ПРИЛОЖЕНИЕ 8
к протоколу заседания Подкомиссии
по использованию информационных технологий
при предоставлении государственных
и муниципальных услуг
Правительственной комиссии
по использованию информационных технологий
для улучшения качества жизни и условий ведения
предпринимательской деятельности
от 21 апреля 2014 г. № ____

ЕДИНАЯ СИСТЕМА ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

Методические рекомендации по использованию Единой системы идентификации и аутентификации

Версия 2.4

2015

СОДЕРЖАНИЕ

ТАБЛИЦА ИЗМЕНЕНИЙ

Версия	**Изменение**
1.0	Документ создан
2.0	Создана новая версия документа в рамках развития ЕСИА в 2013 г.
2.1	Внесены исправления в документ: – уточнено описание процедуры подписания запроса при аутентификаци с помощью протокола SAML; – уточнено описание перечня SAML-атрибутов; – уточнено описание электронного сервиса по регистрации пользователей ЕСИА, опубликованного в СМЭВ (добавлено описание процедуры получения доступа к сервису, добавлены идентификаторы сервиса ЕСИА в СМЭВ, уточнено описание метода восстановления доступа); – уточнено описание областей доступа (scope), используемых программными интерфейсами на основе REST.
2.2	Исключено приложение с описанием электронных сервисов ЕСИА для работы с должностными лицами ОГВ. Произведена перенумерация остальных приложений. Внесены уточнения и детализации в технические описания во всех приложениях.
2.3	Детализация описания механизма аутентификации с использованием OpenID Connect 1.0
2.4	Добавлено описание программного интерфейса на основе REST по получению данных о филиалах и ОГВ. Уточнено описание программного интерфейса на основе REST по получению данных о системных группах. Изменено обозначение типов учетных записей. Добавлены ссылки на Технологический портал ЕСИА. Уточнено описание redirect_uri при использовании сервиса авторизации ЕСИА на основе OAuth 2.0. Уточнено описание сервиса получения данных о субъекте (Приложение Б.7). Уточнен формат адреса, используемый в REST-сервисе ЕСИА.

СПИСОК СОКРАЩЕНИЙ

Сокращение / термин	**Наименование / определение**
ЕГРИП	Единый государственный реестр индивидуальных предпринимателей
ЕГРЮЛ	Единый государственный реестр юридических лиц
ЕПГУ	Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)»
ЕСИА	Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»
ИНН	Идентификационный номер налогоплательщика
ИС	Информационная система
КЭП	Усиленная квалифицированная электронная подпись
ОГВ	Орган государственной власти. Федеральные органы исполнительной власти, государственные внебюджетные фонды, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, государственные и муниципальные учреждения, многофункциональных центров предоставления государственных и муниципальных услуг, а также иные организации, определенные федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации
ОГРН	Основной государственный регистрационный номер
ОГРНИП	Основной государственный регистрационный номер индивидуального предпринимателя
Оператор выдачи ключа ПЭП	Орган или организация, обладающая правом создания (замены) ключа ПЭП в соответствии с постановлением Правительства РФ от 25 января 2013 г. № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг». В соответствии с

Сокращение / термин	Наименование / определение
	указанным постановлением Правительства, качестве Операторов выдачи ключа ПЭП могут выступать федеральные органы исполнительной власти, государственные внебюджетные фонды, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, государственные и муниципальные учреждения, многофункциональные центры предоставления государственных и муниципальных услуг, а также иные организации, определенные федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации (а также уполномоченные ими организации), осуществляющие оказание государственных или муниципальных услуг и подключенные к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме.
Оператор ЕСИА	Министерство связи и массовых коммуникаций Российской Федерации
Оператор ИС	Организация, осуществляющая регистрацию и управление ИС. В качестве операторов ИС, включенных в регистр информационных систем ЕСИА, могут быть организации, обеспечивающие решение следующих задач: – предоставление государственных и муниципальных услуг; – исполнение государственных и муниципальных функций; – формирование БГИР; – межведомственное электронное взаимодействие; – иные задачи, предусмотренные федеральными законами, актами Президента РФ и актами Правительства РФ.
Пользователь ЕСИА	Пользователь информационно-телекоммуникационной сети «Интернет», зарегистрированный в ЕСИА в качестве физического лица. Может иметь роли индивидуального предпринимателя, сотрудника юридического лица, должностного лица ОГВ.

Сокращение / термин	**Наименование / определение**
Поставщик услуг	ИС, интегрированная с ЕСИА и осуществляющая предоставление пользователям ЕСИА данных и услуг, в частности, государственных и муниципальных услуг в электронной форме.
ПЭП	Простая электронная подпись
Регламент	Регламент взаимодействия участников информационного взаимодействия с оператором ЕСИА и оператором инфраструктуры электронного правительства при организации информационно-технологического взаимодействия информационных систем с использованием ЕСИА
СМЭВ	Федеральная государственная информационная система «Единая система межведомственного электронного взаимодействия»
СНИЛС	Страховой номер индивидуального лицевого счета застрахованного лица в системе персонифицированного учета Пенсионного фонда России
Специалист Центра обслуживания	Сотрудник Оператора выдачи ключа ПЭП, осуществляющий подтверждение личности пользователей ЕСИА.
Технологический портал ЕСИА	Специализированное веб-приложение, размещенное по адресу https://esia.gosuslugi.ru/console/tech. Предназначено, в частности, для управления ИС организаций.
ФИО	Фамилия, имя, отчество
Центр обслуживания	Центр обслуживания органа или организации, имеющей право создания (замены) и выдачи ключа ПЭП. В Центре обслуживания специалистами Центра обслуживания осуществляется регистрация и/или подтверждение личности пользователей ЕСИА
ЮЛ	Юридическое лицо
OAuth	Открытый протокол авторизации
REST	Передача репрезентативного состояния (Representational State Transfer)
SAML	Security Assertion Markup Language
SMS	Служба коротких сообщений (Short Message Service)

1 ВВЕДЕНИЕ

Переход к оказанию государственных и муниципальных услуг в электронном виде требует от государства предоставить людям и органам государственной власти возможности безопасно идентифицировать друг друга онлайн. Когда люди и органы государственной власти могут доверять результатам идентификации друг друга, они могут предоставлять и потреблять услуги, чего нельзя было бы достичь в другом случае из-за большой сложности или важности услуг.

В текущей онлайн среде от людей требуется ведение десятков различных имен пользователей и паролей — по одной паре для каждого вебсайта, с которым пользователь взаимодействует. Сложность такого подхода является бременем для людей и потворствует такому поведению, как повторное использование паролей, что упрощает онлайн мошенничества и нарушения идентификации. В то же время органы государственной власти сталкиваются с постоянно возрастающими затратами на управление учётными записями пользователей, последствиями онлайн мошенничеств и неэффективностью электронных услуг в результате нежелания потенциальными пользователями проходить регистрацию еще одной учётной записи.

Созданная Минкомсвязью России ФГИС ЕСИА:

1. Предоставляет использующим ее информационным системам органов государственной власти решение по достоверной идентификации пользователей (как физических, так и должностных лиц ЮЛ и ОГВ), достигнутой благодаря тому, что:
   - регистрация лица в ЕСИА сопряжена с проверкой значимых для удостоверения личности критериев;
   - ЕСИА обеспечивает защиту размещённой в ней информации в соответствии с законодательством Российской Федерации.
2. Является ориентированной на пользователя – предоставляет ему возможности:
   - идентификации и аутентификации с использованием единой учетной записи и широкого спектра поддерживаемых методов аутентификации при доступе к различным информационным системам органов государственной власти;
   - управления своими персональными данными, размещенными в ЕСИА, и контроля над их предоставлением в информационные системы органов государственной власти.

1.1 Назначение документа

Настоящий документ:

1. Описывает базовые сценарии использования ЕСИА:
   - идентификация и аутентификация пользователей при доступе к информационным системам органов государственной власти (раздел 3);
   - ведение идентификационных данных и полномочий пользователей (раздел 4);
   - получения информационными системами органов государственной власти данных из регистров, хранимых в ЕСИА (раздел 4).
2. Поясняет порядок ведения в ЕСИА регистров (справочников), необходимых для реализации базовых сценариев использования ЕСИА:
   - регистр физических лиц;
   - регистр юридических лиц и должностных лиц юридических лиц;
   - регистр органов государственной власти и должностных лиц органов государственной власти;
   - регистр информационных систем.
3. Предоставляет методические рекомендации по интеграции информационных систем с ЕСИА и обеспечению соответствия положениям нормативно-правовых актов в части использования ЕСИА.

1.2 Нормативные ссылки

Настоящий документ разработан в целях реализации и во исполнение следующих нормативно-правовых актов:

- Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».
- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
- Государственная программа Российской Федерации «Информационное общество (2011 – 2020 годы)», утвержденная распоряжением Правительства Российской Федерации от 20 октября 2010 г. № 1815-р.
- Постановление Правительства Российской Федерации от 28 ноября 2011 г. № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем,

используемых для предоставления государственных и муниципальных услуг в электронной форме».

- Постановление Правительства Российской Федерации от 9 февраля 2012 г. № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке её использования, а также об установлении требований к обеспечению совместимости средств электронной подписи».
- Постановление Правительства Российской Федерации от 25 января 2013 г. № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг».
- Постановление Правительства Российской Федерации от 10 июля 2013 г. № 584 «Об использовании федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».
- Положение «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», утверждённое постановлением Правительства Российской Федерации от 8 июня 2011 г. № 451.
- Положение «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», утверждённое приказом Минкомсвязи России от 13 апреля 2012 г. № 107.

2 ОБЩЕЕ ОПИСАНИЕ ЕСИА

В соответствии с постановлением Правительства Российской Федерации от 28 ноября 2011 г. № 977 ЕСИА должна обеспечивать санкционированный доступ участников информационного взаимодействия (заявителей и должностных лиц ОГВ) к информации, содержащейся в государственных информационных системах, муниципальных информационных системах и иных информационных системах.

При этом ЕСИА не обеспечивает выполнение процессов идентификации, аутентификации и авторизации участников межведомственного взаимодействия, возникающих в процессе использования СМЭВ, в частности, при взаимодействии информационных систем с использованием СМЭВ.

Основные функциональные возможности ЕСИА:

- идентификация и аутентификация пользователей, в том числе:
  - однократная аутентификация[1], которая дает пользователям ЕСИА следующее преимущество: пройдя процедуру идентификации и аутентификации в ЕСИА, пользователь может в течение одного сеанса работы обращаться к любым информационным системам, использующим ЕСИА, при этом повторная идентификация и аутентификация не требуется.
  - поддержка различных методов аутентификации: по паролю, по электронной подписи, а также двухфакторная аутентификация (по постоянному паролю и одноразовому паролю, высылаемому в виде sms-сообщения);
  - поддержка уровней достоверности идентификации пользователя (упрощенная учетная запись, стандартная учетная запись, подтвержденная учетная запись).
- ведение идентификационных данных[2], а именно – ведение регистров физических, юридических лиц, органов и организаций, должностных лиц органов и организаций и информационных систем;
- авторизация уполномоченных лиц ОГВ при доступе к следующим функциям ЕСИА:
  - ведение регистра должностных лиц ОГВ в ЕСИА;

[1] Соответствующий термин на английском языке – Single Sign On
[2] Соответствующий термин на английском языке – Identity Management

  - ведение справочника полномочий в отношении ИС и предоставление пользователям ЕСИА (зарегистрированным в ЕСИА как должностные лица ОГВ) полномочий по доступу к ресурсам ИС, зарегистрированным ЕСИА;
  - делегирование вышеуказанных полномочий уполномоченным лицам нижестоящих ОГВ.
- ведение и предоставление информации о полномочиях пользователей в отношении информационных систем, зарегистрированных в ЕСИА.

3 АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ЧЕРЕЗ ЕСИА

Разработчики государственных сайтов, порталов и прочих веб-приложений могут предоставить своим пользователям возможность входить в систему, используя учётную запись ЕСИА. Это избавляет разработчиков от необходимости делать собственное хранилище учётных записей, обеспечивать безопасность хранения паролей, разрабатывать механизмы регистрации, аутентификации пользователей, поддерживать их в рабочем состоянии.

Под пользователями ЕСИА понимаются следующие категории участников информационного взаимодействия:

- физические лица, имеющие учетную запись в регистре физических лиц ЕСИА;
- индивидуальные предприниматели, т.е. физические лица имеющие признак индивидуального предпринимателя;
- должностные лица юридических лиц, т.е. физические лица, присоединенные к учетным записям юридических лиц ЕСИА;
- должностные лица органов и организаций, т.е. физические лица, присоединенные к учетным записям ОГВ.

Пользователи получают возможность однократной аутентификации. Это означает, что пройдя процедуру аутентификации в ЕСИА, пользователь может в течение одного сеанса работы войти в несколько систем, и при этом повторно вводить логин и пароль не потребуется.

С целью обеспечения указанного функционала в ЕСИА реализовано два альтернативных механизма, которые позволяют разработчику использовать наиболее подходящий для его системы:

- механизм, основанный на стандарте SAML версии 2.0;
- механизм, основанный на модели OpenID Connect 1.0.

Аутентификация с использованием стандарта SAML

ЕСИА использует стандарт SAML версии 2.0, который был разработан в 2005 году концерном OASIS. SAML базируется на языке XML и определяет способы обмена информацией об аутентификации пользователей, их полномочиях и идентификационных данных. В соответствии с принятой в этом стандарте терминологией, ЕСИА выступает в роли доверенного поставщика идентификации (Identity Provider), а система выступает в роли

поставщика услуг (Service Provider)[3].

Общая схема подключения системы к ЕСИА представлена на рисунке ниже.

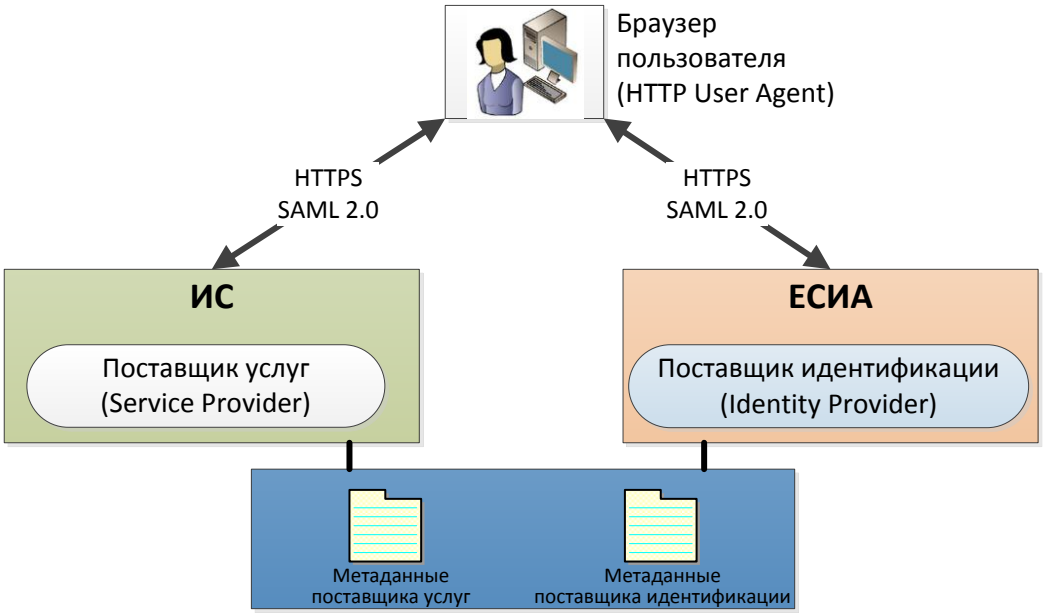

Рисунок 1 – Схема взаимодействия ИС с ЕСИА с целью идентификации и аутентификации с использованием стандарта SAML 2.0

Аутентификация с использованием модели OpenID Connect

В ЕСИА создан механизм аутентификации пользователей, основанный на спецификациях OAuth 2.0 и расширении OpenID Connect 1.0.

Протокол определяет взаимодействие следующих сторон:

- владелец ресурса (resource owner) – сущность, которая может предоставить доступ к защищаемому ресурсу (например, физическое лицо, заявитель);
- система-клиент (client) – приложение, которое запрашивает доступ к защищаемому ресурсу от имени его владельца;
- сервис авторизации (authorization server) – сервис, который выпускает для системы-клиента маркеры идентификации с разрешениями от владельца ресурса, а также маркеры доступа, позволяющие получать доступ к данным;
- поставщик ресурса (resource server) – сервис, обеспечивающий доступ к защищаемому ресурсу на основе проверки маркеров идентификации и маркеров доступа (например, к идентификационным данным пользователя).

[3] Подробное описание схемы интеграции посредством SAML 2.0 представлено в приложении А.

Расширение OpenID Connect 1.0 предполагает использование маркера идентификации (ID Token) в целях проведения идентификации и аутентификации пользователя. Маркер идентификации содержит идентификационные данные пользователя, а также ряд служебных параметров (дата выдачи, время окончания срока действия и пр.).

Для иллюстрации использования OpenID Connect 1.0 в ЕСИА принята следующая терминология:

- владелец ресурса – это пользователь;
- система-клиент – это информационная система интегрированная с ЕСИА с целью идентификации и аутентификации, например региональный портал услуг;
- сервис авторизации и поставщик ресурса – это ЕСИА.

Общая схема подключения системы к ЕСИА для проведения аутентификации представлена на рисунке ниже.

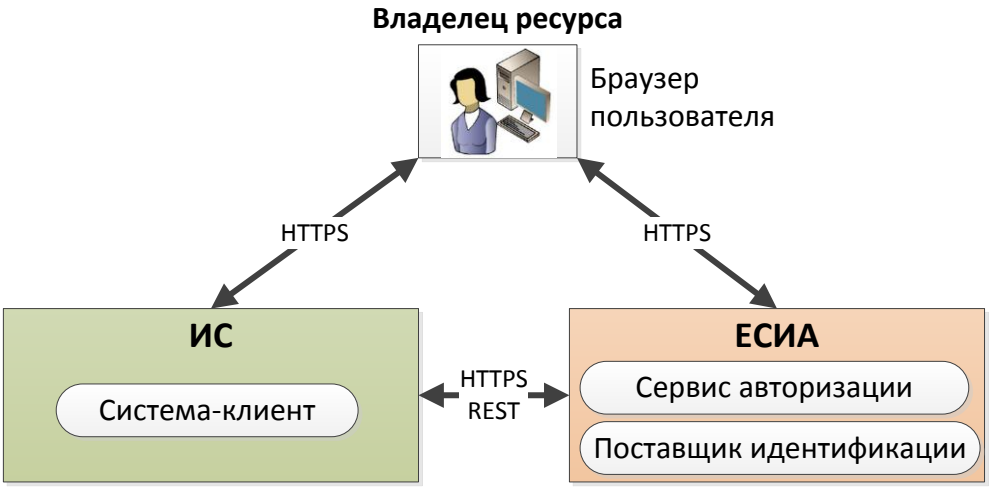

Рисунок 2 – Схема подключения системы к ЕСИА

3.1 Как обеспечить вход пользователей через ЕСИА

Чтобы предоставить пользователям вашей системы возможность входить через ЕСИА, используя тот или иной механизм, со стороны подключающейся системы необходимо обеспечить:

1. Регистрацию ИС в регистре информационных систем ЕСИА (в соответствии с Регламентом[4]).
2. Регистрацию системы с целью идентификации и аутентификации в тестовой среде в соответствии с Регламентом[5]. Исполнение этого процесса предоставляет возможность участнику производить взаимодействие с ЕСИА в тестовой среде.
3. Выполнение доработки интегрируемой системы с целью обеспечения поддержки выбранного механизма идентификации и аутентификации.
4. Подключение продуктивной версии интегрируемой системы к продуктивной среде ЕСИА в соответствии с Регламентом[6].

   Далее каждый из шагов для каждого механизма аутентификации рассмотрен подробнее.

3.1.1 Аутентификация с использованием стандарта SAML

1 и 2 шаг: Регистрация ИС

Регистрация ИС осуществляется согласно Регламенту (раздел 6).

3 шаг: Доработать систему

Рекомендуемая последовательность действий:

1. Сформулировать функциональные требования к взаимодействию своей системы с ЕСИА. Для этого следует:
   - изучить рекомендуемые сценарии использования и выбрать нужные;
   - определить перечень сведений о пользователе, которые вашей ИС требуется получать из ЕСИА в утверждениях SAML;
   - определить требования к уровню достоверности идентификации пользователя (см. п. 4.1.1).

[4] Раздел 6 Регламента.
[5] Раздел 9 Регламента.
[6] Раздел 10 Регламента.

2. Представить или самостоятельно сгенерировать (например, с помощью утилиты keytool из состава Java Development Kit) для своей системы сертификат ключа неквалифицированной электронной подписи в формате X.509 версии 3. Сертификат требуется для идентификации ИС при взаимодействии с ЕСИА. Допускается использование самоподписанного сертификата. Специальные требования: алгоритм RSA, длина ключа 2048 бит. Более подробную информацию о сертификате X.509 можно посмотреть по ссылке http://tools.ietf.org/html/rfc5280.
3. Реализовать интерфейсы поставщика услуг SAML. В качестве исходных данных для разработки следует использовать:
   – функциональные требования, сформированные на 1 шаге;
   – спецификация SAML 2.0 (доступна по ссылке http://saml.xml.org/saml-specifications), в том числе описание профилей Web Browser SSO, Assertion Query/Request, Single Logout Profile;
   – спецификация Interoperable SAML 2.0 Web Browser SSO Deployment Profile (доступна по ссылке http://saml2int.org/profile/current);
   – описание форматов и примеры сообщений SAML в ЕСИА (см. п. А.4–А.7 приложения А);
   – рекомендации по использованию готовых реализаций поставщиков услуг с открытым кодом (см. п. А.2 приложения А).
4. Доработать дизайн сайта, выбрав место для размещения кнопки «Войти через ЕСИА» и реализовать в системе логику обработки данных о пользователях, получаемых из ЕСИА. Недопустимо отображать страницу аутентификации ЕСИА во фрейме сайта.
5. Обеспечить в соответствии с требованиями законодательства комплекс мер, необходимых для обеспечения информационной безопасности и защиты персональных данных пользователей, получаемых информационной системой в процессе ее взаимодействия с системой ЕСИА.
6. Загрузить актуальные метаданные поставщика идентификации ЕСИА:
   – метаданные тестового поставщика идентификации ЕСИА опубликованы по ссылке https://**esia-portal1.test**.gosuslugi.ru/idp/shibboleth[7];

[7] Здесь и далее esia-portal1 в ссылке – имя тестового домена в зависимости от тестовой среды. Конкретную тестовую среду для регистрации устанавливает оператор эксплуатации при обработке заявки на регистрацию.

– метаданные промышленного поставщика идентификации ЕСИА опубликованы по ссылке https://esia.gosuslugi.ru/idp/shibboleth.

7. Подготовить метаданные интегрируемой системы (поставщика услуг). Чтобы подготовить их правильно, рекомендуется использовать следующие исходные данные:
   – описание файла метаданных (п. А.5 приложения А);
   – шаблон файла метаданных (п. А.6 приложения А);
   – требования вашей системы к типу учетной записи:
      - тип роли пользователя (физическое лицо, индивидуальный предприниматель, представителя юридического лица, должностное лицо государственной организации) – блок SupportedGlobalRoles и метаданных;
      - допустимый метод аутентификации (по паролю, по КЭП, усиленная аутентификация) – блок SupportedGlobalRoles метаданных;
      - допустимый уровень (статус) учетной записи (подтверждена или упрощенная/стандартная учетная запись) – блок SupportedAccTypes метаданных.
   – требования вашей системы к перечню сведений о пользователе, которые нужно получать из ЕСИА в утверждениях SAML;
   – сертификат ключа электронной подписи.
8. Синхронизировать системное время сервера, на котором установлена ваша система (поставщик услуг), со значением точного времени. Расхождение более чем в минуту может приводить к возникновению ошибок при взаимодействии поставщика услуг с поставщиком идентификации ЕСИА.
9. Осуществить подключение ИС к тестовой среде и отладить взаимодействие с ЕСИА в тестовой среде в соответствии с Регламентом[8].

4 шаг: Ввести доработку в эксплуатацию

1. Осуществить регистрацию метаданных в промышленной ЕСИА в соответствии с Регламентом[9].
2. После регистрации метаданных проверить работу промышленной версии ЕСИА с промышленной версией вашей системы.

[8] Раздел 9 Регламента.
[9] Раздел 10 Регламента.

3.1.2 Аутентификация с использованием OpenID Connect 1.0

1и 2 шаг: Регистрация ИС

Регистрация ИС осуществляется согласно Регламенту (раздел 6).

При использовании способа аутентификации, основанного на OAuth 2.0 и расширения OpenID Connect, не требуется формирование метаданных.

3 шаг: Доработать систему

Рекомендуемая последовательность действий:

1. Выпустить ключевой контейнер и сертификат ключа квалифицированной электронной подписи для подключаемой информационной системы (должен содержать ОГРН ЮЛ, являющегося оператором информационной системы).

   Дополнительно поддерживается работа с ключевым контейнером и сертификатом ключа неквалифицированной электронной подписи в формате X.509 версии 3. В этом случае является допустимым самостоятельно сгенерировать (например, с помощью утилиты keytool из состава Java Development Kit) для своей системы ключевой контейнер и самоподписанный сертификат. Сертификат требуется для идентификации ИС при взаимодействии с ЕСИА. ЕСИА поддерживает алгоритмы формирования электронной подписи RSA с длиной ключа 2048 бит и алгоритмом криптографического хэширования SHA-256, а также алгоритм электронной подписи ГОСТ Р 34.10-2001 и алгоритм криптографического хэширования ГОСТ Р 34.11-94.
2. Реализовать интерфейсы системы-клиента REST-сервисов ЕСИА и модели контроля доступа, основанной на OAuth 2.0. Детальная информация содержится в приложениях Б и В.
3. Доработать дизайн сайта, выбрав место для размещения кнопки «Войти через ЕСИА» и реализовать в системе логику запроса данных о пользователях, получаемых с помощью программного интерфейса ЕСИА. Недопустимо отображать страницу аутентификации ЕСИА во фрейме сайта.
4. Обеспечить в соответствии с требованиями законодательства комплекс мер, необходимых для обеспечения информационной безопасности и защиты персональных данных пользователей, получаемых информационной системой в процессе ее взаимодействия с системой ЕСИА.
5. Синхронизировать системное время сервера, на котором установлен поставщик услуг, со значением точного времени. Расхождение более чем в минуту может приводить к

возникновению ошибок при взаимодействии поставщика услуг с поставщиком идентификации ЕСИА.

6. Осуществить подключение ИС к тестовой среде и отладить взаимодействие с ЕСИА в тестовой среде в соответствии с Регламентом[10].

4 шаг: Ввести доработку в эксплуатацию

1. Осуществить подключение ИС к промышленной ЕСИА в соответствии с Регламентом[11].
2. После подключения ИС к промышленной ЕСИА проверить работу промышленной версии ЕСИА с промышленной версией вашей системы.

3.2 Рекомендуемые сценарии интеграции по SAML

3.2.1 Сценарии аутентификации пользователей через ЕСИА

Базовый сценарий аутентификации пользователя

Базовым сценарием является сценарий аутентификации физического лица (например, заявителя). Этот сценарий позволяет получить сведения об индивидуальном пользователе (физическом лице) в момент аутентификации и соответствует профилю Web Browser SSO Profile стандарта SAML 2.0. Сценарий включает следующие шаги:

1. Пользователь нажимает на странице системы поставщика услуг кнопку «Войти через ЕСИА».
2. Поставщик услуг формирует и отправляет в ЕСИА запрос на аутентификацию и перенаправляет браузер пользователя на страницу аутентификации ЕСИА.
3. ЕСИА проверяет, статус аутентификации пользователя. Если пользователь в ЕСИА не аутентифицирован, то для продолжения процесса он должен пройти аутентификацию одним из доступных способов. Если пользователь ещё не зарегистрирован в ЕСИА, то он может перейти к процессу регистрации.
4. Когда пользователь аутентифицирован, ЕСИА проверяет, что уровень достоверности идентификации пользователя соответствует требованиям системы, которые зафиксированы в метаданных.

[10] Раздел 9 Регламента.
[11] Раздел 10 Регламента.

5. Когда пользователь успешно аутентифицирован, ЕСИА передаёт в систему ответ на запрос аутентификации, который содержит набор утверждений SAML (SAML Assertions) о пользователе.
6. Поставщик услуг принимает решение об авторизации пользователя на основе полученной из ЕСИА информации.

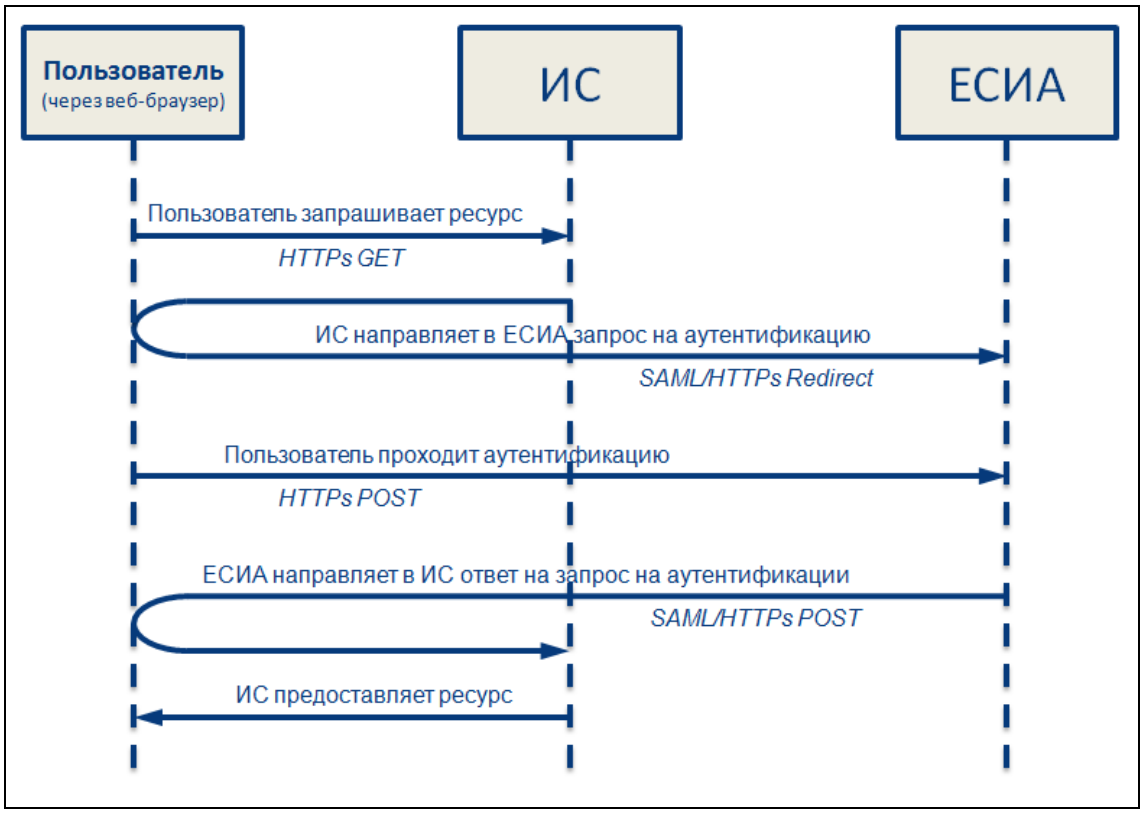

Рисунок 3 – Идентификация и аутентификация пользователей посредством ЕСИА при использовании SAML 2.0

Дополнительный сценарий аутентификации пользователя в качестве представителя организации

ЕСИА также позволяет аутентифицировать пользователя в качестве представителя:

- юридического лица;
- ОГВ.

Эта функция востребована системами, среди пользователей которых есть сотрудники организаций, например, выступающие как заявители услуг или как должностные лица ОГВ. Если включить эту функцию в метаданных поставщика услуг, то ЕСИА в ответе на запрос аутентификации будет передавать сведения об организации пользователя. Если пользователь является участником нескольких организаций, то ЕСИА предварительно попросит пользователя ту из них, от лица которой он осуществляет аутентификацию. Если система поддерживает

работу пользователей с различными ролями, то в процессе аутентификации пользователь будет иметь возможность сделать выбор роли, в которой он будет работать в данной ИС.

Для проверки наличия у аутентифицированного сотрудника ЮЛ необходимых полномочий следует использовать функционал системных групп (4.2.2.3).

Для проверки наличия у аутентифицированного должностного лица необходимых полномочий рекомендуется использовать соответствующее SAML-утверждение (п. 4.3.3).

Сценарий с установкой локальной сессии

Как только пользователь прошел аутентификацию, ЕСИА устанавливает пользовательскую сессию, продолжительность которой составляет 3 часа. Факт начала сессии записывается в файле cookie, который хранится на компьютере пользователя. Система может установить для пользователя свою «локальную» сессию. Рекомендуемая продолжительность сессии – от 15 минут до 3 часов. При завершении «локальной» сессии система должна направлять в ЕСИА новый запрос на аутентификацию.

Сценарий с авторизацией пользователя

Система ЕСИА обладает функционалом по предоставлению поставщику услуг информации, на основании которой возможно проведение авторизации аутентифицированного пользователя. Решение об авторизации пользователя принимает система, в которую пользователь авторизуется (Таблица 1).

Таблица 1 – Требования к авторизации пользователей

Требования	Рекомендуемое решение
Требуется знать что-то о пользователе для одного сеанса работы (например, имя, которым подписывать комментарии пользователя). Нет необходимости хранить данные об активности пользователя до следующего сеанса.	Давать доступ после получения из ЕСИА ответа на запрос аутентификации содержащего требуемый набор сведений о пользователе.
Требуется знать что-то о пользователе (например, ФИО, email и др.) и длительно хранить пользовательский контекст (настройки, заявки, комментарии).	Давать доступ после получения из ЕСИА ответа на запрос аутентификации содержащего требуемый набор сведений о пользователе. При первом входе пользователя регистрировать его идентификатор

	пользователя (userid). В дальнейшем хранить пользовательский контекст в привязке к этому идентификатору.
Требуется ограничить набор предоставляемых функций в зависимости от типа учетной записи, роли пользователя, использованного метода аутентификации.	Давать доступ после получения из ЕСИА ответа на запрос аутентификации содержащего требуемый набор сведений о пользователе. При попытке пользователя обратиться к функции, для предоставления которой текущие тип учетной записи пользователя, роль пользователя или метод аутентификации являются недостаточными, вывести ему сообщение с пояснениями по дальнейшим действиям. Рекомендуемые сообщения для различных ситуаций приведены в таблице 2. В главе 4.1.1 приведены сведения про типы учетных записей пользователей и роли пользователей.

В следующей таблице приведены рекомендации по проверке соответствия требованиям информационной системы типа учетной записи пользователя, роли пользователя и использованного метода аутентификации, а также даны рекомендации по сообщениям, которые стоит предоставить пользователям в случае несоответствия их требованиям системы и приведены рекомендации по дальнейшим действиям.

Таблица 2 – Рекомендации по информированию пользователя о несоответствии авторизации требованиям системы

Ситуация	**Как определить ситуацию**	**Что сообщить и предложить пользователю**
Пользователь с учетной записью с типом упрощенная («непроверенная») попытался обратиться к функциям, предоставляемым только для стандартных («проверенных») и/или	Проанализировать утверждение SAML с именем assuranceLevel или personTrusted (см. таблицу 5)	При доступе к функциям, требующим стандартной (проверенной) учетной записи: «Для доступа вам необходимо пройти процедуру проверки своих данных. Если ваши личные данные только что прошли

«подтвержденных» учетных записей.		проверку, то вам нужно войти в систему повторно.» Ссылка на проверку данных: https://esia-portal1.test.gosuslugi.ru/validate При доступе к функциям, требующим подтвержденной учетной записи: «Для доступа вам необходимо пройти процедуру проверки своих данных и подтверждения личности. Если вы только что подтвердили свою личность, то вам нужно войти в систему повторно.» Ссылка на проверку данных: https://esia-portal1.test.gosuslugi.ru/validate
Пользователь с учетной записью с типом стандартная (проверенная) попытался обратиться к функциям, предоставляемым только для «подтвержденных» учетных записей.	Проанализировать утверждение SAML с именем assuranceLevel (см. таблицу 5)	«Для доступа вам необходимо пройти процедуру подтверждения личности. Если вы только что подтвердили свою личность, то вам нужно войти в систему повторно.» Ссылка на подтверждение личности: https://esia-portal1.test.gosuslugi.ru/confirm
Пользователь с учетной записью с ролью физического лица попытался обратиться к функциям, предоставляемым только для	Проанализировать утверждение SAML с именем globalRole и orgType (см. таблицу 5)	Если необходима роль сотрудника ЮЛ и текущая учетная запись имеет тип «подтверждена»: «Для доступа вам необходимо

ИП / должностных лиц ЮЛ / должностных лиц ОГВ.		войти в систему в качестве сотрудника юридического лица. Если вы являетесь руководителем юридического лица, вы также можете зарегистрировать учетную запись юридического лица» Ссылка для регистрации ЮЛ: https://esia-portal1.test.gosuslugi.ru/org Если необходима роль ИП и текущая учетная запись имеет тип «подтверждена»: «Для доступа вам необходимо войти в систему в качестве индивидуального предпринимателя. Вы также можете зарегистрировать учетную запись индивидуального предпринимателя.» Ссылка: https://esia-portal1.test.gosuslugi.ru/orgs Если необходима роль должностного лица ОГВ и текущая учетная запись имеет тип «подтверждена»: «Для доступа вам необходимо войти в систему в качестве должностного лица органа государственной власти.» Если пользователь имеет упрощенную (непроверенную) /

		стандартную (проверенную) учетную запись, то необходимо его проинформировать о необходимости подтверждения личности. Это является необходимым предварительным условием для возможности получения пользователем роли должностного лица ЮЛ, ОГВ или роли ИП.
Пользователь, аутентифицировавшийся по паролю, попытался получить доступ к функции, требующей аутентификации по электронной подписи	Проанализировать утверждение SAML с именем authnMethod (см. таблицу 5)	«Для доступа вам необходимо использовать средство квалифицированной электронной подписи. Если у вас имеется средство электронной подписи, войдите заново, использовав это средство.» После этого сообщения рекомендуется разместить кнопку вызова единого завершения сессии.

3.2.2 Сценарий единого завершения сессии

В течение действия сессии пользователь может без повторной аутентификации войти в одну или несколько других систем, подключенных к ЕСИА. При возникновении необходимости в одновременном завершении сессии во всех системах используется соответствующий сценарий. Единое завершение сессии необходимо, например, при изменении данных аутентифицированного пользователя – в этом случае для получения информационными системами в утверждениях SAML обновленных данных пользователь должен совершить выход и повторную аутентификацию в ИС.

Единое завершение сессии выполняется в соответствии с профилем Single Logout стандарта SAML. Процесс инициируется пользователем при нажатии кнопки «Выход» в системе поставщика услуг, реализовавшего указанный сценарий. Информационная система не должна самостоятельно инициировать единое завершение сессии.

Сценарий включает следующие шаги:

1. Пользователь нажимает кнопку «Выход» в системе.
2. Система формирует и направляет в ЕСИА запрос на завершение сессии – <LogoutRequest>.
3. ЕСИА определяет остальных участников сессии. Остальные участники сессии – это все системы, в которые пользователь вошёл через ЕСИА на протяжении текущей сессии. Если другие участники существуют, ЕСИА отправляет запрос <LogoutRequest> каждому из них.
4. Система, получившая <LogoutRequest>, завершает на своей стороне активную сессию пользователя (или проверяет, что сессия к этому моменту уже неактивна). Затем формирует и отправляет в ЕСИА ответ о том, что сессия завершена – <LogoutResponse>.
5. Когда все остальные участники корректно завершили свои сессии, ЕСИА формирует и отправляет ответ <LogoutResponse> системе, инициировавшей процедуру завершения сессии. Если какой-то из поставщиков услуг не смог завершить сессию, ЕСИА отображает пользователю веб-страницу, информирующую его о том, что процедура не может быть корректно завершена и что пользователю необходимо перезапустить браузер.
6. Система, инициировавшая процедуру завершения сессии, обрабатывает полученный от ЕСИА ответ. Например, перенаправляет пользователя на веб-страницу завершения сессии.

3.2.3 Форматы сообщений

Основные используемые в ЕСИА форматы электронных сообщений SAML 2.0:

- запрос аутентификации (AuthnRequest);
- ответ на запрос аутентификации(AuthnResponse);
- запрос завершения активной сессии пользователя (LogoutRequest);
- ответ на запрос завершения активной сессии (LogoutResponse);

Детальное описание форматов этих электронных сообщений, а также требований к формированию метаданных для интеграции с ЕСИА, содержится в приложении А.

3.3 Рекомендуемый сценарий аутентификации при интеграции по OpenID Connect 1.0

Базовый сценарий аутентификации

Базовым сценарием аутентификации при использовании OpenID Connect 1.0 является сценарий аутентификации физического лица (например, заявителя).

Сценарий включает следующие шаги:

1. Пользователь нажимает на веб-странице системы-клиента кнопку «Войти через ЕСИА».
2. Система-клиент формирует и отправляет в ЕСИА запрос на аутентификацию и перенаправляет браузер пользователя на специальную страницу предоставления доступа.
3. ЕСИА осуществляет аутентификацию пользователя одним из доступных способов. Если пользователь ещё не зарегистрирован в ЕСИА, то он может перейти к процессу регистрации.
4. Когда пользователь аутентифицирован, ЕСИА сообщает пользователю, что система-клиент запрашивает данные о нем в целях проведения идентификации и аутентификации, предоставляя перечень запрашиваемых системой-клиентом сведений.
5. Если пользователь дает разрешение на проведение аутентификации системой-клиентом, то ЕСИА выдает системе-клиенту специальный авторизационный код.
6. Система-клиент формирует в адрес ЕСИА запрос на получение маркера идентификации, включая в запрос полученный ранее авторизационный код.
7. ЕСИА проверяет корректность запроса (например, что система-клиент зарегистрирована в ЕСИА) и авторизационного кода и передает системе-клиенту маркер идентификации.
8. Система-клиент извлекает идентификатор пользователя из маркера идентификации. Если идентификатор получен, а маркер проверен, то система-клиент считает пользователя аутентифицированным.

После получения маркера идентификации система-клиент использует REST-сервисы ЕСИА для получения дополнительных данных о пользователе, предварительно получив соответствующий маркер доступа (см. приложения Б и В).

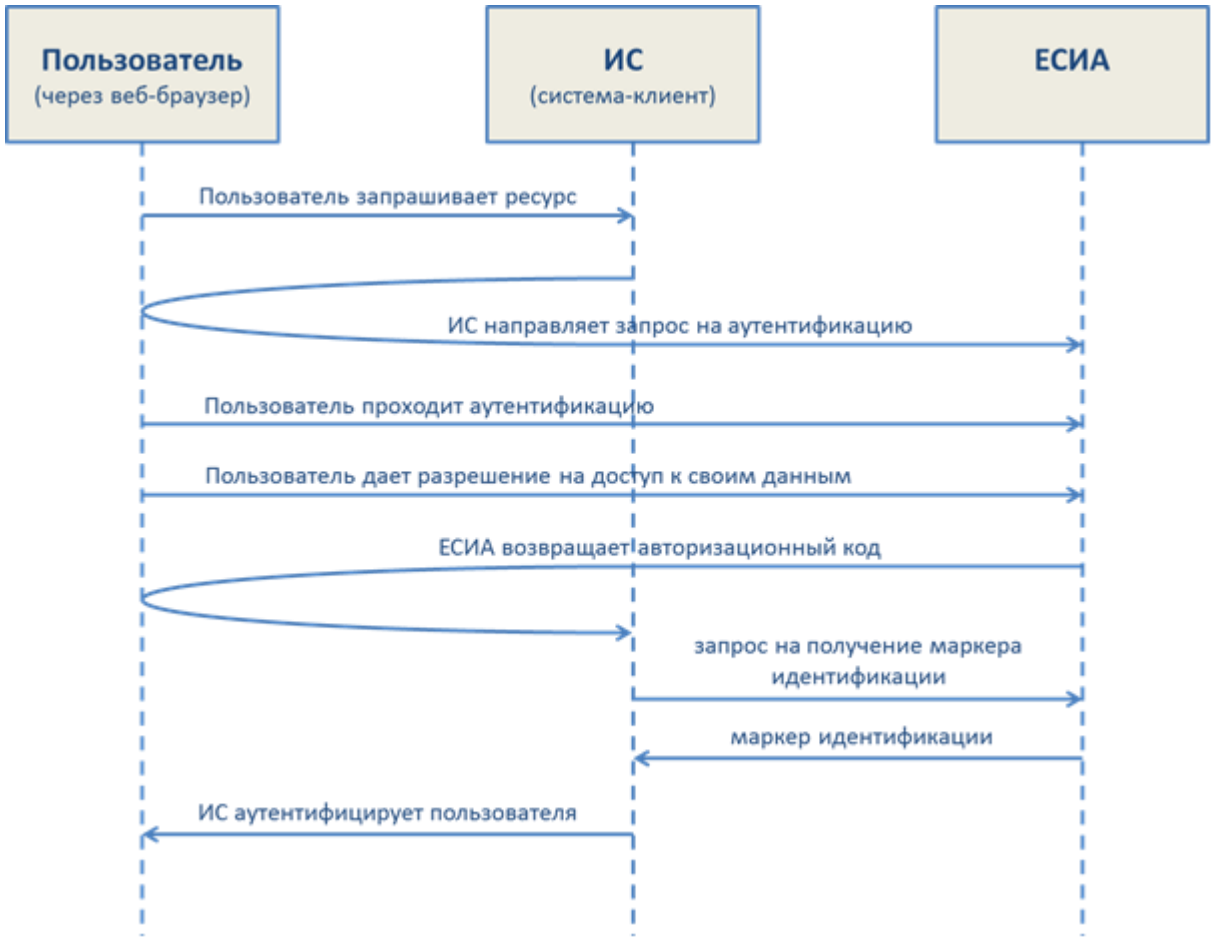

Рисунок 4 – Идентификация и аутентификация пользователей при использовании механизма OpenID Connect 1.0

Дополнительный сценарий аутентификации пользователя в качестве представителя организации

ЕСИА также позволяет аутентифицировать пользователя в качестве представителя организации, для этого ИС должна:

- запросить у ЕСИА не только маркер идентификации, но и маркер доступа (на получение данных пользователя);
- с использованием маркера доступа и программного интерфейса ЕСИА, основанного на REST, получить информацию о том, сотрудником каких организаций является пользователь;
- запросить у пользователя, от имени какой организации он будет работать в данной ИС (если пользователь является сотрудником нескольких организаций).

При необходимости ИС также может проверять, включен ли пользователь в необходимые системные группы юридического лица, является ли он руководителем организации.

Необходимо помнить, что выбор организации, от имени которой будет работать пользователь в ИС, должен происходить на стороне самой ИС с использованием ее средств.

Сценарий с установкой локальной сессии

Как только пользователь прошел аутентификацию, ЕСИА устанавливает пользовательскую сессию, продолжительность которой составляет 3 часа. Факт начала сессии записывается в файле cookie, который хранится на компьютере пользователя. Система может установить для пользователя свою «локальную» сессию. Рекомендуемая продолжительность сессии – от 15 минут до 3 часов. При завершении «локальной» сессии система должна направлять в ЕСИА новый запрос на аутентификацию.

Сценарий с авторизацией пользователя

Система ЕСИА обладает функционалом по предоставлению системе-клиенту информации, на основании которой возможно проведение авторизации аутентифицированного пользователя. Решение об авторизации пользователя принимает система, в которую пользователь авторизуется.

Для получения авторизационных данных следует использовать программный интерфейс, основанный на архитектурном стиле REST (п. 4.3, приложение Б). В этом случае помимо маркера идентификации система должна также запросить маркер доступа к нужным авторизационным данным.

Получив маркер доступа, ИС может получить данные о пользователе и на их основе принять решение о предоставлении доступа пользователю к своим ресурсам.

3.4 Требования к визуальному оформлению входа посредством ЕСИА

При использовании ЕСИА для идентификации и аутентификации пользователей, а также для их регистрации, варианты размещения кнопок для входа могут различаться в зависимости от сценария использования ЕСИА:

- аутентификация исключительно посредством ЕСИА;

– аутентификация посредством ЕСИА в качестве одного из возможных вариантов аутентификации.

Независимо от выбранного сценария, при оформлении входа в систему с использованием ЕСИА не рекомендуется использовать слова «аутентификация» или «авторизация», вместо этого следует использовать слово «вход».

3.4.1 Аутентификация исключительно посредством ЕСИА;

Если системой используется аутентификация посредством ЕСИА в качестве единственного способа аутентификации, то в общем случае рекомендуется размещать кнопку «Вход» в верхней правой части («в шапке») соответствующей страницы.

При нажатии на кнопку «Вход» должно происходить перенаправление пользователя на страницу аутентификации ЕСИА в соответствии с применяемым сценарием аутентификации.

3.4.2 Аутентификация посредством ЕСИА в качестве одного из возможных вариантов аутентификации

Если системой используется аутентификация посредством ЕСИА в качестве одного из возможных способов аутентификации, то рекомендуется размещать ссылку или кнопку «Вход через ЕСИА» в шапке соответствующего сайта, расположив ее рядом со ссылкой (кнопкой), позволяющей войти в систему при помощи альтернативного провайдера аутентификации.

4 ВЕДЕНИЕ РЕГИСТРОВ ЕСИА

Процессы и механизмы ведения данных регистров ЕСИА имеют свою специфику в зависимости от регистра и типа пользователя. Перечень механизмов и процессов представлен в таблице 3.

Таблица 3 – Основные механизмы ведения регистров ЕСИА

Процесс	**Регистр**	**Механизм**	**Ссылка на раздел документа**
Регистрация	Регистр физических лиц	Веб-интерфейс	4.1.1
		Программный интерфейс, доступный через СМЭВ	Приложение Г
	Регистр юридических лиц	Веб-интерфейс	4.1.2
	Регистр ОГВ	Веб-интерфейс	4.1.3
	Регистр ИС	Веб-интерфейс	4.1.4, 4.1.5
Управление данными	Регистр физических лиц	Веб-интерфейс	4.2.1
	Регистр юридических лиц	Веб-интерфейс	4.2.2
	Регистр ОГВ	Веб-интерфейс	4.2.3
	Регистр ИС	Веб-интерфейс	4.2.4
Получение данных	Регистр физических лиц	Программный интерфейс на основе SAML	4.3, Приложение А
		Программный интерфейс на основе REST	4.3, Приложение Б
	Регистр юридических лиц	Программный интерфейс на основе SAML	4.3, Приложение А
		Программный интерфейс на основе REST	4.3, Приложение Б
	Регистр ОГВ	Программный интерфейс на основе SAML	4.3, Приложение А
	Регистр ИС	Программный интерфейс на	4.3, Приложение Б

		основе REST	

4.1 Регистрация

4.1.1 Регистрация физических лиц и получение ролей

В ЕСИА предусмотрены следующие роли пользователей:

- физические лица, имеющие учетную запись в регистре физических лиц ЕСИА;
- индивидуальные предприниматели, т.е. физические лица имеющие признак индивидуального предпринимателя;
- должностные лица юридических лиц, т.е. физические лица, присоединенные в ЕСИА к учетным записям юридических лиц ЕСИА;
- должностные лица органов и организаций, т.е. физические лица, присоединенные в ЕСИА к учетным записям ОГВ.

Наличие у пользователя роли позволяет информационным системам, взаимодействующим с ЕСИА, использовать эту информацию для выполнения собственных процессов (например, для авторизации).

Пользователи могут иметь в ЕСИА одну или несколько ролей. Базовой является роль физического лица: чтобы получить одну из указанных ролей, пользователь должен быть первоначально зарегистрирован в качестве физического лица.

В ЕСИА предусмотрены учетные записи физических лиц следующих типов, каждый из которых соответствует определенному уровню идентификации пользователя:

- упрощенная (непроверенная) учетная запись (содержит минимальный набор данных о пользователе);
- стандартная (проверенная) учетная запись (данные о пользователе проверены в БГИР);
- подтвержденная учетная запись (данные о пользователе проверены в БГИР, а личность пользователя–физического лица подтверждена одним из доступных способов подтверждения).

Схематично связь между ролями и типами учетных записей физического лица отображена на рис. 5.

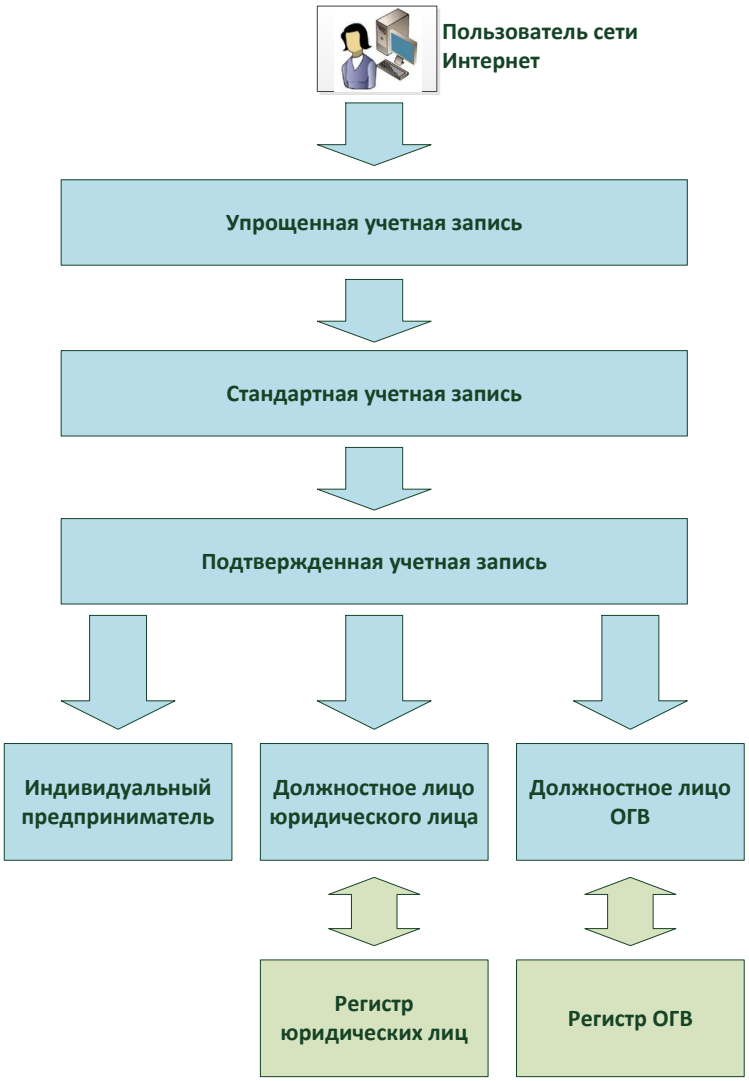

Рисунок 5 – Типы учетных записей и роли пользователя в ЕСИА

4.1.1.1 Регистрация учетной записи физического лица

Регистрация учетной записи физического лица возможна следующими способами:

1. Самостоятельная регистрация пользователя через веб-интерфейс. В этом случае пользователю самостоятельно нужно пройти следующие шаги:
   - регистрация упрощенной (непроверенной) учетной записи пользователя (требуется указать фамилию, имя, один из возможных подтвержденных каналов коммуникации – мобильный телефон или адрес электронной почты);
   - перевод учетной записи в состояние стандартной (проверенной) (включает в себя заполнение пользователем личных данных, инициирование процедуры проверки личных данных в БГИР и автоматическую верификацию личных данных в БГИР).
   - перевод учетной записи в состояние подтвержденной (включает в себя подтверждение личности пользователя одним из доступных способов

подтверждения – с помощью обращения в один из Центров обслуживания[12], отправкой кода подтверждения личности по почте или с помощью КЭП).

2. Регистрация пользователя в одном из Центров обслуживания, ИС которого осуществляет вызов операций с использованием программного интерфейса ЕСИА, опубликованного в СМЭВ. Детальная информация о программном интерфейсе ЕСИА размещена в приложении Г. В результате регистрации в Центре обслуживания пользователь сразу получает подтвержденную учетную запись ЕСИА.

4.1.1.2 Назначение ролей

Назначение всех ролей физического лица в ЕСИА осуществляется с помощью веб-интерфейса.

Детальная информация о назначении основных ролей физического лица представлена в таблице 4.

Таблица 4 – Способы назначения ролей

Роль	Способ назначения роли
Индивидуальный предприниматель	Самостоятельно через веб-интерфейс ЕСИА с помощью направления заявки с данными ИП, включающей в себя: – ФИО; – ИНН физического лица; – ОГРНИП. Заявка проходит проверку в БГИР. Если в ЕГРИП действительно существует запись с указанными данным, то пользователь получает роль индивидуального предпринимателя.
Должностное лицо юридического лица	Получение роли должностного лица ЮЛ в ЕСИА происходит в результате: – регистрации ЮЛ в ЕСИА, в этом случае регистрирующий ЮЛ пользователь получает роль должностного лица ЮЛ с правами руководителя (см. п. 4.1.2); – приглашения руководителем или администратором профиля ЮЛ в ЕСИА сотрудника.

[12] Для подтверждения личности Центры обслуживания могут использовать соответствующий программный интерфейс ЕСИА (см. п. Г.3 приложения Г).

	Процедура приглашения сотрудника для присоединения к организации выполняется с помощью веб-интерфейса ЕСИА. Включает в себя следующие шаги: 1. Руководитель или администратор учетной записи ЮЛ в ЕСИА формирует с помощью веб-интерфейса ЕСИА приглашение на присоединение к организации, включающее в себя: – адрес электронной почты пользователя; – ФИО пользователя; – СНИЛС пользователя (опционально). 2. ЕСИА отправляет на указанный адрес электронной почты пользователя приглашение со ссылкой для присоединения к организации. 3. Пользователь, имеющий подтвержденную учетную запись, входит в ЕСИА по ссылке в приглашении. Если его ФИО и СНИЛС совпадает с данными в приглашении, то он присоединяется к учетной записи ЮЛ. Физическое лицо получает роль должностного лица ЮЛ.
Должностное лицо ОГВ	Получение роли должностного лица ОГВ в ЕСИА происходит в результате: – регистрации ОГВ в ЕСИА, в этом случае регистрирующий ОГВ пользователь получает роль должностного лица ОГВ с правами руководителя (см. п. 4.1.3); – приглашения руководителем или администратором профиля ОГВ в ЕСИА сотрудника. Процедура приглашения сотрудника для присоединения к ОГВ выполняется с помощью веб-интерфейса ЕСИА и аналогична процессу присоединения сотрудника к учетной записи ЮЛ.

Один пользователь ЕСИА может одновременно являться должностным лицом в нескольких ОГВ и ЮЛ, а также иметь роль одного индивидуального предпринимателя.

4.1.2 Регистрация юридических лиц

Регистрация ЮЛ (внесение записи в регистр ЮЛ) осуществляется с помощью веб-

интерфейса ЕСИА. Создавать учетную запись ЮЛ можно только из подтвержденной учетной записи физического лица – руководителя организации или представителя юридического лица, имеющего право действовать от имени организации без доверенности.

Процедура регистрации ЮЛ из подтвержденной учетной записи пользователя включает в себя следующие шаги:

1. Переход во вкладку «Организации» профиля пользователя и инициирование процедуры регистрации.
2. Подключение средства электронной подписи. Для регистрации юридического лица требуется использовать квалифицированную электронную подпись, выданную на имя руководителя юридического лица или на лицо, имеющее право действовать от имени юридического лица без доверенности.
3. Заполнение формы с данными о юридическом лице и данными о руководителе организации. Основные поля предзаполнены, поскольку они были считаны из сертификата электронной подписи, необходимо указать лишь ряд дополнительных сведений об организации:
   - организационно-правовую форму;
   - адрес электронной почты организации.

   Если в личных данных не был указан ИНН, то следует указать ИНН пользователя как физического лица.
4. Ожидание окончания автоматической проверки данных организации и руководителя организации в Федеральной налоговой службе. Если ошибок не возникнет, то юридическое лицо будет зарегистрировано, т.е. будет внесена запись в регистр ЮЛ. Руководитель ЮЛ, осуществлявший регистрацию ЮЛ, автоматически получит роль должностного лица данного ЮЛ и права руководителя.

4.1.3 Регистрация ОГВ

В регистр органов и организаций ЕСИА могут быть включены только организации, подпадающие под действие Постановления Правительства Российской Федерации от 28 ноября 2011 г. № 977.

Регистрация ОГВ осуществляется с помощью единого веб-интерфейса ЕСИА, предусмотренного и для ЮЛ. Специфика заключается в том, что руководитель ОГВ при регистрации в качестве типа своей организации указывает «Орган государственной власти» и выбирает ведомство, подтверждающее статус регистрирующейся организации как ОГВ.

После выполнения проверок данных организации формируется запрос в ведомство, подтверждающее статус регистрирующейся организации как ОГВ. Если данное ведомство подтверждает, что организация имеет статус ОГВ, то учетной записи будет присвоен этот признак и она будет включена в регистр ОГВ. Если не подтверждает, что организация будет иметь учетную запись юридического лица (без признака ОГВ).

4.1.4 Регистрация информационных систем

Регистрация ИС выполняется организацией, являющейся оператором данной ИС. Эта организация предварительно должна быть зарегистрирована в ЕСИА.

В ЕСИА должны быть зарегистрированы ИС, которые:

- используют ЕСИА как поставщик идентификации (Identity Provider) для идентификации и аутентификации пользователей;
- используют ЕСИА в качестве поставщика ресурса (для интеграции по REST и OAuth 2.0);
- осуществляют регистрацию пользователей в ЕСИА.

Для регистрации ИС можно воспользоваться функцией Технологического портала ЕСИА[13].

4.1.5 Регистрация системных групп

Для систем, интегрированных с ЕСИА, имеется возможность проверять наличие у пользователей специфических полномочий по доступу к этой системе. Данная возможность обеспечивается в ЕСИА посредством механизма системных групп – для проведения авторизации сотрудников организаций (ЮЛ или ОГВ). Оператор ИС может зарегистрировать одну или несколько системных групп, которые будут доступны организации; уполномоченные сотрудники ЮЛ смогут включать/исключать своих сотрудников с помощью веб-интерфейса ЕСИА (см. п. 4.2.2.3). После аутентификации данные о принадлежности сотрудника организации к системным группам данной ИС будут переданы в SAML-утверждениях, а также доступны с помощью программного интерфейса, основанного на архитектуре REST.

Регистрацию системных групп можно осуществлять с помощью Технологического портала ЕСИА.

[13] Раздел 6 Регламента.

4.2 Управление данными

4.2.1 Управление данными физических лиц

Управление данными пользователя–физического лица осуществляется им самостоятельно с помощью веб-интерфейса ЕСИА. Доступ к профилю пользователя осуществляется по ссылке:

https://esia-portal1.test.gosuslugi.ru/profile/user/

К персональным данным, размещенным в ЕСИА, относятся:

- основная информация:
  - фамилия, имя, отчество;
  - пол;
  - дата рождения;
  - реквизиты удостоверяющего личность документа (только для стандартной (проверенной) и подтвержденной учетной записи);
  - гражданство (только для стандартной (проверенной) и подтвержденной учетной записи).
- идентификаторы:
  - СНИЛС (только для стандартной (проверенной) и подтвержденной учетной записи);
  - ИНН (только для подтвержденной учетной записи).
- документы:
  - реквизиты водительского удостоверения.
- контактная информация:
  - адрес электронной почты;
  - мобильный телефон;
  - домашний телефон
  - почтовый адрес;
  - адрес регистрации.
- транспортные средства:
  - государственный регистрационный знак транспортного средства и реквизиты свидетельства о регистрации транспортного средства.

Процедура редактирования ряда полей различается в зависимости от того, является ли учетная запись пользователя упрощенной (непроверенной), стандартной (проверенной) или подтвержденной. Для стандартной (проверенной) и подтвержденной учетной записи изменение

ряда полей возможно только после проверки этих данных в БГИР. До тех пор, пока данные не будут подтверждены, изменение данных не произойдет.

4.2.2 Управление данными юридических лиц

Управление данными ЮЛ осуществляется самостоятельно руководителем или администратором профиля ЮЛ с помощью веб-интерфейса ЕСИА. Доступны следующие функции:

- управление идентификационными данными ЮЛ;
- управление сотрудниками ЮЛ;
- управление принадлежностью сотрудников к системным группам (группам доступа).

Войти в профиль организации ЕСИА и управлять данными организации может только уполномоченный сотрудник – т.е. пользователь, который является руководителем организации, выполнившим регистрацию организации, или который включен в группу администраторов профиля ЕСИА.

4.2.2.1 Управление идентификационными данными ЮЛ

Уполномоченный сотрудник имеет возможность редактировать следующие данные ЮЛ:

- организационно-правовая форма;
- адрес электронной почты.

4.2.2.2 Управление сотрудниками ЮЛ

Уполномоченный сотрудник с помощью веб-интерфейса ЕСИА имеет возможность просмотреть перечень сотрудников, т.е. пользователей, присоединенных к организации. Также он имеет возможность:

- отредактировать следующие данные сотрудника:
  - корпоративный адрес электронной почты;
  - должность;
  - КПП филиала (для случаев, когда необходимо, чтобы пользователь действовал от имени филиала данной организации).
- отправить приглашение пользователю для его присоединения к организации (см. п. 4.1.1.2), а также исключить сотрудника из организации. При исключении сотрудника

ЕСИА удаляет пользователя из всех системных групп и исключает сотрудника из ЮЛ, при этом учетная запись сотрудника не удаляется из регистра физических лиц[14].

4.2.2.3 Управление принадлежностью сотрудников к системным группам

Для регулирования доступа сотрудников к интегрированным с ЕСИА информационным системам уполномоченный сотрудник организации имеет возможность с помощью веб-интерфейса ЕСИА включать и исключать сотрудников из системных групп[15].

Группы доступа (системные группы) связаны с информационными системами, доступ к которым они регулируют. Если сотрудник организации был включен в системную группу, то соответствующие данные сможет обрабатывать ИС-владелец данной системной группы: информация о принадлежности к системной группе будет передана в утверждениях SAML, а также может быть получена с помощью программного интерфейса, основанного на архитектурном стиле REST.

Общая схема взаимодействия выглядит следующим образом:

1. ОГВ регистрирует в ЕСИА информационную систему (ИС-1), доступ которой должны получать представители юридических лиц, зарегистрированных в ЕСИА. При регистрации ИС-1 данный ОГВ определяет название соответствующей системной группы (см. п. 4.1.4), например («группа 1»).
2. Уполномоченный сотрудник ЮЛ использует веб-интерфейс ЕСИА для просмотра существующих групп доступа. Находит группы доступа, связанные с системой ИС-1, и видит, что в этом перечне появилась «группа-1».
3. Уполномоченный сотрудник ЮЛ добавляет в «группу-1» сотрудников организации, которым он разрешает действовать в ИС-1 от имени ЮЛ.
4. Сотрудник ЮЛ, включенный в системную группу «группа-1», аутентифицируется с помощью ЕСИА в ИС-1.
5. ИС-1 получает среди SAML-утверждений информацию о том, что пользователь включен в «группу-1» (для этого анализирует утверждение memberOfGroups – см. п. А.5 приложения А), и принимает положительное решение о доступе пользователя к своим ресурсам.

[14] Бывший сотрудник ЮЛ может продолжать использовать свою учетную запись ЕСИА, например, для получения государственных услуг в электронном виде.

[15] Если соответствующими информационными системами предусмотрены группы доступа (системные группы), см. п. 4.1.5.

6. Если другая интегрированная с ЕСИА ИС-2 при аутентификации обрабатывает SAML-утверждение о принадлежности пользователя к группам, то она не увидит информацию о «группе-1», потому что данная ИС-2 не является владельцем этой группы.

4.2.3 Управление данными ОГВ

Управление данными ОГВ осуществляется по аналогии с управлением обычными организации-юридическими лицами, т.е. с помощью веб-интерфейса ЕСИА.

Управление данными ОГВ включает в себя:

- управление должностными лицами ОГВ;
- управление полномочиями должностных лиц ОГВ.

4.2.3.1 Управление должностными лицами ОГВ

Добавление должностных лиц осуществляется в результате выполнения операции приглашения пользователей–физических лиц, имеющих подтвержденную учетную запись ЕСИА. Этот процесс может выполняться с помощью веб-приложения «Профиль организации ЕСИА» по аналогии с управлением сотрудниками ЮЛ.

4.2.3.2 Управление полномочиями должностных лиц ОГВ

Полномочия должностного лица регулируются при помощи механизма системных групп. Выполняется по аналогии с тем, как это реализуется у юридических лиц, не имеющих признака ОГВ (см. п. 4.2.2.3).

4.2.4 Управление данными ИС

Изменение данных ИС осуществляется в соответствии с Регламентом. Уполномоченный сотрудник оператора ИС имеет также возможность с помощью веб-приложения «Технологический портал ЕСИА» осуществлять следующие действия:

- загружать и удалять сертификаты ИС;
- редактировать системные группы (при наличии необходимого полномочия у соответствующей организации).

4.3 Получение данных

Информационная система, подключенная к ЕСИА с целью идентификации и аутентификации, получает информацию о субъектах, данные о которых хранятся в регистрах ЕСИА. С этой целью в ЕСИА предусмотрены следующие программные интерфейсы:

1. Программный интерфейс на основе SAML 2.0. ИС, интегрированная с ЕСИА, получает данные пользователя на момент его аутентификации в ЕСИА. Детальная информация об использовании этого программного интерфейса представлена в приложении А.
2. Программный интерфейс на базе архитектурного стиля “Representational State Transfer” (REST). Он позволяет интегрированным с ЕСИА информационным системам получать доступ к хранящимся в ЕСИА данным в произвольный момент времени после предварительного получения разрешения от пользователя[16]. Обеспечивается доступ к следующим данным:
   - данные о пользователе (идентификационные данные, данные о транспортных средствах, данные о вхождении в организации);
   - данные об организациях (идентификационные данные, данные о сотрудниках);
   - данные об информационных системах (идентификационные данные, данные об организации-владельце).

   Детальная информация об использовании этого программного интерфейса представлена в Приложениях Б и В[17].

4.3.1 Особенности получения данных физических лиц

Получать данные физических лиц (с любыми ролями, за исключением должностных лиц ОГВ) можно с помощью программных интерфейсов, основанных на SAML 2.0 и REST.

Получение данных физических лиц, имеющих роль должностного лица ОГВ, возможно с помощью программных интерфейсов, основанных на SAML 2.0.

При получении данных физических лиц с помощью интерфейса, основанного на SAML 2.0, следует принимать во внимание следующие особенности:

- ИС получает данные пользователя на момент его аутентификации, как результат, если данные о пользователе менялись в течение одной сессии, то ИС сможет получить их только после повторной аутентификации пользователя;
- ИС имеет возможность получать только те данные, которые были определены на стадии подключения ИС к ЕСИА (см. п. 3.1.1).

При получении данных физических лиц с помощью интерфейса, основанного на архитектуре REST, следует принимать во внимание следующие особенности:

[16] За исключением получения данных об ИС (см. п. Б.7 приложения Б и п. В.3 приложения В.
[17] Порядок подключения к ЕСИА с целью использования программных интерфейсов описан в п. 9-10 Регламента.

- ИС получает доступ к данным о пользователе только после явного разрешения со стороны пользователя. У пользователя имеется возможность впоследствии отозвать это разрешение;
- для получения данных о пользователе нет необходимости интегрироваться с ЕСИА по протоколу SAML для аутентификации пользователей.

4.3.2 Особенности получения данных юридических лиц

При получении данных юридических лиц с помощью интерфейса, основанного на SAML 2.0, следует принимать во внимание следующие особенности:

- ИС может получать только данные об одном ЮЛ, в котором состоит физическое лицо, прошедшее аутентификацию (пользователь выбрал ЮЛ, от имени которой будет действовать в данной ИС).

При получении данных юридических лиц с помощью интерфейса, основанного на REST, следует принимать во внимание следующие особенности:

- возможно получение общих данных обо всех ЮЛ, сотрудником которых является данное физическое лицо.
- полный доступ к данным ЮЛ может дать только уполномоченный сотрудник ЮЛ (например, его руководитель), обычный сотрудник ЮЛ может дать разрешение на просмотр лишь ограниченного объема данных.

Схема получения данных о принадлежности сотрудника к системным группам представлена в п. 4.2.2.3.

4.3.3 Особенности получения данных ОГВ и полномочий должностных лиц

Данные об ОГВ могут быть получены с помощью программного интерфейса, основанного на протоколе SAML (в рамках получения данных о должностных лицах ОГВ, аутентифицированных через ЕСИА, см. п. 4.3.1).

Если ИС производит идентификацию и аутентификацию должностных лиц ОГВ с помощью ЕСИА и у нее возникает необходимость проверять наличие у пользователя специфических полномочий, то рекомендуется использовать утверждения SAML systemAuthority (см. Приложение А).

4.3.4 Особенности получения данных ИС

Получать данные об интегрированных с ЕСИА информационных системах можно только посредством программных интерфейсов, основанных на архитектурном стиле REST (см. п. Б.7 приложения Б).

Чтобы система могла быть идентифицирована средствами ЕСИА, она должна загрузить в ЕСИА свой сертификат (см. п. 4.2.4).

Чтобы система могла производить идентификацию ИС через ЕСИА, она должна предварительно получить разрешение на вызов соответствующего REST-сервиса ЕСИА. Необходимость получать данные об ИС должна быть указана в Заявке на создание записи регистра информационных систем в ЕСИА (среди целей подключения ИС в ЕСИА)[18].

[18] См. раздел 6 Регламента.

ПРИЛОЖЕНИЕ А. ИСПОЛЬЗОВАНИЕ ЕСИА В ЦЕЛЯХ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОСРЕДСТВОМ СТАНДАРТА SAML 2.0

А.1 Общие сведения о стандарте SAML 2.0

Взаимодействие ИС с ЕСИА с целью идентификации и аутентификации осуществляется посредством электронных сообщений, основанных на стандарте SAML 2.0.

SAML 2.0 – основанный на XML стандарт по обмену информацией (утверждениями) об аутентификации и авторизации между доверенными доменами безопасности.

Основными компонентами SAML 2.0 являются:

1. Утверждение – информация о подлинности, атрибутах и назначениях;
2. Протокол – правила формирования запросов и ответов в процессе взаимодействий через SAML 2.0.
3. Связывание – отображение протокол SAML 2.0 на транспортные протоколы связи и передачи сообщений;
4. Профиль – сочетание утверждений, протоколов и связываний для поддержки конкретного сценария взаимодействия.

Рисунок 6 – Основные компоненты SAML 2.0

SAML 2.0 определяет синтаксис и семантику утверждений, относящихся к аутентификации, атрибутам и авторизационной информации. Определены следующие типы утверждений:

- утверждение по аутентификации – определяет, что данный субъект прошел аутентификацию определенным способом в определенный момент времени;
- утверждение по авторизации – определяет, на какие действия авторизован конкретный субъект;
- утверждение по атрибутам – определяет специфическую информацию о конкретном субъекте.

SAML 2.0 определяет способ передачи утверждений в протоколах. В ЕСИА используются следующие протоколы SAML 2.0 типа запрос/ответ:

- Authentication Request Protocol (протокол запроса аутентификации) – определяет способы, которыми аутентифицированный субъект может запросить утверждения, содержащие аутентификационные данные и атрибуты субъекта;
- Single Logout Protocol (протокол единого выхода) – определяет механизм одновременного завершения активных сессий, ассоциированных с аутентифицированным субъектом. Выход может инициироваться пользователем или поставщиком идентификации.

Связывания SAML 2.0 определяют, как различные сообщения протоколов SAML 2.0 могут передаваться поверх транспортных протоколов (например, SOAP, HTTP). В ЕСИА используются следующие связывания SAML 2.0:

- HTTP Redirect – определяет, как сообщения протокола SAML 2.0 могут передаваться, используя сообщения HTTP Redirect (ответы с кодом состояния 302);
- HTTP POST – определяет, как сообщения протокола SAML 2.0 могут передаваться с использованием сообщений HTTP POST.

Профили SAML 2.0 определяют, какие утверждения, протоколы и связывания SAML 2.0 могут использоваться в конкретных вариантах использования. В ЕСИА используются следующие профили SAML 2.0:

- Web Browser SSO – определяет, как реализовать однократную аутентификацию в стандартных веб-браузерах;
- Single Logout – определяет, как выполнить одновременный выход из всех сессий.

Как правило, поставщику услуг требуется детальная информация о результатах проведенной аутентификации. Эта информация содержится в контексте аутентификации,

передаваемом в утверждениях SAML 2.0. Аутентификационный контекст (authentication context) определяет синтаксис для описания механизмов аутентификации.

A.2 Общие рекомендации по реализации интерфейсов поставщика услуг

Для реализации интерфейсов поставщика услуг можно использовать уже разработанные различные реализации поставщиков услуг с открытым кодом. Одним из таких поставщиков услуг является OIOSAML, реализованный под различные платформы. Различные реализации OIOSAML можно посмотреть на информационном ресурсе http://digitaliser.dk/group/42063/resources.

Примечание. В сборки последних версий OIOSAML разработчики стали включать библиотеки OpenSAML, которые несовместимы с ЕСИА. В настоящий момент с ЕСИА совместима версия 2.4.1. OpenSAML. Скачать данную версию можно по ссылке: http://www.shibboleth.net/downloads/java-opensaml/2.4.1.

Еще одним возможным вариантом реализации поставщика услуг для сред PHP является SimpleSAMLphp. Более подробную информацию о SimpleSAMLphp можно получить на информационном ресурсе http://simplesamlphp.org.

При самостоятельной реализации интерфейсов поставщика услуг на Java или C++ одним из возможных вариантов является использование набора библиотек с открытым кодом OpenSAML (строго версии 2.4.1.), который поддерживает работу со спецификациями SAML версии 1.0, 1.1 и 2.0. Подробную информацию о библиотеках OpenSAML можно посмотреть на информационном ресурсе https://wiki.shibboleth.net/confluence/display/OpenSAML/Home. Примеры кода по использованию OpenSAML для Java приведены в разделе A.7.

A.3 Общие требования к реализации интерфейса поставщика услуг

Интерфейсы поставщика услуг должны соответствовать следующим профилям SAML 2.0:

- Web Browser SSO с учетом рекомендаций Interoperable SAML 2.0 Web Browser SSO Deployment Profile;
- Single Logout.

Запрос к системе ЕСИА от информационной системы на идентификацию и аутентификацию пользователя должен быть подписан с помощью закрытого ключа информационной системы с использованием следующих алгоритмов:

- алгоритм c14n для каноникализации сообщения в формате XML;
- алгоритмы SHA-1 и RSA – для вычисления цифрового отпечатка сообщения и кода подтверждения целостности сообщения. В качестве протокола доставки должен использоваться метод связывания HTTP-redirect;

Ответ с результатами идентификации и аутентификации пользователя, сформированный системой ЕСИА, подписывается с помощью закрытого ключа системы ЕСИА и преобразуется с использованием открытого ключа информационной системы. При этом используются следующие алгоритмы:

- алгоритм c14n для каноникализации сообщения в формате XML;
- алгоритмы SHA-1 и RSA – для вычисления цифрового отпечатка сообщения и кода подтверждения целостности сообщения;
- алгоритмы RSA и SHA-1 для передачи ключа преобразования сообщения на основе открытого ключа информационной системы, алгоритм AES для осуществления преобразования на переданном ключе. В качестве протокола доставки сообщения от системы ЕСИА информационной системе используется метод связывания HTTP POST.

Запрос к системе ЕСИА от ИС на завершение активной сессии пользователя должен быть подписан с помощью закрытого ключа информационной системы с использованием следующих алгоритмов:

- c14n;
- SHA-1;
- RSA.

В качестве протокола доставки должен использоваться метод связывания HTTP-redirect.

Запрос от системы ЕСИА к ИС на завершение активной сессии пользователя подписывается с использованием закрытого ключа системы ЕСИА. При этом используются следующие алгоритмы:

- c14n;
- SHA-1;
- RSA.

В качестве протокола доставки используется метод связывания HTTP-redirect.

Ответ с результатами завершения активной сессии пользователя от информационной системы к системе ЕСИА должен быть подписан с помощью закрытого ключа информационной системы с использованием следующих алгоритмов:

- c14n;
- SHA-1;
- RSA.

В качестве протокола доставки должен использоваться метод связывания HTTP-redirect.

Ответ с результатами завершения активной сессии пользователя от системы ЕСИА к информационной системе передается подписанным с помощью закрытого ключа системы ЕСИА с использованием следующих алгоритмов:

- c14n;
- SHA-1;
- RSA.

В качестве протокола доставки используется метод связывания HTTP-redirect.

A.4 Описание форматов электронных сообщений SAML 2.0 в ЕСИА

В данном разделе описываются следующие протоколы SAML 2.0, используемые ЕСИА при формировании электронных сообщений:

- протокол запроса аутентификации;
- протокол единого выхода.

Запрос аутентификации (AuthnRequest)

Запрос аутентификации (AuthnRequest) представляет собой XML-документ, который содержит следующие элементы:

1. saml2p:AuthnRequest – описывает параметры запроса AuthnRequest и содержит следующие атрибуты:
   - AssertionConsumerServiceURL – URL провайдера услуг, предназначенный для обработки ответов от поставщика идентификации;
   - Destination – URL-адрес ИС-поставщика идентификации, предназначенный для обработки AuthnRequest;
   - ID – уникальный идентификатор сообщения;
   - IssueInstant – дата создания запроса;

– ProtocolBinding – используемая SAML привязка.

2. saml2:Issuer – идентификатор поставщика услуг, отправившего AuthnRequest (является вложенным по отношению к элементу saml2p:AuthnRequest).

Структура AuthnRequest:

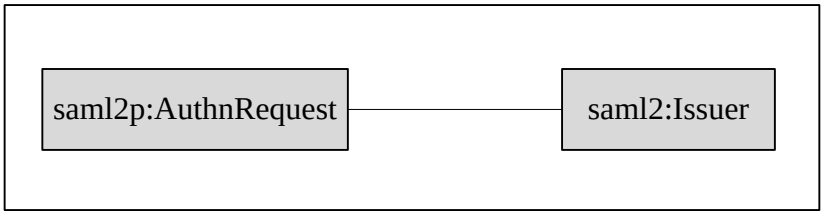

Рисунок 7 – Структура AuthnRequest

Пример AuthnRequest:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
    AssertionConsumerServiceURL="https://atc-504:7002/oiosaml/saml/SAMLAssertionConsumer"
    Destination="https://esia-portal1.test.gosuslugi.ru/idp/profile/SAML2/Redirect/SSO"
    ForceAuthn="false"
    ID="_054240e4-b2a8-48e9-b4c6-e0b5e84d3a35"
    IsPassive="false"
    IssueInstant="2012-02-28T06:43:35.704Z"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Version="2.0">
<saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">sia_test</saml2:Issuer>
</saml2p:AuthnRequest>
```

Для сгенерированного SAML 2.0 сообщения с запросом AuthnRequest должно быть выполнено связывание (binding) с протоколом HTTP по методу HTTP-Redirect с учетом следующих особенностей:

– сообщение подписывается с помощью электронной подписи поставщика услуг, причем подписана должна быть строка запроса на аутентификацию пользователя;

– подписанное сообщение сжимается и кодируется в кодировке Base64.

В процессе связывания формируется конечный URL AuthnRequest, который в качестве GET-параметров должен содержать:

– SAMLRequest – AuthRequest в конечном виде;

– SigAlg – алгоритм подписи запроса, с помощью которого выполнялась подпись запроса аутентификации;

– Signature – подпись, полученная в результате подписания запроса аутентификации.

Пример URL AuthnRequest:

```
https://esia-
portal1.test.gosuslugi.ru/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fZJBa%2BMwEIX%2FitBdlq
zYWyPilLSlbKFLQ%2BzuYS9FkSepwJGyGtn051dxEtpS6EUg9Oabmfc0v37b92SEgNa7muaZoASc8Z11u5o%2Bt%2Fe
soteLOep9Lw9qOcRXt4b%2FA2AkqdChOr3UdAhOeY0WldN7QBWNapZ%2FHpXMhDoEH73xPSVLRAgxtbr1Doc9hAbCaA
08rx9r%2BhrjARXnOhpWikJdCSG5t%2F7Ygk%2FHkfgNQcldGsc6HacVLhS0mnUwZrDzY6YjM0d5n3S7LAzcdgeextr
aHiaq5GvobAATedM8UXLvg4Fp3ZpudY9AycNdTV9EIcy22JRsVpYVK%2FIrzTYm75j%2BVVVFJTeiK02S4koj2hE%2B
ihEHeHAYtYs1lSKXTEgmq1ZUKp%2BpvMhmVfGPktXZqhvrThH85OvmJEL1u21XbPXUtJT8vUSZBPQcnJq6h8%2BJ%2F
QzWF4%2FpItn4EpO%2Fc%2F4ZtThfv36JxTs%3D&RelayState=_12db488a-a516-41e3-801c-
3e8f23547314&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-
```

```
sha1&Signature=k1XL2WfE1KMHzaJtjjaL2O1soweYNM06Xt50E20QgwRzVOBZ0T79HJEjPMu3jBhDdmM47zlrswbh
UFPV22oDbk5KuXJ%2F5FVPwXCTefnVCZGXHU8b1SWuC%2FoKlTSxum6enoommHN5S%2FeYAP9S0KNNW5yEP3eJQHkcs
TYuTKPmyP8%3D
```

Ответ на запрос аутентификации (AuthnResponse).

В случае успешной аутентификации поставщик идентификации формирует ответ на запрос аутентификации – AuthnResponse, который содержит утверждение (Assertion) об аутентификации. AuthnResponse представляет собой XML-документ со следующей структурой:

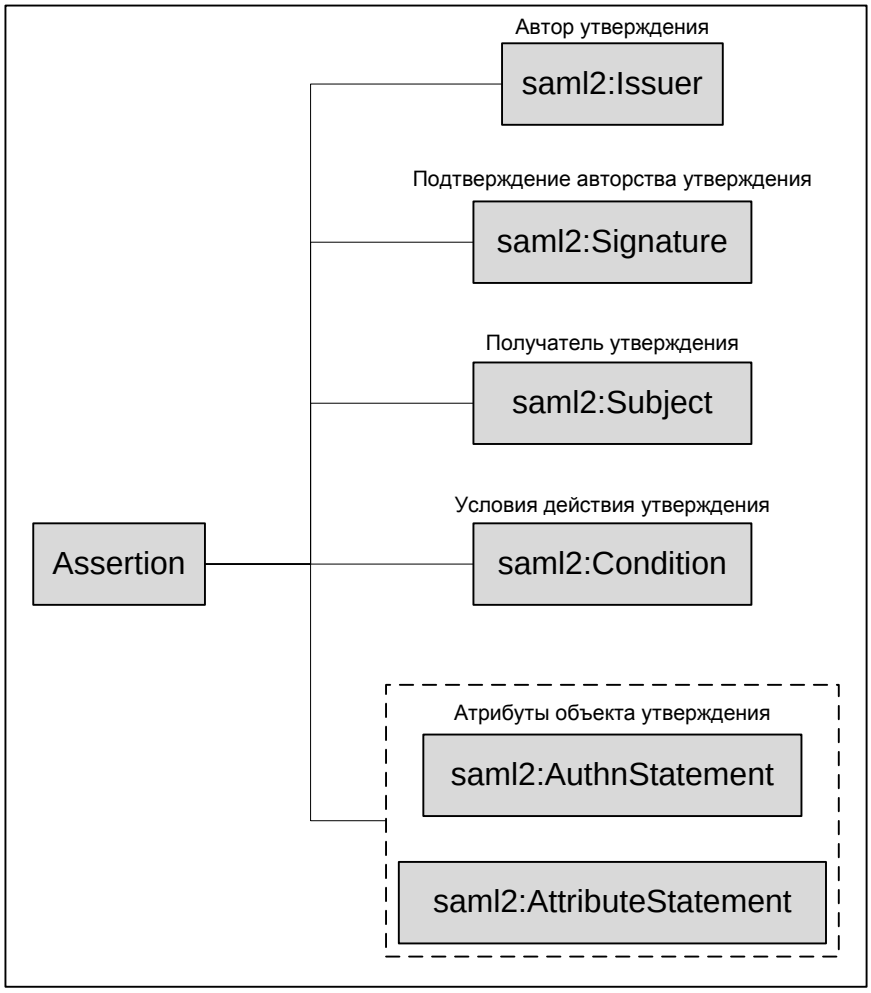

Рисунок 8 – Структура AuthnResponse

Элементы saml2:Issuer и saml2:Signature содержат идентификатор поставщика идентификации и электронную подпись, созданную с помощью сертификата поставщика идентификации.

Элемент saml2:Subject содержит информацию о AuthnRequest, которому соответствует данный AuthnResponse, и представляет собой следующую структуру:

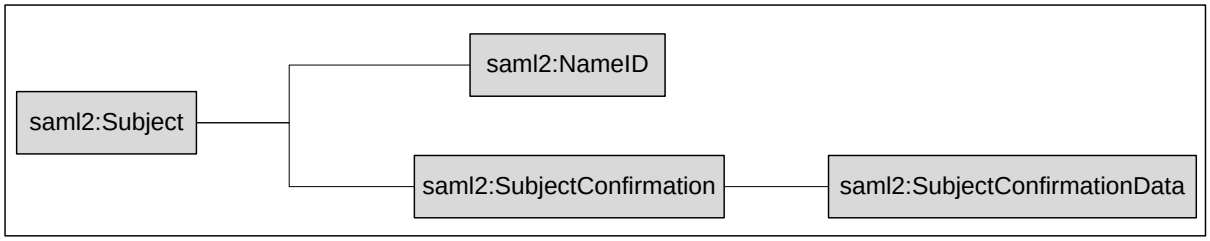

Рисунок 9 – Структура saml2:Subject

Элемент saml2:NameID содержит уникальный идентификатор, присвоенный поставщиком идентификации соответствующему AuthnRequest.

Элемент saml2:SubjectConfirmationData содержит набор атрибутов, в том числе:

- InResponseTo – содержит идентификатор AuthnRequest (соответствует значению атрибута ID);
- NotOnOrAfter – содержит дату, до которой данный AuthnRequest действителен.
- Recipient – URL обработчика AuthnResponse (соответствует значению AssertionConsumerServiceURL).

Элемент saml2:Condition содержит описание условий, при которых данный AuthnResponse считается действительным. Данный элемент имеет два атрибута – NotBefore и NotOnOrAfter, которые указывают на временной промежуток, в который данный AuthnResponse действителен. Также saml2:Condition имеет вложенный элемент saml2:AudienceRestriction, который содержит элемент saml2:Audience с указанием уникального идентификатора поставщика услуг (entity_id).

Элементы saml2:AuthnStatement и saml2:AttributeStatement содержат информацию о результатах аутентификации.

Элемент saml2:AuthnStatement имеет два атрибута:

- AuthnInstant – дата аутентификации;
- SessionIndex – уникальный идентификатор сессии пользователя (с помощью него, например, выполняется повторная аутентификация и операция Logout).

Элемент saml2:AttributeStatement содержит атрибуты пользователя и имеет следующую структуру:

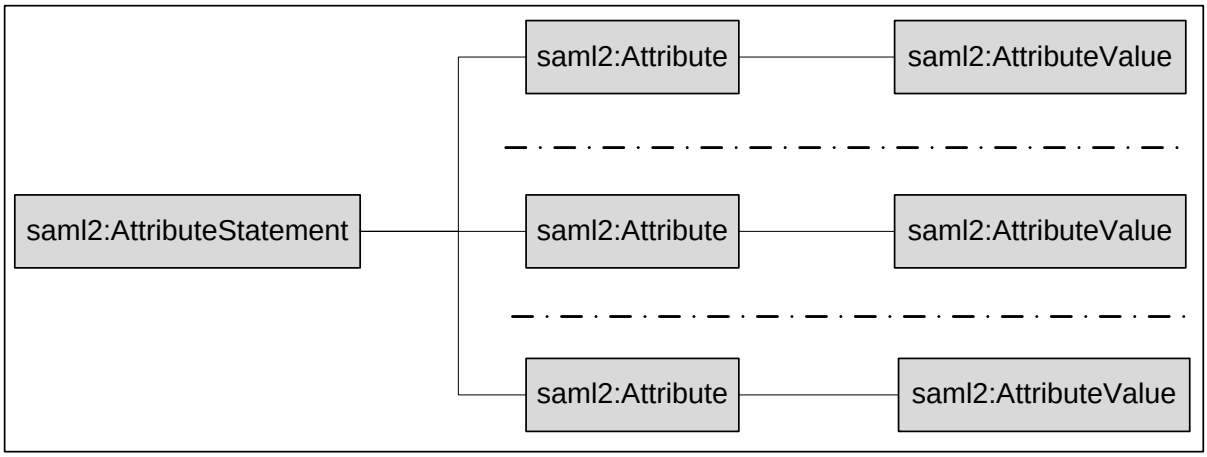

Рисунок 10 – Структура saml2:AttributeStatement

Элемент saml2:Attribute имеет три атрибута:

– FriendlyName – сокращенное наименование атрибута;

– Name – полное наименование атрибута;

– NameFormat – формат полного наименования атрибута.

Элемент saml2:AttributeValues состоит из двух атрибутов: xmlns:xsi и xsi:type. Эти атрибуты определяют формат значения атрибута пользователя.

Пример AuthnResponse приведен в разделе А.9.

Запрос завершения активной сессии пользователя (LogoutRequest)

Запрос завершения активной сессии (LogoutRequest) представляет собой XML-документ со следующей структурой:

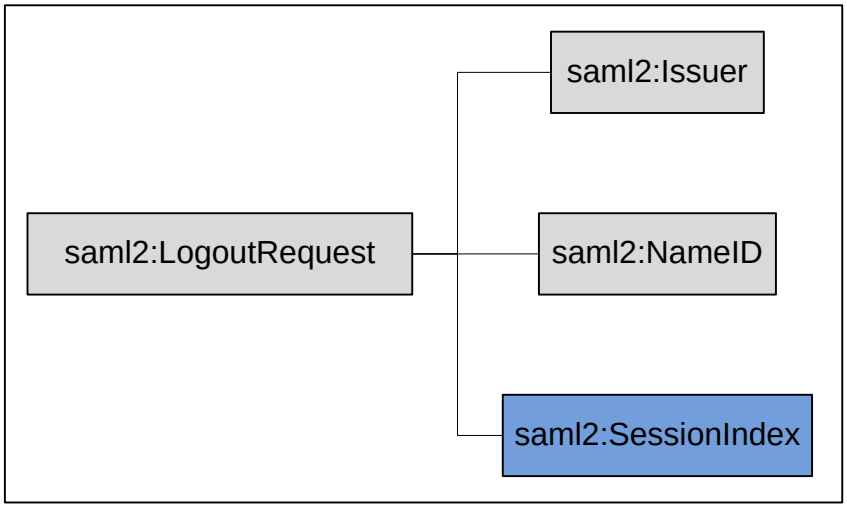

Рисунок 11 – Структура LogoutRequest

Завершение активной сессии пользователя может быть инициировано как со стороны поставщика услуг, так и со стороны поставщика идентификации. В случае, если завершение сессии инициирует поставщик услуг, то LogoutRequest должен содержать обязательный элемент saml2:SessionIndex.

Элемент saml2:LogoutRequest имеет следующие атрибуты:

- Destination – содержит URL обработчика LogoutRequest. В случае если завершение сессии инициировано поставщиком услуг, то содержит URL поставщика идентификации, и наоборот, если инициирован поставщиком идентификации – то URL SP.
- ID – содержит уникальный идентификатор сообщения.
- IssueInstant – дата формирования сообщения.
- Reason – присутствует в случае инициализации завершения сессии со стороны поставщика услуг.

Элемент saml2:Issuer в качестве значения содержит идентификатор (entity_id) инициатора завершения сессии – либо поставщика услуг, либо поставщика идентификации.

Элемент saml2:NameID в качестве значения содержит уникальный идентификатор присвоенный поставщиком идентификации соответствующему AuthnRequest.

Элемент saml2:SessionIndex содержит уникальный идентификатор пользователя, созданный при аутентификации.

Примеры запроса завершения сессии:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:LogoutRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                                                    Destination="https://esia-portal1.test.gosuslugi.ru/idp/profile/SAML2/Redirect/SLO"
                                                    ID="_f51e2082-f899-476d-b88b-6dc743cb4969"
                                                    IssueInstant="2012-03-01T13:46:01.984Z"
                                                    Reason="urn:oasis:names:tc:SAML:2.0:logout:user"
                                                    Version="2.0"
                                                    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        <saml2:Issuer>sia_test</saml2:Issuer>
        <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
                _4b58555ef34da11fae0aa08e8987dbb3
        </saml2:NameID>
        <saml2p:SessionIndex>
                86e46a8d455acd02f5a9ef4072f7b66c46b4422bfc38631aa6e50b8d3f032c43
        </saml2p:SessionIndex>
</saml2p:LogoutRequest>

<?xml version="1.0" encoding="UTF-8"?>
<saml2p:LogoutRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                                                    Destination="https://atc-504:7002/oiosaml/saml/LogoutServiceHTTPRedirect"
                                                    ID="_5741a3cde023a8a669dd720e283642df"
                                                    IssueInstant="2012-03-01T13:51:41.711Z"
                                                    Version="2.0">
        <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
                https://esia-portal1.test.gosuslugi.ru/idp/shibboleth
        </saml2:Issuer>
        <saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
                _4b58555ef34da11fae0aa08e8987dbb3
        </saml2:NameID>
```

```
</saml2p:LogoutRequest>
```

Ответ на запрос завершения активной сессии (LogoutResponse).

Ответ на запрос завершения активной сессии (LogoutResponse) представляет собой XML-документ со следующей структурой:

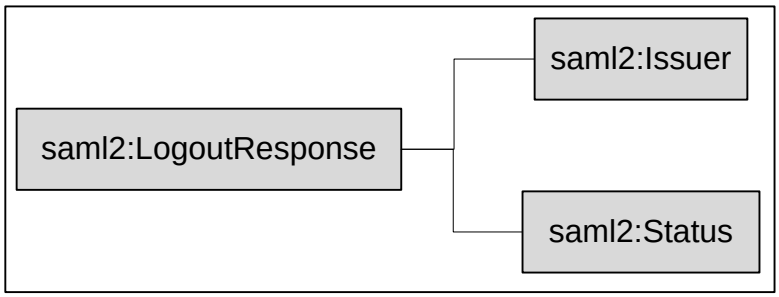

Рисунок 12 – Структура LogoutResponse

Элемент saml2:LogoutResponse имеет следующие атрибуты:

- Destination – содержит URL обработчика LogoutResponse. В случае если завершение сессии инициировано поставщиком услуг, то содержит URL поставщика идентификации, и наоборот, если инициирован поставщиком идентификации – то URL поставщика услуг.
- ID – содержит уникальный идентификатор сообщения.
- InResponseTo – содержит идентификатор LogoutRequest.
- IssueInstant – дата формирования сообщения.

Элемент saml2:Issuer, в зависимости от инициатора завершения сессии, в качестве значения содержит идентификатор (entity_id) инициатора завершения сессии – либо поставщика услуг, либо поставщика идентификации.

Элемент saml2p:Status имеет вложенный элемент saml2p:StatusCode, имеющий атрибут Value, в качестве значения которого передается статус операции.

При этом ответ на запрос завершения сессии не содержит параметр RelayState, переданный изначально при аутентификации пользователя.

Примеры ответа на запрос завершения сессии:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:LogoutResponse xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                                                    Destination="https://atc-504:7002/oiosaml/saml/LogoutServiceHTTPRedirectResponse"
                                                    ID="_a0b3a5b88cf9b96d509ee7b9d497f693"
                                                    InResponseTo="_f51e2082-f899-476d-b88b-6dc743cb4969"
                                                    IssueInstant="2012-03-01T13:45:41.041Z"
                                                    Version="2.0">
        <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                                            Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
                https://esia-portal1.test.gosuslugi.ru/idp/shibboleth
        </saml2:Issuer>
        <saml2p:Status>
                <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
```

```
        </saml2p:Status>
</saml2p:LogoutResponse>

<?xml version="1.0" encoding="UTF-8"?>
<saml2p:LogoutResponse xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                                                    Destination="https://esia-portal1.test.gosuslugi.ru/idp/profile/SAML2/POST/SLO"
                                                    ID="_472d992a-1e50-40ef-8207-fb556eee4893"
                                                    InResponseTo="_5741a3cde023a8a669dd720e283642df"
                                                    IssueInstant="2012-03-01T13:52:08.177Z"
                                                    Version="2.0">
        <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
                sia_test
        </saml2:Issuer>
        <saml2p:Status>
                <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        </saml2p:Status>
</saml2p:LogoutResponse>
```

A.5 Описание метаданных поставщика услуг

Метаданные поставщика услуг определяют способ описания конфигурационных данных (например, URL конечных точек веб-служб, ключи для проверки ЭП). Для описания метаданных ИС поставщика услуг используется язык XML. Структура файла метаданных ИС поставщика услуг приведена на рисунке 13.

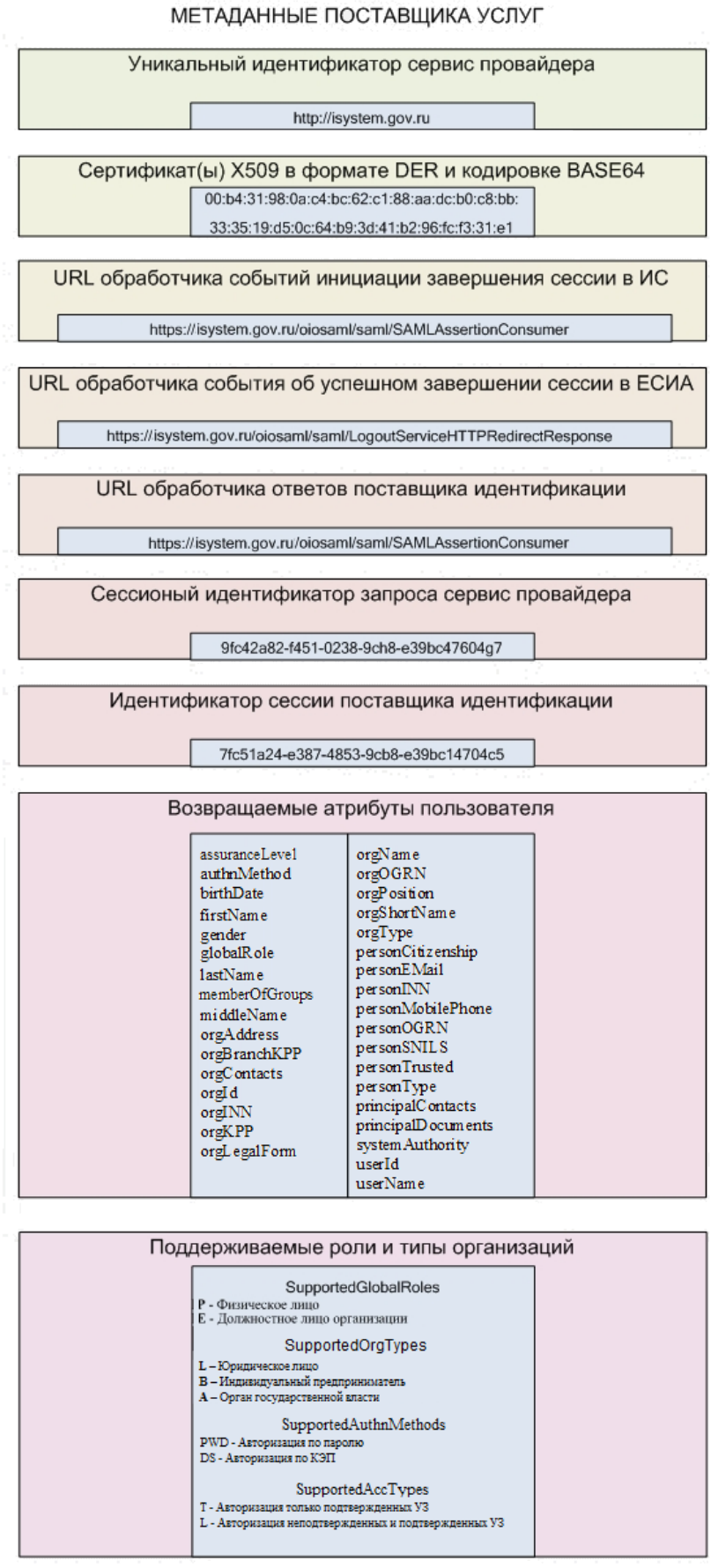

Рисунок 13 – Структура файла метаданных ИС поставщика услуг (пример)

Перечень атрибутов пользователя (организации), содержащихся в файле метаданных поставщика услуг, приведен в таблице 5. Системам, интегрированным с ЕСИА, рекомендуется не использовать или отказаться от использования устаревших утверждений SAML (см. Приложение Д.2).

Если у пользователя или организации отсутствуют те или иные атрибуты, то они не передаются в SAML-утверждениях.

Таблица 5 – Перечень атрибутов, содержащихся в файле метаданных поставщика услуг

№	Атрибут	Описание	Примечание
1.	assuranceLevel	Уровень достоверности идентификации пользователя. Возможны следующие значения: AL10 – упрощенная (непроверенная) учетная запись; AL15 – стандартная (проверенная) учетная запись; AL20 – подтвержденная учетная запись; AL30 – подтвержденная учетная запись (аутентификация по КЭП).	Рекомендуется использовать атрибуты: - personTrusted – для определения подвержденных учетных записей; - authnMethod – для определения метода аутентификации.
2.	attachedToOrg	Признак включенности (присоединения) к организации	Необходимо использовать globalRole
3.	authnMethod	Метод аутентификации. Принимает следующие возможные значения: **PWD** — аутентификации по логину и паролю; **DS —** аутентификации по ЭП.	

№	Атрибут	Описание	Примечание
4.	authToken	Идентификатор сессии пользователя в системе ЕСИА.	
5.	birthDate	Дата рождения пользователя. Передается в формате DD-MM-YYYY	
6.	firstName	Имя пользователя. Не более 256 символов.	
7.	gender	Пол пользователя. Принимает значения: MALE – мужской; FEMALE – женский.	
8.	globalRole	Роль пользователя. Принимает следующие возможные значения: **P** — физическое лицо (Physical person); **E** — должностное лицо организации (Employee).	
9.	inn	ИНН пользователя.	Сохранен для обеспечения совместимости. Вместо него необходимо использовать personINN.
10.	lastName	Фамилия пользователя. Не более 256 символов.	
11.	middleName	Отчество пользователя. Не более 256 символов.	
12.	memberOfGroups	Принадлежность пользователя к группам доступа ИС, осуществляющей идентификацию и	Использовать для определения принадлежности должностных лиц ЮЛ к группам доступа ИС

№	Атрибут	Описание	Примечание
		аутентификацию должностных лиц ЮЛ. Передается в виде мнемоник системных групп через запятую.	
13.	name	Имя пользователя.	Сохранен для обеспечения совместимости. Необходимо использовать lastName / firstName / middleName
14.	nsiId	Мнемоника ОГВ	Сохранен для обеспечения совместимости. Необходимо использовать orgOGRN и orgType
15.	orgAddresses	Адрес организации. Передается в виде XML документа	Каждый адрес в настоящее время описывается следующими атрибутами: <addressType> – тип адреса, в настоящее время может принимать значения: - ORG_LEGAL – юридический адрес; - ORG_POSTAL – почтовый адрес. <contryChar3Code> – код страны из трех символов (для России – RUS); <index> – индекс; <region> – субъект РФ; <street> – улица; <house> – дом; <corpus> – корпус; <structure> – строение;

№	Атрибут	Описание	Примечание
			<flat> – квартира. Все атрибуты, начиная с индекса, – не более 256 символов.
16.	orgBranchKPP	КПП филиала, передается в формате XXXXXXXX, где X – цифры.	
17.	orgBranchName	Имя филиала	
18.	orgContacts	Телефон и Email организации. Передается в виде XML документа	Каждый контакт в настоящее время описывается следующими атрибутами: <contactType> – тип контакта, в настоящее время может принимать значения: - PHN (телефон); - EML (адрес электронной почты); - FAX (факс). <value> – значение контакта, для телефона и факса имеет формат +7(XXX)XXXXXXX*YYYYYY, где *YYYYYY – добавочный номер (только для PHN, опционально, не более 6 цифр), для адреса электронной почты – не более 2000 символов; <verificationStatus> – – статус подтверждения контакта, где S – подтверждено, N – не подтверждено.
19.	orgId	Идентификатор организации.	Сохранен для обеспечения совместимости. Для вновь

№	Атрибут	Описание	Примечание
			подключаемых ИС необходимо использовать orgOid.
20.	orgOid	Идентификатор организации. Любое положительное число.	
21.	orgKPP	КПП организации, передается в формате XXXXXXXX, где X – цифры.	
22.	orgLegalForm	Организационно-правовая форма организации. Передается название формы по справочнику ОКОПФ	
23.	orgINN	ИНН организации пользователя. Передается в формате XXXXXXXXXX, где X – цифры. Данный атрибут устанавливается только для случая, когда атрибут globalRole = E.	
24.	orgName	Наименование организации пользователя. Не более 4000 символов. Данный атрибут устанавливается только для случая, когда атрибут globalRole = E.	
25.	orgShortName	Краткое наименование организации. Не более 500 символов.	

№	Атрибут	Описание	Примечание
26.	orgOGRN	ОГРН организации пользователя. Передается в формате XXXXXXXXXXXXX, где X – цифры. Данный атрибут устанавливается только для случая, когда атрибут globalRole = E.	
27.	orgPosition	Должность пользователя в организации. Не более 256 символов.	
28.	orgType	Тип организации. Принимает следующие возможные значения: **B** — индивидуальный предприниматель (Businessman); **L** — юридическое лицо (Legal entity); **A** — орган исполнительной власти (Agency). Данный атрибут устанавливается только для случая, когда атрибут globalRole = E.	
29.	personCitizenship	Гражданство пользователя Гражданство передается по справочнику ОКСМ. Значение для России – «RUS»	

№	Атрибут	Описание	Примечание
30.	personEMail	Адрес электронной почты пользователя. Не более 2000 символов	
31.	personINN	ИНН пользователя. Передается в формате XXXXXXXXXXXX, где X – цифры. Данный атрибут устанавливается только для случая, когда атрибут personType = R.	
32.	personMobilePhone	Номер мобильного телефона пользователя. Передается в формате +7(XXX)XXXXXXX, где X – цифры.	
33.	personOGRN	ОГРНИП пользователя. Передается в формате XXXXXXXXXXXXXX, где X – цифры. Данный атрибут устанавливается только для случая, когда атрибут orgType = B.	
34.	personSNILS	СНИЛС пользователя. Передается в формате XXX-XXX-XXX XX, где X – цифры. Данный атрибут устанавливается только для стандартных (проверенных) и	

№	Атрибут	Описание	Примечание
		подтвержденных учетных записей	
35.	personTrusted	Подтвержденная или неподтвержденная (упрощенная или стандартная) учетная запись пользователя Y – подтвержденная учетная запись; N – неподтвержденная (упрощенная или стандартная) учетная запись.	
36.	personType	Категория пользователя.	Сохранен для обеспечения совместимости. Необходимо использовать personCitizenship.
37.	principalContacts	Контактные данные пользователя. Передается в виде XML документа .	Каждый контакт в настоящее время описывается следующими атрибутами: <contactType> – тип контакта, в настоящее время может принимать значения: - EML (адрес электронной почты); - MBT (мобильный телефон); - PHN (домашний телефон); - CEM (служебный адрес электронной почты пользователя, только для случая, когда атрибут globalRole = E); - CPH (служебный номер

№	Атрибут	Описание	Примечание
			телефона пользователя, только для случая, когда атрибут globalRole = E). <value> – значение контакта, для телефонов имеет формат +7(XXX)XXXXXXX, для адреса электронной почты – не более 2000 символов; <verificationStatus> – – статус подтверждения контакта, где S – подтверждено, N – не подтверждено.
38.	principalDocuments	Документы пользователя. Передается в виде XML документа.	Каждый документ в настоящее время описывается следующими атрибутами: <documentType> – тип документа, в настоящее время это 01 – паспорт гражданина РФ, 02 – документ иностранного гражданина, 05 – водительское удостоверение. <series> – серия документа, 4 символа для паспорта гражданина РФ; <number> – номер документа, 6 символов для паспорта гражданина РФ; <issueDate> – дата выдачи документа в формате YYYY-MM-DDT00:00:00; <verificationStatus> – статус подтверждения доккумента, где

№	Атрибут	Описание	Примечание
			S – подтверждено, N – не подтверждено; <issuedBy> – орган, выдавший документ, строка не более чем из 2000 символов .
39.	snils	СНИЛС пользователя. Данный атрибут устанавливается только для случая, когда атрибут personType = R.	Сохранен для обеспечения совместимости. Необходимо использовать personSNILS.
40.	systemAuthority	Полномочия должностного лица ОГВ. Передается в виде XML с указанием мнемоники полномочия и мнемоники системы.	Использовать для определения полномочий должностных лиц ОГВ и ЮЛ. Для определения принадлежности представителей юридических лиц к группам доступа использовать memberOfGroups[19]
41.	userId	Числовой идентификатор учетной записи пользователя в системе ЕСИА. Любое положительное число.	
42.	userName	Логин пользователя.	Сохранен для обеспечения совместимости. Необходимо использовать userId, personSNILS

[19] В целях обеспечения совместимости системы, получавшие ранее полномочия юридических лиц в утверждении *systemAuthority*, продолжат получать эти данные в этом утверждении. Однако дальнейшее развитие функционала полномочий будет происходить в терминологии групп доступа, в связи с чем этим системам рекомендуется отказаться от использования *systemAuthority* и анализировать утверждения *memberOfGroups*. При регистрации в ЕСИА новых ИС, ориентированных на работу с ЮЛ, они будут иметь возможность зарегистрировать только системные группы. Данные о них будут передаваться в утверждении memberOfGroups.

№	Атрибут	Описание	Примечание
43.	userType	Тип пользователя.	Сохранен для обеспечения совместимости. Необходимо использовать globalRole

A.6 Шаблон файла метаданных

```
<?xml version="1.0" encoding="UTF-8"?>
<!--TODO
Необходимо указать уникальный (в рамках поставщика идентификации) entityID сервис провайдера.
Рекомендуется, чтобы значение атрибута entityID соответствовало домену информационной системы.
Например, http://moscow.rt.ru
-->
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:esia="urn:esia:shibboleth:2.0:mdext"
entityID="http://moscow.rt.ru">
    <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>
                        <!--TODO
                        Сюда необходимо вставить сертификат электронной подписи X509 сервис провайдера
формата DER в кодировке Base64
                        -->
                    </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:KeyDescriptor use="encryption">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>
                        <!--TODO
                        Сюда необходимо вставить сертификат ключа электронной подписи X509 сервис
провайдера формата DER в кодировке Base64
                        -->
                    </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <!--TODO
        Необходимо заполнить атрибуты вызова обработчика сервис провайдера (тэг SingleLogoutService),
отвечающего за обработку событий завершения сессий (logout):
          - Location - endpoint обработчика событий сервис провайдера, отвечающего за обработку
сообщений от поставщика идентификации о том, что пользователь инициировал событие завершения сессии
пользователя;
          - ResponseLocation - endpoint URL обработчика событий сервис провайдера, отвечающего за
обработку сообщений от поставщика идентификации об успешном выполнении операции завершения сессии
пользователя.
        -->
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="endpoint URL" ResponseLocation="endpoint URL"/>
        <!--TODO
        Необходимо заполнить атрибут Location тэга AssertionConsumerService, определяющий endpoint
обработчика событий сервис провайдера, отвечающего за обработку ответа от поставщика идентификации на
AuthnRequest запрос сервис провайдера.
        -->
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="endpoint URL" index="0" isDefault="true"/>
    </md:SPSSODescriptor>
    <md:AttributeAuthorityDescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol
urn:oasis:names:tc:SAML:2.0:protocol">
        <saml:Attribute NameFormat="urn:mace:shibboleth:1.0:nameIdentifier" Name="transientId"><!--
Сессионый идентификатор запроса сервис провайдера--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="authToken" Name="urn:mace:dir:attribute:authToken"><!--Идентификатор сессии поставщика
идентификации--></saml:Attribute>
```

```
        <!--TODO
        Далее следует список дополнительных атрибутов пользователя, которые могут быть включены в ответ
поставщика идентификации на AuthnRequest запрос сервис провайдера.
        Необходимо оставить только те атрибуты, которые необходимы ИС.
        -->
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="userId" Name="urn:mace:dir:attribute:userId"><!--Уникальный идентификатор пользователя в
рамках поставщика идентификации--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="authnMethod" Name="urn:esia:authnMethod"><!--Метод аутентификации с помощью которого
пользователь прошел аутентификацию--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="globalRole" Name="urn:esia:globalRole"><!--Роль под которой аутентифицировался
пользователь--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="lastName" Name="urn:mace:dir:attribute:lastName"><!--Фамилия пользователя--
></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="firstName" Name="urn:mace:dir:attribute:firstName"><!--Имя пользователя--
></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="middleName" Name="urn:mace:dir:attribute:middleName"><!--Отчество пользователя--
></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="personINN" Name="urn:esia:personINN"><!--ИНН пользователя--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="personSNILS" Name="urn:esia:personSNILS"><!--СНИЛС пользователя--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="personOGRN" Name="urn:esia:personOGRN"><!--ОГРНИП пользователя--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="personEMail" Name="urn:esia:personEMail"><!--Электронный адрес пользователя--
></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="assuranceLevel" Name="urn:esia:assuranceLevel"><!--Уровень достоверности идентификации
пользователя--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="birthDate" Name="urn:esia:birthDate"><!--Дата рождения пользователя--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="gender" Name="urn:esia:gender"><!--Пол пользователя--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="memberOfGroups" Name="urn:esia:memberOfGroups"><!--Принадлежность пользователя к группам
доступа--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="systemAuthority" Name="urn:esia:systemAuthority"><!--Полномочия должностного лица--
></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="personCitizenship" Name="urn:esia:personCitizenship"><!--Гражданство пользователя--
></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="personMobilePhone" Name="urn:esia:personMobilePhone"><!--Номер мобильного телефона
пользователя--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="personTrusted" Name="urn:esia:personTrusted"><!--Подтвержденная или неподтвержденная
учетная запись пользователя--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="principalContacts" Name="urn:esia:principalContacts"><!--Контактные данные пользователя--
></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="principalDocuments" Name="urn:esia:principalDocuments"><!--Документы пользователя--
></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="orgType" Name="urn:esia:orgType"><!--Тип организации пользователя--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="orgName" Name="urn:esia:orgName"><!--Имя организации пользователя--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="orgOGRN" Name="urn:esia:orgOGRN"><!--ОГРН организации пользователя--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="orgINN" Name="urn:esia:orgINN"><!--ИНН организации пользователя--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="orgPosition" Name="urn:esia:orgPosition"><!--Должность пользователя в организации--
></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="orgAddresses" Name="urn:esia:orgAddresses"><!--Адрес организации--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="orgBranchKPP" Name="urn:esia:orgBranchKPP"><!--КПП филиала--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
```

```
friendlyName="orgContacts" Name="urn:esia:orgContacts"><!--Телефон и Email организации--
></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="orgOid" Name="urn:esia:orgOid"><!--Идентификатор организации--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="orgKPP" Name="urn:esia:orgKPP"><!--КПП организации--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="orgLegalForm" Name="urn:esia:orgLegalForm"><!--Организационно-правовая форма организации-
-></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="orgShortName" Name="urn:esia:orgShortName"><!--Краткое наименование организации--
></saml:Attribute>
    </md:AttributeAuthorityDescriptor>
    <md:Organization>
        <!--TODO
        Необходимо заполнить описание организации к которой относится интегрируемая с ЕСИА ИС:
         - OrganizationName - имя организации;
         - OrganizationDisplayName - имя организации, которая может отображаться пользователям при
проведении процедуры аутентификации;
         - OrganizationURL - URL web-сайт компании.
        -->
        <md:OrganizationName xml:lang="ru">ОАО «Ростелеком»</md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="ru">Ростелеком</md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="en">http://www.rt.ru</md:OrganizationURL>
    </md:Organization>
    <!--TODO
    Необходимо заполнить атрибуты организации, к которой относится интегрируемая с ЕСИА информационная
система:
     - Company - имя организации, которая осуществляет эксплуатацию ИС;
     - EmailAddress - электронная почта эксплуатации ИС.
    -->
    <md:ContactPerson contactType="technical">
        <md:Company>ОАО «Ростелеком»</md:Company>
        <md:EmailAddress>support@rt.ru</md:EmailAddress>
    </md:ContactPerson>

    <!--**********-->
    <!--EXTENSIONS-->
    <!--**********-->
    <md:Extensions>
        <!--TODO
        Далее следует список поддерживаемых поставщиком услуг глобальных ролей пользователей, а также
поддерживаемые типы организаций (для роли должностное лицо организации).
        Необходимо оставить только те роли и типы организации, которые поддерживаются поставщиком
услуг.
        Примечание. В случае некорректной обработки тэга <md:Extensions> вашей реализацией поставщика
услуг, данный тэг можно закомментировать.
        -->
        <!--TODO
        В случае, если ИС не поддерживает работу с ролью "Должностное лицо организации" данный тэг не
обязателен.
        В случае, если ИС поддерживает глобальную роль "Должностное лицо организации" необходимо также
указать работу с должностными лицами каких типов организации ИС поддерживает.
        В случае, если ИС поддерживает глобальную роль "Должностное лицо организации" (этот случай
включает отсутствия тэга SupportedGlobalRoles), но тэг SupportedOrgTypes отсутствует - ЕСИА будет
считать, что ИС поддерживает все типы организации.
        -->
        <!--В случае отсутствия тэга SupportedGlobalRoles, ЕСИА будет считать, что ИС поддерживает все
глобальные роли-->
      <esia:SupportedGlobalRoles>
                    <esia:GlobalRole ID="P"></esia:GlobalRole> <!-- Физическое лицо -->
                    <esia:GlobalRole ID="E"> <!-- Должностное лицо организации -->
                                <esia:SupportedOrgTypes>
                                    <esia:OrgType ID="L"/> <!-- Юридическое лицо -->
                                    <esia:OrgType ID="B"/> <!-- Индивидуальный предприниматель-->
                                    <esia:OrgType ID="A"/> <!-- Орган исполнительной власти -->
                                </esia:SupportedOrgTypes>
                            </esia:GlobalRole>
      </esia:SupportedGlobalRoles>
      <esia:SupportedAuthnMethods>
                <esia:AuthnMethod ID="PWD"/> <!-- Авторизация по паролю -->
                <esia:AuthnMethod ID="DS"/>  <!-- Авторизация по КЭП -->
      </esia:SupportedAuthnMethods>
      <esia:SupportedAccTypes>
                 <esia:AccType ID="T"/> <!-- Авторизация только подтвержденных УЗ -->
                 <esia:AccType ID="L"/> <!-- Авторизация упрощенных УЗ, но включая подтвержденные -->
```

```
      </esia:SupportedAccTypes>
    </md:Extensions>
</md:EntityDescriptor>
```

A.7 Рекомендации по указанию URL-адресов и выбору идентификатора поставщика услуг

Все URL-адреса в метаданных для продуктивной среды не должны содержать IP адреса – обязательно указание доменного имени портала информационной системы.

Примеры:

1. Правильно для Единого портала государственных услуг (функций):

```
<md:SingleLogoutService
ResponseLocation="http://www.gosuslugi.ru/pgu/saml/LogoutServiceHTTPRedirectResponse"
Location="https://www.gosuslugi.ru/pgu/saml/LogoutServiceHTTPRedirect"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/> <md:AssertionConsumerService
Location="https://www.gosuslugi.ru/pgu/saml/SAMLAssertionConsumer"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" isDefault="true" index="0"/>
```

2. Неправильно для Единого портала государственных услуг (функций):

```
<md:SingleLogoutService
ResponseLocation="http://109.207.1.97/pgu/saml/LogoutServiceHTTPRedirectResponse"
Location="https://109.207.1.97/pgu/saml/LogoutServiceHTTPRedirect"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/> <md:AssertionConsumerService
Location="https://109.207.1.97/pgu/saml/SAMLAssertionConsumer"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" isDefault="true" index="0"/>
```

При выборе идентификатора поставщика услуг (entityID) в продуктивной среде рекомендуется руководствоваться следующими принципами:

1. Поле EntityID должно однозначно соответствовать URL портала информационной системы которая интегрируется с ИС ЕСИА. Примеры:
   - Единый портал государственных услуг (функций): entityID="http://www.gosuslugi.ru";
   - Российская общественная инициатива: entityID="https://www.roi.ru".
2. Указанный в поле entityID URL не должен содержать IP адрес – обязательно указание доменного имени портала информационной системы. Примеры:
   - Единый портал государственных услуг (функций): entityID="http://www.gosuslugi.ru";
   - Некорректный пример: entityID="http://109.207.1.97".

A.8 Примеры кода на языке Java по использованию OpenSAML

Пример кода поставщика услуг

```
public class Resource extends HttpServlet {
        private static SamlConsumer consumer = new SamlConsumer();
```

```
  public void doGet(HttpServletRequest request, HttpServletResponse response)
  {
     requestMessage = consumer.buildRequestMessage();
     response.sendRedirect(requestMessage);
  }
  public void doPost(HttpServletRequest request, HttpServletResponse response)
  {
     responseMessage = request.getParameter("SAMLResponse").toString();
     result = consumer.processResponseMessage(responseMessage);
  }
}
```

Пример кода создания запроса <AuthnRequest>

```
// Создание элемента <Issuer>
// issuerUrl - это url сервис-провайдера, который генерирует сообщение <authnRequest>
String issuerUrl = "http://localhost:8080/saml-demo/resource";
IssuerBuilder issuerBuilder = new IssuerBuilder();
Issuer issuer =
issuerBuilder.buildObject("urn:oasis:names:tc:SAML:2.0:assertion","Issuer","samlp");
issuer.setValue(issuerUrl);
// создание запроса <AutnRequest>
DateTime issueInstant = new DateTime();
AuthnRequestBuilder authRequestBuilder = new AuthnRequestBuilder();
AuthnRequest authRequest =
authRequestBuilder.buildObject("urn:oasis:names:tc:SAML:2.0:protocol", "AuthnRequest",
"samlp");
authRequest.setForceAuthn(new Boolean(false));
authRequest.setIsPassive(new Boolean(false));
authRequest.setIssueInstant(issueInstant);
authRequest.setProtocolBinding("urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST");
authRequest.setAssertionConsumerServiceURL(issuerUrl);
authRequest.setIssuer(issuer);
authRequest.setID(aRandomId);
authRequest.setVersion(SAMLVersion.VERSION_20);
```

Сообщение <AuthnRequest> может содержать и другие элементы, такие как <NameIDPolicy>, <RequestedAuthnContext>. Эти элементы создаются и добавляются в <AuthnRequest> аналогичным образом.

Сгенерированный запрос <AuthnRequest> должен быть преобразовано (marshaled) с использованием “org.opensaml.xml.io.Marshaller” и должен быть закодирован в кодировке Base64 в URL с использованием org.opensaml.xml.util.Base64.

Считывание ответа <Response>

Для считывания ответа <Response>, например, из сервлета, ответ извлекается из структуры “HttpServletRequest”:

```
responseMessage = request.getParameter("SAMLResponse").toString();
```

Извлеченное сообщение “responseMessage” необходимо преобразовать (unmarshal) и извлечь сообщение <Response>:

```
DocumentBuilderFactory documentBuilderFactory = DocumentBuilderFactory.newInstance();
documentBuilderFactory.setNamespaceAware(true);
DocumentBuilder docBuilder = documentBuilderFactory.newDocumentBuilder();
Document document = docBuilder.parse(new
ByteArrayInputStream(authReqStr.trim().getBytes()));
Element element = document.getDocumentElement();
UnmarshallerFactory unmarshallerFactory = Configuration.getUnmarshallerFactory();
Unmarshaller unmarshaller = unmarshallerFactory.getUnmarshaller(element);
Response response = (Response) unmarshaller.unmarshall(element);
```

Далее с извлеченным SAML 2.0 Response message можно выполнять операции. Например, извлечем Subject's Name Id и сертификат:

```
String subject = response.getAssertions().get(0).getSubject().getNameID().getValue();
String certificate =
response.getSignature().getKeyInfo().getX509Datas().get(0).getX509Certificates().get(0).get
Value();
```

A.9 Пример AuthnResponse

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
ID=" f634a1edd5a52c852641c0943475edd7" IssueInstant="2012-03-01T06:30:00.307Z" Version="2.0"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
       <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://esia-
portal1.test.gosuslugi.ru/idp/shibboleth</saml2:Issuer>
       <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              <ds:SignedInfo>
                     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                     <ds:Reference URI="#_f634a1edd5a52c852641c0943475edd7">
                            <ds:Transforms>
                                   <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                   <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                          <ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xs"/>
                                   </ds:Transform>
                            </ds:Transforms>
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
       <ds:DigestValue>6p7pdI3FulCoSG2kZbGOtW1GCag=</ds:DigestValue>
                     </ds:Reference>
              </ds:SignedInfo>
              <ds:SignatureValue>
              </ds:SignatureValue>
              <ds:KeyInfo>
                     <ds:X509Data>
                            <ds:X509Certificate>
                            </ds:X509Certificate>
                     </ds:X509Data>
              </ds:KeyInfo>
       </ds:Signature>
       <saml2:Subject>
              <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:transient">_a8e8800fa174f41782184cbbd21ee05f</saml2:NameID>
              <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                     <saml2:SubjectConfirmationData Address="127.0.0.1" InResponseTo=" 34efa5b7-47e6-
41bb-b51b-fcb57b7a3f87" NotOnOrAfter="2012-03-01T06:35:00.307Z" Recipient="https://atc-
504:7002/oiosaml/saml/SAMLAssertionConsumer"/>
              </saml2:SubjectConfirmation>
       </saml2:Subject>
       <saml2:Conditions NotBefore="2012-03-01T06:30:00.307Z" NotOnOrAfter="2012-03-01T06:35:00.307Z">
              <saml2:AudienceRestriction>
                     <saml2:Audience>sia test</saml2:Audience>
              </saml2:AudienceRestriction>
       </saml2:Conditions>
       <saml2:AuthnStatement AuthnInstant="2012-03-01T06:30:00.182Z"
SessionIndex="211f42f443924066aec4d5bc8740bce17a93ba3358d9e7003333db957540116b">
              <saml2:SubjectLocality Address="127.0.0.1"/>
              <saml2:AuthnContext>

       <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</
saml2:AuthnContextClassRef>
              </saml2:AuthnContext>
       </saml2:AuthnStatement>
       <saml2:AttributeStatement>
              <saml2:Attribute FriendlyName="personSNILS" Name="urn:esia:personSNILS"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                     <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">000-000-000 00</saml2:AttributeValue>
              </saml2:Attribute>
              <saml2:Attribute FriendlyName="userId" Name="urn:mace:dir:attribute:userId"
```

```
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">2006101</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute FriendlyName="snils" Name="urn:mace:dir:attribute:snils"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">000-000-000 00</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute FriendlyName="authnMethod" Name="urn:esia:authnMethod"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">PWD</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute FriendlyName="principalStatus"
Name="urn:mace:dir:attribute:principalStatus" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri">
                    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">A</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute FriendlyName="globalRole" Name="urn:esia:globalRole"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">P</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute FriendlyName="personEMail" Name="urn:esia:personEMail"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">sdf@ddd.ru</saml2:AttributeValue>
                </saml2:Attribute>
                    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">SNILS</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute FriendlyName="personType" Name="urn:esia:personType"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">R</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute FriendlyName="authToken" Name="urn:mace:dir:attribute:authToken"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">b0db6fd1-d674-47bb-8f22-9f8291e59255</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute FriendlyName="userName" Name="urn:esia:userName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">000-000-000 00</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute FriendlyName="middleName" Name="urn:mace:dir:attribute:middleName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Дмитриевич</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute FriendlyName="attachedToOrg" Name="urn:esia:attachedToOrg"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">1</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute FriendlyName="firstName" Name="urn:mace:dir:attribute:firstName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Дмитрий</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute FriendlyName="lastName" Name="urn:mace:dir:attribute:lastName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Дмитриев</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute FriendlyName="portalVersion"
Name="urn:mace:dir:attribute:portalVersion" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri">
                    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">P</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute FriendlyName="userType" Name="urn:mace:dir:attribute:userType"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
```

```
                        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">P</saml2:AttributeValue>
                </saml2:Attribute>
        </saml2:AttributeStatement>
</saml2:Assertion>
```

ПРИЛОЖЕНИЕ Б. СЕРВИСЫ ЕСИА НА БАЗЕ ПОДХОДА REST

Б.1 Общие сведения о программном интерфейсе ЕСИА

В рамках развития ЕСИА реализован прикладной программный интерфейс на базе архитектурного стиля “Representational State Transfer” (REST). Он позволяет интегрированным с ЕСИА информационным системам получать доступ к хранящимся в ЕСИА ресурсам, т.е. данным (например, о пользователях или других информационных системах), а также выполнять ряд операций.

Вызов прикладного программного интерфейса возможен только теми интегрированными с ЕСИА системами, которые имеют на это соответствующие полномочия. Контроль доступа к ресурсам ЕСИА осуществляет сервис авторизации ЕСИА, реализующий модель контроля доступа, основанную на спецификациях OAuth 2.0 (см. Приложение В).

Для обозначения ресурсов используются специальные идентификаторы. Сами ресурсы организованы иерархически, уровни разделены косой чертой – “/”. Ресурсы более «низкого» уровня являются составными частями «родительского уровня»:

В ЕСИА используется два типа ресурсов:

- *документ* содержит информацию об отдельном объекте в базе данных, который характеризуется некоторыми полями и значениями. Например, при доступе к документу об организации сервис возвращает наименование организации, ее тип, ОГРН и др. Кроме того, в документе могут содержаться ссылки на связанные ресурсы: так, в документе об организации размещаются указатели на ресурсы (документы) по ее сотрудникам;
- *коллекция* представляет собой список некоторых ресурсов, например, документов. Перечень организаций, сотрудников отдельной организации – примеры коллекций. Ресурсы, который включены в коллекцию, снабжены собственными идентификаторами (uri). Обычно для обозначения коллекции используются множественные существительные (orgs, sbjs и др.).

Для вызова сервиса ЕСИА, позволяющего получить доступ к защищенному ресурсу, система-клиент должна направить в https-адрес программного интерфейса ЕСИА запрос. Для этого (в зависимости от типа запроса) используются методы GET или POST. В каждом запросе должен быть указан идентификатор ресурса, к которому запрашивается доступ. Кроме того, в запрос на вызов REST-API должен быть добавлен следующий header:

Authorization: Bearer <access token>

<access token> — маркер доступа, предварительно полученный у сервиса авторизации ЕСИА. Срок действия маркера доступа не должен истечь на момент вызова. Маркер доступа должен быть выдан системе-клиенту на <scope>, позволяющий получить запрашиваемый защищенный ресурс. Пример запроса на получение сведений об организации с идентификатором 1000000000:

```
GET /rs/orgs/1000000000 HTTP/1.1\r\n
Authorization: Bearer 75b2c7cbb8da403491c224c9e431cef9\r\n
Host: esia-portal1.test.gosuslugi.ru\r\n
Accept: */*\r\n
\r\n
```

В случае успешной проверки запроса программный интерфейс возвращает данные о защищенном ресурсе. При невозможности выполнить запрос возвращается код ошибки.

При вызове сервиса могут быть заданы параметры запроса (query), которые оформляются стандартным способом. Следующий запрос позволит получить первые 15 организаций из соответствующей коллекции orgs:

```
GET /rs/orgs?pageIndex=0&pageSize=15 HTTP/1.1\r\n
Authorization: Bearer 75b2c7cbb8da403491c224c9e431cef9\r\n
Host: esia-portal1.test.gosuslugi.ru\r\n
Accept: */*\r\n
\r\n
```

При вызове сервиса может быть указана конкретная **схема предоставления данных** об объекте. Для этого необходимо дать ссылку на соответствующую схему в заголовке запросе (с помощью ACCEPT. Например:

```
GET /rs/prns/402 HTTP/1.1\r\n
Authorization: Bearer 75b2c7cbd9db403489c224c9e431cef9\r\n
Host: esia-portal1.test.gosuslugi.ru\r\n
Accept: application/json; schema="https://esia-
portal1.test.gosuslugi.ru/rs/model/prn/Person-1"\r\n
```

Данный запрос позволяет получить сведения о пользователе с идентификатором 402, сформированные согласно схеме Person-1. Это означает, что по мере развития ЕСИА может быть изменен передаваемый атрибутный состав данных о пользователе, в результате чего появляется новые схемы – Person-2, Person-3 и т.д. В связи с этим для получения неизменного состава атрибутов рекомендуется в запросе указывать конкретную схему. Если в качестве схемы указана схема /model/prn/Person без явного указания версии, то возвращается последняя версия. Если схема не указана вообще, то также возвращается последняя версия схемы.

В ответе на корректный запрос выдается JSON-документ, который представляет собой набор пар ключ/значение или массив значений. В заголовке (headers) ответа содержатся следующие данные:

1. Ссылки (links) на связанные ресурсы. Например, если в запросе указан ресурс с данными конкретного пользователя (prns/402), то ссылки будут содержать ресурсы с его контактными данными, документами, адресам, транспортными средствами, а также на «родительский» ресурс с перечнем всех пользователей в системе.

2. Указатель запрошенного ресурса (location), т.е. uri запрошенного ресурса.
3. Тип предоставляемых данных (Content-Type) с указанием схемы предоставляемых данных. Например, если запрашиваются данные о пользователе в схеме Person-1, то будет указано следующее значение: Content-Type: [application/json; q=.2; schema="https://esia-portal1.test.gosuslugi.ru/rs/model/prn/Person-1"]

Пример раздела headers (разрывы строк даны для удобства чтения):

```
        Link:
[<https://esia-
portal1.test.gosuslugi.ru/rs/prns/402/docs>;rel=documents;schema="https://esia-
portal1.test.gosuslugi.ru/rs/model/docs/Documents-1",
<https://esia-
portal1.test.gosuslugi.ru/rs/prns/402/addrs>;rel=addresses;schema="https://esia-
portal1.test.gosuslugi.ru/rs/model/addrs/Addresses-1",
 <https://esia-
portal1.test.gosuslugi.ru/rs/prns/402/ctts>;rel=contacts;schema="https://esia-
portal1.test.gosuslugi.ru/rs/model/ctts/Contacts-1",
 <https://esia-portal1.test.gosuslugi.ru/rs/prns/>;rel=parent;schema="https://esia-
portal1.test.gosuslugi.ru/rs/model/prns/Persons-1"]
        Date: [Tue, 26 Nov 2013 10:04:24 GMT]
        Transfer-Encoding: [chunked]
        Location: [http://esia-portal1.test.gosuslugi.ru/rs/prns/402]
        server: [grizzly/2.2.16]
        Content-Type: [application/json; q=.2; schema="https://esia-
portal1.test.gosuslugi.ru/rs/model/prn/Person-1"]
```

Содержательная часть ответа на запрос содержится в разделе body. Пример возвращаемых данных (разрывы строк даны для удобства чтения) о физическом лице:

```
{
"stateFacts": ["Identifiable"],
"firstName":"Петр",
"lastName":"Петров",
"birthDate":"1385409600",
"gender":"M",
"trusted":"true",
"citizenship":"RUS",
"snils":"111-111-111 11",
"updatedOn":"1385460263"
}
```

Каждое описание объекта или коллекции содержит параметр stateFacts, указывающий на некоторые факты о предоставляемых сведениях. Возможны следующие значения stateFacts:

- Identifiable - имеет идентификатор (например, это конкретный контакт или документ);
- hasSize - имеет размер (например, для коллекции указывает на число элементов коллекции);
- FirstPage - первая страница списка;
- LastPage - последняя страница списка;
- Paginated - постраничный список;
- EntityRoot- корневой объект;
- ReadOnly - объект только для чтения.

Параметр stateFacts позволяет, в частности, производить разделение выводимых

результатов по страницам. Следующий ответ представляет собой первую страницу некоторого перечня (фрагмент, разрывы строки даны для удобства чтения):

```
{
"stateFacts": ["Paginated","FirstPage"],
"elements":[
    "https://esia-portal1.test.gosuslugi.ru/rs/prns/400",
    "https://esia-portal1.test.gosuslugi.ru/rs/prns/401"
],
"pageSize":"2",
"pageIndex":"1"
}
```

Из данного ответа видно, что на каждой странице отображается по 2 элемента.

Для ряда операций поддерживается возможность *встраивания* (embedding) связанных данных. Для этого в запросе соответствующего ресурса необходимо указывать параметр «embed», а в качестве его значения – сущность, которую требуется включить в ответ запроса. Например, при запросе следующего ресурса будут отображаться *ссылки* на контакты пользователя 100000:

```
https://esia-portal1.test.gosuslugi.ru/rs/prns/100000/ctts
```

Однако указание параметра «embed» позволяет получить данные о контактах непосредственно в ответе на следующий запрос:

```
https://esia-portal1.test.gosuslugi.ru/rs/prns/100000/ctts?embed=(elements)
```

В этом случае запрос данного ресурса будет возвращать ответ (фрагмент, разрывы строки даны для удобства чтения):

```
{
    "stateFacts": ["hasSize"],
    "elements": [
        {
            "stateFacts": [
                "Identifiable"
            ],
            "id": 194,
            "type": "MBT",
            "vrfStu": "VERIFIED",
            "value": "+7(910)1234567"
        }
    ],
    "size": 1
}
```

В данном случае на месте ссылок на связанные элементы встраиваются данные контактов.

При встраивании сохраняется возможность получать схемы возвращаемых ресурсов, например:

```
https://esia-portal1.test.gosuslugi.ru/rs/prns/100000/ctts?embed=(elements-1)
```

В этом случае данные об элементах будут возвращаться согласно первой схеме.

Также возможно встраивание нескольких ресурсов в запросе, например:

```
https://esia-portal1.test.gosuslugi.ru/rs/orgs/100000/emps?embed=(elements.person)
```

В этом случае в ответе вместо ссылок на сотрудников организации будут передаваться:

- данные о сотрудниках (elements) – должность, корпоративный e-mail и пр.;
- краткие персональные данные (ФИО, пол, дата рождения и пр.).

При встраивании нескольких ресурсов также возможно указание на версии, например:

```
https://esia-portal1.test.gosuslugi.ru/rs/orgs/100000/emps?embed=(elements-1.person-1)
```

Перечень ссылок, которые могут быть встроены:

- данные о физических лицах:
  - контактные данные (contacts);
  - адреса (addresses);
  - транспортные средства (vehicles);
  - организации, к которым принадлежит физическое лицо (organizations);
- данные об организациях:
  - контактные данные (contacts);
  - адреса (addresses);
  - транспортные средства (vehicles);
- данные о сотрудниках организации:
  - данные о сотруднике как физическом лице (person).
- данные по ссылкам, отображаемым в содержании ответа в разделе «elements» (возможность встраивания elements есть везде, где параметр stateFacts имеет значение “hasSize”).

Далее приведены описания следующих операций программного интерфейса ЕСИА:

- предоставление персональных данных пользователей;
- удаление учётной записи и связанных с ней персональных данных пользователя из ЕСИА;
- предоставление сведений о вхождении пользователя в группы и организации;
- предоставление данных из профиля организации;
- предоставление списка участников группы или организации.

Б.2 Предоставление персональных данных пользователей

Для получения персональных данных о пользователях система-клиент должна направить в https-адрес REST-API системы ЕСИА[20] запрос методом GET. В запросе должен быть указан ресурс, содержащий необходимые данные. Иерархия идентификаторов этих ресурсов в ЕСИА имеет следующий вид:

/prns/{oid}/{collection_name}/{collection_entity_id}, где:

[20] В тестовой среде сервис доступен по URL https://esia-portal1.test.gosuslugi.ru/rs/prns

- prns – перечень (коллекция) пользователей, зарегистрированных в ЕСИА;
- {oid} – внутренний идентификатор объекта, в том числе пользователя, в ЕСИА;
- {collection_name} – ссылка на перечень (коллекцию) типов данных, указанных пользователем с данным oid, возможные значения:
    - ctts – контактные данные;
    - addrs – адреса;
    - docs – документы пользователя;
    - orgs – организации, сотрудником которых является данный пользователь;
    - vhls – транспортные средства пользователя.
- {collection_entity_id} – внутренний идентификатор контакта или документа пользователя в ЕСИА.

В запрос должен быть добавлен header с маркером доступа, позволяющим получить доступ к данному ресурсу (*scope* http://esia.gosuslugi.ru/usr_inf с параметрами).

Пример запроса (вызов сервиса в среде разработки):

```
GET /rs/prns/6924 HTTP/1.1\r\n
Authorization: Bearer 75b2c7cbb8da403491c224c9e431cef9\r\n
Host: esia-portal1.test.gosuslugi.ru\r\n
Accept: */*\r\n
\r\n
```

Данные, которые ЕСИА возвращает в ответ на запрос, представлены в таблице 6.

Таблица 6 –Параметры ответа на запрос о персональных данных пользователя

№	URI запрашиваемого ресурса	Описание ресурса	Предоставляемые данные
1.	/prns/{oid}	Данные о пользователе с идентификатором prn-id	Данные о физическом лице: <firstName> – имя; <lastName> – фамилия; <middleName> – отчество; <birthDate> – дата рождения (задается как количество секунд, прошедших с 00:00:00 UTC 1 января 1970 года); <birthPlace> – место рождения пользователя; <gender> - пол; <trusted> – тип учетной записи (подтверждена (“true”) / не подтверждена (“false”)); <citizenship> - гражданство (идентификатор страны гражданства); <snils> – СНИЛС; <inn> – ИНН; <updatedOn> - дата последнего изменения учетной записи пользователя (задается как количество секунд, прошедших с 00:00:00 UTC 1 января 1970 года)

№	URI запрашиваемого ресурса	Описание ресурса	Предоставляемые данные
2.	/prns/{oid}/ctts	Перечень контактов физического лица	Перечень контактов физического лица (в виде ссылок на ресурс с указанием {ctt_id}, содержащий данные о каждом контакте)
3.	/prns/{oid}/ctts/{ctt_id}	Сведения об отдельной записи в перечне контактов физического лица	Контактные данные: <type> – тип записи, может иметь значения: - “MBT” – мобильный телефон; - “PHN” – домашний телефон; - “EML” – электронная почта; - “CEM” – служебная электронная почта. <vrfStu> – сведения о «подтвержденности» контактов, может иметь значения: - “NOT_VERIFIED” – не подтвержден; - “VERIFIED” – подтвержден. В настоящее время статус “VERIFIED” может быть только у мобильного телефона (“MBT”) и адреса электронной почты (“EML”). <value> – значение контакта.
4.	/prns/{oid}/addrs	Перечень адресов физического лица	Перечень адресов физического лица (в виде ссылок на ресурс с указанием {addr_id}, содержащий данные о каждом адресе)
5.	/prns/{oid}/addrs/{addr_id}	Сведения об отдельной записи в перечне адресов физического лица	Адреса: <type> – тип записи, может иметь значения: - “PLV” – адрес места проживания; - “PRG” – адрес места регистрации. <zipCode> – индекс; <countryId> – идентификатор страны; <addressStr> – адрес в виде строки (не включая дом, строение, корпус, номер квартиры); <building> – строение; <frame> – корпус; <house> – дом; <flat> – квартира; <fiasCode> – код ФИАС; <region> – регион; <city> – город; <district> – внутригородской район; <area> – район; <settlement> – поселение; <additionArea> – доп. территория; <additionAreaStreet> – улица на доп. территории; <street> – улица.
6.	/prns/{oid}/docs	Перечень документов физического лица	Перечень документов физического лица (в виде ссылок на ресурс с указанием {doc_id}, содержащий данные о каждом документе)
7.	/prns/{oid}/docs/{d	Сведения об	Документы:

№	URI запрашиваемого ресурса	Описание ресурса	Предоставляемые данные
	oc_id}	отдельной записи в перечне документов физического лица	<type> – тип записи, может иметь значения: - “RF_PASSPORT” – паспорт гражданина РФ; - “FID_DOC” – документ иностранного гражданина; - “DRIVING_LICENSE” – водительское удостоверение. <vrfStu> – сведения о «подтвержденности» документов, может иметь значения: - “NOT_VERIFIED” – не подтвержден; - “VERIFIED” – подтвержден. <series> – серия документа; <number> - номер документа; <issueDate> - дата выдачи документа; <issueId> –код подразделения; <issuedBy> – кем выдан; <expiryDate> - срок действия документа.
8.	/prns/{oid}/orgs	Перечень организаций, сотрудником которых является данное физическое лицо	Перечень организаций, сотрудником которых является физическое лицо с данным {oid} (в виде ссылок на ресурс с указанием {oid}, содержащий данные о каждой организации)
9.	/prns/{oid}/vhls	Перечень транспортных средств	Перечень транспортных средств, которыми владеет данный пользователь
10.	/prns/{oid}/vhls/{vhl-id}	Транспортное средство пользователя	<name> - имя автомобиля (например, марка или другое пользовательское описание); <numberPlate> - государственный регистрационный знак; <regCertificate> – данные свидетельства о государственной регистрации, включает в себя атрибуты: – <series> - серия свидетельства; – <number> - номер свидетельства.

При отображении всех коллекций (prns, ctts) используется механизм paging.

Пример ответа на запрос контактных данных физического лица (фрагмент, разрывы строк даны для удобства чтения):

```
{
"stateFacts": ["Identifiable"],
"type":"MBT",
"vrfStu":"VERIFIED",
"value":"+7(777)7777777"
}
```

Пример ответа на запрос конкретного адреса физического лица (фрагмент, разрывы строк даны для удобства чтения):

```
{
```

```
"stateFacts": ["Identifiable"],
"type":"PLV",
"addressStr":"Москва город, Академика Челомея улица",
"building":"98",
"countryId":"RUS",
"fiasCode":"18f5d6bb-c00c-4d06-95a7-7862b8be9e3f",
"frame":"99",
"house":"100",
"region":"Москва Город",
"street":"Академика Челомея Улица",
"zipCode":"117630"
}
```


Пример ответа на запрос конкретного документа физического лица (фрагмент, разрывы строк даны для удобства чтения):


```
{
"stateFacts": ["Identifiable"],
"type":"RF_PASSPORT",
"vrfStu":"VERIFIED",
"series":"3333",
"number":"333333",
"issueDate":"1383249600",
"issueId":"333333"
}
```


Пример ответа на запрос конкретного транспортного средства физического лица (фрагмент, разрывы строк даны для удобства чтения):


```
{
    "stateFacts": ["Identifiable"],
    "name": "Хонда",
    "numberPlate": "A133OH177",
    "regCertificate": {
        "series": "77УЕ",
        "number": "204623"
    }
}
```


Пример ответа на запрос всех транспортных средств физического лица, полученный с использованием возможностей встраивания[21] (фрагмент, разрывы строк даны для удобства чтения):


```
{
    "stateFacts": ["hasSize"],
    "elements": [
        {
            "stateFacts": ["Identifiable"],
            "id": 20,
            "name": "Форд",
            "numberPlate": "O981TE177",
            "regCertificate": {
                "series": "1234",
                "number": "567890"
            }
        },
        {
            "stateFacts": ["Identifiable"],
            "id": 24,
            "name": "VW",
            "numberPlate": "A133OH99",
            "regCertificate": {
                "series": "2222",
                "number": "222222"
            }
        }
    ],
    "size": 2
```


[21] Запрошенный ресурс: /prns/100000/vhls?embed=(elements)

```
}
```

Б.3 Проверка факта удаления учётной записи и связанных с ней персональных данных пользователя из ЕСИА

Вызов данной операции предоставляет интегрированным с ЕСИА информационным системам данные об удаленных пользователях в ЕСИА (идентификатор пользователя). Для получения перечня удаленных пользователей система-клиент должна направить в https-адрес REST-API системы ЕСИА запрос методом GET. В запросе должен быть указан ресурс, содержащий необходимые данные. В качестве этого ресурса используется стандартный идентификатор ресурса с персональными данными пользователей (/prns), возвращающий перечень зарегистрированных в системе пользователей (см. раздел Б.2). Специфика вызова данной операции состоит в том, что запрос должен содержать следующие параметры:

- <status> - статус пользователя, должен иметь значение “DELETED”;
- <updatedSince> - дата, начиная с которой необходимо отобразить удаленных пользователей. Задается как количество секунд, прошедших с 00:00:00 UTC 1 января 1970 года.

В запрос должен быть добавлен header с маркером доступа, позволяющим получить доступ к данному ресурсу (*scope* http://esia.gosuslugi.ru/tech_inf с параметрами).

Пример запроса (вызов сервиса в среде разработки):

```
GET /rs/prns?status=DELETED&updatedSince=1384218061 HTTP/1.1\r\n
Authorization: Bearer 75b2c7cbb8da403491c224c9e431cef9\r\n
Host: esia-portal1.test.gosuslugi.ru\r\n
Accept: */*\r\n
\r\n
```

В качестве ответа передается перечень физических лиц, удаленных с указанной даты. Этот перечень представляет собой список ссылок на ресурс с указанием {oid}, содержащий идентификаторы всех удаленных физических лиц с указанной в запросе даты.

Б.4 Предоставление данных из профиля организации

Для получения данных об организациях система-клиент должна направить в https-адрес REST-API системы ЕСИА[22] запрос методом GET. В запросе должен быть указан ресурс, содержащий необходимые данные. Идентификатор этого ресурса в ЕСИА имеет следующий вид:

/orgs/{orgOid}/{collection_name}/{collection_entity_id}, где:

[22] В тестовой среде сервис доступен по URL https://esia-portal1.test.gosuslugi.ru/rs/orgs

- orgs – коллекция организаций, имеющихся в ЕСИА;
- orgOid – внутренний идентификатор организации в ЕСИА; для определения orgOid соответствующей организации необходимо использовать атрибут orgOid, передающийся в утверждениях SAML;
- {collection_name} – ссылка на перечень (коллекцию) типов данных организации с указанным oid, возможные значения:
    - ctts – контактные данные;
    - addrs – адреса;
    - vhls – транспортные средства;
    - brhs – филиалы организации.
- {collection_entity_id} – внутренний идентификатор контакта, адреса, транспортного средства или филиала.

В запрос должен быть добавлен header с маркером доступа, позволяющим получить доступ к данному ресурсу (*scope* http://esia.gosuslugi.ru/org_inf с параметрами).

Пример запроса (вызов сервиса в среде разработки):

```
GET /rs/orgs/1000000000 HTTP/1.1\r\n
Authorization: Bearer 75b2c7cbb8da403491c224c9e431cef9\r\n
Host: esia-portal1.test.gosuslugi.ru\r\n
Accept: */*\r\n
\r\n
```

Данные, которые ЕСИА возвращает в ответ на запрос, представлены в таблице 7.

Таблица 7 –Параметры ответа на запрос о данных организации

№	URI запрашиваемого ресурса	Описание ресурса	Предоставляемые данные
1.	/orgs/{orgOid}	Данные об организации с идентификатором {orgOid}	Данные об организации: <shortName> – сокращенное наименование организации; <fullName> – полное наименование организации; <type> – тип организации. Для государственных организаций – “AGENCY”, для юридических лиц – “LEGAL”; <ogrn> – ОГРН организации; <inn> - ИНН организации; <leg> - код организационно-правовой формы по общероссийскому классификатору организационно-правовых форм; <kpp> - КПП организации; <agencyTerRange> – территориальная принадлежность ОГВ (только для государственных организаций, код по справочнику «Субъекты Российской

№	URI запрашиваемого ресурса	Описание ресурса	Предоставляемые данные
			федерации» (ССРФ), для Российской Федерации используется код 00; <agencyType> – тип ОГВ (только для государственных организаций)[23].
2.	/orgs/{orgOid}/brhs	Перечень филиалов организации	Перечень филиалов организации (в виде ссылок на ресурс с указанием {branch_id}, содержащий данные о каждом филиале)
3.	/orgs/{orgOid}/brhs/{branch_id}	Сведения о филиале организации	Данные о филиале: <name> – имя филиала; <kpp> – КПП филиала; <leg> – код организационно-правовой формы по общероссийскому классификатору организационно-правовых форм. Для просмотра контактных данных и адресов филиала следует воспользоваться ресурсами /orgs/{orgOid}/brhs/{branch_id}/ctts и /orgs/{orgOid}/brhs/{branch_id}/addrs соответственно. Структура этих ресурсов аналогична ресурсам головной организации.
4.	/orgs/{orgOid}/ctts	Перечень контактов организации	Перечень контактов организации (в виде ссылок на ресурс с указанием {ctt_id}, содержащий данные о каждом контакте)
5.	/orgs/{orgOid}/ctts/{ctt_id}	Сведения об отдельной записи в перечне контактов организации	Контактные данные: <type> – тип записи, может иметь значения: - “PHN” – телефон; - “OFX” – факс; - “OEM” – электронная почта. <vrfStu> – сведения о «подтвержденности» контактов, может иметь значения: - “NOT_VERIFIED” – не подтвержден; - “VERIFIED” – подтвержден. <value> – значение контакта.
6.	/orgs/{orgOid}/addrs	Перечень адресов организации	Перечень адресов организации (в виде ссылок на ресурс с указанием {addr_id}, содержащий данные о каждом адресе)
7.	/otg/{orgOid}/addrs/{addr_id}	Сведения об отдельной записи в перечне адресов	Контактные данные: <type> – тип записи, может иметь значения: - “OLG” – юридический адрес;

[23] В настоящее время используются следующие коды:
10.FED – Федеральный орган исполнительной власти;
30.FND – Государственный внебюджетный фонд;
11.REG – Орган исполнительной власти субъекта РФ;
12.LCL – Орган местного самоуправления;
20.GOV – Государственное учреждение;
21.MCL – Муниципальное учреждение.

№	URI запрашиваемого ресурса	Описание ресурса	Предоставляемые данные
		организации	- “OPS” – фактический адрес; <zipCode> – индекс; <countryId> – идентификатор страны; <addressStr> – адрес в виде строки (не включая дом, строение, корпус, номер квартиры); <building> – строение; <frame> – корпус; <house> – дом; <flat> – квартира; <fiasCode> – код ФИАС; <region> – регион; <city> – город; <district> – внутригородской район; <area> – район; <settlement> – поселение; <additionArea> – доп. территория; <additionAreaStreet> – улица на доп. территории; <street> – улица.
8.	/orgs/{orgOid}/vhls	Перечень транспортных средств	Перечень транспортных средств, которыми владеет данная организация
9.	/orgs/{orgOid}/vhls/{vhl-id}	Транспортное средство организации	<name> - имя автомобиля (например, марка или другое пользовательское описание); <numberPlate> - государственный регистрационный знак; <regCertificate> – данные свидетельства о государственной регистрации, включает в себя атрибуты: – <series> - серия свидетельства; – <number> - номер свидетельства.

Пример ответа с основными данными об организации (разрывы строки даны для удобства чтения):


```
{
    "stateFacts": ["Identifiable"],
    "shortName": "Банк",
    "fullName": "Банк",
    "type": "LEGAL",
    "ogrn": "1027700367507",
    "inn": "7728168971",
    "leg": "12247",
    "kpp": null
}
```


Пример ответа с контактными данными об адресах организации при использовании возможностей встраивания[24] (разрывы строки даны для удобства чтения):


```
{
```


[24] Запрос ресурса: /orgs/100000/addrs?embed=(elements)

```
"stateFacts": ["hasSize"],
"elements": [
{
"stateFacts": ["Identifiable"],
"id": 62,
"type": "OLG",
"region": "Москва Город",
"addressStr": "Москва Город, Ангарская улица",
"countryId": "RUS",
"zipCode": "125635",
"street": "Ангарская улица",
"house": "10",
"flat": "96"
}
],
"size": 1
}
```


Б.5 Предоставление списка участников организации.

Для получения данных об участниках организации система-клиент должна направить по в https-адрес REST-API системы ЕСИА[25] запрос методом GET. В запросе должен быть указан ресурс, содержащий необходимые данные. Идентификатор этого ресурса в ЕСИА имеет следующий вид для получения списка сотрудников организации необходимо использовать uri /orgs/{orgOid}/emps/{prn_oid}, где:

- emps – перечень (коллекция) сотрудников организаций с данным {orgOid}; для определения orgOid соответствующей организации необходимо использовать атрибут orgOid, передающийся в утверждениях SAML;
- prn_oid – внутренний идентификатор физического лица в ЕСИА.

В запрос должен быть добавлен header с маркером доступа, позволяющим получить доступ к данному ресурсу (*scope* http://esia.gosuslugi.ru/org_inf с параметрами).

Пример запроса (вызов сервиса в среде разработки):

```
GET /rs/orgs/1000000000/emps HTTP/1.1\r\n
Authorization: Bearer 75b2c7cbb8da403491c224c9e431cef9\r\n
Host: esia-portal1.test.gosuslugi.ru\r\n
Accept: */*\r\n
\r\n
```

Данные, которые ЕСИА возвращает в ответ на запрос, представлены в таблице 8.

Таблица 8 –Параметры ответа на запрос об участниках организации

№	URI запрашиваемого ресурса	Описание ресурса	Предоставляемые данные
1.	/orgs/{orgOid}/emps	Перечень сотрудников организации	Перечень сотрудников данной организации (в виде ссылок на ресурс с указанием {prn_oid}, содержащий данные о каждом сотруднике)
2.	/orgs/{orgOid}/em	Данные о	Данные о сотруднике:

[25] Сервис доступен по URL https://esia-portal1.test.gosulsugi.ru/rs/orgs

№	URI запрашиваемого ресурса	Описание ресурса	Предоставляемые данные
	ps/{prn_oid}	сотруднике организации с идентификатором {prn_oid}	<position> – должность; <chief> – сведения о том, является ли сотрудник руководителем организации (в этом случае имеет значение “true”) или нет (“false”); <orgOid> – идентификатор организации, сотрудником которой является пользователь; <brhOid> – идентификатор филиала организации, сотрудником которой является пользователь (если сотрудник присоединен к филиалу); <blocked> – признак блокировки сотрудника (имеет значение “true” или “false”).

Для просмотра перечня сотрудников филиала организации необходимо указать в запросе параметр brhOid и значение идентификатора соответствующего филиала. Пример ссылки, по которой будет возвращен перечень сотрудников филиала с идентификатором 1004082214:

```
https://esia-portal1.test.gosuslugi.ru/rs/orgs/1000000001/emps?brhOid=1004082214
```

При отображении всех коллекций (orgs, emps) используется механизм paging.

Пример ответа на запрос сведений о перечне сотрудников организации с идентификатором 1000000000 (фрагмент, разрывы строк даны для удобства чтения):

```
{
"stateFacts": ["hasSize"],
"elements":[
    "https://esia-portal1.test.gosuslugi.ru/rs/orgs/1000000000/emps/222896320",
    "https://esia-portal1.test.gosuslugi.ru/rs/orgs/1000000000/emps/240612402",
    "https://esia-portal1.test.gosuslugi.ru/rs/orgs/1000000000/emps/243280304",
    "https://esia-portal1.test.gosuslugi.ru/rs/orgs/1000000000/emps/243280305",
    "https://esia-portal1.test.gosuslugi.ru/rs/orgs/1000000000/emps/243280312",
    "https://esia-portal1.test.gosuslugi.ru/rs/orgs/1000000000/emps/1000000008",
    "https://esia-portal1.test.gosuslugi.ru/rs/orgs/1000000000/emps/1000000009",
    "https://esia-portal1.test.gosuslugi.ru/rs/orgs/1000000000/emps/1000000385"
    ],
"size":"8"
}
```

Пример ответа с контактными данными о сотрудниках организации при использовании возможности встраивания[26] (разрывы строки даны для удобства чтения):

```
{

    "stateFacts": ["Paginated", "FirstPage", "LastPage"],
    "elements": [
        {
            "stateFacts": ["Identifiable"],
            "prnOid": 1000000125,
            "orgOid": 100000,
            "chief": false,
            "corporateContact": "mail@example.com",
            "person": {
```

[26] Запрос ресурса: /orgs/100000/emps?embed=(elements.person)

```
                "stateFacts": ["Identifiable"],
                "firstName": "Петр",
                "lastName": "Петров",
                "middleName": "Петрович",
                "gender": "M",
                "updatedOn": 1387519441
            }
        },
        {
            "stateFacts": ["Identifiable"],
            "prnOid": 1000004892,
            "orgOid": 100000,
            "position": "Руководитель",
            "chief": true,
            "person": {
                "stateFacts": ["Identifiable"],
                "firstName": "Иван",
                "lastName": "Иванов",
                "middleName": "Иванович",
                "gender": "M",
                "updatedOn": 1387466948
            }
        }
    ],
    "pageSize": 100,
    "pageIndex": 1
}
```


Б.6 Предоставление сведений о вхождении пользователя в группы

Для получения данных о вхождении пользователя в группы организации система-клиент должна направить по в https-адрес REST-API системы ЕСИА[27] запрос методом GET. В запросе должен быть указан ресурс, содержащий необходимые данные.

В запрос должен быть добавлен header с маркером доступа, позволяющим получить доступ к данному ресурсу – *scope* http://esia.gosuslugi.ru/org_inf с параметрами. Для доступа к полному перечню групп, владельцем которых является данная организация, необходим *scope* http://esia.gosuslugi.ru/org_ful. Если система имеет маркер доступа на просмотр данных пользователя (http://esia.gosuslugi.ru/usr_inf), то этот *scope* также позволяет:

- посмотреть краткую информацию о каждой организации, членом которой является сотрудник;
- посмотреть список сотрудников, являющихся руководителями данной организации;
- посмотреть краткую информацию о выбранном руководителе организации;
- посмотреть краткую информацию о руководителе организации как физическом лице (т.е. получить данные по ссылке /prns/{oid}, где oid - идентификатор руководителя организации).

Пример запроса (вызов сервиса в среде разработки):

```
GET /rs/orgs/1000000000/grps HTTP/1.1\r\n
Authorization: Bearer 75b2c7cbb8da403491c224c9e431cef9\r\n
Host: esia-portal1.test.gosuslugi.ru\r\n
```

[27] Сервис доступен по URL https://esia-portal1.test.gosulsugi.ru/rs/orgs

```
Accept: */*\r\n
\r\n
```

Данные, которые ЕСИА возвращает в ответ на запрос, представлены в таблице Таблица 9.

Таблица 9 –Параметры ответа на запрос о вхождении сотрудников организации в группы

№	URI запрашиваемого ресурса	Описание ресурса	Предоставляемые данные
1.	/orgs/{orgOid}/grps	Перечень групп организации	Перечень групп, владельцем которых является данная организация (в виде перечня строк grp_id – указывающих на мнемонику имеющихся в рамках данной организации групп). Для получения этого перечня групп запрос должен быть добавлен header с маркером доступа на scope http://esia.gosuslugi.ru/org_ful
2.	/orgs/{orgOid}/grps/{grp_id}	Данные о группе организации с мнемоникой {grp-id}	Данные о группе: <name> – имя; <description> – описание; <system> – сведения о том, является ли группа системной (в этом случае имеет значение “true”) или нет (“false”). Также при запросе данных о конкретной группе возвращаются ссылки (links) на информационные системы, к которым относятся данные группы.
3.	/orgs/{orgOid}/emps/{prn_oid}/grps	Перечень групп, членом которых является данный сотрудник	Перечень групп, членом которых является сотрудник с данным {prn_oid} (в виде перечня строк grp_id – указывающих на мнемонику имеющихся в рамках данной организации групп).

При запросе перечня групп, членом которых является данный сотрудник, отображается перечень ссылок в следующем формате:

/orgs/{orgOid}/emps/{prn_oid}/grps/{grp_id}/{it_sys_id}, где it_sys_id – мнемоника информационной системы, в рамках которой действует данная группа. Пример ссылки на группу:

```
http://esia-
portal1.test.gosuslugi.ru/rs/orgs/1000000224/emps/1000000105/grps/ORG_ADMIN/ESIA
```

Данная ссылка означает, что пользователь с идентификатором 1000000105 как сотрудник организации 1000000224 включен в группу администраторов профиля организации (ORG_ADMIN) системы ЕСИА (мномоника ESIA). Выполнив запрос по данной ссылке можно получить краткую информацию о группе, которая включает в себя.

- мнемонику группы (grp_id);

- название группы (name);
- описание группы (description);
- признак того, что группа является системной (system);
- мнемоника системы-владельца группы (itSystem).

Например:

```
{
    "stateFacts": [
        "Identifiable"
    ],
    "grp_id": "ORG_ADMIN",
    "name": "Администраторы профиля организации",
    "description": "Сотрудники организации, имеющие право приглашать сотрудников, а также
включать сотрудников в группы доступа",
    "system": "true",
    "itSystem": "ESIA"
}
```

Если группа не является системной и не привязана ни к какой системе, то ссылка на нее имеет следующй формат:

/orgs/{orgOid}/emps/{prn_oid}/grps/{grp_id}/{it_sys_id}

В кратких данных об этой группе атрибут “system” будет иметь значение “false”.

При запросе перечня групп, членом которых является данный сотрудник, имеется возможность получить только те группы, которые относятся к определенной информационной системе. Для этого необходимо добавить условие на отбор групп выбранной системы (itSystemName), равное мнемонике данной системы. Пример запроса на получение групп системы ЕСИА (ESIA), в которые включен сотрудник:

```
GET /rs/orgs/1000000224/emps/1000000105/grps?itSystemName=ESIA HTTP/1.1\r\n
Authorization: Bearer 75b2c7cbb8da403491c224c9e431cef9\r\n
Host: esia-portal1.test.gosuslugi.ru\r\n
Accept: */*\r\n
\r\n
```

Б.7 Предоставление сведений о субъекте

Для получения данных субъекте система-клиент должна направить в https-адрес REST-API системы ЕСИА[28] запрос методом GET. В настоящее время используется исключительно для получения данных об информационных системах. Если уникальный идентификатор ИС в ЕСИА (oid) неизвестен, то возможна идентификация системы по сертификату. В этом случае запрос должен содержать следующие сведения:

- <fingerPrint> – криптографическое хэш-значение сертификата, идентифицирующего субъекта. <fingerPrint> должен быть указан в следующем формате:

[28] Сервис доступен по URL: https://esia-portal1.test.gosulsugi.ru/rs/sbjs

{<alg>}<value>

В качестве <alg> указывается идентификатор алгоритма, использованного для вычисления криптографического хэш. В качестве <value> указывается рассчитанный fingerPrint от всего сертификата по указанному алгоритму и закодированный в Base64 URL safe. Сертификат для расчета криптографического хэш должен быть в binary-формате (DER-формат).

Система ЕСИА поддерживает следующие алгоритмы вычисления криптографического хэш-значения (fingerPrint сертификата):

- SHA-1 (<alg> должен быть SHA1);
- ГОСТ Р 34.11-94 (<alg> должен быть GOST341194).

Ниже приведен пример заполнения <fingerPrint>:

```
{SHA1} at+xg6SiyUovktq1redipHiJpaE=
```

В запрос должен быть добавлен header с маркером доступа, позволяющим получить доступ к данному ресурсу (scope *http://esia.gosuslugi.ru/sbj_inf*).

Пример запроса (вызов сервиса в среде разработки):

```
GET /rs/sbjs?fingerPrint={SHA1}A87E9B9DCD58D1C99389D06A359EA
HTTP/1.1\r\n
Authorization: Bearer 75b2c7cb-d9db-4034-89c2-24c9e431cef9\r\n
Host: esia-portal1.test.gosulsugi.ru\r\n
Accept: */*\r\n
\r\n
```

В ответ на запрос сервис ЕСИА возвращает ссылку на ресурс с данными о соответствующем субъекте:

```
/rs/sbjs/{oid}
```

В данном случае <oid> – это внутренний идентификатор субъекта в ЕСИА;

Для получения данных о субъекте по имеющемуся идентификатору ЕСИА следует использовать запрос с указанием этого идентификатора, например:

```
GET /rs/sbjs/1000023446
HTTP/1.1\r\n
Authorization: Bearer 75b2c7cb-d9db-4034-89c2-24c9e431cef9\r\n
Host: esia-portal1.test.gosulsugi.ru\r\n
Accept: */*\r\n
\r\n
```

Ответ содержит следующие данные о субъекте:

- <oid> – внутренний идентификатор субъекта в ЕСИА
- <name> — имя субъекта в ЕСИА, для информационных систем имя соответствует мнемонике ИС;
- <typ> — тип субъекта, для информационных систем соответствует “S”.

Пример ответа на запрос:

```
{
    "stateFacts": [
        "Identifiable"
    ],
    "oid": 1000023446,
    "name": "PSEUDO_SYSTEM",
```

```
    "type": "S"
}
```

Если данный субъект – информационная система (S), то в заголовке (header) данного ответа также передается ссылка на организацию-владельца данной системы. Для получения данных об организации следует запрашивать следующий ресурс:

```
/orgs/{orgOid}
```

Получение данных этого ресурса осуществляется так, как это описано в Приложении Б.4. Scope *http://esia.gosuslugi.ru/sbj_inf* позволяет получить краткие данные об организации.

При получении данных о субъекте можно использовать режим встраивания, что позволяет в ответе сразу получить и данные о субъекте, и данные об организации-владельце (для ИС). В этом случае в запросе, помимо <fingerPrint>, указывается режим встраивания, например, embed=(elements.organization). Пример запроса:

```
GET /rs/sbjs?fingerPrint={SHA1}A87EGBJHHBBHBBHB9B9DCD58D1C99389D06A359EA&embed=(elements.or
ganization)
HTTP/1.1\r\n
Authorization: Bearer 75b2c7cb-d9db-4034-89c2-24c9e431cef9\r\n
Host: esia-portal1.test.gosulsugi.ru\r\n
Accept: */*\r\n
\r\n
```

Пример ответа на запрос в режиме встраивания (фрагмент, разрывы строк даны для удобства чтения):

```
{
    "stateFacts": [
        "ReadOnly",
        "hasSize",
        "EntityRoot"
    ],
    "size": 1,
    "elements": [
        {
            "stateFacts": ["Identifiable"],
            "oid": 1000000279,
            "name": "TEST SYSTEM",
            "type": "S",
            "organization": {
                "stateFacts": ["Identifiable"],
                "oid": 1000000001,
                "shortName": "Минкомсвязь России",
                "fullName": "Министерство связи и массовых коммуникаций Российской
Федерации",
                "type": "AGENCY",
                "ogrn": "1047702026701",
                "inn": "7710474375",
                "kpp": "771001001"
            }
        }
    ]
}
```

ПРИЛОЖЕНИЕ В. СЕРВИСЫ ЕСИА, ОСНОВАННЫЕ НА ПРОТОКОЛЕ OAUTH2.0 И OPENID CONNECT 1.0

В.1 Общие сведения

OAuth 2.0 определяет протокол взаимодействия следующих сторон:

- владелец ресурса (resource owner) – сущность, которая может предоставить доступ к защищаемому ресурсу (например, конечный пользователь);
- система-клиент (client) – приложение, которое запрашивает доступ к защищаемому ресурсу от имени владельца ресурса;
- сервис авторизации (authorization server) – сервис, который выпускает для клиента маркеры доступа с разрешения владельца ресурса;
- поставщик ресурса (resource server) – сервис, на котором размещены защищаемые ресурсы, и который может принимать запросы на доступ к защищаемым ресурсам и отвечать на эти запросы.

Модель контроля доступа, реализуемая сервисом авторизации ЕСИА, основана на использовании *маркера доступа* (security access token). Этот маркер несет информацию о подмножестве полномочий системы-клиента, о самой системе-клиенте, а также ряд служебных параметров. С точки зрения системы-клиента маркер доступа представляет собой набор символов. Системе-клиенту для получения доступа к защищенным ресурсам (т.е. делать успешные вызовы программного интерфейса), как правило, не требуется расшифровывать маркер доступа, достаточно лишь получать по определенным правилам и корректно использовать. В то же время в ЕСИА предусмотрены и «подписанные» маркеры доступа, которые можно проверить без обращения к ЕСИА.

В ЕСИА используются два способа получения маркера доступа:

1. Система-клиент получает маркер доступа в результате делегированного принятия решения сервисом авторизации на основании согласия владельца ресурса. В этом случае сервис авторизации выдает маркер доступа, если явными образом получает разрешение со стороны владельца ресурса. Например, система-клиент обратилась к сервису авторизации за маркером, позволяющим получить контактные данные пользователя. В этом случае сервис авторизации запрашивает у пользователя, согласен ли он предоставить данные системе-клиенту, и при позитивном решении выдает маркер доступа.

2. Система-клиент получает маркер доступа в результате решения сервиса авторизации на основании наличия у системы-клиента соответствующих полномочий. В этом случае система-клиент не должна получать явного разрешения от владельца ресурса – это разрешение было дано заранее, на стадии регистрации системы-клиента в сервисе авторизации. Такая модель контроля доступа реализуется, например, при взаимодействии информационных систем, если одна система желает получить идентификационные сведения о другой системе, для чего ей необходимо получить соответствующий маркер доступа.

Аутентификация пользователя, реализуемая с помощью модели OAuth 2.0 и распишения OpenID Connect, основана на использовании маркера идентификации (ID token). Этот маркер несет информацию об идентификационных данных пользователя, а также ряд служебных параметров.

B.2 Модель контроля на основе делегированного принятия решения

B.2.1 Общие принципы

Данная модель контроля доступа используется в случаях, когда система-клиент при доступе к ресурсу должна получить разрешение на это действие со стороны владельца ресурса.

В общем виде схема взаимодействия выглядит следующим образом:

- система-клиент запрашивает у владельца ресурса разрешение на доступ к соответствующим ресурсам. Обычно этот запрос осуществляется не напрямую к владельцу ресурса, а опосредованно через сервис авторизации (который, в свою очередь, запрашивает разрешение у владельца ресурса), поскольку сам владелец ресурса не может выдать ни маркер доступа, ни авторизационный код;
- система-клиент получает разрешение на доступ (authorization grant) в виде авторизационного кода;
- система-клиент запрашивает маркер доступа, предъявив авторизационный код сервису авторизации;
- сервис авторизации аутентифицирует систему-клиента, проверяет авторизационный код и выдает маркер доступа и маркер обновления;
- система-клиент запрашивает у поставщика защищенный ресурс, предъявляя маркер доступа;

- поставщик ресурса проверяет маркер доступа, если он валиден, то разрешает доступ к защищенному ресурсу;
- система-клиент вновь запрашивает с помощью выданного ранее маркера доступ к защищенному ресурсу;
- поставщик ресурса проверяет маркер, обнаруживает, что срок его действия истек, возвращает сообщение об ошибке;
- система-клиент обращается к сервису авторизации за получением нового маркера доступа, предъявляя маркер обновления;
- сервис авторизации проверяет валидность маркера обновления и возвращает два новых маркера: доступа и обновления.

Схема взаимодействия представлена на рисунке 14.

После того, как система-клиент получила маркер доступа, она может неоднократно обращаться за получением соответствующего защищенного ресурса, пока не истечет срок действия этого маркера. Когда это произойдет, системе-клиенту потребуется получить новый маркер доступа.

Ключевая особенность этой модели в том, что сам владелец ресурса никогда не получает маркер доступа, его получает сама система-клиент в результате прямой связи с сервисом авторизации (server-side flow).

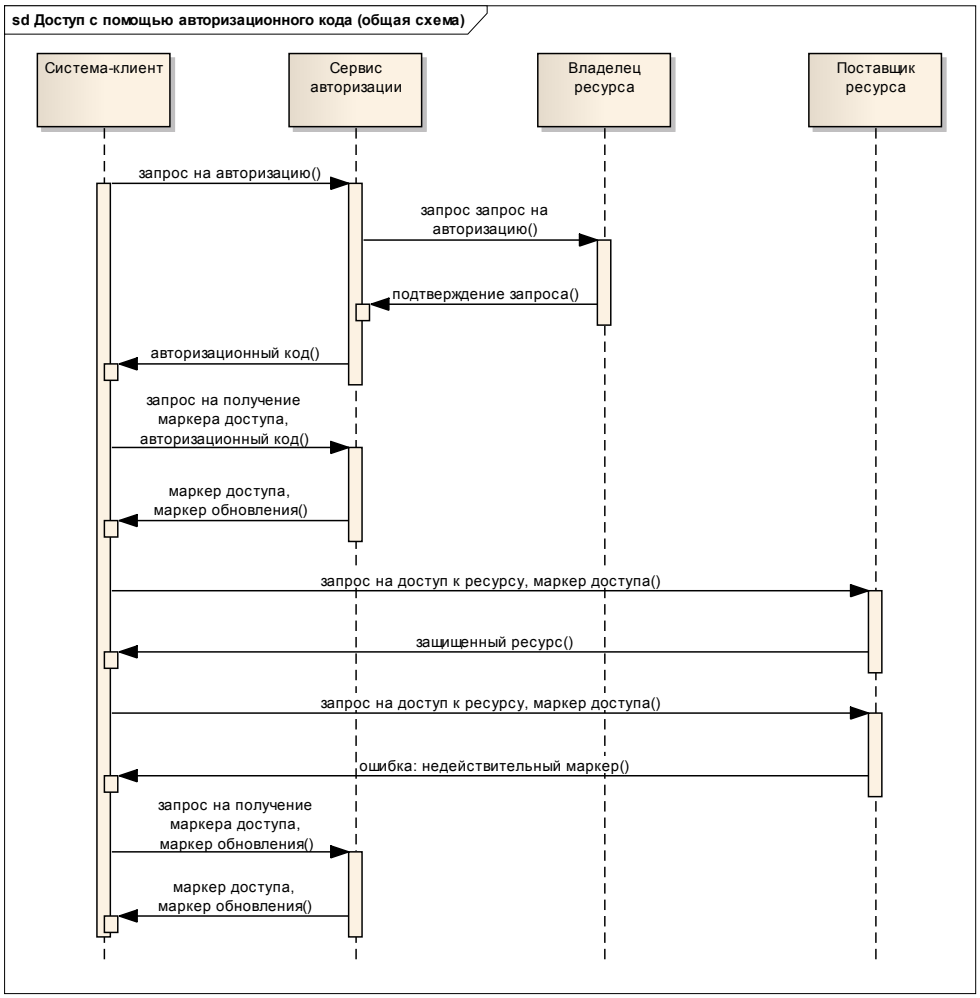

Рисунок 14 – Общая схема взаимодействия при получении маркера доступа с помощью авторизационного кода

Для оптимизации повторного получения маркера доступа используется механизм *маркера обновления* (refresh token): в этом случае первоначально в обмен на авторизационный код системе-клиенту выдается не только маркер доступа, но и маркер обновления. Когда маркер доступа перестает действовать, система-клиент обращается к сервису авторизации за получением нового маркера доступа, предъявляя маркер обновления. Сервис авторизации проверяет валидность маркера обновления (что он не был отозван и что срок его действия не истек) и выдает новый маркер доступа и маркер обновления.

Особенности маркера обновления:

- имеет более длительный (или бессрочный) срок действия, чем у маркера доступа;
- предъявляется исключительно при необходимости получить новый маркер доступа (таким образом, минимизируется риск перехвата);
- выдается сервисом авторизации одновременно с маркером доступа;
- может быть отозван владельцем ресурса.

Таким образом, наличие маркера обновления позволяет системе-клиенту получать новый маркер доступа даже тогда, когда пользователь (владелец ресурса) недоступен, при условии, что владелец ресурса явным образом не запретил доступ.

B.2.2 Получение авторизационного кода

Чтобы получить авторизационный код, система-клиент должна получить разрешение на доступ к защищенному ресурсу со стороны его владельца. В случае, когда владельцем является пользователь ЕСИА, система-клиент должна направить пользователя на страницу предоставления прав доступа в ЕСИА[29] (пользователь должен быть предварительно аутентифицирован в ЕСИА или система ЕСИА попросит его пройти идентификацию и аутентификацию).

Эта ссылка должна содержать следующие обязательные параметры:

- <client_id> – идентификатор системы-клиента (мнемоника системы в ЕСИА);
- <client_secret> – подпись запроса в формате PKCS#7 detached signature в кодировке UTF-8 от значений четырех параметров HTTP–запроса: scope, timestamp, clientId, state (без разделителей). <client_secret> должен быть закодирован в формате base64 url safe. Используемый для проверки подписи сертификат должен быть предварительно зарегистрирован в ЕСИА и привязан к учетной записи системы-клиента в ЕСИА. ЕСИА поддерживает сертификаты в формате X.509. ЕСИА поддерживает алгоритмы формирования электронной подписи RSA с длиной ключа 2048 и алгоритмом криптографического хэширования SHA-256, а также алгоритм электронной подписи ГОСТ Р 34.10-2001 и алгоритм криптографического хэширования ГОСТ Р 34.11-94.
- <redirect_uri> – ссылка, по которой должен быть направлен пользователь после того, как даст разрешение на доступ к ресурсу;
- <scope> – область доступа, т.е. запрашиваемые права; например, если система-клиент запрашивает доступ к сведениям о сотрудниках организации, то scope должна иметь значение http://esia.gosuslugi.ru/org_inf (с необходимыми параметрами); если запрашивается scope http://esia.gosuslugi.ru/usr_inf (данные о пользователе), то не нужно в качестве параметра указывать oid этого пользователя;
- <response_type> – это тип ответа, который ожидается от ЕСИА, имеет значение code, если система-клиент должна получить авторизационный код;

[29] Адрес в тестовой среде: https://esia-portal1.test.gosuslugi.ru/aas/oauth2/ac

– <state> – набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID;
– <timestamp> - время запроса авторизационного кода в формате yyyy.MM.dd HH:mm:ss Z (например, 2013.01.25 14:36:11 +0400), необходимое для фиксации начала временного промежутка, в течение которого будет валиден запрос с данным идентификатором (<state>);
– <access_type> – принимает значение “offline”, если требуется иметь доступ к ресурсам и тогда, когда владелец не может быть вызван (в этом случае выпускается маркер обновления); значение “online” – доступ требуется только при наличии владельца.

Если в ходе авторизации не возникло ошибок, то ЕСИА осуществляет редирект пользователя по ссылке, указанной в redirect_uri, а также возвращает два обязательных параметра:

– <code> – значение авторизационного кода;
– <state> – значение параметра *state*, который был получен в запросе на авторизацию; система-клиент должна провести сравнение отправленного и полученного параметра *state*.

В случае ошибки сервис авторизации вернет в параметре *error* код ошибки (например, “access_denied”) и не перенаправит пользователя по адресу, указанному в *redirect_uri*. Перечень возможных ошибок приведен в таблице 10.

Таблица 10 – Ошибки ошибок при получении маркеров доступа

№	Код параметра	Описание параметра
1.	invalid_request	ESIA-008003: В запросе отсутствует обязательный параметр, запрос включает в себя неверное значение параметра или включает параметр несколько раз.
2.	access_denied	ESIA-008004: Владелец ресурса или сервис авторизации отклонил запрос.
3.	unauthorized_client	ESIA-008005: Система-клиент не имеет права запрашивать получение маркера доступа таким методом.
4.	invalid_scope	ESIA-008006: Запрошенная область доступа (scope) указана неверно, неизвестно или сформирована некорректно.
5.	server_error	ESIA-008007: Возникла неожиданная ошибка в работе сервиса авторизации, которая привела к невозможности выполнить запрос.

№	Код параметра	Описание параметра
6.	temporarily_unavailable	ESIA-008008: Сервис авторизации в настоящее время не может выполнить запрос из-за большой нагрузки или технических работ на сервере.
7.	unsupported_response_type	ESIA-008009: Сервис авторизации не поддерживает получение маркера доступа этим методом.
8.	invalid_client	ESIA-008010: Не удалось произвести аутентификацию системы-клиента.
9.	invalid_grant	ESIA-008011: Авторизационный код или маркер обновления недействителен, просрочен, отозван или не соответствует адресу ресурса, указанному в запросе на авторизацию, или был выдан другой системе-клиенту.
10.	unsupported_grant_type	ESIA-008012: Тип авторизационного кода не поддерживается сервисом авторизации.
11.	invalid_scope	ESIA-008013: Запрос не содержит указания на область доступа (scope).
12.	invalid_request	ESIA-008014: Запрос не содержит обязательного параметра [].
13.	invalid_request	ESIA-008015: Неверное время запроса.

B.2.3 Получение маркера доступа в обмен на авторизационный код

Когда авторизационный код получен, система-клиент может сформировать запрос методом POST на https-адрес ЕСИА для получения маркера доступа[30]. Запрос должен содержать следующие сведения:

- <client_id> – идентификатор системы-клиента (мнемоника системы в ЕСИА);
- <code> – значение авторизационного кода, который был ранее получен от ЕСИА и который необходимо обменять на маркер доступа;
- <grant_type> – принимает значение “authorization_code”, если авторизационный код обменивается на маркер доступа;
- <client_secret> – подпись запроса в формате PKCS#7 detached signature в кодировке UTF-8 от значений четырех параметров HTTP–запроса: scope, timestamp, clientId, state (без

[30] Адрес в тестовой среде: https://esia-portal1.test.gosuslugi.ru/aas/oauth2/te

разделителей). <client_secret> должен быть закодирован в формате base64 url safe. Используемый для проверки подписи сертификат должен быть предварительно зарегистрирован в ЕСИА и привязан к учетной записи системы-клиента в ЕСИА. ЕСИА поддерживает сертификаты в формате X.509. ЕСИА поддерживает алгоритмы формирования электронной подписи RSA с длиной ключа 2048 и алгоритмом криптографического хэширования SHA-256, а также алгоритм электронной подписи ГОСТ Р 34.10-2001 и алгоритм криптографического хэширования ГОСТ Р 34.11-94.

- <state> – набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID; этот набор символов должен отличаться от того, который использовался при получении авторизационного кода;
- <redirect_uri> – ссылка, по которой должен быть направлен пользователь после того, как даст разрешение на доступ (то же самое значение, которое было указано в запросе на получение авторизационного кода);
- <scope> – область доступа, т.е. запрашиваемые права (то же самое значение, которое было указано в запросе на получение авторизационного кода);
- <timestamp> – время запроса маркера в формате yyyy.MM.dd HH:mm:ss Z (например, 2013.01.25 14:36:11 +0400), необходимое для фиксации начала временного промежутка, в течение которого будет валиден запрос с данным идентификатором (<state>);
- <token_type> – тип запрашиваемого маркера, в настоящее время ЕСИА поддерживает только значение “Bearer”.

Если запрос успешно прошел проверку, то ЕСИА возвращает ответ в формате JSON:

- <access_token> – маркер доступа для данного ресурса;
- <expires_in> – время, в течение которого истекает срок действия маркера (в секундах);
- <state> – набор случайных символов, имеющий вид 128-битного идентификатора запроса, генерируется по стандарту UUID (совпадает с идентификатором запроса);
- <token_type> – тип предоставленного маркера, в настоящее время ЕСИА поддерживает только значение “Bearer”;
- <refresh_token> – маркер обновления для данного ресурса.

Пример ответа:


```
{
“access_token” :
“eyJhbGciOiJSUzI1NiIsInNidCI6ImFjY2VzcyIsInR5cCI6IkpXVCIsInZlciI6MX0.eyJleHAiOjEzNTk1NDAxODcsInNjb3BlIjoiaHR0cDpcL1wvZXNpYS5nb3N1c2x1Z2kucnVcL2VtcF9pbmY b3JnX29pZD0xMDAwMDAwMzU3Iiwia XNzIjoiaHR0cDpcL1wvZXNpYS5nb3N1c2x1Z2kucnUiLCJuYmYiOjEzNTk1MzY1ODcsInVybjplc2lhOnNpZCI6IjE2
```

```
ZDdmOTNkLTZjZTgtNDE3OS04ZmFmLTdmZDQ2ZDMyMDhhNiIsInVybjplc2lhOnNial9pZCI6MTAwMDAwMDM4NSwiY2x
pZW50X2lkIjoiRVNJQSIsImlhdCI6MTM1OTUzNjU4N30”,
“expires in” : 3600,
“state” : “9be638a9-0e05-42e1-b4f8-a3e30457fbdd”,
“token_type” : “Bearer”,
“refresh_token” : “54039d1f-9917-43cd-961a-2729c891ef8c”
}
```


При невозможности выдачи маркера доступа возвращается код ошибки (Таблица 10).

B.2.4 Получение нового маркера доступа в обмен на маркер обновления

При использовании маркера доступа системам-клиентам рекомендуется сначала проверять, не истек ли срок его действия. Если маркер просрочен, то для успешного доступа к защищенному ресурсу потребуется предварительно получить новый маркер доступа с использованием маркера обновления. Для этого системе-клиенту следует сформировать запрос методом POST в адрес ЕСИА, имеющий структуру, аналогичную первичному запросу на получение маркера. Особенности значений параметров запроса:

- <refresh_token> – значение имеющегося у системы-клиента маркера обновления, который следует обменять на новый маркер доступа (указывается вместо <code>);
- <grant_type> – должно иметь значение “refresh_token”, поскольку маркер обновления обменивается на маркер доступа;

Ответ на этот дается в формате JSON и имеет ту же структуру, как и при первичном предоставлении маркера доступа. В этом ответе содержится новый маркер обновления, который система-клиент должна хранить вместо уже использованного маркера обновления.

B.3 Модель контроля доступа на основе полномочий системы-клиента

B.3.1 Общие принципы

Эта модель контроля предполагает, что система-клиент самостоятельно обращается к сервису авторизации и получает маркер доступа (client-side flow) на основании имеющихся (и зафиксированных в сервисе авторизации) полномочий системы-клиента. Данная модель контроля доступа предполагает, что система-клиент при доступе к защищенному ресурсу непосредственно получает разрешение (в форме маркера доступа) со стороны сервиса авторизации. В общем виде схема взаимодействия выглядит следующим образом:

- система-клиент обращается к сервису авторизации за выдачей маркера доступа, позволяющего получить доступ к защищенному ресурсу;
- сервис авторизации аутентифицирует систему-клиента и выдает маркер доступа;

– система-клиент запрашивает у поставщика защищенный ресурс, предъявляя маркер доступа;
– поставщик ресурса проверяет маркер доступа, если он валиден, то разрешает доступ к защищенному ресурсу.

Данная модель контроля доступа проиллюстрирована на рисунке 15.

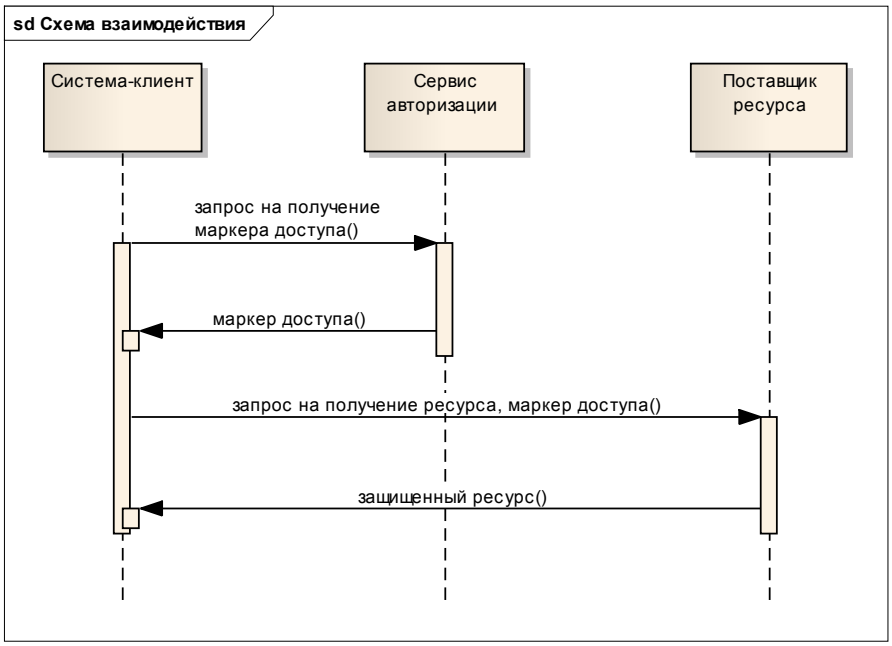

Рисунок 15 – Схема взаимодействия при реализации модели контроля доступа на основе полномочий системы-клиента

Поскольку получение маркера доступа при использовании данной модели контроля не предполагает обращения к владельцу ресурса, то маркер обновления не применяется. Система-клиент после истечения срока действия маркера доступа может обратиться к сервису авторизации и получить новый маркер доступа.

В.3.2 Получение маркера доступа

Для получения маркера доступа система-клиент должна направить по https-адресу сервиса авторизации (ЕСИА) запрос методом POST. Запрос должен содержать следующие сведения:

– <client_id> – идентификатор системы-клиента (мнемоника системы в ЕСИА);
– <response_type> – используемая модель контроля доступа; принимает значение “token”, если происходит безусловное наделения системы-клиента полномочиями;

- <scope> – область доступа, т.е. запрашиваемые права; например, если система-клиент запрашивает доступ к данным ИС, то scope должно иметь значение http://esia.gosuslugi.ru/sbj_inf;
- <state> – набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID; этот набор символов должен отличаться от того, который использовался при получении авторизационного кода.
- <timestamp> – время запроса маркера в формате yyyy.MM.dd HH:mm:ss Z (например, 2013.01.25 14:36:11 +0400), необходимое для фиксации начала временного промежутка, в течение которого будет валиден запрос с данным идентификатором (<state>);
- <token_type> – тип запрашиваемого маркера, в настоящее время ЕСИА поддерживает только значение “Bearer”;
- <client_secret> – подпись запроса в формате PKCS#7 detached signature в кодировке UTF-8 от значений четырех параметров HTTP–запроса: scope, timestamp, clientId, state (без разделителей). <client_secret> должен быть закодирован в формате base64 url safe. Используемый для формирования подписи сертификат должен быть зарегистрирован в ЕСИА и привязан к учетной записи системы-клиента в ЕСИА. ЕСИА поддерживает сертификаты в формате X.509. ЕСИА поддерживает алгоритмы формирования электронной подписи RSA с длиной ключа 2048 и алгоритмом криптографического хэширования SHA-256, а также алгоритм электронной подписи ГОСТ Р 34.10-2001 и алгоритм криптографического хэширования ГОСТ Р 34.11-94.

  Если запрос успешно прошел проверку, то ЕСИА возвращает ответ в формате JSON:
- <access_token> – маркер доступа для данного ресурса;
- <expires_in> – время, в течение которого истекает срок действия маркера (в секундах);
- <state> – набор случайных символов, имеющий вид 128-битного идентификатора запроса, генерируется по стандарту UUID (совпадает с идентификатором запроса);
- <token_type> – тип предоставленного маркера, в настоящее время ЕСИА поддерживает только значение “Bearer”;

  При невозможности выдачи маркера доступа возвращается код ошибки (Таблица 10).

B.4 Особенности указания области доступа (scope)

При запросе на получения маркера доступа система-клиент должна обязательно указывать соответствующий *scope*, т.е. область доступа (тип данных, к которым система-клиент намерена получить доступ).

В ЕСИА используются следующие типы *scope*:

1. Данные о субъекте (*http://esia.gosuslugi.ru/sbj_inf*). Этот *scope* не параметризуется, т.к. субъект, данные о котором намерена получить система-клиент, явным образом указан в запросе, а также содержится в самом маркере доступа.
2. Данные о пользователе. В системе предусмотрены следующие scope, позволяющие получить данные о пользователе (Таблица 11).

Таблица 11 – Предоставляемые ЕСИА наборы данных о пользователе

№	Название scope	Название набора данных	Состав набора данных
1.	http://esia.gosuslugi.ru/usr_brf	Просмотр контактных данных и идентифицирующей информации (ФИО, пол, email, моб. телефон)	− ФИО; − пол; − email (кроме корпоративного); − моб. телефон.
2.	http://esia.gosuslugi.ru/usr_inf	Просмотр всех данных вашей учетной записи ЕСИА	Полная информация из профиля.

Эти *scope* указываются в формате */scope?param1=value1&param2=value2*, где <param1> – название, а *value1* – значение параметра. Может использоваться параметр:

– <oid> – внутренний идентификатор пользователя в ЕСИА (обязательный параметр);

Пример *scope*:

scope="http://esia.gosuslugi.ru/usr_inf?oid=1111111"

Наличие маркера с таким *scope* позволяет получить полный доступ к данным о пользователе с данным уникальным номером (1111111).

Принять решение о предоставлении данных о пользователе (т.е. о выдаче соответствующего маркера) может исключительно сам пользователь.

3. Данные об организации. В системе предусмотрены следующие scope, позволяющие получить данные об организации (Таблица 12).

Таблица 12 – Предоставляемые ЕСИА наборы данных об организации

№	Название scope	Название набора данных	Состав набора данных
1.	http://esia.gosuslugi.ru/org_inf	Просмотр всех данных об организации «{Название}» и ее сотрудниках	Полная информация из профиля организации, а также информация о сотрудниках, т.е. доступ к ресурсам /orgs/{org_oid}/emps и /orgs/{org_oid}/grps. Кроме того, наличие данного позволяет получить краткую информацию о пользователях как физических лицах (/prns/{oid}).
2.	http://esia.gosuslugi.ru/org_ful	Полный доступ ко всем данным организации «{Название}» и ее сотрудников	В дополнение к данным, получаемым по org_inf, данный scope позволяет получить информацию о вхождении сотрудников организации во все группы

Эти *scope* указываются в формате */scope?param1=value1&param2=value2*, где <param1> – название, а *value1* – значение параметра. Должен использоваться параметр:

– <org_oid> – внутренний идентификатор организации в ЕСИА.

Пример *scope*:

scope="http://esia.gosuslugi.ru/org_inf?org_oid=1000000357"

Наличие маркера с таким *scope* позволяет получить полную информацию об организации с данным уникальным номером (название, тип, ОГРН) и ее сотрудниках. Принять решение о предоставлении данных об организации (т.е. о выдаче соответствующего маркера) может исключительно руководитель этой организации или

администратор профиля данной организации в ЕСИА.

4. Данные для идентификации и аутентификации пользователя (*openid*). Этот *scope* используется в целях проведения аутентификации пользователя и получения маркера идентификации (см. Приложение В.6 и В.7). Он не параметризуется, т.к. до аутентификации у системы-клиента отсутствует информация об идентификаторе пользователя.
5. Технологическая информация (*http://esia.gosuslugi.ru/tech_inf*), в том числе – о перечне удаленных пользователей. Для получения данных об удаленных пользователях этот scope должен иметь вид: http://esia.gosuslugi.ru/tech_inf?stu=DELETED. Получение маркера доступа на этот *scope* должно происходить посредством модели контроля доступа на основе полномочий системы-клиента (см. Приложение В.3).

В.5 Сведения о структуре и проверке маркера доступа

Используемый ЕСИА маркер состоит из трех частей:

1. Заголовок (header), в котором содержится общая информация о типе маркера, в том числе об использованных в ходе его формирования криптографических операциях.
2. Набор утверждений (payload / claim set) с содержательными сведениями о маркере.
3. Подпись (signature), которая удостоверяет, что маркер «выдан» ЕСИА и не был изменен при передаче.

Части маркера разделены точкой, так что он имеет вид:

```
HEADER.PAYLOAD.SIGNATURE
```

Маркер передается в виде строки в формате Base64url[31].

Каждая часть маркера содержит набор утверждений (claims) трех типов:

Заголовок (header) содержит описание свойств используемого маркера:

1. Алгоритм шифрования (“alg”, стандартное обозначение); в настоящее время в ЕСИА поддерживается алгоритм электронной подписи RSA SHA-256, рекомендуемый спецификацией (соответствует значению “RS256”)[32] и алгоритм электронной подписи ГОСТ Р 34.10-2001 (соответствует значению “GOST3410”);
2. Глобальный тип маркера (“typ”, стандартное обозначение), который в ЕСИА всегда имеет значение “JWT” (JSON Web Token);

[31] Подробнее см. в: http://tools.ietf.org/html/draft-ietf-jose-json-web-signature-02#appendix-B
[32] См.: http://tools.ietf.org/html/draft-jones-json-web-token-10#section-8

3. ЕСИА-специфический тип маркера и его версия (“sbt” и “ver” соответственно, приватное обозначение), что необходимо для использования в ЕСИА нескольких типов маркера; для маркера доступа – “access”.

   Например, заголовок маркера доступа в ЕСИА будет иметь следующий вид:

```
{"alg":"RS256","typ":"JWT","ver":0,"sbt":"access"}
```

Сообщение (payload) включает в себя содержательные утверждения о субъекте. В случае, если система проводит аутентификацию пользователя с использованием механизма SAML, системе нет необходимости разбираться в формате payload маркера доступа. Однако если система проводит аутентификацию пользователя с использованием REST, ей необходимо извлечь необходимую информацию из сообщения маркера (payload) и проверить подпись ЕСИА.

Сообщение включает в себя содержательные утверждения о маркере доступа и субъекте:

1. Данные о маркере доступа:

– время прекращения действия (“exp”) – в секундах с 1 января 1970 г. 00:00:00 GMT;
– время начала действия (“nbf”) – в секундах с 1 января 1970 г. 00:00:00 GMT, т.е. маркер нельзя обрабатывать до наступления указанного времени;
– время выдачи (“iat”) – в секундах с 1 января 1970 г. 00:00:00 GMT;
– организация, выпустившая маркер (“iss”), для маркеров ЕСИА всегда имеет определенное значение, которое совпадает с полем «субъект» используемого сертификата ЕСИА (http://субъект);
– адресат маркера (“client_id”) – утверждение, ограничивающее системы/приложения («аудитория»), которые могут использовать этот маркер. Для обозначения адресата в ЕСИА используется мнемоника данной ИС, зарегистрированной в ЕСИА. Соответственно, использовать маркер могут только системы с этой мнемоникой.
– идентификатор маркера (“urn:esia:sid”) – набор случайных символов, имеющий вид 128-битного идентификатора, сгенерированного по стандарту UUID.

2. Данные о субъекте:

– идентификатор субъекта (“urn:esia:sbj_id”), в качестве значения указывается oid, этот идентификатор уникален для каждого субъекта, зарегистрированного в ЕСИА;
– область доступа (“scope”), в качестве значения – название области, к которой предоставляется доступ (например, “http://esia.gosuslugi.ru/usr_inf”).

Пример сообщения (payload) маркера доступа в ЕСИА:

```
{"exp":1393858241,
"scope":"http:\/\/esia.gosuslugi.ru\/usr_inf?oid=1000023328",
"iss":"http:\/\/esia.gosuslugi.ru",
```

```
"nbf":1393854641,
"urn:esia:sid":"f9cbc3bf-8fa1-42c8-a838-6e02baae8328",
"urn:esia:sbj id":1000023328,
"client id":"TEST SYSTEM",
"iat":1393854641}
```

Подпись (signature) маркера осуществляется по том алгоритму, который указывается в параметре “alg” маркера. Подпись вычисляется от двух предыдущих частей маркера (HEADER.PAYLOAD).

Системе-клиенту, использующую механизмы REST и OAuth 2.0 для аутентификации пользователей, рекомендуется осуществлять проверку маркера доступа, используя данные о его подписи. В общем виде эта процедура включает в себя следующие шаги[33]:

1. Осуществление base64url-декодирования первых двух частей маркера. В header указан алгоритм шифрования (параметр alg).
2. Третья часть маркера доступа представляет собой подпись в формате PKCS#7 detached signature в кодировке UTF-8 от значений первых двух частей маркера доступа (HEADER.PAYLOAD). Необходимо осуществить проверку данной электронной подписи с использованием сертификата ключа проверки электронной подписи ЕСИА.
3. Проверка времени выдачи, начала и прекращения маркера.
4. Проверка организации, выпустившей маркер, а также адресата маркера.

B.6 Использование OpenID Connect 1.0 для аутентификации пользователя

B.6.1 Общие принципы

В общем виде схема аутентификация с использованием OpenID Connect 1.0 выглядит следующим образом:

- система-клиент готовит запрос на аутентификацию пользователя с необходимыми параметрами;
- система-клиент отправляет запрос на аутентификацию в адрес сервиса авторизации ЕСИА;
- сервис авторизации аутентифицирует пользователя;
- сервис авторизации получает согласие пользователя на проведение аутентификации в данной системе;

[33] Подробнее см.: http://tools.ietf.org/pdf/draft-jones-json-web-token-10.pdf, http://tools.ietf.org/pdf/draft-ietf-jose-json-web-signature-02.pdf, http://tools.ietf.org/pdf/draft-ietf-jose-json-web-encryption-02.pdf

- сервис авторизации перенаправляет пользователя обратно в систему-клиент и передает авторизационный код;
- система-клиент формирует запрос с использованием авторизационного кода на получения маркера идентификации;
- система-клиент получает ответ, содержащий необходимый маркер идентификации;
- система-клиент проводит валидацию маркера идентификации и извлекает из маркера идентификатор пользователя.

Далее более детально рассмотрены формируемые сисиемой-клиентом запросы и получаемые ей ответы от ЕСИА.

B.6.2 Получение авторизационного кода

Чтобы получить авторизационный код, система-клиент должна получить разрешение на проведение аутентификации пользователя[34]. Для этого система-клиент должна направить пользователя на страницу предоставления прав доступа в ЕСИА.

Эта ссылка должна содержать следующие обязательные параметры:

- <client_id> – идентификатор системы-клиента (мнемоника системы в ЕСИА);
- <client_secret> – подпись запроса в формате PKCS#7 detached signature в кодировке UTF-8 от значений следующих параметров HTTP–запроса: scope, timestamp, client_id, state (без разделителей). <client_secret> должен быть закодирован в формате base64 url safe. Используемый для проверки подписи сертификат должен быть предварительно зарегистрирован в ЕСИА и привязан к учетной записи системы-клиента в ЕСИА. ЕСИА поддерживает сертификаты в формате X.509. ЕСИА поддерживает алгоритмы формирования электронной подписи RSA с длиной ключа 2048 и алгоритмом криптографического хэширования SHA-256, а также алгоритм электронной подписи ГОСТ Р 34.10-2001 и алгоритм криптографического хэширования ГОСТ Р 34.11-94.
- <redirect_uri> – ссылка, по которой должен быть направлен пользователь после того, как даст разрешение на проведение аутентификации;
- <scope> – область доступа, т.е. запрашиваемые права; для проведения аутентификации пользователя *scope* должен иметь значение *openid*. Если системе потребуется получение

[34] Адрес в тестовой среде: https://esia-portal1.test.gosuslugi.ru/aas/oauth2/ac

дополнительных данных о пользователе (например, детальная информация о пользователе), то могут быть указаны дополнительные *scope* через пробел;

- <response_type> – это тип ответа, который ожидается от ЕСИА, имеет значение code, поскольку система-клиент должна получить авторизационный код;
- <state> – набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID;
- <timestamp> - время запроса авторизационного кода в формате yyyy.MM.dd HH:mm:ss Z (например, 2013.01.25 14:36:11 +0400), необходимое для фиксации начала временного промежутка, в течение которого будет валиден запрос с данным идентификатором (<state>);
- <state> – набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от повторных запросов), генерируется по стандарту UUID.

Если в ходе аутентификации не возникло ошибок, то ЕСИА осуществляет редирект пользователя по ссылке, указанной в redirect_uri, а также возвращает два обязательных параметра:

- <code> – значение авторизационного кода;
- <state> – значение параметра *state*, который был получен в запросе на аутентификацию; система-клиент должна провести сравнение отправленного и полученного параметра *state*.

B.6.3 Получение маркера идентификации в обмен на авторизационный код

Когда авторизационный код получен, система-клиент может сформировать запрос методом POST в адрес ЕСИА для получения маркера идентификации[35]. Запрос должен содержать следующие сведения:

- <client_id> – идентификатор системы-клиента (мнемоника системы в ЕСИА);
- <code> – значение авторизационного кода, который был ранее получен от ЕСИА и который необходимо обменять на маркер идентификации;
- <grant_type> – принимает значение “authorization_code”, если авторизационный код обменивается на маркер идентификации;

[35] Адрес в тестовой среде: https://esia-portal1.test.gosuslugi.ru/aas/oauth2/te

– <client_secret> – подпись запроса в формате PKCS#7 detached signature в кодировке UTF-8 от значений четырех параметров HTTP–запроса: scope, timestamp, clientId, state (без разделителей). <client_secret> должен быть закодирован в формате base64 url safe. Используемый для проверки подписи сертификат должен быть предварительно зарегистрирован в ЕСИА и привязан к учетной записи системы-клиента в ЕСИА. ЕСИА поддерживает сертификаты в формате X.509. ЕСИА поддерживает алгоритмы формирования электронной подписи RSA с длиной ключа 2048 и алгоритмом криптографического хэширования SHA-256, а также алгоритм электронной подписи ГОСТ Р 34.10-2001 и алгоритм криптографического хэширования ГОСТ Р 34.11-94.
– <state> – набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID; этот набор символов должен отличаться от того, который использовался при получении авторизационного кода;
– <redirect_uri> – ссылка, по которой должен быть направлен пользователь после аутентификации (то же самое значение, которое было указано в запросе на получение авторизационного кода);
– <scope> – область доступа, т.е. запрашиваемые права (то же самое значение, которое было указано в запросе на получение авторизационного кода);
– <timestamp> – время запроса маркера в формате yyyy.MM.dd HH:mm:ss Z (например, 2013.01.25 14:36:11 +0400), необходимое для фиксации начала временного промежутка, в течение которого будет валиден запрос с данным идентификатором (<state>);
– <token_type> – тип запрашиваемого маркера, в настоящее время ЕСИА поддерживает только значение “Bearer”.

Если запрос успешно прошел проверку, то ЕСИА возвращает ответ в формате JSON:
– <id_token> – маркер идентификации;
– <access_token> – маркер доступа для данного ресурса (если он запрашивался);
– <expires_in> – время, в течение которого истекает срок действия маркера (в секундах);
– <state> – набор случайных символов, имеющий вид 128-битного идентификатора запроса, генерируется по стандарту UUID (совпадает с идентификатором запроса);
– <token_type> – тип предоставленного маркера, в настоящее время ЕСИА поддерживает только значение “Bearer”.

Пример ответа:

```
{
“id token”:
“eyJhbGciOiJSUzI1NiIsImtpZCI6IjFlOWdkazcifQ.ewogImlzcyI6ICJodHRwOi8vc2VydmVyLmV4YW1wbGUuY29
tIiwKICJzdWIiOiAiMjQ4Mjg5zYxMDAxIiwKICJhdWQiOiAiczZCaGRSa3F0MyIsCiAibm9uY2UiOiAibi0wUzZfV3p
BMk1qIiwKICJleHAiOiAxMzExMjgxOTcwLAogImlhdCI6IDEzMTEyODA5NzfQ.ggW8hZ1EuVLuxNuuIJKX_V8a_OMXz
R0EHR9R6jgdqrOOF4daGU96Sr_P6qp6IcmD3HP99Obi1PRs-cwh3LO-
p146waJ8IhehcwL7F09JdijmBqkvPeB2T9CJNqeGpe-
gccMg4vfKjkM8FcGvnzZUN4 KSP0aAp1tOJ1zZwgjxqGByKHiOtX7TpdQyHE5lcMiKPXfEIQILVq0pc E2DzL7emopW
oaoZTF m0 N0YzFC6g6EJbOEoRoSK5hoDalrcvRYLSrQAZZKflyuVCyixEoV9GfNQC3 osjzw2PAithfubEEBLuVVk4
XUVrWOLrLl0nx7RkKU8NXNHq-rvKMzqg”,
“expires_in” : 3600,
“state” : “9be638a9-0e05-42e1-b4f8-a3e30457fbdd”,
“token type” : “Bearer”,
}
```


При невозможности выдачи маркера доступа возвращается код ошибки.

B.6.4 Проверка маркера идентификации

После получения маркера идентификации система-клиент должна произвести валидацию маркера идентификации, которая включает в себя следующие проверки:

1. Проверка идентификатора (мнемоники) ЕСИА, содержащейся в маркере идентификации.
2. Проверка идентификатора (мнемоники) системы-клиента, т.е. именно система-клиент должна быть указана в качестве адресата маркера идентификации.
3. Проверка подписи маркера идентификации (с использованием указанного в маркере алгоритма).
4. Текущее время должно быть не позднее, чем время прекращения срока действия маркера идентификации.

После валидации маркера идентификации система-клиент считает пользователя аутентифицированным. Для получения дополнительных данных о пользователе следует использовать идентификатор пользователя, извлеченный из маркера идентификации, и соответствующие программные интерфейсы ЕСИА (требующие, в свою очередь, маркера доступа).

Детальные сведения о маркере идентификации представлены в Приложении В.7.

B.6.5 Выход из системы (логаут)

Для осуществления выхода из системы пользователь должен быть перенаправлен по специальной ссылке с соблюдением следующих требований:

- протокол запроса должен быть https;
- путь в HTTP-запросе должен быть равен /idp/ext/Logout;
- запрос должен иметь параметр (query param) с именем client_id, содержащий мнемонику обращающейся системы, зарегистрированной в ЕСИА;

– запрос может иметь параметр (query param) с именем redirect_url, содержащий адрес, на который пользователь будет перенаправлен после успешного логаута.

Пример запроса:

```
https://esia.gosuslugi.ru/idp/ext/Logout?client_id=ESIA&redirect_url=https://esia.gosuslugi
.ru/registration/
```

В ЕСИА для интегрированной системы может быть определен параметр system.siteUrl, содержащий URL-адрес системы, на который будет возвращен пользователь после логаута. Redirect_url должен быть подстрокой system.siteUrl.

При обработке запроса производятся следующие проверки:

1. Проверка, что передан обязательный параметр client_id. Если он не передан, то возвращается HTTP-код «400 Bad Request».
2. Проверка, что система с мнемоникой, указанной в параметре client_id, зарегистрирована в ЕСИА. Если система не зарегистрирована, то возвращается HTTP-код «403 Forbidden».

После успешного выполнения этих проверок ЕСИА определяет URL переадресации после успешного логаута:

– Если для системы в настройках ЕСИА не задан параметр system.siteUrl, то запрос после логаута будет направлен на сайт ЕСИА.
– Если в запросе не задан параметр redirect_url, то запрос после логаута будет направлен по адресу, заданному в system.siteUrl.
– Если параметры redirect_url и system.siteUrl не соответствуют друг другу (redirect_url должен быть подстрокой system.siteUrl), то запрос после логаута будет направлен на сайт ЕСИА.

B.7 Сведения о структуре маркера идентификации

Структура маркера идентификации аналогична структуре маркера доступа (см. Приложение B.5) и состоит из тех же трех частей: заголовок, набор утверждений и подпись.

Особенность заголовка маркера идентификации состоит в том, что него значение атрибута “sbt” равно “id”.

Пример заголовка маркера идентификации в ЕСИА:

```
{"alg":"RS256","sbt":"id","typ":"JWT","ver":0}
```

Сообщение, включающее в себя содержательные утверждения о маркере идентификации и пользователе, включает следующие атрибуты:

1) время прекращения действия (“exp”), указывается в секундах с 1 января 1970 г. 00:00:00 GMT;
2) время выдачи (“iat”), указывается в секундах с 1 января 1970 г. 00:00:00 GMT;;
3) организация, выпустившая маркер (“iss”), указывается URL ЕСИА;
4) адресат маркера (“aud”), указывается client_id системы, направившей запрос на аутентификацию;
5) идентификатор маркера (“nonce”), передается в неизменном виде из соответствующего запроса на проведение аутентификации;
6) идентификатор субъекта (“sub”), в качестве значения указывается oid. Этот идентификатор уникален для каждого субъекта, зарегистрированного в ЕСИА, и остается неизменным при последующих аутентификациях.
7) время аутентификации (“auth_time”) – время, когда произошла аутентификация пользователя, указывается в секундах с 1 января 1970 г. 00:00:00 GMT;
8) метод аутентификации (“amr”, приватное обозначение), может принимать два значения: “DS” (электронная подпись) или “PWD” (пароль);

Пример сообщения маркера идентификации в ЕСИА:


```
{
"exp":1394034968,
"aud":"TEST SYSTEM",
"iss":"http:\/\/esia.gosuslugi.ru",
"nbf":1394033168,
"nonce":"5111e23b98e8f18b3b2110aca5f5a5c3959f818bc47f30f69fcee99f5145977a",
"sub":1000004892,
"amr":"PWD",
"auth time":1394032133,
"iat":1394033168
}
```


Подпись (signature) маркера осуществляется по алгоритму, который указывается в параметре “alg” маркера. Подпись вычисляется от двух предыдущих частей маркера (HEADER.PAYLOAD).

ПРИЛОЖЕНИЕ Г. СЕРВИС РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЯ И ПОДТВЕРЖДЕНИЯ ЛИЧНОСТИ

В целях регистрации пользователей в ЕСИА, а также подтверждения личности пользователей, создан и опубликован в СМЭВ электронный сервис «Сервис регистрации пользователей Единой системы идентификации и аутентификации»[36]. Сервис предназначен для использования Операторами выдачи ключа ПЭП – организациями, которые в соответствии с постановлением Правительства РФ от 25 января 2013 г. № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг» обладают правом создания (замены) и выдачи ключа простых электронных подписей и усиленных квалифицированных электронных подписей в целях оказания государственных и муниципальных услуг[37].

Данный сервис ЕСИА поддерживает следующие функции:

- инициирование регистрации новой подтверждённой учётной записи пользователя в ЕСИА с выдачей идентификатора заявки на регистрацию пользователя, а также пароля пользователя для первого входа в систему;
- подтверждение учетной записи (подтверждения личности) пользователя ЕСИА;
- инициирование процедуры восстановления доступа к подтверждённой учётной записи пользователя в ЕСИА с выдачей идентификатора заявки на восстановление доступа, а также пароля пользователя для входа в систему;
- проверка статуса выполняемой операции (по регистрации пользователя / восстановлению доступа)[38].

Г.1 Получение доступа к электронному сервису

Каждый орган/организация для использования программного интерфейса ЕСИА по регистрации пользователей должен:

[36] SID данного сервиса в тестовой среде СМЭВ – SID0003419, в продуктивной – SID0003923.

[37] Порядок создания записи регистра органов и организаций, имеющих право создания (замены) и выдачи ключа простой электронной подписи (Операторов выдачи ключа ПЭП), определен в п. 12 Реглмента.

[38] Детальная информация о работе сервиса и получении к нему доступа содержится в Руководстве пользователя электронного сервиса СМЭВ «Сервис регистрации пользователей Единой системы идентификации и аутентификации».

1. Подать заявку на создание записи регистра органов и организаций, имеющих право создания (замены) и выдачи ключа простой электронной подписи согласно п. 12 Регламента.
2. Доработать (разработать) свою ИС, в которой будет предусмотрена функция регистрации пользователей ЕСИА.
3. Сгенерировать для ИС криптографические ключи и выпустить на них квалифицированный сертификат ЭП:
    - Сертификат должен быть выпущен на юридическое лицо (содержит ОГРН и имя организации).
    - Сертификат должен быть выпущен аккредитованным УЦ.
    - Требования к ключевому контейнеру определяются эксплуатационной документацией на ИС, которая будет использовать ключи.
4. Зарегистрировать ИС в СМЭВ (согласно регламенту СМЭВ подается заявка на регистрацию ИС).
5. Получить для ИС в СМЭВ права на доступ к сервису ЕСИА в СМЭВ.
6. Зарегистрировать ИС в ЕСИА согласно п. 6 Регламента.
7. Зарегистрировать подключение ИС в тестовом контуре ЕСИА для отработки интеграции согласно п. 9 Регламента.
8. Зарегистрировать подключение ИС в продуктивном контуре ЕСИА для отработки интеграции согласно п. 10 Регламента.
9. Зарегистрировать в ЕСИА Центры обслуживания органа/организации. Для этого можно воспользоваться Технологическим порталом ЕСИА.
10. Настроить свою ИС согласно ее эксплуатационной документации. В частности, необходимо завести в ИС идентификаторы Центров обслуживания, полученные на предыдущем шаге, а также установить сетевую связность к СМЭВ и задать использование ключей, соответствующих зарегистрированному в ЕСИА и СМЭВ сертификату ИС.
11. Специалистам Центров обслуживания, которые будут выполнять регистрацию пользователей в ЕСИА, нужно выпустить средства КЭП. В сертификатах обязательно должны быть ОГРН организации (из тех, что получили право выдачи ПЭП), СНИЛС сотрудника.
12. Дать доступ специалистам Центров обслуживания к ИС согласно ее эксплуатационной документации.

Г.2 Регистрация пользователей

Общая схема регистрации пользователя с использованием электронного сервиса включает в себя следующие шаги (Рисунок 16):

1. ИС отправляет запрос на регистрацию, включающий персональные данные пользователя, а также ряд дополнительных параметров.
2. ЕСИА возвращает идентификатор заявки на регистрацию пользователя, а также передает пароль для первого входа.
3. ЕСИА проводит проверку данных пользователя в БГИР, если проверки пройдены успешно, то регистрирует учетную запись.
4. ИС при необходимости вызывает метод, позволяющий проверить статус выполняемой регистрации, в качестве входных параметров указывая идентификатор заявки на регистрацию пользователя.
5. ЕСИА возвращает статус регистрации пользователя.

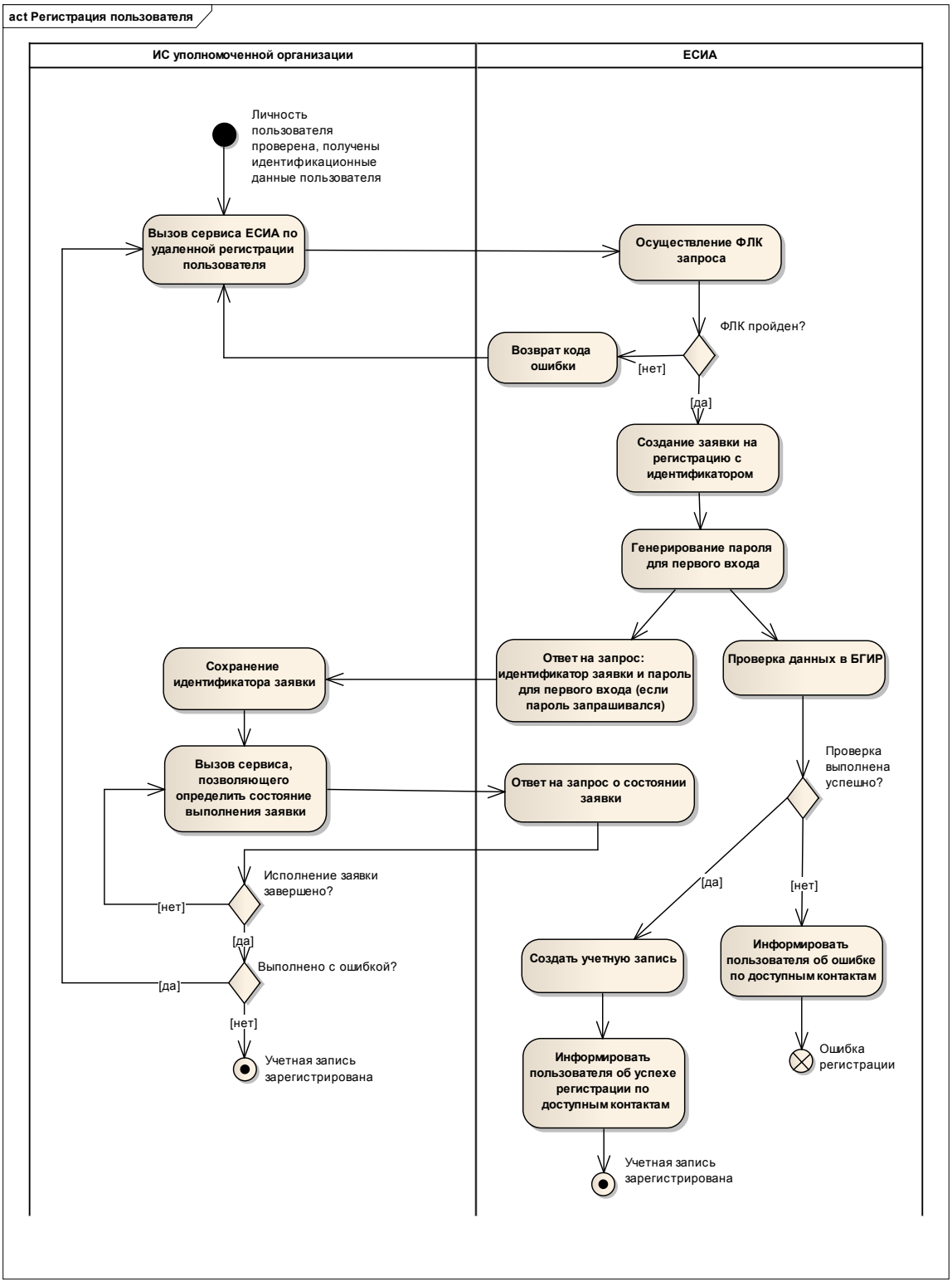

Рисунок 16 – Общая схема регистрации пользователя

Г.2.1 Запрос на регистрацию

Для инициирования регистрации новой подтверждённой учётной записи пользователя в ЕСИА необходимо вызвать метод «Зарегистрировать подтверждённую учётную запись в ЕСИА с выдачей пароля для первого входа».

В качестве входных параметров метод получает персональные данные регистрируемого пользователя, необходимые для проведения операции, а также данные о способе доставки пароля для первого входа в систему. Возможны следующие способы доставки:

- отправка на адрес электронной почты (при условии, что при вызове сервиса адрес указан среди личных данных пользователя);
- отправка на номер мобильного телефона (при условии, что при вызове сервиса номер указан среди личных данных пользователя);
- отправка в ответе на запрос о регистрации;
- отправка пароля не требуется (например, если пользователь будет входить в систему с использованием электронной подписи).

В качестве выходных параметров метод возвращает результат выполнения операции (успешно или не успешно). При успешном завершении в ответном сообщении содержится идентификатор заявки на регистрацию пользователя (requestId), поскольку верификация данных пользователя осуществляется в асинхронном режиме (в силу возможной недоступности БГИР ФОИВ для осуществления верификации персональных данных пользователей), а также пароль для первого входа в систему (если указан соответствующий способ доставки пароля).

При неуспешном завершении метод возвращает ошибку, содержащую код и текстовое описание ошибки.

Если заявка на регистрацию создана успешно, ЕСИА направляет пользователю по указанным в запросе каналам связи уведомление об успехе проверки и возможности входа в учетную запись. Если данные пользователя не прошли проверку по БГИР (и в заявке указан e-mail и/или номер мобильного телефона), ЕСИА направляет пользователю уведомление об этом. Регистрация учётной записи, данные профиля которой не прошли проверку по БГИР, не производится.

Г.2.2 Проверка состояния выполнения запроса

Для проверки статуса регистрации ИС должна произвести вызов метода «Проверить статус заявки на выполнение операции», в качестве входных параметров метод получает идентификатор заявки на регистрацию пользователя (requestId). Система, осуществляющая

вызов сервиса ЕСИА, с использованием requestId может получить данные только по запросам, которые были инициированы ей самой.

В ответном сообщении передается информация о текущем статусе выполнении операции по регистрации пользователя.

Г.3 Подтверждение личности пользователя

Сервис регистрации пользователей, зарегистрированный в СМЭВ, обеспечивает возможность подтверждения личности в Центрах обслуживания Оператора выдачи ключа ПЭП. Для этого необходимо вызвать метод «Подтвердить личность гражданина РФ или иностранного гражданина в ЕСИА» данного сервиса.

Чтобы подтвердить свою учетную запись, пользователь должен предварительно создать упрощенную (непроверенную) или стандартную (проверенную) учетную запись. Это может сделать любой пользователь, имеющий номер мобильного телефона или адрес электронной почты, используя веб-интерфейс ЕСИА. Подтвержденная учетная запись создается пользователем из упрощенной (непроверенной) учетной записи в результате успешной проверки личных данных пользователя в базовых государственных информационных ресурсах (СНИЛС, ФИО, паспортные данные и др.) и подтверждения личности одним из доступных способов, в частности, посредством обращения в один из Центров обслуживания.

При регистрации учетной записи в Центре обслуживания с помощью метода «Зарегистрировать подтверждённую учётную запись в ЕСИА с выдачей пароля для первого входа» сразу создается подтвержденная учетная запись пользователя.

В качестве входных параметров метод, нацеленный на подтверждение личности, получает данные документа, удостоверяющего личность, а также ряд дополнительных параметров. В частности, может быть передан один из возможных типов контакта (email или mobile) для идентификации заявки на подтверждение учетной записи[39].

В качестве выходных параметров метод возвращает результат выполнения операции.

Г.4 Восстановление доступа к учетной записи пользователя

Сервис регистрации пользователей, зарегистрированный в СМЭВ, обеспечивает возможность восстановления доступа к подтвержденной учетной записи пользователя при явке

[39] Указание одного типа контакта необходимо для случая, когда имеется несколько заявок на подтверждение личности с идентичными данными документа, удостоверяющего личность.

в Центр обслуживания Оператора выдачи ключа ПЭП. Для восстановления доступа необходимо вызвать метод « Восстановить доступ к учётной записи ЕСИА с выдачей пароля для входа» данного сервиса.

В качестве входных параметров метод получает персональные данные пользователя, необходимые для проведения операции, а также данные о способе доставки пароля для входа в систему. Возможны следующие способы доставки:

- отправка на адрес электронной почты (при условии, что при вызове сервиса адрес указан среди личных данных пользователя);
- отправка на номер мобильного телефона (при условии, что при вызове сервиса номер указан среди личных данных пользователя);
- отправка в ответе на запрос о восстановлении доступа.

В качестве выходных параметров метод возвращает результат выполнения операции (успешно или не успешно). При успешном завершении в ответном сообщении содержится идентификатор заявки на восстановление доступа (requestId), поскольку при восстановлении доступа осуществляется верификация данных пользователя в асинхронном режиме (в силу возможной недоступности БГИР ФОИВ для осуществления верификации персональных данных пользователей), а также пароль для входа в систему[40].

При неуспешном завершении метод возвращает ошибку, содержащую код и текстовое описание ошибки.

Если заявка на восстановление доступа выполнена успешно, ЕСИА направляет пользователю по указанным в запросе каналам связи уведомление об успехе проверки и возможности входа в учетную запись. Если данные пользователя не прошли проверку по БГИР (и в заявке указан e-mail и/или номер мобильного телефона), ЕСИА направляет пользователю уведомление об этом, при этом восстановление доступа к учетной записи не производится.

Специалист Центра обслуживания Оператора выдачи ключа ПЭП имеет возможность проверить статус восстановления доступа. Для этого ИС Оператора выдачи ключа ПЭП должна произвести вызов метода «Проверить статус заявки на выполнение операции», в качестве входных параметров метод получает идентификатор заявки на восстановление доступа (requestId). Система, осуществляющая вызов сервиса ЕСИА, с использованием requestId может получить данные только по запросам, которые были инициированы ей самой.

[40] Необходимость выполнения проверок данных пользователя связана с тем, что его идентификационные данные (ФИО, данные документа, удостоверяющего личность) могли измениться к моменту восстановления доступа. В этом случае пользователь сохраняет возможность восстановления доступа к своей учетной записи.

В ответном сообщении передается информация о текущем статусе выполнения операции восстановления доступа к учетной записи пользователя.

Г.5 Рекомендации по использованию сервиса

Г.5.1 Общие рекомендации

При обращении пользователя в Центр обслуживания[41] рекомендуется выяснить основную цель обращения, в зависимости от этого выбрать метод сервиса ЕСИА. Основные сценарии представлены в таблице 13

Таблица 13 – Цели обращения пользователя

№	Цель обращения	Рекомендуемое действие
1.	Регистрация в ЕСИА (пользователь не заполнял заявку на подтверждение учетной записи)	Вызов метода «Зарегистрировать подтверждённую учётную запись в ЕСИА с выдачей пароля для первого входа» сервиса ЕСИА
2.	Подтверждение учетной записи ЕСИА (пользователь заполнял заявку на подтверждение учетной записи, заявка проверена)	Вызов метода «Подтвердить личность гражданина РФ или иностранного гражданина в ЕСИА» сервиса ЕСИА
3.	Регистрация в ЕСИА (пользователь не уверен, что корректно заполнил заявку на подтверждение и что она была успешно проверена)	Вызов метода «Зарегистрировать подтверждённую учётную запись в ЕСИА с выдачей пароля для первого входа» сервиса ЕСИА. Следует предупредить пользователя, что для первого входа в учетную запись следует использовать связку СНИЛС и пароль, выданный в Центре обслуживания.
4.	Выяснить, по каким причинам регистрация в ЕСИА не прошла успешно.	Вызов метода «Проверить заявку на регистрацию учетной записи» для выяснения деталей ошибки и последующий вызов метода ««Зарегистрировать подтверждённую

[41] Порядок регистрации Центров обслуживания Операторов выдачи ключа ПЭП определен в п. 13 Регламента.

№	Цель обращения	Рекомендуемое действие
		учётную запись в ЕСИА с выдачей пароля для первого входа»» с исправленными параметрами запроса.
5.	Восстановление доступа (пользователь ранее был зарегистрирован в ЕСИА)	Вызов метода « Восстановить доступ к учетной записи пользователя» сервиса ЕСИА

Г.5.2 Рекомендации по выбору способа доставки пароля

При регистрации подтвержденной учетной записи в ЕСИА рекомендуется отправлять пароль для первого входа на номер мобильного телефона пользователя, если производится обычная регистрация пользователя. Если производится регистрация с выдачей пользователю электронной подписи, то рекомендуется не отправлять пароль.

Если пользователь не имеет мобильного телефона, то допустимо использовать отправку пароля для первого входа на адрес электронной почты.

Если у пользователя нет ни номера мобильного телефона, ни адреса электронной почты, либо он явно попросил выдать ему пароль в Центре обслуживания, возможна передача пароля для первого входа непосредственно специалистом Центра обслуживания.

Г.5.3 Рекомендации по сохранению данных пользователя

При формировании запроса на регистрацию пользователя рекомендуется сохранять:

- идентификатор заявки на регистрацию пользователя (requestId)
- все данные, переданные методу «Зарегистрировать подтверждённую учётную запись в ЕСИА с выдачей пароля для первого входа».

Если пользователь будет проинформирован о возникшей в ходе регистрации ошибке (например, по адресу электронной почты), то он будет иметь возможность обратиться в свой Центр обслуживания для прояснения ситуации. В этом случае идентификатор заявки (requestId) и метод «Проверить заявку на регистрацию учетной записи» позволят получить дополнительную информацию о причинах проблемы. В частности, если при запросе была допущена опечатка, то специалист Центра обслуживания, имея сохраненные данные пользователя, будет иметь возможность отправить исправленную заявку на регистрацию учетной записи.

Г.5.4 Рекомендации по вызову метода «Подтвердить личность гражданина РФ или иностранного гражданина в ЕСИА»

При вызове сервиса «Подтвердить личность гражданина РФ или иностранного гражданина в ЕСИА» следует учесть, что даже при явном указании номера мобильного телефона / адреса электронной почты возможна ситуация, что учетная запись, требующая подтверждения личности, не будет найдена. Это возможно, например, если пользователь сообщил некорректный номер мобильного телефона / адрес электронной почты, либо этот тип контакта не был подтвержден в учетной записи. Следует уточнить у пользователя, какой логин он использует для входа в свою учетную запись и осуществить вызов метода «Подтвердить личность гражданина РФ или иностранного гражданина в ЕСИА» именно с этим параметром.

При указании контактов необходимо передавать только один тип контакта (email или mobile) для идентификации заявки на подтверждение учетной записи.

Если пользователь не помнит номер мобильного телефона / адрес электронной почты, то можно предложить ему провести регистрацию учетной записи. Для этого следует вызвать метод «Зарегистрировать подтверждённую учётную запись в ЕСИА с выдачей пароля для первого входа».

ПРИЛОЖЕНИЕ Д. НЕРЕКОМЕНДУЕМЫЕ К ДАЛЬНЕЙШЕМУ ИСПОЛЬЗОВАНИЮ ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ЕСИА

Д.1 Общие сведения

В результате развития некоторые функциональные возможности ЕСИА сохраняются исключительно в целях обеспечения обратной совместимости.

Разработчикам ранее интегрированных ИС с ЕСИА рекомендуется отказаться от их использования.

Разработчики вновь интегрируемых ИС с ЕСИА рекомендуется использовать актуальные функциональные возможности ЕСИА.

Д.2 Устаревшие утверждения SAML

Таблица 14 – Перечень атрибутов, поддержка которых в будущем будет прекращена

№	Атрибут	Описание	Примечание
1.	assuranceLevel	Уровень достоверности идентификации пользователя. Возможны следующие значения: AL10 – упрощенная (непроверенная) учетная запись; AL15 – стандартная (проверенная) учетная запись; AL20 – подтвержденная учетная запись; AL30 – подтвержденная учетная запись (аутентификация по КЭП).	Рекомендуется использовать атрибуты: - personTrusted – для определения подвержденных учетных записей; - authnMethod – для определения метода аутентификации.
2.	attachedToOrg	Признак включенности (присоединения) к организации	Необходимо использовать globalRole
3.	inn	ИНН пользователя	Необходимо использовать

№	Атрибут	Описание	Примечание
			personINN
4.	name	Имя пользователя	Необходимо использовать lastName / firstName / middleName
5.	nsiId	Мнемоника ОГВ	Необходимо использовать orgOGRN и orgType
6.	personType	Категория пользователя. Принимает следующие возможные значения: **R** — гражданин РФ (Russian); **F** — иностранный гражданин (Foreigner).	Необходимо использовать personCitizenship.
7.	snils	СНИЛС пользователя.	Необходимо использовать personSNILS
8.	userType	Тип пользователя	Необходимо использовать globalRole
9.	userName	Логин пользователя.	Необходимо использовать userId, personSNILS