СРАВНЕНИЕ СИСТЕМ АУТЕНТИФИКАЦИИ

Blitz Identity Provider VS Microsoft AD FS

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 развертывается 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.
- **Microsoft Active Directory Federation Services (AD FS)** – популярное решение для управления аутентификацией пользователей, основанное на платформе Microsoft Windows Server 2016. Данное решение применяется в международной практике для организации единого входа (SSO) и поддерживает такие ключевые протоколы, как OIDC, SAML и WS-Federation. В 2024 году компания Microsoft призвала отказаться от использования AD FS и активно продвигает свое новое облачное решение Microsoft Entra ID (ранее известного как Microsoft Azure AD). Встроенные возможности по MFA в AD FS отсутствуют, но предусмотрена возможность интеграции с Microsoft Entra и со сторонними сервисами MFA. Техническая поддержка российским компаниям не оказывается.

1. ФУНКЦИОНАЛЬНОСТЬ

Критерий	Blitz Identity Provider	Microsoft AD FS
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, • 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.)	Встроенной поддержки нет *Можно подключать сторонние MFA-решения через MFA-адаптеры или разработать свой MFA-адаптер.* *Можно также подключить облачную MFA из Microsoft Entra.*
Возможность самостоятельно добавить поддержку дополнительных методов аутентификации (через разработку расширений)	✅	✅

Критерий	Blitz Identity Provider	Microsoft AD FS
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	✓ Интеграция с MS Active Directory
Интеграция с иными (не LDAP) хранилищами учетных записей	✓ Через разработку REST-коннектора	✓ Подключение по SQL к СУБД
Связывание учетных записей при входе	✓ Гибкая настройка связывания, сценариев подтверждения при связывании	✗
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.	✓ Поддержка клиентских сертификатов X509

Критерий	Blitz Identity Provider	Microsoft AD FS
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)	✗
Встроенная поддержка парольных политик	✓ • проверка сложности пароля • проверка на вхождение в словарь • запрет ранее использованных паролей • ограничение срока действия пароля	✗ *Используются парольные политики из каталога*
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	✗
Технологии аутентификации для мобильных приложений	✓ RFC 8252. Дополнительно возможность аутентификации без использования браузера	✓

Критерий	Blitz Identity Provider	Microsoft AD FS
1.1. Аутентификация		
Настройка сценариев процесса входа	✓	✓
Поддержка множественных аккаунтов для входа	✓	✗
Поддержка имперсонификации аккаунта (замена пользователя при входе)	✓	✗
1.2. Мобильное приложение		
Наличие собственного мобильного приложения	✓	✗
Доступность мобильного приложения	iOS, Android	Microsoft Authenticator доступно только при использовании облачного MS Entra ID
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 адаптера на .NET 4.5
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	Microsoft AD FS
1.4. Регистрация		
Способы регистрации	✓ • 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	✗
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	Microsoft AD FS
1.6. Восстановление пароля		
Способы подтверждения при восстановлении пароля	✓ Email, TOTP, SMS, контрольный вопрос	✗
1.7. Каталог приложений		
Просмотр доступных для входа приложений	✓ Карточки приложений с лого, названием, описанием. Фильтр по доступности для текущего пользователя	✗
Возможность создания списка избранных приложений	✓	✗
Возможность поиска приложения	✓	✗
1.8. Администрирование		
Веб-интерфейс администратора	✓ Полнофункциональный веб-интерфейс	✓ PowerShell
API администрирования	✓	✓ PowerShell

2. АРХИТЕКТУРА, ПРОИЗВОДИТЕЛЬНОСТЬ

Критерий	Blitz Identity Provider	Microsoft AD FS
2.1. Архитектура		
Архитектура	Микросервисы	Монолит
Хранение пользователей	СУБД, LDAP, внешняя система (через коннектор)	MS AD, LDAP, СУБД
Хранение событий безопасности	Кастомизируемое: СУБД, Kafka, файлы и syslog	—
Операционные системы	Rocky Linux, AlmaLinux, Oracle Linux, RHEL, CentOS	Microsoft Windows Server
Российские операционные системы	AstraLinux, ОС Альт, ОСнова, РЕД ОС, РОСА Хром, Мос.ОС	—
СУБД	Postgres или любая JDBC, Tarantool, Couchbase	Microsoft SQL Server
Кэш памяти	Memcached	*Нет данных*
2.2. Производительность		
Производительность (бенчмарк)	200 аутентификаций в секунду для 1vCPU в кластере из 2 серверов	100 аутентификаций в секунду для 8 vCPU сервера
Максимальная подтвержденная производительность по официальным тестам вендора	2000 аутентификаций в секунду	*Нет данных*

3. БЕЗОПАСНОСТЬ

Критерий	Blitz Identity Provider	Microsoft AD FS
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)	Закрытый
3.3. Возможности интеграции с SIEM		
Интеграция с SIEM	Доступна. Через Kafka, через файловый обмен или syslog	Доступна

4. КАСТОМИЗАЦИЯ

Критерий	Blitz Identity Provider	Microsoft AD FS
4.1. Возможности кастомизации		
Настройка интерфейса	Настройка серверного шаблона (HTML, CSS, JS) или конфигурирование через конструктор интерфейса	Настройка предусмотренных областей кастомизации, возможность разместить свой JS
Настройка бизнес-процессов	Через определение на Java алгоритмов процедур входа, регистрации, кастомизации взаимодействия с хранилищами УЗ	Через PowerShell-скрипты
Наличие SDK	Blitz Developer Kit	*Официально не поддерживается*
Наличие API	Да	PowerShell

5. СТОИМОСТЬ ВЛАДЕНИЯ

Критерий	Blitz Identity Provider	Microsoft AD FS
5.1. Лицензирование		
Модель предоставления услуг	On-premise	On-premise
Лицензия	Платная	Платная
Лицензия по сервисной модели	По пользователям, по сроку действия или безлимитная	По пользователям
Лицензии на стороннее ПО	—	Windows Server
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 для российских компаний

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-демостенд
- docker-образ для загрузки

+7 (499) 322-14-04

info@idblitz.ru

identityblitz.ru

identityblitz.ru