附录 1：CARSI 资源共享服务 SAML WebSSO 技术要求

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”【0】适用于本文件。

2. 介绍

本文件是 CARSI 资源共享服务（即 CARSI 身份联盟）的技术要求，内容为如何用 SAML V2.0 浏览器 SSO 要求【1】实现了 CARSI 资源共享服务。

SAML V2.0 浏览器 SSO 要求定义了一种标准来允许身份提供者 IdP 和它的依赖方（服务提供者 SP）来创建基于 SAML 的 Web 单点登录服务。

3. 需求

- 所有 SAML 元文件必须实现 SAML2.0 元文件互操作技术要求 1.0 及以上版本【2】；
- 所有身份提供者 IdP 必须实现互操作 SAML2.0 要求（稳定版本）【3】；
- 所有服务提供者 SP 应该实现互操作 SAML2.0 要求【3】；
- 所有 SAML 属性应该用 urn:oasis:names:tc:SAML:2.0:attrname-format:uri 名字格式来表示；
- 所有 SAML 属性名字应该用 urn:oid 或者 http(s) URI 模式名字空间来表示。使用 MACE-Dir【4】定义的属性必须与 MACE-Dir SAML 属性要求【5】（或任何新版本）一致；
- 所有 SAML 身份提供者 IdP 必须遵照 Shibboleth 元文件模式定义实现 Shibboleth Scope 元文件扩展【6】。Scope 取值必须是属于某一机构的 DNS 域名的字符串，该域名与用户身份一致。
- 所有 SAML 服务提供者 SP 在处理范围属性的时候应该对照 Shibboleth Scope 元文件进行检查。

4. 参考文献

【0】 https://www.carsi.edu.cn/docs/identity_federation_policy_zh.pdf

【1】 http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

【2】 http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf

【3】 http://saml2int.org/

【4】 http://middleware.internet2.edu/dir/

【5】 http://macedir.org/docs/internet2-mace-dir-saml-attributes-200804a.pdf

【6】 https://wiki.shibboleth.net/confluence/display/SC/ShibMetaExt+V1.0

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 指导委员会认可，对所有联盟成员具有约束力。CARSI 资源共享服务运行团队将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/saml_technology_profile_zh.pdf。