SSTG
安全产品技术部

滴滴出行

智能设备标识的困境与出路

杨正军

中国信通院

共建安全新生态
2020滴滴网络安全峰会

2020.12.17

目录

01 智能设备标识困境

01 设备标识是数字经济发展的重要抓手

当前，智能设备标识（如IMEI、MAC、IDFA等）已成为我国数字经济发展的重要抓手，应用于政府监管、商业运营、互联互通等不同业务场景，并为数字经济的安全发展起到一定作用。

在确保数字经济安全中的作用

工商、质检、海关等部门可利用IMEI码辨别手机的真伪

国家相关部门通过设备标识码分辨用户设备，打击电信诈骗等

运营商可来判别复制卡，降低经济损失和网络影响

金融机构利用设备标识形成风控模型，达到风险控制

在数字经济发展中的应用

“互联网+”、“智能+”是数字经济发展的手段，**互联网广告**正是这一手段运用的具体表现。

而从目前中国移动互联网广告市场的商业化现状来看，大部分移动互联网业务均通过IMEI等移动设备标识码进行用户标记、数据拉通、精准广告推送等，可以说**以IMEI为代表的移动设备标识码已成为数字经济中移动互联网广告的基础设施。**

01 操作系统厂商收紧设备标识获取

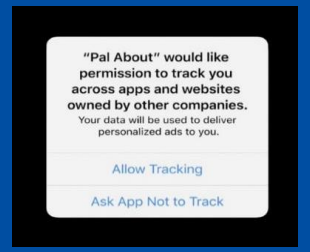
以IMEI、GAID、IDFA为代表的传统设备标识码在获取时均需通过操作系统提供接口，当前全球最主流的两大操作系统Android与iOS均收紧了设备标识的获取途径。

Android

2019年10月份发布的Android Q中提出： “We're limiting access to non-resettable device identifiers, including device IMEI, serial number, and similar identifiers.

iOS

2020年6月苹果提出iOS 14从9月份起：
IDFA： opt-out → opt-in
IDFA：Per Device → Per App
后推迟到2021年初。



01 个人信息保护、企业利益和政府监管之间的矛盾与平衡

用户诉求
保护隐私

公司利益
精准识别

政府部门
保护用户
协调诉求

① 设备标识滥用情况严重

② IMEI获得用户授权率较低

③ 设备标识码已经被认定为用户个人信息

02 设备标识解决方案

平台竞争，生态竞争，路线竞争

02 智能设备标识应遵循的原则

✓ 推进产业发展

- **阶段一致性**，一般设备标识应统一生成
- **有限唯一性**，同一个设备上不同时间获取到的设备标识保持一致，不同设备上获取到的设备标识不相同

✓ 尊重产业利益

- 保障互联网广告产业链的参与方如广告主、媒体、广告平台、第三方监测平台的利益，**数据不落地**，确保服务稳定性、可持续性。

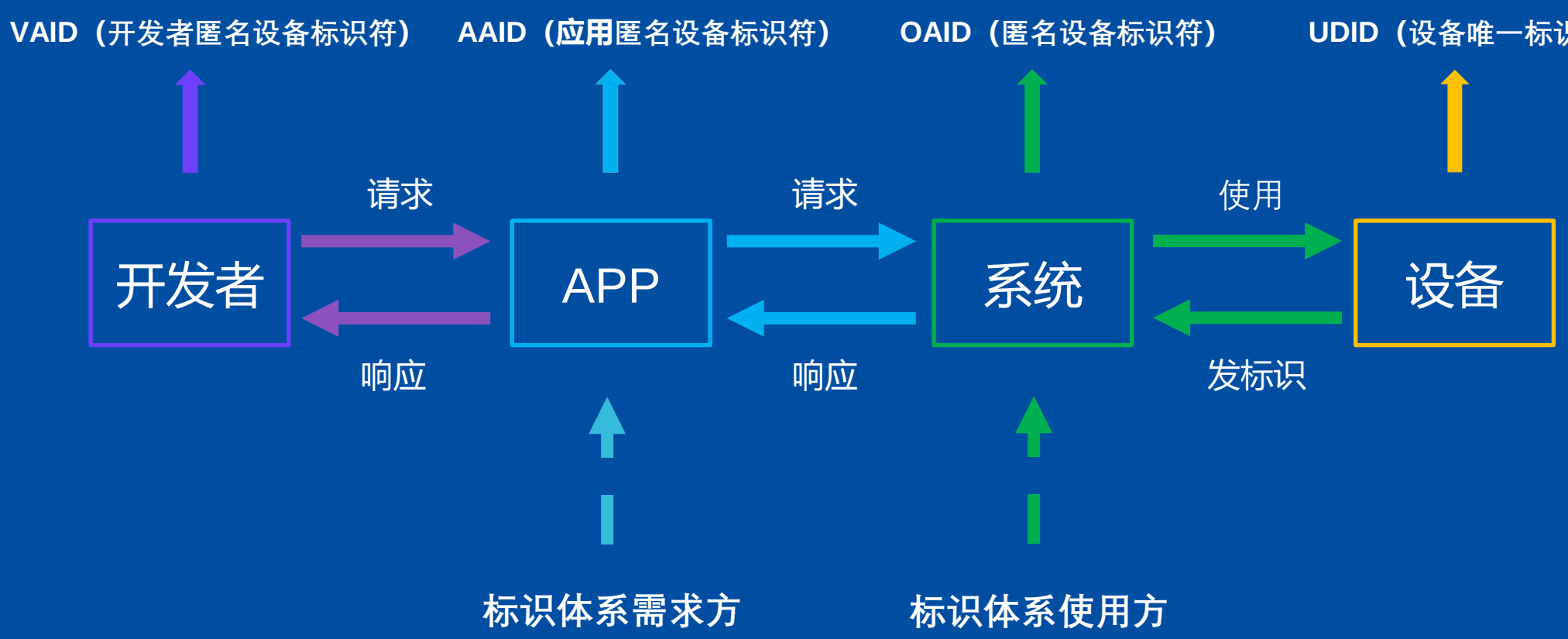
✓ 维护用户权益

- **可开关性**，应通过方便快捷的方式，让消费者对ID进行开启或关闭
- **可重置性**，设置方便快捷的方式，让消费者对设备标识进行重置
- **可更新性**，设备标识的生成算法应用定期更新机制，保证匿名性与强对抗性

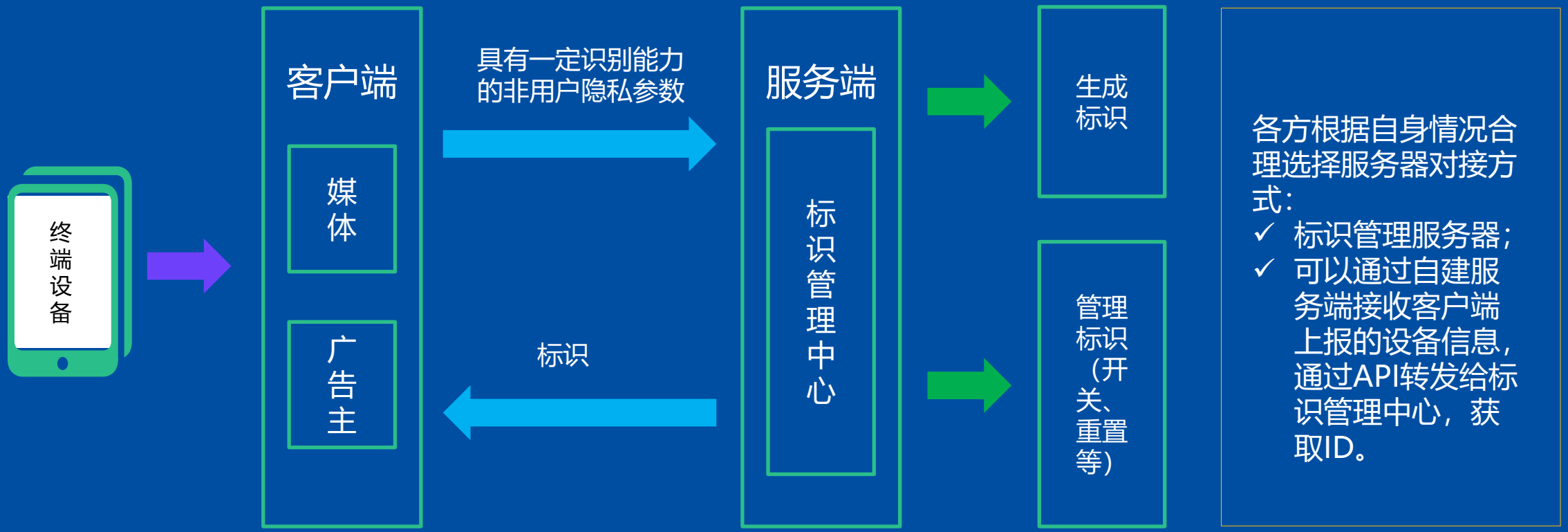
✓ 保障数据安全

- **保密性**，设备标识生成算法应保密，避免被逆向破解
- **匿名性**，设备标识应无法逆推出任何用户设备、个人信息
- **安全性**，客户端采集的数据应不包含任何个人信息，保障用户数据安全

02 基于终端实现的移动互联网设备标识



02 基于第三方平台服务的智能设备标识



各方根据自身情况合理选择服务器对接方式：

- ✓ 标识管理服务器；
- ✓ 可以通过自建服务端接收客户端上报的设备信息，通过API转发给标识管理中心，获取ID。

02 智能设备标识对比

标识名称	实现方	获取方式	开关性	重置性	适用对象
设备唯一标识符 UDID	终端厂商	不对第三方应用开放	无法关闭	无法重置，始终不变，除非硬件改变	不公开，仅用于设备的生产环境及合法性校验
匿名设备标识符 OAID	终端厂商	第三方应用通过厂家接口或集成SDK获取	可以关闭	用户手动重置、恢复出厂设置、设备商重置	用于精准推荐、广告营销等业务
国际移动设备识别码 IMEI	国际组织	第三方应用通过操作系统API获取，后续将关闭	无法关闭	无法重置，但存在被篡改可能	用于工商、质检、海关等监管业务
Android设备标识符 ADID	操作系统厂商Google	通过Google Service获取，**目前国内无法使用**	可以关闭，关闭后获取到的是重置后的真实值	用户手动重置、恢复出厂设置	用于个性化推荐、广告等业务
iOS设备标识符 IDFA	操作系统厂商Apple	操作系统提供API给第三方应用	可以关闭，关闭后获取到的是一串16位的0数值	用户手动重置、恢复出厂设置	用于个性化推荐、广告等业务

02 基于移动设备标识体系的行业应用

设备标识的作用日益明显、应用广泛

移动安全

开发者利用设备标识进行异常设备标记、异常行为溯源，保护用户利益

金融风控

利用设备标识识别诈骗行为、风险追踪，为行业安全稳定运行提供保障

大数据AI

以设备标识为基础开展各类模型训练和前沿技术探索

广告营销

利用设备标识能够精准地追踪广到告转化、识别作弊和假量，与黑灰产对抗

02 设备标识体系应用于数字广告领域的场景

在移动互联网广告活动中，标识是移动互联网广告运行的基础性数据，广泛应用在广告主、媒体平台、第三方监测公司、代理公司等市场主体数字营销业务的全链条。

设备匿名标识（OAID）具有更好的匿名性，并且在IMEI越来越难获取的趋势下，能辅助或替代IMEI标识终端，应用于数字广告领域。

CAICT 中国信通院 ⇌ CAA 中国广告协会 CHINA ADVERTISING ASSOCIATION

CDA TECHLAB 互联网广告技术实验室

中国信息通信研究院联合中国广告协会成立“互联网广告技术实验室”

媒体平台

- 标识用户
- 贴合用户需求展示广告

第三方监测公司

- 打击数据造假
- 广告投放效果评估

广告主

- 投放广告结算依据
- 广告归因的重要指标

02 设备标识体系应用于物联网设备的场景

推动设备标识体系在物联网设备上应用可更好的识别物联网设备，强化对物联网设备的有效监管。目前，补充设备标识体系已在智能手环等可穿戴设备、OTT智能电视等互联网新型接入终端上进行了初步尝试。

支撑“长虹5G智能测温手环”

“长虹5G智能测温手环”将数据安全作为开发核心工作，测温手环应用设备匿名ID技术（OAID），实现用户数据保护。用户的体温、地理位置数据匿名提交，具有用户隐私保护功能。

OTT智能电视统一设备标识体系建设

传统电视vs. OTT电视

OTT是“Over The Top”的缩写，是指通过互联网向大屏用户、尤其是家庭用户提供基于开放互联网的各种视频及数据服务业务，OTT智能电视作为互联网的新型接入终端，具有强烈的设备标识需求。

02 设备标识体系应用于金融风控的场景

对于银行、电商、贷款等对于安全需求更高的金融场景来说，可以利用设备标识形成风控模型，利用大数据技术进行用户征信调查、欺诈用户识别等，从而达到风险控制。基于设备标识相关变量，可根据黑产的欺诈场景开发多种策略。

场景一：黑产发现某贷款平台拉新活动的漏洞，进行批量注册，未修改设备参数。

防范策略：平台通过短期内多人共用同一设备标识，判断遭受黑产攻击，进而在授信或提现环节阻断其交易。同时，亦可修改拉新活动的策略，避免损失扩大。

场景二：中介远程操作帮客户申请贷款，注册、登录、活体检测等环节由客户本人操作，但资料填写及最终提交授信由中介操作。

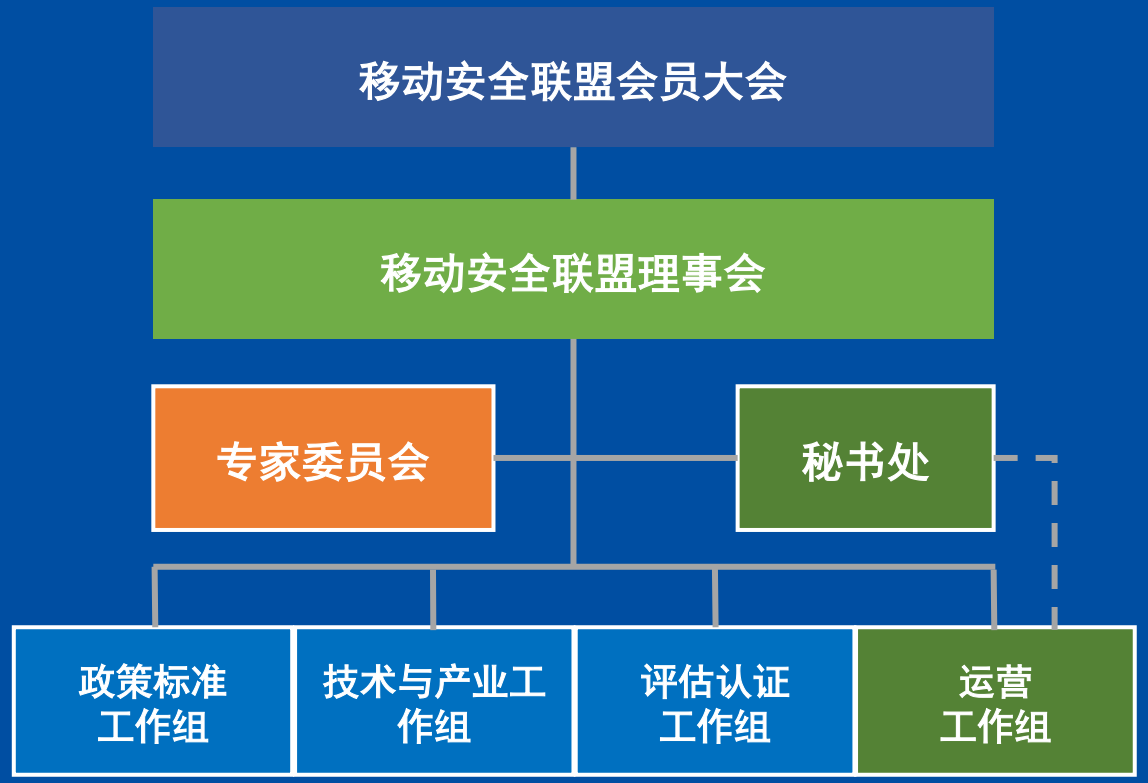
防范策略：通过中介的操作行为，可判断在同一次授信过程中，有两次登录APP行为，且有两个不同的设备标识，最终确定用户此次授信非本人申请的嫌疑很大。

03 灰黑产治理

03 多方合作共赢——移动安全联盟

移动安全联盟Mobile Security Alliance

移动安全联盟于2017年12月成立，立足于搭建移动互联网安全的合作与交流平台，提供公平对话的平台、纽带，促进供需对接和知识共享，形成优势互补，有效推进移动互联网安全产业发展，维护行业秩序，切实解决企业现实问题。



政策标准工作组

- 梳理移动安全产业相关政策法规，开展热点政策法规问题的探讨；
- 推动移动设备和移动互联网行业规则、法律法规的制定，促进移动安全产业发展；
- 研究建立移动安全标准体系，开展联盟标准研制和验证，推进联盟标准转为国标行标。

技术与产业工作组

- 调研、论证移动互联网信息安全问题，提炼移动互联网产业链各方安全需求；
- 研究移动设备和移动互联网安全关键技术，提出移动互联网安全解决方案，
- 组织技术交流，组织评选最佳解决方案。同时发布移动安全相关研究报告、安全事件报告，为各部委决策提供支撑。

评估认证工作组

- 建立移动安全领域评估体系、测试方法和测试集；
- 基于已发布的标准，联盟内的实验室、评估机构可以开展认证认定工作。负责组织开展移动安全最佳技术方案评选，推动企业的互认可工作。

运营工作组

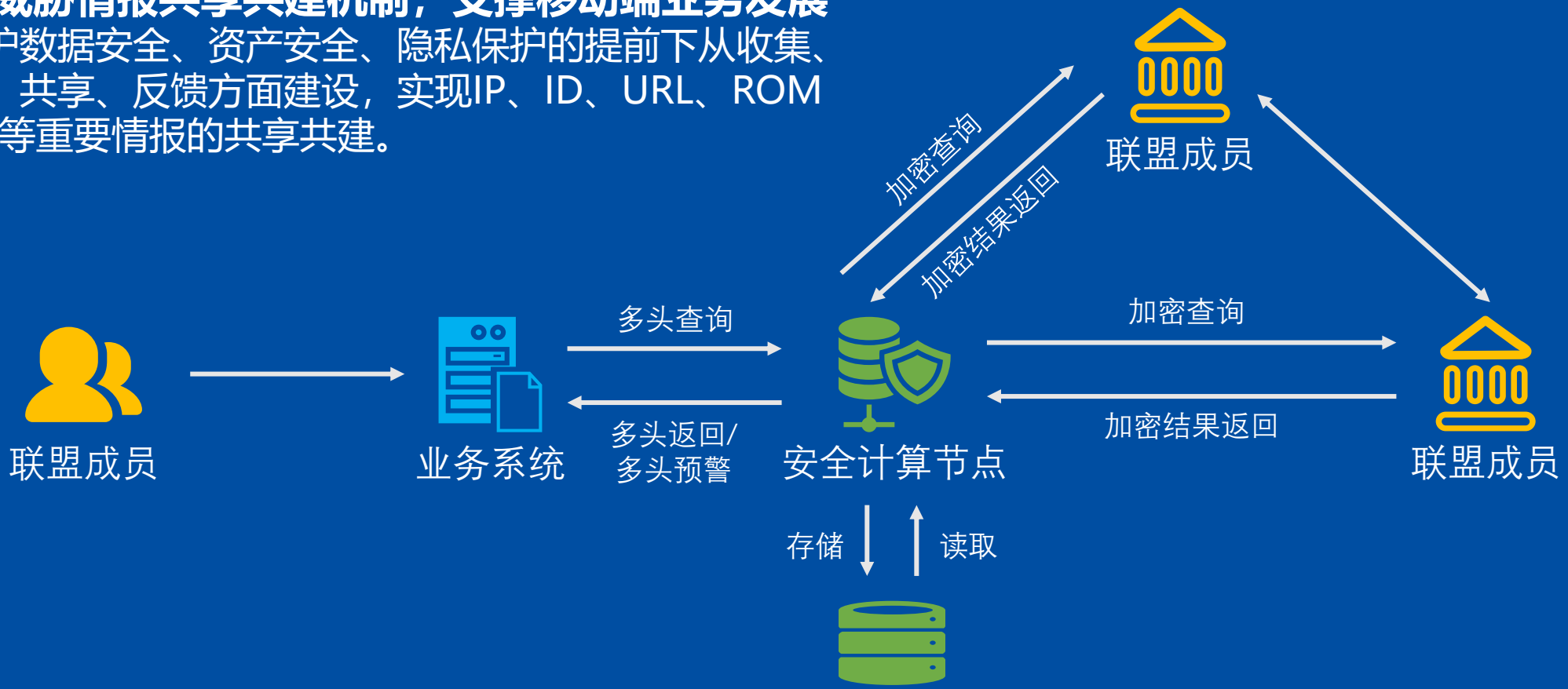
- 联盟公关宣传、日常运营、法律支撑、移动安全应急响应、国际合作交流等工作；
- 开展移动安全试点示范、宣传产业优秀成果、组织大型比赛、进行品牌运作等。

理事长：谢毅

秘书长：杨正军

03 基于威胁情报的灰黑产共治项目

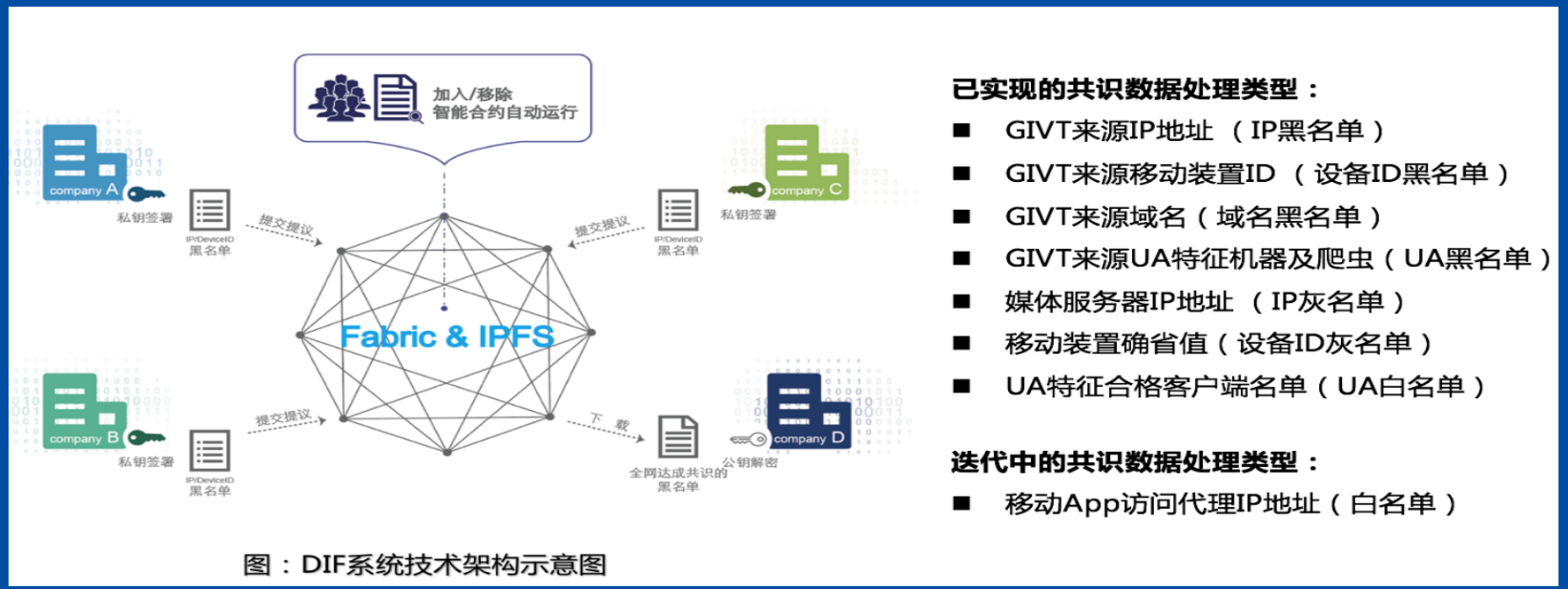
建立威胁情报共享共建机制，支撑移动端业务发展
在保护数据安全、资产安全、隐私保护的提前下从收集、研判、共享、反馈方面建设，实现IP、ID、URL、ROM、PN等重要情报的共享共建。



03 GIVT List

利用新兴技术和方法论，在行业各方力量共同参与和支持下，移动安全联盟联合中国广告协会定期发布“一般无效流量数据”（GIVT数据），包括：IP地址黑名单、IP地址白名单、Device ID黑名单、Device ID白名单，是中国唯一的行业级“一般无效流量数据”。目前工作组已有超过37家企业成员，涵盖了数字经济生态上下游中所有角色，包括数字媒体、程序化广告平台、第三方监测公司、审计机构、学术研究院。

使用开源项目——DIF联盟链，做为无效流量相关数据生产和发布的执行工具。运用创新新技术，打造了基于区块链的黑名单机制与体系，极大提升异常流量发现和共享的效率，这不仅是国内首次，在全球也是首创，体现了以新技术、新思路解决顽固问题的探索精神。



图：DIF系统技术架构示意图

已实现的共识数据处理类型：

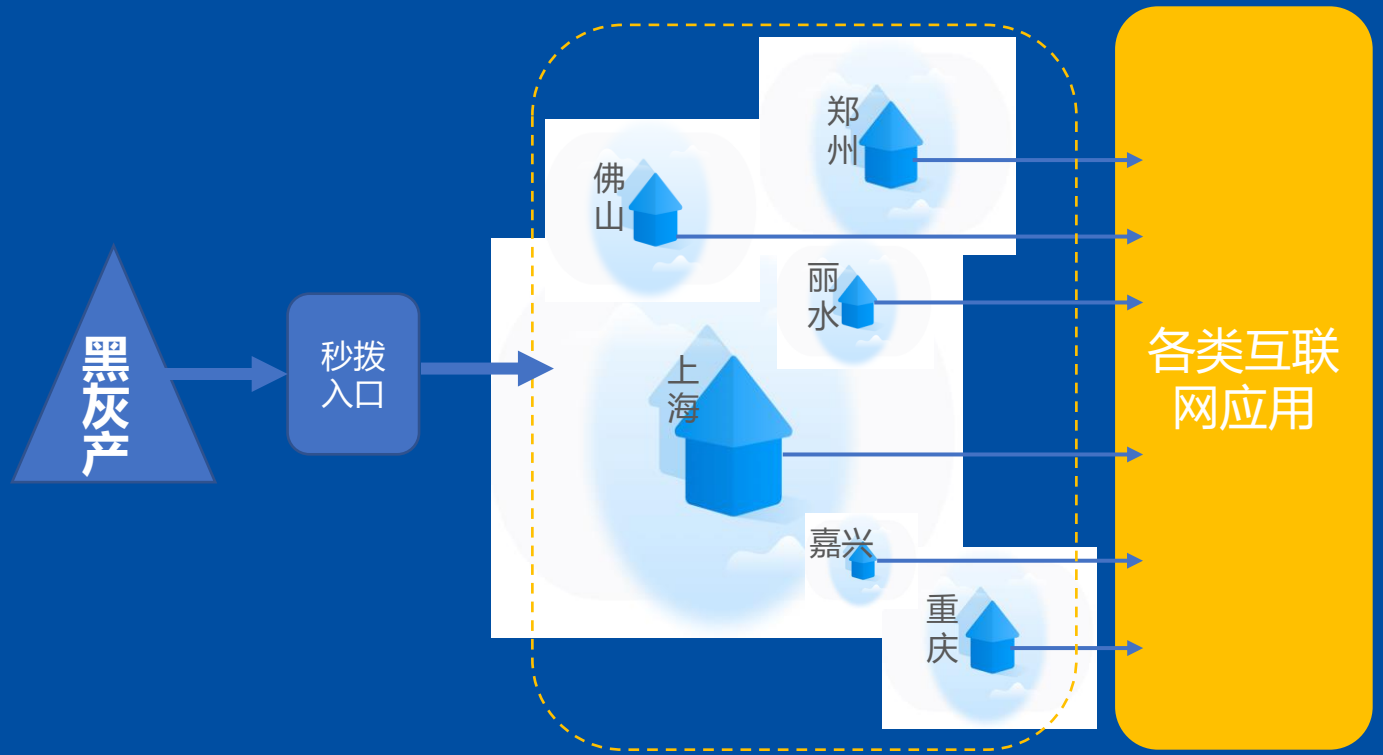
- GIVT来源IP地址（IP黑名单）
- GIVT来源移动装置ID（设备ID黑名单）
- GIVT来源域名（域名黑名单）
- GIVT来源UA特征机器及爬虫（UA黑名单）
- 媒体服务器IP地址（IP灰名单）
- 移动装置确省值（设备ID灰名单）
- UA特征合格客户端名单（UA白名单）

迭代中的共识数据处理类型：

- 移动App访问代理IP地址（白名单）

03 秒播灰产

利用家庭宽带线路分配得到动态IP的特性架设的特殊VPN。通常在全国多城市架设多个家庭宽带接入点，提供统一入口供灰黑产应用自动化地高速切换获得当地家庭宽带IP地址，从而对各类风控系统和策略构成欺骗性。典型的秒拨服务有“城市定向”和“全国混播”两种模式

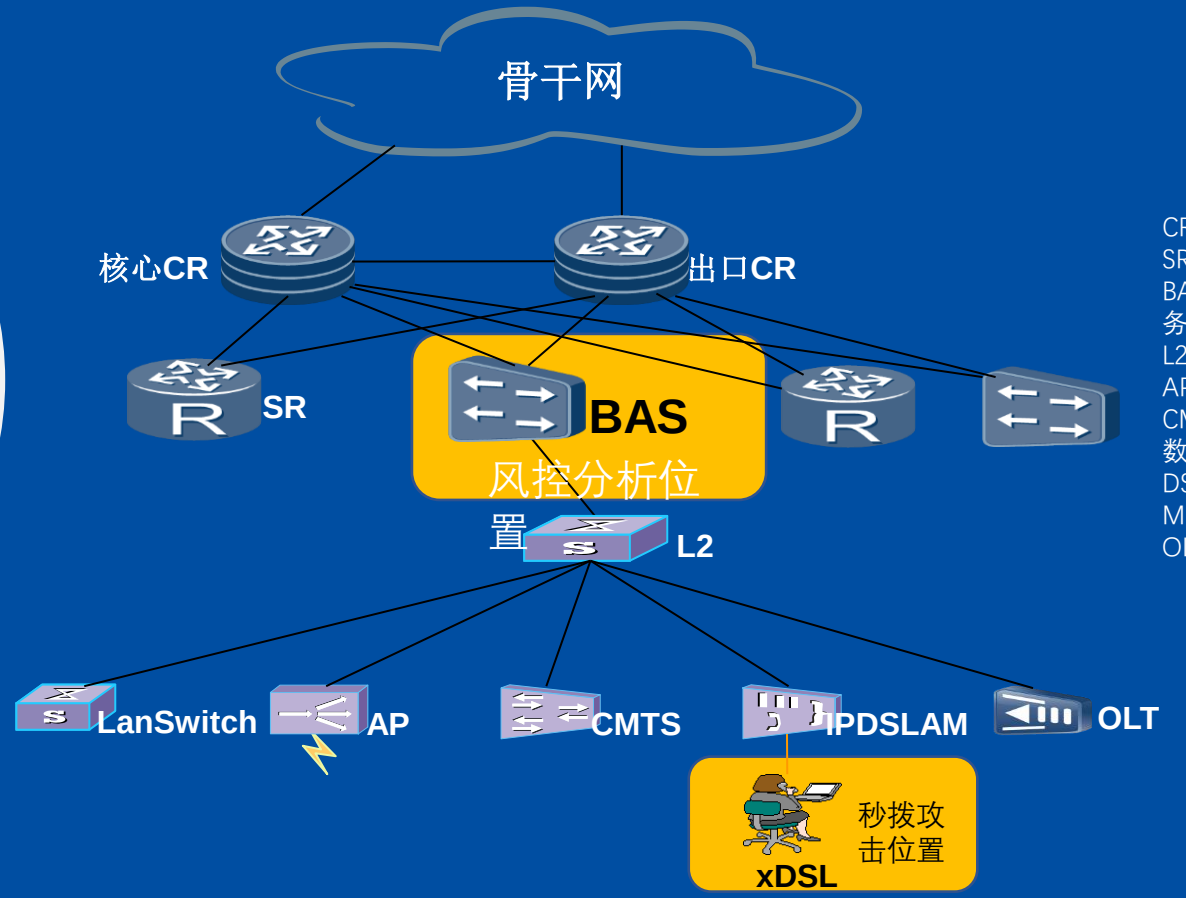


- 对抗各类爬虫采集行为，强化人机识别
- 对抗薅羊毛行为
- 对抗虚假注册、甄别养号行为
- 甄别群控设备
- 甄别虚假交易
- 甄别受操纵的舆情传播、虚假投票和转评赞
- 对抗虚假广告和虚假安装激活留存
- 完善各类金融交易和电商交易过程中的风险控制
- 完善各类防火墙策略

03 秒播灰产治理

通过BAS下网络结构的探测分析，能够高效预测任意IP的秒拨风险

秒拨攻击动作发生在xDSL环节



CR: Core Router 核心路由器
SR: Service Router 业务路由器
BAS: Broadband Access Server 宽带接入服务器
L2: Layer2 Switch
AP： Wireless Access Point
CMTS: Cable Modem Terminal System 电缆数据机终端系统
DSLAM: Digital Subscriber Line Access Multiplexer 数字用户线路接入复用器
OLT: Optical Line Terminal 光线路终端

用户认知、行业水位、监管尺度

生态协同，将安全价值最大化

谢谢观看

THANK YOU