NXP сегодня.

От новых проектов на MIFARE Plus EV1 и DESFire EV2 до fingerprint-карт

О ключевых трендах рынка бесконтактных технологий и иных по-настоящему востребованных рынком прорывных решениях, в том числе в таком новом сегменте, как автономные защищенные автомобили, журнал «ПЛАС» беседует с Виктором Сестреватовским, директором по развитию бизнеса в области банковских, транспортных и NFC-приложений, NXP Semiconductors.

КОНТАКТЫ
+7 917 568 25 80 (офис)
Admin.russia@nxp.com

ПЛАС: Транспорт остается ключевым сегментом для технологии MIFARE, которая в этом году отмечает свой 25-летний юбилей, кстати, как и наш журнал «ПЛАС». Каковы сегодняшние позиции MIFARE на современном рынке? Какие принципиальные изменения она претерпела и в связи с чем? Можно ли говорить, что сегодня MIFARE полностью закрывает вопросы, связанные с безопасностью?

В. Сестреватовский: Действительно, в 2019 году технология MIFARE отмечает двадцатипятилетие своего появления на рынке. Ее родиной является Австрия, где в 1994 году мир узнал о решении MIFARE Classic, предложенном нашей компанией (тогда еще Philips Semiconductors) для построения защищенных систем оплаты на транспорте. Первая бесконтактная транзакция по MIFARE Classic была осуществлена в Сеуле в 1996 году, где и был реализован первый в истории проект такого рода.

А уже в 2000-х годах линейка MIFARE дополнилась новыми защищенными продуктами MIFARE DESFire (2002 год) и MIFARE Plus (2009 год) на базе мощных и открытых криптоалгоритмов.

Как известно, компания NXP Semiconductors является полупроводниковой компанией, лидирующей в сегменте идентификации и выступающей родоначальником решений для построения автоматизированных систем оплаты проезда (АСОП) на транспорте, а также целого ряда инновационных бесконтактных технологий. Так, в 2002 году NXP Semiconductors совместно с коллегами из компании Sony разработала и представила на рынок технологию NFC, которая сегодня де-факто является функцией «по умолчанию» большинства современных мобильных и носимых устройств. Напомню, что своими корнями технология NFC опирается на технологию MIFARE (NXP) и FELICA (Sony). Также во многом стандарт ISO14443 отчасти базируется на решении MIFARE, особенно в рамках бесконтактного интерфейса.

В 2019 году технология MIFARE отмечает двадцатипятилетие своего появления на мировом рынке

Однако в связи со стремительным развитием технологий и вычислительных мощностей проприетарный криптоалгоритм CRYPTO1, который использовался в первом решении MIFARE Classic (на тот момент не было альтернатив данному криптоалгоритму), в 2008 году был скомпрометирован группой исследователей. Но уже до этого момента стало очевидным, что проприетарный криптоалгоритм с длиной ключа в 48 бит со временем должен быть заменен на более стойкий открытый со-

временный криптоалгоритм. Так, в 2002 году появилось первое поколение решения DESFire, которое базировалось на открытом симметричном криптоалгоритме DES, в 2006 году был представлен новый DESFire EV1 на основе открытого криптоалгоритма AES128.

А в 2009 году в массовое производство был запущен продукт MIFARE Plus, который на первом уровне безопасности (SL1) 100%-но эмулирует решение MIFARE Classic, а на третьем уровне безопасности (SL3) – работает с использованием открытой AES-криптографии. За счет использования мощного открытого криптоалгоритма AES, решения MIFARE DESFire EV2 и MIFARE Plus EV1 обеспечивают наивысшую безопасность и полностью (связка HW + SW) сертифицированы по уровню Common Criteria EAL 5+. Для сравнения – современные банковские чиповые карты в большинстве случаев сертифицированы по Common Criteria EAL 4+. Таким образом, по уровню безопасности современные защищенные решения MIFARE DESFire EV2 / Plus EV1 +V1 во многих случаях даже превосходят банковские карточные EMV-продукты и сопоставимы с такими электронными ID-документами, как электронные паспорта, ID-карты и водительские удостоверения. Не случайно существует ряд примеров использования MIFARE DESFire в водительских удостоверениях и других критически значимых проектах, таких как контроль доступа и микроплатежей.

Возвращаясь к транспортным проектам, отмечу, что на MIFARE DESFire уже много лет работают такие мегаполисы мира, как Лондон, Дубай, Дели, Бангкок, Стамбул, Мельбурн, Сан-Франциско и многие другие города.

В целом все решения для построения АСОП можно разделить на два больших кластера:

- Замкнутые системы – на основе симметричных криптоалгоритмов, таких как AES / DES / 3DES и т. д.
- Реально открытые системы – на основе асимметричной криптографии, когда используется PKI инфраструктура.

На сегодняшний день MIFARE продолжает активно развиваться и является лидирующим решением именно в замкнутых системах, управляемых непосредственно оператором

На сегодняшний день MIFARE продолжает активно развиваться и является лидирующим решением именно в замкнутых системах, управляемых непосредственно оператором.

ПЛАС: Какие современные технологические и бизнес-тренды можно выделить в системах оплаты проезда на транспорте?

В. Сестреватовский: Отмечу, что с учетом большой популярности бесконтактных технологий классических и EMV-карт в настоящее время наблюдается очень мощный тренд по конвергенции замкнутых и реально открытых систем. Ярким примером может служить Лондон, где транспортный оператор принимает банковские EMV-карты на всех турникетах, но так же продолжает работать и развивать свою замкнутую систему Oyster (аналог московской «Тройки») на базе решения MIFARE DESFire.

Чем обусловлен упомянутый тренд на конвергенцию этих систем? Не секрет, что транспортному оператору крайне интересно развивать собственную замкнутую АСОП, поскольку именно она позволяет ему полностью

В последние годы активно идет развитие различного рода альтернативных носителей бесконтактных технологий

контролировать свою базу пассажиров. Такие системы отличаются особой гибкостью с точки зрения разработки различных тарифов и механизмов их начисления, а также позволяют обеспечить значительные авансовые потоки по своим картам и остатки по счетам. С другой стороны, сегодня транспортные операторы так же заинтересованы и в осуществлении приема банковских карт. Такой подход позволяет обеспечить простой доступ к транспортным системам для потока туристов и приезжих пассажиров, которые, как правило, готовы немного переплатить, но избавить себя от необходимости покупать локальные транспортные карты.

Оптимальный результат достигается в варианте комбинирования замкнутой и открытой систем. В этом случае транспортный оператор получает максимальные преимущества как открытой, так и замкнутой системы. Например, такая интеграция может выглядеть следующим образом:

- Замкнутая система на основе мощной открытой криптографии используется как основное решение для сбора оплаты проезда жителей города.
- Открытая EMV-система используется как решение для одной/нескольких поездок для приезжих пассажиров/туристов и организовывается, например, на нескольких турникетах метрополитена или стационарных валидаторах наземного транспорта

На фоне этого глобального тренда, характерного, кстати, и для России, транспортный сегмент является фокусным для продвижения технологии MIFARE. По данным исследовательской компании ABI Research, по состоянию на начало 2019 года доля решений MIFARE в системах оплаты проезда на глобальном рынке транспортных проектов составляет порядка 75%, а АСОП на этой технологии работают в более чем 750 городах по всему миру.

ПЛАС: Какие области применения данной технологии помимо транспорта сегодня пользуются популярностью?

В. Сестреватовский: Кроме транспортной отрасли, решения MIFARE в версиях MIFARE DESFire и MIFARE Plus очень активно используются в системах контроля доступа, в системах лояльности, а также в системах микроплатежей. Всего к настоящему моменту на базе MIFARE функционируют более 40 различных приложений.

ПЛАС: Наиболее перспективные альтернативные форм-факторы (AIRTAG, браслеты, кольца), поддерживающие MIFARE, – что можно сказать с точки зрения их защищенности, простоты и удобства использования в различных носителях?

В. Сестреватовский: Исторически потребители привыкли к MIFARE-продуктам в виде пластиковых карт. Однако в последние годы активно идет развитие различного рода альтернативных носителей бесконтактных технологий на фоне роста интереса участников рынка к такого рода решениям и их популярности у конечного потребителя. У нас в регионе, например, очень популярен такой бесконтактный форм-фактор, как брелок. Так, например, компания ISBC разработала и активно продвигает собственное решение AIRTAG на базе MIFARE решений для различных приложений, включая оплату проезда на транспорте, контроль доступа, проектов микроплатежей и лояльности. Наиболее распространены данные решения в проектах «Тройка» и «Подорожник», где каждый пассажир может приобрести данные продукты в виде современных и красочных брелоков.

Таким образом, современный потребитель имеет достаточно широкий выбор носителей и может предпочесть именно тот, который наибольшим образом подходит под его конкретные потребности, вкусы и пользовательские привычки. Это могут быть брелок, браслет или те же платежные кольца.

Решения MIFARE позволяют сделать интеграцию таких носителей в существующие системы оплаты проезда максимально простой, быстрой и прозрачной. Производителю в этом случае не требуется проводить сложную сертификацию готового изделия и своей производственной линейки и площадки… Получить доступ к защищенным решениям MIFARE может любой партнер, который способен и заинтересован разрабатывать и производить такие устройства. И мы видим, что это обстоятельство зачастую выступает решающим фактором в пользу выбора производителями именно MIFARE в качестве платформы для своих решений.

Неслучайно, когда наши партнеры из компании ISBC впервые представили в ходе Международного форума транспортной инфраструктуры, прошедшего в Санкт-Петербурге в мае 2016 года, свой инновационный форм-фактор, на протяжении всех трех дней мероприятия к стенду

организатора перевозок, где продавали эти брелоки, стояла длинная очередь желающих приобрести новинку.

Сейчас мы по-прежнему наблюдаем значительный интерес к использованию таких форм-факторов в самых разных проектах, в том числе в рамках конвергенции транспортных проектов с системами контроля доступа – с теми же домофонами, программами лояльности, проектами автозаправочного бизнеса и банковскими проектами. Это действительно очень удобно и востребовано на сегодняшний день.

ПЛАС: Расскажите о новых возможностях, которые открываются в такого рода проектах благодаря применению новой технологии DESFire EV2.

В. Сестреватовский: Отличительной особенностью нашего нового продукта MIFARE DFSFire EV2 является возможность не только организовать эмиссию защищенных транспортных карт, но и безопасным образом загружать различные приложения на уже выпущенные карты, которые выданы клиентам и работают «в поле». Таким образом, речь идет об аналоге функционала Delegated Management в рамках Global Platform, но оптимизированном именно под специфику транспортного сегмента. Администратор такой карты или ее эмитент могут предоставлять различным сервис-провайдерам и другим сторонним структурам право удаленно размещать свои приложения на уже выпущенных картах. Например, на сегодняшний день в обороте находится несколько миллионов активных карт «Тройка» или «Подорожник». Новое решение MIFARE DFSFire EV2 позволяет пользователям самостоятельно выбирать из какого-либо магазина приложений именно те дополнительные сервисы, которые им наиболее интересны. С помощью NFC-телефона или любого другого защищенного канала потребители смогут удаленно загружать такого рода приложения на свою карту, получая в результате персонифицированный карточный мультифункциональный продукт.

Список авторизованных приложений определяет эмитент карты – это может быть, например, Московский метрополитен, Департамент транспорта, Комитет по транспорту и т. п. В этом случае будут определенные коммерческие условия сотрудничества с такого рода сервис-провайдерами. По большому счету, речь идет о продаже памяти для сторонних сервис-провайдеров на картах, уже находящихся в обращении.

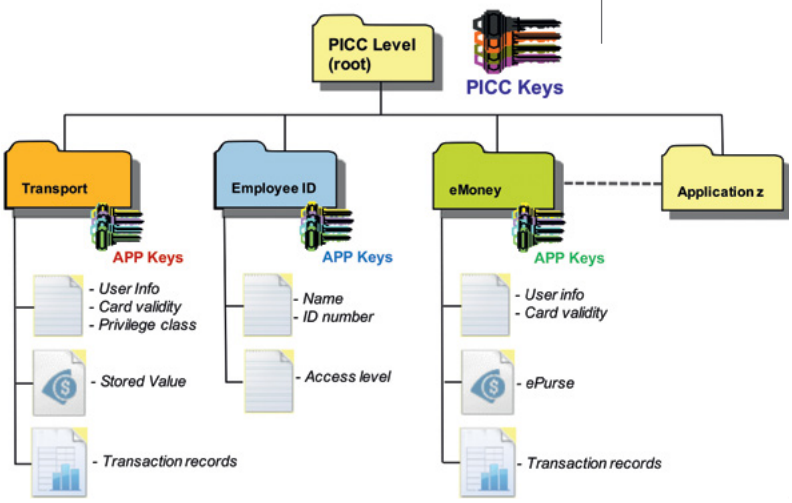
Помимо различных АСОП, продукт DFSFire EV2 получил широкую популярность в проектах в самых разных регионах мира, где используется технология MIFARE. На сегодняшний день по своим функциональным возможностям это решение не имеет аналогов на мировом рынке, и мы видим самые широкие перспективы для его дальнейшего применения в различных регионах мира.

ПЛАС: В связи с этим хотелось бы услышать несколько слов о вашем новом проекте с Google.

В. Сестреватовский: В 2018 году мы совместно с коллегами из Google запустили интересный инновационный проект под названием «MIFARE 2GO» в связке с приложением Google Pay. Мы проработали варианты безопасной удаленной загрузки транспортных карт на решениях MIFARE DFSFire или MIFARE Plus EV1 (в режиме безопасности SL3) в защищенную область памяти приложения Google Pay. Успешно реализовав данную интеграцию, мы запустили этот проект в коммерческую эксплуатацию в рамках проекта АСОП монорельса в Лас-Вегасе.

Основная особенность решения «MIFARE 2GO» и Google Pay заключается в том, что транспортный оператор получает возможность безопасным образом загрузить собственную замкнутую транспортную карту в приложение Google Pay на NFC-телефон с операционной системой Android. Для запуска таких проектов инфраструктура должна поддерживать уже упомянутые современные безопасные решения MIFARE DESFire или MIFARE Plus EV1 (на уровне безопасности SL3). Направление мобильных платежей с помощью телефона активно развивается, и наше решение открывает самые широкие возможности для его продвижения в транспортном сегменте и не только.

Так, совсем недавно, 27 марта 2019 года, мы анонсировали запуск крупного MIFARE 2GO проекта в Мельбурне. В этом австралийском городе сегодня используется 12 млн активных карт MIFARE DFSFire. Поэтому результаты первых дней после запуска проекта превысили наши ожидания в плане уровня активации и загрузок на телефоны транспортных карт Myki. Основное преимущество транспортного оператора – существенная экономия на сборе и обработке наличной выручки, а также возможность предоставить своей аудитории из числа молодежи очень интересный инновационный способ оплаты про-



MIFARE DESFire EV2 card

езда на транспорте с помощью приложения Google Pay. Также принципиально повышается уровень взаимодействия с клиентом-пассажиром благодаря использованию им во время поездки различных Google-сервисов, включая Google Maps (где при составлении маршрута использования общественного транспорта предлагается приобрести и загрузить в приложении Google Pay и транспортную карту с оптимальным тарифом для такого маршрута) и других возможностей Google.

Важно отметить, что решение MIFARE 2GO позволяет подключать различных OEM-производителей, включая производителей умных часов, браслетов и других устройств. И мы видим, что сейчас идет очень активная работа по запуску такого рода проектов в различных регионах мира, и очень надеемся, что в ближайшее время такие проекты будут запущены и в нашем регионе.

ПЛАС: Какие новые востребованные банковские продукты появились в продуктовой линейке NXP? Расскажите о преимуществах решения JCOP.

В. Сестреватовский: В 2019 году мы запускаем новое поколение нашей платформы JCOP (Java Card Operation Platform). Исторически JCOP является результатом совместной деятельности, которую мы вели в начале 2000-х годов с коллегами из IBM, Visa и Philips. На тот момент Philips отвечал за создание защищенного аппаратного микроконтроллера, IBM – за разработку операционной системы JAVA. В свою очередь Visa отвечала за продвижение процесса EMV-миграции в рамках программы Visa Breakthrough. После нескольких лет тесного и успешного сотрудничества компанией Philips было принято решение о покупке операционной системы JCOP у IBM.

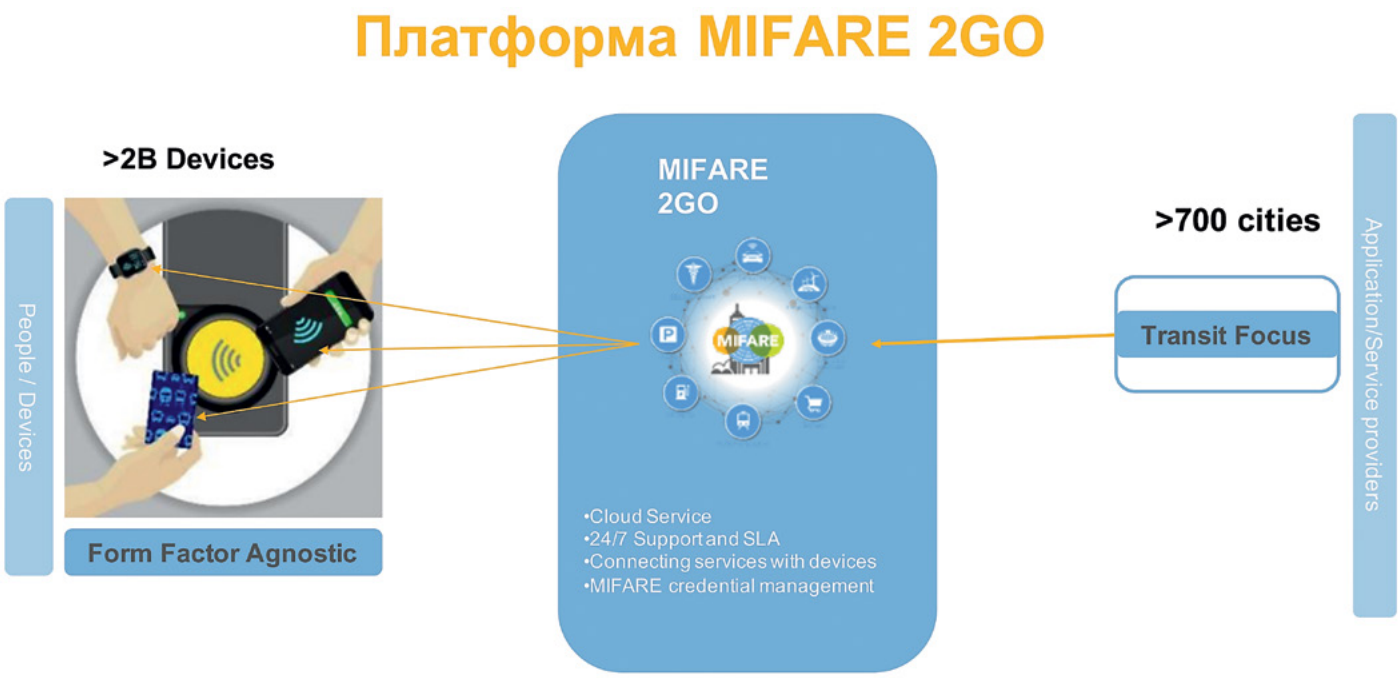
С того времени мы очень активно работаем в направлении развития собственной операционной системы

Производителям наших fingerprint-карт не требуется даже минимальная перенастройка оборудования и процессов

JCOP, ставшей ключевой платформой NXP для многих направлений. На сегодняшний день JCOP используется во многих проектах, причем не только в банкинге, но и в сфере электронных документов. По сути, мы предлагаем полностью готовые решения с приложениями типа ICAO, используемые в электронных паспортах, водительских удостоверениях и других электронных удостоверениях личности.

Также JCOP очень популярна для использования в элементах безопасности, включая встроенные элементы безопасности мобильных телефонов. Сегодня практически все модели ведущих OEM-производителей используют (либо имеют в линейке своих продуктов) платформы и телефоны на базе встроенного элемента безопасности под управлением операционной системы JCOP.

В 2019 году в сегменте банковского направления и электронных документов мы запускаем новую платформу – JCOP4.0 на базе нового защищенного аппаратного микроконтроллера SMART-MX3 от NXP– первого в мире защищенного микроконтроллера, созданного на базе технологии 40 нм. Все эти моменты позволяют достичь рекордного времени осуществления транзакций! Так, недавно мы получили сертификат от Mastercard, подтверждающий, что скорость транзакции Mchip Advance, обеспечиваемая нашим новым решением JCOP4, составляет 191 змиллисекун-



ду. На сегодняшний день это один из лучших показателей по PayPass-транзакциям, текущее требование Mastercard составляет менее 380 миллисекунд. Как видите, мы практически в два раза превысили данную планку.

Также на платформе JCOP4 удалось получить выдающиеся результаты с точки зрения работы ICAO приложений для электронных паспортов и электронных документов (например, скорость выполнения ICAO-приложений и их персонализации увеличилась в несколько раз!), а топология в 40 нм позволяет значительно сократить энергопотребление решения и получить стабильную работу карт и документов даже в слабом поле считывателя.

К настоящему моменту наша платформа JCOP4 также имеет сертификаты Visa, ожидаем сертификацию от UnionPay и AmEx. Кроме того, мы активно работаем с коллегами из НСПК по включению нашего нового решения в перечень авторизованных платформ для работы с приложением «Мир». Важно отметить, что на платформе JCOP4 доступна эмуляция современных решений MIFARE DESFire EV2 и Plus EV1. В связи с чем мы видим существенный интерес к данной платформе во многих проектах как в мире, так и в нашем регионе.

Однако следует отметить, что сегодня карточный банковский сектор переживает не лучшие времена, что сказывается и на производителях EMV-карт. За последние годы произошел настоящий обвал этого сегмента рынка, который превратил его в своего рода коммодити. С одной стороны, это хорошо с точки зрения заказчиков, которые потребляют такого рода продукты. С другой стороны, это плохо для локальной индустрии банковских чиповых карт в целом, поскольку ситуация не позволяет ее участникам реинвестировать в дальнейшее развитие своих компетенций и локальное развитие высокотехнологичного сегмента, в котором России удалось в свое время занять очень серьезные позиции. Возможно, имеет смысл создать ассоциацию либо альянс игроков, объединяющих производителей карт, разработчиков решений и банки, для выработки и продвижения совместной долгосрочной стратегии развития данного сегмента.

ПЛАС: В заключение нашей беседы – как вы оцениваете влияние на рынок появления такой категории продукта, как fingerprint-карты?

В. Сестреватовский: В отношении fingerprint-карт мы можем говорить о появлении такого тренда, как запуск и внедрение на банковском рынке принципиально новых с точки зрения идентификации/аутентификации проектов, в рамках которых пользователю, например, даже не нужно набирать ПИН-код при использовании карточной инфраструктуры.

В 2019 году мы запускаем наше новое решение – fingerprint-модуль, который работает в полностью бесконтактной инфраструктуре. При этом по показателям скорости осуществления транзакции мы нацеливаемся на

общий показатель менее одной секунды, отводимые на все этапы бесконтактной операции, включая валидацию отпечатка пальца держателя карты.

Здесь есть целый ряд моментов, которые выгодно отличают нашу разработку от других решений, существующих на рынке. Во-первых, цифровой образ отпечатка пальца хранится в защищенном контроллере, где производится и само сравнение. Таким образом, критичная информация не покидает пределов защищенного аппаратного устройства. Во-вторых, мы не используем какие-либо аккумуляторы либо конденсаторы на карте – последняя работает исключительно в поле ридера POS-терминала со стандартной POS-инфраструктурой.

Поэтому производителям наших fingerprint-карт не требуется даже минимальная перенастройка оборудования и процессов для их выпуска, например, использование исключительно холодной ламинации и т. д. Напротив, они имеют возможность применять текущие технологические процессы и, соответственно, просто закупать инлеи с fingerprint-модулем. На этапе производства нужно просто имплантировать контактную площадку модуля и непосредственно сенсор.

Мы видим, что этот нишевой продукт в некоторых сегментах может стать действительно востребованным решением, особенно там, где требуется 100%-ная идентификация пользователя, либо где нужно иметь возможность предоставлять пользователю дополнительный уровень безопасности с дополнительным подтверждением его личности с помощью отпечатка пальца.

Отмечу, что за рамками нашей беседы остались такие перспективные сегменты, как RFID-решения, в котором компания NXP занимает ведущие позиции на глобальном рынке, а также интернет вещей и автомобильная электроника, где у нас также множество интереснейших разработок. В силу обширности данных тематик они заслуживают отдельного разговора на страницах журнала «ПЛАС».