CARSI服务及Shibboleth简介

北京大学CARSI项目组

2022年2月

CARSI

CERNET Authentication and Resource Sharing Infrastructure

教育网联邦认证和资源共享 基础设施

关于 CARSI

- 中国教育和科研计算机网联邦认证与资源共享基础设施（CERNET Authentication and Resource Sharing Infrastructure），简称CARSI，是由中国教育和科研计算机网CERNET网络中心管理，北京大学计算中心研发并提供技术支持，赛尔网络有限公司提供日常运行和用户服务，为已经建立校园网统一身份认证的高校和科研单位，提供联邦认证和全球学术信息资源共享服务。加入CARSI，高校师生可以不必通过校园IP地址确认身份，无需使用VPN，就可以在校外任何地方使用校园网账号直接访问学校采购的电子期刊、电子图书等学术资源，也可以随时随地访问特色资源，如正版软件PDF编辑器、高性能计算资源、专利数据等。
- 截至2021年底，CARSI正式接入高校近500所，110余所高校在调试，使用人数超450万。共汇聚了70余个资源提供商近200个产品，包括Web of Science、Science Direct、万方等图书馆电子资源产品，也包括包括3个长期免费使用和52个支持试用的CARSI特色资源，如“福昕高级PDF编辑器”、“赛尔网络下一代互联网视频课程”等。涉及电子图书类、电子期刊类、学位论文类、在线课程类等55种资源类型。其中多家中外知名数据库服务商提供了29万种期刊，35万余种视频等多媒体资源，520余万册电子书及教材，2600多万篇学位论文，超17亿项专利以及超14亿条数据资源。CARSI高校从2020年初的22所快速增加到600余所，同比增长27倍，在eduGAIN联盟正式会员单位中，一举成为英美之外的第三大国际合作组织。
- CARSI已接入高校和学术资源详细清单请参见：https://www.carsi.edu.cn/idp_sp_zh.htm

CARSI发展历史

- 2006年由北京大学发起，在科技部863计划项目支持下，进行小范围试验
- 2008年12月，国家发改委CNGI08项目支持，将规模扩大到30+个CERNET2核心节点
- 2012年，国家发改委2011年度信息安全专项项目，和CALIS合作，进一步将规模扩大到70+学校，6个国外数据库商20+个应用资源
- 2017年8月，正式向eduGAIN提交加入申请
- 2017年10月，和北京大学主持的“全球无线漫游服务eduroam”一起被列入教育网基础服务
- 2019年5月，加入全球身份认证联盟eduGAIN，成为full member
- 2019年10月，完成升级，采用全新的服务模式和管理模式，进入产品化运营阶段
- 2019年底，新模式下，21所高校可通过CARSI访问7个服务提供商的应用资源

CARSI发展历史

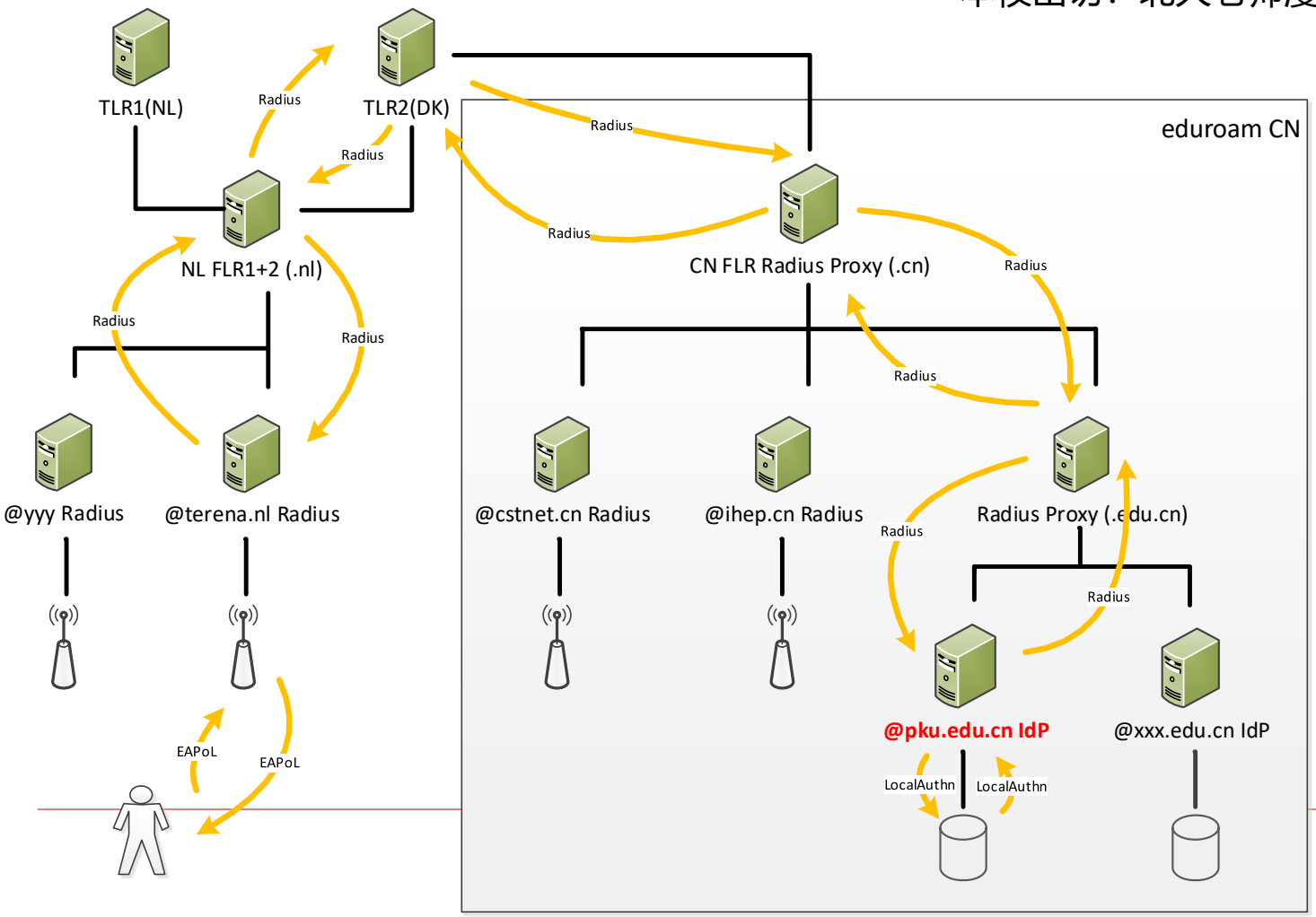
- 2020年春，作为学术资源访问利器，疫情期间，有效支持“停课不停教，停课不停学”，迎来爆发式增长，多年积淀的科研成果正式服务社会，效益显著
- 2020年4月，服务高校突破500所（包括已上线和调试中）
- 2020年11月，“CARSI资源共享门户”上线，支持移动端，可集成到校园门户、微信公众号等，一站式访问CARSI资源
- 2021年4月，第一款全体CARSI师生可长期免费使用的正版软件—福昕PDF编辑器（网页版）正式上线
- 2021年底，近500所高校可访问70余个公司的近200个产品，包括3项免费资源和52项试用资源，CARSI逐渐从支持学术资源访问发展成为为校园教学科研和信息化建设提供支撑

跨越校园网边界的资源共享

eduroam	CARSI
无线网接入层面的资源共享	web应用系统层面的资源共享
突破地理位置限制	突破地理位置限制和应用限制
全球无线漫游	任何时间、任何地点、任何联网方式访问应用系统资源
共性：都是基于高校用户校园身份的域间/互联网漫游	
差异：底层支撑技术不同	

eduroam认证流程—本校出访&访客来访

本校出访：北大老师漫游到欧洲

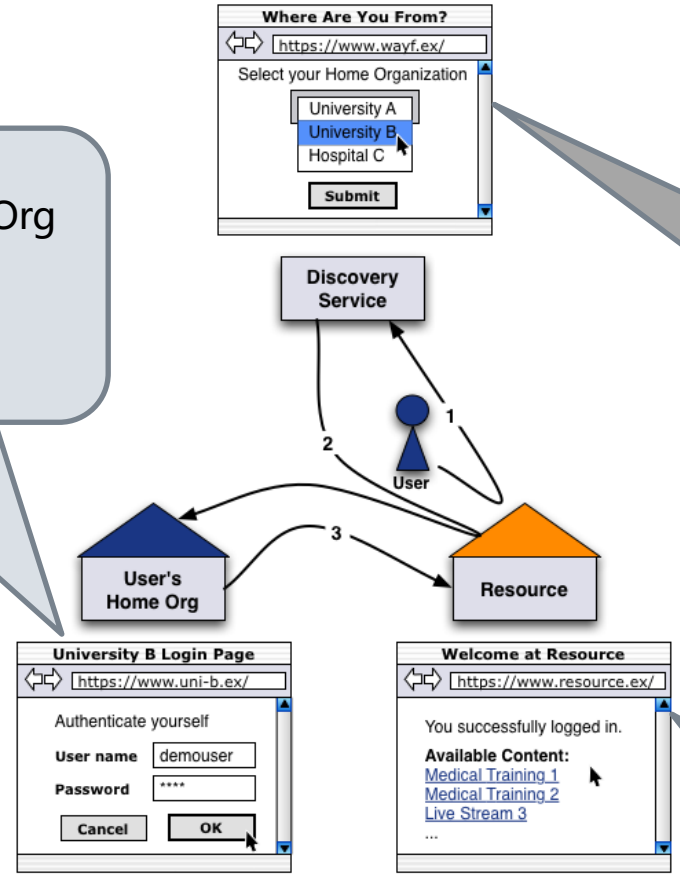


CARSI服务

用户/IdP 《《《 CARSI 》》》 应用系统/SP

CARSI的技术基础——shibboleth/SAML2.0

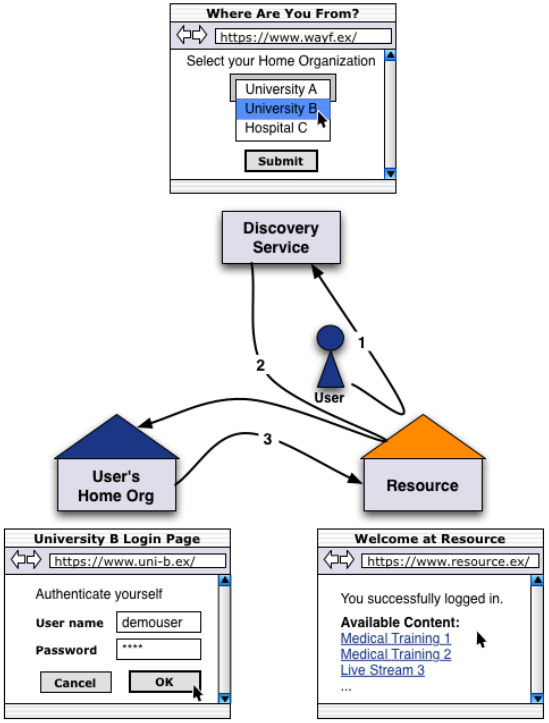
身份提供者IdP/User’s Home Org
- 身份认证
- 发放用户身份属性



目录服务DS/WAYF
- IdP（学校）清单
- SP（资源）目录

服务提供者SP/Resource
- 基于用户属性的授权
- 对接已有的应用系统

CARSI的技术基础——访问流程

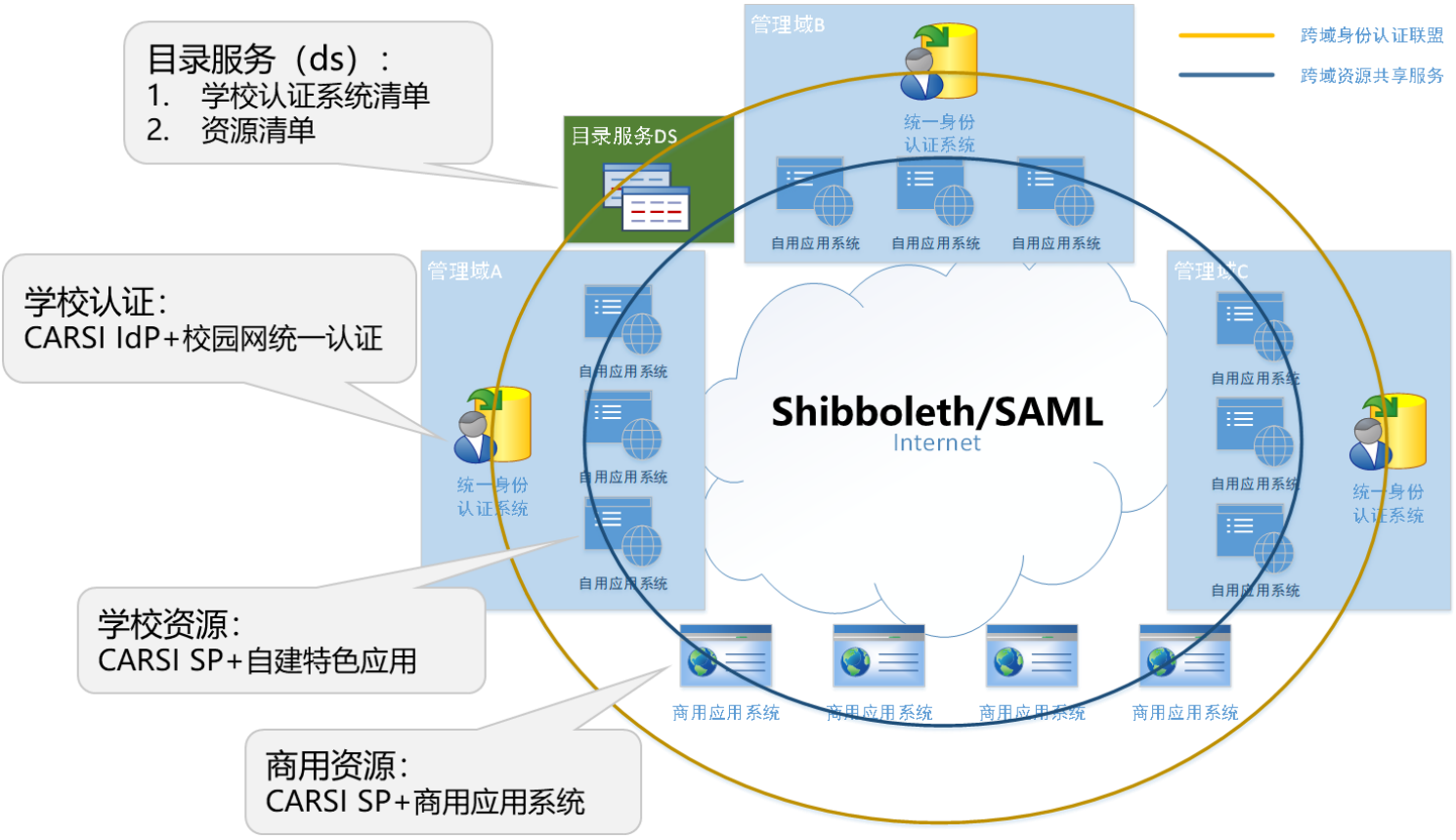


1. 用户通过浏览器访问应用系统，被重定向到CARSI目录服务去选择自己网络身份所属IdP（学校）；
2. 浏览器显示选中学校的身份认证页面；
3. 输入用户名口令、在身份所属学校完成用户认证后，将认证结果返回给应用系统。认证成功的用户进入授权后的应用系统。

Shibboleth简介

- CARSI采用的中间件
- 2000年，作为一项美国Internet2中间件对外发布，免费、开源
- 部署最广的联合身份解决方案之一，全球多个国家和地区的教育科研网普遍采用，教育行业的事实标准
- 一种基于web的单点登录技术
- 兼容现有多种认证方式，技术成熟，运维问题少
- 可应用于机构内部或者机构之间，连接用户和应用
- 特点：可达性（accessibility）、可靠性（reliability）、灵活性（flexibility）
- 在支持个人隐私保护和用户知情的前提下，支持对用户有访问授权需求的应用系统资源
- 国外资源提供方支持率高，技术基础好，国外资源部署门槛低
- https://www.shibboleth.net/

CARSI技术框架



CARSI是：

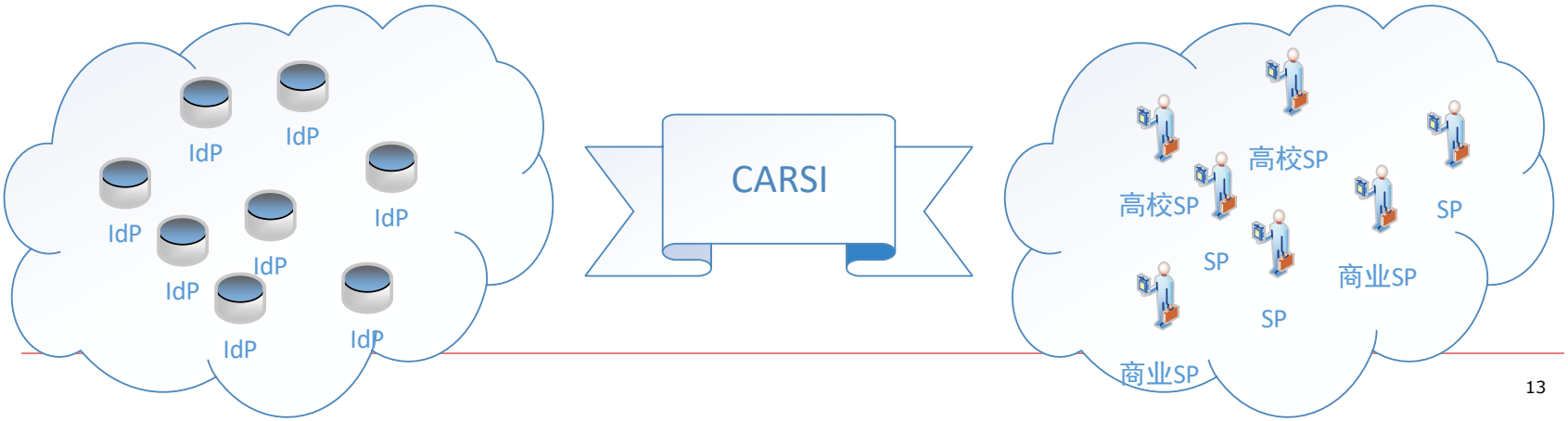
- 一个身份认证联盟
- 一项基础设施
- 一项资源共享服务

典型特征：

- 弱中心，目录服务
- 认证在学校
- 资源在厂商或学校

CARSI是什么？一个身份认证联盟

- 整合高校本地身份认证系统，形成CERNET身份认证联盟
- 一个学校配置一个IdP，对接高校校园网身份认证系统（本地认证）
  - 本地认证，已经建设完成，服务于校内信息化
  - 本地认证+IdP，支持用户以校园网身份访问CARSI资源
- 用户的CARSI身份：校园网身份
- 全球身份认证联盟eduGAIN成员，基于Shibboleth/SAML，遵循国际标准



CARSI是什么？一项基础设施

- 是一条大马路，基石是校园网身份认证系统，车是web应用
- 修CARSI这条路
  - 制定方案、做计划、形成标准（2019年5月24号，成功加入全球身份认证联盟eduGAIN）：
    - 路，怎么修，修多宽，用什么材料，遵循什么样标准，是按照自己想法修，还是参照别人成熟想法修，是否跟别人互通
    - 确定交通规则，车怎么上路，可以怎么跑
    - 体会：枯燥，见不到成效，苦功夫，需要有人做
  - 制造修路工具（管理平台开发）：挖掘机、铺路机、……
  - 修路（接入学校身份认证系统）：IdP越多，路越宽，车越愿意上来跑
  - 通车（接入应用资源）：车越多，学校觉得修这条路有意义，越愿意参与，更多种类、更大量的车愿意上来跑
  - 目前阶段：修路方案、交通规则（联盟管理模式）基本完成、已经造好主要的修路工具（管理和运行软件），路达到一定的宽度（近500所高校、450万用户），通了一定量的车（近200个资源）
- 学校：成为基石（IdP，身份提供方），校园网用户才可以坐车（SP，应用资源）
- 成果形式：CARSI高校师生便捷、安全地访问资源（乘车）
- CARSI项目目标：逐步形成IdP和SP的良性发展生态，扎实建设基础设施

CARSI是什么？一项资源共享服务

- 各种面向教育行业的、有访问控制需求的应用系统（车）
  - 图书馆类资源（公交车）：IEEE（1路）、RSC（2路）……，目前的主流应用
  - 教学科研类应用（货车）：网易云课堂（大货车）、高性能资源调度（厢式货车）……
  - 学校已建特色应用（跑车）：大学博物馆（法拉利）、校园交流平台（保时捷）……
  - 创新应用：跨校学分互认（无人驾驶车）、？？（自动送货机器人）……
- 学校角度（IdP）角度看CARSI的价值：
  - 用户使用校园网身份来访问资源，可通过CARSI访问更多的优质资源
  - 一次接入，访问CARSI平台资源（车）无其他技术门槛，接入新资源无技术调试负担
- 资源厂商（SP）角度看CARSI的价值：
  - 一个几百所高校师生可见的资源共享平台
  - 一组真实的、活的校园网用户身份，解决难于验证用户身份真实性的问题
  - 和CARSI调试一次，享用CARSI IdP高校数量增长的红利，直接带来潜在用户数量的增长
  - 与国际接轨，确定线下协议后，应用系统可直接支持国外用户访问，无需技术调试
- CARSI角度：一次IdP/SP建设可访问多个SP/IdP，学校和资源提供方共同推进资源建设

CARSI技术优势：便捷

任何人（高校校园网用户）

任何时间（白天、晚上、平时、节假日）

任何地点（学校、家里、出差路上、野外）

任何联网形式（手机流量、咖啡店Wi-Fi）

可访问CARSI应用系统/服务

CARSI技术优势：安全

安全认证：

- 个人身份信息提交给本校登录页面，身份认证在本校完成

个人信息安全：

- 用户身份信息，存储在本校
- 认证成功之后，IdP生成用户临时代码，传递给SP。SP不了解用户其他身份，可保护用户隐私。一组属性信息与一个用户临时代码对应，窃取后无价值。
- 个人信息提交给SP使用之前，需用户本人确认同意使用
- IdP系统保留用户代码和用户真实id对应关系，必要时可回溯

IdP和SP防伪冒：

- 提前本地存储的metadata文件，可以找到通信对端的基本信息
- 双向证书认证保证任何一对IdP和SP之间的互相认定

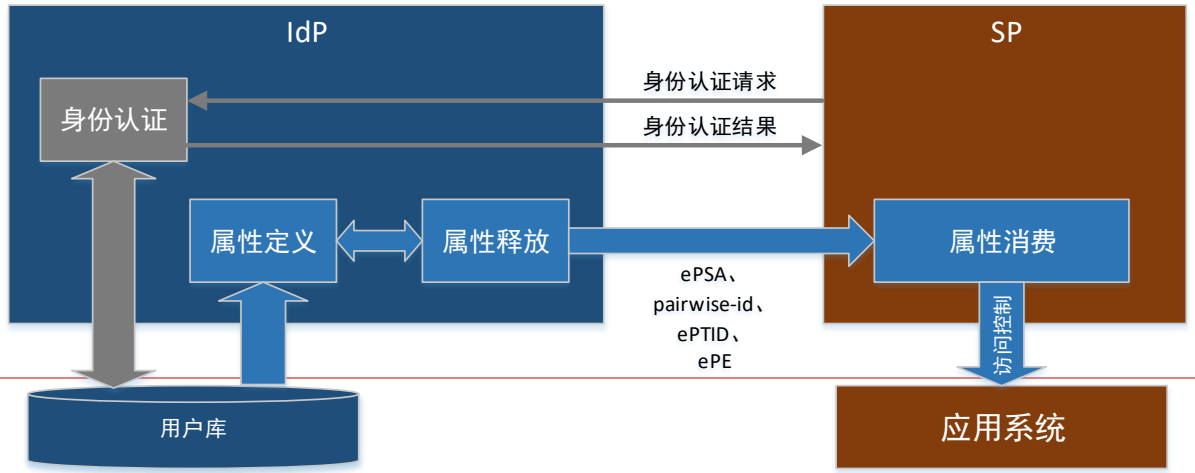
CARSI技术优势：认证和授权分离

灵活的访问控制

- 认证：IdP端单独完成
- IdP端释放属性，SP端使用属性
- 访问控制：依托于属性传递，由SP完成用户授权

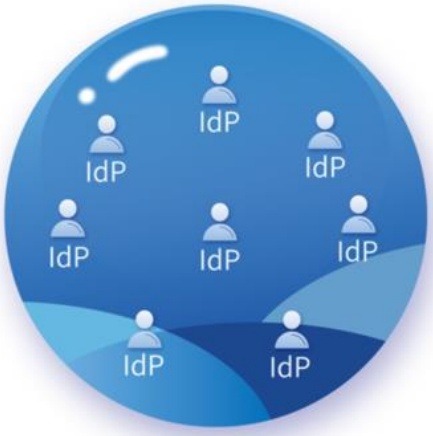
属性集

- eduPersonScopedAffiliation（核心属性），取值：faculty、student、staff……
- pairwise-id（推荐属性，替代eduPersonTargetedID），永久、可读性不强的用户唯一id
- eduPersonTargetedID（推荐属性，弃用），永久、可读性不强的用户唯一id
- eduPersonEntitlement（推荐属性），释放给某些SP，值为“common-lib-terms”



CARSI技术优势：国际化

- 全球身份认证联盟eduGAIN会员单位
- eduGAIN：欧盟发起，覆盖74个国家和地区
- CARSI机构用户可以简单接入eduGAIN资源，无需更多调试
- CARSI资源可以简单服务eduGAIN机构用户，无需更多调试



eduGAIN

4717个机构用户（IdP）

3534个资源提供商（SP）

2022年2月15日数据

CARSI服务

官网：https://www.carsi.edu.cn

交流：

- eduroam&carsi实名交流1群/2群（微信群）
- eduroam&carsi实名工作群（QQ群：459109095）

邮箱：carsi@pku.edu.cn

服务：各省赛尔分公司