КОМПАНИЯ
ИНДИД

ЭКОСИСТЕМА CORPORATE ID ДЛЯ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ И ЗАЩИТЫ ДОСТУПА

КВАЛИФИЦИРОВАННАЯ ЭЛЕКТРОННАЯ ПОДПИСЬ

СКЗИ-чип

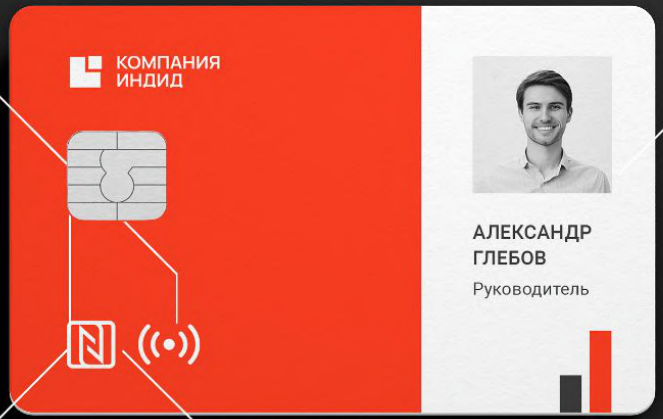
NFC

УДОСТОВЕРЕНИЕ

Визуальная идентификация

ФИО

Должность



ДОСТУП В ИНФОРМСИСТЕМЫ

СКЗИ-чип

RFID

ДОСТУП В ПОМЕЩЕНИЕ

RFID-метка

КОМПАНИЯ
ИНДИД

О НАШЕЙ КОМПАНИИ

Компания Индид — российский вендор программного обеспечения для повышения информационной безопасности в компаниях разных отраслей экономики

3
ОФИСА В РОССИИ
Москва, Санкт-Петербург, Великий Новгород

3
РАЗРАБОТАННЫХ ПРОДУКТА
в Реестре отечественного ПО

5
СТРАН ПРИСУТСТВИЯ В СНГ
Россия, Казахстан, Беларусь, Узбекистан, Кыргызстан

200+
АКТИВНЫХ ЗАКАЗЧИКОВ

14
ЛЕТ ОПЫТА
Проектирование, разработка, тестирование и внедрение комплексных решений

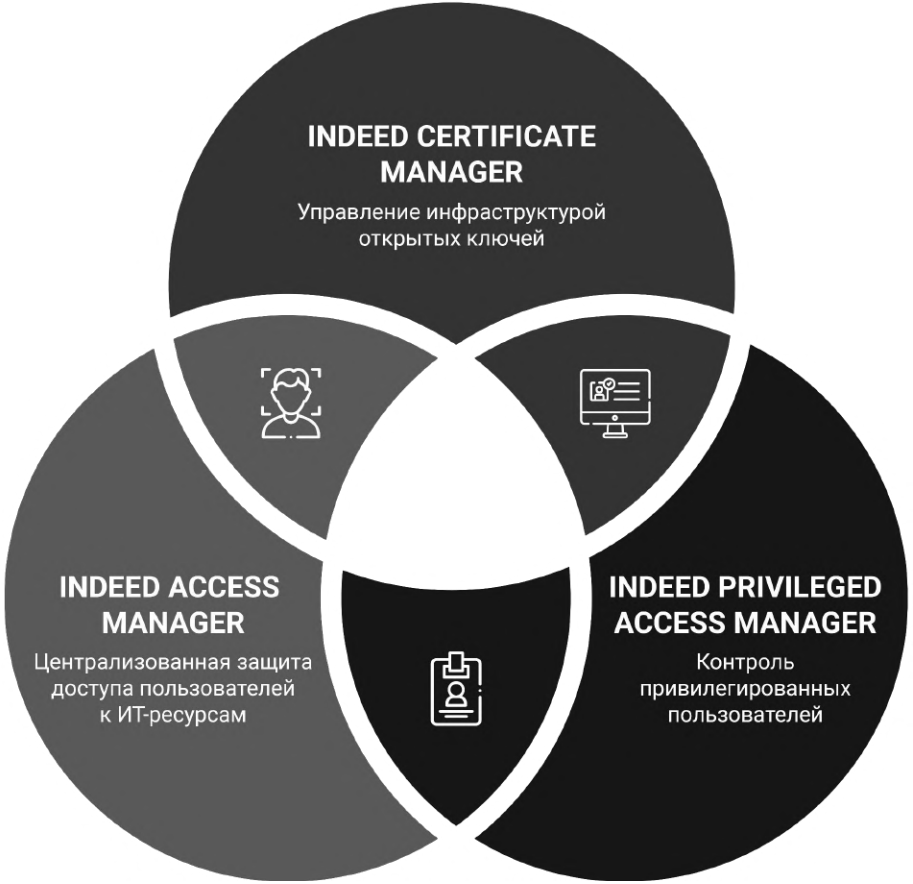
80+
СОТРУДНИКОВ
Распределенная команда: 4 региона, 3 страны

90+
РЕГИОНАЛЬНЫХ ПАРТНЕРОВ

КОМПАНИЯ
ИНДИД

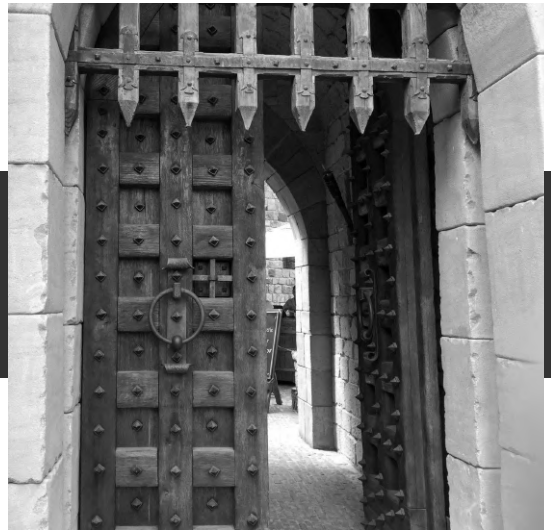
НАШИ ПРОДУКТЫ

Все продукты находятся
в Реестре отечественного
программного обеспечения



КОМПАНИЯ
ИНДИД

ТИПИЧНАЯ СИСТЕМА
ЗАЩИТЫ ДОСТУПА

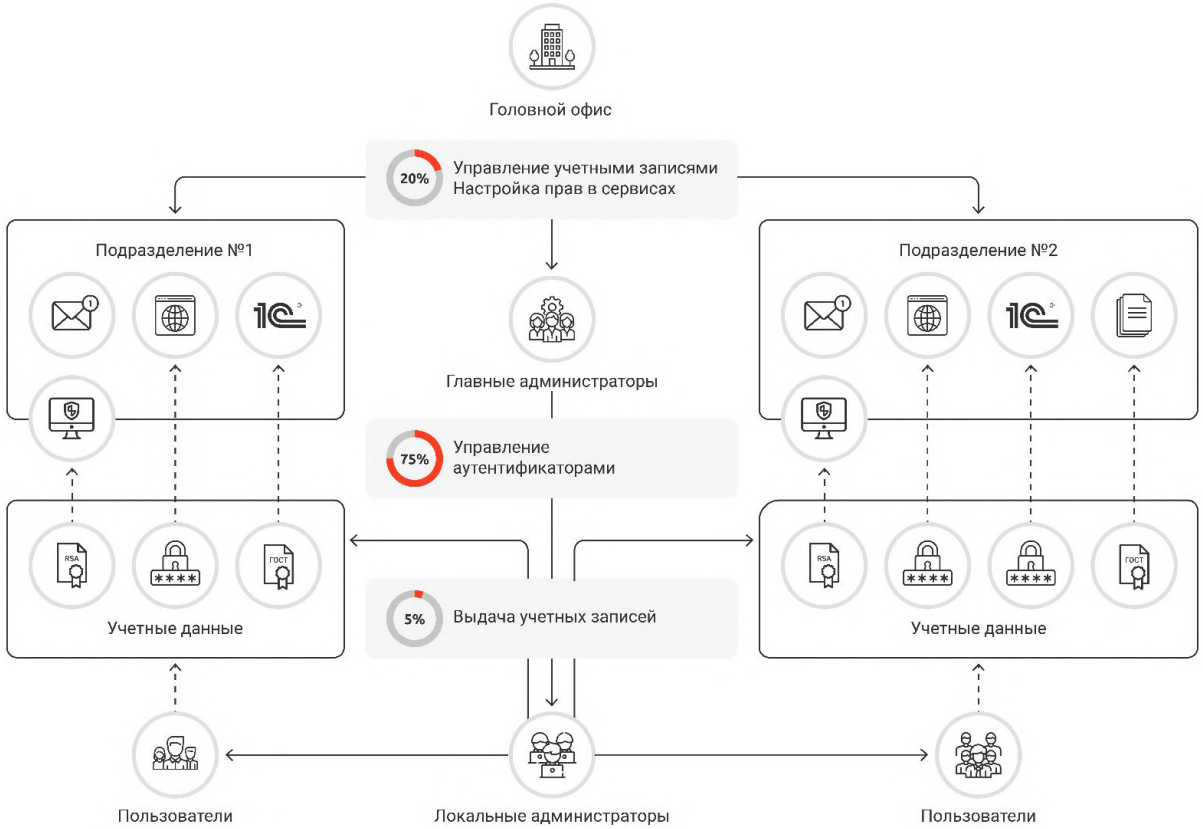


VS

Ожидание

Реальность

«КЛАССИЧЕСКОЕ» УПРАВЛЕНИЕ ДОСТУПОМ



ПРОБЛЕМЫ СИСТЕМ УПРАВЛЕНИЯ ДОСТУПОМ

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Кража и взлом паролей

Многие сервисы и приложения поддерживают только парольную аутентификацию, которая общепризнанно считается уязвимой.

Невыполнение требований безопасности

Практически невозможно реализовать выполнение всех требований безопасности при обращении паролей, включая безопасное хранение

СНИЖЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ ТРУДА

Сложная процедура выдачи учетных данных

Для выдачи учетных записей и аутентификаторов необходимо обеспечить их безопасную доставку и проконтролировать получение

Ручной учет сертификатов и аутентификаторов

Учет цифровых сертификатов, носителей ключевой информации и иных аутентификаторов ведется в ручном режиме

НЕПРОДУКТИВНОЕ РАСХОДОВАНИЕ ВРЕМЕНИ

Несколько аутентификаторов на пользователя

Пользователи могут использовать несколько учетных записей и аутентификаторов в работе для работы в разных сервисах и приложениях

Забывание и сбросы паролей

Существует риск забывания пароля пользователем, что требует последующего сброса и безопасной передачи

ОТСУТСТВИЕ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ

ЭКОСИСТЕМА INDEED CORPORATE ID

Экосистема централизованного управления
доступом пользователей

Единое решение
для идентификации
и аутентификации

Экономия ресурсов
и повышение
производительности труда

Централизованное
управление
и мониторинг

Интеграция
с целевыми
ИТ-системами

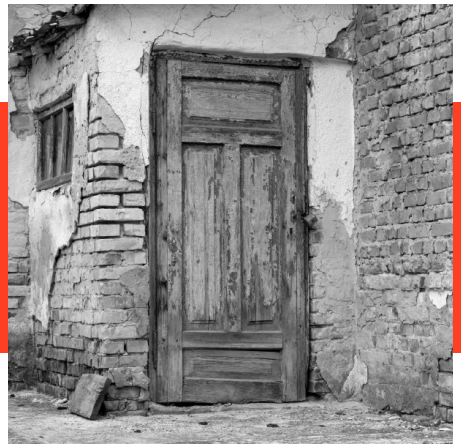
КРАЙНОСТИ НАПРАВЕНИЯ
IDENTITY & ACCESS MANAGEMENT

Применение встроенных средств управления

Управление учетными записями и правами (IdM/IGA)

КОМПАНИЯ
ИНДИД

ВАЖНЕЙШАЯ ДЕТАЛЬ

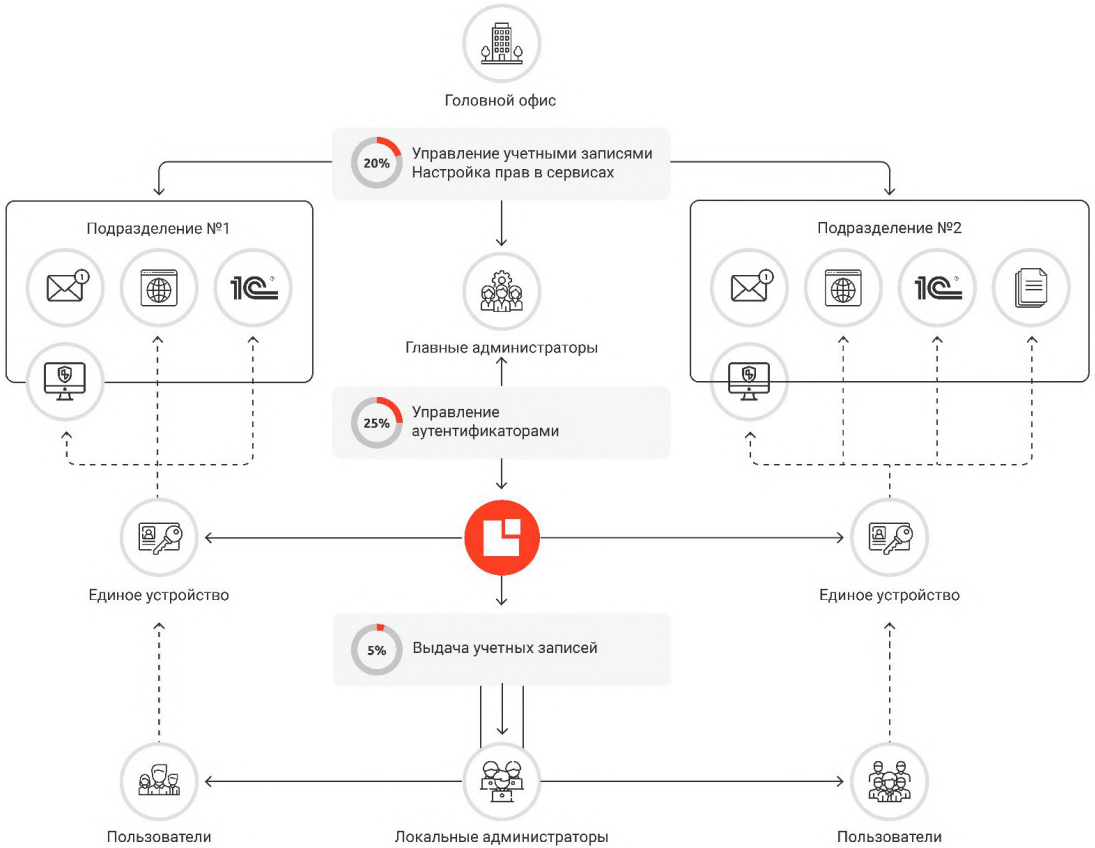


Применение встроенных средств управления

Управление аутентификацией и секретами (AAA, MFA)

Управление учетными записями и правами (IdM/IGA)

ЭКОСИСТЕМА INDEED CORPORATE ID



ЕДИНАЯ АУТЕНТИФИКАЦИЯ
ДЛЯ ЛЮБЫХ ЦЕЛЕВЫХ СИСТЕМ

Поддержка способов усиленной аутентификации:

- Биометрические технологии
- Аппаратные носители
- Одноразовые пароли
- Push-уведомления

Поддержка протоколов аутентификации:

- RADIUS
- SAML
- ADFS
- OpenID Connect
- Kerberos (Active Directory)

Поддержка целевых систем:

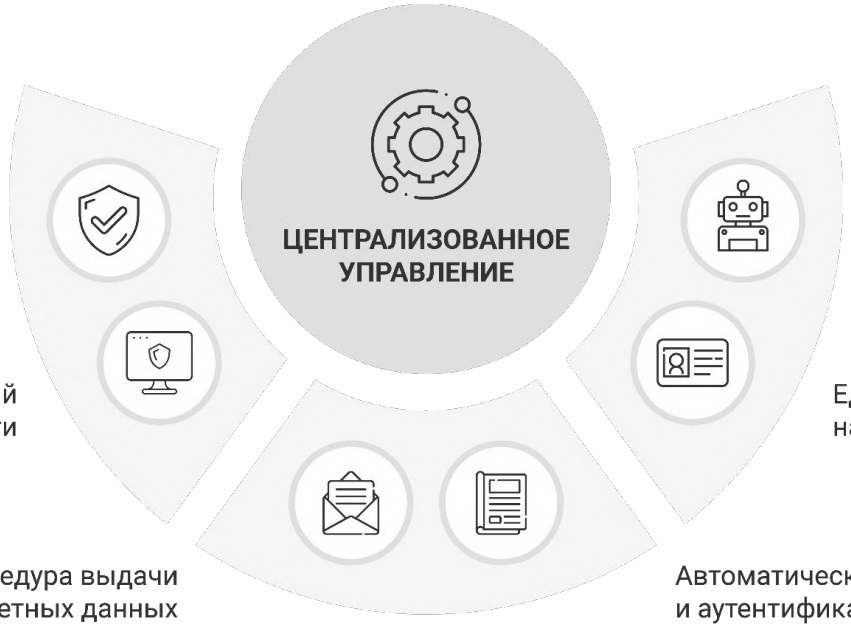
- MS Windows
- MS Remote Desktop Server
- MS Internet Information System
- VPN-Gateway, VDI-Server
- Web & Desktop Application

Поддержка интеграции:

- SIEM (syslog)
- IdM
- СКУД
- PKI-Management
- API

КОМПАНИЯ
ИНДИД

НЕЙТРАЛИЗАЦИЯ ПРОБЛЕМ УПРАВЛЕНИЯ ДОСТУПОМ



УСИЛЕНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ

Нейтрализация угроз кражи и взлома паролей

Выполнение требований безопасности

ЭКОНОМИЯ РАБОЧЕГО ВРЕМЕНИ

Исключение паролей из обращения

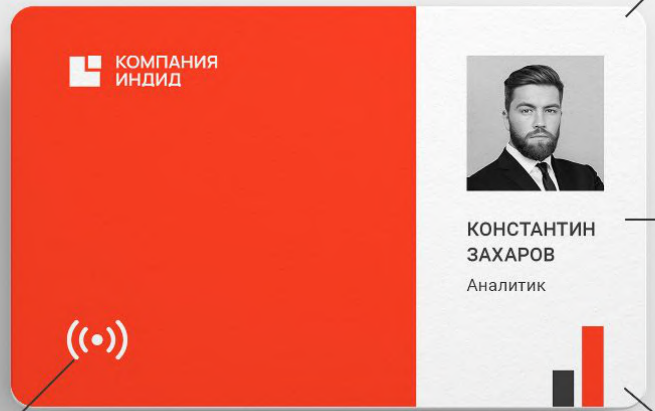
Единый аутентификатор на пользователя

ПОВЫШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ ТРУДА

Простая процедура выдачи учетных данных

Автоматический учет сертификатов и аутентификаторов

CORPORATE ID ДЛЯ СОТРУДНИКОВ:
ОТДЕЛ АНАЛИТИКИ



LOCAL ACCESS

Доступ в помещения

Доступ к ПК

REMOTE ACCESS

Доступ к публичным ресурсам

2ND AUTHENTICATION FACTOR

PIN-код

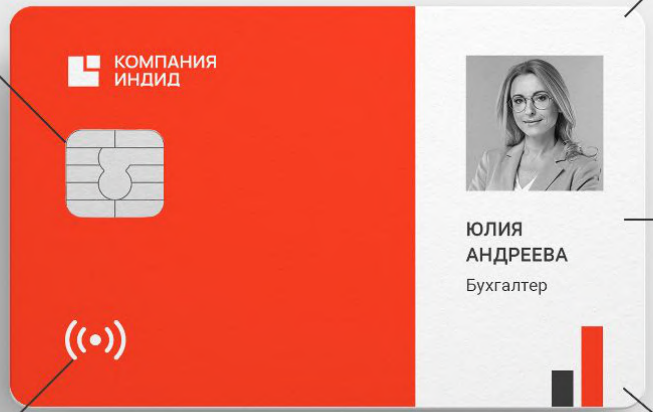
RFID-МЕТКА

CORPORATE ID ДЛЯ СОТРУДНИКОВ:
БУХГАЛТЕРИЯ

PKI-СЕРТИФИКАТЫ

- Сертификат для доступа в Windows
- Сертификат для СЭД

RFID-МЕТКА



LOCAL ACCESS

- Доступ в помещения
- Доступ к ПК
- Доступ к приложениям

REMOTE ACCESS

- Доступ к внутренним ресурсам
- Доступ к публичным ресурсам

2ND AUTHENTICATION FACTOR

- Одноразовый пароль

CORPORATE ID ДЛЯ СОТРУДНИКОВ: РУКОВОДСТВО

PKI-СЕРТИФИКАТЫ

- Сертификат для доступа в Windows
- Сертификат для СЭД

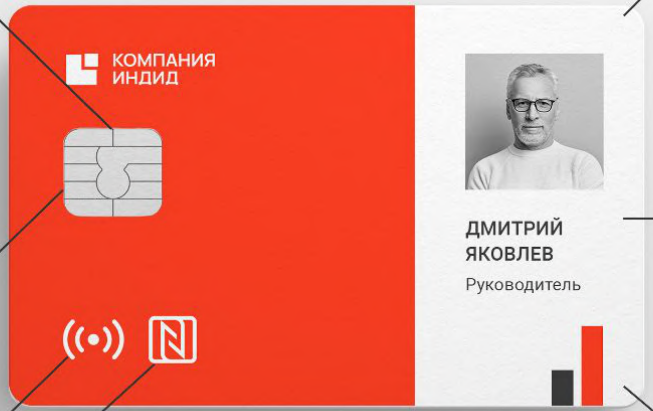
КВАЛИФИЦИРОВАННАЯ ПОДПИСЬ

- ГОСТ Сертификат

RFID-МЕТКА

NFC

- PKI на мобильном устройстве



LOCAL ACCESS

- Доступ в помещения
- Доступ к ПК
- Доступ к приложениям

REMOTE ACCESS

- Доступ к внутренним ресурсам
- Доступ к публичным ресурсам

2ND AUTHENTICATION FACTOR

- Биометрия

КЕЙС — БАНК ВТБ

- Проведена замена конкурирующего решения по управлению цифровыми сертификатами и ключевыми носителями
- Организован контроль подключаемых устройств на рабочих местах пользователей
- Используются смарт-карты различных производителей
- Аутентификация пользователей в ОС и VPN выполняется с помощью цифровых сертификатов, выпущенных на собственном Microsoft CA и Валидата УЦ

Охват пользователей: около 100 000

КЕЙС - НЕФТЕГАЗОВЫЕ КОМПАНИИ

- Создан автоматизированный процесс управления PKI: контролируется использование цифровых сертификатов и аппаратных ключевых носителей
- Используется единая карта-пропуск для физического и логического доступа сотрудников в филиалах
- Используются инструменты выпуска и обновления сертификатов для аутентификации в ОС
- Снижена нагрузка на операторов PKI, в т.ч. автоматизировано управление PKI для решения задач кадрового делопроизводства
- Проведена замена конкурирующих решений

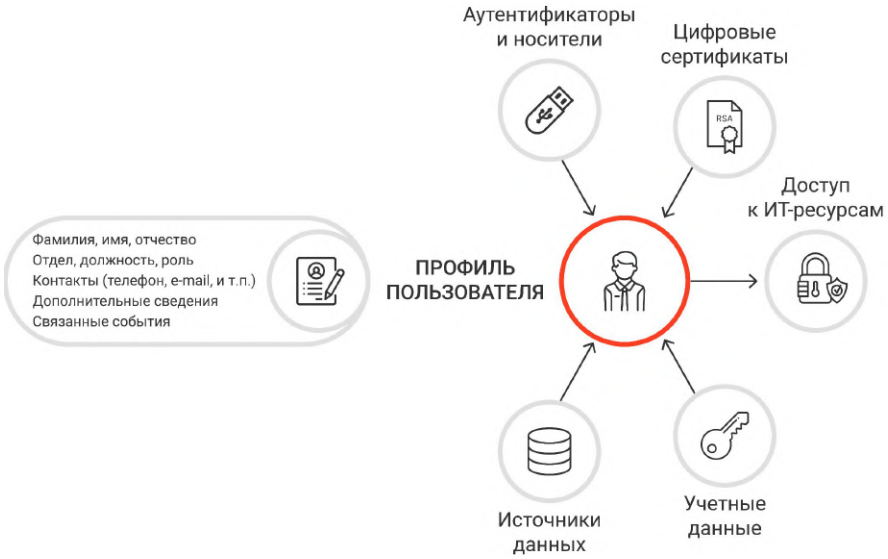
Охват пользователей: около 10 000

КОМПАНИЯ
ИНДИД

ПРИНЦИПЫ РАБОТЫ CORPORATE ID

CORPORATE ID: ПРОФИЛЬ ДОСТУПА ПОЛЬЗОВАТЕЛЯ

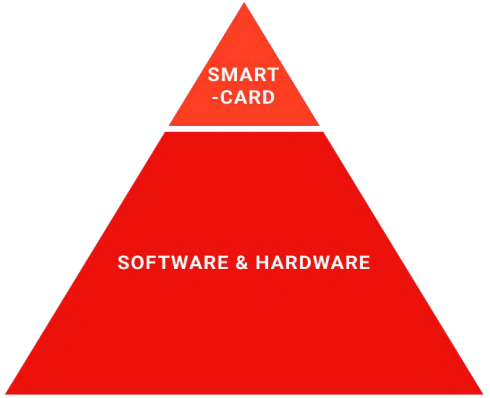
- Информация о пользователе
- Событие доступа пользователя
- Назначенные аутентификаторы, носители и выданные сертификаты
- Политики доступа пользователя



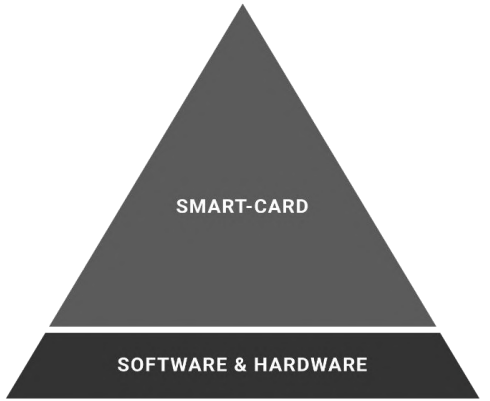
CORPORATE ID: ОТЛИЧИЯ ОТ «КЛАССИЧЕСКИХ» СМАРТ-КАРТ

- Основные функции управления доступом реализуются на уровне инфраструктуры Corporate ID
- Смарт-карты являются только одним из возможных видов аутентификаторов
- Основные сведения и права хранятся в цифровом удостоверении (профиле)
- Такой подход позволяет реализовать управление доступом независимо от типа аутентификатора (и от типа смарт-карт)

Распределение функций управления доступом



УСТРОЙСТВО CORPORATE ID

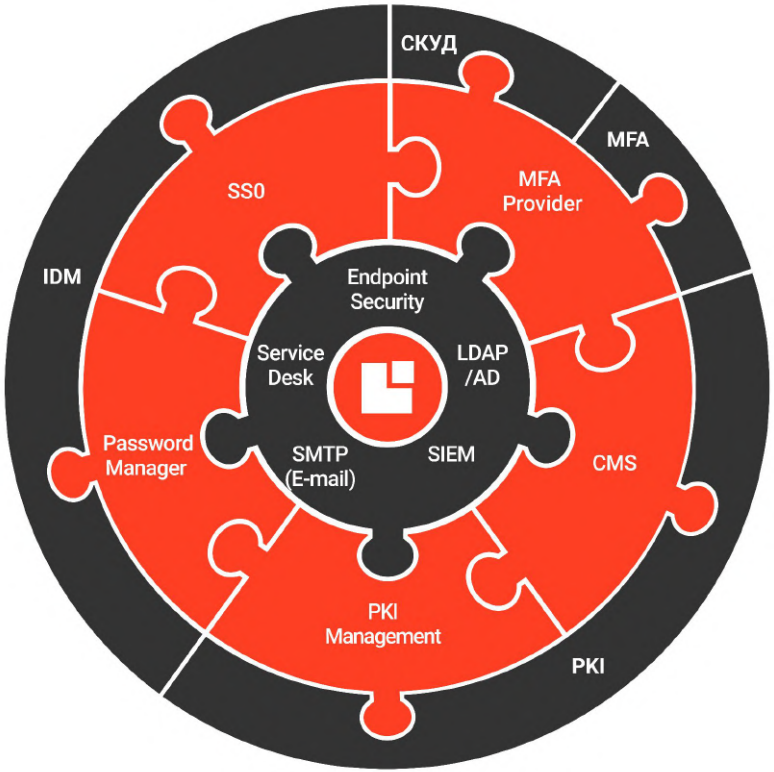


«КЛАССИЧЕСКОЕ» УСТРОЙСТВО

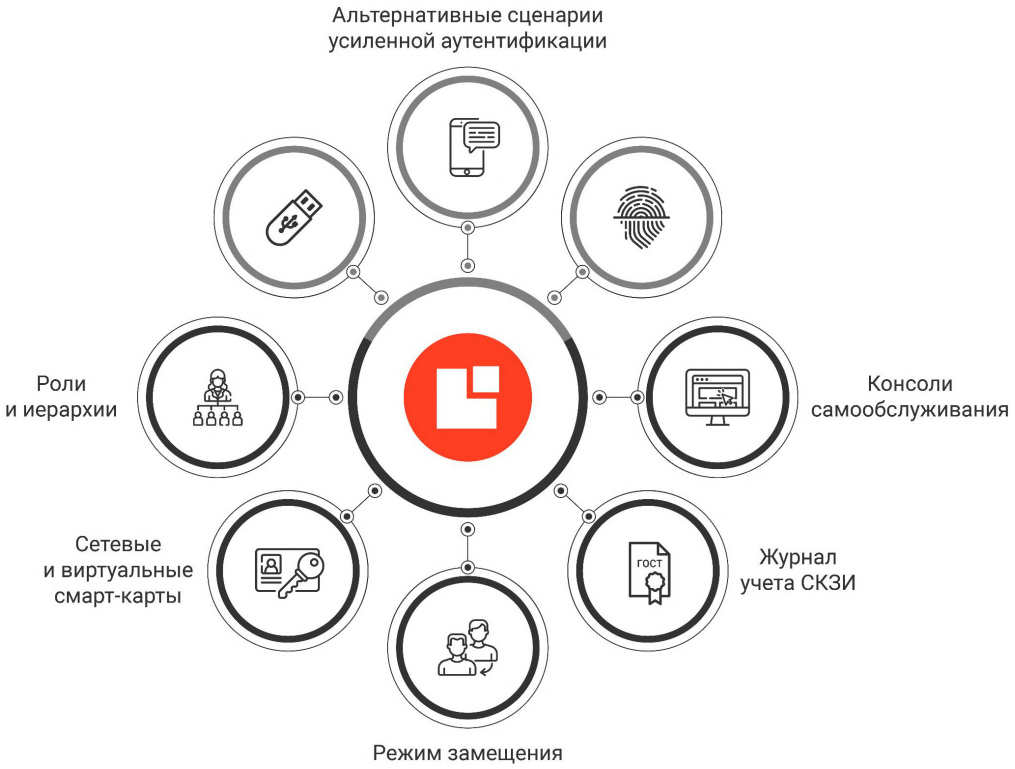
ИНТЕГРАЦИЯ
И ВЗАИМОДЕЙСТВИЕ

Поддерживается интеграция с решениями:

- IdM/IGA - для управления жизненным циклом учетных записей
- Компонентами PKI - для управления выдачей сертификатов и их мониторингом
- Решениями MFA - для централизованного управления сценариями усиленной аутентификации
- СКУД - для контроля доступа к рабочим станциям, основываясь на физическом доступе



ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ



Поддержка способов усиленной аутентификации:

- Биометрические технологии
- Аппаратные носители
- Одноразовые пароли
- Push-аутентификация

Роли и иерархия:

- Применение политик на основе групп
- Иерархия администраторов
- Разные роли администраторов

Поддержка ключевых носителей*:

- Реестр Windows
- Trusted Platform Module
- Windows Hello for Business
- Сетевые смарт-карты (Indeed AirCard Enterprise)

Режим замещения:

- Назначение заместителя
- Возможность авторизации заместителя от лица замещаемого

Учет и мониторинг:

- Сертификатов и носителей
- Аутентификаторов
- Журнал учета СКЗИ (ФАПСИ №152)
- События, связанные с пользователем

***Не поддерживаются ГОСТ-сертификаты**

КЕЙС — РЕГИОНАЛЬНЫЙ МФЦ

Особенности инфраструктуры

- Более 100 филиалов по региону
- Для аутентификации используются сертификаты квалифицированной электронной подписи и пароли
- На каждого оператора - 5 информационных систем с отдельной аутентификацией
- Сотрудники используют единый USB-токен для аутентификации во всех информационных системах и сервисах

Охват пользователей: более 1 000

КЕЙС — АЭРОПОРТ ДОМОДЕДОВО

Особенности инфраструктуры

- Рабочие места сотрудников представляют собой терминалы общего доступа, расположенные на территории аэропорта
- Созданы прозрачный доступ пользователей в целевые приложения и централизованная система двухфакторной аутентификации сотрудников
- Сотрудники используют двухфакторный механизм аутентификации: RFID-карта или биометрия

Охват пользователей: более 15 000

КОМПАНИЯ
ИНДИД

О ВЫГОДАХ СОТРУДНИЧЕСТВА

ВЫГОДЫ ОТ ПРИМЕНЕНИЯ ЭКОСИСТЕМЫ CORPORATE ID

Единое решение для идентификации и аутентификации

Единое решение для идентификации и аутентификации во всех корпоративных сервисах и системах, с поддержкой дополнительных сценариев аутентификации: одноразовые пароли, биометрия

Централизованное управление и мониторинг

Единая система централизованного управления аутентификацией, ключами, доступом с едиными журналами мониторинга соответствующих событий ИБ

Экономия ресурсов и повышение производительности труда

Автоматизация и оптимизация рутинных операций по управлению аутентификаторами, ключами и политиками доступом

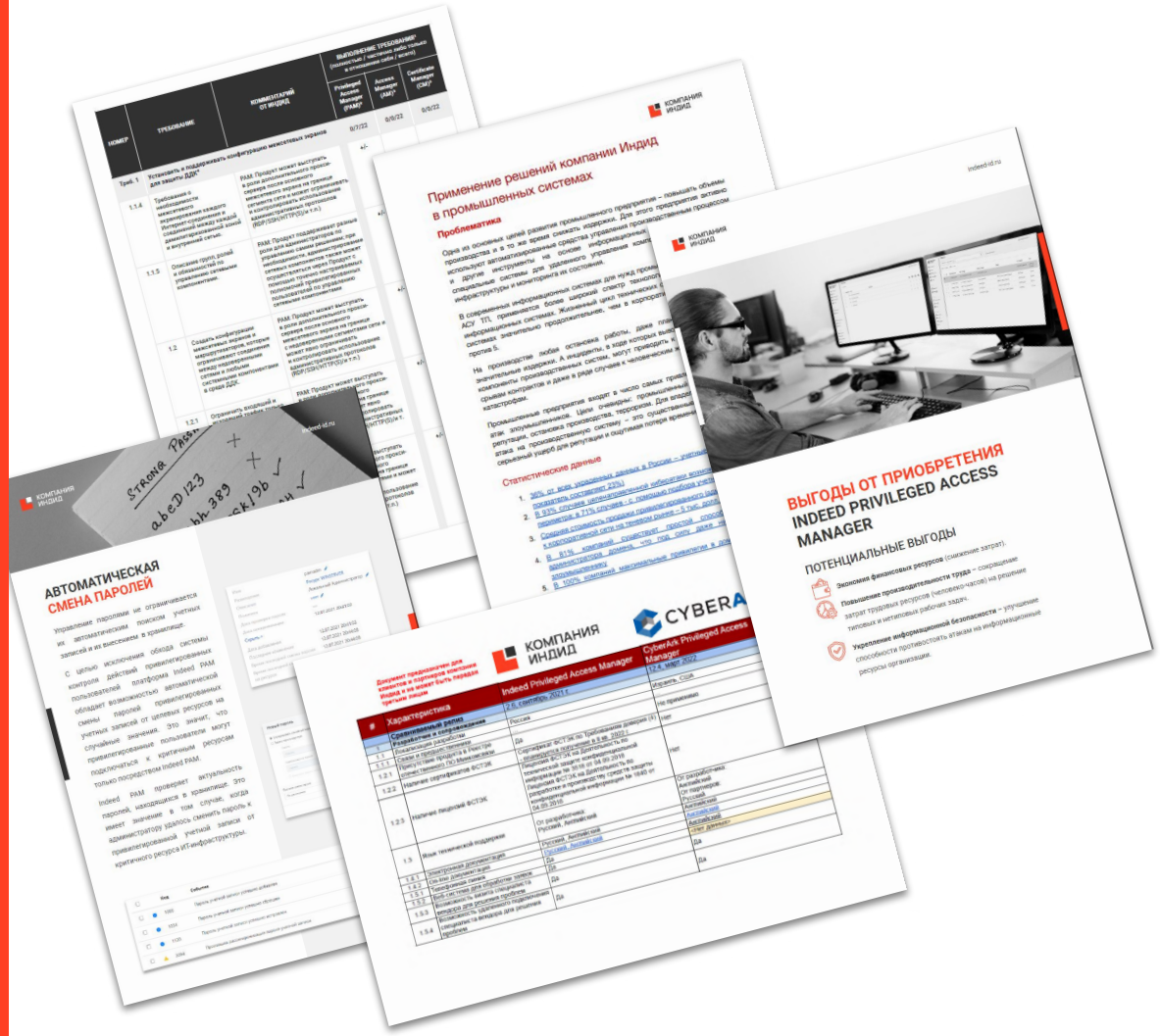
Интеграция с целевыми системами и компонентами ИТ-инфраструктуры

Поддержка интеграции со всеми корпоративными сервисами и системами, а также со средствами защиты информации

КОМПАНИЯ
ИНДИД

ТЕХНИЧЕСКИЕ И АНАЛИТИЧЕСКИЕ МАТЕРИАЛЫ

- Compliance - Оценки выполнения требований
- Comparisons - Сравнения продуктов с конкурентами
- Industry Use Cases - Отраслевые применения продуктов
- Solution Use Cases - Сценарии применения продуктов
- Benefits - Выгоды от применения продуктов
- И другие…

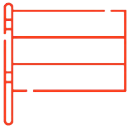


КОМПАНИЯ
ИНДИД

ПРЕИМУЩЕСТВА КОМПАНИИ

Русскоязычная техническая поддержка 8/5

Доработка решений под задачи заказчика



Российский разработчик программного обеспечения

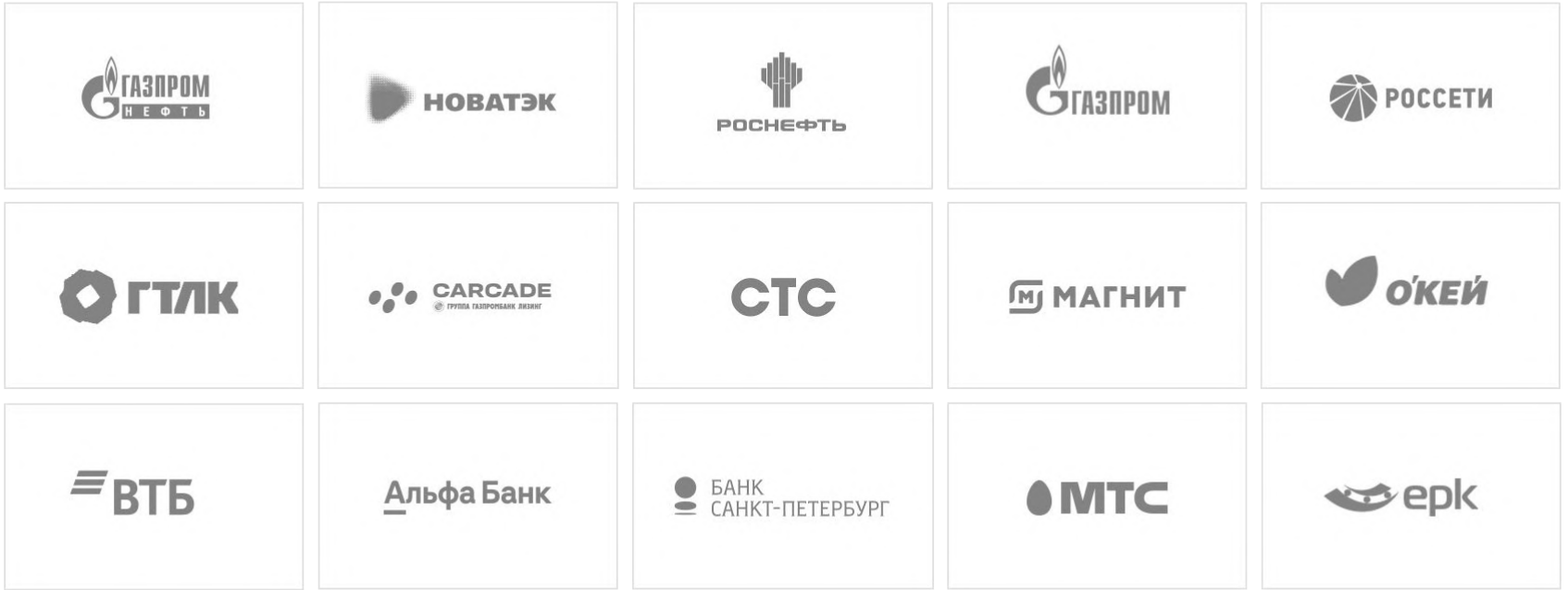
Бесплатное тестирование продуктов с возможностью предоставления оборудования

Организация референсов и презентаций

Партнерская программа

КОМПАНИЯ
ИНДИД

НАШИ ЗАКАЗЧИКИ



КОМПАНИЯ
ИНДИД

КОНТАКТЫ

indeed-id.ru

sales-russia@indeed-id.com

8 800 333-09-06