# 安全核对的业务背景

金融行业的数据使用要求发生了一些变化：

限制：一些使用数据的方式被法规禁止

改进：通过隐私计算手段如果满足可用不可见，那数据依然可以流转，产生价值

政策推动了隐私计算平台和信贷公司的合作

让C端客户方便得到贷款，但是厂家之间的跨域交互容易出现差异

问题：审批流程长、数据容易泄露（未经允许的查看和缓存）

# 产品方案：试点到规模化

## 产品方案

解决方案：风洞隐私安全核对

SecretFlow SCQL的数据对比应用

选择SCQL的原因：PSI适用范围有限，不只是查看是否相等，还要看不相等的地方，

SCQL比较灵活，在上面又封装了一个产品层

产品效果：

1. 多方核对相等时可以直接输出结果
2. 如果不相等，有一套问题排查的方案，可以提出一份报告

产品方案：

展示层:

核对数据大屏：聚合展示、告警提示、筛选下钻

核心业务：

数据授权 -> 核对任务 -> 结果排查

更多参与方管理：

核对机构管理：合作邀约、节点交付、网络授权

和点对点隐私计算产品的区别：

一家机构完成数据授权、核对调试、发布的流程后，可以进行批量（灰度）发布

## 特色功能

1、规模化核对：核对规则编写

SQL内容：检测两边余额是否相等

2、规模化排查：

有一些排查模板对用户进行引导

3、推广

单家机构配置核对，然后进行灰度发布

核对结果可能出问题，需要进行管理并且到现场排查

# 技术共建：和sf共成长

## SCQL封装方式

有两种方式：

用于安全核对的产品方案（极简产品体验）

逻辑固定、批量发布

联合策略的安全方案（风控规则复杂）

风控策略一行一策

## 安全自证

客户想要厂家证明软件的安全

代码扫描、权威认证难以直接关联产品页面

方案：输出数据处理的明细日志

这个方案的问题：

1、安全，日志泄露会导致攻击

2、性能，打印影响性能，需要调试时再打开

sf推出的可视化算法：

<https://www.secretflow.org.cn/zh-CN/experience-zone/welcome?tab=psi>

<https://www.secretflow.org.cn/zh-CN/experience-zone/psi>

这里给出了详细的psi加密计算过程

安全自证的三个阶段：

1. 可审查，进出密态的过程的日志可见、工程实现和算法原理一致
2. 可视化，进出密态的过程的日志可视化，并且支持日志的分析。降低隐私计算解释成本
3. 可攻防，通过攻防验证

目前工业数据日志的可视化没有高效的工具

## 未来工作

1. 低门槛：

方法：黑屏（命令行） -> 白屏（配置化页面）

介质：强要求服务器 -> pc

1. 高性能：面向技术水平高的机构。

数据连接：从文件CSV -> 数据库ODPS

计算上：单机 -> 分布式

1. 易用性：

规则编写：编码 -> 可视化组件

异常排查：表格 -> 图形

1. 实时性：

数据：静态表 -> 流式数据（需要对接流式数据的存储和计算引擎）

任务：日调度 -> 分钟级