CARSI 资源共享服务元数据注册实践声明

版本	1.0
最新修改日期	2019 年 3 月 19 日

致谢

本文档在《REFEDS 元数据注册实践声明模板》基础上完成。

许可

1. 定义和术语

本文档使用如下定义。

定义	描述
联盟	身份联盟。根据需要安全地交换用户和资源信息、以便进行合作和交互的联合组织。
联盟会员	书面同意接受联盟政策约束、加入联盟的单位或组织。
联盟运行团队	为联盟会员提供认证和授权基础设施的单位或组织。
联盟政策	描述联盟会员和联盟运行团队义务和权利的文件。
实体	联盟会员在元数据中注册和描述的具体组件。通常是身份提供者 IdP 或服务提供者 SP。
注册系统	联盟申请者或联盟会员用来注册实体元数据的自服务系统。由联盟运行团队提供。
项目负责人/商务负责人	被授权代表联盟会员管理本单位在 CARSI 资源共享服务中 IdP 或者 SP 的个人。

2. 介绍及适用性

本文件描述了元数据注册实践，自首页所示的发布日期开始执行。在该日期或之后执行的新实体注册均应参照此文件进行处理，直到本文档被替换为止。

本文件公布在 CARSI 资源共享服务网站上 https://www.carsi.edu.cn/docs/CARSI-MRPS-zh.pdf。

文档内容更新应准确反映在实体元数据中。

如果对某实体的引用信息中不包含对登记政策的引用，需确认该实体已经按照某种旧的登记制度进行了登记。如果希望根据当前版本文档重新评估实体，请向联盟运行团队提交申请。

3. 会员资格和所有权

联盟会员利用联邦运行团队提供的注册系统来注册实体。联盟运行团队不接受其他来源的注册申请。

申请成为联盟会员的流程说明详见：https://www.carsi.edu.cn/join_zh.htm。

注册过程中，联盟运行团队通过多种官方渠道检查申请单位提供的正式名称，要求申请单位同意联盟政策并提交申请表和承诺书。并要求申请单位电子表格中填写的单位名称与申请文件中加盖的公章完全一致。

会员注册过程还将确定和核实项目负责人或商务负责人，他们将代表该组织处理实体在CARSI联盟运行相关事宜。

注册过程还将为联盟会员建立一个供注册系统使用的规范名称。该名称将公布在实体的SAML v2.0<md:OrganizationName>元素中，以便于其他单位查看。会员规范名称可以在会员资格期间修改，例如由于公司名称改动或合并。

4. 元数据格式

实体元数据应该包括元数据扩展来表明实体注册者，即实体所属联盟。通常遵循[SAML-Metadata-RPI-V1.0]元数据扩展规范，在注册实体时由联盟注册系统自动添加，并详细说明适用的MRPS版本。以下是非规范性示例：

```
<mdrpi:RegistrationInfo
    registrationAuthority="https://www.carsi.edu.cn"
    registrationInstant="2016-11-29T13:39:41Z">
    <mdrpi:RegistrationPolicy xml:lang="en">
        https://www.carsi.edu.cn/docs/CARSI-MRPS-en.pdf
    </mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

5. 实体资格和验证

5.1 实体注册

联盟申请者或会员通过联盟注册系统https://mgmt.carsi.edu.cn/reg注册实体。

联盟运行团队应该验证会员对于entityID使用特定域名的权利。对于IdP实体，验证域名有效性。

域名使用权应符合以下要求之一：

- 会员规范名称与CARSI注册系统中的注册者信息匹配。
- 会员通过获取域名所有者许可信的方式，获得在实体中使用该域名的权利。所获得的权限不应包括使用子域的权限。

5.2 EntityID格式

注册的entityID属性的值必须是使用http、https或urn绝对的URI。推荐使用https-scheme URI。

用于 entityID 值的 http-scheme 和 https-schemeURI 必须包含 DNS 主机部分。

5.3 范围格式

对于身份提供者 IdP 实体，范围必须基于 DNS 域名，用小写字母表示。允许使用多个范围。

可以使用正则表达式，但是表达式所覆盖的所有 DNS 域必须是中国教育科研计算机网 CERNET 注册域名。正则表达式格式为：(foo|bar)\.edu\.cn$。

5.4 实体验证

在实体注册时，联盟运行团队应进行实体验证检查。这些检查包括：

- 确保元数据中提供了所有需要的信息；
- 确保元数据格式正确；
- 确保元数据中指定的 URL 可访问；
- 确保协议端点受到 TLS/SSL 证书保护。

6. 实体管理

一旦加入联盟成为会员，单位可以添加、更改或删除实体信息。

6.1 实体变更请求

联盟会员提出的任何添加、更改或删除实体的请求都需要由其项目负责人或商务负责人确认。

联盟会员通过联盟注册系统管理实体。

6.2 未请求的实体变更

为了以下目标，联盟运行团队可以在任何时候修改联盟元数据：

- 确保元数据的安全性和完整性；
- 遵守联盟间协议；
- 提高互操作性；
- 向元数据添加值。

更改将通知实体的项目负责人或商务联系人。

参考文献

[RFC2119] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, March 1997.

[SAML-Metadata-RPI-V1.0] SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0. 03 April 2012. OASIS Committee Specification 01. http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/cs01/saml-metadata-rpi-v1.0-cs01.html.

[SAML-Metadata-OS] OASIS Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.