Описание интеграционного профиля СУД

19.07.2023

Оглавление

1. Общие сведения

Система управления доступом (СУД) предназначена для авторизации и аутентификации клиентов государственной информационной системы Санкт-Петербурга «Региональный фрагмент единой государственной информационной системы в сфере здравоохранения» (далее – РЕГИЗ) при обращении к подсистемам РЕГИЗ, а также при запросе данных, хранящихся в ней. СУД реализует модель доступа, основанную на утверждениях, а также поддерживает внешних провайдеров авторизации таких, как LDAP и ЕСИАиА.

Модель доступа на основе утверждений позволяет гибко настраивать систему, что обеспечивает ее быструю адаптацию к существующим процессам региона.

2. Механизмы предоставления доступа

На стороне системы управления доступом СУД реализована возможность предоставления доступа с использованием:

1) данных учетной записи LDAP

2) определения прав на основе утверждений (claims base), которые можно сгруппировать в две группы: **базовые** и **дополнительные.** Далее утверждения будем называть политиками доступа.

Полный перечень политик доступа приведен в таблице ниже:

Уровень политики	Политика	Наименование политики
Набор корневых политик	**urn:SPb.MIAC.Policies**	Набор политик доступа к ресурсам
Корневая	**/.LDAP**	Политика доступа к ресурсам ИЭМК через LDAP.
Корневая	**/.IEMK**	Набор политик доступа к ресурсам ИЭМК.
Базовая	/.MIS	Политика доступа к ресурсам ИЭМК посредством МИС.
Базовая	/.MO.MP	Политика доступа МР из МО к ресурсам ИЭМК (расширенная).
Базовая	/.Patient	Набор Политик доступа к данным ИЭМК Пациента.
Дополнительная	/.ClosedCase	Пациент имеет Закрытый Случай Обслуживания (ЗСО) в МО.
Дополнительная	/.Grant	Пациент дал согласие через ЛК Пациента.
Дополнительная	/.OpenCase	Пациент имеет Открытый Случай Обслуживания (ОСО) в МО.
Дополнительная	/.TMC.Doctor.Access	Пациент направлен к врачу по направлению.
Дополнительная	/.MQ	Наличие активных направлений в целевой МО.
Дополнительная	/.ServicedBy	Пациент прикреплен к МО по программе ОМС.
Корневая	**/.ACPS**	Активная карточка СМП.
Базовая	/.MIS	Политика доступа к ресурсам ИЭМК посредством МИС.
Базовая	/.MO.MP	Политика доступа МР из МО к ресурсам скорой помощи (расширенная).
Базовая	/.Patient	Набор Политик доступа к данным скорой помощи Пациента.
Дополнительная	/.OpenCase	Пациент имеет Открытый Случай Обслуживания (ОСО) в МО.

2.1. LDAP-авторизация

На стороне системы управления доступом (далее – СУД) реализована возможность предоставления доступа с использованием данных учетной записи LDAP (Lightweight Directory Access Protocol). Пример запроса к СУД с использованием LDAP-авторизации приведен в разделе "Примеры запросов".

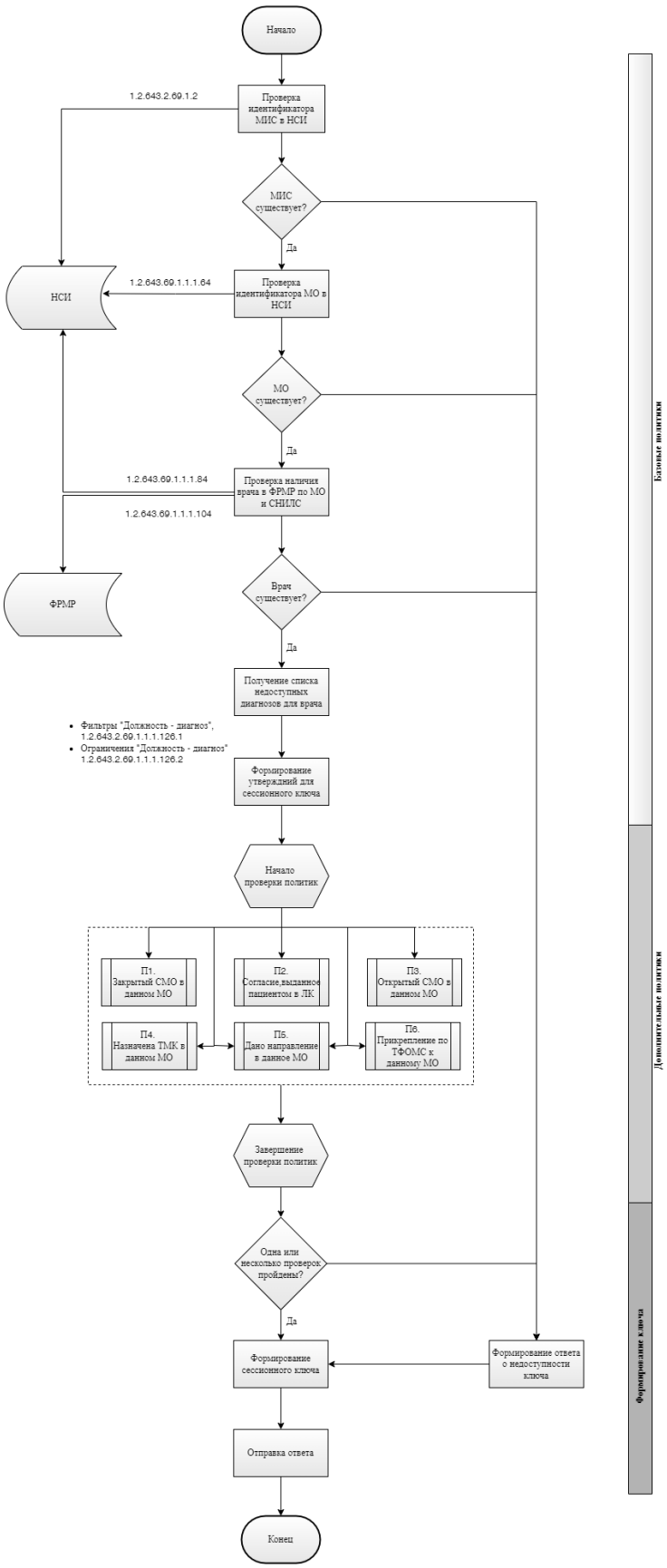
2.2. Авторизация от лица медицинской организации

При получении прав доступа с использованием политик доступа предполагается, что в момент проверки поступившего запроса на доступ, все базовые политики должны разрешиться полностью, в то время как дополнительные политики разрешаются независимо друг от друга. Для предоставления доступа внешнему клиенту необходимо и достаточно разрешения одной из политик.

Состав дополнительных политик доступа определяется оператором каждого региона отдельно. Пример запроса к СУД со стороны МО приведен в разделе "Примеры запросов".

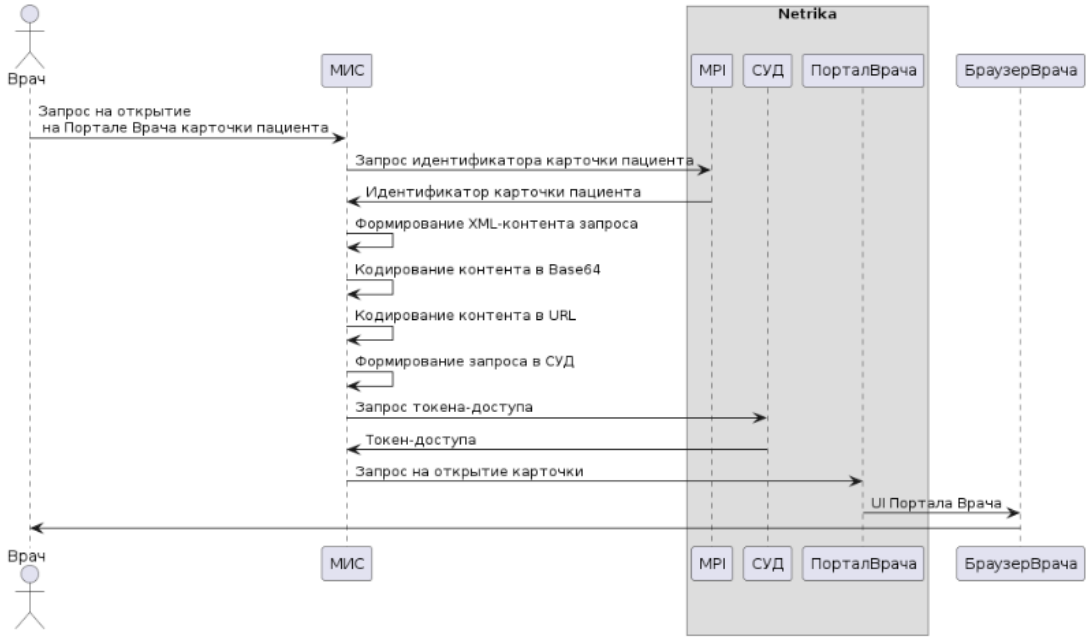
2.2.1. Порядок проверки политик доступа

Алгоритм работы политик СУД
(Доступ от лица МО)



3. Общий порядок получения токена доступа

Общий порядок получения доступа к данным ИЭМК пациента через Портал врача отображен на диаграмме.



Процесс представляет собой последовательность следующих шагов:

1. Получение идентификатора карточки пациента в ИЭМК;
2. Подготовка тела запроса:
    a. Формирование XML контента;
    b. Кодирование контента в Base64;
    c. Кодирование контента в URL;
3. Запрос токена доступа;
4. Формирование URL и вызов Портала врача.

Ниже представлено более подробная информация, касающаяся каждого из указанных шагов.

3.1. Запрос идентификатора карточки пациента в ИЭМК

Запрос идентификатора карточки пациента в ИЭМК производится путем вызова метода GetPatient модуля работы с пациентом сервиса ИЭМК.

Для вызова метода и получения идентификатора ***достаточно*** указать следующие параметры:

- guid - ключ доступа к сервису ИЭМК;
- idLPU - идентификатор МО;
- IdPatientMIS - идентификатор карточки пациента в МИС МО;
- idSource = Reg (константа).

```xml
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body>
        <GetPatient xmlns="http://tempuri.org/">
            <guid>0310c7a6-bdf3-4124-b9d4-5fd5c72fa066</guid>
            <idLPU>282ddd22-7513-47ad-b8fb-3462463768bd</idLPU>
            <patient
xmlns:a="http://schemas.datacontract.org/2004/07/EMKService.Data.Dto"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
                <a:Addresses i:nil="true"/>
                <a:BirthDate>0001-01-01T00:00:00</a:BirthDate>
                <a:BirthPlace i:nil="true"/>
                <a:ContactPerson i:nil="true"/>
                <a:Contacts i:nil="true"/>
                <a:DeathTime i:nil="true"/>
                <a:Documents i:nil="true"/>
                <a:FamilyName i:nil="true"/>
                <a:GivenName i:nil="true"/>
                <a:IdBloodType i:nil="true"/>
                <a:IdGlobal i:nil="true"/>
                <a:IdLivingAreaType i:nil="true"/>
                <a:IdPatientMIS>103038</a:IdPatientMIS>
                <a:IsVip>false</a:IsVip>
                <a:Job i:nil="true"/>
                <a:MiddleName i:nil="true"/>
                <a:Privilege i:nil="true"/>
                <a:Sex>0</a:Sex>
                <a:SocialGroup i:nil="true"/>
                <a:SocialStatus i:nil="true"/>
            </patient>
            <idSource>Reg</idSource>
        </GetPatient>
    </s:Body>
</s:Envelope>
```


Code Block 1 GetPatient Responce

Параметр ответа *Patient.IdGlobal* и будет искомым идентификатором.

3.2. Подготовка тела запроса к СУД

Для того, чтобы получить токен доступа от СУД с телом запроса необходимо выполнить несколько относительно сложных для восприятия шагов:

- 3.2.1. Формирование контента запроса;
- 3.2.2. Кодирование контента с помощью Base64;
- 3.2.3. Кодирование контента с помощью URL;

Ниже указанные шаги описаны более подробно.

3.2.1. Формирование контента запроса (XML)

Для получения сессионного ключа доступа к информационным ресурсам РЕГИЗ необходимо сформировать и отправить в сервис СУД запрос, в котором указываются реквизиты: а) вызывающей стороны, и б) целевого ресурса (например, сервиса ИЭМК).

Запрос представляет собой XML-документ определенного формата, содержащий определенные параметры.

Текущая реализация СУД предполагает использование одной из 2-х групп сценариев, содержащих следующие параметры для построения запросов на доступ:

${<Имя атрибута>}	Описание параметра
Группа "Авторизация через данные МО"	
${MP.snils}	СНИЛС медицинского работника.
${MO.guid}	GUID медицинской организации (См. значения справочника urn:oid:1.2.643.2.69.1.1.1.64 подсистемы НСИ.).
${MIS.oid}	OID МИС (См. значение справочника urn:oid:1.2.643.2.69.1.2 подсистемы НСИ.)
${Patient.IdGlobal}	Идентификатор пациента ИЭМК.
${MP.lastName}	Фамилия медицинского работника.
${MP.firstName}	Имя медицинского работника.
${MP.patronymic}	Отчество медицинского работника.
Группа "LDAP-авторизация"	
${LDAP.login}	Логин учетной записи LDAP медицинского работника/организации;
${LDAP.password}	Пароль учетной записи LDAP медицинского работника/организации.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xacml-samlp:XACMLAuthzDecisionQuery
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_fc31b400-e529-4ac0-a616-10f1e17c5b8b"
  Version="2.0"
  IssueInstant="2017-04-19T15:54:55.1061156Z"
  xmlns:xacml-
samlp="urn:oasis:names:tc:xacml:3.0:profile:saml2.0:v2:schema:protocol:wd-
14"
  xmlns:xacml-context="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
  xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
  xsi:schemaLocation='
    urn:oasis:names:tc:xacml:3.0:profile:saml2.0:v2:schema:protocol:wd-14
    http://login-test.zdrav.netrika.ru:8090/xacml-3.0-profile-saml2.0-v2-
schema-protocol-wd-14.xsd
    n3-healthcare-2018-06-21.xsd'>
  <xacml-context:Request
    xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
    xmlns='urn:oasis:names:tc:xacml:3.0:core:schema:wd-17'
    xmlns:n3="urn:netrika.ru:healthcare:n3:2018-06-21"
    xsi:schemaLocation='urn:oasis:names:tc:xacml:3.0:core:schema:wd-17
    http://docs.oasis-open.org/xacml/3.0/xacml-core-v3-schema-wd-17.xsd
    n3-healthcare-2018-06-21.xsd'
    ReturnPolicyIdList="false"
    CombinedDecision="false">
    <xacml-context:Attributes
        Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject">
      <xacml-context:Content>
        <n3:Identifier тип="медицинский работник"  >
          <n3:System oid="urn:oid:1.2.643.2.69.1.1.1.84">
            <n3:СНИЛС номер="04145926950" />
            <n3:ФИО фамилия="Зуенкова" имя="Ирина" отчество="Юрьевна" />
          </n3:System>
        </n3:Identifier>
      </xacml-context:Content>
    </xacml-context:Attributes>
    <xacml-context:Attributes
        Category="urn:oasis:names:tc:xacml:1.0:subject-category:recipient-
subject">
    </xacml-context:Attributes>
    <xacml-context:Attributes
        Category="urn:oasis:names:tc:xacml:1.0:subject-
category:intermediary-subject">
      <xacml-context:Content>
        <n3:Identifier тип="медицинская организация">
          <n3:System oid="urn:oid:1.2.643.2.69.1.1.1.64">
            <n3:Организация guid="68d62245-d2a4-4d85-83b9-33987aefdcf6" />
          </n3:System>
        </n3:Identifier>
      </xacml-context:Content>
    </xacml-context:Attributes>
    <xacml-context:Attributes
        Category="urn:oasis:names:tc:xacml:1.0:subject-category:codebase">
      <xacml-context:Content>
        <n3:Identifier тип="медицинская информационная система">
          <n3:System oid="urn:oid:1.2.643.2.69.1.2">
            <n3:ИнформационнаяСистема oid="urn:oid:1.2.643.2.69.1.2.10" />
          </n3:System>
        </n3:Identifier>
      </xacml-context:Content>
    </xacml-context:Attributes>
    <xacml-context:Attributes
        Category="urn:oasis:names:tc:xacml:1.0:subject-
category:requesting-machine">
```

```
    </xacml-context:Attributes>
    <xacml-context:Attributes
        Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:resource">
      <xacml-context:Content>
        <n3:Identifier тип="пациент">
          <n3:System oid="urn:oid:1.2.643.2.69.1.1.4">
            <!-- [Опционально] n3:СНИЛС номер="${Пациент.СНИЛС.номер}" /--
>
            <!-- [Опционально] n3:ОМС номер="${Пациент.ОМС.номер}" /-->
            <!-- [Опционально] n3:IdGlobal
value="${N3.ИЭМК.Пациент.IdGlobal}" /-->
            <n3:IdGlobal value="a8e5f24f-96e6-423f-b9da-4aa7e00ff37a" />
          </n3:System>
        </n3:Identifier>
      </xacml-context:Content>
    </xacml-context:Attributes>
    <xacml-context:Attributes
        Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
      <xacml-context:Content>
        <n3:Identifier тип="действие">
          <n3:System oid="urn:oid:1.2.643.2.69.1.1.4">
            <n3:Метод имя="читать" />
          </n3:System>
        </n3:Identifier>
      </xacml-context:Content>
    </xacml-context:Attributes>
    <xacml-context:Attributes
        Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment">
    </xacml-context:Attributes>
  </xacml-context:Request>
</xacml-samlp:XACMLAuthzDecisionQuery>
```

Code Block 2 Пример содержимого XML документа от имени МО

3.2.2. Кодирование контента в Base64

На этом шаге производится кодирование полученного в п. 3.2.1 XML-документа с корневым элементом XACMLAuthzDecisionQuery с помощью кодировки Base64 (см спецификацию «The Base64 Alphabet» приведена в Table 1 в RFC 4648 и в RFC 2045 для операций кодирования и декодирования).

3.2.3. Кодирование контента в URL

Сформированное тело запроса в п. 3.2.2 подвергается URL-кодированию, согласно требованиям, изложенным в стандарте языка JavaScript ECMAScript 2015 (6th Edition, ECMA-262).

4. Запрос токена доступа

4.1. Формирование запроса

Для получения токена доступа требуется отправить POST запрос в сервис СУД с использованием метода POST по адресу: ***<ACS.URL>/connect/token***, где *<ACS.URL>* - адрес сервиса СУД.

```
grant_type=urn:ietf:params:oauth:client-assertion-type:saml2-bearer
&assertion=<КодированныйКонтент>
&scope=iemk_portal+openid
```

Code Block 3 Тело запроса

<КодированныйКонтент> - кодированная результирующая строка из п. 3.2.3, которая закодирована в Base64 и URL, XML-документа с корневым элементом XACMLAuthzDecisionQuery.

Пример кодированного тела запроса приведен в ниже

Заголовок POST-запроса в сервис СУД должен содержать параметры, приведенные в таблице

Свойство	Значение	Примечание
Authorization	Basic {учетные данные}	Учетные данные представляют собой строку в формате {логин}:{пароль}. Далее строка кодируется Base64. Например, учетные данные mis1:secret будут представлены в виде строки: *bWIzMTpzZWNyZXQ=*
Host	<N3.ACS.host>	<N3.ACS.host> - DNS имя или IP адрес узла сети, на котором размещен СУД. Например, login-test.zdrav.netrika.ru
Content-Length	<ДлинаДанных>	Размер передаваемых данных в байтах. В качестве передаваемых данных рассматривается тело HTTP запроса, сформированное на шаге *Формирование запроса к СУД и кодирование URL*.
Accept	application/json	Константа
Content-Type	application/x-www-form-urlencoded	Константа
Expect	100-continue	Константа
Connection	Keep-Alive	Константа

Пример:

```
POST https://login.zdrav.netrika.ru/connect/token HTTP/1.1
Authorization: Basic bWlzMTpzZWNyZXQ=
Accept: application/json
Content-Type: application/x-www-form-urlencoded
Host: login.zdrav.netrika.ru
Content-Length: 5188
Expect: 100-continue
Connection: Keep-Alive
```

Code Block 4 Пример заголовка POST-запроса

4.2. Ответ СУД

В ответе от СУД будет получено сообщение следующего вида:

```
{"access_token":"<ТокенДоступа>","expires_in":3600,"token_type":"Bearer"}
```

Code Block 5 Форма ответа от СУД

<ТокенДоступа> - последовательность символов.

```
{
    "access_token":
"d3c2bdbb1300a99d9e5a8b0f49843a555af39f7efe009775acabdfdfd2e9f5a2",
    "expires_in": 3600,
    "token_type": "Bearer"
}
```

Code Block 6 Пример ответа от СУД

5. Формирование URL и вызов Портала

Для вызова портала ИЭМК полученный токен доступа от СУД должен быть использован для формирования URL следующего вида:

```
<IEMK.Portal.URL>/Patient/<Patient.IdGlobal>/Encounters?access_token=<Токе
нДоступа>
```

где:

- *<IEMK.Portal.URL>* - URL Портала ИЭМК (т.е. базовый адрес портала).
- *<Patient.IdGlobal>* - Идентификатор пациента ИЭМК.
- *<ТокенДоступа>* - токен доступа, полученный из сервиса СУД в ответ на запрос , сформированный на шаге, описанном в пункте 3.

Пример

```
http://r78-rc.zdrav.netrika.ru/EMKUI/Patient/15500e82-75ad-4e31-9e58-
4d9d0957d20a/Encounters?access_token=82ec05795d7d72d28f2dfe300d2fbfcdbf4fa
ea3f9171aac10f26b5b991be870
```

Веб-интерфейс Портала ИЭМК может быть открыт с помощью агента (браузера) при использовании HTTP метода GET. То есть, например, указанный URL может быть введен в адресную строку браузера.

В случае, если сформированный в СУД и используемый в запросе к порталу токен доступа корректен и разрешает доступ к данным ИЭМК Пациента, то Веб-интерфейс Портала ИЭМК позволит просматривать все записи и документы, связанные с данным Пациентом. Если токен доступа *некорректен* относительно запрашиваемых через портал данных ИЭМК Пациента, то в Веб-интерфейсе Портала ИЭМК будет выведено сообщение об отказе в доступе. Если токен доступа *устарел*, то пользователь будет перенаправлен на страницу авторизации с помощью учётной записи LDAP.