CARSI服务及Shibboleth简介

北京大学CARSI开发运行小组

2020年8月

CARSI

CERNET Authentication and Resource Sharing Infrastructure

CARSI发展历史

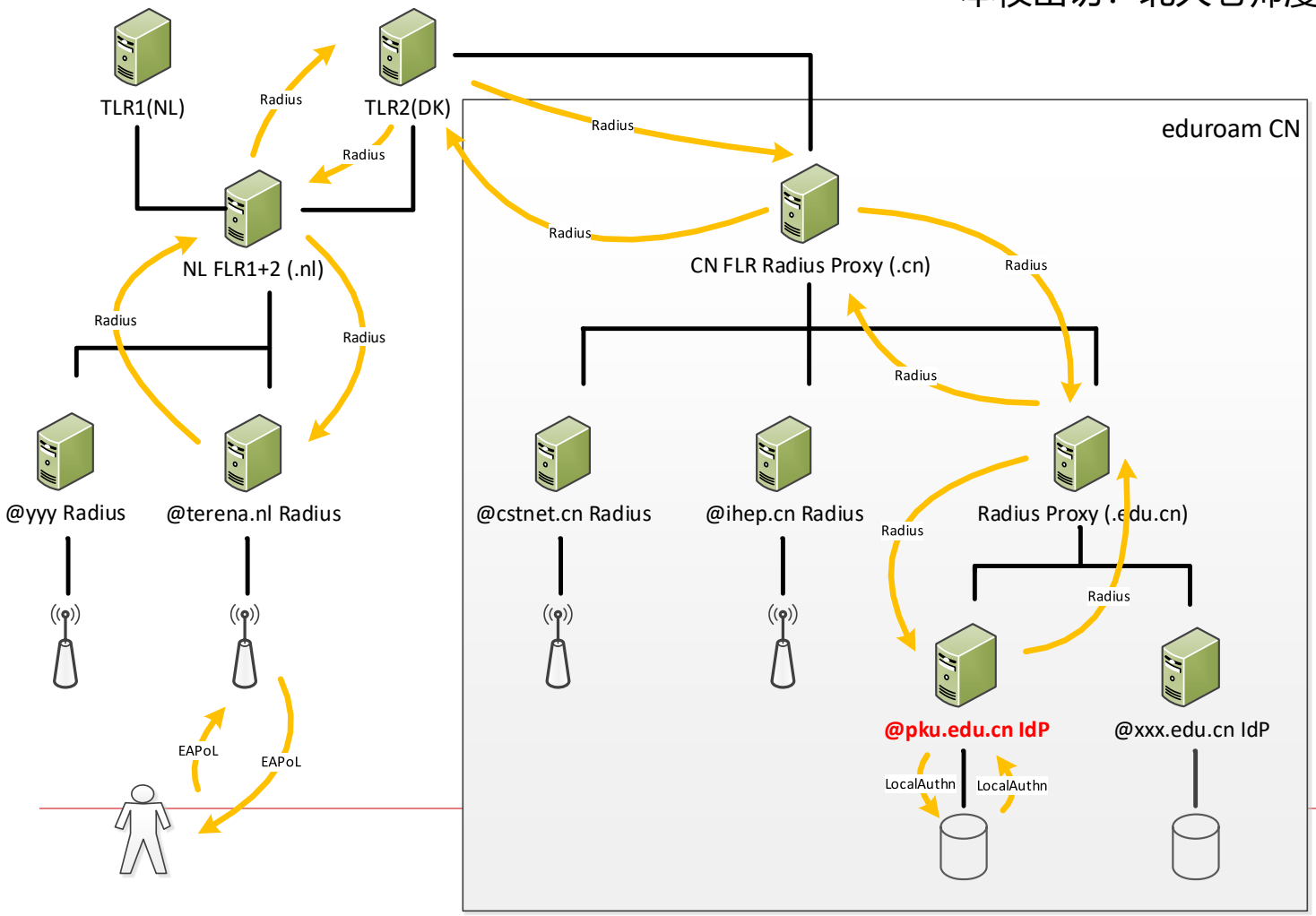
- 2006年，国家863项目支持，基于CNGI环境，小范围试验
- 2008年12月，国家发改委CNGI08项目支持，将规模扩大到30个CERNET2核心节点
- 2011年，和CALIS合作，进一步扩大规模，先后70+学校，7个国外数据库商60+服务
- 2017年8月，CERNET正式向eduGAIN提交加入申请
- 2017年11月，和eduroam一起被列入教育网基础服务
- 2019年5月24日，成功加入eduGAIN，成为full member
- 2019年10月8日，完成试验环境到产品环境过渡，作为教育网基础服务推出

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：都是基于高校身份认证的用户漫游	
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



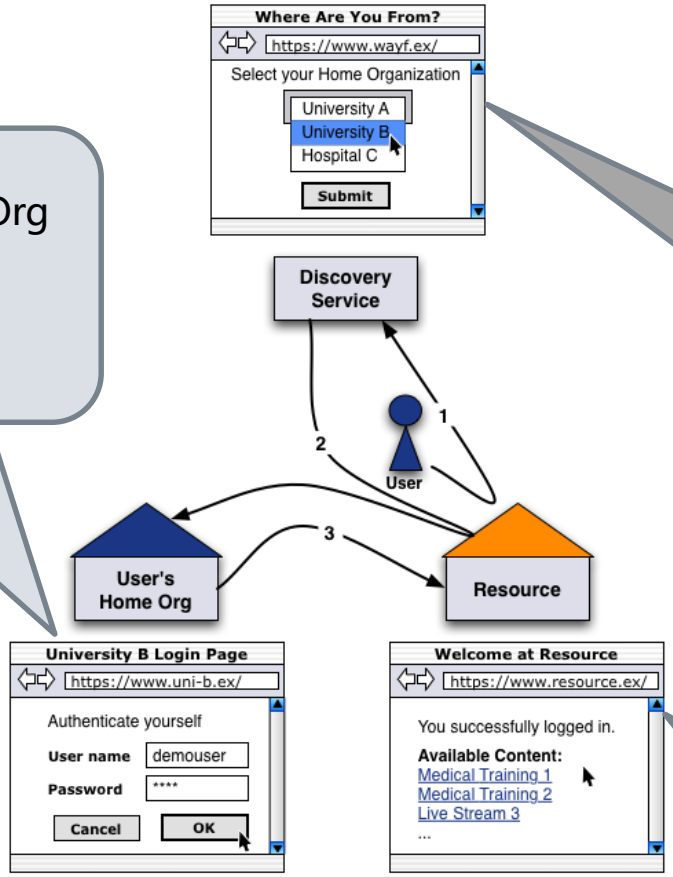
CARSI服务

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



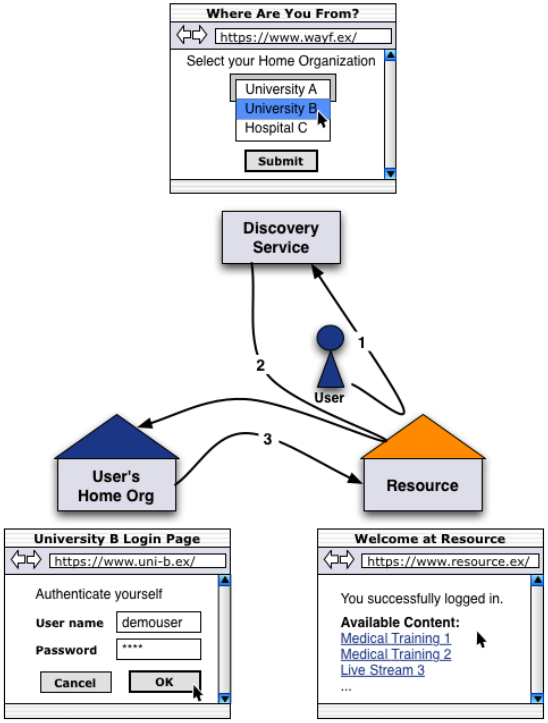
目录服务DS/WAYF

- 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



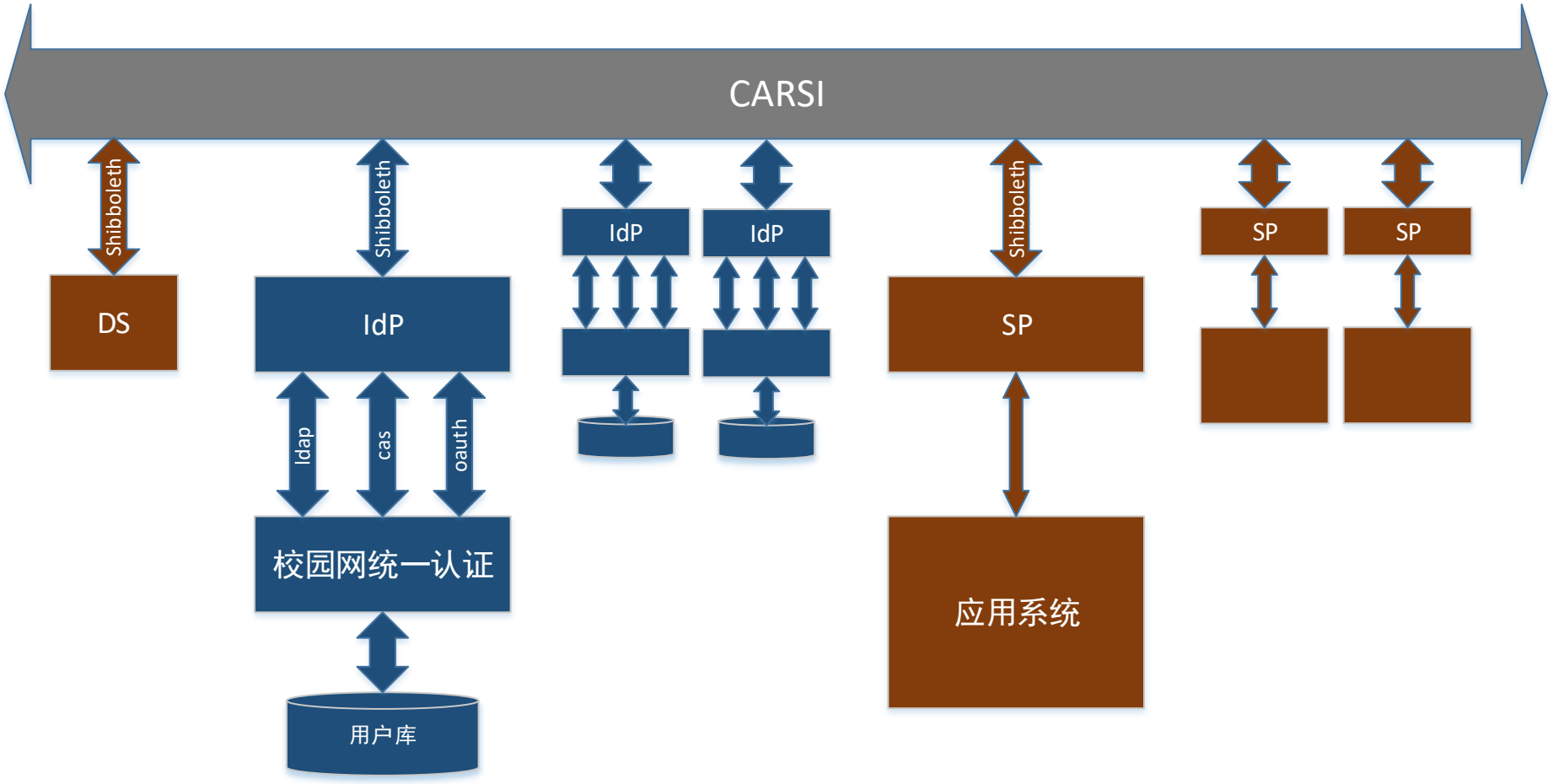
1. 用户通过浏览器访问应用系统，被重定向到CARSI目录服务去选择自己网络身份所属IdP（学校）；
2. 浏览器显示选中学校的身份认证页面；
3. 输入用户名口令、在身份所属学校完成用户认证后，将认证结果返回给应用系统。认证成功的用户进入授权后的应用系统。

Shibboleth简介

- CARSI技术基础
- 美国Internet2提供的中间件，免费、开源
- 部署最广的联合身份解决方案之一，全球多个国家地区NRENs普遍采用
- 基于web的单点登录系统
- 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
- 在支持个人隐私保护和用户知情的前提下，允许单个用户访问受保护的应用系统资源

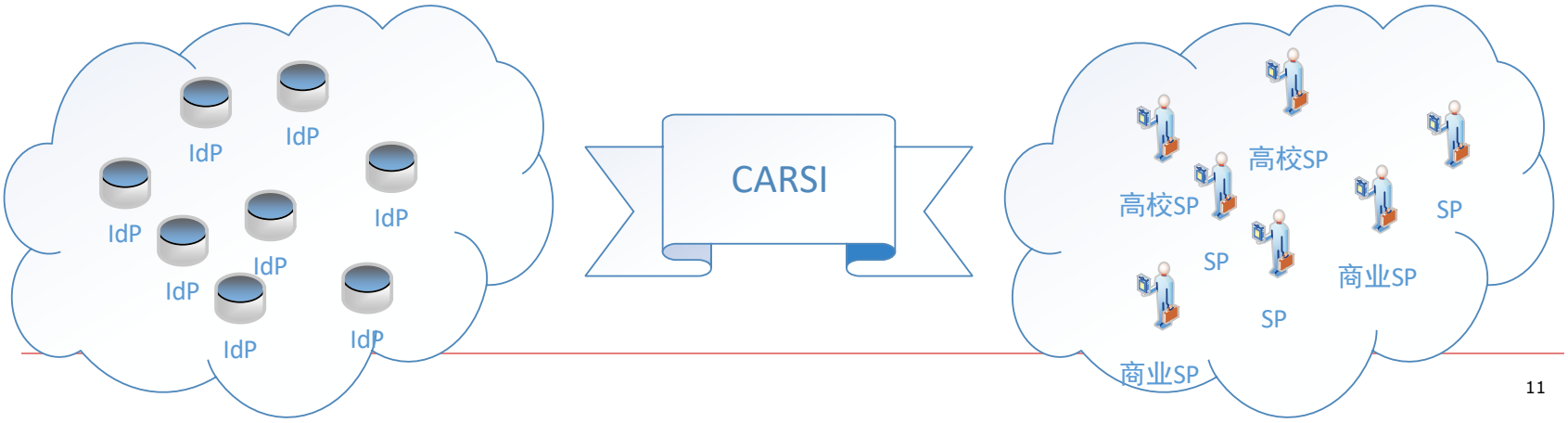
- https://www.shibboleth.net/

CARSI技术框架


CARSI
Shibboleth
DS
Shibboleth
IdP
ldap
cas
oauth
校园网统一认证
用户库
IdP
IdP
Shibboleth
SP
应用系统
SP
SP

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，遵循国际标准



CARSI是什么？一项基础设施

- 是一条大马路，基石是用户，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
- 学校：成为基石（IdP），校园网用户才可以坐车（SP）
- CARSI目标：逐步形成IdP和SP的良性发展生态

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）……
  - 学习类应用（货车）：学堂在线（大货车）、网易云课堂（厢式货车）……
  - 科研类应用（轿车）：高性能资源调度（大众）、云服务（丰田）……
  - 生活类应用（摩托车）：苹果（大摩托）、东航（电动摩托）……
  - 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）……
- 应用系统（SP）角度看CARSI的价值：
  - 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
  - 无需维护本地用户库，用户数量增长与用户管理成本不挂钩
  - 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服务技术优势：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4G、咖啡店Wi-Fi）

可访问CARSI应用系统/服务

CARSI服务技术优势：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不知道用户是谁，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。
- 用户可参与确认为哪个SP提供哪些个人属性

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

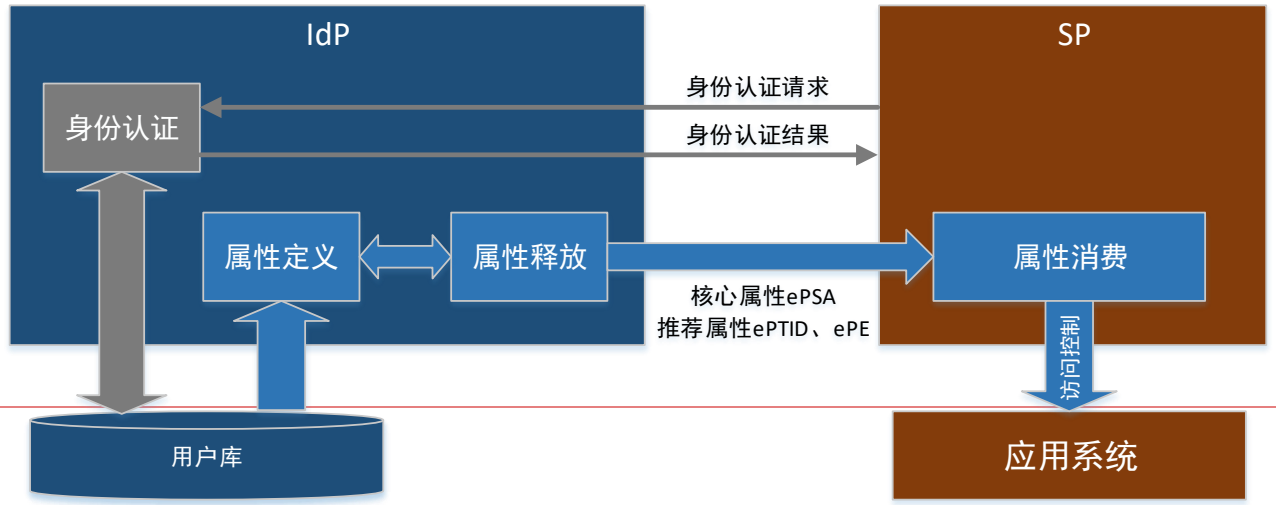
CARSI服务技术优势：灵活的访问控制

认证和授权分离

- 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……
- eduPersonTargtedID（推荐属性），永久、可读性不强的用户唯一id
- eduPersonEntitlement（推荐属性），释放给Elsevier，值为“common-lib-terms”



CARSI服务技术优势：国际化

- 基于其他国家教育科研网普遍采用的Shibboleth中间件，符合国际标准
- 国际身份认证联盟eduGAIN会员单位
- 在其他国家支持Shibboleth访问的应用系统（SP）技术上可以直接支持CARSI IdP（学校），完成业务协商即可使用
- 通过CARSI加入eduGAIN的国内应用系统（SP）技术上可支持全球eduGAIN IdP用户访问，完成业务协商即可使用
- CARSI IdP（学校）用户可以使用校园网身份访问国内外已经接入CARSI的应用系统

CARSI服务特点（2019年10月8日升级后）

- 新的部署软件
  - IdP+校园网统一身份认证支持方式：ldap、oauth、CAS
  - SP接入方式：oauth或Shibboleth
- 新的运行数据
  - 清理十余年试验阶段发展中积累的特例和不规范
  - 现有IdP和SP符合CARSI运行新要求
- 新的管理要求
  - 遵守中国相关法律法规的前提下，符合CARSI和eduGAIN标准，提升服务管理规范程度
- 新的运维方式
  - 自服务安装包、文档、管理系统为主、社交媒体交流为辅，提高主动和自动运维能力

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