



СРАВНЕНИЕ СИСТЕМ АУТЕНТИФИКАЦИИ

Blitz Identity Provider VS Keycloak

 identityblitz.ru

ОПИСАНИЕ ПРОДУКТОВ

В данном документе сравниваются системы многофакторной аутентификации:

- **Blitz Identity Provider** – российское программное обеспечение, объединяет функционал IAM, CIAM, SSO, MFA решений. Продукт разворачивается на серверах компании и позволяет оснастить внутреннюю ИТ-инфраструктуру функциями защиты учетных записей пользователей. Поддерживает современные стандарты (OIDC, OAuth 2, SAML, WS-Fed, RADIUS, LDAP, REST API, JWT, WebAuthn), популярные отечественные операционные системы и СУБД.
- **Keycloak** – популярное open source решение для управления аутентификацией пользователей, разработанное сообществом JBoss и поддерживаемое американской компанией Red Hat. Keycloak предоставляет компании платформу для управления аутентификацией, покрывая большинство стандартных потребностей «из коробки». Однако для реализации нестандартных задач и дополнительных интеграций необходима разработка модулей расширения. При выборе Keycloak в качестве решения IAM заказчику, как правило, необходимо сформировать команду разработчиков, обладающих знаниями в предметной области и опытом работы с платформой. Эти специалисты будут заниматься разработкой и внедрением функций, расширяющих базовые возможности Keycloak, а также сопровождением созданных модулей, чтобы обеспечить совместимость с обновлениями платформы. Keycloak ориентирован на международные рынки, многие его функции и интеграции не адаптированы к специфике российских требований. Например, интеграция с ЕСИА, банками, отечественными провайдерами идентификации, поддержка УКЭП и взаимодействие с популярными компонентами российской инфраструктуры и системами обеспечения информационной безопасности, потребует дополнительные интеграционные работы.

1. ФУНКЦИОНАЛЬНОСТЬ

Критерий	Blitz Identity Provider	Keycloak
1.1. Аутентификация		
Поддерживаемые способы входа пользователей	• логин и пароль, • банки, госуслуги (ЕСИА, цифровой профиль, Mos ID), • российские и зарубежные интернет-сервисы, • биометрическая аутентификация на устройстве (Face ID, Touch ID, Windows Hello), • WebAuthn (FIDO2 и Passkey), • Kerberos, • X509-сертификат из HTTPS-соединения, • федеративный вход (OIDC IDP, SAML IDP), • смарт-карты и USB-ключи УКЭП (ruToken, JaCarta и др.), • QR-код, • мобильное приложение Blitz Key (push) или приложение Заказчика, • логин и код из SMS, • логин и код из email • ПИН-код для упрощенного повторного входа	• логин и пароль, • зарубежные интернет-сервисы, • WebAuthn (FIDO2 и Passkey), • Kerberos, • X509-сертификат из HTTPS-соединения, • федеративный вход (OIDC IDP, SAML IDP)
Поддерживаемые способы подтверждения входа пользователей (2FA, MFA)	• TOTP, HOTP, • WebAuthn (FIDO2, Passkey и U2F), • мобильное приложение Blitz Key (push) или приложение Заказчика, • код из SMS, • код из MAX • код из email, • код из push, • код из Flash Call, • смарт-карты и USB-ключи УКЭП (ruToken, JaCarta и др.), • ответ на контрольный вопрос, • иные MFA (Aladdin JAS, MFA Soft, Indeed AM, Duo Mobile и др.)	• TOTP, HOTP, • WebAuthn (FIDO2, Passkey и U2F)
Возможность самостоятельно добавить поддержку дополнительных методов аутентификации (через разработку расширений)	✓	✓



Критерий	Blitz Identity Provider	Keycloak
1.1. Аутентификация		
Назначение пользователю аппаратного HOTP/TOTP-генератора	✓ По серийному номеру. Поддержка популярных форматов файлов с описаниями устройств	✗
Интеграция с каталогами	✓ Поддержка множества LDAP-каталогов (совместимость с 389 DS, OpenDJ, OpenLDAP, ALD PRO, РЕД АДМ, Samba, MS Active Directory, FreeIPA, IBM Tivoli Directory Server). Предварительная миграция учетных записей из LDAP в Blitz не требуется	✓ Поддержка LDAP-каталогов и MS Active Directory. Требуется периодическая синхронизация УЗ в Keycloak с УЗ в подключенных каталогах
Интеграция с иными (не LDAP) хранилищами учетных записей	✓ Через разработку REST-коннектора	✓ Через разработку SPI-провайдера (Java)
Связывание учетных записей при входе	✓ Гибкая настройка связывания, сценариев подтверждения при связывании	✓ Только базовая настройка. Для кастомной настройки требуется разработка
Возможность дополнительной аутентификации при подтверждении связывания учетных записей	✓	✓
Поддержка MFA при входе в не-веб приложения (VPN, VDI, RDP, SSH)	✓	✗
Поддержка MFA при входе в ОС (Windows, Linux)	✓	✗
Электронная подпись	✓ Смарт-карты и USB-ключи: Rutoken, JaCarta, ISBC ESMART, КриптоПро CSP и др.	✓ Через разработку SPI-провайдера (Java)



Критерий	Blitz Identity Provider	Keycloak
1.1. Аутентификация		
Встроенная защита от атак перебора паролей	✓ Ограничение кол-ва попыток входа (временное блокирование метода входа). Тест CAPTCHA. Замедление проверки пароля (использование проверки Proof of Work)	✓
Встроенная защита от атак перебора кодов подтверждения	✓ Ограничение кол-ва попыток входа (временное блокирование метода вход)	? Нет данных
Встроенная поддержка парольных политик	✓ • проверка сложности пароля • проверка на вхождение в словарь • запрет ранее использованных паролей • ограничение срока действия пароля	✓ • проверка сложности пароля • проверка на вхождение в словарь • запрет ранее использованных паролей • ограничение срока действия пароля
TOTP-генератор / HOTP-генератор	✓	✓
Технологии единого входа с использованием браузера	OIDC, SAML, Reverse Proxy, Kerberos	OIDC, SAML, Kerberos
API аутентификации без использования браузера	✓ HTTP API, RADIUS, LDAP-адаптер	? Нет данных
Технологии аутентификации для мобильных приложений	✓ RFC 8252. Дополнительно возможность аутентификации без использования браузера	✓ RFC 8252



Критерий	Blitz Identity Provider	Keycloak
1.1. Аутентификация		
Настройка сценариев процесса входа	✓	✓
Поддержка множественных аккаунтов для входа	✓	✓ Ограничено (Beta-тестирование)
Поддержка имперсонафикации аккаунта (замена пользователя при входе)	✓	✓ Ограничено (только для администратора)
1.2. Мобильное приложение		
Наличие собственного мобильного приложения	✓	✗
Доступность мобильного приложения	iOS, Android	✗
Функция TOTP-генератора	✓	✗
Функция входа по QR-коду	✓	✗
Подтверждение входа (push) через собственное приложение	✓	✗
Подтверждение входа (push) через стороннее приложение	✓ API, поддержка популярных приложений	✓ Через разработку SPI-провайдера (Java)
1.3. Авторизация		
Уровни авторизации	✓ При входе в приложение, При вызове защищаемых API	✓ При входе в приложение
Модели контроля доступа	RBAC, GBAC, ABAC	RBAC, GBAC, ABAC



Критерий	Blitz Identity Provider	Keycloak
1.4. Регистрация		
Способы регистрации	✓ • регистрация администратором через UI • самостоятельная регистрация пользователем • REST API	✓ • регистрация администратором через UI • самостоятельная регистрация пользователем • REST API
Проверки при регистрации	✓ • проверка email • проверка номера телефона • проверка регистрируемых УЗ во внешних системах • обогащение регистрируемых УЗ данными из внешних систем	✓ • проверка email
1.5. Личный кабинет		
Просмотр и редактирование УЗ пользователем	✓	✓
Изменение пароля	✓	✓
Изменение секретного вопроса	✓	✗
Настройка TOTP	✓	✓
Настройка Passkey	✓	✓
Управление привязками УЗ внешних поставщиков идентификации	✓	✓
Проверка использованных для входа устройств	✓	✓
Просмотр событий безопасности	✓	✗



Критерий	Blitz Identity Provider	Keycloak
1.6. Восстановление пароля		
Способы подтверждения при восстановлении пароля	✓ Email, TOTP, SMS, контрольный вопрос	✓ Email, TOTP
1.7. Каталог приложений		
Просмотр доступных для входа приложений	✓ Карточки приложений с лого, названием, описанием. Фильтр по доступности для текущего пользователя	✓ Список с названием и типом приложения
Возможность создания списка избранных приложений	✓	✗
Возможность поиска приложения	✓	✗
1.8. Администрирование		
Веб-интерфейс администратора	✓ Полнофункциональный веб-интерфейс	✓ Полнофункциональный веб-интерфейс
API администрирования	✓	✓

2. АРХИТЕКТУРА, ПРОИЗВОДИТЕЛЬНОСТЬ

Критерий	Blitz Identity Provider	Keycloak
2.1. Архитектура		
Архитектура	Микросервисы	Монолит
Хранение пользователей	СУБД, LDAP, внешняя система (через коннектор)	СУБД, LDAP, внешняя система (через коннектор)
Хранение событий безопасности	Кастомизируемое: СУБД, Kafka, файлы и syslog	СУБД
Операционные системы	Rocky Linux, AlmaLinux, Oracle Linux, RHEL, CentOS	Linux
Российские операционные системы	AstraLinux, ОС Альт, ОСнова, РЕД ОС, РОСА Хром, Мос.ОС	—
СУБД	Postgres или любая JDBC, Tarantool, Couchbase	MariaDB, MSSQL, Oracle, Postgres
Кэш памяти	Memcached	Infinispan
2.2. Производительность		
Производительность (бенчмарк)	200 аутентификаций в секунду для 1vCPU в кластере из 2 серверов	45 аутентификаций в секунду для 1 vCPU в кластере из 3 серверов
Максимальная подтвержденная производительность по официальным тестам вендора	2000 аутентификаций в секунду	300 аутентификаций в секунду

3. БЕЗОПАСНОСТЬ

Критерий	Blitz Identity Provider	Keycloak
3.1. Соответствие стандартам		
Международные стандарты безопасности	NIST, OWASP	NIST, OWASP
Сертификация ФСТЭК	Сертификат ФСТЭК №4525 от 10.03.2022. Соответствие 4 уровню доверия	—
3.2. Тип исходного кода		
Исходный код	Закрытый (по запросу доступ предоставляется ИБ-лабораториям для проверок)	Открытый
3.3. Возможности интеграции с SIEM		
Интеграция с SIEM	Доступна. Через Kafka, через файловый обмен или syslog	Требуется доработка

4. КАСТОМИЗАЦИЯ

Критерий	Blitz Identity Provider	Keycloak
4.1. Возможности кастомизации		
Настройка интерфейса	Настройка серверного шаблона (HTML, CSS, JS) или конфигурирование через конструктор интерфейса	Настройка серверного шаблона Freemarker
Настройка бизнес-процессов	Через определение на Java алгоритмов процедур входа, регистрации, кастомизации взаимодействия с хранилищами УЗ	Через разработку модулей расширения
Наличие SDK	Blitz Developer Kit	Официально не поддерживается
Наличие API	Да	Ограничено

5. СТОИМОСТЬ ВЛАДЕНИЯ

Критерий	Blitz Identity Provider	Keycloak
5.1. Лицензирование		
Модель предоставления услуг	On-premise	On-premise
Лицензия	Платная	Бесплатная
Лицензия по сервисной модели	По пользователям, по сроку действия или безлимитная	—
Лицензии на стороннее ПО	—	—
5.2. Поддержка		
Поддержка требований, актуальных для российского рынка	Из коробки	Дополнительная стоимость
Поддержка обратной совместимости	Входит в лицензию и ТП	Дополнительные затраты на техническую поддержку
Техническая поддержка с SLA	Да	Нет

КОНТАКТНАЯ ИНФОРМАЦИЯ

IDENTITY BLITZ – российский разработчик программного обеспечения. На рынке информационной безопасности с 2014 года.

Специализируется в решении задач управления идентификацией, аутентификацией и контролем доступа пользователей к корпоративным информационным ресурсам.

Эксперты компании готовы ответить на вопросы и предложить индивидуальные решения для вашего бизнеса.

По работе с Blitz Identity Provider доступны:

-  подробные руководства и инструкции
-  база знаний по интеграции приложений
-  онлайн-демонстратор
-  docker-образ для загрузки

 +7 (499) 322-14-04

 info@idblitz.ru

 identityblitz.ru





Identity Blitz, 2026

 identityblitz.ru