据交互进行安全评估，评估通过后才允许实现数据交互业务需求。在系统

安全架构规划时，开展数据分类分级工作，明确数据安全级别，对不同级别数据采取不同的数据安全保护措施。在需求设计阶段，围绕数据生命周期，建立数据安全需求基线，通过服务开放平台实现通用的数据安全交互功能，明确 API 接口和数据安全保护要求，并制定相应的安全测试用例，对 API 接口进行安全测试，确保在系统投产上线前满足监管合规要求。对已上线的存量系统建立了 API 接口资产台账，进行分级管理，并开展专项的数据安全评估工作，及时发现相关数据安全风险，采取相应的数据安全保护策略，降低由于 API 接口导致数据安全泄露的风险。

（六）开放银行整合银企直连的代发工资服务输出

案例关键字：开放银行版前置机加密机；

案例提供方：中国交通银行

1. 合规概况介绍

在数据收集合规方面，为满足《个人信息保护法》中的“知情同意”原则，在企业入驻开通产品的时候会通过签署协议告知获取用户信息的授权，同时企业也会征询员工的授权；在数据传输合规方面，链路采用 TLS1.2 进行通信，链路数据是按照国密或国际加密算法进行加密保护，用户通过加密机和硬件 KEY 进行解密获取，最大程度上保证数据传输的安全性；在数据存储方面，密钥存储在加密机或者前置机中，银行端交易日志存储在专用历史库中，客户端交易日志按照入驻协议要求进行安全存储并在有效期过后进行删除。

2. 背景

银企直联发展至今已近 20 年，在此期间，客户需求、市场环境都发生了显著的变化。基于银行企业网银客户体系构建的银企直联模式已经在一些地方面临业务发展和客户诉求的压力：

1、银企直联业务功能与企业网银同源，产品定位为银行企业客户群体，这种模式决定了通过银企直联提供给企业用户和服务与企业网银高度耦合，在接口参数、多步骤访问流程、权限控制等方面都带有明显的企业网银特征，客户如果选择通过银企直联访问银行服务则需要连带开通企业网银产品权限并设置企业网银相关业务参数。

2、银企直联在证书下载、接口调试、网络连通、密钥管理等方面都比 OpenAPI 方式繁琐、成本高，企业客户出于开发效率和运维成本的考虑，往往倾向于 OpenAPI 模式。

3、各家银行都在推广 OpenAPI，大量产品业务已经支持 OpenAPI 模式输出。与此同时，企业网银客户或主动或被动与银行 OpenAPI 平台进行服务对接。企业对于维护两套直联系统、两种直联标准感觉繁琐。从调研来看，很多客户希望可以将银企直联提供的产品统一到 OpenAPI 接口标准中，以 OpenAPI 的方式对接银行。

开放银行和银企直联的区别：

1、SSL 链路安全。开放银行是基于 TLS1.2 标准通过 DigiCert 颁发证书建立 HTTPS 协议下的安全链路完成可信网络。银企直联基于自建证书体系，通过前置机和服务端硬件设备建立 SSL 安全链路。

2、报文安全。开放银行在请求和响应都会对报文进行一次加签加密，保证双向的数据安全。银企直联只会对请求报文进行加签验签，返回报文没有任何安全处理，并且加签算法也比开放银行弱。

3、身份认证。开放银行通过商户管理的安全密钥来校验商户身份是否合法，通过平台的安全密钥提供给商户校验平台的身份。银企直联通过银行颁发的硬件 KEY 证书密钥来保证商户访问的合法性

4、密钥管理。开放银行的密钥管理在商户端是本地自己保存，银行端是保存在安全部。银企直联按要求存放在硬件 key 或加密机中。

在以上背景下，交行以代发工资项目为试点，落地动账类交易的系统整合。

3. 方案

(1) 整体架构

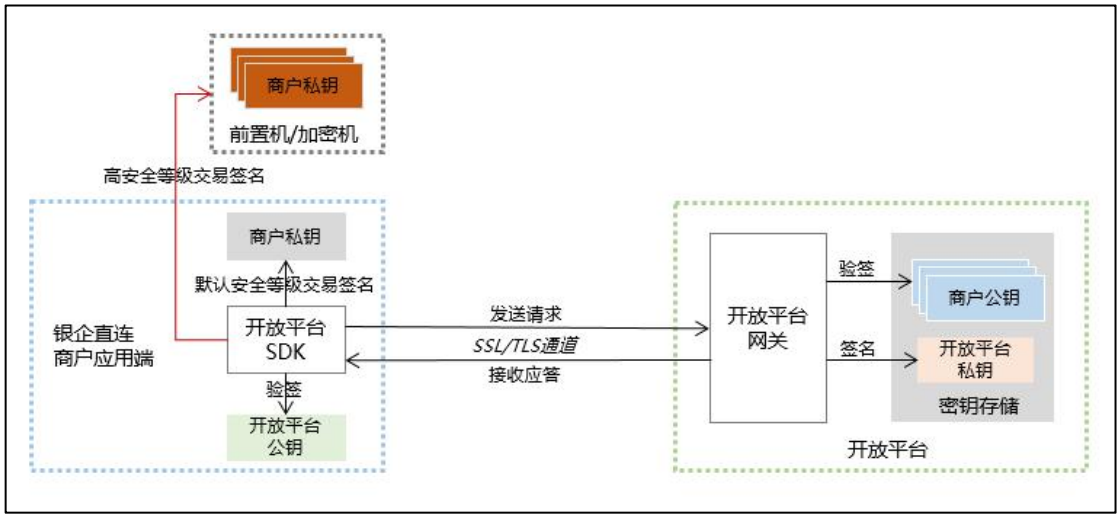

图 15 基于前置机/加密机的双密钥安全通讯架构

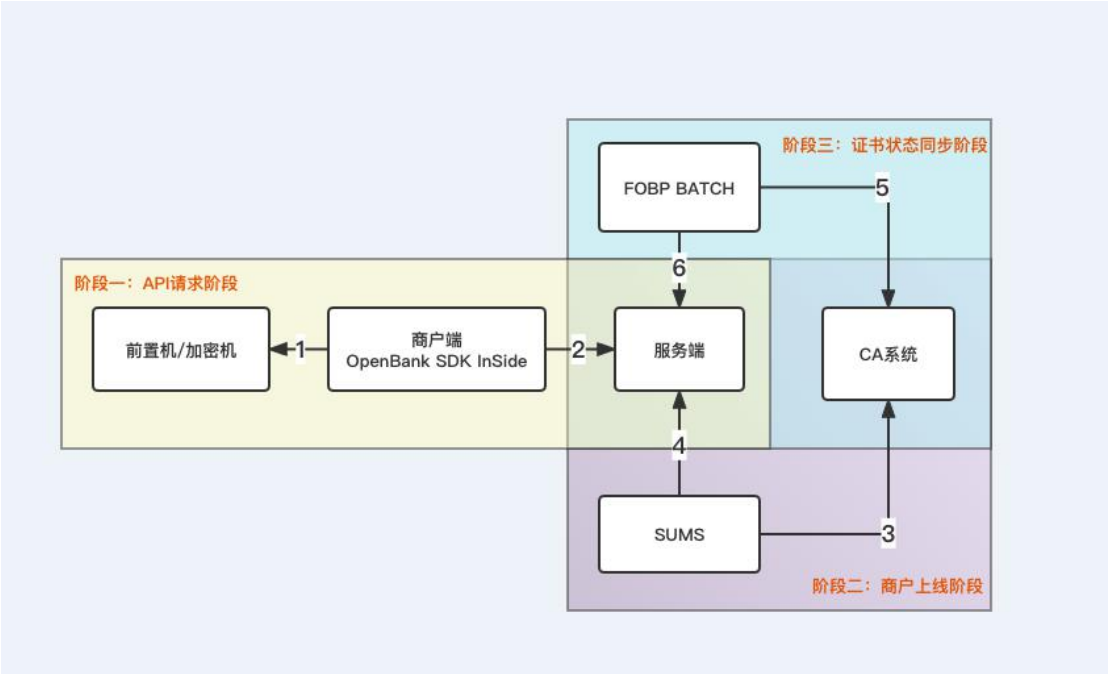

图 16 密钥交互流程

交行通过设置 API 的不同等级来识别是否配套使用前置机或加密机模式，若使用前置机或加密机，开放银行平台需要在交易中通过鉴权中心 CA 系统的接口去验证客户的密钥。

（2）业务流程

1、客户通过门户网站申请开通代发工资产品，根据产品在治理平台配置的安全校验等级为硬件 KEY 校验，提示客户待银行审批通过后需至柜面领取硬件 key，并在上线后通过网站权限管理功能将开放银行产品接口与硬件 key 及网站用户做关联绑定。如由分行代为客户进行入驻操作的，需提示客户经理在上线前需及时领取硬件 KEY。

2、完成入驻审批后，客户经理通知用户至网点领取硬件 KEY 并进行企业现场身份识别，开通网络金融客户号、企业对公结算帐号（如需）及核心客户号。

3、经开放银行入驻审批通过的客户可登录开放银行门户网站使用手机或者企业网银身份登录，并在用户权限管理中新增虚拟操作员，关联产品及硬件 KEY，并为每位操作员配置接口调用的权限。

4、用户开通产品后，可调用接口推送交易。如用户开通的产品为需要加密机和前置机的代发工资接口，每次发送交易前需要经前置机硬件 key 或加密机完成相应的授权操作。

4. 成效及价值

（1）技术成效

本案例针对不同客户群设置不同的密钥等级，按照密钥等级给客户设置不同的安全校验方式，保证了高等级客户的链路和交易的安全性，增加账务类数据的安全落地。

(2) 业务成效

由于对公业务对于交易安全的要求较高。有鉴于此，平台扩充了高安全等级的加密模式，涵盖硬件加密机模式、前置机+硬件 KEY 模式，并实现了分离式密钥的加密模式。当前这些模式已经应用到多个合作项目中，客户反映很好。

（七）信贷模型预测服务

案例关键字：隐私计算；普惠信贷

案例提供方：中国工商银行

1. 合规概况介绍

在数据收集合规方面，为满足《个人信息保护法》中的“知情同意”原则，在用户提出申请时通过签署协议的方式获取用户信息的授权；在数据传输合规方面，模型训练阶段不涉及用户原始数据的传输，并且对于所传输的中间参数、梯度等信息采用同态加密等方式进行了保护，在模型预测阶段，由于涉及用户三要素的传输，采用了国密等加密算法对原始数据进行了保护；在数据存储方面，最需要关注的模型资产数据及推理结果采用了加密手段被存储在合作方，密钥储存在工商银行侧，保障了用户的预测标签只有工商银行能够获取。

2. 背景

在银行业务场景中，小微商户市场发展前景广阔，客户数量多、总体规模大，在繁荣经济、稳定就业、促进创新、方便群众生活等方面发挥着独特的重要作用，以个体工商户为典型的经营主体，金融需求多样、交易活跃，是未来优质客户的重要来源。为落实国家进一步扶持中小企业的要求，结合开放银行理念，工商银行普惠部网金中心与银联合作，以“银行组织、联盟、协会或银行+银行”模式，以银联数据服务输出方式，嵌入在工商银行业务流程中，实现小微商户违约评分模型的构建，并支持面向小微商户的“商户贷”产品的模型驱动自动审批。

为确保数据共享的合规性，本次合作基于联邦学习技术，在数据不出库的情况下，实现银联和工商银行商户信息融合互补，深入描述小微商户画像，为客户风险评估等提供更全面有效的数据基础。

3. 方案

(1) 模型构建阶段

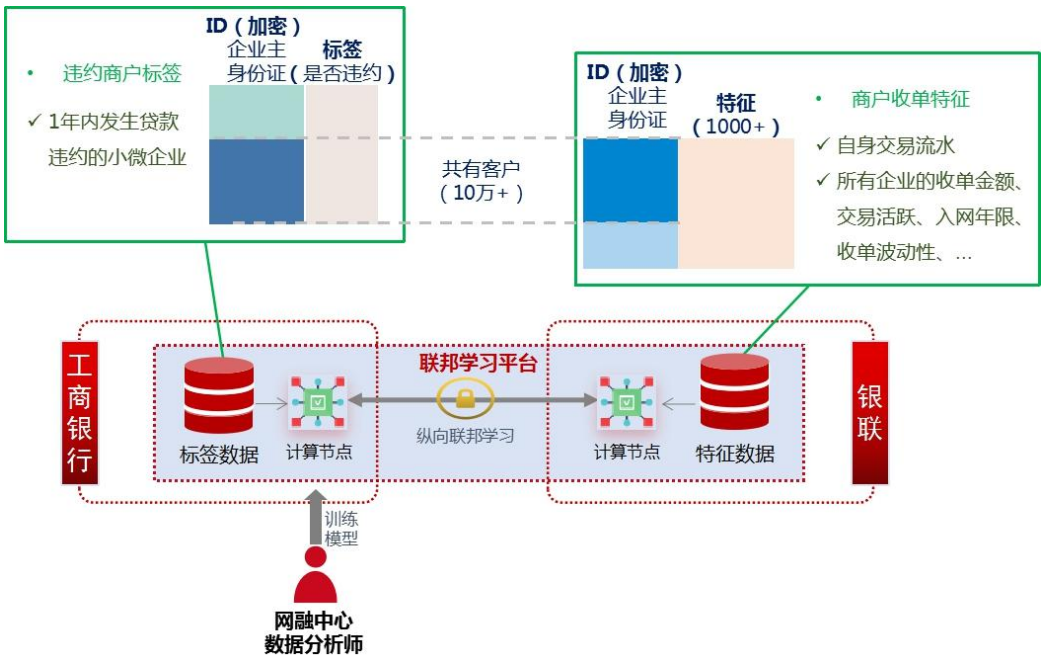

图 17 商户违约评分模型训练

1、银联提供收单商户特征数据。

2、双方数据构建样本：双方通过加密的“企业主身份证号码”，通过隐私求交算法完成数据对齐，得到训练样本。

3、双方数据联合训练：在联邦学习平台上选择梯度提升树中的 Xgboost 算法开展纵向联邦模型训练，模型以密文方式保存在中国银联侧的联邦学习节点上，供后续推理商户违约评分计算使用（该模型的评分结果会进行非对称加密，在没有工商银行密钥情况下，银联无法将该模型给其他机构使用）。

(2) 开放银行服务提供违约评分测算

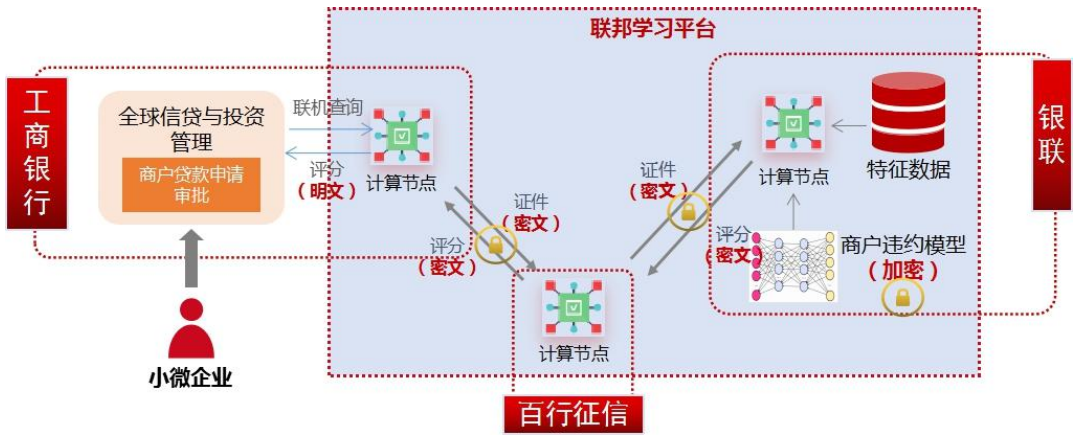

图 18 商户违约评分模型正式线上服务（因涉及征信，需要持牌机构百行参与中转）

工商银行通过银联开放银行服务查询加密评分：银联将训练完成的联邦模型包装为开放银行数据服务提供给工商银行调用。当小微企业通过申请工商银行“商户贷”产品的贷款时，工商银行将小微企业主的身份证加密后作为查询条件，调用银联侧通过开放银行提供的模型服务，查询计算出该商户的违约评分（密文）后，返回工商银行。

工商银行解密商户违约评分：工商银行侧的联邦学习节点收到密文的商户违约评分后，使用密钥进行解密并将解密后的明文商户违约评分返回给信贷管理平台，基于贷款审批策略根据评分进行贷款自动审批，实现精准授信。

图 19 商户贷申请流程

4. 成效及价值

(1) 技术成效

银联在本案例中提供的模型服务，其建设过程基于联邦学习完成，有效保障了数据安全和用户隐私，满足了现有数据安全相关政策的要求。同时，银联的模型服务调用过程和结果传递均为密文传递，有效防止了银联和工商银行双方数据特征分布、用户标签等数据资产的泄露。基于联邦学习技术的开放银行数据共享模式，有效打破了工商银行和银联数据壁垒，在满足监管要求的前提下，实现了便捷、高效、安全的数据共享，实现了数据的高价值应用和流转，相比工商银行原有模型，引入银联特征数据所构建的联合模型效果提升高达 20%。

(2) 业务成效

银联通过开放银行提供了模型评分服务，向工商银行进行了高效优质的数据共享，为工商银行在小微商户授信领域提供了有力的支撑和赋能，帮助工商银行实现更精确的风险评分和信贷审批，进而更全面、更准确地判断客户资质，有效扩大小微商户客群的服务规模。项目上线仅 3 个月后，即成功新增拓户万余户，放款超数十亿元，在常态化疫情下为小微企业纾困解难。

（八）多方安全数据分析平台与金融反诈应用

案例关键字：金融反诈；联邦学习；多方安全计算

案例提供方：中国农业银行

1. 合规概况介绍

在数据收集合规方面，本项目严格按照《个人金融信息保护技术规范》（JR/T 0171—2020）、《区块链技术金融应用 评估规则》（JR/T 0193—2020）、《金融科技创新安全通用规范》等相关金融行业技术标准规范要求进行；在数据传输合规方面，平台使用区块链平台负责管理控制流，具有“不可伪造”“全程留痕”“可以追溯”“公开透明”“集体维护”等特征，隐私计算引擎负责基于多方安全计算及联邦学习等技术，实现数据的安全计算流，真正做到数据的“可用不可见”。安全计算基于盲签名、秘密分享和不经意传输技术实现了安全求和、安全求交和隐私查询功能，整体协议安全性归约到 RSA，SM2 的安全性，其满足《中华人民共和国金融行业标准》（JR/T 0025.17 – 2013）以及国密局《GB/T 32918-2016 信息安全技术 SM2 椭圆曲线公钥密码算法》规范标准。两种科技手段的结合使用将有效解决平台建设阶段中数据信息安全、效率成本、监督管理等方面存在的欠缺，进一步完善机制、提升效率，扩大成果；在数据存储合规方面，各参与方数据均在本地存储，查询完成后，查询方存储查询结果，保证数据存储安全。

2. 背景

为严厉打击新型网络犯罪，提高金融风控能力，响应人民银行、公安部、工信部、银监会等关于组织开展打击治理电信网络新型违法犯罪专项行动，加强跨机构、跨行业风险信息规范共享和系统互联互通，掌握风险来源、分布和变化趋势，提高基于高频大数据精准动态监测预测预警水平，增强风险多渠道态势感知、综合性分析评估和差异化处置能力，建设安全计算平台。本平台基于多方安全计算、联邦学习、联盟区块链等新一代信息技术，遵循“数据可用而不可见”“数据不动价值动”原则，构建了跨机构间数据合规流通与融合使用的新型信息基础设施，在保障各方间数据安全隐私前提下，促进了对各家商业间数据的合规融合与使用，实现了涉诈线索的精准识别、事中阻诈等多类别关键需求，以科技能力有效保障了人民群众财产安全，并取得显著效果。

3. 方案

系统具体功能模块分为隐私计算平台、区块链平台和账号反诈业务系统三部分：隐私计算平台以可用不可见的方式实现了数据隐私安全的联合计算；具体包含隐私查询、可信数据分析和联合建模功能，隐私查询在不泄露查询条件的情况下获取查询结果；可信数据分析提供了四则运算、逻辑运算等基础算子及其组合计算；联合建模提供了聚类、回归模型、树模型、神经网络等丰富的算法类型。区块链平台的定位是实现对联合计算产生的任务数据请求、授权、使用、计算等环节进行存证，保证隐私计算任务全流程可追溯、可验证，确保数据使用的合法合规。账户反诈业务系统通过建设数

据综合应用平台，为用户提供黑灰名单匿名查询、潜在风险识别预警、风险排查处置管理、反洗钱调查等功能。

4. 成效及价值

(1) 技术成效

本项目融合区块链与隐私计算技术体系搭建了安全可信、隐私强化的数据流通基础设施，有效支撑了多家银行与机构之间的数据共享，实现了黑灰名单核查、精准阻诈等实时/批量统计功能。

(2) 业务成效

本项目所构建的多方数据分析联合实验室平台覆盖多家银行和机构，系统规模进一步扩大，这也是至今国内所运用“区块链+隐私计算”技术最大规模的生产级应用案例，在全国具有首创性与先进性。项目的成功实施应用也为行业大数据走出去提供了开放共享高价值参考。基于联盟区块链、安全多方计算与联邦学习并搭载高效通用的数据隐私算法，有效解决多方数据归集模式下的数据隐私违规问题，可服务于包括信贷风控的联合建模、大数据隐私查询、精准营销用户画像等诸多数据融通场景。

(九) 行司联动提升风控能力

案例关键字：隐私计算；联邦学习；联合风控

案例提供方：中国银行

1. 合规概况介绍

在数据收集合规方面，为满足《个人信息保护法》中的“知情同意”原则，在用户提出申请“好客贷”时签署相应授权协议获取用户信息的授权；在数据传输合规方面，模型训练阶段不涉及用户原始数据的传输，并且对于所传输的中间参数、梯度等信息采用同态加密等方式进行了保护，在模型预测阶段，由于涉及用户 ID 的传输，采用了国密等加密算法对原始数据进行了保护，推理中间结果采用了加密手段进行传输；在数据存储方面，模型资产数据和预测数据均在中国银行和附属子公司域内分别存储，保障了用户信息不出域，保护客户隐私。

2. 背景

隐私计算技术可以实现“数据可用不可见”，在双方或多方数据均不出域的情况下进行数据价值的安全共享。运用联邦学习技术，使用行司两方的数据进行安全建模，在保证双方数据隐私与合规要求的同时挖掘数据价值。中银消费行司联合风控建模项目是风控场景。利用联邦学习技术，进行分析建模，可打通双方数据，提高数据利用率，并可将模型接口集成现有系统内，方便中银消费及时掌握模型运行及表现情况。联合行内数据建立风险评估模型，对“好客贷”以及公司其他产品均可以提升风控能力。

3. 方案

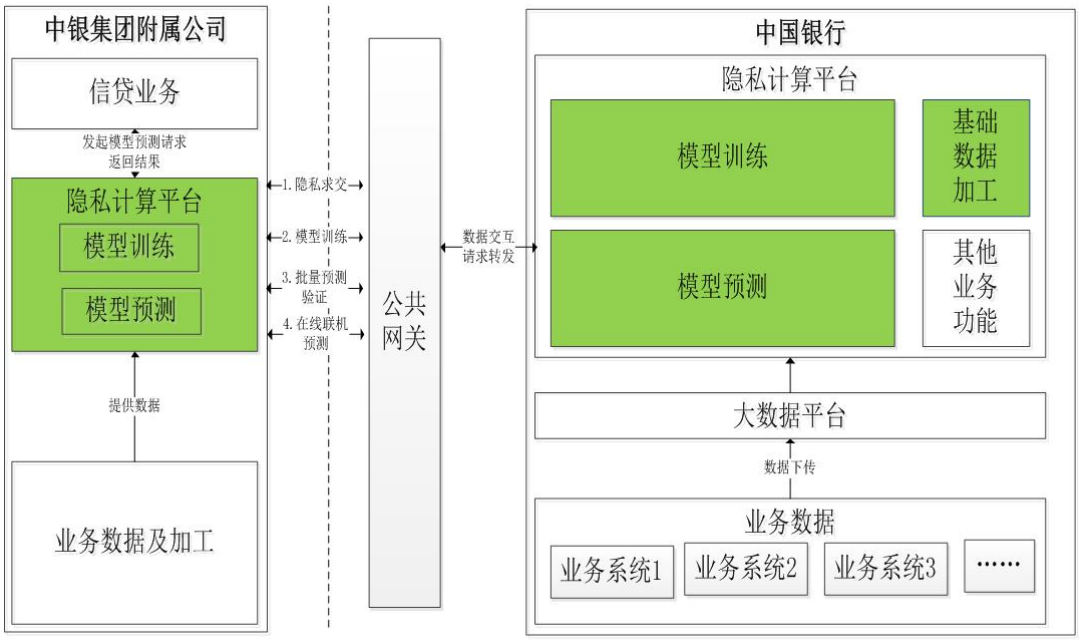

图 20 中银消费行司联动架构图

（1）贷前审批模型

1）运用中银消费的历史数据包括模型评价标识、客群数字画像等信息，联合行内数据包含资产数据、交易数据、信贷记录、手机银行行为等数据,通过逻辑回归、树模型等可解释性强的算法进行联合建模。

2）模型训练阶段：中银消费提供目标值（Y）——评价体系，特征值基本信息等；中国银行提供特征值包括：资产数据特征、交易数据特征、信贷记录特征、手机银行行为特征等数据。输出为模型。

3）预测调用阶段：根据用户 id，中银消费与中国银行分别得到各自模型部分的评分，两部分评分的和作为结果输出。

4）在审批阶段调用模型或模型结果，得到评分。对于评分区间划分风险等级，应用于准入策略，客群策略以及额度策略。对低分客户限制准入；对中高分客户，根据客户评分高低，给予不同授信额度。

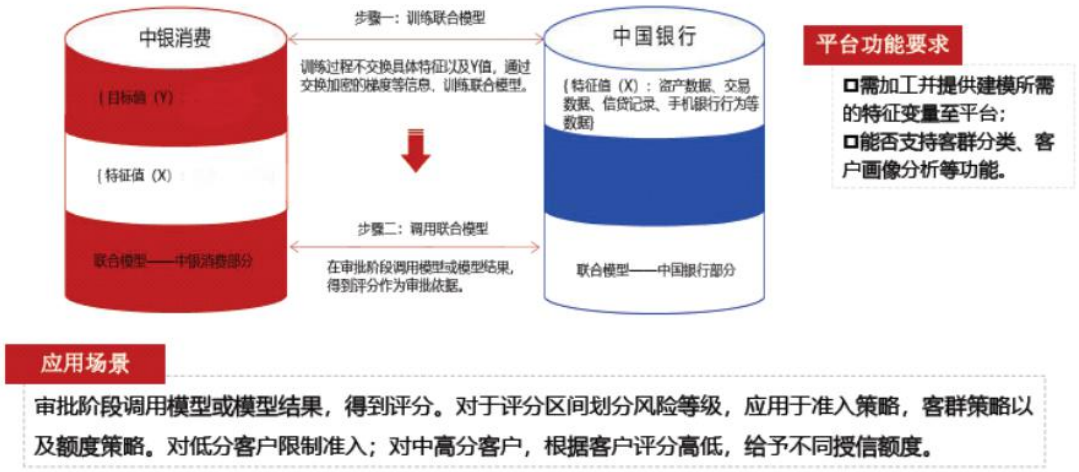

图 21 贷前审批模型

(2) 贷中风控模型

1、运用中银消费的客户行为数据与中国银行的客户资产、交易流水、手机银行行为、信贷记录等数据进行联合建模。

2、模型训练阶段：中银消费提供目标值（Y）——风险评分，特征值用户行为信息等；中国银行提供特征值包括：客户资产、交易流水、手机银行行为、信贷记录等数据。输出为模型。

3、预测调用阶段：根据用户 id，中银消费与中国银行分别得到各自模型部分的评分，两部分评分的和作为结果输出。

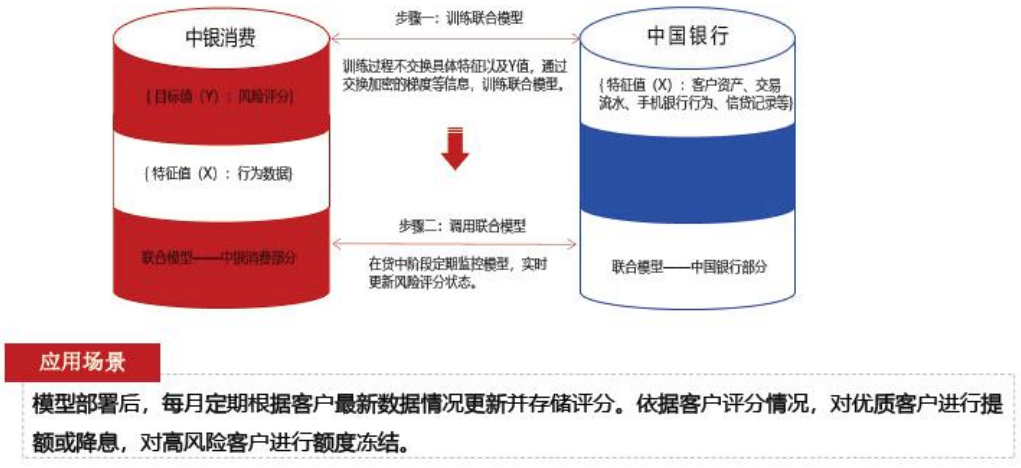

图 22 贷中风控模型

4. 成效及价值

(1) 技术成效

本案例采用了联邦学习技术，实现了模型训练参数交互过程中全密态保护，切实保护了数据安全。中国银行与中银消费双方通过专线接入，保证了通讯安全。对数据中的客户特征和标签进行加密，确保建模过程中客户隐私保护。

数据用以客户维度按月加工，用于训练和预测的数据加工逻辑保持一致。在训练过程中，会传递加密 id 和中间结果和梯度，待训练完成验证模型验证后，为了防止加密 id 泄露或中间结果数据反推，相关数据会进行清理；用于预测的数据的 id 采用加密存储，更好保护客户隐私安全。

(2) 业务成效

本案例是中国银行和集团子公司中银消费金融有限公司利用隐私计算开展跨机构数据融合，基于纵向联邦学习 XGBoost 算法共建个人信贷风控模型。行司联动“好客贷”业务是由中银消费金融联动中国银行，基于行内存量客户金融属性数据联合建模，在保证数据安全、信息安全的前提下，有效筛选需求真实、消费意愿强、还款能力可靠、信用风险可控的目标客群，经客户授权后，匹配差异化申请流程、定价、利率，通过合规经营、正确引导，为客户提供合理、便捷、安全的纯线上金融服务，满足下沉客群消费信贷需求。

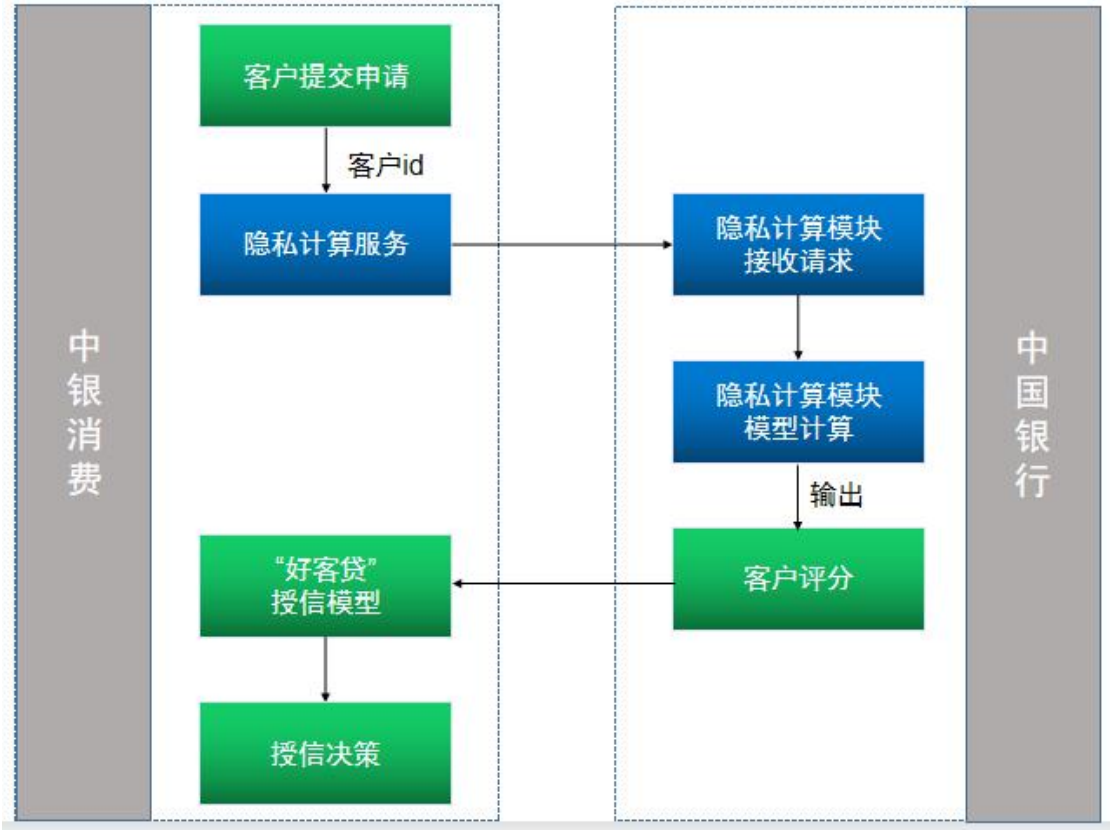

图 23 中银消费“好客贷”申请流程图

（十）高价值户识别模型预测服务

案例关键字：隐私计算；企业智慧营销

案例提供方：招商银行

1. 合规概况介绍

该场景仅涉及企业相关数据。模型训练阶段不涉及用户原始数据的传输，并且对于所传输的中间参数、梯度等信息采用同态加密等方式进行了保护，仅凭这些参数无法反推各自原始数据，且建模完后各自建模数据销毁，建模阶段仅输出一个模型，模型是没有 ID 属性或和 ID 有相关性的，也不会指向任何特定客户 ID。在模型预测阶段，采用了国密等加密算法对原始数据进行了保护。

2. 背景

招商银行某分行逐步探索隐私计算技术与实际业务结合的新模式。分行客户经理人数有限，需要有效的资源分配形式，将更多精力放在优质客户经营上。地方某金融大数据公司数据翔实、全面、可靠，包含多方面政务数据，可全面真实地反映出企业的实际质量。考虑到数据安全法律法规，传统方式下此类数据仅能在获得用户充分授权的前提下直接调用。因此，分行考虑使用联邦学习等隐私计算技术，在各方底层数据不出本地的前提下，使用双方数据建模提升模型效果，从而获得更加精准的模型预测结果，实现数据价值的合规流动。

3. 方案

该模型引入可衡量客户真实价值的政务数据作为特征及客户价值标签构建模型，模型对客户进行分层，分层结果对于营销和高质量拓客经营有很高的指导意义。

1、地方大数据公司提供特征，以及用于衡量客户真实价值的政务数据生成客户标签。

2、行内提供特征。

3、双方训练联邦 xgb 模型，模型形成服务获得客户分层，客户名单分别用于分行各类产品的精准营销。

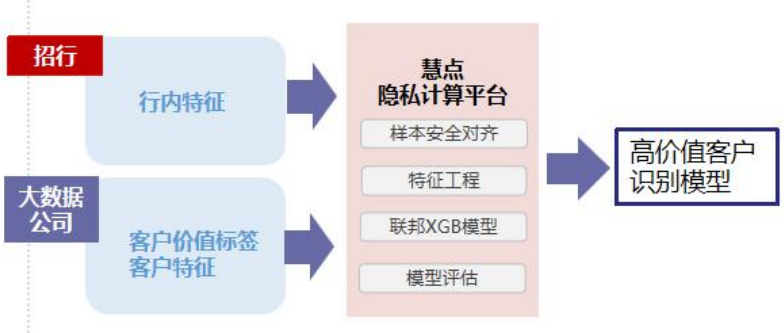

图 24 招商银行高价值客户识别场景示意图

4. 成效及价值

该模型是一个以客户真实价值为预测目标的联邦模型，相较于分行传统客户价值模型，准确度增幅 38%，可提升分行营销效率。

政府侧公信力数据分散，存在“数据孤岛”现象，数据无法得到有效利用，政府具有“服务实体经济、发展普惠金融”的职责，当前困境下推动难、落地难；招商银行利用隐私计算技术主动赋能业务，在完善用户画像实现客群快速高质增长提升效率的同时，也通过联合建模方式，帮助政府更好发挥高质量政务数据价值，为政府监管、定向帮扶困难企业，在主动构建互信共赢的“银企命运共同体”打造普惠金融服务金字招牌，推动民营、小微企业融资增量扩面、减费降本，协助中小微企业复产复工等方面做出了一定的社会贡献。

四、总结与展望

由于开放银行提供数据共享服务的模式多样，涉及到数据流转的环节复杂，同时其应用的场景十分丰富，不同场景下数据的合规要求也不尽相同。因而，开放银行在现阶段的数据保护手段及合规实现也呈现出百花齐放的状态。在本报告中，各家银行根据自身优势、定位、需求等差异，从开放银行数据流转的不同阶段采用了多样化的技术方案或管理手段，力求从多个层面保障数据的安全、合规的共享，为开放银行数据保护及合规实现的体系化发展打造了坚实的基础。

在数据传输和流转方面，华夏银行重点关注了传输阶段的数据安全保护，针对在服务端、移动端、浏览器端的开放银行接口实施了支持多种加密算法的加密配置，同时对开放银行 SDK 的开发、使用、监测等全生命周期执行严格的安全标准，提升其安全性。在数据访问控制方面，建行基于属性（ABAC）构建了访问控制上下文模型，搭配以业务过程对个人信息的访问情况所实施的控制策略，以平台化的方式实现了数据访问控制的统一管理，充分保护了客户个人信息安全。在敏感信息采集传输方面，民生银行结合个人授权机制及标记化处理，有效地保障了数据安全和用户隐私。在授权认证方面，农业银行基于责任链模式构建了开放银行认证授权及数据保护体系，通过责任链上不同的节点保障对数据流转过程中的安全和隐私；在合规制度方面，邮储银行通过建立服务开放平台管理办法、服务开放接口安全规范、数据安全评估办法等安全管理制度以及内部数据合规评估、研发安全管控机制，并同时引入专业第三方 API 安全、数据安全评估服务，共同保障服务开放平台数据安全。在银企直连向开放银行模式转型过程中，交通银行保留了银企直连模式中的前置加密机进行密钥管理，用户通过加密机和硬件 KEY 进行解密获取，最大程度上保证数据传输的安全性。除此之外，本报告中，工商银行、农业银行、中国银行和招商银行还采用了隐私计算技术实现了在原始数据不出域的前提下，完成了数据价值的传输，在黑名单查询、信贷风险预测等场景下实现了对银行及合作机构的业务赋能，在数据流转阶段用一种新的技术保障了数据安全和隐私。

数字经济的产业规模正在快速增长，推进高质量数字化转型、健全适应数字经济发展的现代金融服务体系将是金融行业未来发展的主旋律。开放银行是银行业数字化转型

的重要形式。随着国家不断加大对金融敏感数据安全的监管力度，商业银行在推进开放银行进程中面临着越来越艰巨的数据安全挑战。依据 2021 年发布的《开放银行数据保护与合规研究报告》中提及的关于平台互联存在的数据信任等问题14，中国银联技术管理委员会开放银行课题组就开放银行场景中数据安全现状开展研究，在系统掌握开放银行数据安全痛点的基础上，从监管科技的角度出发提出了“监管前哨”的安全框架，并从数据识别、数据脱敏和数据水印三项监管前哨的核心技术开展创新研究，为解决商业银行和应用方在数据共享使用中的安全隐患提供技术支撑，促进开放银行生态的持续健康发展。

针对我国的开放银行创新发展模式的需求，以及监管环境的现状，结合技术研究中发现的、技术层面解决不了、需要在政策层面解决的若干问题，提出如下三方面的政策建议。

1、**进一步推动制定开放银行的数据保护标准，充分发挥标准的规范引领作用。**开放银行的参与主体多样、应用场景丰富。我们从本报告可以看到，大部分商业银行在开放银行的数据保护方面制定了行内数据安全管理制度，采取了必要、先进的技术手段。但是在整个生态层面还没有相对统一和细化的数据安全处理标准，开放银行各参与方对数据安全的合规意识不尽相同、对金融敏感数据的保护能力存在一定差异，阻碍了开放银行的规模化发展。因此，建议监管机构加快制定监管前哨功能相关技术标准，引导和鼓励开放银行参与方提升数据识别、数据脱敏和数据水印等技术能力的研发和应用，逐步提升各参与方之间数据互联互通的可操作性和安全性；同时，建议监管机构进一步制定开放银行的管理标准，如开放银行的合作准入标准、应用方安全管理规范等，全面保障开放生态的安全。

2、**鼓励监管科技创新，提升开放银行场景安全。随着开放银行实践的不断深入，不同参与方之间交互的频率和复杂度将持续提升，对金融监管的实时性、精准性、全面性提出了更高的要求。**因此，建议监管机构鼓励监管科技核心领域的技术攻关和应用，探索应用方 API 异常使用行为事先/事中监控的技术手段，利用人工智能、大数据、区块链等信息技术，建立开放银行数字监管平台，提升事前、事中和事后全链条的监管和风控能力。通过数字化新型监管模式，切实保障开放银行的 API 安全、数据安全和业务场景安全。

3、**建立开放银行的安全检测认证及规范的执行流程。**在行业标准的基础上，建议监管机构加快推动开放银行安全检测工作，包括服务接口安全测评、数据安全防护测评等，对达到检测标准的机构给予相应认证，并对其组织定期评估和巡检，逐步形成开放银行领域规范化的安全检测体系。

[14]中国银联技术管理委员会开放银行工作组：《开放银行数据保护与合规研究报告》第九章

五、附录

本报告涉及的主要法律法规及行业标准包括：

(1) 《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》，2022 年 12 月 2 日发布；

(2) 《个人信息保护认证实施规则》，2022 年 11 月 4 日发布；

(3) 《个人信息出境标准合同办法》，2023 年 2 月 22 日日发布；

(4) 《数据出境安全评估办法》，2022 年 7 月 7 日发布；

(5) 《网络安全审查办法（2021）》，2021 年 12 月 28 日发布；

(6) 《银行保险机构消费者权益保护管理办法》，2022 年 12 月 26 日发布；

(7) 《网络安全标准实践指南—个人信息跨境处理活动安全认证规范》，2022 年 6 月 24 日发布；

(8) 《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》，2022 年 12 月 16 日发布；

(9) 《关于加强信用信息共享应用推进融资信用服务平台网络建设的通知》，2022 年 4 月 7 日发布；

(10) 《金融数据安全 数据安全评估规范（征求意见稿）》，2021 年 12 月 3 日发布；

(11) 《网络数据安全管理条例（征求意见稿）》，2021 年 11 月 14 日发布。