国金测评 National Fintech Evaluation Center | DataFun.

金融科技测评
助力金融数据安全共享

罗丰 隐私计算实验室负责人

2022.7.9

目录 CONTENT

国金测评 National Fintech Evaluation Center | DataFun.

01

基本背景

数据成为生产要素

中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见

2020-04-09 19:00 来源：新华社 【字体：大 中 小】 打印

新华社北京4月9日电

中共中央 国务院

关于构建更加完善的要素市场化配置体制机制的意见

（2020年3月30日）

完善要素市场化配置是建设统一开放、竞争有序市场体系的内在要求，是坚持和完善社会主义基本经济制度、加快完善社会主义市场经济体制的重要内容。为深化要素市场化配置改革，促进要素自主有序流动，提高要素配置效率，进一步激发全社

1. 数据可信
2. 数据确权
3. 数据保护
4. 数据交换
5. 价值分配

数据安全不可忽视

中国2017年6月生效的《中华人民共和国网络安全法》

“网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度；网络运营者.....应当遵循合法、正当、必要的原则.....经被收集者同意.....应当依照法律.....的个人信息；网络运营者不得泄露、篡改、毁损其收集的个人信息处理其保存；未经被收集者同意，不得向他人提供个人信息.....确保其收集的个人信息安全，防止信息泄露、毁损、丢失.....”

中国2021年9月生效的《中华人民共和国数据安全法》

“鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展.....坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展.....鼓励数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品、产业体系。”

中国2021年11月生效的《中华人民共和国个人信息保护法》

“个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全.....不得超出约定的处理目的、处理方式等处理个人信息.....未经个人信息处理者同意，受托人不得转委托他人处理个人信息

- 坚持谁授权谁负责
- 谁采集谁负责
- 谁使用负责
- 谁保管谁负责的原则。

行业配套政策逐步完善

ADD RELATED TITLE WORDS

顶层设计 01

《金融科技发展规划(2022-2025年)》

- 加强数据能力建设
- 保障数据安全与个人隐私
- 有序推动数据共享与综合应用
- 健全适应数字经济发展的现代金融体系
- 助力数字经济高质量发展

规范指引 02

《金融业数据能力建设指引》

- 数据战略、数据治理
- 数据架构、数据规范
- 数据保护、数据质量
- 数据应用、数据生存周期管理

指导意见 03

《关于银行业保险业数字化转型的指导意见》

- 完善数据治理体系
- 加强数据安全和隐私保护
- 提高数据应用能力

02

金融数据安全共享关键技术

关键技术路线概述

隐私计算是目前实现数据安全共享的主流技术路径：

根据行业内调研结果，行业基本认同多方安全计算、联邦学习、可信执行环境和区块链辅助下的隐私计算工具是目前隐私计算产业形成的3+1技术发展方向。

多方安全计算	联邦学习	可信执行环境
• 同态加密 • 混淆电路 • 秘密分享 • 不经意传输	• 横向联邦学习 • 纵向联邦学习 • 联邦迁移学习	• 独立、可信、安全的硬件环境 • 安全性要求较高的场景

区块链（辅助隐私计算）

区块链与隐私计算互为补充、相辅相成，基于区块链分布式、可溯源、不可篡改、共识机制等特点，助力构建了分布式多方协作的信任机制，帮助实现数据确权、数据流通防篡改等。

区块链，提升数据共享安全

隐私计算

- 对参与者要求高，要求参与者之间需相互信任、协作
- 对数据质量和参与者的高要求，一直是隐私计算的痛点。

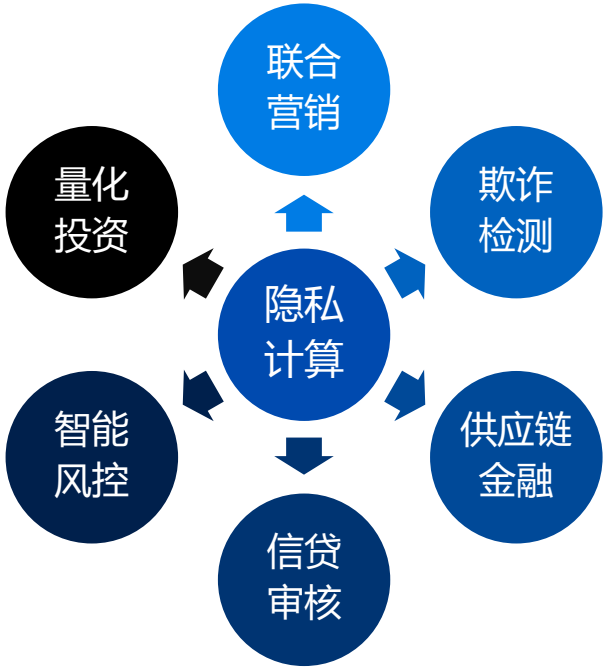
区块链

- 可溯源、难篡改、公开透明
- 构建信任协作的网络
- 区块链可解决参与者信任问题

区块链与隐私计算融合应用

- 数据溯源、数据确权、校验数字授权真实性
- 提升整个隐私计算过程的检测能力
- 提高违法成本，实现安全可信的数据共享

隐私计算技术金融应用场景



国金测评 National Fintech Evaluation Center | DataFun.

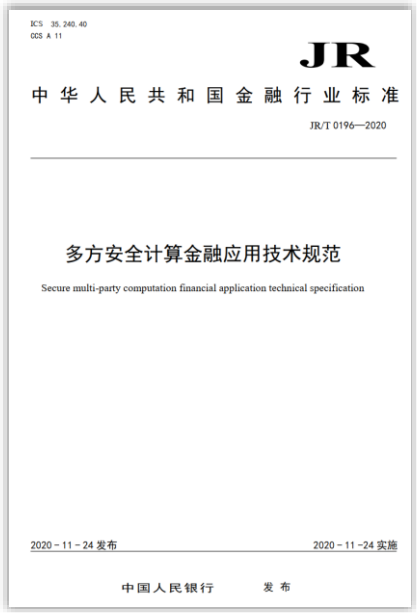
03

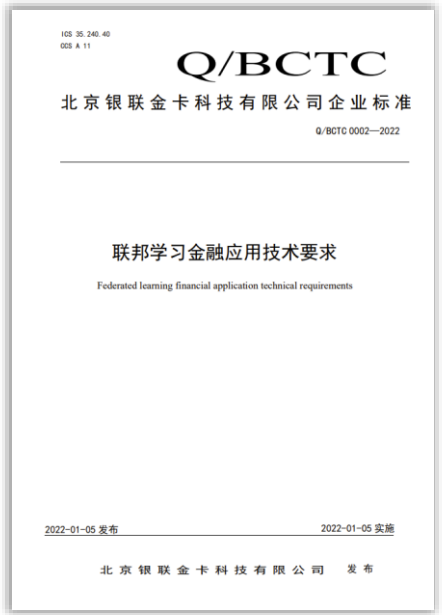
金融科技测评探索与实践

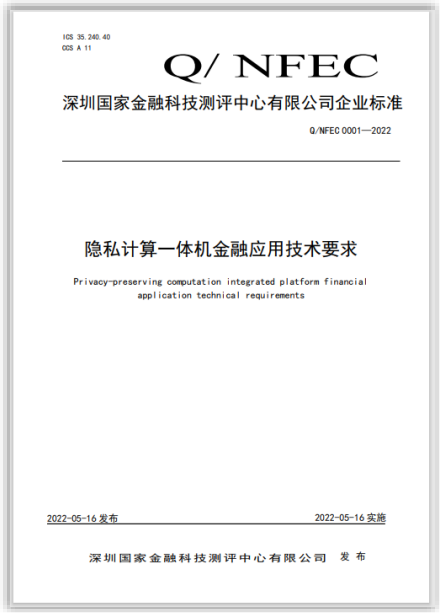
金融技术标准逐步健全

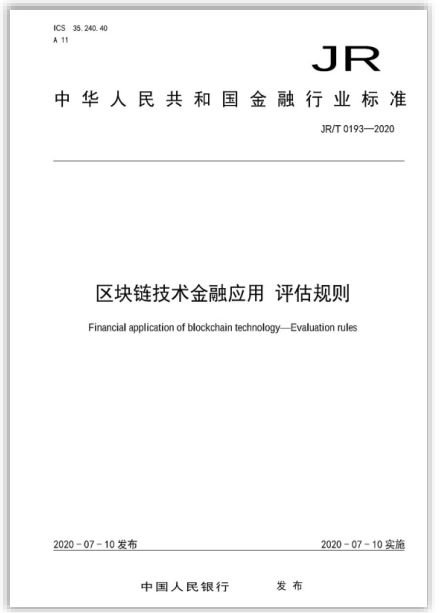
序号	标准类型	标准名称	标准状态
1	金融行业标准	**JR/T 0171-2020 个人金融信息保护技术规范**	已发布
2	金融行业标准	**JR/T 0184-2020 金融分布式账本技术安全规范**	已发布
3	金融行业标准	**JR/T 0193-2020 区块链技术金融应用 评估规则**	已发布
4	金融行业标准	**JR/T 0196-2020 多方安全计算金融应用技术规范**	已发布
5	金融行业标准	JR/T 0197-2020 金融数据安全 数据安全分级指南	已发布
6	金融行业标准	JR/T 0202-2020 基于大数据的支付风险智能防控技术规范	已发布
7	金融行业标准	JR/T 0218-2021 金融业数据能力建设指引	已发布
8	金融行业标准	JR/T 0221-2021 人工智能算法金融应用评价规范	已发布
9	金融行业标准	JR/T 0223-2021 金融数据安全 数据生命周期安全规范	已发布
10	金融行业标准	金融数据安全 数据安全评估规范	编制中

隐私计算及区块链测评依据





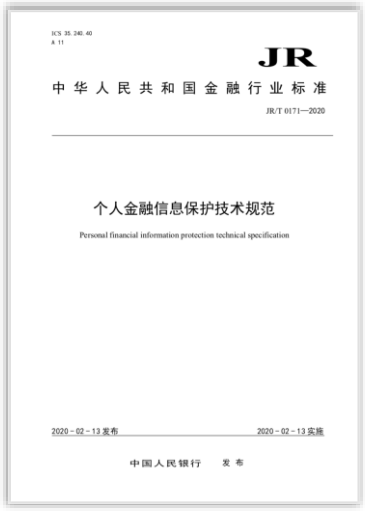


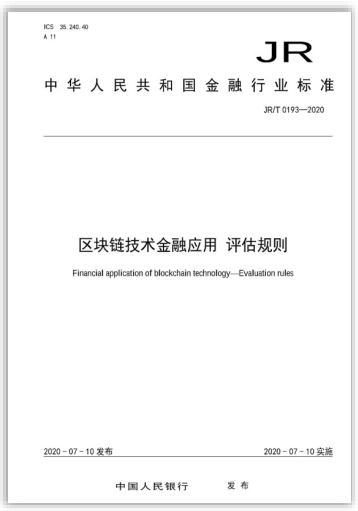


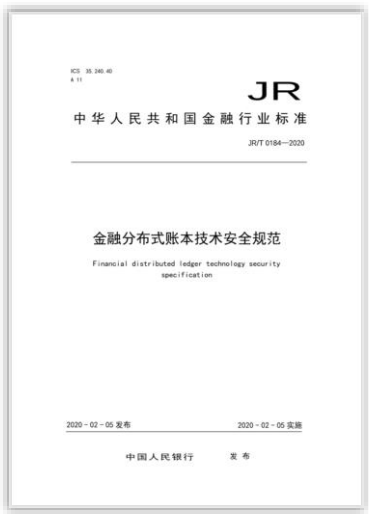
国金测评 National Fintech Evaluation Center | DataFun.

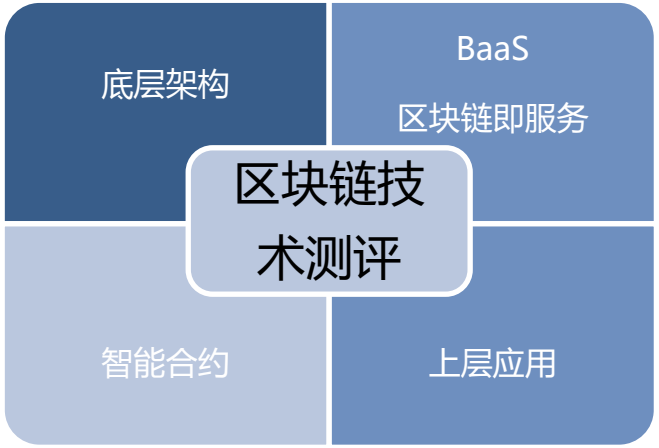
区块链-测评依据及对象

2020年7月，《中国人民银行关于发布金融行业标准推动区块链技术规范应用的通知》：发布**《区块链技术金融应用评估规则》**，金融机构结合实际认真落实《规则》，建立健全区块链技术应用风险防控机制，**定期开展外部安全评估**，推动区块链技术在金融领域的规范应用









测评对象

国金测评 National Fintech Evaluation Center | DataFun.

区块链-评估规范框架

基本要求评估	
账本技术	共识协议
智能合约	节点通信
事件分发	密钥管理
状态管理	成员管理
交易系统	接口管理

安全评估	
基础硬件	基础软件
密码算法	节点通信
账本数据	共识协议
智能合约	身份管理
隐私保护	监管支撑
安全运维	安全治理

性能评估
交易吞吐率
查询吞吐率
交易同步性能
部署效率
账本数据增长速率

区块链-技术产品测评能力及经验

金融科技公司	区块链产品
腾讯云计算（北京）有限责任公司	腾讯云区块链TBaaS平台
深圳壹账通智能科技有限公司	加马区块链开放平台
北京百度网讯科技有限公司	百度超级链 BaaS 平台
前海联合交易中心	前海仓单平台
蚂蚁金服（杭州）网络技术有限公司	蚂蚁链BaaS平台
杭州趣链科技有限公司	区块链底层平台 Hyperchain

测评案例

MPC-测评依据

1 标准预研阶段

2019年2-4月：收集现状和需求，**确定标准修订方案**

2 标准立项

2019年5月：专家评审，标准初稿通过

3 征求意见阶段

2019年6月：进一步完善，形成征求意见稿。

4 送审阶段

2020年9月：集中讨论，意见处理，报送金标委。

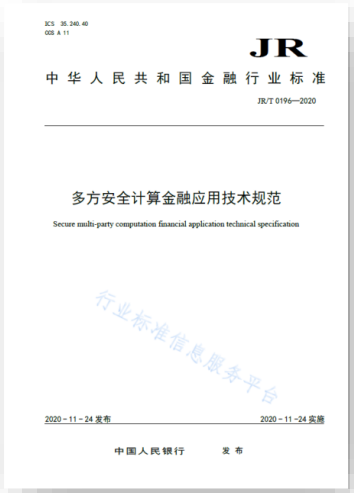
5 正式发布

2020年11月：**标准正式发布。**

《规范》规定了多方安全计算技术金融应用的基础要求、安全要求、性能要求等，适用于金融机构开展相关产品设计、软件开发、技术应用等。《规范》的发布有助于实现在不泄露原始数据、保障信息安全前提下推动多个主体间的数据共享与融合应用，确保数据专事专用、最小够用，杜绝数据被误用、滥用。

国金测评 National Fintech Evaluation Center | DataFun.

MPC-标准框架


ICS 35.240.40
CCS A 11

JR

中华人民共和国金融行业标准

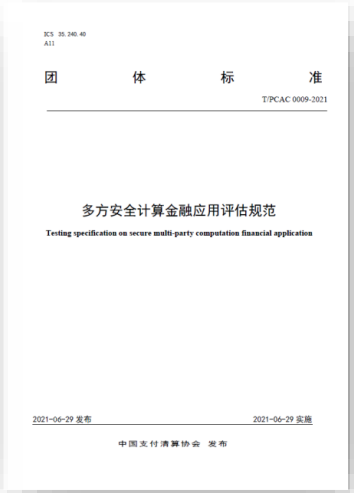
JR/T 0196—2020

多方安全计算金融应用技术规范

Secure multi-party computation financial application technical specification

2020-11-24 发布　　2020-11-24 实施

中国人民银行　发布


ICS 35.240.40
A11

团　体　标　准

T/PCAC 0009-2021

多方安全计算金融应用评估规范

Testing specification on secure multi-party computation financial application

2021-06-29 发布　　2021-06-29 实施

中国支付清算协会　发布

技术评估	M项22项 | O项14项 | C项11项
安全评估	M项23项 | O项8项 | C项8项
性能评估	M项0项 | O项4项 | C项5项

术语、定义和缩略语

概述

参与方及工作时序　应用目标　总体要求

基础要求

数据输入　算法输入　协同计算

结果输出　调度管理

安全要求

协议安全　隐私数据安全　认证授权

密码安全　通信安全　存证与日志

性能要求

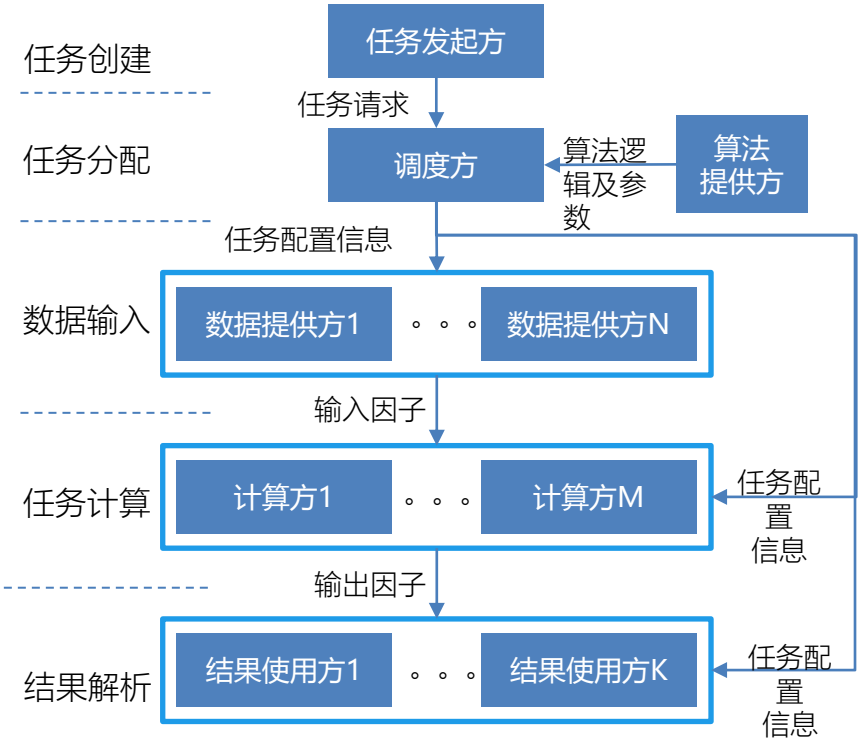
计算延迟　吞吐量　计算精度

M：必须评估项目

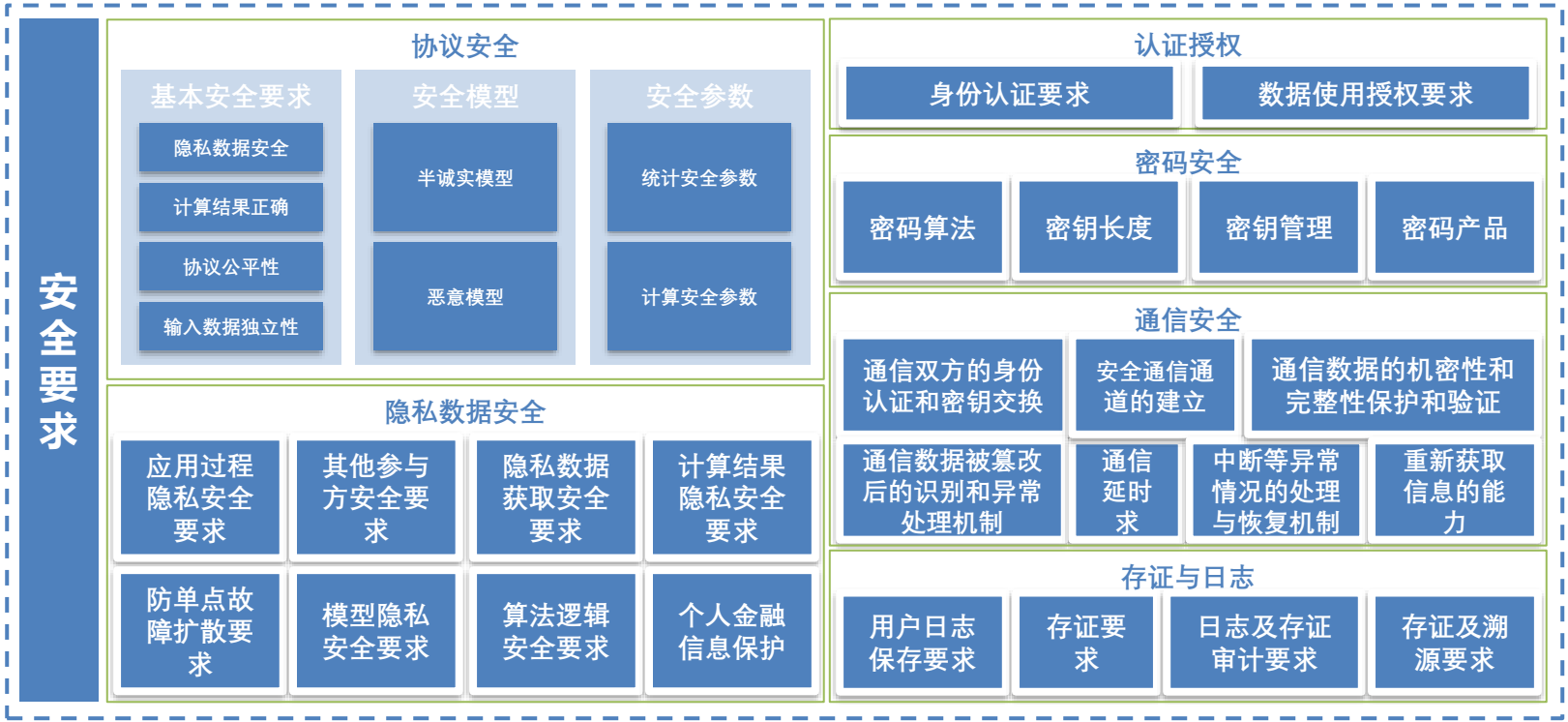
C：条件可选评估项目

O：可选评估项目

MPC-参与方和工作时序



MPC-安全要求



MPC-性能要求

性能要求

资金场景		时延	TPS	精度
实时	整数万次乘法	≤100	≥100	≥22
	整数万次比较	≤200	≥10	--
非实时	浮点数万次乘法	≤1000	≥500	≥32
	浮点数万次比较	≤10000	≥100	--

非资金场景		时延	TPS	精度
实时	浮点数万次乘法	≤200	≥100	≥26
	浮点数万次比较	≤300	≥10	--
非实时	浮点数万次乘法	≤1000	≥500	≥32
	浮点数万次比较	≤10000	≥500	--

MPC-测评经验及实践

完成两批，目前已完成超18款多方安全计算产品的测评工作，并为企业颁发测评证书。

金融科技公司	测评产品
华控清交信息科技（北京）有限公司	清交PrivPy多方计算平台
矩阵元技术（深圳）有限公司	矩阵元隐私计算服务系统
蚂蚁区块链科技（上海）有限公司	蚂蚁链摩斯安全计算平台（MORSE）
蚂蚁智信（杭州）信息技术有限公司	蚂蚁多方安全计算平台
深圳前海微众银行股份有限公司	FATA企业版联邦数据网络平台
上海富数科技有限公司	富数阿凡达阿安全计算平台软件

第一批

金融科技公司	测评产品
北京瑞莱智慧科技有限公司	RealSecure-MPC多方安全计算平台
北京数牍科技有限公司	Tusita隐私计算平台
第四范式（北京）有限公司	云知隐私计算平台
华为云计算技术有限公司	华为云可信智能计算服务-可信计算节点
蓝象智联（杭州）科技有限公司	GAIA金融级隐私计算平台
上海光之树科技有限公司	光之树隐私计算平台
深圳前海环融联易	联易融蜂蜜隐私计算平台
深圳市洞见智慧科技有限公司	洞见数智联邦平台（INSIGHTONE）
深圳致星科技有限公司	星云隐私计算平台
淘宝（中国）软件有限公司	DataTrust阿里云隐私增强计算软件
天翼数智科技（北京）有限公司	PrivTorrent密流安全计算平台
亚信科技（成都）有限公司	亚信安全隐私计算平台

第二批

联邦学习-测评依据

2021年2月
北京金融科技产业联盟立项

2021年7月
形成标准草案

2021年9月7日
第一次金标委专家·审议

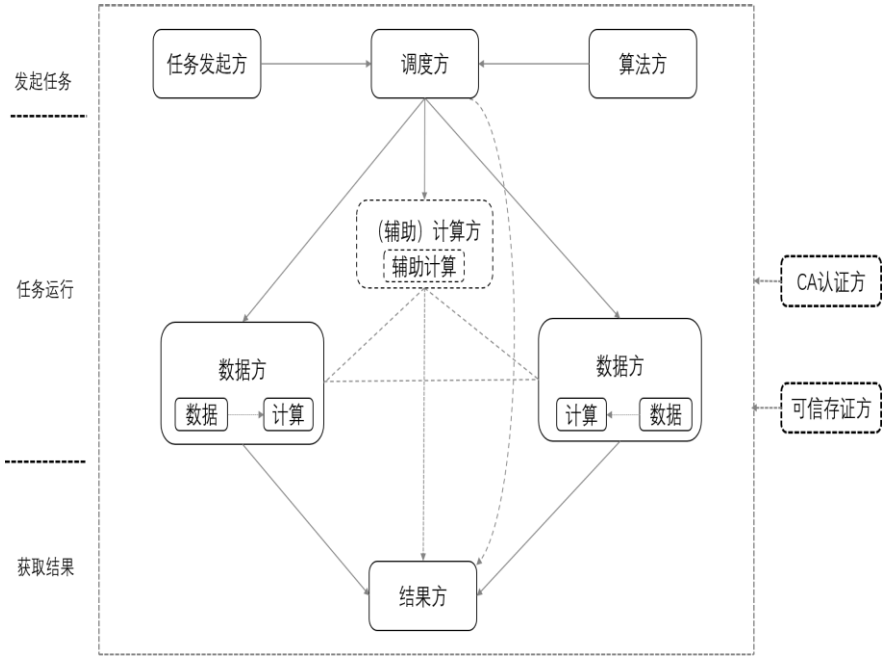
2022年1月4日
第二次金标委专家·审议

目前
征求意见稿阶段

建立企业标准
使用企业标准对联邦学习产品完成评测

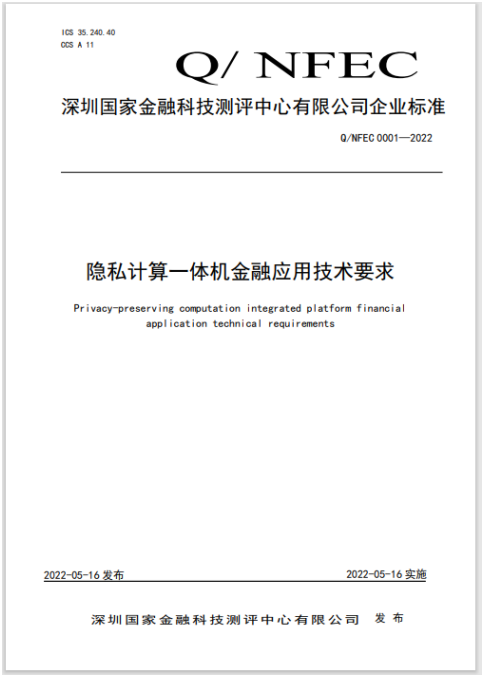
国金测评 National Fintech Evaluation Center | DataFun.

联邦学习-标准框架



术语、定义和缩略语		
概述		
参与方	工作时序	
基础要求		
数据输入	算法输入	调度管理
安全要求		
数据安全与隐私	横向联邦学习安全	通信安全
纵向联邦学习安全	联邦迁移学习安全	安全审计
参与方可信性	认证授权	密码安全
性能要求		
准确率	效率	

隐私计算一体机-企标发布



ICS 35.240.40
CCS A 11

Q/ NFEC

深圳国家金融科技测评中心有限公司企业标准

Q/NFEC 0001—2022

隐私计算一体机金融应用技术要求

Privacy-preserving computation integrated platform financial application technical requirements

2022-05-16 发布　　2022-05-16 实施

深圳国家金融科技测评中心有限公司　发布

Q/NFEC 0001-2022
《隐私计算一体机金融应用技术要求》

国金测评 National Fintech Evaluation Center | DataFun.

隐私计算一体机-价值及逻辑架构

图1：隐私计算一体机逻辑架构图

隐私计算一体机-企业标准框架

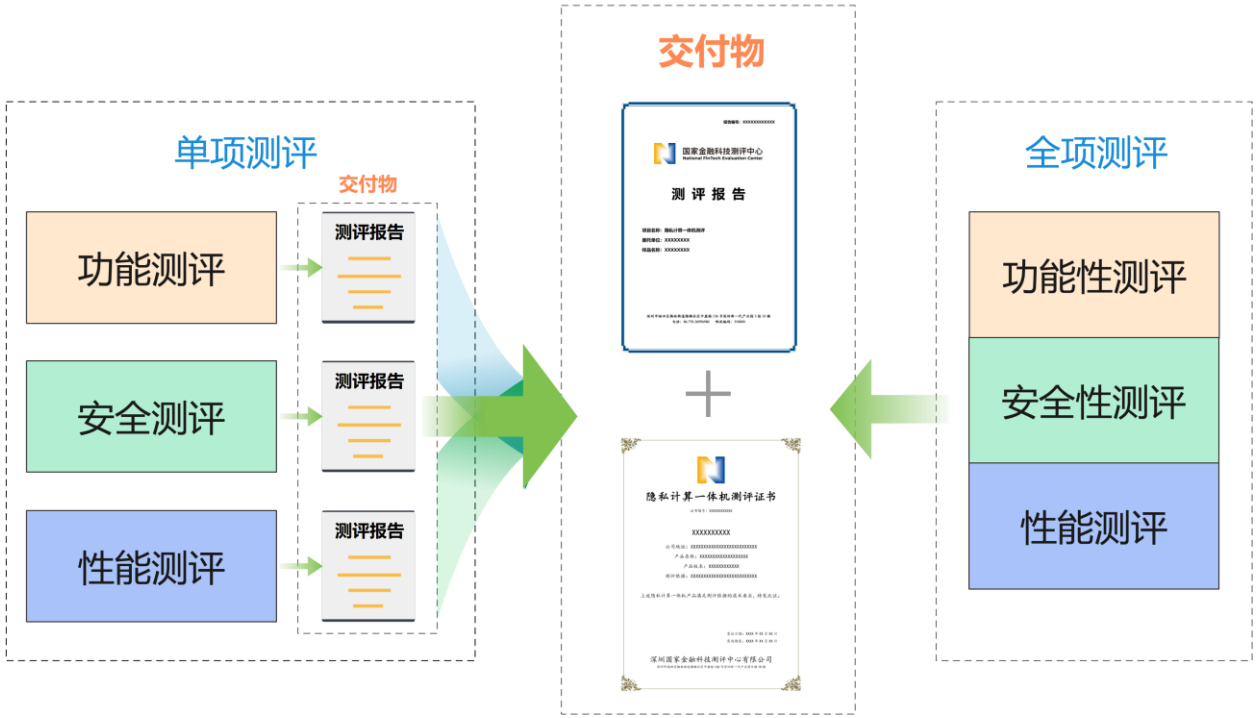
功能测评项

安全测评项

性能测评项

硬件要求	运行环境要求	通用功能要求	隐私计算要求	性能要求
加密存储设备	容器安全	人机交互	隐私计算安全管理	隐私计算效率
可信平台模块		访问控制	隐私计算节点管理	
可信密码模块		日志及审计	隐私计算算法管理	
可信执行环境	操作系统安全	通信安全	隐私计算任务管理	隐私计算精准性
加速硬件		身份验证	隐私计算数据管理	
加密模块		容器镜像安全		
		固件及应用更新安全		
		防拆机制		

隐私计算一体机-测评服务



金融科技产品认证名录

《金融科技产品认证目录（第一批）》

2019年10月

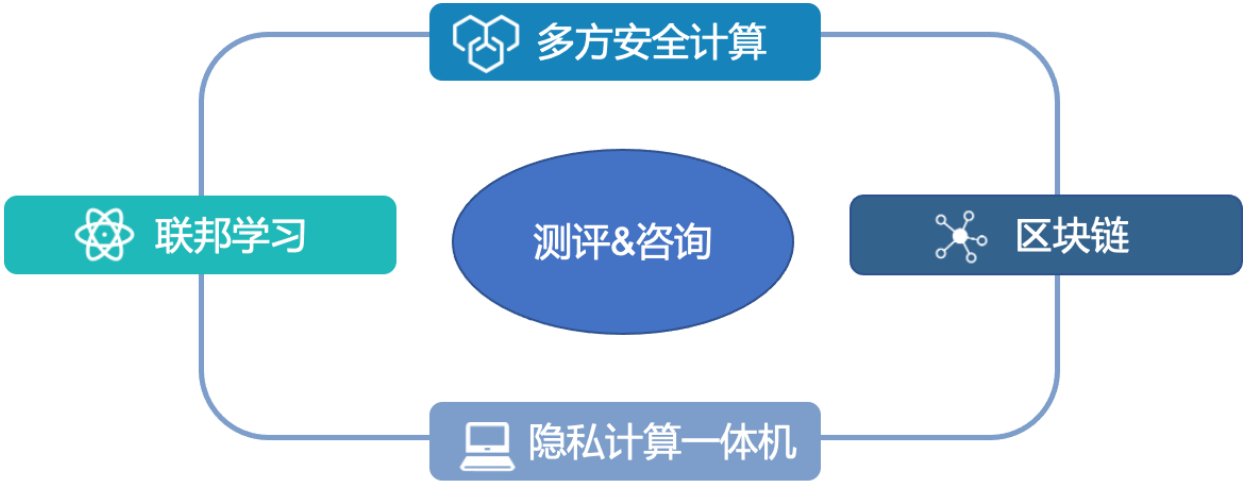
序号	产品类型
1	客户端软件
2	安全芯片
3	安全载体
4	嵌入式应用软件
5	ATM终端
6	支付销售点（POS)终端
7	移动终端可执行环境（TEE)
8	可信应用程序
9	条码支付受理终端
10	声纹识别系统
11	云计算平台

《金融科技产品认证目录（第二批）》

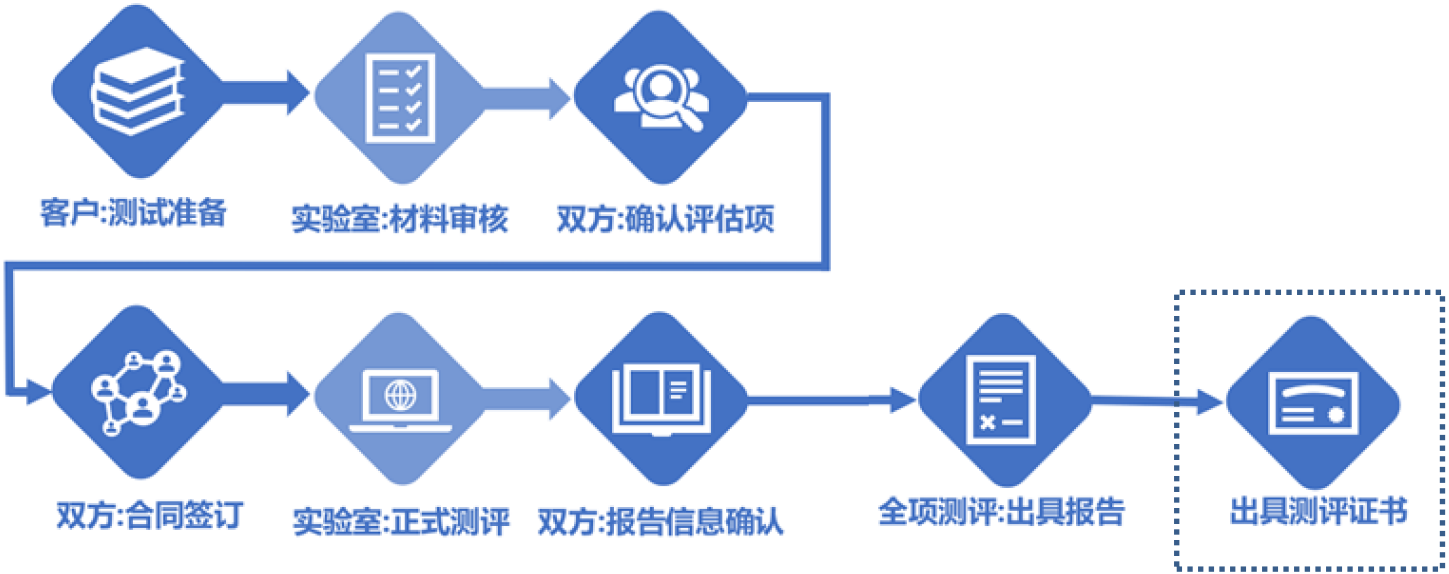
2022年2月

序号	产品类型
12	区块链技术产品
13	多方安全计算金融应用
14	商业银行应用程序接口

隐私计算测评领域及实践



常规测评流程



充分释放数据要素潜能
金融科技测评保驾护航

非常感谢您的观看

国金测评 National Fintech Evaluation Center | DataFun.

市场合作部-吴祖顺