智慧身份平台建设实践分享

——深化人员生涯治理 支撑业务实时响应

信息技术中心：郭炜杰

目录

CONTENTS

浙江理工大学 “十三五”信息化建设回顾

“十三五”期间，我校深入学习贯彻习近平总书记关于**“没有信息化就没有现代化”、“没有网络安全就没有国家安全”**的重要讲话精神。结合教育部**《教育信息化2.0行动计划》**、**《浙江省教育信息化“十三五”发展规划》**和**《浙江理工大学改革和发展“十三五”规划》**等要求，以推进“最多跑一次”改革和建设“幸福浙理”民生工程为契机，在网络和信息化基础设施建设、信息系统建设、信息化支撑和保障教学科研生活服务等方面取得了跨跃式发展，信息化工作取得显著成效，师生体验感、获得感、幸福感、安全感显著增强。

浙江理工大学召开
“最多跑一次”改革工作会议

十三五智慧校园建设成果

信息化体制机制逐步建成

- 成立学校网络安全和信息化领导小组
- 逐步形成“统一领导、归口管理、分级负责、协同推进”的信息化工作机制

信息化支撑能力日益增强

- 建立私有云平台，集中部署、统一管理
- 网站群、浙理云盘和视频会议系统
- 信息化系统覆盖全校主要业务，形成“移动办公、掌上办事”格局

数据中心建设成效初显

- 完成数据中心系统平台建设，打破数据壁垒和孤岛。
- “数据多跑路，师生少跑腿”。

校园一卡通功能不断丰富

- 引进社会投资，完成一卡通系统升级改造
- 虚拟卡、人脸支付、门禁、门锁
- 不断扩大一卡通应用邻域和范围

校园网络基础设施日趋完善

- 校区高速无线网络全覆盖，无线为主、有线为辅
- 建成“万兆光纤骨干，千兆铜缆接入”的高速校园网络系统
- 安防、一卡通、标准化考场等智能专网

信息技术助力“最多跑一次”改革落地

- 建成网上办事大厅、掌上浙理移动应用平台、自助服务大厅，师生办事更方便更快捷。

网络安全体系初步成型

- 做好G20、十九大、国庆、建党百年等重要时期网络安全技术防护工作
- 做好网络安全相关运维、监测、预警、风险评估和等保测评
- 完善网络安全体系，建立网络安全通报机制

临平校区智慧校园建设有序开展

- 推进临平校区智慧校园整体建设
- 谋划新校区“智慧、时尚”的信息化顶层设计理念
- 实现校区智慧管理和服务的数字化转型

目录

CONTENTS

关键要求 - 统一身份平台是支撑学校信息化建设的关键

一、校园主要业务围绕身份开展

- 人靠身份取得校园活动的凭据
- 财靠身份执行各项财务制度
- 物靠身份管理固资并为不同身份的人员提供服务

二、智慧身份“两面”，身份全互通，账号智慧授权

- 基本面：
  - 身份认证，认证统一，全互通
  - 实名核验，人脸库内部+外部双重核验，准确性、合法性、安全性
  - 数据治理，信息准确、完整、可靠、规范
- 智慧面：
  - 多身份多ID，基于多身份的自动授权、一键授权，及时高效
  - 多身份多ID管理，人员多标签管理，找人快，易管理

身份ID多元多态、认证大互通、一键授权、智慧授权是关键趋势

问题分解 - 具体还有哪些问题?

缺乏统一权威数据源，人员状态变更同步不及时

校内人员**身份类型多，不同身份的账号对应有不同的权威数据源系统**，如在编教职工由人事系统管理，本科生由教务系统管理，账号体系和编码规则各不相同。

用户实名核身难，密码找回不便

1、新用户没有做过实名核身，不确定登录的账号是否被正确的人使用。

2、用户**忘记密码**，但原先绑定的手机号已注销，无法通过手机号来重置密码。**走申诉通道，用户操作繁琐，而且每个申诉都要管理员人工核对身份信息。**

同人有多身份/多账号

1、**同一时期多个身份，如本校老师读本校在职博士；不同时期多个身份：本校本科毕业读本校研究生。**

2、同一个人不同身份就要用不同的账号登陆不同的业务系统。

3、一个人只有**一个手机号码，只能和一个账号绑定。**需要统一身份认证系统的管理员干预,把手机号码从本科生账号解绑，再绑定到研究生账号上，增加了时间成本。

弱密码问题普遍

1、**默认初始密码**用**“身份证末6位”**，存在弱密码风险，不符合网络安全要求。

2、默认初始密码使用**复杂随机密码,存在如何告知用户的问题**

3、弱密码一旦被盗用修改以后，申诉修改密码繁琐。

临时人员开户，缺乏统一管理和回收

临时人员种类多，如挂职干部、访问学者、培训人员、外聘教师、客座教授、评审专家等，临时人员有使用校内业务系统的需要，这类人员目前**没有统一归口系统在管理，目前做法是需要用哪个系统找那个系统的部门，在业务系统里单独开账号。权限和账号开通使用管理混乱，回收不及时存在安全隐患。**

人员生涯状态变化，业务不联动

1、人员离校后账号的管理和系统联动还存在不足，**教职工离职、退休、学生毕业，账号不能跟着人员状态的变化马上停用，需要延期使用一段时间。**

2、非编人员、临时人员管理未形成闭环，离校手续不完整，业务系统上**人员状态更新不及时，存在安全隐患。**

实践计划 - 统一身份平台建设路标

2019

基础软件平台

- 统一身份认证，其他业务系统单点登录对接
- 组织和用户管理
- SID和SAM上网认证等系统的账密统一

平台初见雏形

业务持续精进

2020

持续解决了诸多问题

- 完成两次迭代升级。
- 密码安全易用性管理
- 人员和组织标签管理
- 组织和人员信息优化

2021

1.9 实验局全人员/全生涯

- 身份数据治理
- 临时人员管理
- 多身份多ID体系
- 全生涯管理，生涯事件流
- 多身份ID在线切换
- 账号激活，刷脸找回密码

建立全生涯多场景访问体系

需求编号	标题	需求提出人	解决版本	需求达成状态
REQ-70	密码框中的眼睛图标需要写成文字，老教师不知道图标是什么意思		R1.5.1版本已解决，已部署到线上	已达成
REQ-69	密码输入框禁止输入中文		R1.5.1版本已解决，已部署到线上	已达成
REQ-76	【微信】微信绑定弱密码没绑定成功需要再次绑定		R1.5.1版本已解决，已部署到线上	已达成
REQ-73	用户身份状态可配置(字典在页面可配置)		R1.6.0版本已解决，已部署到线上	已达成
REQ-61	自助修改密码需要发送验证码		R1.6.0版本已解决，已部署到线上	已达成
REQ-87	【树表】人员管理， 所在单位， 要默认选中二级部门， 而不是岗位上面的部门（岗位上的部门没有意义）		R1.6.1版本已解决，已部署到线上	已达成
REQ-88	【访客管理】人事招聘，外部人员会点击应聘链接进入，这时需要注册账号，需要身份平台管理这个入口和此类人员的信息。		R1.6.1版本已解决，已部署到线上	已达成
REQ-75	强制修改密码页面会有滚动条（郭老师建议去掉）		R1.6.3版本已解决，已部署到线上	已达成
REQ-76	【Isni认证】SourceID支持Isni认证对接		R1.6.3版本已解决，已部署到线上	已达成
REQ-80	【安全漏洞修复】1、暴力破解；2、水平越权。		临时版本，已解决，已部署到线上	已达成
REQ-90	手机端页面功能（认证页面、忘记密码、完善用户信息、强制修改密码）		R1.6.3.5浙江理工专项版本已完成部分功能，已部署到线上。 R1.6.4版本已完成，目前已部署到线上	已达成
REQ-107	提供一个所有人员的用户管理界面，在只知道学工号的情况下，直接能找到具体人		R 1.6.4版本已解决，已部署到线上	已达成
REQ-103	浙江理工需求要修改为“初始密码为身份证号后6位，末尾为字母X的要大写”，或者通告可以配置为默认展开， 在通告里面告知		R1.6.4版本已解决，已部署到线上	已达成
REQ-96	提供一个所有人员的用户管理界面，在只知道学工号的情况下，直接能找到具体人		R1.6.4版本已解决，已部署到线上	已达成
REQ-95	绑定手机总人数、学生数和老师数， 这类信息， 后台要展示出来			已达成
REQ-94	人员管理搜索结果点击查看再返回后，搜索结果不保存，回到了全部人员列表，非常不方便		R1.6.4版本已解决，已部署到线上	已达成
REQ-93	浙江理工需求要修改为“初始密码为身份证号后6位，末尾为字母X的要大写”，或者通告可以配置为默认展开， 在通告里面告知		R1.6.4版本已解决，已部署到线上	已达成
REQ-160	浙江理工 --让老师看到、理解“SSO密码后，VPN、邮箱、WIFI密码会同步修改		已拉分支解决，部署到线上	已达成
REQ-156	浙江理工。临时人员用户数据从数据中心采集需求		汉青已实施解决	已达成

全场景价值落地计划

关键里程碑	状态	计划完成时间	实际完成时间
升级前数据治理完成	已完成	2021/8/20	2021/8/20
1.9版本现场升级	已完成	2021/8/25	2021/8/25
新生账号激活实名认证大规模使用落地	已完成	2021/8/31	2021/9/2
教工离职，但仍需在校内工作一顿时间落地	已完成	2021/9/3	2021/9/3
多身份切换落地	已完成	2021/9/3	2021/9/3
刷脸找回密码落地	已完成	2021/9/5	2021/9/5
生涯事件流支撑离退休人员延期收回权限落地	已完成	2021/9/7	2021/9/7
根据生涯状态规范配置不同身份类型和状态的用户可以认证和授权的应用梳理	已完成	2021/9/7	2021/9/7
1.9版本升级后数据治理完成	已完成	2021/9/10	2021/9/10
所有老生密码为弱密码的修改成随机密码，强制走账号激活	进行中	2021/9/30	2021/9/30
半委托授权（角色映射）价值场景落地	完成	2021/10/29	2020/10/29
临时人员/访客管理	完成	2021/11/3	2021/11/4

身份数据质量现状分析

组织身份类型	教职工	本科生	研究生	非编人员	临时人员	合计
账号数量	3503	86421	16451	620	486	107482

身份ID异常情况

证件号增加前缀或者后缀：487

学号是证件号的：185

工号是证件号的：180

学工号为手机号：2493

学号不符合规则：0

工号不符合规则：289

姓名、证件类型、证件号异常情况

姓名连续包含两个空格及以上： 756

证件号与证件类型不匹配：570

证件类型缺失：6

用户单位部门不存在：77

证件号大于18位：541

相同证件号，姓名不同：190

相同证件号，手机号不同：180

密码异常情况

初始密码用户数：9252

弱密码用户数：4252

身份数据质量的完整、准确，可靠、规范、连贯是**全人员身份可信，全生涯访问管控**的关键保障

生涯连贯质量 待治理

（1）学校共有5种身份类型，5种类型人员生涯均未闭环。

（2）多身份共有4252人，多身份账号9000多，无法进行生涯连贯。

账号安全质量 待治理

- 密码符合安全要求的占 98%
- 手机绑定率 29%，外籍人士中仅8%已绑定
- 仍为初始化密码的账号占 71%
- 无有效生涯状态支撑判断是否该失效

生涯数据质量 待治理

- 教职工分类清晰，状态信息明确
- 本科生状态未细分，占总体账号 **61%**
- 研究生状态多达 **13个**，包含多个重复状态
- 与实际组织对应不上关系的约 **77** 人
- 临时人员账号基本无状态管理

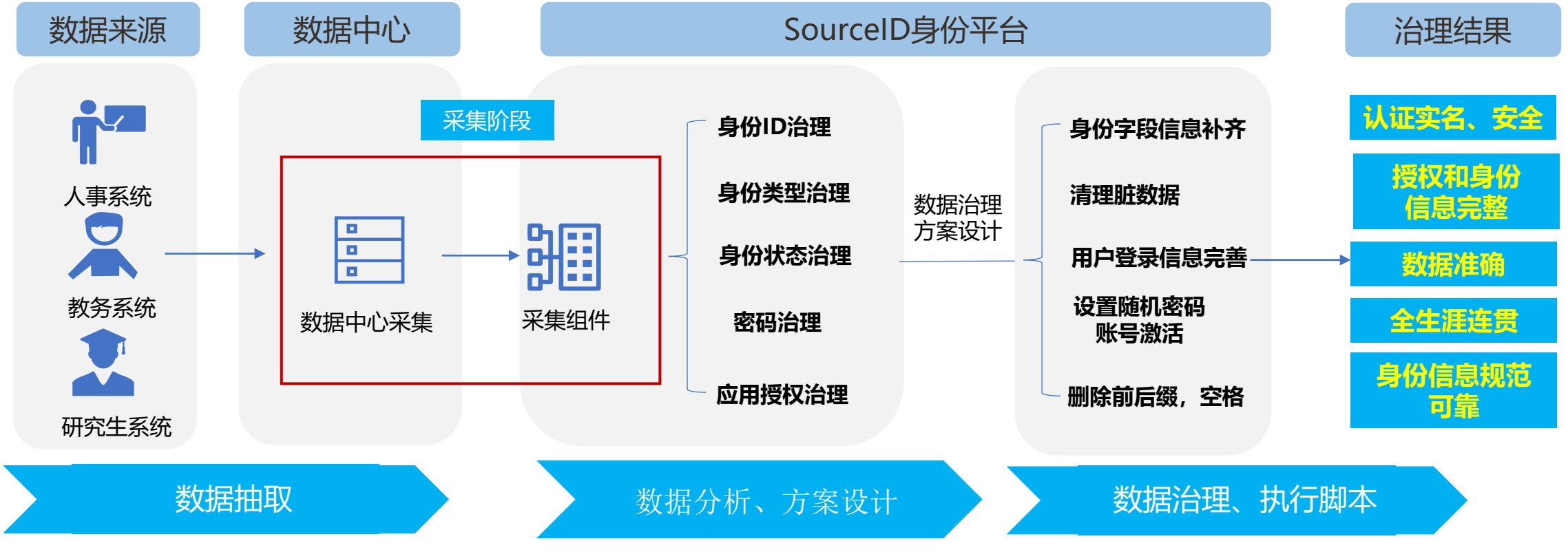
通过数据治理打造可靠数据中枢

身份数据治理

1、通过数据中心补齐部分个人信息，结合脚本处理不规范、不准确的用户信息，确保所有人的信息完整，安全，可靠，准确，规范。

2、用户首次登录时需要修改不符合密码强度规则的密码；或者设置随机密码走账号激活彻底解决弱密码问题。

3、多账号信息采集进行同人合并，多账号密码合并，构建多身份多ID身份体系。



SourceID通过身份数据治理夯实数据基础，增强业务流转中身份数据的“可信度”、“准确度”、“连贯度”

构建全校人员身份标准和生涯状态

自然人身份标准

人员	状态	ID	操作
自然人	正常 下落不明 死亡	SID 身份证号 港澳居民来往内地通行证号 港澳居民居住证号 台湾居民来往内地通行证号 台湾居民居住证号 护照号 绑定手机号 人脸照片 微信ID 企业微信ID 微信入网ID 微信扫脸ID 微信公众号ID 钉钉ID 动态口令ID 第三方oauth ID 企业微信内应用ID ISNI 飞书ID 其他	标

学生身份标准

学生	博士研究生	13	新生 已报到新生 休学生 保留入学资格 出国 已转段 未注册老生 在校生 放弃入学资格 毕业生 退学 死亡 转校 取消入学资格
	硕士研究生	03	新生 已报到新生 在校生 未注册老生 休学生 出国 保留入学资格 放弃入学资格 毕业生 已转段 退学 死亡 转校 取消入学资格
	本科生	02	有效在校生 其他 在读 休学 停学 复学 保留入学资格 公派出国 保留学籍 退学 流失 毕业 结业 肄业 转学(转出) 死亡 开除 下落不明 取消入学资格

教职工身份标准

分类	组织身份类型	代码	状态
教职工	在编教职工	01	在职 返聘 延聘 待退休 调出 退休 离休 死亡 辞职 离职 开除 下落不明 离退休
	非编教职工	04	在职 返聘 延聘 待退休 调出 退休 离休 辞职 离职 开除 下落不明 离退休 死亡
	博士后	20	在职 返聘 延聘 待退休 调出 退休 离休 死亡 辞职 离职 开除 下落不明 离退休

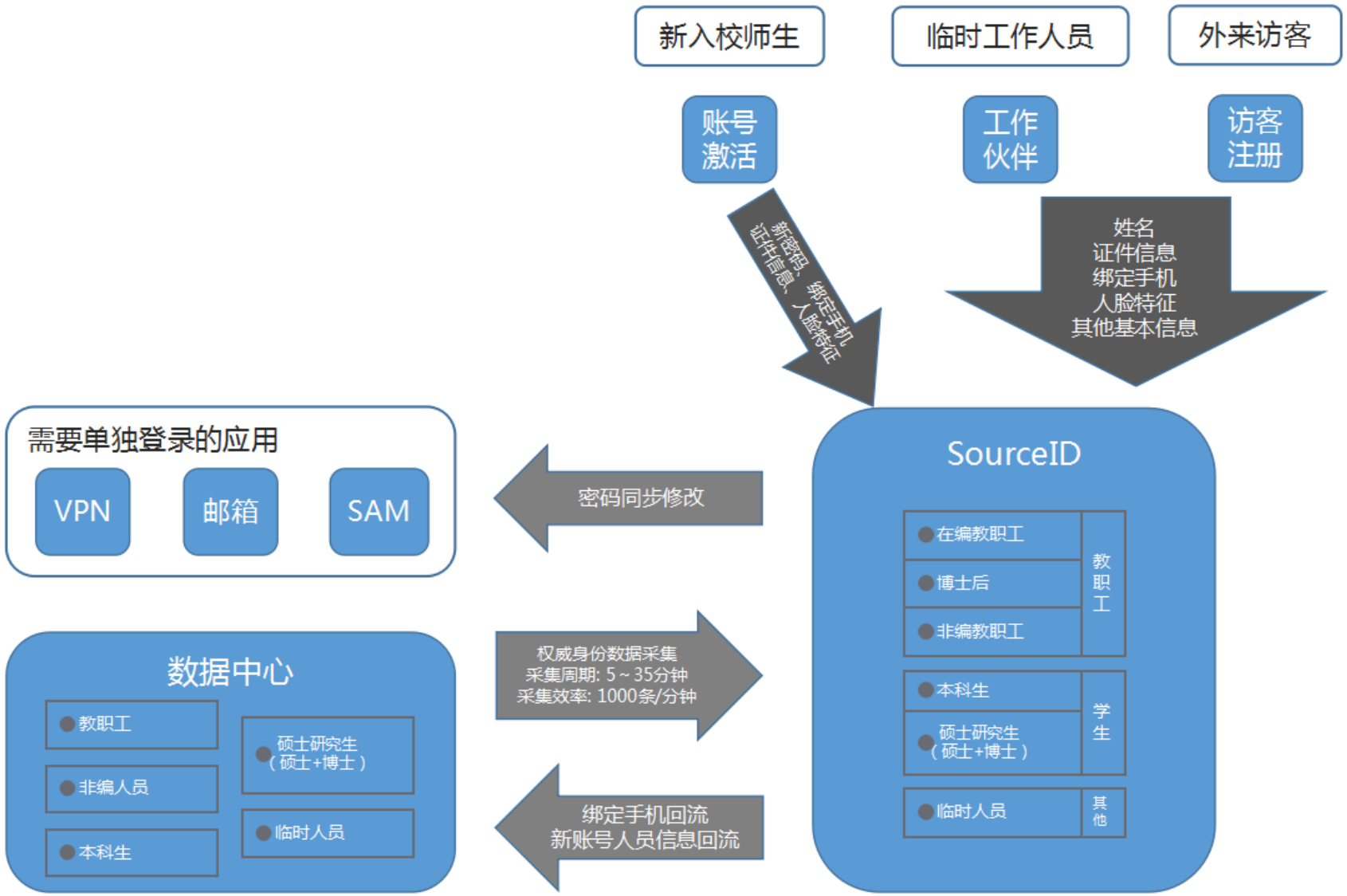
其他人员身份标准

其他	临时人员	05	在校 离校
	座客教授	21	在校 离校
	访问学者	22	在校 离校
	外聘行政人员	23	在校 离校
	外聘教学人员	24	在校 离校
	挂职干部	25	在校 离校

SourceID通过生涯ID体系理顺了校内“全人员”的身份，建立了清晰的身份标准

整体业务数据流向分析

数据流向示意

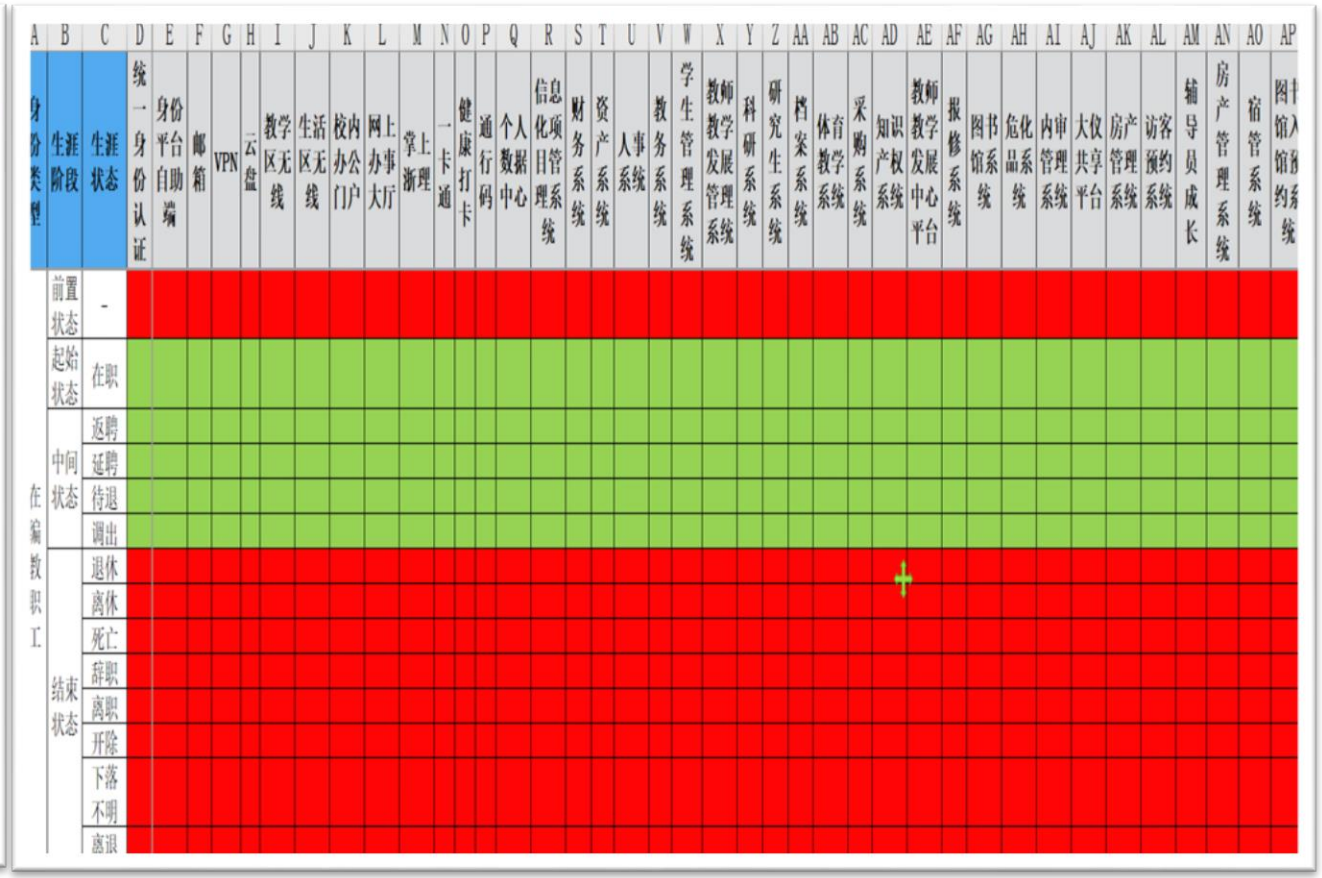


全生涯状态联动访问控制体系

生涯状态访问控制联动

生涯联动认证

生涯联动入口授权



基于身份标准和生涯状态管理，身份分类、准确精细地支撑认证和授权，精准把握了人员状态，使得业务联动响应更及时、更高效

工作伙伴轻应用，支撑各类临时人员访问和开户

老故事

角色	职责部门	账号	是否规范
教职工	人事处	教工号	规范
学生	教务处/研究生院	学号	规范
挂职和客座教授	用人归口部门	各系统开独立账号	否
其他临时人员	无	无	否

老的实现方式：

✓ 人事处管正式教职工，教务处管正式学生，用人部门或对接部门**开证明到业务部门在业务系统上单独开账号，办理周期长，需要来回跑。**

✓ 其他临时人员如访客虽有访客预约系统，但实际上没有做身份核验

根因：

信息部门：其他人员类型和数量不清楚、每种类型人员需要的权限不明确；权限到期不能回收、沉淀账号引发安全问题，管理困难；

业务部门：缺乏系统流程支撑，权责不清晰，人员账号管理混乱。

用户：开号麻烦，需要去各部门协调；开权限的周期长，影响工作开展，体验不好；

新故事

新的实现方式：

工作伙伴轻应用支撑：

1. 在SID人员标准中设置其他人员的组织身份类型，有上网，访问系统的权限，设置老师临时账号有效期，如6个月，身份到期，账号自动失效。
2. 其他人员扫码自助注册统一身份认证账号并进行实名核验（实名可选）。
3. 对应的业务部门进行审批。
4. 账号开户成功，可顺利访问业务系统。

业务部门、信息中心梳理相关标准；

临时人员扫码注册

业务部门审核
信息部门审核

其他人员类型（5类）	客座教授	访问学者	外聘行政人员	外聘教学人员	挂职干部

带来效果：

1.**信息部门**：全面梳理其他人员身份类型，给其他临时在校工作人员合理的校内身份，账号开通、回收及时、准确；

2.**业务部门**：提供人员管理规范，信息部门提供技术支撑，技管分离、权责分明；

3.**临时人员**：自助扫码注册+实名核身，获取相关权限，方便快捷，高效、及时，提升用户体验；

规范临时人员管理，账号快速开通和回收，账号使用可控可管

新生开学账号实名激活，去弱密码身份更安全

老故事

场景：

新生进校后需要激活自己的统一身份认证账号。使用校园无线网。

老的做法：

- 在校用户存在大量采用身份证后6位作为密码；
- 账号激活通过线上申诉流程完成，给信息中心管理员带来了额外的巨大工作量。

问题：

1. 根据统计共**107482**历史账号，其中有76691为初始密码或者身份证后六位弱密码，初始密码弱强度会引发安全问题。且无法通过护网行动检查。
2. 默认密码导致账号可能被冒用，不安全；通过申诉来激活账户，给管理员带来了大量的工作量，人工耗费大。
3. 如何防止冒名顶替等特殊情况。

新故事

新的做法

- 新生账号采取随机高强度密码，学生需要走激活流程才能使用账号
- **校内核验：**工号+姓名+身份证件类型+身份证件号+人脸核验
- **校外核验：**公安实名核验（姓名、证件类型、证件号、人脸）

Portal 登录账号激活

学校微信公众平台账号激活

关键价值

1、新生入学/新教工入校更好的账号体验方式，快速，实名，安全

2、实名核身新生的真实，公安背书，杜绝冒名顶替的情况。

3、去除所有弱密码情况，满足等保要求和安全合规检查。

密码找回从分钟到秒级，刷脸让密码管理更简单

老故事

场景：

- 采用账号+密码的方式进行认证，如果忘记密码，采用手机号+动态验证码的方式登录，并重置密码。
- 部分用户原手机号已注销，需要绑定新的手机号码

老的实现方式

账号申诉流程：

✓ 师生扫描二维码进入申诉，在统一身份平台提交申诉流程。

✓ 在申诉流程里面上传个人，个人身份证、照片、学号、姓名等信息。

✓ 管理员比对，审核确认，新的手机号会绑定到学工号上，学生可以使用新的手机号码+动态验证码登录和修改

问题

- 信息部门每天都要处理，对提交信息进行严格比对审核，耗时耗力，影响部门正常业务流转
- 师生需要提交流程和催办，等待时间长，影响师生正常登录业务系统

新故事

新的解法：

- SourceID支持刷脸重置密码，静默活体检测保证人脸准确性。
- 同时提供用户多种找回密码的渠道，如手机号验证码、申诉找回密码

密码找回

多种找回方式

密码重置

带来效果：

1、增加人脸找回密码方式，用户可以自助找回密码，避免通过申诉找回，效率低的问题

2、提升了信息化部门快速响应师生密码服务的能力，提升了用户体验

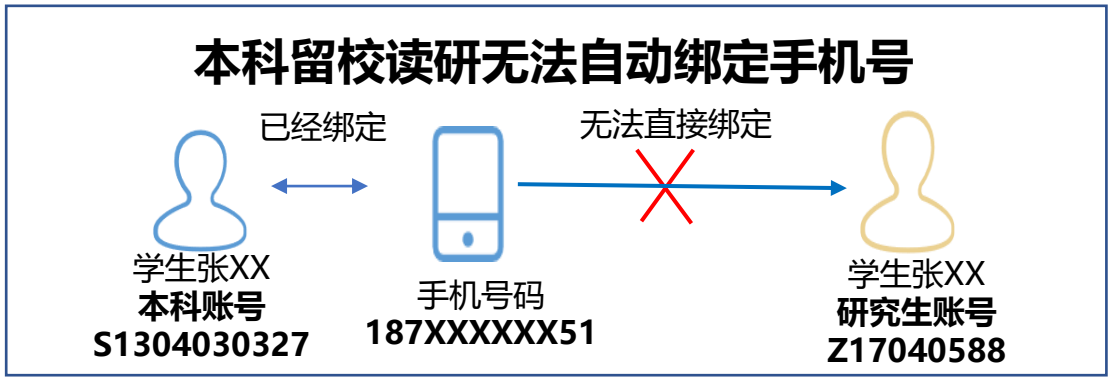
多身份ID体系，助力本科留校读研账号快速使用

老故事

场景：

1、本科生报考本校研究生，会有一个研究生学号。

2、一个手机号码只能绑定一个学工号，所以研究生账号无法绑定其原有的手机号。



老的解决方式

- 持本人证件到信息部门进行本科账号和手机号解绑；
- 手机号重新绑定研究生新账号；

问题：

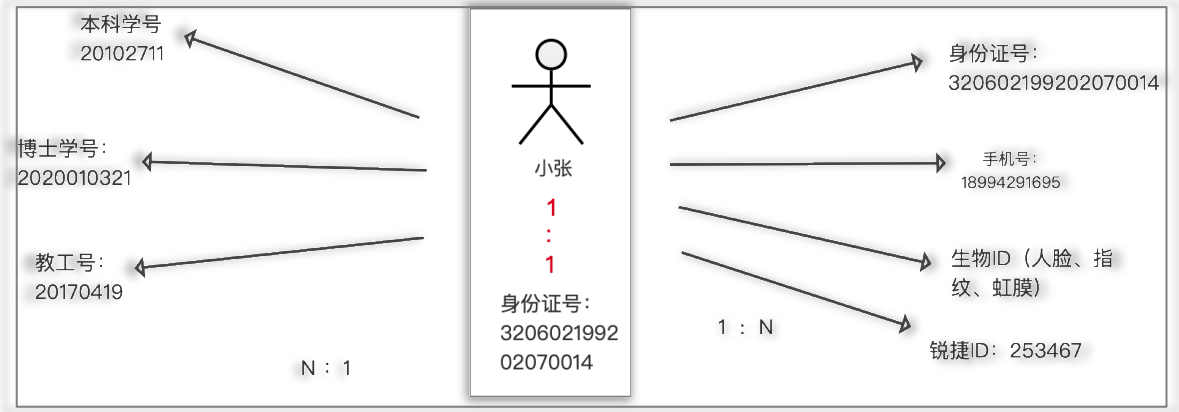
1、信息部门需要核实，并帮学生手工解绑，时间紧，且频次较高。

2、影响学生正常使用，无法快速使用账号，办理需要来回跑。

新故事

新的解决办法：

1. 重新定义了ID体系，将手机号、证件号等作为人ID，不同的校内身份拥有不同组织ID，**身份随人。**
2. 一个人可以绑定多个组织身份ID，利用数据合并的方式将本科和研究生的账号均挂靠同一个人身上，无需反复解绑和重新绑定。



学生张XX

身份证号
412822XXXXXX26666
手机号
187XXXXXX51
本科账号（已失效）
S1304030327
研究生账号
Z17040588

关键价值：

- ✓ 手机号直接绑定在自然人身上，当毕业留校读研的时候无需解绑、重新绑定，直接可以使用新账号。
- ✓ 信息中心无需再人工解绑，省时省力。

多身份ID账号在线一键切换

老故事

场景：

- 老师在校内有多个身份，既是教职工又是研究生或者博士生，使用多个账号，身份切换需要频繁登入登出使用，比较麻烦
- 根据统计多身份账号数9252，多身份用户数4252，需要记忆多套账号密码；

一人多身份/多套账号密码

姓名	学工号	身份
李老师	研究生学号	博士研究生
	工号	教职工

问题

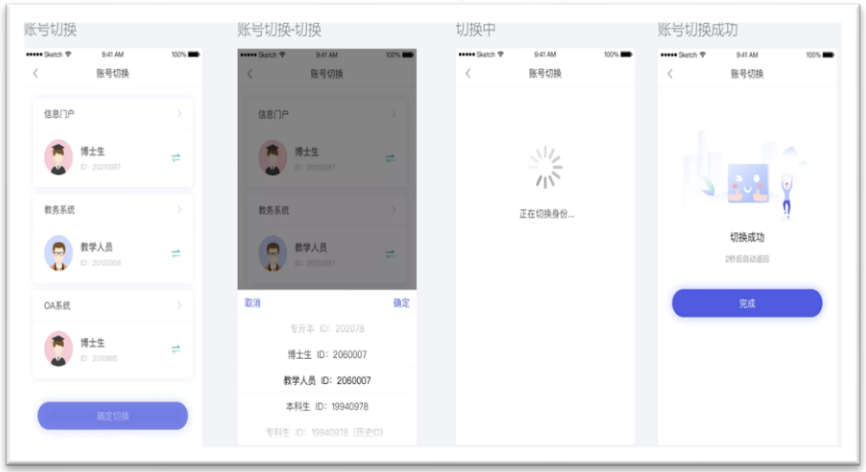
- ✓ 频繁地登入登出来切换身份登录，麻烦，用户体验差；
- ✓ 需要记忆多套账户及对应的密码。

新故事

新的用户体验：

- 用人ID，如手机号，选择不同的身份进入系统；可切换使用
- 用身份ID，如教工号，直接进入相应的身份

在线多ID切换



历史身份ID访问历史数据

带来的效果和价值

- 多身份教师和学生无需登出频繁切换账号，可一键切换身份。
- 可以快速精准查询历史身份账号信息。

教职工生涯事件流，离职自动精细化访问控制

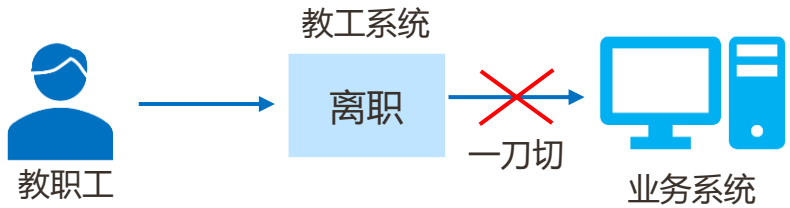
老故事

场景：

教职工基本信息在人事系统里维护，当教职工离职后，人事系统里会将人员状态变更为离职，随即就不可以访问应用系统了。

要求：

教师聘期结束、退休、或者离职的教职工，还需要在校工作一段时间，有些会长达几个月甚至半年。



教工离职，之前做法一刀切

- 教职工发现自己无法进行统一身份认证，到信息中心找管理员来重新开通原来的账号。
- 信息中心的管理员对于这部分已退休或聘期结束还需要用账号的人员，手动将他们的已经失效的账号延长一段有效期，让他们可以继续使用

问题

- ✓ 用户权限被一刀切了，需要人工配合特定场景调整认证授权策略，麻烦且工作重复。
- ✓ 调整不及时，办理时间长，会影响老师业务办理。

新故事

新的做法：

1、SourceID自定义生涯事件流，教职工离职可继续认证7天，同时发送短信通知告知本人，需要到学校网办重新走账号延期使用权限流程，设置延期时间同步给SourceID。

2、生涯事件流触发条件为：“在编教职工状态”变为“离职”时，触发执行。

3、执行动作：调整认证权限，允许继续认证单点登录时间为180天（可设置）。

生涯事件名称	触发条件	响应动作
离职教职工可以继续使用统一身份认证1周	“在编教职工状态”变为“离职”	允许全部ID认证7天
离职教职工继续使用统一身份认证生涯事件	“在编教职工状态”变为“离职”	调用“短信发送服务”
在编教职工离职延长账号有效期半年	“在编教职工状态”变为“离职”	允许部分ID认证180天

关键价值：

通过自动的精细化访问控制来匹配人员的特殊场景需求，及时、准确、便捷地调整认证、授权策略。

实践价值汇总

临时人员/访客管理

工作伙伴轻应用：解决临时人员管理，开账号开权限来回跑问题！

刷脸登录/修改密码

账号激活，实名核身：解决密码忘记，手机号注销申诉需要到信息部门来回跑的问题。

全人员身份数据治理

身份数据治理：数据准确，可靠，实时同步，解决数据不流通，账号无法登录，信息部门和用户来回跑问题。

建立生涯多ID体系

生涯多ID体系，多ID在线切换：解决多身份用户手机号解绑，需要重新绑定，到业务部门和信息中心来回跑问题

构建师生身份生涯规范，生涯访问控制

解决生涯状态不联动，**师生身份状态变化，业务不联动，需要来回确认，审批，开通办理等问题**

生涯事件流

实现生涯状态变更时触发事件流。**解决教职工离职账号和权限一刀切特殊情况，开通账号和权限还需要来回跑问题。**

深化人员生涯治理，提升业务响应效率；实现用户业务**办理跑一次，到一次不跑！**

目录

CONTENTS

下一步规划和设想

短期计划

- 实现SAM网络认证，所有业务系统访问统一单点登录。
- 通过工作伙伴注册的临时人员信息，快速且及时回流到数据中心和应用。
- 继续梳理生涯事件，基于身份状态变化，如学生毕业，教职工离职等产生的生涯事件，联动网办大厅，流程平台，消息平台，人脸等应用触发认证和权限的自动变化。
- 借助身份平台的数据治理能力，进一步提高学校师生账号数据准确性，完整性，可靠性，规范性，连贯性。
- 通过身份平台的多维度身份标签，实现用户接入网络和VPN的精细化管理。
- 企业微信的群组推送，企业微信内应用免认证。

长期计划

- 应用SID授权功能探索建立校内应用的统一授权体系
- 结合人脸应用，构建学校统一的人脸库管理平台。
- 通过SourceID身份中台构建学校统一的组织中心和用户中心

感谢聆听

THANK YOU