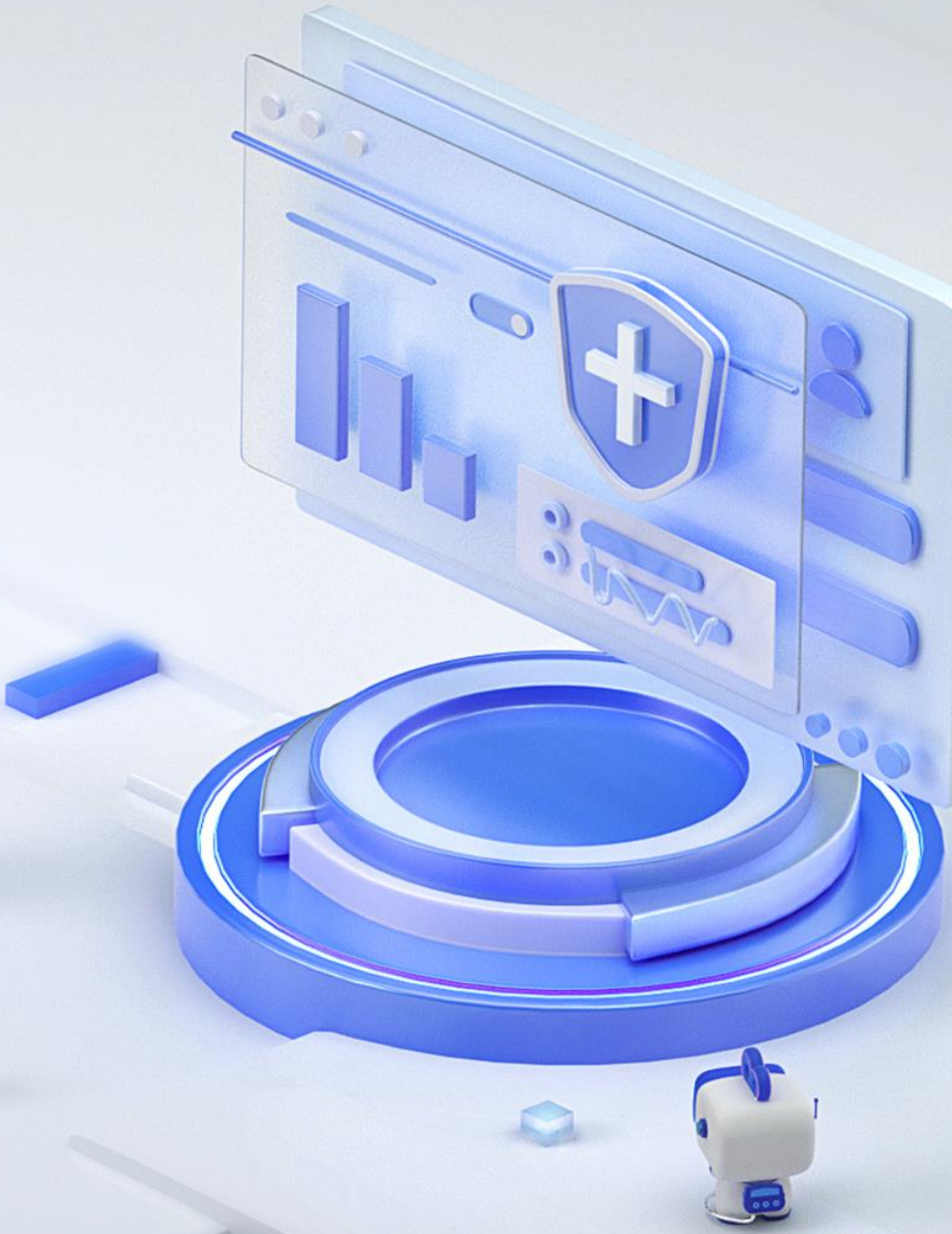
快手安全
KUAISHOU SECURITY

快手安全手护者沙龙

快手对用户隐私数据保护的技术探索和实践

张伟利 | 2022.03.05



行业变化

2021年开始，特别从7月滴滴上市以来，
各种互联网政策密集发布，其中影响比较大的有
而且政策的实施也是越来越严格

《中华人民共和国个人信息保护法》

《网络安全审查办法》

5月脉脉被下架

8月微信被禁止注册

12.9号豆瓣、唱吧等106款App被下架

11.24号腾讯100+APP被禁止更新

7月滴滴被下架

22年2月18日工信部通报百度定位等
120款APP或SDK违规问题

应对之策

监管环境的趋严

当前监管及舆情趋严，工信部对于同一企业反复出现的问题将直接下架APP，网信办目前发现问题直接通报，预留给企业内部整改时间越来越少。

行动目标

01 符合国家相关法律法规要求

02 对快手内部用户隐私数据采集、流转情况做到心里有数。

03 统一管理快手内部用户隐私数据，探索和挖掘用户数据的新内容

这就需要有一套对快手用户隐私数据采集、加工、存储、消费和销毁全流程的可监控和可管控的技术能力

下面我将从可控采集、保密传输、加密存储、授权消费来分别谈谈快手对用户隐私数据保护的技术探索和实践

CONTENTS

01 可控采集

02 保密传输

03 加密存储

04 授权消费

可控采集

管控手段

01 通过建立“敏感信息访问控制” 对业务获取敏感信息进行控制。

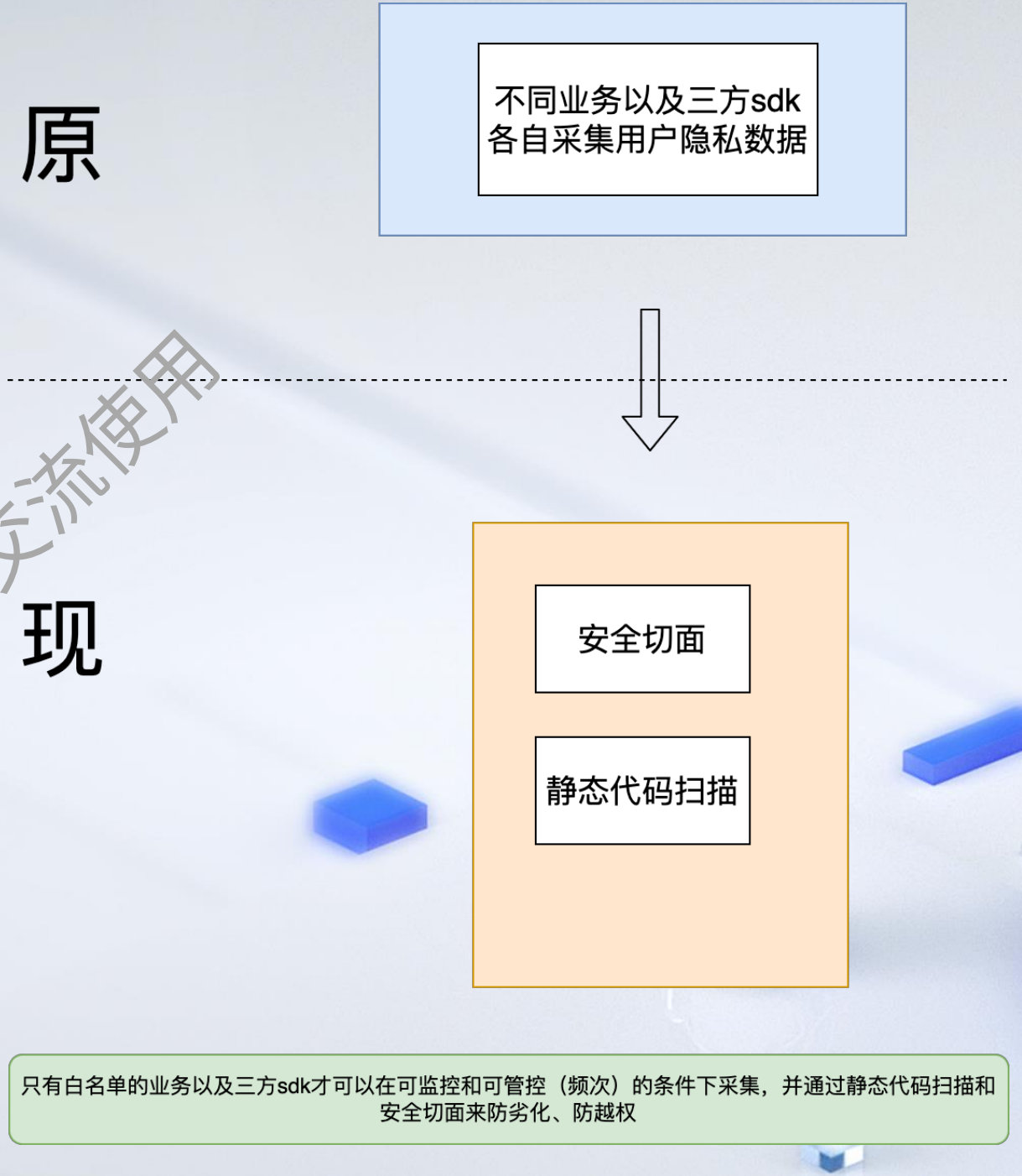
02 将原有业务对敏感信息的直接（或简单封装）获取调整为需要通过权限系统进行获取。

业务整改

01 需要有技术方案对当前 App 健康度进行评估

02 对客户端系统API进行梳理，列出可能获取到用户隐私数据的API

03 针对上述API列表，可通过静态代码扫描、动态安全切面等方式进行分析，排查是否有越权或劣化行为。



安全切面

什么是移动端安全切面技术?

快手使用安全切面技术主要是建立一个**符合隐私要求**的沙箱隔离环境，**切断三方sdk**以及客户端对用户隐私数据**不合理**的采集请求。

应用场景：某些业务使用xx定位sdk，而xx定位sdk最近被通报违规使用用户的andriodId，可以通过安全切面技术直接拦截xx定位sdk对用户andriodId的采集和使用，可以直接拒绝或者返回空信息

安全切面

移动端安全切面技术主要用于解决：

01 对APP内部不同代码角色进行更精细化的管控

02 对APP内部代码的行为进行监控和追溯

03 建立一套独立于业务的安全和隐私管控体系

静态代码扫描

什么是静态代码扫描?

在编译流水线上对新增代码执行静态扫描，发现对敏感接口的直接调用可以及时提醒开发人员。

静态代码扫描是防劣化的主要途径，防劣化的需求是对于敏感API，业务不能直接使用。

静态代码扫描

静态代码主要为了避免业务自行使用系统的敏感API

一些敏感API

地理位置　通讯录　剪切板

基建能力

01 增量代码防劣化

02 对存量代码做离线扫描任务

CONTENTS

01 可控采集

02 保密传输

03 加密存储

04 授权消费

保密传输

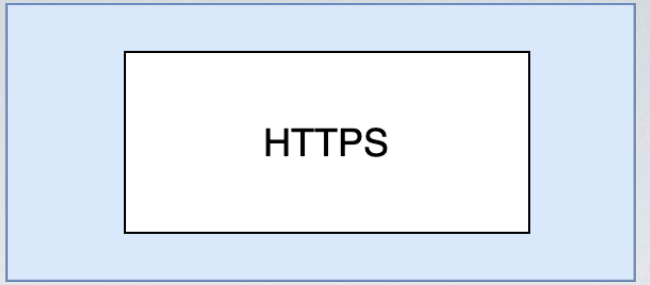
HTTPS

HTTPS协议是由SSL/TLS+HTTP协议构建的可进行加密传输、身份认证的网络协议，要比HTTP协议安全。
HTTPS也存在着“中间人攻击”等安全问题。

端对端加密方案

快手选择在HTTPS的基础上加入端对端加密方案，对用户隐私数据先使用端对端加密方案进行加密，然后再通过HTTPS进行传输。

原



现

由于HTTPS也存在着“中间人攻击”等安全问题，快手选择在HTTPS的基础上加入了端对端加密、安全签名等方案

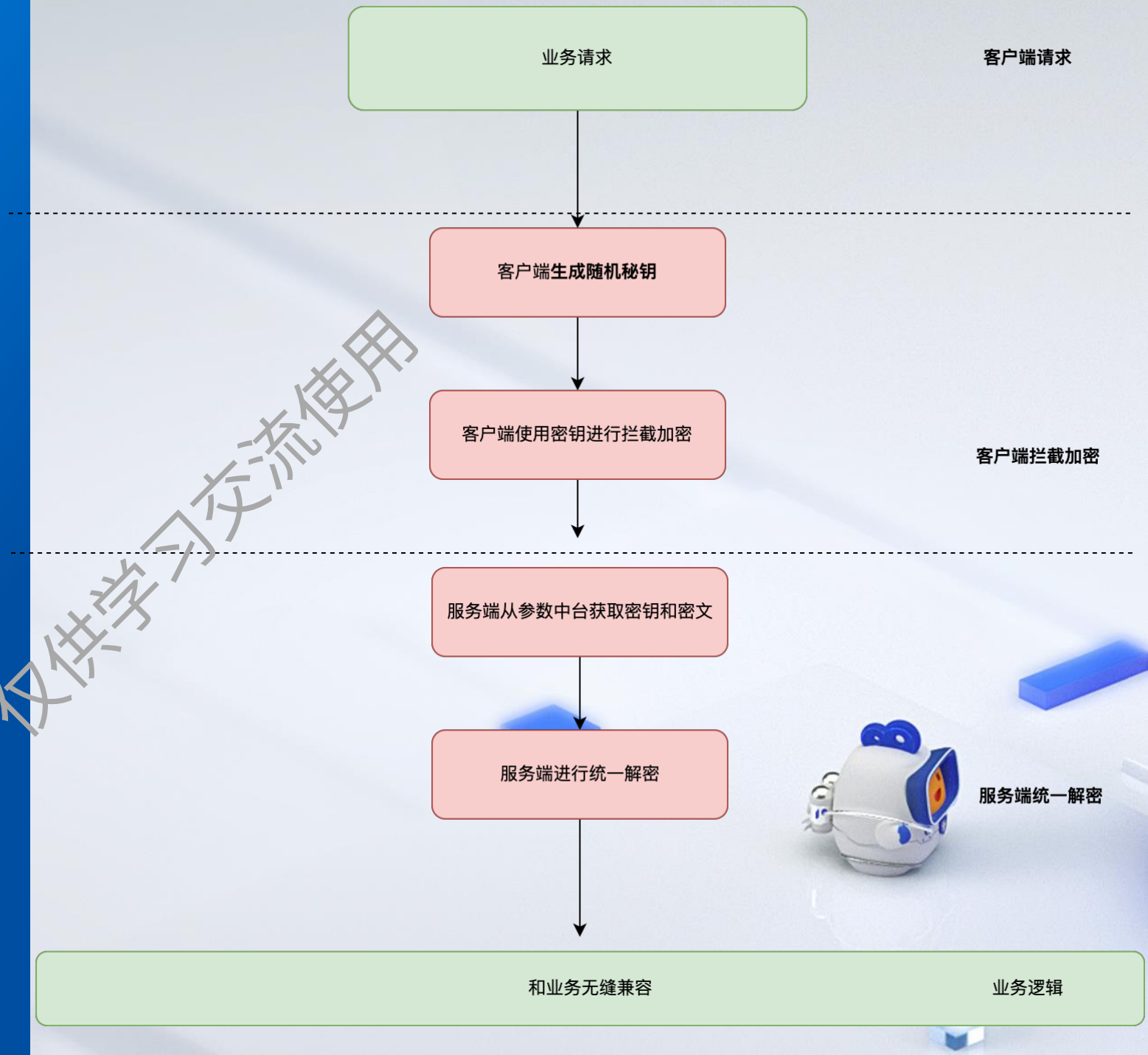
端对端加密方案

客户端

由客户端的统一网关拦截，随机生成秘钥，然后客户端使用秘钥进行拦截加密。

服务端

服务端通过统一的filter做解密，从参数中获取密钥和密文，然后进行统一解密，和业务无缝兼容。



端对端加密方案的落地

端对端加密方案目前已经在**快手主站、电商**等多个部门使用

此安全方案助力电商等部门顺利通过了**相关监管部门**的现场安全检查

CONTENTS

01 可控采集

02 保密传输

03 加密存储

04 授权消费

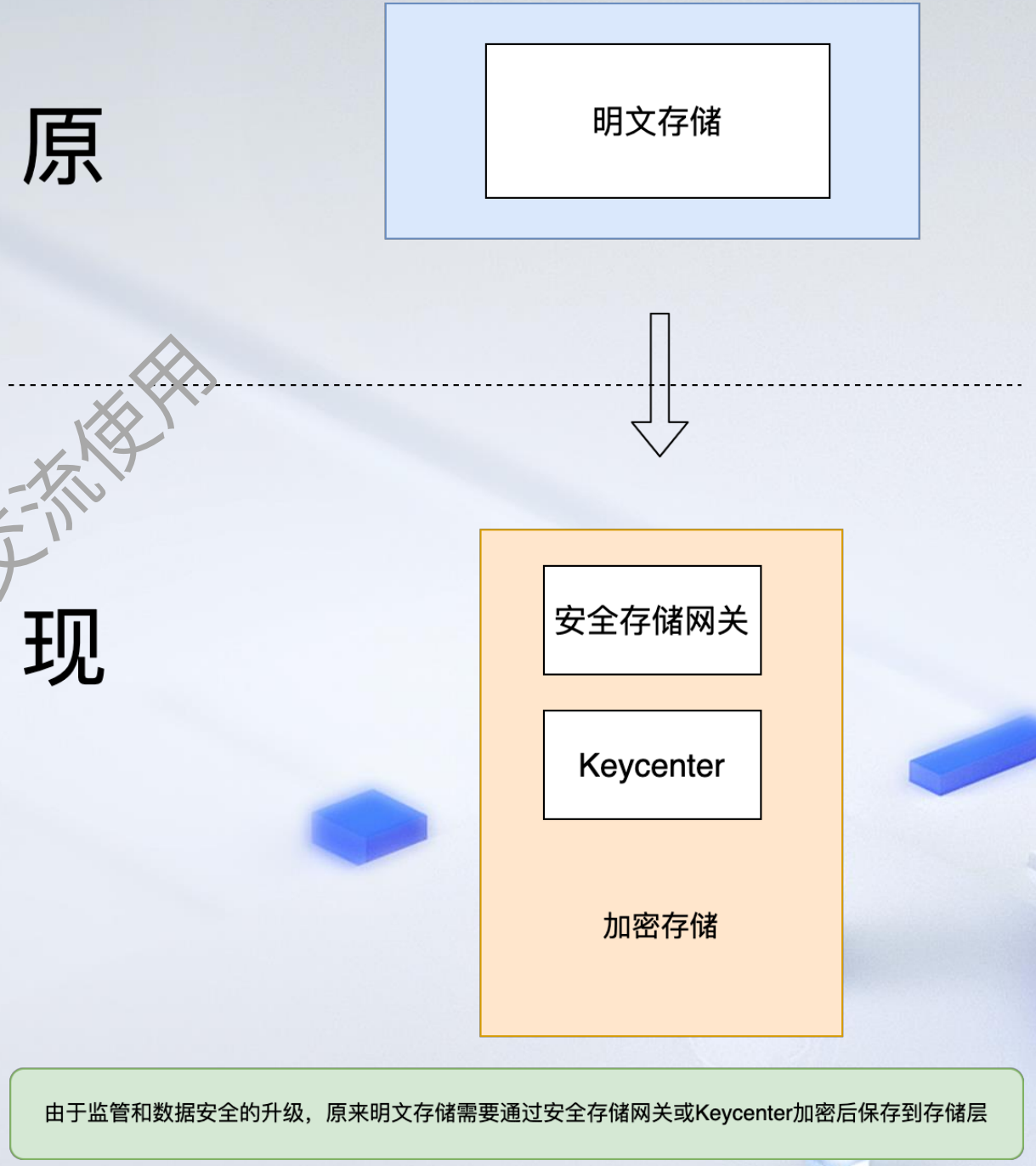
加密存储

监管

监管部门对于用户隐私数据的重视程度不断提升，对于针对用户隐私数据存储等环节的要求也逐渐提高。
需要推动对用户隐私数据如身份证、手机号、银行卡等在内的多个高敏感个人信息字段数据加密存储等。

业务风险

业务中隐私数据如果是明文存储，存在被拖库或内部人员直接复制文件还原解析等数据泄漏风险。
为防止原始数据被窃取后导致敏感数据泄露加密是最典型的防护手段，数据经过加密后即使黑客拿到数据库文件黑客也无法解密。



安全存储网关

为各公司内各业务方提供统一的加密存储支持

凡涉及到用户隐私的敏感数据都应逐步收拢到本服务
并且会依据服务名称和Namespace进行访问控制和底层数据隔离，保证数据的安全性

用户身份证	姓名	照片
支付账单	商家信息	地址

应用

系统对外主要提供三类服务：KV、对象存储、大文件

采用公司专用加密工具Keycenter对保存的数据进行加解密

特点

01

为应用层提供一致的读写接口，屏蔽数据加解密的细节，数据本身在写入时加密，读取时解密。

02

针对不同的业务需求可以选择不同的存储方式

03

秘钥隔离，不同的上层应用分配不同的加密秘钥

04

权限隔离，不同的业务方只能访问自己有权限的数据

安全存储网关 接入情况

接入方

主站、电商、游戏、
增长、商业化、支付等。

KV服务

qps峰值10W+

对象存储

qps峰值1w+

大文件服务

最大支持20G文件上传

采用内部密钥管理系统Keycenter进行密钥托管，使用Keycenter提供的加密工具对保存的数据进行加解密

KeyCenter

快手内部密钥的生成、管理和分发的系统

公司级非常重要底层基建之一

目标是让开发同学对密钥的概念透明，
只专注于开发加解密等功能场景。

对称加密能力

AES-CBC、AES-GCM

国标：SM4

非对称加密能力

RSA：默认的签名是rsawithsha256

国标：SM2 (类椭圆曲线)

ECIES：ECIESwithAES-CBC 和 ECIES功能

MYSQL密码托管

大数据网关：大数据平台托管

其他产品集成加密

配置网关：配置加密

安全存储网关

CONTENTS

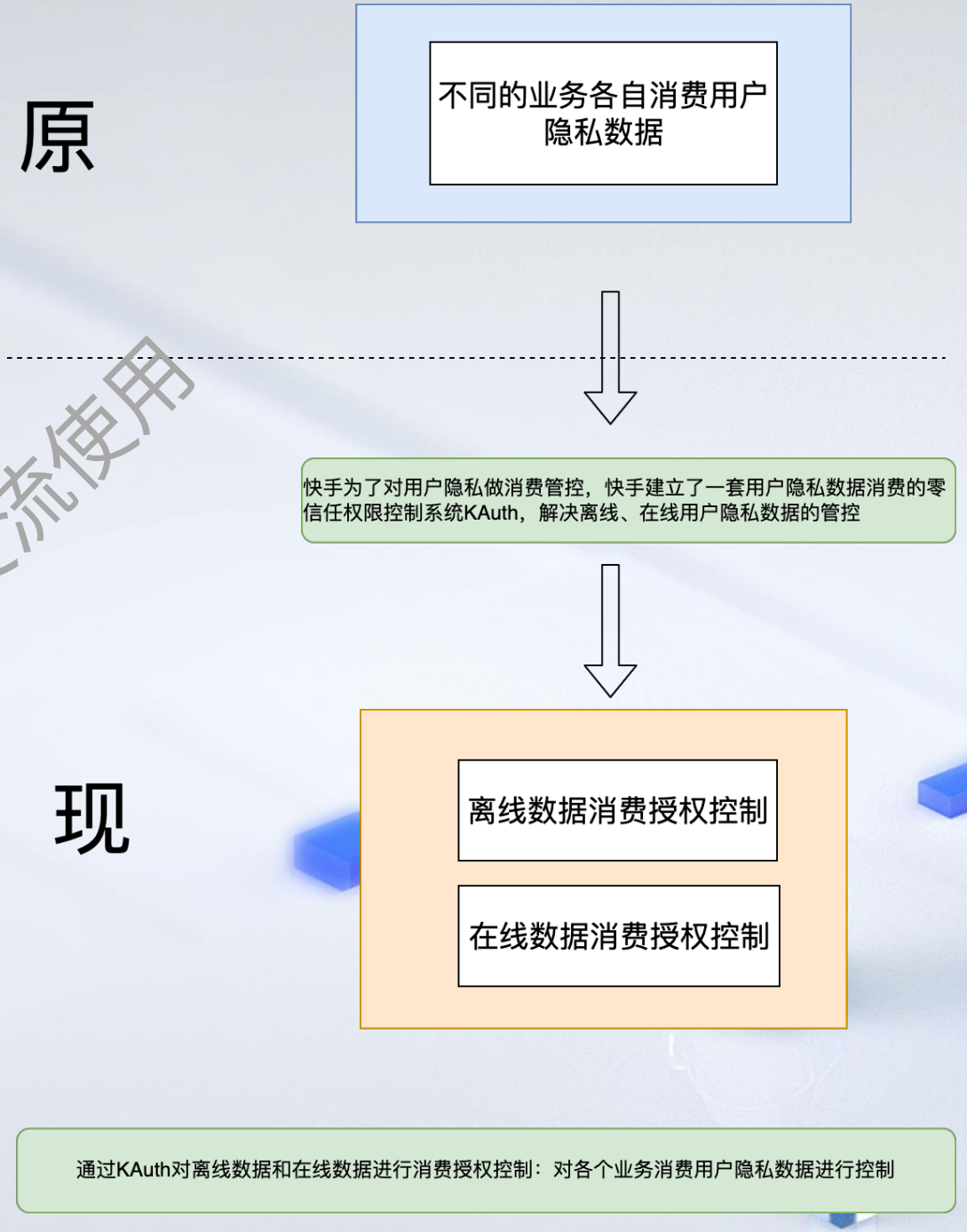
授权消费

消费控制的理念

用户隐私数据无必要不消费

消费控制的原则

中华人民共和国个人信息保护法最小化原则：处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。



KAuth

托管了服务身份认证、服务权限管理、在线访问控制等能力的一站式通用基础工具

支持多种业务/平台场景

服务于快手内 10+ 不同的业务

支付	IM	短信
Push	账号	实名认证

多租户平台，具备开箱即用、资源复用、全流程闭环

日过滤请求：1500 亿+，峰值: 3,300,000+ QPS，

日示警非法调用：1.70亿+，日示警非法主调：300+

KAuth 特性

支持多租户

参数粒度、 规则聚合

支持IM，支付，短信，账号的
多租户场景

高性能

高并发 单服务QPS 3M+

极低耗时 P995 300us

高稳定性

配置更新拉取：
保证一致性，非阻塞

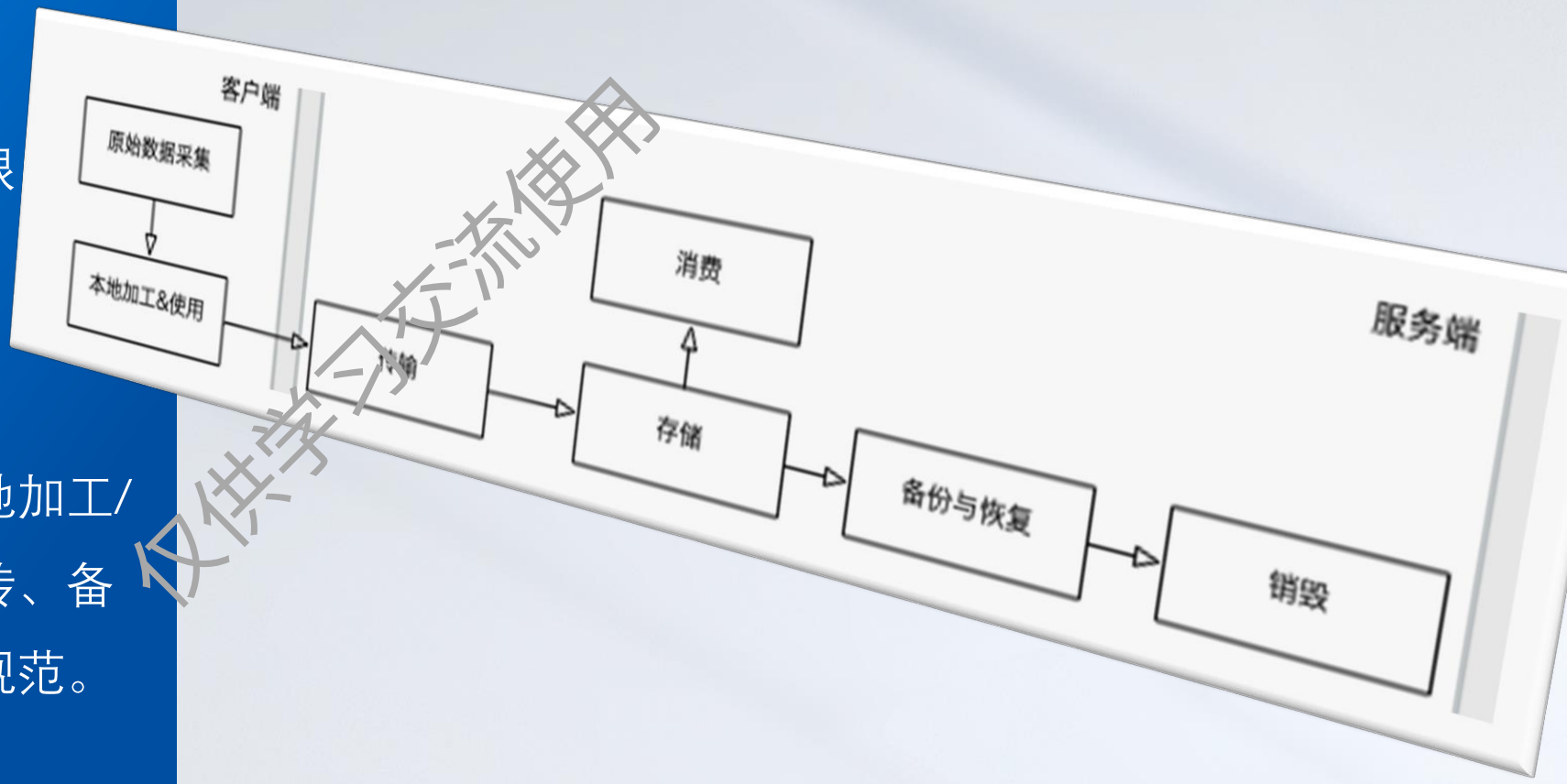
单元覆盖率 > 95%

未来计划

隐私数据全链路保护

采用数据分级机制，
对不同业务授予不同级别的权限

主要是对隐私数据的采集、本地加工/使用、传输、存储、消费、外传、备份与恢复、销毁等环节的进行规范。



硬件加密机

根密钥安全

当密钥存储在软件系统中，攻击者只需找到服务器备份文件的一份拷贝，或者等待或主动发现一个系统漏洞即可得逞。

而采用基于硬件设备的安全数字签名，能够确保现实世界中的安全机制应用到密钥保护上，应用系统通过客户端程序与存储在HSM中的密钥进行通讯，但是密钥绝对不会离开HSM。

引入硬件加密机（HSM）来保证快手Keycenter根密钥安全。

助力快手将来进入金融、支付等安全监管要求更高的行业。

市场驱动力向/业务问题

需要对敏感数据、知识版权、交易和应用进行安全保护

需要实现有效控制以满足合规性

需要最少的部署和集成费用

使用了加密机之后

对数据进行严密保护 – HSM能够将加密密钥安全的存储在硬件内部

法规遵从 – 完全符合PCI-DSS、EMV、GDPR等法规标准对数据加密的要求，同时提供完善的审计能力

降低运行成本 – 极其容易的集成部署，无需维护

Thanks !