

СИСТЕМЫ МОБИЛЬНОГО ДОСТУПА КАК СДЕЛАТЬ ПРАВИЛЬНЫЙ ВЫБОР?

Умнов Алексей Валентинович
технический консультант HID Global

Первая коммерческая система мобильного доступа появилась более 4 лет тому назад — в сентябре 2014 года. Спустя некоторое время большое количество производителей, как отечественных, так и зарубежных, создали или только начали разрабатывать свои решения по мобильному доступу. При этом многие из таких решений делались наспех, поскольку производителями руководило стремление быть «в первых рядах».

В итоге ситуация на рынке систем мобильного доступа напоминает ситуацию, которая в свое время сложилась с цифровыми фотоаппаратами: большинство производителей «бросали пыль в глаза» потребителю размерами матрицы (чем больше, тем круче), но мало кто уделял внимание множеству других параметров (качество оптики, светосила, процессор обработки, ПО...), определяющих то, насколько хорошим может получиться снимок.

На сегодняшний момент времени, большинство мобильных СКУД обладают схожими друг с другом составными частями. Как правило, присутствует четыре основных компонента:

- мобильный идентификатор — виртуальная карта, хранящаяся на смартфоне;
- мобильный считыватель — устройство для считывания мобильного идентификатора и передачи его номера в контроллер СКУД;
- мобильное приложение — предназначено для получения и хранения мобильного идентификатора, а также для осуществления взаимодействия с мобильным считывателем;
- портал администратора — «облачный» сервис или приложение для ПК, служащее для выдачи/отзыва мобильного идентификатора на смартфон.

В данной статье я хочу рассмотреть параметры, на которые следует обратить внимание при выборе системы мобильного доступа, чтобы сделать действительно грамотный выбор.

ПОДДЕРЖИВАЕМЫЕ МОБИЛЬНЫЕ УСТРОЙСТВА

Начать нужно с вопроса о том, какие беспроводные интерфейсы поддерживаются считывателем? По-прежнему, у очень большого числа как специалистов, так и рядовых пользователей фраза «мобильная СКУД» прочно ассоциируется только с интерфейсом NFC. Однако поддержка одного лишь NFC неизбежно приведет к большим проблемам при использовании мобильных устройств компании Apple, которыми наверняка пользуется часть сотрудников практически

в любой организации. Во-первых, поддержка NFC появилась, лишь начиная с iPhone 6. Это означает, что более ранние устройства Apple автоматически выпадают из числа поддерживаемых в том случае, если считыватель обладает лишь интерфейсом NFC. Во-вторых, долгое время интерфейс NFC мог использоваться в iPhone лишь для одной задачи — выполнения бесконтактных платежей с помощью Apple Pay. Для сторонних разработчиков доступ к NFC в iPhone был закрыт до появления iOS 11, но даже в этой версии операционной системы разработчики получили доступ к NFC в режиме Read Only, чего недостаточно для обеспечения нормального взаимодействия между считывателем и мобильным приложением в рамках мобильной СКУД.

Помимо трудностей с поддержкой смартфонов iPhone, использование одного лишь интерфейса NFC приводит к другому существенному ограничению — малому расстоянию чтения мобильного идентификатора, речь идет лишь о нескольких сантиметрах. Поэтому, в качестве альтернативы NFC, стал активно применяться интерфейс BLE (Bluetooth Low Energy). Использование данного интерфейса позволяет увеличить расстояние считывания и значительно расширить количество совместимых устройств. Говоря о совместимых устройствах, хочется отдельно остановиться на смартфонах на базе Android. Многие производители таких устройств (особенно, если речь идет об относительно дешевых моделях) заявляют о поддержке как NFC, так и BLE. Но зачастую реализации этих интерфейсов зачастую оставляет желать много лучшего. По вполне очевидным причинам, производители мобильных СКУД не в состоянии протестировать работу их систем со все-

ми моделями Android-смартфонов, доступных на рынке. Однако, неоспоримым преимуществом для системы мобильного доступа будет являться наличие на официальном сайте производителя постоянно обновляемой информации о гарантированно совместимых смартфонах.

БЕЗОПАСНОСТЬ РЕШЕНИЯ

К сожалению, у нас по-прежнему довольно распространены случаи, когда при проектировании СКУД практически не уделяется никакого внимания тому, насколько хорошо защищена выбираемая система от тех или иных потенциальных угроз безопасности. В первую очередь, надо учитывать угрозы, связанные с копированием/клонированием идентификаторов и с возможным перехватом информации, передающейся по интерфейсам идентификатор-считыватель и считыватель-контроллер.

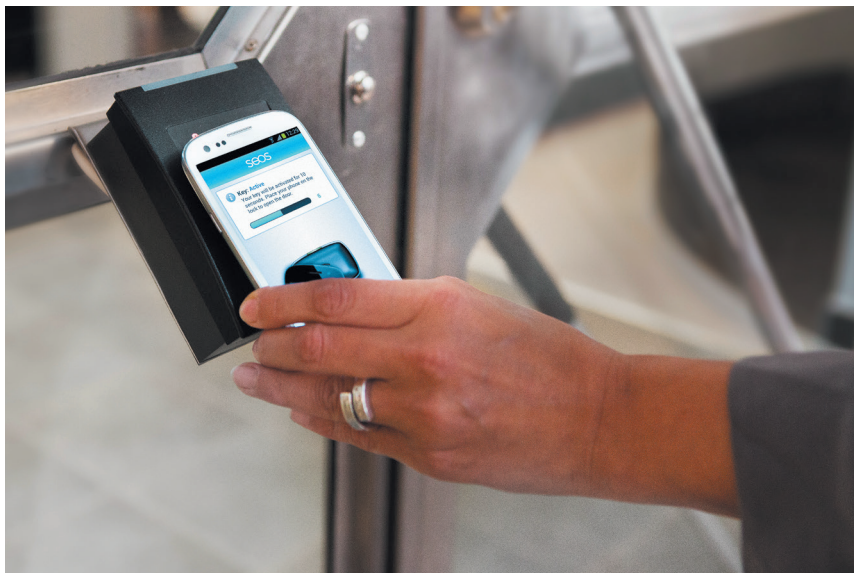
В применении к системе мобильного доступа, важно знать, как хранится мобильный идентификатор (в открытом или в зашифрованном виде, в открытой области памяти смартфона или в защищенной) и каким образом обеспечивается защита канала связи между считывателем и мобильным устройством (применяются ли дополнительные средства защиты помимо тех стандартных, что заложены в коммуникационной технологии)?

Дополнительным плюсом системы мобильного доступа является поддержка привязки мобильных идентификаторов к считывателям конкретного клиента. Это осуществляется с помощью специальных аутентификационных ключей, делаая систему уникальной для клиента и предотвращая саму возможность использования «чужих» мобильных идентификаторов (выпущенных на смартфонах пользователей других организаций).

Ну и, разумеется, говоря о безопасности, нельзя обойти стороной вопрос, связанный с соответствием мобильной СКУД федеральному закону о защите персональных данных (152-ФЗ). При выборе системы от зарубежного производителя следует поинтересоваться, соответствует ли мобильная СКУД новой Европейской директиве о защите персональных данных (GDPR), принятой в мае 2018 года, которая по своей строгости даже превосходит 152-ФЗ. Согласно этой директиве, ужесточается ответственность за нарушение правил обработки персональных данных — штрафы достигают 20 миллионов евро или 4% годового дохода компании (в зависимости от того, что больше).

УДОБСТВО РЕШЕНИЯ

Удобство является краеугольным фактором для того, чтобы система была принята и пользовалась успехом у конечных заказчиков из самых разных областей бизнеса.



Необходимо, чтобы обеспечивалась удобная выдача/отзыв мобильного идентификатора и удобное его использование. Самым комфортным с точки зрения выдачи является вариант, при котором мобильный идентификатор попадает на смартфон «по воздуху» с помощью сети Интернет.

Теперь давайте рассмотрим возможности, влияющие на удобство использования.

- Мобильный считыватель может поддерживать различные режимы считывания мобильного идентификатора со смартфона: «карточный» (полностью аналогичен использованию бесконтактной карты), считывание с расстояния (для запуска процесса считывания могут применяться различные способы, включая технологию жестов), использование виджета.
- Поддержка работы мобильного приложения в фоновом режиме и при заблокированном устройстве. Данная возможность позволяет использовать смартфон полностью аналогично карте (не требуется никаких дополнительных действий для активации идентификатора), и отсутствие такого режима может сильно сказаться на успешной адаптации системы.
- Одновременная поддержка нескольких мобильных идентификаторов в одном приложении с автоматическим выбором мобильных считывателем совместимого с ним (по аутентификационному ключу) идентификатора. Данная возможность позволяет уйти от ситуации, когда пользователь вынужден носить с собой стопку карт в случае, если ему требуется доступ в разные организации / на разные объекты.
- Считывание со смартфона после выдачи мобильного идентификатора должно происходить без необходимости интернет-соединения. В противном случае, это делает невозможным применение мобильной СКУД в тех точках, где отсутствует мобильная связь или Wi-Fi.

- Поддержка умных часов — это отдельная тема с точки зрения удобства использования. Если таковая имеется, то не лишним будет уточнить, какие платформы поддерживаются, потому что их разнообразие в часах даже шире, чем в смартфонах (Apple Watch, Android Wear, Samsung Tizen...). Также, надо выяснить, потребуется ли для смарт-часов отдельный мобильный идентификатор (независимый режим работы часов) или будет использоваться тот же самый, что хранится на смартфоне (совместный режим работы).

СОВМЕСТИМОСТЬ И ОТКРЫТОСТЬ РЕШЕНИЯ

Система мобильного доступа не будет пользоваться популярностью, если ее нельзя интегрировать в уже существующую в организации СКУД или если доступ по смартфону нельзя использовать одновременно с доступом по картам.

Поэтому очень важно, чтобы мобильные считыватели обладали стандартными интерфейсами связи, позволяющими их использовать совместно с большинством известных на рынке систем контроля доступа. К таковым интерфейсам относятся Wiegand и OSDP.

Кстати, поддержка OSDP тоже является очень сильной возможностью для мобильных считывателей. Было бы странным, если бы считыватель был высокозащищенным с точки зрения беспроводных интерфейсов, но не обеспечивал современного шифрованного канала связи с контроллером, каковым и является OSDP.

Если же говорить про поддержку тех или иных бесконтактных карт, то здесь подход простой — чем больше различных технологий поддерживает считыватель, тем лучше. Если, скажем, мобильный считыватель одновременно поддерживает чтение карт EM-Marine и Seos, то конечному заказчику можно будет предложить не только мобильный доступ, но и мигра-

цию с устаревшей и уязвимой технологии на современную и наиболее защищенную.

Современное решение также должно предоставлять возможности по его персонализации под заказчика. Как следствие, наличие SDK становится неотъемлемой чертой системы мобильного доступа. При помощи SDK можно не только изменить вид интерфейсов мобильного приложения и портала администратора, но и встроить доступ по смартфону в какое-либо стороннее решение, например, в гостиничную систему.

ЕДИНИЧНОЕ ИЗДЕЛИЕ ИЛИ ЭКОСИСТЕМА ПРОДУКТОВ

Наличие у производителя целого ряда различных устройств (а не только настенного считывателя), совместимых со смартфоном, является показателем основательности решения и возможности использования смартфона не только для физического доступа, но и для целого ряда других задач. Если, к примеру, доступен настольный USB-считыватель, то его можно использовать для автоматизации ввода номеров мобильных идентификаторов в ПО СКУД и для доступа к ПК/LAN/VPN с помощью смартфона.

А если доступны встраиваемые считывающие модули, то их можно использовать:

- Для реализации системы защищенной печати на принтере «Follow Me», в которой печать задания, отправленного на се-

тевой принтер, начнется лишь после того, как отправивший это задание пользователь подтвердит печать, поднеся свой смартфон к встроенному в принтер считывающему модулю.

- Для интеграции мобильного доступа в сторонние устройства, такие как турникет, ключница, биометрический считыватель и т.п.

ДРУГИЕ ХАРАКТЕРИСТИКИ

Помимо всего уже перечисленного выше, есть еще ряд параметров, которые могут стать существенными характеристиками при выборе системы мобильного доступа. К таковым можно отнести:

- Способ лицензирования, который используется для мобильных идентификаторов.

Есть два наиболее часто применяемых варианта. При первом пользователь приобретает мобильный идентификатор в так называемое «вечное» пользование — он будет работать на смартфоне до тех пор, пока сам смартфон находится в работоспособном состоянии. Однако потребуется покупка нового идентификатора в случае замены/потери/кражи смартфона.

Второй вариант — это подписная модель, в рамках которой приобретается лицензия, дающая право использовать мобильные идентификаторы на протяжении определенного времени. В течение времени подписки можно неограниченное коли-

чество раз перевыдавать мобильный идентификатор одному и тому же или разным пользователям на один и тот же или на разные мобильные устройства.

- Возможность и способы изменения тех или иных параметров считывателя (режимы считывания мобильного идентификатора, чувствительность, световая и звуковая индикация, выходной интерфейс и т.п.).

- Проверенность решения временем и различными условиями использования. Для того чтобы это определить, необходимо получить ответы на ряд простых вопросов:

- Как давно система предлагается на рынке и как она себя зарекомендовала среди инсталляторов и конечных пользователей?

- Какое количество реальных инсталляций есть на текущий момент времени?

- Какие отзывы можно найти о системе?

ЦЕНА

Разумеется, сравнивая различные системы мобильного доступа, нельзя уйти от ценового вопроса. Но я бы ни в коем случае не рекомендовал делать ее основополагающим критерием для принятия финального решения. Как это не банально прозвучит, но опираться нужно на соотношение цена/качество, которое и определяется тем множеством возможностей, которые мы рассмотрели выше.

НОВОСТИ

- Извещатель дымовой линейный OSI-R от Honeywell Fire Safety обеспечивает значительную невосприимчивость к движению конструкций, к фоновой засветке и защиту от ложных срабатываний. В качестве чувствительного элемента применяется КМОП-матрица, где формируется изображение квадратного отражателя, и интенсивность сигнала измеряется в каждой точке изображения. Для защиты от ложных срабатываний анализируется характер изменения изображения. Полное перекрытие оптической оси будет точно определено как неисправность. Также игнорируются точечные загрязнения рефлектора или наличие насекомых.
- HID Global® объявляет о доступности своей облачной платформы HID Origo™. Платформа HID Origo позволяет встраивать облачные подключения и функционал IoT-устройств в качестве расширений приложений в мобильные устройства, считыватели и контроллеры HID. Также разработчикам предоставляется прямой доступ к оборудованию через API-интерфейсы HID Origo и комплект разработчика программного обеспечения (SDK), уже проверенные с помощью решения мобильного доступа HID.
- Компания «АРМО-Системы» объявила о начале продаж оборудования для пожарной сигнализации торговой марки Smartec. На складе компании доступна адресная система серии VESTA, которая строится на принципе децентрализации и позволяет оснащать пожарной сигнализацией объекты любого масштаба. Линейка продуктов VESTA включает в себя приемно-контрольные приборы, извещатели, допол-

нительное оборудование и ПО для управления пожарной сигнализацией. При этом все оборудование Smartec для пожарной сигнализации имеет 5-летнюю гарантию производителя.

- В линейке устройств Bosch появился видеомонитор UML-554-90 с 55-дюймовым дисплеем и разрешением 4K Ultra HD, который способен отображать более 1 000 000 000 оттенков. Он обеспечивает передачу цветов с максимальной точностью и имеет высокую яркость и контрастность. При этом время отклика пикселя не превышает 6,5 мс, а наблюдать за происходящим на экране можно под углами вплоть до 178°/178° по горизонтали/вертикали. Для приема изображения используются не только традиционные порты HDMI, DVI и VCA, но и DisplayPort, чем UML-554-90 отличается от многих аналогов.
- Revisor Lab представляет новый интеллектуальный модуль интерактивного управления камерами SPEED DOME. Использование модуля позволяет осуществлять видеоконтроль на территории объектов большой площади, задействовав при этом минимальное количество оборудования и значительно сократив время реакции на тревожные события. Модуль может работать как в ручном (редакция STD), так и автоматическом режиме (редакция PRO). Интеллектуальный программный модуль интерактивного управления камерами Speed Dome позволяет обеспечить взаимодействие обзорной и PTZ-камеры для автоматического управления скоростными поворотными камерами.