1. Обеспечение интеграции портала с ЕСА

1.1. Тестовые учетные записи ЕСА и ЕСИА

Портал для входа использует ЕСА. В тестовой среде ЕСА настроена возможность входа через учетные записи в тестовом контуре ЕСИА (https://esia-portal1.test.gosuslugi.ru).

Временно до готовности в ЕСА функции выбора роли при входе в ЕСА настроен вход для следующих тестовых учетных записей ЕСИА с данными как перезаполнено в ЕСИА:

№	Логин/пароль в тестовой ЕСИА	Тип учетной записи
1	EsiaTest002@yandex.ru / 11111111	Физ.лицо
2	000-000-600 14 / 11111111	Представитель ИП
3	EsiaTest008@yandex.ru / 11111111	Представитель ЮЛ
4	esiatest005@yandex.ru / 11111111	Представитель ЮЛ
5	EsiaTest010@yandex.ru / 11111111	Представитель ОГВ

Тестовые учетные записи ЕСА в одной организации:

№	Логин/пароль в ЕСА	Организация
1	EsiaTest010@yandex.ru / j6BhE5sF	org_id: 61e47d9a-d7b0-4e69-a629-845281a6b927 org_shortname: ОРГАНИЗАЦИЯ 1181280564
2	altai-agro-complex@test.com / dU8e2j3K	
3	mcx_econom3@mail.orb.ru / Yq3fGS4V	
4	mcx_jiv5@mail.orb.ru / Mq8eNryM	

1.2. Вход пользователя в портал через ЕСА, получение данных о пользователе

Портал должен запрашивать идентификацию пользователя в ЕСА. Подключение должно быть выполнено по OpenID Connect.

Для подключения в ЕСА порталу заведены настройки:

- идентификатор приложения (client_id);
- секрет приложения (client_secret);
- префиксы разрешенных обработчиков ответа от ЕСА (redirect_uri);
- разрешенные scope.

Портал через браузер вызывает обработчик https://login.dev-mcx.ru/blitz/oauth/ae и запрашивает получение кода авторизации. В качестве query-параметров указываются:

- scope – запрашиваемые разрешения (scope), для проведения аутентификации должно быть передано разрешение openid и необходимые дополнительные scope для получения

данных пользователя, например, profile (при запросе нескольких scope они передаются одной строкой и отделяются друг от друга пробелом);

- response_type – тип ответа (принимает значение code);
- redirect_uri – ссылка для возврата пользователя в приложение, ссылка должна соответствовать одному из зарегистрированных значений;
- access_type – необходимо ли приложению получать refresh_token, необходимый для получения сведений о пользователе в дальнейшем, когда пользователь будет оффлайн (принимает значение “online“/“offline“, refresh_token предоставляется при access_type=offline) – опциональный параметр, если значение не задано, то поведение определяется настройкой, заданной для указанного приложения в ЕСА;
- state – набор случайных символов, имеющий вид 128-битного идентификатора запроса (используется для защиты от перехвата), это же значение будет возвращено в ответе – опциональный параметр;
- client_id – идентификатор клиента;
- prompt (необязательный параметр) – может принимать один из следующих параметров:
    - none – если при выполнении запроса у ЕСА возникнет потребность отобразить пользователю экран запроса идентификации/аутентификации, то при prompt=none ЕСА не будет этого делать, а вернет системе на ее redirect_uri ошибку login_required. Вызов с параметром prompt=none нужно делать в случае, если приложение хочет проверить наличие у пользователя сессии ЕСА, но не хочет, чтобы при выполнении такой проверки пользователю отобразился экран входа ЕСА;
    - login – при получении такого запроса ЕСА принудительно запросит пользователя пройти идентификацию/аутентификацию, даже если у пользователя уже существует SSO-сессия.

Пример запроса (запрошены разрешения openid и profile):

```
https://login.dev-mcx.ru/blitz/oauth/ae?scope=openid+profile
&response_type=code&access_type=offline &redirect_uri=https%3A%2F%2Fais.company.ru%2Fre
&state=342a2c0c-d9ef-4cd6-b328-b67d9baf6a7f
&client_id=portal-bitrix
```

Пример ответа со значением кода авторизации (*code*) и параметром *state*:

```
https://ais.company.ru/re?code=f954nEzQ08DXju4wxGbSSfCX7TkZ1GvXUR7TzVus8fG
nu4AUl-YIosgax-BLXMeQQAlasD6CN2qG_0KXK5NIjARoKykhuR9IpbuzqeFxS0
&state=342a2c0c-d9ef-4cd6-b328-b67d9baf6a7f
```

Возможные ошибки при вызове /oauth/ae соответствуют RFC 6749 и описаны по ссылке https://tools.ietf.org/html/rfc6749#section-4.1.2.1.

Полученный код авторизации бэкенд портала обменивает на маркеры: маркер доступа,

обновления, идентификации. Для этого делается HTTP POST запрос на обработчик https://login.dev-mcx.ru/blitz/oauth/te, передается HTTP-заголовок Authorization со значением Basic {secret}, где secret – это "client_id:client_secret" (например, ais:topsecret) в формате base64.

Тело запроса должно содержать следующие параметры:

- code – значение кода авторизации, который был ранее получен;
- grant_type – принимает значение authorization_code;
- redirect_uri – ссылка, точно такая же, как ранее передавалась при вызове https://login.dev-mcx.ru/blitz/oauth/ae.

Пример запроса:

```
POST /blitz/oauth/te HTTP/1.1
Host: login.dev-mcx.ru
Authorization: Basic cG9ydGFsLmlhc2l1LmxvY2FsOnBvcnRhbC5pYXNpdS5sb2NhbA==
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache

grant_type=authorization_code&code=FLZHSMMqXTxU8EFW3bse7qOIYqarfbdbxGaDbVflffFENxBltpREKs7dEkN33dFvN
yUggDb2XpP4nyTlUIZUMf4xBDreSmKrOkrVV7qK8GU
&redirect_uri=https%3A%2F%2Fais.company.ru%2Fre
```

В ответ возвращается маркер доступа, маркер обновления и маркер идентификации:

```
{
    "id_token": "eyJ…hb.Ckt…dr.fk2…sQ",
    "access_token": "dOx…ym.wdu…YR.8uF…qv",
    "expires_in": 3600,
    "scope": "openid userinfo",
    "refresh_token": "1lE… Iw",
    "token_type": "bearer"
}
```

Если код был уже использован или истек срок его действия (1 минута) или указан иной redirect_uri, чем при выдаче кода авторизации, то в качестве ответа будет возвращена ошибка. Пример ответа с ошибкой:

```
{
    "error": "invalid_grant",
    "error_description": "The provided authorization grant (e.g., authorization code, resource owner
credentials) or refresh token is invalid, expired, revoked, does not match the redirection URI used
in the authorization request, or was issued to another client."
}
```

Возможные ошибки при вызове /oauth/te соответствуют RFC 6749 и описаны по ссылке https://tools.ietf.org/html/rfc6749#section-5.2.

Полученные от ЕСА маркер идентификации и маркер доступа представляют собой JWT-токены. Из маркеров можно извлечь следующие идентификационные данные пользователя:

- sub – уникальный идентификатор пользователя;
- global_role – код роли пользователя, с которой он вошел через ЕСИА. Возможные

роли:

- P – физическое лицо
- B – представитель ИП
- L – представитель ЮЛ
- A – представитель ОГВ

- org_id (опционально, в случае входа ИП/ЮЛ/ОГВ) – уникальный идентификатор организации;
- rights (опционально, в случае входа ИП/ЮЛ/ОГВ и наличия у пользователей полномочий в своей организации) – список полномочий (ролей) пользователя в организации (ИП/ЮЛ/ОГВ), указанной им при входе.

Примечание: атрибуты global_role, org_id, rights присутствуют только в маркере идентификации и маркере доступа, полученных приложением в момент входа пользователя. В случае получения приложением маркера доступа в обмен на маркер обновления в новом маркере доступа будет присутствовать только атрибут sub, а сессионные атрибуты global_role, org_id, rights будут отсутствовать.

Пример разобранного access_token:


```
{
  "phone_number": "79582025217",
  "email": "EsiaTest015@yandex.ru",
  "family_name": "Воронков",
  "given_name": "Петр",
  "middle_name": "Петрович",
  …
  "sub": "BIP-BXOM2RI",
  "global_role": "L",
  "org_id": "5182b1b6-3d56-4b8d-aecf-d2e6161d673d",
  "rights": [
    "ADMIN_22",
    "USER_1"
  ],
  "jti": "0HYJ0oPUsYLxvcNMqONfxZejf7qON4b1NscEiMAXLZ0",
  "iss": "https://login.dev-mcx.ru",
  "aud": [
    "portal-bitrix"
  ],
  "exp": 1612288958,
  "iat": 1612285358,
  "scope": "profile openid",
  "crid": "N926aOFXWA7X17t1XRGdmg",
  "client_id": "portal-bitrix",
  "amr": [
    "password"
  ]
}
```


Получить данные о пользователе портал может через REST-сервис. Для этого бэкенд портала делается HTTP GET запрос на обработчик https://login.dev-mcx.ru/blitz/oauth/me,

передает HTTP-заголовок Authorization со значением Bearer {access_token}, где access_token – это полученный ранее валидный маркер доступа.

Пример запроса:

```
GET /blitz/oauth/me HTTP/1.1
Host: login.dev-mcx.ru
Authorization: Bearer dOx…ym.wdu…YR.8uF…qv
Cache-Control: no-cache
```

В ответе придет JSON с данными о пользователе.

Пример ответа:

```
{
    "given_name":"Сергей",
    "middle_name":"Петрович",
    "family_name":"Иванов",
    …
    "sub":"6796a37b-000a-4076-945d-0b589895e458"
}
```

Значения атрибутов пользователя заполняются из учетной записи ЕСИА, используемой в ЕСА для идентификации и аутентификации пользователя, или из предварительно созданной в ЕСА учетной записи. Возможные атрибуты и их назначение описаны ниже:

- sub – уникальный идентификатор пользователя;
- family_name – фамилия;
- given_name – имя;
- middle_name – отчество;
- email – адрес электронной почты;
- phone_number – номер мобильного телефона;
- birthdate – дата рождения (формат DD.MM.YYYY);
- birthplace – место рождения;
- passport – паспортные данные (строка с JSON, содержащим компоненты реквизитов паспорта);
- address_reg – адрес регистрации (строка с JSON, содержащим компоненты адреса);
- snils – СНИЛС (строка в формате 123-456-789 00);
- inn – ИНН (строка в формате 770012345678).

1.3. Получение данных об организации по org_id

Портал может получить сведения по любой организации по ее идентификатору org_id, полученному из ЕСА. Для этого портал должен сначала получить маркер доступа на системное разрешение blitz_groups, разрешающее получать системе сведения по любой организации.

Для этого бэкенд портала должен сделать HTTP POST запрос на обработчик

https://login.dev-mcx.ru/blitz/oauth/te, передать HTTP-заголовок Authorization со значением Basic {secret}, где secret – это "client_id:client_secret" (например, ais:topsecret) в формате base64.

Тело запроса должно содержать параметры:

- grant_type, принимающий значение client_credentials;
- scope, принимающий значение blitz_groups.

Пример запроса:

```
POST blitz/oauth/te HTTP/1.1
Host: login.dev-mcx.ru
Content-Type: application/x-www-form-urlencoded
Authorization: Basic ZG5ldm5pay10ZXN0Lm1vcy5ydTphUU56S0JuY2VBQVQwelg
Cache-Control: no-cache

grant_type=client_credentials&scope=blitz_groups
```

В качестве ответа будет возвращен маркер доступа (access_token), время его жизни (expires_in) и тип маркера (token_type).

```
{
    "access_token": "QFiJ9mPgERPuusd36mQvD4mfzYolH_CmuddAJ3YKTOI",
    "expires_in": 3600,
    "token_type": "Bearer"
}
```

Системе рекомендуется получать и кэшировать маркер доступа на время, меньшее чем параметр expires_in, после чего осуществлять получение нового маркера доступа.

Если с использованием просроченного маркера будет вызван какой-либо REST-сервис, описанный в последующих главах, то будет получена ошибка HTTP 401 Unauthorized.

После успешного получения маркера доступа портал может вызывать ECA для получения сведений об организации по org_id. Получить атрибуты организации можно вызовом REST-сервиса https://login.dev-mcx.ru/blitz/api/v2/grps/{id}. Вызов нужно осуществить методом HTTP GET, включить в вызов HTTP-заголовок Authorization со значением Bearer {access_token}, где access_token – это полученный ранее валидный маркер доступа на scope с именем blitz_groups. В качестве id передать значение org_id организации, полученное из пользовательского id_token/access_token. Также в обращении к сервису должен быть передан параметр profile=orgs, указывающий ECA, что запрашиваются группы пользователей, описывающие организации.

Пример запроса:

```
GET /blitz/api/v2/grps/14339e8e-a665-4556-92f1-5c348eff6696/profile=orgs HTTP/1.1
Host: login.dev-mcx.ru
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache
```

Пример ответа:

```
HTTP/1.1 200 OK
{
```

```
    "instanceId":
"Mzg5LWRzOnVpZD01ZjdiMDU4MC1jZDJlLTQxNDYtOGZjNS02ZWI1YTk1YzdiNDIsb3U9c3ViLGRjPXN1ZGlyLGRjPXJlYXhvZnQsZGM9cnU",
    "id": "14339e8e-a665-4556-92f1-5c348eff6696",
    "org_ogrn": "1234567890329",
    "org_inn": "7743151614",
    …
    "profile": "orgs"
}
```


Кроме системных атрибутов instanceId и profile, которые порталу не нужно интерпретировать, могут вернуться следующие атрибуты, описывающие сведения об организации, полученные ЕСА из ЕСИА:

- org_shortname – сокращенное наименование организации;
- org_fullname – полное наименование организации;
- org_type – тип организации (B – ИП, L – ЮЛ, A – ОГВ);
- org_ogrn – ОГРН организации;
- org_inn – ИНН организации;
- org_leg – ОПФ организации;
- org_kpp – КПП организации;
- org_agencyterrange – территориальная принадлежность ОГВ;
- org_agencytype – тип ОГВ по справочнику ЕСИА;
- org_oktmo – ОКТМО организации;
- org_ctts – контакты организации (строчка с JSON-объектом с контактами из ЕСИА: номер телефона, номер факса, адрес электронной почты);
- org_address_leg – юридический адрес организации (строчка с JSON-объектом);
- org_address_post – почтовый адрес организации (строчка с JSON-объектом).

1.4. Получение списка представителей организации по org_id

Помимо данных организации портал может вызывать ЕСА для получения списка представителей организации по org_id. Получить список представителей организации можно вызовом REST-сервиса https://login.dev-mcx.ru/blitz/api/v2/grps/{id}/members. Вызов нужно осуществить методом HTTP GET, включить в вызов HTTP-заголовок Authorization со значением Bearer {access_token}, где access_token – это полученный ранее валидный маркер доступа на scope с именем blitz_groups. В качестве id передать значение org_id организации, полученное из пользовательского id_token/access_token. Также в обращении к сервису должен быть передан параметр profile=orgs, указывающий ЕСА, что запрашиваются группы пользователей, описывающие организации, и параметр expand=true/false, указывающий, нужно ли включать в ответ детальные сведения о пользователях группы (представителях организации).

В результате выполнения запроса ЕСА вернет JSON, содержащий перечень subjectId

(уникальный идентификатор пользователя) представителей организации и дополнительно (если включен expand=true) данные этих представителей.

Пример запроса:

```
GET /blitz/api/v2/grps/61e47d9a-d7b0-4e69-a629-845281a6b927/profile=orgs&expand=false HTTP/1.1
Host: login.dev-mcx.ru
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Cache-Control: no-cache
```

Пример ответа (при expand=false):

```
HTTP/1.1 200 OK
[
    {
        "instanceId": "Mzg5LWRzOnVpZD1CSVAtRVlYVENGQSxvdT1zdWIsZGM9bG9naW4sZGM9dHIsZGM9bG9jYWw",
        "storeId": "389-ds",
        "subjectId": "BIP-EYXTCFA"
    },
    {
        "instanceId":
"Mzg5LWRzOnVpZD1hbHRhaS1hZ3JvLWNvbXBsZXgsb3U9c3ViLGRjPWxvZ2luLGRjPXRyLGRjPWxvY2Fs",
        "storeId": "389-ds",
        "subjectId": "altai-agro-complex"
    }
]
```

Пример ответа (при expand=true):

```
HTTP/1.1 200 OK
[
    {
        "instanceId": "Mzg5LWRzOnVpZD1CSVAtRVlYVENGQSxvdT1zdWIsZGM9bG9naW4sZGM9dHIsZGM9bG9jYWw",
        "storeId": "389-ds",
        "family_name": "Фамилия010",
        "subjectId": "BIP-EYXTCFA",
        "middle_name": "Отчество010",
        "given_name": "Имя010"
    },
    {
        "instanceId":
"Mzg5LWRzOnVpZD1hbHRhaS1hZ3JvLWNvbXBsZXgsb3U9c3ViLGRjPWxvZ2luLGRjPXRyLGRjPWxvY2Fs",
        "storeId": "389-ds",
        "family_name": "Васильев",
        "subjectId": "altai-agro-complex",
        "middle_name": "Петрович",
        "given_name": "Владимир"
    }
]
```

1.5. Сохранение в ЕСА сведений о региональных полномочиях пользователя

У пользователя в рамках его организации может быть задан один или несколько регионов, по которым пользователь уполномочен запрашивать субсидии (если пользователь – представитель ИП/ЮЛ), или по которым пользователь уполномочен администрировать субсидии/атрибуты (если пользователь – представитель Минсельхоза и его региональных подведомственных ОГВ).

Для целей сохранения в ЕСА региональных полномочий в ЕСА заведен справочник региональных полномочий вида ADMIN_XX и USER_XX, где XX – код региона. Например, ADMIN_22 и USER_22 для Алтайского края.

Назначить и отозвать права можно с помощью REST-сервиса

Проверить наличие у пользователя региональных полномочий, назначить и отозвать

права можно с помощью REST-сервиса https://login.dev-mcx.ru/blitz/api/v3/rights. Для этого портал должен получить маркер доступа на системный scope с именем blitz_rights_full_access. Назначение прав выполняется через HTTP PUT вызов сервиса, а отзыв через HTTP DELETE. Пример запроса на назначение:

```
PUT /blitz/api/v3/rights
Host: login.dev-mcx.ru
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache

[{
          "subject": "указать sub пользователя",
          "object": "указать org_id организации",
          "objectType": "grps",
          "rights": ["USER_22"],
          "tags": ["set_from_lk"]
}]
```

Пример запроса на отзыв:

```
DELETE /blitz/api/v3/rights
Host: login.dev-mcx.ru
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache

[{
          "subject": "указать sub пользователя",
          "object": "указать org_id организации",
          "objectType": "grps",
          "rights": ["USER_22"],
          "tags": ["set_from_lk"]
}]
```

Получить права пользователя относительно объекта можно с помощью REST-сервиса https://login.dev-mcx.ru/blitz/api/v3/rights/on/grps/<org_id>?objectExt=orgs.

2. Данные о пользователях и организациях в ЕСА

№	Данные	Тип	Название	Как получить?
1.	Идентификатор (ключ) учетной записи пользователя	Атрибут пользователя, Атрибут (claim) в id_token/access_token	sub	Глава 0
2.	Фамилия	Атрибут пользователя	family_name	Глава 0
3.	Имя	Атрибут пользователя	given_name	Глава 0
4.	Отчество	Атрибут пользователя	middle_name	Глава 0
5.	Адрес электронной почты	Атрибут пользователя	email	Глава 0
6.	Номер мобильного телефона	Атрибут пользователя	phone_number	Глава 0
7.	Дата рождения	Атрибут пользователя	birthdate	Глава 0
8.	Место рождения	Атрибут пользователя	birthplace	Глава 0
9.	Паспортные данные	Атрибут пользователя	passport	Глава 0

№	Данные	Тип	Название	Как получить?
10.	Адрес регистрации	Атрибут пользователя	address_reg	Глава 0
11.	СНИЛС	Атрибут пользователя	snils	Глава 0
12.	ИНН	Атрибут пользователя	inn	Глава 0
13.	Глобальная роль пользователя	Атрибут (claim) в id_token/access_token	global_role	Глава 0
14.	Идентификатор организации, выбранной пользователем при входе	Атрибут (claim) в id_token/access_token	org_id	Глава 0
15.	Сокращенное наименование организации	Атрибут группы	org_shortname	Глава 1.3
16.	Полное наименование организации	Атрибут группы	org_fullname	Глава 1.3
17.	Тип организации	Атрибут группы	org_type	Глава 1.3
18.	ОГРН организации	Атрибут группы	org_ogrn	Глава 1.3
19.	ИНН организации	Атрибут группы	org_inn	Глава 1.3
20.	ОПФ организации	Атрибут группы	org_leg	Глава 1.3
21.	КПП организации	Атрибут группы	org_kpp	Глава 1.3
22.	Территориальная принадлежность ОГВ	Атрибут группы	org_agencyterrange	Глава 1.3
23.	Тип ОГВ по справочнику ЕСИА	Атрибут группы	org_agencytype	Глава 1.3
24.	ОКТМО организации	Атрибут группы	org_oktmo	Глава 1.3
25.	Контакты организации	Атрибут группы	org_ctts	Глава 1.3
26.	Юридический адрес организации	Атрибут группы	org_address_leg	Глава 1.3
27.	Почтовый адрес организации	Атрибут группы	org_address_post	Глава 1.3
28.	Назначенные пользователю в организации регионы	Право доступа пользователя в группе	ADMIN_XX и USER_XX, где XX – код региона	Глава -
29.	Полномочия пользователя в организации	Право доступа пользователя в группе	Справочник возможных полномочий (кроме регионов) пока не определен.	Глава -