中国教育和科研计算机网 CERNET
认证和资源共享基础设施 CARSI
资源共享服务政策（试行）

第 1.3 版

作者	陈萍、王博
版本号	1.3
文件状态	草稿
修改日期	2021 年 9 月 1 日

目录

文件修订历史

版本	修订日期	修订说明	修订人	审阅人
1.0	2019 年 5 月 6 日	第一稿	陈萍、万里、吕洁	
1.1	2019 年 9 月 12 日	在“附录 2：属性要求” 4.2 节“推荐属性”中添加 eduPersonPrincipalName	王博	陈萍、赖清楠
1.2	2019 年 12 月 12 日	在“附录 2：属性要求” 4.2 节“推荐属性”中添加 eduPersonTargetedID 和 eduPersonEntitlement，删除 eduPersonPrincipalName。 修改“资源共享服务政策”、“附件 2：属性要求”、“附件 3：数据保护要求”、“附件 4：服务提供者 SP 管理标准”中的“修订”部分内容。	陈萍	赖清楠、王博
1.3	2021 年 9 月 1 日	在“附录 2：属性要求” 4.2 节“推荐属性”中添加 pairwise-id，修改关于 eduPersonTargetedID 的说明。 校正英文表达。	王博	陈萍

1 定义和术语

属性 Attribute	描述用户的一组特性，如在某一机构中的身份、邮箱等信息。
认证 Authentication	确认已注册用户身份的过程。
授权 Authorization	判断某个已认证通过用户是否拥有某项服务的访问权限的过程。
CARSI 身份联盟/CARSI 资源共享服务 CARSI Identity Federation/ CARSI Resource Sharing Service	中国教育和科研计算机网身份认证和资源共享基础设施。
CARSI 资源共享服务运行团队 CARSI Operator Team	由北京大学和赛尔网络有限公司人员组成，负责 CARSI 资源共享服务运行和维护。
数字身份 Digital Identity	归属于某用户的一组信息，由属性组成，由用户身份所属机构发布和管理，用于区分用户。
用户 End User	隶属于某机构、使用服务提供商所提供服务或资源的自然人，如员工、研究人员或学生等。
联盟 Federation	身份联盟，支持以交换用户属性的方式完成用户访问资源的机构联合体。
联盟运行者 Federation Operator	为联盟会员提供认证和授权基础设施的机构。
联盟会员 Federation Member	以书面形式接受联盟政策规定而加入联盟的机构。在联盟框架内，联盟会员可以是身份提供者和/或服务提供者。
身份所属机构 Home Organization	用户身份所隶属的机构，负责用户认证和用户身份数据管理。
身份管理 Identity Management	发布和管理用户数字身份的过程。
身份提供者 Identity Provider	进行用户身份认证、提供身份属性的机构。服务提供者信任它的认证结果并根据提供的用户信息完成用户授权和访问控制。
跨联盟，全球身份联盟 Interfederation	两个或多个身份联盟自发组成的一种合作模式，使得一个身份联盟中的用户可以访问另一身份联盟服务提供者提供的资源。
资源共享 Resource Sharing	依托于 CARSI 身份联盟提供的校园网用户身份资源共享和应用资源共享服务。
服务提供者 Service Provider	向用户提供某种服务和资源的机构。它需要身份所属机构提供该用户的认证结果和/或者身份属性。

2 简介

CERNET 认证和资源共享基础设施（CARSI）是中国教育和科研计算机网（以下简称 CERNET）资源共享服务。引入 CARSI 是为了方便和简化 CERNET 中各联盟成员之间共享服务的过程。它采用身份联盟技术，以一种多机构联合体的形式、通过交换用户属性的方式完成用户访问资源的过程，将用户数字身份的应用范围从一个联盟会员单位扩大到整个联盟，促进联盟会员单位之间的用户身份资源共享和应用资源共享。联盟依靠身份所属机构 IdP（Identity Provider）准确地判定用户身份，服务提供者 SP（Service Provider）以用户身份信息为依据管理用户访问服务和资源的权限。

本联盟政策文件定义了 CARSI 资源共享服务的基本规则以及联盟会员单位的权利和义务，以便通过联盟技术标识用户身份、使用用户属性和授权信息。

“联盟技术要求”描述了某种技术（比如 SAML）的具体实现。通过某种具体的认证和授权技术，联盟政策可以在更大应用范围内支撑联邦身份。SAML、802.1x、WS-Federation、OpenID 等具体联盟技术支持“联盟技术要求”。

本文件连同下表附录共同组成联盟政策文件。附录详细信息见 https://www.carsi.edu.cn/docs/join_zh.htm。

附录	文件类型	文件	目标
1	联盟技术要求	SAML WebSSO 技术要求	以 SAML 语言的角度，描述了“政策和保证要求”的具体实现
2	属性管理	属性要求	定义核心属性集和推荐属性集，包括详细信息、取值参考、IdP 和 SP 必须遵守的部署原则
3	服务提供者 SP 管理	数据保护要求	定义部署 SP 必须遵守的属性处理原则
4		服务提供者 SP 管理标准	定义部署 SP 必须遵守的规则
5	身份提供者 IdP 管理	身份提供者 IdP 管理标准	定义部署 IdP 必须遵守的规则

3 目标和范围

CARSI 资源共享服务的目标是在中国高校已经广泛建立的校园网统一身份认证和用户管理系统基础之上，将中国高校和各级教育机构、科研机构用户数字身份的使用范围从校园网扩大到中国教育科研计算机网和全球，支持使用唯一的、真实的校园网身份访问 CERNET 和全球的教学、科研、管理、生活相关的应用系统资源。CARSI 资源共享服务支持用户访问中国和国外的各类教育资源和商用资源。

本 CARSI 资源共享服务政策文件的范围限于那些符合“联盟技术要求”、对用户进行安全认证和授权的技术。联盟会员同意加入 CARSI 资源共享服务意味着遵守本联盟政策文件，并满足所有相关附录的要求。遵循分级管理的原则，联盟会员自行监督单位内部的 IdP 服务和/或 SP 服务执行联盟政策。

为了促进国家间和机构间的合作以及便捷的资源访问，CARSI 资源共享服务可以加入全球身份联盟 eduGAIN。

4 管理和角色

CARSI 资源共享服务，主要面向教育网大中小学、各级教育管理部门和科研机构等 CERNET 会员单位提供服务。联盟管理由 CARSI 资源共享服务指导委员会、CARSI 资源共享服务运行团队共同完成。CARSI 资源共享服务指导委员会由 CERNET 技术专家委员会兼任，对联盟事务具有最终决策权。联盟运行团队负责 CARSI 资源共享服务相关的技术开发、运行维护、市场推广等工作。

4.1管理

除非联盟政策另有说明，CARSI 资源共享服务指导委员会负责：

- 批准联盟章程、政策和相关联盟文件及其修订。
- 确定联盟会员单位管理规定，包括允许成为联盟会员的机构类别、允许成为联盟身份所属机构 IdP 的机构类别、允许成为联盟服务提供者 SP 的机构类别、联盟会员资格撤销标准等。
- 决定联盟未来技术方向和发展计划。
- 决定签署全球身份联盟协议。
- 对联盟运行提供财政支持。批准联盟运行团队的年度财务预算，并对财务报告进行审计。
- 根据联盟运行团队的提案，批准联盟会员应支付的费会员用，用以支付联盟的运行成本。
- 决定联盟运行团队提出的联盟政策变更及其他建议。

4.2CARSI 资源共享服务运行团队的权利和义务

联盟运行团队负责 CARSI 资源共享服务技术开发和相关系统日常的运行和维护，由北京大学计算中心和赛尔网络有限公司相关人员组成。除非联盟政策另有说明，CARSI 资源共享服务运行团队负责：

- 执行 CARSI 资源共享服务指导委员会关于联盟会员单位相关管理规定。
- 按照本文件及其附录规定的程序和技术要求对联盟进行运行管理并提供核心服务。
- 为联盟会员指定的联系人提供支持服务，解决与联盟服务相关的运行问题。
- 作为联盟的技术中心：测试软件、推荐解决方案并编写文件，为在联盟内选定使用的软件和操作系统进行部署和配置。
- 准备年度财务预算报告并提请联盟指导委员会批准，向联盟指导委员会提交财务报告供审计。
- 与国内和国际相关组织和负责人保持联系，积极参与国际或本地区相关技术研讨和交流活动。
- 提出联盟技术发展方向建议。
- 进行市场推广，推动联盟发展。

除非联盟政策另有说明，CARSI 资源共享服务运行团队保留以下权利：

- 临时向扰乱联盟安全稳定运行的联盟会员停止技术支持。
- 为了促进联盟发展，在不涉及联盟会员单位隐私的前提下，公布联盟会员列表、所采用技术等基本信息。

4.3联盟会员单位的权利和义务

除非联盟政策另有说明，所有 CARSI 资源共享服务会员单位：

- 应指定一位项目负责人、一位技术运维人员与联盟运行团队进行沟通。
- 必须与联盟运行团队或其他会员合作解决问题，为避免对联盟或其会员的安全、信誉或名誉造成负面影响，发现问题后及时向联盟运行团队进行报告。
- 必须遵守其已经实施的技术要求。
- 必须保证单位内部与技术要求实现相关信息系统的安全运行。
- 必须按照费用标准缴费。
- 若可以接触到个人数据信息，必须遵守适用的数据保护法律并遵守“附录 3：CARSI 资源共享服务数据保护要求”，详见 https://www.carsi.edu.cn/docs/data_protection_profile_zh.pdf。

如果联盟会员单位提供身份认证服务 IdP，

- 负责管理本单位用户的网络身份，包括：新用户生成、用户信息更新和用户身份信息生命周期管理，确保用户信息准确和用户数据安全。
- 完成用户身份认证功能，为联盟服务提供者 SP 提供身份认证结果。
- 提供用户支持服务，处理本机构用户在通过联盟访问资源过程中遇到的问题，至少在正常工作时间。
- 为用户设定属性值，确保属性信息的正确、实时更新和真实可靠。
- 向服务提供者发送属性。
- 不可向非 CARSI 资源共享服务会员单位提供联盟 IdP 服务。
- 必须保证遵守“附录 5：CARSI 资源共享服务身份提供者 IDP 管理标准”，详见 https://www.carsi.edu.cn/docs/idp_management_standard_zh.pdf。
- 合理使用所下载软件和资源，不侵犯第三方合法权益。

若联盟会员提供应用资源服务 SP，其

- 有权利决定哪些用户可以访问所提供的服务，以及用户的访问权限。
- 确保正确使用获得的用户信息并保证用户信息的安全。
- 必须保证每个应用资源服务遵守“附录 3：CARSI 资源共享数据保护要求”，详见 https://www.carsi.edu.cn/docs/data_protection_zh.pdf。
- 必须保证每个应用资源服务遵守“附录 4：CARSI 资源共享服务服务提供者 SP 管理标准”，详见 https://www.carsi.edu.cn/docs/sp_management_standard_zh.pdf。
- 合理使用所下载软件和资源，不侵犯第三方合法权益。

5 程序

5.1 如何加入

要成为 CARSI 资源共享服务会员，机构需根据拟加入联盟会员的类别（全资格会员或者服务提供会员）在线提交申请 https://mgmt.carsi.edu.cn/reg，由申请单位负责人签字并加盖公章后交给联盟运行团队，以书面形式同意遵循联盟政策规定。

CARSI 资源共享服务运行团队评估会员申请，在十个工作日内做出同意或拒绝决定。如果拒绝申请，需提供拒绝申请的理由。

5.2 如何退出

联盟会员单位需至少提前一个月以书面形式向 CARSI 资源共享服务运行团队提出联盟退出申请。退出联盟意味着在退出联盟约定的日期之后联盟不再公布该单位 IdP 或者 SP 相关信息，无法再通过联盟与其他会员单位进行身份认证交流。

5.3 暂停或终止服务

联盟会员（全资格会员或服务提供会员）单位需至少提前一个月向 CARSI 资源共享服务运行团队提出申请暂停或者终止一项或多项服务。如果联盟会员单位和该项服务的提供机构签订过其他服务协议或合同，

需自行协商暂停或者解除协议或合同。联盟运行团队负责通知其他联盟会员。由于暂停或者终止服务给其他联盟会员造成的损失，联盟运行团队不承担后果，不负责任何赔偿责任。

对于半年之内，无任何访问记录的联盟会员单位，联盟运行团队将暂停其会员服务。暂停服务需至少提前一个月书面通知该服务提供商及全体联盟会员。

如果一个 SP 会员提供的所有服务均已终止，该会员资格将被取消。

5.4 被取消资格

未能遵守联盟政策的会员单位有可能被取消会员资格。若 CARSI 资源共享服务运行团队发现联盟会员违反以下规定，将正式通知该会员单位并责令在指定时间内改正。

1. 违反《网络安全法》等中国互联网管理相关法律法规；
2. 违反联盟政策要求；
3. 发生发动网络攻击、散播病毒等影响互联网安全稳定运行的行为；
4. 没有按时交费。

若违反联盟政策单位未能在规定的时间内完成整改或无正当理由要求延长整改日期，将被取消会员资格。联盟运行团队通知其他联盟会员此项取消。由于某个会员单位被取消资格而给其他联盟会员造成的损失，联盟运行团队不承担后果，不负责赔偿。

取消会员资格意味着在联盟技术框架中删除该会员信息。

6 费用

联盟会员需向 CARSI 资源共享服务运行单位支付运行费用。费用标准由 CARSI 资源共享服务指导委员会讨论通过并向所有的联盟会员公布。最新的费用标准公布在联盟网站 http://www.carsi.edu.cn/docs/fee_policy_zh.pdf。

已支付费用不可退回。如遇费用调整，最少提前一个月公布。逾期未缴费，将取消会员资格。

7 责任和赔偿

对于由联盟会员单位造成的、为联盟内其他会员或者联盟外的第三方带来的损失和伤害，CARSI 资源共享服务运行团队无需承担连带责任、进行错误修正、返还付款或者赔偿损失。联盟运行团队努力保证在合理期间内修正重大错误和缺陷。

联盟会员因使用联盟服务或者联盟相关其他系统产生的丢失、损害或者费用，联盟运行团队无需负责。该免责范围不适用于联盟运行团队人员存在重大过失或故意行为的情况。

联盟运行团队无需对给联盟会员单位或者给用户造成的损害负责。联盟会员无需为使用联盟服务、服务中断、或使用联盟服务过程中产生的其他损害向联盟运行团队负责。

其他会员单位使用本单位服务过程中遇到的服务下线或使用相关异常情况对联盟运行团队和联盟服务使用单位负责。

除非联盟会员单位之间另有书面约定，联盟会员单位不会仅因为联盟会员资格而为其他联盟会员单位承担责任。特别是，会员资格不能在联盟会员之间产生任何可强制执行的权利和义务。联盟运行团队和联盟会员应避免要求其他联盟会员对因使用联盟服务、服务宕机或其他与使用联盟服务过程中造成的损害进行赔偿。联盟会员间可酌情达成其他免责协议。该协议只适用于他们之间。

联盟会员必须保证遵守相关法律。联盟运行团队不对联盟会员或其用户未能遵守与联盟服务相关法律法规造成的损害负责。

各方均不对任何间接或后续损害负责。

全球身份联盟协议的存在以及因此进行的信息交换不应在任何联盟的任何会员之间或任何联盟会员和任何联盟运行团队之间产生新的法定权利或义务。相关联盟运行团队和联盟会员只受联盟所在国家的法律和管辖权约束。

CARSI 资源共享服务会员单位和 CARSI 资源共享服务运行团队应避免要求全球身份联盟协议中其他联盟实体进行损害赔偿。

8 管辖权和调解纠纷

与联盟政策相关的纠纷应首先通过协商解决。若问题未能通过协商解决，则应该提交给具有管辖权的法院。

一方以书面形式提出正式协商请求之日起 4 周内，若未能协商成功，则各方可将争议提交给有管辖权的法院。

如果任何具有管辖权的法院认为联盟政策的任何条款不可执行，其他条款仍然有效。

联盟政策及其附录、申请书&承诺书等相关文件以中文版为准，英文仅供参考。

9 全球身份联盟

全球身份联盟 eduGAIN（https://edugain.org）是欧盟 GEANT 发起的一个全球身份联盟，也称跨联盟（Inter Federation）。它在技术上为国家级身份联盟、他们的用户和服务之间提供了高效、灵活的互通方式。

为促进国家之间和国内机构之间的合作，CARSI 资源共享服务可申请加入全球身份联盟。全球身份联盟管理和技术文档参见《eduGAIN 政策框架-声明》和《eduGAIN 政策框架-章程》。

CARSI 资源共享服务会员单位在提交申请时，可选择是否加入全球身份联盟 eduGAIN。加入 eduGAIN 的会员单位，在与其他国家的身份联盟会员交流时，需要遵守联盟会员所在国家的法律法规和联盟政策。这些法律法规可能不同于 CARSI 资源共享服务法律法规。

10 修正

CARSI 资源共享服务运行团队有权随时修订本文件。任何此类变更应取得 CARSI 资源共享服务指导委员会的批准，向所有联盟会员发出书面通知，并在修订日期 90 天后生效。