登录易SIG
for“基于登录易的OpenHarmony用户账号管理系统”

刘文印 liuwy@gdut.edu.cn

广东工业大学网络身份安全实验室WISLab

公众号：“登录易”denglu-1 | 官网：denglu1.cn

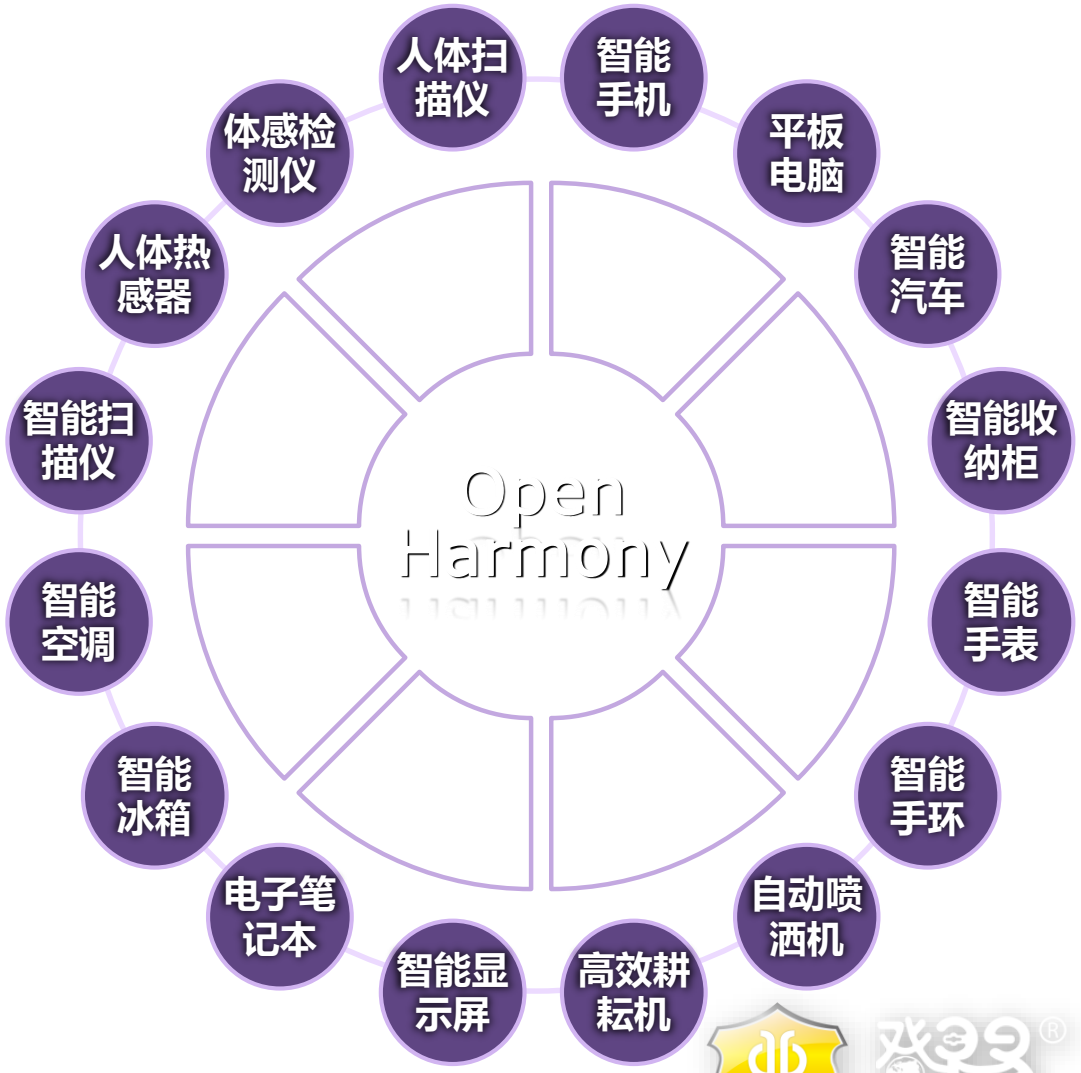
2021年9月30日

OpenHarmony 登录易 SIG定位

基于目前华为 OpenHarmony对数据信息保护的迫切需求以及物联网行业的数据安全问题，登录易开创了**全场景物联网设备数据安全管理平台**，为企业提供优质安全的物联网设备数据保护，保障万物互联时代下的信息安全。登录易希望可以通过产品创新的服务模式与成熟的技术基础为华为等杰出国产品牌提供数据安全保护屏障，助力国产品牌数据安全，保障国家数据安全，开创万物互联的新阶段。

建立 OpenHarmony 用户生态

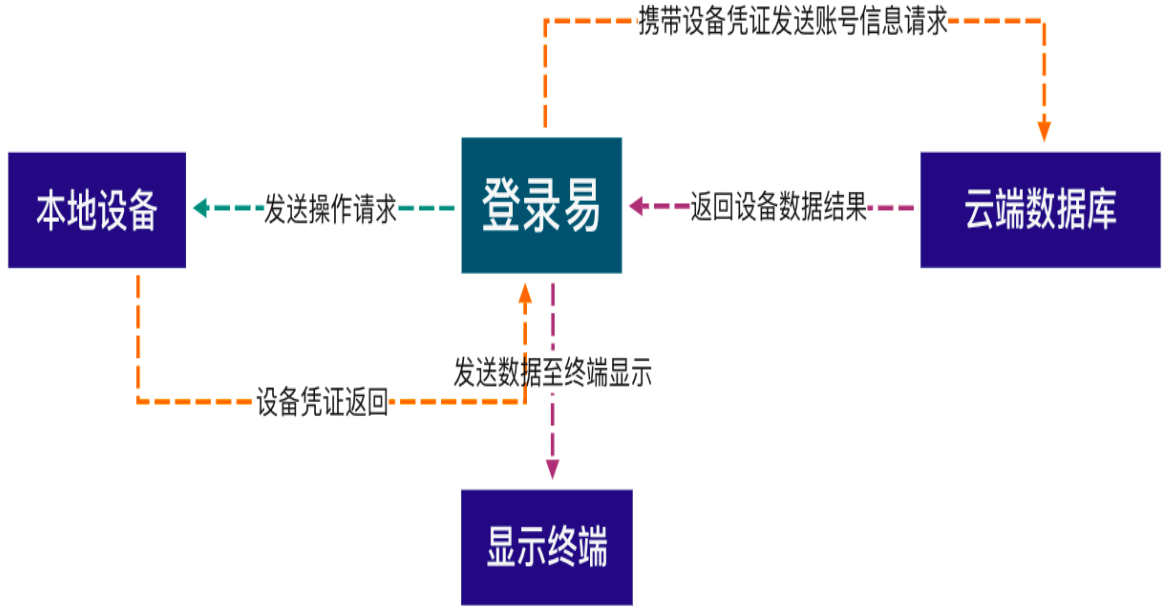
通过在 OpenHarmony 环境嵌入与一个标准的多账号管理模块，与手机登录易App通信互操作，实现新用户（包括人类用户和其他设备用户）的**自动注册，老用户的自动登录，自动修改密码**等功能，**建立“登录易+Harmony”生态账号系统，搭建 OpenHarmony 账号安全生态社区。**用户除了可以使用专属的原的华为账号体系，还可以通过OpenHarmony开源环境中增加的登录易账号系统与其他 OpenHarmony 用户（和设备）进行安全验证和授权后的资源分享，也可通过账号划定个人私域空间，建立个人云端数据库。通过这种方式提升用户粘性，构建具有完整安全功能的 OpenHarmony 生态社区。



针对物联网设备弱密码造成的数据泄露问题

为每个用户建立集中、统一、单点管控的信息与设备管理终端，实施个人用户对多个设备的统一认证管理

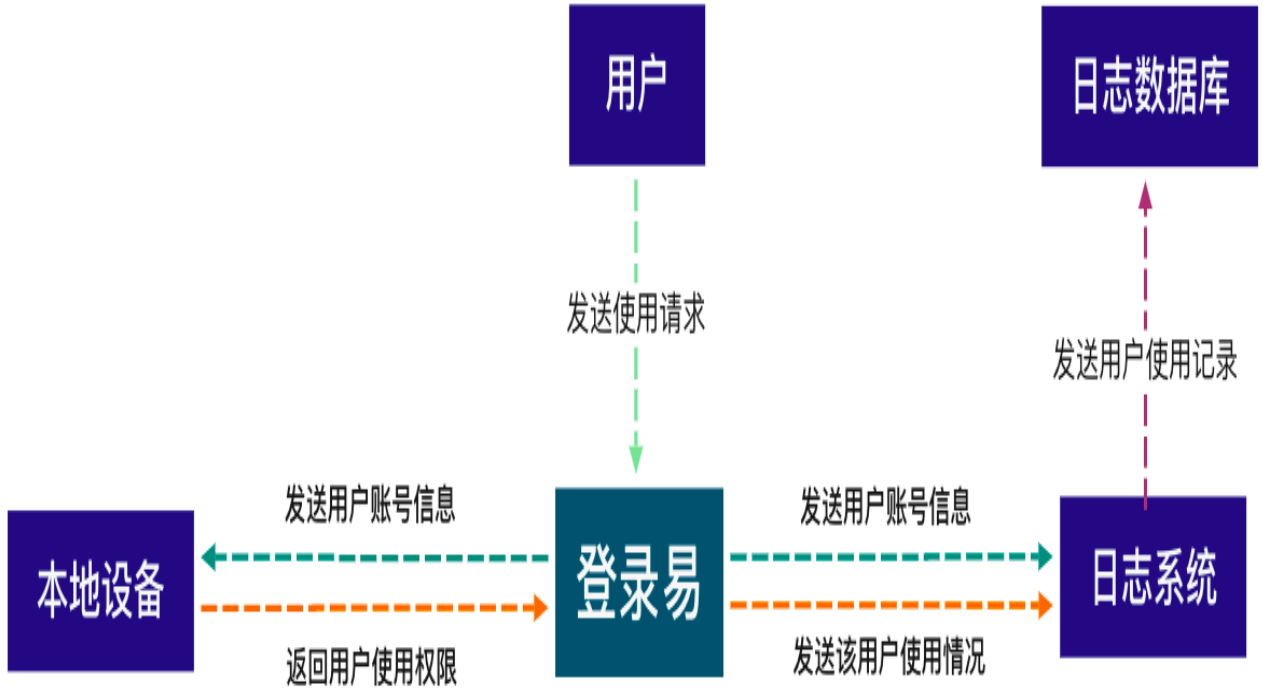
用户注册登录易账号后，可直接**通过登录易集中、统一、单点管控自己的所有已搭载 OpenHarmony 系统的智能消费物联网设备**，登录易自动为设备设置专属的强密码并可（人工设定或定期）自动修改，用户使用时只需通过装有登录易App的手机等智能设备进行**“刷卡”**（或同一局域网内的通信）即可完成认证，在降低产品密钥的记忆成本的同时解决产品的数据安全问题。



针对物联网数据安全保护体系的缺位

实施权限管理/审计记录

用户每次使用搭载“登录易+ OpenHarmony”系统的智能物联网设备时，需要通过登录易App进行信息认证与记录。通过账号信息限制该设备的使用权限并上传使用记录至日志系统，没有该设备使用权限的用户可通过登录易提交使用请求，没有权限的用户也可通过登录易提交针对部分核心权限功能的使用请求，**所有进行使用设备请求的用户的账号信息都会记录在日志系统，存储在日志数据库，便于管理者随时进行调用审计。**



OpenHarmony 登录易先期筹备单位

一、网络身份安全粤港联合实验室（WISLab）

本实验室参与主持了国家自然科学基金、广东省“珠江人才计划”引进创新创业团队等多个项目，实验室致力于网络身份认证与安全管理机制的理论研究和产品开发，在此领域已发表高水平论文20多篇，申请发明专利20余项，十多项已授权，发布多项受用户欢迎的网络安全产品，研发团队近20人，为该项目的顺利完成提供强有力的保证。

二、登录易开发团队

团队是由广东工业大学计算机学院WISStudio实验室的学生组成，致力于为用户的个人信息提供高强度安全防护，减少发生用户个人隐私信息泄露的情况，提高信息保护的安全性。团队成员由本科生和研究生组成，部分成员拥有项目运营的经验，还拥有丰富的技术研发经验和实践。团队成员拥有良好的分工合作及团队协作精神，团队内部凝聚力强，成员责任心强。确保了团队的高效运转。同时团队还拥有多位顾问：国际模式识别学会会士刘文印、“青年百人A”杨振国、广东工业大学优秀指导老师柯婷等。

登录易 SIG工作思路

| 基于全场景可信服务平台—针对市场共性问题

搭建面向全场景应用的可信管理平台，制定接口标准，易于对接信息管理方、信息请求方及服务提供方，利用基于公钥体系的数字证书技术对用户代理、信息请求方及提供方的合法性进行认证，同时构建个人敏感 信息的合规监管机制，降低敏感信息泄露的风险，实现个人信息的有效保护和高效利用。

| OpenHarmony账户系统—针对 OpenHarmony账号系统的缺位

针对目前市场上搭载 OpenHarmony的物联网设备缺乏账号系统的市场痛点，本团队采取“登录易+ OpenHarmony”这一模式。因为登录易该产品不仅仅是密码管理器，其工作原理更是本团队独创的**基于可信用户代理的多方闭环网络身份认证机制**，颠覆了现有的B/S架构用户认证机制，但兼容传统账号密码系统，同时可以**检测钓鱼和网络非法（包括入侵、后门等）请求**，与 OpenHarmony系统缺乏账号管理体系这一弊端进行完美的**有机互补**。具体表现在 OpenHarmony源码同级层面上添加账户管理系统，给用户分配对应的权限，并以登录易为第三方协助管理账户密码，传输账户密码，从而实现人与设备之间，设备之间的互相认证。总而言之，登录易账户管理系统的嵌入，会使用户与搭载了OpenHarmony的智能设备粘合度更高。

登录易 SIG工作思路

| 强密码全周期管理机制—针对账号泄露问题

利用登录易现有的强大的密码管理功能，一键生成强密码，一键加密传输强密码，并可自动定时修改密码。针对敏感信息保密性弱、匿名性差、重复收集、滥用、甚至随意出境等问题，利用用户个人信息的访问请求控制策略，实现对隐私信息集合的设计、构建，设置预授权策略，根据个人备案自动监管请求的合规性，确定访问请求的合法性，有效实现对敏感数据的扩散范围和使用权限的控制，防止用户隐私泄露。

| 多账号协同安全管理

基于登录易以单账号登录多物联网设备，实现统一管理。用户要查看并使用智能设备的数据需要登录易授权，且由登录易云端存储的数据采用AES256算法加密，也可离线使用，支持数据仅在本地加密存储。即使泄露也无法解密，具有极强的加密性能。用户查看物联网设备数据会在登录易端留下审计记录，实现可视化监控，可以有效杜绝数据泄漏。

| 物联网设备便捷认证

追求登录易与搭载了 OpenHarmony的设备结合统一的新模式，其原理基于登录易APP，利用近场通信如蓝牙，NFC，WIFI等方式将存储在登录易APP上的强密码数据一键传输到搭载OpenHarmony的智能设备上，为智能设备提供账户身份信息，便于智能设备进行账户密码本地验证，达到用户便携交互的效果，提高用户体验，增强用户粘性。

对接单位及其贡献模块详情表（目前团队10+，10月再另招新10+）

序号	单位/个人名称	对接人	贡献功能模块	工作范围	预计投入人力	预计开始时间	预计完成时间	贡献能力具体描述
1	广东工业大学网络身份安全实验室WISLab	刘文印	登录易统筹	登录易统筹	50小时/周	2021.9.1	2021.12.31	架构设计；产品设计
2	广东工业大学粤港网络身份安全实验室wislab	吴宇鹏	登录易插件	登录易插件	30小时/周	2021.9.1	2021.12.31	代码实现
3	广东工业大学粤港网络身份安全实验室wislab	邱棋锋	登录易后端	登录易后端	30小时/周	2021.9.1	2021.12.31	代码实现
4	广东工业大学粤港网络身份安全实验室wislab	何楷聪	登录易与设备通信	登录易与设备通信	30小时/周	2021.9.1	2021.12.31	代码实现
5	广东工业大学粤港网络身份安全实验室wislab	颜文圣	登录易前端	登录易前端	30小时/周	2021.9.1	2021.12.31	代码实现

THANKS