

Powering the trusted identities of
the world's people, places & things

От чипа к виртуальному идентификатору. Тенденции безопасной идентификации. Как осуществить миграцию на высокостащенные технологии в существующей СКУД.

21 ноября 2019

Сергей Гордеев – Региональный менеджер по продажам HID Global

Основные вопросы

- Эволюция бесконтактных технологий идентификации: от Prox-карт до мобильных идентификаторов
- Миграция на высокозащищенные технологии
- Основные тенденции в СКУД



«... Безопасность — это категория неизмеримо более высокая, чем величие».

**Арман Жан дю Плесси,
герцог де Ришельё**

(1585 – 1642)



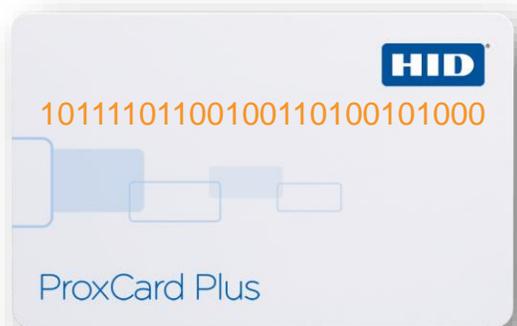
Эволюция бесконтактных технологий



1-ое поколение: EM, HID Prox, Indala

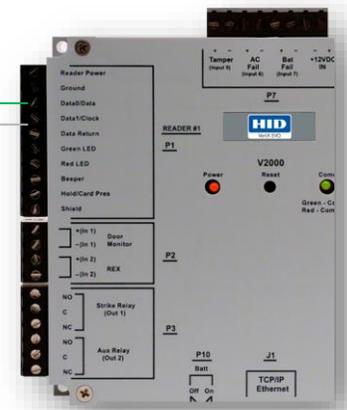
- Низкочастотная технология (125 кГц)
- Единственная функция – передача идентификационного признака
- Идентификационная информация хранится в открытом виде
- Отсутствие режима аутентификации

Первое поколение: 125кГц Proximity – No Encryption



Data 0

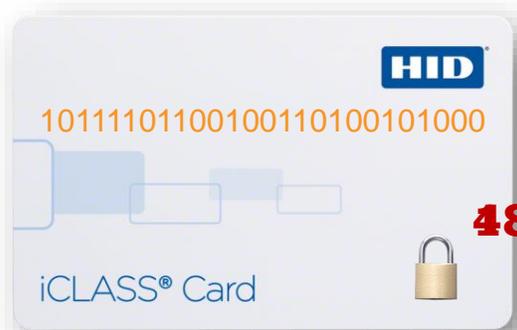
Data 1



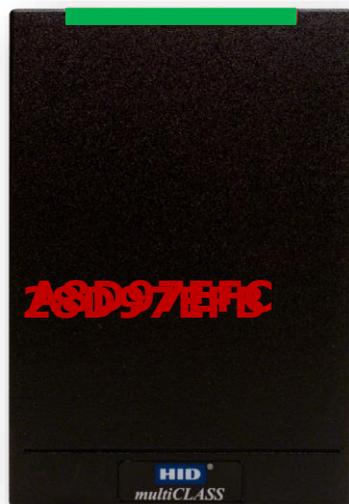
2-ое поколение: карты и считыватели Mifare Classic, iCLASS, Legic

- Частота: 13,56 МГц
- Поддержка разных приложений - защищённая область памяти, разбитая на независимые области
- Идентификатор СКУД хранится в открытом виде
- Взаимная аутентификация (диверсификационные ключи длиной 8 байт)

Второе поколение: Смарт-карта 13,56МГц с памятью, взаимная аутентификация

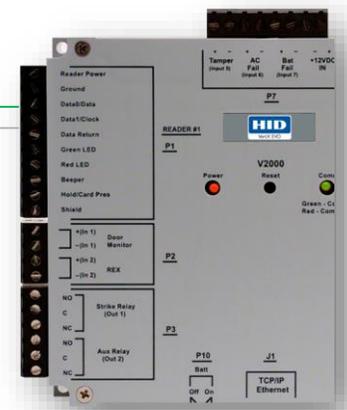


48B93EFD



Data 0

Data 1



3-е поколение: iCLASS SE, DESFire

- В считыватель добавлен специальный модуль SAM
- Идентификатор СКУД хранится в виде SIO (ключ шифрования 16 байт + ключ для цифровой подписи 12 байт)
- Многоуровневая аутентификация

Secure Identity Object (SIO)

- Безопасный объект идентификационных данных (SIO) усиливает безопасность существующих идентификационных технологий
- SIO добавляет дополнительный слой защиты в добавлении к тем, которые обеспечиваются технологией носителя
- SIO можно записать практически в любой носитель с памятью. Например, SIO может храниться на картах iCLASS, MIFARE Classic, DESFire EV1, iCLASS Seos и на мобильных устройствах, оснащённых хранилищем Seos.



Что из себя представляет SIO?

- В SIO используются лучшие практики по созданию многоуровневой безопасности:
 - Шифрование информации
 - Привязка к выбранному носителю
 - Цифровая подпись информации



4-ое поколение: Seos

- Усиленная защита информации (6 ключей длиной 16 байт + ключи для SIO, динамический CSN)
- Портруемость
- Независимость от аппаратной платформы и коммуникационного интерфейса

Ключевые особенности современных бесконтактных технологий

- Идентификатор – это программа (апплет), которая выполняется на безопасной компьютерной платформе, такой как чип бесконтактной микропроцессорной смарт-карты
- Применяется многоуровневая модель защиты данных
- Идентификационная технология обеспечивает возможность одновременного использования карты для множества независимых приложений
- Идентификатор не зависит от вида коммуникационного интерфейса и от носителя

Основные вопросы

- Эволюция бесконтактных технологий идентификации: от Prox-карт до мобильных идентификаторов
- **Миграция на высокозащищенные технологии**
- Основные тенденции в СКУД

Почему нужен апгрейд системы?

- Привести уровень безопасности к требованиям сегодняшнего дня
- Слияние, приобретение компаний, новые владения ...
- Использование карт для других целей (не только для доступа)
- Требуется контактный чип для PKI
- Повышение удобства для клиента (мобильный доступ)

Пути апгрейда



Вариант №1: Мультитехнологичные карты

- Преимущества:
 - Считыватели заменяются постепенно > поэтапные затраты
 - Выпуск карт может также быть постепенным
- Недостатки:
 - Мультитехнологичные карты – более дорогие
 - Уязвимость в безопасности существует до тех пор, пока не заменены полностью все считыватели

Вариант №2: Мультитехнологичные считыватели

- Преимущества:
 - Карты заменяются постепенно > поэтапные затраты
 - Выдача новых карт может осуществляться в рамках уже существующего процесса на предприятии (износ, потеря, приём на работу/увольнение сотрудников)
- Недостатки:
 - Мультитехнологичные считыватели – более дорогие
 - Уязвимость в безопасности существует до тех пор, пока на считывателях не отключена поддержка старой технологии



Вариант №3: Полная замена карт и считывателей

- Преимущества:
 - За один этап реализуется современная безопасная система доступа
 - Общая стоимость затрат на оборудование меньше
- Недостатки:
 - Большие единовременные инвестиции
 - Считыватели должны быть заменены в короткий период > большие расходы на установку
 - Карты должны быть заменены одновременно > административные расходы



Рекомендации по миграции

1

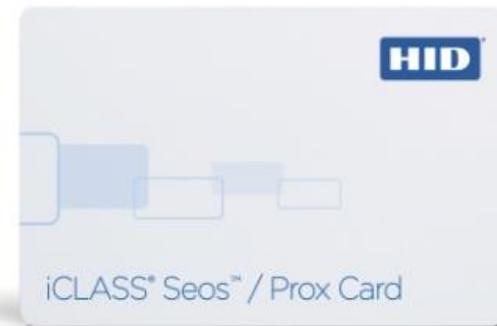
Определитесь с
новой технологией

2

Проведите
модернизацию
считывателей

3

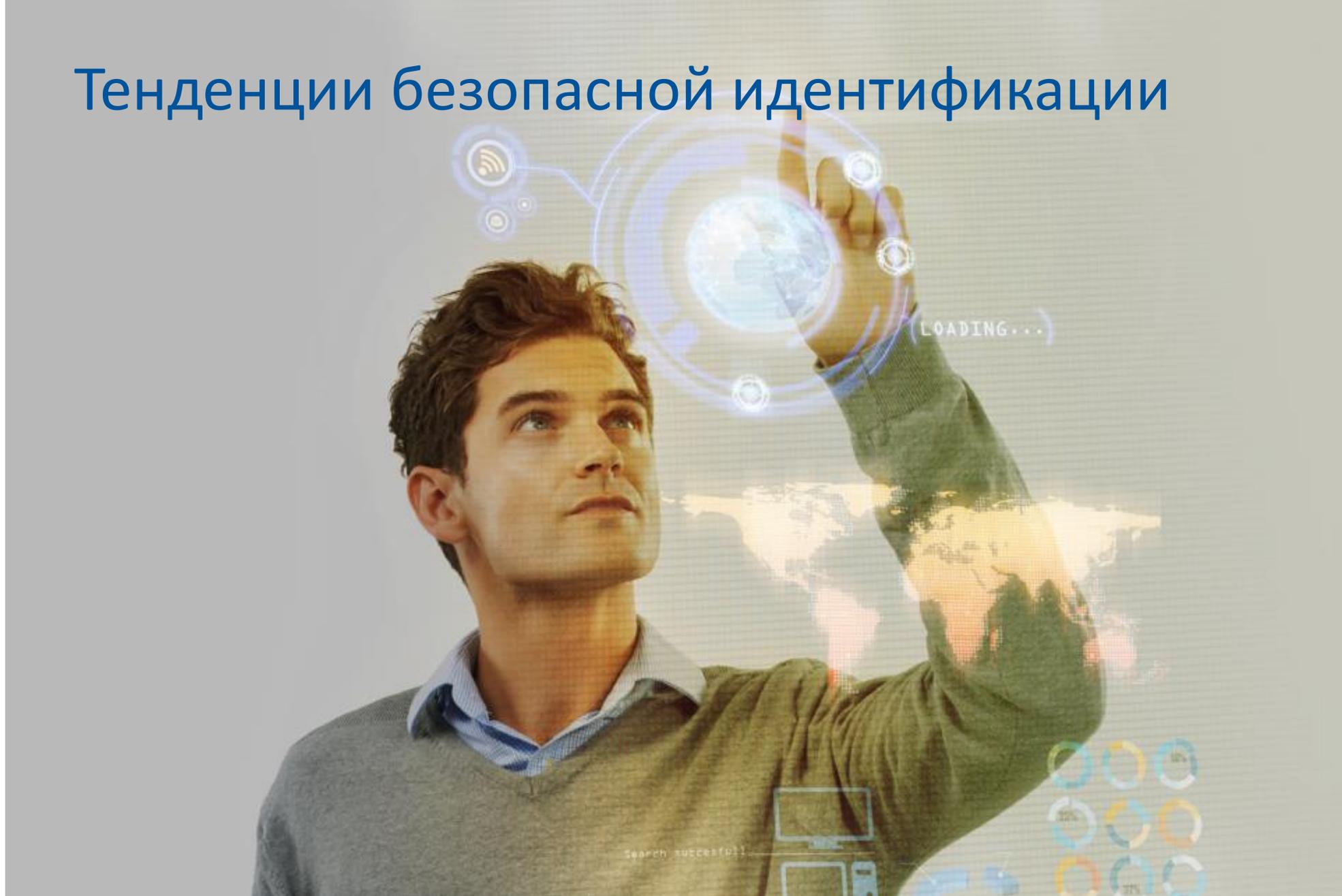
Проведите
модернизацию
идентификаторов



Основные вопросы

- Эволюция бесконтактных технологий идентификации: от Prox-карт до мобильных идентификаторов
- Миграция на высокозащищенные технологии
- Основные тенденции в СКУД

Тенденции безопасной идентификации



1. Безопасность

Цифровая безопасность в физическом доступе



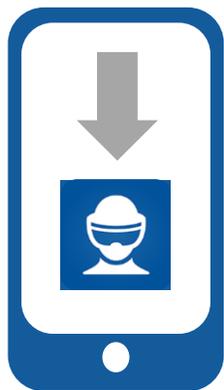
HID AR (Augmented Reality) Reader Tool

Добро пожаловать в мир дополненной реальности



HID AR Reader - это новое мобильное приложение, использующее технологию дополненной реальности для сбора цифровых данных (3D) о считывателях HID Global и их переноса в реальный мир!

Что требуется для начала работы



**СКАЧАТЬ
ПРИЛОЖЕНИЕ**

HID AR Reader Tool



СКАЧАТЬ и РАСПЕЧАТАТЬ

AR Marker



<http://bit.ly/HIDARMARKER>



**ПРОЧИТАТЬ
ИНСТРУКЦИЮ ПО
ИСПОЛЬЗОВАНИЮ**

<http://bit.ly/HIDARREADER-HOWTOUSE>

Как это работает



Разместите
маркер на
поверхности



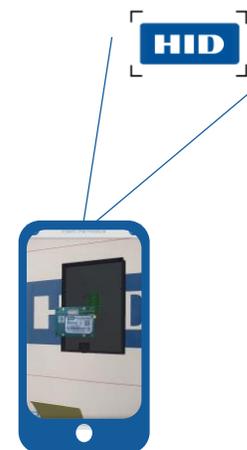
Запустите
приложение



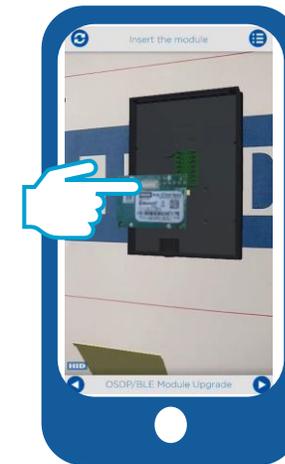
Выберите
считыватель



Выберите тип
задачи



Сканируйте
маркер камерой
смартфона



Очередной шаг
подтвердите
нажатием на
экран

Reader Manager

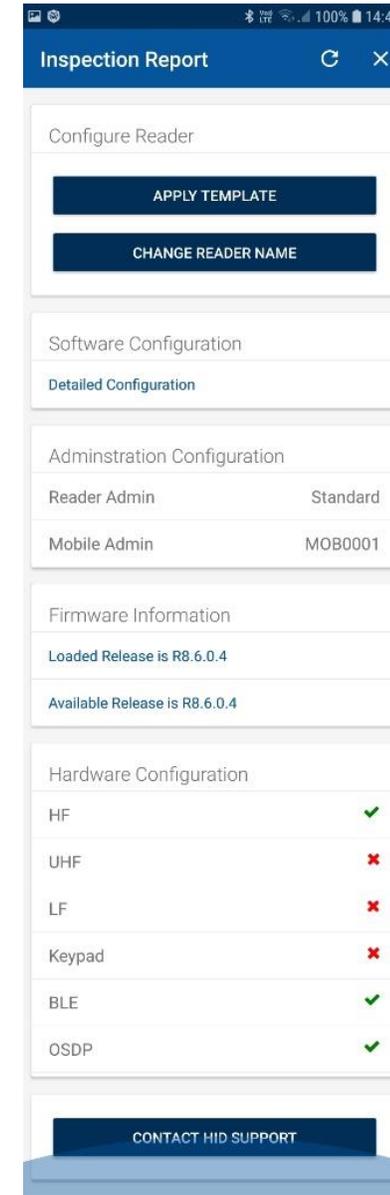
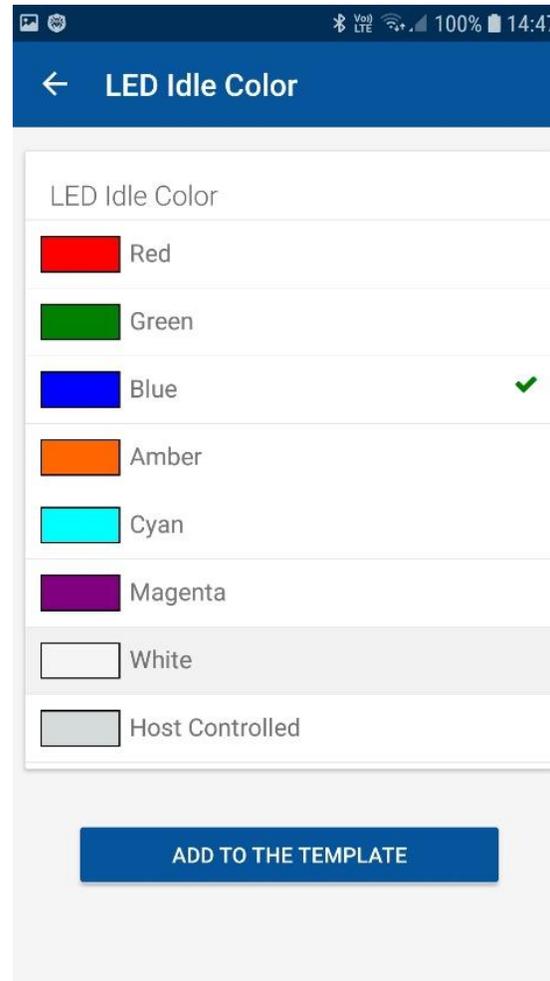
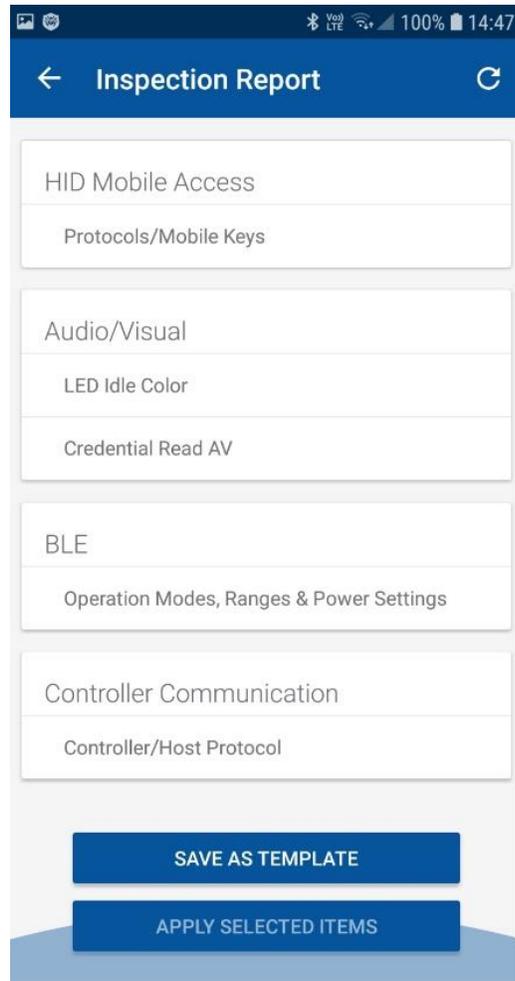
Как получить считыватель в требуемой конфигурации?

1. Изначально заказать в нужной конфигурации
2. Заказать конфигурационную карту или подготовить её самостоятельно с помощью программатора
3. READER MANAGER

Reader Manager Inspect – Configure – Upgrade

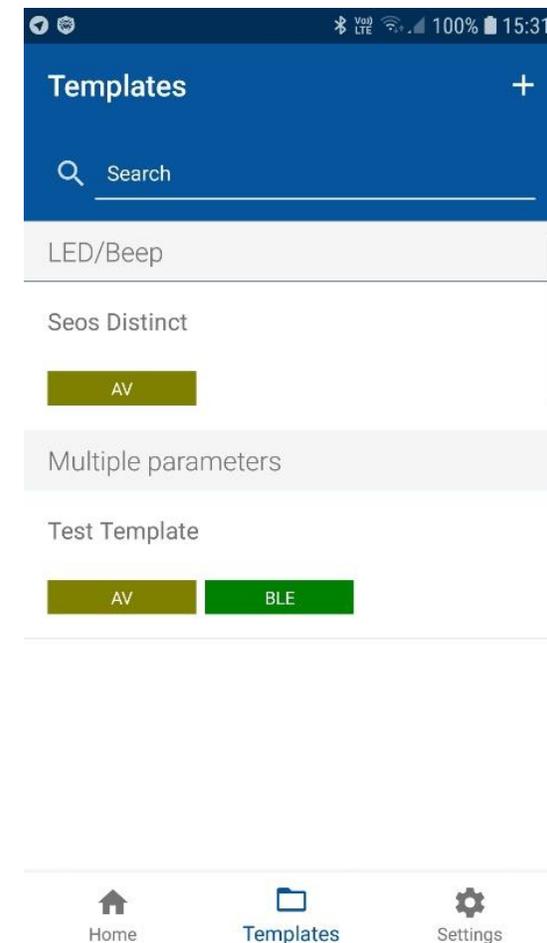


Инспектирование



Конфигурирование

- Reader Manager позволяет:
 - настраивать светодиодную и звуковую индикацию
 - изменять интерфейс считывателя (Wiegand <-> OSDP)
 - управлять мобильными ключами MOB/ICE
 - больше нет необходимости в карте Mobile Key Card
 - настраивать параметры мобильного доступа без необходимости использования карты Mobile Admin Card
 - больше нет необходимости в BLE Config App
 - создавать шаблоны, содержащие несколько конфигурационных параметров
 - шаблонами можно делиться



Upgrade

- Обновление прошивки считывателя

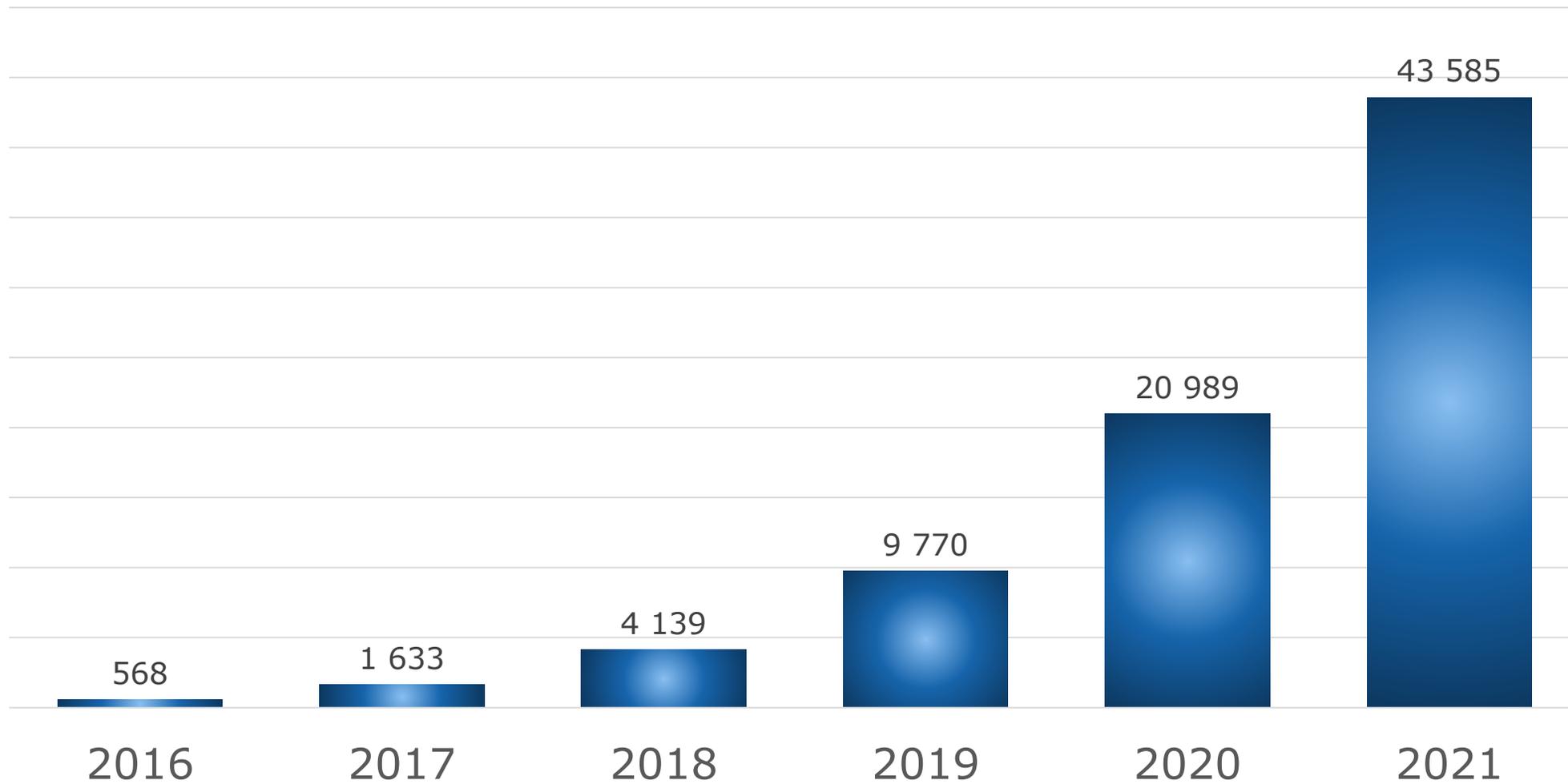
BLE Upgrade Kit (BLE-модуль, экранирующая наклейка, инструкция)

2. Мобильный доступ

Мобильный доступ достигает переломного момента для массового принятия



Прогноз глобальных продаж мобильных идентификаторов (тысячи)



© 2017 IHS Markit

Мобильный доступ

Безопасен

Эффективен

Удобен

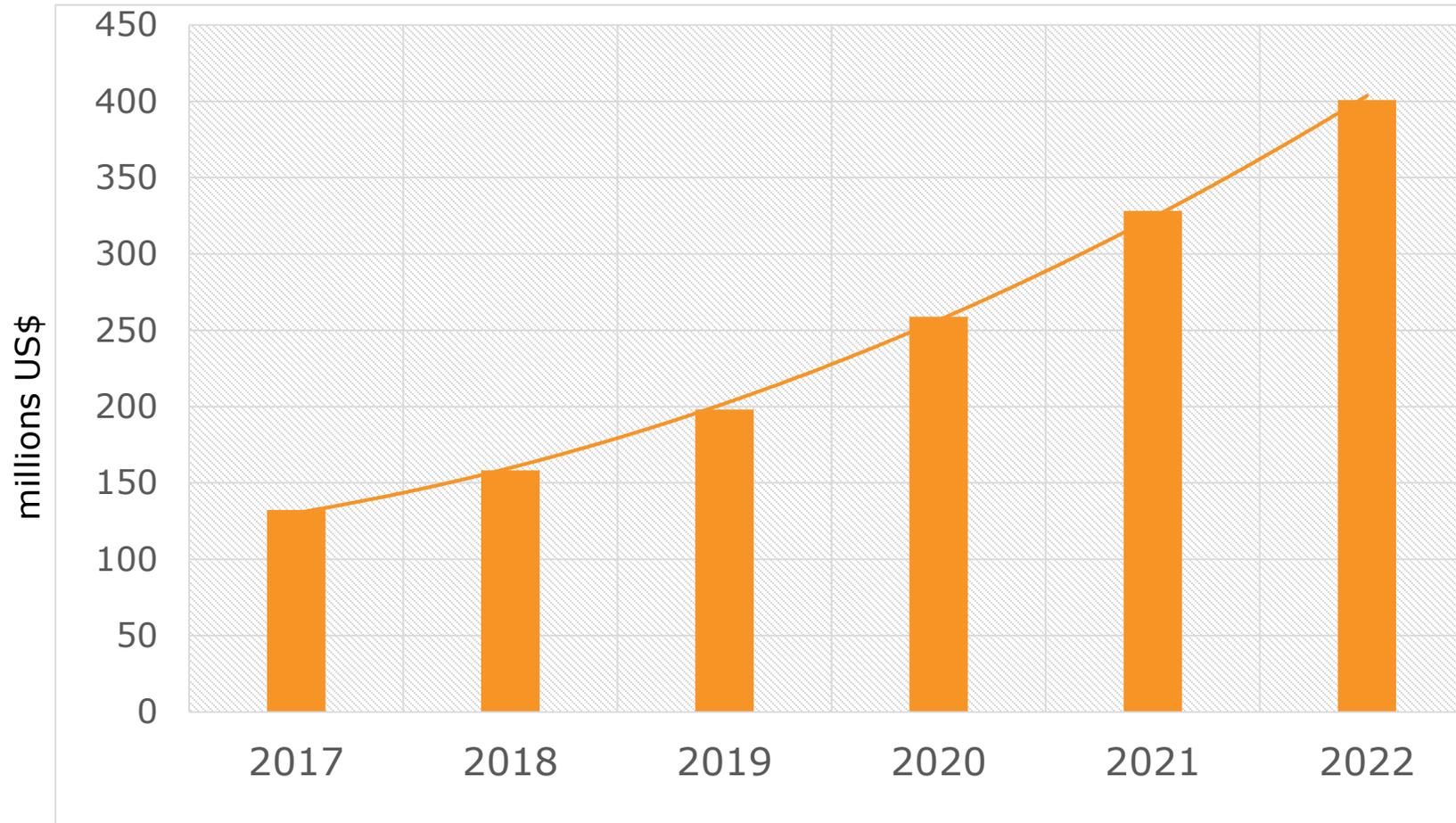


3. Облачные технологии

Организации используют преимущества облака



Прогноз облачного контроля доступа



© 2017 IHS Markit

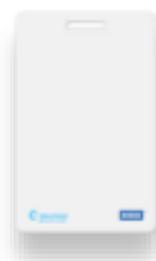
Оптимизация рабочего пространства



Метки-маяки

Шлюзы

Панель мониторинга



BLE



Real Time Data



Wifi



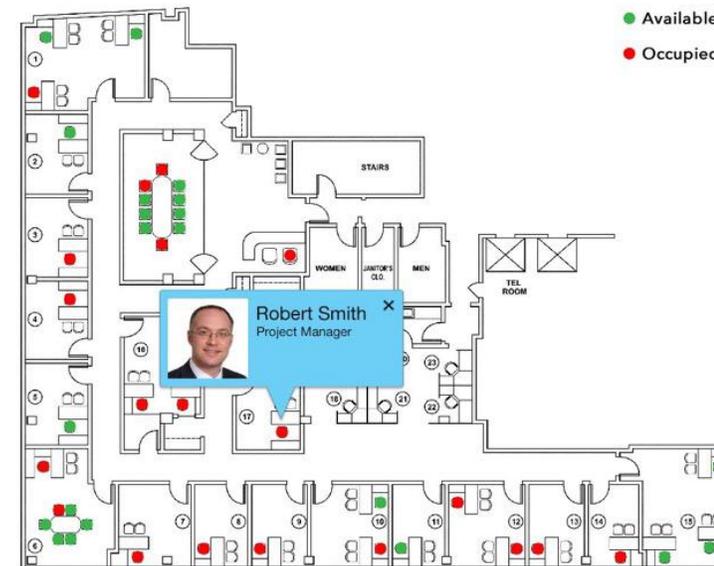
Real Time Data



Location Services

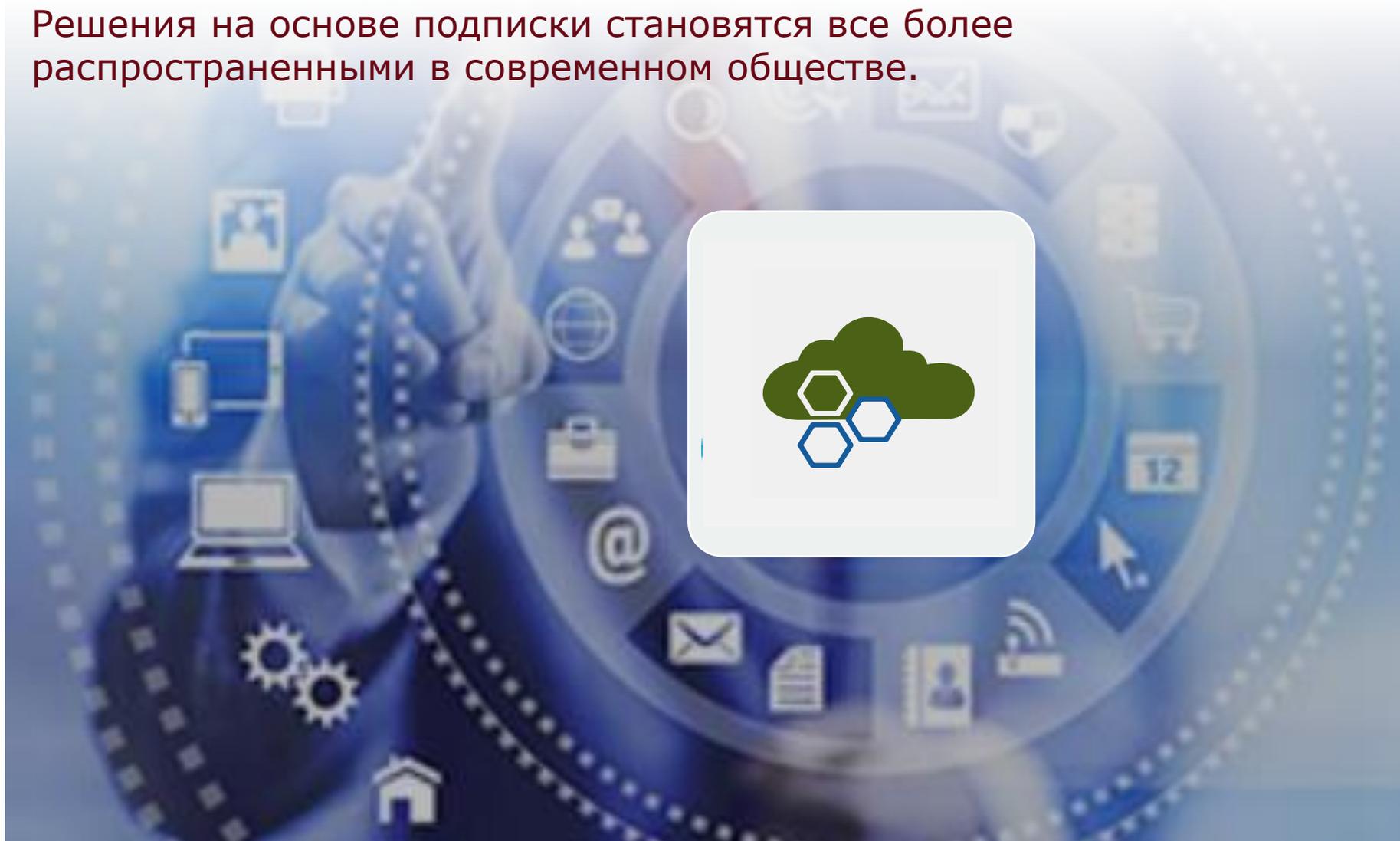
Оптимизация рабочего пространства

- Определение местонахождение посетителей и сотрудников в режиме реального времени
- Местонахождение людей в случае чрезвычайной ситуации и эвакуации
- История занятости офисных помещений

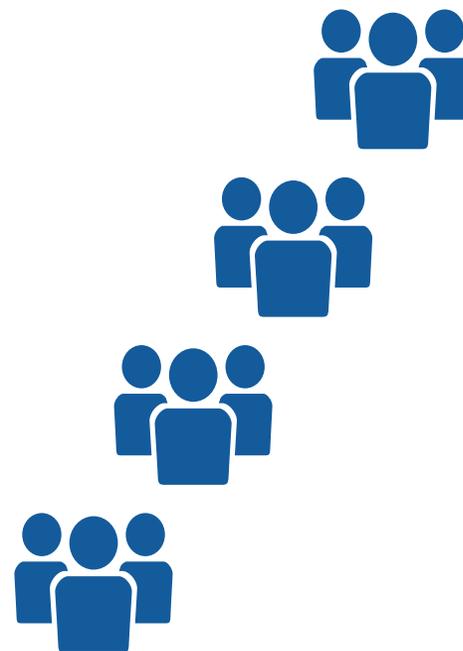


4. Эволюция бизнес-моделей

Решения на основе подписки становятся все более распространенными в современном обществе.

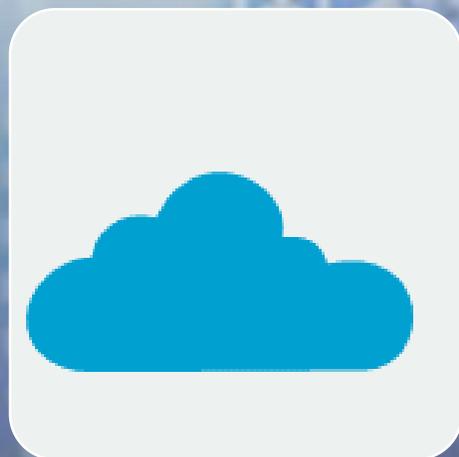


Преимущества подписки



4. Анализ данных

Анализ данных будет использоваться для моделей прогнозирования и других новых возможностей



Предиктивная безопасность в СКУД

- Позволяет организациям прогнозировать и предотвращать возможные угрозы на основе контекстного анализа данных из множества устройств и систем безопасности
- Используется для идентификации человека, устройства, приложения или сети, которая имеет более высокую вероятность стать угрозой.
- Раннее выявление отклонение от норм, которые могут помочь идентифицировать инциденты с безопасностью прежде чем они приведут к потере.

6. Новые технологии



FiRa Consortium (**F**ine **R**anging)

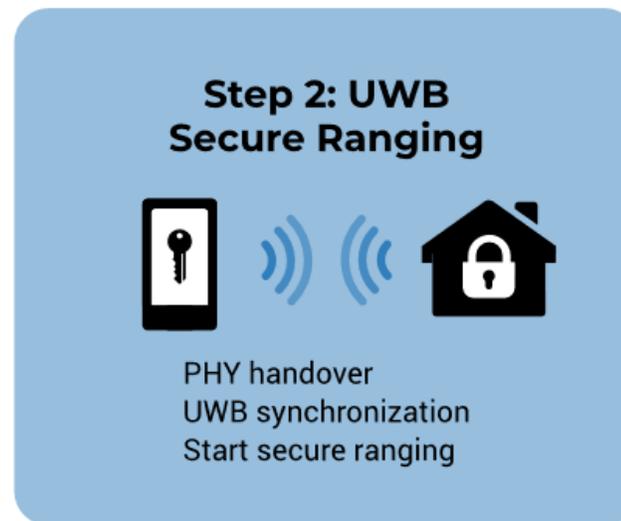
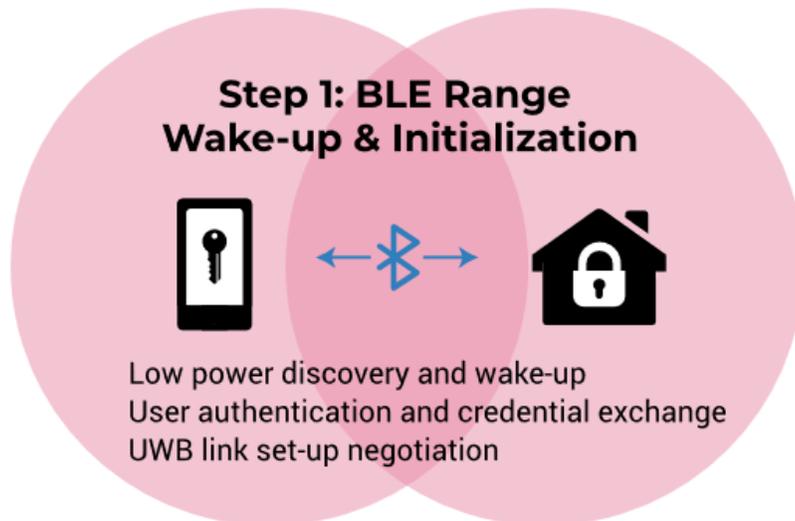
- Консорциум FiRa занимается разработкой и широким внедрением использования технологии сверхширокополосной связи Ultra-Wideband (UWB)
- Текущее управление консорциумом: HID Global, Samsung, NXP и Bosch

	Smart Home and Enterprises	Smart Cities and Mobility	Consumer	Smart Retail	Industrial and Healthcare
Hands-Free Access Control	<ul style="list-style-type: none"> • Residential access control • Restricted enterprise access 	<ul style="list-style-type: none"> • Smart parking garage • Keyless car access (standardized by CCC) 	<ul style="list-style-type: none"> • Logical access control 	<ul style="list-style-type: none"> • Unmanned store access 	<ul style="list-style-type: none"> • Barrier-free and restricted access control
Location-Based Services	<ul style="list-style-type: none"> • Employee mustering in emergencies 	<ul style="list-style-type: none"> • Ride sharing • Bike sharing 	<ul style="list-style-type: none"> • AR gaming 	<ul style="list-style-type: none"> • Indoor navigation • Foot traffic and shopping behavior analytics 	<ul style="list-style-type: none"> • Asset tracking • Patient tracking
Device-to-Device (Peer-to-Peer) Services	<ul style="list-style-type: none"> • Smart conference systems 	<ul style="list-style-type: none"> • Drone-controlled delivery • V2X*, autonomous driving 	<ul style="list-style-type: none"> • VR gaming and group play • Find someone nearby 	<ul style="list-style-type: none"> • Targeted marketing 	<ul style="list-style-type: none"> • Proximity-based patient data sharing • Find equipment

Основные преимущества технологии UWB

Обеспечивает беспрецедентную точность и безопасность при измерении расстояния до цели или определения положения

Превосходит другие технологии с точки зрения точности, энергопотребления, надежности и безопасности





Требования по безопасности будут расти с ростом потенциальных угроз



Мобильные телефоны будут все чаще использоваться для доступа



Применение облачных технологий повсеместно возрастет



Анализ данных приведет к укреплению безопасности и более высокой эффективности



Клиенты будут все больше требовать услуги, чем покупать продукты



Powering
Trusted Identities



Спасибо!

hidglobal.com