Приложение №2. Технические условия на подключение к ПДС

УТВЕРЖДАЮ
Директор по информационным технологиям
АО «Гринатом»

_____/ А.Н. Киселёв /

М.П.

ПЛАТФОРМА ДОВЕРЕННЫХ СЕРВИСОВ ГОСКОРПОРАЦИИ «РОСАТОМ»

Технические условия на подключение

Версия 4.0

Москва
2022

Аннотация

Настоящий документ является Техническими условиями на подключение Корпоративных информационных систем к Платформе доверенных сервисов Госкорпорации «Росатом».

В целях оптимизации затрат на использование средств криптографической защиты, создания условий обеспечения юридической значимости электронных документов и обеспечения необходимого уровня доверия к электронным документам в разных информационных системах создана настоящая платформа доверенных сервисов (далее ПДС). Для интеграции информационных систем с ПДС необходимо выполнить ряд технических и организационных условий, которые сведены в настоящий документ.

1. Термины и определения

Термин/ Сокращение	Определение/Наименование
AD	Корпоративный каталог на базе Microsoft Active Directory со службой федерализации OAuth 2.0
ADFS	Active Directory Federation Services (служба федерации) позволяет управлять федеративными удостоверениями и доступом, обеспечивая безопасный общий доступ к цифровым удостоверениям и правам прав в рамках безопасности и границ предприятия.
API	Интерфейс прикладного программирования
DSS	Программно-аппаратный комплекс КриптоПро DSS предназначен для централизованного, защищенного хранения закрытых ключей пользователей, а также для удаленного выполнения операций по созданию электронной подписи (ЭП)
IAM	Identity and Access Management Системы управления идентификацией и доступом к информационным ресурсам
IAM Mail.ru – работники	Подсистема в составе ИС «Сеть профессиональных сообществ»
OCSP	Online Certificate Status Protocol, Протокол состояния сетевого сертификата
TSP	Time stamp protocol, Протокол штампа времени
WAP	Web Application Proxy (прокси-сервер веб-приложений) позволяет публиковать веб-приложения для доступа извне, обеспечивая требуемый уровень безопасности

Термин/ Сокращение	Определение/Наименование
АБ	Администратор безопасности
АО	Акционерное общество
АРМ	Автоматизированное рабочее место
БД	База данных
Договор на оказание услуг	Договор присоединения, двусторонний договор или иной договор, заключаемый между АО «Гринатом» и организацией, которая является получателем услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств
Домен GK	Домен ГК Росатом для предприятий РФ, GK (gk.rosatom.local)
ЕСИА	Единая система идентификации и аутентификации
ИАСУП	Корпоративная система управления персоналом на базе SAP
Инструкция №152	Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденная приказом ФАПСИ России от 13.06.2001 №152
КИС	Корпоративная информационная система Госкорпорации «Росатом»
Ключевой документ, отчуждаемый ключевой носитель	Электронный носитель ключевой информации, содержащий один или несколько ключей
Корпоративная информационная система	Информационная система, расположенная на серверах в ЦОД Госкорпорации «Росатом»
Корпоративный удостоверяющий центр	Удостоверяющий центр АО «Гринатом»
КСПД	Корпоративная сеть передачи данных ГК Росатом
КТ	Коммерческая тайна
КУЦ	Корпоративный удостоверяющий центр
ЛИС	Локальная информационная система

Термин/ Сокращение	Определение/Наименование
Локальная информационная система	Информационная система, которая принадлежит отраслевой компании, но не расположена на серверах в ЦОД Госкорпорации «Росатом», или информационная система, которая установлена в организации, заключившей Договор на оказание услуг с Заказчиком и не входит в отрасль
ОКЗ	Орган криптографической защиты АО «Гринатом»
ПД	Персональные данные
ПДС, Система	Платформа доверенных сервисов
ПО	Программное обеспечение
Подписка	Доступ конкретного пользователя или пользователей организации к получению той или иной услуги, посредством запроса через API или через интерфейс ПДС
Подписчик	Физическое лицо, для которого оформлена подписка на обеспечение сертификатом и (или) лицензией на СКЗИ
Протокол состояния сетевого сертификата	Интернет-протокол, используемый для получения статуса отзыва цифрового сертификата X.509
Протокол штампа времени	Криптографический протокол, позволяющий создавать доказательство факта существования электронного документа на определённый момент времени
Сертификат	Сертификат ключа проверки электронной подписи
Сертификат ключа проверки электронной подписи	Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи
СКЗИ	Средство криптографической защиты информации
Средство криптографической защиты информации	Совокупность программно-технических средств, обеспечивающих применение электронной подписи и шифрования при организации обмена электронными документами. СКЗИ могут

Термин/ Сокращение	Определение/Наименование
	применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение. В настоящем документе под СКЗИ будут пониматься только программные средства.
СУИТ	Система управления ИТ, внутренняя система ГК Росатом управления обращениями\заявками по ИТ
Удостоверяющий центр	Юридическое лицо или индивидуальный предприниматель, осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом № 63-ФЗ «Об электронной подписи»
УКЭП	Усиленная квалифицированная электронная подпись
УНЭП	Усиленная неквалифицированная электронная подпись
УЦ	Удостоверяющий центр
ЭП	Электронная подпись

2. Платформа доверенных сервисов

2.1. Общие сведения о ПДС

Наименование системы - Платформа доверенных сервисов

ПДС это облачное решение, состоящее из:

комплекса единых отраслевых доверенных сервисов на базе инфраструктуры открытых ключей;

единых условий интеграции информационных систем с ПДС;

свидетельств доверия, полученных в результате оценки, позволяющих обеспечить высокий уровень доверия к электронным документам и их юридическую значимость с использованием усиленных электронных подписей в соответствии со стандартами и НПА РФ.

ПДС поддерживает квалифицированные и неквалифицированные сервисы и может работать с документами разного уровня доверия.

2.2. Назначение ПДС

Платформа доверенных сервисов предназначена для предоставления на договорной основе централизованных услуг доверия на базе инфраструктуры открытых ключей предприятиям отрасли и их контрагентам в разных информационных (документных) системах. ПДС предоставляет единый программный интерфейс для всех интегрируемых с ней информационных систем.

ПДС по требованию Госкорпорации «Росатом» осуществляет оценку уровня доверия и соответствия требованиям стандарта для электронных документов и интегрируемых документных систем с формированием свидетельств доверия.

Платформа доверенных сервисов предназначена для автоматизации деятельности АО «Гринатом» по управлению электронными ключами и средствами криптографической защиты пользователей предприятий Госкорпорации «Росатом», заключивших с АО «Гринатом» договор на оказание услуг

Перечень сервисов и порядок функционирования ПДС:

Сервис управления ключами усиленной квалифицированной электронной подписи и сертификатами ключа проверки квалифицированной электронной подписи.

Сервис удаленной усиленной квалифицированной электронной подписи.

Сервис проверки усиленной квалифицированной электронной подписи.

Сервис управления ключами усиленной неквалифицированной электронной подписи и сертификатами ключа проверки квалифицированной электронной подписи.

Сервис удаленной усиленной неквалифицированной электронной подписи.

Сервис проверки усиленной неквалифицированной электронной подписи.

Для подключения к ПДС предприятия заключают договор с Оператором ПДС и указывают объемы запрашиваемых услуг ПДС.

Подключение к ПДС осуществляется в рамках услуги Интеграционная поддержка ПДС (CLB.32)

Для интеграции информационных систем с ПДС оператор ПДС проводит оценку соответствия требованиям стандарта для электронных документов и интегрируемых документных систем с формированием свидетельств доверия.

Информационные системы проводят работы по тестированию совместимости и подключению к ПДС с формированием акта о прохождении приёмо-сдаточных испытаний по окончанию интеграции Информационной системы с Платформой доверенных сервисов».

После проведения работ по интеграции с ПДС, интеграционное взаимодействие ИС с ПДС переводится в постоянную эксплуатацию в соответствии с услугой функциональная поддержка (CLB.32).

2.3. Порядок подключения корпоративной/локальной информационной системы к платформе доверенных сервисов Госкорпорации «Росатом»:

Описания порядка подключения опубликованы на сайте: https://crypto.rosatom.ru/uslugi/platforma-doverennykh-servisov-integratsionnaya-podderzhka-pds-clb-32/

1.Оператор КИС/ЛИС должен присоединиться к Договору №22/2143-Д. https://crypto.rosatom.ru/dokumentatsiya/dogovor/

Администраторам поддержки КИС/ЛИС из числа АО «Гринатом» присоединяться к договору не требуется, только выполнить п.2 (предоставить заполненное и подписанное Заявление) и п. 3.

2.Подготовить и направить в орган криптографической защиты АО «Гринатом» (далее – ОКЗ АО «Гринатом») заявление на интеграционную поддержку ПДС в тестовой зоне и в продуктивной (далее – Заявление) с приложением №1.

Первично на основании заявления производится подключение к тестовой зоне ПДС.

После проведения успешной интеграции с тестовой средой ПДС и аудита КИС/ЛИС требуется предоставить отдельное заявление с новыми данными для подключения к продуктивной зоне ПДС. Вместе с Заявлением необходимо направить в ОКЗ АО «Гринатом» следующий комплект документов:

копию или скан-копию аттестата соответствия объекта информатизации на соответствие требованиям по безопасности информации;

копию или скан-копию анализа степени конфиденциальности сведений, передаваемых из КИС/ЛИС в ПДС;

разрешение на информационный обмен между интегрированной КИС/ЛИС и ПДС;

программу методику испытаний или сценарий интеграционного тестирования КИС/ЛИС с ПДС в части проверки функционала, реализованного на стороне КИС/ЛИС:

1. проверка/получения данных о сертификате пользователя;
2. выпуск неквалифицированного сертификата для пользователя через запрос от КИС/ЛИС в случае отсутствия;
3. получения токена безопасности через доменный ADFS (GK, INTER), IAM (GK)
4. создание подписи;
5. проверка подписи.

Сценарий интеграционного тестирования или программа методики испытаний в обязательном порядке должна быть согласована в системе ЕОСДО, для утверждения этапов тестирования и неотрицаемости в дальнейшем, функционала подписи и проверки подписи, реализуемой в информационной системе, подключаемой к ПДС. Согласование отправить в ЕОСДО на следующих сотрудников:

Савин А.В. (AndVlSavin);

Степанов А.В. (AleVlaStepanov);

РП или менеджер услуги в рамках которой работает ИС;

Владельца системы (если владельцем системы выступает компания не Гринатом, то не обходимо указать ответственное лицо от оператора, которым выступает Гринатом).

Скан-копии заполненных, подписанных и заверенных печатью организации Заявлений нужно направить на электронную почту: pds@rosatom.ru или менеджеру услуги на адрес AndVlSavin@Greenatom.ru, AleVlaStepanov@Greenatom.ru.

Оригиналы документов необходимо направить в ОКЗ АО «Гринатом» с курьером или почтовым отправлением по адресу: 115230, г. Москва, 1-й Нагатинский проезд, д. 10, стр. 1.

3.Заполнить программу аудита на соответствие требованиям ГОСТ Р ИСО 30300-2015 и ГОСТ Р ИСО 15489-1-2019.

Форму программы аудита можно запросить обратившись по адресу электронной почты audit_pds@rosatom.ru.

3. Обеспечение юридической значимости электронных документов.

3.1. Подтверждение выполнения требований к ПДС

ПДС обеспечивает выполнение требований по обеспечению безопасности информации в соответствии с Аттестатом соответствия № № 08/12/2020 – АС МЕТРОКЛАСТЕР/ ПДС от 08 декабря 2020 года

ПДС переведена в промышленную эксплуатацию в соответствии с Приказом АО «Гринатом» №22/1179-1-П от 28.12.2020

Эксплуатация ПДС производится на основании Лицензии ФСБ России ЛСЗ №0014254 Рег.№15686 Н от 19.01.2017 на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)

Процесс оказания услуг по выдаче сертификатов УКЭП производится в рамках свидетельства об аккредитации удостоверяющего центра №758 от 21 августа 2017 г.

Процесс управления СКЗИ производится с учётом требований Приказа ФАПСИ № 152 от 13 июня 2001г. «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

3.2. Подтверждение выполнения требований к документам и документным системам.

Должен быть проведен аудит документов и документных систем на соответствие требованиям ГОСТ Р ИСО 30300-2015 и ГОСТ Р ИСО 15489-1-2019 в соответствии с Программой аудита, которую можно запросить обратившись по адресу электронной почты audit_pds@rosatom.ru..

В рамках аудита рассматриваются свойства документной системы (надежность, безопасность, соответствие, комплексность, системность) и свойства документов (аутентичность, достоверность, целостность, пригодность для использования), и их соответствие требованиям ГОСТ Р ИСО 30300-2015 и ГОСТ Р ИСО 15489-1-2019.

Аудит на соответствие требованиям ГОСТ Р ИСО 30300-2015 и ГОСТ Р ИСО 15489-1-2019 должен быть проведен рабочей группой по проведению аудита, назначенной распоряжением по Госкорпорации «Росатом». По результатам проведенного аудита должен быть составлен отчет, в котором указываются охваченные вопросы в рамках аудита, методы аудита, результаты, ссылки на подтверждающие документы, выводы и рекомендации.

При наличии рекомендаций в отчете составляется план устранения недостатков с указанием ответственных и сроков устранения.

Документные системы, не отвечающие требованиям ГОСТ Р ИСО 30300-2015 и ГОСТ Р ИСО 15489-1-2019, должны быть подключены к ПДС при наличии утвержденного плана устранения недостатков.

3.3. Регулирование отношений в области использования электронных подписей.

Отношения в области использования электронных подписей регулируются Федеральным законом «Об Электронной подписи», и другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, а также соглашениями между участниками электронного взаимодействия. Если иное не установлено федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или решением о создании корпоративной информационной системы, порядок использования электронной подписи в корпоративной информационной системе может устанавливаться оператором этой системы или соглашением между участниками электронного взаимодействия в ней.

Шаблон Соглашения между участниками электронного взаимодействия при использовании усиленной неквалифицированной электронной подписи опубликован на общедоступном ресурсе https://crypto.rosatom.ru/uslugi/predostavlenie-uslug-platformy-doverennykh-servisov-v-otnoshenii-nekvalifitsirovannykh-sertifikatov-/

3.4. Подтверждение выполнение требований при интеграции КИС/ЛИС с ПДС.

Для успешного прохождения интеграции КИС/ЛИС с ПДС необходимо выполнить следующие условия:

КИС/ЛИС должна обеспечить выполнение требований по информационной безопасности изложенных в Приказах Госкорпорации «Росатом»:

1/4-П от 01.01.2019 г.

1/ 1517-П от 30.12.2019 г.

КИС/ЛИС должна предоставить в адрес ПДС:

Согласованное с отделом криптографической защиты АО «Гринатом» техническое решение описывающее реализацию интеграции между КИС/ЛИС и ПДС.

Аттестат соответствия объекта информатизации на соответствие требованиям по безопасности информации.

Анализа степени конфиденциальности сведений, передаваемых из КИС/ЛИС в ПДС.

Разрешение ПДТК на информационный обмен между КИС/ЛИС и ПДС.

Сценарий интеграционного тестирования между КИС/ЛИС и ПДС.

Отчет о проведенном аудите.

Предоставить информацию о наличии технической поддержки КИС/ЛИС в виде маршрутной карты, в которой указано, что обращения, связанные с функционалом КИС/ЛИС, в том числе при работе с сертификатом и/или ЭП, обрабатывает техническая поддержка КИС/ЛИС. В случае не выявления причины обращения на стороне КИС/ЛИС, направлять от имени технической поддержки КИС/ЛИС новое обращение через СУИТ в адрес технической поддержки ПДС (рабочая групп ПДС(интеграция) с указанием следующей информации:

1. Описание проблемы;
2. Контур тестирования;
3. SLD код КИС/ЛИС;
4. Upn – учетная запись в домене;
5. Email;
6. Время запроса;
7. Если запрос подписания документа тогда + Jwt-токен.

4. Интеграция с внешними системами

4.1. Сценарии интеграции КИС/ЛИС с ПДС.

Представители подключаемых КИС/ЛИС для подключения к ПДС должны оформить заявление на интеграцию с ПДС в соответствии с приложением №1.

Заявление направляется администратору ПДС в адрес pds@rosatom.ru

Контактное лицо для связи Савин Андрей Владимирович AndVlSavin@Greenatom.ru

Подключение КИС производится в два этапа. Опытная эксплуатация производится при подключении КИС/ЛИС к тестовому сегменту ПДС.

Существуют три тестовые зоны (контура) тестирования:

тестовая (зона разработки DEV);

тестовая (зона тестирования);

зона предпрод.

В зоне разработки DEV и в зоне тестирования выполняет тестирование сценариев УНЭП и УКЭП. Пользователи заводятся путем направления данных в тестовый ИАСУП и тестовый OIM.

В зоне предпрода выполняется тестирование УНЭП и УКЭП, пользователи заводятся в тестовой зоне предпрода ИАСУП и в продуктивном OIM.

По итогам опытной эксплуатации производятся приёмосдаточные испытания совместно с представителями КИС/ЛИС и ПДС и принимается решение о переводе на постоянную эксплантацию интеграции КИС/ЛИС.

Для согласования подключения, подключаемая система должны быть технически готова к подключению, а именно:

определить и согласовать паттерн интеграции (напрямую с серверами ПДС или посредством корпоративной шины передачи данных ЕСИК БП);

реализовать на своей стороне сервисы для получения асинхронных ответов (коллбэков) на операции подписания (сущность документ), операцию

подтверждения вторым фактором аутентификации при подписании документов, информировании о сертификатах (сущность сертификат) и получение тела расшифрованного документа (в случае использования функциональности шифрования/расшифрования);

в КИС/ЛИС должен быть реализован запрет на отправку запросов в ПДС от имени пользователей и/или для пользователей, которые не имеют сертификатов, выпущенных посредством ПДС, за исключением запросов о наличии таких сертификатов и запросов на выпуск сертификата для пользователя;

при прямом подключении к ПДС КИС/ЛИС должна реализовать на своей стороне механизм межсистемной аутентификации (mutual TLS) и предоставить SSL сертификат для такой аутентификации, а также предоставить адреса для коллбэк сервисов;

при подключении к ПДС посредством ЕСИК БП межсистемная аутентификация не требуется, необходимо предоставить SLD код КИС для маршрутизации запросов (формат запросов и коллбэк сервисов может отличаться от указанного в данном документе в случае взаимодействия через ЕСИК БП, в случае согласования изменения формата с ЕСИК БП, однако последовательность и логика запросов остается неизменной). Запросить SLD код можно через направление запрос на адрес DESurygin@Greenatom.ru;

согласовать и открыть сетевое взаимодействие до серверов ПДС (в соответствии с приложением №2) и до серверов ЕСИК БП.

4.2. Регистрация КИС/ЛИС при интеграции с ПДС.

ПДС должна предоставлять сервисы для КИС/ЛИС посредством взаимодействия через ЕСИК БП. Сервисы ПДС должны быть предоставлены для систем, зарегистрированных в Реестре подключенных КИС и ЛИС.

Администратор КИС/ЛИС указывает в заявлении (приложение №1) следующие атрибуты и направляет их в адрес Администратора ПДС:

наименование КИС/ЛИС;

контур подключения к ПДС: зона разработки DEV, тест Тестирования, предпрод или продуктивный;

организация, владеющая КИС/ЛИС;

контур подключения:

ЕСИК БП;

Интернет;

тип аутентификации:

для КИС/ЛИС, подключенных через ЕСИК БП: код внешней системы (далее – SLD код);

для КИС/ЛИС, подключенных из сети Интернет: сертификат для TLS-аутентификации;

UPN системного пользователя;

включен ли режим callback;

URL на сервис callback.

Администратор ПДС регистрирует КИС/ЛИС в соответствии с полученными данными.

4.3. Аутентификация КИС при интеграции с ПДС.

Со стороны КИС/ЛИС, подключенных из сети Интернет, должен быть выпущен сертификат для TLS-аутентификации.

Для использования этого способа аутентификации в ПДС должны быть внесены данные о КИС/ЛИС в соответствии с требованиями раздела 5.2

При установке соединения должна быть реализована взаимная проверка сертификата ПДС и сертификата КИС/ЛИС.

Запрос сертификата клиента должен быть реализован по протоколу TLS (ГОСТ).

Должна быть реализована проверка соответствия сертификата и срока действия сертификата.

Схема взаимодействия приведена на рисунке 1.

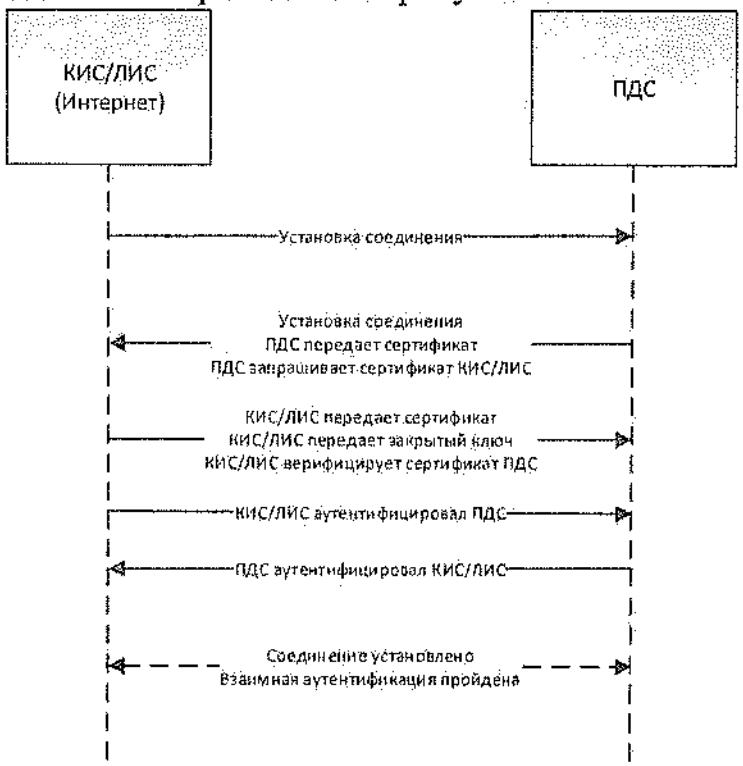

Рис. 1.

4.4. Режимы взаимодействия с ПДС.

В ПДС реализованы следующие режимы взаимодействия:

асинхронный;

синхронный.

Для использования асинхронного режима взаимодействия со стороны ЕСИК БП должен быть реализован callback-сервис, обеспечивающий получение ответов для каждой операции и передачу ответов в КИС/ЛИС.

КИС/ЛИС необходимо обеспечить callback-сервис, позволяющий получать ответы от ПДС в асинхронном режиме о следующих событиях:

Ответ о выпущенном сертификате при запросе на выпуск сертификата;

Информация о результате подписи;

Подтверждение второго фактора аутентификации;

Широковещательная рассылка при изменении статуса сертификата пользователя.

Со стороны КИС/ЛИС необходимо обеспечить callback-сервис позволяющий получать ошибки со стороны ПДС при выполнении следующих функций:

формирование сертификата;

формирование подписи;

проверка подписи;

шифрование данных.

В случае появления ошибок, ПДС отправляет в сторону КИС/ЛИС код ошибки.

КИС/ЛИС обязана обработать/устранить полученную ошибку и направить повторный запрос в сторону ПДС.

4.5. Требования к интерфейсу пользователя КИС при интеграции с ПДС.

Интерфейс пользователя КИС/ЛИС должен соответствовать требованиям Федерального Закона 63-ФЗ об Электронной подписи от 06.04.2011 г. в действующей редакции на момент подключения.

Владелец КИС/ЛИС обязан дорабатывать систему после подключения в случае изменения требований указанного федерального закона.

При создании ЭП интерфейс КИС должен:

показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

создавать ЭП только после подтверждения лицом, подписывающим электронный документ, операции по созданию ЭП;

однозначно показывать, что ЭП создана.

При проверке ЭП интерфейс КИС должен:

показывать содержание электронного документа, подписанного ЭП;

показывать информацию о внесении изменений в подписанный ЭП электронный документ;

указывать на лицо, с использованием ключа ЭП которого подписаны электронные документы.

Интерфейс КИС должен содержать страницу с настройками сертификатов ЭП пользователя КИС. Должна быть реализована возможность скачивания файла ЭП.

На странице настроек должны отображаться сведения о сертификате ЭП, применяемом для подписания в КИС:

Серийный номер сертификата

ФИО владельца сертификата

Имя издателя сертификата

Сведения о шаблоне сертификата

Дата создания сертификата

Дата окончания действия сертификата

Должна быть реализована возможность скачивания сертификата в формате *.cer, а также в текстовом виде для ознакомления с содержанием сертификата ЭП.

В ПДС может осуществляться подписание сертификатами, выданными аккредитованным УЦ (квалифицированные сертификаты) и неаккредитованным УЦ (неквалифицированные сертификаты), требования по отображению подписываемой информации следует считать одинаковыми для подписания квалифицированным и неквалифицированным сертификатов, в соответствие с требованиями 63-ФЗ к усиленной квалифицированной электронной подписи.

4.6. Правила визуального отображения документов в электронном виде.

КИС/ЛИС должна реализовывать визуализацию ЭП в подписанном документе подписанта.

Визуальное отображение документа в электронном виде должно содержать:

1. текст ЭД;

2. сведения о регистрации документа (графические элементы регистрационных данных);

3. сведения об ЭП, которой был подписан документ (отметка/отметки об ЭП).

Сведения об ЭП, которой был подписан документ в электронном виде (отметка/отметки об ЭП), содержат следующие элементы:

1. границы отметки об ЭП (служит для визуального разграничения сведений отметки об ЭП от текста документа и других отметок);

2. эмблема участника взаимодействия (при наличии);

3. информация о подписании документа ЭП;

4. сведения о сертификате ЭП, использованном при подписании ЭД.

Отметка об ЭП отображается путем наложения ее изображения на изображение текста ЭД. При задании местоположения, размера и других характеристик отметки об ЭП и ее элементов должны выполняться следующие требования:

1. место размещения отметки об ЭП должны соответствовать месту размещения личной подписи в аналогичном документе на бумажном носителе;

2. элементы отметки об ЭП должны быть видимыми и читаемыми при отображении документа в натуральном размере;

3. элементы отметки об ЭП не должны перекрываться или накладываться друг на друга;

4. элементы отметки об ЭП не должны перекрывать элементы текста документа и другие отметки об ЭП (при наличии).

Эмблема участника взаимодействия, в котором был подписан ЭД, в случае ее формирования располагается в верхней части отметки об ЭП, слева от информации о подписании.

Информация о подписании документа ЭП содержит текст "ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ" и располагается в верхней части отметки об ЭП справа от эмблемы участника взаимодействия (при наличии) и выравнивается горизонтально по центру области.

Сведения о сертификате ЭП, использованном при подписании, располагаются в нижней части отметки об ЭП и содержат следующие элементы:

1. номер сертификата ЭП;

2. данные владельца сертификата ЭП;

3. срок действия сертификата ЭП.

Элементы сведений о сертификате ЭП, использованном при подписании документа, располагаются на отдельных строках друг под другом.

Элемент "Номер сертификата электронной подписи" содержит текст "Сертификат" и номер сертификата ЭП, использованного при подписании документа.

"Владелец сертификата электронной подписи" содержит текст "Владелец", фамилию, имя и отчество (при наличии) владельца сертификата ЭП.

Элемент "Срок действия сертификата электронной подписи" содержит текст "Действителен с", дату начала действия сертификата ЭП, текст "по" и дату окончания действия сертификата.

Примеры отметок об ЭП и их размещения приведены в приложении 2 приказу Министерства связи и массовых коммуникаций российской федерации №186 Федеральной службы охраны Российской Федерации №258 от 27 мая 2015 года «Об утверждении требований к организационно-техническому взаимодействию государственных органов и государственных организаций посредством обмена документами в электронном виде»

4.7. Требования к данным пользователя при создании сертификата в ПДС

В ПДС используются два типа работников «Внутренний» (работник отраслевой организации, имеющий учетную запись в домене GK) и «Внешний» (работник сторонней организации, не имеющий учетную запись в домене GK и не зарегистрированный в ИАСУП).

4.8. Требования к данным внешнего пользователя ПДС

Создание внешних пользователей производится из интерфейса ПДС привилегированным пользователем Организации с ролью «Куратор ПДС от Организации»

При необходимости создания сертификата УНЭП для внешнего пользователя в КИС/ЛИС должен быть предусмотрен порядок информирования Кураторов ПДС от Организации о необходимости регистрации внешних пользователей в ПДС.

Если работник относится к сторонней организации и его данные отсутствуют в ИАСУП, необходимо указать Тип работника «Внешний». Все данные по внешнему пользователю заполняются Куратором организации вручную.

Куратор ПДС от Организации производит действия по созданию пользователя в соответствии с «Инструкция куратора Организации. Платформа доверенных сервисов Госкорпорации «Росатом» (ПДС)»

ВАЖНО! Для «Внешнего» пользователя в поле «Организация» необходимо выбрать из выпадающего списка наименование отраслевой организации, к которой прикреплен пользователь. В поле «Подразделение» необходимо ввести наименование внешней организации.

4.9. Требования к данным внутреннего пользователя ПДС создаваемого из КИС/ЛИС

ПДС организует создание сертификатов в два этапа:

создание пользователя ПДС;

выпуск сертификата для пользователя ПДС.

Для возможности создания пользователя на основании запроса КИС/ЛИС направленного в сторону ПДС через API, КИС/ЛИС должна обеспечить:

1.Наличие информации о пользователе в Корпоративной системе управления персоналом на базе SAP (ИАСУП):

№	Поле
1.	Фамилия
2.	Имя
3.	Отчество
4.	Наименование организации
5.	ИНН подписчика
6.	СНИЛС
7.	Серия паспорта
8.	Номер паспорта
9.	Наименование подразделения выдавшего паспорт
10.	Код подразделения выдавшего паспорт
11.	Дата выдачи паспорта
12.	Телефонный номер
13.	Пол
14.	Дата рождения

2.Наличие электронной почты Пользователя КИС/ЛИС в OIM.

3.Наличие корпоративной учетной записи (UPN) в домене GK или в Inter в OIM.

Обязательные данные для выпуска сертификата и состав полей сертификатов ПДС приведены в Приложении 3

В случае отсутствия данных (поле Субъект) приведенных в Приложении 3, **выпуск сертификата не возможен.**

КИС/ЛИС должна обеспечить наличие данных приведенных в Приложении 3 перед началом отправки запроса на сертификат для пользователя КИС/ЛИС. В случае отсутствия данных, необходимо технической поддержке КИС/ЛИС проконсультировать пользователя о порядке внесения данных.

4.10. Порядок заведения внутренних пользователей в ИАСУП и OIM

Заведение и учет данных пользователя осуществляется в Корпоративной системе управления персоналом на базе SAP (ИАСУП). Для заведения данных и внесение изменений необходимо пользователю направить заявку:

через СУ ИТ http://support.rosatom.ru/sm/index.do

через электронное письмо на п/я 1111@greenatom.ru

звонок в центр поддержки пользователей АО «Гринатом» +7 499 949 49 19, доб. 1111).

Для КИС/ЛИС которым требуется провести тестирование интеграционных потоков с ПДС в контурах предпрод ПДС, тест (зона разработки DEV) или Зоне

Тестирования необходимо завести пользователей и наполнить данными приведенными в приложении 3.

Для заведения пользователя в ИАСУП необходимо:

1.Опередить контур тестирования:

Код тестового ИАСУП «HR0100» и тестового OIM (если тестирование проходит в тестовой зоне разработки DEV ПДС).

Код тестового ИАСУП «GK_IASUP200_Q» и тестового OIM (если тестирование проходит в тестовой зоне тестирования ПДС.

Код тестового ИАСУП «HRC200» и продуктивного OIM (если тестирование проходит в тестовой зоне предпрода ПДС.

2.Направить обращение на портале http://support.rosatom.ru/sm/index.do для заведения пользователя. Пример приведен в приложении 3.

Для зон разработки DEV и тестирования необходимо в теме и кратком содержании указывать: «Просьба создать пользователей в HR0 (HRC) для подключения к ПДС»

В «Описании»:

Если «HR0100» или «GK_IASUP200_Q», то предоставить\завести вымышленные данные.

Обязательные поля для создания пользователя для выпуска УКЭП:

Фамилия
Имя
Отчество
Наименование организация
Электронная почта
Табельный номер
UPN
Телефонный номер подписчика (Мобильный)
ИНН подписчика
СНИЛС подписчика
Серия паспорта
Номер паспорта
Наименование подразделения, выдавшего паспорт
Код подразделения, выдавшего паспорт
Дата выдачи паспорта
Пол
Дата рождения

Дополнительно необходимо указать вымышленные данные для какой организации необходимо завести пользователя:

Наименование организации
ИНН организации
ОРГ организации
GID Организации

Для зоны предпрода ПДС («HRC200») необходимо проверить наличие данных по фактическому Табельному номеру сотрудника.

Обязательные поля для создания пользователя для выпуска УКЭП:

Фамилия
Имя
Отчество
Наименование организация
Электронная почта
Табельный номер
UPN
Телефонный номер подписчика (Мобильный)
ИНН подписчика
СНИЛС подписчика
Серия паспорта
Номер паспорта
Наименование подразделения, выдавшего паспорт
Код подразделения, выдавшего паспорт
Дата выдачи паспорта
Пол
Дата рождения

3.Направить информацию через электронное письмо на п/я andvlsavin@greenatom.ru об успешном заведении пользователей на шаге 2 и дополнительно указать:

1.Данные для выпуска тестового квалицированного сертификата:
ФИО пользователя.
табельный номер.
УЗ в домене GK или INTER.
Email.
Зона интеграции с ПДС.
2.Вымышленные поля организации для заведения в ПДС
Наименование организации
ИНН организации
ОРГ организации
GID Организации

4.11. Требования к идентификации пользователей

Первичная идентификация обеспечивается двумя способами – приём на работу для внутренних пользователей или куратором ПДС от организации для внешних пользователей (прикрепление пользователя к организации отрасли «прикомандированный сотрудник»).

Куратор Организации несет ответственность за идентификацию внешних пользователей организации.

Вторичная идентификация – на основании учётных данных (идентификатора) из доверенного LDAP каталога домена GK либо домена INTER

При необходимости подключения стороннего доверенного LDAP каталога необходимо обеспечить доверительные отношения с доменом GK либо INTER установленным порядком.

4.12. Требования к аутентификации пользователей

4.12.1. Общие сведения (уровни доверия)

Для обеспечения среднего (для подписания неквалифицированными сертификатами) и высокого (для квалицированных сертификатов) уровней доверия в ПДС используется двухфакторная аутентификация.

Должна быть реализована аутентификация пользователей (подписчиков, являющихся пользователями КИС/ЛИС, или системных пользователей) посредством передачи в заголовках запросов при первичном обращении к ПДС:

JWT-токена;

SAML-токена.

При передаче данных о пользователе запрос должен содержать UPN этого пользователя. Токен должен быть подписан доверенным ADFS или IAM.

При подписании электронных документов ЭП должен использоваться второй фактор аутентификации для подписания:

Посредством OTP, отправляемого на электронную почту пользователя, при наложении УНЭП;

Посредством DSS Client (mydss) или pin-кода при наложении УКЭП;

4.12.2. Подтверждение операций

Для операций по подписанию и расшифрованию документа требуется подтверждение операции пользователем в явном виде вторым фактором аутентификации.

Для создания усиленной неквалифицированной электронной подписи (УНЭП) предусматривается передача OTP токена на электронную почту сотрудника. КИС после операции подписания должна отобразить пользователю окно для ввода OTP токена и передать соответствующий запрос в ПДС.

Для создания усиленной квалифицированной электронной подписи (УКЭП) используется сертифицированное средство MyDSS, которое должно быть установлено на мобильный телефон пользователя. В этом случае дополнительных требований к КИС не предъявляется, после запроса на подписание подтверждение вторым фактором осуществляется вне рамок КИС. После подтверждения пользователем КИС получит соответствующий коллбэк с информацией о подписании.

4.12.3. Получение маркера доступа

Для первичной аутентификации в ПДС используются федеративные маркеры (токены) формата SAML или JWT, подписанные доверенными центрами аутентификации ПО «Гринатом». В качестве доверенных центров аутентификации ПДС принимает сервера ADFS корпоративного домена GK и внешнего корпоративного домена Inter, и сервер IAM корпоративного домена GK.

КИС необходимо обеспечить аутентификацию пользователя в указанных центрах аутентификации с передачей в ПДС запросов от имени пользователя с

заголовком x-saml-token при использовании SAML токена или x-jwt-token в случае использования JWT токена.

Адреса доверенных центров аутентификации принимаемых ПДС (сервера ADFS и IAM):

Подробное описание по подключению описано в Приложении 6

4.12.4. Подключение центра идентификации к серверу электронной подписи «ПДС»

В случае, если КИС использует для аутентификации пользователей другой сервер аутентификации, чем указано в приложении 6, но при этом этот сервер также использует каталоги доменных пользователей gk.rosatom.local и inter.interatom.local, указанный сервер аутентификации может быть добавлен в ПДС в качестве доверенного.

Для добавления нового центра аутентификации необходимо согласовать такое добавления с оператором ПДС, и предоставить информацию о домене и открытую часть сертификата, которым подписываются SAML или JWT токены.

5. Описание программного интерфейса для работы с сервисами ПДС

5.1. Общие положения

Подробное описание программного интерфейса для работы с сервисами ПДС с примерами обращений размещены в справочнике запросов по адресам:

https://core-s-tp01.gk.rosatom.local:8443/crypto-service/swagger-ui/index.html

https://core-s-TPDS01.gk.rosatom.local:8443/crypto-service/swagger-ui/index.html

https://core-s-tpds.gk.rosatom.local:8443/crypto-service/swagger-ui/index.html

6. Описание программного интерфейса для работы с Сервисом управления сертификатами

6.1. Получение сформированного запроса на сертификат

КИС может получить данные о сертификате подписчика передав следующий запрос:

(Здесь и далее ссылка действительна для тестового контура ПДС, для других контуров необходимо изменить host адрес в соответствии с приложением №2).

POST https://core-s-tp01.gk.rosatom.local:8443/crypto-service/user/certificate/request

Пример запроса на сертификат ниже:

{
"organizationGid": "__", (Идентификатор организации согласно ЕОС НСИ АО «Гринатом»)
"requestComment": "string",
"user": {
"id": 56, идентификатор пользователя

"orEmail": "string", или почтовый адрес
"orEmployeeId": "string", или табельный номер
"orUpn": "string" или UPN
}
}

В синхронном ответе от ПДС будет сообщение формата:

{
"code": 1,
"message": " Запрос на сертификат принят, пользователь с переданными идентификационными данными не зарегистрирован в системе, выполняется регистрация с последующим выпуском сертификата"
}

(код и текст может меняться в зависимости от ситуации, может быть указание, что у организации отсутствуют свободные подписки для выпуска сертификата)

После обработки запроса и выпуска сертификата ПДС рассылает через ЕСИК БП сообщение на callback сервис системы по сертификату, от нас сообщение уходит в формате CertificateOutDto.

ИЛИ, если пользователь зарегистрирован в системе и сертификат выпущен автоматически, то уведомление с сущностью CertificateDTO будет передано в синхронном ответе. Это сообщение, которое будет, если запросить сертификат по id (GET:/crypto-service/user/certificate/{id}). Сообщение, которое отправляется в ЕСИК БП, по договоренности с владельцами корпоративной шины ЕСИК БП может быть трансформировано в ответе для системы, если это необходимо КИС. В случае если для КИС необходим свой уникальный ответ от шины в формате JSON, а также XML для передачи через SOAP.

6.2. Уведомление о выпущенном сертификате

Для уведомления о выпущенном сертификате подписчику ПДС отправляет уведомление на адрес callback сервиса, разработанного на стороне КИС для получения информации о сертификатах (Требования пункта 5.1).

Обязательные данные для выпуска сертификата приведены в Приложении 4.

В случае отсутствия данных приведенных в Приложении 4, выпуск сертификата не возможен.

6.3. Получение сертификата подписчика

КИС может получить данные о сертификате подписчика передав следующий запрос:

GET https://core-s-tp01.gk.rosatom.local:8443/crypto-service/user/certificate/{идентификатор сертификата}

ПДС ответит сущностью Certificate DTO, пример ответа следующий:

{
"code": 0,
"data": {
"id": 6,
"externalId": "8",
"dateCreated": 1599165872609,
"certificateReceived": 1599165872555,(Дата выпуска)
"status": "VALID",(признак валидный или нет, может быть EXPIRED – истек срок действия, DELETED – отозван/аннулирован)
"validUntil": 1638564272000,(Дата окончания срока действия)
"serialNumber": "2bd255012bacbbbf4e64fc0a309b451a",
"canResendRequest": **false**,
"commonName": "Акционерное общество /"ГРИНАТОМ/": Кондратьев Михаил Сергеевич",
"qualified": **false**,
"user": (Данные пользователя, комы выдан сертификат){
"id": 47,
"email": "_____",
"firstName": "_____"
"middleName": "_____",
"lastName": "_____",
"occupancy": "_____",
"upn": "_____",
"employeeId": "_____"
},
"cloud": **true**
}
}

Также КИС может получить тело сертификата, направив запрос

https://core-s-tp01.gk.rosatom.local:8443/crypto-service/user/certificate-content/{идентификатор сертификата}/

В ответе вернется тело сертификата в формате BASE64:

{
"code": 0,
"data": "BASE^$ сертификата"
}

Или

https://core-s-tp01.gk.rosatom.local:8443/crypto-service/user/certificate-content/{идентификатор сертификата}/stream

для получения тела сертификата в бинарном потоке.

6.4. Получение списка сертификатов подписчика

КИС может получить список сертификатов по пользователю передав следующий запрос:

(Здесь и далее ссылка действительна для тестового контура ПДС, для других контуров необходимо изменить host адрес).

GET https://core-s-tp01.gk.rosatom.local:8443/crypto-service/user/certificate?ownerEmail= {почтовый адрес пользователя}
или
GET https://core-s-tp01.gk.rosatom.local:8443/crypto-service/user/certificate?upn= {upn пользователя в ад}

В качестве ответа ПДС вернет:

{
"code": 0,
"data": [
{
"id": 203, (идентификатор сертификата)
"externalId": "199",
"certHash": "kJ7oxZTNs4gHNEAHSpEF6gu+W2/NwXKy2f0YcOYr+eA=",
"dateCreated": 1604301892271,
"certificateReceived": 1604301892235,
"status": "VALID", (признак валидный или нет, может быть EXPIRED – истек срок действия, DELETED – отозван/аннулирован)
"validUntil": 1643786692000,
"serialNumber": "6f2e7a0067acc7a04734e983928162df",
"canResendRequest": **false**,
"pinCode": "null",
"commonName": "_____",
"template": {
"id": 1,
"title": "Шаблон УНЭП облако по умолчанию",
"active": **true**,
"publishToLdap": **true**
},
"qualified": **false**, (Признак квалифицированности)
"userId": 184, (идентификатор пользователя в ПДС)
"cloud": **true**
}

],
"offset": 0,
"limit": 20,
"total": 1
}

7. Описание программного интерфейса для работы с Сервисом электронной подписи

7.1. Отправка документа

Первым шагом система должна загрузить документ в ПДС, используя метод

POST https://core-s-tp01.gk.rosatom.local:8443/crypto-service/user/document

(Здесь и далее ссылка действительна для тестового контура ПДС, для других контуров необходимо изменить host адрес). Запрос выполняется, используя tls аутентификацию, без токена пользователя.

Пример JSON:

{
"base64Document": "тело документа в base64 или hash сумма документа",
"documentTitle": "Наименование документа",
"fileName": "имя файла.расширение",

"hash": false/true, признак определяющий, что будет подписываться, сам документ или его хэш (рекомендуется использовать хэш только для больших файлов – более 10-ти мегабайт)

"messageForSigner": "Текст сообщения подписанту"(будет передан при передаче второго фактора аутентификации),

"qualified": false/true, (признак, определяющий, какой тип сертификата необходимо использовать для данного документа квалифицированный -true или неквалифицированный – false)

"storageMode": "DELETE_WHEN_SIGNED" (признак хранения документа DELETE_WHEN_SIGNED – по умолчанию – удаляет контент документа в ПДС после полного подписания документа, DO_NOT_SAVE – не сохраняет контент в ПДС, документ подписывается и удаляется, SAVE – хранить до удаления документ)

Внимание!!! Хранение документов в ПДС осуществляется не более 90 дней с момента загрузки.

"signingMode": "REGULAR_ASSIGNING" (значение по умолчанию, в этом случае документ уйдет сразу на подписание пользователю, под чьим токеном загружен документ, и не уйдет на подписание списку пользоваетелей, переданному в блоке signers),

"sourceId": "_____" (идентификатор документа в КИС/ЛИС),

"signers": блок для указания подписантов, в качестве идентификаторов может использоваться

[
{

"orEmail": m41@mail.ru (почта пользователя)
},
{
"orEmployeeId": "123456" (табельный номер пользователя)
},

{
"orUpn": sid43.p.m@gk.rosatom.local (UPN пользователя в AD АО «Гринатом»)
}
]
}

В ответ (синхронный) будет возвращено сообщение следующего формата, описывающее сущность загруженного документа:

{
"code": 0,
"data": {
"id": 313 (идентификатор документа),
"sourceId": "string",
"documentTitle": "string",
"messageForSigner": "string",
"status": "IN_SIGNING" (NEW – в случае, если документ загружен и никому не направлен на подпись и IN SIGNING если документ загружен и сразу направлен на подписание хотя бы одному подписанту, PARTLY_SIGNED – документ подписан хотя бы одной подписью, но не всеми назначенными пользователями),
"dateCreated": 1602255104409 (дата создания, UNIX time),
"fileName": "file.txt",
"storageMode": "DELETE_WHEN_SIGNED",
"signatures" (блок описывающий сущность подписи): [
{
"id": 407 (идентификатор подписи),
"dateCreated": 1602255104410 (дата создания),
"errorCode": 0,
"externalId": "58fc420f-72ab-4ad9-93aa-1b3c1425d3b3",
"signingStatus": "IN_SIGNING" (статус подписания для данной подписи IN_SIGNING – на подписании, пользоьнвателю нужно ввести второй фактор, SIGNED – подписано данной подписью),
"userSecondaryAuthType": "EMAIL" (тип второго фактора аутентификации для данной подписи/пользователя, в случае значения MY_DSS КИС не должна показывать пользователю окно для ввода подтверждающего кода, при остальных значениях – вывод окна для ввода кода требуется),
"certificate": (описание сертификата, который определен для подписи){
"id": 113,
"externalId": "115",

"certHash": "/VkIHVQMBWl9MFDO/ejb7FyHMxofq92IFTCBbDaZbTk=",
"dateCreated": 1602250936594,
"certificateReceived": 1602250936586,
"status": "VALID",
"validUntil": 1641735736000,
"serialNumber": "57d7e1004facc5b44f6bcdda36602e06",
"canResendRequest": **false**,
"pinCode": "null",
"commonName": "string",
"template": {
"id": 1,
"title": "Шаблон УНЭП облако по умолчанию",
"active": **true**
},
"qualified": **false**,
"user": {
"id": 42,
"email": "mipetrikov@mail.ru",
"firstName": "Павел",
"middleName": "Михайлович",
"lastName": "Кузнецов12",
"occupancy": "Администратор"
},
"cloud": **false**
}
}
],
"user" (автор документа, может не совпадать с подписантом): {
"id": 42,
"email": "mipetrikov@mail.ru",
"firstName": "Павел",
"middleName": "Михайлович",
"lastName": "Кузнецов12",
"occupancy": "Администратор"
}
}
}

Вторым шагом необходимо выполнить подписание, используя метод

PATCH https://core-s-tp01.gk.rosatom.local:8443/crypto-service/user/document/sign/{id}

Где id = id документа полученному от ПДС на первом шаге в синхронном ответе.

ВАЖНО: данный запрос должен быть выполнен с JWT или SAML токеном подписанта, указанного в блоке signers на 1-м шаге.

После отправки указанного запроса необходимо отобразить на экране подписанта в КИС/ЛИС окно для ввода OTP кода для подтверждения подписания вторым фактором аутентификации, во всех случаях, кроме случаев "userSecondaryAuthType": "MY_DSS".

Информацию, введенную пользователем, необходимо передать в следующем запросе:

PATCH https://core-s-tp01.gk.rosatom.loca:8443/crypto-service/user/document/submit/{id}/by-pop-code/{OTPCODE}

Где id = id документа полученному от ПДС на 1-м шаге, а OTPCODE – информация, введенная пользователем в окно для ввода OTP

На адрес, указанный КИС/ЛИС, указанный в качестве callback сервиса для получения данных о подписании документа, придет сообщение описывающее сущность загруженного документа, совпадающее с синхронным ответом после загрузки документа и статусом подписи SIGNED.

7.2. Получение подписанного документа

Получение подписи возможно с использованием следующих запросов:

(для получения в виде потока для скачивания) GET https://core-s-tp01.gk.rosatom.loca:8443/crypto-service/user/signature-content/{id}/stream

(для получения в base64) GET https://core-s-tp01.gk.rosatom.loca:8443/crypto-service/user/signature-content/{id}

Где id=id подписи полученное на callback сервис для получения данных о подписании на шаге 10.1.

Подпись можно получать как сразу после подписания одним подписантом, так и, при необходимости, запросить сразу несколько подписей после полного подписания документа.

Указанные методы применимы для получения как присоединенных, так и отсоединенных подписей. В случае присоединенных подписей возвращается файл подписанного документа.

7.3. Отправка пакета документов

Первым шагом система должна загрузить документ в ПДС, используя метод

POST https://core-s-tp01.gk.rosatom.local:8443/crypto-service/user/package

(Здесь и далее ссылка действительна для тестового контура ПДС, для других контуров необходимо изменить host адрес). Запрос может выполнятся, используя tls аутентификацию, без токена пользователя.)

Пример JSON:

```
{
"documents": [
 {
 "base64Document": "Тело документа в base64",
```

"documentTitle": "Документ1 txt",
"fileName": "New Text Document.txt",
"hash": true, (признак, что необходимо подписать хэш сумму – true или сам документ – false)
"sourceId": "735431231" идентификатор документа во внешней системе
},
{
"base64Document": "_____",
"documentTitle": "Документ2 txt",
"fileName": "document2.txt",
"hash": false,
"sourceId": "6650190547"
}
],
"messageForSigner": "Подпишите плиз!",
"packageTitle": "2дока txt",
"qualified": false,
"signers"(блок определяющий подписантов пакета, аналогичен по заполнению подписанию Документа, раздел 9): [
{
"orUpn": "_____"
}

],
"sourceId": "78751075332"
}

В ответ ПДС вернет в синхронном ответе сообщение следующего формата:

{
"code": 0,
"data": {
"id": 117, (идентификатор пакета)
"sourceId": "78751075332",
"dateCreated": 1605260409074,
"status": "NEW",
"packageTitle": "2дока txt",
"messageForSigner": "Подпишите плиз!",
"storageMode": "DELETE_WHEN_SIGNED", (аналогично разделу 9)
"user": {
"id": 2,
"title": null
},
"documents": [
{

"id": 1597, (идентификатор документа)
"sourceId": "735431231",
"documentHash": "KMuKV7weE9+njhwPrpES+VA7y8F8nGdZEQE6Wv9M+Lo=",
(в случае, если hsch=true в запросе)
"documentTitle": "Документ1 txt",
"status": "NEW",
"dateCreated": 1605260409078,
"fileName": "New Text Document.txt"
},
{
"id": 1596, (идентификатор документа)
"sourceId": "6650190547",
"documentHash": "KMuKV7weE9+njhwPrpES+VA7y8F8nGdZEQE6Wv9M+Lo=",
"documentTitle": "Документ2 txt",
"status": "NEW",
"dateCreated": 1605260409075,
"fileName": "климов, трушина и лапшин.txt"
}
]
}
}

Вторым шагом необходимо выполнить подписание, используя метод
PATCH https://core-s-tp01.gk.rosatom.local:8443/crypto-service/user/package/sign/{id}

Где id = id пакета полученному от ПДС на первом шаге в синхронном ответе.

ВАЖНО: данный запрос должен быть выполнен с JWT или SAML токеном подписанта, указанного в блоке signers на 1-м шаге.

После отправки указанного запроса необходимо отобразить на экране подписанта в КИС/ЛИС окно для ввода OTP кода для подтверждения подписания вторым фактором аутентификации, во всех случаях, кроме случаев "userSecondaryAuthType": "MY_DSS".

Информацию, введенную пользователем, необходимо передать в следующем запросе:

PATCH https://core-s-tp01.gk.rosatom.loca:8443/crypto-service/user/package/submit/{id}/by-pop-code/{OTPCODE}

Где id = id пакета полученному от ПДС на 1-м шаге, а OTPCODE – информация, введенная пользователем в окно для ввода OTP

На адрес, указанный КИС/ЛИС, указанный в качестве callback сервиса для получения данных о подписании документа, ДЛЯ КАЖДОГО ДОКУМЕНТА ПАКЕТА придет сообщение описывающее сущность загруженного документа, совпадающее с синхронным ответом после загрузки документа и статусом подписи SIGNED.

7.4. Получение подписанного пакета документов

Для получения подписи по каждому документу пакета необходимо выполнить действия аналогичные получению подписи по документу, раздел 9.2

Установка сертификата

Зашифрование документа

Расшифрование документа

7.5. Снятие хэш-суммы с электронного документа

Снятие хэш-суммы документа доступно КИС при вызове метода

POST https://core-s-tp01.gk.rosatom.local:8443/crypto-service/user/document/hash

В теле запроса необходимо передать JSON следующего формата:

{

"base64Document": "string" (тело документа в кодировке Base64),

"is512BytesHash": true (значение ГОСТ алгоритма для снятия хэш-суммы false - ГОСТ Р 34.10-2012, 256, true - ГОСТ Р 34.10-2012, 512)

}

В синхронном ответе ПДС вернет значение хэш-суммы в следующем формате:

{

"code": 0,

"data": "ASLh5JFuyd66YKGzxeUE1Jghvc/SMypOYTkEl9nD54dwDd6CgFGtpsNxDYHFsv/vw94zMTM8APMIJ3BKEzAISQ==" (значение хэш-суммы)

}

8. Описание программного интерфейса для работы с Сервисом валидации ЭП и сертификатов

8.1. Проверка ЭП, наложенных на электронный документ

Проверка подписи доступна КИС при вызове метода

POST https://core-s-tp01.gk.rosatom.local:8443/crypto-service/user/signature/validate

В теле запроса необходимо передать JSON следующего формата:

{

"documentContent": "string" (тело документа в кодировке Base64 или хэш-сумма),

"hash": false, (true – если передана хэш сумма)

"signature": "string" (тело подписи в кодировке Base64, не заполняется для signatureType = {XMLDSig, PDF, MS_OFFICE}, т.к. является для данных типов всегда присоединенной и входит в состав документа),

"signatureType": "CAdES" (возможные значения XMLDSig, GOST3410, CAdES, PDF, MSOffice, CMS)

}

В ответ на запрос КИС получит синхронный ответ следующего формата:

{
"code": 0,
"data": [
{
"message": string (сообщение о проверке),
"result": true (результат проверки true – соответствует документу, false – не соответствует),
"signerCertificate": "string" (тело сертификата в кодировке Base64 с которым была наложена подпись),
"signerCertificateInfo": (данные о сертификате) {
"subjectName": "CN=, SN=, C=RU, S=77 г Москва, L=г Москва, STREET=/"улица Ордынка Б., д.24/", O=/"Акционерное общество /"/"ГРИНАТОМ/"/"/", OU=, T=, ОГРН=, ИНН=, E=",
"issuerName"(данные удостоверяющего центра): "CN= , O=/"АО /"/"Гринатом/"/"/", OU=TestCA, STREET=/"1-й Нагатинский проезд, д. 10, стр. 1/", L=Москва, S=77 г. Москва, C=RU, ИНН=, ОГРН=",
"notBefore": 1601470752000 (дата выпуска сертификата),
"notAfter": 1640869752000 (дата окончания срока действия сертификата) ,
"serialNumber": "1452A70046ACAD9F46C5D4718A59321C" (номер сертификата),
"thumbprint": "09BDF308C0171A4A196559A0C10078216EE1B674" (отпечаток сертификата)
},
"signatureInfo": {
"signingTime": 1601645740000 (время подписания),
"caDEsType": (тип подписи)
}
}
]
}

9. Описание программного интерфейса для работы с Сервисом актуального статуса сертификатов

9.1. Получение штампа статуса сертификата

Проверка статуса сертификата доступна по ссылке

http://ssca.rosatom.ru/OCSPN/ocsp.srf для неквалифицированных сертификатов.

http://ssca.rosatom.ru/OCSPQ/ocsp.srf для квалифицированных сертификатов.

Для проверки используется протокол OCSP. Описание протокола https://tools.ietf.org/html/rfc6960

10. Описание программного интерфейса для работы с Сервисом меток времени

10.1. Получение штампа времени

Наложение штампа точного времени доступно по ссылкам

http://ssca.rosatom.ru/TSPQ/tsp.srf

http://ssca.rosatom.ru/TSPN/tsp.srf

Ссылки введут на идентичные сервисы, использовать можно любую из двух ссылок.

Для проверки используется протокол TSP. Описание протокола

https://tools.ietf.org/html/rfc3161

Приложение №1. Заявление на интеграционную поддержку ПДС

Заявление на интеграционную поддержку ПДС
(Услуга CLB.32)

ПОДКЛЮЧЕНИЕ/ОТКЛЮЧЕНИЕ « _____ » _____ 202___ г.
(нужное подчеркнуть)

_____
наименование организации, включая организационно-правовую форму

в лице _____
должность

_____
фамилия, имя, отчество

действующего на основании _____
Устав/доверенность/приказ

в рамках оказания услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств запрашивает услугу по интеграционной поддержке «Платформы доверенных сервисов» (далее – ПДС), сервисы, обеспечивающие функционал усиленной электронной подписи Корпоративной информационной системы

_____
Наименование корпоративной информационной системы

Данные по подключению:

Этап подключения	Тестовое подключение контур разработки DEV	+
	Тестовое подключение контур тестирования	
	Тестовое подключение Предпрод Inside	
	Промышленное подключение	
Контур подключения	ЕСИК БП;	+
	Прямое подключение (КСПД)	
	Прямое подключение (Интернет)	
Тип аутентификации:	Для КИС/ЛИС, подключенных через ЕСИК БП: SLD код: _____	+
	Для КИС/ЛИС, подключенных напрямую: сертификат для TLS-аутентификации;	
UPN системного пользователя;	_____@gk.rosatom.local _____@inter.interatom.local	

(заполняется в случае подключения к ПДС напрямую)		
URL сервиса callback (заполняется в случае подключения к ПДС напрямую)		
Включен ли режим callback; (заполняется в случае подключения к ПДС напрямую)	Да	+
	нет	
Сведения о контактном лице, отвечающем за интеграцию с ПДС и техническую поддержку КИС/ЛИС	ФИО, Email, телефон – не менее двух лиц ответственных за ИС интегрированную с ПДС. Название услуги рабочей группы в СУИТ.	

И предоставить доступ к сервисам:

№	Название доверенного сервиса	Тип подписи: квалифицированная(УКЭП) /неквалифицированная(УНЭП)	Необходимость подключения (отметить галочкой)
6.	Сервис управления сертификатами и ключами	УКЭП	
		УНЭП	
		Не требуется	
7.	Сервис электронной подписи	УКЭП	
		УНЭП	
		Не требуется	
8.	Сервис валидации электронной подписи и сертификатов	УКЭП	
		УНЭП	
		Не требуется	
9.	Сервис меток времени	УКЭП	
		УНЭП	
		Не требуется	
10.		УКЭП	
		УНЭП	

	Сервис актуального статуса сертификатов	Не требуется	

Данные по списанию трудозатрат:

Списание затрат на (Поддержка интеграционных процессов)	Бюджет/код услуги
Списание затрат на (Функциональная поддержка)	Бюджет/код услуги

Уполномоченное должностное лицо

_____ _____ _____

(должность) (подпись) (ФИО)

м.п.

Приложение №2. Адреса подключения к ПДС

Адреса подключения к ПДС

1. Тестовый контур для разработчиков (зона разработки DEV):
2. https://core-s-tp01.gk.rosatom.local:8443
3. Тестовый контур для тестирования (зона тестирования):
4. https://core-s-dpds01.gk.rosatom.local:8443
5. Тестовый контур предпрод: https://core-s-tpds.gk.rosatom.local:8443
6. Продуктивный контур INSIDE: https://core-s-pdsb.gk.rosatom.local:8443
7. Продуктивный контур DMZ: https://core-s-pdsp.gk.rosatom.local:8443

Приложение №3. Пример регистрация обращения на портале

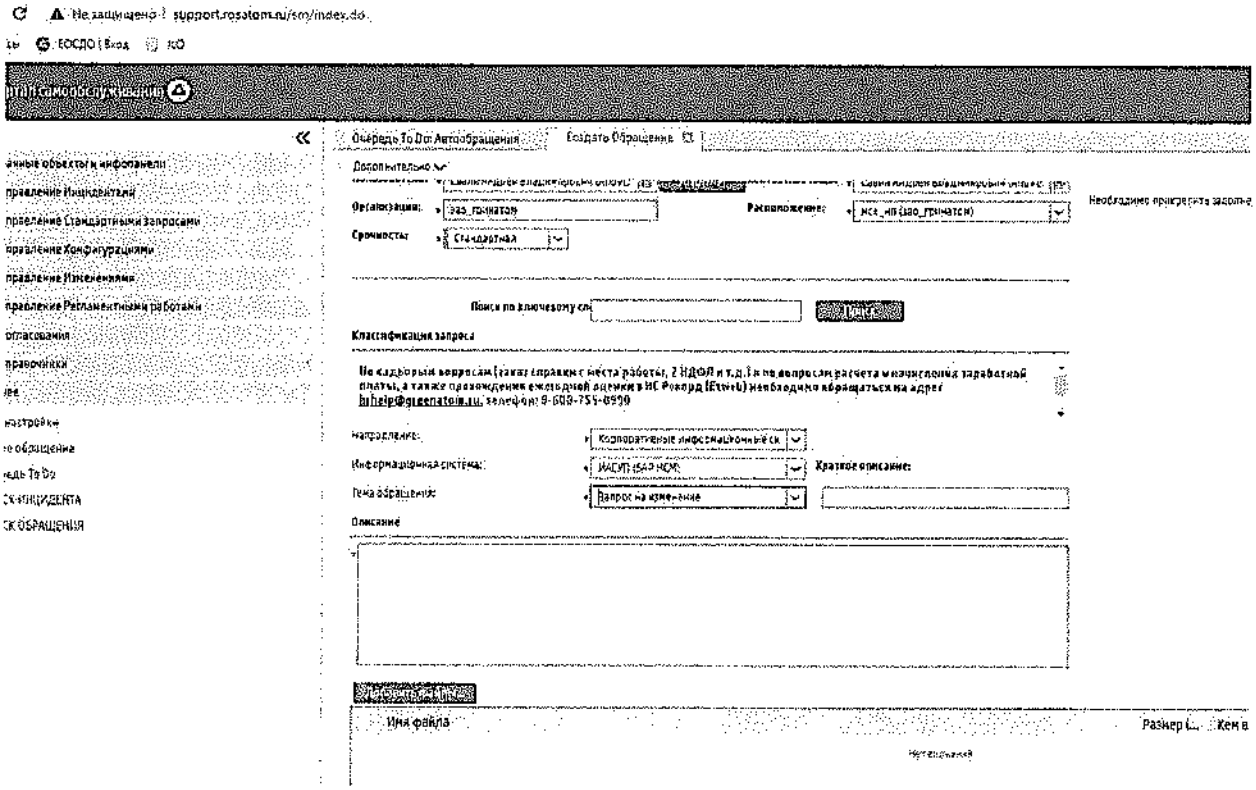

Рис. 2 – регистрация обращения

Приложение №4. Состав полей пользователей, организаций и сертификатов электронной подписи ПДС

Обязательные поля для создания пользователя ПДС для выпуска УНЭП

№	Поле
	Фамилия
	Имя
	Отчество
	GID Организации
	Электронная почта
	Табельный номер
	UPN
	Телефонный номер подписчика

Обязательные поля Организации-заказчика в ПДС для выпуска УНЭП

№	Поле
1.	Наименование организации
	Название улицы, номер дома
	Наименование населенного пункта
	Наименование области
	ИНН организации
	ОРГ организации
	GID Организации

Формат неквалифицированного сертификата ключа проверки электронной подписи

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	CN = Росатом O = АО "Гринатом" OU = ОКЗ STREET = ул. Большая Ордынка д. 24 L = г. Москва S = 77 Москва C = RU ИНН = 007706729736 ОГРН = 1097746819720

Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CN = ФИО O = наименование организации STREET = название улицы, номер дома L = наименование населенного пункта S = наименование области ИНН = ИНН организации ОГРН = ОГРН организации C = RU SN = Фамилия GN = Имя Отчество T = Должность OU = подразделение организации или наименование внешней организации E = Адрес электронной почты Неструктурированное имя = Табельный номер
Public Key	Открытый ключ	Уникальный ключ проверки электронной подписи (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения сертификата		
Private Key Validity Period	Срок действия закрытого ключа, соответствующего сертификату	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Key Usage	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшеный ключ	Могут быть внесены дополнительные области использования
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица удостоверяющего центра, на котором подписан данный сертификат

CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида:
certificatePolicies	Политики сертификата	Обозначение класса средств ЭП владельца квалифицированного сертификата
subjectSignTool		Наименование используемого владельцем квалифицированного сертификата средства ЭП
IssuerSignTool		Полное наименование средства ЭП, которое было использовано для создания ключа ЭП, ключа проверки ЭП и квалифицированного сертификата.
		Конкретный перечень используемых расширений устанавливается удостоверяющим центром
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280 и RFC 5280

Обязательные поля для создания пользователя для выпуска УКЭП

№	Поле
1.	Фамилия
	Имя
	Отчество
	Наименование организация
	Электронная почта
	Табельный номер
	UPN
	Телефонный номер подписчика
	ИНН подписчика
	СНИЛС подписчика
	Серия паспорта
	Номер паспорта
	Наименование подразделения выдавшего паспорт
	Код подразделения выдавшего паспорт
	Дата выдачи паспорта
	Пол
	Дата рождения

Обязательные поля Организации-заказчика в ПДС для выпуска УКЭП

№	Поле

1.	Наименование организации
	Название улицы, номер дома
	Наименование населенного пункта
	Наименование области
	ИНН организации
	ОРГ организации
	GID Организации

Формат квалифицированного сертификата ключа проверки электронной подписи

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	1) commonName (общее имя). 2) countryName (наименование страны). 3) stateOrProvinceName (наименование штата или области). 4) localityName (наименование населенного пункта). 5) streetAddress (название улицы, номер дома). 6) organizationName (наименование организации). 7) organizationUnitName (подразделение организации). 8) title (должность). 9) OGRN (ОГРН). 10) INN (ИНН).
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	1) commonName (общее имя). 2) surname (фамилия). 3) givenName (приобретенное имя). 4) countryName (наименование страны). 5) stateOrProvinceName (наименование штата или области). 6) localityName (наименование населенного пункта). 7) streetAddress (название улицы, номер дома).

		8) organizationName (наименование организации). 9) organizationUnitName (подразделение организации). 10) title (должность). 11) E = электронная почта 12) UnsructuredName (UN) 13) OGRN (ОГРН). 14) SNILS (СНИЛС). 15) INN (ИНН).
Public Key	Открытый ключ	Уникальный ключ проверки электронной подписи (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения сертификата		
Private Key Validity Period	Срок действия закрытого ключа, соответствующего сертификату	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Key Usage	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшеный ключ	Могут быть внесены дополнительные области использования
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида:
certificatePolicies	Политики сертификата	Обозначение класса средств ЭП владельца квалифицированного сертификата
subjectSignTool		Наименование используемого владельцем квалифицированного сертификата средства ЭП

IssuerSignTool		Полное наименование средства ЭП, которое было использовано для создания ключа ЭП, ключа проверки ЭП и квалифицированного сертификата.
		Конкретный перечень используемых расширений устанавливается удостоверяющим центром
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280 и RFC 5280

Приложение №5. Технические условия для подключения к шине ЕСИК БП

Общее описание

Интерфейс взаимодействия информационной системы и интеграционной шины ЕСИК БП должен быть реализован при помощи технологии межсистемного взаимодействия REST API с использованием формата JSON, для информационных систем, которые не поддерживают технологию REST API, для взаимодействия может быть использован протокол SOAP. В этом случае интеграционные сервисы, реализуемые в информационных системах, должны быть созданы на основе интеграционного интерфейса ЕСИК БП, для этого необходимо получить техническое описание интерфейса в формате WSDL.

Для аутентификации в ЕСИК БП на уровне транспорта HTTP должна использоваться "Basic" (базовая) аутентификация (пароль и имя пользователя)

Для каждой подключаемой информационной системы в ЕСИК БП создается своя учетная запись.

Каждой подключаемой информационной системе в ЕСИК БП присваивает уникальный идентификатор системы (SLD код).

С точки зрения организационно-функционального объема автоматизируемых бизнес-процессов информационные системы делятся на три группы:

Информационные системы уровня Корпорации. Системы данной группы автоматизируют бизнес-процессы ряда организаций атомной отрасли, независимо от их принадлежности к тому или иному дивизиону

Информационные системы уровня дивизиона. Системы данной группы автоматизируют бизнес-процессы организаций одного определенного дивизиона

Информационные системы уровня предприятия. Данные системы автоматизируют бизнес-процессы только одной организации

В зависимости от типа ИС, для реализации интеграционного взаимодействия могут использоваться две технологические схемы.

Интеграционное взаимодействие ИС уровня Корпорации реализуются только с использованием ЕСИК БП

Интеграционное взаимодействие с ИС уровня дивизиона и предприятия может быть реализовано с использованием дивизиональной шины, которая в свою очередь должна взаимодействовать с ЕСИК БП.

Исходя из требований по безопасности информации, все информационные системы должны быть сегментированы в зависимости от категории обрабатываемой информации

В зависимости от сегмента сети КСПД, в которой расположена ИС, интеграционное взаимодействие с ИС может осуществляться с одним из контуров ЕСИК БП:

ЕСИК БП(внешний контур) - зона DMZ
ЕСИК БП(внутренний контур) - зона INSIDE

Системный ландшафт ЕСИК БП(внутренний контур) состоит из 3-х серверов:

сервер разработки – зона develop
сервер тестирования – зона develop
продуктивного сервера – зона inside

Исходя из этого интеграционное взаимодействие ЕСИК БП с системой ПДС, организовано следующим образом:

ЕСИК БП (сервер разработки) и ПДС(разработка/тест)
ЕСИК БП (сервер тестирования) и ПДС(разработка/тест)
ЕСИК БП (продуктивный сервер) и ПДС(продуктив)
ЕСИК БП (продуктивный сервер) и ПДС(предпрод)

Параметры для подключения к ЕСИК БП(внутренний контур):
сервер разработки: http://poddb01:51000
сервер тестирования: http://rxtwd:80 или https://rxtwd:443
продуктивный сервер: http://popwd:80 или https://popwd:443

Параметры для подключения к ЕСИК БП(внешний контур):
сервер разработки: http://core-s-aed01:51000
сервер тестирования: http://core-s-aet01:80 или https://core-s-aet01:443
продуктивный сервер: http://aepwd:80 или https://aepwd:443

Приложение №6. Технические условия для подключения к ADFS

Технические условия для подключения к WAP-ADFS

Общее описание работы системы публикации WAP и сервиса ADFS

Система публикации WAP-ADFS

Вводная часть

Система WAP-ADFS служит с одной стороны для публикации веб-приложений (как вариант и прочих приложений), а с другой выступает провайдером аутентификации и идентификации пользователей и назначения им ролей и клеймов (атрибутов).

Система состоит из следующих компонентов:

1. Серверы WAP
2. Серверы ADFS

Подробное описание реализации служб федерации ADFS и публикаций WAP приведено в ТР, может быть предоставлено по запросу.

Роль серверов WAP

Web Application Proxy (прокси-сервер веб-приложений) позволяет публиковать веб-приложения для доступа извне, обеспечивая требуемый уровень безопасности.

Для каждой клиентской сессии WAP устанавливает с одной стороны сессию с клиентом в виде защищенного TLS-туннеля (трафик между клиентом и сервером приложений на отрезке клиент-WAP-сервер идет внутри этого тунеля), а с другой стороны устанавливает сессию с сервером приложений, устанавливая и поддерживая между этими сессиями соответствие.

Публикации приложений на WAP могут быть двух типов:

1. Pass-Through
2. ADFS

Помимо публикаций приложений, WAP сервер осуществляет проксирование ADFS (STS) сервиса. Для этого на WAP-сервере работает компонент ADFS-proxy. В этом смысле Active Directory Federation Service (ADFS) является неотъемлемой частью WAP.

Для приложений, опубликованных с типом ADFS (в отличии от публикаций с типом Pass Through) WAP передает все запросы на подключение службе ADFS, для аутентификации пользователя средствами Active Directory и контроля доступа на основе заявок (Claims Based Access). Помимо этого, публикация с типом ADFS позволяет использовать политики доступа, которые могут основываться на различных факторах, таких, как ip-адрес клиента, вхождение в группы, зоны Intranet и Extranet и пр.) В случае удачи (правильных данных аутентификации и соответствии политикам доступа) ADFS выдает SSO-маркер безопасности, содержащий идентификатор пользователя и ресурса, к которому запрашивались доступ и срок. Информация о разрешениях доступа к приложению сохраняется браузером в Cookies или в приложении, и далее идет соединение с приложением. Приложение после проверки маркера допускает пользователя без ввода пароля.

WAP выполняет функции прокси ADFS, обеспечивая аутентификацию пользователей и контроль доступа на основе заявок (Claims Based Access, CBA) средствами ADFS, принимая HTTPS-запрос на внешний адрес и транслируя его на сервис, работающий по протоколу HTTP или HTTPS.

Краткое описание служб федерации ADFS (Active Directory Federation Services)

Обзор служб федерации Active Directory:

https://docs.microsoft.com/ru-ru/windows-server/identity/ad-fs/ad-fs-overview

Общие сведения о ключевых понятиях AD FS:

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/understanding-key-ad-fs-concepts

https://docs.microsoft.com/ru-ru/windows-server/identity/ad-fs/technical-reference/understanding-key-ad-fs-concepts

Роль серверов ADFS

ADFS – это роль, представленная в ОС Windows Server.

Использование ADFS дает приложению возможность передать процедуру идентификации и аутентификации на сторону ADFS. Приложение может не проверять парольную информацию, приложение может даже не иметь никакой информации об УЗ пользователей: в нем могут быть только роли, определяющие права доступа к компонентам системы, например, к разделам портала. Когда пользователь проходит процедуру аутентификации на ADFS сервере, он получает токен, подтверждающий подлинность УЗ пользователя, идентификатор пользователя (в его качестве может быть выбран произвольный атрибут), а также клеймы - атрибуты УЗ пользователя, группы, которые могут быть сконвертированы в атрибуты, понятные приложению или роли. Правила конвертации атрибутов УЗ в клеймы, понятные приложению, доменных групп в названия ролей, все эти правила описываются в правилах Claim Rules.

Службы ADFS тесно интегрированы с Active Directory. ADFS извлекает атрибуты пользователей из Active Directory, а также проверяет подлинность пользователей в Active Directory. Кроме того, ADFS поддерживает встроенную проверку подлинности Windows.

В качестве стандарта для взаимодействия компонентов федерации ADFS (STS), прикладных подсистем (проверяющих сторон, Relying Party Trusts) и клиентских приложений сервис ADFS на базе Windows 2016 поддерживает следующие стандартны (протоколы):

1. WS-Trust
2. WS-Federation
3. SAML
4. OAuth2.0

Для взаимодействия клиентов и серверных компонентов приложений в качестве транспорта используется протокол HTTPS.

Сервис маркеров доступа (СМД) использует службу каталога Active Directory для аутентификации пользователей и хранения информации о них.

Основными операциями, выполняемыми СМД, являются:

1. Первоначальная аутентификация пользователя
2. Выпуск маркера доступа (Issue)
3. Проверка маркера доступа (Validate)
4. Обновление маркера доступа (Renew)
5. Аннулирование маркера доступа (Cancel)

Маркер доступа выпускается СМД по факту успешной аутентификации пользователя. Маркер доступа однозначно связан с пользователем и достоверно идентифицирует пользователя приложения, являясь, одновременно, унифицированным форматом для передачи данных о пользователе в приложение. В качестве информации для подтверждения своей идентичности пользователь может использовать:

имя пользователя и пароль

сертификат пользователя

Маркер доступа соответствует спецификации SAML (SAML Token), и JWT (JSON Web Token). Для интеграции с системой ПДС требуется формат маркера: JSON.

Сценарии доступа пользователей

Подключение через сеть Интернет с использованием TLS соединения алгоритм ГОСТ

Для пользователей домена GK, подключающихся через сеть Интернет, подключение идет к серверам WAP у которых в биндинге подключения установлен ГОСТ сертификат, а так же ГОСТ сертификат должен быть добавлен в ExternalURL публикации.

ADFS сервер sts1.rosatom.ru

Подключение через сеть Интернет с использованием TLS соединения алгоритм RSA

Для пользователей домена GK, подключающихся через сеть Интернет, подключение идет к серверам WAP у которых в биндинге подключения установлен ГОСТ сертификат, а так же ГОСТ сертификат должен быть добавлен в ExternalURL публикации.

ADFS сервер sts3.rosatom.ru

Подключение через сеть КСПД пользователей домена GK

Для пользователей домена GK, подключающихся через сеть КСПД. Это могут быть предприятия в составе домена GK, так и без подключения к домену GK, но имеющие УЗ в домене, т.е. АРМ в КСПД, но не подключенные к домену GK.

Для АРМов в составе домена GK подключение будет обращено к серверам ADFS, минуя публикации на WAP-серверах. HTTPS запрос принимается WAP сервером (WAP – sts2.rosatom.local). WAP сервер передает запрос серверу ADFS (ADFS – sts2.rosatom.local,) для аутентификации пользователя средствами Active Directory и контроля доступа на основе заявок (Claims Based Access) и JWT (JSON Web Token).

Для АРМов в составе ДЗО подключенных к КСПД, обращение будет идти через WAP-серверы.

ADFS сервер sts2.rosatom.local

Подключение через сеть Интернет для пользователей домена INTER, домена GK

Возможны два сценария работы: Пользователь с аттестованного АРМ из сети домена GK или персонального устройства обращается к ресурсу из сети Internet, при доступе к ресурсу указывает учетные данные из домена INTER.

В данном случае, обращение идет к приложению расположенному в сегменте международного бизнеса (СБИС-МБ) с использование серверов WAP, пользователь должен в обязательном порядке, пройти аутентификацию, на WAP сервере, указав учетную запись от домена INTER. В случае, если приложение поддерживает и настроено на аутентификацию через ADFS, запрос передается серверу ADFS (adfs.rosatom.com). В случае удачи ADFS выдает серверу приложений SSO-маркер безопасности, содержащий идентификатор пользователя и ресурса, к которому запрашивался доступ и срок. Приложение после проверки маркера допускает пользователя без ввода пароля.

ADFS сервер adfs.rosatom.com

Табл. 1. Фермы WAP-ADFS и их параметры

Ферма WAP-ADFS	sts1.rosatom.ru	sts3.rosatom.ru	sts2.rosatom.local	sts2.rosatom.local	adfs.rosatom.com	adfs.rosatom.ru
Продуктивный ландшафт	Продуктивный ландшафт	Продуктивный ландшафт	Продуктивный ландшафт	Продуктивный ландшафт	Продуктивный ландшафт	Продуктивный ландшафт
Публикация веб-приложений	Да	Да	Да	Не используется	Да	Да
Расположение АРМ	АСЗИ, подключение с использованием Интернета	Интернет	АСЗИ в КСПД не в домене GK	АСЗИ в домене GK	АСЗИ в КСПД не в домене GK	АСЗИ в домене GK
Вариант подключения (см. Таблица 2	Вариант 2	Вариант 3	Вариант 1	Вариант 1	Вариант 3	Вариант 3

Варианты подключения)						
Категория пользователей	А, Б	А, Б	А, Б	А, Б	А, Б	А, Б
Классификация информации	Общедоступная, Конфиденциальная информация	Общедоступная	Общедоступная, Конфиденциальная информация	Общедоступная, Конфиденциальная информация	Общедоступная	Общедоступная
Требование к аутентификации	1. Логин и пароль пользователя 2. Токен с сертификатом пользователя	Логин и пароль пользователя	Логин и пароль пользователя	Логин и пароль пользователя (текущие, без дополнительного ввода)	Логин и пароль пользователя	Логин и пароль пользователя
Тип аутентификации	Form Authentication	Form Authentication	Form Authentication	Windows authentication (SSO)	Form Authentication	Form Authentication

Таблица 2 Варианты подключения

Название	Описание
Вариант 1	Доступ к ИТ-ресурсам из локальной вычислительной сети Госкорпорации «Росатом» и организации Госкорпорации «Росатом», аттестованной на соответствие требованиям безопасности информации, посредством КСПД - АСЗИ
Вариант 2	Удаленный доступ пользователя - подключение к ИТ-ресурсам с аттестованного на соответствие требованиям безопасности информации АРМ организации Госкорпорации «Росатом» с

	использованием общедоступных сетей передачи данных. Обмен данными производится по каналу, зашифрованному с использованием сертифицированных СКЗИ.
Вариант 3	Удаленный доступ пользователя - подключение к ИТ-ресурсам с использованием общедоступных сетей передачи данных

Порядок подключения к серверам WAP-ADFS

Для подключения к серверам WAP-ADFS сначала нужно определить, какую ферму требуется использовать, исходя из «Табл. 1. Фермы WAP-ADFS и их параметры».

После этого нужно заполнить шаблоны в «Приложение 6.1. Шаблон СВ для создания новой публикации» и «Приложение 6.2. Параметры приложения на WAP-ADFS»

Для приложения с OAuth2.0 приложить инструкции по настройке ADFS.

Приложение 6.1. Шаблон СВ для создания новой публикации

Табл. 3. Шаблон сетевых взаимодействий для публикации

Пункт №			**Номер порта или диапазон портов источника**	**Приемник (Куда)**		**Протокол взаимодействия**	**Номер порта или диапазон портов приемника**	**Пояснение**
	Филиал, организация	**IP адрес устройства или подсеть**	Пример: 3389, 53, 8085-8090	Филиал, организация	IP адрес устройства или подсеть	Пример: TCP, UDP, TCP/UDP, ICMP	Пример: 3389, 53, 8085-8090	Описание назначения указанных портов
1.	ЦОД	CORE-S-WAPXXX <IP> [DMZ]	1024-65535	ЦОД	CORE-S-xxxxx [10.xx.xx.xx] [имя зоны]	ICMP/TCP/UDP	80,443	**WAP ->APP** WAP -> сервера

Пункт №			Номер порта или диапазон портов источника	Приемник (Куда)		Протокол взаимодействия	Номер порта или диапазон портов приемника	Пояснение
	Филиал, организация	**IP адрес устройства или подсеть**	Пример: 3389, 53, 8085-8090	Филиал, организация	IP адрес устройства или подсеть	Пример: TCP, UDP, TCP/UDP, ICMP	Пример: 3389, 53, 8085-8090	Описание назначения указанных портов
								приложений
2.	ЦОД	CORE-S-xxxx [10.xx.xx.xx] [имя зоны]	1024-65535	ЦОД	stsX.rosatom.ru (local) <IP> CORE-S-ADFS0XXX <IP> [PUBLIC]	TCP/UDP	443	**APP – ADFS** Взаимодействие серверов приложений с серверами ADFS

Приложение 6.2. Параметры приложения на WAP-ADFS

Табл. 4. Информация для реестра Приложений

Название веб-ресурса (Название приложения)	Название сервиса	Услуга	Владелец (менеджер услуги)	Ответственный администратор (ответственная рабочая Группа)

Табл. 5. Параметры публикуемого ресурса на WAP

№ п/п	Имя (имя приложения)	External URL (url для публикации Интернет)	Backend server URL (url сервера в КСПД)	Redirect HTTP to HTTPS (включить/ не включать)	External сертификат[1] Указать CN	Тип аутентификации (Pass-Through/ ADFS)
	URL (без https://)			Включен		

Табл. 6. Тип Application Group на ADFS

№ п/п	Поле	Значение	Обязательное поле, информация предоставляется владельцем системы
	Client ID	Предоставляется заказчиком или формируется автоматически в момент создания	По умолчанию ID формируется автоматически
	Redirect URI	URL системы куда будет отправляться JWT-токен	Информацию предоставляет владелец системы
	Client Permissions (Scope)	По умолчанию добавляем scope'ы: • allatclaims • openid	Опционально, определяет владелец системы
	Issuance Transform Rules	Правило трансформации claim	Опционально, определяет владелец системы

		–Дополнительная информация по Claims доступ на docs.microsoft.com: The Role of Claims: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/the-role-of-claims The Role of the Claims Pipeline: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/the-role-of-the-claims-pipeline The Role of the Claim Rule Language: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/the-role-of-the-claim-rule-language Determine the Type of Claim Rule Template to Use: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/determine-the-type-of-claim-rule-template-to-use	

Доступные scope в ADFS

Scope Name	Description
allatclaims	Requests the access token claims in the identity token.
aza	Scope allows broker client to request primary refresh token
email	Request the email claim for the signed in user
logon_cert	The logon_cert scope allows an application to request logo certificates, which can be used to interactively logon authenticated
openid	Request use of the OpenID Connect authorization protocol
profile	Request profile related claims for the signed in user

user_impersonation	Request Permission for the application to access the resource as the signed in user
vpn_cert	The vpn_cert scope allows an application to request VPN certificates, which can be used to establish VPN connections using EAP-TLS authenticate
winhello_cert	The winhello_cert scope allows an application to request Windows Hello credentials encoded as Certificate.

Дополнительная информация:

Потоки OpenID Connect или OAuth в AD FS и сценарии использования приложений:

https://docs.microsoft.com/ru-ru/windows-server/identity/ad-fs/overview/ad-fs-openid-connect-oauth-flows-scenarios

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/overview/ad-fs-openid-connect-oauth-flows-scenarios

Основные понятия AD FS OpenID Connect / OAuth:

https://docs.microsoft.com/ru-ru/windows-server/identity/ad-fs/development/ad-fs-openid-connect-oauth-concepts

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/development/ad-fs-openid-connect-oauth-concepts

Приложение 6.3. Как подать запрос на создание\публикацию или редактирование в службе ADFS

За настройки сервиса ADFS, и добавления новых RPT и Application отвечает отдел базовых сервисов (ОБС), УЦОД, ДИТ:

- Мальгинов Андрей Владимирович <AVMalginov@Greenatom.ru>
- Ефремов Антон Валерьевич <AntVaEfremov@Greenatom.ru>

Все запросы на создание и редактирование RPT и Application должны быть оформлены, как запрос на изменение в системе СУИТ. Задачи нужно назначать на рабочую группу «админ систем ms»

Приложение №7. Технические условия для подключения к IAM

Общее описание системы идентификации и доступа для работников IAM MAIL.RU – РАБОТНИКИ

Вводная часть

«IAM Mail.ru – работники» (далее по тексту IAM) создан в целях обеспечения защиты хранения и обработки конфиденциальной информации, снижения рисков несанкционированного входа, а также для обеспечения функций единой точки входа для корпоративных систем.

IAM, реализуется продуктом Mail.ru Identity Manager Enterprise (на базе свободного распространяемого ПО «KeyCloak») и представляет собой сертифицированный ФСТЭК России программный комплекс по защите конфиденциальной информации.

IAM реализован как подсистема в составе ИС «Сеть профессиональных сообществ».

Для интеграции информационных систем с IAM необходимо выполнить ряд технических и организационных условий, которые описаны ниже. Также подробно изложены в документе: СИСТЕМА ИДЕНТИФИКАЦИИ И ДОСТУПА ДЛЯ РАБОТНИКОВ «IAM MAIL.RU – РАБОТНИКИ» Технические условия на подключение Версия 1.10. Документ предоставляется по запросу в адрес Клычникова Н. В. (nivklychnikov@greenatom.ru) или сотруднику, замещающему его.

Выполняемые функции

«IAM Mail.ru – работники» реализует следующие функции:

авторизацию и аутентификацию пользователей, сервисов с поддержки SSO, OpenID Connect, Oauth 2.0;

гибкое управление политиками через настройки realm, application и учетных записей пользователей;

синхронизацию пользователей из LDAP и Active Directory;

управление настройками и параметрами Системы;

управление пользователями;

привязка атрибутов пользователей, ролей и иных требуемых атрибутов в токены;

ведение журналов аудита.

«IAM Mail.ru – работники» интегрирована по протоколу SAML 2.0 с провайдером ADFS для использования сквозной аутентификации пользователей сети КСПД, которые выполняют доступ с компьютеров домена GK под управлением ОС Windows. Такие пользователи могут быть автоматически аутентифицированы в «IAM Mail.ru – работники» без необходимости снова указывать свое имя пользователя и пароль. В качестве доверенного провайдера аутентификации для «IAM Mail.ru – работники» может использоваться не только

ADFS, то и любой другой доверенный корпоративный провайдер, поддерживающий протокол SAML 2.0 (функция требует дополнительной настройки «IAM Mail.ru – работники» командой сопровождения).

Примечание: ввиду того, что «IAM Mail.ru – работники» выступает как посредник идентификации (функционал Identity Brokering) только для домена GK. Подключение к системе ПДС с использованием «IAM Mail.ru – работники» возможно только для пользователей с учетными записями в домене GK. Подключение сотрудников с учетными записями в домене INTER с использованием системы идентификации «IAM Mail.ru – работники» невозможно.

«IAM Mail.ru – работники» интегрирована с ГосСОПКА и передает информацию как по собственным событиям безопасности, так и по событиям безопасности связанным с подключаемой системой (подробнее информация описана в пояснительной записке на интеграцию с ГосСОПКА).

Роль «IAM Mail.ru – работники»

Система «IAM Mail.ru – работники» при интеграции с ПДС, выполняет роль посредника идентификации, для УЗ из домена GK.

Общий поток указан на рис. 1

1. Информационная система направляет запрос на проверку данных в IAM-работники

2. IAM пересылает запрос в сторону ADFS домена GK

3. ADFS получает запрос и обращается к каталогу AD домена GK, выполняет проверку реквизитов пользователя.

4. Результат проверки идентификации пользователя возвращается в ADFS

5. ADFS формирует SAML токен, и в которой включена информация о пользователе, токен пересылается в сторону IAM-работники.

6. IAM-работники получает SAML-токен трансформирует токен в формат в JWT и отправляет в сторону Информационной системы (ИС)

7. ИС передает JWT-токен в шину данных ЕСИК-БП

8. Информация из шины данных передается в ПДС

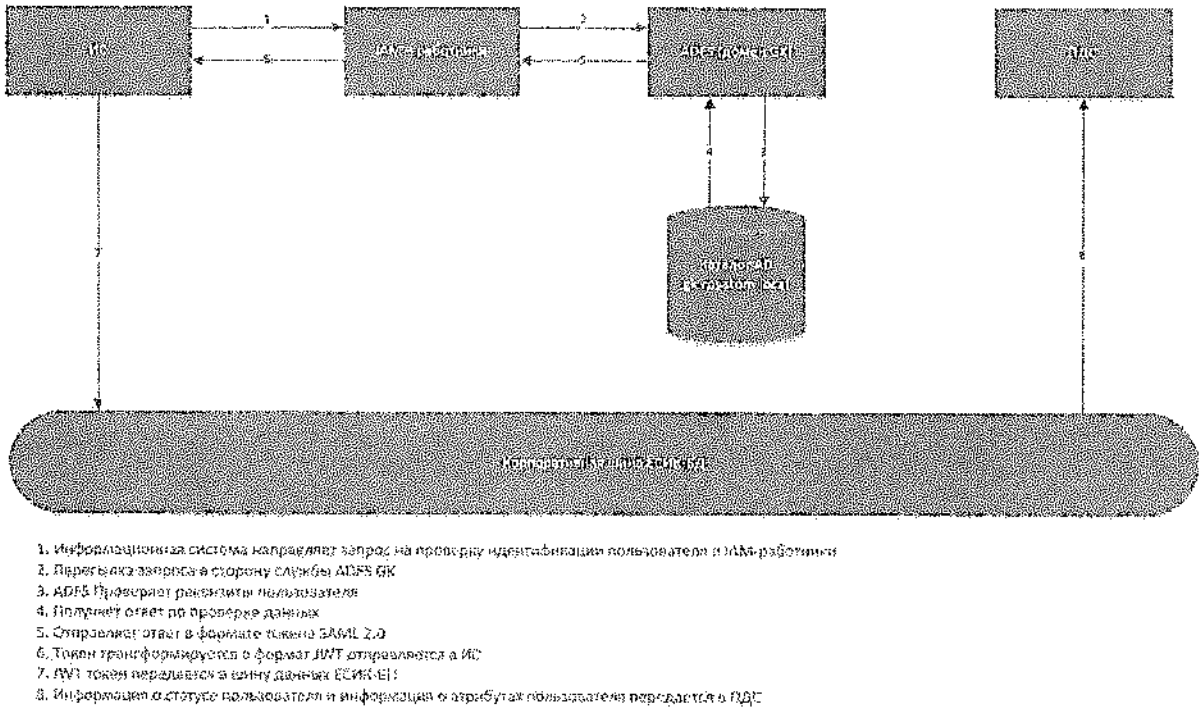

Рис. 3 схема описания передачи идентификационного токена через IAM

Требования для подключения к IAM

Система должна поддерживать взаимодействие по следующим протоколам:

OAuth 2.0;

OpenID Connect.

Для подключение к системе можно использовать как один из готовых адаптеров (библиотека), предоставляемых разработчиками keycloak (https://www.keycloak.org/docs/latest/securing_apps/index.html#supported-platforms), так и выполнять взаимодействие посредством прямого обращения к API.

Необходимо настроить межсетевой экран и открыть сетевые порты от системы в «IAM Mail.ru – работники». Список портов, которые необходимо открыть, представлен в Таблице 7.

Табл. 7. Тип Application Group на ADFS

№	Тип протокола	Номер порта	FQDN	Направление пакетов	Примечание
1.	tcp	443	TEST: iam.tkci.rosatom.local PROD: iam.rosatom.local [ЗКО]	OUTPUT	Запросы от подключаемой ИС к IAM.
2.	tcp	9092, 9093	TEST: kafka1.tkci.rosatom.local	OUTPUT	При необходимости выполнять запись логов

			kafka2.tkci.rosatom.local kafka3.tkci.rosatom.local PROD: kafka1.kci.rosatom.local kafka2.kci.rosatom.local kafka3.kci.rosatom.local [ЗКО]		Authorization Services в Kafka (если используется гранулярное разграничение доступа средствами IAM для подключаемой системы).

OUTPUT – СВ из подключаемой системы в IAM.

Сервера располагаются в тенантах 1TKCI (тестовый контур https://iam.tkci.rosatom.local) и 1KCI (продуктивный контур https://iam.rosatom.local). В случае необходимости получения конкретных IP адресов следует обратиться к Клычникову Никите Валентиновичу (nivklychnikov@greenatom.ru), Лавров Артём Игоревич (ArILavrov@greenatom.ru) или сотруднику, замещающего его.

Технические условия на подключение к «IAM Mail.ru – работники». Заявление на подключение направляется ответственному лицу – Клычникову Никите Валентиновичу (NiVKlychnikov@Greenatom.ru).

Техническая поддержка осуществляется в соответствии с маршрутной картой для ИС «Сеть профессиональных сообществ». Техническая поддержка относится к услуге WEB.45, менеджер услуги Гимон Александр Валерианович.