IDETRIS APP

Технология мобильного доступа на базе интерфейсов QR/Bluetooth

Сколково

ΛΔVENT IDETRIS

- ОБЗОР: «Физические» ID-карты доступа
- IDETRIS APP Смартфон + APP
- IDETRIS APP (Bluetooth)
- IDETRIS APP (QR | Blutooth)
- Система Авторизации

IDETRIS APP (secured Bluetooth)

НЕДОСТАТКИ «ФИЗИЧЕСКИХ» ID-КАРТ ДОСТУПА

ПРОБЛЕМЫ ЗАЩИЩЕННОСТИ ID КАРТ

Технологии RFID-идентификации с помощью карт более не является защищенными. Некоторые интерфейсы – были взломаны. Конечные пользователи в итоге вынуждены менять карты и считыватели. А в условиях санкций доступ к идентификаторам и оборудованию кодирования карт ограничен, при этом сервис не стабилен.

ПЕРЕДАЧА ID КАРТ ДРУГИМ ЛИЦАМ

Иногда сотрудники могут передавать свои ID карты коллегам. Не часто в организациях к этому относятся серьезно.

ДИСТАНЦИЯ СЧИТЫВАНИЯ КАРТ

Существуют карты с несколькими интерфейсами RFID, что представляется более защищенной альтернативой стандартным решениям. Это действительно так, но при построении мульти-форматной архитектуры считывателей карт, 90% имеют дистанцию считывания – около 5 сантиметров, однако если есть другие интерфейсы, в частности, другой частотности и это может потребовать, либо меньшей, либо большей дистанции. Также, «дуальные карты – чрезвычайно дорогие.

Приложение IDETRIS APP + Считыватель IDETRIS QUB:

РАЗЛИЧНЫЕ МОДАЛЬНОСТИ ДОСТУПА:

Интерфейсы Физических Карт

- SSID, ISO14443A, ISO15693,125KHz.., EM, Desfire, Mifare, HID iClass
- Поддерживает различные форматы карт

IDETRIS QUB

Bluetooth

- Show-to-Go (BT/NFC) | Показать и пройти
- Shake-to-Go | Потрясти и пройти
- Hands Free | Бесконтактный
- Кнопка

QR-код

- Динамический QR-код
- Статический QR-код

PIN

IDETRIS APP

IDETRIS APP: Смартфон + APP (Bluetooth + NFC)

1

Смартфон = Личная собственность = Сложнее «позаимствовать» для доступа на объект

- Смартфон становится все более совершенным, защищенным личным устройством
- В среднем человеку требуется 5 минут, чтобы заметить пропажу телефона, при этом, по результатам исследований, – 30 минут, чтобы осознать что кошелек или «кардхолдер» потеряны.

2

Обновление новой версий Приложений

- Номер карты генерируется с помощью **Защищенного приложения**. В случае, если возникают опасения относительно угроз или «проблем» с приложением, его можно относительно простым образом обновить до новой рабочей версии и добиться нужного уровня защиты.
- Конечный пользователь не должен менять карты или считыватели при смене стандарта или модальности доступа.

3

Доработанная технология Bluetooth

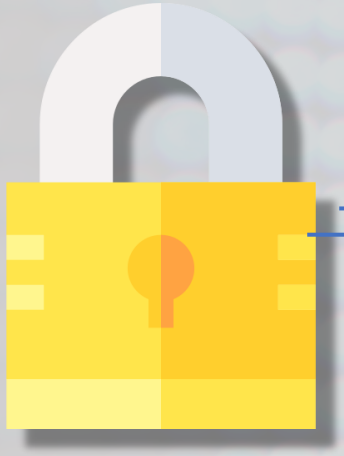
- Технология рассчитана на дистанцию от 0,1 до 5m, что обеспечивает удобство для использования различных Приложений для Контроля доступа. Технология имеет шифрование AES128, а Bluetooth модуль специальным образом доработан до необходимого уровня безопасности и стабильности работы.

4

Технология NFC

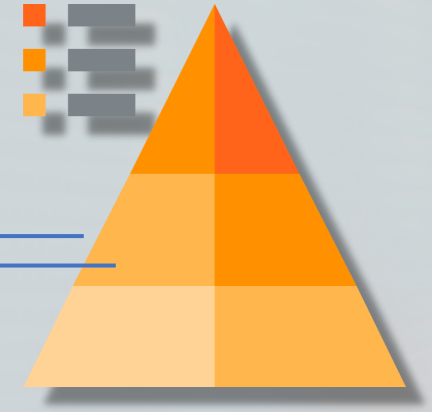
- Скорость получения ответного кода при считывании сравним с индукционной реакцией обычной карты.
- Мобильное приложение осуществляет симуляцию процесса аутентификации CPU карты и позволяет «кастомизировать» ключ Аутентификации и ID файл. Что является безопасным и надежным алгоритмом.

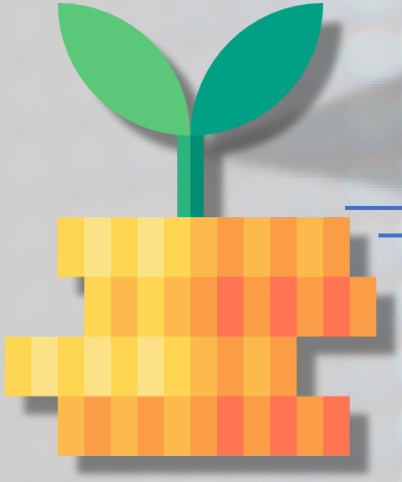
IDETRIS APP (Bluetooth + NFC) обеспечивает:



БЕЗОПАСНОСТЬ

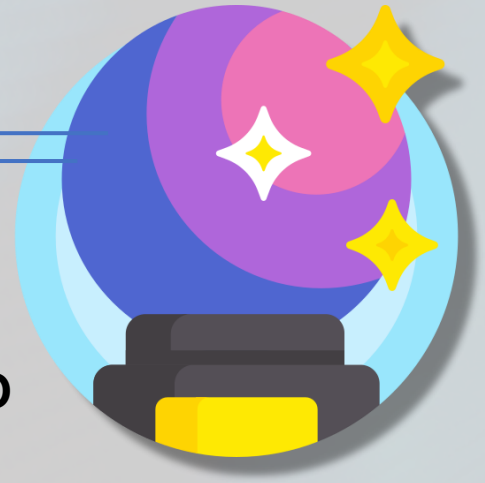
УНИКАЛЬНОСТЬ





ЭКОНОМИЯ

ИНФРАСТРУКТУРА ДОСТУПА БУДУЩЕГО



IDETRIS APP (Bluetooth) – Это Безопасно!:

Используется **«Динамический»** ключ для аутентификации Смартфона

Все данные хранятся в телефоне и коммуникационный протокол шифруется AES128

Дополнительный инструментарий защиты: **Корпоративный Ключ** и **Ключ конечного пользователя.** Как итог, «дублированная» внешняя карта не сможет быть использована для доступа

Во время «Процесса Авторизации» могут быть добавлены временные рамки для контроля периода Валидации номера карты, которая должна быть авторизована

Посредством отправки Email, только один номер карты будет привязан к соответствующему номеру телефона (привязка к MAC коду).

IDETRIS APP (Bluetooth) – Это Уникальная технология!:

Авторизованный пользователь может назначить «Имя» считывателю **Bluetooth**. Например, **«Вход»**, **«Переговорная 1»** итд.

Поддерживает множество режимов доступа: **NFC**, **«Покажи и проходи»**, **«Потряси и проходи»**, **«Бесконтактная и контактная кнопка (на экране смартфона)»** для разных задач. Каждый режим может быть включен или выключен

За исключением функции «**Ручной кнопки»**, другие режимы доступа могут быть активными если экран телефона выключен – фоновый режим

Если более чем один **Bluetooth** считыватель в зоне считывания, на экране пользователя появится **«Имя считывателя Bluetooth»** для того, чтобы Пользователь решил, какой считыватель должен быть активирован у какой из дверей

Поддержка **Вход/Выход** и ограниченного временем режима **«Антивозврата»** для конкретного считывателя в рамках различных задач управления доступом

IDETRIS APP (Bluetooth) ТЕХНОЛОГИЧЕСКИЕ ФУНКЦИИ:

Технологии

- Bluetooth
- Mobile NFC
- Физическая карта

Режимы доступа

- Show-to-Go (BT/NFC) | Показать и пройти
- Shake-to-Go | Потрясти и пройти
- Hands Free | Бесконтактный
- Кнопка

NFC Функция

- Симуляция процесса Аутентификации карты CPU.
- «Кастомизируемый» ключ аутентификации и Файл ID.

Дистанция

- Bluetooth: 0.1~5m
- Card & NFC: 2~8cm

Время Валидации

- Может быть установлено время валидации.
- Количество раз для конкретного номера авторизации карты может быть также установлено.

Настройка параметров

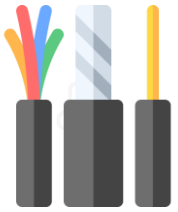
- Configuration Card | Карта конфигурирования
- Bluetooth (by App)

Функция клавиатуры

- PIN в Карте
- Card + PIN
- Только PIN

Multi-technologies

- SSID, ISO14443A, ISO15693,125KHz...
- Поддерживает различные форматы карт.



Комм. интерфейсы

- Wiegand
- OSDP V1,V2.2
- WiFi
- Bluetooth
- TCP/IP

IDETRIS APP: ФУНКЦИОНАЛЬНЫЕ ПАРАМЕТРЫ

PIN-КОД НА ЭКРАНЕ:

Часто возникает обеспокоенность защитой пароля при введении его на клавиатуре считывателя, мы предлагаем не только полностью бесконтактный принцип, но и возможность введения **Пароля на экране телефона.** При этом используется функция «**Смены порядка цифровых значений на кнопках»** для дополнительной защиты **(Scrumble)**.

- **Card + PIN** — Приложение не хранит **PIN**, как номер карты так и введенный **PIN** – отправляются в **Контроллер** и сверка может производиться в Контроллере.

- **Только PIN** — Считыватель отправляет введенный **PIN** в **Контроллер** управления после подключения к **APP**.

Преимущества:

- Поддерживает множество режимов – гибкий алгоритм переключения интерфейсов, может работать с разными типами контроллеров.
- Введение PIN на Вашем личном телефоне – обеспечит защиту данных и Вам не потребуется контактировать со считывателем, особенно, в публичных местах.
- Поддержка разных типов клавиатуры.
- Поддержка **«Scramble» клавиатуры** (со сменным порядком цифровых значений кнопок) для более высокого уровня безопасности.

УДОБСТВО ТЕХНОЛОГИИ:

Пользователь Android … NFC формат “Покажи и Проходи”

- Различные компании и производители, использующие Bluetooth в Смартфонах делают это разным образом, в итоге функциональность Bluetooth может иметь ограничения. Это может привести к проблемам при использовании технологии «Виртуальных крипто-карт».

- Для того, чтобы добиться надежного функционала Bluetooth, приложение использует обе технологии одновременно – **NFC + Bluetooth** в рамках модальности «Покажи и Проходи» (Show-to-Go). Помимо этого, NFC «разбудит» APP в случае, если приложение деактивировано или ушло в «фоновый режим».

- Кроме того, как известно, NFC – это коммуникационный стандарт, в рамках которого номер карты встраивается в «сгенерированную» карту DesFire или карту других стандартов внутри Приложения.

Пользователь IOS: iBeacon

- Для телефонов с IOS, даже если приложение закрыто, все режимы доступа с использованием коммуникационного интерфейса Bluetooth работают нормально, без накладок или задержек.

iBeacon

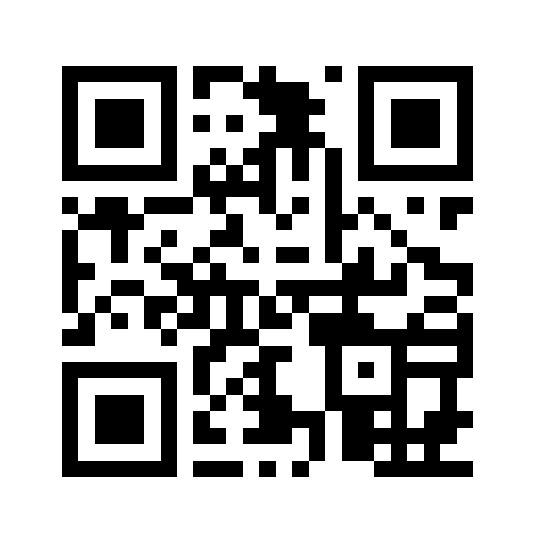
IDETRIS QUB: BLUETOOTH И QR-СЧИТЫВАТЕЛИ

- Когда требуется использование дополнительной модальности QR-кодов, У нас есть уникальное решение!

ДИНАМИЧЕСКИЙ QR-КОД В IDETRIS APP

● **QR Code** – Это, по сути, двухмерный Bar-code. При этом аббревиатура QR означает **«Быстрый ответ» (Quick Response)**. В целом **QR-код** может содержать больше информации, нежели стандартный Bar-Code и также предоставлять больше типов данных. QR-код – это технология, которая конвертирует номер, символы и алфавитную информацию в стандартную графическую форму.

Пользователи могут использовать «сканеры» или QR - считыватели для сканирования графического образа. Двухмерные «Баркоды», могут выдавать информацию в горизонтальном и вертикальном порядках, соответственно больший объем данных может содержаться в QR-коде в рамках меньшей зоны сканирования.



Существует 2 Типа QR-кодов:

- **Статический QR-код (Static QR Code)** – Фиксированный QR-код и его значение неизменно с течением времени.
- **Динамический QR-код (Dynamic QR Code)** – Как видно из названия, «Динамический» QR-код меняется в соответствии с установленными временными интервалами, однако содержание данных остается тем же: ссылка, код, информация.

IDETRIS APP: РАБОТА СЧИТЫВАТЕЛЯ QR-КОДОВ

AVENT IDETRIS

IDETRIS-QUB: СЧИТЫВАТЕЛИ ВИРТУАЛЬНЫХ КАРТ И ДИНАМИЧЕСКИХ QR-КОДОВ

Инновационный, единственный в своем роде Bluetooth считыватель динамических QR-кодов.

● Простая инсталляция

Считыватели Динамических QR-кодов не требуют Дополнительного канала синхронизации. Мы используем специально доработанный под наши задачи **канал Bluetooth** для синхронизации работы считывателя с Приложением телефона. Когда **Приложение (APP)** показывает **Динамический QR-код**, он использует механизм **«Умной Синхронизации» (Smart Synchronization)** для отправки информации о **«Времени» (Time)** в **Считыватель (если Bluetooth включен).** При этом, ввиду того, что считыватель **QR-кодов** укомплектован **«Точными часами реального времени» (PRTC – Precise Real Time Clock)** нет необходимости, чтобы **Bluetooth** был включен при использовании функции динамических **QR-кодов (DQRCF – Dynamic QR Code Function)**.

● Защищенная, но гибкая в использовании система

Если считыватель переведен в режим **«Динамического QR-кода с высоким уровнем безопасности» (High Security Dynamic QR Code)**, потребуется, чтобы телефон включил режим **Bluetooth**, для верификации того, что конкретный динамический **QR-код (Dynamic QR code)** исходит от правильного телефона. При этом Пользователь телефона может переключаться между использованием учетных данных **Bluetooth** или учетных данных **динамического QR-кода**, если оба набора учетных данных были предоставлены во время авторизации изначально при регистрации **Пользователя**.

ФУНКЦИИ:

Технологии доступа

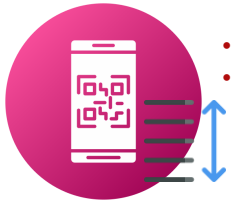
- QR Code
- Bluetooth
- Физическая карта

Режимы доступа

- Динамический QR-код (через Приложение (APP))
- Статический QR-код

Интерфейс

- Встроенная подсветка. Функциональность устройства в любых условиях освещения



Дистанция

- Дистанция считывания 4-18cm
- Точность – 6,6 mil

Время Валидации

- Может быть установлено время валидации.

Настройка параметров

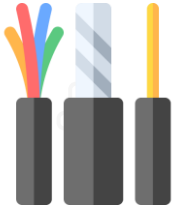
- Configuration Card | Карта конфигурирования
- Bluetooth (by App)
- Конфигурирование QR/Bar кодов

Bluetooth

- Полностью совместимо с Bluetooth считывателем

Multi-technologies

- SSID, ISO14443A, ISO15693,125KHz...Legic, Desfire, Mifare, iClass итд
- Поддерживает различные форматы карт.



Комм. интерфейсы

- Wiegand
- OSDP V1,V2
- WiFi
- Bluetooth
- TCP/IP

ТЕХНОЛОГИИ RFID:

Поддержка разных технологий RFID:

- **Низкочастотные RFID стандарты (125кHz)**

  HID compatible with FSK

  EM ASK machester

- **Высокочастотные RFID стандарты (13,56MHz)**

  Mifare (CSN, Sector)

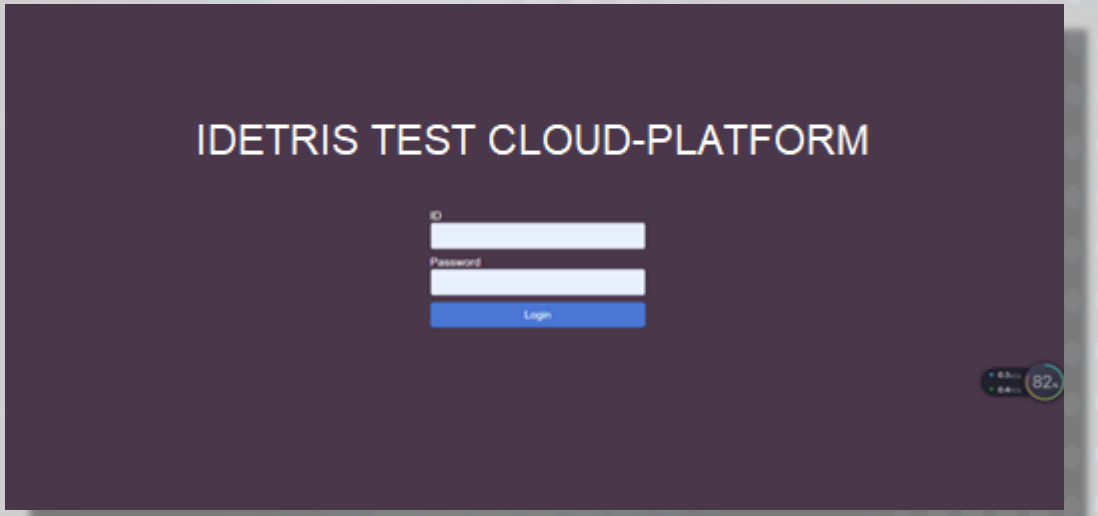
  Mifare Plus (56bits UID)

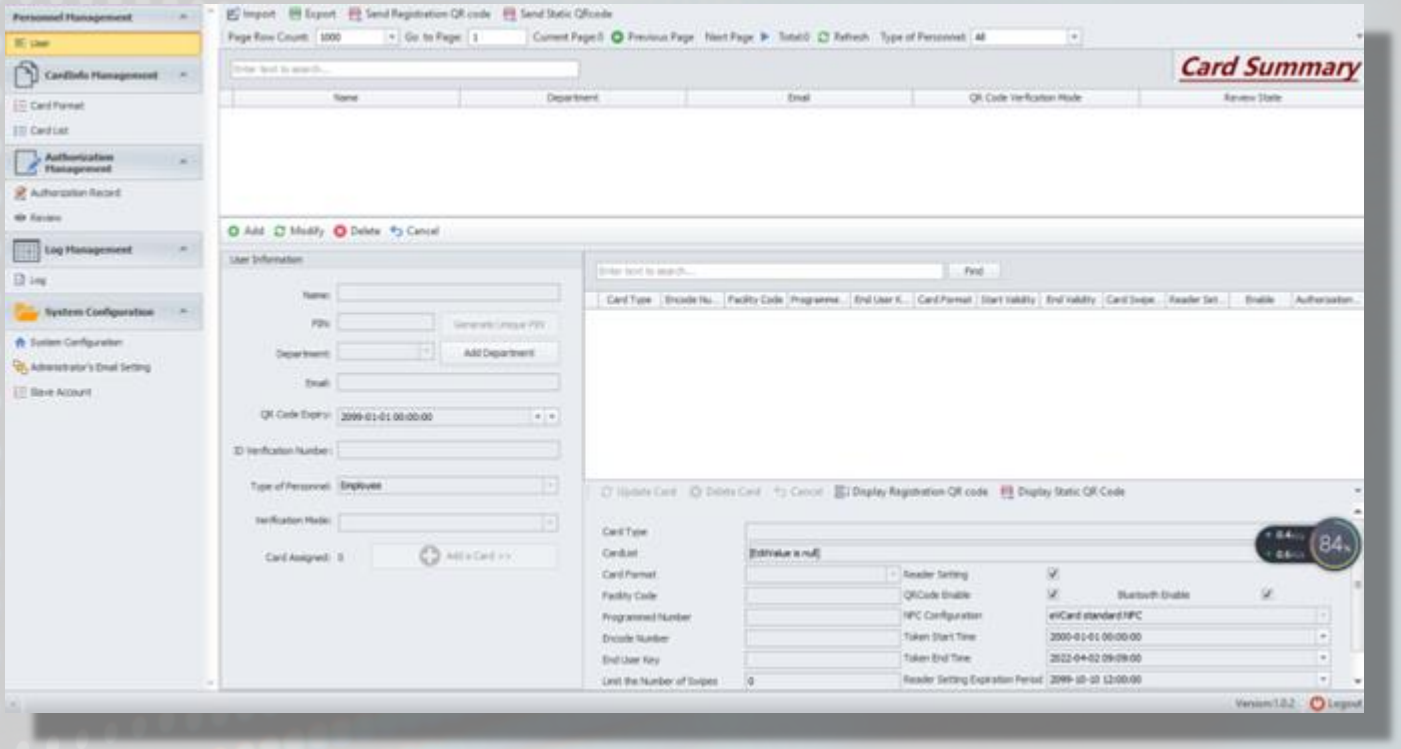
  DesFire (56bits UID, File)

  Sony Felica（64bits UID)

  Legic (Legic's Segment & UID, ISO14443A, ISO15693's CSN and iCLASS's Content & UID)

Off-Line Облачная система Авторизации eV-Cloud:





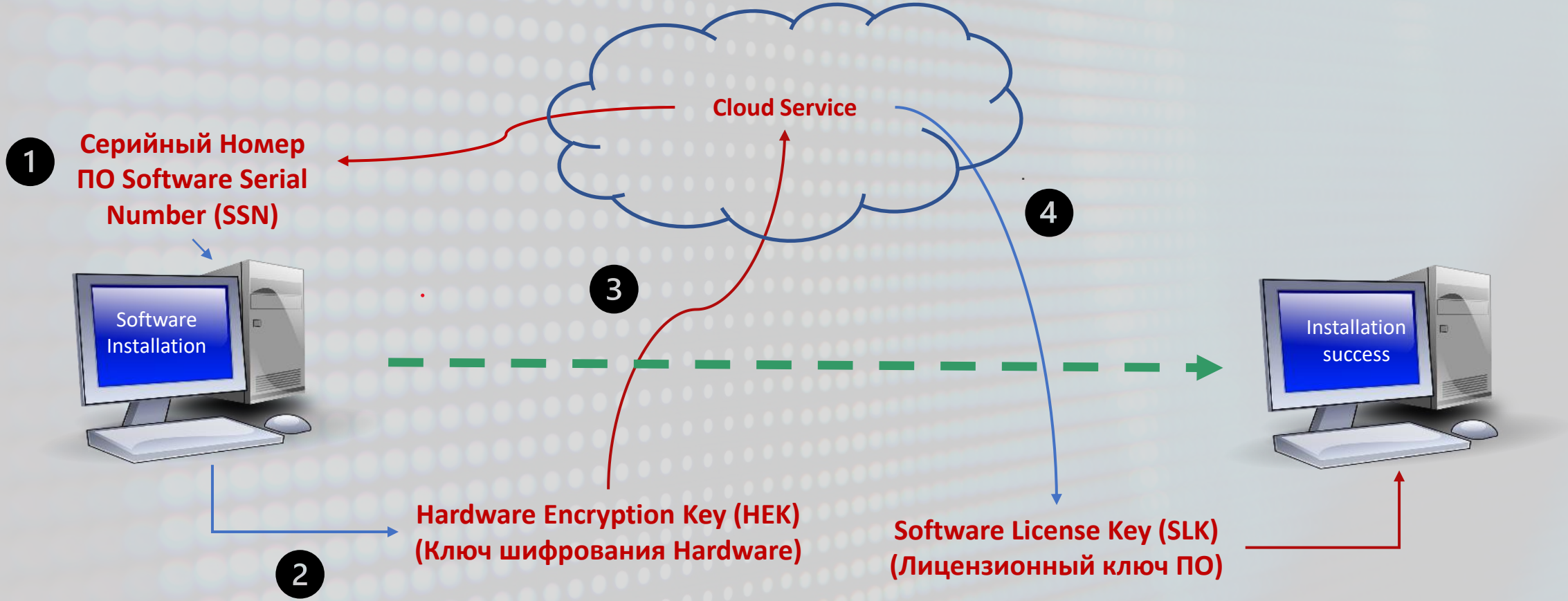
IDETRIS Cloud Система в Облаке

IDETRIS Client Система Авторизации «на Клиентской Стороне»

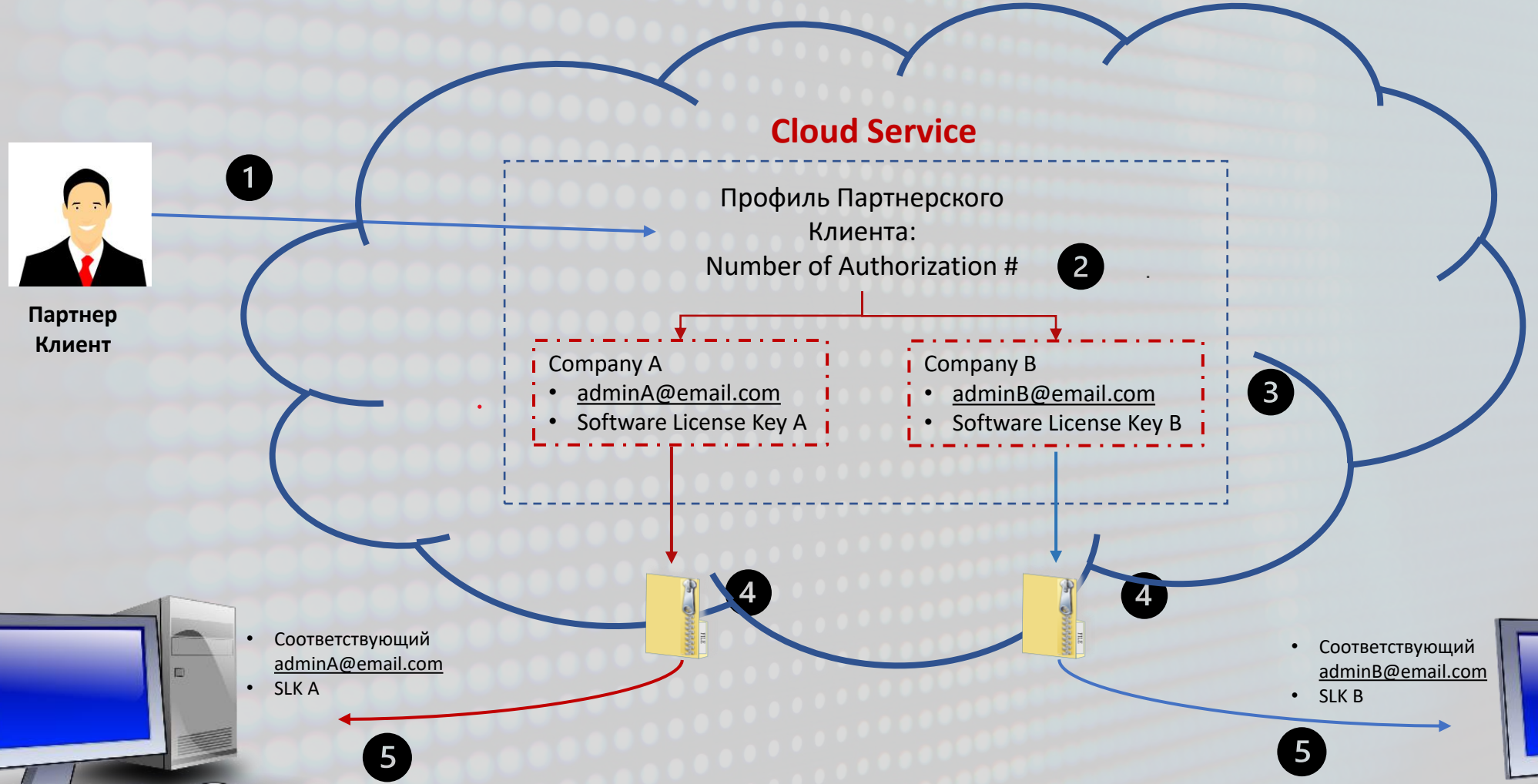
Главные характеристики Системы Авторизации:

- **Безопасность:** **ОДИН** номер карты может позволить **АВТОРИЗОВАТЬ** только **ОДИН** мобильный телефон.
- **Защита Личных данных:** Все **Персональные данные** конечных пользователей хранятся **на сервере Клиента**.
- **Экономичность:** Один и тот же номер карты может быть использован в последующем **для других сотрудников** – это обеспечивает экономию и защиту от утечки карт (виртуальных или физических).
- **Удобство и утилитарность:** **Пользователь** Мобильного телефона может передать номер своей карты со старого телефона на новый телефон **без привлечения «Оператора»**. Процесс передачи – простой и удобный.
- **Гибкость и Простота:** **Система Авторизации** также поддерживает принцип **Локальной Авторизации**.
- **Мульти-модальность:** Система поддерживает принцип Авторизации посредством **«Динамических QR-кодов»**.
- **Доступность:** При использовании **Статичного QR-кода Авторизации**, функция является абсолютно бесплатной, однако время Авторизации ограничено 24-часами.

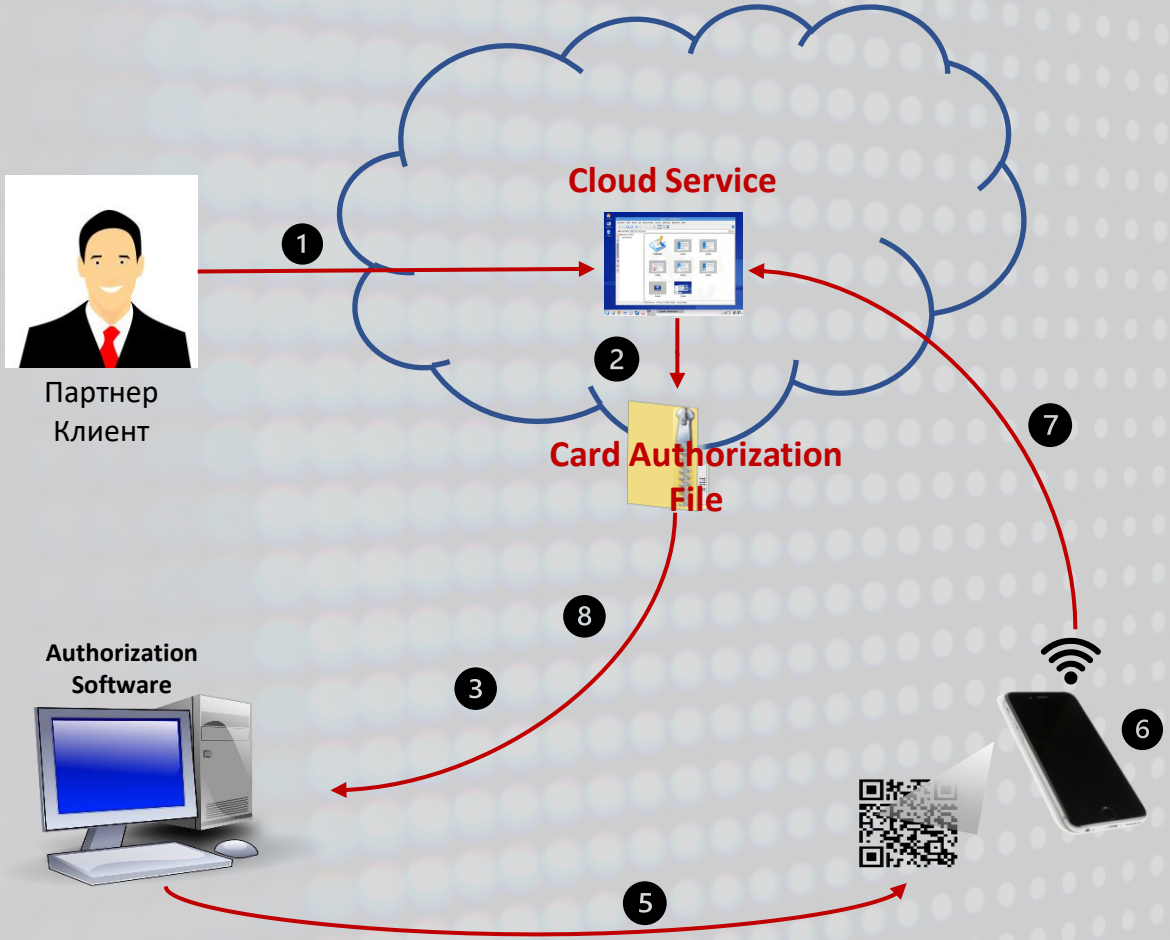
Процедура установки ПО:



Процедура Регистрации в Облаке:



Процедура Регистрации в Облаке:



- Соответствующий admin@email.com
- Software License Key

Удаленная Авторизация

① Компания-Партнер создает **«Проект»** для своего **«Конечного пользователя» (Заказчика)**, посредством **«Email адреса»** и **«Лицензионного ключа ПО» (Software License Key)**. **«Код Конечного Пользователя (Покупателя/Заказчика) (End User Code)** или набор **«Кодов Конечного пользователя» (End User Codes)** будет создан и привязан к данному **«Конечному Пользователю»**.

② Зашифрованный «**Файл Карты Авторизации» (Card Authorization File)** будет создан с соответствующим **«Форматом Карты» (Card Format)**, **«Кодом Объекта» (Facility Code)** и **«Номером Карты» (Card number)**.

③ **«Файл Авторизации» (The Authorization File)** будет отправлен на зарегистрированный соответствующий Email Админа.

④ Детали и реквизиты будут введены в **ПО eV Cloud** на основе полученных соответствующих номеров карт.

⑤ **«Авторизационный QR-код» (Authorization QR Code)** будет отправлен на Email адрес пользователя конкретного телефона.

⑥ После того как **Приложение (App)** отсканирует информацию QR-кода, Пользователь получит запрос на введение **ID Номера (ID Number)** и / или Email адрес и / или Персональный ID для верификации данных Пользователя.

⑦ После успешной верификации **ID, App (Приложение)** свяжется с **Облаком (Cloud)** для получения разрешения авторизации и отправит **Серийный номер телефона (Phone Serial Number)** **(BTAN = encrypted IMEI code)**, номер карты (Card number), дату срока годности карты (Card Expiration date), дат Авторизации Начала и Завершения действия QR-кода (Card Expiration date, Auth QR Code start and expiry dates) **в «Облачный Сервис» (Cloud Service)** для Записи. Отправка **никакой другой Персональной или Критической информации** не предусмотрена нашей технологией.

⑧ После успешной **Авторизации, Облачный Сервис (Cloud Service)** отправит Email на зарегистрированный адрес Админа.

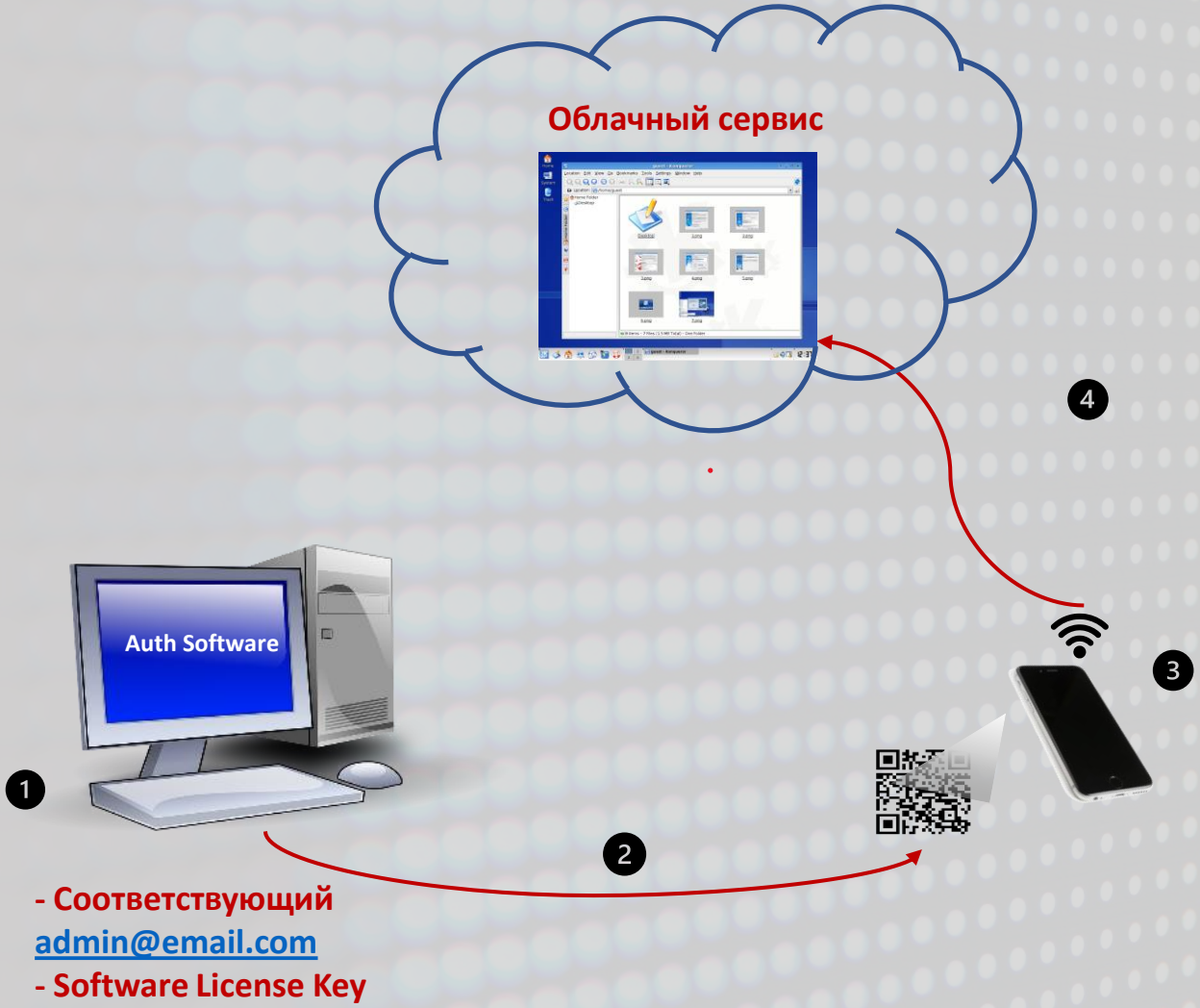
AAVENT IDETRIS

Варианты Авторизации:

Наша Технология поддерживает ТРИ типа авторизации «Виртуальных» карт:

1) **Одноразовая Авторизация (One time Auth)**
   - Каждая **«Сессия авторизация»** может привязать ОДИН номер карты к ОДНОМУ телефону ОДИН раз. Какая бы не была причина смена авторизации, потребуется НОВАЯ авторизация, даже если Сотрудник просто сменил телефон. Тем не менее, дата окончания Авторизационного периода может быть изменена.
2) **Авторизация карты – На весь срок использования (Life-Time Card Number Auth)**
   - Каждая авторизация связана с **выделенным «Номером карты»** и **«Форматом».** Пока этот номер Назначен, но не авторизован с телефона, Пользователь может назначить этот же номер карты другому телефону или пользователю без дополнительных операций.
3) **Умная Авторизация (Smart Authorization)**
   - Это Авторизация на весь срок использования, и она не привязана какому-либо **«Номеру карты»** или **«Формату»**. Если Пользователь телефона деактивировал данный номер карты (уехал в командировку, ушел в декрет), клиент может использовать эту авторизацию для назначения нового пользователя с новым номером карты или форматом, если это необходимо.

Варианты Авторизации:



Изменить параметры конечного пользователя

① **Оператор** меняет параметры авторизации или реквизиты/установки существующего Пользователя, за исключением имени, Email адреса, номера карты.

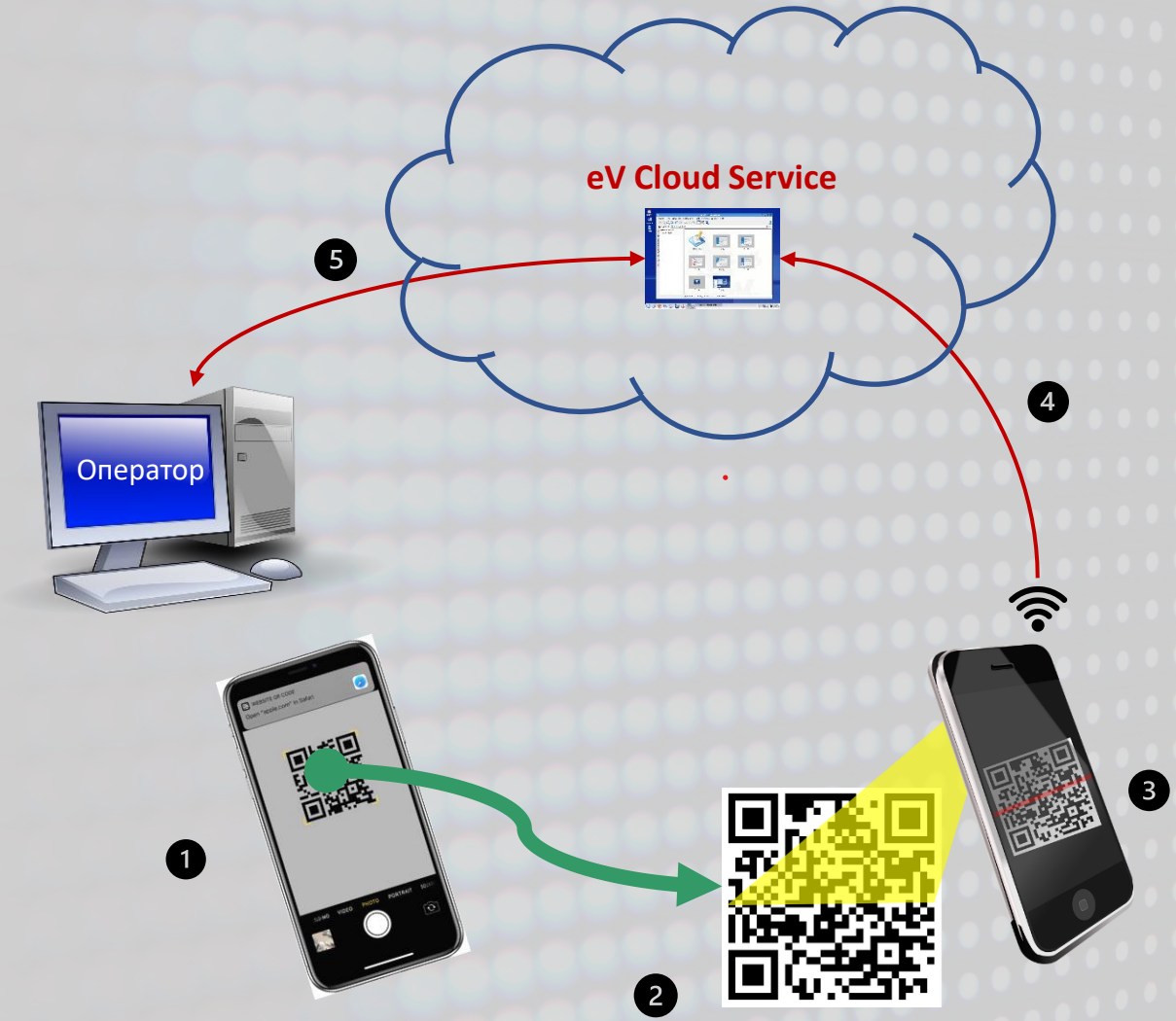
② Новый зашифрованный **«Файл Карты Авторизации» (Card Auth File)** будет создан и отправлен на email **«Конечному пользователю» (End User)**.

③ Когда **Приложение (App)** сканирует QR код авторизации, оно будет проверять если Данные содержат те же данные, что и в Мобильном телефоне.

④ Если данные верные и верифицированы, Телефон снова свяжется с **Облачным сервисом (Cloud Service)** для обновления данных.

Операция Завершена!

Замена телефона для зарегистрированных Пользователей



Замена личного телефона после Авторизации

① В **Приложении**, найдите иконку функции **«Изменить Личный телефон» (Change Personal Phone)**.

② В итоге Новый **зашифрованный «QR код Авторизации» (Auth QR Code)** будет создан на экране. Пользователь может сохранить его или сделать снимок.

③ При наличии Нового телефона, Пользователь может прямым образом отсканировать QR код посредством Сканера, встроенного в Приложение на **Новом телефоне**. После Сканирования нового **«QR кода Авторизации»**, Пользователь должен ответить на вопросы в рамках алгоритма «Верификации данных».

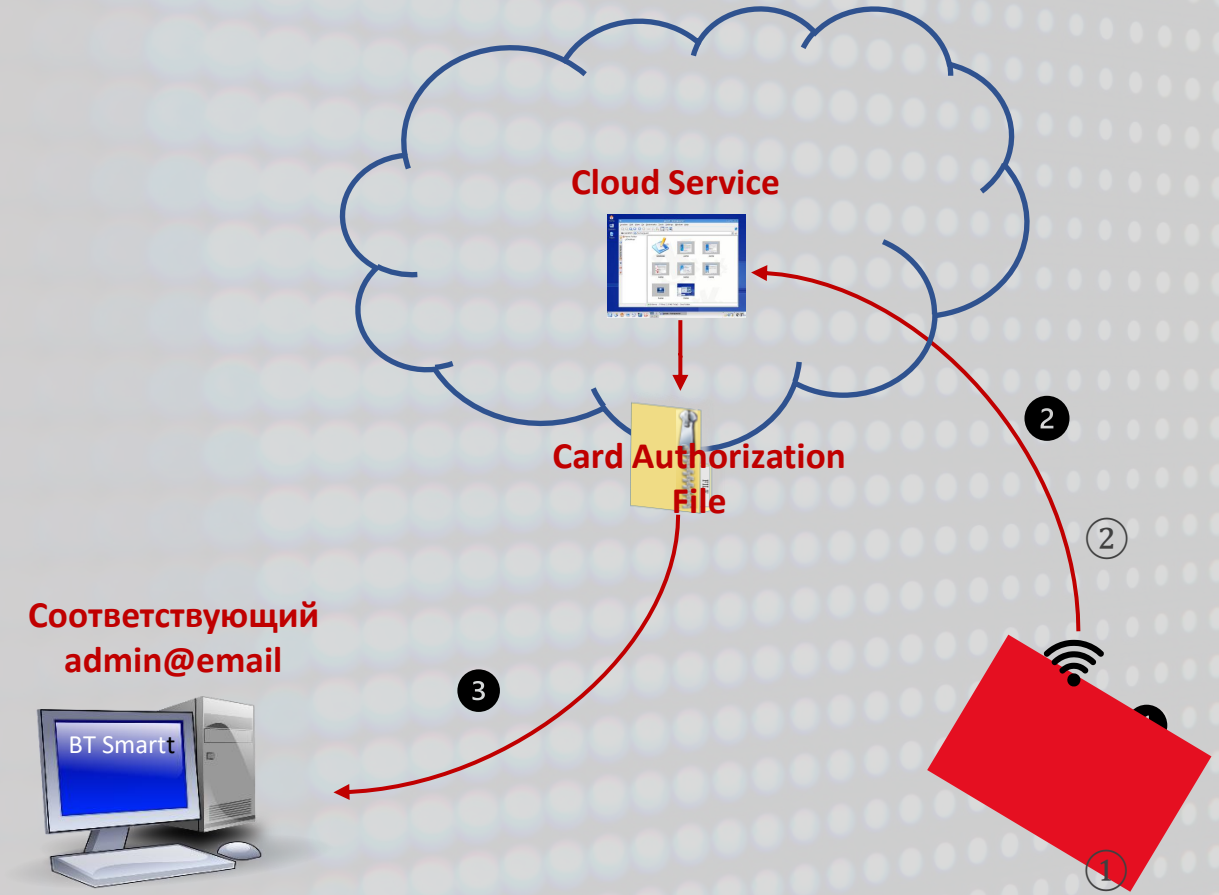
④ Если все данные корректные, телефон снова свяжется с **Облачным сервисом (Cloud Service),** чтобы получить разрешение для обновления всех данных в **НОВОМ** телефоне.

⑤ Облако отправит Email с уведомлением в панель Оператора для относительно **«Смены телефона»**.

Примечания: Один телефон может передать данные Авторизации единожды. Другими словами как только пользователь передаст данные авторизации на новый телефон, Пользователь не сможет передать данные на старый телефон обратно.

Операция Завершена!

OFF-Line Система Авторизации: Отмена (Dismiss)



Отменить Авторизацию с Телефона

① Пользователь должен нажать кнопку **«Отменить» (Dismiss)**, чтобы «вернуть» авторизованный номер карты владельцу. Номер **BTDA** будет создан после подтверждения операции.

② Приложение свяжется автоматически с **«Облачным сервисом»** для того, чтобы отправить уведомление о том, что **«Номер карты»** был выпущен.

③ **«Файл Авторизации Карты»** с неавторизированной информацией будет отправлен на зарегистрированный **E-mail Администратора**.

④ После того как Email получен, номер карты будет **«Разблокирован»** и может быть привязан к другому **Пользователю**.

Отменить, если Wi-Fi не подключен

① Конечный пользователь должен нажать кнопку **«Отменить»**, чтобы «вернуть» авторизованный номер карты владельцу. Будет создан номер **BTDA**. По какой-то причине приложение не может автоматически подключиться к **«Облачной службе»**, чтобы **«уведомить»** о выпуске этого номера карты.

② **Приложение (App)** свяжется обратной связью с **«Облачным сервером»** как только **WiFi** будет доступен и процесс Отмены будет завершен.

ADVENT IDETRIS

Вывод:

1) Опасения насчет Уровня Кибербезопасности (Cyber Security Concern)

Ввиду того, что Вся **«Система Авторизации» (в целом)** не имеет прямой связи от **«Облачного сервиса»** к **«Серверу Клиента»**, соответственно, **НЕТ** опасений насчет уровня Кибербезопасности.

2) Защита «Персональных данных» (Personal Data Privacy)

Все **«Персональные данные»** хранятся на **«Клиентском сервере»**. Единственный тип **«Персональных данных»**, который отправляется на сервер системы – Это зашифрованный код **IMEI Мобильного телефона**.

3) Безопасность (Security)

Все Письма шифруются в рамках стандарта **SLK**, по принципу **«Невозможности»** Дешифровки Email на другом ПК даже с тем же Email. Плюс все данные шифруются **AES128**.

4) Гибкость

Пользователь должен авторизовать сервис лишь один раз для множественного использования с тем же номером.

Преимущества нашей технологии Auth в рамках IDETRIS APP (QUB):

- Поддерживает как **Локальную**, так и **удаленную Авторизацию.**

- Комплексная **Аутентификация IDETRIS-APP** простая и безопасная. Только один телефон может быть **Авторизован**.

- Компании не нужно делиться/внедрять облачное решение. Подойдет **обычная сеть** с FireWall.

- Позволяет Специалистам по безопасности полностью контролировать весь процесс **Авторизации**.

- Позволяет **Партнерам** добиться экономии при организации систем Управления Посетителями, так как не требует использования **«Физических карт»**.

- Позволяет Специалистам по Безопасности установить **«Время валидации Приложений»** и **«Количество допустимых Валидаций»** для эмиссии **«Токенов Авторизации» (Auth Tokens).** Этот механизм упрощает Систему **«Управления Посетителями в рамках корпоративного управления»**, потому-что сотрудник службы безопасности не должен иметь дело с номерами карт, которые хранятся внутри «**Системы Контроля Доступа»**. Другими словами, Специалист службы безопасности должен контролировать данные **Front End**.

- Если Пользователь меняет телефон, необходимо просто **«Отменить» (Dismiss) «Токен Авторизации»** внутри оригинального телефона и выполнить процедуры Авторизации снова.

AAVENT IDETRIS

Преимущества AUTH технологии IDETRIS-APP:

- Пользователь вносит символическую **плату только один раз** за **один номер виртуальной карты**. Другими словами, если конечный пользователь переключится на новый телефон с исходным номером карты, дополнительной платы **НЕТ**!

- В качестве физического «Удостоверения» или ID, в рамках проекта может быть использована **карта без чипа**, Задачи доступа решает – виртуальная крипто-карта, что обеспечивает большую экономию.

- Поскольку оплата производится только **один раз за один номер карты** и можно установить период проверки виртуальной карты, это делает управление посетителями более эффективным и экономичным.

- **Виртуальные карты** не изнашиваются и не приходят в негодность.

- **«Токен авторизации» (Auth Token)** приложений можно удаленно отправить на авторизованный телефон по электронной почте, что может помочь сэкономить много времени. В итоге, можно простым образом реализовать концепцию **«Централизованной авторизации» (Centralized Auth)** на любом корпоративном уровне.

- Новый считыватель **@Mini Bluetooth** поддерживает передачу данных «Wiegand IN» и «Wiegand OUT», его можно установить рядом с существующим считывателем, где клиент по-прежнему может использовать физические карты с исходным считывателем, но новые учетные данные с Bluetooth. Это поможет покупателю сэкономить средства, но одновременно использовать все функции Bluetooth. Это приложение является эффективным, если Конечному пользователю требуется учет большого количества временных сотрудников или посетителей.

AAVENT IDETRIS

ADVENT SYSTEMS
Москва, Бизнес-ТехноПарк G10
Киевское ш., домовладение 3, стр. 1
4 этаж офис XCIII (офис 93)

+7(499) 213 00 58
info@sprx.ru

www.advent-id.com
IDETRIS