# Лекция 4

# Технология NFC

Near field communication, NFC («коммуникация ближнего поля», «ближняя бесконтактная связь») — технология беспроводной высокочастотной связи малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров, анонсирована в 2004 г.

Эта технология — простое расширение стандарта бесконтактных карт (ISO 14443), которая объединяет интерфейс смарт-карты и считывателя в единое устройство. Устройство NFC может поддерживать связь и с существующими смарт-картами, и со считывателями стандарта ISO 14443, и с другими устройствами NFC, и, таким образом, — совместимо с существующей инфраструктурой бесконтактных карт, уже использующейся в общественном транспорте и платежных системах. NFC нацелена прежде всего на использование в цифровых мобильных устройствах.

# Принцип работы

В основе NFC лежит индуктивная связь (см. рис. 1). Частота работы — 13,56 МГц, скорость передачи — 106 кбит/с (возможны 212 кбит/с и 424 кбит/с). Сигнал подвергается амплитудной манипуляции ООК с различной глубиной 100% или 10% и фазовой манипуляции BPSK

# Основные характеристики технологии NFC

Технология NFC - следующее поколение технологий беспроводной связи, основанных на физическом принципе взаимной индукции. Создана на основе существующих стандартов и технологий бесконтактных смарт-карт.

* несущая частота 13,56 Мгц
* дальность действия до 10 см
* скорость передачи данных 106, 212, и 424 кбит/с
* автоматическая инициация сеанса связи
* конфигурирование канала связи менее 0,1 секунды

Технология NFC в настоящее время главным образом нацеливается на использование в мобильных телефонах и планшетах.

# Области применения NFC

Три основных области применения NFC:

1. эмуляция карт: устройство NFC ведет себя как существующая бесконтактная карта;
2. режим считывания: устройство NFC является активным и считывает пассивную RFID-метку, например, для интерактивной рекламы;
3. режим P2P: два устройства NFC вместе связываются и обмениваются

информацией.

Технология NFC - следующее поколение технологий беспроводной связи, основанных на физическом принципе взаимной индукции. Создана на основе существующих стандартов и технологий бесконтактных смарт-карт.

* несущая частота 13,56 Мгц
* дальность действия до 10 см
* скорость передачи данных 106, 212, и 424 кбит/с
* автоматическая инициация сеанса связи
* конфигурирование канала связи менее 0,1 секунды

Технология NFC совместима:

* ISO 14443
* Mifare
* Felica

### Возможно множество других применений:

Оплата проезда в общественном транспорте— расширение существующей бесконтактной инфраструктуры.

Мобильные платежи — устройство действует как платёжная карта[2].

Электронная доска — мобильный телефон используется для чтения RFID-меток, с уличных досок для объявлений, чтобы на ходу получать информацию.

Спаривание Bluetooth — для соединения устройств Bluetooth 2.1 и выше, поддерживающих NFC, достаточно сблизить их и принять соединение. Процесс активации Bluetooth с обеих сторон, поиска, ожидания, соединения и авторизации заменён простым «прикосновением» мобильных телефонов.

# Стандарты по NFC

NFC — технология с открытой платформой, стандартизированная в ECMA-340 и ISO/IEC 18092-2003. Эти стандарты определяют схемы модуляции, кодирование, скорости передачи и радиочастотную структуру интерфейса устройств NFC, а также схемы инициализации и условия, требуемые для контроля за конфликтными ситуациями во время инициализации — и для пассивных и для активных режимов NFC. Кроме того, они также определяют протокол передачи, включая протокол активации и способ обмена данными. Радиоинтерфейс для NFC стандартизирован в: ISO/IEC 18092 / ECMA-340 : Near Field Communication Interface and Protocol-1 (NFCIP-1)[3]

ISO/IEC 21481 / ECMA-352 : Near Field Communication Interface and Protocol-2 (NFCIP-2)[4]

NFC объединяет множество ранее существовавших стандартов, включая ISO 14443, ISO 15693. Таким образом, телефоны, снабженные NFC, способны к взаимодействию с существующей ранее инфраструктурой считывателей. В «режиме эмуляции карты» устройство NFC должно по крайней мере передать уникальный идентификационный номер существующему ранее считывателю.

# Сценарии выполнения платежей: спецификации SIM SE (SIM Secure Element) и НСЕ (Host Card Emulation)

1. Что такое HCE? Host Card Emulation — это технология, позволяющая эмулировать NFC-карты на мобильных устройствах, используя специальное программное обеспечение. В качестве исходников могут выступать банковские, транспортные и иные карты. Технология Host Card Emulation стала доступной широкой публике 31 октября 2013 с выходом Android KitKat 4.4.

2. До появления HCE информацию для осуществления NFC-транзакций в мобильных устройствах можно было хранить на специальном безопасном элементе, который мог быть размещен либо на SIM-карте, либо в телефоне, либо на специальной версии карты MicroSD. Минус такой технологии в том, что разработчикам сервисов NFC-платежей приходилось договариваться с производителями носителя безопасного элемента.

Для пользователей основным неудобством при таком подходе является привязка системы безопасности к аппаратным средствам, следовательно, неизбежная необходимость смены SIM-карты или даже телефона для подключения сервиса NFC-платежей.

Именно эти неудобства устраняет технология Host Card Emulation, позволившая эмулировать бесконтактные smart-карты прямо в телефоне, никак не регламентируя вопросы безопасного хранения и обработки данных с разработчиками.

3. Большинство современных смартфонов поддерживают HCE. Поддержка есть в аппаратах с Android KitKat 4.4 и выше, Blackberry OS 7 и выше, а также Windows 10.

4. Мобильная платформа Apple HCE не поддерживает. И не будет поддерживать, потому что Apple предпочитает собственные проприетарные решения, используя для кодирования данных свой собственный криптопроцессор и никому не раскрывая его ключи — в результате загружать данные платежных карт в телефоны Apple можно только через Apple.

5. При реализации HCE существует два подхода: карта эмулируется либо облачной платформой, либо мобильным приложением. В первом случае эмуляция карты производится в облаке, и все данные, включая транзакционную логику и платежные реквизиты клиента, хранятся на удаленном сервере. Мобильное приложение в таком случае производит аутентификацию пользователя, предоставляет пользовательский интерфейс и обеспечивает безопасный канал до облака и передачу данных в NFC-контроллер. Минусом этого подхода является большое время обработки транзакций (в среднем более 500 миллисекунд).

Альтернативным является эмулирование карты с помощью мобильного приложения на устройстве. Этот подход требует повышенной безопасности и, как правило, использует токенизацию платежных данных. Авторизационный центр платформы при каждом изменении данных карты делится ими с «провайдером токенов», который создает токены и периодически загружает в мобильное приложение. Для каждой транзакции мобильное приложение создает транзакционную криптограмму и передает ее на POS-терминал через NFC. Процессинговый фильтр определяет, что транзакция была токенизирована, и направляет ее обратно провайдеру для детокенизации и получения реальных платежных данных (например, PAN).

6. HCE перекладывает обеспечение безопасности с оператора связи на эмитента карты.

• Данные, необходимые и достаточные для осуществления NFC-платежей, хранятся непосредственно в памяти смартфона. Однако, как правило, для защиты этих данных используется ряд мер, обеспечивающих защиту лучшую, чем при пользовании физическими банковскими картами. Операции с HCE по заблокированному телефону невозможны. В этом смысле HCE-решение защищено надежнее, чем обычная пластиковая карта с бесконтактным интерфейсом. Снимается опасность удаленного считывания данных HCE, хранящихся в телефоне, если злоумышленник с необходимым оборудованием просто пройдет мимо в толпе.

• Приложение может быть защищено от клонирования «фингерпринтингом» устройства — при каждом запуске сравнивается записанное на сервере «окружение выполнения» (модель телефона или OS и множество других параметров) с текущим, и в случае несоответствия поднимается тревога.

• Процессинг может использовать стандартные антифрод-системы, блокирующие HCE-карту при обнаружении подозрительной активности. Также операции с HCE-приложениями можно защищать с помощью одноразовых паролей, генерирующихся на стороне процессинга и получаемых в мобильном приложении. Также новые модели телефонов позволяют защищать приложения еще и встроенными биометрическими датчиками.

7. С HCE совместимо любое POS-оборудование с поддержкой NFC. На начало 2015 года порядка 5% платежных терминалов уже оснащены функцией NFC. В масштабах всей России это, по экспертным оценкам, около 30 тысяч устройств, и их количество продолжает расти.

8. HCE может использоваться для хранения карт лояльности. Опыт Starbucks показывает, что NFC позволяет объединить платежный процесс, процесс формирования персональных предложений и начисления бонусов лояльности.

9. При использовании HCE есть свои риски.

• Во-первых, реализация платежной функциональности всегда привязана к конкретному банку, выпускающему карту, и для самого банка может быть довольно сложной и требующей дорогостоящей интеграции с процессингом.

• Во-вторых, при использовании подхода с эмуляцией через мобильное приложение устройство должно быть постоянно в интернете для частой замены токенов, что существенно сокращает время автономной работы смартфона.

• Трудности при использовании HCE для совместной реализации платежей и бонусной программы лояльности — в настоящий момент фактически нет стандартов для неплатежных функций, поэтому могут потребоваться доработки программного обеспечения POS и, возможно, смены провайдера бонусной системы.

• Использование HCE для эмуляции транспортных карт возможно, но может усложняться тем, что из-за очень высоких требований к скорости срабатывания билета его обслуживание через интернет может быть затруднено, что влияет на безопасность операций. Более того, в отличие от платежной индустрии, использующей открытые стандарты, транспортная отрасль в основном базируется на проприетарных технологиях, которые невозможно эмулировать.

10. Примеры реализации HCE в России. Первым из банков приложение с HCE самостоятельно запустил Инвестторгбанк, среди сотовых операторов — «Билайн» (приложение «Карта Билайн»), среди розничных ретейлеров — «Евросеть» для карты «Кукуруза». Также отметим компанию I-Free, реализовавшую подобный функционал в приложении «Кошелек» (именно это приложение использует «Тинькофф — кредитные системы»). В «Кошельке» можно выпускать в электронном виде не только карты от ТКС, но и транспортные карты ряда городов России и скидочные купоны от «Купикупон».

**Транзакция** — передача биткоинов между пользователями сети. Она содержит хеш предыдущей транзакции, подписанный кошельком пользователя, и публичный ключ получателя. Транзакции отправляются в сеть широковещательным запросом и подхватываются майнерами, которые включают их в блоки. Чтобы исключить возможность отмены транзакции, нужно дождаться ее включения в несколько последовательных блоков. Такой процесс называется подтверждением.

**Блокчейн (blockchain)** — цепочка транзакций в сети Bitcoin, в которой отражаются все платежи. Хранится на всех узлах сети с полной версией кошелька. Транзакции в блокчейне публичны и хранятся вечно, с момента генерации первого блока по текущий момент.

**Кошелек (клиент) Bitcoin** — программное обеспечение, поддерживаемое группой независимых разработчиков. Обеспечивает хранение закрытого ключа и основные функции по осуществлению транзакций в сети. Кошелек может иметь несколько адресов.

**Адрес Bitcoin** — идентификатор в сети, который используется для проведения платежей. Технически адрес Bitcoin представляет собой 160-битный хеш открытого ключа. Адрес в среднем состоит из 33 алфавитно-цифровых символов и начинается с символа 1. Количество адресов в сети условно бесконечно, вероятность дублирования стремится к нулю.

**Сложность майнинга** — один из параметров расчета хеш-функции для генерации блока. Сложность предназначена для регулировки скорости добычи биткоинов в зависимости от суммарной вычислительной мощности сети, чтобы в среднем блок находился за десять минут. Через каждые 2016 блоков происходит автоматический пересчет сложности.

**Майнинг** — процесс добычи биткоинов путем шифрования блоков транзакций по алгоритму двойного SHA-256. Майнеры перебирают случайно генерируемые последовательности (nonce), чтобы найти хеш, меньший, чем текущая цель, обратно пропорциональная сложности. Майнер, сформировавший блок, получает от сети вознаграждение в 25 BTC. Через каждые 210 000 блоков, то есть примерно четыре года, награда за блок уменьшается в два раза.

**Пулы** — сетевые ресурсы, объединяющие мощности множества майнеров. Вероятность найти блок у пула гораздо выше, чем у одиночного майнера. Вознаграждение за все блоки, найденные пулом, делится между майнерами в соответствие с их вкладом — подключенной к пулу вычислительной мощностью.