Identity Blitz

Сервер аутентификации Blitz Identity Provider

Версия 5.0

РУКОВОДСТВО ПО ИНТЕГРАЦИИ

Москва, 2021

Содержание

ВВЕДЕНИЕ

В данном документе содержится техническая информация о процессе подключения приложений к Blitz Identity Provider. Этот процесс включает следующие этапы:

1. Выбор протокола взаимодействия.
2. Получение регистрационных данных для подключения приложения.
3. Конфигурирование приложения или его доработка для подключения к Blitz Identity Provider.

1. Выбор протокола взаимодействия

При интеграции приложения с Blitz Identity Provider для проведения идентификации и аутентификации пользователя следует выбрать один из протоколов взаимодействия:

- OpenID Connect 1.0 (OIDC)[1]/OAuth 2.0[2] – современный SSO-протокол, изначально ориентированный на работу с веб-приложениями в сети Интернет. Если создается новое приложение, то рекомендуется подключить его к Blitz Identity Provider с использованием OIDC/OAuth 2.0.
- SAML 1.0/1.1/2.0[3] – SSO-протокол, позволяющий подключить различное корпоративное ПО или облачные приложения к сервису входа. Подключаемое приложение возможно имеет встроенную поддержку SAML или такая поддержка может быть добавлена в качестве дополнительной опции или через установку интеграционного коннектора/плагина.

Выбор протокола во многом зависит от того, какое приложение требуется подключить:

- если приложение поддерживает один из SSO-протоколов, то стоит подключать его с использованием данного протокола;
- если предложение не поддерживает протоколы, то следует провести его доработку – в этом случае рекомендуется поддержать взаимодействие по OIDC;
- если приложение только создается, то на этой стадии целесообразно поддержать один из SSO-протоколов – поддержку OIDC реализовать проще, однако при использовании доступных библиотек SAML можно использовать и этот протокол.

В таблице ниже приведены некоторые особенности протоколов OIDC и SAML.

Таблица 1 — Особенности протоколов подключения

	OIDC/OAuth 2.0	**SAML 1.0/1.1/2.0**
Способ обеспечения доверия между приложением и Blitz Identity Provider	Секрет приложения (обычно в виде строки), известный Blitz Identity Provider	Электронная подпись. И запросы на аутентификацию, и ответы – это подписанные XML-документы
Способ взаимодействия	Через веб-браузер пользователя проходит аутентификация. Для завершения аутентификации серверная часть приложения должна	Обычно запрос на аутентификацию и ответ проходят через веб-браузер пользователя. Приложение и

[1] OpenID Connect Core 1.0, см.: https://openid.net/specs/openid-connect-core-1_0.html

[2] RFC 6749 «The OAuth 2.0 Authorization Framework», см.: https://tools.ietf.org/html/rfc6749

[3] См.: https://www.oasis-open.org/standards#samlv2.0

	сформировать HTTP-запрос в адрес Blitz Identity Provider	Blitz Identity Provider могут не иметь сетевой связности
Получение сведений о пользователе	Два способа получения данных о пользователе: – Приложение обращается к REST-сервису Blitz Identity Provider и получает данные о пользователе в формате JSON. Приложение может продолжать получать данные о пользователе, даже когда пользователь завершает свою онлайн-сессию – Приложение получает данные пользователя из маркера идентификации (id_token в форме JWT), полученного от Blitz Identity Provider по результатам входа	Данные о пользователе содержатся в ответе на запрос на аутентификацию в формате XML. Приложение может получать от Blitz Identity Provider данные только в момент входа пользователя
Поддерживаемые приложения	Веб-приложения и мобильные приложения	Веб-приложения

OIDC позволяет реализовать все основные сценарии SAML, но при этом используется более простой JSON/REST-протокол. Существенное преимущество OIDC – поддержка мобильных приложений.

2. Подготовка заявки на подключение

2.1. Подключение приложений по OIDC

Взаимодействие приложения с Blitz Identity Provider при проведении идентификации и аутентификации пользователя осуществляется по спецификации OpenID Connect 1.0 (далее – OIDC)[4], в основе которой лежит фреймворк OAuth 2.0[5].

OIDC является современной спецификацией, описывающей порядок использования OAuth 2.0 при обеспечении идентификации/аутентификации пользователей. OIDC изначально ориентирован на работу с веб-приложениями и мобильными приложениями в сети Интернет.

В таблице ниже приведена краткая характеристика спецификации OIDC.

Таблица 2 – Краткая характеристика спецификации OIDC

Способ обеспечения доверия между приложением и Blitz Identity Provider	Секрет приложения (обычно в виде строки), известный Blitz Identity Provider и приложению
Способ взаимодействия	Через браузер пользователя проходит инициируется идентификация/аутентификация. Для завершения идентификации серверная часть приложения должна сформировать HTTP-запрос в адрес Blitz Identity Provider
Получение сведений о пользователе	Два способа получения данных о пользователе: – приложение обращается к REST-сервису Blitz Identity Provider (пп. 3.5) и получает данные о пользователе в формате JSON. Приложение может продолжать получать данные о пользователе, даже когда пользователь завершает свою онлайн-сессию – приложение получает данные пользователя из маркера идентификации (*id_token* в форме JWT), полученного от Blitz Identity Provider по результатам аутентификации
Поддерживаемые приложения	Веб-приложения и мобильные приложения

Аутентификация в терминологии OIDC/OAuth 2.0 является результатом взаимодействия трех сторон:

– сервиса авторизации (*Authorization Server*) или поставщика ресурса (*Resource Server*), в качестве которых выступает Blitz Identity Provider;

[4] «OpenID Connect Core 1.0», см.: https://openid.net/specs/openid-connect-core-1_0.html

[5] RFC 6748 «The OAuth 2.0 Authorization Framework», см.: https://tools.ietf.org/html/rfc6749

– системы-клиента (*Client*), в качестве которой выступает приложение, которое запрашивает доступ ресурсу (информации и данным пользователя);
– владельца ресурса (*Resource Owner*), в качестве которого выступает пользователь, так как в ходе аутентификации он разрешает доступ к данным о себе.

2.1.1. Регистрация приложения в Blitz Identity Provider

Приложение как система-клиент должно зарегистрироваться в Blitz Identity Provider и получить следующие данные, необходимые для формирования запросов на проведение аутентификации.

При подключении к Blitz Identity Provider веб-приложений:

– идентификатор приложения (*client_id*);
– секрет приложения (*client_secret*).

При подключении к Blitz Identity Provider мобильных приложений:

– идентификатор мобильного приложения (*software_id*);
– первичный маркер доступа (*Initial Access Token*);
– метаданные приложения[6] в форме JWS-токена (*software_statement*).

Для регистрации приложения в Blitz Identity Provider необходимо направить заявку, которая включает в себя следующие сведения:

1. Тип подключаемого приложения (веб-приложение или мобильное приложение).
2. Разрешенные адреса возврата (списки *redirect_uri* и *post_logout_redirect_uri*).
3. Перечень запрашиваемых разрешений (список *scope*).
4. Указание нестандартных режимов, необходимых приложению:
   – приложению необходимо получать *refresh_token* – по умолчанию приложению *refresh_token* возвращаться не будет; при выборе этого режима нужно дополнительно указать требуемый срок действия *refresh_token* (по умолчанию срок действия маркера будет 1 день, максимально можно запросить срок действия 365 дней);
   – приложению необходимо использовать нестандартный сценарий взаимодействия (например, Implicit Flow, Hybrid Flow) – по умолчанию приложению разрешено использовать только Authorization Code Flow;

[6] При разработке мобильного приложения можно использовать как общие Initial Access Token и software_statement для своих iOS/Android-реализаций, так и запросить получение различных наборов Initial Access Token и software_statement для каждой ОС и, возможно, каждой редакции (телефон/планшет) и даже версии приложения. Для простоты дальнейшего изложения в тексте документа будет подразумеваться, что мобильное приложение использует один общий Initial Access Token и один общий software_statement.

- приложению нужно получать маркер доступа в формате JWT – по умолчанию маркер доступа предоставляется в формате opaque;
- приложению нужно получать маркер доступа (*access_token*) с нестандартным сроком действия – стандартно маркер доступа действует 1 час.

> **П р и м е ч а н и е —** При указании в заявке на подключение к Blitz Identity Provider необходимости нестандартных режимов, перечисленных выше, **необходимо предоставить обоснование** причин их необходимости.

5. Перечень дополнительных атрибутов, которые Blitz Identity Provider должен добавить в маркер идентификации (дополнительные атрибуты для передачи в составе *id_token*).
6. Режим входа (вход как физического лица или как представителя организации).

2.1.2. Определение разрешенных адресов возврата

Запрос на проведение идентификации/аутентификации пользователя содержит ссылку возврата при авторизации (*redirect_uri*), куда должен быть возвращен пользователь после прохождения идентификации/аутентификации. Допустимые ссылки возврата должны соответствовать зарегистрированным в Blitz Identity Provider разрешенным префиксам. Если в запросе на идентификацию/аутентификацию указана ссылка возврата, и она не соответствует ни одному из указанных префиксов, то в идентификации/аутентификации будет отказано.

В зависимости от типа подключаемого приложения рекомендуется использовать следующие префиксы ссылок возврата:

- При подключении веб-приложений в качестве префиксов ссылок возврата использовать доменные имена приложений. Например, если после проведения аутентификации требуется вернуть пользователя на *https://domain.com/callback*, то в качестве префикса ссылки возврата следует указать в заявке *https://domain.com*.

> **П р и м е ч а н и е —** при подключении к продуктивной среде Blitz Identity Provider веб-приложение должно использовать в качестве redirect_uri и post_logout_redirect_uri только HTTPS-обработчики. Использование HTTP для взаимодействия с продуктивной средой Blitz Identity Provider запрещено.

- При подключении мобильных приложений в качестве префиксов ссылок возврата рекомендуется указать сами ссылки возврата одного из типов: ссылки типа «private-use URI scheme» (например,

com.example.app:/oauth2redirect/example-provider) или ссылки типа «Universal links»[7] (например, *https://app.example.com/oauth2redirect/example-provider*).

Запрос на проведение логаута содержит ссылку возврата при логауте (*post_logout_redirect_uri*). Эта ссылка указывает, куда должен быть возвращен пользователь после успешно выполненного логаута. Допустимые ссылки возврата должны соответствовать зарегистрированным в Blitz Identity Provider разрешенным префиксам (префикс должен содержать доменное имя приложения и часть пути, минимум, *https://domain.com/*). Если в запросе на логаут указана ссылка возврата, и она не соответствует ни одному из указанных префиксов, то будет отображена ошибка.

2.1.3. Определение запрашиваемых разрешений

Разрешения (*scope* в терминологии OIDC/OAuth 2.0) определяют, какие данные и какие именно права на выполнение каких операций получит приложение по результатам аутентификации. Перечень предусмотренных в Blitz Identity Provider разрешений представлен в таблице 3.

Таблица 3 – Доступные разрешения (scope)

№	Разрешение	Описание	Состав получаемых атрибутов[8]
1.	openid	Техническое разрешение, указывающее на то, что аутентификация проводится согласно спецификации OIDC	При запросе этого *scope* Blitz Identity Provider предоставляет приложению *id_token*. Из *id_token* приложение может получить нужные ему атрибуты пользователя (см. пп. 3.3.4).
2.	profile	Основные данные профиля пользователя	– *sub*– уникальный идентификатор – *family_name* – фамилия – *name* – имя – *middle_name* – отчество – *email* – служебный адрес электронной почты – *phone_number* – номер мобильного телефона
3.	usr_grps	Получение списка групп пользователя	– *groups* – список групп, в которые включен пользователь. Каждая

[7] Ссылки типа «Universal links» доступны начиная с iOS 9 и Android 6.0 и являются предпочтительными для использования. Ссылки «private-use URI scheme» рекомендуется использовать только в случае, если приложение должно работать на более ранних версиях iOS/Android.

[8] Для получения сведений о пользователе используется сервис, описанный в пп. 3.5.

			запись в списке включает следующие атрибуты организации: • *id* – идентификатор группы • *name* – имя группы
4.	native	Разрешение на выполнение сквозного входа в веб-приложение из мобильного приложения	Актуально только для мобильных приложений (пп. 3.4.8).
Список разрешений и набор предоставляемых атрибутов пользователя приведены в качестве образца. Содержание таблицы необходимо скорректировать в зависимости от конкретных настроек, сделанных при внедрении Blitz Identity Provider. См. «Руководство администратора»			

2.1.4. Определение дополнительных атрибутов для включения в id_token

Обычно нет необходимости получать атрибуты пользователя непосредственно из маркера идентификации (*id_token*) – более простым и рекомендуемым способом является получение данных пользователя через вызов REST-сервиса (пп. 3.5).

Если все же необходимо получить сведения о пользователе в составе *id_token* (пп. 3.3.4), то в заявке на подключение необходимо перечислить необходимые для включения в маркер идентификации дополнительные атрибуты. Доступные для получения атрибуты приведены в таблице 4.

Таблица 4 – Возможные дополнительные атрибуты пользователя в id_token

№	Атрибут	Описание
1.	family_name	Фамилия
2.	name	Имя
3.	given_name	Отчество
4.	email	Адрес электронной почты
5.	phone_number	Мобильный телефон
Следующие атрибуты заполняются только если пользователь вошел в Blitz Identity Provider через ЕСИА в качестве сотрудника организации.		
6.	org_id	Идентификатор организации в Blitz Identity Provider
7.	global_role	Выбранная роль при входе через ЕСИА: – P – физическое лицо – B – индивидуальный предприниматель – L – сотрудник юридического лица – A – сотрудник органа государственной власти

8.	org_shortname	ОГРН организации (по сведениям из учетной записи ЕСИА)
9.	org_fullname	ОГРН организации (по сведениям из учетной записи ЕСИА)
10.	org_ogrn	ОГРН организации (по сведениям из учетной записи ЕСИА)
11.	org_inn	ИНН организации[9] (по сведениям из учетной записи ЕСИА)
Список дополнительных атрибутов приведен в качестве образца. Содержание таблицы необходимо скорректировать в зависимости от конкретных настроек, сделанных при внедрении Blitz Identity Provider. См. «Руководство администратора»		

2.2. Подключение приложений по SAML

Аутентификация в терминологии SAML является результатом взаимодействия трех сторон:

- поставщик идентификации (*Identity Provider*), в качестве которого выступает Blitz Identity Provider;
- поставщик услуги (*Service Provider*), в качестве которого выступает подключаемое приложение;
- веб-браузер пользователя (*User Agent*).

Приложение (поставщик услуг) должно быть зарегистрировано в Blitz Identity Provider. Для этого необходимо направить заявку согласно Регламенту подключения к Blitz Identity Provider. Заявка включает XML-файл с метаданными поставщика услуг или значения параметров, необходимые для самостоятельной подготовки метаданных администраторами Blitz Identity Provider.

2.2.1. Подготовка метаданных поставщика услуг

Метаданные поставщика услуг описывают настройки подключения приложения к Blitz Identity Provider (например, URL конечных точек приложения, ключи для проверки ЭП). Для описания метаданных используется язык XML[10].

Метаданные должны быть подготовлены по результатам выполнения работ по добавлению поддержки протокола (п. 4.1).

Если приложение является готовым ПО, поддерживающим SAML, то метаданные должны быть получены согласно документации на это ПО. Обычно такое ПО предоставляет URL, по которому может быть получены метаданные.

---

[9] При аутентификации юридического лица с помощью электронной подписи ИНН организации передается в формате «00 + 10 цифр ИНН юридического лица», при аутентификации юридического лица с помощью учетной записи ЕСИА - в формате «10 цифр ИНН юридического лица».

[10] Подробнее про метаданные SAML см.: https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

Если ПО подключаемого приложения не предусматривает выгрузку метаданных, но в документации на ПО описаны параметры, которые должны быть настроены для подключения приложения, то можно указать эти параметры, так, чтобы метаданные на их основе были самостоятельно подготовлены Администратором Blitz Identity Provider. В этом случае необходимо указать следующие параметры:

1. Идентификатор поставщика услуг (*entityID*) – следует указать, только если приложению необходим конкретный *entityID*. Иначе *entityID* будет самостоятельно присвоен Администратором Blitz Identity Provider.
2. Сертификат[11] открытого ключа приложения (поставщика услуг) – должен быть указан только в случае, если приложение подписывает SAML-запрос при отправке к Blitz Identity Provider. Должны использоваться ключи RSA-2048. Допустимо использовать самоподписанные сертификаты с длительным сроком действия.
3. URL для приема от Blitz Identity Provider SAML-ответа – приложение должно предоставлять обработчик, осуществляющий прием от Blitz Identity Provider SAML-ответов с результатами входа. Обычно эта настройка приложения называется *Assertion Consumer Service*.
4. URL для приема от Blitz Identity Provider запроса на логаут – выборочная настройка. Если приложение поддерживает единый логаут, то оно может предоставлять обработчик единого логаута. Обычно эта настройка приложения называется *Single Logout Service Location*.
5. URL для перенаправления пользователя в приложение после успешного логаута – опциональная настройка. Если приложение поддерживает единый логаут и может инициировать единый выход, то оно может предоставлять URL для возврата пользователя после логаута. Обычно эта настройка приложения называется *Single Logout Service Response Location*.
6. Перечень запрашиваемых атрибутов (*SAML Assertion*).
7. Признак необходимости передачи атрибутов в зашифрованном виде[12].

2.2.2. Перечень запрашиваемых атрибутов (SAML Assertion)

В метаданных указывается перечень атрибутов пользователя (*SAML Assertion*). Предусмотренные в Blitz Identity Provider атрибуты пользователя приведены в таблице ***5***.

[11] Сертификат поставщика услуг отличается от TLS-сертификата подключаемого веб-сайта. Обычно это самоподписанный сертификат с длительным сроком действия.

[12] Атрибуты в SAML-сообщении всегда передаются подписанными. Включать шифрование атрибута целесообразно, если пользователь не должен иметь возможности прочитать значение атрибута.

Таблица 5 — Доступные атрибуты пользователя (SAML Assertion)

№	Атрибут	Описание
1.	logonname	Логин пользователя в домене
2.	surname	Фамилия
3.	firstname	Имя
4.	middlename	Отчество
5.	email	Служебный адрес электронной почты
Список SAML атрибутов приведен в качестве образца. Содержание таблицы необходимо скорректировать в зависимости от конкретных настроек, сделанных при внедрении Blitz Identity Provider. См. «Руководство администратора».		

2.3. Особенности подключения мобильных приложений

При создании в мобильных приложениях функции входа с использованием Blitz Identity Provider рекомендуется учитывать следующие особенности:

- пользователям мобильных приложений неудобно вводить при каждом входе логин и пароль на веб-странице аутентификации Blitz Identity Provider. Вместо этого им привычнее при повторных входах использовать ПИН-код приложения или Touch ID/Face ID;
- пользователь может использовать свою учетную запись Blitz Identity Provider для входа в несколько установок одного и того же мобильного приложения (например, войти в приложение, установленное на iPhone, и войти в это же приложение, установленное на iPad). Пользователь должен иметь возможность отозвать выданные этим установкам приложений права доступа к своим сведениям в Blitz Identity Provider;
- по причинам безопасности нежелательно хранить на устройстве пользователя (внутри сборки мобильного приложения) пароль приложения (*client_secret*), используемый для взаимодействия приложения с Blitz Identity Provider.

Чтобы учесть изложенные выше особенности, в Blitz Identity Provider предусмотрен ряд специальных механизмов, предназначенных для использования мобильными приложениями. Рекомендуемый сценарий взаимодействия мобильного приложения с Blitz Identity Provider описан в пп. 3.4.

2.4. Добавление элементов дизайна приложения на страницу входа

Blitz Identity Provider позволяет поместить элементы дизайна приложения на страницу входа Blitz Identity Provider. При желании создать для подключаемой системы персонифицированную страницу входа нужно отметить соответствующий пункт в заявке на подключение. В этом случае при обработке заявки Администратор Blitz Identity Provider

вместе с данными о зарегистрированных параметрах подключения вышлет шаблон оформления страницы входа.

Шаблон оформления страницы входа представляет собой zip-архив, внутри которого записаны HTML каркаса страницы входа и используемые на странице таблица стилей, изображения, JavaScript обработчики.

Ответственные за подключаемую систему могут скорректировать присланное содержимое, адаптировав тем самым верстку страницы входа под требования дизайна подключаемой системы.

Подготовленный архив темы страницы входа нужно передать Администратору Blitz Identity Provider для загрузки и проверки в тестовом контуре. Если полученный внешний вид страницы входа будет приемлемым, то Администратор Blitz Identity Provider перенесет настройки внешнего вида в ПРОД-контур Blitz Identity Provider.

Ответственность за дальнейшее сопровождение нестандартной темы сохраняется за ее разработчиками (ответственными за подключаемую систему). В случае системных изменений в основной теме Администратор Blitz Identity Provider обращается к ответственным с требованием внести аналогичные изменения в нестандартную тему. В случае если изменения не внесены в отведенный срок, то приложение переключается на использование стандартной темы Blitz Identity Provider.

3. Подключение приложений по OIDC

3.1. Настройки подключения

По результатам рассмотрения направленной заявки и регистрации веб-приложения в Blitz Identity Provider Администратором Blitz Identity Provider будет предоставлена следующая информация:

- идентификатор, присвоенный приложению в Blitz Identity Provider (*client_id*);
- секрет приложения (*client_secret*);
- зарегистрированные для приложения URL возврата при авторизации;
- зарегистрированные для приложения URL возврата при логауте;
- зарегистрированные для приложения разрешения (*scope*).

По результатам исполнения заявки на подключение к Blitz Identity Provider мобильного приложения будет предоставлена следующая информация:

- идентификатор, присвоенный приложению в Blitz Identity Provider (*software_id*);
- первичный маркер доступа (*Initial Access Token*);
- метаданные приложения (*software_statement*);
- зарегистрированные для приложения URL возврата при авторизации;
- зарегистрированные для приложения URL возврата при логауте;
- зарегистрированные для приложения разрешения (*scope*).

Все URL в данном разделе необходимо скорректировать в зависимости от конкретных настроек, сделанных при внедрении Blitz Identity Provider. См. «Руководство администратора».

В целях взаимодействия с Blitz Identity Provider приложение должно использовать следующие адреса:

- URL для проведения авторизации и аутентификации:
  - *https://login-test.company.com/blitz/oauth/ae* (тестовая среда)
  - *https://login.company.com/blitz/oauth/ae* (продуктивная среда)
- URL для получения и обновления маркера доступа:
  - *https://login-test.company.com/blitz/oauth/te* (тестовая среда)
  - *https://login.company.com/blitz/oauth/te* (продуктивная среда)
- URL для получения данных пользователя:
  - *https://login-test.company.com/blitz/oauth/me* (тестовая среда)
  - *https://login.company.com/blitz/oauth/me* (продуктивная среда)
- URL для динамической регистрации экземпляра мобильного приложения:
  - *https://login-test.company.com/blitz/oauth/register* (тестовая среда)
  - *https://login.company.com/blitz/oauth/register* (продуктивная среда)
- URL для получения данных о маркере доступа:

  - *https://login-test.company.com/blitz/oauth/introspect* (тестовая среда)
  - *https://login.company.com/blitz/oauth/introspect* (продуктивная среда)
- URL для выполнения логаута:
  - *https://login-test.company.com/blitz/login/logout* (тестовая среда)
  - *https://login.company.com/blitz/login/logout* (продуктивная среда)

Все эти URL, а также дополнительные сведения, размещены по адресу динамически обновляемых настроек (метаданных) каждой среды Blitz Identity Provider[13]:

- *https://login-test.company.com/blitz/oauth/.well-known/openid-configuration* (тестовая среда)
- *https://login.company.com/blitz/oauth/.well-known/openid-configuration* (продуктивная среда)

Разработчики приложений могут не прописывать все указанные URL в конфигурации своего приложения, а использовать в настойках единую ссылку на метаданные Blitz Identity Provider.

3.2. Готовые библиотеки

Для интеграции приложения с Blitz Identity Provider можно использовать одну из множества готовых OAuth 2.0 библиотек[14] или реализовать взаимодействие самостоятельно.

Для интеграции мобильных приложений с Blitz Identity Provider будет полезен информационный ресурс *https://appauth.io/*, предоставляющий SDK для iOS/Android.

В подразделе 3.3 описан сценарий интеграции с Blitz Identity Provider веб-приложения для проведения идентификации/аутентификации пользователя.

В подразделе 3.4 описан сценарий интеграции с Blitz Identity Provider мобильного приложения для проведения идентификации/аутентификации пользователя.

В разделе 4 описаны предоставляемые Blitz Identity Provider сервисы доступа к информации о пользователе.

[13] RFC 8414 «OAuth 2.0 Authorization Server Metadata», см.: https://tools.ietf.org/html/rfc8414

[14] См.: https://oauth.net/code/#client-libraries

3.3. Подключение веб-приложения

3.3.1. Общие сведения

Взаимодействие веб-приложения с Blitz Identity Provider по OIDC включает в себя следующие этапы[15]:

– приложение через веб-браузер отправляет запрос на идентификацию и аутентификацию пользователя в адрес Blitz Identity Provider;
– Blitz Identity Provider проводит идентификацию/аутентифицирует пользователя;
– Blitz Identity Provider получает согласие пользователя на передачу информации о нем в приложение (для приложений, которые размещены на домене *company.com*, согласие предоставляется автоматически без запроса пользователя);
– Blitz Identity Provider через веб-браузер перенаправляет пользователя обратно в приложение и передает в приложение код авторизации;
– приложение с использованием кода авторизации формирует запрос на получение маркера идентификации, маркера обновления, маркера доступа;
– приложение получает ответ, содержащий необходимые маркеры;
– приложение запрашивает данные пользователя по маркеру доступа. При необходимости приложение может провести проверку маркера идентификации и извлечь из этого маркера идентификатор пользователя и дополнительные атрибуты.

На рисунках 1 – 3 представлены процессы получения кода авторизации, маркеров, данных пользователя.

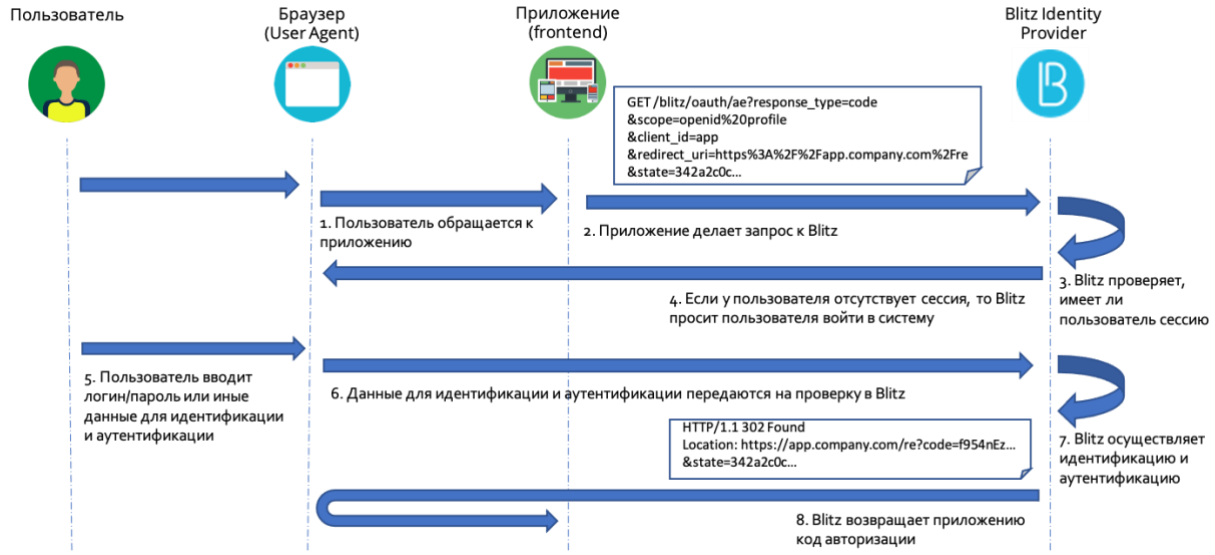

Рисунок 1 – Получение кода авторизации

[15] Данный процесс совпадает с моделью авторизации приложения Authorization Code Grant, предусмотренной спецификацией OAuth 2.0.

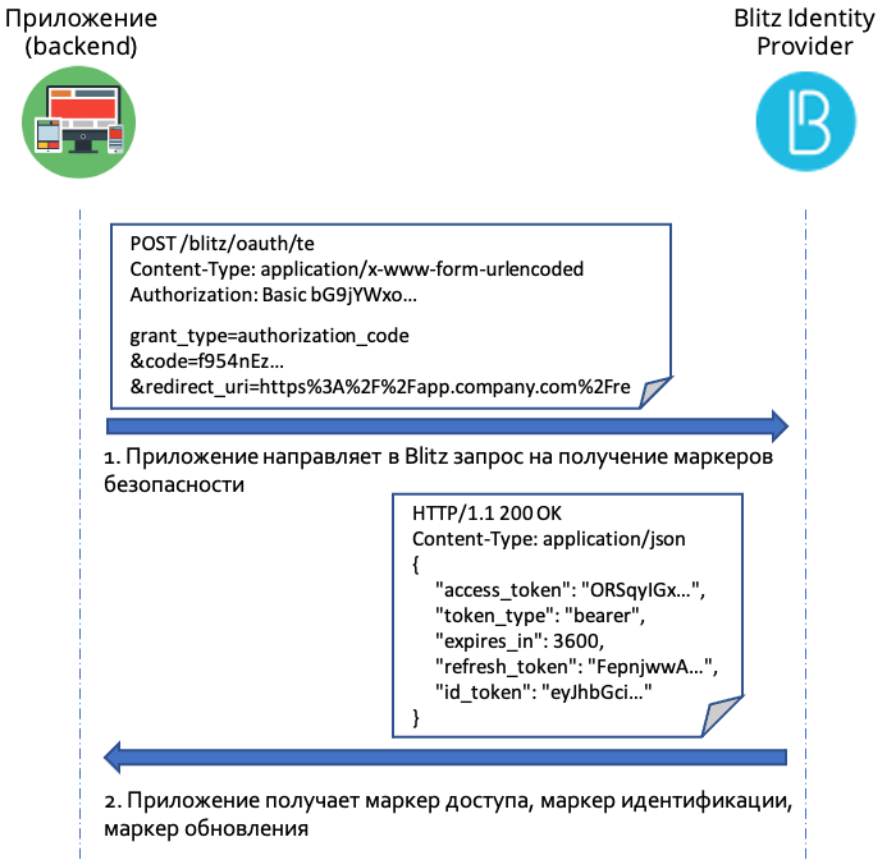

Рисунок 2 – Получение маркеров безопасности

Рисунок 3 – Получение данных пользователя

3.3.2. Запрос на получение кода авторизации

Для проведения идентификации и аутентификации пользователя приложение должно направить пользователя на URL для получения в Blitz Identity Provider кода авторизации, передав в качестве параметров:

- *client_id* – идентификатор клиента;
- *response_type* – тип ответа (принимает значение[16] “code”, “token”, “code token”, “code id_token”, “code id_token token”, “id_token token”, “id_token”);
- *response_mode* (необязательный параметр) – позволяет явно указать требуемый способ передачи кода авторизации. При обычном подключении приложения к Blitz Identity Provider данный параметр передаваться не должен, так как рекомендуется использовать стандартные способы передачи кода авторизации (query – для Authorization Code Flow и fragment – для Implicit/Hybrid Flow).

  Возможные значения параметра response_mode:

  - query – значение кода авторизации (code) возвращается на redirect_uri приложения в форме query-параметра. Стандартный режим для Authorization Code Flow.
  - fragment – значение кода авторизации (code) возвращается на redirect_uri приложения в форме fragment-параметра (#). Стандартный режим для Implicit Flow.
- *scope* – запрашиваемые разрешения, 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);
- *redirect_uri* – ссылка для возврата пользователя в приложение, ссылка должна соответствовать одному из зарегистрированных значений;
- *state* – набор случайных символов, имеющий вид 128-битного идентификатора запроса (используется для защиты от перехвата), это же значение будет возвращено в ответе – опциональный параметр;

[16] Использование иных режимов, кроме “code”, требует специального согласования при подаче заявки на регистрацию приложения в Blitz Identity Provider. Значение параметра response_type указывает выбранный приложением способ взаимодействия с Blitz Identity Provider:
- “code” – Authorization Code Flow;
- “code token”, “code id_token token”, “code id_token token” – Hybrid Flow;
- “id_token token”, “id_token” – OIDC Implicit Flow;
- “token” – OAuth 2.0 Implicit Flow.

- *access_type* (необязательный параметр) – требуется ли приложению получать *refresh_token*, необходимый для получения сведений о пользователе в дальнейшем, когда пользователь будет оффлайн. Принимает значение *online* или *offline*, *refresh_token* предоставляется при *access_type=offline*. Если значение не задано, то поведение определяется настройкой, заданной для указанного приложения в Blitz Identity Provider;
- *prompt* (необязательный параметр) – указывает Blitz Identity Provider требуемый режим входа. Возможные значения параметра prompt:
  - *none* – запрет на аутентификацию. Если при выполнении запроса у Blitz Identity Provider возникнет потребность отобразить пользователю экран запроса идентификации/аутентификации, то Blitz Identity Provider 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 Blitz Identity Provider, но не хочет, чтобы при выполнении такой проверки пользователю отобразился экран входа Blitz Identity Provider.
  - *login* – запрет на SSO. Если при выполнении запроса Blitz Identity Provider выяснит, что пользователь уже проходит идентификацию/аутентификацию ранее, то Blitz Identity Provider явно потребует от пользователя пройти идентификацию/аутентификацию заново. При этом Blitz Identity Provider дополнительно проверит, что вход будет осуществлен именно тем же самым пользователем, пользовательская сессия которого открыта. Если при повторной идентификации/аутентификации пользователь выполнит вход под другой учетной записью, то Blitz Identity Provider вернет системе на ее *redirect_uri* ошибку *login_required*. Вызов с параметром prompt=login нужно делать в случае, если приложение хочет явно запросить у пользователя идентификацию/аутентификацию, например, при доступе к требующей повышенной защиты функции приложения.

Примечание — Для *prompt=login* для приложения можно при необходимости включить иной сценарий обработки ситуации, что пользователь вошел под другой учетной записью, чем был ранее залогинен в сессии. А именно, можно включить, чтобы при вызове *prompt=login* осуществлялся принудительный логаут текущей сессии и создание сессии под новой учетной записью. Такое поведение не является рекомендуемым, но может быть включено для приложения по отдельному запросу.

- *nonce* (необязательный параметр) – строка, используемая для привязки сессии приложения с маркером идентификации. При стандартном подключении приложения к Blitz Identity Provider с использованием Authorization Code Flow

параметр *nonce* использовать нет необходимости. При подключении по Implicit Flow или Hybrid Flow данный параметр должен передаваться. Значение *nonce* должно быть случайной текстовой строкой.

– *bip_action_hint* (необязательный параметр) – указывает Blitz Identity Provider, что страница входа должна открыться в одном из специальных режимов:
  - *open_reg* – открыть в режиме регистрации пользователя; при использовании этого режима можно дополнительно указать параметр *login_hint* со значением email пользователя, и тогда поле «Адрес электронной почты» будет перезаполнено указанным значением email;
  - *open_recovery* – открыть в режиме восстановления пароля; при использовании этого режима можно дополнительно указать параметр *login_hint* со значением email пользователя, и тогда поле «Логин» будет перезаполнено указанным значением email;
  - *used_externalIdps:esia:esia_1* – открыть в режиме входа через ЕСИА;
  - *used_externalIdps:sbrf:sbrf_1* – открыть в режиме входа через Сбер ID;
  - *used_externalIdps:mos:mos_1* – открыть в режиме входа через Mos ID (СУДИР);
  - *used_externalIdps:facebook:facebook_1* – открыть в режиме входа через Facebook;
  - *used_externalIdps:google:google_1* – открыть в режиме входа через Google;
  - *used_externalIdps:mail:mail_1* – открыть в режиме входа через Mail ID;
  - *used_externalIdps:ok:ok_1* – открыть в режиме входа через Одноклассники;
  - *used_externalIdps:vk:vk_1* – открыть в режиме входа через VK;
  - *used_externalIdps:yandex:yandex_1* – открыть в режиме входа через Яндекс;
  - *used_password* – открыть в режиме входа по паролю (поведение по умолчанию);
  - *used_x509* – открыть в режиме входа по электронной подписи;
  - *used_spnego* – открыть в режиме входа по сеансу операционной системы;
  - *used_sms* – открыть в режиме входа по коду в SMS.
– *code_challenge_method* (необязательный параметр) – передается значение “S256”, если подключенное приложение поддерживает спецификацию PKCE[17] для дополнительной защиты взаимодействия с Blitz Identity Provider. Для подключения веб-приложений применение PKCE не является обязательным. Для подключения мобильных приложений к Blitz Identity Provider должен использоваться PKCE.

[17] RFC 7636 «Proof Key for Code Exchange by OAuth Public Clients», см.: https://tools.ietf.org/html/rfc7636

– *code_challenge* (необязательный параметр) – при использовании PKCE в этот параметр передается значение, вычисленное от *code_verifier* по следующей формуле[18]:

```
code_challenge=BASE64URL-ENCODE(SHA256(ASCII(code_verifier)))
```

> **Примечание** — Запрещается открывать страницу входа во фрейме. Пользователь должен видеть URL страницы входа, а также иметь возможность убедиться в наличии HTTPS-соединения веб-порталом *login.company.com*.

Пример запроса на получение кода авторизации (запрошена идентификация/аутентификация и маркер доступа с разрешениями openid и profile):

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

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

```
https://app.company.com/re?code=f954…nS0&state=342a2c0c-d9ef-4cd6-b328-b67d9baf6a7f
```

Возможные ошибки при вызове */oauth/ae* соответствуют RFC 6749 и описаны по ссылке[19].

Пример запроса на получение кода авторизации, при котором Blitz Identity Provider не должен открыть страницу входа в случае, если пользователь еще не проходил идентификацию/аутентификацию в текущем веб-браузере:

```
https://login.company.com/blitz/oauth/ae?client_id=ais
&response_type=code
&scope=openid+profile&access_type=offline
&state=342a2c0c-d9ef-4cd6-b328-b67d9baf6a7f&prompt=none
&redirect_uri=https%3A%2F%2Fapp.company.com%2Fre
```

Пример ответа с ошибкой, если для получения кода авторизации пользователь должен явно пройти идентификацию/аутентификацию на странице входа Blitz Identity Provider, а запрос был выполнен с параметром *prompt=none*:

```
https://app.company.com/re?error=login_required
&error_description=The+Authorization+Server+requires+End-User+authentication…
&state=342a2c0c-d9ef-4cd6-b328-b67d9baf6a7f
```

Пример запроса на получение кода авторизации, при котором Blitz Identity Provider должен осуществить вход в режиме входа через ЕСИА:

```
https://login.company.com/blitz/oauth/ae?client_id=ais
&response type=code
&scope=openid+profile&access type=offline
&state=342a2c0c-d9ef-4cd6-b328-b67d9baf6a7f
&bip_action_hint=used_externalIdps:esia:esia_1
&redirect_uri=https%3A%2F%2Fapp.company.com%2Fre
```

Пример запроса на получение маркера доступа и маркера идентификации с использованием OIDC Implicit Flow:

```
https://login.company.com/blitz/oauth/ae?client_id=ais
&response_type=id_token%20token
&scope=openid+profile
```

[18] При отладке удобно использовать онлайн-калькулятор, см.: https://example-app.com/pkce

[19] См.: https://tools.ietf.org/html/rfc6749#section-4.1.2.1

```
&state=342a2c0c-d9ef-4cd6-b328-b67d9baf6a7f
&nonce=n-0S6_WzA2Mj
&redirect_uri=https%3A%2F%2Fapp.company.com%2Fre
```

Пример ответа от Blitz Identity Provider с маркерами доступа и идентификации, полученными с использованием OIDC Implicit Flow:

```
https://app.company.com/re#access_token=SlAV32hkKG
&token_type=bearer
&id token=eyJ0…NiJ9.eyJ1c…I6IjIifX0.DeWt4Qu…ZXso
&expires in=3600
&state=342a2c0c-d9ef-4cd6-b328-b67d9baf6a7f
```

Пример запроса на получение кода авторизации и маркера идентификации с использованием OIDC Hybrid Flow:

```
https://login.company.com/blitz/oauth/ae?client id=ais
&response_type=code%20id_token
&scope=openid+profile
&state=342a2c0c-d9ef-4cd6-b328-b67d9baf6a7f
&nonce=n-0S6_WzA2Mj
&redirect_uri=https%3A%2F%2Fapp.company.com%2Fre
```

Пример ответа от Blitz Identity Provider с маркерами доступа и идентификации, полученными с использованием OIDC Hybrid Flow:

```
https://app.company.com/re#code=f954…FxS0
&id_token=eyJ0…NiJ9.eyJ1c…I6IjIifX0.DeWt4Qu…ZXso
&state=342a2c0c-d9ef-4cd6-b328-b67d9baf6a7f
```

3.3.3. Получение маркеров

В целях проведения результата идентификации/аутентификации пользователя и получения его данных Blitz Identity Provider выпускает приложению различные маркеры. Перечень маркеров и их назначение приведены в таблице 6.

Таблица 6 – Используемые в Blitz Identity Provider маркеры

№	Название	Обозначение	Предназначение и срок действия
1.	Маркер доступа	*access_token*	Получение доступа к защищенному ресурсу, например, к данным пользователя. Маркер действителен 3600 секунд.
2.	Маркер обновления	*refresh_token*	Обновление маркера доступа. Маркер *refresh_token* предоставляется, только если для приложения при регистрации была указана необходимость получения *refresh_token*, или если в запросе на получение кода авторизации был указан параметр access_type=offline Маркер действителен до момента использования, но не дольше 365 дней.
3.	Маркер идентификации	*id_token*	Получение идентификационной информации, например, идентификатора пользователя. Маркер действителен 3 часа.

После получения кода авторизации приложение должно обменять его на маркеры. Для этого приложение должно сформировать запрос методом POST на URL для получения маркера. Запрос должен содержать заголовок *Authorization* со значением *Basic {secret}*, где *secret* – это *client_id:client_secret* (например, *app:topsecret*) в формате Base64.

> **Примечание** — Сервис получения маркеров должен обязательно вызываться с серверов подключенного к Blitz Identity Provider приложения. Вызов сервиса из выполняемого на стороне веб-браузера программного кода (например, из JavaScript кода веб-страницы) **ЗАПРЕЩАЕТСЯ**. Полученный маркер доступа (access_token) должен обрабатываться серверной частью приложения и не должен передаваться через браузер пользователя.

Пример заголовка:

```
Authorization: Basic YWlzOmNsaWVudF9zZWNyZXQ=
```

Тело запроса должно содержать следующие параметры:

- *code* – значение кода авторизации, который был ранее получен;
- *grant_type* – принимает значение *authorization_code*, если код авторизации обменивается на маркер доступа;
- *redirect_uri* – ссылка, по которой должен быть направлен пользователь после того, как даст разрешение на доступ (то же самое значение, которое было указано в запросе на получение кода авторизации);
- *code_verifier* (только если используется PKCE) – значение проверочного кода, использованного при расчете *code_challenge* при получении кода авторизации.

Пример запроса:

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

grant_type=authorization_code&code=FLZHS…GU
&redirect_uri=https%3A%2F%2Fapp.company.com%2Fre
```

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

Пример ответа с успешным выполнением запроса:

```
{
    "id_token": "eyJhbGciOiJSUzI1NiJ9.eyJub…n0=.Ckt…sQ",
    "access_token": "dO-xym…BE",
    "expires_in": 3600,
    "refresh_token": "1lEWX…Iw",
    "token_type": "bearer"
}
```

Используя полученный маркер доступа, приложение может запросить (пп. 3.5) актуальные данные пользователя из Blitz Identity Provider.

Если код авторизации был уже использован, не совпал *redirect_uri* с ранее использованным в вызове к */oauth/ae*, или истек срок действия кода, либо переданный

code_verifier не соответствует *code_challenge*, то в качестве ответа будет возвращена ошибка.

Пример ответа с ошибкой:

```
{
    "error": "invalid_grant",
    "error description": "The provided authorization grant … is invalid, expired, revoked…"
}
```

Возможные ошибки при вызове /oauth/te соответствуют RFC 6749 и описаны по ссылке[20].

Для обновления маркера доступа приложение должно сформировать запрос методом POST на URL для получения и обновления маркера. Запрос должен содержать аналогичный заголовок *Authorization*, а также следующие параметры в теле запроса:

- *refresh_token* – маркер обновления;
- *grant_type* – принимает значение *refresh_token*, если маркер обновления обменивается на маркер доступа.

Пример запроса:

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

grant_type=refresh_token&refresh_token=jj2DA…bQ
```

3.3.4. Маркер идентификации. Получение данных идентификации

Для получения данных об идентификации и аутентификации приложение может самостоятельно анализировать содержание маркера идентификации (*id_token*). Но можно это не делать, а использовать полученный маркер доступа для запроса в Blitz Identity Provider через специальный сервис (пп. 3.5) актуальных данных пользователя.

Маркер идентификации состоит из трех частей:

- заголовок (*header*), в котором содержится общая информация о типе маркера, в том числе об использованных в ходе его формирования криптографических операциях;
- набор утверждений (*payload* / *claim set*) с содержательными сведениями о маркере;
- подпись (*signature*), которая удостоверяет, что маркер «выдан» Blitz Identity Provider и не был изменен при передаче.

Части маркера разделены точкой, так что он имеет вид:

```
HEADER.PAYLOAD.SIGNATURE
```

Маркер передается в виде строки в формате Base64url.

Заголовок (header) содержит описание алгоритма шифрования (параметр *alg*); в настоящее время в Blitz Identity Provider поддерживается алгоритм электронной подписи RSA SHA-256, рекомендуемый спецификацией (соответствует значению *RS256*).

[20] См.: https://tools.ietf.org/html/rfc6749#section-5.2

Набор утверждений включает следующие атрибуты:

- *exp* – время прекращения действия, указывается в секундах с 1 января 1970 г. 00:00:00 GMT;
- *iat* – время выдачи, указывается в секундах с 1 января 1970 г. 00:00:00 GMT;
- *sub* – идентификатор субъекта, в качестве значения указывается значение идентификатора пользователя;
- *aud* – адресат маркера, указывается *client_id* приложения, направившего запрос на аутентификацию;
- *iss* – организация, выпустившая маркер, указывается URL Blitz Identity Provider;
- *nonce* – строка безопасности, указывается значение *nonce*, которое было передано приложением к Blitz Identity Provider в исходном запросе к */oauth/ae*. Используется только при Implicit или Hybrid Flow. При получении приложением маркера с использованием Implicit или Hybrid Flow приложение должно сопоставить *nonce* из состава маркера идентификации с *nonce* из своего запроса;
- *at_hash* – половина хэша маркера доступа, передается только при использовании Implicit или Hybrid Flow. Представляет собой закодированную в Base64 левую половину значения функции SHA-256 от *access_token*; Приложение, получившее маркер доступа с использованием Implicit или Hybrid Flow должно извлечь из маркера идентификации значение *at_hash* и сравнить с маркером доступа.
- *c_hash* – половина хэша кода авторизации, передается только в случае использования Hybrid Flow. Представляет собой закодированную в Base64 левую половину (128 бит) значения функции SHA-256 от кода авторизации (*code*); Приложение, получившее код авторизации с использованием Hybrid Flow, должно извлечь из маркера идентификации значение *c_hash* и сравнить с кодом авторизации.
- *amr* – пройденные методы аутентификации, указывается список пройденных пользователем методов аутентификаций. Список может включать следующие идентификаторы методов:
  - *password* – вход с использованием пароля;
  - *cls:<метод>* (например, *cls:password*) – автоматический вход с запомненного устройства (в названии идентификатора после двоеточия указан метод аутентификации, первично пройденной пользователем, в результате чего произошло запоминание пользователя на данном устройстве);
  - *css* – автоматический вход по результатам регистрации пользователя, восстановления пароля или перехода в веб-приложение из мобильного приложения, использующего вызов с использованием *scope=native*;

- *sms* – подтверждение входа с помощью кода в SMS-сообщении (второй фактор аутентификации);
- *push* – подтверждение входа с помощью кода в push-уведомлении в мобильное приложение (второй фактор аутентификации);
- *totp* – подтверждение входа с помощью кода, сгенерированного программным TOTP-генератором кодов подтверждения (второй фактор аутентификации);
- *spnego* – вход с использованием сеанса операционной системы;
- *userApp* – вход в мобильное приложение привязанной к устройству учетной записью пользователя (Touch ID/Face ID/ПИН-код);
- *x509* – вход с использованием электронной подписи;
- *externalIdps:esia:esia_1* – вход с использованием учетной записи ЕСИА;
- *externalIdps:sbrf:sbrf_1* – вход с использованием учетной записи Сбер ID;
- *externalIdps:mos:mos_1* – вход с использованием учетной записи Mos ID (СУДИР);
- *externalIdps:facebook:facebook_1* – вход с использованием учетной записи в социальной сети Facebook;
- *externalIdps:google:google_1* – вход с использованием учетной записи Google;
- *externalIdps:mail:mail_1* – вход с использованием учетной записи Mail ID;
- *externalIdps:ok:ok_1* – вход с использованием учетной записи в социальной сети Одноклассники;
- *externalIdps:vk:vk_1* – вход с использованием учетной записи в социальной сети VK;
- *externalIdps:yandex:yandex_1* – вход с использованием учетной записи Яндекс;
- *outside_methodname* – признак, что в процессе входа пользователь использовал внешний метод аутентификации с именем *methodname*.

– дополнительные атрибуты в соответствии с заявкой на подключение приложения к Blitz Identity Provider (возможные атрибуты для включения в *id_token* приведены в таблице 4.

Пример набора утверждений:

```
{
  "exp": 1445004777,
  "iat": 1444994212,
  "sub": "3d10f626-ea77-481d-a50bd4a4d432d86b",
  "amr": [
    "externalIdps:esia:esia_1"
  ],
  "aud": [
    "ais"
  ],
  "iss": "https://login.company.com"
}
```

Подпись (*signature*) маркера осуществляется по алгоритму, который указывается в параметре *alg* маркера. Подпись вычисляется от двух предыдущих частей маркера (HEADER.PAYLOAD). Сертификат открытого ключа Blitz Identity Provider, необходимый для проверки подписи, можно загрузить по следующим ссылкам (находится в атрибуте *x5c*):

- *https://login-test.company.com/blitz/oauth/.well-known/jwks* (тестовая среда)
- *https://login.company.com/blitz/oauth/.well-known/jwks* (продуктивная среда)

После получения маркера идентификации приложению рекомендуется произвести валидацию маркера идентификации, которая включает в себя следующие проверки:

1. Получение идентификатора Blitz Identity Provider (*sub*), содержащегося в маркере идентификации, и получение иных необходимых приложению дополнительных атрибутов пользователя.
2. Проверка идентификатора приложения, т.е. именно приложение должно быть указано в качестве адресата маркера идентификации.
3. Проверка подписи маркера идентификации (с использованием указанного в маркере алгоритма).
4. Проверка, что текущее время должно быть не позднее, чем время прекращения срока действия маркера идентификации.

После валидации маркера идентификации приложение может считать пользователя аутентифицированным.

Для анализа содержания маркера идентификации, а также для упрощения разработки модулей по его проверке можно воспользоваться доступными онлайн-декодерами и библиотеками[21].

3.3.5. Проверка маркера доступа с использование сервиса интроспекции

Данные о маркере доступа (*access_token*) необходимо проверять в следующих случаях:

- приложению требуется отслеживать срок действия маркера, чтобы оперативно менять его на новый;
- к приложению предъявляются повышенные требования к безопасности, и приложение хочет через проверку маркера убедиться, что маркер не аннулирован досрочно. Аннулирование маркера доступам (*access_token*) или маркера идентификации (*id_token*) может произойти в целях безопасности в случае, если

[21] См.: http://jwt.io/ и http://kjur.github.io/jsjws/mobile/tool_jwt.html#verifier

произошли сброс/изменение пароля учетной записи пользователя или если учетная запись пользователя была заблокирована;

– приложение является поставщиком ресурсов и предоставляет доступ к этим ресурсам по предъявлению маркера доступа, выданного Blitz Identity Provider приложению, запрашивающему ресурс.

Для запроса данных о маркере доступа необходимо выполнить запрос методом POST по адресу сервиса интроспекции маркера доступа[22]. В запрос для аутентификации системы-клиента должен быть добавлен описанный ранее заголовок *Authorization: Basic*. Также должен быть добавлен заголовок *Content-Type*, принимающий значение *application/x-www-form-urlencoded*.

Сервис интроспекции может быть вызван любой системой, зарегистрированной в Blitz Identity Provider, для проверки любого маркера доступа (система может проверить маркер, выданный другой системе). Проверять можно не только маркер доступа, но и маркер обновления.

В теле запроса могут быть указаны параметры:

– *token* – маркер доступа, данные о котором требуется просмотреть (обязательный параметр);

– *token_type_hint* – тип маркера доступа (например, *access_token*), предназначен для ускорения поиска (опциональный параметр).

Пример запроса:

```
POST /blitz/oauth/introspect HTTP/1.1
Authorization: Basic cG9ydGFsLmlhc2l1LmxvY2FsOnBvcnRhbC5pYXNpdS5sb2NhbA==
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache

token=MkvRf…No
```

В ответе будут переданы следующие данные о маркере доступа:

– *active* – признак действительности маркера доступа, принимает значения *true* или *false*. Маркер действителен, если он выдан сервисом авторизации Blitz Identity Provider, не был отозван и срок его действия не истек;

– *scope* – область доступа, на которую выдан маркер доступа. Передается в виде перечня разрешений;

– *client_id* – идентификатор системы-клиента, которая получила данный маркер доступа;

– *sbj* – идентификатор пользователя (владельца ресурса, предоставившего доступ к своим данным), определенный как базовый идентификатор в Blitz Identity Provider.

[22] RFC 7662 «OAuth 2.0 Token Introspection», см.: https://tools.ietf.org/html/rfc7662

Значение параметра возвращается только в том случае, если он может быть передан в рамках *scope* по предъявленному маркеру доступа;

- *jti* – идентификатор маркера доступа (в виде строки);
- *token_type* – тип предъявленного маркера доступа.

Пример ответа:

```
{
    "sbj": "3d10f626-ea77-481d-a50bd4a4d432d86b",
    "scope": "openid profile",
    "jti": "10jdlNohfHzuv3xoFurvWSPheEJEC7KHdHr-dcaVyYYvV3h0l2sh",
    "token type": "Bearer",
    "client_id": "ais",
    "active": true
}
```

3.3.6. Самостоятельная проверка маркера доступа приложением

При регистрации приложения в Blitz Identity Provider можно указать, что приложение должно получать маркер доступа (*access_token*) в формате JWT. В этом случае приложение получает возможность самостоятельно проверить маркер доступа, выполнив его разбор. Структура первично полученного маркера доступа будет аналогична структуре маркера идентификации, описанной в пп. 3.3.4. Во вторичных маркерах доступа, полученных в результате обмена маркера обновления (refresh_token), не будет содержаться сессионная информация (будут отсутствовать *amr* и дополнительные атрибуты пользователя).

Маркеры доступа в формате JWT следует использовать, только в случае если у приложения на это есть особые причины. В остальных случаях рекомендуется использовать обычные маркеры доступа в формате *opaque*.

3.3.7. Обеспечение логаута

Если приложение предоставляет пользователю возможность инициировать выход из приложения (логаут), то приложению для обеспечения выхода недостаточно завершить локальную сессию. Необходимо также вызвать в Blitz Identity Provider операцию логаута. Если этого не сделать, то может возникнуть ситуация, что пользователь в приложении нажал кнопку *Выход*, после чего сразу попробовал нажать кнопку *Вход*, и вместо ожидаемого запроса идентификации и аутентификации сработал *Single Sign-On*, и пользователь сразу автоматически оказался авторизованным.

Для инициирования логаута в Blitz Identity Provider приложение после закрытия своей локальной сессии должно осуществить HTTP Redirect на следующий URL в Blitz Identity Provider, передав в качестве параметра *post_logout_redirect_uri* адрес возврата в приложение. Если для приложения настроен индивидуальный дизайн страниц входа, то рекомендуется также при вызове логаута указать параметр *client_id*, в котором указать client_id вызывающего логаут приложения – в этом случае страница логаута будет показана

в правильном для приложения дизайне.

Пример запроса логаута:

```
https://login.company.com/blitz/login/logout?client_id=ais&post_logout_redirect_uri=https://redirect_uri
```

Если Blitz Identity Provider успешно завершит логаут, то он перенаправит пользователя по переданному URL обратно в приложение.

Допустимые префиксы страниц возврата должны быть зарегистрированы в настройках Blitz Identity Provider, иначе при логауте будет выдана ошибка.

3.4. Подключение мобильного приложения

3.4.1. Общие сведения

Взаимодействие мобильного приложения с Blitz Identity Provider дополнительно к штатным средствам протокола OIDC/OAuth 2.0 использует спецификации RFC 7591[23] и RFC 7592[24].

Взаимодействие мобильного приложения с Blitz Identity Provider включает следующие этапы:

1. Динамическая регистрация в Blitz Identity Provider экземпляра мобильного приложения. Получение экземпляром приложения от Blitz Identity Provider уникальной пары *client_id*/*client_secret*.
2. Первичный вход пользователя в мобильное приложение с помощью Blitz Identity Provider. Установка пользователем ПИН-кода или Touch ID/Face ID. Сохранение на устройстве шифрованной пары *client_id*/*client_secret*, полученной от Blitz Identity Provider.
3. Вторичные входы пользователя с помощью ПИН-кода или Touch ID/Face ID. Авторизация в Blitz Identity Provider с помощью шифрованной пары *client_id/client_secret*.
4. Удаление в Blitz Identity Provider полученной пары *client_id/client_secret* при логауте (смене учетной записи, выхода из учетной записи) пользователя из мобильного приложения.

Схематично последовательность действий этапов 1-2 представлена на рисунке 4, а этапа 3 – на рисунке 5.

[23] RFC 7591 «OAuth 2.0 Dynamic Client Registration Protocol», см.: https://tools.ietf.org/html/rfc7591

[24] RFC 7592 «OAuth 2.0 Dynamic Client Registration Management Protocol», см.: https://tools.ietf.org/html/rfc7592

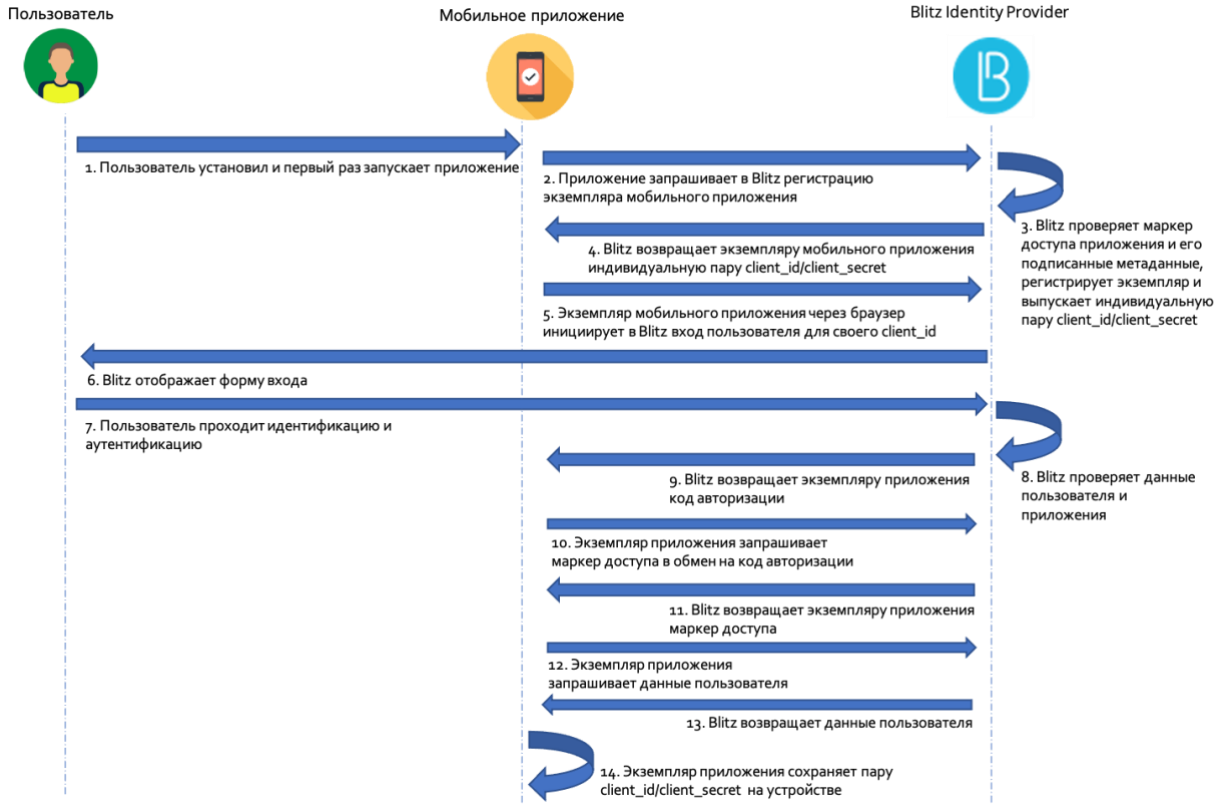

Рисунок 4 – Первый вход пользователя в мобильное приложение

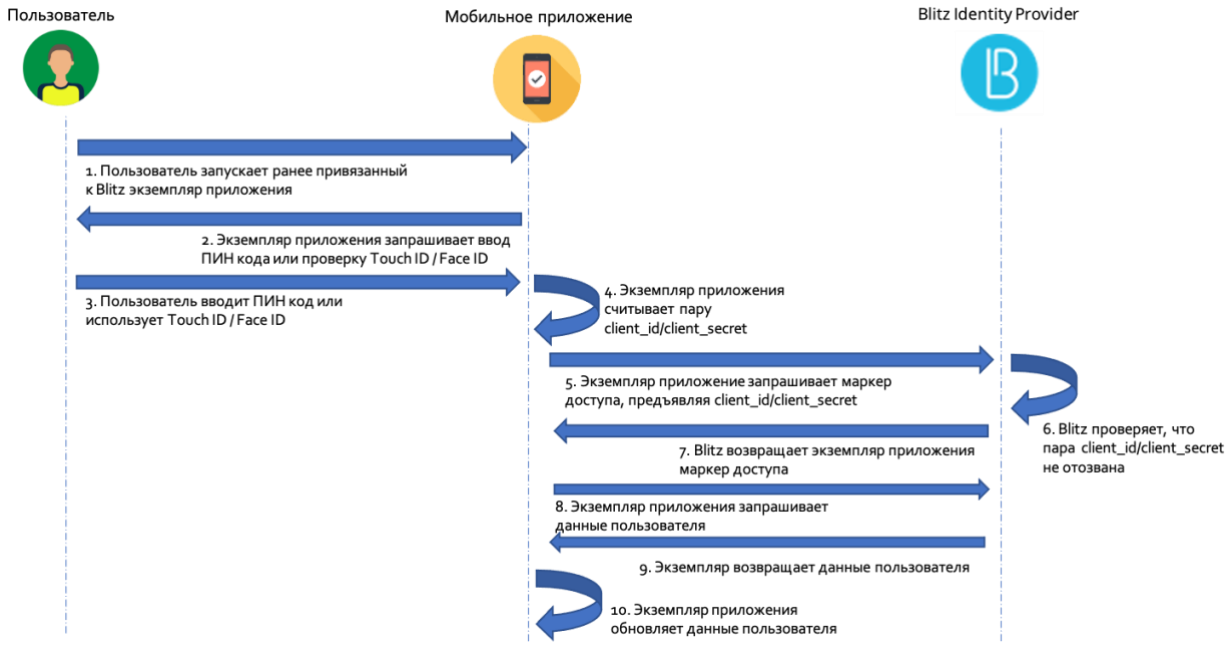

Рисунок 5 – Повторные входы пользователя в мобильное приложение

3.4.2. Динамическая регистрация в Blitz Identity Provider экземпляра мобильного приложения

Предварительные условия для динамической регистрации экземпляра мобильного приложения:

– пользователь должен установить мобильное приложение;

– мобильное приложение должно иметь следующие данные, полученные по результатам обработки заявки на подключение мобильного приложения к Blitz Identity Provider:
  - идентификатор мобильного приложения (*software_id*);
  - первичный маркер доступа (*Initial Access Token*);
  - метаданные мобильного приложения[25] (*software_statement*).

Мобильное приложение должно отправить HTTP-запрос методом POST в Blitz Identity Provider по адресу сервиса динамической регистрации */blitz/oauth/register*. Должны быть переданы параметры:

– идентификатор мобильного приложения (*software_id*);
– метаданные мобильного приложения (*software_statement*);
– тип устройства, на котором работает мобильное приложение (*device_type*) – одно из возможных значений, представленных в таблице 7:

Таблица 7 – Используемые в Blitz Identity Provider маркеры

№	Тип устройства (device_type)	Описание
1.	iphone	Смартфоны семейства iPhone
2.	ipad	Планшеты семейства iPad
3.	android_phone	Смартфоны под управлением ОС Android
4.	android_tab	Планшеты под управлением ОС Android
5.	win_mobile	Устройства под управлением Windows 10 Mobile

Запрос на динамическую регистрацию должен содержать заголовок *Authorization* с первичным маркером доступа (тип – *Bearer*), выданным приложению.

Пример запроса:

```
POST /blitz/oauth/register HTTP/1.1
Content-Type: application/json
Authorization: Bearer NINxnizbgYYQg94vEd6MjkTPxR3r2s9IAHBO92AszgTIqItY
{
      "software id": "CSI",
      "device_type": "iphone",
      "software_statement": "eyJ0e…xQ"
}
```

[25] Метаданные мобильного приложения (*software_statement*) представляют собой JWS-токен, состоящий из трех частей, разделенных точками и закодированных Base64: заголовка, тела, подписи.

Заголовок содержит служебную информацию о типе токена и методе подписи.

Тело токена содержит утверждения, используемые для регистрации экземпляра приложения. В частности, среди утверждений указаны:

– разрешенные префиксы ссылок возврата (*redirect_uris*);
– перечень допустимых разрешений (*scope*).

Подписанный JWS-токен выпускает администратор Blitz Identity Provider в процессе обработки заявки на подключение мобильного приложения к Blitz Identity Provider.

При успешном выполнении запроса Blitz Identity Provider возвращает экземпляру мобильного приложения перечень утверждений, среди которых для дальнейшей работы необходимы следующие (их нужно защищенным образом сохранить в устройстве пользователя):

- идентификатор экземпляра мобильного приложения (*client_id*);
- секрет экземпляра мобильного приложения (*client_secret*);
- маркер управления конфигурацией (*registration_access_token*);
- URL управления конфигурацией (*registration_client_uri*).

Пример ответа:


```
{
    "grant types": [
        "authorization_code"
    ],
    "registration_client_uri": "https://login.company.com/blitz/oauth/register/dyn:CSI:4e6904c5-
ef29-4ae5-8d30-99c359b8270f",
    "scope": "openid profile",
    "registration_access_token": "eyJ0e…tw",
    "client_id": "dyn:CSI:4e6904c5-ef29-4ae5-8d30-99c359b8270f",
    "software_id": "CSI",
    "software_version": "1",
    "token_endpoint_auth_method": "client_secret_basic",
    "response types": [
        "code"
    ],
    "redirect_uris": [
        "com.example.app:/oauth2redirect/example-provider"
    ],
    "client secret": "3r0tt2OlyeGecWq",
    "client_secret_expires_at": 0
}
```


3.4.3. Первичный вход пользователя в мобильное приложение

Получив пару *client_id/client_secret* (пп. 3.4.2) экземпляр мобильного приложения должен провести идентификацию и аутентификацию пользователя согласно спецификациям OIDC/OAuth 2.0 и с учетом дополнительной спецификации RFC 7636[26] (мобильное приложение при взаимодействии с Blitz Identity Provider должно использовать PKCE).

Сценарий идентификация и аутентификации включает следующие шаги:

- запрос на получение кода авторизации;
- получение маркера доступа;
- получение данных пользователя в обмен на маркер доступа.

Первичный вход пользователя в мобильное приложение должен произойти в течение 1 часа с завершения динамической регистрации в Blitz Identity Provider экземпляра мобильного приложения. Иначе *client_id* будет аннулирован и потребуется повторная динамическая регистрация.

[26] RFC 7636 «Proof Key for Code Exchange by OAuth Public Clients», см.: https://tools.ietf.org/html/rfc7636

3.4.4. Запрос на получение кода авторизации

Для проведения аутентификации экземпляр мобильного приложения должен вызвать штатный браузер мобильной платформы и перенаправить в нем пользователя на URL Blitz Identity Provider сервиса проведения авторизации и аутентификации (*/blitz/oauth/ae*). При использовании браузера мобильным приложением следует учесть следующие особенности:

- для iOS необходимо использовать встроенный браузер: класс *SFSafariViewController* или класс *SFAuthenticationSession* (in-app browser tab pattern);
- для Android необходимо использовать встроенный браузер: функция «Android Custom Tab» (реализует in-app browser tab patter).

> **Примечание —** Использование Embedded-браузера не допускается.

В качестве параметров запроса следует указать:

- *client_id* – идентификатор экземпляра мобильного приложения;
- *response_type* – тип ответа (принимает значение “code”);
- *scope* – запрашиваемые разрешения, должно быть передано разрешение *openid* и необходимые дополнительные *scope* для получения данных пользователя (эти *scope* должны быть предусмотрены метаданными);
- *redirect_uri* – ссылка для возврата пользователя в приложение, ссылка должна соответствовать одному из указанных в метаданных значений. Чтобы после авторизации Blitz Identity Provider смог обратно вызвать мобильное приложение, следует использовать следующие схемы:
  - для iOS[27]:
    - вариант 1 – использовать private-use URI scheme («custom URL scheme»). Вид ссылок возврата: *com.example.app:/oauth2redirect/example-provider* (регистрируются в Info.plist ключи типа CFBundleURLTypes);
    - вариант 2 – использовать URI вида «https» («Universal links»). Вид ссылок возврата: *https://app.example.com/oauth2redirect/example-provider* (используется функция «Universal links», URL регистрируются в entitlement-файле в приложении и ассоциированы с доменом приложения). Этот способ предпочтительнее для iOS 9 и выше.

[27] Пример реализации – см.: https://github.com/openid/AppAuth-iOS

- для Android[28]:
  - вариант 1 – использовать private-use URI scheme («custom URL scheme»). Вид ссылок возврата: *com.example.app:/oauth2redirect/example-provider* (поддержка ссылок с помощью Android Implicit Intents, ссылки регистрируются в manifest);
  - вариант 2 – использовать URI вида «https» («Universal links»). Вид ссылок возврата: *https://app.example.com/oauth2redirect/example-provider* (доступно начиная с Android 6.0, ссылки регистрируются в manifest). Этот способ предпочтительнее для Android 6.0 и выше.

– *state* – набор случайных символов, имеющий вид 128-битного идентификатора запроса (используется для защиты от перехвата), это же значение будет возвращено в ответе – опциональный параметр;

– *access_type* (необязательный параметр) – требуется 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. Если значение не задано, то поведение определяется настройкой, заданной для указанного приложения в Blitz Identity Provider;

– *code_challenge_method* – метод шифрования идентификатора запроса, следует указывать “S256”;

– *code_challenge* – зашифрованный идентификатор запроса. Идентификатор запроса (*code_verifier*) должен быть запомнен экземпляром мобильного приложения для последующей передачи в запрос на получение маркера доступа. Шифрованное значение вычисляется следующим образом:

```
code_challenge=BASE64URL-ENCODE(SHA256(ASCII(code_verifier)))
```

Пример запроса на получение кода авторизации (запрошена аутентификация и маркер доступа с разрешениями *openid* и *profile*, используется PKCE):

```
https://login.company.com/blitz/oauth/ae?scope=openid+profile
&access_type=online&response_type=code
&state=342a2c0c-d9ef-4cd6-b328-b67d9baf6a7f
&client id=dyn:CSI:4e6904c5-ef29-4ae5-8d30-99c359b8270f
&code challenge method=S256&code challenge=qjrzSW9gMiUgpUvqgEPE4
&redirect_uri=https%3A%2F%2Fapp.example.com%2Foauth2redirect%2Fexample-provider
```

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

```
https://app.example.com/oauth2redirect/example-
provider?code=f954nEzQ08DXju4wxGbSSfCX7TkZ1GvXUR7TzVus8fG
nu4AUl-YIosgax-BLXMeQQAlasD6CN2qG 0KXK5NIjARoKykhuR9IpbuzqeFxS0
&state=342a2c0c-d9ef-4cd6-b328-b67d9baf6a7f
```

[28] Пример реализации – см.: https://github.com/openid/AppAuth-Android

Возможные ошибки при вызове */oauth/ae* соответствуют RFC 6749 и описаны по ссылке[29].

3.4.5. Получение маркеров

После получения кода авторизации экземпляр мобильного приложения должен обменять его на маркеры. Для этого экземпляр должен сформировать запрос методом POST на URL для получения маркера. Запрос должен содержать заголовок *Authorization* со значением *Basic {secret}*, где *secret* – это *client_id:client_secret* (например, *dyn:CSI:4e69…Wq*) в формате Base64.

Пример заголовка:

```
Authorization: Basic ZHluOkNTSTo…dx
```

Тело запроса должно содержать следующие параметры:

- *code* – значение кода авторизации, который был ранее получен экземпляром мобильного приложения от Blitz Identity Provider;
- *grant_type* – значение *authorization_code*;
- *redirect_uri* – должно быть то же самое значение, которое было указано в запросе на получение кода авторизации;
- *code_verifier* – идентификатор запроса, сгенерированный экземпляром мобильного приложения при запросе на получение кода авторизации.

Пример запроса:

```
POST /blitz/oauth/te HTTP/1.1
Authorization: Basic
ZHluOkNTSTo0ZTY5MDRjNS1lZjI5LTRhZTUtOGQzMC05OWMzNTliODI3MGY6M3IwdHQyT2x5ZUdlY1dx
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache

grant_type=authorization_code&code=FLZHS…GU
&redirect uri=https%3A%2F%2Fapp.example.com%2Foauth2redirect%2Fexample-provider
&code_verifier=M25iVXpKU3puUjFaYWg3T1NDTDQtcW1ROUY5YXlwalNoc0hhakxifmZHag
```

В ответ возвращается маркер доступа и маркер идентификации.

Пример ответа с успешным выполнением запроса:

```
{
    "id token": "eyJhb…J9. eyJub…0=.Ckt dr…sQ",
    "access token": "dO-xym…BE",
    "expires_in": 3600,
    "scope": "openid profile",
    "token_type": "bearer"
}
```

После получения маркера доступа экземпляр мобильного приложения становится связанным с учетной записью пользователя. Рекомендуется, чтобы мобильное приложение предложило пользователю установить ПИН код или включить Touch ID/Face ID.

Также с помощью полученного маркера доступа приложение может запросить

[29] См.: https://tools.ietf.org/html/rfc6749#section-4.1.2.1

данные о пользователе (пп. 3.5).

Если код авторизации был уже использован, не совпал *redirect_uri* с ранее использованным в вызове к */oauth/ae*, или истек срок действия кода, либо переданный *code_verifier* не соответствует *code_challenge*, то в качестве ответа будет возвращена ошибка.

Пример ответа с ошибкой:

```
{
    "error": "invalid grant",
    "error_description": "The provided authorization grant… is invalid, expired, revoked…"
}
```

Возможные ошибки при вызове */oauth/te* соответствуют RFC 6749 и описаны по ссылке[30].

3.4.6. Повторный вход пользователя в мобильное приложение

При каждом входе пользователя в экземпляр мобильного приложения, если с устройства доступен выход в сеть Интернет, следует производить аутентификацию пользователя посредством вызова сервиса Blitz Identity Provider. В частности, при каждом входе в экземпляр мобильного приложения необходимо проверить ПИН-код пользователя или Touch ID/Face ID, после чего извлечь защищенно хранимые на устройстве *client_id/client_secret* и сделать запрос в Blitz Identity Provider на проведение повторного входа пользователя. Использовать полученный в ответ от Blitz Identity Provider маркер доступа для получения актуальных данных пользователя.

Запрос в Blitz Identity Provider на проведение повторного входа должен быть выполнен методом POST на URL для получения маркера (*/oauth/te*). Запрос должен содержать заголовок *Authorization* со значением *Basic {secret}*, где *secret* – это *client_id:client_secret* экземпляра мобильного приложения в формате Base64.

Тело запроса должно содержать параметры:

- *grant_type* – значение *client_credentials*;
- *scope* – перечень запрашиваемых экземпляром мобильного приложения разрешений.

Пример запроса:

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

grant_type=client_credentials&scope=profile
```

В ответ возвращается маркер доступа и информация об этом маркере.

Пример ответа с успешным выполнением запроса:

```
{
    "access_token": "dO-xym…BE",
```

[30] См.: https://tools.ietf.org/html/rfc6749#section-5.2

```
    "expires_in": 3600,
    "scope": "openid profile",
    "token_type": "bearer"
}
```

Используя полученный маркер доступа, экземпляр мобильного приложения может запросить (пп. 3.5) актуальные данные пользователя из Blitz Identity Provider, чтобы при необходимости визуализировать или обновить эти данные в устройстве.

Если пользователь в Blitz Identity Provider отозвал у экземпляра мобильного приложения право авторизации в Blitz Identity Provider, то в результате вызова Blitz Identity Provider экземпляр мобильного приложения получит ошибку.

Пример ответа с ошибкой:

```
{
    "error": "invalid_client",
    "error_description": " Client authentication failed…"
}
```

Возможные ошибки при вызове */oauth/te* соответствуют RFC 6749 и описаны по ссылке[31].

3.4.7. Переключение или выход пользователя из мобильного приложения

Если в мобильном приложении предусмотрена функция выхода или смены пользователя, то при вызове пользователем такой функции мобильное приложение должно также вызвать Blitz Identity Provider и удалить выпущенную для данного экземпляра мобильного приложения пару *client_id/client_secret*. Если это не будет сделано, то при выходе пользователя из мобильного приложения, пользователь в веб-приложении Blitz Identity Provider «Настройки безопасности[32]» все равно будет видеть, что мобильное приложение все еще привязано к его учетной записи.

Чтобы удалить из Blitz Identity Provider выпущенную для экземпляра мобильного приложения пару *client_id/client_secret*, мобильное приложение должно отправить в Blitz Identity Provider запрос методом DELETE на URL управления конфигурацией (*registration_client_uri*), полученный и запомненный мобильным приложением при вызове динамической регистрации в Blitz Identity Provider экземпляра мобильного приложения (пп. 3.4.2). Запрос должен содержать заголовок *Authorization* со значением *Bearer {registration_access_token}*, где *registration_access_token* – это маркер управления конфигурацией, также полученный и запомненный в процессе динамической регистрации. Запрос не требует указания параметров.

Пример запроса:

```
DELETE /blitz/oauth/register/dyn:CSI:4e6904c5-ef29-4ae5-8d30-99c359b8270f HTTP/1.1
Authorization: Bearer eyJ0e…tw
```

[31] См.: https://tools.ietf.org/html/rfc6749#section-5.2
[32] См.: https://login.company.com/blitz/profile

3.4.8. Открытие веб-ресурсов из мобильного приложения в режиме сквозной аутентификации

В некоторых мобильных приложениях разработчикам может потребоваться предусмотреть функцию открытия веб-ресурсов, также требующих идентификации/аутентификации пользователя, и использующих для этой цели Blitz Identity Provider. При доступе к веб-ресурсу пользователь, вошедший в мобильное приложение, может столкнуться с ситуацией, что Blitz Identity Provider повторно потребует у него пройти идентификацию/аутентификацию в веб-ресурсе в результате запроса соответствующим веб-приложением идентификации/аутентификации пользователя в Blitz Identity Provider. Чтобы такого не произошло, мобильное приложение может непосредственно перед вызовом веб-ресурса запросить в Blitz Identity Provider получение маркера доступа (*access_token*) на специальное разрешение (*scope*) с именем *native*. Получить маркер доступа можно способом, описанным в пп. 3.4.6 или в пп. 3.3.3 (при наличии у приложения *refresh_token*).

Пример запроса:

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

grant_type=client_credentials&scope=native
```

В ответ возвращается не только маркер доступа и информация об этом маркере, но и специальный атрибут – маркер сквозного входа *css* (*cookie short session*).

Пример ответа с получением атрибута *css*:

```
{
    "access_token": "dO-xym…BE",
    "css": "nUngQ…LA",
    "expires_in": 3600,
    "scope": "native",
    "token_type": "bearer"
}
```

После этого мобильное приложение может открывать веб-ресурс. При этом в запускаемом веб-браузере мобильное приложение должно предварительно установить cookie со следующими параметрами:

- имя cookie – *css*;
- домен cookie – *login.company.com*;
- путь (path) cookie – */blitz*;
- флаги *HTTPOnly=true* и *Secure=true*;
- значение cookie – значение, полученное в параметре *css* при получении от Blitz Identity Provider маркера доступа на scope с именем *native*.

Если запущенный веб-ресурс в течение 300 секунд с момента запуска инициирует в Blitz Identity Provider идентификацию/аутентификацию, и cookie была корректно

установлена, то Blitz Identity Provider по запросу веб-приложения проведет автоматическую сквозную идентификацию и аутентификацию пользователя под учетной записью, с которой пользователь ранее входил в экземпляр мобильного приложения, вызвавшего веб-ресурс.

3.5. Получение атрибутов пользователя

Для запроса данных о пользователе необходимо выполнить запрос методом GET по URL-адресу получения данных пользователя (*/oauth/me*[33]). В запрос должен быть добавлен следующий заголовок:

```
Authorization: Bearer <access token>
```

В заголовке <access token> – это маркер доступа, полученный от Blitz Identity Provider (пп. 3.3.3 и 3.4.5).

Пример запроса:

```
GET /blitz/oauth/me HTTP/1.1
Authorization: Bearer NINxn…tY
Cache-Control: no-cache
```

В ответе будут отображены только те данные, которые определены в scope, на который получен маркер доступа (пп. 2.1.3).

Пример ответа:

```
{
    "family_name": "Иванов",
    "given_name": "Иван",
    "middle name": "Иванович",
    "email": "iivanov@company.com",
    "phone number": "79162628910",
    "sub": "3d10f626-ea77-481d-a50bd4a4d432d86b"
}
```

[33] Для получения данных о юридическом лице следует использовать данные из *id_token* согласно описанию в пп. 3.3.4.

4. Подключение приложений по SAML

4.1. Данные для подключения по результатам рассмотрения заявки

По результатам исполнения заявки на подключение к Blitz Identity Provider будет предоставлена следующая информация:

- идентификатор, присвоенный приложению в Blitz Identity Provider (*entityID*);
- уточненный файл метаданных поставщика услуг[34].

Все URL в данном разделе необходимо скорректировать в зависимости от конкретных настроек, сделанных при внедрении Blitz Identity Provider. См. «Руководство администратора».

Приложение взаимодействует с сервисами Blitz Identity Provider, используя следующие адреса:

- метаданные Blitz Identity Provider:
  - *https://login-test.company.com/blitz/saml/profile/Metadata/SAML* (тестовая среда)
  - *https://login.company.com/blitz/saml/profile/Metadata/SAML* (продуктивная среда)
- URL для аутентификации:
  - *https://login-test.company.com/blitz/saml/profile/SAML2/Redirect/SSO* (тестовая среда)
  - *https://login.company.com/blitz/saml/profile/SAML2/Redirect/SSO* (продуктивная среда)
- URL для логаута:
  - *https://login-test.company.com/blitz/saml/profile/SAML2/Redirect/SLO* (тестовая среда)
  - *https://login.company.com/blitz/saml/profile/SAML2/Redirect/SLO* (продуктивная среда)
- URL издателя:
  - *https://login-test.company.com/blitz/saml/* (тестовая среда)
  - *https://login.company.com/blitz/saml/* (продуктивная среда)

Если приложение поддерживает протокол подключения SAML, то указанных данных должно быть достаточно для конфигурирования приложения. Если приложение не поддерживает протокол SAML, следует произвести его доработку согласно рекомендациям, изложенным в пп. 4.2 и пп. 4.3 настоящего документа.

[34] Как правило, этот файл будет совпадать с тем, что был приложен к заявке. Но Администратор Blitz Identity Provider может скорректировать файл метаданных и прислать его вместе с результатами рассмотрения заявки.

Типичные вопросы о том, как настроить приложение для подключения к Blitz Identity Provider по протоколу SAML, приведены в таблице ***8***.

Таблица 8 — Типичные вопросы при подключении приложения по протоколу SAML

Вопрос	Ответ
Где найти метаданные поставщика идентификации?	Чтобы загрузить метаданные, пройдите по ссылке *https://login.company.com/blitz/saml/profile/Metadata/SAML* и скопируйте открытый XML документ в приложение
Где найти сертификат SAML поставщика идентификации?	Откройте XML документ с метаданными поставщика идентификации. Найдите раздел `<ds:X509Certificate></ds:X509Certificate>` – в нем и располагается сертификат SAML поставщика идентификации. Пример:  Иногда для корректной загрузки в приложение перед строкой с сертификатом нужно вставить строку `-----BEGIN CERTIFICATE-----` , а после – `-----END CERTIFICATE-----`
Где найти адреса SAML-обработчиков поставщика идентификации?	Запросы на идентификацию/аутентификацию приложение должно отправлять на следующие обработчики (*SingleSignOnService*) в ПРОД-среде: – *https://login.company.com/blitz/saml/profile/SAML2/Redirect/SSO* – для приема сжатых с помощью алгоритма Deflate запросов – стандартный SAML-обработчик.

Вопрос	Ответ
	– *https://login.company.com/blitz/saml/profile/SAML2/Redirect/Plain/SSO* – для приема несжатых запросов – следует использовать только в случае, если подключаемое приложение не использует deflate. Запросы на единый логаут приложение должно отправлять на следующие обработчики (*SingleLogoutService*) в ПРОД-среде: – *https://login.company.com/blitz/saml/profile/SAML2/Redirect/SLO* – для приема сжатых с помощью алгоритма Deflate запросов – стандартный SAML-обработчик. – *https://login.company.com/blitz/saml/profile/SAML2/Redirect/Plain/SLO* – для приема несжатых запросов – следует использовать только в случае, если подключаемое приложение не использует deflate. В ТЕСТ-среде аналогичные адреса начинаются с *https://login-test.company.com*.
Какой entityID у поставщика идентификации?	Blitz Identity Provider как поставщик идентификации имеет следующие entityID: – Для ПРОД-среды – *https://login.company.com/blitz/saml* – Для ТЕСТ-среды – *https://login-test.company.com/blitz/saml*

4.2. Готовые библиотеки

Так как самостоятельная разработка программного интерфейса клиента SAML является трудоемкой задачей, а ошибки в реализации чреваты угрозами безопасности, при интеграции приложения по SAML рекомендуется использовать существующие популярные библиотеки SAML-клиентов: OIOSAML[35] (Java, .NET), OpenSAML[36] (Java), Spring Security SAML[37] (Java), SimpleSAMLphp[38] (PHP), ruby-saml[39] (Ruby on Rails). Далее приводятся ключевые сведения, необходимые для понимания процесса аутентификации по протоколу SAML.

4.3. Разработка взаимодействия приложения с Blitz Identity Provider по SAML

4.3.1. Общие сведения

Для подключения к Blitz Identity Provider в целях идентификации и аутентификации пользователей приложение может использовать стандарт SAML версий 1.0, 1.1, 2.0[40]. При

[35] См.: http://digitaliser.dk/group/42063/resources

[36] См.: https://wiki.shibboleth.net/confluence/display/OS30/Home

[37] См.: http://projects.spring.io/spring-security-saml/

[38] См.: https://simplesamlphp.org/

[39] См.: https://rubygems.org/gems/ruby-saml/

[40] См.: http://saml.xml.org/saml-specifications

этом процесс взаимодействия приложения и Blitz Identity Provider должен быть построен в соответствии с профилем SAML Web Browser SSO Profile[41].

Стандарт SAML основан на XML и определяет способы обмена информацией об аутентификации пользователей и их идентификационных данных (атрибуты, полномочия).

Для возможности осуществлять взаимодействия поставщик услуг и поставщик идентификации предварительно должны обменяться настройками взаимодействия, описанными в форме XML-документов и называемых метаданными. Поставщик услуг должен получить настройки Blitz Identity Provider, называемые метаданными поставщика идентификации (пп. 2.2.1).

4.3.2. Процесс проведения идентификации и аутентификации

В процессе взаимодействия приложение (поставщик услуг) посылает в Blitz Identity Provider SAML-запрос на идентификацию пользователя (SAML Request). Запрос представляет собой оформленный в соответствии со стандартом SAML XML-документ. В запросе присутствует идентификатор запрашивающего идентификацию приложения, называемый *entityID*, а также дополнительная служебная информация. Сам запрос передается подписанным электронной подписью приложения. В качестве транспортного протокола для передачи сообщения используется протокол HTTPS, вызов поставщика идентификации осуществляется через HTTP Redirect. Это означает, что запрос от приложения к Blitz Identity Provider осуществляется опосредованно, через браузер пользователя, и прямое сетевое взаимодействие между приложением и Blitz Identity Provider при использовании SAML не требуется.

Получив SAML-запрос на идентификацию, Blitz Identity Provider идентифицирует принадлежность запроса определенному приложению, после чего отображает пользователю веб-страницу единого входа для проведения идентификации и аутентификации пользователя. В случае успешной идентификации и аутентификации пользователя Blitz Identity Provider передает приложению (поставщику услуг) SAML-ответ (SAML Response). В зависимости от заданных настроек взаимодействия запрос может быть подписанным и зашифрованным. Для формирования подписи и для шифрования используются стандарты XML Signature и XML Encryption. В качестве транспортного протокола для передачи сообщения с результатами идентификации используется протокол HTTPS, вызов поставщика услуг осуществляется через HTTP POST.

[41] См.: http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

Получив от Blitz Identity Provider SAML-ответ, приложение проверяет его подпись, выполняет расшифровку, после чего извлекает из SAML-утверждений (SAML Assertions) идентификационные данные пользователя (идентификаторы, атрибуты, полномочия).

Процесс взаимодействия приложения и Blitz Identity Provider с использованием SAML приведен на рисунке 6.

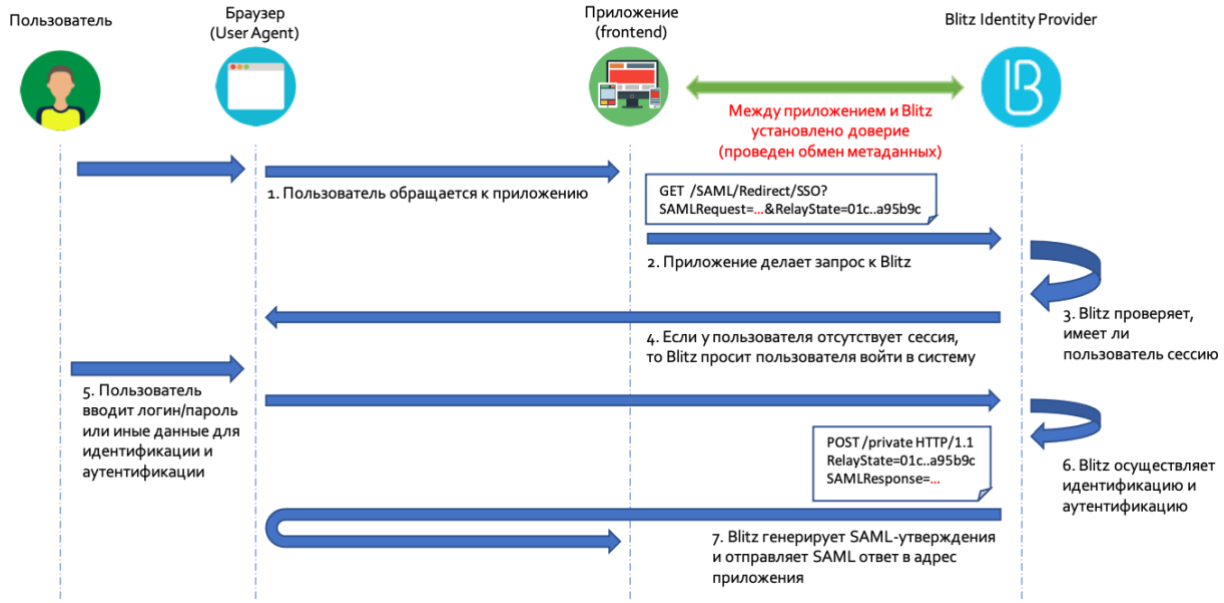

Рисунок 6 — Идентификация пользователя с использованием SAML

4.3.3. Обеспечение логаута при использовании SAML

Подключенное к Blitz Identity Provider по SAML приложение также может предусматривать возможность реализации единого выхода (логаута). Для этих целей Blitz Identity Provider поддерживает SAML Single Logout Profile[42]. Приложение может направить в Blitz Identity Provider SAML-запрос `<LogoutRequest>` и в случае успешного завершения единого логаута получить от Blitz Identity Provider SAML-ответ `<LogoutResponse>`. Если приложение должно быть задействовано в едином логауте, инициированным другим приложением, подключенным к Blitz Identity Provider, то оно также должно предусматривать возможность обработки запросов `<LogoutRequest>`, поступивших к приложению от Blitz Identity Provider. В случае успешного завершения локальной сессии приложение должно уведомлять Blitz Identity Provider путем отправки ему SAML-ответа `<LogoutResponse>`.

Если приложению достаточно при инициировании пользователем логаута только завершить собственную сессию приложения и глобальную сессию в Blitz Identity Provider, то вместо SAML Single Logout Profile можно для простого логаута инициировать HTTP

[42] См.: https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

Redirect на следующий URL в Blitz Identity Provider, передав в качестве параметра *post_logout_redirect_uri* адрес возврата в приложение. Если для приложения настроен индивидуальный дизайн страниц входа, то рекомендуется также при вызове логаута указать параметр *client_id*, в котором указать *entityId* вызывающего логаут приложения – в этом случае страница логаута будет показана в правильном для приложения дизайне.

Пример запроса логаута:

```
https://login.company.com/blitz/login/logout?client id=ais&post logout redirect uri=https://redir
ect_uri
```

Если Blitz Identity Provider успешно завершит логаут, то он перенаправит пользователя по переданному URL.

5. Требования по безопасности к приложению

Оператором приложения, подключенного к Blitz Identity Provider, должно обеспечиваться соблюдение следующих требований к безопасности:

1. Должна обеспечиваться конфиденциальность полученного для приложения при регистрации в Blitz Identity Provider значения *client_secret*:
   - Запрещается предавать значение *client_secret* лицам, не связанным с обеспечением эксплуатации приложения.
   - Запрещается использовать *client_secret* в клиентской части ПО (код, выполняемый на стороне браузера, мобильного приложения, десктопного приложения). Применяться *client_secret* должен только в серверных компонентах приложения. Исключение – *client_secret*, полученный мобильным или десктопным приложением с помощью операции динамической регистрации, такой *client_secret* можно хранить и обрабатывать в мобильном или десктопном приложении.
   - В случае если *client_secret* скомпрометирован, то должна быть подана заявка на замену *client_secret* приложения. В Blitz Identity Provider предусмотрена возможность «плавной замены» *client_secret*, а именно, приложению может быть присвоен дополнительный *client_secret* на время, пока будет выполняться перенастройка приложения с прежнего на новое значение *client_secret*.
2. Должна обеспечиваться конфиденциальность полученных приложением от Blitz Identity Provider маркеров доступа (*access_token*) и маркеров обновления (*refresh_token*).
   - Нужно избегать использования маркеров доступа в браузерной части приложения. Если все-таки это необходимо (SPA-приложение), то использующий маркер доступа JS-код должен предусматривать защиту от возможности получения значения маркера доступа из браузерной консоли.
   - Запрещено хранить/обрабатывать маркер обновления на стороне браузерной части приложения – маркер обновления должен использоваться исключительно в серверных компонентах приложения. При хранении маркеров обновления в приложении (в БД, файлах и т.д.) доступ к хранимым маркерам обновления должен быть ограничен.
3. Взаимодействие приложения с Blitz Identity Provider в продуктивном контуре должно осуществляться исключительно с использованием защищенного соединения (HTTPS). Запрещено использовать HTTP в обработчиках приложения (адреса возврата *redirect_uri, post_logout_redirect_uri*).

4. Приложению запрещено открывать страницу входа Blitz Identity Provider во фрейме.
5. При подключении мобильных приложений к Blitz Identity Provider:
   - использованием PKCE является обязательным;
   - запрещено использовать Embedded-браузер.

Приложение А. Описание REST API в Blitz Identity Provider

А.1. Список разрешений для доступа к REST API

В данном разделе приведен перечень разрешений (*scope* в терминологии OIDC/OAuth 2.0), используемых для доступа к REST API, предоставляемым Blitz Identity Provider. Данные разрешения назначаются отдельным приложениям при необходимости предоставления им доступа к REST API в Blitz Identity Provider, описанным в данном приложении.

Таблица 9 – Разрешения (scope) для REST API в Blitz Identity Provider

№	Разрешение	Название	Описание
Пользовательские разрешения (разрешения, получаемые на пользователя)			
1.	blitz_change_password	Разрешение на изменение пароля	Для использования сервиса POST /blitz/api/v2/users/{subjectId}/password
2.	blitz_user_rights	Разрешение на управление правами учетной записи	Для использования сервиса POST /blitz/api/v2/users/rights/change
3.	blitz_api_user	Получение атрибутов	Для использования сервиса GET /blitz/api/v3/users/{subjectId}
4.	blitz_api_user_chg	Изменение атрибутов	Для использования сервиса POST /blitz/api/v3/users/{instanceId}
5.	blitz_api_usec	Получение настроек двухфакторной аутентификации, разрешений	Для использования сервисов: GET /blitz/api/v3/users/{subjectId}/auth GET /blitz/api/v3/users/{subjectId}/totps GET /blitz/api/v3/users/{subjectId}/acls
6.	blitz_api_usec_chg	Изменение пароля, настроек двухфакторной аутентификации, отзыв разрешений	Для использования сервисов: POST /blitz/api/v3/users/{instanceId}/pswd POST /blitz/api/v3/users/{subjectId}/auth GET /blitz/api/v3/users/{subjectId}/totps /attach/qr POST /blitz/api/v3/users/{subjectId /totps /attach/qr DELETE /blitz/api/v3/users/{subjectId} /totps/{id} DELETE /blitz/api/v3/users/{subjectId} /acls/{id}

7.	blitz_api_uapps	Получение запомненных устройств	Для использования сервиса GET /blitz/api/v3/users/{subjectId}/apps
8.	blitz_api_uapps_chg	Удаление запомненных устройств	Для использования сервиса DELETE /blitz/api/v3/users/{subjectId} /apps/{id}
9.	blitz_api_uaud	Получение событий безопасности	Для использования сервиса GET blitz/api/v3/users/{subjectId}/audit
Системные разрешения (разрешения, получаемые на приложение)			
10.	blitz_groups	Разрешение на доступ к сервисам работы с организациями	Для использования сервисов: GET /blitz/api/v2/grps/{id} POST /blitz/api/v2/grps POST /blitz/api/v2/grps/{id}?profile={profile} DELETE /blitz/api/v2/grps/{id}?profile={profile} GET /blitz/api/v2/grps/{id}/members POST /blitz/api/v2/grps/{id}/members/add?profile={ profile} POST /blitz/api/v2/grps/{id}/members/rm?profile={p rofile}
11.	blitz_rights_full_access	Разрешение на назначение и отзыв прав доступа	Для использования сервисов: PUT /blitz/api/v3/rights DELETE /blitz/api/v3/rights GET /blitz/api/v3/rights/on/grps/<grp_id>?objectExt =<profile> GET /blitz/api/v3/rights/of/<sub>
12.	blitz_rm_rights	Разрешение на отзыв прав доступа ведомых учетных записей	Для использования сервиса POST /blitz/api/v2/users/rights/change
13.	blitz_api_sys_users	Получение атрибутов любого пользователя	Для использования сервиса GET /blitz/api/v3/users/{subjectId}

14.	blitz_api_sys_user_chg	Изменение атрибутов любого пользователя	Для использования сервиса POST /blitz/api/v3/users/{instanceId}
15.	blitz_api_sys_usec	Получение настроек двухфакторной аутентификации, разрешений любого пользователя	Для использования сервисов: GET /blitz/api/v3/users/{subjectId}/auth GET /blitz/api/v3/users/{subjectId}/totps GET /blitz/api/v3/users/{subjectId}/acls
16.	blitz_api_sys_usec_chg	Изменение пароля, настроек двухфакторной аутентификации, отзыв разрешений любого пользователя	Для использования сервисов: POST /blitz/api/v3/users/{instanceId}/pswd POST /blitz/api/v3/users/{subjectId}/auth GET /blitz/api/v3/users/{subjectId}/totps /attach/qr POST /blitz/api/v3/users/{subjectId}/totps /attach/qr DELETE /blitz/api/v3/users/{subjectId} /totps/{id} DELETE /blitz/api/v3/users/{subjectId} /acls/{id}
17.	blitz_api_sys_uapps	Получение запомненных устройств любого пользователя	Для использования сервиса GET /blitz/api/v3/users/{subjectId}/apps
18.	blitz_api_sys_uapps_chg	Удаление запомненных устройств любого пользователя	Для использования сервиса DELETE /blitz/api/v3/users/{subjectId} /apps/{id}
19.	blitz_api_sys_uaud	Получение событий безопасности любого пользователя	Для использования сервиса GET blitz/api/v3/users/{subjectId}/audit

Маркер доступа на пользовательские разрешения приложение получает в момент идентификации и аутентификации пользователя, осуществляя взаимодействие в соответствии с описанием в пп. 3.3.2 и пп. 3.3.3.

Чтобы получить маркер доступа на системное разрешение, приложение должно выполнить запрос методом POST на URL для получения маркера

(*https://login.company.com/blitz/oauth/te*). Запрос должен содержать заголовок *Authorization* со значением *Basic {secret}*, где *secret* – это *client_id:client_secret* (например, *app:topsecret*) в формате Base64.

Пример заголовка:

```
Authorization: Basic YWlzOm…XQ=
```

Тело запроса должно содержать следующие параметры:

- *grant_type* – принимает значение *client_credentials*;
- *scope* – запрашиваемое системное разрешение.

Пример запроса:

```
POST blitz/oauth/te HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Authorization: Basic ZG5ld…lg
Cache-Control: no-cache

grant_type=client_credentials&scope=blitz_groups
```

В ответ приложение получит маркер доступа (*access_token*), время его жизни (*expires_in*) и тип маркера (*token_type*). Возможные ошибки при вызове */oauth/te* соответствуют RFC 6749 и описаны по ссылке[43].

Пример ответа с успешным выполнением запроса:

```
{
    "access token": "QFiJ9mPgERPuusd36mQvD4mfzYolH CmuddAJ3YKTOI",
    "expires in": 3600,
    "scope": "blitz_groups",
    "token_type": "bearer"
}
```

Рекомендуется, чтобы приложение кэшировало полученный маркер доступа для многократного использования на время, немного меньшее, чем параметр *expires_in*, после чего осуществляло получение нового маркера доступа для обновления в кэше.

Если приложение попытается вызвать с просроченным маркером доступа соответствующий ему REST-сервис, то получит ошибку *HTTP 401 Unauthorized*.

A.2. Регистрация учетной записи пользователя

Для регистрации учетной записи пользователя приложение должно выполнить запрос методом PUT по адресу *https://login.company.com/blitz/reg/api/v1/users*.

В запрос должен быть добавлен следующий заголовок, где *secret* – это присвоенные приложению при регистрации в Blitz Identity Provider *client_id:rest_secret* в формате Base64:

```
Authorization: Basic <secret>
```

Список атрибутов приведен в качестве образца. Содержание списка необходимо скорректировать в зависимости от конкретных настроек, сделанных при внедрении Blitz

[43] См.: https://tools.ietf.org/html/rfc6749#section-5.2

Identity Provider. См. «Руководство администратора».

Тело запроса должно содержать атрибуты регистрируемой учетной записи:

– *first_name* – фамилия;
– *name* – имя;
– *middle_name* – отчество;
– *phone_number* – номер мобильного телефона в виде составного объекта с атрибутами:
  - *value* – номер телефона в формате 7XXXXXXXXXX;
  - *verified* – признак, что телефон подтвержден – *true* или *false*;
– *email* – адрес электронной почты в виде составного объекта с атрибутами:
  - *value* – адрес электронной почты;
  - *verified* – признак, что адрес подтвержден – *true* или *false*;
– *password* – пароль для создаваемой учетной записи пользователя (должен соответствовать настроенной парольной политике).

Пример запроса:

```
PUT /blitz/reg/api/v1/users HTTP/1.1
Authorization: Basic YXBwX2lkOmFwcF9zZWNyZXQ=
Content-Type: application/json
Cache-Control: no-cache

{
      "first_name":"Иванов",
      "name":"Иван",
      "middle_name":"Иванович",
      "phone_number": {
         "value": "79991234567",
         "verified": true
      },
      "email": {
          "value":"mail@example.com",
          "verified": true
      },
      "password":"QWErty$123"
}
```

В результате вызова сервиса в Blitz Identity Provider будет зарегистрирована учетная запись пользователя с предоставленными атрибутами и паролем. Сервис вернет присвоенный учетной записи ребенка идентификатор пользователя (*subject*). Кроме того, вернется ряд сервисных атрибутов (*instructions* и *context*).

Пример ответа:

```
{
    "subject": "c629340d-4aa9-48b1-b890-bc030020b4eb",
    "instanceId": "dGFtOk…3M",
    "instructions": [],
    "context": "HDTR…UA"
}
```

Регистрация может завершиться ошибкой. Тогда в теле ответа будет пояснение проблемы. В частности, если в Blitz Identity Provider нарушена уникальность атрибута, то сообщение будет содержать перечень полей, по которым нарушена уникальность.

Пример ответа с сообщением об ошибке:

```
{
    "errors": [
        {
            "errMsg": "Такой пользователь уже зарегистрирован…",
            "field": "email"
        },
        {
            "errMsg": "Такой пользователь уже зарегистрирован…",
            "field": "phone_number"
        }
    ],
    "context": ""
}
```

A.3. Назначение и отзыв права доступа

A.3.1. Назначение и отзыв прав пользователей к пользователям

Назначение права ведущему пользователю в отношении ведомого пользователя осуществляется методом POST по адресу *https://login.company.com/blitz/api/v2/users/rights/change*.

В запрос должен быть добавлен заголовок с маркером доступа на разрешение с именем *blitz_user_rights*, полученным учетной записью ведущего пользователя.

Если назначаются права, то тело запроса должно содержать заполненный блок update с перечнем прав, которые должны быть добавлены в результате выполнения операции. Каждое право описывается следующими параметрами:

- *subject* – идентификатор (*sub*) учетной записи ведущего пользователя;
- *object* – идентификатор (*sub*) учетной записи ведомого пользователя;
- *rights* – перечень прав в виде массива, который получает учетная запись ведущего пользователя в отношении учетной записи ведомого пользователя. Например, для права менять пароль от учетной записи должно быть указано право *change_password* (смена пароля);
- *tags* – перечень тегов, указывающих на основания, по которым данный пользователь получил права.

Если отзываются права, то тело запроса должно содержать заполненный блок delete с перечнем прав, которые должны быть отозваны в результате выполнения операции. Каждое право описывается следующими параметрами:

- *subject* – идентификатор (*sub*) учетной записи ведущего пользователя;
- *object* – идентификатор (*sub*) учетной записи ведомого пользователя;
- *rights* – перечень прав в виде массива, которые отзываются у ведущей учетной записи в отношении ведомой учетной записи;
- *tags* – перечень тегов, указывающих на основания, по которым данный пользователь получил права.

Если при выполнении запроса права не назначаются или не отзываются, то в теле запроса должен соответственно присутствовать или пустой блок *update*, или пустой блок *delete*.

В одном запросе может быть указано сразу несколько назначаемых/отзываемых прав, но в качестве субъекта (*subject*) должен быть указан только тот пользователь, на которого был получен маркер доступа, используемый для вызова сервиса.

Пример запроса на назначение прав:

```
POST /blitz/api/v2/users/rights/change HTTP/1.1
Authorization: Bearer cNwIX…Tg
Content-Type: application/json
Cache-Control: no-cache
{
   "update":[
      {
         "subject":"6561d0d9-5583-4bb5-a681-b591358e5fcd",
         "object":"5cffd68f-2cb8-4f7a-b0f3-9fa69a1fbbcd",
         "rights":[
            "change password"
         ],
         "tags":[
            "parent"
         ]
      },
      {
         "subject":"6561d0d9-5583-4bb5-a681-b591358e5fcd",
         "object":"b855957d-bf24-48d4-bb63-cce4f5064590d",
         "rights":[
            "change_password"
         ],
         "tags":[
            "parent"
         ]
      }
   ],
   "delete":[
   ]
}
```

Пример запроса на отзыв прав:

```
POST /blitz/api/v2/users/rights/change HTTP/1.1
Authorization: Bearer cNwIX…Tg
Content-Type: application/json
Cache-Control: no-cache
{
   "update":[
   ],
   "delete":[
      {
         "subject":"b855957d-bf24-48d4-bb63-cce4f5064590d",
         "object":"5cffd68f-2cb8-4f7a-b0f3-9fa69a1fbbcd",
         "rights":[
            "change password"
         ],
         "tags":[
            "parent"
         ]
      }
   ]
}
```

Запрос может завершиться ошибкой. В этом случае Blitz Identity Provider отклонит запрос целиком и вернет перечень возникших ошибок. Пример ответа с ошибками:

```
{
   "errors" : [
      {
         "code" : "validation_error",
         "params" : {},
```

```
         "desc" : "(For subject 'dea75b73-a2ba-4b60-a41c-bb640968826b') Incorrect right '' to
object '5cffd68f-2cb8-4f7a-b0f3-9fa69a1fbbcd'"
      },
      {
         "params" : {},
         "code" : "validation_error",
         "desc" : "(For subject 'dea75b73-a2ba-4b60-a41c-bb640968826b') Incorrect tag '' for
right 'write' to object '5cffd68f-2cb8-4f7a-b0f3-9fa69a1fbbcd'"
      },
      {
         "desc" : "(For subject 'dea75b73-a2ba-4b60-a41c-bb640968826b') Incorrect object ''",
         "code" : "validation error",
         "params" : {}
      },
      {
         "desc" : "Incorrect subject ''",
         "code" : "validation_error",
         "params" : {}
      }
   ]
}
```

Запрос на отзыв прав может быть выполнен приложением не только с использованием пользовательского маркера доступа, полученного на разрешение с именем *blitz_user_rights*, но и с использованием системного маркера доступа, полученного на разрешение с именем *blitz_rm_rights*. В этом случае запрос на отзыв может включать *subject* любых пользователей (для отзыва у пользователя права не потребуется, чтобы именно этот пользователь осуществлял вход в систему и получал маркер доступа – система может отзывать права любого пользователя).

A.3.2. Просмотр, назначение и отзыв прав доступа пользователей к приложениям и группам

Для выполнения запросов по просмотру, назначению, отзыву прав доступа пользователей к приложениям и группам приложение должно получить маркер доступа с системным разрешением *blitz_rights_full_access*.

Назначение прав выполняется через HTTP PUT вызов сервиса, а отзыв через HTTP DELETE.

Пример запроса на назначение права доступа пользователя на группу:

```
PUT /blitz/api/v3/rights
Authorization: Bearer cNwIX…Nz
Content-Type: application/json
Cache-Control: no-cache

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

Пример запроса на отзыв права доступа на группу:

```
DELETE /blitz/api/v3/rights
Authorization: Bearer cNwIX…Nz
Content-Type: application/json
Cache-Control: no-cache

[{
    "subject": "указать sub пользователя",
    "object": "указать org_id организации",
    "objectType": "grps",
    "rights": ["ORG_ADMIN"],
```

```
    "tags": ["set_from_lk"]
}]
```

Пример запроса на назначение права доступа пользователя на приложение:

```
PUT /blitz/api/v3/rights
Authorization: Bearer cNwIX…Nz
Content-Type: application/json
Cache-Control: no-cache

[{
    "subject": "указать sub пользователя",
    "object": "указать client_id приложения",
    "objectType": "its",
    "rights": ["APP_ADMIN"],
    "tags": ["set from lk"]
}]
```

Пример запроса на отзыв права доступа на приложение:

```
DELETE /blitz/api/v3/rights
Authorization: Bearer cNwIX…Nz
Content-Type: application/json
Cache-Control: no-cache

[{
    "subject": "указать sub пользователя",
    "object": "указать client id приложения",
    "objectType": "its",
    "rights": ["APP_ADMIN"],
    "tags": ["set_from_lk"]
}]
```

Получить права всех пользователей к конкретной группе можно с помощью HTTP GET вызова сервиса *https://login.company.com/blitz/api/v3/rights/on/grps/<org_id>?objectExt=<profile>*

Пример ответа сервиса:

```
{
    "BIP-3SGR7TA": [
        "ORG_ADMIN"
    ]
}
```

Получить права всех пользователей к конкретному приложению можно с помощью HTTP GET вызова сервиса *https://login.company.com/blitz/api/v3/rights/on/its/<app_id>*

Пример ответа сервиса:

```
{
    "BIP-3SGR7TA": [
        "APP_ADMIN"
    ]
}
```

Получить все права пользователя можно с помощью HTTP GET вызова сервиса *https://login.company.com/blitz/api/v3/rights/of/<sub>*

Пример ответа сервиса:

```
{
    "grps|1002333570|orgs": {
        "ORG_ADMIN": [
            "set_from_api"
        ]
    }
}
```

A.4. Изменение пароля ведомой учетной записи пользователя

Изменение пароля ведомой учетной записи пользователя с помощью ведущей учетной записи пользователя осуществляется методом POST по адресу *https://login.company.com/blitz/api/v2/users/{subject}/password*, где subject – это

идентификатор (*sub*) ведомой учетной записи. В запрос должен быть добавлен заголовок с маркером доступа на разрешение с именем *blitz_change_password*, полученным ведущей учетной записью. Ведущий пользователь может вызвать смену пароля ведомого только если ранее ведущему пользователю было дано право на изменение пароля change_password (см. А.3.1).

Тело запроса должно содержать атрибут *value* со значением нового пароля. Переданный пароль должен соответствовать требованиям настроенной парольной политики.

Пример запроса:

```
POST /blitz/api/v2/users/c574a512-3704-4576-bc3a-3fe28b636e85/password HTTP/1.1
Authorization: Bearer cNwIX…Tg
Content-Type: application/json
Cache-Control: no-cache
{"value":"QWErty1234"}
```

При успешной смене пароля сервис возвращает статус *200 (OK)*.

При наличии ошибки сервис возвращает описание полученной ошибки.

Пример ответа с обнаруженными ошибками:

```
{
    "errors": [
        {
            "code": "access_denied",
            "desc": "Not enough rights: change password",
            "params": {}
        }
    ]
}
```

А.5. Сервисы для работы с группами пользователей

Blitz Identity Provider предоставляет системе сервисы для выполнения действий с группами пользователей:

- получение атрибутов группы.
- создание группы.
- изменение атрибутов группы.
- удаление группы.
- получение списка пользователей группы.
- добавление пользователей в группу.
- исключение пользователей из группы.

Для вызова сервисов система должна получить маркер доступа на системное разрешение *blitz_groups* (инструкцию в пп. А.1) и включать его во все вызываемые сервисы, описанные в следующих подразделах.

Список атрибутов групп пользователей приведен в качестве образца. Содержание списка необходимо скорректировать в зависимости от конкретных настроек, сделанных при

внедрении Blitz Identity Provider. См. «Руководство администратора».

Группы в Blitz Identity Provider описываются следующими атрибутами:

– *id* – идентификатор группы в Blitz Identity Provider;
– *name* – наименование группы пользователей.

A.5.1. Получение атрибутов группы

Если известен id группы, то получение атрибутов группы выполняется с помощью вызова методом GET сервиса по адресу *https://login.company.com/blitz/api/v2/grps/{id}*. Запрос должен включать следующие URL-параметры:

– *profile* – имя профиля групп пользователей (например, *orgs*);
– *expand* – значение true, указывающее, что необходимо вернуть все атрибуты группы.

Пример запроса получения атрибутов группы:

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

Пример ответа:

```
{
    "instanceId":
"Mzg5LWRzOnVpZD01ZjdiMDU4MC1jZDJlLTQxNDYtOGZjNS02ZWI1YTk1YzdiNDIsb3U9c3ViLGRjPXN1ZGlyLGRjPXJlYXhv
ZnQsZGM9cnU",
    "id": "14339e8e-a665-4556-92f1-5c348eff6696",
    "OGRN": "1234567890329",
    "INN": "7743151614",
    "name": "ООО Тестовая компания",
    "profile": "orgs"
}
```

Если не известен id группы, то поиск группы и получение ее атрибутов выполняется с помощью вызова методом GET сервиса по адресу *https://login.company.com/blitz/api/v2/grps*. Запрос должен включать следующие URL-параметры:

– *profile* – имя профиля групп пользователей;
– *rql* – указывается поисковый запрос по атрибутам группы. Запрос имеет формат Resource Query Language (RQL)[44].Поддерживаются следующие операции:
  - *and* – одновременное выполнение поисковых условий;
  - *or* – альтернативное выполнение поисковых условий (например, поиск по разным атрибутам);
  - *eq* – проверка условия равенства;
  - *limit* – ограничение числа возвращаемых записей.

[44] См.: https://github.com/kriszyp/rql

– *expand* (необязательный параметр) – требуется ли включать в полученный ответ атрибуты групп (true) или достаточно только вернуть идентификаторы найденных группы (false).

В результате выполнения запроса Blitz Identity Provider вернет JSON, содержащий перечень групп, удовлетворяющих заданным поисковым условиям. Группы будут возвращены с указанием их идентификатора (*id*), а также значения остальных атрибутов групп (в случае expand=true).

Пример запроса с поиском групп по атрибутам (ОГРН или ИНН в примере):

```
GET /blitz/api/v2/grps?profile=orgs&expand=true&rql=
or(eq(OGRN,string:1230123456789),eq(INN,string:7743151614)) HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache
```

Пример ответа:

```
[
    {
        "instanceId": "Mzg5L…nU",
        "id": "14339e8e-a665-4556-92f1-5c348eff6696",
        "OGRN": "1234567890329",
        "INN": "7743151614",
        "name": "ООО Тестовая компания",
        "profile": "orgs"
    }
]
```

A.5.2. Создание группы пользователей

Для создания группы пользователей необходимо вызвать методом POST сервис по адресу *https://login.company.com/blitz/api/v2/grps*.

Тело запроса должно содержать следующие параметры:

– *profile* – имя профиля групп пользователей;

– *id* – уникальный идентификатор группы;

– {остальные атрибуты группы и их значения}

Пример запроса:

```
POST /blitz/api/v2/grps/ HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache

{
    "id":"95339e8e-a665-4556-92f1-5c348eff6696",
    "OGRN":"9876543210321",
    "INN":"5012345678",
    "name":"ООО Тестовая компания 2",
    "profile":"orgs"
}
```

Пример ответа:

```
{
    "instanceId": "b3Jnc…dQ",
    "name": "ООО Тестовая компания 2",
    "OGRN": "9876543210321",
    "id": "95339e8e-a665-4556-92f1-5c348eff6696",
    "profile": "orgs",
    "INN": "5012345678"
}
```

A.5.3. Изменение атрибутов группы пользователей

Для изменения атрибутов группы необходимо вызвать методом POST сервис по адресу *https://login.company.com/blitz/api/v2/grps/{id}?profile=orgs* с новым набором атрибутов.

Тело запроса должно содержать следующие параметры:

- *profile* – имя профиля групп (должно быть передано и в составе URL, и в теле запроса);
- *id* – идентификатор группы;
- {остальные атрибуты группы и их значения}

Пример запроса:

```
POST /blitz/api/v2/grps/5f7b0580-cd2e-4146-8fc5-6eb5a95c7b42? profile=orgs HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache

{
    "id": "5f7b0580-cd2e-4146-8fc5-6eb5a95c7b42",
    "OGRN": "1147746651733",
    "INN": "7715434658",
    "name": "Новое название",
    "profile": "orgs"
}
```

Пример ответа:

```
{
    "instanceId": "Mzg5L…nU",
    "id": "5f7b0580-cd2e-4146-8fc5-6eb5a95c7b42",
    "OGRN": "1147746651733",
    "INN": "7715434658",
    "name": "Новое название",
    "profile": "orgs"
}
```

Привет ответа с ошибкой (организация не существует):

```
{
    "errors": [
        {
            "code": "group_not_found",
            "desc": "Group with '95339e8e-…97' id not found in '389-ds' LDAP group store",
            "params": {}
        }
    ]
}
```

A.5.4. Удаление группы пользователей

> **Примечание** — МПГУ не требуется вызывать этот сервис в ПРОД-окружении. Но использование сервиса может быть полезно для отладки в ТЕСТ-окружении.

Для удаления группы необходимо вызвать методом DELETE сервис по адресу *https://login.company.com/blitz/api/v2/grps/{id}?profile=orgs* без передачи тела запроса.

Пример запроса:

```
DELETE /blitz/api/v2/grps/5f7b0580-cd2e-4146-8fc5-6eb5a95c7b42? profile=orgs HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache
```

A.5.5. Получение списка пользователей в группе пользователей

Для получения списка пользователей из группы пользователей необходимо вызвать методом GET сервис по адресу *https://login.company.com/blitz/api/v2/grps/{id}/members*. Запрос должен включать следующие URL-параметры:

- *profile* – имя профиля групп пользователей;
- *expand* (необязательный параметр) – требуется ли включать в полученный ответ ФИО пользователя (true) или достаточно только вернуть их идентификаторы (false).

Пример запроса:

```
GET /blitz/api/v2/grps/14339e8e-a665-4556-92f1-5c348eff6696/members? profile=orgs&expand=false
HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache
```

Пример ответа (при expand=false):

```
[
    {
        "instanceId": "Mzg5L…J1",
        "subjectId": "d434b7d4-9816-460a-83aa-0a994226cbe7"
    },
    {
        "instanceId": "Mzg5L…J1",
        "subjectId": "2cafa5f4-bc84-4f6f-91aa-080da47975f0"
    }
]
```

Пример ответа (при expand=true):

```
[
    {
        "instanceId": "Mzg5L…J1",
        "LastName": "Иванов",
        "MiddleName": "Иванович",
        "FirstName": "Иван",
        "subjectId": "d434b7d4-9816-460a-83aa-0a994226cbe7"
    },
    {
        "instanceId": "Mzg5L…J1",
        "LastName": "Сергеев",
        "MiddleName": "Сергеевич",
        "FirstName": "Сергей",
        "subjectId": "2cafa5f4-bc84-4f6f-91aa-080da47975f0"
    }
]
```

A.5.6. Включение пользователей в группу

Для добавления пользователей в группу необходимо вызвать методом POST сервис по адресу *https://login.company.com/blitz/api/v2/grps/{id}/members/add?profile=orgs*.

Тело запроса должно содержать список добавляемых в группу пользователей с указанием их идентификаторов (*sub)* в атрибуте *subjectId*.

Пример запроса:

```
POST /blitz/api/v2/grps/5f7b0580-cd2e-4146-8fc5-6eb5a95c7b42/members/add? profile=orgs HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache

[
    {
        "subjectId": "45ff69f2-6c40-418f-a21d-cbe6f07b88c9"
    },
    {
```

```
        "subjectId": "cc8c4589-b2f8-40b8-b351-36d643808943"
    }
]
```

Пример ответа (при успешном исполнении):

```
[
    {
        "instanceId": "Mzg5L…J1",
        "storeId": "tam",
        "subjectId": "45ff69f2-6c40-418f-a21d-cbe6f07b88c9"
    },
    {
        "instanceId": "Nzg5L…J1",
        "storeId": "tam",
        "subjectId": "cc8c4589-b2f8-40b8-b351-36d643808943"
    }
]
```

Пример ответа при ошибке (попытка добавить несуществующего пользователя):

```
{
    "errors": [
        {
            "code": "user_not_found",
            "desc": "User with subjectId 'd2580c98-e584-4aad-a591-97a8cf45cd2q' not found",
            "params": {}
        }
    ]
}
```

Пример ответа при ошибке (попытка добавить того, кто уже есть в группе):

```
{
    "errors": [
        {
            "code": "some members already in group",
            "desc": "Some of adding members are already included in group",
            "params": {}
        }
    ]
}
```

A.5.7. Исключение пользователей из группы

Для исключения пользователей из группы необходимо вызвать методом POST сервис по адресу *https://login.company.com/blitz/api/v2/grps/{id}/members/rm?profile=orgs*.

Тело запроса должно содержать список исключаемых из организации доверенных лиц с указанием их идентификаторов (*sub*) в атрибуте *subjectId*.

Пример запроса:

```
POST /blitz/api/v2/grps/5f7b0580-cd2e-4146-8fc5-6eb5a95c7b42/members/rm? profile=orgs HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache

[
    {
        "subjectId": "d2580c98-e584-4aad-a591-97a8cf45cd2a"
    }
]
```

Пример ответа (при успехе):

```
[
    {
        "instanceId": "Mzg5L…J1",
        "storeId": "389-ds",
        "subjectId": "d2580c98-e584-4aad-a591-97a8cf45cd2a"
    }
]
```

Пример ответа (при попытке удалить из группы того, кого там уже нет):

```
{
    "errors": [
```

```
        {
            "code": "some_members_not_in_group",
            "desc": "Some of removing members are not included in group",
            "params": {}
        }
    ]
}
```

Пример ответа (при попытке удалить несуществующего пользователя):

```
{
    "errors": [
        {
            "code": "user_not_found",
            "desc": "User with subjectId 'd2580c98-e584-4aad-a591-97a8cf45cd2b' not found",
            "params": {}
        }
    ]
}
```

A.6. Сервисы для управления учетной записью пользователя

Blitz Identity Provider предоставляет сервисы для управления учетной записью пользователя, позволяющие осуществлять следующие операции для существующих функций Blitz Identity Provider:

- получение атрибутов пользователя;
- изменение пароля пользователем;
- проверка состояния режима двухфакторной аутентификации;
- включение/отключение режима двухфакторной аутентификации;
- проверка наличия у пользователя привязки TOTP-генератора;
- привязка TOTP-генератора в качестве средства двухфакторной аутентификации;
- отвязка TOTP-генератора от учетной записи пользователя;
- получение списка привязанных к учетной записи пользователя социальных сетей;
- создание новой привязки социальной сети к пользователю;
- удаление привязки учетной записи социальной сети;
- получение списка событий аудита пользователя;
- получение списка известных устройств пользователя;
- удаления устройства пользователя из списка известных устройств;
- получение списка разрешений, выданных пользователем;
- отзыв выданного пользователем разрешения;
- получение списка привязанных к учетной записи пользователя мобильных приложений;
- отвязка от учетной записи пользователя привязанного мобильного приложения;
- изменение значения атрибута учетной записи пользователя;
- изменение номера мобильного телефона;
- изменение адреса электронной почты;

– получение атрибутов любого пользователя по его идентификатору.

Предоставляемые Blitz Identity Provider сервисы можно вызывать в двух режимах:

– Пользовательский режим;
– Системный режим.

В пользовательском режиме сервис вызывается с правами в отношении учетной записи текущего авторизованного пользователя. При вызове сервиса должны передаваться следующие заголовки:

– Authorization: Bearer <*маркер доступа с пользовательскими разрешениями*> – авторизационный заголовок, содержащий маркер доступа с разрешениями текущего пользователя. Разрешения описаны в таблице 1.
– X-Forwarded-For*:* <*IP-адрес пользователя*> – заголовок, в котором должно быть передано значение IP-адреса пользователя. Данное значение будет записано в событие безопасности Blitz Identity Provider.
– User-Agent: <*значение User-Agent пользователя*> – заголовок, в котором должно быть передано значение User-Agent устройства пользователя. Данное значение будет записано в событие безопасности Blitz Identity Provider.

A.6.1. Получение атрибутов пользователя

Для получения атрибутов любого пользователя по его идентификатору необходимо методом GET вызвать сервис по адресу *https://login.company.com/blitz/api/v3/users/{subjectId}*.

Необходимые разрешения: blitz_api_user или blitz_api_sys_users.

В результате выполнения запроса Blitz Identity Provider вернет JSON, содержащий атрибуты пользователя.

Пример запроса:

```
GET /blitz/api/v3/users/d2580c98-e584-4aad-a591-97a8cf45cd2a HTTP/1.1
Authorization: Bearer cNw…Nz
Content-Type: application/json
```

Пример ответа:

```
{
    "family_name": "Иванов",
    "sub": "d2580c98-e584-4aad-a591-97a8cf45cd2a",
    "name": "Иван",
    "locked": false,
    "meta": {
        "instanceId": "Mzg…J1",
        "unmodifiable": [
            "sub"
        ]
    }
}
```

В блоке meta передаются метаданные учетной записи. Атрибут instanceId нужен для возможности вызова в последующем сервисов изменения атрибутов учетной записи и изменения пароля.

A.6.2. Изменение пароля пользователем

Для изменения пароля необходимо вызвать методом POST сервис по адресу *https://login.company.com/blitz/api/v3/users/{instanceId}/pswd*.

Чтобы узнать значение instanceId для пользователя, необходимо предварительно вызвать методом GET сервис получения атрибутов пользователя (A.6.1).

Необходимые разрешения: blitz_api_usec_chg или blitz_api_sys_usec_chg.

При смене пароля в пользовательском режиме необходимо передать заголовки с IP-адресом пользователя и User-Agent.

В Blitz Identity Provider есть функция безопасности, что при смене пользователем пароля происходит аннулирование всех сессий пользователя и удаление всех запомненных устройств, с которых пользователь ранее осуществлял вход, и на которых был возможен повторный вход без ввода пароля. В сценарии самостоятельной смены пользователем пароля в Личном кабинете может быть нежелательно, чтобы произошел выход пользователя в том числе с текущего устройства/браузера. Для того, чтобы указать Blitz Identity Provider, что определенное устройство необходимо сохранить по результатам успешной смены пароля (не делать с него логаут), необходимо в вызов сервиса смены пароля передать от приложения Cookie со следующими характеристиками:

- имя cookie – bfp;
- домен cookie – https://login.company.com
- путь (path) cookie – /blitz
- срок действия cookie – 30 дней
- значение cookie – рассчитанный с помощью JS-библиотеки fingerprint2js версии 1.7.0 (https://github.com/fingerprintjs/fingerprintjs2/tree/1.7.0) браузерный отпечаток. Вызов функции расчета браузерного отпечатка должен производиться со следующими параметрами:

```
var options = {excludeAvailableScreenResolution: true}
new Fingerprint2(options).get(function(result, components) {
  console.log(result)
});
```

Тело запроса должно содержать следующие параметры:

- *current* – текущий пароль пользователя (только при смене пароля в пользовательском режиме);
- *new* – новый пароль пользователя.

Пример запроса (в пользовательском режиме смены пароля):

```
POST /blitz/api/v3/users/Mzg…J1/pswd HTTP/1.1
Content-Type: application/json
X-Forwarded-For: 200.200.100.100
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.106 Safari/537.36
Authorization: Bearer wzb…Tw
Cookie: bfp=b29d8214bad71e2511151d6a27c7ce15
```

```
{
    "current": "QWErty123",
    "password": "P@$$w0rd"
}
```

Пример запроса (в режиме смены пароля системой):

```
POST /blitz/api/v3/users/Mzg…J1/pswd HTTP/1.1
Content-Type: application/json
Authorization: Bearer qwa…Ez
{
    "password": "P@$$w0rd"
}
```

В случае успешного вызова Blitz Identity Provider вернет код *HTTP 204 No Content*. Смена пароля также приведет к аннулированию ранее полученных маркеров доступа и маркеров обновления текущего пользователя.

Если смена пароля завершилась ошибкой, то Blitz Identity Provider вернет сообщение об ошибке. Возможны коды ошибок *HTTP 401 Unauthorized* в случае ошибки контроля доступа (неправильный маркер доступа или неправильный текущий пароль пользователя) или *HTTP 400 Bad Request* (новый пароль не удовлетворяет требованиям парольной политики).

Пример ошибки с неправильным текущим паролем:

```
{
    "type": "security_error",
    "error": "invalid credential",
    "desc": "Wrong subject identifier or current password"
}
```

Пример ошибки с неправильным маркером доступа:

```
{
    "type": "security_error",
    "error": "bad_access_token",
    "desc": "BEARER_AUTH: CRID does not match"
}
```

Пример ошибки, что новый пароль не соответствует парольной политике (слишком короткий):

```
{
    "type": "input_error",
    "error": "wrong_values",
    "errors": [
        {
            "type": "input_error",
            "error": "password_policy_violated",
            "desc": "Password's length must be greater than 6",
            "pos": "password",
            "params": {
                "rule": "to short",
                "low": 6
            }
        }
    ]
}
```

Пример ошибки, что новый пароль не соответствует парольной политике (совпадает с ранее использованным):

```
{
    "type": "input_error",
    "error": "password_policy_violated",
    "desc": "Failed to update password\n",
    "pos": "password",
    "params": {
        "rule": "id_store"
    }
}
```

Пример ошибки, что новый пароль не соответствует парольной политике (не содержит требуемых групп символов):

```
{
    "type": "input_error",
    "error": "wrong_values",
    "errors": [
        {
            "type": "input error",
            "error": "password policy violated",
            "desc": "Password doesn't match enough symbols groups",
            "pos": "password",
            "params": {
                "rule": "not enough groups",
                "no matched groups": [
                    {
                        "desc": "password.policy.desc.digits",
                        "min_number_symbols": 1
                    },
                    {
                        "desc": "password.policy.desc.capital",
                        "min_number_symbols": 1
                    },
                    {
                        "desc": "password.policy.desc.special",
                        "min number symbols": 1
                    }
                ]
            }
        }
    ]
}
```

A.6.3. Проверка состояния режимов аутентификации

Можно проверить состояния следующих режимов аутентификации учетной записи:

- включена ли у пользователя двухфакторная аутентификация;
- установлен ли у пользователя признак необходимости смены пароля;
- установлен ли у пользователя временный запрет по входу с использованием определенного метода входа.

Для проверки состояния режимов аутентификации необходимо вызвать методом GET сервис по адресу *https://login.company.com/blitz/api/v3/users/{subjectId}/auth*.

Необходимые разрешения: blitz_api_usec или blitz_api_sys_usec.

В ответ будут получены следующие режимы:

- *requiredFactor* – признак включенной двухфакторной аутентификации. Может принимать следующие значения:
  - *отсутствует, 0 или 1* – выключен
  - *2* – включен (требуется 2-й фактор аутентификации)
- *needPasswordChange* – признак (*true/false*) необходимости смены пароля при входе;
- *methodsLocked* – список заблокированных методов аутентификации – пользователь не может использовать именно эти методы входа, но может использовать остальные.

Пример запроса:

```
GET /blitz/api/v3/users/d2580c98-e584-4aad-a591-97a8cf45cd2a/auth HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache
```

Пример ответа:

```
{
    "requiredFactor": 2,
    "needPasswordChange": false,
    "methodsLocked": ["password"]
}
```

A.6.4. Изменение режимов аутентификации

Для изменения режимов аутентификации пользователя необходимо вызвать методом POST сервис по адресу *https://login.company.com/blitz/api/v3/users/{subjectId}/auth*.

Необходимые разрешения: blitz_api_usec_chg или blitz_api_sys_usec_chg.

При изменении настройки в пользовательском режиме необходимо передать заголовки с IP-адресом пользователя и User-Agent.

Тело запроса может содержать следующие параметры:

– *requiredFactor* – признак включенной двухфакторной аутентификации. Может принимать следующие значения:
  - *null* – выключен
  - *2* – включен (требуется 2-й фактор аутентификации)
– *needPasswordChange* – признак (*true/false*) необходимости смены пароля при входе;
– *methodsLocked* – список заблокированных методов аутентификации – пользователь не может использовать именно эти методы входа, но может использовать остальные.

  В настоящий момент Blitz Identity Provider поддерживает только блокирование использования парольного входа (password).

Пример запроса:

```
POST /blitz/api/v3/users/d2580c98-e584-4aad-a591-97a8cf45cd2a/auth HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb yPPqLOFWDuwzMDc0Nz
X-Forwarded-For: 200.200.100.100
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.106 Safari/537.36
Content-Type: application/json
Cache-Control: no-cache

{
    "requiredFactor": 2,
    "needPasswordChange": false,
    "methodsLocked": ["password"]
}
```

Пример ответа:

```
{
    "requiredFactor": 2,
    "needPasswordChange": false,
    "methodsLocked": ["password"]
}
```

Пример ошибки *HTTP 400 Bad Request* (если у пользователя не настроен ни один метод для второго фактора аутентификации):

```
{
    "type": "input_error",
    "error": "wrong values",
    "errors": [
        {
            "type": "input_error",
```

```
            "error": "has_not_sf_methods",
            "desc": "User 'd2580c98-e584-4aad-a591-97a8cf45cd2a' has not any second factor
method",
            "pos": "requiredFactor"
        }
    ]
}
```

A.6.5. Проверка наличия у пользователя привязки TOTP-генератора

Для проверки того, настроен ли у пользователя TOTP[45]-генератор кодов подтверждения, необходимо вызвать методом GET сервис по адресу *https://login.company.com/blitz/api/v3/users/{subjectId}/totps*. Если метод настроен, то в ответ будут получены его настройки.

Необходимые разрешения: blitz_api_usec или blitz_api_sys_usec.

Пример запроса:

```
GET /blitz/api/v3/users/d2580c98-e584-4aad-a591-97a8cf45cd2a/totps HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache
```

Пример ответа:

```
[
    {
        "id": "SW TOTP 1 d2580c98-e584-4aad-a591-97a8cf45cd2a",
        "len": 6,
        "name": "Google Authenticator"
    }
]
```

A.6.6. Привязка TOTP-генератора

Привязка к учетной записи пользователя TOTP-генератора осуществляется в два этапа:

- Запрос в Blitz Identity Provider QR-кода и строки привязки
- Подтверждение регистрации привязки

Необходимые разрешения: blitz_api_usec_chg или blitz_api_sys_usec_chg.

При изменении настройки в пользовательском режиме необходимо передать заголовки с IP-адресом пользователя и User-Agent.

На первом этапе приложение должно вызвать методом GET сервис по адресу *https://login.company.com/blitz/api/v3/users/{subjectId}/totps/attach/gr*. В ответ от Blitz Identity Provider будут получены атрибуты:

- *base64QRCode* – QR-код привязки генератора, который нужно отобразить пользователю;
- *base32Secret* – секретная строка привязки генератора, которую нужно отобразить пользователю, если ему неудобно будет фотографировать QR-код, и он предпочтет ввести код привязки в генератор вручную.

[45] RFC 6238 «TOTP: Time-Based One-Time Password Algorithm», см.: https://tools.ietf.org/html/rfc6238

Пример запроса:

```
GET /blitz/api/v3/users/d2580c98-e584-4aad-a591-97a8cf45cd2a/totps/attach/gr HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache
```

Пример ответа:

```
{
    "base64QRCode":
"iVBORw0KGgoAAAANSUhEUgAAAT4AAAE+AQMAAAAu9u5zAAAABlBMVEX///8AAABVwtN+AAAACXBIWXMAAA7EAAAOxAGVKw4b
AAACWUlEQVRoge2ZYW7sMAiEkXKAHMlX95FyAEsUZiC72e47QOcZRZVrf+kPCgMmZtu2bdu27U/b6WHLzC+Ln3jGOmec5IFPU
TCXcXhcI/bjPbMRm8GuPpUEwwdwzzjST4HPWKefTl/a4OnHZfFYecUzRv4DMJZHeiXzIN6QB61TIbyS0ZHvcfNfOSMAQvaY8c
/nqz6KgGWDe4iFmZFyfRJSINSd5xQAPN5HoiBEPTPeUwks1wM7of3zGRRCYOyhpoVX6qSTvuRfE5wUPIeHGBFUPuxPUZCpMFr
/8tfQfm4+/agEQuFQ3BbiAn0cIuWzYVcCHewAgjsKfEMVXC/vqIHlDIQAuvW+pZ3zmQpK4DyQAVS+hQY2380kGG/eUQPZuVT2
p/b7S/l+5YwMyG2WOBR29O89kxAF/Wj3MO8rLi5WgCkKzsp1s2riSv+sE0IRTHW313ipGva6mguDmDpg4VXr2Ly/zx7UwLuq5
3apO8AaRaiCnDR0ZcvouEv9o52RAtHOxD2saprTMdnMQgw0Qcwe4p/PC+i6VRAxcjwEQAiES9i2x29s6NjTrZ4/KYK8pmRQsJ
ExuKeTQxbEBYUjc3wX6nnb7xGyEkidY7eOnLjvo59DFyGwZoeYIzq1nx7qTkcUvKB8VyYBcgLDJ5ipgoVju8rd4B/grFET7E9
Dznm5v1Tw8yIuBeayB8b82jmoAfdtVRL0Hij2BJ2TNgTIs7OXA0vXKQP9nn1xjxaYsxaf1Lwepn4LChXQkAqMfdY03Mysy50k
WLK3+rtf3s96dv5uUuC2bdu2bfuT9gNGBejlELmovwAAAABJRU5ErkJggg==",
    "base32Secret": "W247OHVTPPTIAOXMGKK6Z7BZ3DEYWO74"
}
```

На втором этапе приложение должно вызвать методом POST сервис по адресу *https://login.company.com/blitz/api/v3/users/{subjectId}/totps/attach/gr*.

Тело запроса должно содержать следующие параметры:

- *base32Secret* – секретная строка инициализации TOTP-генератора;
- *otpCode* – код подтверждения, выработанный генератором по алгоритму TOTP от строки secret и текущего временного слота;
- *name* – отображаемое имя TOTP-генератора (необязательно).

Пример запроса:

```
POST /blitz/api/v3/users/d2580c98-e584-4aad-a591-97a8cf45cd2a/totps/attach/gr HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
X-Forwarded-For: 200.200.100.100
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.106 Safari/537.36

{
    "base32Secret": "W247OHVTPPTIAOXMGKK6Z7BZ3DEYWO74",
    "name": "Google Authenticator",
    "otpCode": "123456"
}
```

Пример ответа:

```
{
    "base64QRCode": "iVB…g==",
    "base32Secret": "W247OHVTPPTIAOXMGKK6Z7BZ3DEYWO74"
}
```

В случае успешного выполнения сервис вернет *HTTP 204 No Content*.

В случае ошибки сервис вернет *HTTP 400 Bad Request*.

Пример ошибки, если передан неправильный код:

```
{
    "type": "process_error",
    "error": "wrong_otp_code"
}
```

A.6.7. Удаление привязки TOTP-генератора

Чтобы удалить привязку TOTP-генератора к учетной записи пользователя, необходимо вызвать методом DELETE сервис по адресу

https://login.company.com/blitz/api/v3/users/{subjectId}/totps/{id}, где в качестве id указать идентификатор привязки, полученный в пп. А.6.5.

Необходимые разрешения: blitz_api_usec_chg или blitz_api_sys_usec_chg.

При вызове в пользовательском режиме необходимо передать заголовки с IP-адресом пользователя и User-Agent.

Пример запроса:

```
DELETE /blitz/api/v3/users/d2580c98-e584-4aad-a591-97a8cf45cd2a/totps/SW TOTP 1 d2580c98-e584-
4aad-a591-97a8cf45cd2a HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
X-Forwarded-For: 200.200.100.100
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10 15 5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.106 Safari/537.36
```

При успешном выполнении сервис вернет *HTTP 204 No Content*.

А.6.8. Получение списка привязанных социальных сетей

Чтобы получить список привязок социальных сетей к учетной записи пользователя, необходимо вызвать методом GET сервис по адресу *https://login.company.com/blitz/api/v2/users/{subjectId}/fa*. В ответ будут получены тип привязки (*fpKey*) и идентификатор привязки (*sid*).

Пример запроса:

```
GET /blitz/api/v2/users/d2580c98-e584-4aad-a591-97a8cf45cd2a/fa HTTP/1.1
Authorization: Basic ZG5ldm5pay10ZXN0Lm1vcy5ydTphUU56S0JuY2VBQVQwelg
Cache-Control: no-cache
```

Пример ответа:

```
[
    {
        "sid": "1169460959792489",
        "fpKey": "facebook:facebook_1",
        "sbjId": "d2580c98-e584-4aad-a591-97a8cf45cd2a"
    },
    {
        "sid": "385956543",
        "fpKey": "vk:vk_1",
        "sbjId": "d2580c98-e584-4aad-a591-97a8cf45cd2a"
    }
]
```

А.6.9. Создание новой привязки социальной сети к пользователю

Привязка к учетной записи социальной сети осуществляется в два этапа:

- Запрос инструкции привязки
- Выполнение привязки

На первом этапе приложение должно вызвать методом POST сервис по адресу *https://login.company.com/blitz/api/v2/users/current/fa/bind*.

Тело запроса должно содержать следующие параметры:

- *fp* – идентификатор поставщика, связь с профилем которого должна быть установлена;

– *callback* – адрес, на который должен быть возвращен пользователь после успешной привязки аккаунта соцсети;
– *isPopup* – требуется ли открытие страницы поставщика идентификации в popup-окне (опционально).

Пример запроса:

```
POST /blitz/api/v2/users/current/fa/bind HTTP/1.1
Authorization: Basic ZG5ldm5pay10ZXN0Lm1vcy5ydTphUU56S0JuY2VBQVQwelg
Content-Type: application/json
Cache-Control: no-cache

{
    "fp": "vk:vk_1",
    "callback": "https://app.company.com/callback"
}
```

В ответ от Blitz Identity Provider будет получен параметр *redirectTo* с ссылкой, на которую необходимо направить пользователя в браузере для выполнения второго этапа и создания привязки учетной записи пользователя к социальной сети.

Пример ответа:

```
{
    "redirectTo": "https://oauth.vk.com/authorize?state=5c415063-a153-424c-af9c-023a6bbf1892&scop
e=email&redirect_uri=https%3A%2F%2Flogin.company.com%2Fblitz%2Fapi%2Fusers%2Fcurrent%2Ffps%2Fbind
%2Fcb%2Fvk%2Fvk_1&client_id=5566286&v=5.52&response_type=code"
}
```

A.6.10. Удаление привязки социальной сети

Чтобы удалить привязку социальной сети к пользователю, необходимо вызвать методом DELETE сервис по адресу *https://login.company.com/blitz/api/v2/users/{subjectId}/fa/{sid}*, где в качестве параметров передается *guid* пользователя (*subjectId*) и идентификатор привязки (*sid*), полученный в пп. A.6.8.

Пример запроса:

```
DELETE /blitz/api/v2/users/d2580c98-e584-4aad-a591-97a8cf45cd2a/fa/385956543 HTTP/1.1
Authorization: Basic ZG5ldm5pay10ZXN0Lm1vcy5ydTphUU56S0JuY2VBQVQwelg
Cache-Control: no-cache
```

A.6.11. Получение списка событий аудита пользователя

Для получения списка событий безопасности, зарегистрированных на учетную запись пользователя, необходимо методом GET вызвать сервис по адресу *https://login.company.com/blitz/api/v3/users/{subjectId}/audit*.

Необходимые разрешения: blitz_api_uaud или blitz_api_sys_uaud.

Запрос должен включать следующие URL-параметры:

– *rql* – указывается запрос фильтрации выводимых сведений. Поддерживается фильтрация по атрибуту *ts* (время события). Запрос имеет формат Resource Query Language (RQL)[46].Поддерживаются следующие операции:

[46] См.: https://github.com/kriszyp/rql

- *and* – одновременное выполнение поисковых условий;
- *lt* – проверка условия «меньше»;
- *gt* – проверка условия «больше»;
- *limit* – ограничение числа возвращаемых записей.

В результате выполнения запроса Blitz Identity Provider вернет JSON, содержащий перечень событий аудита учетной записи за указанный период времени.

Пример запроса:

```
GET /blitz/api/v3/users/d2580c98-e584-4aad-a591-97a8cf45cd2a/audit?
rql=and(le(ts,1552894000000),gt(ts,1552898000000),limit(10)) HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache
```

Пример ответа:

```
[
    {
        "ts": 1552896932780,
        "client id": "app1",
        "event": "login",
        "ip": 2887320577,
        "device": "iPhone"
    }
]
```

A.6.12. Получение списка известных устройств пользователя

Для получения списка устройств пользователя необходимо методом GET вызвать сервис по адресу *https://login.company.com/blitz/api/v3/users/{subjectId}/devices*.

Необходимые разрешения: blitz_api_uapps или blitz_api_sys_uapps.

В результате выполнения запроса Blitz Identity Provider вернет JSON, содержащий перечень устройств пользователя.

Пример запроса:

```
GET /blitz/api/v3/users/d2580c98-e584-4aad-a591-97a8cf45cd2a/devices HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache
```

Пример ответа:

```
[
    {
        "fingerprint": "8b29b8861a4d3affb315aee498a3dc17",
        "browser": "Chrome",
        "name": "iPhone",
        "lastUsed": 1552894761331
    }
]
```

A.6.13. Удаления устройства пользователя из списка известных устройств

Для удаления устройства из числа запомненных необходимо методом DELETE вызвать сервис *https://login.company.com/blitz/api/v3/users/{subjectId}/devices/{fingerprint}*, передав в качестве *fingerprint* полученный в пп. A.6.12 отпечаток устройства.

Необходимые разрешения: blitz_api_uapps_chg или blitz_api_sys_uapps_chg.

При вызове в пользовательском режиме необходимо передать заголовки с IP-адресом пользователя и User-Agent.

Пример запроса:

```
DELETE /blitz/api/v3/users/d2580c98-e584-4aad-a591-97a8cf45cd2a/devices/8b29b8861a4d3affb315aee49
8a3dc17 HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache
X-Forwarded-For: 200.200.100.100
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.106 Safari/537.36
```

A.6.14. Получение списка разрешений, выданных пользователем

Для получения списка выданных пользователем разрешений необходимо методом GET вызвать сервис по адресу *https://login.company.com/blitz/api/v3/users/{subjectId}/acls*.

Необходимые разрешения: blitz_api_usec или blitz_api_sys_usec.

В результате выполнения запроса Blitz Identity Provider вернет JSON, содержащий перечень устройств пользователя.

Пример запроса:

```
GET /blitz/api/v3/users/d2580c98-e584-4aad-a591-97a8cf45cd2a/acls HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache
```

Пример ответа:

```
[
    {
        "id": "d2580c98-e584-4aad-a591-97a8cf45cd2a app1",
        "updated": 1552896932780,
        "client_id": "app1",
        "scopes": [
            "openid",
            "profile",
        ]
    }
]
```

A.6.15. Отзыв выданного пользователем разрешения

Для отзыва выданного разрешения необходимо методом DELETE вызвать сервис *https://login.company.com/blitz/api/v3/users/{subjectId}/acls/{acl_id}*, передав в качестве *acl_id* полученный в пп. A.6.14 идентификатор (id) разрешения.

Необходимые разрешения: blitz_api_usec_chg или blitz_api_sys_usec_chg.

При вызове в пользовательском режиме необходимо передать заголовки с IP-адресом пользователя и User-Agent.

Пример запроса:

```
DELETE /blitz/api/v3/users/d2580c98-e584-4aad-a591-97a8cf45cd2a/acls/
d2580c98-e584-4aad-a591-97a8cf45cd2a_app1 HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache
```

A.6.16. Получение списка привязанных мобильных приложений

Для получения списка привязанных мобильных приложений необходимо методом GET вызвать сервис по адресу *https://login.company.com/blitz/api/v3/users/{subjectId}/apps*.

Необходимые разрешения: blitz_api_uapps или blitz_api_sys_uapps.

В результате выполнения запроса Blitz Identity Provider вернет JSON, содержащий перечень устройств пользователя.

Пример запроса:

```
GET /blitz/api/v3/users/d2580c98-e584-4aad-a591-97a8cf45cd2a/apps HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache
```

Пример ответа:

```
[
    {
        "id": "dyn:test_app:afae0cab-2649-482d-9832-5f73816afb59",
        "name": {
            "_default_": "Тестовое приложение (test_app)"
        },
        "availableScopes": [
            "openid",
            "profile"
        ],
        "softwareId": "test_app"
    }
]
```

A.6.17. Отвязка от учетной записи пользователя привязанного мобильного приложения

Для отзыва выданного разрешения необходимо методом DELETE вызвать сервис *https://login.company.com/blitz/api/v3/users/{subjectId}/apps/{app_id}*, передав в качестве *app_id* полученный в пп. A.6.16 идентификатор (id) привязки приложения.

Необходимые разрешения: blitz_api_uapps_chg или blitz_api_sys_uapps_chg.

При вызове в пользовательском режиме необходимо передать заголовки с IP-адресом пользователя и User-Agent.

Пример запроса:

```
DELETE /blitz/api/v3/users/d2580c98-e584-4aad-a591-97a8cf45cd2a/apps/
d2580c98-e584-4aad-a591-97a8cf45cd2a app1 HTTP/1.1
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
X-Forwarded-For: 200.200.100.100
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10 15 5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.106 Safari/537.36
Cache-Control: no-cache
```

A.6.18. Изменение атрибута учетной записи

Для изменения секретного вопроса и ответа на секретный вопрос необходимо методом POST вызвать сервис по адресу *https://login.company.com/blitz/api/v2/users/{instanceId}*.

Тело запроса должно содержать значения изменяемых атрибутов пользователя.

Пример запроса:

```
POST /blitz/api/v2/users/Mzg…J1 HTTP/1.1
Authorization: Basic ZG5ldm5pay10ZXN0Lm1vcy5ydTphUU56S0JuY2VBQVQwelg
Content-Type: application/json
Cache-Control: no-cache

{
   "family_name":"Петров"
}
```

Пример ответа:

```
{
    "family name": "Петров",
    "name": "Иван",
    "locked": false,
    "sub": "5cffd68f-2cb8-4f7a-b0f3-9fa69a1fbbcd",
    "meta": {
        "instanceId": "Mzg…J1",
        "unmodifiable": [
            "sub"
        ]
    }
}
```

A.6.19. Изменение номера мобильного телефона

Для изменения номера мобильного телефона необходимо методом POST вызвать сервис по адресу *https://login.company.com/blitz/api/v2/users/{subjectId}*.

Предусмотрены следующие режимы изменения:

– Изменение телефона сразу на подтвержденный

– Изменение телефона с прохождением подтверждения

Тело запроса должно содержать следующие параметры:

– *phone_number* – мобильный телефон, передается в виде составного объекта с атрибутами:

- *value* – номер телефона в формате 7XXXXXXXXXX;
- *vrf* – признак, что телефон подтвержден – true.

Пример запроса с изменением сразу на подтвержденный:

```
POST /blitz/api/v2/users/Mzg…J1 HTTP/1.1
Authorization: Basic ZG5ldm5pay10ZXN0Lm1vcy5ydTphUU56S0JuY2VBQVQwelg
Content-Type: application/json
Cache-Control: no-cache

{
   "phone number":{"value":"79991234567","vrf":true}
}
```

Пример ответа:

```
{
    "name": "Иван",
    "surname": "Иванов",
    "meta": {
        "instanceId": "Mzg5L…2M",
        "unmodifiable": [
            "uid"
        ]
    },
    "email": {
        "value": "aivanov+2@gmail.com",
        "vrf": true
    },
    "sub": "BIP-LIR6BO33XBBDHANE6DZPUTYVME",
    "phone_number": {
        "value": "+7(999)1234567",
        "vrf": true
    }
}
```

Пример запроса с изменением атрибута с прохождением подтверждения:

```
POST /blitz/api/v3/users/Mzg…J1 HTTP/1.1
Content-Type: application/json
X-Forwarded-For: 200.200.100.100
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.106 Safari/537.36
```

```
Authorization: Bearer wzb…Tw
{
    "phone_number":{"value":"+79999999998","vrf":false}
}
```

Пример ответа:

```
{
    "name": "Иван",
    "surname": "Иванов",
    "meta": {
        "instanceId": "Mzg5L…2M",
        "unmodifiable": [
            "sub"
        ]
    },
    "email": {
        "value": "aivanov+2@gmail.com",
        "vrf": true
    },
    "sub": "BIP-LIR6BO33XBBDHANE6DZPUTYVME",
    "notes": {
        "actions": {
            "state": "ch_EludIw5fEDouy8wpT_GVOJ7rLxKfZUi-G3blijf34yQ",
            "exp": 300,
            "code": "290334",
            "status": "code_waiting",
            "from": "+7(964)1234567",
            "attr": "mobile",
            "sbjId": "BIP-LIR6BO33XBBDHANE6DZPUTYVME",
            "ttl": 900,
            "attempts left": 3,
            "value": "+7(999)9999998",
            "action": "validate_mobile",
            "created": 1598446512
        }
    },
    "phone number": {
        "value": "+7(964)1234567",
        "vrf": true
    }
}
```

Пример запроса на подтверждение смены (в URL используется *action* и *state* из ответа сервиса):

```
POST /blitz/api/v3/ users/notes/validate_mobile/ch_El…yQ HTTP/1.1
Content-Type: application/json
X-Forwarded-For: 200.200.100.100
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10 15 5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.106 Safari/537.36
Authorization: Bearer wzb…Tw
{
    "cmd": "code",
    "value": "123456"
}
```

Пример ответа:

```
{
    "name": "Иван",
    "family name": "Иванов",
    "meta": {
        "instanceId":
"Mzg5LWRzOnVpZD1CSVAtTElSNkJPMzNYQkJESEFORTZEWlBVVFlWTUUsb3U9ZGVtbyxvdT1zdWIsZGM9cmVheG9mdCxkYz1s
b2M",
        "unmodifiable": [
            "uid"
        ]
    },
    "email": {
        "value": "aivanov+2@gmail.com",
        "vrf": true
    },
    "sub": "BIP-LIR6BO33XBBDHANE6DZPUTYVME",
    "phone_number": {
        "value": "+7(999)9999998",
        "vrf": true
    }
}
```

A.6.20. Изменение адреса электронной почты

Для изменения адреса электронной почты необходимо методом POST вызвать сервис по адресу *https://login.company.com/blitz/api/v2/users/{subjectId}*.

Предусмотрены следующие режимы изменения:

– Изменение email сразу на подтвержденный

– Изменение email с прохождением подтверждения

Тело запроса должно содержать следующие параметры:

– *email* – адрес электронной почты:

- *value* – адрес электронной почты;
- *vrf* – признак, что адрес подтвержден – true;

Пример запроса с изменением сразу на подтвержденный:

```
POST /blitz/api/v2/users/Mzg…J1 HTTP/1.1
Authorization: Basic ZG5ldm5pay10ZXN0Lm1vcy5ydTphUU56S0JuY2VBQVQwelg
Content-Type: application/json
Cache-Control: no-cache

{
   "email":{"value":"mail@example.com","vrf":true}
}
```

Пример ответа:

```
{
    "name": "Иван",
    "family name": "Иванов",
    "meta": {
        "instanceId": "Mzg5LW…2M",
        "unmodifiable": [
            "sub"
        ]
    },
    "mail": {
        "value": "mail@example.com",
        "vrf": true
    },
    "sub": "BIP-LIR6BO33XBBDHANE6DZPUTYVME",
    "phone_number": {
        "value": "+7(999)1234567",
        "vrf": true
    }
}
```

Пример запроса с изменением атрибута с прохождением подтверждения:

```
POST /blitz/api/v3/users/Mzg…J1 HTTP/1.1
Content-Type: application/json
X-Forwarded-For: 200.200.100.100
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10 15 5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.106 Safari/537.36
Authorization: Bearer wzb…Tw
{
    "email":{"value":"mail@example.com","vrf":false}
}
```

Пример ответа:

```
{
    "name": "Иван",
    "family_name": "Иванов",
    "meta": {
        "instanceId": "Mzg5L…2M",
        "unmodifiable": [
            "sub"
        ]
    },
    "email": {
        "value": "aivanov+2@gmail.com",
```

```
        "vrf": true
    },
    "sub": "BIP-LIR6BO33XBBDHANE6DZPUTYVME",
    "notes": {
        "actions": {
            "state": "ch_EludIw5fEDouy8wpT_GVOJ7rLxKfZUi-G3blijf34yQ",
            "exp": 86400,
            "code": "290334",
            "status": "code waiting",
            "from": "aivanov+2@gmail.com",
            "attr": "mail",
            "sbjId": "BIP-LIR6BO33XBBDHANE6DZPUTYVME",
            "ttl": 900,
            "attempts left": 3,
            "value": "mail@example.com",
            "action": "validate_mail",
            "created": 1598446512
        }
    },
    "phone_number": {
        "value": "+7(964)1234567",
        "vrf": true
    }
}
```

Пример запроса на подтверждение смены (в URL используется *action* и *state* из ответа сервиса):

```
POST /blitz/api/v3/ users/notes/validate_mail/ch_El…yQ HTTP/1.1
Content-Type: application/json
X-Forwarded-For: 200.200.100.100
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10 15 5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.106 Safari/537.36
Authorization: Bearer wzb…Tw
{
    "cmd": "code",
    "value": "123456"
}
```

Пример ответа:

```
{
    "name": "Иван",
    "family_name": "Иванов",
    "meta": {
        "instanceId":
"Mzg5LWRzOnVpZD1CSVAtTElSNkJPMzNYQkJESEFORTZEWlBVVFlWTUUsb3U9ZGVtbyxvdT1zdWIsZGM9cmVheG9mdCxkYz1s
b2M",
        "unmodifiable": [
            "sub"
        ]
    },
    "email": {
        "value": "mail@example.com",
        "vrf": true
    },
    "sub": "BIP-LIR6BO33XBBDHANE6DZPUTYVME",
    "phone_number": {
        "value": "+7(999)9999998",
        "vrf": true
    }
}
```

A.6.21. Получение атрибутов любого пользователя по его идентификатору

Для получения атрибутов любого пользователя по его идентификатору необходимо методом GET вызвать сервис по адресу *https://login.company.com/blitz/api/v3/users/{subjectId}*.

В результате выполнения запроса Blitz Identity Provider вернет JSON, содержащий атрибуты пользователя.

Пример запроса:

```
GET /blitz/api/v3/users/d2580c98-e584-4aad-a591-97a8cf45cd2a HTTP/1.1
```

```
Authorization: Bearer cNwIXatB0wk5ZHO0xG5kxuuLubesWcb_yPPqLOFWDuwzMDc0Nz
Content-Type: application/json
Cache-Control: no-cache
```

Пример ответа:

```
{
      "family name": "Иванов",
      "name": "Иван",
      "middle name": "Иванович",
      "phone_number": "79991234567",
      "email": "mail@example.com"
}
```

Приложение Б. Добавление дополнительного метода аутентификации

К Blitz Identity Provider могут быть подключены «внешние» методы аутентификации. Система, выступающая в качестве «поставщика» такого метода аутентификации, должна предоставить следующие API:

1. **Обработчик запроса на аутентификацию.**

Представляет собой URL для приема HTTP-запросов от Blitz Identity Provider. При запросе на аутентификацию Blitz Identity Provider будет делать запрос методом POST по данному адресу. В теле данного запроса Blitz Identity Provider в формате SON передаст следующие данные:

- идентификатор запроса (id);
- утверждения, характеризующие пользователя (claims) – опционально, только при вызове в качестве второго фактора;
- идентификатор системы, запросивший вход (rpId);
- идентификатор контекста аутентификации (loginContextId);
- данные о запросе (request), включающий в себя заголовки (headers), IP-адрес пользователя (remoteAddress), адрес метода (uri), перечень cookie (cookies) и User Agent пользователя (userAgent).

  Пример тела запроса:

```
{
    "id": "a9692091-4613-41aa-91d2-9a71a3fc2e07",
    "claims": {},
    "rpId": "_blitz_profile",
    "loginContextId": "4502aa51-f28c-4a64-951c-5ab1e77b1294",
    "request": {
      "headers": {},
      "remoteAddress": "172.25.0.1",
      "uri": "/blitz/login/methods2/outside_test",
      "cookies": {},
      "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101
Firefox/80.0"
    }
  }
```

На стороне «поставщика» внешнего метода необходимо предусмотреть обработку данного запроса. В результате внешний метод должен вернуть либо HTTP-ответ для выполнения в браузере пользователя (например, вернуть код HTML-страницы или инициировать редирект браузера на необходимую страницу внешнего метода), либо сообщение об ошибке.

Требования к HTTP-ответу на запрос:

- ответ должен включать в себя установку cookie (на общий домен Blitz Identity Provider и внешнего метода);

- название cookie должно быть предварительно зарегистрировано в Blitz Identity Provider;
- в качестве значения cookie должен быть использован идентификатор сессии, сгенерированный внешним методом.

Пример HTTP-ответа с редиректом и установкой cookie:

```
HTTP/1.1 302 Found
Location: https://method.identityblitz.ru/sps/begin?id=a9692091-4613-41aa-91d2
Set-Cookie: Bmr=YTk2OTIwOTEtNDYxMy00MWFhLTkxZDItOWE3MWEzZmMyZTA3; Domain=mos.ru; path=/sps;
Secure; HttpOnly
```

При прохождении внешнего метода «поставщик» должен проверить, что значение cookie для данного запроса не было изменено.

В случае невозможности провести аутентификацию пользователя, внешний метод должен вернуть ошибку. Пример рекомендуемых к возврату ошибок приведен в таблице ниже.

№	Код ответа HTTP	Значение ответа	Описание ответа
1	200	OK	Инициирование внешнего метода посредством отображения контента страницы
2	302	Found	Инициирование внешнего метода посредством редиректа
3	400	Bad Request	Отсутствуют обязательные параметры запроса
4	500	Internal Server Error	Внутренняя ошибка обработки входящего запроса

2. Функцию обратного вызова Blitz Identity Provider с передачей результатов аутентификации.

После прохождения внешнего метода «поставщик» должен выполнить следующие действия:

a) серверная часть «поставщика» должна вызвать Blitz Identity Provider методом POST по следующему адресу:
{hostname}/blitz/login/methods/outside/save?methodName=outside_{name}, где *name* – имя внешнего метода, присвоенное ему в Blitz Identity Provider.

В случае успеха в теле запроса должны быть указаны:

- идентификатор запроса (id);

- extSessionId – идентификатор сессии, сгенерированный внешним методом. Идентификатор должен совпадать со значением, переданным в исходном запросе в cookie;
- claims – перечень утверждений, которыми нужно обогатить сессию пользователя. Перечень может быть пустым;
- subjectId – идентификатор пользователя (только для первого фактора; при вызове внешнего метода в качестве второго фактора нельзя передавать идентификатор пользователя);
- loginContextId – идентификатор контекста аутентификации, соответствующий исходному запросу.

Пример запроса:

```
POST /blitz/login/methods/outside/save?methodName=outside test HTTP/1.1
Host: auth.identityblitz.ru
Content-Type: application/json

{
    "id": "426b5139-e4f7-41e6-a206-9503de6f34dd",
    "extSessionId": "YTk2OTIwOTEtNDYxMy00MWFhLTkxZDItOWE3MWEzZmMyZTA3",
    "claims": {},
    "loginContextId": "3ca4d1f0-654a-4665-be98-d105ab6ec35d",
    "subjectId": "2db787c7-6e37-4018-abe9-2bea1011c047"
  }
```

В случае ошибки в теле запроса должны быть указаны:

- id – идентификатор запроса;
- extSessionId – идентификатор сессии, сгенерированный внешним методом. Идентификатор должен совпадать со значением, переданным в исходном запросе в cookie;
- error – код ошибки;
- msg – текстовое описание ошибки (опционально).

```
POST /blitz/login/methods/outside/save?methodName=outside_test HTTP/1.1
Host: auth.identityblitz.ru
Content-Type: application/json

{
    "id": "426b5139-e4f7-41e6-a206-9503de6f34dd",
    "extSessionId": "YTk2OTIwOTEtNDYxMy00MWFhLTkxZDItOWE3MWEzZmMyZTA3",
    "error": "not found",
    "msg": "User not found"
  }
```

В случае сохранения результатов аутентификации (как успешной, так и неуспешной) Blitz Identity Provider возвращает ответ *HTTP 200 OK*.

b) браузерная часть «поставщика» должна обеспечить перенаправление пользователя обратно в Blitz Identity Provider. Для этого необходимо перенаправить браузер по адресу: *{hostname}/blitz/login/methods/outside/callback?methodName=outside_{name}*, где *name* – имя внешнего метода, присвоенное ему в Blitz Identity Provider.

3. Сервис определения применимости (опционально).

Представляет собой URL для приема HTTP-запросов от Blitz Identity Provider. До запроса на аутентификацию Blitz Identity Provider будет делать запрос методом POST по данному адресу, передав в теле в формате JSON те же данные, что и в запросе на аутентификацию.

В качестве ответа внешний метод должен вернуть JSON со следующими атрибутами:

- идентификатор запроса (*id*);
- результат проверки применимости (*result*), принимающий значение либо *true* (метод применим) или *false* (метод не применим);
- идентификатор контекста аутентификации (*loginContextId*), соответствующий запросу.

Соответственно, если сервис вернет *false* в качестве результата проверки применимости, то далее Blitz Identity Provider не будет выполнять запрос на аутентификацию для данного пользователя.

Приложение B. API для аутентификации пользователя посредством встроенного в страницу скрипта

Blitz Identity Provider предоставляет API, необходимые для реализации на веб-странице приложения функции идентификации и аутентификации пользователя с запросом логина и пароля непосредственно в веб-приложении, без перенаправления пользователя на отдельную страницу входа. При этом обеспечивается Web Single Sign-On, а именно при последующем входе в той же веб-сессии пользователя в другое подключенное к Blitz Identity Provider приложение, у него не будет повторно запрашиваться вход.

1. Необходимые настройки для использования API

Приложение должно быть зарегистрировано в Blitz Identity Provider. Приложению в Blitz Identity Provider должны быть присвоены client_id и client_secret, и в Blitz Identity Provider должны быть зарегистрированы URL возврата приложения.

Взаимодействие страницы портала и Blitz Identity Provider основано на выполнении серии AJAX-взаимодействий. Для возможности такого взаимодействия на веб-сервере портала и на веб-сервере Blitz Identity Provider должны быть сделаны следующие настройки CORS (Cross-origin resource sharing):

На сервере Blitz Identity Provider для обработчика /blitz/oauth/ae нужно настроить CORS-разрешение, добавив следующие HTTP Headers (нужно указать origin для ПРОД-сайта и необходимые origin для нужных тестовых сред):

```
"Access-Control-Allow-Origin" -> "https://{portaldomain}",
"Access-Control-Allow-Credentials" -> "true"
```

В этом заголовке {portaldomain} – это домен портала.

На сервере портала для callback-обработчика (см. следующую главу) ответа от Blitz Identity Provider нужно настроить следующее CORS-разрешение (разрешение на null, так как после редиректа браузер сбрасывает origin):

```
"Access-Control-Allow-Origin" -> null,
"Access-Control-Allow-Credentials" -> "true"
```

2. Схема интеграции и описание API

Приложение портала должно реализовать:

1. Стандартный способ входа с использованием отдельной страницы входа в соответствии со спецификацией OpenID Connect. Используется в случае: 1) попытки пользователя перейти по прямому URL в закрытый раздел сайта; 2) попытки войти с помощью аккаунта социальной сети. В данном документе этот способ интеграции не описывается.
2. Вход с использованием скрипта на главной странице портала. Схема интеграции приведена на рисунке ниже.

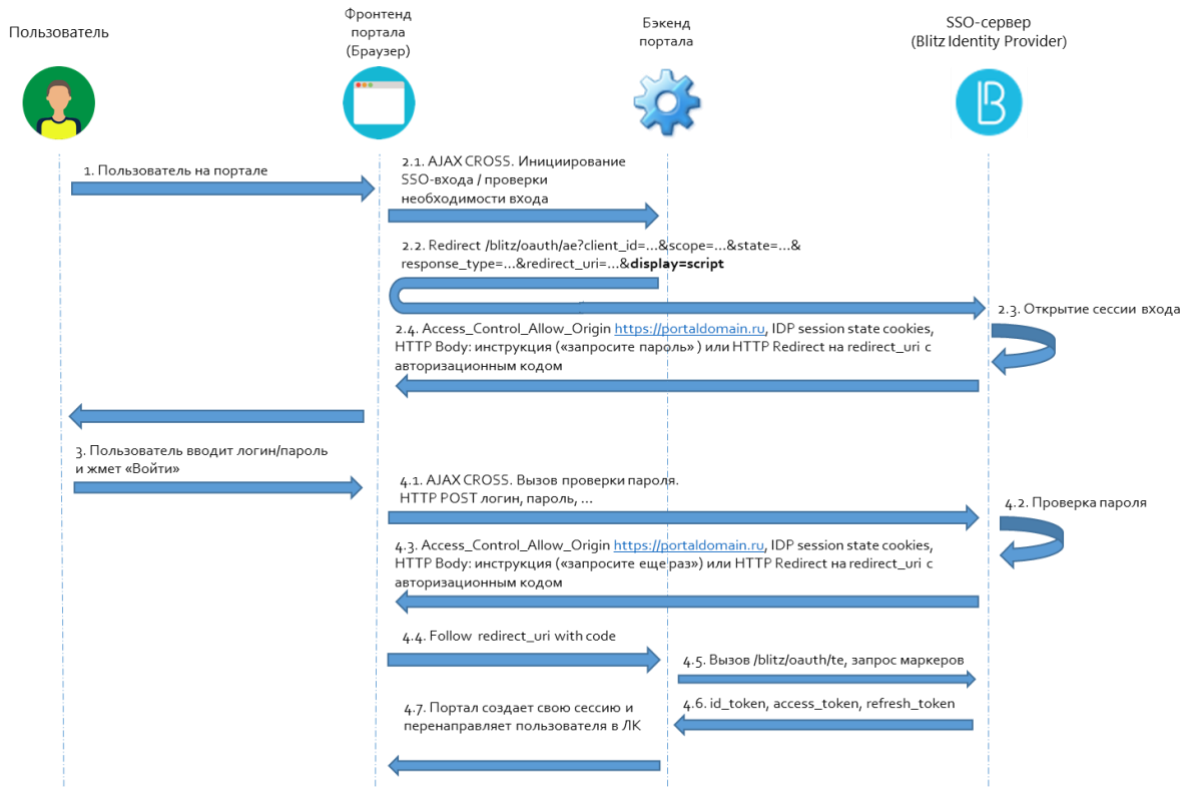

Схема интеграции портала и Blitz Identity Provider

Пояснения к схеме взаимодействия:

1. На шаге 1 пользователь обращается к главной странице портала. В этот момент портал может инициировать шаги 2.1–2.4, чтобы проверить, аутентифицирован ли уже пользователь, и если нет, то отобразить пользователю кнопку «Личный кабинет», по нажатию на которую запросить ввод логина/пароля, или если пользователь уже аутентифицирован, то получить данные о пользователе, вызывая Blitz по предоставляемой им спецификации OpenID Connect 1.0.
2. Вызовы 2.1–2.4 выполняются с использованием серии AJAX-запросов. Причем обращение к Blitz осуществляется на существующий обработчик /blitz/oauth/ae, но с указанием специального параметра display=script.
   2.1. На шаге 2.1 фронтенд портала взаимодействует со своим бэкенд. В результате взаимодействия с сервера сайта формируется AJAX-запрос (шаг 2.2)
   2.2. AJAX-запрос на шаге 2.2 на /blitz/oauth/ae нужно делать обязательно с withCredentials: true, чтобы сохранялись и передавались cookie.

   Пример запроса:

```
https://blitzdomain.portal.ru/blitz/oauth/ae?response_type=code&client_id=portal.ru&scope=openid+profile&redirect_uri=https://apitest.portal.ru/success&state=342a2c0c-d9ef-4cd6-b328-b67d9baf6a7f&display=script
```

   2.3. Blitz Identity Provider при получении запроса с шага 2.2 не отображает свою страницу входа. Вместо этого он проверяет наличие SSO-сессии.
      - Если SSO-сессия есть, то Blitz вызывает HTTP Redirect на переданный

redirect_uri и передает в него код авторизации. Портал дальше может продолжить взаимодействие по OpenID Connect стандартным образом и обменять код авторизации на маркеры и получить данные пользователя.

- Если SSO-сессии нет (либо если сессия есть, но ее недостаточно, чтобы впустить пользователя в приложение), то Blitz Identity Provider открывает сессию входа и переходит к шагу 2.4 схемы.

2.4. На шаге 2.4. Blitz Identity Provider возвращает приложению одну из возможных инструкций.

Пример основного ответа от Blitz Identity Provider с инструкцией, что нужно запросить у пользователя ввод логина/пароля или прохождение аутентификации одним из способов с использованием внешнего поставщика идентификации:

```
{
  "inquire": "choose_one",
  "items": [
     { "inquire": "login_with_password" },
     { "inquire": "request auth with fed point",
                    "fps": ["google:google 1","vk:vk 1","facebook:facebook 1",
                              "esia:esia_1","yandex:yandex_1","ok:ok_1"] }
  ]
}
```

Если в Blitz Identity Provider настроен режим необходимости использования CAPTCHA при входе, то основной ответ от Blitz Identity Provider с инструкцией будет дополнительно содержать параметр captchaId, который необходимо использовать приложению для теста CAPTCHA:

```
{
    "inquire": "choose_one",
    "items": [
        {
            "inquire": "login_with_password",
            "captchaId": "9cf48a75-6be1-4008-b34e-8906220c472f"
        },
        {
            "inquire": "request auth with fed point",
            "fps": [
                "esia:esia_1"
            ]
        }
    ]
}
```

При получении таких ответов приложение переходит к шагу 3 сценария.

Пример другого возможного ответа от Blitz Identity Provider с инструкцией, что нужно перенаправить пользователя на URL для завершения процесса входа в интерфейсе Blitz Identity Provider:

```
{
 "inquire": "redirect_to",
 "to": "https://blitzdomain.portal.ru/blitz/methods/password/change"
}
```

Примеры возможных ситуаций, когда Blitz Identity Provider может вернуть приложению инструкции redirect_to:

- по требованию парольной политики пользователя нужно принудить к смене пароля при очередном входе;

- по требованию настроенной процедуры входа приложения Blitz Identity Provider должен запросить у пользователя проверку 2 фактора аутентификации.

3. На шаге 3 приложение может сразу отобразить пользователю окно входа во фрейме или, например, сделать это отложено, когда пользователь нажмет кнопку «Личный кабинет».

   Пользователь в окне может ввести логин/пароль и нажать кнопку «Войти в личный кабинет». Тогда приложение должно перейти к шагу 4 сценария.

   Также пользователь может решить войти с помощью аккаунта внешнего поставщика идентификации (кнопки входа через внешние поставщики могут быть предусмотрены статично, либо состав кнопок может отображаться в зависимости от инструкции, полученной от Blitz Identity Provider на шаге 2.4.).

   В случае входа через внешний поставщик входа приложение может послать к Blitz Identity Provider в новом окне или в popup-окне стандартный запрос на /blitz/oauth/ae по спецификации OpenID Connect, но указать выбранный способ входа с помощью параметра bip_action_hint. Значение параметра bip_action_hint= used_externalIdps:<fp>, где вместо fp должно быть значение, соответствующее выбранного пользователем поставщика входа.

   Пример запроса:

```
https://blitzdomain.portal.ru/blitz/oauth/ae?response type=code&client id=portal.ru&scope=openid+
profile&redirect_uri=https://apitest.portal.ru/success&state=342a2c0c-d9ef-4cd6-b328-
b67d9baf6a7f& bip_action_hint=used_externalIdps:facebook:facebook_1
```

   Завершение процесса входа в этом случае будет происходить стандартным образом в соответствии с OpenID Connect – Blitz Identity Provider вернет код авторизации на redirect_uri обработчик приложения.

4. Если пользователь ввел логин/пароль и нажал кнопку «Войти в личный кабинет», то приложение выполняет серию AJAX-запросов к Blitz Identity Provider.

   4.1. Если настроено использование CAPTCHA, то до вызова проверки логина/пароля приложение должно осуществить вызовы по получению и проверке CAPTCHA. Запросы на проверку должны формироваться через специализированные proxy-сервисы Blitz, а не напрямую к сервисам CAPTCHA.

   Ниже приведены примеры в случае использования reCAPTCHA v3 (нужно только вызвать проверку):

   Инициализация reCAPTCHA v3 осуществляется в соответствии с документаций https://developers.google.com/recaptcha/docs/v3. При инициализации необходимо использовать reCAPTCHA v3 sitekey такой же как в настройках Blitz Identity Provider.

Пример запроса на проверки CAPTCHA (операция verify):

```
POST /blitz/login/captcha/verify Content-Type: 'text/json'
{
    "ctx": {
         // captchaId
        "id": "c4812c56-439b-4b5d-bcc5-815ea3b548d0",
        "method": "password"
    },
    "params": {
        // token для проверки капчи (полученный от google)
        "response": "03…sA"
    }
}
```

Ответ:

```
200 Ok
{
    "action": "submit",
    "challenge_ts": "2021-03-16T11:18:41Z",
    "success": true,
    "hostname": "testhost.ru",
    "score": 0.9
}
```

4.2. Для проверки логина/пароля приложение посылает AJAX POST запрос с обязательным withCredentials: true. Запрос посылается на URL /blitz/login/methods/headless/password с Content-Type x-www-form-urlencoded и Body, содержащим параметры login и password.

Пример запроса:

```
POST /blitz/login/methods/headless/password HTTP/1.1
Host: blitzdomain.portal.ru
Content-Type: application/x-www-form-urlencoded

login=<логин>&password=<пароль>
```

4.3. Blitz Identity Provider при получении запроса с шага 4.1 проверяет полученные логин/пароль (и тест на CAPTCHA):

- Если логин/пароль правильные и их достаточно для создания сессии, то Blitz Identity Provider создает SSO-сессию, вызывает HTTP Redirect на переданный redirect_uri и передает в него код авторизации. Сайт дальше может продолжить взаимодействие по OpenID Connect стандартным образом и обменять код авторизации на маркеры и получить данные пользователя.
- Если логин/пароль неправильный или возникла другая возможная ошибка, то Blitz Identity Provider возвращает приложению инструкцию с ошибкой (шаг 4.3).
- Если логин/пароль правильные, но нужны дальнейшие действия от пользователя, то Blitz Identity Provider возвращает приложению инструкцию на переход пользователя (шаг 4.3).

4.4. На шаге 4.3 Blitz Identity Provider возвращает приложению одну из возможных инструкций.

Пример ответа от Blitz Identity Provider в случае ошибки проверки логина/пароля с инструкцией по ошибке:

```
{
  "inquire": "login_with_password",
  "errors": [{ "code": "invalid_credentials", "params": {} }]
}
```

При получении такого ответа приложение может отобразить текст ошибки и предложить пользователю ввести еще логин/пароль, после чего можно повторить шаг 3 сценария.

Все возможные коды ошибок:

- invalid_credentials – неправильный логин/пароль, нужно предложить ввести логин/пароль еще раз;
- account_is_locked – аккаунт заблокирован. В целях безопасности можно не отличать эту ошибку от invalid_credentials и обрабатывать точно также;
- password_expired – пароль от аккаунта просрочен, аккаунт заблокирован. В целях безопасности можно не отличать эту ошибку от invalid_credentials и обрабатывать точно также;
- inappropriate_authentication – недопустимый для пользователя метод аутентификации;
- invalid_captcha – произошла ошибка при проверке теста CAPTCHA.

Пример получения ошибки, что не прошла проверка CAPTCHA:

```
{
    "inquire": "login_with_password",
    "captchaId": "9aac130e-c161-463a-a8e4-93f9f7719719",
    "errors": [
        {
            "code": "invalid_captcha",
            "params": {}
        }
    ]
}
```

Пример другого возможного ответа от Blitz с инструкцией, что нужно перенаправить пользователя на URL для завершения процесса входа в интерфейсе Blitz Identity Provider:

```
{
 "inquire": "redirect_to",
 "to": "https://blitzdomain.portal.ru/blitz/methods/password/change"
}
```

Примеры возможных ситуаций, когда Blitz Identity Provider может вернуть приложению инструкции redirect_to:

- По требованию парольной политики пользователя нужно принудить к смене пароля при очередном входе.
- По требованию настроенной процедуры входа приложения Blitz Identity Provider должен запросить у пользователя проверку 2 фактора аутентификации.

4.5. Если аутентификация на шаге 4.2 успешна или если после шага 2.3 выяснилось, что аутентификация вовсе не требовалась, то Blitz перенаправляет во фрейме пользователя на обработчик redirect_uri приложения. Выполняется стандартное завершение процесса входа – шаги 4.5 – 4.7.

4.6. Приложение вызывает Blitz Identity Provider, обменивает код авторизации на маркеры. Вызов сервиса /blitz/oauth/te производится стандартным образом по спецификации OpenID Connect.

4.7. Приложение получает от Blitz Identity Provider и интерпретирует полученные маркер обновления, маркер доступа, маркер идентификации.

4.8. Приложение создает на frontend нужные ему cookie приложения и перенаправляет пользователя внутрь личного кабинета.

3. Пример скрипта, позволяющего провести идентификацию и аутентификацию пользователя

Ниже приведен пример простейшего скрипта, который инициирует аутентификацию пользователя (запрос на /ae) и при ответе с HTTP-кодом 200 отправляет логин и пароль пользователя на проверку:

```
let xhrGet = new XMLHttpRequest();
xhrGet.withCredentials = true;
xhrGet.open("GET",
"https://hostname/blitz/oauth/ae?scope=openid+profile&client_id=test_app&response_type=code&redir
ect_uri=https://portal.hostname/app&display=script", true);
xhrGet.send();
xhrGet.onload = function() {
  if (xhrGet.status != 200) {
    console.log(`Ошибка ${xhrGet.status}: ${xhrGet.statusText}`);
  } else {
    console.log(xhrGet.responseText);
    let xhr = new XMLHttpRequest();
    xhr.withCredentials = true;
    xhr.open("POST", "https://hostname/blitz/login/methods/headless/password", true);
    xhr.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
    xhr.send("login=user123&password=12345678");
    xhr.onload = function() {
    if (xhr.status != 200) {
      console.log(`Ошибка ${xhr.status}: ${xhr.statusText}`);
    } else {
      console.log(xhr.responseText);
    }
  }
}
```

4. Особенности

На стороне приложения нужно предусмотреть следующие особенности:

1. Вызов входа из мобильных приложений. Так как экран мобильных приложений мал, чтобы отображать фреймы с окнами входа, то рекомендуется, чтобы приложение проверяло UserAgent, и если обнаружено, что пользователь обратился из мобильного приложения, то не использовать сценарий аутентификации через скрипт, а запрашивать вход в Blitz Identity Provider стандартным образом с открытием отдельной страницы входа и использованием сценария OpenID Connect.

2. Браузер Safari для macOS имеет встроенный механизм Intelligent Tracking Prevention, который запрещает работу схемы аутентификации в случае, если домен приложения (origin) отличается от домена Blitz Identity Provider. При вызове описанного в документе сценария Safari заблокирует установку cookie из Blitz Identity Provider, если браузер имеет стандартные настройки. Поведение браузера можно изменить, если пользователь войдет в настройки Safari (Настройки - Конфиденциальность - Отслеживание на веб-сайтах) и уберет чекбокс «Мешать перекрестному отслеживанию».

Приложение Г. Вызов вспомогательного приложения в момент входа

В момент входа Blitz Identity Provider имеет возможность вызвать вспомогательное приложение. Это приложение может выполнить дополнительные операции (например, показать пользователю информационное сообщение или запросить актуализацию сведений), после чего вернуть пользователя в Blitz Identity Provider для последующего входа в целевое приложение.

Вспомогательное приложение должно выполнять следующие действия:

1. Прием запроса об открытии вспомогательного приложения

Переход во вспомогательное приложение происходит посредством перенаправления пользователя на предоставленную вспомогательным приложением ссылке. Ссылка в качестве параметра будет содержать код авторизации (code). Пример ссылки для инициирования запроса:

```
https://<app_hostname>/?lang=ru&theme=default&code=0Tj…qw
```

При необходимости получить данные пользователя приложение должно обменять код авторизации на токен согласно спецификации OAuth 2.0. Вспомогательное приложение должно быть предварительно зарегистрировано в Blitz Identity Provider с учетом следующих особенностей:

- должен быть указан предопределенный URL возврата, именно он далее должен быть использован для получения токена;
- должны быть настроены разрешения по умолчания (scope), именно они определяют объем данных, получаемых вспомогательным приложением.

Пример запроса:

```
curl -k -d
"grant_type=authorization_code&redirect_uri=https%3A%2F%2Fapp.company.com%2F&client_id=app&client
_secret=EW…l0&code=0Tj…qw" -X POST https://login.company.com/blitz/oauth/te
```

В ответ будет возвращен маркер доступа, который должен быть использован для получения идентификатора сессии, а также при необходимости данных пользователя.

Пример полученного маркера доступа:

```
{
  "access token": "ey…J9.ey…n0.Wa…Pw",
  "token type": "Bearer",
  "expires_in": 3600,
  "scope": "profile"
}
```

2. Возврат пользователя в Blitz Identity Provider

Выполнив необходимые действия (например, показав пользователю информационное сообщение), вспомогательное приложение должно вернуть пользователя в Blitz Identity Provider. Для этого необходимо декодировать полученный маркер доступа,

полученный в формате JWT, и извлечь из него утверждение с сессией пользователя (sessionId).

Пример тела декодированного access_token:

```
{
  "scope": "blitz_api_user blitz_api_user_chg blitz_api_usec_chg",
  "jti": "kfP…jA",
  "client id": "app",
  "exp": 1631026605,
  "sessionId": "ce9f3109-ac79-46b4-b277-099ff1aa1ff0",
  "iat": 1631023005,
  "sub": "8b970179-e141-43b9-b9d5-25997be99261",
  "aud": [
    "app"
  ],
  "crid": "u9th2LzMXZdwb3rRmI3Paw",
  "iss": "https://login.company.com"
}
```

После этого вспомогательное приложение должно сделать POST-запрос на URL обработчика завершения аутентификации Blitz Identity Provider, имеющий вид /login/pipe/save/<sessionId>. В теле запроса может быть указан набор утверждений (claims), которые следует добавить в сессию пользователя, либо информацию об ошибке (error).

Пример запроса:

```
curl -v --location --request POST 'https://login.company.com/blitz/login/pipe/save/ce9f3109-ac79-
46b4-b277-099ff1aa1ff0' \
--header 'Content-Type: application/json' \
--header 'Authorization: Basic Z2…ww' \
--data-raw '{"claims":{"org_id":"12345678"}}'
```

В случае успеха Blitz Identity Provider вернет HTTP-код 204. Получив его, вспомогательное приложение должно вернуть браузер пользователя по адресу /login/pipe/callback, чтобы пользователь завершил вход в целевое приложение. Пример ссылки для перенаправления:

```
https://login.company.com/blitz/login/pipe/callback
```