ТЕХНИЧЕСКОЕ ОПИСАНИЕ

Технология NFC и смартфоны открывают новые возможности для контроля доступа

Благодаря последним инновациям, смартфоны с технологией NFC можно использовать не только для совершения платежей, но также для открывания дверей и доступа к данным

Согласно определению организации NFC Forum, технология NFC (Near Field Communications) – это технология беспроводной связи малого радиуса действия (см. также ISO 18092), которая обеспечивает простое и безопасное взаимодействие различных электронных устройств. В справочном документе NFC Forum указывается, что обмен данными происходит в том случае, если два устройства с поддержкой NFC находятся на расстоянии 4 сантиметров друг от друга.

Принятие технологии NFC стимулируется ритейлерами мобильных устройств, операторами сотовой связи, финансовыми учреждениями и производителями систем контроля доступа. В число продвигаемых ими возможностей технологии входят мобильные платежи, обмен фотографиями и другими данными между мобильными телефонами, целенаправленная реклама и бонусные программы. Технология также хорошо сочетается с опытом работы пользователей с сенсорным экраном, т.к. они уже привыкли выбирать картинку, чтобы запустить приложение. Главная идея: конвергенция с целью решения различных повседневных задач на мобильном телефоне, например, совершение платежей и банковских операций, транспортные услуги и задачи безопасного доступа, такие как открывание дверей и безопасное управление печатью (в т.ч. печать по запросу, когда задание на печать находится на сервере и выполняется только после предъявления пользователем соответствующего идентификатора на смартфоне с технологией NFC). Кроме того, для управления доступом на телефонах NFC отлично подходят приложения для учета рабочего времени, безопасного доступа к ПК и хранения биометрических шаблонов для многофакторной аутентификации.

Принцип работы NFC в различных областях применения

Совершение платежей является основной, но не единственной областью применения технологии NFC. Технология NFC полностью совместима со стандартами ISO, регламентирующими работу с бесконтактными смарт-картами, поэтому контроль доступа становится идеальным способом применения данной технологии. Соединения NFC устанавливаются быстрее, чем стандартное соединение Bluetooth и его вариация с малой мощностью Bluetooth 3.0. Соединение между двумя устройствами NFC автоматически устанавливается менее чем за 0,1 секунду, при этом ручная настройка конфигурации устройств не требуется. Мобильный телефон с поддержкой NFC можно использовать как беспроводное переносное удостоверение личности. Достаточно просто поднести телефон к считывателю, чтобы открыть дверь.

Технология NFC предусматривает устройство-инициатор и целевое устройство. Инициатор генерирует радиочастотное поле, создающее энергию для целевого устройства, что позволяет использовать простые целевые устройства без отдельного электропитания (например, бесконтактные смарт-карты). Устройства NFC могут работать в различных режимах:

- В *режиме «точка-точка»* два устройства могут активно обмениваться данными.
  - Возможности применения: установление соединения для обмена визитными карточками или печать файла с мобильного телефона с помощью любого принтера, поддерживающего NFC.
- В *режиме чтения/записи* устройство NFC может выступать в роли считывателя, который считывает или записывает данные на совместимую метку.
  - Возможности применения: интерактивная реклама, где плакат со встроенной поддержкой NFC может приказать устройству открыть определенный веб-сайт, или дистанционная проверка безопасности, где охранник может использовать мобильное устройство для считывания карты доступа.
- В *режиме эмуляции карт* устройство NFC работает аналогично стандартной бесконтактной карте.
  - Возможности применения: вход в жилое здание, гостиничный номер или офис без использования ключа. Выдача или отзыв виртуальной карты может осуществляться дистанционно.

Создание инфраструктуры для мобильного контроля доступа

К системе мобильного контроля доступа предъявляются четыре основные требования:

- **Мобильные телефоны с поддержкой NFC и функциями мобильного контроля доступа:** для мобильных телефонов со встроенным чипом NFC требуется элемент безопасности (secure element) для хранения личной идентификационной информации и мини-приложение, запускаемое на элементе безопасности для предоставления этой информации. Также необходимы 1) приложение для взаимодействия с пользователем; 2) цифровые ключи, использующие новый способ представления идентификационной информации, которую можно передавать на мобильные устройства; 3) стандартизированные встроенные интерфейсы API для вывода идентификационной информации в приложении.
- **Экосистема, состоящая из совместимых устройств:** кроме мобильных телефонов, требуются считыватели, замки и прочее аппаратное обеспечение, способное считывать и реагировать на цифровые ключи, хранящиеся в мобильных телефонах с поддержкой NFC. Эти устройства должны находиться в пределах надежной сети контроля доступа, которая обеспечивает безопасную идентификацию в экосистеме из совместимых продуктов.
- **Безопасный механизм управления средствами идентификации:** необходимо определить способ управления жизненными циклами цифровых карт доступа и ключей (включая все процессы представления идентификатора,отзыва идентификатора и совместного использования) – в пределах надежной системы. Это означает, что между проверенными конечными точками всегда существует безопасный канал для обмена идентификационными данными, поэтому в результате все транзакции между телефонами, считывателями и замками осуществляются в пределах надежной и безопасной системы связи.
- **Экосистема поставщиков услуг:** также требуется экосистема, состоящая из операторов сотовой связи (MNO, Mobile Network Operator), надежных менеджеров услуг (TSM, Trusted Service Manager) и прочих поставщиков услуг (SP, Service Provider), способных предоставлять мобильные средства доступа и управлять ими.

Существуют различные точки зрения на то, какие типы организаций будет включать эта экосистема и как она будет развиваться в будущем. Дальнейшее развитие этой экосистемы повлияет на то, как быстро технология NFC будет принята для решения различных задач: от мобильных платежей и оплаты транспортных услуг до контроля доступа.

Оценка скорости распространения технологии NFC в мобильных телефонах

Изначально смартфоны с поддержкой NFC предполагалось использовать прежде всего для совершения платежей. Однако намного более интересной будет возможность с помощью телефона забронировать номер в гостинице и напрямую пройти в номер без предварительной регистрации на стойке администратора. Пользователи также с радостью воспримут возможность хранения в телефоне различных карт и цифровых ключей, например, карт доступа в здания, платежных карт, проездных билетов, брелков для ключей, бонусных карт покупателя и прочих удостоверений личности.

Для реализации этих возможностей необходимо широкое внедрение технологии NFC в различных моделях телефонов со всеми основными операционными системами. Согласно оценкам Berg Insight, уровень продаж мобильных телефонов, оснащенных технологией NFC, в 2016 году достигнет отметки в 700 миллионов штук. Исследовательская компания M for Mobile предсказывает достижение переломного момента на 2015 год, когда доля телефонов с NFC достигнет 51%. В июне 2012 года на сайте Techcrunch.com была опубликована информация о том, что около 15% всех новых устройств Android оснащены технологией NFC, а IHS iSuppli предполагает, что в 2015 году производителями будет выпущено около 550 миллионов телефонов с NFC. Компания ABI Research утверждает, что в настоящий момент на рынке имеется более 60 моделей смартфонов с поддержкой NFC, и что в ближайшие два года более половины дохода в сфере мобильной безопасности будет приходиться на устройства безопасности с технологией NFC.

Где расположен элемент безопасности?

Основу системы NFC составляет элемент безопасности, ставший предметом горячих споров, т.к. тот, кто контролирует его, может определять набор установленных приложений, а также оказывать значительное влияние на восприятие пользователей. При использовании в пределах надежной системы смартфон обеспечивает платформу для максимально безопасной мобильной идентификации, которая включает в себя защищенный канал связи для передачи идентификационной информации между проверенными телефонами, их элементами безопасности и прочими защищенными средами и устройствами. Существует несколько вариантов:

- Использование элемента безопасности внутри телефона в модуле идентификации абонента (SIM, Subscriber Identity Module), который также известен как универсальная карта с интегральной схемой (UICC, Universal Integrated Circuit Card). Этот вариант предпочтителен для операторов сотовой связи (MNO), т.к. именно они контролируют SIM-модуль. Данный метод распространяется операторами сотовой связи. На SIM-карте хранится информация об абоненте и связанных с ним услугах. Применение SIM-карты в качестве элемента безопасности гарантирует сохранность пользовательской информации в случае потери или хищения телефона, т.к. оператор способен активировать или деактивировать услуги по воздуху (OTA, Over The Air). Телефоны NFC и их SIM-карты также обладают функциями повышенной безопасности, например, PIN-коды для доступа к услугам, надежные методы аутентификации для защиты транзакций, защита от несанкционированного вмешательства и соответствие международным стандартам по безопасности.

- Некоторые производители оборудования предпочитают встраивать элемент безопасности в мобильный телефон, т.к. таким образом они могут контролировать область телефона, используемую для услуг NFC. Примеры компаний, продающих мобильные телефоны NFC со встроенными элементами безопасности: Nokia, HTC, Blackberry и Samsung. Встроенные элементы безопасности также используются в других мобильных устройствах, в т.ч. в планшетных компьютерах и ноутбуках.

- Третий вариант: размещение элемента безопасности на внешнем устройстве, например, карте microSD, чехле, наклейке и пр. По аналогии с SIM-картами и встроенными элементами безопасности, эти внешние устройства должны получать электропитание от телефона, при этом для питания карты microSD также требуется запуск соответствующего приложения пользователем. Зачастую дополнительное устройство NFC имеет меньший диапазон считывания, чем телефон со встроенной антенной NFC (для устранения этой проблемы можно использовать усилитель). Преимущество данного подхода заключается в том, что телефоны, не поддерживающие технологию NFC, можно дополнительно оснащать этими внешними устройствами, которые в настоящее время предлагаются лишь небольшим числом производителей.

TSM играет решающую роль во многих областях применения NFC

Одним из основных факторов при внедрении технологии NFC являются надежные менеджеры услуг (TSM), которые отвечают за предоставление и управление мини-приложениями в элементе безопасности. Они устанавливают технические соединения между владельцем элемента безопасности и поставщиком услуг (SP), желающим получить доступ к этому элементу безопасности. Каждый оператор MNO и поставщик SP нуждается в TSM, чтобы дистанционно по воздуху распределять приложения и получать доступ к элементам безопасности в пределах надежной системы по всему миру. В том случае, если в качестве элемента безопасности используются карты microSD, поставщики SP могут эффективно выпускать средства идентификации самостоятельно.

Чтобы создать инфраструктуру для предоставления средств идентификации TSM, менеджер TSM общего контроля доступа должен прозрачно взаимодействовать с MNO, его TSM, поставщиками SP, которые поддерживаются MNO и его TSM, и смартфонами NFC, которые получают зашифрованные ключи для хранения в элементе безопасности. Благодаря этому гарантируется более эффективное управление ключами и средствами идентификации, включая все процессы предоставления идентификатора, отзыва идентификатора и совместного использования. Все операции должны осуществляться в пределах надежной системы, содержащей защищенный канал связи для передачи идентификационной информации между проверенными конечными точками. А за защиту всех транзакций отвечает растущая экосистема, состоящая из совместимых телефонов, считывателей и замков. При наличии этой инфраструктуры производители систем контроля доступа станут поставщиками услуг (SP), предлагающими множество новых функций для конечных пользователей для удобного доступа в любое время и в любой точке мира.

Новейшая технология переносных смарт-карт играет ключевую роль в этой среде предоставления услуг. Современные смарт-карты работают по стандартизированной технологии, которую можно передавать на смартфоны NFC, поэтому пользователи могут применять смарт-карты и/или мобильные устройства в рамках имеющейся системы контроля физического доступа (PACS). Новейшая технология смарт-карт также обеспечивает полную конфиденциальность, т.к. данные для конкретной карты невозможно обнародовать или клонировать благодаря тому, что в ходе сеансов не происходит обмен отслеживаемыми

идентификаторами. Это особенно важно для коммерческих организаций и государственных учреждений, в которых процессы идентификации регламентируются нормативными требованиями. Кроме того, в современной экосистеме смарт-карт используются механизмы безопасности, такие как двусторонняя аутентификация и диверсификация ключей, а также протоколы шифрования на основе открытых стандартов (например, 3DES или AES). Все эти функции, реализованные в пределах надежной системы, гарантируют способность TSM обеспечивать высокий уровень безопасности и защиты данных при предоставлении и управлении мобильными средствами идентификации.

Приложения, выходящие за рамки мобильных платежей, могут стать главными преимуществами NFC

Возможности применения технологии NFC для совершения платежей широко известны общественности, однако смартфоны NFC способны на большее. Мобильные платежи изначально послужили толчком к массовому распространению технологии NFC, которое будет приобретать все больший масштаб по мере роста числа телефонов и платежных терминалов, поддерживающих технологию NFC. Это приведет к тому, что NFC станет стандартной функцией всех мобильных устройств (такой же, какой на сегодняшний день является Bluetooth) и будет составлять основу для множества новых приложений, выходящих за рамки мобильных платежей. Смартфоны будут хранить различные цифровые ключи и карты для физического доступа в жилые дома и прочие здания, а также для логического доступа к компьютерам, сетям и другим ресурсам.

Например, путешественники уже проявили интерес к применению мобильного телефона в качестве посадочных талонов, на которые в настоящее время еще наносится штрих-код авиакомпании. Эта технология штрих-кода пригодна для транзакций на небольшие суммы и операций с малой степенью риска. Популярность мобильных телефонов, позволяющих совершать различные транзакции, непрерывно растет. Смартфоны NFC позволят более просто и комфортно путешествовать по миру. По прибытии на место путешественники могут с помощью смартфона арендовать автомобиль или получить ключи от гостиничного номера на свой смартфон, поэтому регистрация прибытия и отбытия на стойке администратора не потребуется. На сегодняшний день более 650 тысяч замков в гостиницах уже оборудованы технологией NFC и могут работать со смартфонами NFC.

Цифровые ключи и средства идентификации также станут идеальной платформой для различных приложений, например, для зарядных станций для электромобилей. Водители смогут подключать свои электромобили к счетчикам потребленной энергии и, в качестве альтернативы кредитной карте для доступа и оплаты данной услуги, они смогут использовать свои мобильные телефоны с поддержкой NFC. Телефоны NFC также можно будет использовать для представления доступа к истории болезни пациента. В больнице пациент может предъявить свой телефон, не заполняя какие-либо формуляры, и при наличии прав доступа врачи получат всю необходимую информацию для оказания неотложной медицинской помощи.

В коммерческих областях применения, таких как офисы или больницы, пользователи смогут получать цифровые ключи на свои смартфоны, дающие им право доступа к различным считывателям и замкам в инфраструктуре здания, при этом поддерживаются различные уровни безопасности и функции назначения правил доступа. Замки с поддержкой NFC будут обеспечивать точно регламентированный и ограниченный по времени доступ в зоны для хранения конфиденциальной коммерческой и личной информации. Если требуются повышенные уровни безопасности, возможен динамический запуск двухфакторной аутентификации, а на телефон можно будет отправить приложение, которое попросит

пользователя ввести 4-значный PIN-код или совершить определенный жест перед отправкой сообщения – только в этом случае дверь будет открыта. Многофакторная аутентификация становится зависящей от контекста услугой реального времени.

В сфере торговли магазины смогут реализовать более гибкие бонусные программы покупателя. А в домашних условиях члены семьи смогут получать цифровые ключи от входной двери по воздуху на свои смартфоны. Если владелец дома желает выдать ремонтной службе временное право доступа, он может отправить временный ключ и отозвать его после завершения ремонтных работ. Замки для входных дверей с поддержкой NFC будут доступны на потребительском рынке уже в 2013 году.

Функции физического и логического контроля доступа также будут совмещаться на смартфонах NFC. Все чаще пользователи желают иметь одну карту для доступа в здание, входа в сеть, запуска приложений и прочих систем, удаленного доступа к защищенным сетям без необходимости ввода одноразового пароля (OTP) или использования множества ключей. Совмещение всех этих функций в одном смартфоне NFC позволяет повысить удобство для пользователя и значительно улучшить безопасность благодаря применению надежной аутентификации в ИТ-инфраструктуре ключевых систем и прикладных программ. Это также означает сокращение расходов на внедрение и эксплуатацию. Организации могут использовать имеющиеся у них идентификацторы для добавления функций логического доступа и создания полностью совместимой многоуровневой системы безопасности, охватывающей различные сети, системы и объекты данной организации.

Платформы, объединяющие различные технологии. Простой переход

Маловероятно, что мобильный контроль доступа с помощью технологии NFC полностью заменит собой ключи и карты доступа в ближайшие годы. Вместо этого, мобильные средства доступа внутри смартфонов NFC будут использоваться наряду с картами доступа и пропусками. Многие организации будут по-прежнему выдавать своим сотрудникам традиционные идентификационные карты с фотографией. Пользователям будет важно заранее спланировать поддержку обоих типов средств идентификации в их системе физического контроля доступа (PACS).

Оптимальный подход заключается в использовании стандартизированной технологии смарт-карт, которую можно переносить на мобильные телефоны NFC и, таким образом, одновременно использовать оба типа средств идентификации в одной системе PACS. При этом важно обеспечить совместимость между телефонами NFC и имеющейся технической базой, т.к. установленные считыватели карт доступа, как правило, имеют срок службы 10 лет и более. Решением этой задачи становятся считыватели на основе нескольких технологий, которые обеспечивают совместимость с большинством стандартных технологий карт доступа и при этом поддерживают новое поколение средств идентификации. В целях обеспечения совместимости, для инфраструктуры PACS требуются решения, основанные на открытых стандартах. За счет этого также гарантируется в будущем окупаемость инвестиций в современные технологии.

Особенно интересными станут в будущем решения, не включающие в себя физическую карту и подключенный «умный» считыватель. Они составляют контраст с наиболее простой современной моделью мобильного контроля доступа, которая просто копирует существующие принципы контроля доступа с помощью карт, передавая идентификационные данные с телефона на считыватель карт, который отправляет запрос на сервер с правилами контроля доступа и получает от него команду на открывание двери. В будущем можно будет

также использовать возможности смартфонов для значительного сокращения затрат на внедрение приложений контроля доступа.

Другими словами, современные смартфоны обладают достаточной вычислительной мощностью для выполнения большинства задач, которые ранее выполнялись совместно считывателем карт и сервером или панелью управления. В результате можно будет создавать считыватели (и замки) без каких-либо встроенных вычислительных средств или функций связи. Телефоны NFC будут подтверждать личность пользователя и проверять соответствие заданным правилам: например, отправлен ли запрос доступа во время разрешенного интервала времени или находится ли пользователь в настоящий момент рядом с соответствующей дверью (с помощью функций GPS на телефоне). Телефон также может использовать криптографическую защиту для отправки защищенного сообщения с командой открывания двери. От считывателей карт (или замков) требуется всего лишь интерпретация и выполнение зашифрованной команды. Считыватели карт (или замки) выступают в роли кодированных дверных переключателей, которые не соединены с какой-либо панелью управления или сервером. Это означает значительное снижение стоимости интернет-портала, управляющего системой контроля доступа. Производители будут способны встраивать недорогие и, тем не менее, надежные системы контроля доступа в различные изделия, например, межкомнатные двери, картотечные шкафы и сейфы для хранения ценных или подлежащих учету материалов (например, лекарственные препараты класса A), тогда как ранее контроль доступа здесь был нецелесообразен по причине необходимости дорогостоящего монтажа проводки. Компания HID Global рассматривает этот процесс как изменение точки зрения на систему PACS, что можно сравнить с концепцией «смены системы воззрений Негропонте». Это понятие в сфере телекоммуникаций было введено Николасом Негропонте, директором и основателем лаборатории Media Lab Массачусетского технологического института, для описания его взгляда на переход от проводных к беспроводным системам связи.

Переход на мобильную модель

Старый сценарий, который мы прокручиваем в голове, выходя из дома – «ключи – проверить; бумажник – проверить; телефон – проверить» – теперь станет намного короче. Все задачи будут решаться с помощью мобильного телефона, поддерживающего технологию NFC, при этом каждая функция будет выполняться более эффективно за счет «облачных» Интернет-сервисов. Трудности с переходом на новую модель и обеспечением совместимости будут преодолены благодаря применению стандартизированных переносных средств идентификации и платформ, объединяющих различные технологии. Эти средства идентификации и платформы гарантируют рентабельность структур для защиты данных в пределах надежной системы связи, в которой используются современные методы криптографии, защищенный протокол обмена сообщениями и безопасный канал связи. Результатом становится значительное повышение удобства для пользователя и более безопасная среда контроля доступа.