ESMART® Доступ

Виртуальные карты

esmart.ru

Мобильное приложение

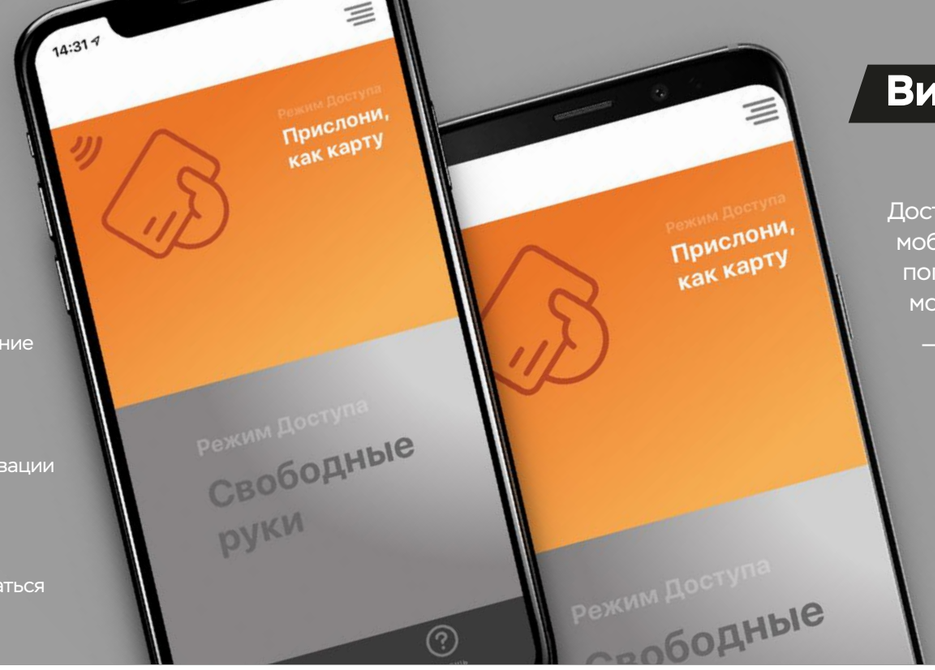
Прислони, как карту

Используйте ваш телефон, как бесконтактную карту, для считывания подносите его вплотную к считывателю. Режим работает по **NFC** и **BLE**.

Свободные руки

Не требует подносить телефон вплотную. Считывание происходит при вашем приближении, начиная с 10 метров, даже если телефон лежит в кармане. Режим работает только по **BLE**.

esmart.ru/access



Виртуальные карты

Доступ по виртуальным идентификаторам для мобильных телефонов становится все более популярным в современных СКУД. К плюсам мобильной идентификации относятся:

– удобство выдачи карты пользователю без личного участия, по e-mail или другим способом

– смартфон всегда с собой и может полностью заменять карты и метки

– передача телефона третьим лицам происходит крайне редко, что исключает махинации с контролем доступа или учетом рабочего времени.

Технология ESMART® Доступ

Виртуальные карты работают с помощью технологии ESMART® Доступ и имеют пять степеней защиты от копирования и подделки:

- Шифрование **AES-128**
- **Диверсификация** ключей шифрования
- **CMAC** подпись идентификатора
- Защита от **Replay-атак**
- Гарантия **уникальности** идентификатора

Благодаря им мобильная идентификация становится такой же безопасной, как и идентификация с помощью физических карт.

Покупка виртуальной карты

Штатные методы идентификации мобильных устройств по NFC или с помощью банковской карты из Apple Pay, Google Pay и др. имеют ряд существенных недостатков:

- **вариативность работы от модели телефона**
- **нарушение требований банков при работе с персональными данными**
- **отсутствие функции «Свободные руки»**
- **возможность подделки**

Покупка виртуального идентификатора ESMART® Доступ гарантирует пользователю удобство и безопасность мобильной идентификации на любых устройствах.

Передача кода активации

Код активации выдается конкретному пользователю системы Администратором СКУД и не рассчитан на передачу другим пользователям.

Таким образом, **код активации** каждой виртуальной карты **действителен только один раз**, повторное получение карты по нему на этом же или другом телефоне невозможно.

Это реализует защиту от несанкционированной передачи кода стороннему пользователю, повышая уровень безопасности.

Утрата виртуальной карты

К виртуальным картам стоит относиться так же, как и к физическим, важно иметь в виду, что

- стирание идентификатора
- удаление приложения
- сброс телефона к заводским настройкам
- восстановление телефона из резервной копии

приведет к **безвозвратному удалению мобильного идентификатора без возможности его восстановления**.

Это сделано в целях безопасности, по аналогии с потерей реальной физической карты.

Работа приложения в фоновом режиме

iBeacon

Технология **iBeacon** позволяет «разбудить» мобильный телефон на iOS при приближении к считывателю, даже если приложение было завершено. Время срабатывания зависит от iOS и может варьироваться системой.

Restore State

Технология **Restore State** дополнительно восстанавливает работу завершенного пользователем приложения, если это случилось в поле видимости хотя бы одного считывателя ESMART® Reader.

Геопозиция

Для нормальной работы обеих технологий требуется дать разрешение мобильному приложению доступ к **геопозиции «Всегда»**: «Настройки» > «Конфиденциальность» > «Службы геолокации».

Виджет ESMART®

Платформа Android имеет меньше доступных инструментов. Наличие **виджета ESMART®** в области нотификаций смартфона позволяет максимально долго сохранять свернутое мобильное приложение работоспособным. Завершенное пользователем приложение можно запустить автоматически только при использовании NFC, для BLE это недоступно.

Технические характеристики

Поддержка мобильных устройств	iOS 9.0 и выше с BLE Android 4.4 и выше с BLE, а также NFC HCE
Дистанция считывания	NFC: до 10 см, Bluetooth Low Energy: до 10 м
Режимы доступа	«Прислони, как карту» (для iOS по BLE, для Android по NFC, BLE) «Свободные руки» (для iOS и Android по BLE)
Настройка расстояния срабатывания по BLE	**На стороне считывателя с помощью Конфигурации** • отдельно для каждого из режимов доступа • отдельно для iOS и Android • ограничение общей дальности (например, для турникетов) **На стороне приложения самим пользователем** • отдельно для каждого из режимов доступа (устаревающий режим, не рекомендуется для новых внедрений)
Настройка частоты срабатывания	Только для BLE, в секундах
Безопасность	• Защищенная технология ESMART® Доступ • Безопасное хранение идентификатора карты средствами ОС • Связка идентификатора с уникальным UUID телефона, без участия IMEI и IMSI

Этап 1 Добавление карты в СКУД

Способ 1

Импорт идентификаторов из таблицы в контроллер

После приобретения виртуальных карт на e-mail администратора СКУД, отправляется таблица соответствия идентификаторов карт их кодам активации.

Администратор добавляет идентификаторы в софт СКУД-контроллера, используя стандартный метод импорта таблицы, реализованный производителем софта.

Затем сообщает пользователям коды активации виртуальных карт удобным для себя образом.

Способ 2

СКОРО

Импорт из личного кабинета ESMART® Конфигуратор

Администраторы СКУД получают возможность выдачи и управления виртуальными картами с помощью приложения **ESMART® Конфигуратор**.

Приобретенные карты отобразятся в приложении, с возможностью отправки кода активации на e-mail пользователя. Идентификатор каждой карты доступен администратору для внесения в СКУД.

Для управления картами зарегистрируйтесь в мобильном приложении, используя **e-mail**, указанный при заказе карт.

Способ 3

СКОРО

Интеграция контроллеров с ESMART® Доступ API

Технология выдачи и управления виртуальными картами ESMART® Доступ становится свободно доступной для сторонних производителей СКУД-контроллеров.

Открытый API позволяет производителям легко интегрировать виртуальные карты в собственные программные платформы и продукты. Глубокая интеграция позволит администраторам СКУД выдавать виртуальные карты **привычным способом** (как физические), в уже знакомом интерфейсе софта производителя.

Пользователю останется активировать виртуальную карту с помощью кода, полученного по e-mail.

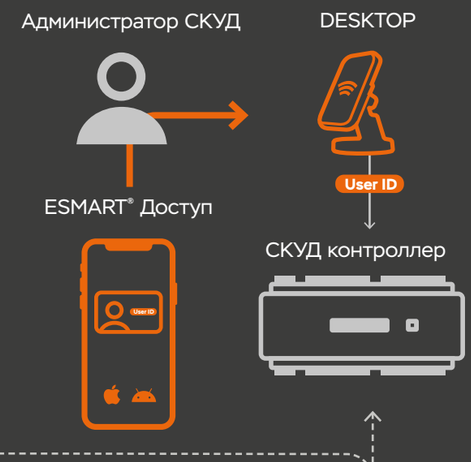
Способ 4

Прописывание через контрольный считыватель

Классический способ внесения идентификаторов в софт контроллера СКУД с использованием настольного к**онтрольного USB-считывателя**. Контроллер переводится в режим записи идентификаторов, которые подносятся к контрольному считывателю.

Администратор СКУД просит пользователя поднести свой телефон к контрольному считывателю **ESMART® Reader DESKTOP**, который поддерживает **NFC** и **BLE** и передает идентификатор карты в контроллер.

Способ работает только после активации виртуальной карты на телефоне пользователя.

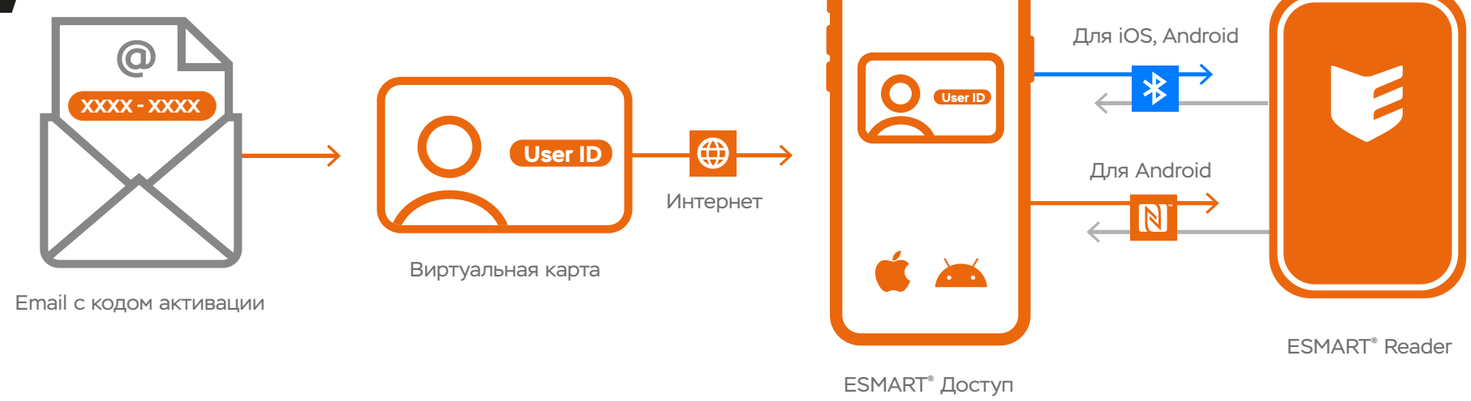


Этап 2 Активация и использование карты

В процессе получения виртуальной карты пользователю системы СКУД приходит **код активации** от **ESMART® Доступ API** или непосредственно от **Администратора СКУД** (Способ 1).

Для начала работы требуется **скачать** мобильное приложение **ESMART® Доступ** и ввести в него код активации. После ввода кода активации приложение получит виртуальную карту через Интернет. Для дальнейшей работы подключение к Интернет больше не требуется.

После того, как карта активирована, приложение готово к передаче идентификатора **(User ID)** в считыватели ESMART® Reader по **NFC** и **BLE**.



ESMART® Доступ SDK

Набор разработчика ESMART® Доступ для платформ iOS и Android основан на Библиотеке libEsmartVirtualCard.

Подключив ее, клиентское приложение получает возможность передавать идентификатор пользователя, с помощью **BLE** и **NFC** в считыватели ESMART® Reader, используя защищенную технологию ESMART® Доступ.

Поставляется в комплекте **с одним считывателем** ESMART® Reader DESKTOP серии USB и **одним месяцем технической поддержки** по встраиванию.

Требования к инфраструктуре

Перед встраиванием SDK ESMART® Доступ клиенту требуется подготовить собственную инфраструктуру, которая должна включать три ключевых составляющих:

- реализованный на стороне клиента, сервер выдачи идентификаторов, имеющий связь с мобильным приложением (с достаточным уровнем безопасности)
- настроенная работающая система СКУД
- реализованная клиентом схема интеграции системы СКУД с сервером выдачи идентификаторов по API или иным способом на усмотрение клиента.

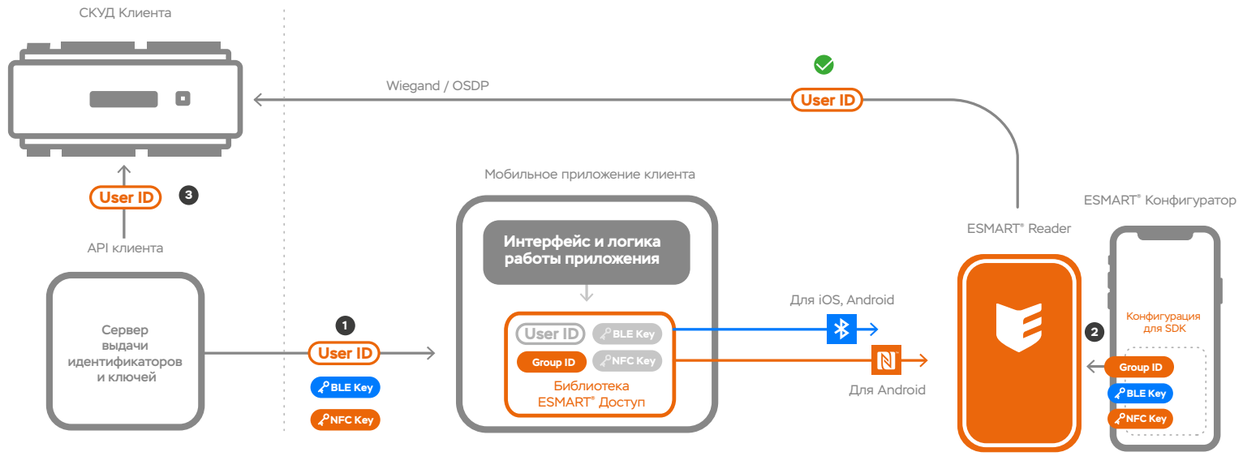
Только после реализации всех трех составляющих стоит приступать к встраиванию SDK.

Три этапа при встраивании SDK

1. На первом этапе загрузите в Библиотеку:
   - User ID идентификатор пользователя
   - NFC Key ключ для обмена по NFC
   - BLE Key ключ для обмена по BLE
   - Group ID уникальный идентификатор SDK
2. На втором этапе сконфигурировать считыватель, загрузив:
   - NFC Key ключ для обмена по NFC
   - BLE Key ключ для обмена по BLE
   - Group ID уникальный идентификатор SDK
3. User ID На третьем этапе необходимо загрузить идентификатор пользователя в СКУД контроллер.

При поднесении телефона к считывателю произайдет обмен защифрованными данными, которые будут отправлены в контроллер.

Схема СКУД при реализации мобильной идентификации с помощью ESMART® Доступ



Основная функция Библиотеки ESMART® Доступ заключается в осуществлении безопасной передачи идентификатора пользователю из мобильного приложения клиента в считыватель по NFC и BLE.

Фактически, Библиотека отвечает только за «транспортную» функцию, логика работы приложения, а также пользовательские сценарии реализуются клиентом на свое усмотрение.

www.esmart.ru
sale@esmart.ru

+7 (495) 133-00-13

Сделано в России

«ESMART® Доступ
Виртуальные карты»
v.01 01.06.2020