



Аутентификация

- от паролей к 2ФА, биометрии и адаптивной МФА

2ФА - двухфакторная аутентификация, МФА - многофакторная

V6



[Скачать презентацию](#)

Сергей Груздев
ген. директор АО "Аладдин Р.Д."

апрель, 2025 г.

Мир сильно изменился, а мы нет...

С какими вызовами столкнулись после 2022 г?

- ◆ Беспрецедентный рост успешных атак на ИС и утечек
 - Цели атак
 - Кража/блокирование главных информационных активов (баз данных, персональных данных)
 - Типовая проблема
 - В большинстве инцидентов виноват **внутренний нарушитель** (явно или неявно) - его роль была сильно недооценена
 - После инцидента начинается **борьба не с причинами, а с последствиями** (атак, взломов, краж)
 - ИБ-бюджеты по-прежнему тратятся на системы мониторинга, DLP, ИИ, устранение уязвимостей и пр., а не на системы аутентификации и селективное шифрование/обезличивание персональных данных
- ◆ Причины?
 - 1) **Неправильная подсистема аутентификации**
 - Оборудования в ИТ-инфраструктуре (использование MAC-адресов вместо цифровых сертификатов)
 - Пользователей (пароли, QR-коды, SMS, не привязанные к "железу"/телефону)
 - Госуслуги - неправильная реализация идентификации и аутентификации породила гигантскую проблему национального масштаба
 - 2) **Удалённый доступ - использование небезопасного "самопала"**



Как меняется рынок аутентификации

- ◆ Рынок ИБ подвержен моде больше, чем сама индустрия моды
 - Блокчейн, постквантовая криптография, ИИ...
- ◆ Сегмент идентификации и аутентификации - самый консервативный - большинство сидит на паролях
 - Нормативная база не менялась десятилетиями...
- ◆ Парадокс
 - ИБ начинается с аутентификации (фундамент)
 - Нас учили, что **надёжность системы определяется её самым слабым звеном**
 - ✓ **Слабая аутентификация = слабая ИБ всей ИС**
 - Продолжаем пользоваться паролями и строить замки на песке
 - Выучив сложный пароль к своим рабочим ресурсам кто-нибудь из пользователей обязательно использует его при заказе пиццы, в э-сервисах, а их базы часто утекают...
 - ✓ **Если организация использует пароли, значит она не контролирует свои аккаунты**
- ◆ Незнание матчасти и следование навязанной моде
 - Всё больше организаций внедряет 2ФА (хотя бы для удалённого доступа) с грубейшими ошибками
 - "Смартфон - модно, удобно, не дорого" - но в ущерб безопасности
 - SMS, push, QR-коды - это 2х этапная аутентификация, доп. атрибуты идентификации, а не 2ФА
 - Облачная аутентификация (аутентификация как сервис)
 - Использование УКЭП для аутентификации в ИС, в эл. сервисах
 - ✓ **Бич сегодняшнего дня - неверный выбор технологии и решения МФА для своей ИС (ГИС)**



Всё это неприемлемо для ГИС, КИИ
- новые Требования 17го приказа ФСТЭК

Как выбрать правильное решение 2ФА для своей ИС

Немного матчасти...

Уровни доверия в ИС

- Низкий
- Средний
- Высокий
 - ГОСТ Р 58833-2020
 - ГОСТ Р 70262.1-2022
 - ГОСТ Р 70262.2-202х*

Уровень значимости информации в ИС

Высокий

Средний

Низкий

Высокий	Средний	Высокий	Высокий
Средний	Низкий	Средний	Высокий
Низкий	Низкий	Низкий	Средний

Низкий

Средний

Высокий

Размер возможного ущерба в случае утечки, инцидента

- Какая у вас ИС? ГИС, КИИ?
- Какой уровень доверия нужен?
 - Новые Требования 17го Приказа ФСТЭК

ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ

- Гос. организации
- Федеральные структуры
- Организации КИИ
- Крупный и ср. бизнес
- Операторы ИСПДн (уголовная и административная ответственность, оборотные штрафы)

Здесь важнее не доверие, а ГАРАНТИИ

Из цитаты В.В. Путина

Как уровень доверия определяет выбор нужного решения

Доверие

- пришло из ISO 15408



Как выбрать правильное решение 2ФА для своей ИС

Уровень значимости информации в ИС

Требования к аутентификации в ИС

- ГОСТ Р 58833-2020
- ГОСТ Р 70262.1-2022
- ГОСТ Р 70262.2-202х*

Высокий

Средний

Низкий

Высокий	Усиленная	Строгая	Строгая
Средний	Простая	Усиленная	Строгая
Низкий	Простая	Простая	Усиленная

Низкий

Средний

Высокий

Размер возможного ущерба в случае утечки, инцидента



Низкий уровень доверия

Средний уровень доверия

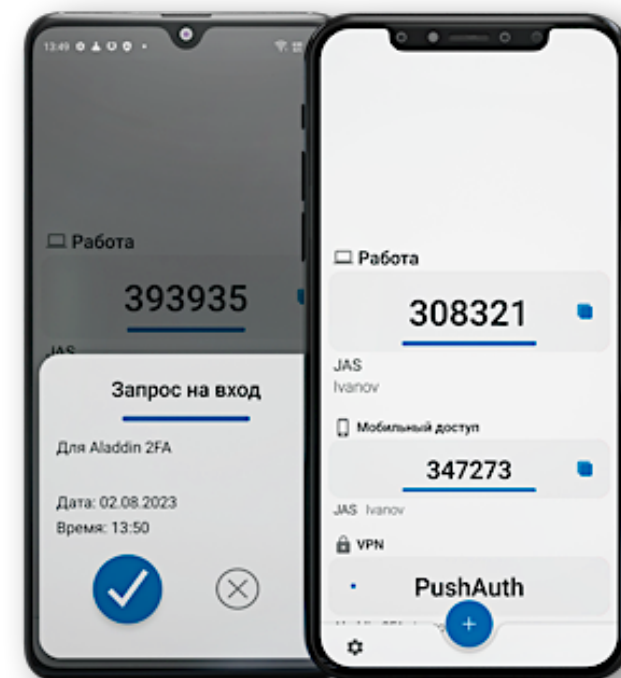
Высокий уровень доверия



Пароли
(однофакторная
односторонняя)



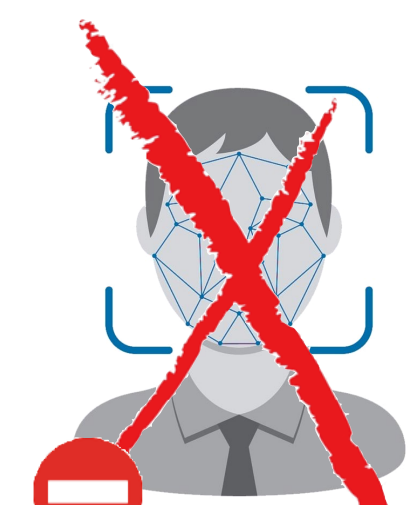
Содержит секрет



PKI-токены



+BIO
для привязки
к личности



Нельзя
Бесконтактная BIO

Усиленная аутентификация (для ИС со средним уровнем доверия)

◆ 2ФА

- Обязательно должен быть **фактор ВЛАДЕНИЯ** (1)
 - Электронный идентификатор (защищённое неклонированное устройство)
 - [Смартфон] + [QR-код, SMS, push, OTP]

✓ Только при работе на компьютере - чтобы было разделение сред

✓ Если работа на смартфоне - это 2х этапная аутентификация (не 2ФА)

- Второй фактор (2) - **ЗНАНИЕ** (PIN-код устройства) или **БИОМЕТРИЯ**

◆ Первичная идентификация *- важно, про неё все забывают*

- **Личная явка** (вручение эл. идентификатора)
- **Допускается удалённая**, но с обязательным использованием доп. атрибутов идентификации
 - [Смартфон] + [QR-код, SMS, push, OTP] и/или [Биометрия (лицо, голос)]
 - Должна быть **безопасная передача общего секрета** (нет практически ни у кого)

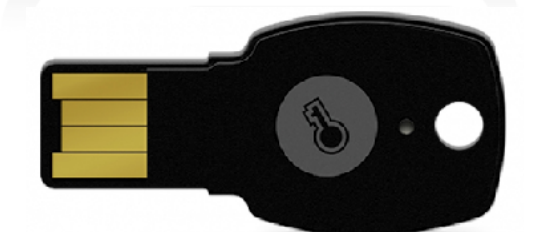
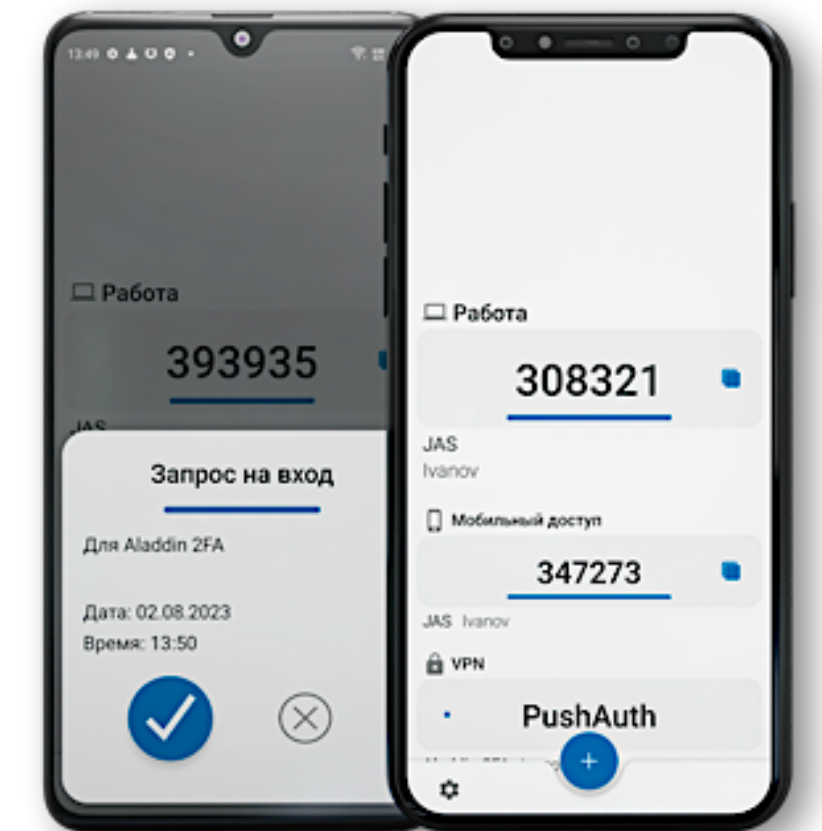
◆ Необходимые компоненты

- **Сервер аутентификации**
 - Важно: база данных с ключами, профилями и аутентификационной информацией должна быть надёжно защищена с помощью СКЗИ (нет практически ни у кого)
- **Клиентское ПО** (приложение)
- **Система централизованного управления ЖЦ**
- **Эл. идентификаторы** / смартфон пользователя



Аутентификация

- это подтверждение идентификационных данных



Строгая аутентификация (для ИС с высоким уровнем доверия)

◆ 2ФА/3ФА

- Обязательно должен быть **фактор ВЛАДЕНИЯ**

- Неклонированное устройство с аппаратной реализацией асимметричной криптографии (RSA, ECDSA, ГОСТ/ЭП) и поддержкой PKI
- Незвлекаемый закрытый ключ

- Второй фактор - **ЗНАНИЕ** (PIN-код устройства) и/или **БИОМЕТРИЯ** (2ФА/3ФА)

◆ Первичная идентификация

- **Личная явка** с подтверждением личности

- Проверка идентификационных данных, официальных подтверждений
- Вручение аппаратного токена
- Выпуск цифрового сертификата на токен
- [Регистрация отпечатков пальцев на токен - BIO]
- [Выдача специализированного средства с предустановленной замкнутой программной средой для безопасной дистанционной работы]

✓ **ВАЖНО: необходимо фиксировать характеристики среды функционирования, для которой результат будет признаваться правильным (достоверным)**

✓ **Для разных сред и условий** (например, работа на удалёнке, из новых регионов, из-за границы) **должен быть определён разный набор факторов и дополнительных атрибутов** (больше рисков - больше дополнительных атрибутов и компенсационных мер) - **адаптивная МФА**

◆ Необходимые компоненты

- Развёрнутый корпоративный **PKI** (основа для обеспечения высокого доверия в ИТ/ИС)

Secure Element



"Ноутбуко-заменитель"

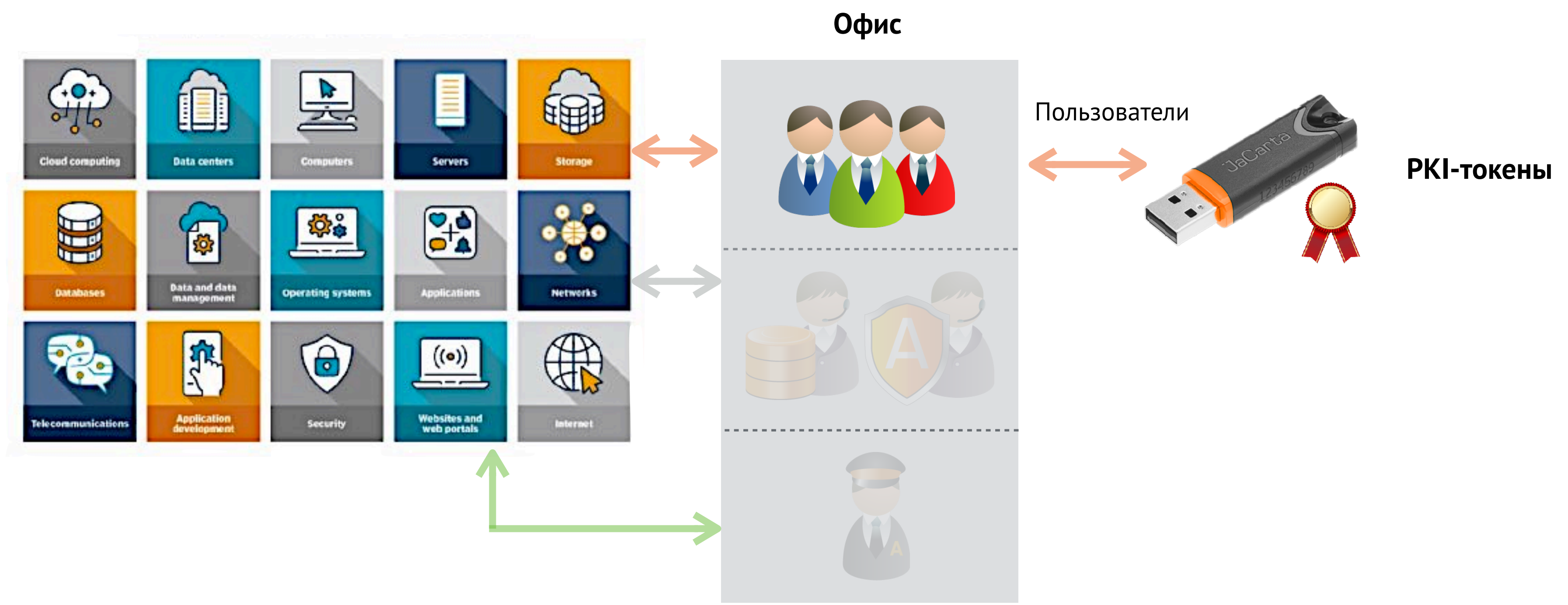
- терминальный клиент + VPN + RDP/VDI
- безопасная работа из недоверенной среды

Адаптивная МФА

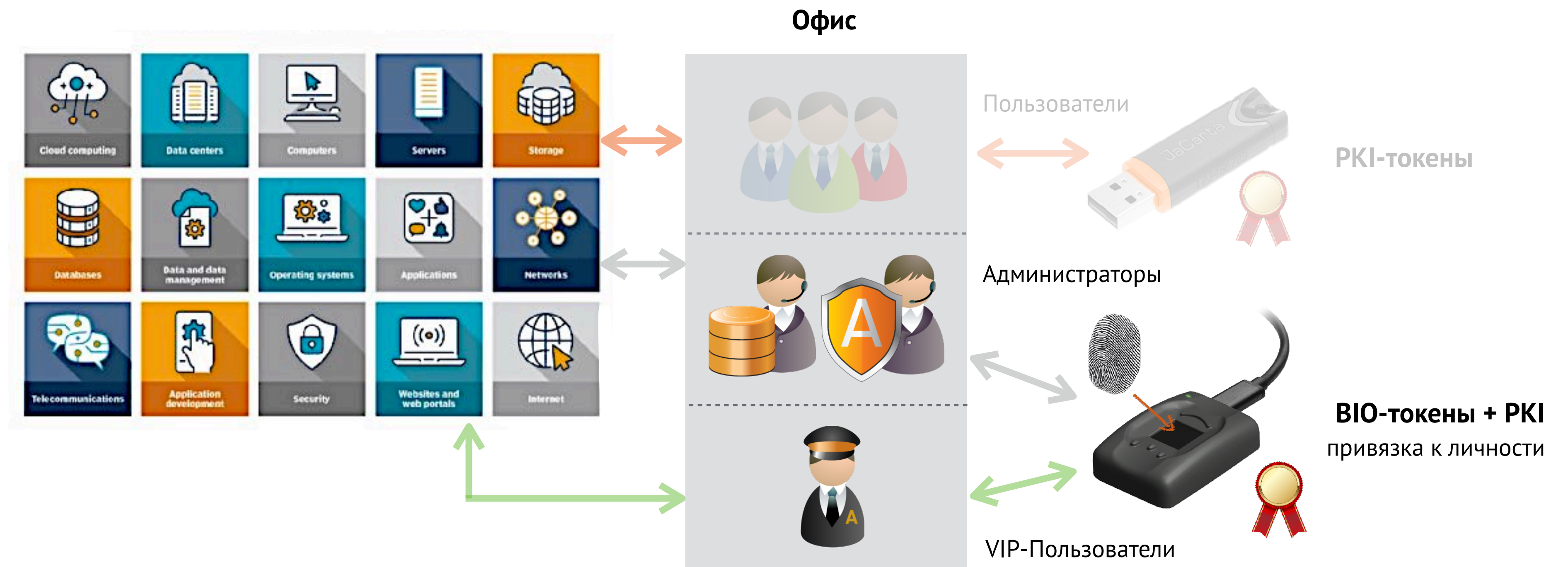
Для разных сред функционирования, условий работы, сегментов ИС должен быть определён РАЗНЫЙ набор факторов и дополнительных атрибутов для подтверждения идентификационных данных и их связи с личностью пользователя

Больше рисков - больше дополнительных атрибутов и компенсационных мер

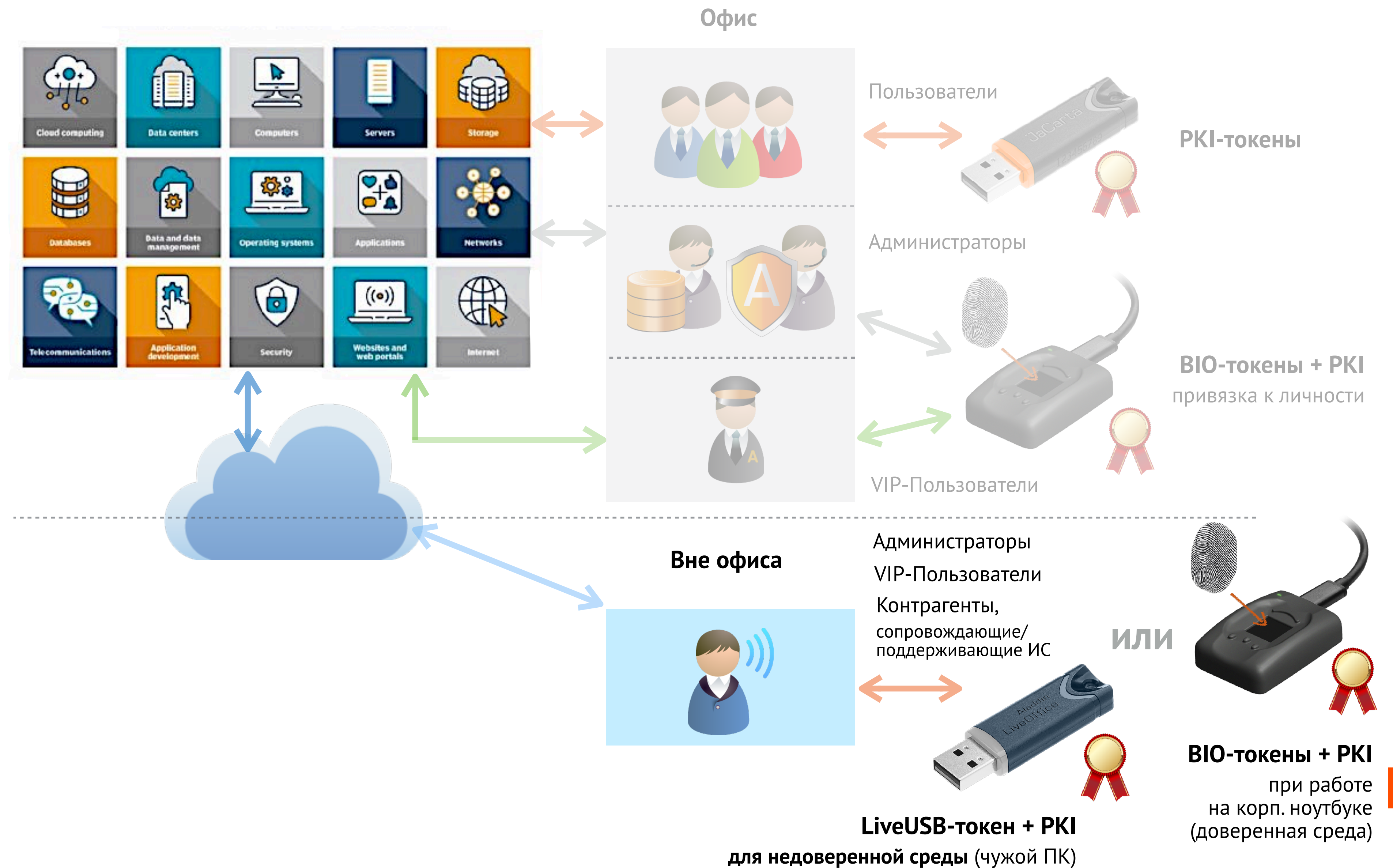
Адаптивная МФА в ИС



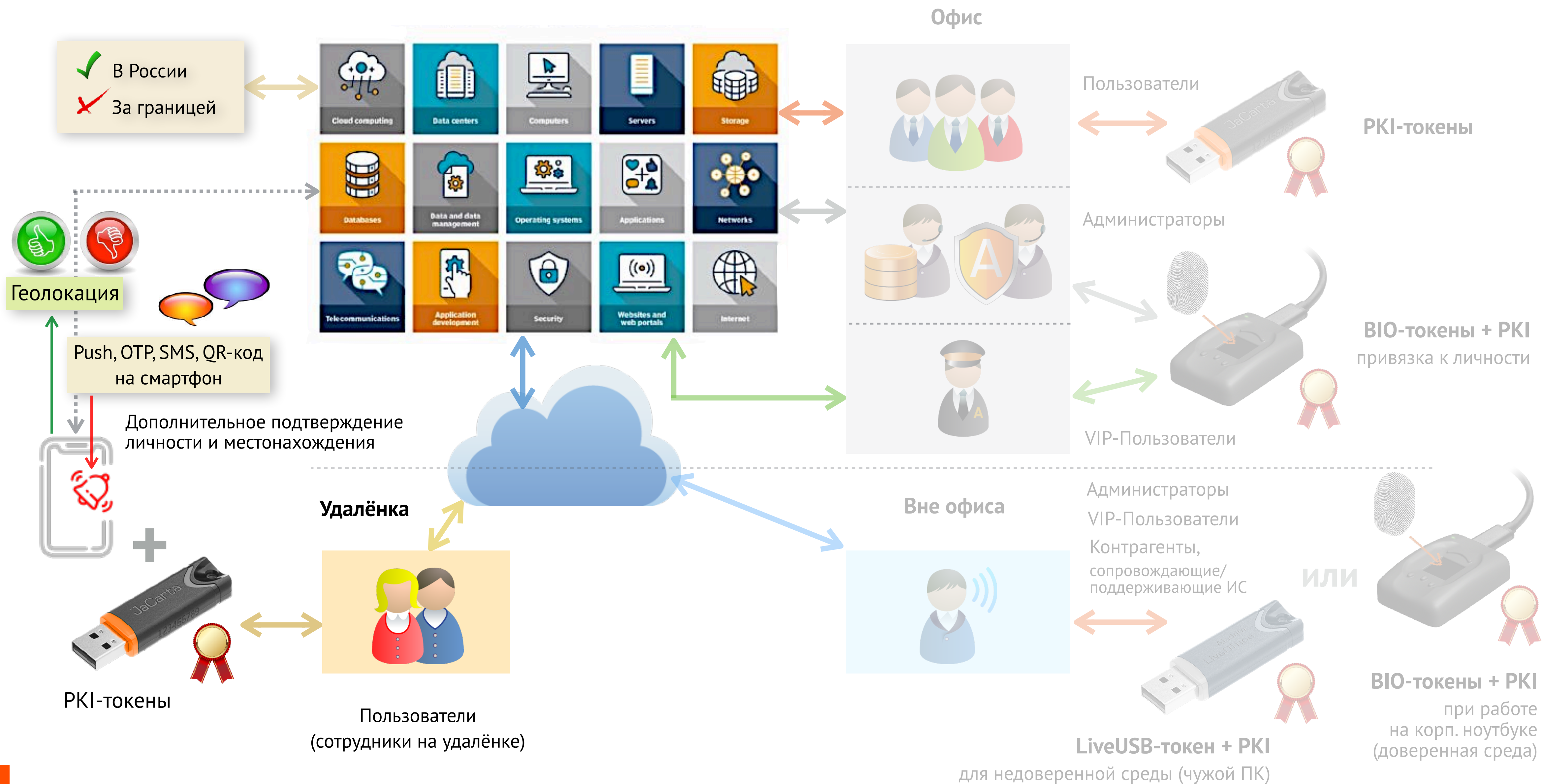
Адаптивная МФА в ИС



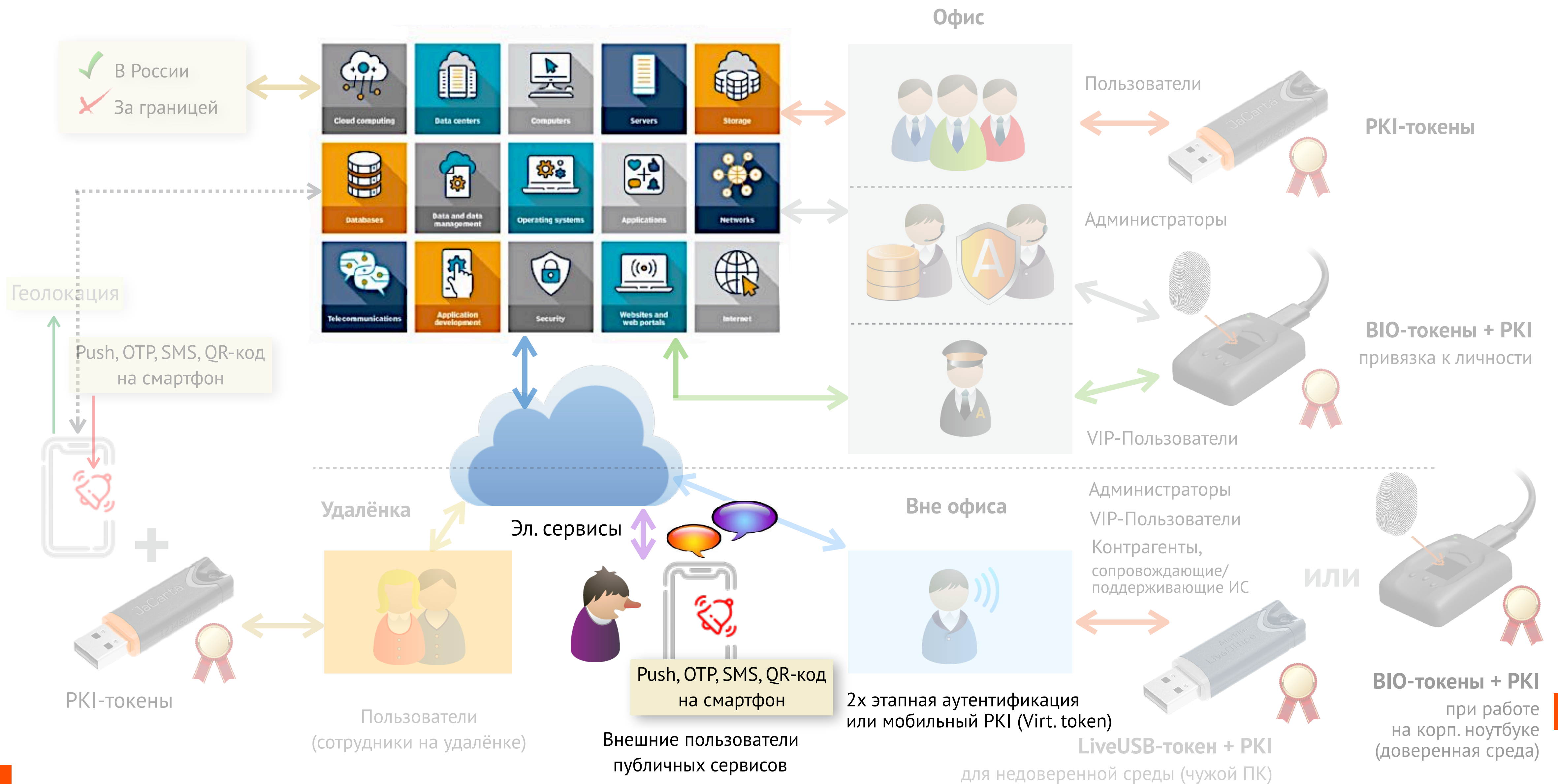
Адаптивная МФА в ИС



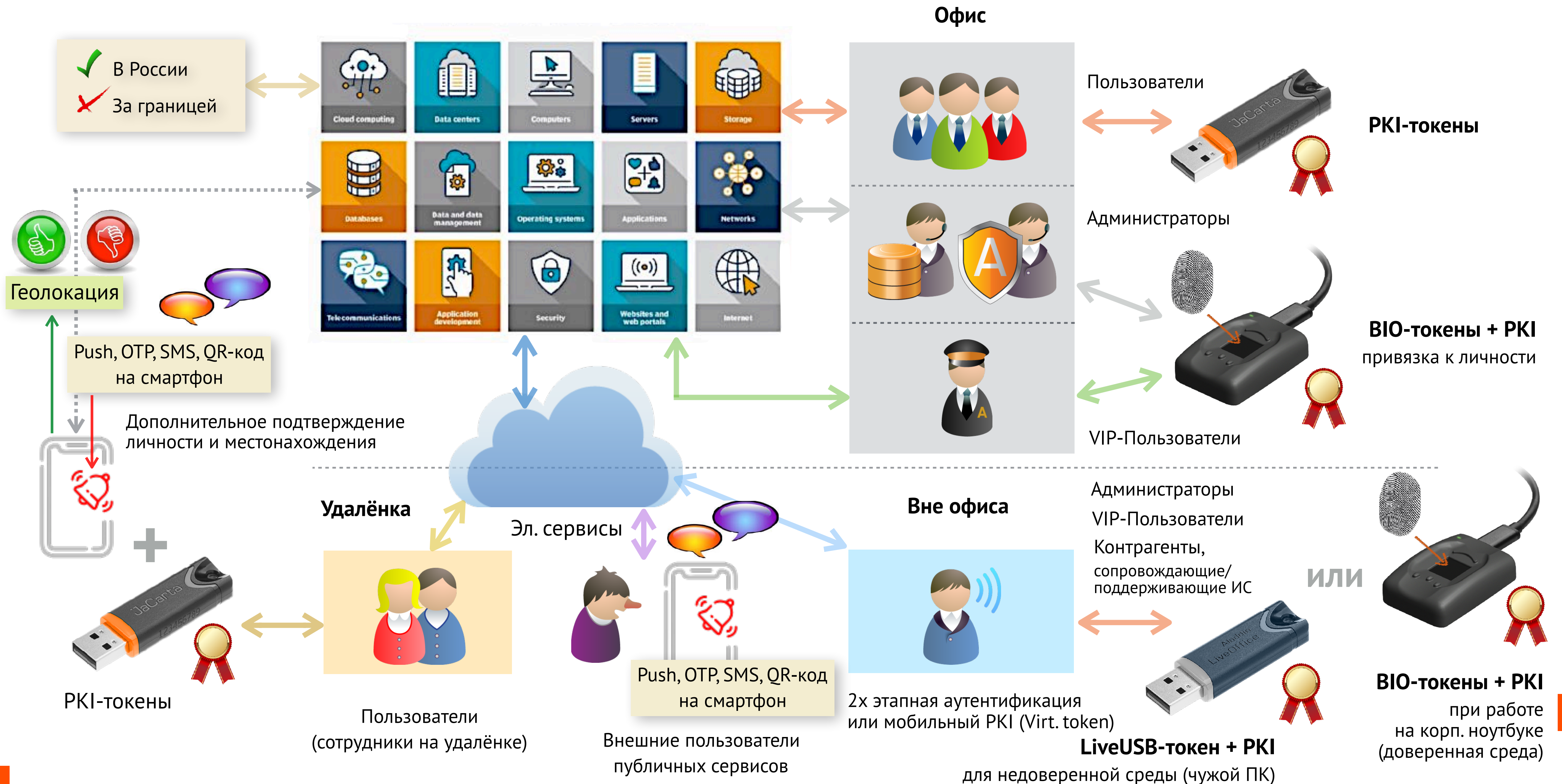
Адаптивная МФА в ИС



Адаптивная МФА в ИС



Адаптивная МФА в ИС



Что нужно
для внедрения строгой и адаптивной 2ФА/3ФА в ИС

Что нужно для внедрения строгой аутентификации в ИС

В экосистеме Windows

◆ Корп. центр сертификации

- MS CA (CS), входит в состав MS Windows Server
- ✓ **Отвечает за выпуск и валидацию сертификатов**

◆ Служба каталога/контроллер домена

- MS Active Directory (AD)
- ✓ **Отвечает за доменную аутентификацию**

◆ Клиент PKI и 2ФА

- MS Windows Smart Card Logon
- ✓ **Отвечает за аутентификацию пользователей**

◆ PKI-токены, смарт-карты, BIO-токены

◆ Система централизованного управления ЖЦ токенов и сертификатов



- Все необходимые компоненты для построения корпоративной PKI **встроены** в MS Windows
- MS CA выпускает и обслуживает
 - машинные сертификаты (для аутентификации оборудования в ИТ-инфраструктуре)
 - программные сертификаты (code signing)
 - пользовательские сертификаты



- Для внедрения строгой 2ФА пользователей достаточно приобрести
 - средства 2ФА
 - систему централизованного управления ЖЦ токенов и сертификатов

Что нужно для внедрения строгой аутентификации в ИС

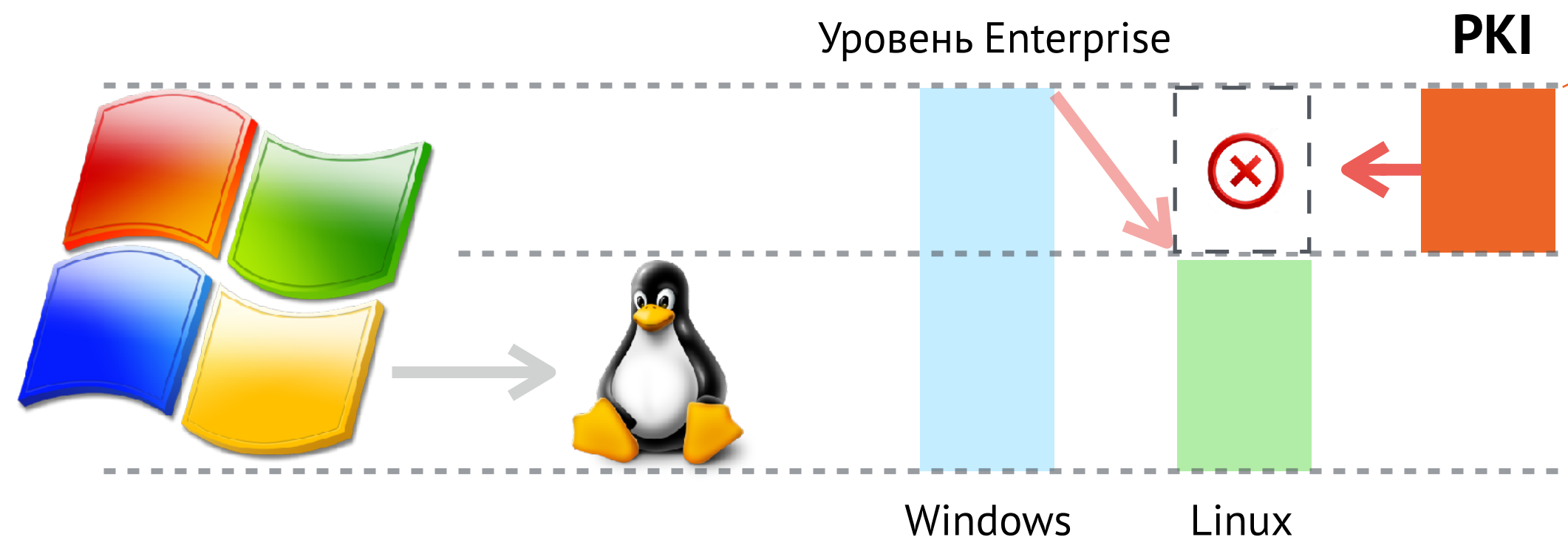
Импортозамещение

- Возможна ли полноценная миграция на Linux без кардинального снижения безопасности в ИС?
- Возможна ли бесшовная миграция на Linux?

- **В составе Linux нет полноценного PKI Enterprise-уровня**

- **Нельзя обеспечить строгую аутентификацию** (по сертификатам)
 - оборудования
 - ПО
 - пользователей

- Чтобы подняться до уровня **Enterprise** и обеспечить такой же уровень безопасности и управляемости как в Windows, **необходимо внедрить полноценный PKI**



Что нужно для внедрения строгой аутентификации в ИС

Импортозамещение

- Возможна ли полноценная миграция на Linux без кардинального снижения безопасности в ИС?
- Возможна ли бесшовная миграция на Linux?

- В составе Linux нет полноценного PKI Enterprise-уровня

- **Нельзя обеспечить строгую аутентификацию** (по сертификатам)
 - оборудования
 - ПО
 - пользователей

В экосистеме отечественных ОС (Linux)

◆ **Корп. центр сертификации (CA)**



◆ **Служба каталога/контроллер домена**
- ALD Pro, РЭД АДМ, Альт Домен



◆ **Клиент PKI (полный стек PKI)**



◆ **Клиент 2ФА/3ФА**



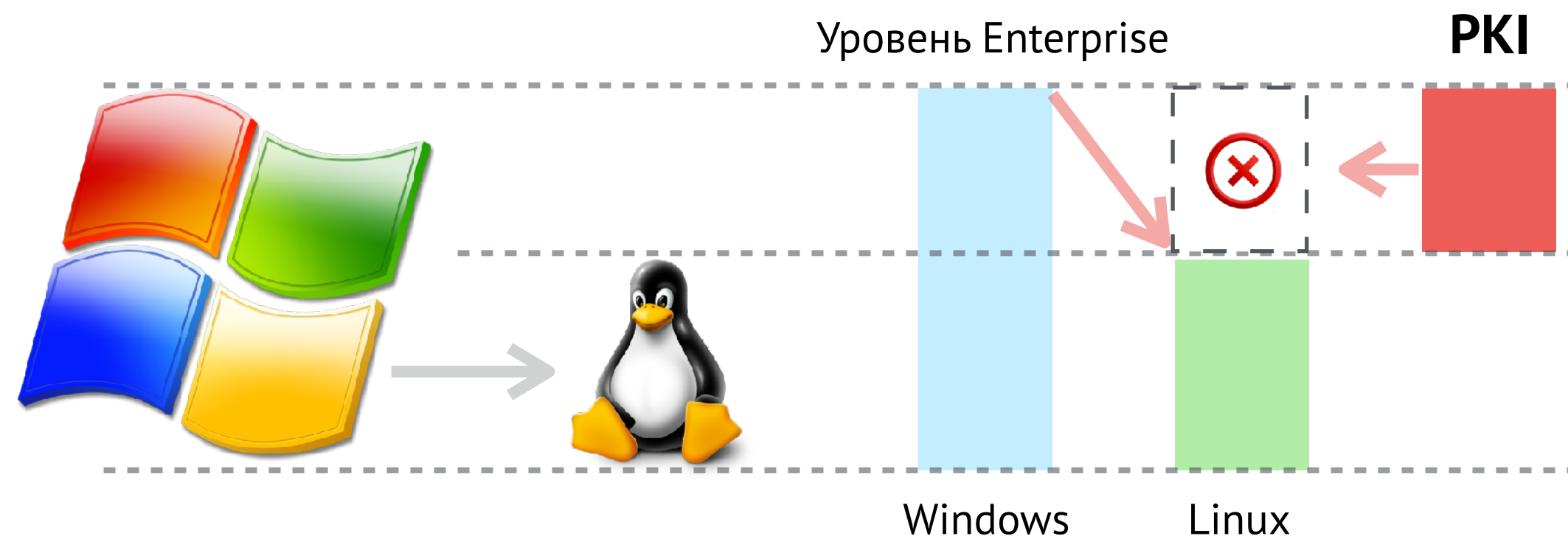
◆ **PKI-токены, смарт-карты, BIO-токены**



◆ **Система централизованного управления ЖЦ токенов и сертификатов**



Аладдин



Что нужно для внедрения строгой аутентификации в ИС

В экосистеме Windows

Бесшовная миграция и работа в двух экосистемах

В экосистеме отечественных ОС (Linux)

◆ Корп. центр сертификации

- MS CA (CS), входит в состав MS Windows Server

Aladdin eCA

◆ Корп. центр сертификации (CA)

◆ Служба каталога/контроллер домена

- MS Active Directory (AD)

◆ Служба каталога/контроллер домена

- ALD Pro, РЭД АДМ, Альт Домен

◆ Клиент PKI и 2ФА

- MS Windows Smart Card Logon

Aladdin SecurLogon

◆ Клиент PKI (полный стек PKI)

◆ Клиент 2ФА/3ФА

◆ PKI-токены, смарт-карты, BIO-токены

JaCarta-3 PKI/ГОСТ
JaCarta Virtual Token
JaCarta SecurBIO
JaCarta Mobile
Aladdin 2FA + JAS

◆ PKI-токены, смарт-карты, BIO-токены

◆ Система централизованного управления ЖЦ токенов и сертификатов

Aladdin JMS/JAS

◆ Система централизованного управления ЖЦ токенов и сертификатов

+



Ключевые компоненты для

- для построения безопасной доверенной ИТ-инфраструктуры и ИС с **высоким** уровнем доверия и **строгой** 2ФА/3ФА
- для адаптивной МФА

Практически все продукты (далее) спроектированы с учётом требований по безопасности и уровню доверия УД-2 (гостайна "СС"), имеют сертификаты ФСТЭК России по УД-4:

- обеспечивают защиту от действий нарушителей с высоким потенциалом (возможностями)
- могут использоваться для защиты ГИС 1-го класса защищённости, на объектах КИИ
- зарегистрированы в реестрах отечественного ПО и/или ПАКов
- имеют соответствующие сертификаты соответствия ФСБ России или заключения по результатам тематических исследований на входящие в состав продуктов компоненты СКЗИ.

Доверенный корпоративный центр сертификации (CA)

◆ Для замещения MS CA (CS)

- MS CA - **единая точка отказа** для всей ИТ-инфраструктуры

✓ **Отказ (блокирование работы) Центра валидации (и/или корневого ЦС) парализует работу сети уже через сутки**

◆ Обеспечивает

- Создание и функционирование корпоративной инфраструктуры открытых ключей (PKI)
- Объединение всех компонентов ИТ-инфраструктуры в **единый домен безопасности**, их аутентификацию и безопасное взаимодействие

◆ Позволяет

- Бесшовно (без остановки сервисов) полноценно заместить MS CA, работать параллельно с ним (под Linux)
- Переехать на отечественные ОС (Linux) без снижения уровня ИБ и управления
- Построить полноценный PKI в сложной гетерогенной инфраструктуре
- Одновременно работать в двух экосистемах (Windows / Linux)
- Реализовать строгую аутентификацию (по сертификатам)
 - Используемого оборудования (роутеров, маршрутизаторов, межсетевых экранов, VDI, VPN, RDP-шлюзов и пр.)
 - ПО
 - Пользователей
- Одновременно работать с различными службами каталогов (Windows AD, Linux - ALD Pro, РЕД АДМ, Альт Домен и др.)
- Выполнить новые Требования 17-го Приказа ФСТЭК (для ГИС)

- *Владелец ИС обязан иметь собственный Центр сертификации, обеспечить строгую аутентификацию...*

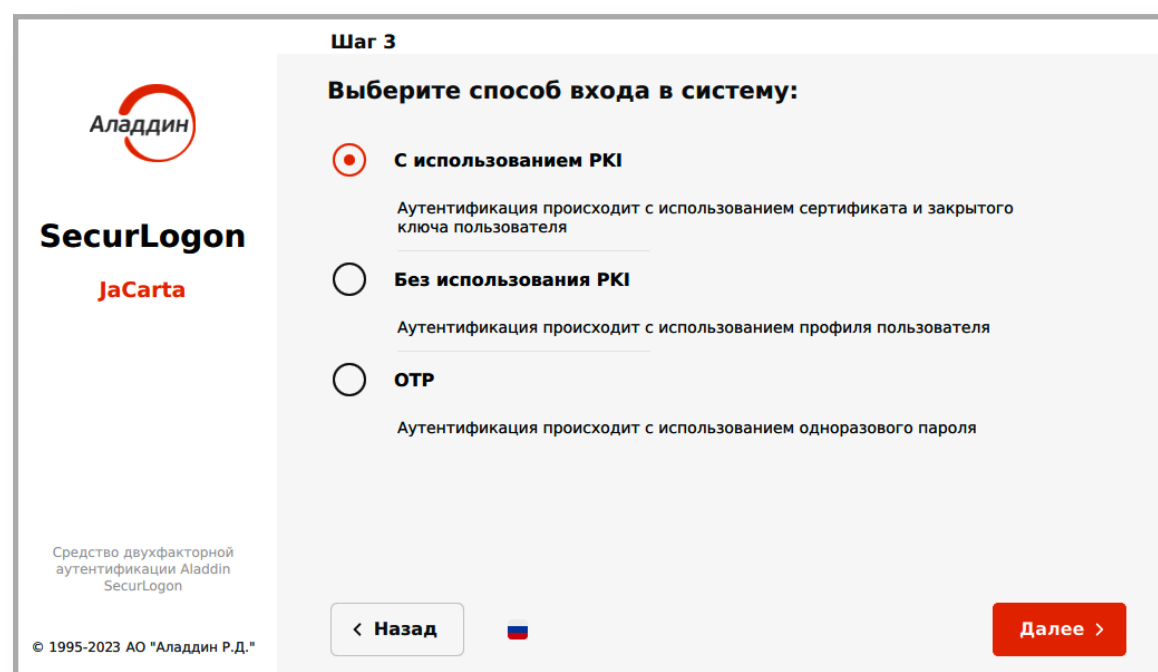
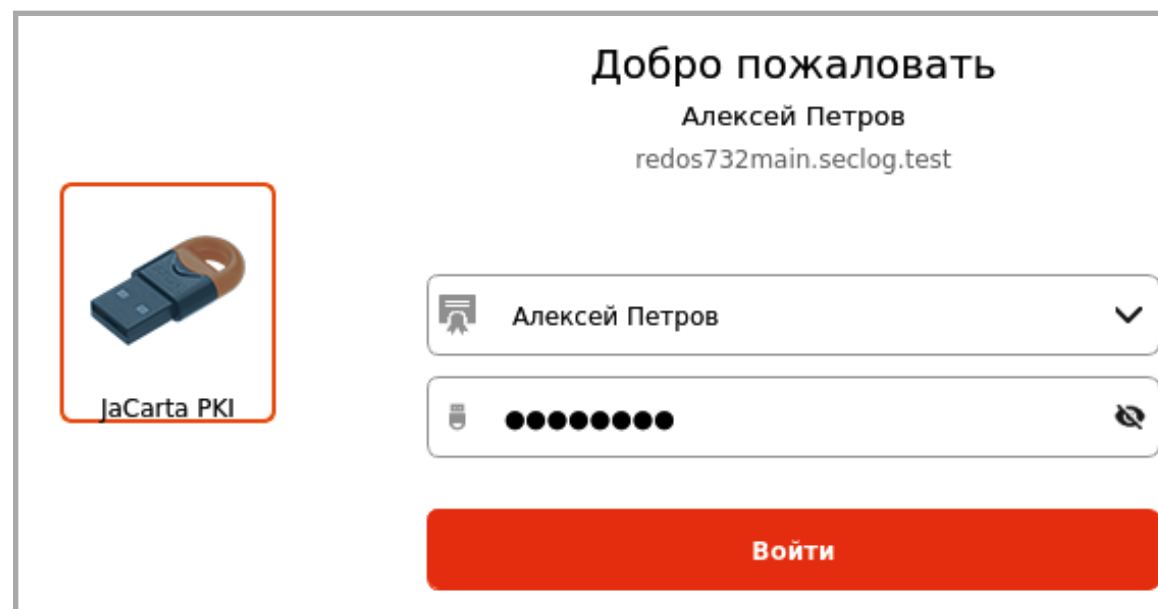


- Сертификат ФСТЭК России
- Заключение ФСБ* России
- В Реестре отечественного ПО

PKI-клиент и поддержка средств МФА в Linux

◆ Обеспечивает

- Полноценную альтернативу Windows Smartcard Logon на Linux в привычном для пользователей интерфейсе
- Усиленную аутентификацию пользователей
 - С использованием автоматически сгенерированного сложного пароля длиной до 63 символов, который **неизвестен пользователю**
- Строгую аутентификацию пользователей
- 2ФА/3ФА
 - Локальную
 - Доменную - в различных службах каталога (**Windows AD**, ALD Pro, РЕД АДМ, Альт Домен, Samba DC, FreeIPA и др.)
- Применение различных групповых политик для 2ФА/3ФА
- Групповое развёртывание
- Удалённое администрирование и настройку с рабочего места администратора
- Защиту удалённых соединений (RDP, SSH)
- Дополнительные сервисные функции, позволяющие до входа в ОС
 - Разблокировать токен
 - Сменить ПИН-код пользователя
 - Кастомизировать окно приветствия и др.



- Сертификат ФСТЭК России
- В Реестре отечественного ПО
- Работает с USB-токенами, ВЮ-токенами, смарт-картами JaCarta, Aladdin LiveOffice



JMS (JaCarta Management System)

Система централизованного управления жизненным циклом сертификатов, токенов, СЗИ, СКЗИ

◆ Обеспечивает

- Учёт и управление жизненным циклом
 - Аппаратных USB-токенов, BIO-токенов, смарт-карт, U2F-токенов, смарт-карт ридеров, BIO-ридеров
 - Программных (виртуальных) токенов, OTP/PUSH/SMS-аутентификаторов
 - Специализированных средств безопасной дистанционной работы (Aladdin LiveOffice)
 - Защищённых съёмных носителей (флеш-накопителей)
 - СЗИ, СКЗИ
 - Цифровых сертификатов доступа и ЭП
 - Объектов PKI, профилей
- Автоматическое взятие под управление средств 2ФА/3ФА
 - Ранее введённых в эксплуатацию (до внедрения JMS)
 - Новых
- Автоматизацию большинства рутинных операций и применения политик безопасности (например, требований к ПИН-кодам)
- Автоматическую рассылку уведомлений
- Быструю подготовку типовых профилей и конфигураций для разных групп пользователей
- Мониторинг и аудит действий пользователей и администраторов
- Удобный сервис самообслуживания пользователей (Web-портал)

◆ Включает

- Высокопроизводительный **сервер аутентификации** Enterprise-класса - JAS для усиленной и адаптивной 2ФА/3ФА



- Сертификаты ФСТЭК и Минобороны (для гостайны до "СС")
- В Реестре отечественного ПО
- Работает с USB-токенами, BIO-токенами, смарт-картами JaCarta, Aladdin LiveOffice

JAS (JaCarta Authentication Server)

Высокопроизводительный сервер аутентификации Enterprise-класса

◆ Обеспечивает

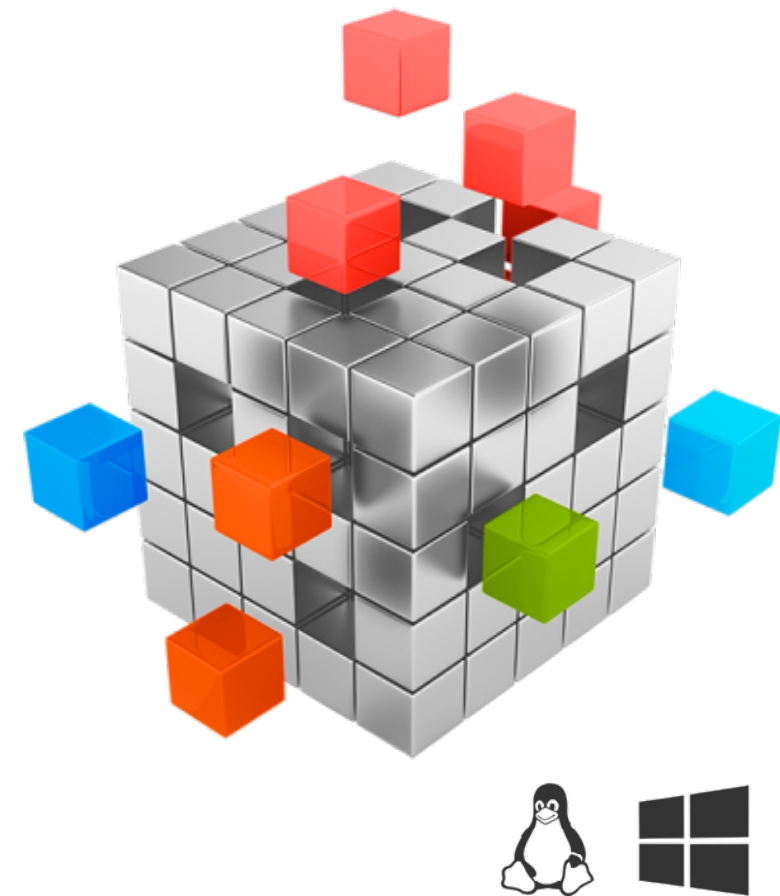
- Усиленную и/или адаптивную (дополнительную) аутентификацию по одноразовым паролям (PUSH/OTP/SMS)
 - Внутренних пользователей ИС на их ПК
 - Внешних пользователей (подрядные организации, получатели информации из ГИС и др.)

при доступе к системам и сервисам:

- Шлюзы удалённого доступа Microsoft, Cisco, Citrix, Palo Alto, Check Point, VMware, Fortinet, NGate и др.
- Шлюз к рабочим столам Microsoft (MS RDG)
- Корпоративные системы (CRM, порталы, электронная почта и т.д.), в т.ч. MS SharePoint, MS Outlook Web App
- Web-приложения, сайты и облачные сервисы
- Системы дистанционного банковского обслуживания (ДБО) и ЭДО
- Высокую производительность (более 1,000 аутентификаций в сек.)

◆ Позволяет

- Использовать **смартфон в качестве второго фактора** при работе на ПК (ВЛАДЕНИЕ)
- Работать с различными приложениями
 - **Aladdin 2FA** (с безопасной передачей общего секрета - QR-код)
 - Яндекс.Ключ
 - Google Authenticator и др.
- Использовать стандартные протоколы
 - RADIUS
 - REST
 - WCF
 - WS-Federation (ADFS)
 - HTTP и SMPP (для интеграции с SMS-шлюзами)



- Сертификат ФСТЭК России
- В Реестре отечественного ПО
- Глубоко интегрирован с JMS (системой централизованного управления ЖЦ токенов)

Аппаратные средства для адаптивной 2ФА/3ФА

USB-токены



С биометрией



Смарт-карты и ридеры



С NFC



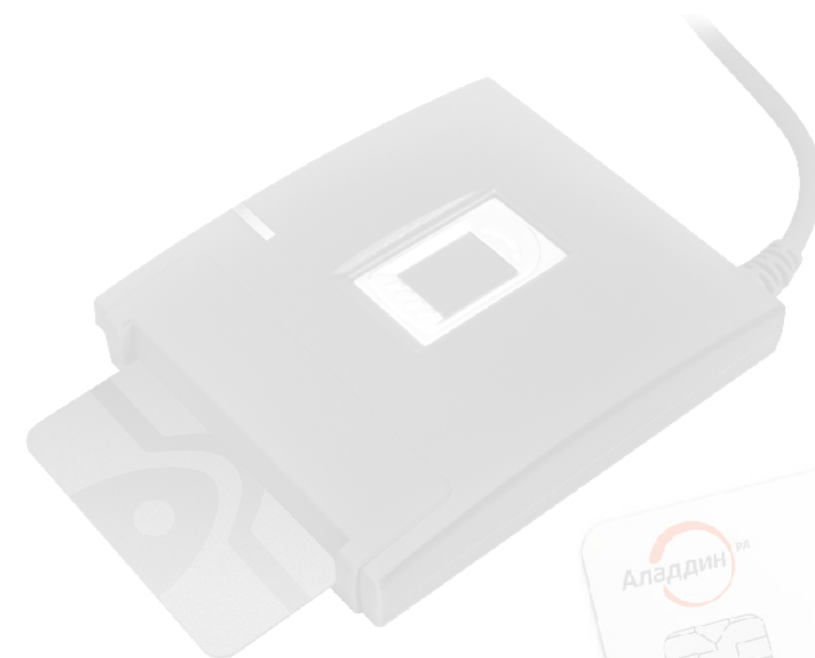
Терминальный клиент



JaCarta-3 PKI/ГОСТ



SecurBIO PKI [ЭП]



JaCarta PKI/ГОСТ/SC + JCR-721

SecurBIO Reader
JCR-781



JaCarta-3 PKI/ГОСТ/NFC

JaCarta PKI/ГОСТ/NFC



SecurRing PKI/ЭП



Aladdin LiveOffice

LiveUSB+OC+VPN+RDP/VDI+PKI+УКЭП

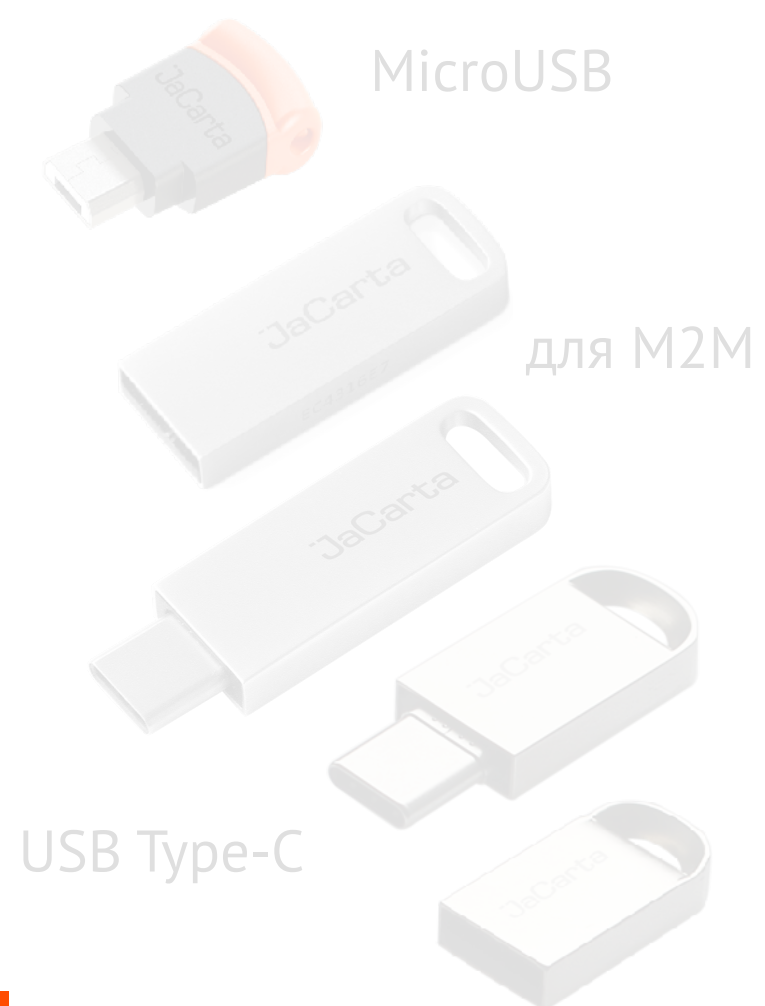


Аппаратные средства для адаптивной 2ФА/3ФА

USB-токены



JaCarta-3 PKI/ГОСТ



С биометрией



SecurBIO PKI [ЭП]



SecurBIO Reader JCR-761



JaCarta PKI/ГОСТ/BIO

Смарт-карты и ридеры



JaCarta PKI/ГОСТ/SC + JCR-721

SecurBIO Reader JCR-781



С NFC



JaCarta-3 PKI/ГОСТ/NFC

JaCarta PKI/ГОСТ/NFC



SecurRing PKI/ЭП



Терминальный клиент



Aladdin LiveOffice

LiveUSB+OC+VPN+RDP/VDI+PKI+УКЭП



Аппаратные средства для адаптивной 2ФА/3ФА

USB-токены



JaCarta-3 PKI/ГОСТ

С биометрией



SecurBIO PKI [ЭП]

Смарт-карты и ридеры



JaCarta PKI/ГОСТ/SC + JCR-721

С NFC

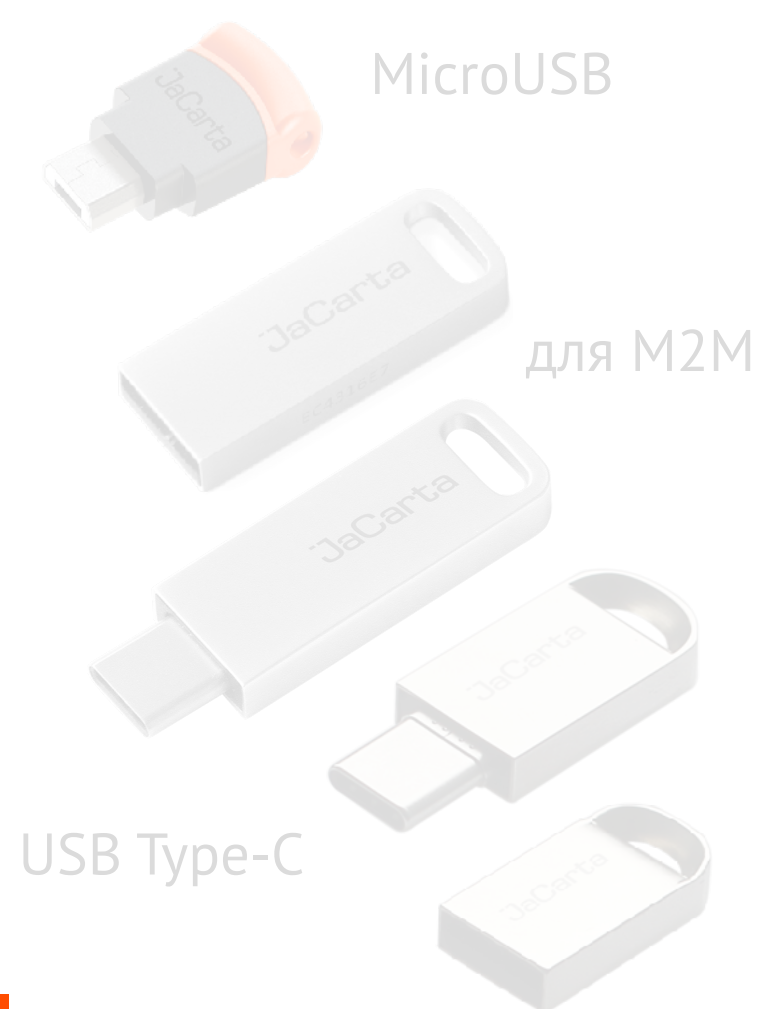


JaCarta-3 PKI/ГОСТ/NFC

Терминальный клиент



Aladdin LiveOffice



USB Type-C



SecurBIO Reader JCR-761

SecurBIO Reader JCR-781



JaCarta PKI/ГОСТ/BIO

JaCarta PKI/ГОСТ/NFC



SecurRing PKI/ЭП



LiveUSB+OC+VPN+RDP/VDI+PKI+УКЭП



Аппаратные средства для адаптивной 2ФА/3ФА

USB-токены



JaCarta-3 PKI/ГОСТ

С биометрией



SecurBIO PKI [ЭП]

Смарт-карты и ридеры



JaCarta PKI/ГОСТ/SC + JCR-721

С NFC

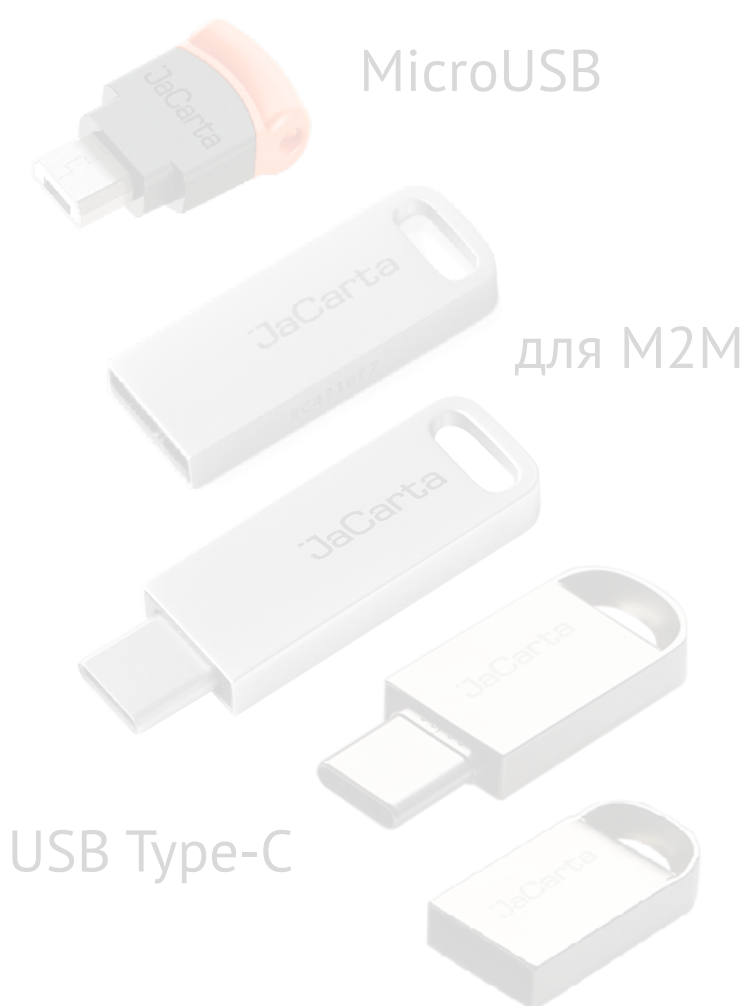


JaCarta-3 PKI/ГОСТ/NFC

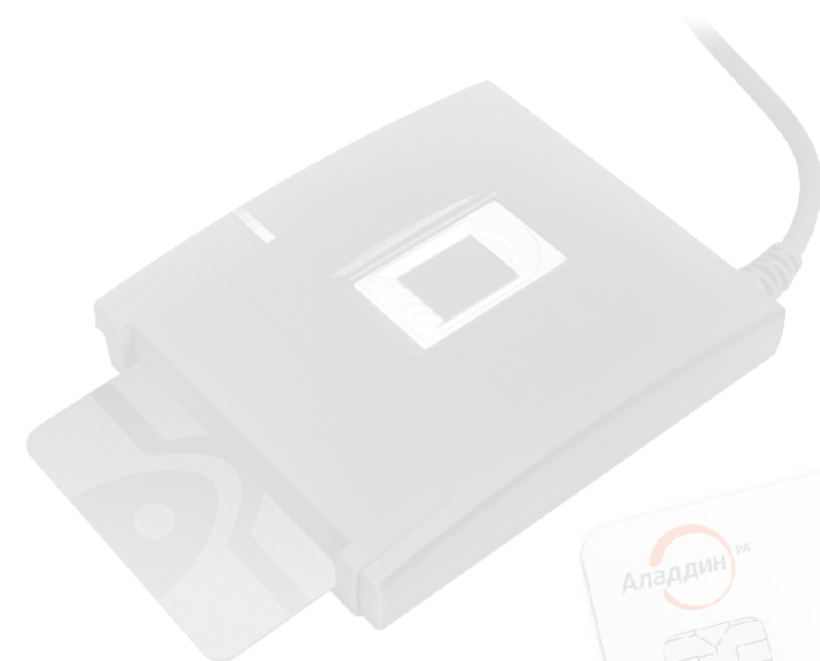
Терминальный клиент



Aladdin LiveOffice



USB Type-C



SecurBIO Reader JCR-761

SecurBIO Reader JCR-781



JaCarta PKI/ГОСТ/BIO

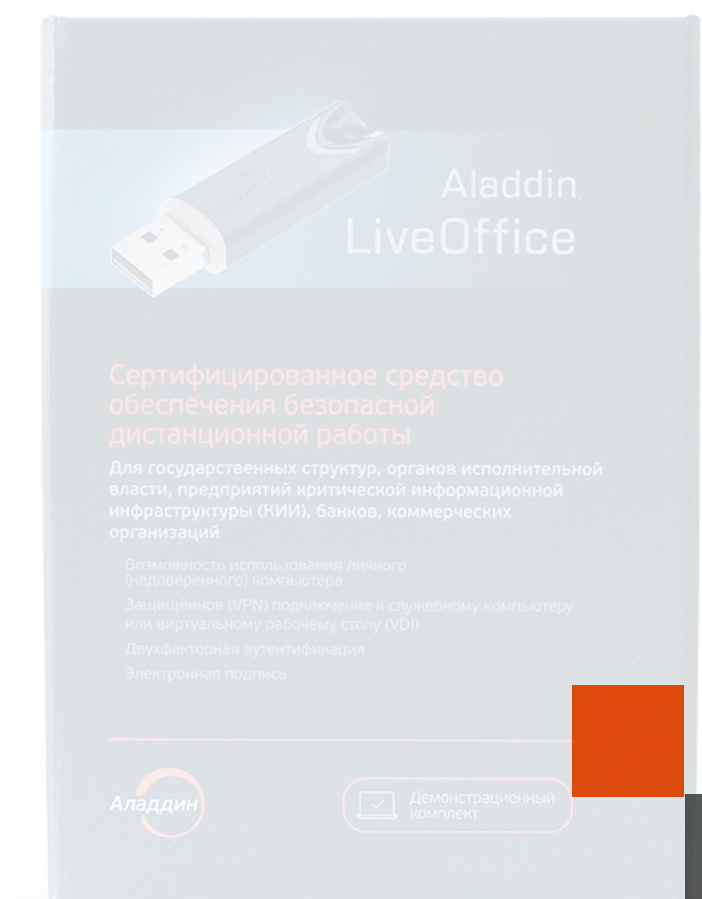
JaCarta PKI/ГОСТ/NFC



SecurRing PKI/ЭП



LiveUSB+OC+VPN+RDP/VDI+PKI+УКЭП



Аппаратные средства для адаптивной 2ФА/3ФА

USB-токены



JaCarta-3 PKI/ГОСТ

С биометрией



SecurBIO PKI [ЭП]

Смарт-карты и ридеры



JaCarta PKI/ГОСТ/SC + JCR-721

С NFC

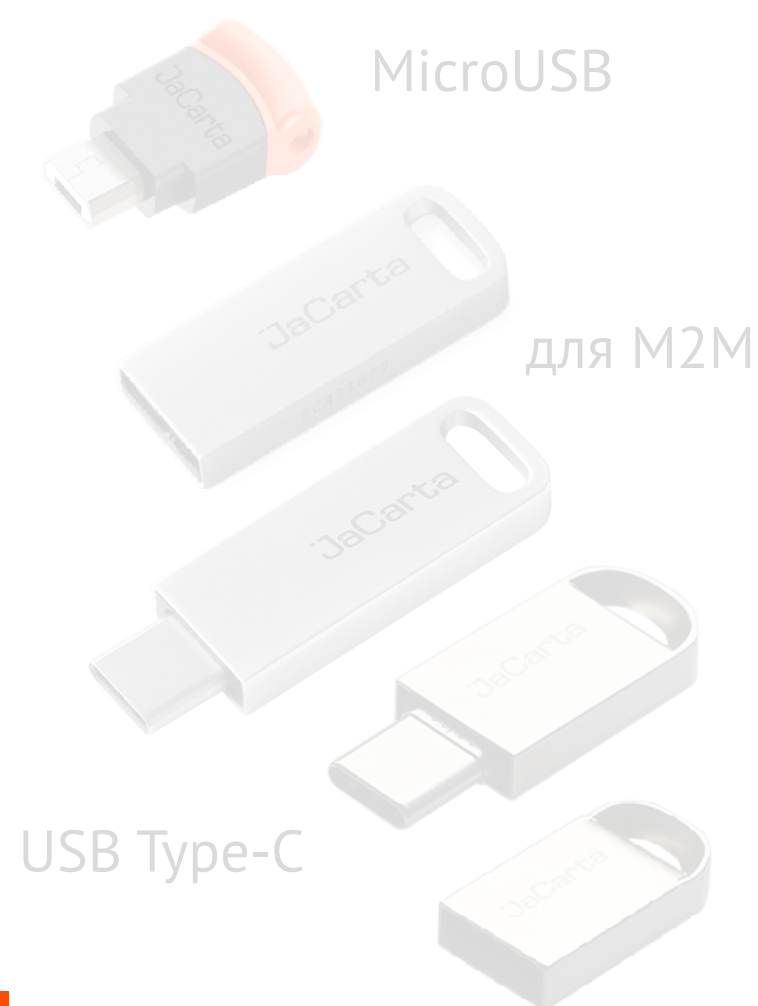


JaCarta-3 PKI/ГОСТ/NFC

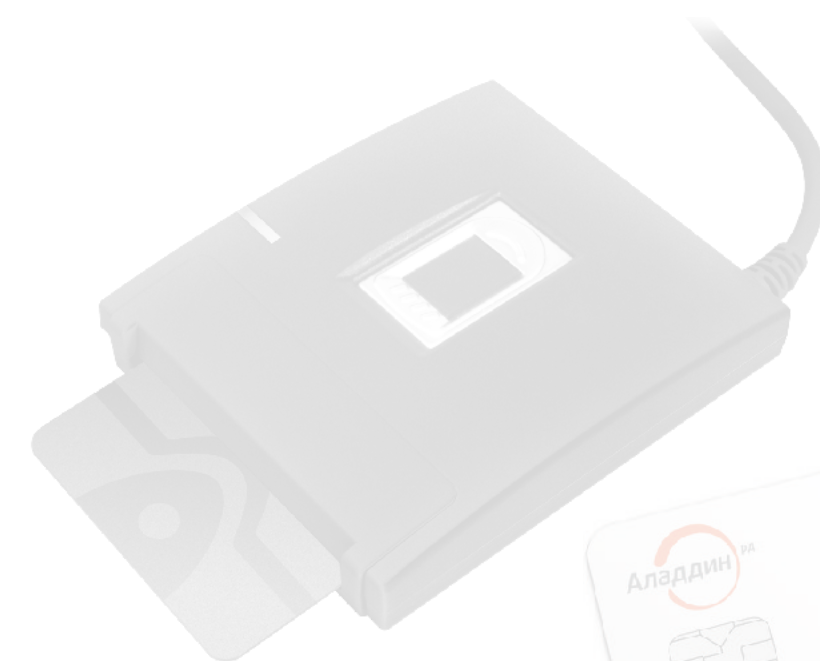
Терминальный клиент



Aladdin LiveOffice



USB Type-C



SecurBIO Reader JCR-761

SecurBIO Reader JCR-781



JaCarta PKI/ГОСТ/BIO



JaCarta PKI/ГОСТ/NFC



SecurRing PKI/ЭП



LiveUSB+OC+VPN+RDP/VDI+PKI+УКЭП



Аппаратные средства для адаптивной 2ФА/3ФА

USB-токены



JaCarta-3 PKI/ГОСТ



С биометрией



SecurBIO PKI [ЭП]



SecurBIO Reader JCR-761

Смарт-карты и ридеры



JaCarta PKI/ГОСТ/SC + JCR-721

SecurBIO Reader JCR-781



JaCarta PKI/ГОСТ/BIO



С NFC



JaCarta-3 PKI/ГОСТ/NFC

JaCarta PKI/ГОСТ/NFC



SecurRing PKI/ЭП



Терминальный клиент



Aladdin LiveOffice

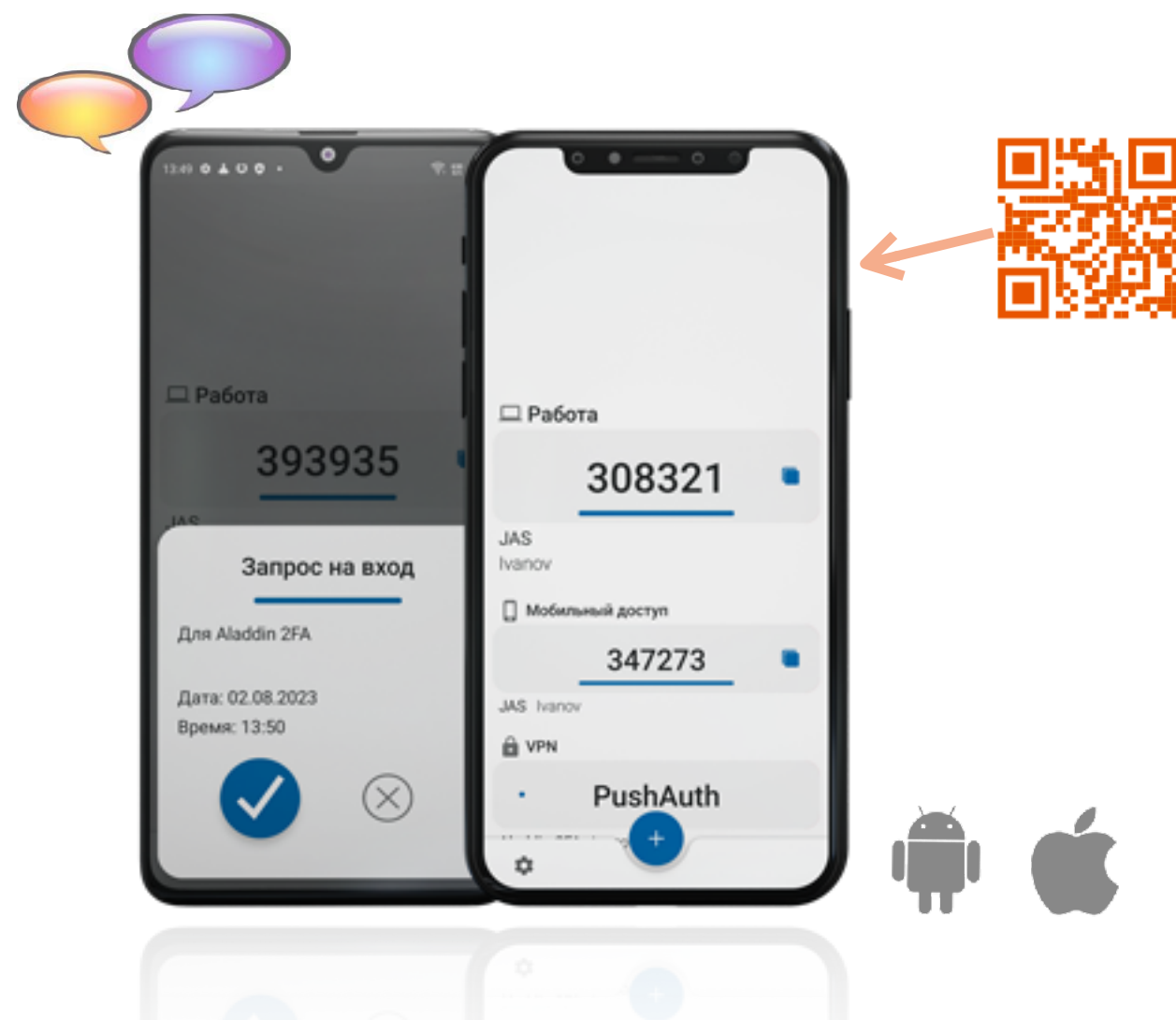
LiveUSB+OC+VPN+RDP/VDI+PKI+УКЭП



Aladdin 2FA

Мобильное приложение

- Обеспечивает
 - Аутентификацию пользователя с использованием OTP/Push
- Позволяет
 - Использовать смартфон в качестве второго фактора при работе на ПК
 - Выпускать неклонировемые аутентификаторы (важно!)
 - Безопасно получить вектор инициализации с помощью одноразового QR-кода
 - Получать и передавать в ИС геолокацию

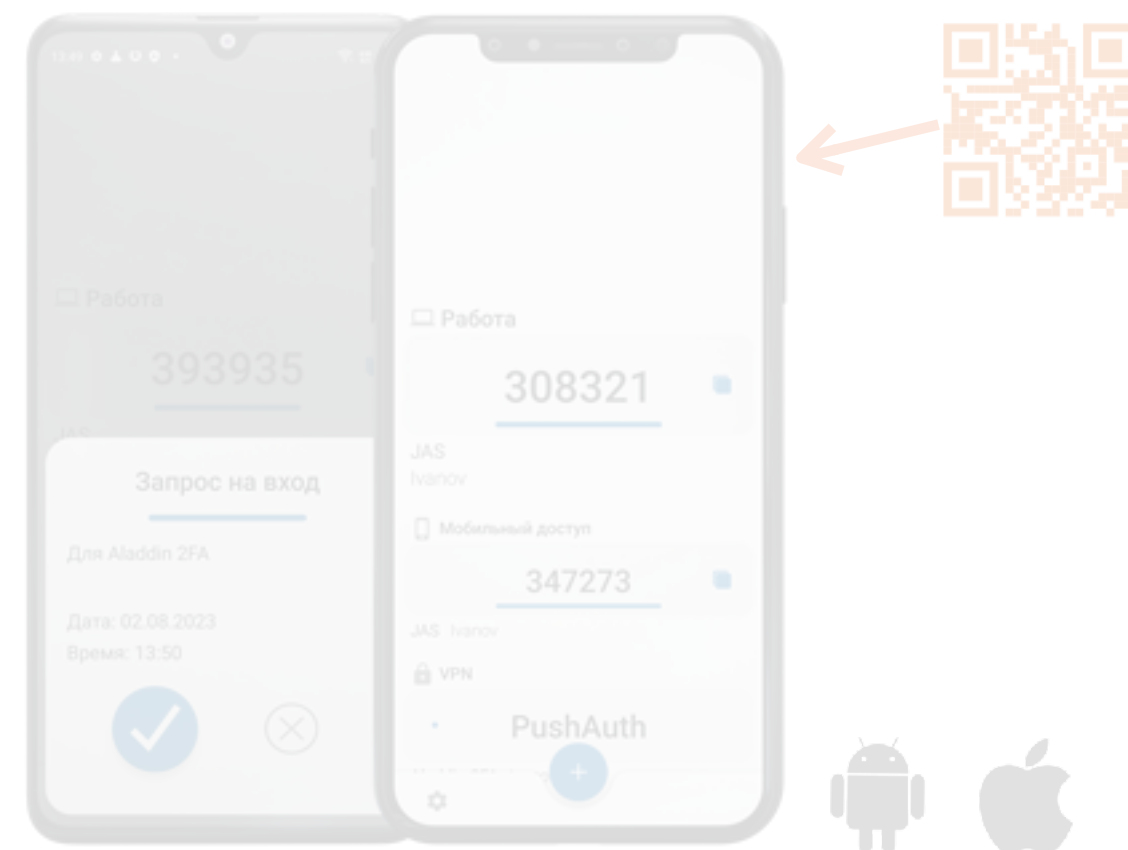


Программные средства для 2ФА/3ФА и адаптивной аутентификации

Aladdin 2FA

Мобильное приложение

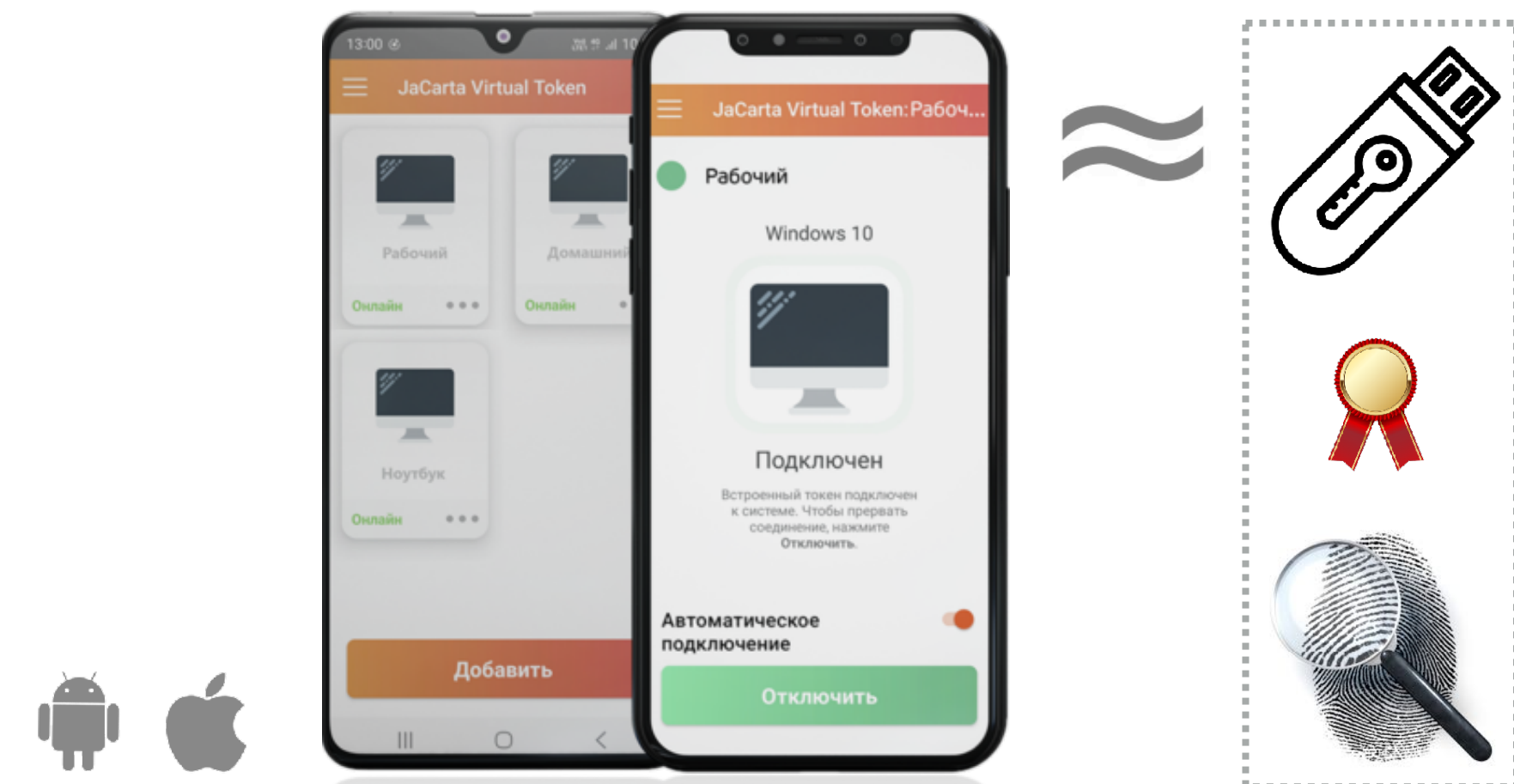
- Обеспечивает
 - Аутентификацию пользователя с использованием OTP/Push
- Позволяет
 - Использовать смартфон в качестве второго фактора при работе на ПК
 - Выпускать неклонироваемые аутентификаторы (важно!)
 - Безопасно получить вектор инициализации с помощью одноразового QR-кода
 - Получать и передавать в ИС геолокацию



JaCarta Virtual Token

Мобильное приложение

- Обеспечивает
 - Функциональность аппаратного токена JaCarta PKI
 - Строгую 2ФА пользователя по цифровым сертификатам (не для ГИС)
- Позволяет
 - Использовать смартфон в качестве второго фактора при работе на ПК (в т.ч. без Интернета)
 - Моментально получить дубликат USB-токена при его блокировании/утере (Rescue-token)
 - Быстро выдавать VT подрядчикам и контрагентам

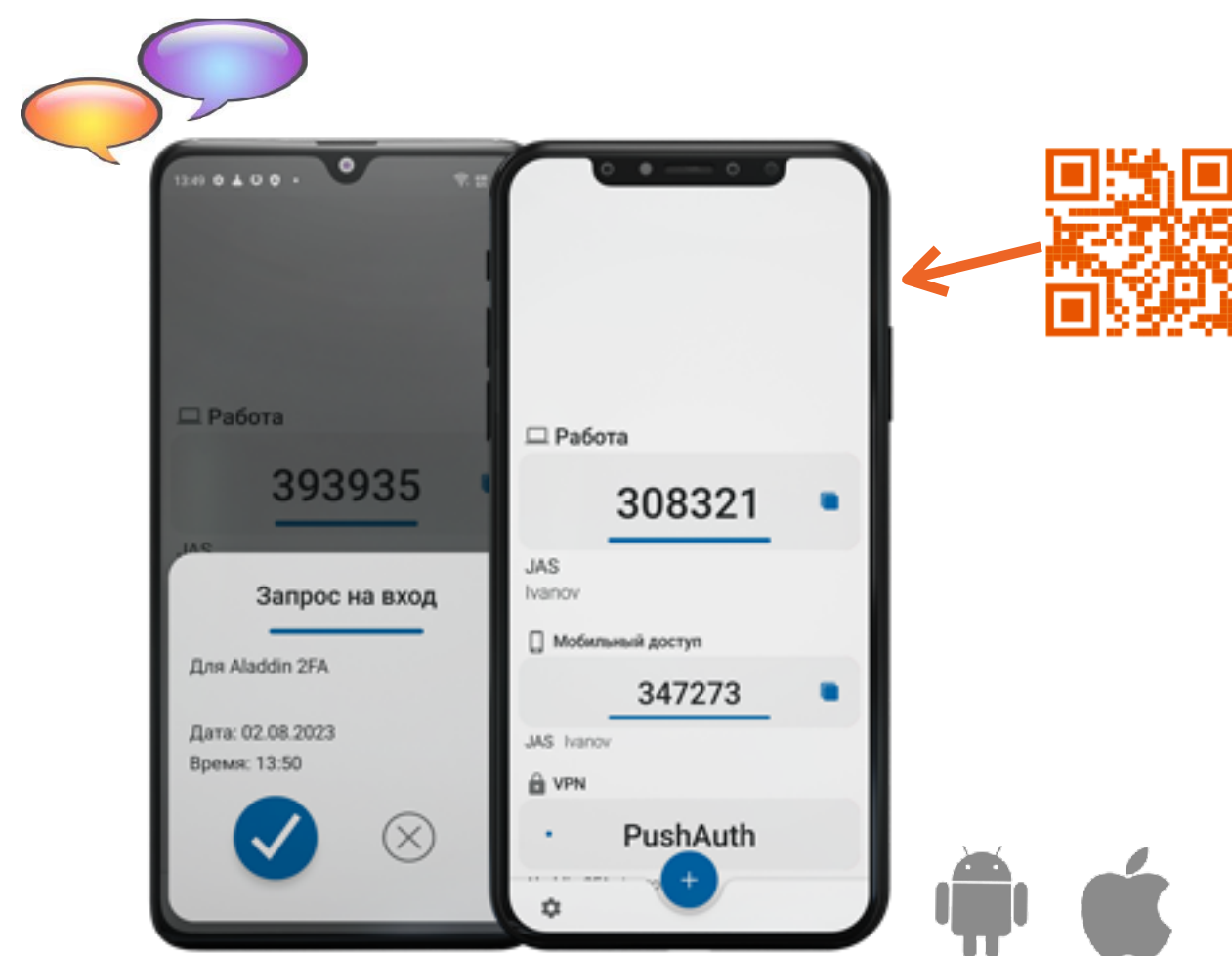


Программные средства для 2ФА/3ФА и адаптивной аутентификации

Aladdin 2FA

Мобильное приложение

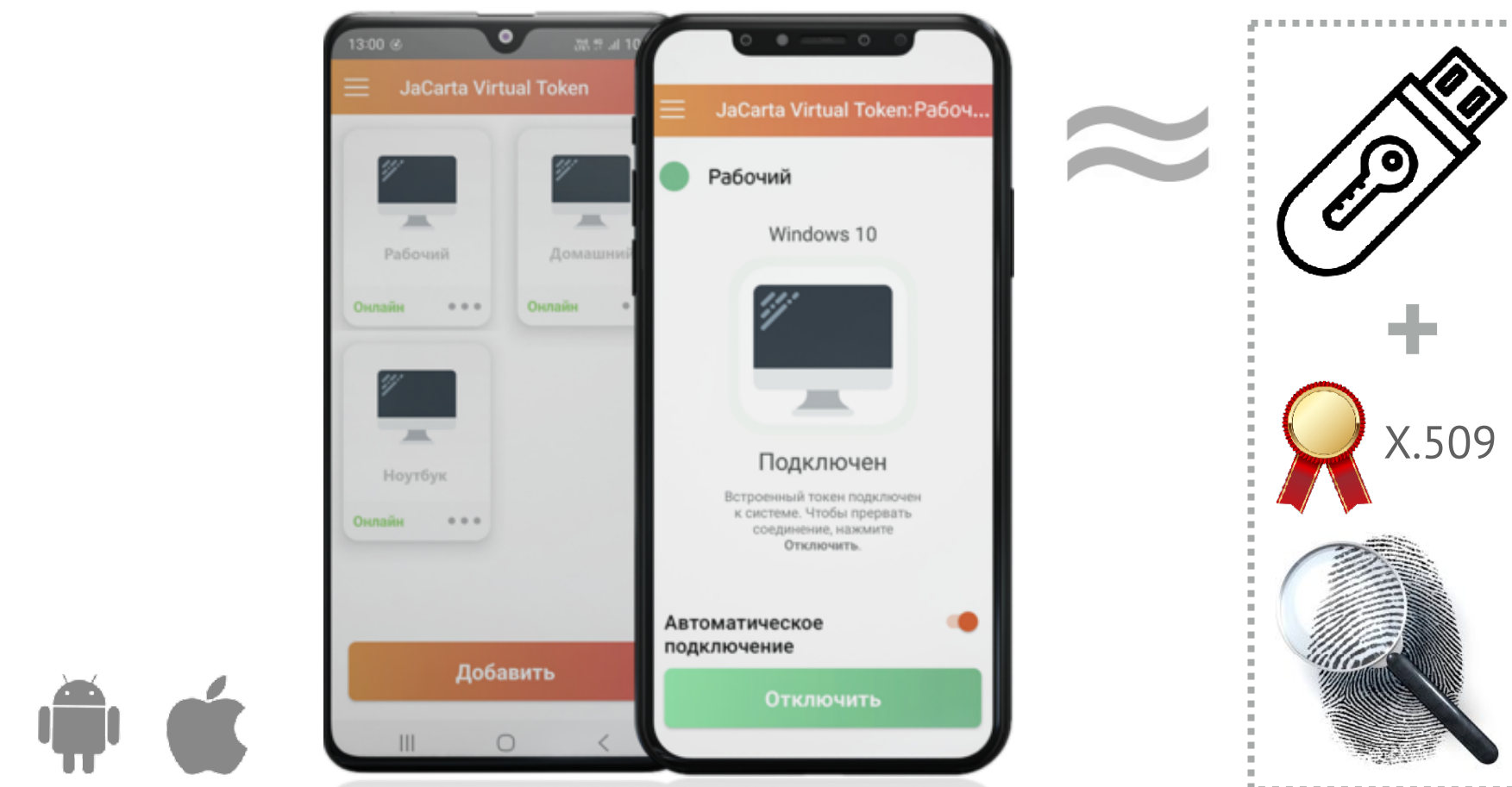
- Обеспечивает
 - Аутентификацию пользователя с использованием OTP/Push
- Позволяет
 - Использовать смартфон в качестве второго фактора при работе на ПК
 - Выпускать неклонлируемые аутентификаторы (важно!)
 - Безопасно получить вектор инициализации с помощью одноразового QR-кода
 - Получать и передавать в ИС геолокацию



JaCarta Virtual Token

Мобильное приложение

- Обеспечивает
 - Функциональность аппаратного токена JaCarta PKI
 - Строгую 2ФА пользователя по цифровым сертификатам (не для ГИС)
- Позволяет
 - Использовать смартфон в качестве второго фактора при работе на ПК (в т.ч. без Интернета)
 - Моментально получить дубликат USB-токена при его блокировании/утере (Rescue-token)
 - Быстро выдавать VT подрядчикам и контрагентам



Правильная подсистема аутентификации в ИС - залог её безопасности



Скачать презентацию

Сергей Груздев

ген. директор
АО "Аладдин"

www.aladdin.ru

Приглашаем на вебинар

- 24 апреля 2025 г.
- 11-00



О компании

АЛАДДИН – ведущий российский разработчик и производитель ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры предприятий и защиты её главных информационных активов.

Компания работает на рынке с апреля 1995 г. - 30 лет!

Многие продукты, решения и технологии компании стали лидерами в своих сегментах, а во многих крупных организациях и Федеральных структурах - стандартом де-факто.

Компания имеет все необходимые лицензии ФСТЭК, ФСБ и Минобороны России для проектирования, производства и поддержки СЗИ и СКЗИ, включая работу с гостайной, производство, поставку и поддержку продукции в рамках гособоронзаказа.

Большинство продуктов компании имеют сертификаты соответствия ФСТЭК, ФСБ, Минобороны России и могут использоваться при работе с гостайной со степенью секретности до "Совершенно Секретно".

С 2012 г. в компании внедрена система менеджмента качества продукции (СМК), ежегодно проводится внешний аудит, имеются соответствующие сертификаты ГОСТ Р ИСО 9001-2015 (ISO 9001:2015) и ГОСТ РВ 0015.002-2020 на соответствие требованиями российского военного стандарта, необходимые для участия в реализации гособоронзаказа.

Ключевые компетенции

- ◆ Аутентификация
 - Подготовлено 12 национальных стандартов по идентификации и аутентификации (ГОСТ 58833-2020, ГОСТ Р 70262-2022)
 - Выпущено учебное пособие "Аутентификация – теория и практика"
 - Защищена докторская диссертация
- ◆ Доверенная загрузка и технология "стерилизации" импортных ARM-процессоров с TrustZone
- ◆ Разработка встраиваемых (embedded) Secure OS и криптографии для микроконтроллеров, смарт-карт, JavaCard
- ◆ Биометрическая идентификация и аутентификация по отпечаткам пальцев (Match On Card/Device)
- ◆ PKI для Linux и российских ОС
- ◆ Прозрачное шифрование на дисках, флеш-накопителях
- ◆ Защита баз данных и технология "опровославливания" зарубежных СУБД
- ◆ Аутентификация и электронная подпись для Secure Element (SE), USB-токенов, смарт-карт, IoT-устройств, Web-порталов и эл. сервисов.