

**Федерация доступа к удалённым ресурсам учебной среды «ФЕДУРУС»**

Документы Оператора Федерации: **Регламент регистрации метаданных**

|  |  |
| --- | --- |
| Авторы | Соколов А. В., Белов А. М., Усманов Р. Т. |
| Дата публикации | 00.00.2018 |
| Версия | 0.1a |

**Использование**

http://i.creativecommons.org/l/by/3.0/88x31.png

Настоящий документ построен на основе шаблона и лицензируется по Creative Commons CC BY 3.0. Возможно свободное использование и адаптация с указанием ссылки на исходный шаблон, составленный UK Access Management Federation и ACOnet Identity Federation.

**Содержание**

1. Термины и определения 3

2. Введение и область применения 4

3. Права и регистрация Членов Федерации 5

4. Формат метаданных 6

5. Entity Eligibility and Validation 7

6. Entity Management 8

7. Ссылки 9

# 1. Термины и определения

В настоящем документе используются следующие термины и определения, в соответствии с «Положением о проекте АРБИКОН «Федерация доступа к удалённым ресурсам учебной среды (ФЕДУРУС)» [Положение] и «Техническим регламентом проекта АРБИКОН: Федерация доступа к удалённым ресурсам учебном среды (ФЕДУРУС)» [Технический регламент]:

|  |  |
| --- | --- |
| Федерация | Распределённая информационная система, объединяющая и согласовывающая сервисы аутентификации Членов Федерации на основе утверждённых правил и политик, позволяющая эффективно использовать электронные ресурсы через глобальные сети передачи данных. |
| Член Федерации | Организация, принимающая на себя обязательства по подключению к сервисам Федерации в соответствии с Техническим регламентом. |
| Оператор Федерации | Организация, оказывающая услуги предоставления, сопровождения, методического и документарного обеспечения инфраструктуры Федерации. |
| Политика Федерации | Совокупность описаний прав и обязанностей Членов Федерации, Оператора Федерации, а также основных принципов функционирования Федерации, изложенная в Положении и Техническом регламенте. |
| Объект | Составной компонент, обычно представленный Сервис Провайдером или Провайдером идентификации, который Член Федерации регистрирует и описывает на основе метаданных. |
| Реестр | Информационная система, используемая Оператором Федерации для регистрации метаданных Объекта как в ручном, так и в автоматизированном режимах. |
| Уполномоченные пользователи | Лица, уполномоченные Членом Федерации на выполнение функций регистрации, управления, текущего обслуживания и администрирования Объектов. |

# 2. Введение и область применения

В этом документе описывается методика регистрации метаданных у Оператора Федерации, применяемая с даты публикации, указанной на титульном листе. Регистрация Объектов, выполняемая с и после указанной даты, осуществляется по нижеприведённой методике до изменения данного документа.

Регламент регистрации метаданных в обязательном порядке публикуется на официальном сайте Оператора Федерации по адресу <http://www.fedurus.ru>. Обновления методики регистрации метаданных у Оператора Федерации должны быть в обязательном порядке отражены в метаданных Объектов Членов Федерации.

Объект, который не содержит ссылку на регистрационную политику должен рассматриваться как устаревший и использующий нерегламентированный метод регистрации метаданных. Запросы на использование такого Объекта в обход настоящего Регламента могут быть направлены в службу поддержки Оператора Федерации.

Настоящий Регламент составлен на двух языках: русский и английский. При возникновении спорных и иных вопросов приоритет имеет русская версия

.

# 3. Права и регистрация Членов Федерации

Члены Федерации имеют право использовать Реестр Операторов Федерации только для регистрации юридических лиц через специальную форму. Запросы на регистрацию в Реестре из других источников не принимаются.

Форма регистрации в качестве Члена Федерации размещена по адресу: <https://arbicon.ru/projects/FEDURUS/registered.html>. Техническая документация по регистрации и настройке Объектов размещена по адресу: <http://www.fedurus.ru>.

Процедура регистрации Членов Федерации заключается в проверке кандидатов на соответствие юридическим и техническим требованиям Оператора Федерации и акцептируется заключением Договора об оказании услуг по подключению к библиотечно-информационным сервисам проекта ФЕДУРУС, неотъемлемой частью которого являются Положение и Технический регламент. Процедура проверки осуществляется с использованием ??????

Процедура регистрации также включает проверку и идентификацию Уполномоченных пользователей и осуществляется путём ??????

В рамках регистрации устанавливается каноническое имя Члена Федерации, которое может быть изменено позднее, в случае смены юридического названия. Данное имя приводится в элементе <md:OrganizationName> [SAML-Metadata-OS] Объекта Члена Федерации.

# 4. Формат метаданных

Метаданные всех Объектов, регистрируемых Оператором Федерации, должны включать расширение метаданных [SAML-Metadata-RPI-V1.0] указывающее, что Оператор Федерации является регистратором Объекта, и содержащее версию регистрационной политики, применяемой в Объекте.

Пример:

<mdrpi:RegistrationInfo registrationAuthority="http://www.fedurus.ru" registrationInstant="2018-06-28T13:39:41Z"> <mdrpi:RegistrationPolicy xml:lang="ru"> http://www.fedurus.ru/doc/MRPS20180628</mdrpi:RegistrationPolicy> </mdrpi:RegistrationInfo>

# 5. Entity Eligibility and Validation

*This section describes the processes and checks put in place before an entity is registered. Readers will be looking to understand how you determine a member’s right to publish information about a given entity and any checks you make to ensure the entity metadata is well constructed.*

*Text regarding entityIDs using URIs is included below. Some Federations will also permit URN-based entityIDs. You should describe what you do and do not permit under each schema. Please ensure that any processes described here reflect your current practice and any published documentation currently available for your Federation.*

**Example Wording:**

**5.1 Entity Registration**

The process by which a Federation member can register an entity is described at <url>.

The Federation Operator SHALL verify the member’s right to use particular domain names in relation to entityID attributes.

The right to use a domain name SHALL be established in one of the following ways:

* A member’s canonical name matches registrant information shown in DNS.
* A member MAY be granted the right to make use of a specific domain name through a permission letter from the domain owner on a per-entity basis. Permission SHALL NOT be regarded as including permission for the use of sub-domains.

**5.2 EntityID Format**

Values of the entityID attribute registered MUST be an absolute URI using the http, https or urn schemes.

https-scheme URIs are RECOMMENDED to all members.

http-scheme and https-scheme URIs used for entityID values MUST contain a host part whose value is a DNS domain.

**5.3 Entity Validation**

On entity registration, the Federation Operator SHALL carry out entity vaildations checks. These checks include:

* Ensuring all required information is present in the metadata;
* Ensuring metadata is correctly formatted;
* Ensuring protocol endpoints are properly protected with TLS / SSL certificates.

# 6. Entity Management

*This section describes the processes undertaken once an entity has been registered – including processes for change requests, removal and any intervention the Federation Operator may take. If you have a Monitoring Practice Statement, this is likely to be referenced here. The reader will want to understand that any changes made to an entity are completed with the correct permission and for good reasons. Please ensure that any processes described here reflect your current practice and any published documentation currently available for your Federation.*

*If you have multiple different roles under the Registered Representative category (e.g. management contacts, technical contacts, administrative contacts) the different rights of these roles can be detailed here.*

**Example Wording:**

Once a member has joined the Federation any number of entities MAY be added, modified or removed by the organisation.

**6.1 Entity Change Requests**

Any request for entity addition, change or removal from Federation members needs to be communicated from or confirmed by their respective Registered Representatives.

Communication of change happens via *(e-mail, Federation registry tool etc.)*

**6.2 Unsolicited Entity Changes**

The Federation Operator may amend or modify the Federation metadata at any time in order to:

* Ensure the security and integrity of the metadata;
* Comply with interFederation agreements;
* Improve interoperability;
* Add value to the metadata.

Changes will be communicated to Registered Representatives for the entity.

# 7. Ссылки

|  |  |
| --- | --- |
| [Положение] | Положение о проекте АРБИКОН «Федерация доступа к удалённым ресурсам учебной среды (ФЕДУРУС). <https://arbicon.ru/download/FEDURUS/pril1.docx> |
| [Технически регламент] | Технический регламент проекта АРБИКОН: Федерация доступа к удалённым ресурсам учебном среды (ФЕДУРУС). <https://arbicon.ru/download/FEDURUS/pril2.docx> |
| [RFC2119] | Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, [RFC 2119](http://tools.ietf.org/html/rfc2119), 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>. |