MULTIFACTOR

Просто. Надёжно. Безопасно.

Многофакторная аутентификация (MFA)
Единый вход (SSO)

1. Боли рынка

Проблемы удалённого доступа

Обзор

- **до 18%** Казахстанцев работают удаленно[1]
- **7 место** в мире занял Казахстан по кол-ву кибератак в 2023 г.[2]
- **на 120%** выросло кол-во фишинговых атак в корпоративном секторе[3]
- **X 3,5** рост кол-ва утечек информации в мире в 2022 г.[4]
- **>223 млн** кибератак зарубежных хакеров зафиксировано в РК в 2023 г. [6]

В результате компании сталкиваются с:

- прямым и косвенным финансовым ущербом;
- ущербом репутации и потерей клиентов;
- кражей интеллектуальной собственности и коммерческой тайны;
- Санкциями регуляторов за несоблюдение нормативных требований.

$1 млн.

Средний ущерб от кибер-атак для средних и крупных компаний в РК[5]

[1] Национальный доклад «Рынок труда Казахстана: на пути к цифровой реальности», 2022 г.
[2] Исследование Kaspersky Lab, 2023 г.
[3] в 1 квартале 2023 г. в сравнении с 1 кварталом 2022 г. Исследование Kaspersky Lab, 2023 г.
[4] Аналитический отчет Infowatch, 2022 г.
[5] Исследование Kaspersky Lab, 2022 г.
[6] Кибердайджест государственной технической службы Казахстана, 2023 г.

Проблемы

1 Небезопасность удалённых подключений

- Вирусы, социальная инженерия, фишинг и другие векторы атаки указывают на то, что **пароли недостаточны для адекватной защиты**;
- Подключения к ресурсам организации со скомпрометированных аккаунтов;
- Не отозванные доступы при увольнении сотрудника.

Реализация киберриска – вопрос времени, если превентивно не принять мер защиты подключений к корпоративным ресурсам.

2 Неэффективные процессы управления доступом

Высокая нагрузка на команду IT-поддержи в связи с онбордингом и офбордингом пользователей, организацией удалённого доступа, обслуживанием учётных записей, смене забытых паролей и паролей с истёкшим сроком действия.

Результат простоя бизнес-процессов из-за нерешённых проблем с доступом – высокие финансовые и временные издержки.

2. Решение

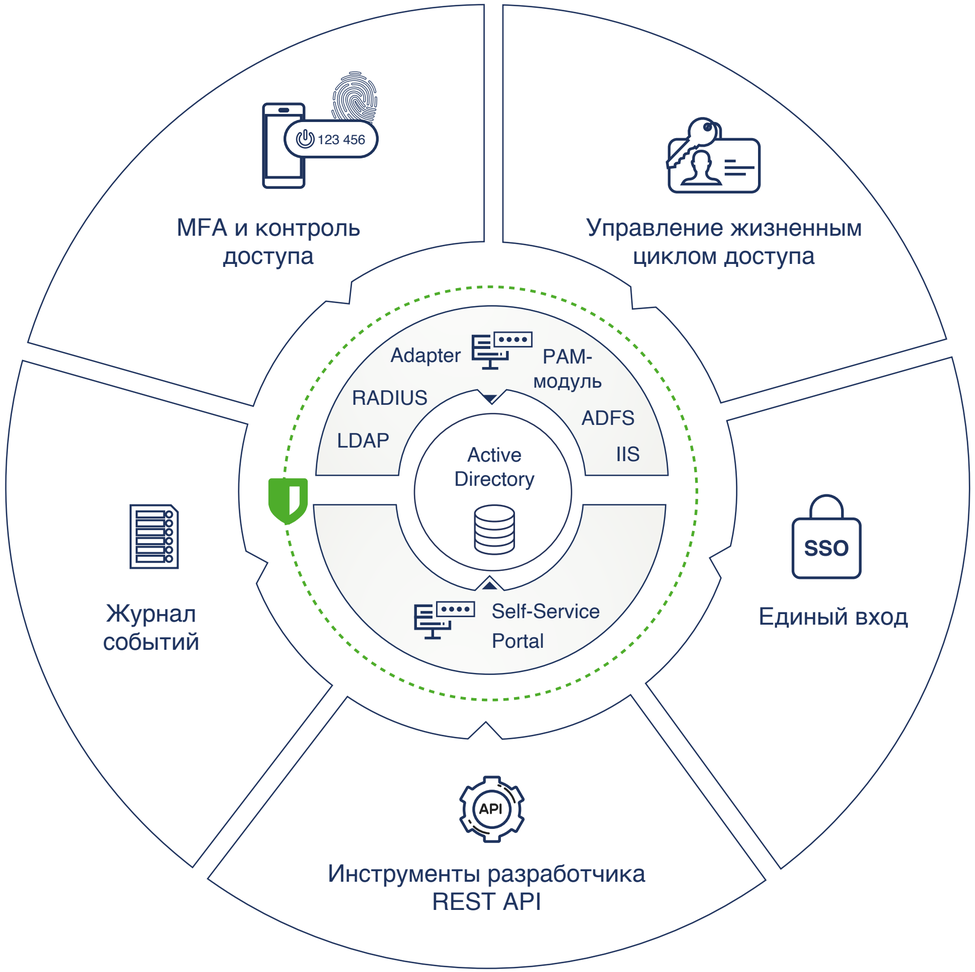
Продукт Мультифактор

Мультифактор с одного взгляда

Сотрудники

Партнёры

Клиенты



1. **VPN**
   Cisco ASA, Check Point, Fortigate, OpenVPN, Huawei, MiktoTik, Windows VPN и др.
2. **VDI**
   VMware, Citrix, Remote Desktop и др.
3. **Облачные приложения, виртуализация, web**
   SAML, OIDC / Oauth, Outlook Web Access (OWA) , Huawei Cloud и др.
4. **Linux-инфраструктура**
   SSH, SUDO, OpenVPN, PAM и др.
5. **Windows-инфраструктура**
   Windows Logon, VPN, RD Gateway, NPS и др.

✓ Защита входа

✓ Простая интеграция

✓ Покрытие всей инфраструктуры

SIEM

Решение Мультифактор

CAPEX
0 ₸

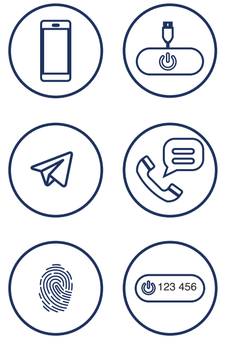
Не требует затрат на внедрение и инфраструктуру.

от
2 часов

Интеграция и ввод в эксплуатацию.
Быстрый онбординг.

до
99%

Снижение рисков неавторизованного доступа **без создания новых.**



MFA и контроль доступа

- Безопасность доступа к инфраструктуре;
- Предотвращение угонов учетных записей, утечек данных и сетевых атак;
- Защита VPN и VDI-подключений;
- Защита облачных SAML-приложений;
- Защита Windows и Linux инфраструктуры.

Портал самообслуживания

- Самостоятельный онбординг пользователей;
- Самостоятельная конфигурация 2FA;
- Решение проблем с доступом без участия IT-поддержки (включая смену просроченного пароля).

Единый вход и Управление доступом

- Исключает мультипликацию учётных записей в облачных системах;
- Единый поставщик учётных записей для доступа к вашим приложениям;
- Упрощает приём на работу и увольнение сотрудников для IT.

✓ **Безопасность**
Дополнительный уровень защиты поверх ваших основных методов аутентификации.

✓ **Снижение затрат на поддержку**
Упрощение разрешения проблем с доступом.

✓ **Непрерывность процессов**
Интуитивный UX, повышение продуктивности сотрудников.

Почему Multifactor?

Высокая доступность
Аптайм 99.98% времени.
Решение, проверенное реальными интеграциями с клиентами.

Отказоустойчивость
Отказ облака Мультифактор не скажется на работе вашего бизнеса. В худшем случае инфраструктура возвращается на предыдущий уровень доступа, без использования второго фактора.

Производительность
Облако Multifactor– 1800 tps
RADIUS Adapter – 120 tps[1]

Безопасность инфраструктуры
Облако Multifactor располагается в датацентрах PS Cloud Services в Алматы с многоуровневой физической защитой, резервными интернет-каналами и источниками питания.

Масштабируемость
Без ограничений по количеству пользователей и ресурсов.

Нулевой CAPEX
SaaS решение для любого бизнеса.

Простая адаптация пользователей
Интуитивный и простой процесс подключения пользователей к многофакторной аутентификации. Возможность автоматического подключения.

Упрощение работы пользователей
Мультифактор позволяет упростить парольные политики. Комбинируется с возможностями SSO.

Настройка любых процессов
Возможность добавить любую необходимую бизнес-логику.

Режим ByPass
Позволяет группам или отдельным пользователям входить без второго фактора.

SLA

- Аптайм **99.98%**
- Техподдержка **7×24×1H**

[1] Горизонтальное масштабирование при необходимости

3. Обзор технологии

Многофакторная аутентификация (MFA)

Мультифакторная аутентификация

Пользователи могут подтвердить свою личность тем, что они знают (основной метод аутентификации, как правило, логин и пароль); тем, что у них есть (например, аппаратный или программный токен); тем, кем они являются (биометрия). Последние два – возможные способы проверки второго фактора.

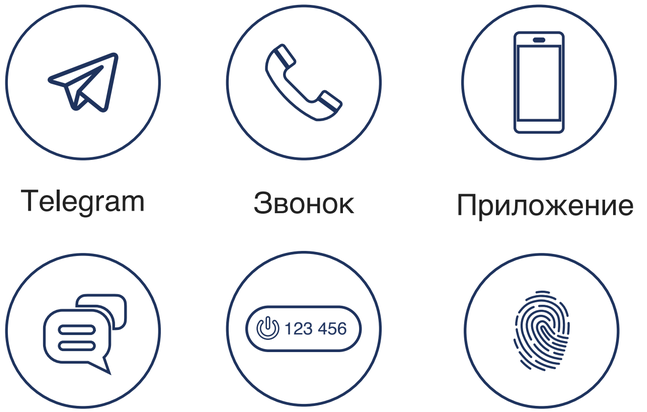
1 Первый фактор

Что пользователь знает:

Логин и пароль

2 Второй фактор

Что пользователь имеет или кем является:



3 Доступ

Доступ разрешён.

[1]FIDO, U2F токены и биометрия недоступны в конфигурации с межсетевыми экранами NAS (Checkpoint, Cisco, Mikrotik и др.) и VDI.

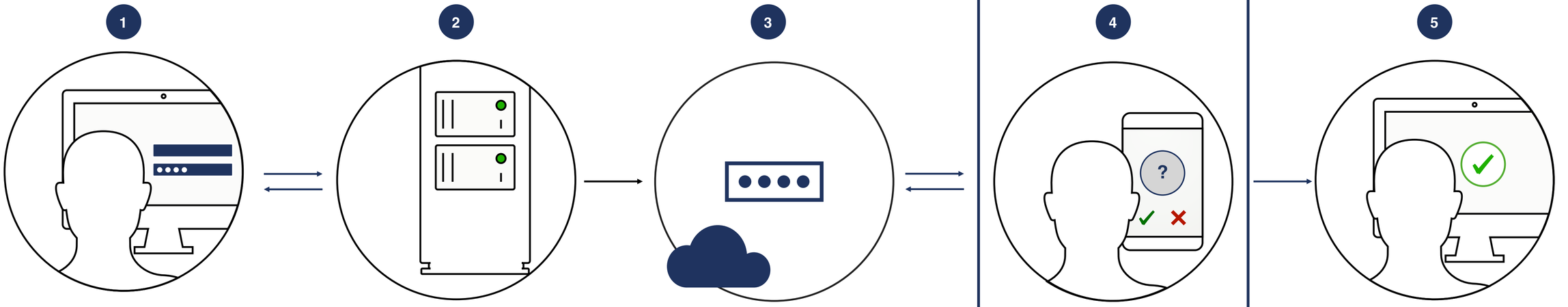
Поддерживаемые методы аутентификации

В таблице ниже представлены 6 основных методов проверки второго фактора, поддерживаемых Мультифактором в зависимости от сценария использования.

	VPN и VDI	Linux инфраструктура	Windows инфраструктура	Облачные приложения (SAML)	API (Web)
 Мобильное приложение Multifactor	✓	✓	✓	✓	✓
 Telegram-бот Multifactor	✓	✓	✓	✓	✓
 SMS или звонок	✓	✓	✓	✓	✓
 OTP токены (Аппаратные и программные)	✓	✓	✓	✓	✓
 U2F / FIDO токены				✓	✓
 Биометрия				✓	✓

Мультифактор не получает доступ к вашим учётным данным

Система работает поверх основного метода аутентификации, никогда не обрабатывает и не хранит пароли ваших пользователей.



Устройство пользователя

Внутренний периметр сети

Подтверждение доступа

Устройство пользователя

Проверка первого фактора

Пользователь самостоятельно вводит свой логин и пароль. Мультифактор не получает доступа к ним.

Данные проверяются в вашей сети

Вы аутентифицируете пользователя с помощью Active Directory и отправляете запрос на 2FA аутентификацию в облако Мультифактор.

Запрос отправлен в Мультифактор

Запрос на аутентификацию вторым фактором отправлен в облако Мультифактора, где реализована вся обработка.

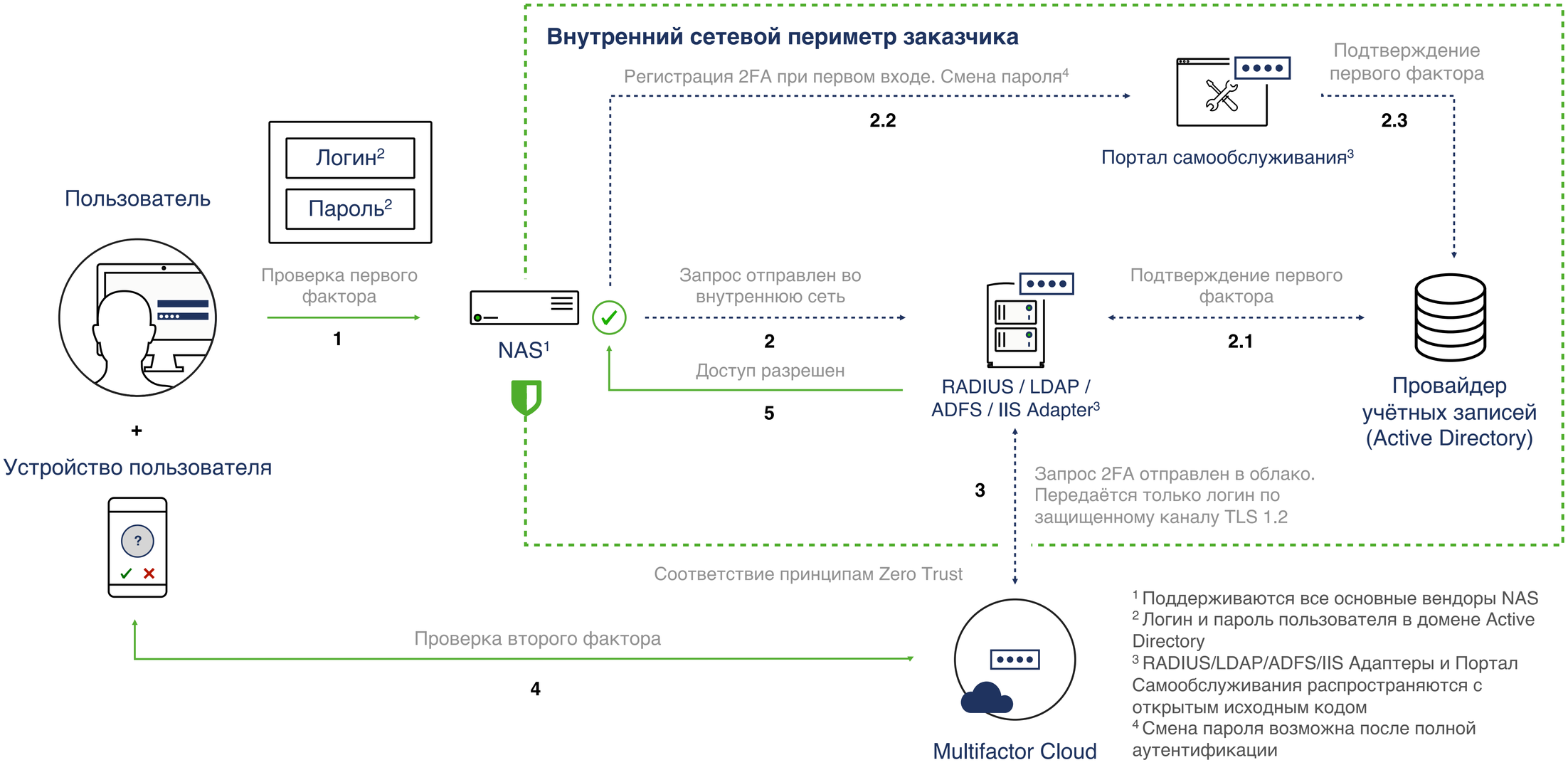
Проверка второго фактора

- Мобильное приложение Multifactor
- Telegram
- SMS или звонок
- OTP-токены

Доступ разрешен

Пользователь залогинен в систему.

Высокоуровневая схема решения



Состав решения

1 Компоненты On-Premise

1. Портал самообслуживания

Расширение для Active Directory

- Самостоятельная регистрация сотрудником второго фактора аутентификации в Multifactor Cloud;
- Смена пароля в корпоративном домене Active Directory с обязательной проверкой текущего пароля и подтверждением вторым фактором в Multifactor Cloud;
- Компонент поставляется с открытым исходным кодом для Windows и Linux.

Мин. системные требования:
1 ядро CPU, 2Gb RAM, Windows Server 2012 и выше

2. RADIUS, LDAP, ADFS, IIS Адаптер

Адаптер для Active Directory

- Приём запросов на аутентификацию сотрудника в CheckPoint VPN, RDP и Citrix по протоколу RADIUS;
- Проверка первого фактора аутентификации (логин и пароль) в домене AD или NPS;
- Проверка второго фактора аутентификации в Multifactor Cloud;
- Компоненты поставляются с открытым исходным кодом для Windows и Linux.

Мин. системные требования:
4 ядра CPU, 4Gb RAM, Windows Server 2012 и выше

2 Облако Multifactor

multifactor.kz

Безопасное размещение в нескольких ДЦ

- Подтверждение и подпись запросов на аутентификацию пользователей вторым фактором;
- Личный кабинет IT-службы вашей организации для управления и контроля доступа сотрудников к ресурсам с 2FA;
- Журнал событий;
- API и инструменты разработчика.

SLA

- Аптайм **99.98%**
- Техподдержка **7×24×1H**

4. Обзор технологии

Единый вход (SSO)

SSO Мультифактор – упрощение контроля доступа к корпоративным приложениям и второй фактор

Уменьшение затрат
Единый провайдер учётных записей позволяет с простотой управлять всеми пользователями организации, выдавая доступы в зависимости от должности.

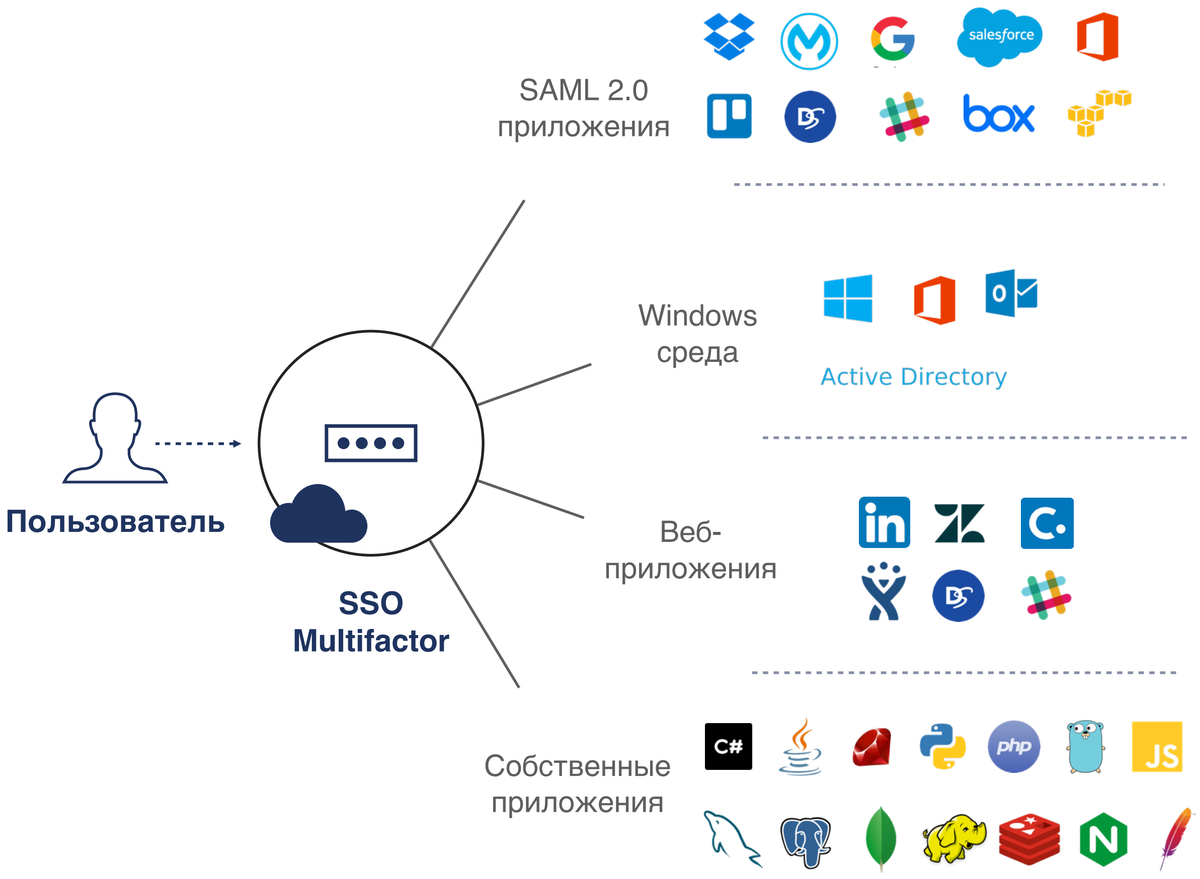
Улучшенный пользовательский опыт
Отпадает необходимость запоминать множество паролей и учётных записей. Возможность изменения паролей во всех сервисах в пару кликов.

Лучшее соответствие требованиям безопасности
Внедрение второго фактора во все системы, вне зависимости от их возможностей.

Настраиваемые парольные политики
Парольные политики зависят от провайдера учётных записей, а не от сторонней системы.

Увеличенная продуктивность
Упрощённый контроль за доступами пользователей. Простое управление перемещением человеческих ресурсов организации.

Упрощённая связность
Интеграция нового приложения в инфраструктуру компании занимает меньше времени.



5. Регистрация 2FA пользователями

Подключение второго фактора доступа пользователями системы

3 режима настройки 2FA

1 Автоматическая регистрация

Пользовательский опыт | Простота интеграции | Скорость подключения пользователей

Автоматическая регистрация SMS в качестве второго фактора доступа (синхронизация телефонных номеров с ActiveDirectory).

2 Регистрация в режиме самообслуживания

✓ 1) Диалог с пользователем (подробнее)

Пользовательский опыт | Простота интеграции | Скорость подключения пользователей

Технология позволяет настроить второй фактор в режиме диалога с пользователем непосредственно в VPN/VDI клиенте или в API/SAML-интерфейсе Multifactor при первом подключении.

✓ 2) Портал самообслуживания (подробнее)

Пользовательский опыт | Простота интеграции | Скорость подключения пользователей

Портал позволяет настроить второй фактор в режиме самообслуживания. В этом сценарии необходимо подготовить и разослать пользователям инструкцию.

3 Регистрация вручную

Пользовательский опыт | Простота интеграции | Скорость подключения пользователей

Администраторы вручную добавляют или импортируют пользователей и рассылают регистрационные ссылки на email.

Пример 1: Регистрация 2FA в режиме диалога с пользователем

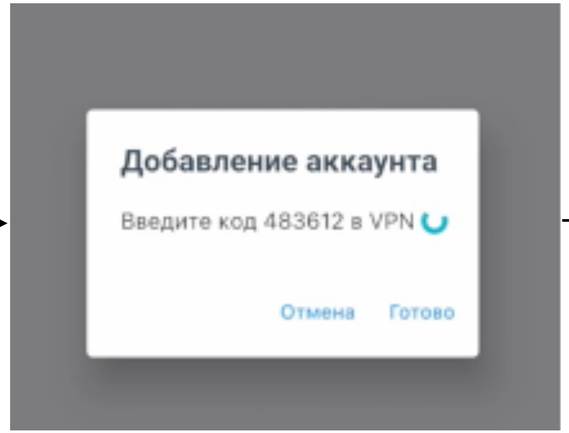
1 Выбор фактора

Пользователь выбирает удобный ему способ двухфакторной аутентификации из преднастроенного списка[1] , вводя соответствующую цифру.

2 Привязка фактора

Клиент сообщает пользователю код, который ему необходимо ввести в приложении или Telegram-боте Multifactor.

3 Подтверждение владения



Пользователь подтверждает владение фактором, вводя код из Telegram, мобильного приложения Multifactor или SMS обратно в клиент.

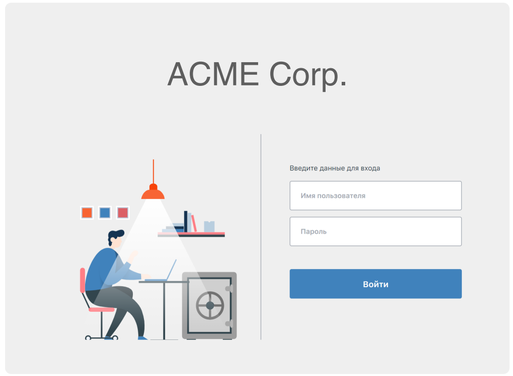
4 Готово!

Регистрация второго фактора завершена. Вход дополнительно защищён вторым фактором.

[1] Telegram, SMS, Приложение Мультифактор в случае защиты VPN и VDI соединений.

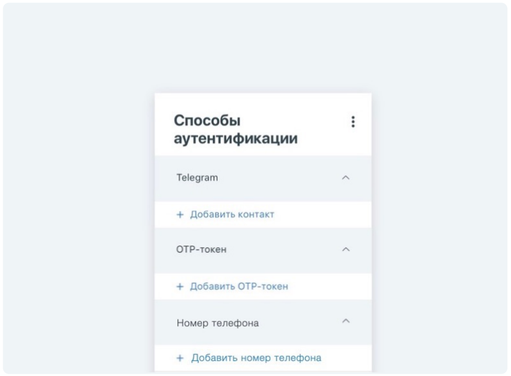
Пример 2: Регистрация 2FA на портале самообслуживания

1 Первое подключение



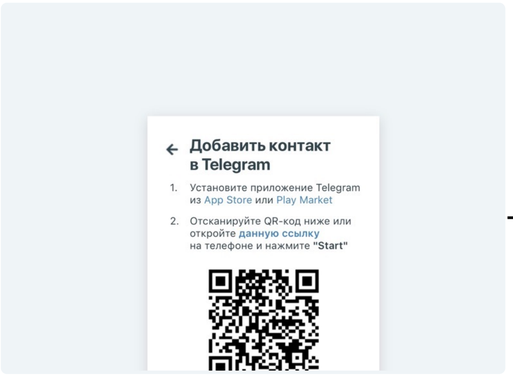
Пользователь проходит аутентификацию на Портале Самообслуживания (учетные данные Active Directory).

2 Выбор фактора



Пользователь выбирает удобный ему способ двухфакторной аутентификации из преднастроенного списка[1].

3 Подтверждение владения



Пользователь подтверждает владение фактором.

4 Готово!

Регистрация второго фактора завершена. Вход дополнительно защищён вторым фактором.

[1] Telegram, SMS, Звонок, Приложение Мультифактор или OTP-токены (аппаратные или программные) в случае защиты VPN и VDI соединений.
[2] Например, в случае подтверждённой утери второго фактора или объективной невозможности использования второго фактора.

Свяжитесь с нами, обсудим детально ваш кейс!

sales@multifactor.kz

+7 727 339 69 16

multifactor.kz
ТОО «Мультифактор Казахстан»