附录 2：CARSI 资源共享服务属性要求

1. 定义和术语

https://www.carsi.edu.cn 网站上公布的最新版本“CARSI 资源共享服务政策”的第一部分“定义和术语”适用于本文件。

2. 介绍

本文件是在 CARSI 资源共享服务（即 CARSI 身份联盟）中交换用户属性所需的要求。涵盖了“附录 1：CARSI 资源共享服务 SAML WebSSO 技术要求”下的场景。后续，可以通过添加具有不同需求的场景来修订本文件。

本要求归纳了用户的属性细节，它们在联盟中处理和交换的细节。

3. 属性标准

CARSI 资源共享服务支持的多种属性，包括：

1) 【eduPerson】
- eduPerson 对象类详细文档（202001）；
- https://wiki.refeds.org/display/STAN/eduPerson+2020-01

2) 【SAML Core】
- OASIS 标准，OASIS Security Assertion Markup Language (SAML) V2.0 断言和协议标准（2005 年 3 月 15 日）
- https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

3) 【SAML-SubjectID-v1.0]】
- OASIS 标准，OASIS SAML V2.0 主体身份属性描述 版本 1.0，委员会规范 01（2019 年 1 月 16 日）
- https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/cs01/saml-subject-id-attr-v1.0-cs01.pdf

CARSI 资源共享服务属性语法应该遵守 MACE-Dir SAML 属性要求【MACEDir】(http://macedir.org/docs/internet2-mace-dir-saml-attributes-200804a.pdf).

4. SAML Web 单点登录属性集

CARSI 资源共享服务政策要求，如果联盟成员是服务提供者 SP，它在提供资源或者服务访问权限时都必须遵守“附录 3： CARSI 资源共享服务数据保护要求”的属性处理原则。

联盟中传递属性遵照 CARSI 资源共享服务 SAML WebSSO 技术要求。

4.1. 核心属性

一般来讲，核心属性对大部分用户可用。但是，对于那些找不到合适的词汇描述的用户，也可以设置为空。

CARSI 资源共享服务的联盟政策要求联盟成员必须为他们的身份提供者 IdP 收集或生成用户的核心属性。核心属性集如下表所示：

属性	定义模式	含义	取值样例
eduPersonScopedAffiliation	[eduPerson]	指定某个安全域内个人与学校的关系，如学生、教师、员工、校友等。	staff@pku.edu.cn

表 1：CARSI 资源共享服务核心属性

核心属性集可以随着联盟成员需求的发展进行修改。

4.2. 推荐属性

联盟身份提供者 IdP 推荐支持如下属性。联盟服务可选择使用这些属性。

属性	定义模式	含义	取值样例
Pairwise Subject Identifier (pairwise-id)	[SAML-SubjectID-v1.0]	替代eduPersonTargetedID。长期的、不可重新分配的单向用户标识，适合用作特定依赖方的唯一外部关键字。对于某个特定主体的取值与依赖方有关，避免无关的依赖系统使用。	HA2TKNZZGE2TOZDCGMZWKOLDHBQWIMBSGM4TGZBYGUYGINRQHAYTINBZGYZDOZBZMZRGKNZTME3TMNBXGYYTIOBYGMYWKNLFMYYDAYY=@osu.edu
SAML2 Persistent NameID (eduPersonTargetedID)	[SAMLCore, eduPerson]	弃用。在一对实体之间可共享的主体标识符，具有持久、不可重用的、保护隐私的特点。	7eakOQQIEhygtPXtpgmu515hRnY
eduPersonEntitlement	[eduPerson]	一个简单的例子是IdP与授权使用该属性的SP之间签订合同的URL。双方必须是通过线下关系建立之间的信任关系。	urn:mace:dir:entitlement:common-lib-terms

表 2 CARSI 资源共享服务推荐属性

推荐属性集可以随着联盟成员需求的发展进行修改。

4.3. 受控词汇表

4.3.1. eduPersonScopedAffiliation

eduPersonScopeAffiliation 在【eduPerson】中定义。CARSI 资源共享服务联盟成员应该限制身份提供商 IdP 使用如下属性值：

- faculty，教师
- student，学生
- staff，员工
- alum，校友
- member，成员
- affiliate，附属人员
- employee，聘用人员
- other，其他

4.3.2. eduPersonEntitlement

eduPersonEntitlement 在【eduPerson】中定义。CARSI 资源共享服务联盟成员应该限制身份提供商 IdP 使用如下属性值：

- urn:mace:dir:entitlement:common-lib-terms，图书馆业务通用条款

4.4. 作用域属性

如果联盟成员决定在它的服务提供者 SP 中使用作用域属性（比如 eduPersonScopedAffiliation），建议使用某种机制来确保身份提供者 IdP 发出的属性“作用域”的值与身份所属机构事前关联的许可一致。

5. 修订

CARSI 资源共享服务运行团队有权不定期修订此文件。任何此类修订需要获得 CARSI 指导委员会的认可，对所有联盟成员具有约束力。所有联盟成员必须在他们的身份提供者 IdP 中支持最新版本的核心属性。本文件最新版本发布在 CARSI 资源共享服务官方网站 https://www.carsi.edu.cn/docs/attribute_profile_zh.pdf。修订后的数据保护要求对所有联盟成员具有约束力。联盟成员必须遵循本文档的最新版本，详见 CARSI 资源共享服务官方网站 https://www.carsi.edu.cn/docs/data_protection_profile_zh.pdf。