Приложение № 1
к приказу ООО "Абсолют Технологии"
№ ПА-301123-2 от 30.11.2023

Абсолют Технологии
создаем возможности

Авторизация ЛК ЕСИА. Функциональные характеристики.

г. Москва, 2023 год

ОГЛАВЛЕНИЕ

1. ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК

Сервис авторизации с помощью Личного кабинета Единой системы идентификации и аутентификации (далее Авторизация ЛК ЕСИА) – это механизм, который содержит в себе алгоритм интеграции с ЕСИА OpenId для подключения к личному кабинету компании-клиента. Задача сервиса – обеспечить возможность пользователю веб-решения авторизоваться с помощью его логина и пароля, привязанного к порталу "Госуслуги". Для использования сервиса компании-клиенту необходимо дополнительно получить соответствующее разрешение на использование интеграции на портале "Госуслуги".

Единая система идентификации и аутентификации (ЕСИА) OpenId – это компонент для авторизации на портале "Госуслуги". Решение позволяет гражданам использовать единый логин и пароль на различных порталах и сайтах для получения услуг в электронной форме.

Авторизация ЛК ЕСИА:

- Предоставляет упрощенную возможность интеграции личного кабинета компании-клиента с ЕСИА OpenId
- Обеспечивает возможность пользователю авторизоваться в личном кабинете компании-клиента используя свой логин и пароль, привязанный к порталу "Госуслуги"
- Позволяет управлять ролевой моделью системы авторизации компании-клиента

2. ТЕХНОЛОГИЧЕСКИЙ СТЕК

php - ^8.1.5

Дополнительные модули php

- crypto
- curl
- intl
- json
- mbstring
- mcrypt
- openssl (GOST 28147-89 MAC|GOST R 34.11-2012 with 256 bit hash|GOST R 34.11-2012 with 512 bit hash|GOST R 34.11-94|gost-mac|gost-mac-12)
- pdo_mysql

- Reflection
- SimpleXML
- zip

Фреймворк
- laravel - ^8.83.18

База данных
- mysql - 10.6.11-MariaDB

Панель управления
- Orchid - ^10.5

Openssl ciphers
- GOST2012-GOST8912-GOST8912
- GOST2001-GOST89-GOST89

2.1. ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Раздел содержит наборы персональных данных клиентов.
Доступ к разделу ограничен разрешением Персональные данные пользователей.

2.2. ПОЛЬЗОВАТЕЛИ И РОЛИ

Добавление нового пользователя панели управления доступна как через саму панель, так и через командную строку.

Для добавления через панель, необходимо перейти в раздел Пользователи и роли/ Пользователи и добавить пользователя, указав в разрешениях минимальный набор разрешений (Основное|Вложение). Остальные разрешения добавляются по мере необходимости доступа к отдельным функциям панели управления.

Для добавления пользователя через командную строку, необходимо выполнить следующую команду в корневой директории проекта php artisan orchid:admin и следовать указаниям мастера добавления нового пользователя.

В данном случае пользователь получит все доступные разрешения, при необходимости, ограничить их можно через панель управления в настройках пользователя.

Так же наборы разрешений можно группировать в роли и наделять пользователя функциональными возможностями через добавление определенного набора ролей.

Использование ролей и разрешений равнозначно и сводится к проверке конечного списка разрешений.

2.3. ИНТЕГРАЦИИ

Раздел содержит список всех доступных интеграций с порталом Госуслуг. Доступ к разделу ограничен разрешением Интеграции. Интеграция заключает в себе набор следующих настроек

- **Название** - Название интеграции, используется для идентификации конкретной интеграции
- **Строковый идентификатор** - Уникальный строковый идентификатор интеграции
- **Секретный ключ интеграции** - Секретный ключ, используется для верификации запросов на получение данных
- **Адрес обратного вызова** - Адрес, на который будет произведено перенаправление после успешной авторизации
- **Интеграция активна** - Флаг активности интеграции
- **Дата валидности сертификата** - Пометка о дате истечения срока валидности загруженных сертификатов
- **Мнемоника интеграции** - Мнемоника системы в пространства ЕСИА Госуслуг
- **Адрес портала госуслуг** - Адрес портала Госуслуг
- **Публичный ключ (RSA)** - Публичный ключ в формате RSA
- **Приватный ключ (RSA)** - Приватный ключ в формате RSA
- **Ключ сертификата** - Кодовая фраза сертификата, запролняется при наличии
- **Запрашиваемые наборы доступов** - Наборы доступов запрашиваемые при авторизации

2.4. ЭКСПОРТ СЕРТИФИКАТА

openssl pkcs12 -in p12.pfx -out cert.pem -clcerts -nokeys

openssl pkcs12 -in p12.pfx -out private.key -nocerts -nodes

2.5. ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Раздел содержит наборы персональных данных клиентов. Доступ к разделу ограничен разрешением Персональные данные пользователей.

2.6. ОБЩИЙ ПРОЦЕСС АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЯ

Для авторизации клиента, и получения его персональных данных необходимо выполнить следующую цепочку взаимодействий с сервисом авторизации и порталом Госуслуг.

1. Перенаправляем клиента на системный адрес esia.host/integration-name/auth. Где esia.host - адрес на котором запущен сервис авторизации, integration-name - строковый идентификатор интеграции настроенный в панели управления сервиса.

2. Из полученных настроек интеграции формируется авторизационный адрес портала Гос услуг, с подготовленным набором разрешений и происходит перенаправление клиента на страницу авторизации портала Гос услуг.

3. После успешной авторизации, клиент перенаправляется обратно на системный адрес, где мы получаем все доступные пользовательские данные согласно заявленным разрешениям, сохраняем их в локальной базе данных, формируем внутренний идентификатор клиента и перенаправляем клиента обратно на адрес сайта,

с которого был инициирован процесс авторизации (устанавливается в настройках интеграции)

4. Из параметров адреса забираем идентификатор клиента и секретный ключ, необходимый для верификации запроса на получение персональных данных. Передаем эти данные в метод API сервиса авторизации и получаем в ответе данные по клиенту.

2.7. БЕЗОПАСНОСТЬ

Для обеспечения пользовательских данных используется ряд ограничений при вызове метода API.

1. Ограничение на время активности запроса. Обеспечивается за счет обязательного размещения параметра временной метки timestamp в теле запроса. Возможность повторного выполнения ограничена 5 минутами (возможно изменение данного ограничения параметрами конфигурации).
2. Передача цифровой подписи запроса hash. Формируется на основе структуры и набора данных всего запроса, с участием закрытой части секретного ключа, не передаваемого в теле запроса.
3. Передача секретного клиентского ключа доступа к персональным данным. Доступен только пользователю в момент прохождения авторизации на портале Гос услуг, что позволяет ограничить возможность несанкционированного доступа к чужим клиентским данным.
4. Ограничение на итерирование клиентских идентификаторов, за счет использования случайной последовательности символов в формате UUID для соответствующего идентификатора записи данных.

2.8. РАСЧЕТА ЦИФРОВОЙ ПОДПИСИ ЗАПРОСА

2.8.1. ПАРАМЕТРЫ

- integration - Идентификатор интеграции.
- secret - Секретный ключ интеграции
- timestamp - Текущая временная метка, время жизни запроса не превышает 300 секунд.
- salt - Постоянный секретный ключ стенда.
- uuid - Уникальный идентификатор клиента.
- code - Персональный секретный ключ пользователя.

2.8.2. АЛГОРИТМ

Цифровая подпись запроса - md5 сигнатура данных приведенных к виду {secret}{raw_data_string}{salt}

raw_data_string - Строка в json формате содержащая данные запроса, за исключением параметра hash. Данные предварительно сортируются по ключу в порядке возрастания на всей глубине вложенности.

При формировани json используется следующий набор параметров

- JSON_UNESCAPED_UNICODE - Не кодировать многобайтовые символы Unicode (по умолчанию они кодируются как \uXXXX).
- JSON_UNESCAPED_SLASHES - Не экранировать /.
- JSON_NUMERIC_CHECK - Кодирование строк, содержащих числа, как числа.