



信息网络中心
Information Network Center

成都大学身份系统建设 实践分享

信息网络中心 何源

提要



信息网络中心
Information Network Center

- 建设背景
- 项目落地
- 实施效果
- 下一步应用



项目建设的背景



信息网络中心
Information Network Center

项目背景

- 新需求使老认证系统面临诸多挑战
- 学校“十四五”规划需要项目落地验证可行性

学校十三五信息化规划



信息网络中心
Information Network Center



组织保障



信息化安全流程



网络安全体系



网络运维体系



监控基础设施

信息化保障体系建设

信息化服务对象的角色



教师



学生



管理人员



决策者

管理服务信息化建设



校园GIS



教务业务系统



科研管理系统



人事管理系统



办公自动化



一卡通系统



平安校园平台



决策支持系统



财务系统



学工系统



后勤



迎新、离校系统

信息化基础支撑平台建设



统一数据共享平台



统一身份认证



综合信息门户



数字化图书馆



数字化档案馆



大数据研究应用平台

信息化基础设施平台建设



现代化教学支撑



校园云平台



网络基础管线



无线网络



新一代高速网络



信息网络中心
Information Network Center

十三五信息建设成果

- 校园网建设全面提升
- 云计算初具规模
- 业务系统全面覆盖
- 网络安全体系基本形成



十三五信息化建设反思

- 单一的业务驱动建设
 - 数据一致性差
 - 信息系统建设水平参差不齐
- 数据资产难以有效盘活
 - 数据流动性差
 - 没有有效挖掘

A large, solid magenta oval containing the Chinese characters '数据' (Data) in white, serif font.

数据



信息网络中心
Information Network Center

十四五信息化规划 工作理念

- 以需求为导向
- 以数据为核心
- 以服务为目标
- 以信息技术为手段



信息网络中心
Information Network Center

十四五信息化建设 方向

信息化引领驱动学校现代化发展



信息网络中心
Information Network Center

认证系统面临的挑战

- 如何为不同类型人、不同场景、不同时段提供认证
- 如何构建一套符合数据安全和网络安全的认证系统
- 如何进一步挖掘认证数据的价值



如何在项目建设落实 十四五规划工作理念



以需求为导向 认证业务三个维度

- 认证对象
 - 教职工（人事）
 - 学生（教务、研究生）
 - 临时人员
 - 外籍教职工
 - 留学生
 - 校外进校办事人员
 - 临聘工作人员
- 认证场景
 - 接入校园网
 - VPN
 - 刷脸进入校园
 - 应用系统
- 认证时段
 - 在校生
 - 留校工作
 - 临聘

以数据为核心



信息网络中心
Information Network Center

- 确定数据的权威源（认证系统通常不是数据权威源）
- 数据流动（认证系统拥有丰富的接口）
- 细致地数据治理
- 将认证生物特性统一管理，保障数据安全



信息网络中心
Information Network Center

以服务为目标（解决了谁的什么问题）

- 解决用户账号生命周期和多身份的问题
- 解决网络接入认证管理中的精细化管理
- 解决各类应用人脸认证和精细化管理
- 解决用户账号分发和安全问题
- 解决账号状态变化系统间联动



信息网络中心
Information Network Center

以信息技术为手段（产品选型）

- 认证系统应该用成熟产品功能实现需求而不是靠大量定制开发
- 认证系统应该提供丰富的上、下游接口
- 认证系统开发者能提供优质的需求落地服务
- 认证系统开发者能提供优质的数据治理服务



项目实施流程

- 方案落实
 - 通过访谈多个部门掌握用户需求，落实解决方案
 - 通过分析现有数据设计数据治理方案
 - 通过分析现有认证系统设计系统整体迁徙方案
- 项目实施
 - 数据治理
 - 系统部署
 - 灰度测试
 - 正式上线



Source ID 实施效果



全校人员数据治理，身份数据完整准确安全

身份信息异常字段	异常情况	影响结果	数量
姓名	姓名为空，有空格，相同姓名	人和账号无法实名	750
手机号	缺乏手机号，临时人员手机号有空格	修改信息；群组推送；无法信息推送。	21377
护照/身份证号	证件类型缺乏，证件号和人员姓名，手机号匹配不准确	个人信息不准确；管理不准确；无法多身份合并，缺乏实名核身信息	1076
学工号	学工号、手机号、证件号混用	身份信息采集不准确，影响账号激活和认证	2678
密码	账号使用弱密码	弱密码不安全，不合规易被盗用	18012
组织单位	用户缺少组织单位	缺乏组织无法准确推送群组	45365

原始数据分析：

- 1、全人员信息核心字段：姓名、手机号，证件类型、证件号，学工号，组织单位和密码等使用异常。
- 2、人员关键信息异常主要影响人员实名验证；人员信息传递不准确；账号被盗用引发的安全问题，导致师生体验不好；以及信息中心管理不便等。

异常数据	处理方法	治理结果
姓名为空、包含空格	1、数据源头补齐姓名 2、SID采集时去除空格	账号实名，准确
没有手机号，包含空格	登录使用时需要强制绑定手机	人员手机号全，准确
无证件类型，证件号长度异常	1、缺失类型：用脚本补齐证件字段 2、多余空格：脚本去除异常字段。	身份证/护照类型全，证件号准确
学工号=手机号=证件号混用	1、确认账号真实性和属性 2、清空绑定手机号，用户再绑定	全员学工号，手机号，证件号准确
使用身份证后六位初始密码	新老用户走账号认证激活流程	强密码，安全
用户无组织	数据中心补齐组织单位，SID再采集	组织完整，对外同步准确

数据治理结果分析：

- 1、对全校人员27000余人，合计49000多账号进行统一治理，确保治理以后，所有人员，（1）身份类型，姓名，手机，证件，学工号等账号信息齐全；（2）全人员身份账号准确，账号密码使用安全。



信息网络中心
Information Network Center

临聘人员账号可控可管

老的实现方式:

- 1、学院部门外聘人员接口人，在流程平台为临时老师填写申请，如设置有效期6个月，并开通**网络接入+科研系统**的访问权限。
- 2、所在单位领导审批，审批完成以后，账号自动生成，并知会人事处。
- 3、账号同步到数据中心，需要找各系统开权限，发起人拿到账号，给临时老师使用。



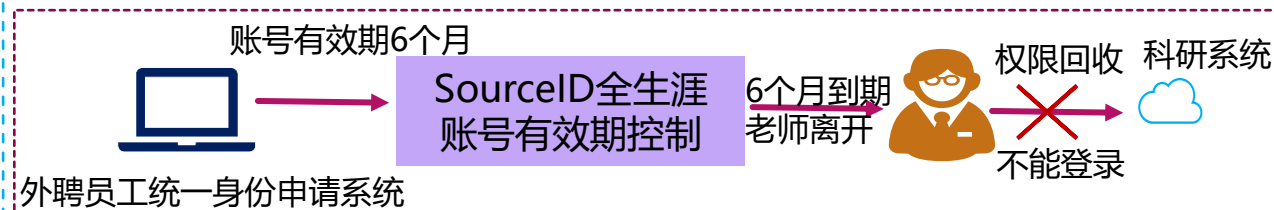
问题:

1. 临时老师账号有效期到期，**人员离开**，该有效期信息无法同步到对应业务系统，临时老师离开以后，权限无法回收，账号依旧能用，有安全隐患。
2. 如果临时人员二次返校，流程走完以后会重开新的账号，因此造成大量历史遗留账号，管理困难。

根因：网办设置的账号期限无法同步控制系统的访问权限和访问时间。

新的解法:

- 1、学校临时人员账号申请流程不变，申请者在网办填写的有效期6个月会同步到SourceID，
- 2、SourceID做生涯有效期控制：有效期到期，临时老师的账号不可以继续认证和访问科研系统，权限进行回收。
- 3、外聘人员的账号延期管理，如临时人员二次返校场景，账号申请流程不变，信息管理员在SID管理端设置账号重新生效，并设置一个新的有效期。



带来效果:

- 临时人员身份信息，**账号开通、设置有效期限，回收及时、准确**；
- 账号延期机制辅助外聘人员**再次使用账号和权限**。可更新用户的有效期限，SID采集有效期限，使用户重新生效，减少大量临时人员账号的产生。



信息网络中心
Information Network Center

生涯多ID体系实现身份随人走

背景:

杨老师是成都大学信息学院的一位老师，她本科就读于本校，然后又在本校读研究生。最后留校任教，在学校的学术生涯里，她前后拥有了三个组织身份（本科生、研究生、教职工），对应三个组织身份ID（本科生学号、研究生学号、教工号），杨老师拥有新身份的时候拿到新的ID，管理上身份平台要求绑定手机和身份证，往往绑定失败，导致新ID不能使用，原因是杨老师的手机号和身份证号已经被老身份ID绑定，并且身份ID与手机号/身份证号是1:1的对应关系

身份ID与手机号/身份证号是1:1对应关系

 杨XX	角色	学工号	手机号	身份证号
	本科生	2012666	18888888888 (解绑)	L513126XXXXXXXXX0015 (增加前缀进行区分)
	研究生	2016888	18888888888 (解绑)	ML513126XXXXXXXXX0015 (增加前缀进行区分)
	教职工	2020999	18888888888 (绑定)	513126XXXXXXXXX0015 (绑定)

处理办法:

管理员在数据中心将她过期身份对应的身份证号增加前缀字母，并将手机号解绑以后重新绑定新的身份。

痛点:

杨老师: 杨老师的身份证号被研究生账号绑定，教工账号没有绑定手机号和身份证号，造成业务不能使用，体验不好

信息中心管理员:

- 1、人工调整麻烦，新身份用户需要重新绑定手机号
- 2、修改用户历史身份的手机号、身份证件号造成脏数据，使得人员历史身份信息不准确
- 3、丢失了人员历史身份信息

根因: ID体系的不合理造成身份数据错乱，最终造成用户不能正常使用业务

新的解法:

- 重构人员和身份ID的关系，把原来账号绑定人的方法，转变为一个人可对应多个ID账号的模型
 - ✓ 对身份数据采集并治理，基于证件号/手机号来做同人判定，将一个人的多种身份聚合到这个人身上，形成人与身份ID的1:N的关系，即多个身份ID关联到同一个人身上
- 结合人员的生涯状态规范，自动调整各类身份的访问权限。比如已毕业的本科生/研究生账号失效，不能再访问，访问权限更加可控



人ID

手机号: 18888888888

身份证号: 513126XXXXXXXX0015

1:N

人拥有的
身份ID

本科生账号: 2021666

研究生账号: 2016888

教职工账号: 2020999

带来效果:

杨老师:

- 新身份用户无需再次绑定手机号，新身份账号可以立刻使用，体验好;
- 生涯过程完整; 历史连贯，如果有多身份可在线切换使用，可登录查看个人完整历史信息。

信息中心管理员:

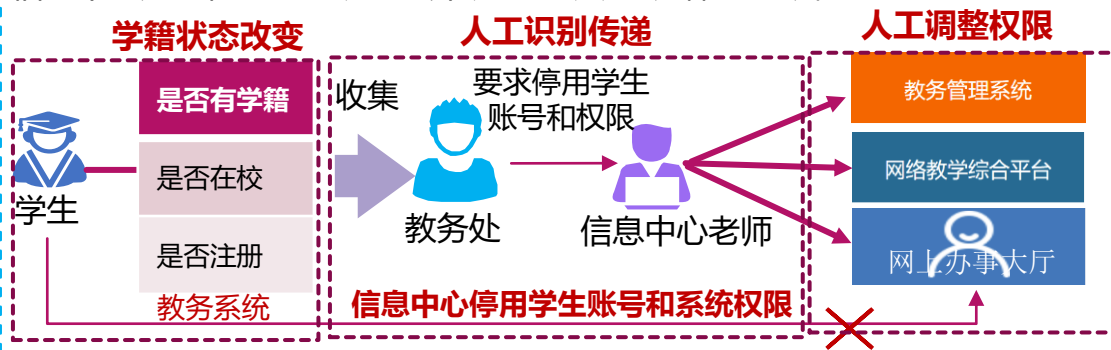
- 1、无需人工调整，省事
- 2、人员身份数据不被修改，保障数据准确可信
- 3、提供人员生涯身份变化的连贯能力，为今后人员画像分析提供支撑



学生学籍有变动，账号和权限快速调整

业务目标：

1、每年都有部分学生出现参军入伍，或者转学，休学，出国留学，或者退学的情况，需要及时同步到系统管理员或者信息中心，进行账号和权限调整。但目前信息中心无法和各学院就学籍异动情况做跟踪并保持一致，



老的实现方式：

信息中心被动响应，若教务处要求某账号停用，信息中心老师再去停用此账号，关闭系统访问权限。

问题根因：

- 缺乏简单且快捷的方式及时了解学籍异动学生的情况。
- 主要依靠人工统计和调整权限，处理不及时，多的时候每天几十例，工作量大。

新的解法：

- ✓ 教务系统梳理关键状态，“是否有学籍、是否在校、是否注册”三个状态。不同组合规则表示学生的异动状态。
- ✓ SID通过采集规则识别，设置学生的状态为“在校、入伍、转学、休学、退学”等，设置不同生涯状态匹配相应的认证、授权策略，如(有学籍，不在校，已注册)>休学>休学权限
- ✓ 当学生的学籍状态变动，Source ID会触发生涯状态变化为休学、并自动触发策略执行异动的账号不可登录和访问系统。



带来效果：

信息中心：当学生的学籍异动时，可快速及时调整账号权限，限制学生学籍异动账号继续访问学校系统，保障教学计划的正常开展。



信息中心
Information Network Center

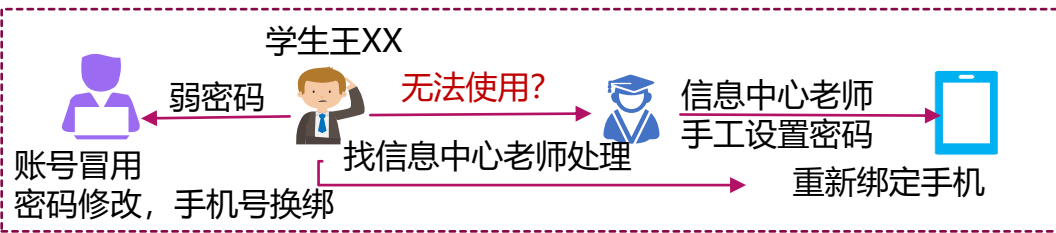
实名账号激活和复杂密码设置

问题:

每年开学大量新生入学,信息中心会提前为每位学生准备账号,为了方便学生使用账号,默认密码采用身份证后6位方式,学生报到后自行修改密码,如果不改密码,身份证容易被他人获取、冒名修改密码,导致本人无法登录,造成个人信息安全问题与使用不便;同时国家相关部门也在定期检查,不允许使用弱密码,一经发现勒令整改。

业务目标:

- 保证密码安全,满足账号强密码合规要求
- 确保学生本人自主激活账号或修改密码,无需学生到信息中心设置密码,避免因学生密码修改麻烦造成的投诉



当前做法:

- 由于当前学校身份平台技术限制,学生初始密码只能设置为身份证后6位等弱密码,密码天然存在安全漏洞
- 人员核验采用身份证件+人工比对实现,不准确、易遗漏
- 弱密码账号易被盗用,如果账号和密码被冒用,手机号被换绑,学生必须来信息中心找老师设置新密码

痛点:

信息中心老师: 学生默认密码导致账号被冒用,新生开学前2个月,需要处理上百个账号被冒用事件,对学生重置密码,开学期间工作量大且易被投诉

学生: 无法登录使用,需要到信息中心修改密码,影响学习业务办理,耗时耗力。

新的解法: 采用校内+校外公安实名加人脸认证激活账号使用并设置密码

SID全新的账号激活流程:

1、初始密码为**随机强密码**,确保不被盗用

2、**校内、校外身份核验: 确保本人操作**

- 学工号核验、(身份证件号/手机号)
- 绑定手机
- 设置密码
- 公安人脸核验

3、自主修改密码: 刷脸核验后即可完成密码修改

带来效果:

信息中心:

- **初始强密码, 满足密码合规要求**
- **多维度精准实名核身, 杜绝冒名顶替, 满足国家政策要求**
- 学生自主完成线上密码修改, 降低信息中心工作量

学生:

- 账号不被盗, 有安全感
- 自主修改密码, 有好体验





信息网络中心
Information Network Center

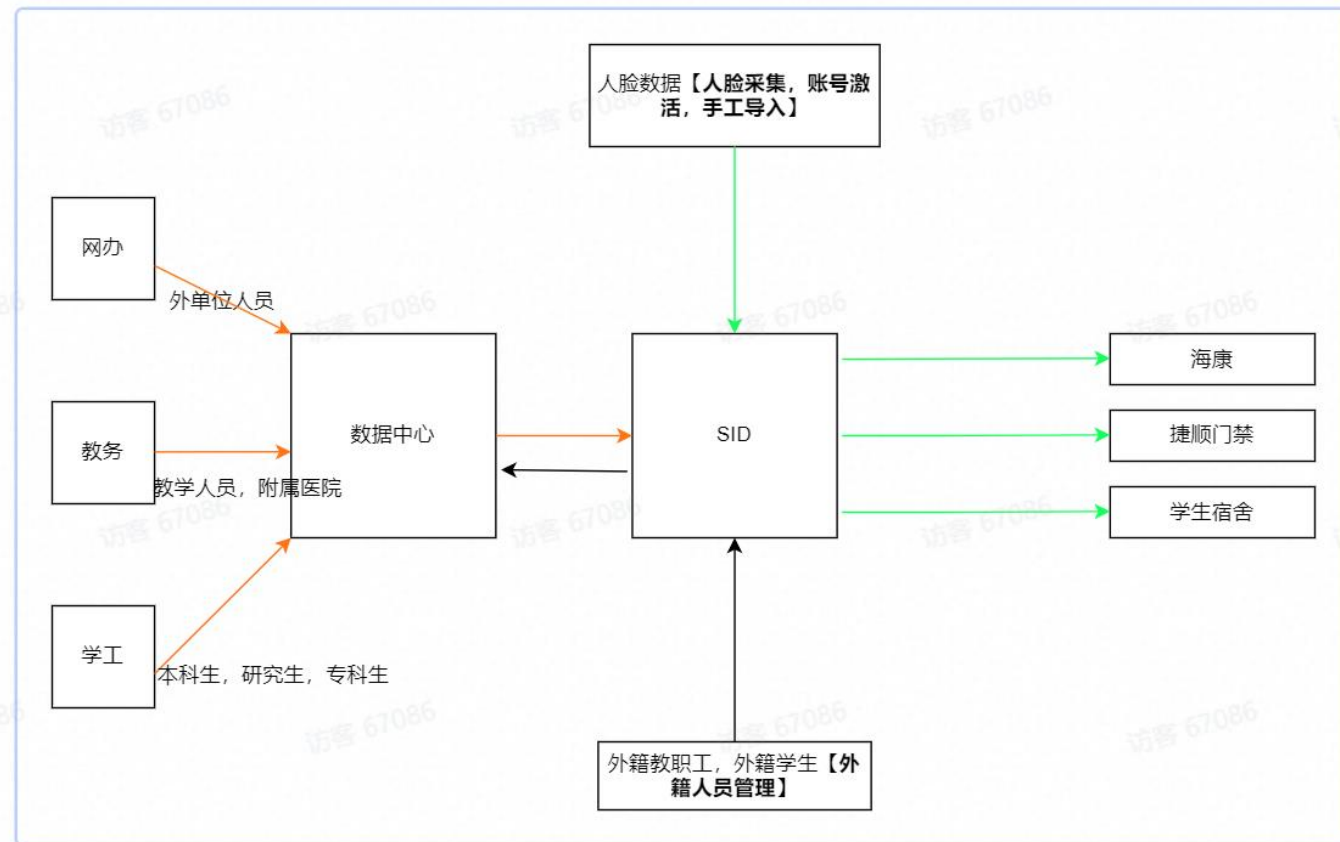
保证身份数据权威性

- 数据治理删除僵尸账号
- 人脸数据权威源比对
- 外籍教职工身份信息统一管理



身份数据统一管理

成都大学身份数据流向图





Source ID 下一步应用



信息网络中心
Information Network Center

近期计划

- 借助多身份功能进一步提高账号数据准确性
- 应用标签实现用户接入网络和VPN的精细化管理

长期计划



信息网络中心
Information Network Center

- 应用SID授权功能探索建立校内应用的统一授权体系
- 挖掘认证日志数据为用户画像服务
- 挖掘认证登录数据探索建立轻量APM系统

成都大学身份认证实践分享



信息网络中心
Information Network Center

谢 谢