

Aladdin LiveOffice

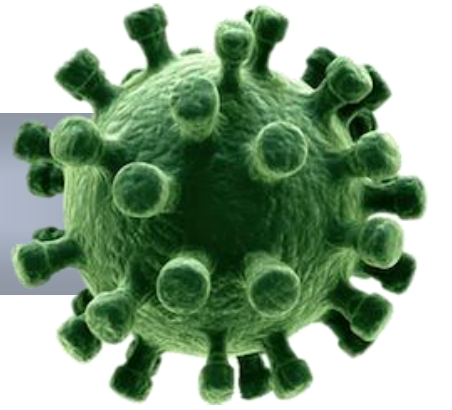
- доверенная платформа для безопасной дистанционной работы сотрудников при использовании ими личных средств вычислительной техники

Для государственных структур
и коммерческих компаний



Валерий Бабурин,
Менеджер продукта направления
"Защищенные носители информации"





- ◆ Актуальность решения для безопасной удалённой работы
 - Эпидемия коронавируса, карантин, режим домашней изоляции показали **неготовность** федеральных структур, органов исполнительной власти, государственных организаций и многих компаний к организации эффективной удалённой работы своих сотрудников
- ◆ Причины
 - Действующие требования регуляторов предписывают необходимость "реализации защищенного удаленного доступа" (УПД.13) к ГИС, ИСПДн и КИИ
 - В стране нет столько денег, чтобы для работы на "удалёнке" обеспечить каждого сотрудника служебным ноутбуком и набором средств защиты для него
- ◆ Поручения Правительства РФ
 - №ММ-П9-1861, №ДГ-П17-1987 от 16 и 18.03.2020
 - Для противодействия распространению коронавирусной инфекции обеспечить работу сотрудников органов исполнительной власти и гос. организаций в удалённом режиме с использованием личных средств вычислительной техники с предоставлением им удалённого доступа к ГИС

Важность и актуальность работы на "удалёнке"



- ♦ Отпадет ли необходимость в работе "на удалёнке"?
 - Нет. Возможны новые вспышки заболеваний и новый массовый переход на "удалёнку"
 - Многие коммерческие организации смогли организовать эффективную работу на "удалёнке", и КПД вырос
 - **Возможность работы "на удалёнке" для многих федеральных структур, органов исполнительной власти и гос. структур остаётся как никогда актуальной и востребованной**
- ♦ Что было сделано:
 - Проработаны **Требования** к технологии и средствам для удалённой работы
 - При использовании **личных** средств вычислительной техники (СВТ)
 - С возможностью подключения к рабочему компьютеру и к ГИС (ИСПДн, КИИ) до 1-го класса и обработки информации ограниченного распространения (ДСП)
 - Требования **согласованы** с регуляторами (ФСТЭК России, ФСБ России, Минцифры России, ЦБ)
 - **Официально утверждены (ДСП, только для вендоров и испытательных лабораторий)**
 - Подготовлено решение, начато пилотирование, осуществлена сертификация

Что даёт использование LiveOffice



Возможности

- ♦ Использование **личных** компьютеров сотрудников при работе на "удалёнке"
- ♦ Удалённое подключение к своему служебному компьютеру и/или к виртуальному рабочему столу
- ♦ Удалённая работа в привычной среде, с набором привычных приложений и документов - **как в офисе**
- ♦ Работа с документами ограниченного распространения
- ♦ Работа с различными системами электронного документооборота (**ЭДО**) и использование электронной подписи (**ЭП**)
- ♦ **Выход в Интернет** - только со служебного компьютера через корпоративный шлюз и корпоративные средства защита

Что даёт использование LiveOffice



Решение не позволяет

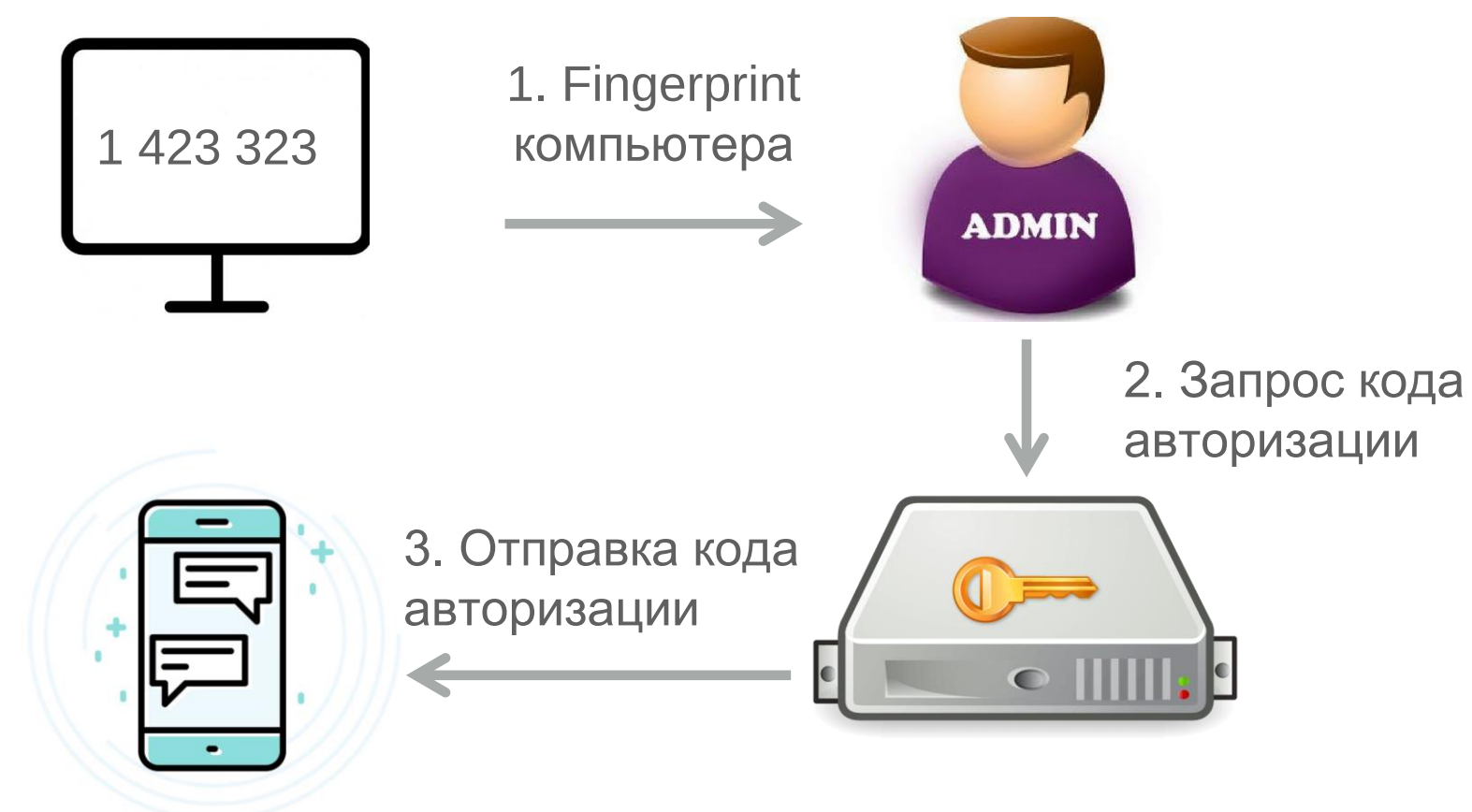
- ♦ **Копировать** обрабатываемую информацию на локальные, съёмные диски, флеш-накопители и на другие устройства
- ♦ **Загрузить** какой-либо файл (возможно, зараженный) на свой служебный ПК или в ГИС
- ♦ **Распечатать** обрабатываемую информацию на подключенный локальный или сетевой принтер
- ♦ **Напрямую выходить в Интернет** с личного ПК (во время работы LiveOffice)
- ♦ **Раскрыть** обрабатываемую информацию в случае утери или кражи USB-устройства
- ♦ **Скомпрометировать пароль** для удалённого подключения с служебному ПК и к ГИС
 - При развёрнутой PKI для 2ФА пользователя используются цифровые сертификаты
 - Если PKI не развёрнута, то используется технология SecurLogon - подстановка сложного длинного пароля, который неизвестен пользователю (а следовательно, он не сможет использовать его при заказе пиццы или в соцсетях)

LiveOffice - как это работает



Если подключаешься первый раз:

1. Подключить LiveToken к USB-порту **личного** компьютера
2. При загрузке **войти в BIOS/UEFI**
3. В меню **выбрать источник загрузки: Aladdin LiveOffice**
4. **Ввести пароль пользователя**
5. **Отправить код запроса на регистрацию администратору**



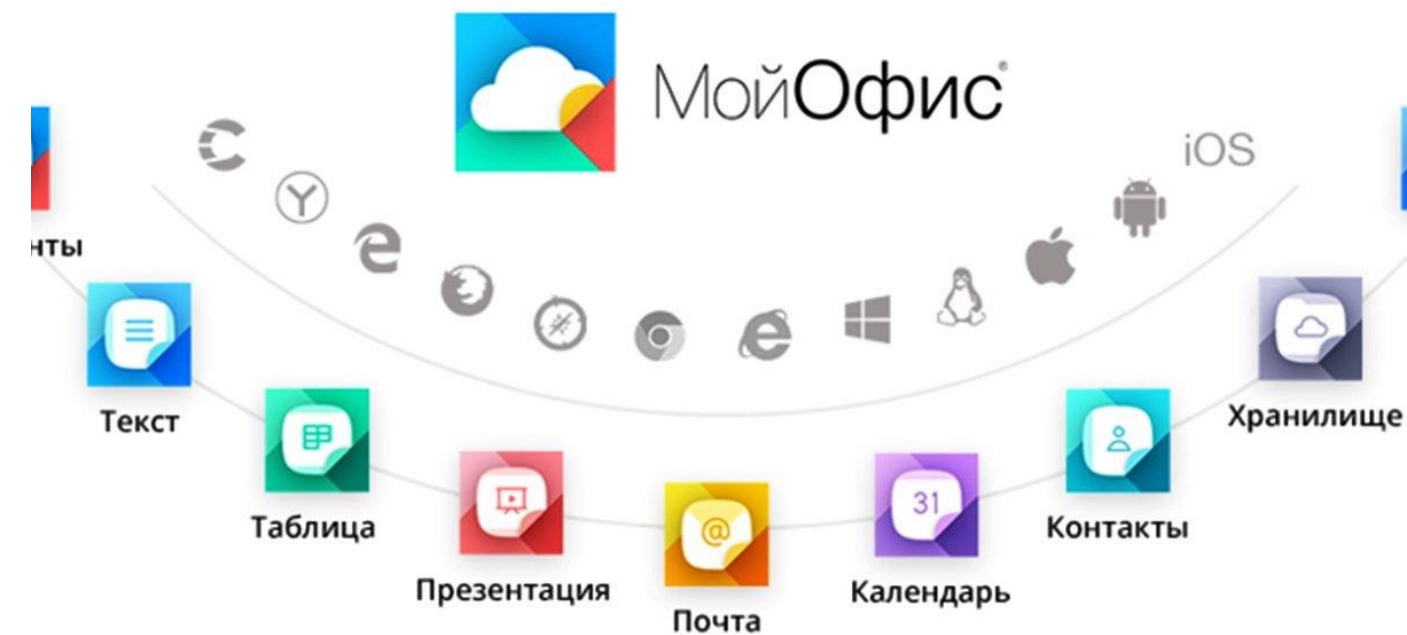
6. **Ввести код регистрации** компьютера ("спарить" его с LiveToken)

7. Настроить **сетевое подключение** (WiFi)

8. Подключиться к своему удалённому служебному компьютеру или виртуальному рабочему столу

Всё. Можно начинать работать

LiveOffice - как это работает



Если заранее всё настроено:

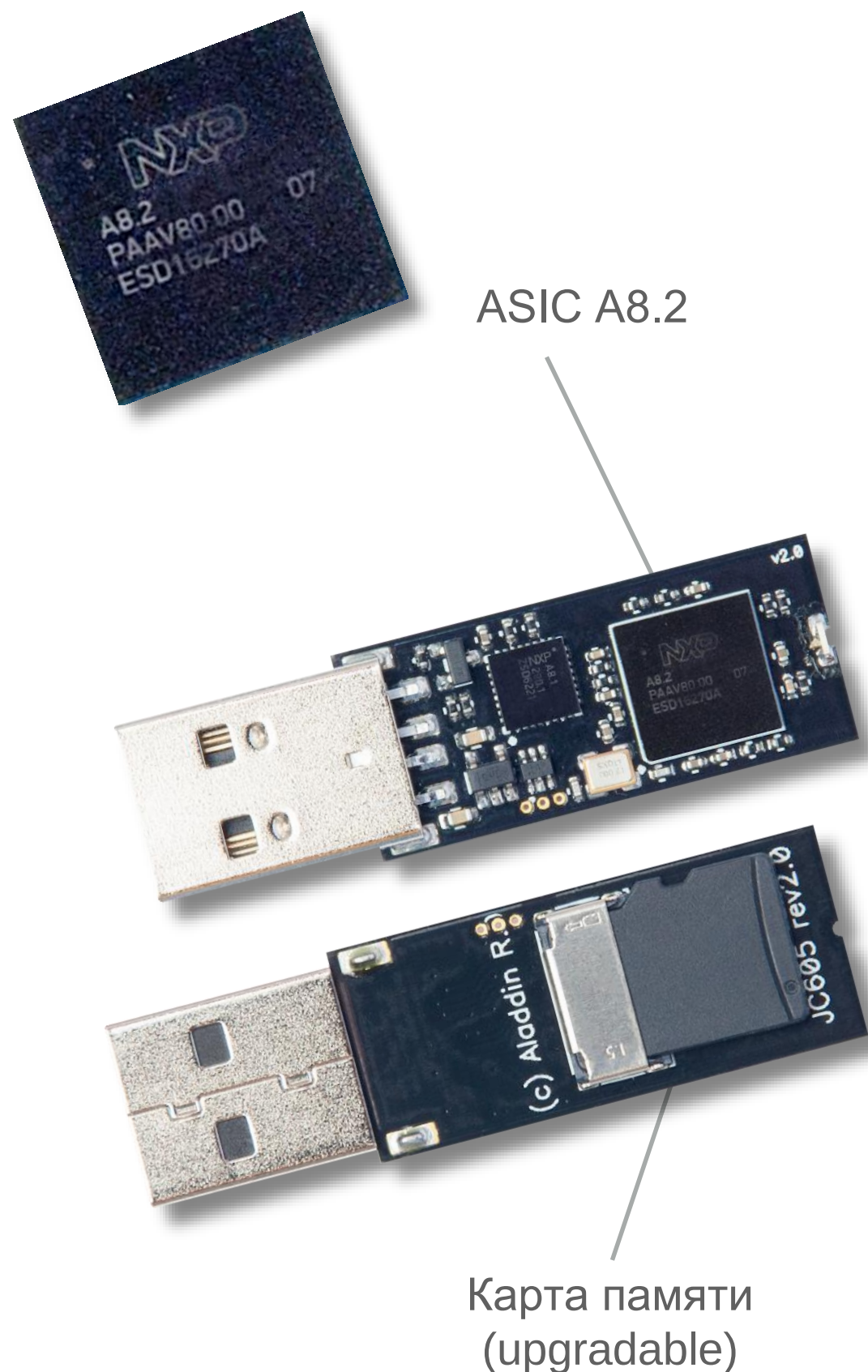
1. **Подключить** токен к USB-порту компьютера
2. **Загрузить** (или перезагрузить) компьютер
3. **Ввести пароль пользователя**
4. Подключиться к своему удалённому служебному компьютеру или виртуальному рабочему столу и начать работу

Компоненты решения

- как обеспечивается безопасность

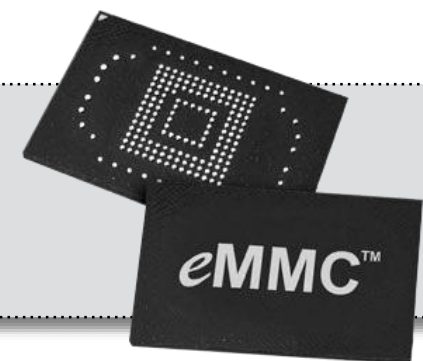


Как обеспечивается безопасность



- ♦ Безопасная архитектура устройства
 - Взаимная аутентификация активных эл. компонентов
 - Защищённый обмен данными
- ♦ Доверенная реализация
 - Заказной (ASIC) микроконтроллер на базе ARM-процессора
 - **Secure Element** на базе смарт-карточного чипа (сертифицированная российская криптография, неизвлекаемые ключи), неклонируемость и защита от взлома
 - "Изолирование" карты памяти, загрузка и контроль прошивки встроенного контроллера
 - APDU-Firewall, работа только по "белым спискам" команд
- ♦ Собственная ОС РВ для микроконтроллера
 - Доверенная загрузка для встроенной ОС микроконтроллера
 - Аппаратное шифрование защищённых разделов флеш-памяти
 - Безопасный обмен с ПО на хосте (защита команд и данных)
 - ▶ **Взламывать украденное устройство и пытаться извлечь из него информацию бесполезно**
- ♦ Внедрена технология разработки безопасного ПО (ГОСТ Р 56939-2016), автоматизированного тестирования и поиска уязвимостей

Компоненты решения



Логические диски флеш-памяти USB-токена

- **Доверенный загрузчик**

- Модуль аутентификации пользователя до загрузки LiveOS

- Модуль авторизации ПК

- Модуль КЦ

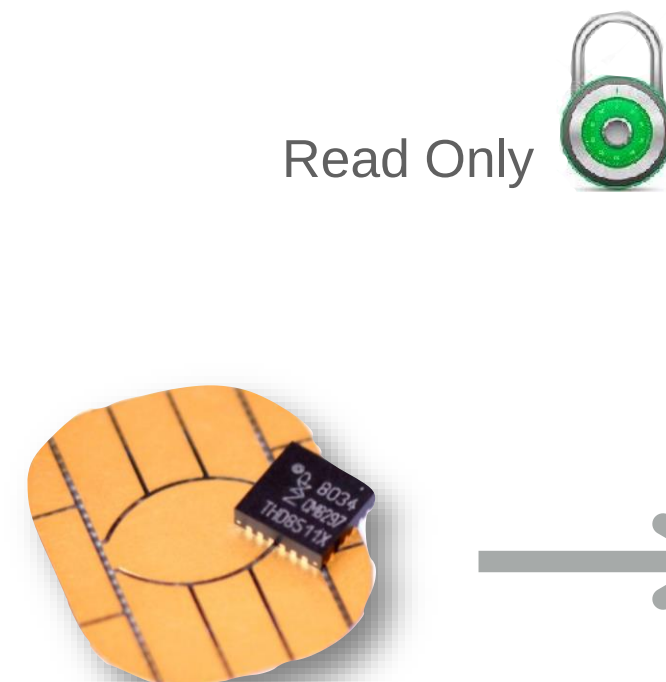
- **Подключаемый раздел - LiveOS**

- Фиксированный набор предустановленных и преднастроенных приложений:
 - VPN-клиент (сертифицированный)
 - RDP/VDI-клиент
 - Набор офисных приложений
- Клиент для работы с PKI и ЭП

- **Скрытый защищённый раздел**
хранение реквизитом и настроек для подключения к удаленному рабочему столу

- Журнал событий безопасности

- **Защищённый раздел для данных пользователя**



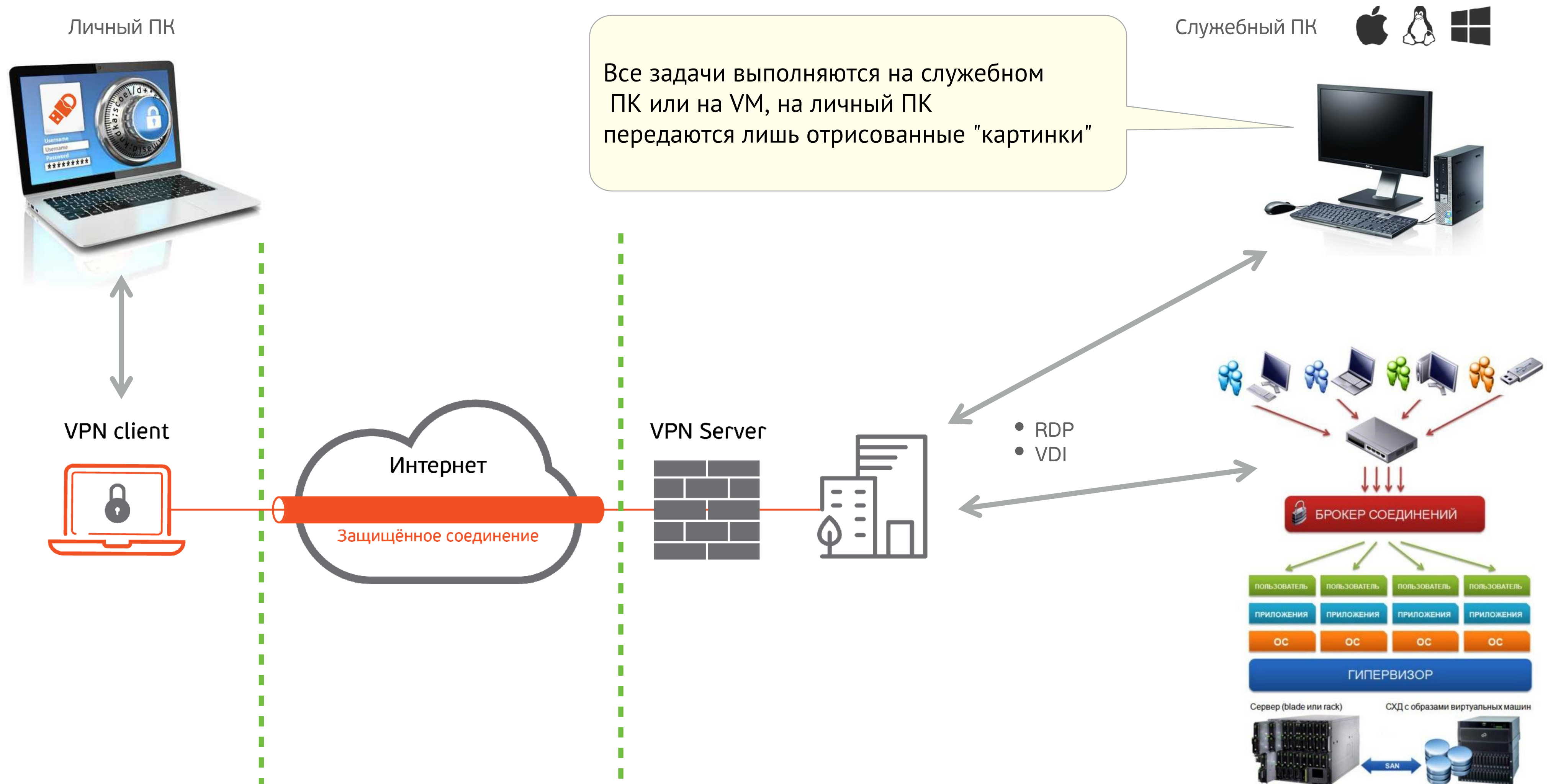
Secure Element на базе защищённого смарт-карточного чипа

Сертифицированное средство:

- ЭП
- 2ФА

Защищённое хранилище криптографических ключей, сертификатов

Как обеспечивается безопасность





◆ Сертификация ФСТЭК России

- Требования по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий по **4-му уровню доверия, технические условия**
- LiveOS в составе продукта
 - Сертифицированная ОС "Astra Linux Special Edition" версия 1.6 SE "Смоленск" (профиль защиты ИТ.ОС.А4.ПЗ)
- МДЗ уровня платы расширения – в перспективе

◆ Сертификация ФСБ России

- **СКЗИ** и **СЗИ от НСД** (даст **КС-2** для **VPN**-клиентов) - в процессе
- VPN-клиент в составе продукта
 - Сертифицированный ViPNet Client 4U for Linux

Соответствие новым Требованиям к средствам дистанционной работы

Защищенный съёмный машинный носитель информации		
Средство доверенной загрузки с аутентификацией пользователя ДО загрузки LiveOS		
Использование сертифицированных LiveOS и VPN		
ПО для 2ФА в информационной (автоматизированной) системе		
SSO (однократный ввод аутентификационной информации)		
Возможность работы ТОЛЬКО с авторизованных СBT (<=3 шт.)		
Возможность безопасной транспортировки персонализированных USB-устройств с использованием недоверенных каналов (курьеры, почта)		
Безопасное обновление LiveOS и LiveBoot		
Возможность работы с ЭП (УКЭП) в системах ЭДО		
Это глубоко интегрированное программно-аппаратное решение, а не "конструктор"		



Aladdin LiveOffice

Средство обеспечения безопасной работы сотрудников на "удалёнке"

Будь собой в электронном мире!



Валерий Бабурин
V.Baburin@aladdin-rd.ru
+7 (915) 100-2390
www.aladdin-rd.ru

