Система управления доступом
к информационным ресурсам города Москвы (СУДИР)

Регламент подключения к СУДИР

(внешний контур СУДИР)

Листов 12

Москва, 2019

Аннотация

Настоящий документ определяет порядок регистрации приложения во внешнем контуре автоматизированной информационной системы «Система управления доступом к информационным ресурсам города Москвы» (далее – СУДИР, Система).

Содержание

Введение

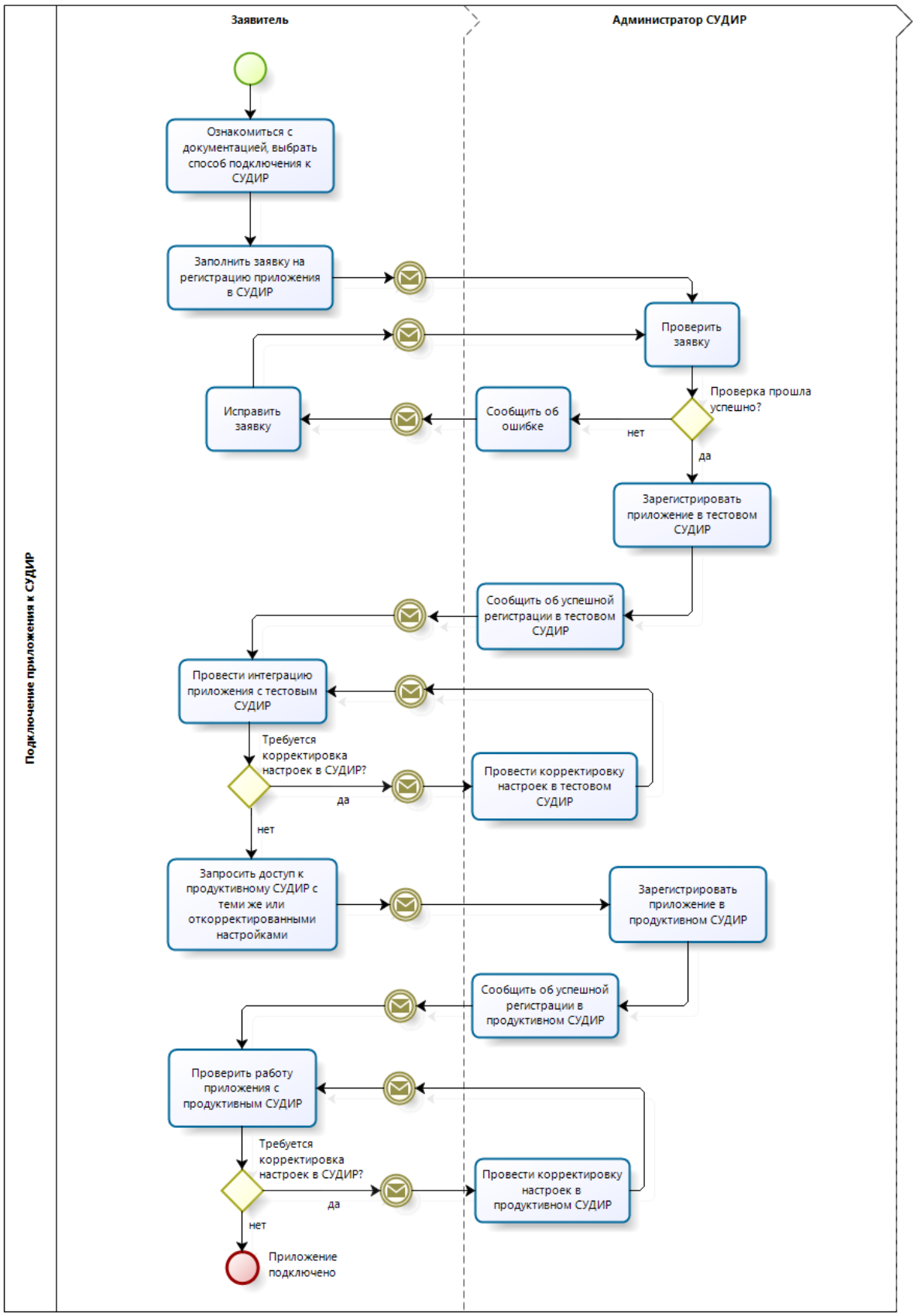
Безопасная достоверная идентификация горожан при онлайн доступе к городским информационным системам – одна из основных задач защиты информации.

Многие сайты и мобильные приложения в целях идентификации требуют от людей заведения новых учетных записей, что создает пользователям сложности при регистрации и необходимость помнить множество связок логин/пароль. Чтобы упростить запоминание, люди начинают повторно использовать один пароль на множестве сайтов и задают простые для подбора пароли. Следствием является невысокий уровень безопасности идентификации, низкая достоверность зарегистрированных учетных записей, что ведет к большому количеству мошенничеств в онлайн и снижению доверия пользователей к интернет-ресурсам.

СУДИР берет на себя решение задачи безопасной достоверной идентификации/аутентификации пользователей при доступе к городским информационным системам.

1. Регламент подключения к СУДИР

1.1 Схема процесса



1.2 Шаги процесса

№	Шаг	Процесс	Входные артефакты	Выходные артефакты	Ответственный
1.	Знакомство с документацией	Заявитель знакомится с документом «Методика подключения к СУДИР (внешний контур)»	Документ «Методика подключения к СУДИР (внешний контур)»	–	Заявитель
2.	Заполнение заявки на регистрацию приложения в СУДИР	Заявитель заполняет заявку на подключение приложения к СУДИР. Заполненная заявка и дополнительные файлы отправляются администратору СУДИР по электронной почте (см. в главе 2)	Шаблон заявки (приведен в главе 1.3) Параметры подключаемого приложения	Заявка и дополнительные файлы отправлены администратору СУДИР	Заявитель
3.	Проверка заявки	Администратор СУДИР проверяет правильность и полноту заполнения заявки, корректность прикрепленных дополнительных файлов Если заявка поступила от сторонней организации, то Администратор СУДИР согласует с ответственным в ДИТ возможность подключения данного приложения	Заявка и дополнительные файлы	Уведомление о необходимости исправить заявку в случае выявления проблем Уведомление об отказе в подключении к СУДИР (в случае если ДИТ не дал разрешения)	Администратор СУДИР
4.	Регистрация в тестовом СУДИР	Администратор СУДИР регистрирует настройки приложения в тестовом СУДИР Администратор СУДИР уведомляет заявителя об успешной регистрации, сообщает параметры подключения к тестовому СУДИР	Заявка и дополнительные файлы	Уведомление об успешной регистрации в тестовом СУДИР Параметры подключения (по шаблону из главы 0)	Администратор СУДИР
5.	Интеграция с тестовым СУДИР	Заявитель отрабатывает интеграцию приложения в тестовом СУДИР. При необходимости заявитель запрашивает корректировку настроек на стороне СУДИР	Приложение	Приложение подключено к тестовому СУДИР	Заявитель
6.	Запрос доступа к продуктивному СУДИР	Заявитель извещает Администратора СУДИР о готовности переключения на промышленный контур СУДИР	Приложение подключено к тестовому СУДИР Уточненные настройки для ПРОД-контура (при необходимости)	Уведомление о готовности переключения на ПРОД. Уточненные настройки для ПРОД-контура (при необходимости)	Заявитель
7.	Регистрация в продуктивном СУДИР	Администратор СУДИР регистрирует настройки приложения в продуктивном контуре СУДИР. За основу берет настройки приложения в тестовом контуре. Вносит корректировки согласно присланным уточнениям для ПРОД-контура. Администратор СУДИР уведомляет заявителя об успешной регистрации, сообщает параметры подключения к продуктивному СУДИР	Уведомление о готовности переключения на ПРОД. Уточненные настройки подключения к ПРОД (при необходимости)	Уведомление об успешной регистрации в продуктивном СУДИР	Администратор СУДИР
8.	Переключение на продуктивный СУДИР	Заявитель переключает приложение на ПРОД-контур СУДИР и проверяет работу При необходимости заявитель запрашивает корректировку настроек на стороне СУДИР и консультируется по возникающим проблемам	Приложение подключено к тестовому СУДИР	Приложение подключено к продуктивному СУДИР	Заявитель

1.3 Шаблон заявки на регистрацию приложения в СУДИР

Внешний контур СУДИР	
Общая информация о подключаемом приложении	
Краткое описание приложения и цели подключения к СУДИР	(рекомендуется заполнить, достаточно одного абзаца о том, для чего используется приложение, и для чего ему подключение к СУДИР)
Организация, являющаяся оператором приложения	(заполнить только если к СУДИР подключается приложение, оператором которого не является ДИТ Москвы. Указать имя организации и ОГРН/ОГРНИП)
Ответственный за приложение от заявителя	
Фамилия, имя, отчество	(обязательно)
Телефон	(обязательно)
Адрес электронной почты	(обязательно)
Дополнительная информация	(необязательно)
Техническая поддержка приложения	
Адрес электронной почты*	(обязательно)
Адрес для оповещений о сбоях и изменениях на стороне СУДИР*	(обязательно)
* – указывайте общие почтовые ящики для приложения, поскольку личные адреса сотрудников могут быть изменены или сотрудники могут быть недоступны, что приведет к нарушению взаимодействия.	
Тестовая среда	
Наименование приложения	(обязательно; как оно будет отображаться на странице аутентификации - "Вход в …")
Адрес (URL) главной страницы	(обязательно)
К СУДИР подключается мобильное приложение и будет использоваться динамическая регистрация клиента?	(отметить эту графу, только если подключается мобильное приложение и будет использоваться динамическая регистрация клиента; при исполнении заявки приложению будут выпущены software_id, Initial Access Token, software_statement)
Адреса страниц, на которые будет перенаправлен пользователь после авторизации (redirect_uri)	(допустимо указать один или несколько разрешенных адресов возврата при входе)
Перечень запрашиваемых разрешений (список scope)	(полный список доступных scope приведен в документе «Методика подключения к СУДИР (внешний контур)»)
Адреса страниц, на которые будет перенаправлен пользователь после логаута (post_logout_redirect_uri)	(допустимо указать один или несколько разрешенных адресов возврата при логауте не заполнять, если логаут не планируется использовать)
Перечень дополнительных атрибутов для передачи в составе id_token	(полный список доступных для передачи в id_token атрибутов приведен в документе «Методика подключения к СУДИР (внешний контур)» не заполнять, если атрибуты из id_token не планируется использовать)
Необходимо ли приложению получать refresh_token?	(если приложение использует refresh_token, то нужно явно указать это, по умолчанию refresh_token приложению предоставляться не будут)
Дополнительная информация и специальные пожелания	(необязательно, заполняется если есть особые требования к подключению к СУДИР, необходимо использовать нестандартный протокол или учесть какие-то особенности подключаемого приложения)

Продуктивная среда	
Наименование приложения	(обязательно; как оно будет отображаться на странице аутентификации - "Вход в …")
Адрес (URL) главной страницы	(обязательно)
К СУДИР подключается мобильное приложение и будет использоваться динамическая регистрация клиента?	(отметить эту графу, только если подключается мобильное приложение и будет использоваться динамическая регистрация клиента; при исполнении заявки приложению будут выпущены software_id, Initial Access Token, software_statement)
Адреса страниц, на которые будет перенаправлен пользователь после авторизации (redirect_uri)	(допустимо указать один или несколько разрешенных адресов возврата при входе)
Перечень запрашиваемых разрешений (список scope)	(полный список доступных scope приведен в документе «Методика подключения к СУДИР (внешний контур)»)
Адреса страниц, на которые будет перенаправлен пользователь после логаута (post_logout_redirect_uri)	(допустимо указать один или несколько разрешенных адресов возврата при логауте не заполнять, если логаут не планируется использовать)
Перечень дополнительных атрибутов для передачи в составе id_token	(полный список доступных для передачи в id_token атрибутов приведен в документе «Методика подключения к СУДИР (внешний контур)» не заполнять, если атрибуты из id_token не планируется использовать)
Необходимо ли приложению получать refresh_token?	(если приложение использует refresh_token, то нужно явно указать это, по умолчанию refresh_token приложению предоставляться не будут)
Дополнительная информация и специальные пожелания	(необязательно, заполняется если есть особые требования к подключению к СУДИР, необходимо использовать нестандартный протокол или учесть какие-то особенности подключаемого приложения)

1.4 Шаблон предоставления администратором СУДИР параметров подключения

1.4.1. В случае подключения веб-приложения

Приложение зарегистрировано в тестовом *(продуктивном)* СУДИР. Для настройки приложения и проверки подключения используйте следующие параметры:

Параметр	Значение	Пояснение
client_id	(заполняется администратором СУДИР)	Идентификатор, присвоенный приложению в СУДИР
client_secret	(заполняется администратором СУДИР)	Секретный код, присвоенный приложению в СУДИР
разрешенные redirect_uri	(заполняется администратором СУДИР)	Зарегистрированные для приложения разрешенные URL-возврата при входе
разрешенные post_logout_redirect_uri	(заполняется администратором СУДИР)	Зарегистрированные для приложения разрешенные URL-возврата при логауте
разрешенные scope	(заполняется администратором СУДИР)	Зарегистрированные для приложения разрешенные OAuth scope
предоставляемые дополнительные атрибуты в составе id_token	(заполняется администратором СУДИР)	Назначенные для передачи приложению в id_token дополнительные атрибуты
включено ли предоставление refresh_token	(заполняется администратором СУДИР)	Будут ли по умолчанию предоставляться приложению refresh_token?
Метаданные СУДИР **ТЕСТ:** https://login-tech.mos.ru/blitz/oauth/.well-known/openid-configuration **ПРОД:** https://login.mos.ru/blitz/oauth/.well-known/openid-configuration		

1.4.2. В случае подключения мобильного приложения

Приложение зарегистрировано в тестовом *(продуктивном)* СУДИР. Для настройки приложения и проверки подключения используйте следующие параметры:

Параметр	Значение	Пояснение
software_id	(заполняется администратором СУДИР)	Идентификатор, присвоенный мобильному приложению в СУДИР
Initial Access Token	(заполняется администратором СУДИР)	Зарегистрированный для мобильного приложения первичный маркер доступа
software_statement	(заполняется администратором СУДИР)	Метаданные приложения в форме JWS-токена
разрешенные redirect_uri	(заполняется администратором СУДИР)	Зарегистрированные для приложения разрешенные URL-возврата при входе

разрешенные post_logout_redirect_uri	(заполняется администратором СУДИР)	Зарегистрированные для приложения разрешенные URL-возврата при логауте
разрешенные scope	(заполняется администратором СУДИР)	Зарегистрированные для приложения разрешенные OAuth scope
предоставляемые дополнительные атрибуты в составе id_token	(заполняется администратором СУДИР)	Назначенные для передачи приложению в id_token дополнительные атрибуты
включено ли предоставление refresh_token	(заполняется администратором СУДИР)	Будут ли по умолчанию предоставляться приложению refresh_token?
Метаданные СУДИР **ТЕСТ:** https://login-tech.mos.ru/blitz/oauth/.well-known/openid-configuration **ПРОД:** https://login.mos.ru/blitz/oauth/.well-known/openid-configuration		

2. Правила коммуникации в процессе подключения к СУДИР

Все обращения Заявителей, описанные в данном Регламенте, должны направляться Администратору СУДИР в электронной форме на адрес: sudir_support@mos.ru.

Первичные заявки, полученные от внешних заявителей (сторонних организаций) Администратор СУДИР согласует с ответственным за СУДИР в ДИТ руководителем.

Заявки, полученные от согласованных ранее заявителей или полученные от сотрудников департамента города Москвы, ответственных за подключаемое приложение, принимаются к исполнению.

В теме сообщения заявки на подключение к СУДИР должно быть указано «Подключение к внешнему СУДИР».

Из текста сообщения должно быть понятно, о подключении какого приложения идет речь. Если приложению ранее был присвоен идентификатор приложения в СУДИР (client_id/software_id), то этот идентификатор должен быть указан в сообщении.

Первичное сообщение на подключение к СУДИР должно содержать заявку на подключение, заполненную на основе шаблона, приведенного в главе 1.3.

Последующие обращения могут как содержать уточненную заявку на подключение, так и просто могут быть изложены в тексте электронного письма.

Для решения проблем, возникающих в процессе интеграции приложения с СУДИР, а также для получения консультаций по вопросам интеграции обращения также направляются на адрес sudir_support@mos.ru. В тексте обращения должна быть описана суть проблемы и приведены контакты технического специалиста, с которым необходимо взаимодействовать в процессе решения проблемы.

> **Внимание!** Все работы по одному обращению должны вестись в режиме ответных писем для возможности отслеживания истории переписки по обращению.

Актуальные версии документов «Методика подключения к СУДИР (внешний контур)» и «Регламент подключения к СУДИР (внешний контур)» размещены на ресурсе «Технологический портал СУДИР» и доступны по адресу https://login.mos.ru/support.

Перечень терминов, сокращений и обозначений

Используемые в настоящем документе сокращения, определения и основные понятия области автоматизированных систем определены в ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения». Также в тексте настоящего документа введены специальные термины на русском и английском языках:

Термин, сокращение, обозначение	Полная форма
JSON	Текстовый формат обмена данных, основанный на JavaScript (JavaScript Object Notation)
JWS	Подписанный JSON-токен (JSON Web Signature)
OAuth	Открытый протокол авторизации
OIDC	Профиль, определяющий способ использования OAuth в процессе идентификации/аутентификации пользователя (OpenID Connect)
URL	Унифицированный указатель ресурса (Uniform Resource Locator)
ГОСТ	Государственный стандарт
СУДИР	Автоматизированная информационная система «Система управления доступом к информационным системам и ресурсам города Москвы»