教育网资源共享服务CARSI
进展汇报

陈萍 博士，教授级高工

北京大学计算中心

2019年11月14日

主要内容

- CARSI介绍
- 国外身份联盟和资源共享发展情况
- CARSI发展历史及进展
- CARSI加入流程
- CARSI近期工作

CARSI

CERNET Authentication and Resource Sharing Infrastructure

CARSI

CERNET Authentication and Resource Sharing Infrastructure

跨校身份认证（统一身份认证、联合认证）

——

基础设施

资源共享——目标

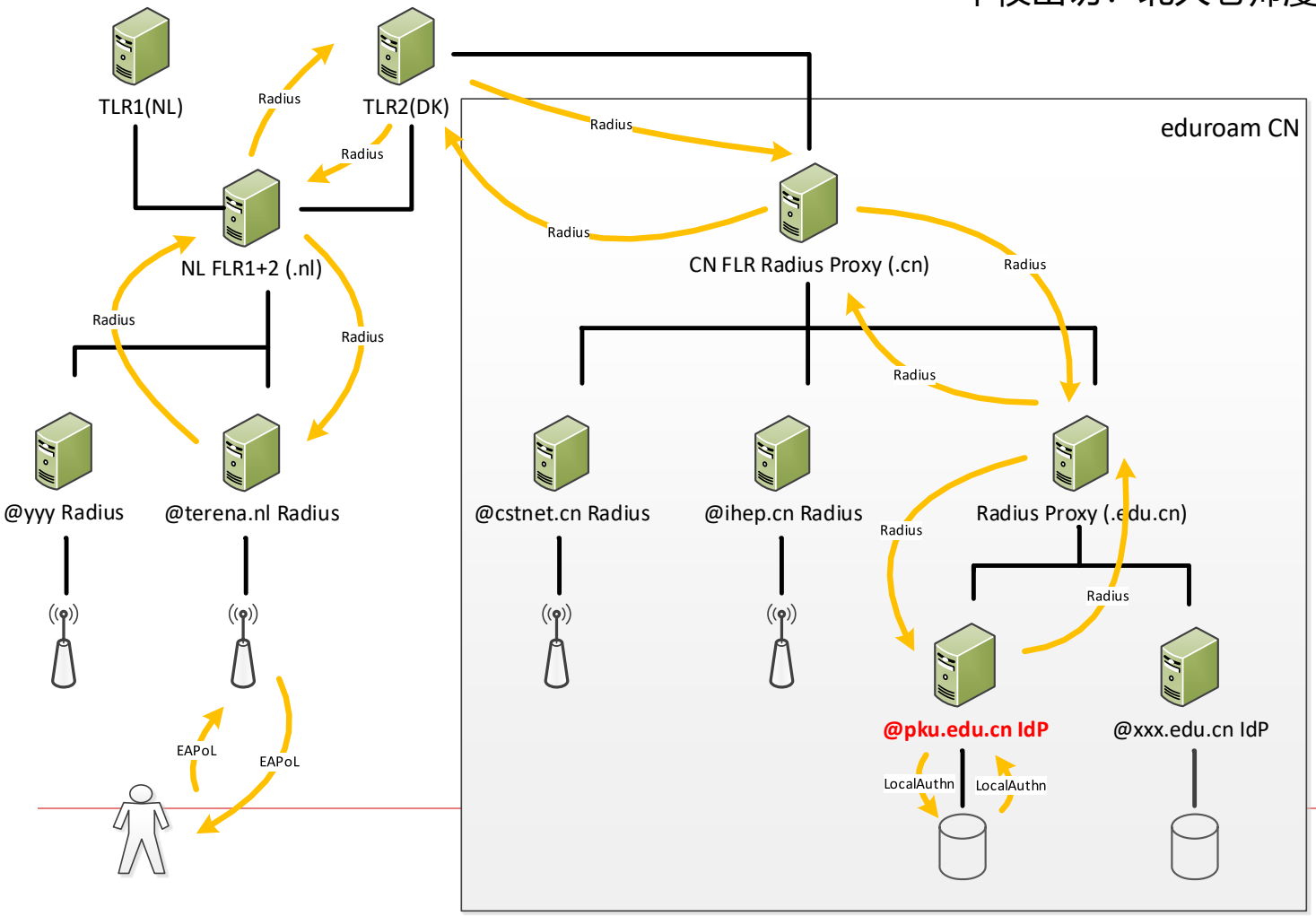
跨校身份认证——服务于——资源共享

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	

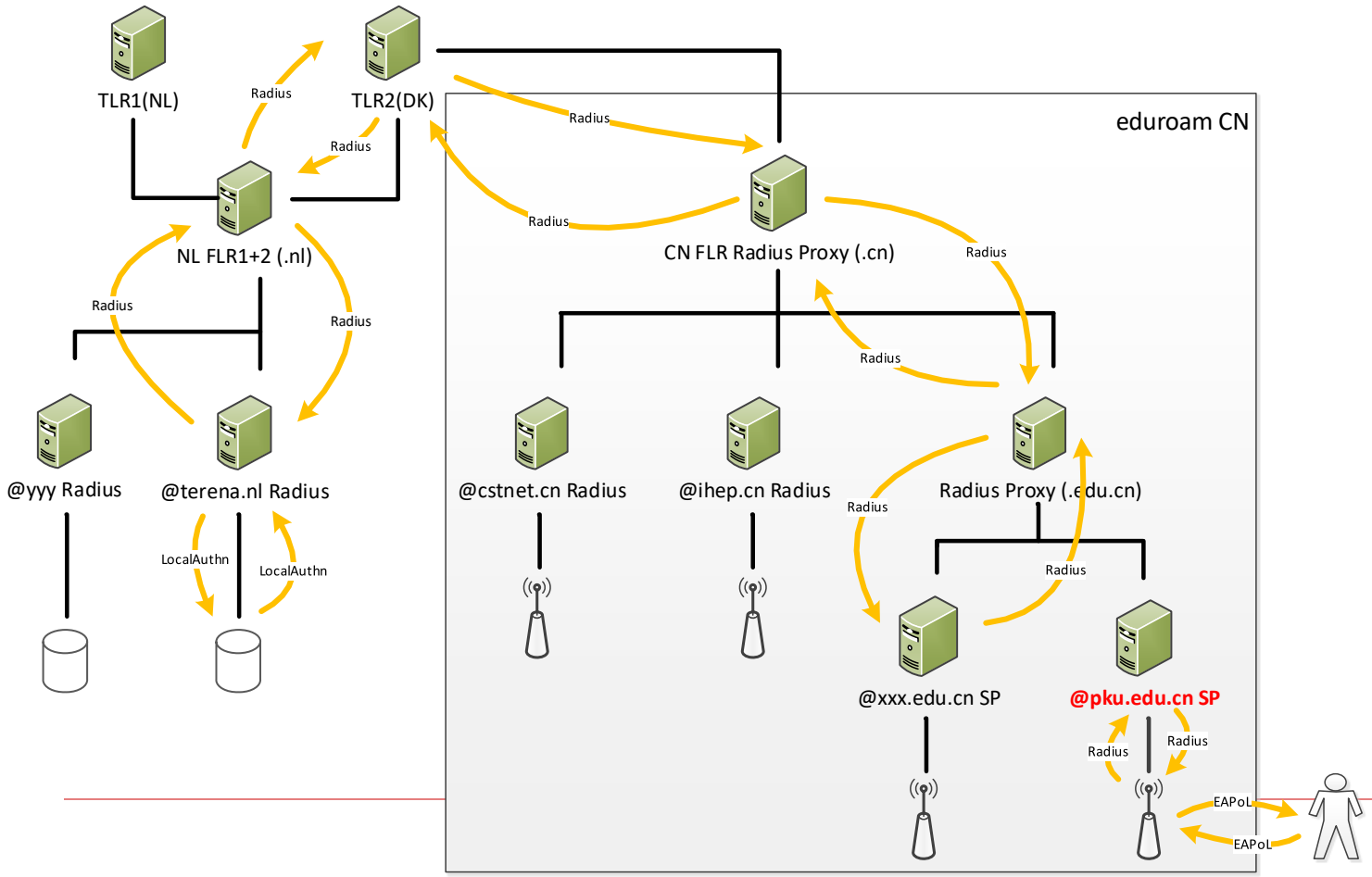
eduroam认证流程——本校出访&访客来访

本校出访：北大老师漫游到欧洲



eduroam认证流程——本校出访&访客来访

访客来访：欧洲学生参加北大暑期学校



eduroam——基于radius的全球无线漫游认证

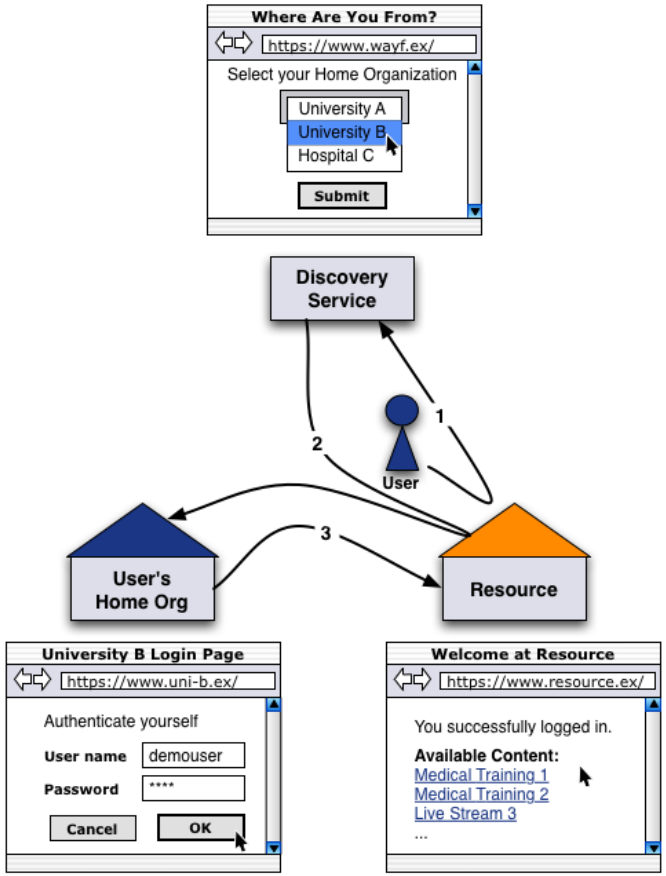
- 共享内容：
  - 全球教育科研网中的无线网
- 无线用户角度：
  - 一套身份（校园网身份），可接入全球的eduroam wifi
- Wifi提供者角度：
  - 本地不再进行身份认证，通过某种信任机制，使用认证方的认证结果
- 技术优势：
  - 用户身份：真实的、活的
  - 认证方：官方、权威、可信

radius vs saml/shibboleth

	eduroam/radius	CARSI/Shibboleth
用户身份认证	由身份所属机构radius完成	saml idp + 本地认证
认证过程通信协议	eap	saml
认证结果使用方	服务提供端radius	saml sp
认证结果使用	服务提供端radius + ac	sp + 应用系统/服务
访问控制依据	服务提供端radius属性	sp从idp获取的用户属性
访问控制	ac依据服务提供端radius属性决定	sp根据应用系统/服务根据用户在idp的属性决定
漫游范围	eduroam成员单位	任何有网的地方（如4G）
特点	仅限于无线网漫游	可扩展性强、可支持应用类型多

CARSI：应用系统资源共享

CARSI的技术基础——saml/shibboleth



- 核心组件——身份提供者IdP
  - 身份认证
  - 身份属性发放
- 核心组件——服务提供者SP
  - 基于用户属性的授权
  - 对接已有的应用系统
- 辅助组件——目录服务DS&资源门户

- 国外其他国家地区NRENs普遍采用
- 教育科研领域事实标准
- eduGAIN遵循标准

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
- 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
- 一个学校配置一个IdP，用户的CARSI身份：校园网身份
- 全球身份认证联盟成员，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（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、交通规则基本完成、已经造好主要的修路工具，需要根据实际情况不断完善
- 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

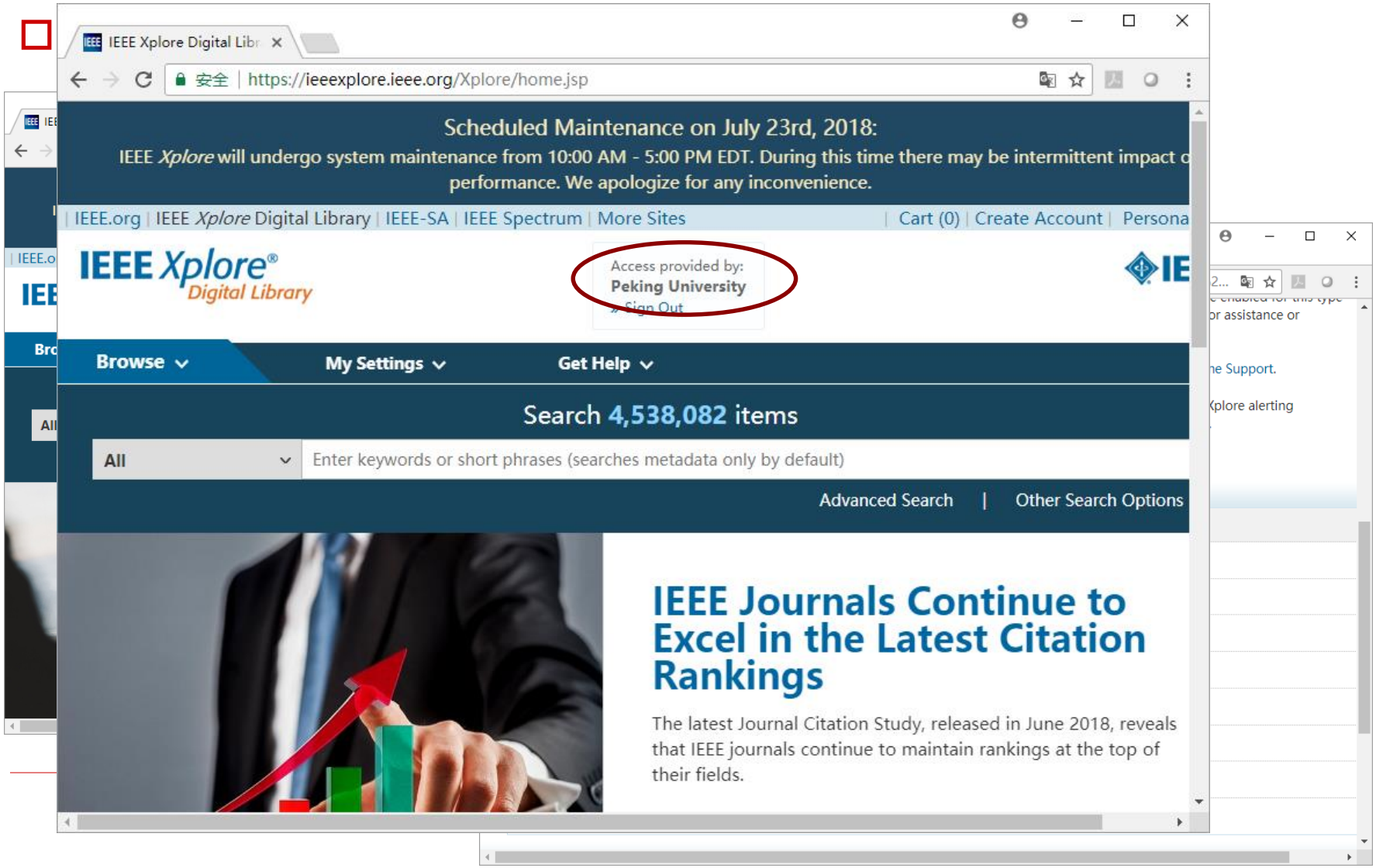
CARSI是什么？一项资源共享服务

- 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，面向海外提供服务的应用系统，确定线下协议后，可直接支持国外用户访问，无需技术调试

CARSI应用场景举例——北大用户从IEEE下载文献

- CARSI之前：
  - 图书馆已经采购IEEE资源
  - 可以在北大IP范围内随意下载
  - 人在校园网外，vpn回到校园网再下载
- 弊端：
  - 用户角度：依赖于学校vpn或者各种代理，下载不方便，增加业务关联点
  - 图书馆角度：
    - 存在使用校内IP恶意下载的情况，特别是资源采购较多的大学校
    - 数据库提供商根据黑盒信息涨价，图书馆有苦难言
    - 为了了解真实下载情况，部分高校投入大量人力物力进行统计分析，效果甚微
    - 无法把有限的学校经费服务于最需要的人群

CARSI应用场景举例——北大用户从IEEE下载文献



CARSI应用场景举例——北大用户从IEEE下载文献

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）

访问线下已经获取权限的应用系统/服务

CARSI服务——资源共享中的安全

IdP和SP之间的安全

- 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

用户个人信息的安全

- 认证过程：个人用户通过浏览器将身份提交给身份所属机构的登陆界面
- 安全级别与portal认证相同，由身份所属机构决定，取决于idp是否采用https以及证书可靠性
- 认证成功之后，IdP生成用户临时代码，在IdP和SP之间传递。SP只能获得临时代码，不知道用户是谁。

用户属性信息的传输安全

- 一组属性信息与一个用户临时代码对应。窃取后价值不大。

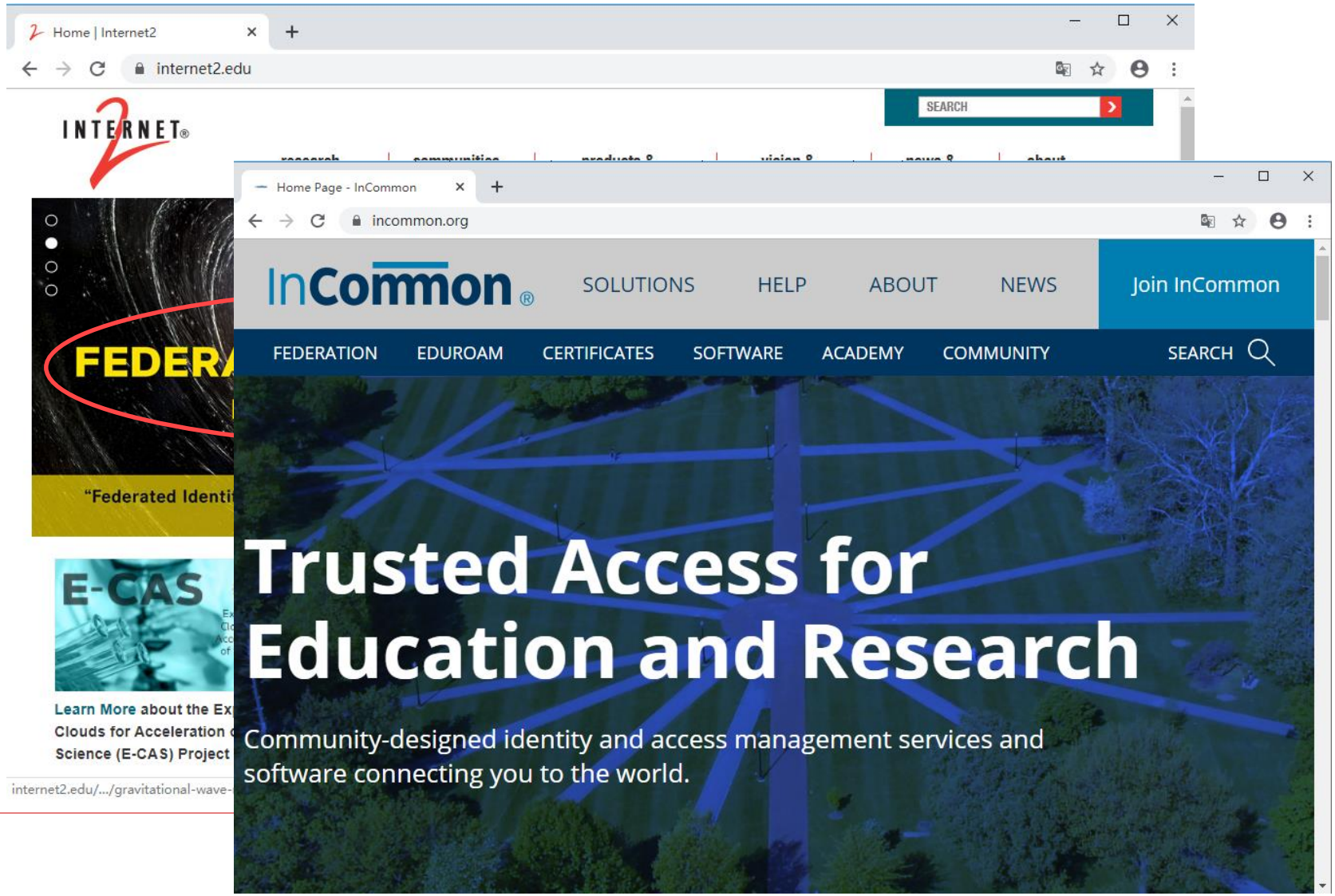
用户个人信息的隐私保护

- 用户参与确认哪些属性提供给哪个sp

主要内容

- CARSI介绍
- 国外身份联盟和资源共享发展情况
- CARSI发展历史及进展
- CARSI加入流程
- CARSI近期工作

美国Internet2



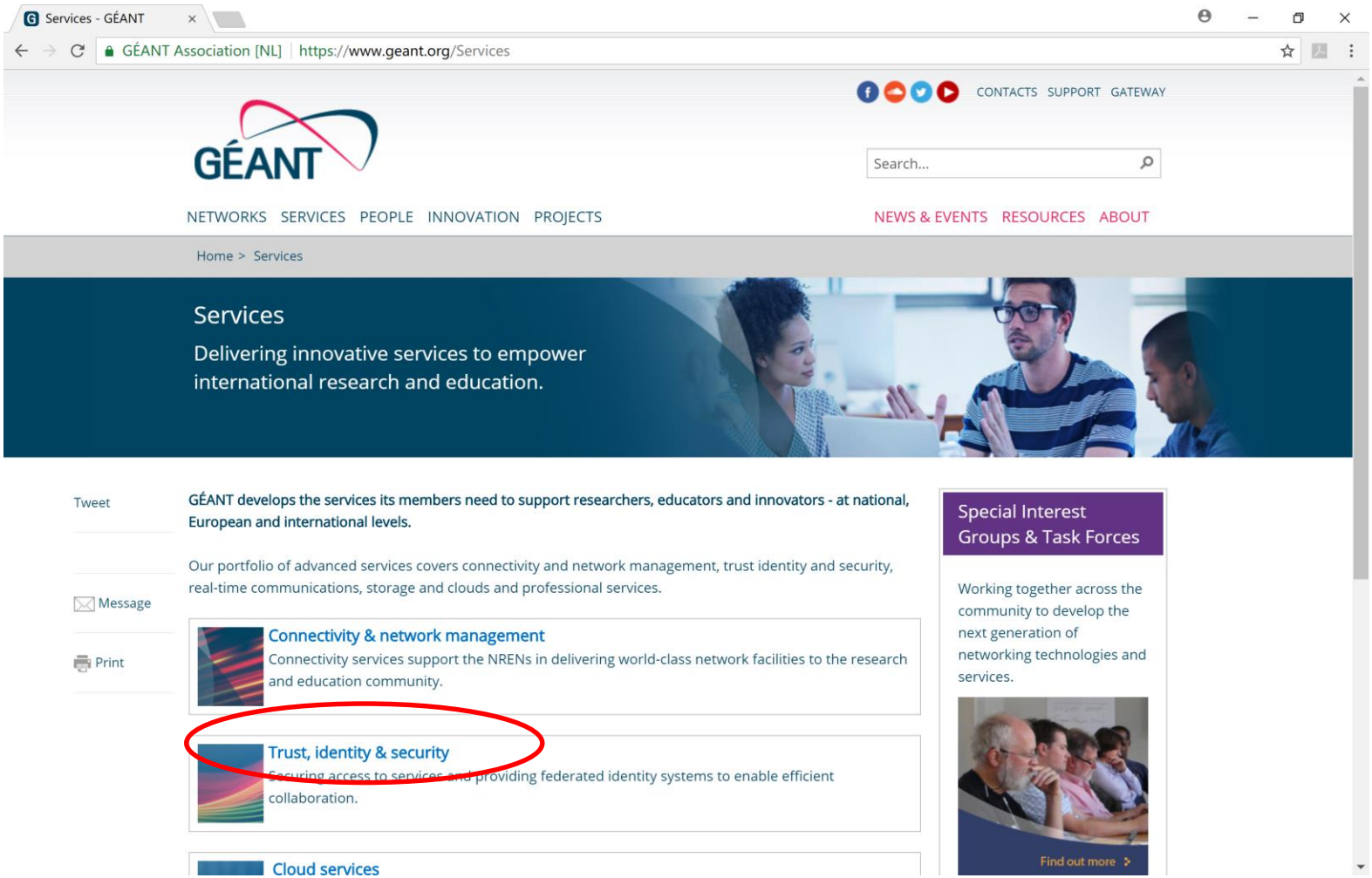
美国身份认证联盟InCommon

- Inernet2可信和身份服务的重要部分，主要面向高等教育机构、研究组织和他们的合作者提供服务

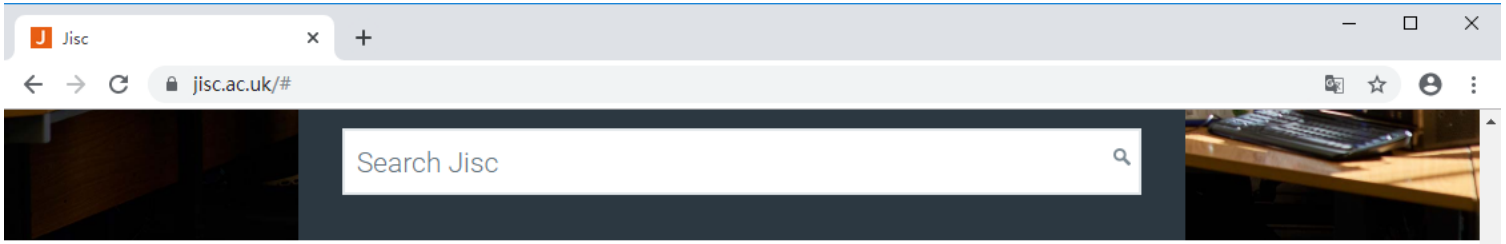
	InCommon
运行模式	商业化运行 1. 专设管理办公室 2. 一次性注册费：$700 3. 年费， 高等教育：按照卡内基分类，1个IdPs，<50SPs 目前：$5,025/$4,025/$2,575/$1,755； 2020.1：$12,000/$9,000/$6,000/$2,500 研究机构：按照全职人员，最高$3,250 合作伙伴：年营业额，最高$5,025
Orgs	767
IdPs	553
SPs	4764
成员	高等教育（656）、政府、非盈利组织、实验室、研究中心（31）、合作伙伴（284）
Certificate service	427学校，按照卡内基分类，Internet2会员年费$4,138/$3,363/$2,088/$1,468
其他典型应用	图书馆电子资源、google、微软、等

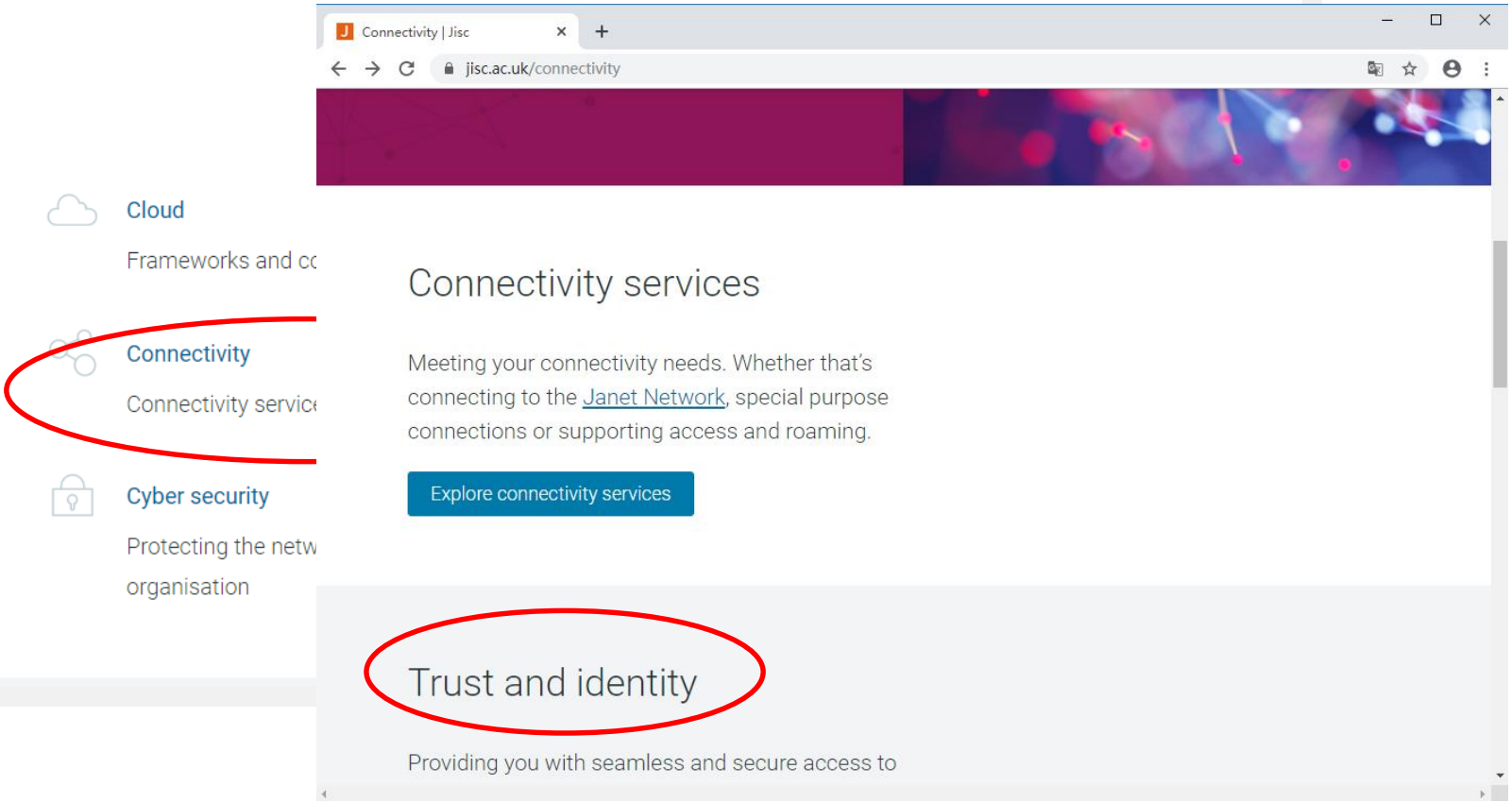
2019年11月6日，根据www.incommon.org网站数据整理

欧洲GEANT


Services - GÉANT
GÉANT Association [NL] | https://www.geant.org/Services
CONTACTS SUPPORT GATEWAY
GÉANT
Search...
NETWORKS SERVICES PEOPLE INNOVATION PROJECTS
NEWS & EVENTS RESOURCES ABOUT
Home > Services
Services
Delivering innovative services to empower international research and education.
Tweet
Message
Print
GÉANT develops the services its members need to support researchers, educators and innovators - at national, European and international levels.
Our portfolio of advanced services covers connectivity and network management, trust identity and security, real-time communications, storage and clouds and professional services.
Connectivity & network management
Connectivity services support the NRENs in delivering world-class network facilities to the research and education community.
Trust, identity & security
Securing access to services and providing federated identity systems to enable efficient collaboration.
Cloud services
Special Interest Groups & Task Forces
Working together across the community to develop the next generation of networking technologies and services.
Find out more

UK JISC


Jisc
jisc.ac.uk/#
Search Jisc


Cloud
Frameworks and co
Connectivity
Connectivity servic
Cyber security
Protecting the netw
organisation
Connectivity | Jisc
jisc.ac.uk/connectivity
Connectivity services
Meeting your connectivity needs. Whether that's connecting to the Janet Network, special purpose connections or supporting access and roaming.
Explore connectivity services
Trust and identity
Providing you with seamless and secure access to

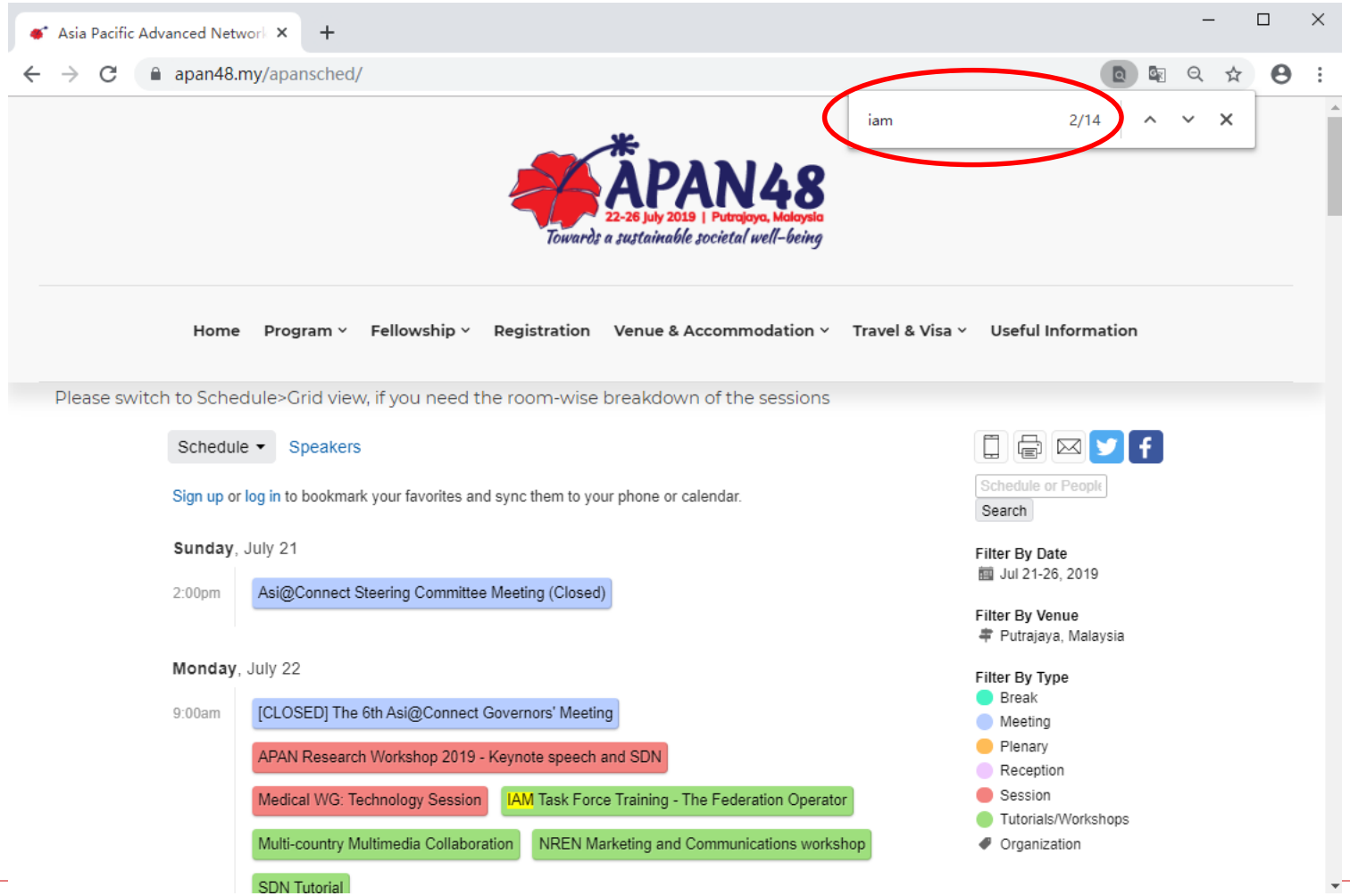
英国Access Management Federation

	UK federation
成员单位	**1175**
商业服务	**238**
是否收费	免费

- IdP收益：
  - 技术成熟
  - 改善用户服务
  - 兼容现有访问控制
  - 运维问题少
- SP收益
  - 无需维护用户库
  - 用户支持要求低
  - 运维空间要求低
- 终端用户收益
  - 用户身份简单
  - 用户信息保存可控
  - 服务提供商可以细化服务
- 教育部门收益
  - 教育行业管理一致
  - 改善用户体验
  - 专业技术人员要求少
  - 教育机构之间模式复制简单
  - 推动机构间的内容共享和合作

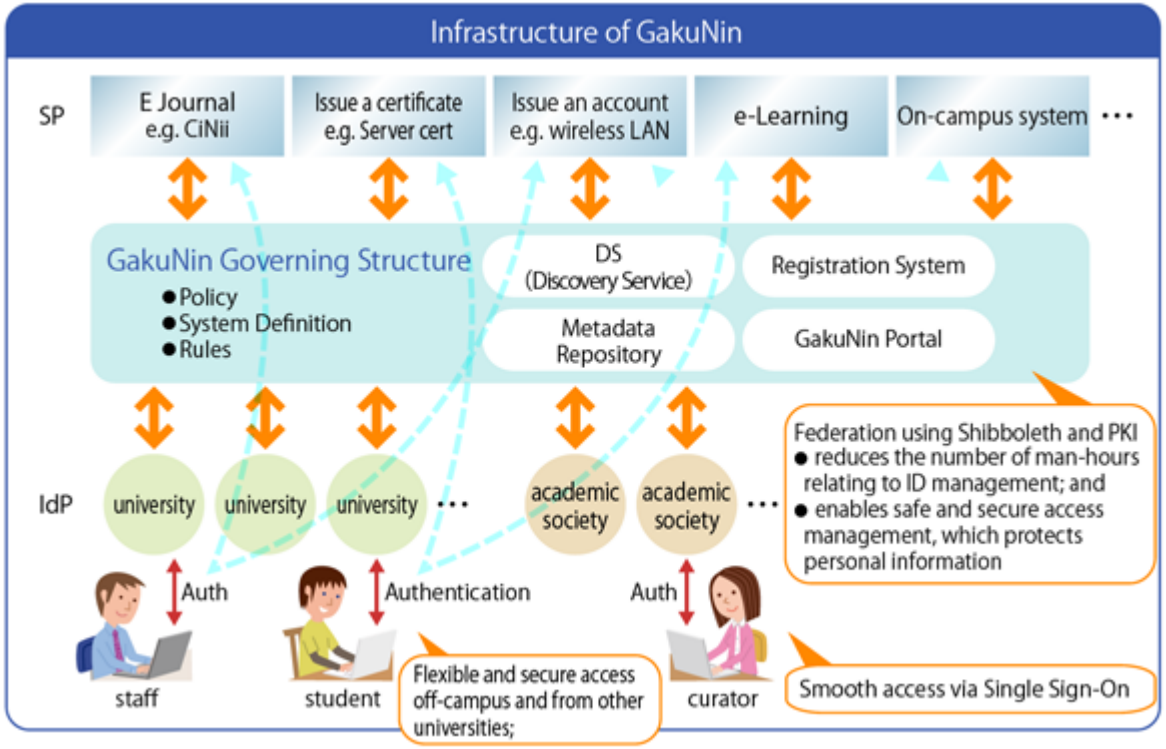
2019年11月6日，根据www.ukfederation.org.uk网站数据整理

APAN 46 PROGRAM (Aug, 05 - 09, 2018)



日本Gakunin

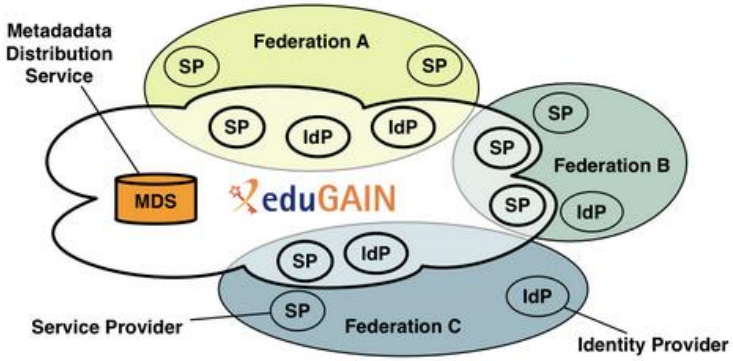
- 国立情报学研究所NII（National Institute of Informatics）主持建设



	GakuNin
IdP	228
SP	96

2019年11月6日，根据www.gakunin.jp数据整理

eduGAIN: interfederation of NREN Identity Federations

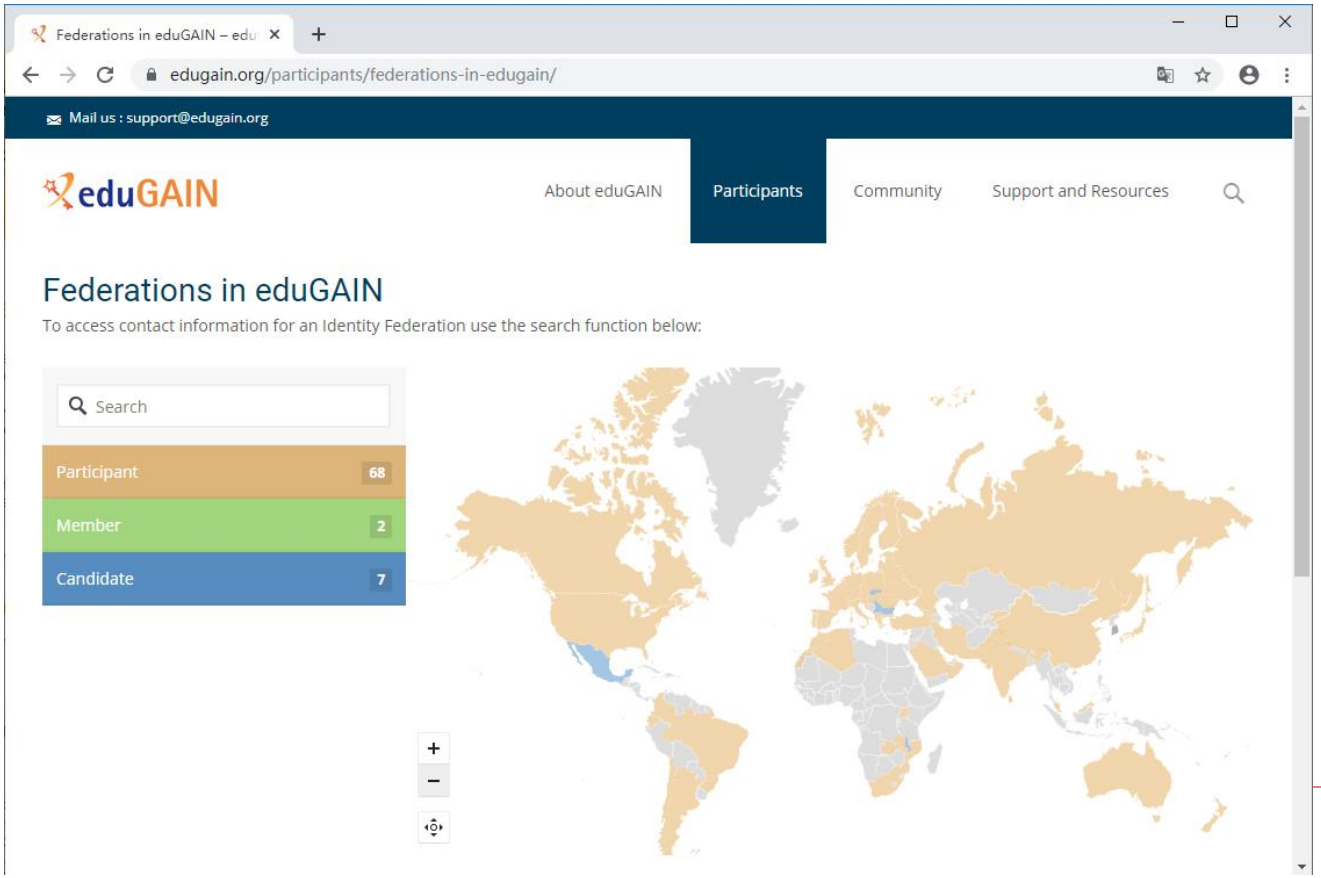


eduGAIN Service diagram - How eduGAIN works

- 欧盟发起，欧洲GEANT项目开发的网络服务之一
- 最初目标：促进欧盟和欧洲各国NREN的合作
- 实现世界各地身份联盟的互联，简化全球教育科研界的资源访问
- 技术优势：
  - 实现联盟间信息的可信交换
  - 降低开发运维新服务的成本
  - 增加已建设服务的用户规模
  - 扩大用户本校身份应用范围

全球身份认证联盟eduGAIN

68个正式成员，3148个IdP，2640个SP



Federations in eduGAIN	
Members	68
Voting-only Members	2
Candidates	7
Entities in eduGAIN	
All entities	5790
IdPs	3148
SPs	2640
Standalone AAs	4

主要内容

- CARSI介绍
- 国外身份联盟和资源共享发展情况
- CARSI发展历史及进展
- CARSI加入流程
- CARSI近期工作

CARSI发展历史及进展

- 2007年，北京大学内部试验
- 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
  - 新的软件版本，支持高校部署较多的ldap、oauth、CAS本地认证，支持oauth方式接入SP
  - 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，要求现有idp和sp全部符合新标准
  - 新的管理要求，遵守中国法律法规的前提下，符合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，提高自动运维能力

发展CARSI的时机已经成熟

- 基础具备：
  - 大部分高校校园网已部署统一用户管理和身份认证系统
  - 部分高校已建设特色应用，存在扩大影响力和访问量的蓄力和需求
- 高校发展内驱力开始萌芽，在部分地区已经蓬勃发展：
  - 高校基本完成网络基础设施建设，更多关注资源建设
  - 高校国际化发展的需要，有技术上跟国际接轨的需求
  - 近几年eduroam在教育网的快速发展，以无线网为切入点，让更多人了解并体会资源共享，从侧面推动了CARSI的发展
  - 上海跨校认证实施多年，东北片跨校选辅修、东航机票打折、等成功案例
  - 其他省市在建跨校联合项目
  - 截止11月11号，19个学校IdP已上线，约60-80万用户可按照此方式访问资源

发展CARSI的时机已经成熟

- 国外SP发展动力雄厚：
  - 在国外，NREN身份联盟技术已成熟多年，国外资源提供商认可身份共享技术
  - eduGAIN有68个成员、2640个SP，国外教学科研主流应用系统技术上均支持
  - CARSI加入eduGAIN，为有意在中国发展的国外厂商打通了技术通路
  - 截止10月8日，5个国外图书馆电子资源厂商成功升级，占试验期厂商70%
    - EBSCO、EMERALD、IEEE、RSC、SPRINGERNATURE
  - 少量其他应用在接触
- 国内SP发展初见端倪：
  - 新增2个国内SP，知网、并行科技
  - CALIS正在讨论通过CARSI部分解决它的用户身份认证问题
  - 阿里云、钉钉、百度云等沟通过的厂商普遍认可技术先进性

CARSI服务成员清单

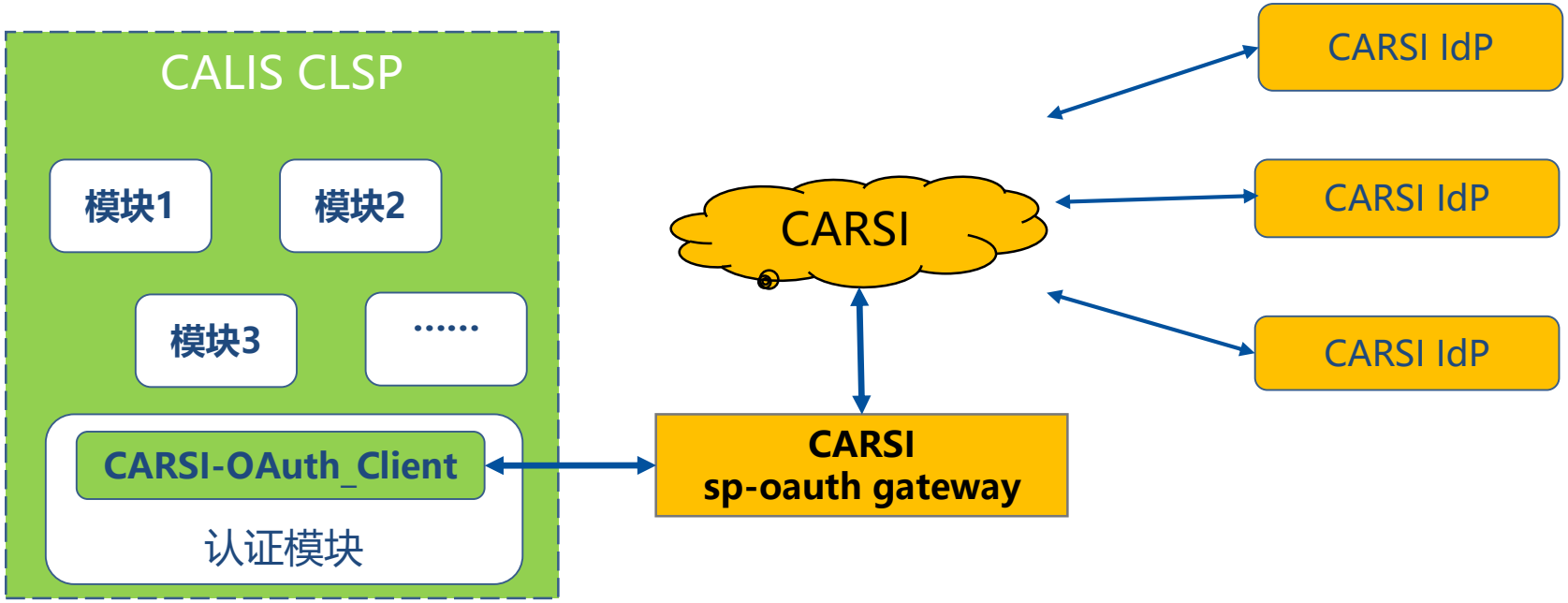
服务提供商SP（7厂家44项服务）	
知网	国内电子资源
并行科技	国内高性能计算资源
EBSCO	国外电子资源
EMERALD	国外电子资源
IEEE	国外电子资源
Royal Society of Chemistry	国外电子资源
SPRINGERNATURE	国外电子资源

2019年11月13日数据

学校IdP（21上线+21调试中）		
1	北京大学	2019-06-01
2	厦门大学	2019-06-25
3	沈阳农业大学	2019-07-15
4	中国科学技术大学	2019-07-26
5	山东大学	2019-09-20
6	华东师范大学	2019-09-23
7	重庆建筑工程职业学院	2019-09-26
8	西交利物浦大学	2019-10-08
9	北京师范大学	2019-10-17
10	长春理工大学	2019-10-18
11	河南师范大学新联学院	2019-10-21
12	浙江工商大学	2019-10-23
13	上海财经大学	2019-10-29
14	浙江大学城市学院	2019-10-30
15	天津大学	2019-10-31
16	中国人民大学	2019-11-04
17	清华大学	2019-11-05
18	武汉大学	2019-11-11
19	上海师范大学	2019-11-11
20	深圳大学	2019-11-12
21	大学数字图书馆国际合作计划	2019-11-13

CARSI+CALIS

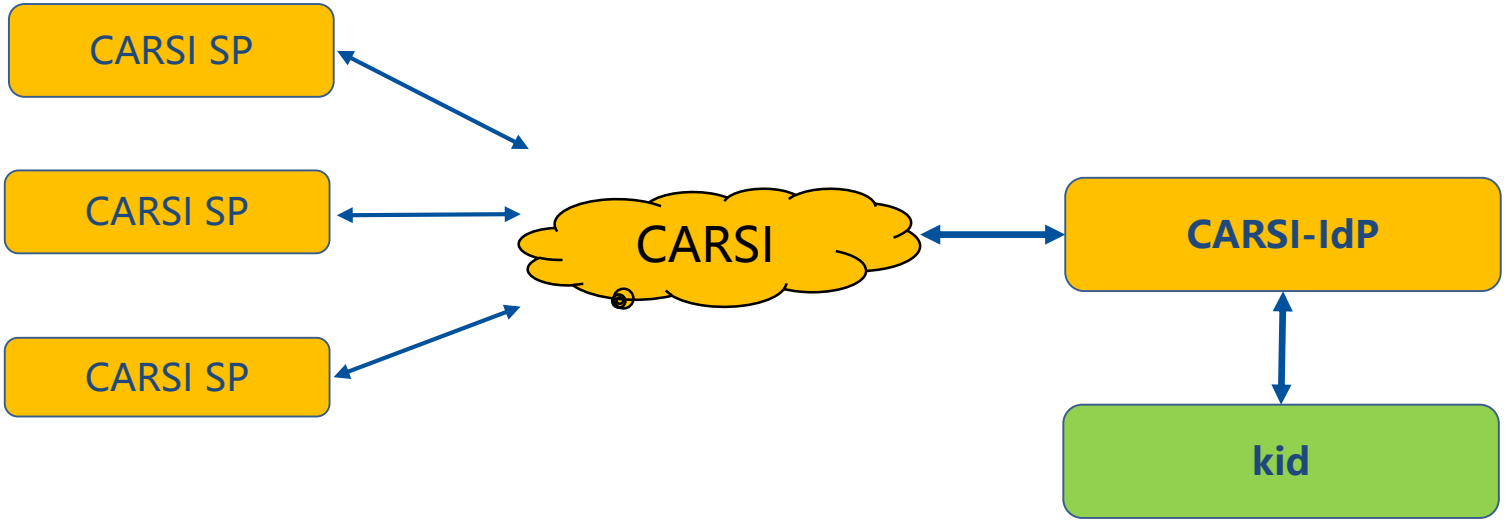
CALIS —— CARSI SP



本论坛“CALIS新一代图书馆服务平台与CARSI认证集成方案”

CARSI+中国工程学者kid

kid —— CARSI IdP



本论坛“基于学者唯一标识符的应用实践”

国内数字资源提供商——知网

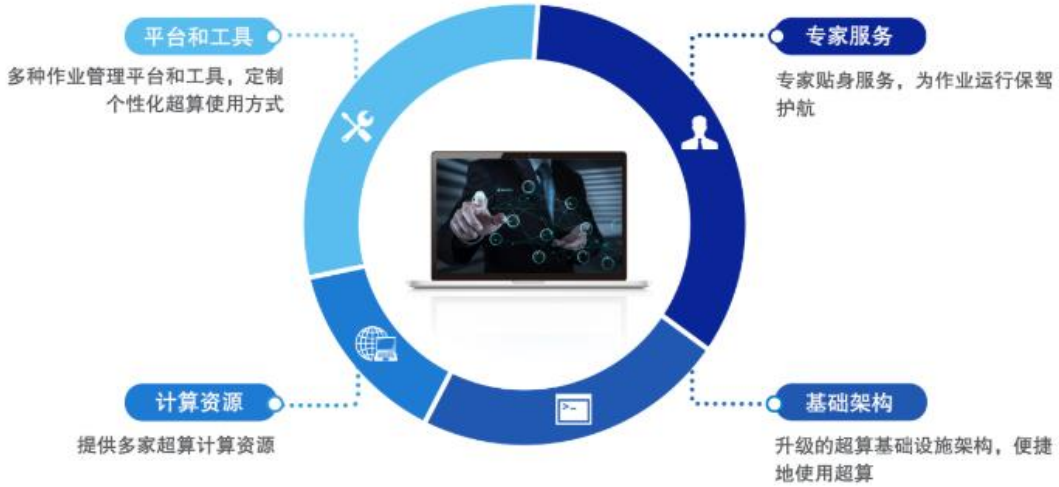
- 知网CNKI，世界上全文信息量规模最大的数字图书馆，包括：
  - 研究型资源，如期刊、论文、专刊、国际行标、项目成果、法律法规、案例、报纸；
  - 学习型资源，如各类字词典、专业百科、专业辞典、术语；阅读型资源，如文学、艺术作品与评论，文化生活期刊；
  - 其他
- 90%以上国内高校采购知网产品

CARSI+知网

- 知网初衷：
  - 企业目标：不断追求和提升用户服务质量和水平，切实解决用户所需
  - 符合知网产品发展趋势，基于ID认证、深入到团队的个人用户产品
  - CARSI正式加入eduGAIN，有助于知网更好地服务上千家海外用户，拓展海外市场
- 使用方式：http://fsso.cnki.cn
  - 按IP地址限制访问权限（现有）+按用户身份进行访问（补充）
  - 电子资源访问更方便：CARSI用户，依托校园网真实身份，随时（白天、晚上、平时、节假日）、随地（学校、家里、出差路上、野外）、以任何联网形式（手机4G、咖啡店Wi-Fi）下载所需文献。
- 注意：可访问电子资源范围与学校图书馆采购方案一致

HPC服务提供商——并行科技

- 并行超算云，一站式超算云平台
- 网络基础：教育网全国超算中心互联项目
- 基于IPv6网络建设全国超算互联网，直通各大超算中心与数据中心
- 搭建高速专用数据传输通道，突破远程高速数据交换的瓶颈
- 满足教育科研行业多、快、好、省的计算需求，支撑高校基础科研



CARSI+并行超算云

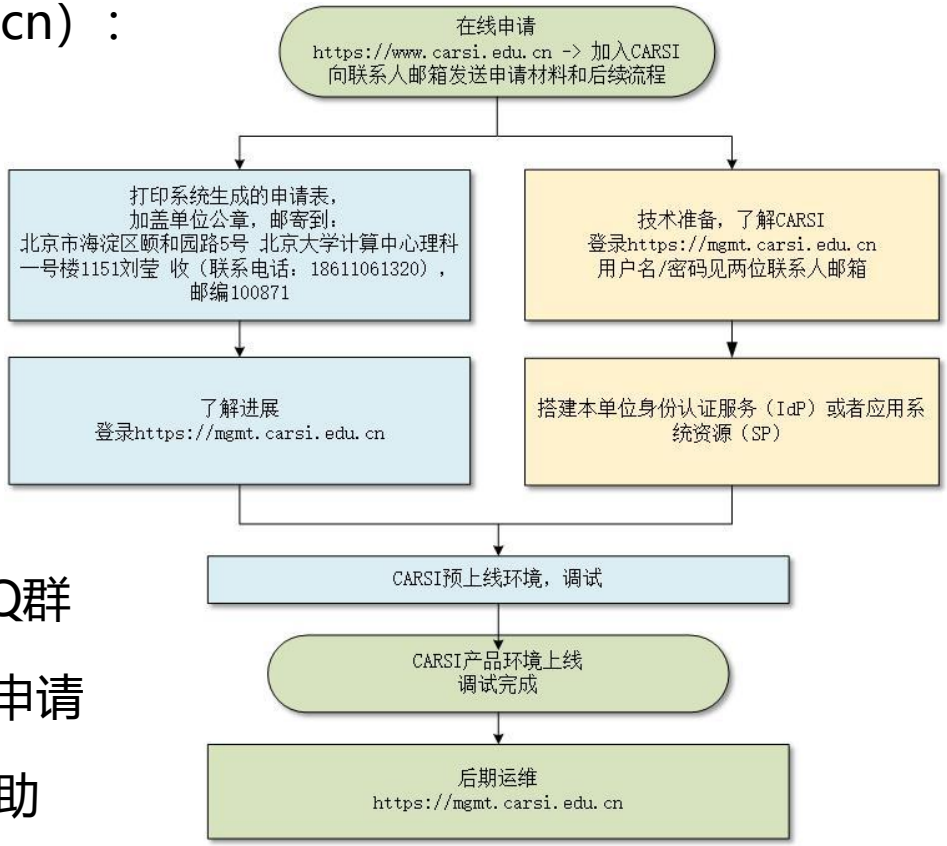
- 大大降低超算云平台与高校对接用户认证系统的工作量
  - 避免了与各高校单独做一次认证系统的对接
  - 减轻了与高校90%以上的对接工作量
  - 为超算云平台和超算互联网络的推广铺平了道路
  - 极大加速了高校基础科研的超算生态环境建设
- 方便用户使用
  - 用户可使用本人校园网身份在任何时间、任何地点、使用任何联网方式，直接登录超算云平台，使用超算互联网络
  - 突破只有特定IP地址可访问的限制
  - 为教育科研工作创造高效便捷的计算环境。
- 高校的统一身份认证通过CARSI访问并行超算云更安全可靠

主要内容

- CARSI介绍
- 国外身份联盟和资源共享发展情况
- CARSI发展历史及进展
- CARSI加入流程
- CARSI近期工作

加入CARSI（https://www.carsi.edu.cn）

- 2019年10月8日之后，新服务、新规则
- 申请流程（https://mgmt.carsi.edu.cn）：
  1. 在线提交申请
  2. 邮寄申请材料，同时启动技术调试
  3. 线上提交metadata文件
  4. 预上线环境，调试
  5. 产品环境上线



- 通过当地赛尔工程师加入微信群和QQ群
- 试验阶段加入过CARSI的学校需重新申请
- 重视通知邮件，按照邮件提示寻求帮助

加入CARSI（https://www.carsi.edu.cn）

全资格会员

- CERNET会员单位
- 面向中国大中小学、教育行政管理部门和教育科研机构
- 必须且只能部署一个IdP
- 可部署多个SP
- 只接收网络中心或图书馆提交的申请

服务提供会员

- 全资格会员推荐
- 对教学科研领域感兴趣、致力于为CARSI提供服务
- 只部署SP

CARSI——idp部署

三封邮件

1、在线注册成功，学校可开始技术调试

2019/8/28 (周三) 16:00

CARSI Admin <carsisender@pku.edu.cn>

" 大学"CARSI在线注册成功，欢迎加入！

收件人 .edu.cn

抄送 carsi@pku.edu.cn

PDF .edu.cn-app...

，您好！

欢迎 大学 加入CARSI资源共享服务！您已完成在线注册，请继续以下流程：

1. 打印附件材料，负责人签字、盖章后，邮寄到：北京市海淀区颐和园路5号北京大学计算中心理科一号楼1151刘莹（联系电话：18 320），邮编100871（为了确保邮件准时到达，建议使用顺丰）；

2. 登录CARSI会员自助服务系统，用户名： .edu.cn， 密码：项目负责人手机号，建议您首次登陆后修改密码。

3. “调试帮助”页面提供了帮助文档，供您参考。

祝CARSI部署调试顺利，

北京大学CARSI开发运行团队

CARSI——idp部署

三封邮件

1、在线注册成功，学校可开始技术调试

2、收到邮寄材料，完成审核，学校可预上线环境测试

2019/10/5 (周六) 15:02

CARSI Admin <carsisender@pku.edu.cn>

全资格会员"、 大学"通过审核

收件人 .edu.cn

抄送 carsi@pku.edu.cn

，您好！

. edu. cn 全资格会员申请已通过审核，您现在可以：

1. 访问https://mgmt.carsi.edu.cn/frontend/web/docs/idp3_ldap_install_v1.0.ova，下载IdP安装包，参照安装文档，本地安装调试IdP服务；

2. 登录CARSI会员自助服务系统，上传IdP元数据文件；

3. 开始IdP加入CARSI技术调试；

4. 在预上线环境（https://dspre.carsi.edu.cn/)试验访问；

5. 试验成功后，请发送邮件给 carsi@pku.edu.cn，申请在CARSI产品环境上线。

6. 同时，可通过CARSI会员自助服务系统，修改注册信息、添加/管理SP，将更多本单位特色应用共享给其他CARSI会员单位用户使用。

CARSI——idp部署

三封邮件

1、在线注册成功，学校可开始技术调试

2、收到邮寄材料，完成审核，学校可预上线环境测试

3、产品环境上线，完成调试

2019/10/17 (周四) 17:32

CARSI Admin <carsisender@pku.edu.cn>

" 大学"IdP产品环境上线

收件人 .edu.cn; .bnu.edu.cn

抄送 carsi@pku.edu.cn

，您好！

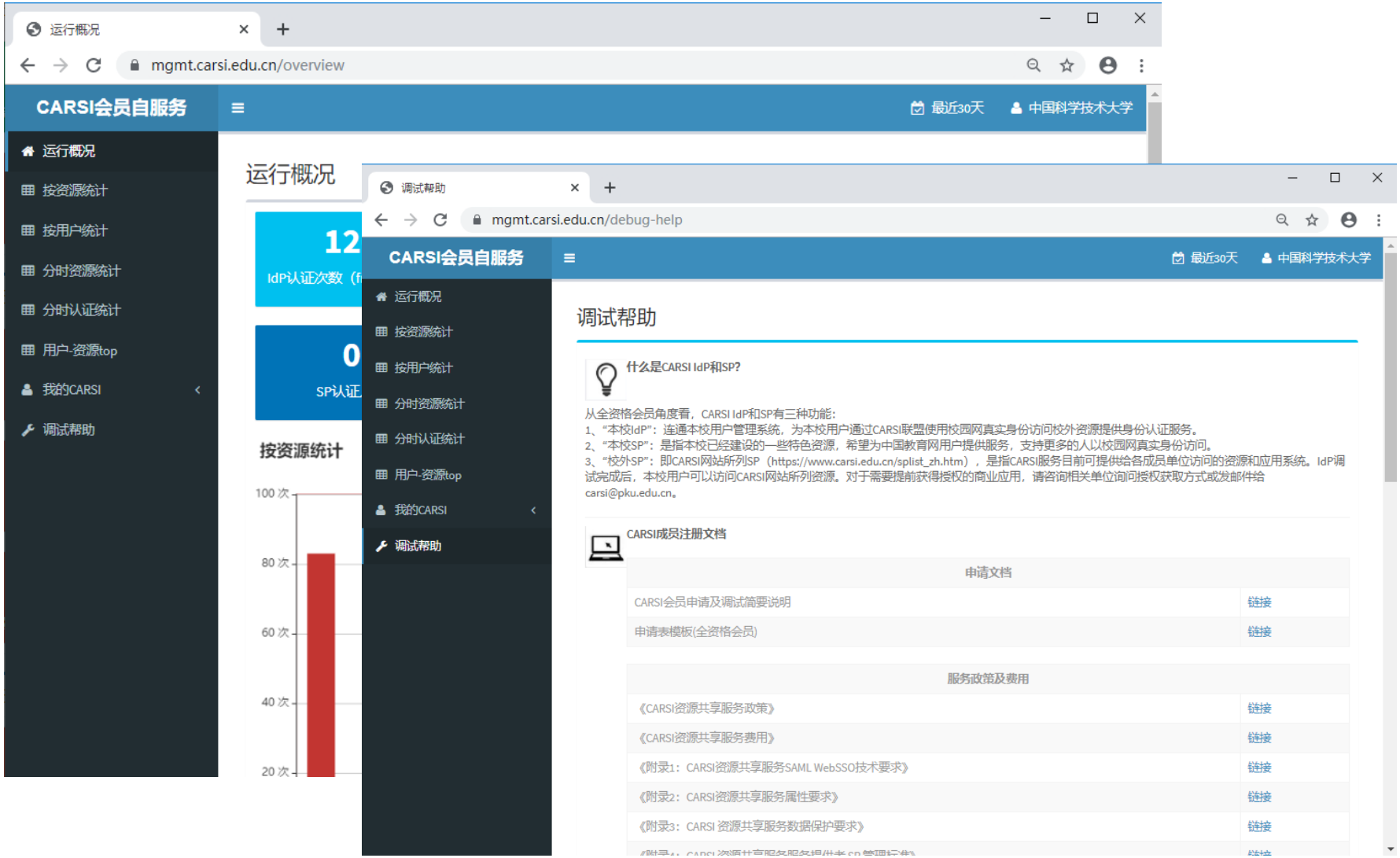
恭喜您！IdP服务 “idp. .edu.cn” 已在CARSI产品环境上线。请参照学校开通Shibboleth服务流程向SP提交服务开通申请。

后续，可通过CARSI会员自助服务系统，修改注册信息、添加/管理SP，将更多本单位特色应用共享给其他CARSI会员单位用户使用。

祝CARSI服务运行顺利，

北京大学CARSI开发运行团队
2019-10-17

CARSI——idp自服务调试及运维



CARSI——idp自服务调试及运维

本论坛“在高校部署CARSI服务相关技术介绍”

技术文档：https://github.com/carsi-cernet/doc

主要内容

- CARSI介绍
- 国外身份联盟和资源共享发展情况
- CARSI发展历史及进展
- CARSI加入流程
- CARSI近期工作

CARSI近期工作

- 目标：“社区驱动，共同发展”
- 技术开发：北京大学为主、更多老师参与
- 运维：更简单易懂的形式，如培训视频、面对面培训、文档、等
- 推广：更多的应用系统资源
  - 来自国外和eduGAIN的免费资源
  - 来自国外教学、科研、生活相关商业应用
  - 来自国内的成熟应用，如CADAL数字资源、商业云服务等
  - 来自学校的、具有扩大访问需求的特色应用
- 目前：一辆刚刚启动的重载车，已经迈出了几步
- 发展：一个平台，可着力的点很多，更多参与、更多火花、更多资源

CARSI服务

该二维码7天内(11月20日前)有效，重新进入将更新

CARSI官网：https://www.carsi.edu.cn

CARSI自服务系统：https://mgmt.carsi.edu.cn

服务开发&运行维护：北京大学

用户服务&市场推广：赛尔公司、北京大学

沟通交流：

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

工作邮箱：carsi@pku.edu.cn

Cerpark下一代互联网创新基地—创课天地

www.ctrunk.cn