ТМК

Корпоративные
IT-решения

ТМК ID

КАК ОРГАНИЗОВАТЬ АУТЕНТИФИКАЦИЮ ЭФФЕКТИВНО, БЕЗОПАСНО И УДОБНО

Антон Кокин
Директор по инфраструктуре
и кибербезопасности

О чем буду рассказывать:

- О компании ТМК
- Зачем?
- Что делать?
- Как делали?
- Что получили?
- Какие планы?
- Отвечу на вопросы

ТМК – уникальное портфолио передовых компетенций

7,6 млн т
МОЩНОСТЬ ПО ПРОИЗВОДСТВУ СТАЛЬНЫХ ТРУБ

0,3-2520 мм
СОРТАМЕНТ ПРОИЗВОДИМОЙ ТРУБНОЙ ПРОДУКЦИИ

ТМК UP
СОБСТВЕННАЯ ЛИНЕЙКА ПРЕМИАЛЬНЫХ СОЕДИНЕНИЙ

R&D
СОБСТВЕННЫЕ R&D ЦЕНТРЫ В РОССИИ

TMK2U
СОБСТВЕННЫЙ КОРПОРАТИВНЫЙ УНИВЕРСИТЕТ

- ТМК является одним из ведущих поставщиков трубных решений для энергетики и индустриального сектора промышленности и уникальной трубной продукции для энергоперехода.
- ТМК поставляет продукцию в сочетании с широким комплексом сервисных услуг по термообработке, нанесению защитных покрытий, нарезке премиальных соединений, супервайзингу, складированию и ремонту труб.
- ТМК – ведущий промышленный производитель, имеющий признанный опыт, высокопрофессиональную экспертизу в сфере управления и модернизации производственных активов, внедрения и реализации передовых управленческих практик.
- ТМК входит в лидеры рейтингов устойчивого развития (топ-3 рейтинга журнала «Эксперт», «золотой работодатель России» по версии Forbes, лауреат премии «Компания будущего»).
- Акции ТМК обращаются на российской биржевой площадке – Московской Бирже.

Зачем? – с точки зрения Пользователя

- Менять пароль каждые XX дней >> Придумаю систему
- Разные пароли в разных системах (В крупных компаниях может измеряться десятками) >> Буду использовать одни
- Вводить в разных окнах каждый раз в различных системах, особенно из дома >> Запомню в браузере
- Помнить их, когда и где поменял >> Запишу их
- Писать заявки в поддержку (или звонить, если повезет) чтобы сбросили пароль >> Постоянное обращение в службу ИТ

Да сделайте уже с этим что-нибудь!!!

Зачем? – Проблематика с точки зрения ИТ

- Множество различных ИС, в том числе поддерживающих **устаревшие протоколы авторизации** (NTLM, LDAP)
- Не во всех корпоративных системах реализована **процедура единого входа**
- **Пароли уязвимое место** системы и постоянно увеличиваются требования к его стойкости (Из повышения возможностей злоумышленников)
- **Необходимость MFA** добавляет сложности как с точки зрения интеграции, так и процесса жизненного цикла
- Есть системы, в которых доступ требуется сотрудникам, не являющимся **пользователями ПК** (Сайты обучения, Мобильные приложения)
- Разработка большого количества новых корпоративных систем с **различными требованиями к процессу входа** и предоставлению доступа
- Разработчики (как внутренние так и внешние) **не поддерживают современные протоколы SSO** (OpenID, SAML)
- Необходимо обеспечивать **единые подходы** с точки зрения кибербезопасности сопровождения и жизненного цикла учетных записей

Что делать?

Автоматизация жизненного цикла УЗ пользователей

- Создание единого хранилища БД пользователей (Внутренняя разработка)
- Интеграция БД с Кадровыми системами
- Автоматизация жизненного цикла (Внутренняя разработка)

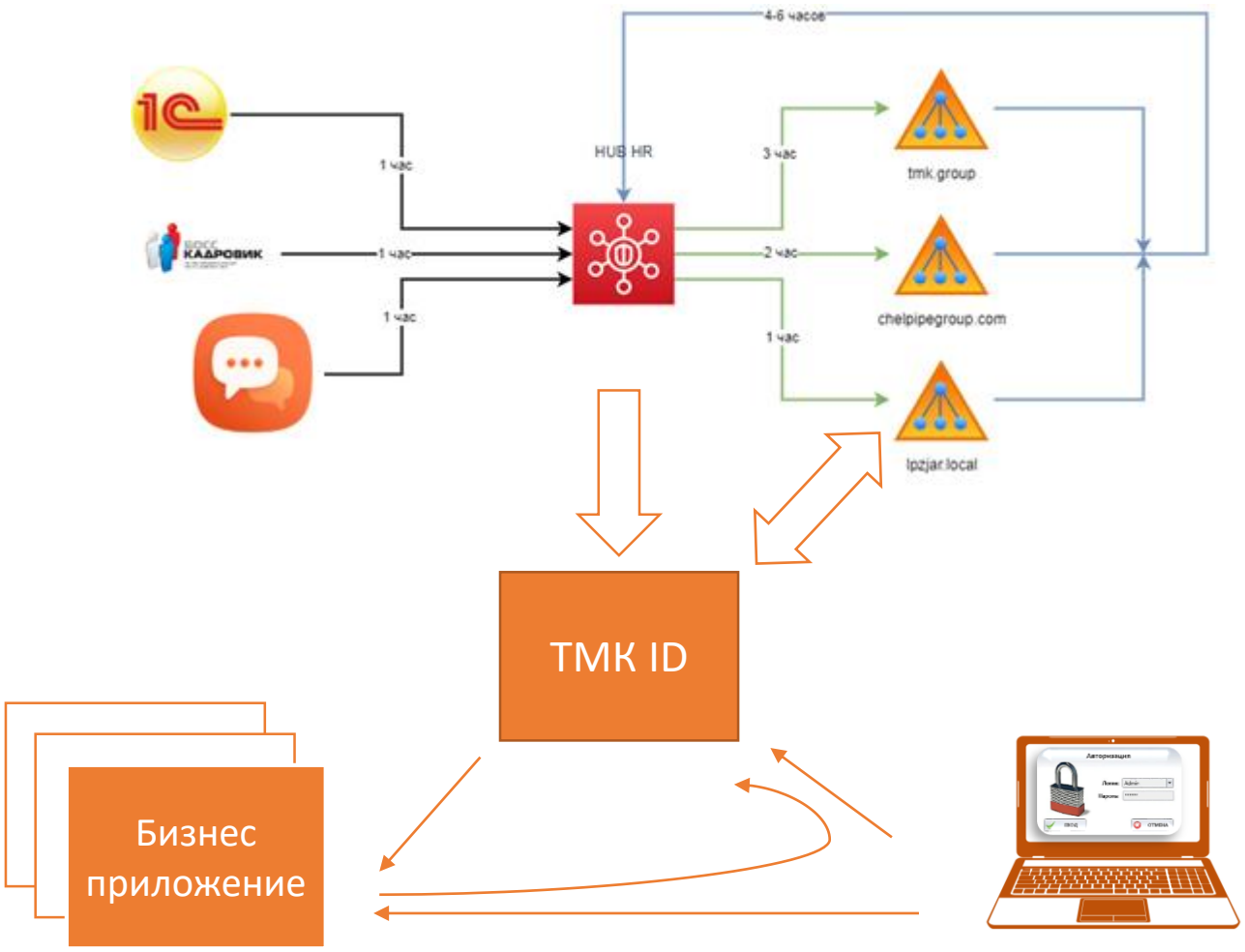
Внедрения системы IDP (Identity Provider)

- Поддержка современных протоколов SSO
- Поддержка формата самообслуживания
- Поддержка MFA

Интеграция систем

- Доработка критичным и массовых систем для поддержки SAML и OpenID
- Доработка систем собственной разработки
- Жесткие требования на внедряемые системы (Стандартизация)

Архитектура (схематично)



Сценарии входа

Пользователь (AD) | Корпоративное устройство | Внутри

- SSO (без ввода дополнительного пароля)

Пользователь (AD) | Не корпоративное устройство или Снаружи

- Ввод пароля (Корпоративный) |
- MFA (Push\SMS\OTP) | или QR код

Не пользователь (AD) | Не корпоративное устройство

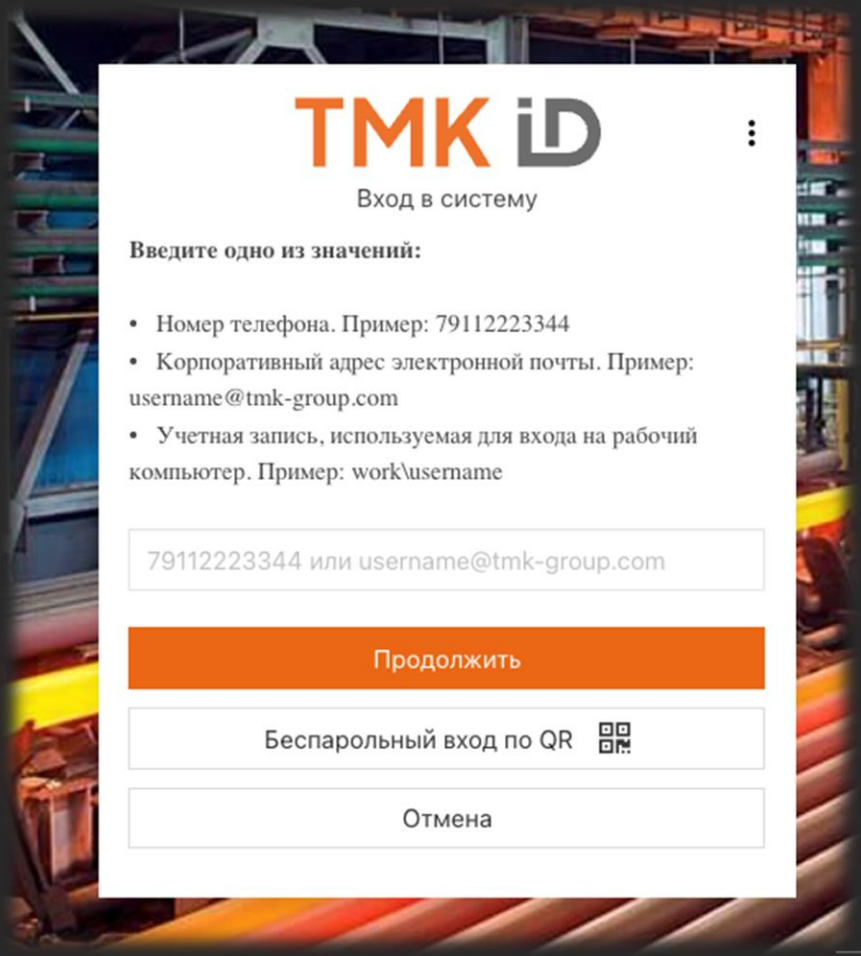
- MFA (Push\SMS\OTP) | или QR код

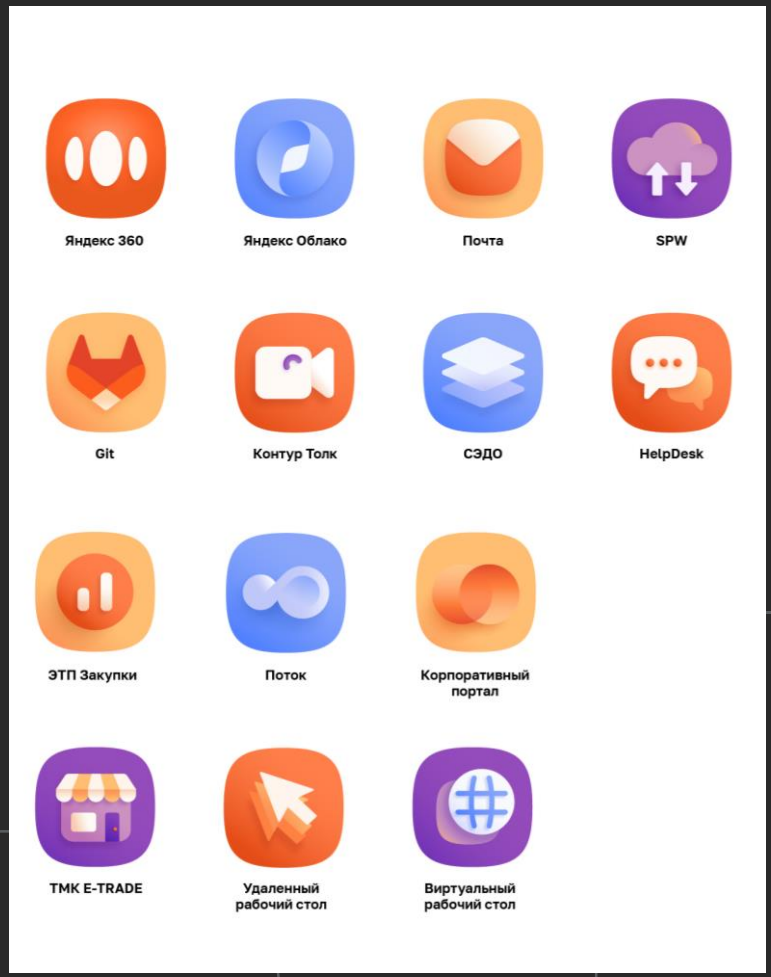
Администратор | Все сценарии

- Ввод пароля (Корпоративный)
- MFA (Push\SMS\OTP)

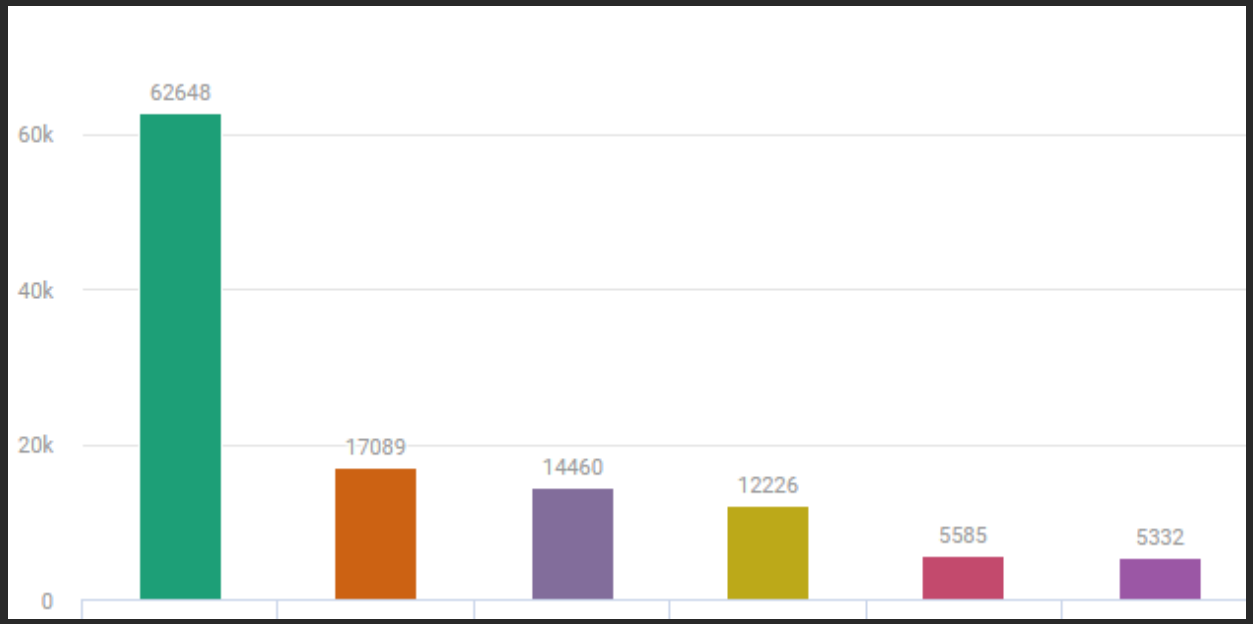
Минимальный риск | Средний риск | Высокий риск

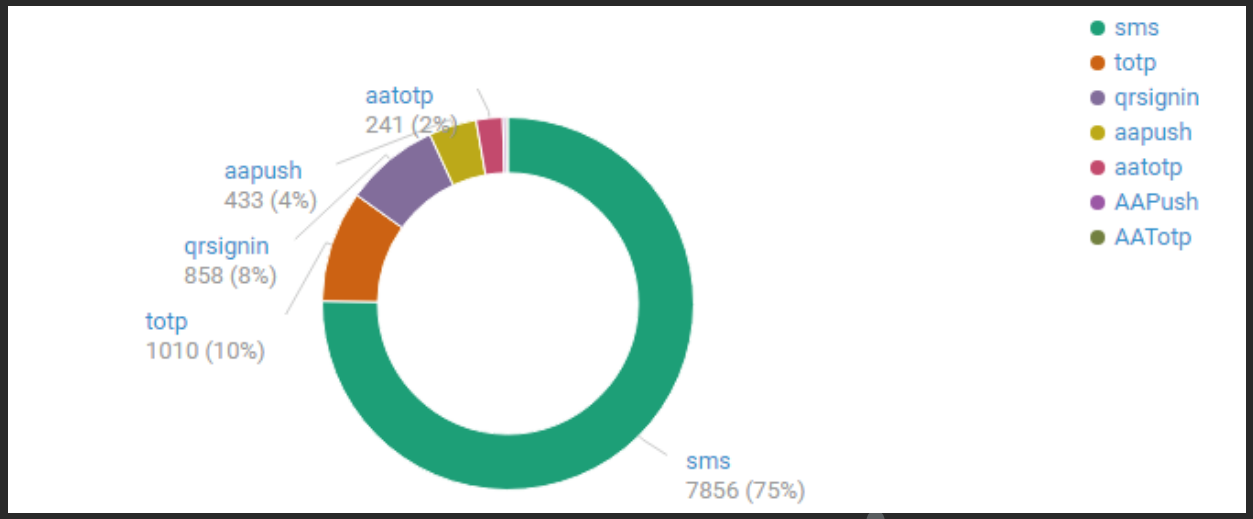
Интеграция систем



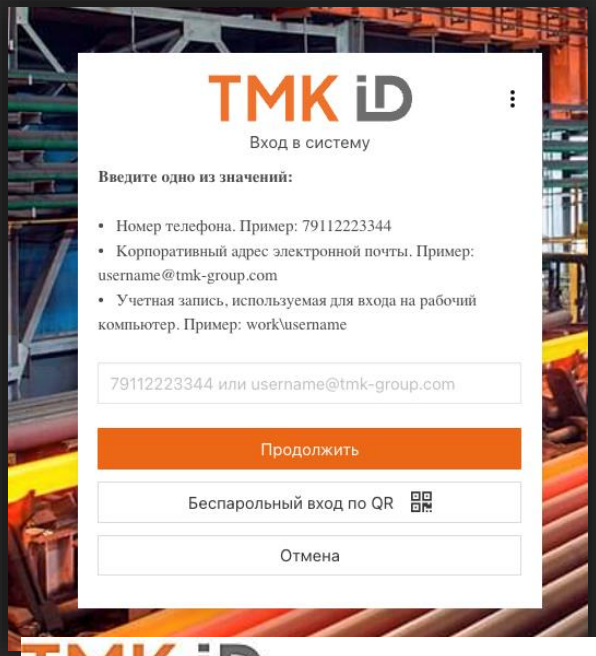


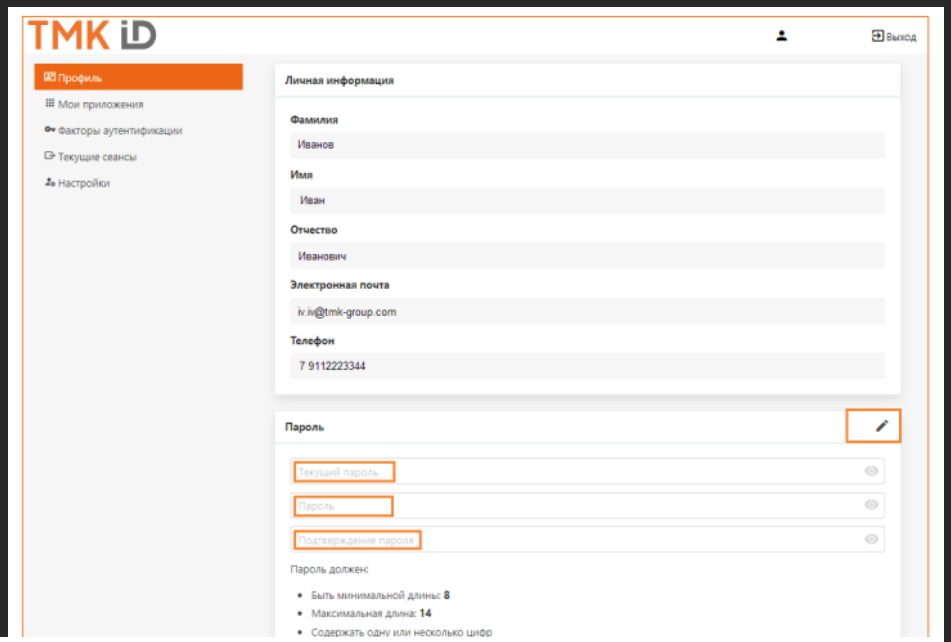
Статистика использования

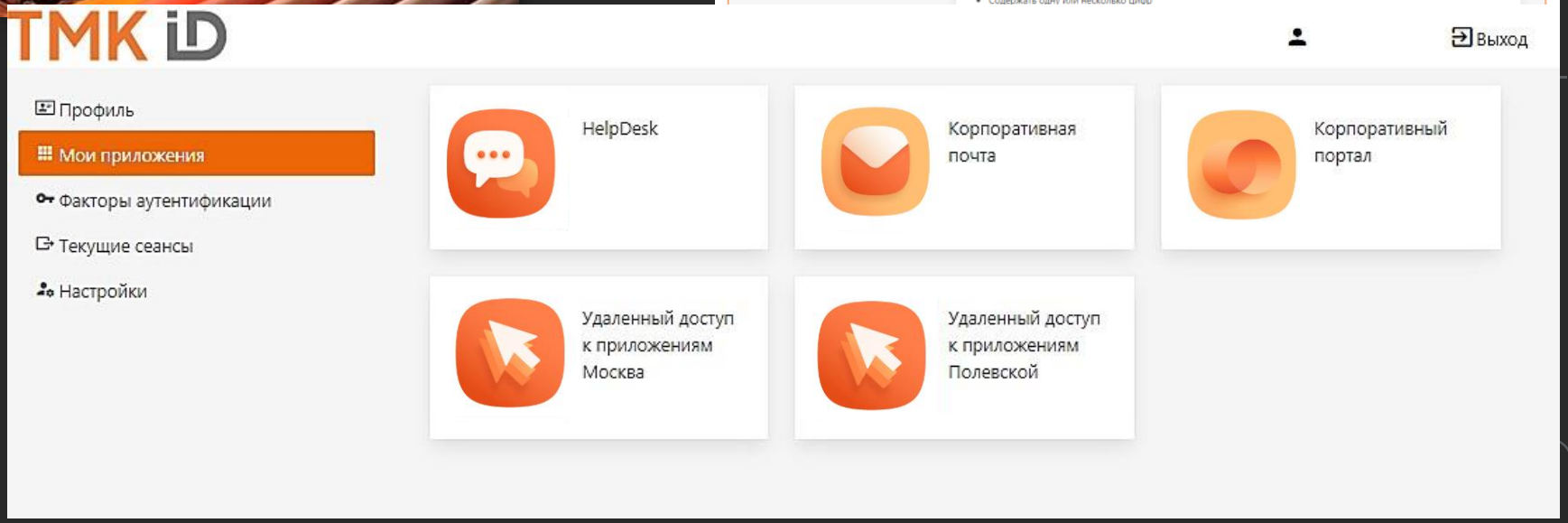




Как это выглядит для пользователя







Планы

1	Вход на компьютер по QR коду
2	Переопределение срока действия сессии для отдельного приложения
3	Корпоративное мобильное приложение в качестве аутентификатора
4	Регистрация информации об устройствах с возможностью просмотра сведений об устройствах пользователя, завершения сессий на устройстве, использования характеристик устройства для изменения сценария аутентификации или запрета аутентификации
5	Построение федеративных отношений (ЕСИА, Яндекс ID и др.)
6	Механизм отправки уведомлений пользователю (E-mail, SMS, push в Приложение) Возможные уведомления: ✓ Предоставление/отзыв доступа к приложению; ✓ Приветственное письмо при регистрации нового пользователя; ✓ Вход с нового устройства; ✓ Восстановление пароля; ✓ Смена пароля; ✓ Привязка/удаление аутентификатора; ✓ Изменение критичных атрибутов (E-mail, номер телефона).
7	Отчетность: ✓ Статистика аутентификаций пользователей за период в приложениях; ✓ Фактические полномочия пользователей, включая приложения, группы и роли; ✓ Отчёт по защищённости пользовательских учётных записей и готовности к работе в системе.
8	Дальнейшая интеграция с приложениями

Кокин Антон Александрович

Директор по инфраструктуре и безопасности

Т.: +7 (495) 775-76-00, доб. 2085
anton.kokin@tmk-group.com
@KokinAntonA

Вопросы? >>>