身份管理

www.ruijie.com.cn

高教身份中台建设白皮书

如有疑问
扫一扫在线咨询

Ruijie 锐捷 Networks

寄语

福州大学网络安全与信息化办公室主任 岳志强

高校信息化因用户而产生身份、因身份而办理业务、因业务而生成数据、因数据而导致混乱、因混乱而大力治理，锐捷的SourceID在发展中提纲挈领、去繁存简，抓住高校数据治理的痛点，以身份中台进行切入，类同于将思维导图嵌入高校信息化平台中，将身份、业务、数据这三者有机统一，可以让高校信息化数据真正用起来、活起来，为高校进入DT时代夯实了基础。

西南大学信息化建设办公室系统运维部主任 钟剑

在推进高校数字化转型过程中，高校师生员工的数字身份变得越来越重要，数字身份的管理及服务也变得越来越复杂。锐捷高教身份中台立足“身份”基点，以聚合身份数据、抽象身份业务、提供身份服务为途径，形成全身份通达、全生涯服务、全业务赋能的三“全”数字身份“一站式”解决方案，能有效解决高校数字化转型过程中师生员工数字身份管理及服务的难点和痛点问题。

温州大学信息技术中心副主任 姚渺波

随着学校数字化改革的不断深入，越来越多的跨部门、多业务协同应用场景被构建，成为数字化改革牵一发动全身的重要抓手。而这种校内外跨部门多业务的联系势必要引入大量的身份类型，不仅包含师生，还有诸如校内商户、合作伙伴、校外访客等其它身份类型。锐捷提出的身份中台不仅从全人员、全生涯的角度解决了上述身份问题，创新性地利用半委托授权的方式解决了角色孤岛的问题，还通过人脸底库、群组等能力复用的方式提升了应用在业务管理、业务办理和业务服务等方面的效率。希望能够有更多像锐捷身份中台这样切中学校信息化痛点的解决方案，从而助力学校治理体系和治理能力现代化。

前言

从“功能”到“服务”，教育数字化转型的新时代已到来

从上个世纪90年代开始，高校作为教育信息化的排头兵一直不断推进各类建设活动，从最基础的“应用信息系统建设阶段”到“数据交换与共享平台建设阶段”，再到更深入的“面向服务、数据治理阶段”。本质上是从“烟囱式” 到“共享式”的跨越， 高等教育体系的数字化转型已初见雏形。随着教育信息化2.0的到来，开启了教育信息化的“智能时代”；另一方面立足“十四五”的新起点，更安全、更高效、更开放的高质量信息化发展建设已经扬帆起航。

不论是从大环境浪潮的背景看，还是基于校园信息化发展现状中遇到的痛点障碍，或是从技术发展的复杂度和成熟度考量，纯粹的、单一的、为了实现某种功能的基础平台已经无法满足新时代建设的目标和挑战，顺应潮流的是“面向服务、聚焦能力”的身份服务类平台。

新挑战和新机遇下，“新基建”的构建势在必行。

中台思维是提升校园业务服务与管理效率的核心手段

身份数据资源作为智慧校园中的“软财富”，是提高教育决策与服务效率的关键所在。 然而，当前教育数据多呈现碎片化特征，距离形成完整的应用价值链还有一定的差距，业务系统之间的数据、业务、管理都相对独立。

据锐捷网络调研，79%的参与调研的高校信息化负责人认为很有必要建设一个聚焦“身份服务”的信息化能力集合平台以提升校园内各类业务办理的效率，并要重视身份数据的流向顺畅、身份质量的持续健康、数据服务能力的对外赋能；其中又有85%的受访者表示以往传统的泳道式、将业务数据隔离的建设思维亟待摒弃，需要一种“资源整合、能力沉淀”的新架构形式来应对教育数字化转型。

另外，已有近70%的参与调研学校已经部署了中台类平台，以及15%正在规划设计中。

智慧校园视域下的身份数据精细化管理是大势所趋

新阶段建设的重中之重，是如何瞄准推动高校业务数字化发展的核心驱动力。显然，数字化转型对信息技术的要求已经变成了精细化支撑能力。

在建设智慧校园的愿景下，数字化转型的实质是面向发展建设和孵化各类业务创新，以数据拉通、业务协同为特点，以大平台加微服务为主要形式。所以，无论是围绕个人发展还是组织业务创新发展，数据精细化支撑能力已成为业务数字化最重要的能力，而身份的精准、可信、全面、安全则是焦点。

目录

背景与机遇

势在必行的教育数字化转型——“十四五”规划

《“十四五”国家信息化规划》中对教育信息化的重要指导

随着 “十四五”开局，教育信息化发展迈上了新征程，教育信息化战略规划的价值日益凸显，全国掀起了研制教育信息化战略规划的浪潮。“十四五”时期的教育规划是以高质量发展为主题，坚持稳中求进的工作总基调，增强系统观念，沿着体系建设的思路推开。“十四五”规划教育方面着重需要关注三个方面（引用自《“十四五”国家信息化规划》）：

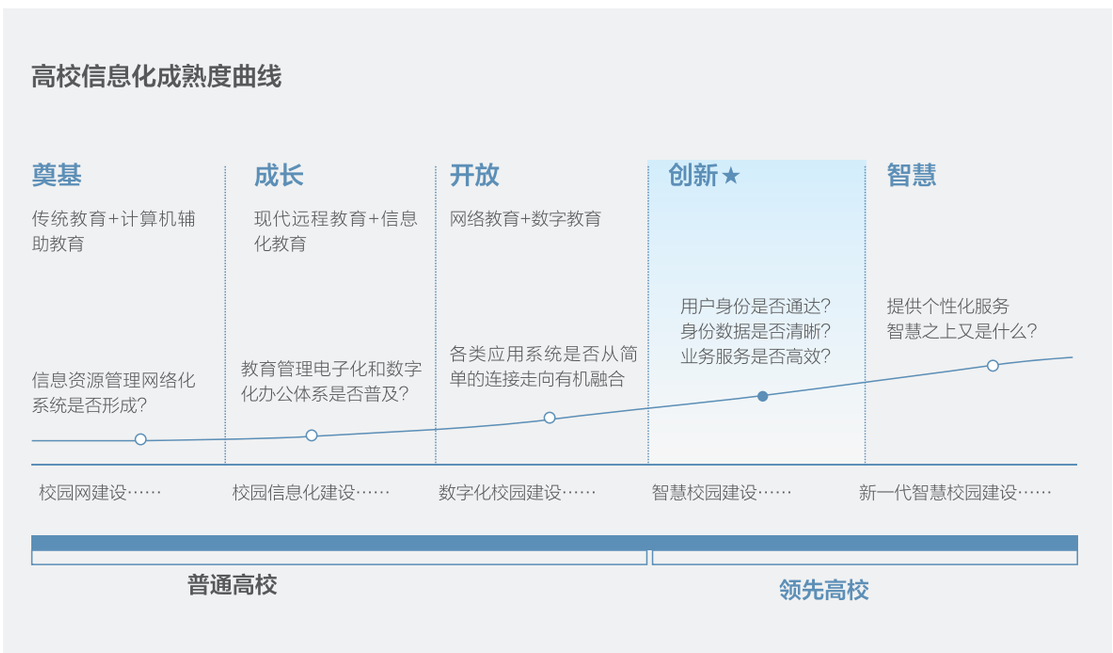
一是“立德树人”。以贯彻“三全育人”理念为主线，即“全员育人”、“全过程育人”、“全方位育人”。

二是“深化改革创新，推动教育高质量发展”。重点是要增强教育服务创新发展能力。

三是“完善终身学习体系，建设学习型社会”。构建服务全民终身学习的教育体系，形成人人皆学、处处可学、时时能学的学习型社会，是文明进步和国家强盛之基。当下，我国正处于实现中华民族伟大复兴关键时期，当顺势而为，不断学习，更新观念、升级知识、拥抱变革，才能增强与时代和发展同行共进的过硬本领。

聚焦思考：身份数据基础支撑终身数字教育

高等教育信息化建设经历了二十多年，在数字化转型的历史进程中，最有代表性的目标转变则是从数字化校园建设到智慧校园建设的愿景转变。



（来源：锐捷网络2022）

智慧校园是以物联网为基础的智慧化的校园工作、学习和生活一体化环境，是利用物联网和云计算，强调对教学、科研、校园生活和管理的数据采集、智能处理，为管理者和各个角色按需提供智能化的数据分析、教学、学习的智能化服务环境。以环境全面感知、网络无缝互通、海量数据支撑、开放学习环境、师生个性服务为主要特征。

新时代的创新建设主题也逐渐明朗：以“身份数据通达”为治理方式、以“业务高效服务”为手段、以“支撑全人员终身数字教育”为最终目标。

那么，机遇以至，如何破局？如何从容的面对各类复杂的新技术、新战略、新体系、新模式？在众多要求和挑战下，最根本和最核心的焦点一直没有变，那就是“人”。在数字化转型的视角下，即组织内用户的“数字身份”。

《“十四五”国家信息化规划》在十项重大任务中首次明确提出“开展终身数字教育”（引用自《“十四五”国家信息化规划》专家谈：加快教育信息化支撑终身数字教育-中共中央网络安全和信息化委员会办公室），从最高纲领角度表明了数字身份管理的重要性、必要性。

教育部教育信息化专家组副组长杨宗凯教授从基础能力建设、资源服务体系、大数据分析应用、信息技术融合教育变革等方面提出了独到、明确的解读：

- 以数字为基础对校园建设管理进行运营、决策，赋予智慧化重要设施和基础能力；
- 基于不断完善的师生画像，智能识别师生的需求和关注点，智能匹配和推送服务，实现从“人找服务”到“服务找人”；
- 基于大数据变革现有学习方式，促进个性化学习。教育组织要建立大数据共享机制和数据治理的标准规范，并建设大数据基础平台；
- 构建“招生、学习、就业全生命周期导学服务和课程评价、专业评估、专业认证、教师发展”自闭环的质量保障体系。

不难看出，“数据基础”、“个性化”、“终身学习”、“数字服务体系”是其中的高频词。

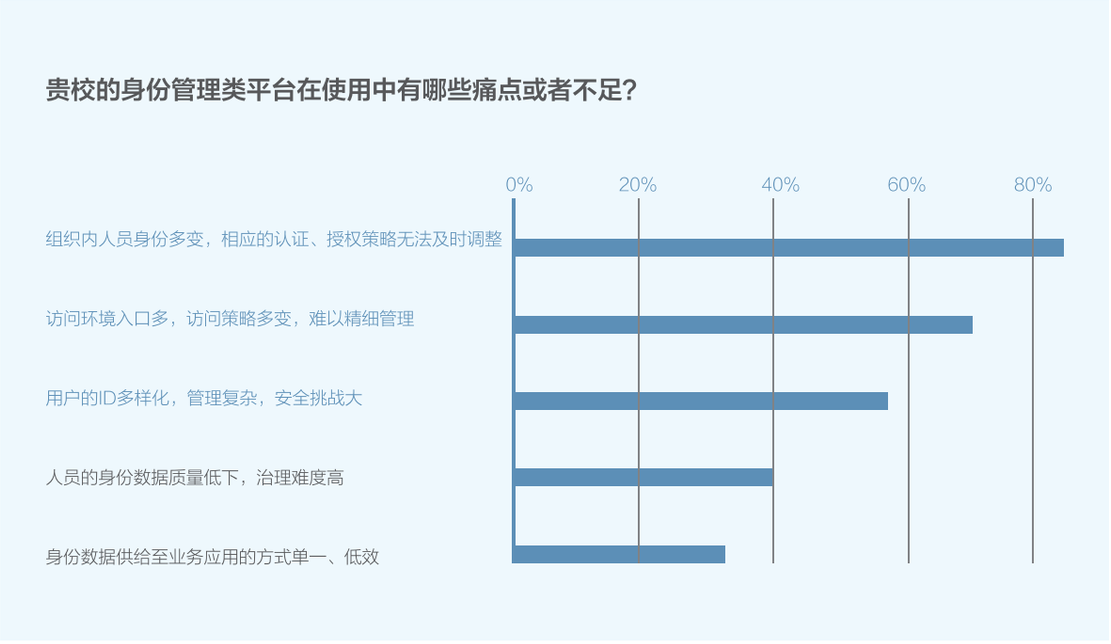
另一方面，“十四五”期间，号召加快数字化发展，大力发展数字经济。数据成为推动经济发展关键的生产要素，数字基础设施成为新的基础设施。高校作为高等人才的培育聚集地，数字化需始终以人为中心，在数字领域相对应的则是围绕着人员数字身份的各类数据建设：如何从技术和机制上做到对校内外不同领域、不同层级组织、不同业务体系中的身份数据进行汇集、整合、治理、赋能、复用，如何解决目前“身份数据不好用、不够用、不敢用、不会用”的问题，是制约发展的两大核心思考。

制约教育数字化快速建设的因素——业务管理、办理、服务的效率

教育数字化转型中的新架构、新思路、新做法层出不穷，各大高校都依据自身的建设目标、发展现状、制约条件等等不断尝试和优化。万变不离其宗，针对实际业务中出现的痛点问题进行归纳、反思、抽象是提出任何解法思路前最重要的前提。

当前高教信息化基础平台面临的三大现实挑战

据调研，高教行业的身份管理类平台当前在人员身份类型的精细度、身份状态的时效性、身份数据的准确性、数据的服务效率、认证的安全性和便捷性、鉴权的灵活性等六个方面表现尚不足。



（来源：锐捷网络2022）

目前身份支撑教育数字化改革中导致业务与服务低效的问题，经过提炼呈现三个方向：

挑战一：

IT侧，访问控制隐患大。身份数据的质量不佳，会制约认证防御策略的执行；

挑战二：

应用侧，供给数据低效。当前应用获取身份数据仍低效，影响业务开展效率；

挑战三：

用户侧，访问业务不便捷。组织人员开展线上业务不便捷，影响业务办理效率。

“身份”在业务数字化发展下的核心定位

不难看出，这三类挑战始终围绕着“身份”展开，与人员身份、组织身份、业务数字化息息相关。剥丝抽茧，具体哪些因素导致了这些挑战的出现呢？

■ 挑战一：IT侧，访问控制隐患大。

- **账号安全漏洞多：**多入口账号重复开、账号信息不真实、失效账号残留；
- **个人信息安全意识不够：**弱密码、账号共享；
- **访问管理手段简单：**单点登录一通全通、不同时空访问限制；
- **权限管理不及时：**人员变化后权限迟迟未回收；
- **人员类型覆盖不全：**仍有大量校聘院聘人员、临时工作人员、研究合作人员等数字身份未覆盖。

■ 挑战二：应用侧，供给数据低效。

- 人员身份数据显现数据源头多、标准不统一、状态复杂多变等特点，应用侧对于数据的要求是从业务视角出发的。所以每次应用侧需要数据时，如果都是生硬的从数据源取数据，再进行检验编排，会大大降低业务服务的响应效率。

总结来看，本质上都是数据按需精细化供给困难。

■ 挑战三：用户侧，访问业务不便捷。

- **身份验证方式不便捷：**安全密码（高强度密码）记忆负担大，新用户首次认证不合规、人脸ID重复采集等；
- **访问不同系统常常重复登录：**用户在上网、访问业务系统、登录互联网平台、SaaS应用等场景时常常需要重复登录；
- **身份变化后访问业务受阻，权限未调整：**用户在一种身份状态或角色时申请权限、变动时需再申请权限，体验差；
- **历史身份数据无法访问：**历史身份失效，无法查询过往数据和追溯以往生涯相关信息。

这三个挑战恰恰说明“身份”在业务数字化发展下的核心定位：

■ 针对业务管理效率

保驾护航，“身份可信”是业务数字化发展的安全基石；

■ 针对业务办理效率

降本增效，“身份供给”是推进业务数字化建设效率的重要引擎；

■ 针对业务服务效率

以人为本，“身份通达”是业务数字化服务成效的显著特征。

价值内涵

建立在业务之上新思路——中台应运而生

通过对制约教育数字化快速建设因素的分析，可以清晰的看到，高校数字化转型的迫切诉求：建设的要求变高了，业务的复杂度呈持续上升态势，亟待实现以具体需求驱动的持续赋能、共用、复用能力。身份的业务数字化需要以一种承上启下、智慧精准、高效共享的新型平台作为中枢，因此“中台”应运而生。

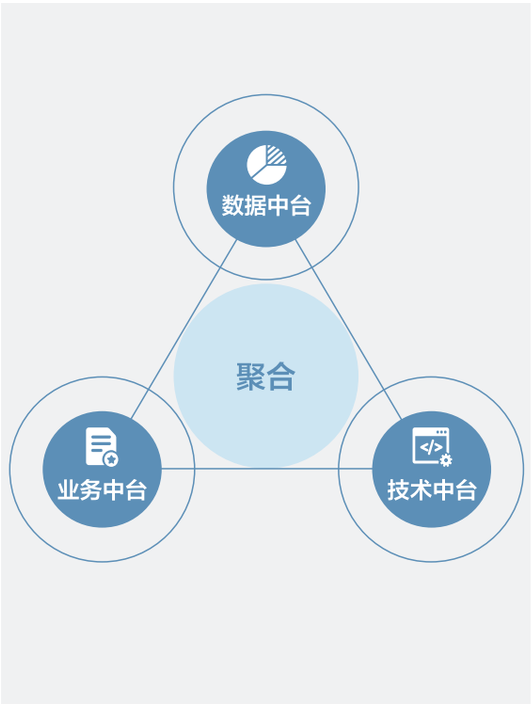
认知：中台是一系列系统可复用能力的集合

中台不是一个新词，但对它的定义一直没有一个官方的解释。这里，我们仍以业务视角来稍作展开：

“中台”的源起，其实出自我国东汉时期中央集权政府的中枢，号称中台，所以最开始它是以一种“业务体制”的形式出现的。

近年来，中台一词再次走入大众视野，是阿里巴巴集团运用中台理念，把所有的基础服务用中台的思路建设，达成“联通前后台，共同支持上端的业务持续发展和创新”的效果。

无独有偶，全球性软件及咨询公司Thoughtworks定义中台为“企业级能力复用平台”。



（来源：锐捷网络2022）

综上，可以看出，中台是一种介于前台和后台之间的业务体制，一种聚焦“共享、联通、融合、创新”的解决思路。

回归软件领域，我们定义中台概念为：通过向组织层面引入针对性的业务分工、唯一性的数据标准规则，达成对传统软件平台加强和升级的效果，避免重复造轮子，消除数据孤岛。

从受众视角来看，强调中台对于其他应用或平台的建设有更统一的要求：入口统一、数据统一、服务统一，以达成能力沉淀和复用的效果。

从种类上来看，有数据中台、业务中台、技术中台、组织中台等等形式，叫法不一，但核心是一致的：数据中台助力组织进行全业务视角下的全生命周期的数据管理，实现的本质是数据聚合；业务中台负责为组织内外的客户或用户需求提供解决能力和解决方案，本质是服务聚合；技术中台则是顺应代码平台化架构发展而形成的技术能力的聚合。

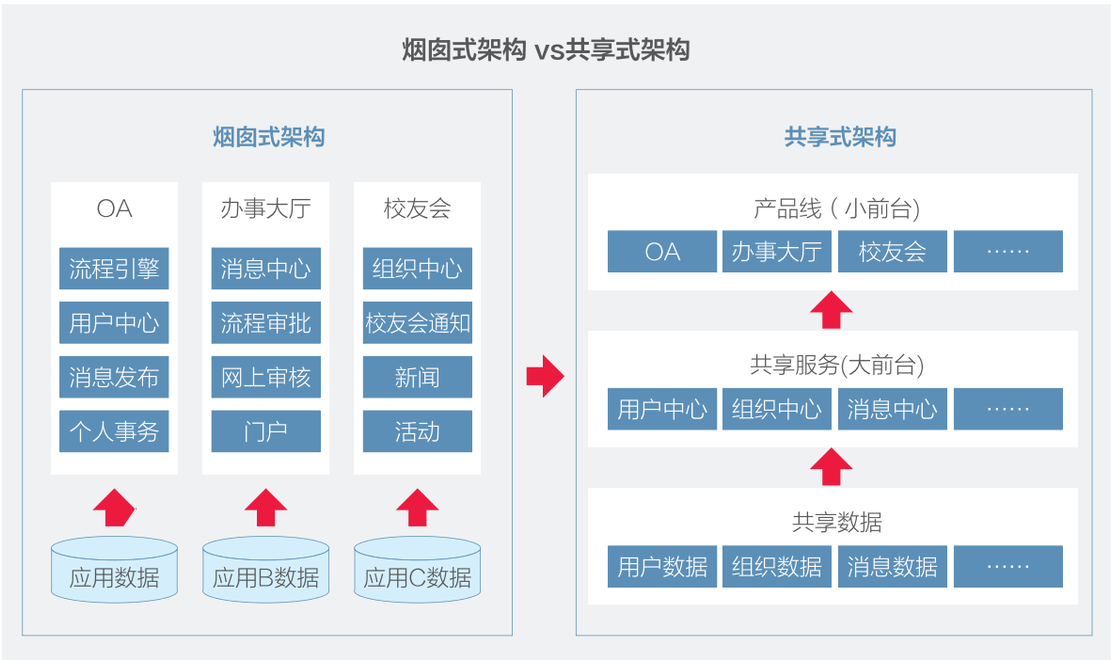
那么，聚焦到高等教育的范畴，为了不断提升业务的管理、办理、服务效率，到底需要一种什么特点的中台解决方案呢?

立新：打造“数据-身份-业务”闭环的身份中台

前文提到，高校的身份管理要围绕着“身份可信”、“身份供给”、“身份通达”展开，就必须要立足于“身份”这个切入点。**其实，随着业务复杂度的提升，“身份”一词也有了新的内涵。**

（来源：锐捷网络2022）

结合高校数字化转型的挑战分析，传统的烟囱式业务系统构建模式在架构层面一直在制约突破，一个中心系统解决一个业务域的问题的做法必须整改。



（来源：锐捷网络2022）

显然，要突破传统建设方式的壁垒，“共享式”的中台化思想恰能契合新时代的建设目标。“中台化”既可以包容各式各样的“身份”新内涵，更加易于拓展与身份管理相关的业务；最重要的是，高校数字化转型需要校园业务管理、办理、服务效率的不断提升，与中台提倡的业务能力复用、业务数据高可用、业务资源聚集的思想不谋而合。

智慧校园需要智慧解决方案，高校的数字化转型需要破旧立新，针对服务校园身份管理业务的新基建——身份中台应时而生：

立足“身份”基点，以聚合身份数据、抽象身份业务、提供身份服务为途径，整合校园中的“人员”和“组织”，打通前台和后台，赋能业务场景，安全可信，降本增效。

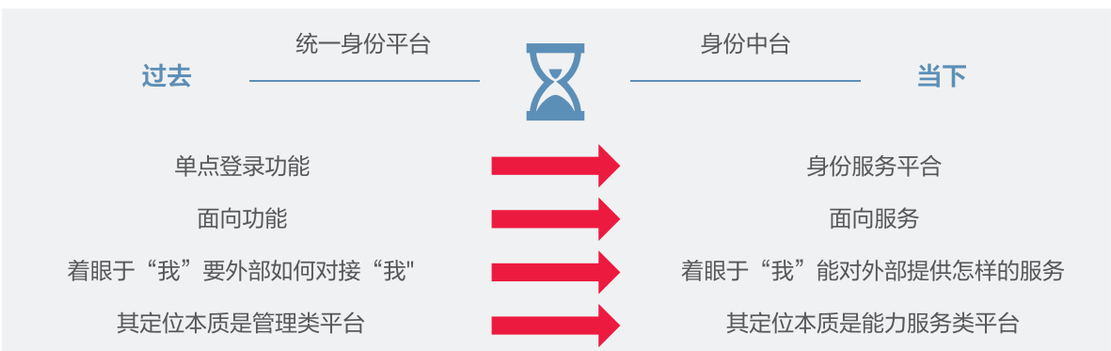
高教身份中台的构建，本质上是对新一代校园身份管理服务提出的一种新要求：

通过深化身份能力真正的激活信息化效能，以人为中心、以赋能为目标开展身份治理、身份安全、身份服务等能力构建，打造“懂”人员身份的能力，真正支撑学校规划、管理、业务、服务等信息化应用落地成效，为更好的达成高校数字化转型的发展目标提供可信、高效、便捷的基础能力底座。

（来源：锐捷网络2022）

身份中台的价值——赋能业务场景，安全可信、降本增效

身份中台不论是从基本定位还是面向对象来看，都是与传统的身份管理型平台（统一身份认证平台）有实质性的区别。从面向对象看，高校身份中台是面向服务的，它的定位本质是能力服务类平台。

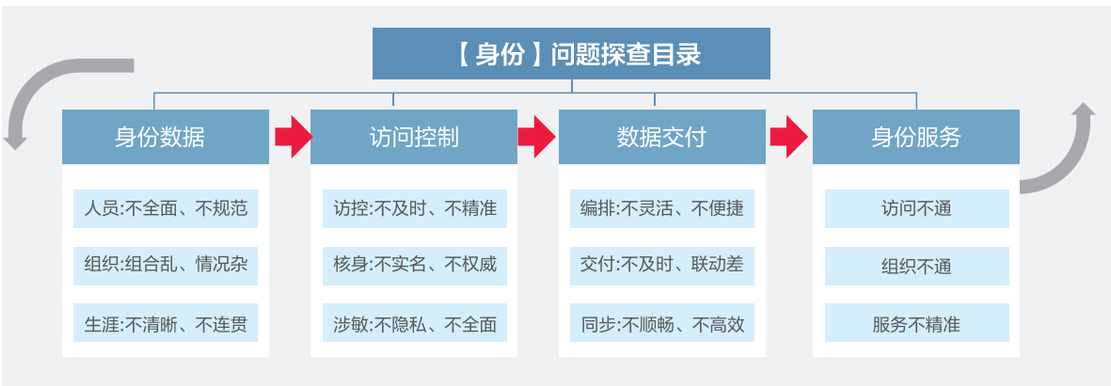


（来源：锐捷网络2022）

从实际需求和痛点出发，探查校园信息化中的身份问题

其实，如何定义身份中台不重要，它能解决什么问题最重要。结合上文总结的当前高教信息化发展面临的三大现实挑战，继续深入剖析一下具体的障碍痛点和业务问题。

不论在IT侧、应用侧还是用户侧，对“身份”相关问题的铺陈可由浅入深。



（来源：锐捷网络2022）

身份数据质量是身份问题最根本、基础的部分

· 人员：

在校人员大致分为三部分。首先是数量最大的学生，还有各种类型的教职工，这两类人员数字身份的管理已经趋向于成熟，并且身份数据的权威源比较清晰和固定（教务系统、学工系统、研究生系统、留学生系统、人事系统等）。

随着校园业务不断进化、扩张，除两大类统管人员之外，涌现出了十余种其他身份类型：院聘教师（不纳入人事管理）、联合学习的专家学者（外校）、临时工作人员（校企合作、合作项目、项目支持人员等）、后勤人员、校内租住商户、附属学校人员、成教生、教职工亲属，等等...但往往这类人员面临“无规范开户流程”“数字身份管理权责不清”“账号全生命周期不闭环”“身份数据流向错乱”“身份数据质量低下”等现实问题。

后疫情时代对数字身份覆盖的全面度要求更加严格，例如像健康打卡等不容遗漏和出错的活动已成为日常；另一方面，从信息安全的角度，在全面的基础上，对身份数据有更规范、更标准、更连贯、更实名的要求。

数字化转型的基本面就是需要校内的数字身份覆盖全面，在管理的全流程中做到不遗漏、精准、安全，才能为校内各类人员提供更便捷和高效的数字服务打下坚实的基础。

· 组织：

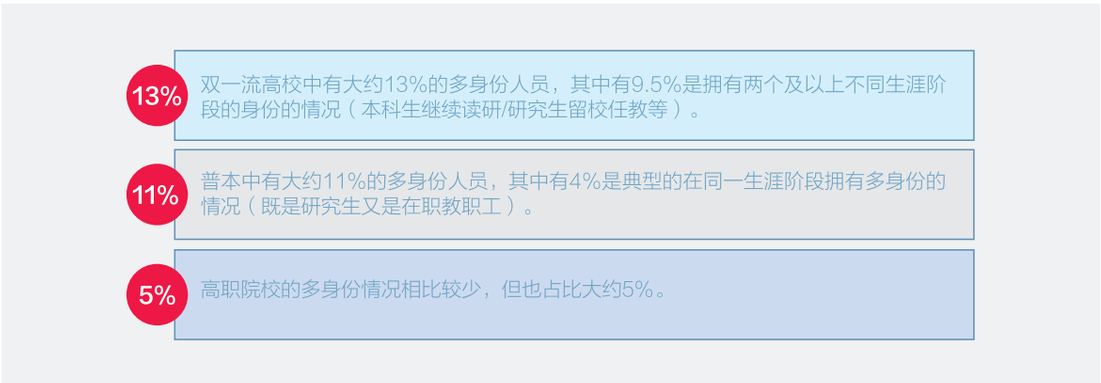
高校中常见的组织管理是根据各类人员的归口部门自行管理的。例如，常见的教职工的行政组织由人事处管理；各个二级学院会有不同的组织架构，例如党政组织、团学组织、学工组织、科研组织、社团组织等等。各类组织中的主副岗，人员角色，多身份人员等情况；人员上下级关系，管理授权关系，人与部门的从属关系等等，这些关键的要素一般都是跨单一组织结构的，而且数据维护不及时、不准确、不规范的问题是普遍现象。

加之业务/二级部门围绕着各自的业务特性，各层级人员数据、组织数据的形态和结构大不相同，各类数据之间也会因为业务诉求的不同而三两搭配或重组。显然，各组织要管好自己的数据，又要能在各式各样具体的业务事件（如校庆、防疫、科研申报、高基填报等）发生时提供好业务所需的数据，往往耗时费力。

· 生涯：

“生涯”是一个二维的概念，指的是人员在校内的组织身份类型，在不同的阶段有所变化，相关身份的定义、角色的定义、权限的定义也都会相应变化。

所以，人员在校内由于生涯状态的更迭或工作、学习不同的需求，会出现“多身份”的情况。据调研和抽样，多身份的情况非常普遍，而且在不同类型的高校有些许差异。



（来源：锐捷网络2022）

多身份的现状自然会带来多ID的现实问题：师生在校期间随着生涯发展、状态变化，不同阶段会有不同身份ID。随着互联网应用丰富，社会环境进步，能代表人员身份的 ID 越来越多样化，在此背景下，校园生活、学习、 工作、科研、保卫、防疫等场景中，身份验证也呈现多样化，实际情况是人人需要反复开通不同账号，在不同场景验证身份常常受阻，着急申请办理，未统一整合人员多种 ID，不能为各种场景提供直接可用、适合的 ID，身份复用能力差。同时，当一段生涯结束，标识这段生涯身份的ID则应该失效或者做相应的权限调整，事实上这一点与设想的差距很大，往往是用户的生涯情况丢失，或者不连贯，无法呈现一个真实的、全面的生涯面貌。

常见的场景有：

- “用户本科毕业升为本校的研究生，由于身份证、手机号和微信号已经绑定原本科生账号，所以研究生账号无法直接绑定，要去线下人工换绑”
- “某教职工同时在本校读研，两种身份的业务办理需要不同的账号，来回切换体验差”
- “用户时隔几年回到学校，之前的身份信息已经全部丢失，业务痕迹也被抹去”

访问控制体系是身份问题最核心的部分

- **防控：**

谈到访问控制，离不开“认证”“授权”两大部分，更离不开依托的主体，则是“身份”。认证是相对简单的，只有是与否，禁止与放行；但是影响授权的因素就颇为复杂，而且权限的大小、粒度会根据这些因素的变化或者组合而实时变化，数字化转型中一直强调的“精细化”其实就是针对授权谈的。

其实，在高校的数字化转型中，有关访问控制也离不开“从RBAC到ABAC演变”的影响。与RBAC模型不同，ABAC可以根据用户属性、动作属性、上下文属性（如时间、设备和位置）、资源属性（如记录的敏感度）等等来调整授权策略。事实上，在高校的访问控制场景中，身份类型，工作角色，身份标签，生涯状态，网络通道，终端设备，访问对象敏感度，时间，地点，数量等多种属性（数据）都会影响用户、资源和上下文。

（来源：锐捷网络2022）

更具象地讲，例如校内的某位用户，他以不同的身份类型和工作角色，在某一个生涯状态时，他用不同的终端、在不同的网络通路中访问不同的敏感度的资源时，其中任意一个因素发生了变化，授权的策略就会不同。其中差异，正是“精细化”的内核。

常见的场景有：

- “学生休学、入伍，其访问和业务权限未做调整，影响了业务办理效率的同时还埋下了安全隐患”
- “不同身份类型的用户在不同工作角色下，访问门户类应用的权限无差异，用户体验不佳，信息化部门被诟病”
- “人员入职自己逐个申请开通权限，低效且会有遗漏”。

- **核身：**

“实名”是由于“安全”引出的，是信息化到了一定的成熟阶段，必然会面临和追求的目标。在身份管理领域，关于身份的三大问“Who you are”“What you have”“What you know”是验证身份的精髓，所有的身份认证的方式或者综合的解决方案归根到底都是围绕这三点展开设计的。

核身场景中的业务要求决定了核身的方式，本质是“提供怎样的凭证，可以证明人员的身份”。很多情况下，仅凭一些弱校验方式就与身份认证划等号，不安全、不权威，后患无穷；还有一些情况，由于不能提供多元的核身方式，导致业务办理效率低下。

目前在校园中，此类场景有：

- “新生入校，用身份证后六位作为初始密码，不合规不安全，会出现冒名顶替事件”
- “用户忘记密码，绑定手机号也更换了无法换绑，需要线下核验身份再求助人工重置密码”

- **涉敏**

《个人信息保护法》中强调严格保护敏感个人信息。值得关注的是，《个人信息保护法》将生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息列为敏感个人信息。并严肃要求，只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，方可处理敏感个人信息，同时应当事前进行影响评估，并向个人告知处理的必要性以及对个人权益的影响。

学校基于教学管理的需要以及可能涉及配合公共事务管理的需要，不可避免的成为“个人信息处理者”，需要对其个人（敏感）信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。在高校数字化转型中，学校如何合法合规处理个人信息，是身份数据管理中必须严肃面对的问题。

身份数据交付能力是除了以上的基本面问题之外，最影响业务效率的部分

- **编排：**

身份数据的编排是由于提供、管理、使用数据的业务事件的差异造成的。由于各个业务部门对组织身份数据、人员身份数据的定义不同，数据标准也有差异，编码间缺少映射，所以身份数据的编排效率不高。这往往是业务变更不灵活、业务管理不高效的根因。

- **交付：**

校办、人事、科研、学工、教务、后勤等校园主体业务部门往往对师生整体发展现状与趋势比较关心，常常需要汇总数据支撑决策，不同统计对象往往是某种类型的人员群体，而在当下的数据中心建设下，根本无法从人员身份类型来支撑数据的聚合，所谓一张表只是数据层面的清洗，难以满足各部门、校领导关心的某类人员的数据快速供给，数据依赖人员 ID 分别提供，靠统计人员人工清洗、映射、汇总，工作量巨大、周期长，完全满足不了校园发展决策灵活多变的需求。

- **同步：**

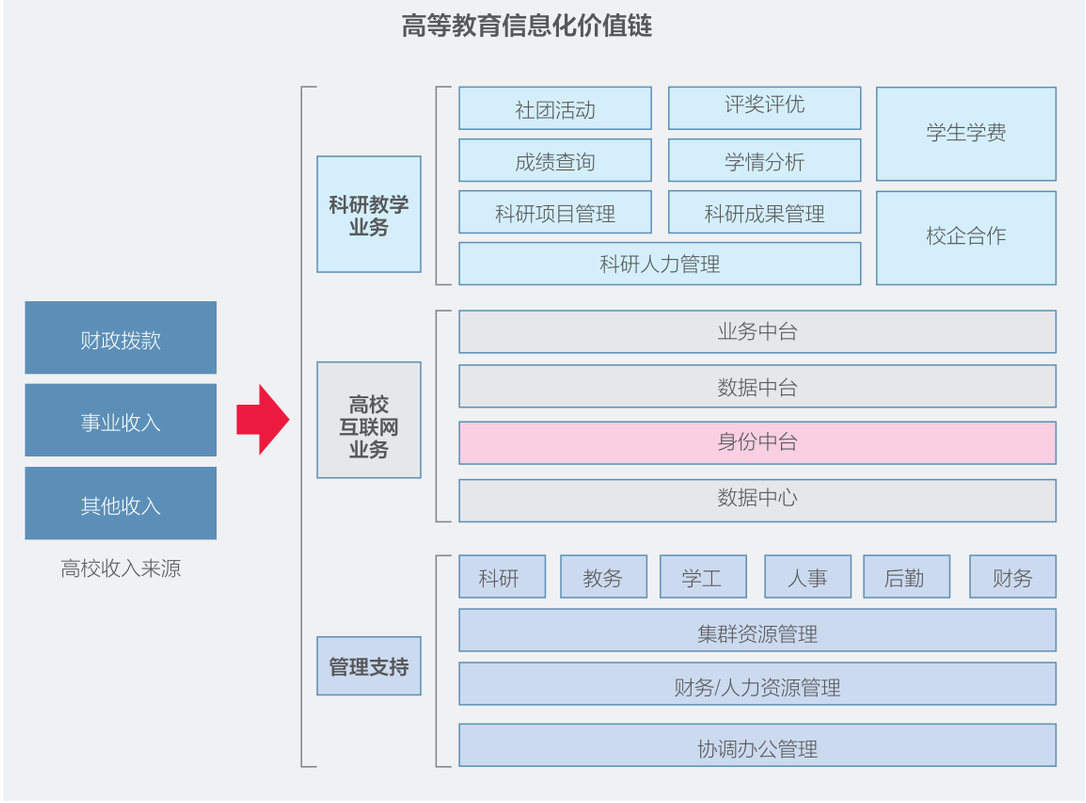
身份数据同步的现状大致有几种，其一：校内应用从数据中心全量取数据，毫无数据安全可言，且每个应用都需要过滤、组装、调整、管理，数据的使用效率极低；其二：校内应用通过定制化开发数据API调用数据，对于复杂的用户组开发难度大，业务的响应效率低；其三，手动为校外平台提供数据，维护工作量大，整合复杂数据、多组织架构困难。

常见场景有：

- “某教职工已经调岗，但OA和流程平台未及时根据数据进行调整，造成审批延迟，需要人工干预”
- “用户的绑定手机更换，未能同步至其他应用，数据中心中留存着数条脏数据”
- “数千名毕业生不能再使用企业微信办理业务，需要调整到校友节点中，人工审核并且核对，耗费大量人力和时间成本，还易出错。

身份服务则是最顶层能力和愿景

基于当下以业务为中心的信息化建设模式，如果身份服务不到位，学校很难了解到师生在多个方面的情况，上级依赖下级部门汇总，下级部门依赖常规填报与部门惯例，在机会面前不容易识别合适的人才，在多种机会与服务场景中，做不到端到端、点到点的服务，人才培养工作被动，学生关怀、发展、就业工作被动，不能精准管理、服务。

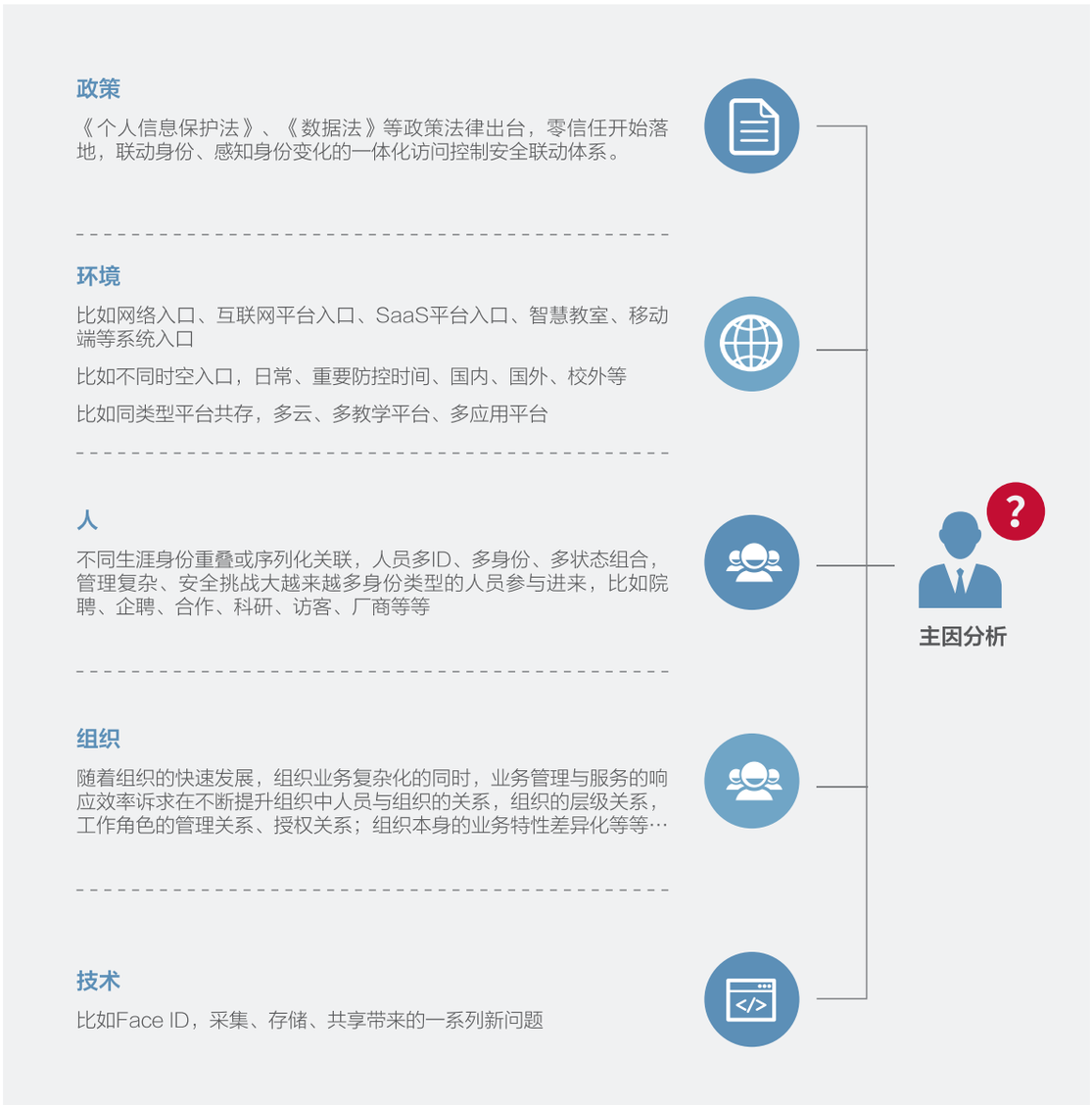


（来源：锐捷网络2022）

其实所有的高校信息化建设都是为了学生培养，科研的发展，围绕着师生校内外学习、工作、生活，如何更好的为师生提供发展机会，更好的关心人才、挖掘人才、培养人才，聚焦资源到最大可行的对象上，数字身份的精准服务责无旁贷。

挖掘背后的制约因素，主因洞察

造成以上诸多高校信息化中身份问题的原因，是环环相扣的。从政策、环境、人、组织、技术等方面进行一些归纳和分析：



（来源：锐捷网络2022）

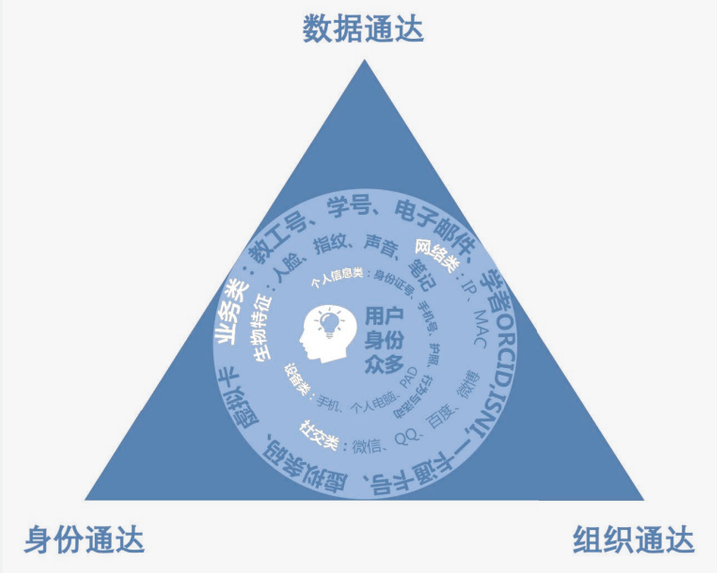
很明显，组织与环境发展已经呈现了高复杂度特征，传统身份管理类平台的定位，依靠如单点登录等基本功能，在面对这些的高复杂度情况，是无法应对的。往往会走进“出现一新的业务场景，就定制化解决一次”的恶性循环。

身份中台的价值主张：三全

所以，为了校园业务数字化高效持久的发展，当下还是要从架构上、从能力上去深入考量，到底高校需要什么样的身份能力去面对这些复杂度呢？

■ 全身份通达，“识”人

提炼人员、身份、角色、组织、数据等关键要素，构建基于身份的通达体系：



（来源：锐捷网络2022）

- **身份感知：**

可感知人员多种身份的变化，用户凭借匹配的身份和当下的状态在不同入口、业务、环境中通行，业务同行和授权自动调整。

- **身份通达：**

即身份随人，无论在何种场景，都能识别身份标识（ID）背后的“人”是谁，了解其多元身份，为应用传递需要的身份角色 。

- **组织通达：**

从技术视角看，按照规范接口调用、同步至业务应用；从整体目标上看，校内各种组织、群体都可以统一定义，让师生在不同平台、应用中穿行时可以使用熟悉、一致的组织信息。

- **数据通达：**

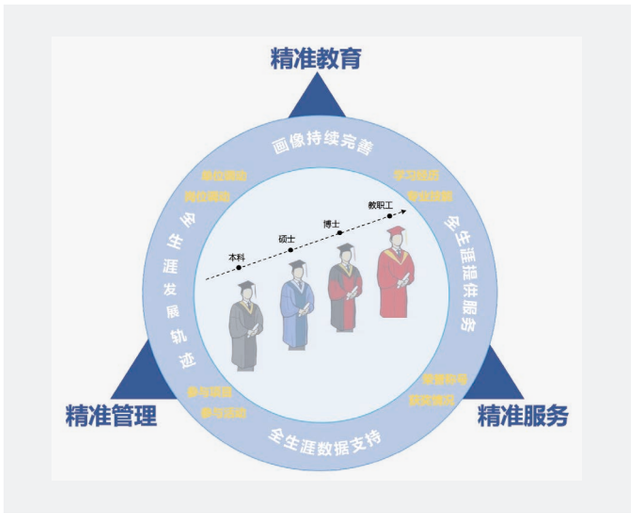
构建身份标签化数据集合与生产线，根据业务需求供给各种身份标签、组合。快速支撑业务数据需求，在新业务数据产生后按照规范路径回流。经过加工得到新身份标签与相关数据，使得各项业务与决策的快速使用。

全生涯服务，“懂”人

首先从信息化视角，要重视和尊重用户的生涯信息，人员与校园产生联系的所有数据和痕迹都要尽可能的保留下来，并且与每一段生涯阶段关联上。

“精准”在校园范畴中主要体现在几个方面：

- 一是人员身份数据质量持续健康；
- 二是校内各应用与数据中枢间的身份数据流向顺畅；
- 三是访问控制策略颗粒度精细；
- 四是身份数据高效率赋能具体的、有差异化的校园业务。

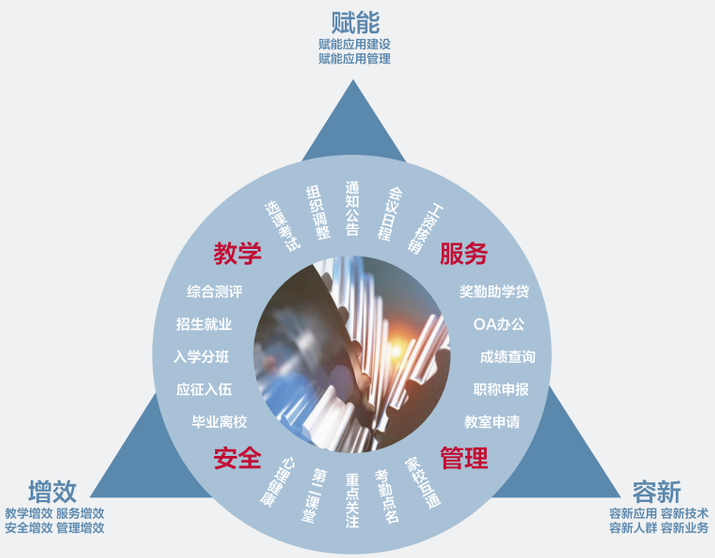


（来源：锐捷网络2022）

达成基本面构建之后，要持续聚合、挖掘师生身份标签，构建学业、职业生涯画像，联动互联网平台网罗师生数据。在师生与学校、外部机构、未来就业公司之间建立精准身份桥梁，不断为师生发展提供精准教育、精准管理、精准服务、精准关怀、精准就业、精准招聘等数智化场景服务。

全业务赋能，“智”撑

围绕校园“人、财、物”业务域，提供全面的身份 4A 管理与扩展接口，保障人员身份数据、组织身份数据的准确性、及时性、一致性、规范性，有效支撑业务变化与服务响应。



（来源：锐捷网络2022）

构建方式

架构致胜——大中台小前台

“智慧校园–身份中台” 的架构构成

身份中台的构建首先是以建设智慧校园为总体目标的，中台架构采用“中台+微应用”的形式。如果把智慧校园的建设愿景看做是一个统一的“能力池”，那么中台能力则是“资源池”+“数据池”+“业务池”。

其中身份中台则是整个智慧中枢的能力底座，以三个“统一”（统一单点登录、统一认证服务、统一授权管理）和五个服务模块（身份标准与元模型、身份数据治理、组织数据管理、标签与事件流、身份数据服务）为能力集合。

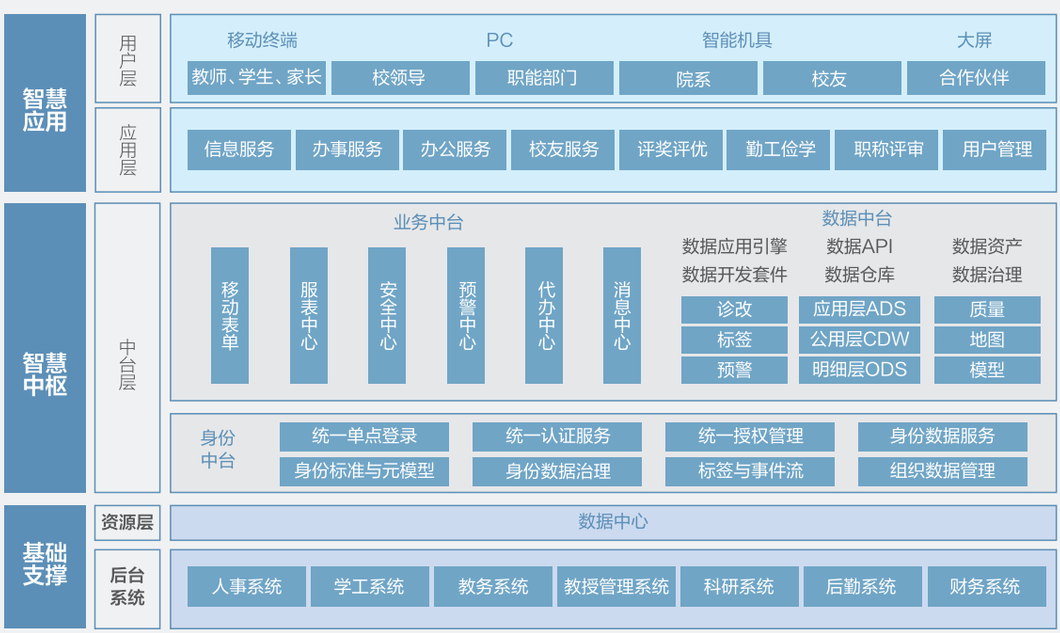
向下，整合与治理

从身份业务角度汇聚、治理来自后台系统和资源层的身份数据；

向上，辐射与支撑

第一层面是在中枢内部，身份中台之于数据中台是对身份数据的补充、深化；之于业务中台是对身份业务的支撑和赋能。第二层面是面向智慧应用层，通过微服务API相互调用，实现智慧校园业务的弹性伸缩、能力复用和快速重构。

智慧校园中台架构图



（来源：锐捷网络2022）

身份中台以身份数据治理、身份业务梳理为主要途径，旨在推动高教智慧校园建设实现“个性化、服务化、整体化、智能化”的目标。

从业务需求出发的能力体系建设

身份中台是以“身份数据管理” +“身份服务”为核心构建理念的，目标是打造一个由“身份治理体系”、“访问控制体系、“身份数据交付体系”、“身份服务体系”集成的身份能力体系。

身份治理体系

通过人员身份治理、组织身份治理、生涯数据治理进行身份数据根基建设。

访问控制体系

遵守个人信息防护，以实名核身为手段，安全防控为目标进行业务安全防御。

身份数据交付体系

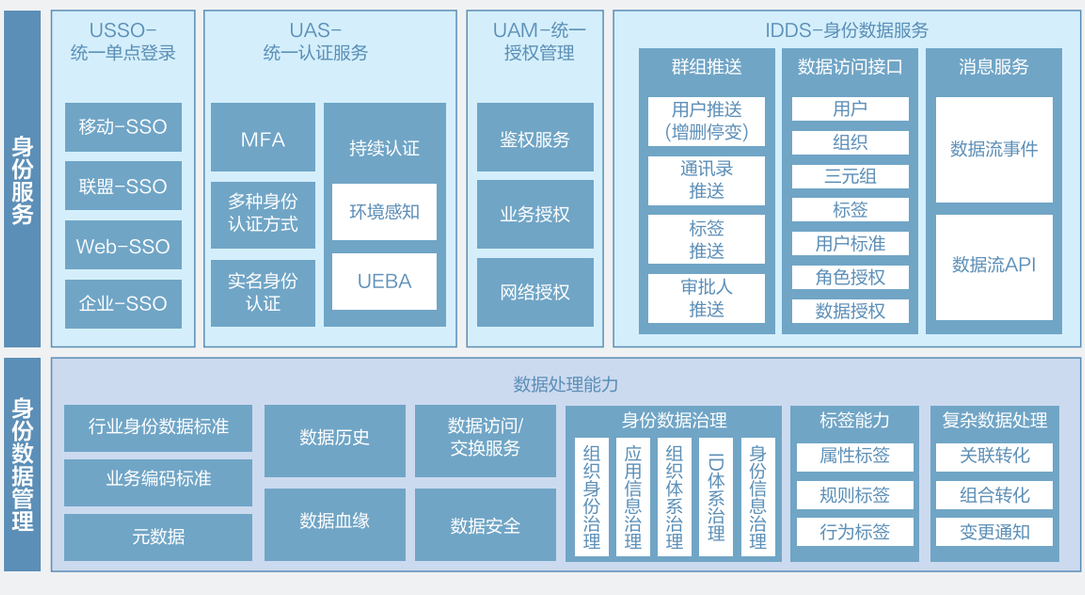
通过身份数据的编排、交付达成数据通达目标，提供身份能源服务。

身份服务体系

以“访问通，组织通”达成身份精准服务的终极目标。

从业务架构视角，身份中台最基础的数据处理能力是由数据标准规划、身份数据治理、数据标签能力、复杂数据处理机制层层递进构建的；身份服务能力则通过三个“统一”为构建基础，以多元的数据访问接口、群组推送、生涯数据流等形式对外部应用赋能。

身份中台业务架构图



（来源：锐捷网络2022）

从业务能力视角，身份中台主要通过以下模型来构建：

身份标准模型

身份标准体系模型，实质上是建立人员标准管理模式。基于人员类型、身份状态、数据集字段三元组标准管理用户数据，规范高校人员信息管理。

- **组织岗位体系模型**

  构建多组织体系模型，包含部门模型、岗位模型、工作角色模型。部门、岗位、工作角色都有上下级关系，可从容满足流程系统需求；同时可以定义多种工作体系，满足校园内各类人员的不同业务需求，以及各种维度的管理需求。

- **多元ID模型**

  人有多种身份信息，在计算机系统中可以定义 UID 串连各系统用户 ID 信息，在生活中可以使用身份证、护照、人脸等实名 ID 作为身份标识。身份中台将多种用户身份 ID 聚合管理， 做到以人为本，身份聚合，身份随人。

- **身份标签模型**

  支持从多维度定义用户身份，通过定义身份标签规则，自动维护符合规则的动态标签名单；为各个业务部门、业务系统提供多维度人员名单，支撑各种业务的高效开展。

- **认证策略模型**

  支持灵活定义多因子认证策略，并灵活定义因子顺序，灵活定义二次认证策略。

- **功能与数据双层授权模型**

  构建功能、数据双层授权体系，实现对应用入口权限、应用功能权限、应用 API 权限管理，对数据权限、数据密级、数据脱敏加密授权管理。全面保障学校信息资源安全，规范信息化系统建设、管理。

- **大单点登录模型**

  实现入网认证与业务单点认证合一。

除7大能力模型之外，身份中台在“应用可视化管理 ”“微服务架构 ”“性能与压力”“安全性” “兼容性设计” 等方面也有相应的设计和规划。

聚焦服务——“一站式”解决方案

诊断摸底：从身份数据治理开

在身份中台落地之前，要进行一项不可或缺的摸底：即当前校园中真实的身份数据质量情况诊断。身份中台的能力构建最终是为了身份业务的高效赋能，所以只有明确了当前身份质量的缺陷才能有的放矢，并通过身份数据治理为业务抽象打好基础。

身份中台以六度整体评估来开展诊断，包括：

- **身份质量的准确度**

  主要诊断身份类型划分、身份状态情况、组织部门岗位情况以及学工号重复率等。

- **身份质量的规范度**

  主要诊断各类证件号、学工号和其他ID是否真实合规。

- **身份质量的完整度**

  主要诊断人员身份信息、相关的岗位、部门、院系情况是否全面。

- **身份质量的实名度**

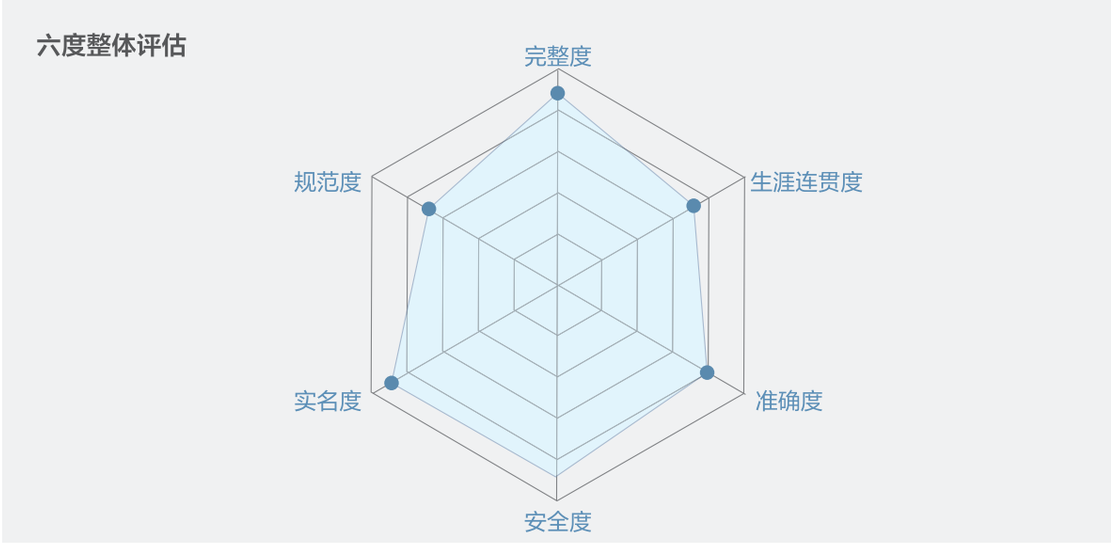
  主要诊断人员姓名、证件、绑定手机、生物ID等是否真实匹配，是否经过权威源核验。

身份质量的安全度

主要诊断密码安全度，绑定手机准确性、不活跃用户情况、生物信息加密情况等。

身份质量的生涯连贯度

主要诊断多生涯人员分布情况、生涯转变情况和生涯画像信息。

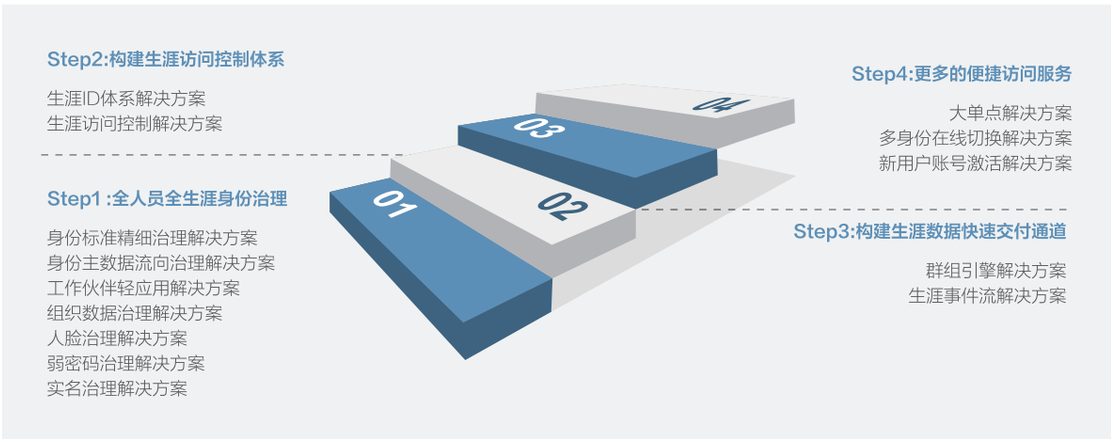


（来源：锐捷网络2022）

价值交付：治、控、通、协

身份中台的交付要如何展开，遵循以终为始，即以“身份服务”为最终目标。首先数字身份要能覆盖校内所有的身份类型，达成人人有身份；其次要让身份都可信，数字身份合理合法合规，达成全人员实名；再者，以精细化的生涯访问控制和灵活实时的身份数据交互两部分体现。

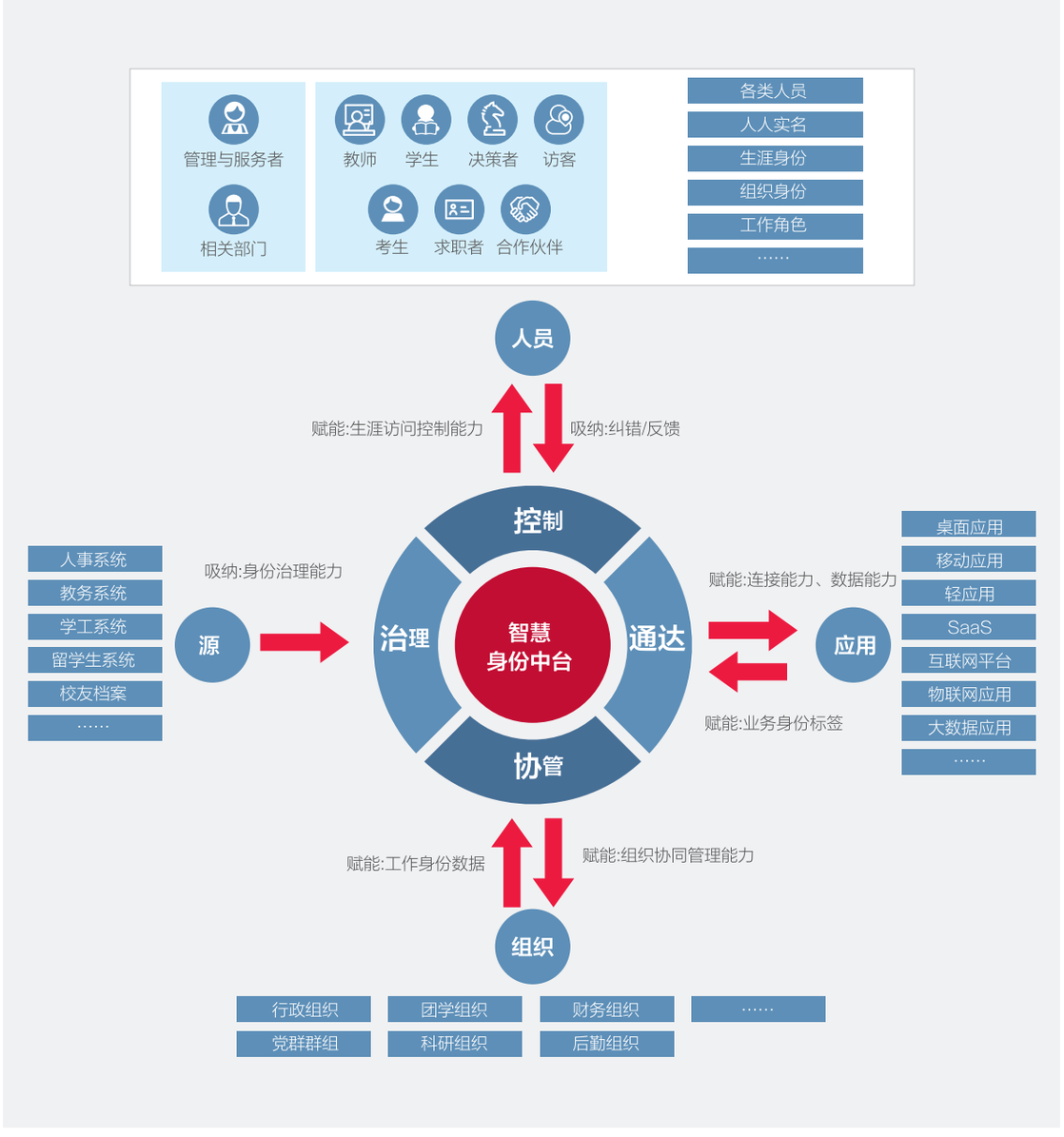
对照前文介绍的身份能力体系建设，继续细化由多个“单一能打”、“组合灵活”的解决方案组成的四步走交付策略：第一步，身份治理；第二步，构建生涯访问控制体系；第三步，构建生涯数据快速交付通道；第四步，提供更多的便捷访问服务。



（来源：锐捷网络2022）

从价值交付视角看，身份中台在整个智慧校园建设中的位置，和各个相邻系统之间的关系：

- **治理：**从源头上，身份中台从人事、教务、学工等权威源吸纳身份数据，通过以业务触发的身份数据治理先打好基础。
- **控制：**从对于学校格式各样人员的管理来看，身份中台通过实名校验、生涯贯穿、角色梳理等方面不断纠错与丰富各类人员组织身份的管理。
- **通达：**对下游应用而言，通过业务身份标签的链接能力来不断赋能各类轻应用、移动应用。
- **协管：**对于校内的组织，不论是最基础的行政、党群、团学组织，还是极具业务特色的科研组织、财务组织都可通过身份中台的组织协同管理的能力，来不断从组织身份数据的层面完善、优化。

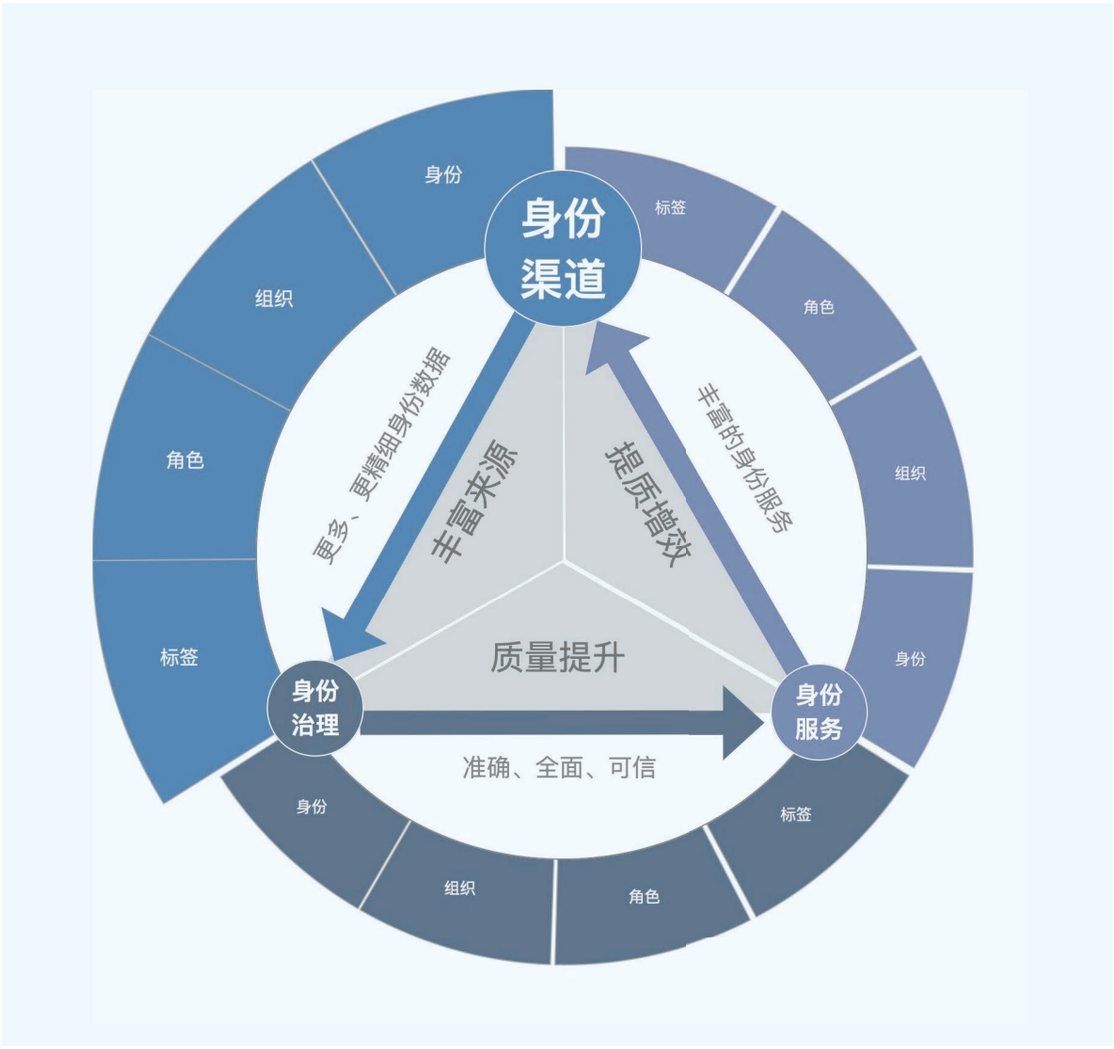


（来源：锐捷网络2022）

发展规划

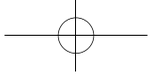
智慧校园的重要基石: 生涯服务体系

身份中台建设完成的标志大约分成三层面，一是全链路体系化建设“身份、组织、角色、标签渠道”，深度解决ID、组织、角色、标签的精准数据来源；二是进阶化的“身份、组织、角色、标签治理”，旨在达成身份数据的准确、全面、可信；最终提供全方位的“身份、组织、角色、标签服务”。



（来源：锐捷网络2022）

智慧校园建设的步伐是不会停歇的，高教身份中台的构建也会随着发展不断进行理念完善和价值淘金。目前可以明确的是，以身份业务为抓手、以中台思维为指导的身份中台建设理念顺应了时代的潮流，对于教育信息化发展会是一个跨越式的升级。


Ruijie 锐捷 Networks

锐捷网络股份有限公司

欲了解更多信息，欢迎登录www.ruijie.com.cn，咨询电话：400-620-8818