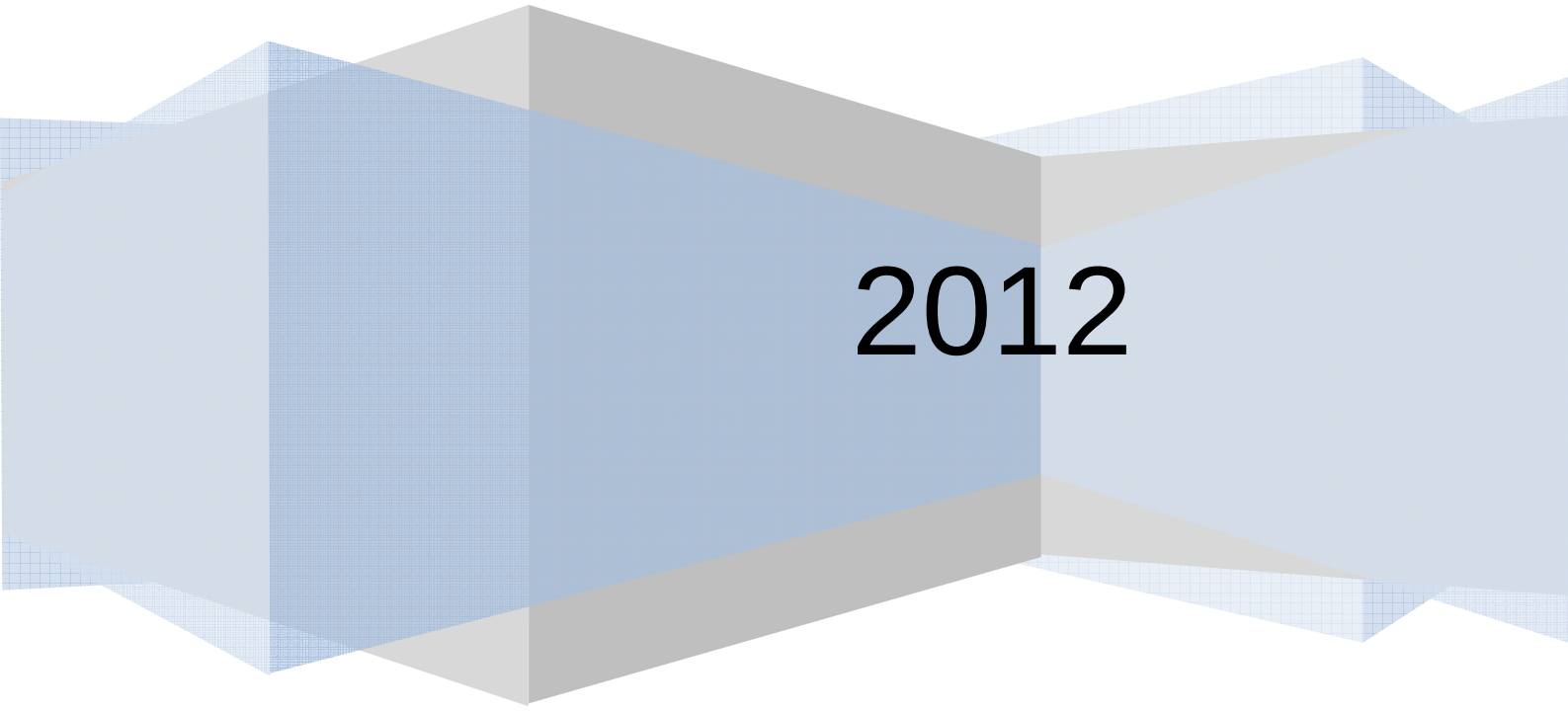
ЕДИНАЯ СИСТЕМА
ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

Методические рекомендации по использованию Единой системы идентификации и аутентификации

Версия 1.0



2012

Содержание

Таблица изменений

Версия	Изменение
1.0	Документ создан

Термины и определения

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»
ЕСНСИ	Федеральная государственная информационная система «Единая система нормативно-справочной информации»
ИС ГУЦ	Федеральная государственная информационная система «Информационная система головного удостоверяющего центра»
СМЭВ	Федеральная государственная информационная система «Единая система межведомственного электронного взаимодействия»
Администратор профиля ОИВ	Уполномоченное должностное лицо ОИВ, которое является пользователем ЕСИА и обладает полномочиями по ведению профиля ОИВ в ЕСИА.
ИС	Информационная система
ИТ	Информационные технологии
ОИВ	Орган исполнительной власти
Органы и организации	Федеральные органы исполнительной власти, органы государственных внебюджетных фондов, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, государственные и муниципальные учреждения, многофункциональные центры, а также иные организации в случаях, предусмотренных федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации

Должностные лица	Физические лица, состоящие в трудовых отношениях с органами и организациями, и участвующие в предоставлении государственных и (или) муниципальных услуг
Заявитель	Физическое или юридическое лицо, обращающееся за получением государственных и (или) муниципальных услуг в органы и организации
Пользователь ЕСИА	Любой человек, имеющий доступ к информационно-телекоммуникационной сети «Интернет» и зарегистрированный в ЕСИА. Пользователем ЕСИА может стать любой заявитель.
Оператор ЕСИА	Министерство связи и массовых коммуникаций Российской Федерации (в соответствии с Постановлением Правительства Российской Федерации от 28.11.2011 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»)
Оператор ИС	Гражданин или организация, осуществляющие деятельность по эксплуатации информационной системы
Регламент	Регламент взаимодействия участников информационного взаимодействия, оператора единой системы идентификации и аутентификации и оператора инфраструктуры электронного правительства при организации информационно-технологического взаимодействия информационных систем с использованием единой системы идентификации и аутентификации
Положение	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 Министерства связи и массовых коммуникаций Российской Федерации от 13.04.2012 г. № 107 (зарегистрирован в Минюсте России 26.04.2012 под № 23952)

1 Введение

1.1 Назначение документа

Цели создания документа:

- Разъяснение базовых сценариев использования ЕСИА:
  - Идентификация и аутентификация заявителей при доступе к порталам государственных и муниципальных услуг и прочим ресурсам Интернет (см. раздел 2.2).
  - Авторизация должностных лиц при межведомственном взаимодействии (см. раздел 3) и предоставление информации о полномочиях должностных лиц (см. раздел 3.4.2).
  - Авторизация информационных систем при межведомственном взаимодействии с использованием СМЭВ (см. раздел 4.2).
- Разъяснение порядка ведения в ЕСИА регистров (справочников), необходимых для реализации базовых сценариев использования ЕСИА:
  - регистр физических лиц;
  - регистр юридических лиц;
  - регистр ОИВ;
  - регистр должностных лиц ОИВ;
  - регистр ИС.
- Разъяснение порядка интеграции информационных систем с ЕСИА.
- Исполнение положений нормативно-правовых актов, перечисленных в п. 1.2.

Документ предназначен:

- для специалистов, которые участвуют в разработке регламентов и инструкций по использованию ЕСИА в ОИВ;
- для руководителей подразделений ОИВ, которые организуют интеграцию информационных систем с ЕСИА;
- для ИТ-специалистов, которые выполняют интеграцию информационных систем с ЕСИА.

1.2 Нормативные ссылки

- Федеральный закон от 27.07.2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».
- 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 08.06.2011 г. № 451.
- Постановление Правительства Российской Федерации от 28.11.2011 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».
- 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 Министерства связи и массовых коммуникаций Российской Федерации от __.__.2012 г. № ____.

1.3 Краткие сведения о ЕСИА

В соответствии с постановлением Правительства Российской Федерации от 28.11.2011 г. № 977 ЕСИА должна обеспечивать санкционированный доступ участников информационного взаимодействия (заявителей и должностных лиц ОИВ) к информации, содержащейся в государственных информационных системах, муниципальных информационных системах и иных информационных системах.

Основные функциональные возможности ЕСИА:

- Идентификация и аутентификация пользователей, в том числе:
  - Однократная аутентификация[1]. Пользователям ЕСИА это даёт следующее преимущество: пройдя процедуру идентификации и аутентификации в ЕСИА, пользователь может в течение одного сеанса работы обращаться к любым

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

информационным системам, использующим ЕСИА, при этом повторная идентификация и аутентификация не требуется.

- Поддержка различных методов аутентификации: по паролю и по электронной подписи;
- Поддержка уровней достоверности идентификации (Приложение Б).

- Управление идентификационными данными[2], а именно – ведение регистров физических, юридических лиц, органов и организаций, должностных лиц органов и организаций и информационных систем;
- Авторизация уполномоченных лиц ОИВ при доступе к следующим функциям ЕСИА:
  - ведение регистра должностных лиц ОИВ в ЕСИА;
  - ведение справочника полномочий ИС и предоставление пользователям ЕСИА (зарегистрированным в ЕСИА как должностные лица ОИВ) полномочий по доступу к ресурсам ИС, зарегистрированным ЕСИА;
  - делегирование вышеуказанных полномочий уполномоченным лицам нижестоящих ОИВ.
- Ведение и предоставление информации о полномочиях пользователей в отношении информационных систем.

[2] Соответствующий термин на английском языке – Identity Management

2 Использование ЕСИА заявителями

В соответствии с п. 2.1 Положения, заявители являются участниками информационного взаимодействия с использованием ЕСИА. Заявители – это физические или юридические лица, обращающиеся за предоставлением государственных и (или) муниципальных услуг в органы и организации.

В соответствии с п. 3.2 (а, б) Положения, в состав ЕСИА входят регистры физических и юридических лиц.

В соответствии с п. 3.3 Положения, формирование регистра физических лиц производится:

- заявителями,
- органами и организациями, «имеющими право на выдачу кода активации и ключа простой электронной подписи в целях оказания государственных и муниципальных услуг, перечень которых утвержден Правительством Российской Федерации», с добровольного согласия заявителей;
- аккредитованными удостоверяющими центрами с добровольного согласия заявителей.

В соответствии с п. 3.4 Положения, формирование регистра юридических лиц производится руководителями юридических лиц.

В соответствии с п. 1.5 (а, б) Положения, ЕСИА осуществляет идентификацию и аутентификацию участников взаимодействия.

Далее в текущем разделе рассмотрено, каким образом в ЕСИА осуществляется:

- формирование и ведение регистров физических и юридических лиц;
- идентификация и аутентификация заявителей при доступе к ресурсам информационных систем, подключенных к ЕСИА.

2.1 Формирование и ведение регистров заявителей

2.1.1 Формирование и ведение регистра физических лиц

Формирование и ведение регистра физических лиц включает следующие операции:

- создание записи в регистре физических лиц (регистрация физического лица);
- изменение записи в регистре физических лиц (изменение данных физического лица);

- исключение записи из регистра физических лиц (удаление учетной записи физического лица).

Регистрация физического лица

В ЕСИА возможны следующие сценарии регистрации физических лиц:

- самостоятельная регистрация физического лица с использованием функции регистрации, доступной на ЕПГУ, или посредством прямой ссылки, размещаемой в ИС, использующей ЕСИА;
- регистрация физического лица в офисах уполномоченных организаций:
  - в федеральных и региональных органах исполнительной власти;
  - в Центрах продаж и обслуживания клиентов оператора эксплуатации ИЭП;
  - в аккредитованных в соответствии с законодательством удостоверяющих центрах.

В ЕСИА могут зарегистрироваться следующие категории физических лиц:

- граждане РФ (в том числе являющиеся индивидуальными предпринимателями);
- иностранные граждане и лица без гражданства.

Сценарий самостоятельной регистрации для граждан РФ (в том числе являющихся индивидуальными предпринимателями):

1. Гражданин РФ переходит на web-страницу ЕСИА для регистрации граждан РФ: http://esia.gosuslugi.ru/sia-web/rf/registration/lp/Index.spr;
2. Гражданин РФ:
   - знакомится с порядком регистрации;
   - подтверждает своё согласие с условиями регистрации;
   - вводит личные данные.
3. ЕСИА проверяет достоверность личных данных.
4. Гражданин РФ вводит аутентификационные данные: пароль, подтверждение пароля, секретный вопрос и ответ на него;
5. Гражданин РФ выбирает способ активации учетной записи:
   - доставка кода активации ФГУП «Почта России»;
   - получение кода активации в Центре продаж и обслуживания клиентов оператора эксплуатации ИЭП;
   - с помощью носителя электронной подписи, выданного доверенным удостоверяющим центром (только для индивидуальных предпринимателей);

6. Гражданин РФ вводит контактные данные: адрес электронной почты и номер мобильного телефона (при согласии его предоставить).
7. Гражданин РФ, не являющийся индивидуальным предпринимателем, активирует свою учетную запись после получения кода активации:
   - переходит на web-страницу https://esia.gosuslugi.ru/sia-web/rf/activation/Index.spr
   - вводит СНИЛС и код активации;
   - вводит пароль.
8. Гражданин РФ, являющийся индивидуальным предпринимателем, активирует свою учетную запись с помощью носителя электронной подписи, выданного доверенным удостоверяющим центром:
   - вводит основной государственный регистрационный номер индивидуального предпринимателя (ОГРНИП);
   - вставляет носитель электронной подписи, выданной доверенным удостоверяющим центром ФНС России и вводит PIN-код.

Сценарий самостоятельной регистрации для иностранных граждан (и лиц без гражданства):

1. Иностранный гражданин переходит на web-страницу ЕСИА для регистрации иностранных граждан: http://esia.gosuslugi.ru/sia-web/fn/registration/lp/Index.spr.
2. Иностранный гражданин:
   - знакомится с порядком регистрации;
   - подтверждает своё согласие с условиями регистрации;
   - вводит личные данные.
3. ЕСИА проверяет достоверность личных данных.
4. Иностранный гражданин вводит адрес электронной почты.
5. ЕСИА высылает на указанный адрес электронной почты код активации.
6. После получения кода активации, иностранный гражданин:
   - переходит на web-страницу https://esia.gosuslugi.ru/sia-web/fn/activation/Index.spr
   - вводит логин и код активации.

Сценарий регистрации гражданина РФ в офисе уполномоченной организации:

1. Гражданин РФ приходит в офис уполномоченной организации.
2. Сотрудник уполномоченной организации вводит личные данные.
3. ЕСИА проверяет достоверность личных данных.
4. Сотрудник уполномоченной организации выдаёт гражданину РФ код активации.

5. Гражданин РФ самостоятельно активирует свою учетную запись:
   - переходит на web-страницу https://esia.gosuslugi.ru/sia-web/rf/activation/Index.spr
   - вводит СНИЛС и код активации;
   - вводит пароль.

ЕСИА автоматически проверяет достоверность личных данных физических лиц в процессе регистрации, используя электронные сервисы ОИВ (например, ПФР для проверки СНИЛС, ФНС России для проверки ИНН, ФМС России для проверки паспортных данных). Если проверка достоверности не пройдена, регистрация невозможна.

Изменение данных физического лица

Физические лица имеют возможность самостоятельно изменять свои данные в Личном Кабинете ЕПГУ (https://epgu.gosuslugi.ru/pgu/personcab). Для этого они должны предварительно пройти идентификацию и аутентификацию в ЕСИА (см. пункт 2.2). При изменении ФИО ЕСИА выполняет проверку достоверности изменённых данных, используя электронный сервис ПФР. При изменении адреса электронной почты или номера мобильного телефона, ЕСИА выполняет запрос подтверждения изменённых данных.

Удаление учетной записи физического лица

Физические лица имеют возможность самостоятельно удалить свою учётную запись ЕСИА через Личный Кабинет ЕПГУ. Для этого они должны предварительно пройти идентификацию и аутентификацию в ЕСИА (см. пункт 2.2).

2.1.2 Формирование и ведение регистра юридических лиц

Формирование и ведение регистра юридических лиц в ЕСИА включает следующие операции:

- создание записи в регистре юридических лиц (регистрация юридического лица);
- изменение записи в регистре юридических лиц (изменение данных юридического лица).

Регистрация юридического лица

Выполнить регистрацию юридического лица может только руководитель юридического лица самостоятельно с использованием ЕПГУ. В процессе регистрации ЕСИА автоматически проверяет, что физическое лицо является руководителем

регистрируемого юридического лица, используя электронный сервис проверки ФНС России. Если проверка достоверности не пройдена – регистрация невозможна.

Изменение данных юридического лица

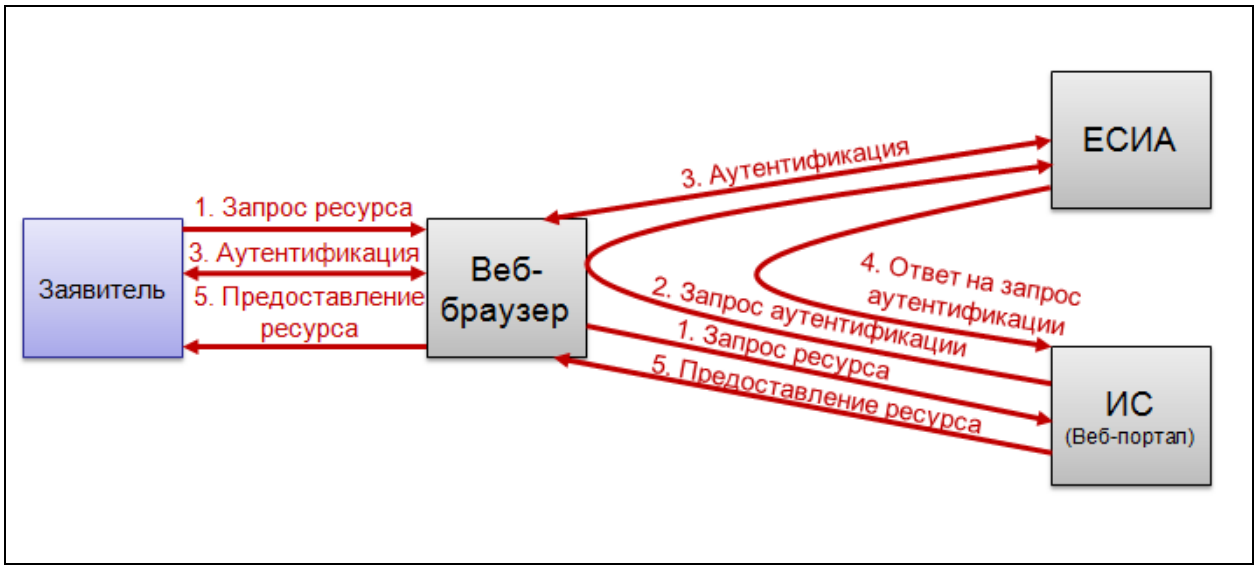
Руководитель юридического лица имеет доступ к Личному Кабинету юридического лица на ЕПГУ (https://epgu.gosuslugi.ru/pgu/personcab#_data-common), где он может:

- изменить общую информацию о юридическом лице (организационно-правовую форму, сокращённое наименование, КПП);
- изменить контактные данные юридического лица;
- зарегистрировать любого пользователя ЕСИА в качестве сотрудника организации и предоставить ему доступ в кабинет юридического лица.

Для доступа к Личному Кабинету юридического лица необходимо пройти идентификацию и аутентификацию в ЕСИА.

2.2 Идентификация и аутентификация заявителей

ЕСИА выполняет идентификацию и аутентификацию заявителей при доступе к ресурсам информационных систем, использующих ЕСИА.



Сценарий:

1. Пользователь обращается к защищённому ресурсу ИС (например, ведомственному или региональному порталу государственных услуг).
2. ИС направляет в ЕСИА запрос на аутентификацию.
3. ЕСИА проверяет наличие у пользователя открытой сессии и, если активная сессия отсутствует, проводит его аутентификацию. Для этого ЕСИА направляет

пользователя на веб-страницу аутентификации ЕСИА[3]. Заявитель проходит идентификацию и аутентификацию, используя доступный ему метод аутентификации (Таблица 1).

4. Если пользователь успешно аутентифицирован, то ЕСИА передаёт в ИС набор утверждений, содержащих идентификационные данные пользователя, информацию о контексте аутентификации, в том числе данные об уровне достоверности идентификации (Приложение Б).
5. На основании полученной из ЕСИА информации, ИС авторизует заявителя на доступ к защищаемому ресурсу.

Таблица 1 - Методы идентификации / аутентификации пользователей ЕСИА

Категория пользователя ЕСИА	**Доступные методы идентификации / аутентификации**
Граждане РФ (в том числе – граждане РФ, являющиеся индивидуальными предпринимателями и представителями юридических лиц)	Идентификатор (СНИЛС) и пароль
	PIN-код и носитель ключа электронной подписи физического лица, индивидуального предпринимателя или руководителя юридического лица
Иностранные граждане и лица без гражданства	Идентификатор (Логин) и пароль

2.3 Подключение ИС к ЕСИА с целью идентификации и аутентификации заявителей

Подключение ИС к ЕСИА обеспечивает возможность идентификации и аутентификации заявителей с помощью ЕСИА. Пользователями ИС могут являться физические лица, в том числе должностные лица юридических лиц и ОИВ.

Результатом подключения ИС к ЕСИА является обеспечение следующих возможностей взаимодействия ИС и заявителей:

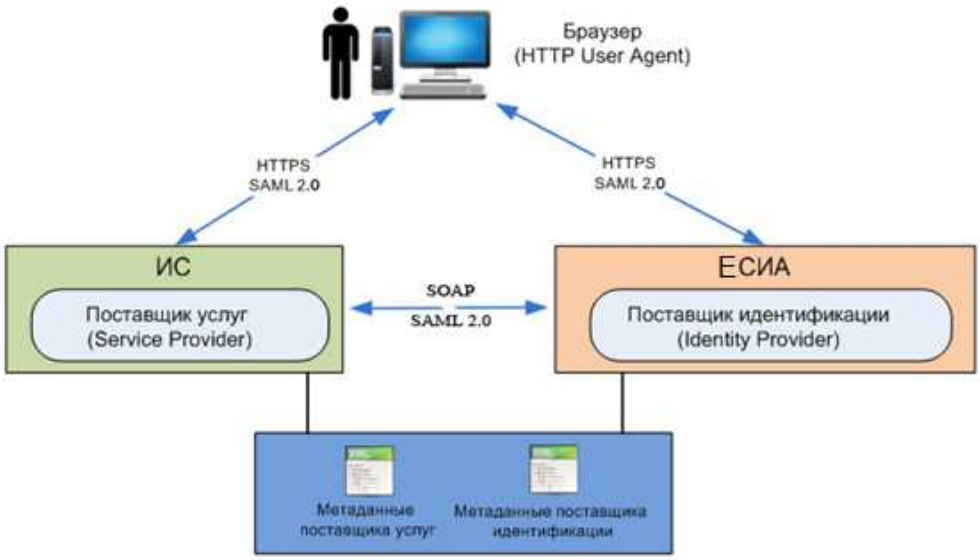
- идентификация и аутентификация пользователей ИС (заявителей) средствами ЕСИА;

[3] В настоящее время страница доступна по адресу https://esia.gosuslugi.ru/idp/Authn/CommonLogin

- завершение активной сессии пользователя для двух сценариев:
  - выход инициирован ИС,
  - выход инициирован ЕСИА.

ИС выступает в роли поставщика услуг (Service Provider). ЕСИА выступает в роли доверенного поставщика идентификации (Identity Provider).

Общая схема подключения ИС к ЕСИА представлена на рисунке.



Поставщику услуг (ИС) должны быть известны параметры подключения (протокол, адреса вызовов, сертификат и т.д.) к поставщику идентификации (ЕСИА). Указанные параметры описаны в метаданных поставщика идентификации. В свою очередь, поставщику идентификации (ЕСИА) должны быть известны параметры подключения к поставщику услуг (ИС). Указанные параметры должны быть описаны в метаданных поставщика услуг.

Таким образом, для подключения ИС к ЕСИА необходимо:

- разработать программный интерфейс поставщика услуг (см. Приложение Г);
- выполнить настройку метаданных (см. Приложение Г, раздел Г.4):
  - настроить метаданные поставщика услуг (ИС) и передать их поставщику идентификации (ЕСИА);
  - загрузить метаданные поставщика идентификации (ЕСИА).

Порядок подключения ИС к ЕСИА для идентификации и аутентификации заявителей

Для подключения ИС к ЕСИА оператор ИС должен:

1. Самостоятельно сгенерировать (например, с помощью утилиты keytool из состава Java Development Kit) для своей ИС сертификат ключа неквалифицированной

электронной подписи в формате X.509 версии 3. Сертификат требуется для осуществления взаимодействия с поставщиком идентификации ЕСИА. Допускается использование самоподписанного сертификата. Специальные требования: алгоритм RSA, длина ключа 1024 бит. Более подробную информацию о сертификате X.509 можно посмотреть по ссылке http://tools.ietf.org/html/rfc5280.

2. Зарегистрировать ИС в ЕСИА (порядок регистрации ИС см. в разделе 3.3).
3. Реализовать в ИС интерфейсы поставщика услуг (см. Приложение Г), учитывающие особенности реализации ЕСИА соответствующие следующим профилям SAML 2.0:
   - Web Browser SSO с учетом рекомендаций Interoperable SAML 2.0 Web Browser SSO Deployment Profile;
   - Single Logout.
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. Загрузить актуальные метаданные поставщика идентификации ЕСИА:
   - метаданные тестового поставщика идентификации ЕСИА опубликованы по ссылке https://demo1-esia.gosuslugi.ru/idp/shibboleth;
   - метаданные промышленного поставщика идентификации ЕСИА опубликованы по ссылке https://esia.gosuslugi.ru/idp/shibboleth.
6. Обеспечить сетевую связанность информационной системы с системой ЕСИА с учетом следующих особенностей:
   - Подключение информационных систем, обеспечивающих работу пользователей категорий «Граждане РФ», «Иностранные граждане», «Индивидуальные предприниматели», «Должностные лица юридических лиц», к системе ЕСИА должно производиться через сеть Интернет по протоколу HTTPS.
   - Подключение информационных систем, обеспечивающих работу пользователей категории «Должностные лица органов и организаций исполнительной власти» к системе ЕСИА должно производиться только через каналы связи, использующиеся в т.ч. системой межведомственного электронного взаимодействия.
7. Синхронизировать системное время информационной системы со значением точного времени для той временной зоны, которая установлена настройками для

данной информационной системы. Допустимое отклонение от точного времени не должно превышать 1 минуту.

8. Подать заявку на подключение ИС к тестовой ЕСИА для идентификации и аутентификации заявителей. Подача заявки и ее подтверждение осуществляются в соответствии с Регламентом.
9. Разработать и передать Оператору ЕСИА метаданные поставщика услуг для отработки взаимодействия в тестовой среде ЕСИА. Шаблон метаданных поставщика услуг приведен в разделе Г.5 (см. Приложение Г).
10. Протестировать взаимодействие с ЕСИА в тестовой среде. При необходимости доработать интерфейсы поставщика услуг.
11. Подать заявку на подключение ИС к промышленной ЕСИА для идентификации и аутентификации заявителей. Подача заявки и ее подтверждение осуществляются в соответствии с Регламентом.

3 Использование ЕСИА в органах и организациях

В соответствии с п. 2.1 Положения, должностные лица ОИВ являются участниками информационного взаимодействия с использованием ЕСИА.

В соответствии с п. 3.2 (в, г, д) Положения, в состав ЕСИА входят регистры органов и организаций, должностных лиц, информационных систем.

В соответствии с п. 3.5 Положения, формирование и ведение регистра органов и организаций осуществляется:

- оператором ЕСИА – для ФОИВ, государственных внебюджетных фондов[4], субъектов РФ;
- операторами ФОИВ, государственных внебюджетных фондов – для центральных аппаратов и территориальных органов (подразделений);
- операторами субъектов РФ – для ОИВ субъектов РФ, органов местного самоуправления, государственных и муниципальных учреждений, многофункциональных центров;
- оператором ЕСИА – для иных организаций.

В соответствии с п. 3.6 Положения, «*формирование и ведение регистра должностных лиц органов и организаций осуществляется уполномоченными должностными лицами органов и организаций*».

В соответствии с п. 4.5 Положения, «*должностные лица органов и организаций несут ответственность за достоверность информации (сведений, данных) при формировании регистра должностных лиц единой системы идентификации и аутентификации*».

В соответствии с п. 3.6 Положения, «*в регистре информационных систем указываются сведения об информационных системах, … информация о которых имеется в федеральной государственной информационной системе «Единая система нормативной справочной информации*».

В соответствии с п. 1.5 (а, б) Положения, ЕСИА осуществляет идентификацию и аутентификацию участников информационного взаимодействия.

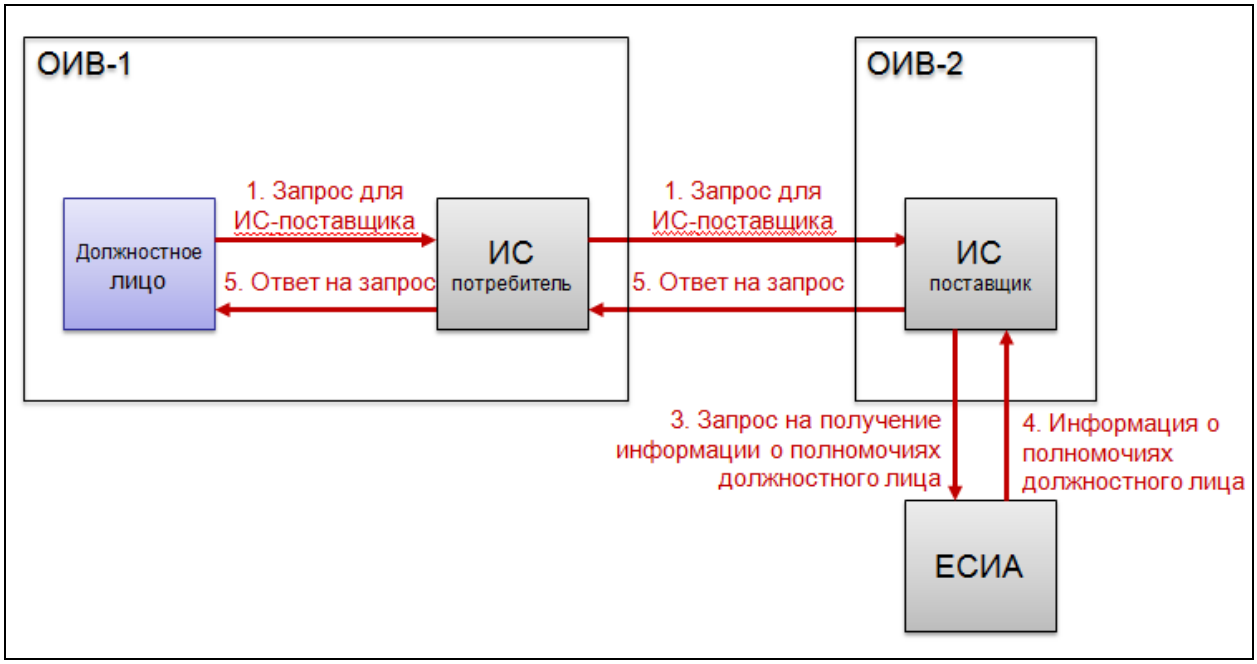
В соответствии с п. 1.5 (в) Положения, ЕСИА осуществляет авторизацию участников информационного взаимодействия — «*в части ведения и предоставления*

[4] В соответствии со ст. 144 Бюджетного Кодекса РФ – Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования

информации о полномочиях участников информационного взаимодействия в отношении информационных систем».

Базовый сценарий авторизации должностных лиц ОИВ при межведомственном взаимодействии (доступе к ресурсам ИС, операторами которых являются другие ОИВ)[5]:

1. Пользователь (должностное лицо) с использованием ИС-потребителя направляет запрос ИС-поставщику.
2. ИС-поставщик извлекает из запроса сведения о пользователе, отправившем запрос:
   – идентификатор пользователя как физического лица – СНИЛС;
   – идентификатор ОИВ, в котором пользователь является должностным лицом, – ОГРН.
3. ИС-поставщик направляет в ЕСИА запрос на предоставление информации о полномочиях пользователя (см. также раздел 3.4.2) в отношении ИС-поставщика. Для отправки запроса ИС-поставщик использует электронный сервис ЕСИА (см. Приложение А, раздел А.4).
4. ЕСИА передаёт в ИС-поставщик данные о действующих полномочиях должностного лица.
5. ИС-поставщик на основании полученных из ЕСИА данных о полномочиях должностного лица авторизует запрос пользователя.



В приведённом выше сценарии ЕСИА используется для предоставления данных о полномочиях должностных лиц.

[5] Реализация этого сценария необходима только в случае предъявления поставщиком сервиса требований к наличию у должностного лица потребителя нормативно установленных полномочий на обращение к сервису.

Далее в текущем разделе рассмотрено, каким образом в ЕСИА осуществляется:

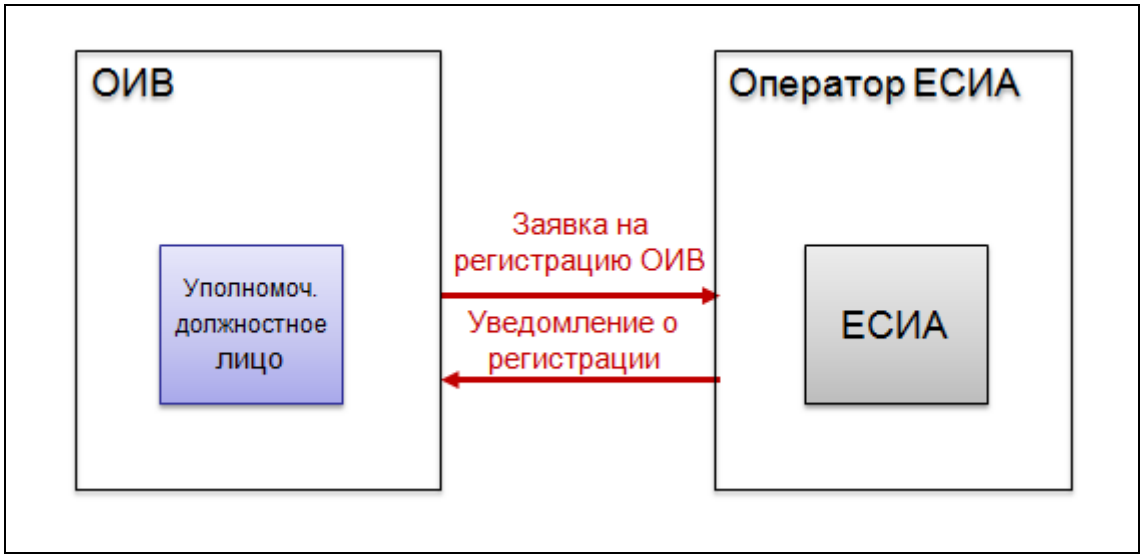
- формирование и ведение регистров органов и организаций, должностных лиц, информационных систем;
- ведение полномочий:
  - назначение (предоставление) и отзыв полномочий должностных лиц;
  - получение информации о предоставленных должностным лицам полномочиях.

3.1 Формирование и ведение регистра органов и организаций

Формирование и ведение регистра ОИВ включает следующие операции:

- создание записи в регистре органов и организаций (регистрация ОИВ);
- изменение записи в регистре органов и организаций (изменение данных ОИВ);
- исключение записи из регистра органов и организаций (удаление данных ОИВ).

Регистрация ОИВ



1. Уполномоченное лицо ОИВ подаёт оператору ЕСИА *заявку на регистрацию ОИВ* (форма заявки приведена в Регламенте) в ЕСИА. Заявка должна быть утверждена уполномоченным заместителем руководителя ОИВ и должна содержать:
   - полное наименование ОИВ;
   - краткое наименование ОИВ;
   - ИНН;
   - ОГРН;
   - ОГРН и наименование вышестоящего ОИВ (при наличии);
   - сведения об уполномоченном должностном лице ОИВ:

- Фамилия, имя, отчество (при наличии);
- СНИЛС;
- пол;
- дата рождения;
- данные паспорта гражданина РФ (серия, номер, дата выдачи, кем выдан);
- адрес электронной почты;
- телефон;
- подразделение;
- должность;
- комментарий.

2. Регистрация ОИВ осуществляется в соответствии с Регламентом.
3. В результате успешного исполнения заявки:
   - ОИВ зарегистрирован в регистре органов и организаций;
   - уполномоченное лицо ОИВ зарегистрировано в качестве должностного лица ОИВ и ему предоставлено полномочие *администратора профиля ОИВ* в ЕСИА.

Уполномоченное лицо ОИВ, которому предоставлены полномочия *администратора профиля ОИВ*, получит доступ к веб-приложению «Профиль органа власти», где сможет вести регистр должностных лиц своего ОИВ (см. раздел 3.2.1).

Изменение данных ОИВ

1. Уполномоченное лицо ОИВ подаёт оператору ЕСИА *заявку на изменение данных ОИВ* (форма заявки приведена в Регламенте) в ЕСИА. Заявка должна быть утверждена уполномоченным заместителем руководителя ОИВ и должна содержать те же данные, что и *заявка на регистрацию ОИВ* (форма заявки приведена в Регламенте) в ЕСИА.
2. Изменение данных ОИВ осуществляется в соответствии с Регламентом.
3. В результате успешного исполнения заявки:
   - данные об ОИВ в регистре органов и организаций скорректированы;
   - данные о полномочиях *администратора профиля ОИВ* скорректированы.

Удаление данных ОИВ

1. Уполномоченное лицо ОИВ подаёт оператору ЕСИА *заявку на удаление данных ОИВ* (форма заявки приведена в Регламенте) из ЕСИА. Заявка должна содержать описание причины (например, ликвидация ОИВ) и должна быть утверждена уполномоченным заместителем руководителя ОИВ.
2. Удаление данных ОИВ осуществляется в соответствии с Регламентом.
3. В результате успешного исполнения заявки:
   - все должностные лица исключены из ОИВ;
   - данные об ОИВ удалены из ЕСИА.

3.2 Формирование и ведение регистра должностных лиц органов и организаций

В ЕСИА хранятся следующие данные должностных лиц ОИВ:

- личные данные:
  - СНИЛС – является основным идентификатором;
  - фамилия, имя, отчество (при наличии);
  - пол;
  - дата рождения;
  - ИНН (при наличии);
  - данные паспорта гражданина РФ (серия, номер, дата выдачи, кем выдан);
- служебные данные:
  - признак принадлежности должностного лица к определённому ОИВ, включённому в регистр ОИВ;
  - подразделение (полное наименование в соответствии с положением о подразделении);
  - должность;
  - служебный адрес электронной почты;
  - номер служебного телефона (при наличии);
  - сведения об используемом (-ых) сертификате (-ах) ключа проверки квалифицированной электронной подписи;
  - перечень назначаемых должностному лицу базовых полномочий (список поддерживаемых в настоящий момент базовых полномочий должностного лица приведен в разделе 3.4.1).

Формирование и ведение регистра должностных лиц ОИВ в ЕСИА может осуществляться двумя способами:

- через графический веб-интерфейс ЕСИА – уполномоченным лицом ОИВ;
- через электронный сервис ЕСИА – информационной системой ОИВ.

Электронные сервисы ЕСИА являются специализированными сервисами, не относящимися к СМЭВ, и работающими по стандарту вызова электронных сервисов ЕСИА. Описание электронных сервисов ЕСИА размещено в разделе 3.2.2 и в приложении (Приложение А).

Формирование и ведение регистра должностных лиц включает следующие операции:

- создание записи в регистре должностных лиц (регистрация должностного лица);
- изменение записи в регистре должностных лиц (изменение данных должностного лица);
- исключение записи из регистра должностных лиц (исключение должностного лица из ОИВ).

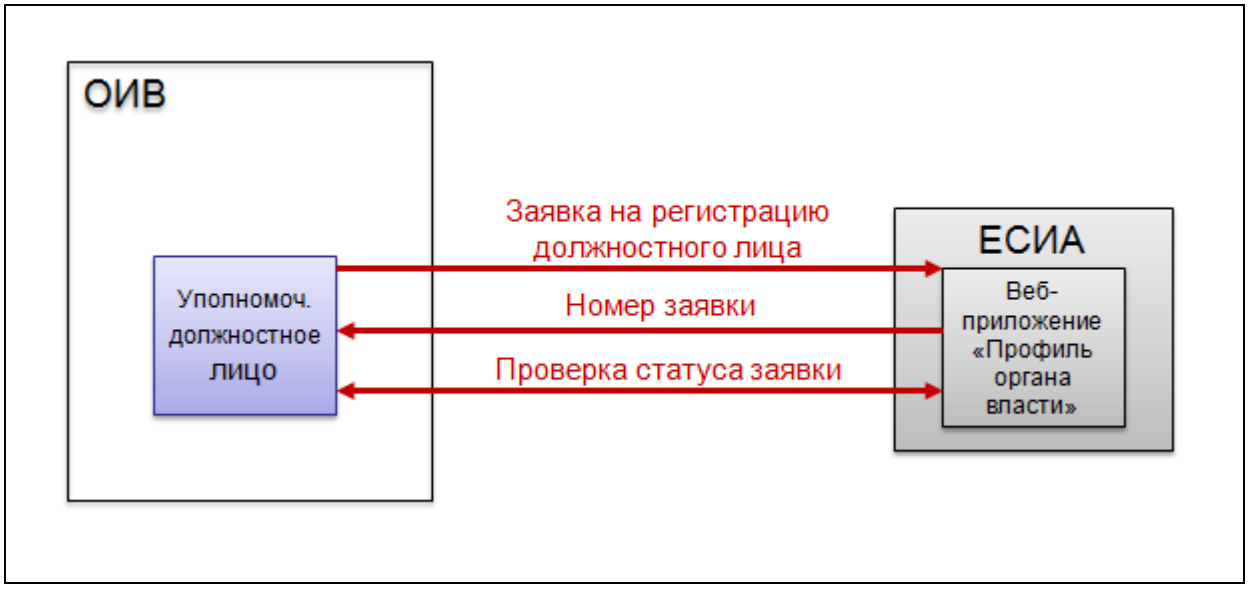
3.2.1 Формирование и ведение регистра должностных лиц с использованием графического интерфейса ЕСИА

Формирование и ведение регистра должностных лиц ОИВ выполняет уполномоченное лицо ОИВ, которое было зарегистрировано в ЕСИА в качестве *администратора профиля ОИВ* в процессе регистрации ОИВ в ЕСИА (см. раздел 3.1).

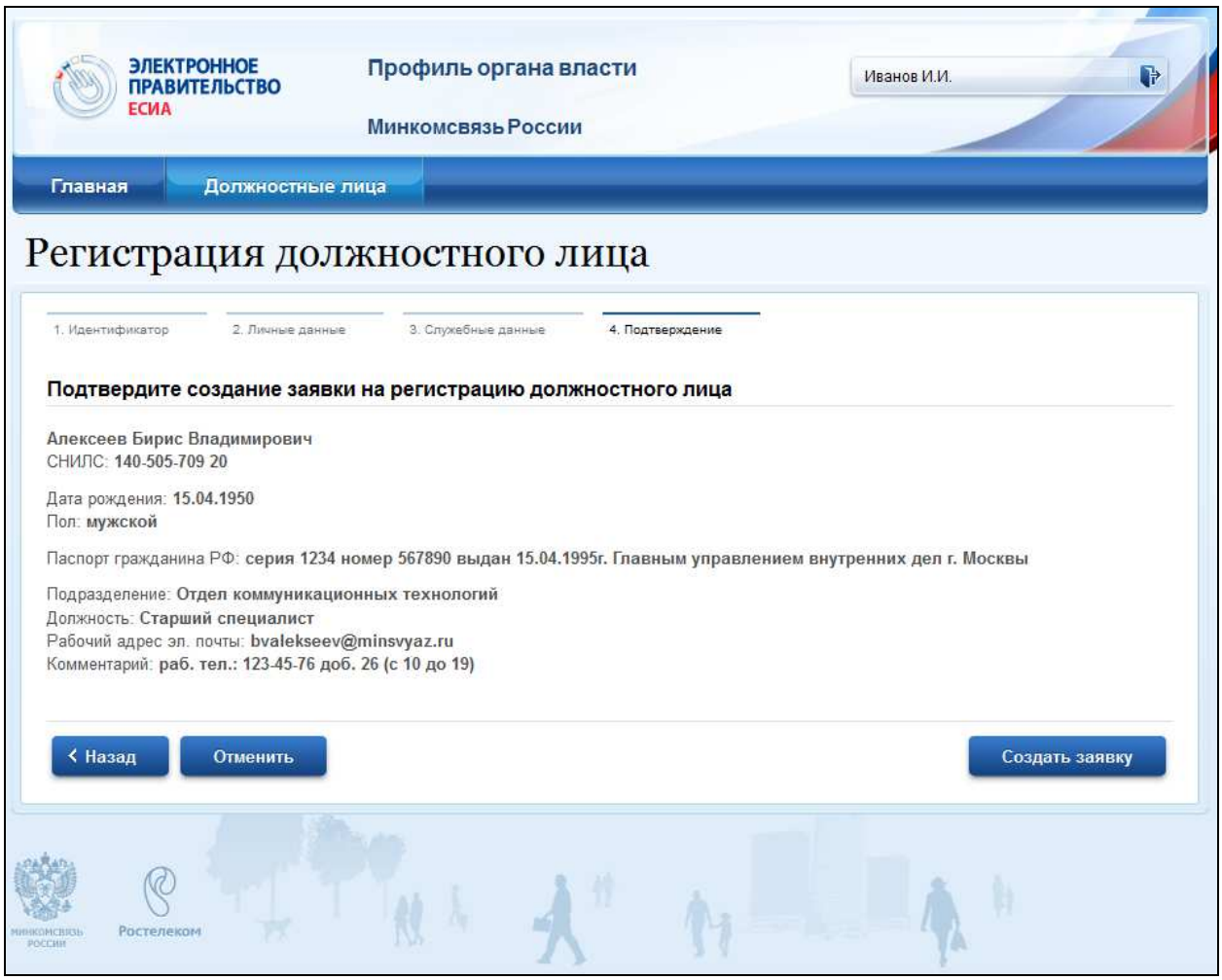
Оператор ЕСИА назначает полномочия *администратора профиля ОИВ* только для одного должностного лица ОИВ, указанного в заявке на регистрацию ОИВ. При необходимости это должностное лицо с полномочием *администратора профиля ОИВ* может зарегистрировать подчиненных должностных лиц с полномочиями *администратора профиля ОИВ* и поручить им регистрацию должностных лиц ОИВ.

Далее рассмотрены сценарии формирования и ведения регистра должностных лиц ОИВ уполномоченным лицом ОИВ.

Регистрация должностного лица ОИВ



1. Уполномоченное лицо ОИВ входит в веб-приложение «Профиль органа власти», выбирает функцию регистрации нового должностного лица ОИВ, вводит идентификационные данные регистрируемого должностного лица ОИВ.
2. ЕСИА создаёт заявку на регистрацию должностного лица и сообщает уполномоченному лицу номер заявки.
3. ЕСИА автоматически выполняет заявку. В процессе выполнения заявки ЕСИА проверяет достоверность личных данных должностного лица, вызывая электронные сервисы ОИВ, зарегистрированные в СМЭВ (например, сервисы ПФР для проверки СНИЛС, ФНС России для проверки ИНН, ФМС России для проверки паспортных данных). Если все проверки пройдены успешно, ЕСИА регистрирует должностное лицо ОИВ и изменяет статус заявки на «Успешно выполнена».
4. Уполномоченное лицо ОИВ может отследить текущий статус выполнения заявки, используя идентификатор заявки.



Изменение данных должностного лица ОИВ

1. При изменении данных должностного лица (например, в случае смены фамилии или паспорта), уполномоченное лицо ОИВ входит в веб-приложение «Профиль органа власти», находит должностное лицо ОИВ и выбирает функцию редактирования данных должностного лица ОИВ.
2. ЕСИА создаёт заявку на изменение данных должностного лица и сообщает уполномоченному лицу номер заявки.
3. ЕСИА проверяет достоверность личных данных должностного лица, вызывая электронные сервисы соответствующих ОИВ (например, сервисы ПФР для проверки СНИЛС, ФНС России для проверки ИНН, ФМС России для проверки паспортных данных), зарегистрированные в СМЭВ. Если все проверки пройдены успешно, ЕСИА изменяет данные должностного лица ОИВ и изменяет статус заявки на «Успешно выполнена».
4. Уполномоченное лицо ОИВ может отследить текущий статус выполнения заявки, используя идентификатор заявки.

Исключение должностного лица из ОИВ

1. При увольнении должностного лица из ОИВ, уполномоченное лицо ОИВ входит в веб-приложение «Профиль органа власти», находит должностное лицо ОИВ и выбирает функцию исключения должностного лица из ОИВ.
2. ЕСИА создаёт заявку на исключение должностного лица и сообщает уполномоченному лицу номер заявки.
3. ЕСИА отзывает все полномочия, которые были предоставлены должностному лицу ОИВ[6], и исключает должностное лицо из ОИВ.[7]
4. Уполномоченное лицо ОИВ может отследить текущий статус выполнения заявки, используя идентификатор заявки.

3.2.2 Формирование и ведение регистра должностных лиц ОИВ через электронные сервисы ЕСИА

Для автоматизированного формирования и ведения регистра должностных лиц ОИВ следует использовать следующие электронные сервисы ЕСИА:

- OfficerManagement (см. раздел А.1);
- Request (см. раздел А.3).

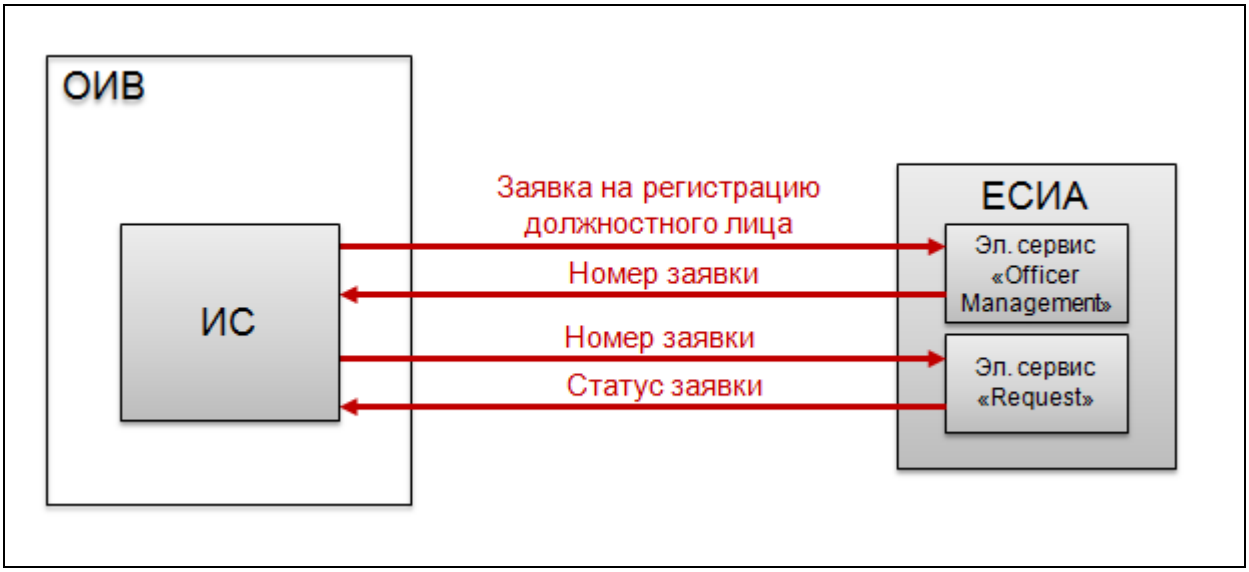
Далее рассмотрены сценарии использования электронных сервисов ЕСИА для:

- регистрации должностного лица ОИВ;
- изменения служебных данных должностного лица ОИВ;
- исключения должностного лица из ОИВ.

[6] Процесс предоставления полномочий рассмотрен в разделе 3.4

[7] Учетная запись бывшего должностного лица остаётся в ЕСИА в регистре физических лиц. Бывшее должностное лицо может продолжать использовать свою учетную запись ЕСИА (например, для получения государственных услуг в электронном виде)

Регистрация должностного лица ОИВ



1. ИС ОИВ вызывает операцию regOfficer электронного сервиса OfficerManagement и передаёт данные должностного лица.
2. Электронный сервис создаёт в ЕСИА заявку на регистрацию должностного лица и, при успешном создании заявки, возвращает в ИС ОИВ идентификатор заявки.
3. В процессе обработки заявки ЕСИА проверяет достоверность личных данных должностного лица, вызывая электронные сервисы соответствующих ОИВ, зарегистрированные в СМЭВ. Если все проверки пройдены успешно, ЕСИА регистрирует должностное лицо ОИВ и изменяет статус заявки на «Успешно выполнена».
4. ИС ОИВ вызывает операцию getStatus электронного сервиса Request и передаёт идентификатор заявки.
5. Электронный сервис возвращает текущий статус обработки заявки.

Изменение служебных данных должностного лица ОИВ

1. ИС ОИВ вызывает операцию modifyOfficer электронного сервиса OfficerManagement и передаёт данные должностного лица.
2. Электронный сервис создаёт в ЕСИА заявку на изменение данных должностного лица и возвращает в ИС ОИВ идентификатор заявки.
3. ЕСИА изменяет служебные данные зарегистрированного должностного лица ОИВ) и изменяет статус заявки на «Успешно выполнена».
4. ИС ОИВ вызывает операцию getStatus электронного сервиса Request и передаёт идентификатор заявки.
5. Электронный сервис возвращает текущий статус обработки заявки.

Исключение должностного лица из ОИВ

1. ИС ОИВ вызывает операцию dismissOfficer электронного сервиса OfficerManagement и передаёт идентификатор физического лица (СНИЛС) и идентификатор ОИВ, в котором данное физическое лицо является должностным лицом.
2. Электронный сервис создаёт в ЕСИА заявку на исключение должностного лица из ОИВ и возвращает в ИС ОИВ идентификатор заявки.
3. ЕСИА исключает должностное лицо из ОИВ и отзывает его полномочия в данном ОИВ[8], изменяет статус заявки на «Успешно выполнена».
4. ИС ОИВ вызывает операцию getStatus электронного сервиса Request и передаёт идентификатор заявки.
5. Электронный сервис возвращает текущий статус обработки заявки.

3.3 Формирование и ведение регистра информационных систем

Формирование и ведение регистра ИС включает следующие операции:

- создание записи в регистре информационных систем (регистрация ИС);
- изменение записи в регистре информационных систем (изменение данных ИС);
- исключение записи из регистра информационных систем (удаление данных об ИС).

Регистрация ИС

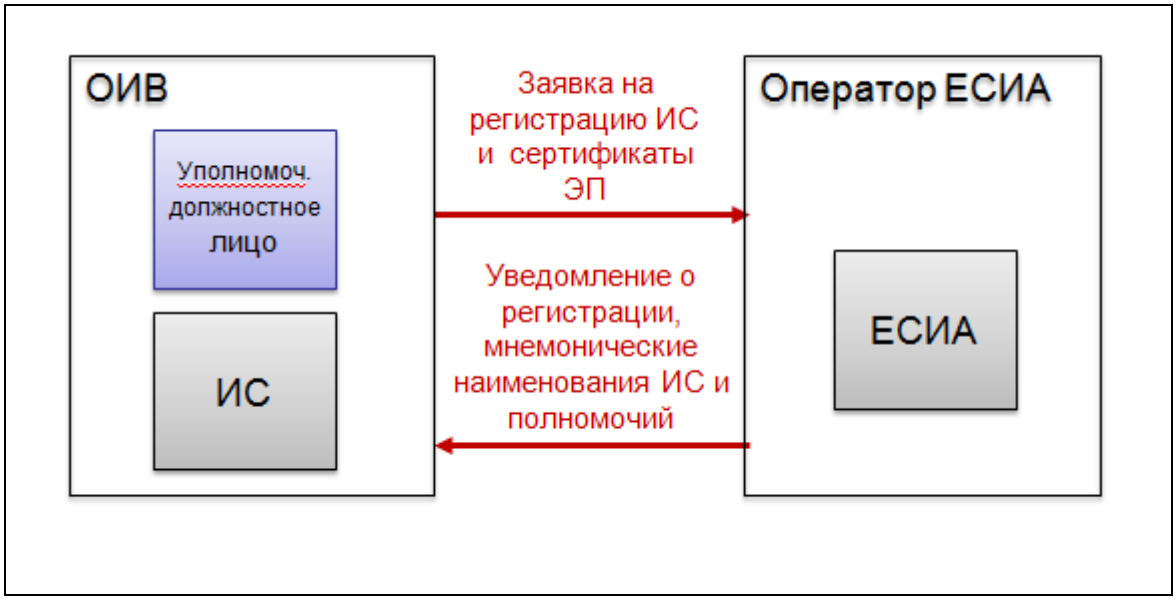
Регистрация ИС выполняется по заявке ОИВ, являющегося оператором регистрируемой ИС. ОИВ предварительно должен быть зарегистрирован в ЕСИА (см. раздел 3.1).

В ЕСИА должны быть зарегистрированы ИС, которые:

- используют ЕСИА как поставщик идентификации (Identity Provoder) для идентификации и аутентификации пользователей (см. разделы 2.2, 2.3, Приложение В, Приложение Г);
- используют электронные сервисы ЕСИА (см. разделы 3.2.2, 3.4.2, Приложение А)

[8] Процесс предоставления полномочий рассмотрен в разделе 3.4

Регистрация информационных систем производится следующим образом:



1. ОИВ (оператор ИС) подаёт оператору ЕСИА *заявку на подключение ИС* (форма заявки приведена в Регламенте) к ЕСИА. Заявка должна быть утверждена уполномоченным заместителем руководителя ОИВ и должна содержать следующие данные:
   - наименование ИС;
   - сведения об операторе ИС:
     - наименование ОИВ;
     - ОГРН;
   - сведения о лице, ответственном за эксплуатацию ИС:
     - ФИО;
     - должность;
     - телефон;
     - Email.
   - (опционально, если планируется использовать функциональность ЕСИА по управлению полномочиями) список полномочий[9] в формате:
     - название полномочия на русском языке.
2. ОИВ (оператор ИС) передаёт оператору ЕСИА цифровой сертификат ИС в формате X.509 версии 3, алгоритм RSA, длина ключа 1024 бит.
3. Регистрация ИС осуществляется в соответствии с Регламентом.

[9] Список полномочий определяется спецификой системы (см. раздел 3.4.1). В качестве примера можно взять систему нормативно-справочной информации некоторого ОИВ. Для такой системы в качестве полномочий можно, например, задать следующие полномочия: *ведение справочников*, *чтение справочников*.

4. В результате успешного исполнения заявки ИС и справочник полномочий ИС зарегистрированы в регистре информационных систем, ИС и ее полномочиям присвоены идентификаторы (мнемонические наименования[10]).

Изменение данных ИС

1. ОИВ (оператор ИС) подаёт оператору ЕСИА *заявку на изменение данных ИС* (форма заявки приведена в Регламенте) в ЕСИА. Заявка должна быть утверждена уполномоченным заместителем руководителя ОИВ и должна содержать те же данные, что и *заявка на регистрацию ИС* (форма заявки приведена в Регламенте) в ЕСИА.
2. Изменение данных об ИС осуществляется в соответствии с Регламентом.
3. В результате успешного исполнения заявки изменения данных ИС внесены в регистр информационных систем.

Удаление данных об ИС

1. ОИВ (оператор ИС) подаёт оператору ЕСИА *заявку на удаление данных об ИС* (форма заявки приведена в Регламенте) из ЕСИА. Заявка должна содержать описание причины (например, прекращение эксплуатации ИС) и должна быть утверждена уполномоченным заместителем руководителя ОИВ.
2. Удаление данных об ИС осуществляется в соответствии с Регламентом.
3. В результате успешного исполнения заявки:
   - все предоставленные пользователям ЕСИА полномочия данной ИС отозваны;
   - данные об ИС удалены из регистра информационных систем.

3.4 Ведение полномочий должностных лиц ОИВ

Ведение полномочий должностных лиц включает следующие операции:

- предоставление полномочия должностному лицу;
- отзыв полномочия у должностного лица;
- получение информации о предоставленных должностному лицу полномочиях.

[10] Если ИС была ранее зарегистрирована в СМЭВ, то сохраняется присвоенная ей при регистрации в СМЭВ мнемоника ИС

3.4.1 Типы полномочий в ЕСИА

В ЕСИА выделено два типа полномочий должностных лиц ОИВ, отражающих специфику выполнения операций по их предоставлению/отзыву и предоставлению информации о полномочиях:

- базовые полномочия должностных лиц;
- полномочия должностных лиц в отношении систем.

Базовые полномочия

Базовые полномочия должностных лиц включают следующие полномочия:

- полномочие *администратора профиля ОИВ*;
- полномочие на *подписание межведомственного запроса*;
- полномочие на *предоставление ответа на межведомственный запрос*;
- полномочие на *подписание результата оказания услуги*.

Информационные системы ОИВ, зарегистрированные в ЕСИА, могут использовать электронные сервисы ЕСИА для предоставления и отзыва базовых полномочий должностным лицам своего ОИВ и для получения информации о базовых полномочиях должностных лиц своего и любых других ОИВ.

Особенности выполнения операций с базовыми полномочиями:

- операция по предоставлению/отзыву базовых полномочий должностному лицу ОИВ может быть выполнена только от имени *администратора профиля* того же ОИВ или вышестоящего ОИВ;
- операция по получению информации о базовых полномочиях должностного лица ОИВ может быть выполнена от имени *администратора профиля* любого ОИВ.

Полномочия в отношении систем

Полномочия в отношении систем определяются операторами соответствующих ИС следующим образом:

1. Если при подаче заявки на регистрацию ИС оператор ИС включил в заявку перечень полномочий ИС, то оператор ЕСИА создаёт в ЕСИА справочник полномочий ИС.
2. После регистрации ИС и создания справочника полномочий, оператор ИС (его информационная система) может использовать электронные сервисы ЕСИА для выполнения операций с полномочиями в отношении своей ИС.

Особенности выполнения операций с полномочиями в отношении систем:

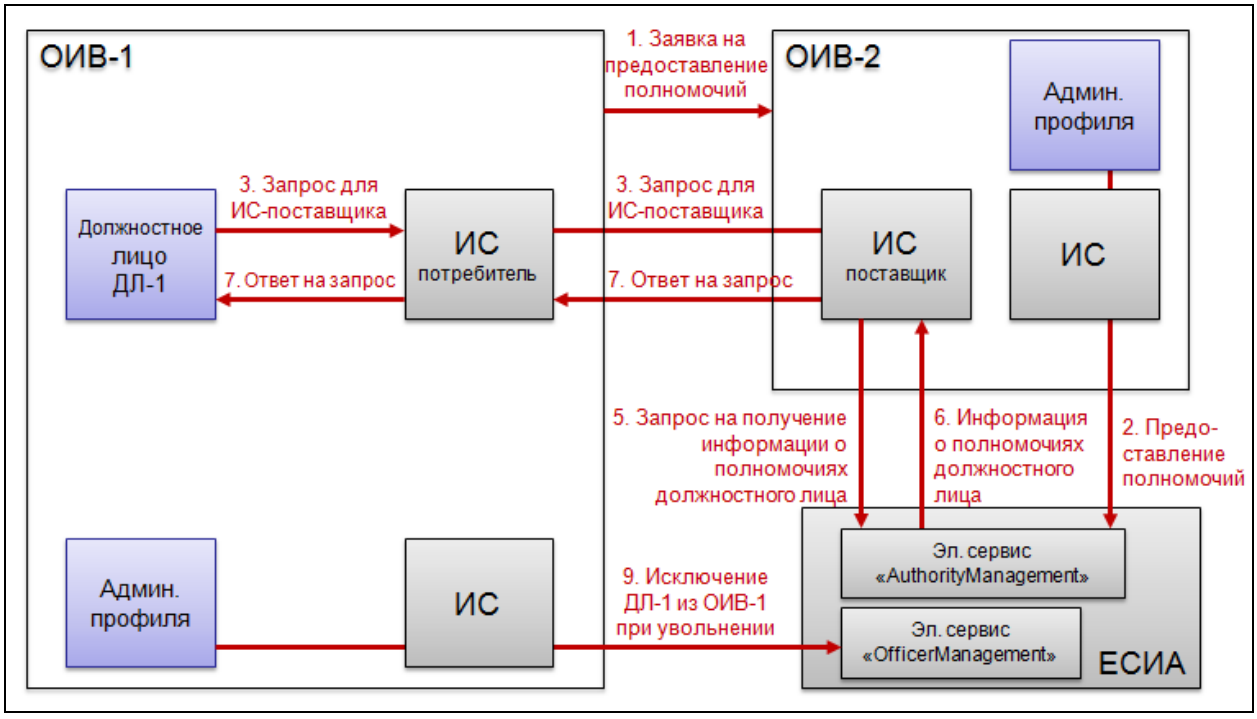
- все операции[11] с полномочиями в отношении систем могут быть выполнены только от имени *администратора профиля* ОИВ, являющегося оператором ИС, или *администратора профиля* вышестоящего ОИВ.

В качестве примера для пояснения использования полномочий в отношении систем приведем следующий сценарий использования полномочий при межведомственном взаимодействии.

Предварительные условия для реализации сценария:

- ОИВ-1 зарегистрирован в ЕСИА (см. раздел 3.1).
- ОИВ-1 является оператором ИС-потребителя. ОИВ-1 зарегистрировал в ЕСИА ИС-потребителя (см. раздел 3.3).
- Администратор профиля ОИВ-1 зарегистрировал в ЕСИА пользователя ДЛ-1 в качестве должностного лица ОИВ-1 (см. раздел 3.2)
- ОИВ-2 зарегистрирован в ЕСИА (см. раздел 3.1).
- ОИВ-2 является оператором ИС-поставщика. ОИВ-2 зарегистрировал в ЕСИА ИС-поставщика и справочник полномочий ИС-поставщика. В справочнике полномочий есть полномочие ПЛН-2 (см. раздел 3.3).

Сценарий:



[11] Предоставление и отзыв полномочий, получение информации о предоставленных полномочиях

1. ОИВ-1 запросил у ОИВ-2 предоставить должностному лицу ДЛ-1 из ОИВ-1 полномочие ПЛН-2 в отношении ИС-поставщика.
2. Администратор профиля ОИВ-2, используя электронный сервис AuthorityManagement (см. раздел 3.4.2), предоставил полномочие ПЛН-2 должностному лицу ОИВ-1.
3. ДЛ-1 с использованием ИС-потребителя направляет запрос ИС-поставщику.
4. ИС-поставщик извлекает из запроса сведения о должностном лице, отправившем запрос:
   - идентификатор пользователя как физического лица – СНИЛС;
   - идентификатор ОИВ, в котором пользователь является должностным лицом, – ОГРН.
5. ИС-поставщик, используя электронный сервис AuthorityManagement, направляет в ЕСИА запрос на получение информации о полномочиях пользователя в отношении ИС-поставщика.
6. ЕСИА передаёт в ИС-поставщик данные о том, что должностное лицо ОИВ-1 обладает полномочием ПЛН-2.
7. ИС-поставщик на основании полученных из ЕСИА данных о полномочиях должностного лица авторизует запрос должностного лица ОИВ-1.
8. Спустя некоторое время ДЛ-1 увольняется из ОИВ-1.
9. Администратор профиля ОИВ-1 в ЕСИА при увольнении ДЛ-1 исключает его учетную запись из ОИВ-1. ЕСИА автоматически отзывает все полномочия ДЛ-1, в том числе и полномочия в отношении ИС-поставщика.
10. ДЛ-1 больше не может получить доступ к ИС-поставщику.

3.4.2 Ведение полномочий должностных лиц ОИВ с помощью электронных сервисов ЕСИА

Для ведения полномочий должностных лиц (базовых полномочий и полномочий в отношении систем) следует использовать следующие электронные сервисы ЕСИА:

- AuthorityManagement (см. раздел А.4);
- Request (см. раздел А.3).

Электронные сервисы ЕСИА являются специализированными сервисами, не относящимися к СМЭВ и работающими по стандарту вызова электронных сервисов ЕСИА. Описание электронных сервисов ЕСИА размещено в разделе Приложение А.

Далее рассмотрены сценарии использования электронных сервисов ЕСИА для выполнения операций по предоставлению/отзыву полномочий и получению информации о предоставленных полномочиях.

Предоставление полномочия должностному лицу

1. ИС ОИВ вызывает операцию grantAuthority электронного сервиса AuthorityManagement и передаёт идентификатор пользователя ЕСИА, которому нужно предоставить полномочие и идентификационные данные полномочия, которое нужно предоставить.
2. Электронный сервис создаёт в ЕСИА заявку на предоставление полномочия и, при успешном создании заявки, возвращает в ИС ОИВ идентификатор заявки.
3. При успешном выполнении заявки статус заявки изменяется на «Успешно выполнена».
4. ИС ОИВ вызывает операцию getStatus электронного сервиса Request и передаёт идентификатор заявки.
5. Электронный сервис возвращает текущий статус обработки заявки.

Отзыв полномочия у должностного лица[12]

1. ИС ОИВ вызывает операцию revokeAuthority электронного сервиса AuthorityManagement и передаёт идентификатор пользователя ЕСИА, у которого нужно отозвать полномочие и идентификационные данные полномочия, которое нужно отозвать.
2. Электронный сервис создаёт в ЕСИА заявку на отзыв полномочия и, при успешном создании заявки, возвращает в ИС ОИВ идентификатор заявки.
3. При успешном выполнении заявки статус заявки изменяется на «Успешно выполнена».
4. ИС ОИВ вызывает getStatus электронного сервиса Request и передаёт идентификатор заявки.
5. Электронный сервис возвращает текущий статус обработки заявки.

Получение информации о полномочиях должностного лица

Для получения информации о базовых полномочиях должностного лица:

[12] ЕСИА также автоматически отзывает все полномочия должностного лица при исключении его из ОИВ (см. раздел 3.2).

1. ИС ОИВ вызывает операцию getBaseAuthority электронного сервиса AuthorityManagement и передаёт идентификатор пользователя ЕСИА, ОГРН организации (в которой пользователь является должностным лицом).
2. Электронный сервис возвращает перечень базовых полномочий указанного пользователя.

Для получения информации о полномочиях должностного лица в отношении системы:

1. ИС ОИВ вызывает операцию getSystemAuthority электронного сервиса AuthorityManagement и передаёт идентификатор пользователя ЕСИА, ОГРН организации (в которой пользователь является должностным лицом), идентификатор системы.
2. Электронный сервис возвращает перечень полномочий указанного пользователя по отношению к указанной системе.

4 Использование ЕСИА при взаимодействии информационных систем с использованием СМЭВ

В соответствии с п. 1.4 (в) Положения, ЕСИА используется при межведомственном электронном взаимодействии.

В текущем разделе рассмотрено, каким образом в ЕСИА осуществляется:

- регистрация информационных систем, взаимодействующих с использованием СМЭВ;
- авторизация информационных систем при межведомственном взаимодействии.

4.1 Регистрация информационных систем

Регистрация ИС, использующей электронные сервисы СМЭВ, выполняется оператором СМЭВ в соответствии с *«Регламентом взаимодействия Участников информационного взаимодействия, Оператора единой системы межведомственного электронного взаимодействия и Оператора эксплуатации инфраструктуры электронного правительства при организации межведомственного взаимодействия с использованием единой системы межведомственного электронного взаимодействия»*.

4.2 Идентификация, аутентификация, авторизация информационных систем при межведомственном взаимодействии с использованием СМЭВ

При взаимодействии ИС-потребителя с ИС-поставщиком с использованием СМЭВ сервис регламентации доступа СМЭВ последовательно выполняет следующие операции, связанные с идентификацией ИС-потребителя:

1. Сервис регламентации доступа СМЭВ (далее – СРД) выполняет проверку соответствия ЭП передаваемому сообщению.
2. СРД взаимодействует через ЕСИА с сервисом проверки электронной подписи ИС ГУЦ для проверки действительности сертификата ЭП.
3. СРД выполняет контроль доступа ИС-потребителя к ИС-поставщику. Для этого СРД взаимодействует с сервисом проверки прав доступа ЕСИА.

4. Сервис прав доступа ЕСИА осуществляет проверку наличия в регистре ИС ЕСИА записи об ИС и предоставляет информацию о её полномочиях.
5. На основании этой информации СРД авторизует ИС-потребителя.
6. СМЭВ выполняет дальнейшие шаги по передаче сообщения ИС-поставщику.

Редактирование полномочий ИС-потребителей СМЭВ выполняется оператором СМЭВ через защищённый контур Техпортала СМЭВ.

Информация о полномочиях ИС-потребителей к электронным сервисам ИС-поставщика указывается поставщиком сервиса данной ИС в паспорте электронного сервиса и передается оператору СМЭВ.

Приложение А. Электронные сервисы ЕСИА

А.1 Авторизация при вызове электронных сервисов ЕСИА

При вызове электронных сервисов ЕСИА выполняется авторизация в соответствии со следующими правилами:

- Вызов любого электронного сервиса ЕСИА производится от имени определенного должностного лица ОИВ.
- При вызове любых операций электронного сервиса OfficerManagement выполняется проверка, что должностное лицо ОИВ, вызывающее сервис, обладает полномочиями *администратора профиля ОИВ* в рамках того ОИВ, в котором в рамках операции регистрируется/изменяется/исключается должностное лицо.
- При вызове операций электронного сервиса AuthorityManagement:
  - при вызове любых операций с полномочиями в отношении систем выполняется проверка, что должностное лицо ОИВ, вызывающее сервис, обладает полномочиями *администратора профиля ОИВ* в рамках того ОИВ, к информационной системе которого в рамках операции предоставляется/отзывается полномочие должностного лица или запрашивается информация о полномочиях должностных лиц к данной системе;
  - при вызове операций по предоставлению/отзыву базовых полномочий выполняется проверка, что должностное лицо ОИВ, вызывающее сервис, обладает полномочиями *администратора профиля ОИВ* в рамках того ОИВ, в котором должностному лицу предоставляются/отзываются базовые полномочия;
  - при вызове операций по получению информации о базовых полномочиях электронного сервиса AuthorityManagement выполняется проверка, что должностное лицо ОИВ, вызывающее сервис, обладает полномочиями *администратора профиля любого ОИВ*.
- При вызове операций электронного сервиса Request выполняется проверка, что должностное лицо ОИВ, вызывающее сервис, является владельцем заявки, по которой выполняется операция.

В целях осуществления системой ЕСИА идентификации вызывающего электронный сервис должностного лица, его ОИВ и информационной системы,

осуществляющей вызов сервиса от имени должностного лица, в ЕСИА предусмотрено два доступных режима вызова электронных сервисов:

- режим 1 — с использованием WS-Security и неквалифицированной электронной подписи информационной системы в соответствии с алгоритмами RSA, SHA-1;
- режим 2 — с использованием WS-Security и неквалифицированной электронной подписи информационной системы в соответствии с алгоритмами RSA, SHA-1, а также, дополнительной квалифицированной электронной подписи, сертификат которой признается действительным в ИС ГУЦ.

Режим 1 действует в качестве временного и обусловлен необходимостью обеспечить возможность упрощенного взаимодействия с электронными сервисами ЕСИА для информационных систем (ИС управления персоналом, ИС управления идентификационными данными и другие ИС), реализованных с использованием, в том числе, зарубежного общего и прикладного программного обеспечения, не позволяющего использовать сертифицированные в РФ алгоритмы формирования и проверки электронной подписи.

Для вызова электронного сервиса ЕСИА информационная система должна сформировать сообщение вызова, соответствующее следующим требованиям:

- Информационной системой **должен** быть сформирован и добавлен к сообщению вызова электронного сервиса заголовок WS-Security, содержащий СНИЛС должностного лица ОИВ (в токене UsernameToken в атрибуте Username) и подписанный неквалифицированной электронной подписью информационной системы, установленной на:
  - метку времени заголовка WS-Security;
  - токен WS-Security;
  - тело сообщения вызова электронного сервиса ЕСИА.
- Информационной системой **может** быть сформирован и добавлен к сообщению вызова электронного сервиса заголовок ESIA, содержащий квалифицированную электронную подпись информационной системы, установленную на:
  - заголовок WS-Security;
  - тело сообщения вызова электронного сервиса ЕСИА.
- Неквалифицированная электронная подпись **должна** быть сформирована с использованием сертификата ИС в формате X.509 версии 3 алгоритма RSA с длиной ключа 1024 бит, предварительно зарегистрированного в ЕСИА в регистре информационных систем.

- Квалифицированная электронная подпись, в случае ее установки, **должна** быть сформирована с использованием сертификата ИС, проходящего проверку подлинности в ИС ГУЦ. Предварительная регистрация этого сертификата в ЕСИА в регистре информационных систем не требуется.
- Квалифицированная и неквалифицирвоанная электронные подписи информационной системы должны быть помещены в сообщение в формате xmldsig. Должен использоваться алгоритм xml-ext-c14n каноникализации XML-сообщения Для неквалифицированной электронной подписи должны использоваться алгоритмы RSA и SHA-1 формирования криптографического хэш и электронной подписи. Для квалифицированной электронной подписи должны использоваться алгоритмы ГОСТ Р 3410-2001 формирования электронной подписи и ГОСТ Р 3411 формирования криптографического хэша. Значения электронной подписи и криптографических хэш должны помещаться в сообщение в формате Base64.

Пример корректного заголовка сообщения вызова электронного сервиса ЕСИА приведен ниже:

```
<?xml version='1.0' encoding='UTF-8'?>
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
  <S:Header>
    <esia:Security
      xmlns:esia="http://esia.gosuslugi.ru/2012/04/eservice">
      <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">

        <dsig:SignedInfo>
          <dsig:CanonicalizationMethod
            Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          <dsig:SignatureMethod
            Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411"/>

          <dsig:Reference URI="#ESIA_WS_SECURITY_HEADER">
            <dsig:Transforms>
              <dsig:Transform
                  Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </dsig:Transforms>
            <dsig:DigestMethod
              Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>
            <dsig:DigestValue>
              Значение хэша WS-Security заголовка сообщения в формате Base64
            </dsig:DigestValue>
          </dsig:Reference>

          <dsig:Reference URI="#ESIA_API_CALL_BODY_REFERENCE">
            <dsig:Transforms>
              <dsig:Transform
                Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </dsig:Transforms>
            <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>
            <dsig:DigestValue>
              Значение хэша тела вызова электронного сервиса ЕСИА в формате Base64
            </dsig:DigestValue>
          </dsig:Reference>
        </dsig:SignedInfo>

        <dsig:SignatureValue>
           Значение подписи в формате Base64
        </dsig:SignatureValue>
      </dsig:Signature>
```

```
    </esia:Security>

    <wsse:Security
       xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd"
       S:mustUnderstand="1"
       wsu:Id="ESIA_WS_SECURITY_REFERENCE">

       <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
         <dsig:SignedInfo>
           <dsig:CanonicalizationMethod
             Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
           <dsig:SignatureMethod
             Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
           <dsig:Reference URI="#TIMESTAMP_REFERENCE">
             <dsig:Transforms>
               <dsig:Transform
                 Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
             </dsig:Transforms>
             <dsig:DigestMethod
               Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
             <dsig:DigestValue>
               Значение хэша метки времени в формате Base64
             </dsig:DigestValue>
           </dsig:Reference>

           <dsig:Reference URI="#ESIA_API_CALL_BODY_REFERENCE">
             <dsig:Transforms>
               <dsig:Transform
                 Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
             </dsig:Transforms>
             <dsig:DigestMethod
               Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
             <dsig:DigestValue>
               Значение хэша тела вызова электронного сервиса ЕСИА в формате Base64
             </dsig:DigestValue>
           </dsig:Reference>

           <dsig:Reference URI="#ESIA_SECURITY_TOKEN">
             <dsig:Transforms>
               <dsig:Transform
                 Algorithm="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
message-security-1.0#STR-Transform">
                 <wsse:TransformationParameters>
                   <dsig:CanonicalizationMethod
                     Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                 </wsse:TransformationParameters>
               </dsig:Transform>
             </dsig:Transforms>
             <dsig:DigestMethod
               Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
             <dsig:DigestValue>
               Значение хэша токена безопасности ЕСИА в формате Base64
             </dsig:DigestValue>
           </dsig:Reference>
         </dsig:SignedInfo>
         <dsig:SignatureValue>
           Значение подписи WS-Security в формате Base64
         </dsig:SignatureValue>
         <dsig:KeyInfo>
           <wsse:SecurityTokenReference
             xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd"
             wsu:Id="ESIA_SECURITY_TOKEN">
             <X509Data xmlns="http://www.w3.org/2000/09/xmldsig#">
               <X509IssuerSerial>
                 <X509IssuerName>
                   CommonName УЦ, выпустившего сертификат RSA
                 </X509IssuerName>
                 <X509SerialNumber>
                   Серийный номер сертификата RSA
                 </X509SerialNumber>
               </X509IssuerSerial>
             </X509Data>
           </wsse:SecurityTokenReference>
         </dsig:KeyInfo>
       </dsig:Signature>

       <wsse:UsernameToken
```

```
         xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"
         wsu:Id="ESIA_SECURITY_TOKEN">
         <wsse:Username>
            СНИЛС должностного лица, от имени которого идет вызов электронного сервиса ЕСИА (в
формате XXX-XXX-XXX XX)
         </wsse:Username>
       </wsse:UsernameToken>

       <wsu:Timestamp
         xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"
         wsu:Id="TIMESTAMP_REFERENCE">
         <wsu:Created>
           Время формирования сообщения, например, 2012-04-04T15:40:35Z
         </wsu:Created>
         <wsu:Expires>
           Время окончания срока действия сообщения, например, 2012-04-04T15:41:35Z
         </wsu:Expires>
       </wsu:Timestamp>
     </wsse:Security>
   </S:Header>

   <S:Body
     xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"
     wsu:Id="ESIA_API_CALL_BODY_REFERENCE">
       Тело сообщения вызова сервиса
    </S:Body>
</S:Envelope>
```

При получении сообщения ЕСИА выполняет следующие операции:

1. В случае наличия в сообщении квалифицированной электронной подписи выполняет проверку соответствия сообщения и его квалифицированной электронной подписи, а также проверку действительности сертификата квалифицированной электронной подписи через взаимодействие с ИС ГУЦ.
2. Проверяет соответствие сообщения и его неквалифицированной электронной подписи.
3. Проверяет, что сертификат, использованный для формирования неквалифицированной электронной подписи сообщения, зарегистрирован в ЕСИА.
4. Проверяет, что срок действия сообщения не истек (по временной метке Expired).
5. Осуществляет выборку информационной системы, соответствующей сертификату, а также определяет по информационной системе тот ОИВ, к которому принадлежит система.
6. Выбирает из заголовка сообщения данные о СНИЛС должностного лица ОИВ (токен UsernameToken, атрибут Username).
7. Выполняет проверку наличия у должностного лица ОИВ полномочий на выполнение запрошенной операции.
8. Выполняет запрошенную операцию от имени должностного лица в случае достаточности его полномочий.
9. Формирует ответ, в который включает заголовок WS-Security, подписанный технологической неквалифицированной электронной подписью ЕСИА. Сообщение

с ответом выглядит также как и сообщение с запросом, но не содержит тэга с токеном UsernameToken.

10. В случае если запрос электронного сервиса ЕСИА был сформирован с добавлением квалифицированной электронной подписи информационной системы, то ЕСИА также подписывает сообщение с ответом своей квалифицированной электронной подписью.

Оператор информационной системы самостоятельно принимает решение, должна ли его информационная система выполнять проверку квалифицированной и неквалифицированной электронной подписи ЕСИА в ответных сообщениях.

A.2 Электронный сервис OfficerManagement

Наименование	Формирование и ведение регистра должностных лиц ОИВ
Код	OfficerManagement
Назначение	Создание, изменение, удаление записей регистра должностных лиц ОИВ в ЕСИА

A.2.1 Операции

Операция	**Назначение**
regOfficer	Создание в ЕСИА заявки на регистрацию должностного лица. Метод принимает на вход данные регистрируемого должностного лица.
modifyOfficerData	Изменение служебных данных должностного лица.
dismissOfficer	Исключение должностного лица из ОИВ.

A.2.1.1 Операция regOfficer

Наименование	Создание заявки на регистрацию должностного лица
Код	regOfficer
Назначение	Создание в ЕСИА заявки на регистрацию должностного лица. Метод принимает на вход данные регистрируемого должностного лица. Если в ЕСИА уже зарегистрирован пользователь с таким СНИЛС, то в результате выполнения заявки его учетная запись будет присоединена к ОИВ, но личные данные обновлены не будут.

Входные данные: regOfficerRequest

Код параметра	**Описание параметра**	**Обязательность**
snils	СНИЛС	+
agencyOGRN	ОГРН организации	+
fullName	ФИО	+
gender	Пол	+
birthDate	Дата рождения	+
inn	ИНН	-
passport	Паспорт гражданина РФ	+
department	Подразделение	-
position	Должность	-
officialEmail	Служебный адрес электронной почты	+
description	Комментарий	-

Выходные данные: regOfficerResponse

Код параметра	**Описание**	**Обязательность**
requestId	Идентификатор заявки	-[13]

Сообщение об ошибке: fault

Код параметра	**Описание**	**Обязательность**
faultElem	Идентификатор ошибки	-[14]

[13] Возвращается в случае успешного выполнения вызова
[14] Возвращается в случае возникновения ошибки при обработке вызова

A.2.1.2 Операция modifyOfficerData

Наименование	Создание заявки на изменение данных должностного лица ОИВ
Код	modifyOfficerData
Назначение	Создание в ЕСИА заявки на изменение служебных данных должностного лица.

Входные данные: modifyOfficerDataRequest

Код параметра	**Описание**	**Обязательность**
snils	СНИЛС	+
agencyOGRN	ОГРН организации	+
department	Подразделение	-
position	Должность	-
officialEmail	Служебный адрес электронной почты	+
description	Комментарий	-

Выходные данные: modifyOfficerDataResponse

Код параметра	**Описание**	**Обязательность**
requestId	Идентификатор заявки	-

Сообщение об ошибке: fault

Код параметра	**Описание**	**Обязательность**
faultElem	Идентификатор ошибки	-

A.2.1.3 Операция dismissOfficer

Наименование	Создание заявки на исключение записи из регистра должностных лиц ОИВ
Код	dismissOfficer
Назначение	Создание в ЕСИА заявки на отсоединение учетной записи физического лица от ОИВ.

Входные данные: dismissOfficerRequest

Код параметра	**Описание**	**Обязательность**
snils	СНИЛС	+

agencyOGRN	ОГРН организации	+

Выходные данные: dismissOfficerResponse

Код параметра	Описание	Обязательность
requestId	Идентификатор заявки	-

Сообщение об ошибке: fault

Код параметра	Описание	Обязательность
faultElem	Идентификатор ошибки	-

A.2.2 Описание сервиса (WSDL)

```
<?xml version='1.0' encoding='UTF-8'?>
<definitions xmlns:wssutil="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" xmlns:wsp="http://www.w3.org/ns/ws-policy"
xmlns:wsp1_2="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:tns="http://esia.atc.ru/ws/agency/officerManagement/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://schemas.xmlsoap.org/wsdl/"
targetNamespace="http://esia.atc.ru/ws/agency/officerManagement/" name="OfficerManagerService">
    <wsp:UsingPolicy wssutil:Required="true"/>
    <wsp1_2:Policy wssutil:Id="defaultpolicy">
        <ns1:AsymmetricBinding xmlns:ns1="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702">
            <wsp1_2:Policy>
                <ns1:InitiatorToken>
                    <wsp1_2:Policy>
                        <ns1:X509Token ns1:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                            <wsp1_2:Policy>
                                <ns1:WssX509V3Token10/>
                            </wsp1_2:Policy>
                        </ns1:X509Token>
                    </wsp1_2:Policy>
                </ns1:InitiatorToken>
                <ns1:RecipientToken>
                    <wsp1_2:Policy>
                        <ns1:X509Token ns1:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never">
                            <wsp1_2:Policy>
                                <ns1:WssX509V3Token10/>
                            </wsp1_2:Policy>
                        </ns1:X509Token>
                    </wsp1_2:Policy>
                </ns1:RecipientToken>
                <ns1:AlgorithmSuite>
                    <wsp1_2:Policy>
                        <ns1:Basic256/>
                    </wsp1_2:Policy>
                </ns1:AlgorithmSuite>
                <ns1:IncludeTimestamp/>
                <ns1:ProtectTokens/>
                <ns1:OnlySignEntireHeadersAndBody/>
            </wsp1_2:Policy>
        </ns1:AsymmetricBinding>
        <ns2:SignedSupportingTokens xmlns:ns2="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702">
            <wsp1_2:Policy>
                <ns2:UsernameToken ns2:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                    <wsp1_2:Policy>
                        <ns2:NoPassword/>
                    </wsp1_2:Policy>
```

```
                </ns2:UsernameToken>
            </wsp1_2:Policy>
        </ns2:SignedSupportingTokens>
        <ns3:Wss11 xmlns:ns3="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
            <wsp1_2:Policy>
                <ns3:MustSupportRefIssuerSerial/>
            </wsp1_2:Policy>
        </ns3:Wss11>
    </wsp1_2:Policy>
    <types>
        <xsd:schema>
            <xsd:import namespace="http://esia.atc.ru/ws/types/simple/error/"
schemaLocation="http://172.18.5.127:7001/OfficerManager/OfficerManagerService?xsd=1"/>
        </xsd:schema>
        <xsd:schema>
            <xsd:import namespace="http://esia.atc.ru/ws/agency/officerManagement/"
schemaLocation="http://172.18.5.127:7001/OfficerManager/OfficerManagerService?xsd=2"/>
        </xsd:schema>
        <xsd:schema>
            <xsd:import namespace="http://esia.atc.ru/ws/types/complex/common/"
schemaLocation="http://172.18.5.127:7001/OfficerManager/OfficerManagerService?xsd=3"/>
        </xsd:schema>
        <xsd:schema>
            <xsd:import namespace="http://esia.atc.ru/ws/types/simple/simple/"
schemaLocation="http://172.18.5.127:7001/OfficerManager/OfficerManagerService?xsd=4"/>
        </xsd:schema>
    </types>
    <message name="createOfficer">
        <part name="createOfficerRequest" element="tns:createOfficerRequest"/>
    </message>
    <message name="createOfficerResponse">
        <part name="createOfficerResponse" element="tns:createOfficerResponse"/>
    </message>
    <message name="Fault">
        <part xmlns:ns4="http://esia.atc.ru/ws/types/simple/error/" name="fault"
element="ns4:faultElem"/>
    </message>
    <message name="modifyOfficerData">
        <part name="modifyOfficerDataRequest" element="tns:modifyOfficerDataRequest"/>
    </message>
    <message name="modifyOfficerDataResponse">
        <part name="modifyOfficerDataResponse" element="tns:modifyOfficerDataResponse"/>
    </message>
    <message name="deleteOfficer">
        <part name="deleteOfficerRequest" element="tns:deleteOfficerRequest"/>
    </message>
    <message name="deleteOfficerResponse">
        <part name="deleteOfficerResponse" element="tns:deleteOfficerResponse"/>
    </message>
    <portType name="OfficerManagement">
        <operation name="createOfficer">
            <input wsam:Action="createOfficer" message="tns:createOfficer"/>
            <output
wsam:Action="http://esia.atc.ru/ws/agency/officerManagement/OfficerManagement/createOfficerRespon
se" message="tns:createOfficerResponse"/>
            <fault message="tns:Fault" name="Fault"
wsam:Action="http://esia.atc.ru/ws/agency/officerManagement/OfficerManagement/createOfficer/Fault
/Fault"/>
        </operation>
        <operation name="modifyOfficerData">
            <input wsam:Action="modifyOfficerData" message="tns:modifyOfficerData"/>
            <output
wsam:Action="http://esia.atc.ru/ws/agency/officerManagement/OfficerManagement/modifyOfficerDataRe
sponse" message="tns:modifyOfficerDataResponse"/>
            <fault message="tns:Fault" name="Fault"
wsam:Action="http://esia.atc.ru/ws/agency/officerManagement/OfficerManagement/modifyOfficerData/F
ault/Fault"/>
        </operation>
        <operation name="deleteOfficer">
            <input wsam:Action="deleteOfficer" message="tns:deleteOfficer"/>
            <output
wsam:Action="http://esia.atc.ru/ws/agency/officerManagement/OfficerManagement/deleteOfficerRespon
se" message="tns:deleteOfficerResponse"/>
            <fault message="tns:Fault" name="Fault"
wsam:Action="http://esia.atc.ru/ws/agency/officerManagement/OfficerManagement/deleteOfficer/Fault
/Fault"/>
        </operation>
    </portType>
    <binding name="OfficerManagementPortBinding" type="tns:OfficerManagement">
```

```
        <wsp:PolicyReference URI="#defaultpolicy"/>
        <soap:binding transport="http://schemas.xmlsoap.org/soap/http" style="document"/>
        <operation name="createOfficer">
            <soap:operation soapAction="createOfficer"/>
            <input>
                <soap:body use="literal"/>
            </input>
            <output>
                <soap:body use="literal"/>
            </output>
            <fault name="Fault">
                <soap:fault name="Fault" use="literal"/>
            </fault>
        </operation>
        <operation name="modifyOfficerData">
            <soap:operation soapAction="modifyOfficerData"/>
            <input>
                <soap:body use="literal"/>
            </input>
            <output>
                <soap:body use="literal"/>
            </output>
            <fault name="Fault">
                <soap:fault name="Fault" use="literal"/>
            </fault>
        </operation>
        <operation name="deleteOfficer">
            <soap:operation soapAction="deleteOfficer"/>
            <input>
                <soap:body use="literal"/>
            </input>
            <output>
                <soap:body use="literal"/>
            </output>
            <fault name="Fault">
                <soap:fault name="Fault" use="literal"/>
            </fault>
        </operation>
    </binding>
    <service name="OfficerManagerService">
        <port name="OfficerManagementPort" binding="tns:OfficerManagementPortBinding">
            <soap:address
location="http://172.18.5.127:7001/OfficerManager/OfficerManagerService"/>
        </port>
    </service>
</definitions>
```

A.3 Электронный сервис Request

Наименование	Заявки ЕСИА
Код	Request
Назначение	Проверка статуса заявки в ЕСИА

A.3.1 Операции

Операция	**Назначение**
getStatus	Проверка статуса заявки.

A.3.1.1 Операция getStatus

Наименование	Проверка статуса заявки
Код	getStatus
Назначение	Получение текущего статуса заявки. Метод принимает на вход идентификатор заявки.

Входные данные: getStatusRequest

Код параметра	**Описание параметра**	**Обязательность**
requestId	Идентификатор заявки	+

Выходные данные: getStatusResponse

Код параметра	**Описание**	**Обязательность**
status	Статус	-

Сообщение об ошибке: fault

Код параметра	**Описание**	**Обязательность**
faultElem	Идентификатор ошибки	-

A.3.2 Описание сервиса (WSDL)

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<wsdl:definitions name="Request"
                  targetNamespace="http://esia.atc.ru/ws/agency/request/"
                                  xmlns:wssutil="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd"
                                  xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
                  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
                  xmlns:tns="http://esia.atc.ru/ws/agency/request/"
                  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
                  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  xmlns:stypes="http://esia.atc.ru/ws/types/simple/simple/"
                  xmlns:error="http://esia.atc.ru/ws/types/simple/error/">
       <wsp:Policy wssutil:Id="usernametoken">
        <ns1:AsymmetricBinding xmlns:ns1="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702">
            <wsp:Policy>
                <ns1:InitiatorToken>
                    <wsp:Policy>
                        <ns1:X509Token ns1:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                            <wsp:Policy>
                                <ns1:WssX509V3Token10/>
                            </wsp:Policy>
                        </ns1:X509Token>
                    </wsp:Policy>
                </ns1:InitiatorToken>
                <ns1:RecipientToken>
                    <wsp:Policy>
                        <ns1:X509Token ns1:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never">
                            <wsp:Policy>
                                <ns1:WssX509V3Token10/>
                            </wsp:Policy>
                        </ns1:X509Token>
                    </wsp:Policy>
                </ns1:RecipientToken>
                <ns1:AlgorithmSuite>
```

```
                    <wsp:Policy>
                        <ns1:Basic256/>
                    </wsp:Policy>
                </ns1:AlgorithmSuite>
                <ns1:IncludeTimestamp/>
                <ns1:ProtectTokens/>
                <ns1:OnlySignEntireHeadersAndBody/>
            </wsp:Policy>
        </ns1:AsymmetricBinding>
        <ns2:SignedSupportingTokens xmlns:ns2="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702">
            <wsp:Policy>
                <ns2:UsernameToken ns2:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                    <wsp:Policy>
                        <ns2:NoPassword/>
                    </wsp:Policy>
                </ns2:UsernameToken>
            </wsp:Policy>
        </ns2:SignedSupportingTokens>
        <ns3:Wss11 xmlns:ns3="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
            <wsp:Policy>
                <ns3:MustSupportRefIssuerSerial/>
            </wsp:Policy>
        </ns3:Wss11>
    </wsp:Policy>

    <wsdl:types>
        <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                    targetNamespace="http://esia.atc.ru/ws/agency/request/">
            <xsd:import namespace="http://esia.atc.ru/ws/types/simple/simple/"
schemaLocation="types/simple/common.xsd"/>
            <xsd:import namespace="http://esia.atc.ru/ws/types/simple/error/"
schemaLocation="types/simple/error.xsd"/>

            <xsd:complexType name="GetStatusRequest">
                <xsd:sequence>
                    <xsd:element name="requestId" type="xsd:long"/>
                </xsd:sequence>
            </xsd:complexType>

            <xsd:complexType name="GetStatusResponse">
                <xsd:sequence>
                    <xsd:element name="status" type="stypes:RequestStatus"/>
                </xsd:sequence>
            </xsd:complexType>

            <xsd:element name="getStatusRequest" type="tns:GetStatusRequest"/>
            <xsd:element name="getStatusResponse" type="tns:GetStatusResponse"/>
        </xsd:schema>
    </wsdl:types>

    <wsdl:message name="getStatusRequest">
        <wsdl:part name="getStatusRequest" element="tns:getStatusRequest"/>
    </wsdl:message>

    <wsdl:message name="getStatusResponse">
        <wsdl:part name="getStatusResponse" element="tns:getStatusResponse"/>
    </wsdl:message>

    <wsdl:message name="fault">
        <wsdl:part name="fault" element="error:faultElem"/>
    </wsdl:message>

    <wsdl:portType name="Request">
        <wsdl:operation name="getStatus">
            <wsdl:input message="tns:getStatusRequest"/>
            <wsdl:output message="tns:getStatusResponse"/>
            <wsdl:fault name="fault" message="tns:fault"/>
        </wsdl:operation>
    </wsdl:portType>

    <wsdl:binding name="RequestSOAP" type="tns:Request">
               <wsp:PolicyReference URI="#usernametoken"/>
        <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
        <wsdl:operation name="getStatus">
            <soap:operation soapAction="createOfficer"/>
            <wsdl:input>
                <soap:body use="literal"/>
```

```
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="fault">
                <soap:fault name="fault" use="literal"/>
            </wsdl:fault>
        </wsdl:operation>
    </wsdl:binding>

    <wsdl:service name="Request">
        <wsdl:port binding="tns:RequestSOAP" name="Request">
            <soap:address location=""/>
        </wsdl:port>
    </wsdl:service>
</wsdl:definitions>
```

A.4 Электронный сервис AuthorityManagement

Наименование	Управление полномочиями в ЕСИА
Код	AuthorityManagement
Назначение	Предоставление и отзыв полномочий, получение информации о полномочиях должностного лица

A.4.1 Операции

Операция	**Назначение**
getBaseAuthorities	Получение информации о базовых полномочиях должностного лица
getSystemAuthorities	Получение информации о полномочиях должностного лица в отношении системы
grantAuthority	Предоставление полномочия
revokeAuthority	Отзыв полномочия

A.4.1.1 Операция getBaseAuthorities

Наименование	Получение информации о базовых полномочиях должностного лица
Код	getBaseAuthorities
Назначение	Получение информации о базовых полномочиях должностного лица

Входные данные : getBaseAuthoritiesRequest

Код параметра	**Описание параметра**	**Обязательность**
snils	СНИЛС	+
agencyOgrn	ОГРН организации	+

Выходные данные: getBaseAuthoritiesResponse

Код параметра	Описание	Обязательность
authorities	Список полномочия (и их параметров)	-

Сообщение об ошибке: fault

Код параметра	Описание	Обязательность
faultElem	Идентификатор ошибки	-

A.4.1.2 Операция getSystemAuthorities

Наименование	Получение информации о полномочиях должностного лица на систему
Код	getSystemAuthorities
Назначение	Получение информации о полномочиях должностного лица на систему

Входные данные : getSystemAuthoritiesRequest

Код параметра	Описание параметра	Обязательность
snils	СНИЛС	+
agencyOgrn	ОГРН организации	+
systemExtId	Идентификатор системы	+

Выходные данные: getSystemAuthoritiesResponse

Код параметра	Описание	Обязательность
authorities	Список полномочия (и их параметров)	-

Сообщение об ошибке: fault

Код параметра	Описание	Обязательность
faultElem	Идентификатор ошибки	-

A.4.1.3 Операция grantAuthority

Наименование	Предоставление полномочия
Код	grantAuthority
Назначение	Предоставление полномочия

Входные данные : grantAuthorityRequest

Код параметра	**Описание параметра**	**Обязательность**
snils	СНИЛС	+
agencyOgrn	ОГРН организации	+
authority	Полномочие (с параметрами)	+

Выходные данные: grantAuthorityResponse

Код параметра	**Описание**	**Обязательность**
requestId	Идентификатор заявки	-

Сообщение об ошибке: fault

Код параметра	**Описание**	**Обязательность**
faultElem	Идентификатор ошибки	-

A.4.1.4 Операция revokeAuthority

Наименование	Отзыв полномочия
Код	revokeAuthority
Назначение	Отзыв полномочия

Входные данные : revokeAuthorityRequest

Код параметра	**Описание параметра**	**Обязательность**
snils	СНИЛС	+
agencyOgrn	ОГРН организации	+
authority	Полномочие	+

Выходные данные: revokeAuthorityResponse

Код параметра	**Описание**	**Обязательность**
requestId	Идентификатор заявки	-

Сообщение об ошибке: fault

Код параметра	Описание	Обязательность
faultElem	Идентификатор ошибки	-

A.4.2 Описание сервиса (WSDL)

```
<?xml version='1.0' encoding='UTF-8'?>
<definitions xmlns:wssutil="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd"
             xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd"
             xmlns:wsp="http://www.w3.org/ns/ws-policy"
xmlns:wsp1_2="http://schemas.xmlsoap.org/ws/2004/09/policy"
             xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata"
             xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
             xmlns:tns="http://esia.atc.ru/ws/authz/authorityManagement/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
             xmlns="http://schemas.xmlsoap.org/wsdl/"
targetNamespace="http://esia.atc.ru/ws/authz/authorityManagement/"
             name="AuthorityManagerService">
    <wsp:UsingPolicy wssutil:Required="true"/>
    <wsp1_2:Policy wssutil:Id="defaultpolicy">
        <ns1:AsymmetricBinding xmlns:ns1="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702">
            <wsp1_2:Policy>
                <ns1:InitiatorToken>
                    <wsp1_2:Policy>
                        <ns1:X509Token
                                ns1:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                            <wsp1_2:Policy>
                                <ns1:WssX509V3Token10/>
                            </wsp1_2:Policy>
                        </ns1:X509Token>
                    </wsp1_2:Policy>
                </ns1:InitiatorToken>
                <ns1:RecipientToken>
                    <wsp1_2:Policy>
                        <ns1:X509Token
                                ns1:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never">
                            <wsp1_2:Policy>
                                <ns1:WssX509V3Token10/>
                            </wsp1_2:Policy>
                        </ns1:X509Token>
                    </wsp1_2:Policy>
                </ns1:RecipientToken>
                <ns1:AlgorithmSuite>
                    <wsp1_2:Policy>
                        <ns1:Basic256/>
                    </wsp1_2:Policy>
                </ns1:AlgorithmSuite>
                <ns1:IncludeTimestamp/>
                <ns1:ProtectTokens/>
                <ns1:OnlySignEntireHeadersAndBody/>
            </wsp1_2:Policy>
        </ns1:AsymmetricBinding>
        <ns2:SignedSupportingTokens xmlns:ns2="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702">
            <wsp1_2:Policy>
                <ns2:UsernameToken
                        ns2:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
                    <wsp1_2:Policy>
                        <ns2:NoPassword/>
                    </wsp1_2:Policy>
                </ns2:UsernameToken>
            </wsp1_2:Policy>
        </ns2:SignedSupportingTokens>
        <ns3:Wss11 xmlns:ns3="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
            <wsp1_2:Policy>
                <ns3:MustSupportRefIssuerSerial/>
```

```
            </wsp1_2:Policy>
        </ns3:Wss11>
    </wsp1_2:Policy>
    <types>
        <xsd:schema>
            <xsd:import namespace="http://esia.atc.ru/ws/authz/authorityManagement/"

schemaLocation="http://172.18.4.52:7001/AuthorityManager/AuthorityManagerService?xsd=1"/>
        </xsd:schema>
        <xsd:schema>
            <xsd:import namespace="http://esia.atc.ru/ws/types/simple/error/"

schemaLocation="http://172.18.4.52:7001/AuthorityManager/AuthorityManagerService?xsd=2"/>
        </xsd:schema>
    </types>
    <message name="getSystemAuthorities">
        <part name="getSystemAuthoritiesRequest" element="tns:getSystemAuthoritiesRequest"/>
    </message>
    <message name="getSystemAuthoritiesResponse">
        <part name="getSystemAuthoritiesResponse" element="tns:getSystemAuthoritiesResponse"/>
    </message>
    <message name="Fault">
        <part xmlns:ns4="http://esia.atc.ru/ws/types/simple/error/" name="fault"
element="ns4:faultElem"/>
    </message>
    <message name="getBaseAuthorities">
        <part name="getBaseAuthoritiesRequest" element="tns:getBaseAuthoritiesRequest"/>
    </message>
    <message name="getBaseAuthoritiesResponse">
        <part name="getBaseAuthoritiesResponse" element="tns:getBaseAuthoritiesResponse"/>
    </message>
    <message name="grantAuthority">
        <part name="grantAuthorityRequest" element="tns:grantAuthorityRequest"/>
    </message>
    <message name="grantAuthorityResponse">
        <part name="grantAuthorityResponse" element="tns:grantAuthorityResponse"/>
    </message>
    <message name="revokeAuthority">
        <part name="revokeAuthorityRequest" element="tns:revokeAuthorityRequest"/>
    </message>
    <message name="revokeAuthorityResponse">
        <part name="revokeAuthorityResponse" element="tns:revokeAuthorityResponse"/>
    </message>
    <portType name="AuthorityManagement">
        <operation name="getSystemAuthorities">
            <input wsam:Action="getSystemAuthorities" message="tns:getSystemAuthorities"/>
            <output
wsam:Action="http://esia.atc.ru/ws/authz/authorityManagement/AuthorityManagement/getSystemAuthori
tiesResponse"
                    message="tns:getSystemAuthoritiesResponse"/>
            <fault message="tns:Fault" name="Fault"

wsam:Action="http://esia.atc.ru/ws/authz/authorityManagement/AuthorityManagement/getSystemAuthori
ties/Fault/Fault"/>
        </operation>
        <operation name="getBaseAuthorities">
            <input wsam:Action="getBaseAuthorities" message="tns:getBaseAuthorities"/>
            <output
wsam:Action="http://esia.atc.ru/ws/authz/authorityManagement/AuthorityManagement/getBaseAuthoriti
esResponse"
                    message="tns:getBaseAuthoritiesResponse"/>
            <fault message="tns:Fault" name="Fault"

wsam:Action="http://esia.atc.ru/ws/authz/authorityManagement/AuthorityManagement/getBaseAuthoriti
es/Fault/Fault"/>
        </operation>
        <operation name="grantAuthority">
            <input wsam:Action="grantAuthority" message="tns:grantAuthority"/>
            <output
wsam:Action="http://esia.atc.ru/ws/authz/authorityManagement/AuthorityManagement/grantAuthorityRe
sponse"
                    message="tns:grantAuthorityResponse"/>
            <fault message="tns:Fault" name="Fault"

wsam:Action="http://esia.atc.ru/ws/authz/authorityManagement/AuthorityManagement/grantAuthority/F
ault/Fault"/>
        </operation>
        <operation name="revokeAuthority">
            <input wsam:Action="revokeAuthority" message="tns:revokeAuthority"/>
```

```
            <output
wsam:Action="http://esia.atc.ru/ws/authz/authorityManagement/AuthorityManagement/revokeAuthorityR
esponse"
                    message="tns:revokeAuthorityResponse"/>
            <fault message="tns:Fault" name="Fault"

wsam:Action="http://esia.atc.ru/ws/authz/authorityManagement/AuthorityManagement/revokeAuthority/
Fault/Fault"/>
        </operation>
    </portType>
    <binding name="AuthorityManagementPortBinding" type="tns:AuthorityManagement">
        <wsp:PolicyReference URI="#defaultpolicy"/>
        <soap:binding transport="http://schemas.xmlsoap.org/soap/http" style="document"/>
        <operation name="getSystemAuthorities">
            <soap:operation soapAction="getSystemAuthorities"/>
            <input>
                <soap:body use="literal"/>
            </input>
            <output>
                <soap:body use="literal"/>
            </output>
            <fault name="Fault">
                <soap:fault name="Fault" use="literal"/>
            </fault>
        </operation>
        <operation name="getBaseAuthorities">
            <soap:operation soapAction="getBaseAuthorities"/>
            <input>
                <soap:body use="literal"/>
            </input>
            <output>
                <soap:body use="literal"/>
            </output>
            <fault name="Fault">
                <soap:fault name="Fault" use="literal"/>
            </fault>
        </operation>
        <operation name="grantAuthority">
            <soap:operation soapAction="grantAuthority"/>
            <input>
                <soap:body use="literal"/>
            </input>
            <output>
                <soap:body use="literal"/>
            </output>
            <fault name="Fault">
                <soap:fault name="Fault" use="literal"/>
            </fault>
        </operation>
        <operation name="revokeAuthority">
            <soap:operation soapAction="revokeAuthority"/>
            <input>
                <soap:body use="literal"/>
            </input>
            <output>
                <soap:body use="literal"/>
            </output>
            <fault name="Fault">
                <soap:fault name="Fault" use="literal"/>
            </fault>
        </operation>
    </binding>
    <service name="AuthorityManagerService">
        <port name="AuthorityManagementPort" binding="tns:AuthorityManagementPortBinding">
            <soap:address
location="http://172.18.4.52:7001/AuthorityManager/AuthorityManagerService"/>
        </port>
    </service>
</definitions>
```

Приложение Б. Уровни достоверности идентификации в ЕСИА

С целью обеспечения возможности гибкого управления процессами аутентификации и авторизации пользователей введены 4 уровня достоверности идентификации пользователя.

Каждый уровень характеризуется своими требованиями к процессам, связанным с регистрацией пользователей, идентификацией и аутентификацией. При этом уровни сравнимы друг с другом, то есть требования высокого уровня строже требований низкого уровня.

Задачей ИС является обеспечить выбор допустимых уровней достоверности идентификации пользователей, удовлетворяющих потребностям ИС. Описание уровней достоверности идентификации приведено в таблице.

Уровень достоверности идентификации	**Описание**
Уровень 1	Минимальный уровень достоверности идентификации. Данный уровень присваивается учетным записям пользователей, личность которых не подтверждена. Предполагается использование данного уровня в ИС, которым требуется осуществлять взаимодействие с пользователями в рамках определенного контекста. При этом отсутствует необходимость гарантии, что данные о пользователе соответствуют реальной личности и что пользователь действительно является этой личностью.
Уровень 2	Данный уровень присваивается учетным записям пользователей, личность которых подтверждена со стандартным уровнем гарантии (проверяется реальное существование физического лица с помощью сервисов ОИВ, осуществляется подтверждение соответствия личности пользователя посредством отправки регистрируемого почтового отправления с кодом активации Почтой России или выдачи кода активации в центре регистрации). Для аутентификации используется пароль.

Уровень достоверности идентификации	Описание
Уровень 3	Данный уровень присваивается учетным записям пользователей, личность которых подтверждена с повышенным уровнем гарантии (проверяется реальное существование личности при персональном посещении пользователем центра регистрации – офиса уполномоченной организации). Для аутентификации используется электронная подпись.
Уровень 4	Максимальный уровень достоверности идентификации. Данный уровень присваивается учетным записям пользователей (к таким пользователям, например, относятся пользователи с ролью должностного лица органа власти), регистрация которых выполняется только уполномоченным сотрудником ОИВ (оператором). Самостоятельная регистрация указанных пользователей исключена.

Приложение В. Стандарт SAML 2.0

Взаимодействие ИС с ЕСИА 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.

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 SAML 2.0 присутствуют следующие протоколы типа запрос/ответ:

– Authentication Request Protocol (протокол запроса аутентификации) – определяет способы, которыми аутентифицированный субъект (или агент, действующий от его имени) 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, поставщиком идентификации или поставщиком услуг (например, в результате таймаута сессии, команды администратора и т.п.);
– Assertion Query and Request Protocol (протокол запроса и выборки утверждений) – определяет способы запросов утверждений SAML 2.0;
– Artifact Resolution Protocol (протокол определения артефактов) – предоставляет механизм, с помощью которого сообщения протоколов SAML 2.0 могут передаваться в виде ссылки как небольшое, фиксированной длины значение, называемое артефактом;
– Name Identifier Management Protocol (протокол управления идентификаторами имен) – предоставляет механизмы для обмена значением или форматом идентификатора имени аутентифицированного субъекта.

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

– 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;

– HTTP Artifact – определяет, как артефакт передается от отправителя сообщения к получателю сообщения, используя HTTP;
– SAML SOAP – определяет, как сообщения протокола SAML 2.0 передаются внутри сообщений SOAP;
– Reverse SOAP (PAOS) – определяет обмен SOAP/HTTP сообщениями в несколько стадий, который позволяет HTTP клиенту быть получателем SOAP;
– SAML 2.0 URI – определяет способы получения существующих утверждений SAML 2.0 с помощью разрешения (обнаружения) URI.

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

– Web Browser SSO – определяет, как реализовать однократную аутентификацию в стандартных веб-браузерах;
– Enhanced Client and Proxy (ECP) определяет, как реализовать однократную аутентификацию для специальных клиентов, которые могут использовать протокол SOAP;
– Identity Provider Discovery – определяет механизм, позволяющий поставщику услуг получить информацию о поставщике идентификации субъекта;
– Single Logout – определяет, как выполнить одновременный выход из всех сессий;
– Assertion Query/Request – определяет, как участники SAML 2.0 могут использовать протокол запроса и ответа SAML 2.0 для получения утверждений SAML 2.0;
– Artifact Resolution – определяет, как участники SAML 2.0 могут использовать протокол получения артефакта при синхронном способе доставки, таком как SOAP, для получения сообщения протокола, на которое ссылается артефакт;
– Name Identifier Management – определяет, как протокол управления идентификатором имени может быть использован со связываниями SOAP, HTTP Redirect, POST и Artifact;
– Name Identifier Mapping – определяет, как протокол отображения идентификатора имени использует синхронный способ передачи, такой как SOAP.

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.

Приложение Г. Руководство по разработке интерфейсов поставщика услуг для интеграции с поставщиком идентификации ЕСИА

Г.1 Рекомендации

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 Г.6.

Г.2 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.

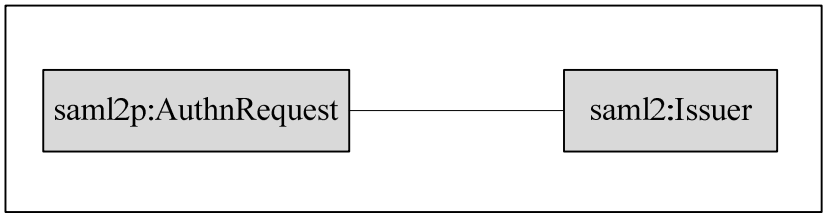
Г.3 Описание форматов электронных сообщений SAML 2.0 в ЕСИА

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 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:



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://demo1-esia.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 СКП поставщика услуг;
- 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.

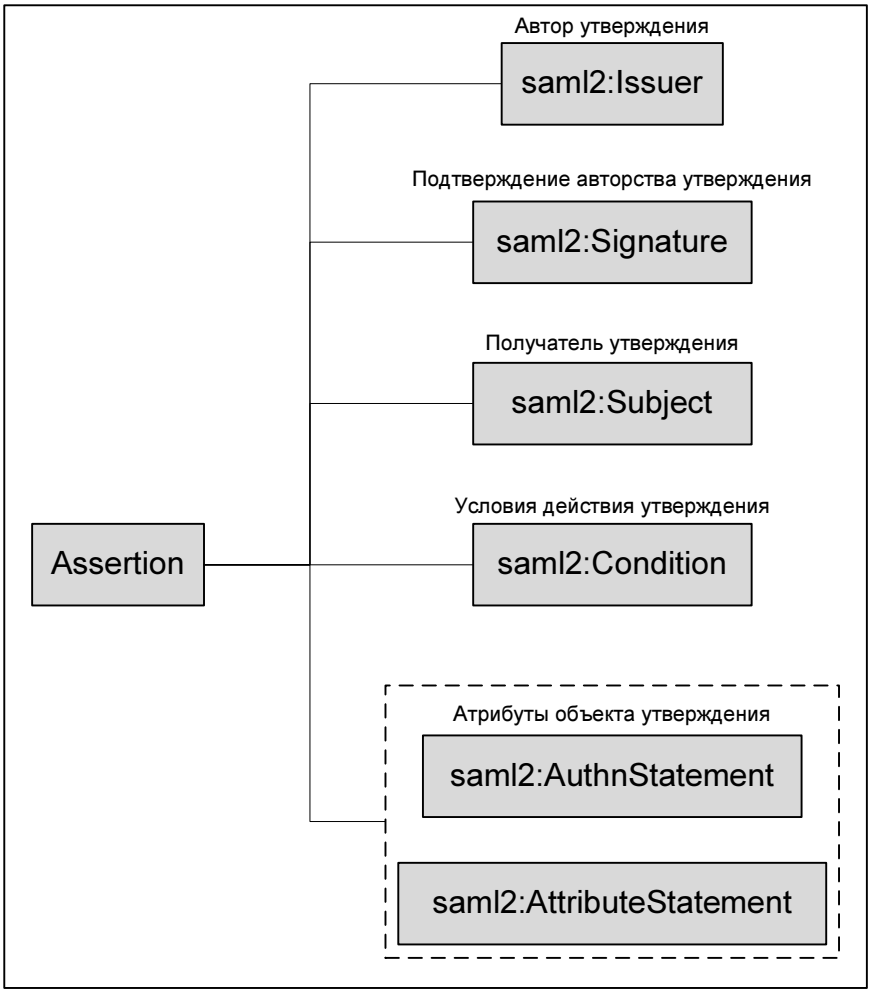
Пример URL AuthnRequest:

```
https://demo1-
esia.gosuslugi.ru/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fZJBa%2BMwEIX%2FitBdlqzYWyPilLSlbKFL
Q%2BzuYS9FkSepwJGyGtn051dxEtpS6EUg9Oabmfc0v37b92SEgNa7muaZoASc8Z11u5o%2Bt%2FesoteLOep9Lw9qOcRXt4b
%2FA2AkqdChOr3UdAhOeY0WldN7QBWNapZ%2FHpXMhDoEH73xPSVLRAgxtbr1Doc9hAbCaA08rx9r%2BhrjARXnOhpWikJdCS
G5t%2F7Ygk%2FHkfgNQcldGsc6HacVLhS0mnUwZrDzY6YjM0d5n3S7LAzcdgeextraHiaq5GvobAATedM8UXLvg4Fp3ZpudY9
AycNdTV9EIcy22JRsVpYVK%2FIrzTYm75j%2BVVVFJTeiK02S4koj2hE%2BihEHeHAYtYs1lSKXTEgmq1ZUKp%2BpvMhmVfGP
ktXZqhvrThH85OvmJEL1u21XbPXUtJT8vUSZBPQcnJq6h8%2BJ%2FQzWF4%2FpItn4EpO%2Fc%2F4ZtThfv36JxTs%3D&Rela
yState=_12db488a-a516-41e3-801c-
3e8f23547314&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-
sha1&Signature=k1XL2WfE1KMHzaJtjjaL2O1soweYNM06Xt50E20QgwRzVOBZ0T79HJEjPMu3jBhDdmM47zlrswbhUFPV22
oDbk5KuXJ%2F5FVPwXCTefnVCZGXHU8b1SWuC%2FoKlTSxum6enoommHN5S%2FeYAP9S0KNNW5yEP3eJQHkcsTYuTKPmyP8%3
D
```

Ответ на запрос аутентификации(AuthnResponse).

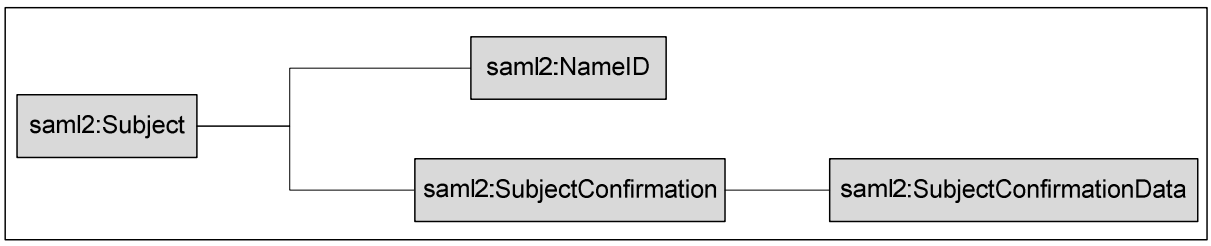
В случае успешной аутентификации поставщик идентификации формирует ответ на запрос аутентификации – AuthnResponse, который содержит утверждение (Assertion) об

аутентификации. AuthnResponse представляет собой XML-документ со следующей структурой:



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

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



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).

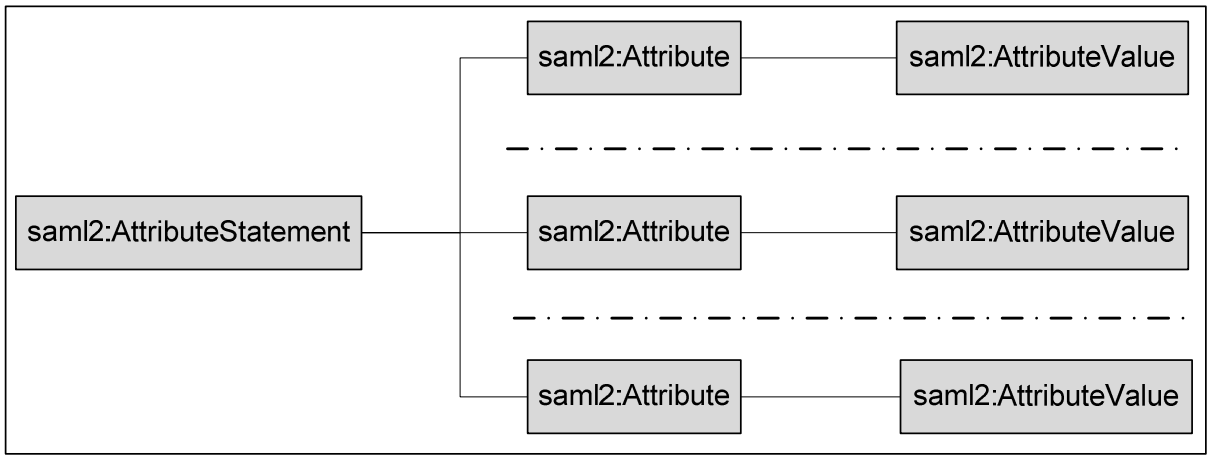
Элемент saml2:Condition содержит описание условий, при которых данный AuthnResponse считается действительным. Данный элемент имеет два атрибута – NotBefore и NotOnOrAfter, которые указывают на временной промежуток, в который данный AuthnResponse действителен. Также saml2:Condition имеет вложенный элемент 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:



Элемент saml2:Attribute имеет три атрибута:

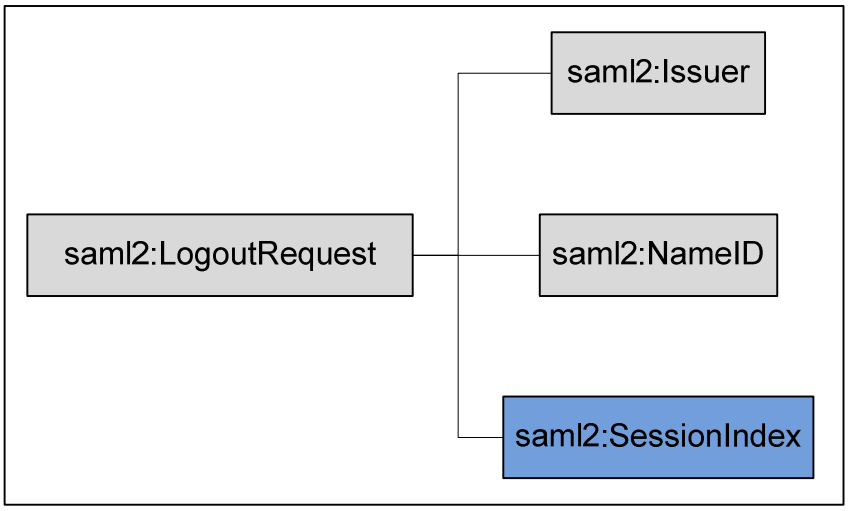
– FriendlyName – сокращенное наименование атрибута;
– Name – полное наименование атрибута;
– NameFormat – формат полного наименования атрибута.

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

Пример AuthnResponse приведен в разделе Г.7.

Запрос завершения активной сессии пользователя (LogoutRequest).

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



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:

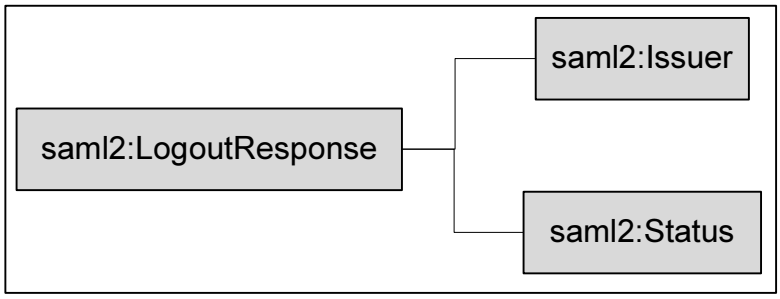
```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:LogoutRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                                                    Destination="https://demo1-esia.gosuslugi.ru/idp/profile/SAML2/Redirect/SLO"
```

```
                                                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://demo1-esia.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:



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.

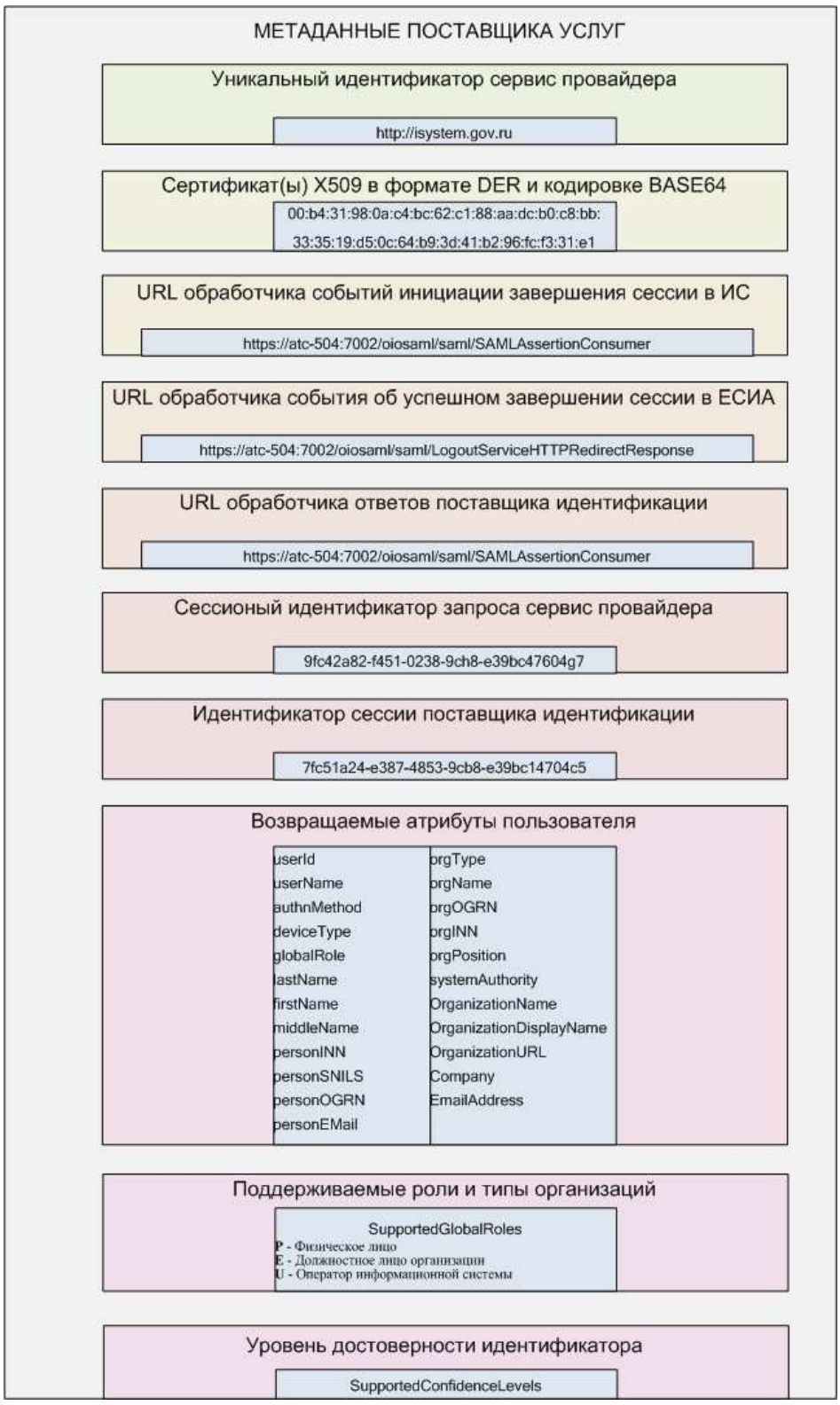
Примеры ответа на запрос завершения сессии:

```
<?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://demo1-esia.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://demo1-esia.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>
```

Г.4 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.



Перечень атрибутов пользователя (организации), содержащихся в файле метаданных поставщика услуг, приведен в таблице.

№	Атрибут	Описание
1.	authnMethod	Метод аутентификации. Принимает следующие возможные значения: **PWD** — аутентификации по логину и паролю;

№	Атрибут	Описание
		DS — аутентификации по ЭП.
2.	deviceType	Тип носителя СКП, используемого при аутентификации по ЭП. Данный атрибут устанавливается только для случая, когда атрибут AuthMethod равен DS.
3.	personType	Категория пользователя. Принимает следующие возможные значения: **R** — гражданин РФ (Russian); **F** — иностранный гражданин (Foreigner).
4.	globalRole	Роль пользователя. Принимает следующие возможные значения: **P** — физическое лицо (Physical person); **E** — должностное лицо организации (Employee); **U** — оператор информационной системы (User).
5.	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.
6.	userName	Логин пользователя.
7.	orgName	Наименование организации пользователя. Данный атрибут устанавливается только для случая, когда атрибут globalRole = E.
8.	orgOGRN	ОГРН организации пользователя. Данный атрибут устанавливается только для случая, когда атрибут globalRole = E.
9.	orgINN	ИНН организации пользователя. Данный атрибут устанавливается только для случая, когда атрибут globalRole = E.
10.	personOGRN	ОГРНИП пользователя. Данный атрибут устанавливается только для случая,

№	Атрибут	Описание
		когда атрибут orgType = B.
11.	personINN	ИНН пользователя. Данный атрибут устанавливается только для случая, когда атрибут personType = R.
12.	personSNILS	СНИЛС пользователя. Данный атрибут устанавливается только для случая, когда атрибут personType = R.
13.	personEMail	Адрес электронной почты пользователя.
14.	userId	Числовой идентификатор учетной записи пользователя в системе ЕСИА.
15.	authToken	Идентификатор сессии пользователя в системе ЕСИА.
16.	lastName	Фамилия пользователя.
17.	firstName	Имя пользователя.
18.	middleName	Отчество пользователя.
19.	systemAuthority	Полномочия пользователя в отношении ИС, проходящей идентификацию и аутентификацию в ЕСИА
20.	orgPosition	Должность пользователя в организации.
21.	SupportedConfidenceLevels	Уровень достоверности идентификации пользователя (пояснения приведены в разделе Приложение Б).

Г.5 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 ключа подписи (СКП) 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 СКП 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="userName" Name="urn:esia:userName"><!--Логин пользователя--></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="deviceType" Name="urn:esia:deviceType"><!--Тип носителя СКП, используемого при
авторизации по ЭП--></saml:Attribute>
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
friendlyName="personType" Name="urn:esia:personType"><!--Категория пользователя--
></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="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="systemAuthority" Name="urn:esia:systemAuthority"><!--Полномочия пользователя в
системе, которая запрашивает аутентификацию--></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>
    </md:AttributeAuthorityDescriptor>
    <md:Organization>
        <!--TODO
        Необходимо заполнить описание организации к которой относится интегрируемая с ЕСИА ИС:
         - OrganizationName - имя оранизации;
         - 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"><!--Физическое лицо-->
                <esia:SupportedPersonTypes>
                    <esia:PersonType ID="R">
                        <esia:SupportedAuthnMethods>
                            <esia:AuthnMethod ID="PWD"/>
                            <esia:AuthnMethod ID="DS">
                                <esia:SupportedDeviceTypes>
                                    <esia:DeviceType ID="ETOKEN"/>
                                    <esia:DeviceType ID="RUTOKEN"/>
                                </esia:SupportedDeviceTypes>
                            </esia:AuthnMethod>
```

```
                        </esia:SupportedAuthnMethods>
                    </esia:PersonType>
                    <esia:PersonType ID="F">
                        <esia:SupportedAuthnMethods>
                            <esia:AuthnMethod ID="PWD"/>
                        </esia:SupportedAuthnMethods>
                    </esia:PersonType>
                </esia:SupportedPersonTypes>
            </esia:GlobalRole>
            <esia:GlobalRole ID="E"><!--Должностное лицо организации-->
                <esia:SupportedOrgTypes>
                    <esia:OrgType ID="B"/><!--Индивидуальный предприниматель-->
                    <esia:OrgType ID="L"><!--Юридическое лицо-->
                        <esia:SupportedAuthnMethods>
                            <esia:AuthnMethod ID="PWD"/>
                            <esia:AuthnMethod ID="DS">
                                <esia:SupportedDeviceTypes>
                                    <esia:DeviceType ID="ETOKEN"/>
                                    <esia:DeviceType ID="RUTOKEN"/>
                                </esia:SupportedDeviceTypes>
                            </esia:AuthnMethod>
                        </esia:SupportedAuthnMethods>
                    </esia:OrgType>
                    <esia:OrgType ID="A"><!--Орган исполнительной власти-->
                        <esia:SupportedAuthnMethods>
                            <esia:AuthnMethod ID="PWD"/>
                            <esia:AuthnMethod ID="DS">
                                <esia:SupportedDeviceTypes>
                                    <esia:DeviceType ID="ETOKEN"/>
                                </esia:SupportedDeviceTypes>
                            </esia:AuthnMethod>
                        </esia:SupportedAuthnMethods>
                    </esia:OrgType>
                </esia:SupportedOrgTypes>
            </esia:GlobalRole>
            <esia:GlobalRole ID="U"><!--Оператор информационной системы-->
                <esia:SupportedAuthnMethods>
                    <esia:AuthnMethod ID="PWD"/>
                    <esia:AuthnMethod ID="DS">
                        <esia:SupportedDeviceTypes>
                            <esia:DeviceType ID="ETOKEN"/>
                        </esia:SupportedDeviceTypes>
                    </esia:AuthnMethod>
                </esia:SupportedAuthnMethods>
            </esia:GlobalRole>
        </esia:SupportedGlobalRoles>
    </md:Extensions>
</md:EntityDescriptor>
```

Г.6 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).getValue(
);
```

Г.7 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://demo1-
esia.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:PasswordProtectedTranspo
ort</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">028-718-303 62</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">028-718-303 62</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:Attribute FriendlyName="authMethod"
Name="urn:mace:dir:attribute:authMethod" 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">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">Валерьевич</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">Борцов</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>
```