ВикипедиЯ

NFC

Материал из Википедии — свободной энциклопедии

> Текущая версия страницы пока не проверялась опытными участниками и может значительно отличаться от версии, проверенной 20 декабря 2023 года; проверки требуют 10 правок.

NFC (англ. *near field communication — связь на ближнем расстоянии*, дословно *связь в пределах ближнего поля*) — технология беспроводной передачи данных малого радиуса действия, которая даёт возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров[1][2][3]; анонсирована в 2004 году.

NFC

Медиафайлы на Викискладе

Эта технология — простое расширение стандарта бесконтактных карт (ISO 14443), которое 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 платёжных системах. NFC нацелена прежде всего на использование в цифровых мобильных устройствах.

NFC мобильный телефон, взаимодействующий с «электронной доской»

Содержание

Ссылки

Основные спецификации

Так же, как и в стандарте ISO 14443, в NFC связь поддерживается посредством индукции магнитного поля, где две рамочные антенны располагаются в пределах ближнего поля друг друга, фактически формируя трансформатор с воздушным сердечником. Этот стандарт работает в пределах общественно доступных и нелицензируемых радиочастот ISM band — промышленные, научные и медицинские радиочастоты около 13,56 МГц, с шириной полосы пропускания почти 2 МГц;

Рабочее расстояние с компактными стандартными антеннами: около 10 см[2];

Существуют два режима: пассивный и активный. В пассивном режиме связи устройство-инициатор обеспечивает несущее поле, а целевое устройство отвечает посредством модулирования имеющегося поля. В этом режиме целевое устройство может вытягивать свою рабочую мощность из предоставленной Инициатором электромагнитной области, таким образом делая целевое устройство ретранслятором. В активном режиме связи и инициатор, и целевое устройство взаимодействуют путём поочерёдного создания своих собственных полей. Устройство дезактивирует своё радиочастотное поле в то время, как оно ожидает данных. В активном режиме у обоих устройств должно быть электропитание.

Для передачи данных NFC использует два различных вида кодирования. Если активное устройство передаёт данные со скоростью 106 кбод, тогда используется модифицированный код Миллера со 100%-й модуляцией. Во всех других случаях используется манчестерское кодирование с коэффициентом модуляции 10 %.

Скорость	Активное устройство	Пассивное устройство
424 кбод	манчестерское, 10 % AMн	манчестерское, 10 % AMн
212 кбод	манчестерское, 10 % AMн	манчестерское, 10 % AMн
106 кбод	модифицированный код Миллера, 100 % AMн	манчестерское, 10 % AMн

Устройства NFC в состоянии одновременно и получать, и передавать данные. Таким образом, они могут контролировать радиочастотное поле и обнаруживать противоречия, если полученный сигнал не соответствует переданному.

Конструкция

NFC — это беспроводная короткодистанционная технология, которая работает на расстоянии не более 10 сантиметров. NFC работает на частоте 13,56 МГц. NFC всегда включает инициатор и цель; инициатор активно генерирует радиочастотное поле, которое может влиять на пассивную цель. Также возможна NFC-связь между двумя устройствами при условии, что оба устройства включены.

Благодаря компактным размерам и низкому потреблению энергии NFC можно использовать в небольших устройствах. В смартфонах антенна часто крепится на задней стороне гаджета, под крышкой. Чтобы у пользователей не возникало вопроса, как именно прикладывать гаджет для передачи данных (особенно такая проблема характерна для планшетов из-за их большого размера и маленького радиуса действия технологии), местонахождение чипа часто помечается специальной наклейкой на корпусе[4].

Сравнение с аналогами

NFC и Bluetooth — технологии связи малого радиуса действия, которые были интегрированы в мобильные телефоны в двухтысячные годы. Существенное преимущество NFC над Bluetooth — более короткое время установки соединения. Вместо выполнения инструкций по согласованию для идентифицирования Bluetooth-устройства связь между двумя устройствами NFC устанавливается сразу (менее чем за одну десятую секунды). При этом скорость передачи данных Bluetooth существенно выше, чем при NFC-соединении, что позволяет передавать данные мультимедиа через Bluetooth (изображения, видеоролики, аудиофайлы и т.д.).

	NFC	Bluetooth
Тип сети	точка-точка	точка-многоточка
Радиус действия	< 0,2 м	10 м
Скорость	424 кбод	24 Мбод
Время установления соединения	< 0,1 с	6 с
Совместимость с RFID	Да	Нет

Области применения

Технология NFC в 2019—2020 году главным образом нацеливается на использование в мобильных телефонах и планшетах. Существует три основных области применения NFC:

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

Возможно множество применений, таких как:

- Мобильная покупка в общественном транспорте — расширение существующей бесконтактной инфраструктуры[5].
- Мобильные платежи — устройство действует как платёжная карта[6].
- Мобильный доступ — в системах контроля доступа смартфоны, ключи-карты и бейджи с технологией NFC могут применяться в качестве идентификатора[7].
- NFC-метка — это ультратонкий чип, в который может быть заложена любая информация. Информация с метки считывается любым устройством с NFC-модулем.
- Микрочип имплантат. Благодаря своему крохотному размеру он может располагаться на любой поверхности, может быть даже имплантирован под кожу человека.
- Спаривание Bluetooth — для соединения устройств Bluetooth 2.1 и выше, поддерживающих NFC, достаточно сблизить их и принять соединение. Процессы поиска устройства и авторизации заменены простым «соприкосновением» мобильных телефонов.

Наклейки TecTiles со встроенной NFC-меткой

Идентификация по смартфону с помощью приложения «PERCo. Доступ»

Также технология применяется в устройствах персональной коммуникации (например, Poken), для конфигурирования и инициализации других беспроводных соединений, таких как Bluetooth, Wi-Fi или Ultra-wideband.

Среди прочих возможных применений — электронная покупка билетов (авиабилетов, билетов на концерт), электронные деньги, карты путешественника, удостоверения личности, мобильная торговля, электронные ключи (от автотранспорта, домов, помещений, гостиничных номеров).

Программа лицензирования патента для NFC в настоящее время (2018 год) разрабатывается в Via Licensing Corporation — независимый филиал Dolby Laboratories.

Стандартизация и промышленные проекты

Стандарты

NFC была одобрена как ISO/IEC стандарт 8 декабря 2003 года и позже как стандарт Ecma International.

NFC — технология с открытой платформой, стандартизированная в ECMA-340 и ISO/IEC 18092. Эти стандарты определяют схемы модуляции, кодирование, скорости передачи и радиочастотную структуру интерфейса устройств NFC, а также схемы инициализации и условия, требуемые для контроля над 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)[8]
- ГОСТ Р ИСО/МЭК 18092-2015 Информационные технологии. Телекоммуникации и обмен информацией между системами. Коммуникация в ближнем поле. Интерфейс и протокол (NFCIP-1)
- ISO/IEC 21481 / ECMA-352 : Near Field Communication Interface and Protocol-2 (NFCIP-2)[9]

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

Кроме того, NFC Forum определил общий формат данных, названный NDEF (https://web.archive.org/web/20120123222433/http://www.nfc-forum.org/specs/), который может использоваться, чтобы сохранить и передавать различные виды элементов данных, в пределах от любого MIME-typed объекта к ультракоротким RTD (https://web.archive.org/web/20120123222433/http://www.nfc-forum.org/specs/)-документам, таким как URL. NDEF концептуально очень подобен MIME. Это — сжатый двоичный формат так называемых «записей», в которых каждая запись может держать различный класс объекта. В соответствии с соглашением тип первого отчёта определяет контекст всего сообщения.

NFC Forum

NFC Forum является некоммерческой ассоциацией, основанной 18 марта 2004 года компаниями NXP Semiconductors, Sony и Nokia, чтобы продвинуть использование NFC в бытовой электронике, мобильных устройствах и персональных компьютерах. NFC Forum призван содействовать реализации и стандартизации технологии NFC, чтобы гарантировать способность к взаимодействию между устройствами и услугами. В сентябре 2007 насчитывалось более чем 130 членов NFC Forum.

В октябре 2010 году к международной организации NFC Forum присоединилась компания i-Free, став, таким образом, первой российской компанией, вступившей в NFCForum[10]. Среди проектов на базе NFC, реализованных i-Free — построение опытной зоны NFC-решений. Тестовые испытания этого проекта успешно прошли в Санкт-Петербурге[11].

В марте 2011 к NFC Forum в качестве ведущего участника (Principal Member) присоединился Google. Это вторая по старшинству роль в NFC Forum. Она позволяет проводить тестирование оборудования на соответствие стандартов NFC Forum в собственных лабораториях, не раскрывая коммерческую тайну производимого оборудования.

GSMA

GSM Association (GSMA) является глобальной торговой ассоциацией, представляющей 700 операторов мобильной связи в 218 странах мира.

Они подали две инициативы:

- **Mobile NFC initiative**: четырнадцать операторов мобильных сетей, которые вместе представляют 40 % глобального рынка мобильной связи, поддерживающих NFC, и сотрудничают, чтобы развивать приложения для NFC. Вот они: Bouygues Télécom, China Mobile, AT&T, KPN, Mobilkom Austria, Orange, SFR, SK Telecom, Telefonica Móviles España, Telenor, TeliaSonera, Telecom Italia Mobile (TIM), Vodafone and 3 (telecommunications)[12].

13 февраля 2007 они издали техническое описание NFC, чтобы дать точку зрения операторов мобильной связи на экосистему NFC[13].

- **Pay buy mobile initiative** стремится определить общий глобальный подход к использованию технологии Near Field Communications (NFC), чтобы связать мобильные устройства с платёжными и бесконтактными системами[14][15]. До настоящего времени[*когда?*] 30 операторов мобильной связи присоединились к этой инициативе.

StoLPaN

StoLPaN ('Store Logistics and Payment with NFC') является европейским консорциумом, поддерживаемым программой European Commission's и Information Society Technologies. StoLPaN будет исследовать пока ещё не использованный потенциал с целью согласования новых видов локальных беспроводных интерфейсов, NFC и мобильной связи.

Другие стандарты

Другие стандарты, которые вовлечены в NFC, включают:

- ETSI / SCP (Платформа Смарт-карт), чтобы установить связь между SIM-картой и набором микросхем NFC.
  - Single Wire Protocol — стандарт ETSI на протокол обмена SIM-карты и микросхемы физического уровня NFC.
- GlobalPlatform, чтобы определить многоприкладную архитектуру защищённой микросхемы.
- EMVCo для воздействий на платёжные приложения EMV.

Аспекты безопасности

Атака с использованием эксплойта

На конференции EuSecWest по вопросам безопасности, прошедшей 19—20 сентября 2012 года, компанией MWR Labs был представлен эксплойт oday, показавший уязвимость технологии NFC в мобильных устройствах. Специалистам по безопасности удалось передать через NFC-соединение вредоносный файл и получить полный контроль над принимающим устройством. Таким образом

конфиденциальные данные и денежные средства «жертвы» оказались под угрозой. Для предотвращения захвата контроля необходимо внесение доработок разработчиками устройств с целью ограничения активности данных, принятых посредством NFC[16][17].

Хотя радиус связи NFC ограничен несколькими сантиметрами, NFC сама по себе не гарантирует безопасности соединений. В 2006 году австрийские специалисты описали различные возможные типы атак[*уточнить*][18].

Подслушивание

Радиочастотный сигнал беспроводной передачи данных может быть перехвачен антеннами. Расстояние, с которого атакующий в состоянии подслушать радиочастотный сигнал, зависит от многочисленных параметров, но в любом случае — это всего несколько метров[19]. Кроме того, на подслушивание чрезвычайно влияет режим связи. Устройство без собственного источника питания, которое производит очень слабый радиосигнал, намного тяжелее подслушать, чем устройство с источником питания.

Стандарт NFC сам по себе не предлагает защиты против подслушивания. По изначальному замыслу, стек протоколов должен использовать криптоалгоритмы поверх NFC для защиты данных.

Модификация данных

Разрушение данных относительно легко осуществить средствами радиоэлектронной борьбы (РЭБ), то есть глушилками RFID. Нет способа предотвратить такое нападение, однако единственным его результатом будет невозможность установить связь.

Несанкционированная модификация данных внутри сообщения атакующим устройством нереализуема на практике в связи с невозможностью предсказать амплитуду и сдвиг фазы наведённого сигнала на приёмном устройстве. RFID-приёмник чувствителен к внезапной смене амплитуды и фазы несущего сигнала.

Атака с использованием ретрансляции (Relay attack)

Поскольку NFC-устройства обычно также обеспечивают функциональность ISO 14443, описанная Relay attack также выполнима и для NFC[20][21]. Для этого нападения злоумышленник должен отправить жертве запрос считывателя и её ответ в режиме реального времени передать дальше на считывающее устройство. Это делается для того, чтобы выполнить задачу, симулирующую владение смарт-картой жертвы.

Примечания

1. *Ortiz, C. Enrique.* An Introduction to Near-Field Communication and the Contactless Communication API (http://java.sun.com/developer/technicalArticles/javame/nfc/) (англ.) (июнь 2006). Дата обращения: 24 октября 2008. Архивировано (https://www.webcitation.org/67IthbBfo?url=http://java.sun.com/developer/technicalArticles/javame/nfc/) 19 мая 2012 года.
2. *Diego A. Ortiz-Yepes.* Enhancing Authentication in eBanking with NFC-Enabled Mobile Phones (https://pdfs.semanticscholar.org/6a4a/894fc69ec79047dce8991b30831809413fb7.pdf) // ERCIM News. — 2009. — Т. 2009. Архивировано (https://web.archive.org/web/20200213130405/https://pdfs.semanticscholar.org/6a4a/894fc69ec79047dce8991b30831809413fb7.pdf) 13 февраля 2020 года.
3. *C. Enrique Ortiz.* An Introduction to Near-Field Communication and the Contactless Communication API (https://www.oracle.com/technetwork/articles/javame/nfc-140183.html) (англ.). Oracle (июнь 2008). Дата обращения: 19 сентября 2019. Архивировано (https://web.archive.org/web/20181223113317/https://www.oracle.com/technetwork/articles/javame/nfc-140183.html) 23 декабря 2018 года.

4. Технология NFC в смартфоне: что это и как работает? | AndroidLime (http://androidlime.ru/nfc-android-smartphones/). androidlime.ru. Дата обращения: 24 декабря 2016. Архивировано (https://web.archive.org/web/20161225075804/http://androidlime.ru/nfc-android-smartphones/) 25 декабря 2016 года.
5. Во всех коммерческих автобусах можно оплатить проезд с помощью NFC-смартфона (https://www.mos.ru/news/item/20539073/). Сайт Москвы (6 февраля 2017). Дата обращения: 19 сентября 2019. Архивировано (https://web.archive.org/web/20210308150817/https://www.mos.ru/news/item/20539073/) 8 марта 2021 года.
6. Google Wallet - электронный кошелёк в смартфоне (https://web.archive.org/web/20190912232538/http://paysyst.ru/news/google-wallet.html). paysyst.ru. Дата обращения: 19 сентября 2019. Архивировано из оригинала (http://paysyst.ru/news/google-wallet.html) 12 сентября 2019 года.
7. Что такое NFC в смартфоне: где находится и как подключить — UParts (https://uparts.in.ua/chto-takoe-nfc-v-smartfone). UParts (22 ноября 2023). Дата обращения: 14 августа 2024. Архивировано (https://web.archive.org/web/20240814103317/https://uparts.in.ua/chto-takoe-nfc-v-smartfone) 14 августа 2024 года.
8. Standard ECMA-340 (http://www.ecma-international.org/publications/standards/Ecma-340.htm) (англ.). ecma-international.org. Дата обращения: 19 сентября 2019. Архивировано (https://web.archive.org/web/20191102210158/http://www.ecma-international.org/publications/standards/Ecma-340.htm) 2 ноября 2019 года.
9. Standard ECMA-352 (http://www.ecma-international.org/publications/standards/Ecma-352.htm) (англ.). ecma-international.org. Дата обращения: 19 сентября 2019. Архивировано (https://web.archive.org/web/20071004181325/http://www.ecma-international.org/publications/standards/Ecma-352.htm) 4 октября 2007 года.
10. Компания i-Free стала участником международной организации NFC Forum (https://web.archive.org/web/20170427122137/http://www.i-free.com/press/news/1536). i-Free.com (26 октября 2010). Дата обращения: 19 сентября 2019. Архивировано из оригинала (https://www.i-free.com/press/news/1536) 27 апреля 2017 года.
11. Компании NXP Semiconductors и i-Free представили сервисы на базе технологии NFC (https://web.archive.org/web/20190918024309/http://www.i-free.com/press/news/4277). i-Free.com (21 февраля 2012). Дата обращения: 19 сентября 2019. Архивировано из оригинала (https://www.i-free.com/press/news/4277) 18 сентября 2019 года.
12. Mobiles hope to be 'smart wallet' (http://news.bbc.co.uk/2/hi/technology/6168222.stm). 21 ноября 2006. Архивировано (https://web.archive.org/web/20201127094330/http://news.bbc.co.uk/2/hi/technology/6168222.stm) 27 ноября 2020. Дата обращения: 19 сентября 2019.
13. GSMA Publishes White Paper On Near Field Communications (NFC) (https://web.archive.org/web/20080610110701/http://www.gsmworld.com/news/press_2007/press07_22.shtml) (англ.). *GSM Association* (13 февраля 2007). Дата обращения: 19 сентября 2019. Архивировано из оригинала (http://www.gsmworld.com/news/press_2007/press07_22.shtml) 10 июня 2008 года.
14. GSM Association Aims For Global Point Of Sale Purchases by Mobile Phone (https://web.archive.org/web/20081024031301/http://www.gsmworld.com/news/press_2007/press07_21.shtml) (англ.). *GSM Association* (13 февраля 2007). Дата обращения: 19 сентября 2019. Архивировано из оригинала (http://www.gsmworld.com/news/press_2007/press07_21.shtml) 24 октября 2008 года.
15. Momentum Builds Around GSMA's Pay-Buy Mobile Project (https://web.archive.org/web/20070828063004/http://www.gsmworld.com/news/press_2007/press07_33.shtml) (англ.). *GSM Association* (25 апреля 2007). Дата обращения: 19 сентября 2019. Архивировано из оригинала (http://www.gsmworld.com/news/press_2007/press07_33.shtml) 28 августа 2007 года.
16. Анонс на официальной сайте MWR Labs о вопросах безопасности (https://labs.mwrinfosecurity.com/archive/mobile-pwn2own-at-eusecwest-2012/) (англ.) (недоступная ссылка — *история* (https://web.archive.org/web/*/https://labs.mwrinfosecurity.com/archive/mobile-pwn2own-at-eusecwest-2012/)). MWR Labs. Дата обращения: 19 сентября 2019.
17. Технология NFC подвержена незаконному списанию денег со счета абонента (https://web.archive.org/web/20141129031857/http://www.cybersecurity.ru/crypto/161661.html). www.cybersecurity.ru (8 октября 2012). Архивировано из оригинала (http://www.cybersecurity.ru/crypto/161661.html) 29 ноября 2014 года.
18. Ernst Haselsteiner, Klemens Breitfuß: Security in near field communication (NFC) (http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf) Архивная копия (https://web.archive.org/web/20140804134757/http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf) от 4 августа 2014 на Wayback Machine, *Philips Semiconductors*, Printed handout of Workshop on RFID Security RFIDSec 06, July 2006

19. Gerhard's Homepage (https://web.archive.org/web/20120818124157/http://www.rfidblog.org.uk/research.html#eavesdrop2008). www.rfidblog.org.uk. Дата обращения: 19 сентября 2019. Архивировано из оригинала (http://www.rfidblog.org.uk/research.html#eavesdrop2008) 18 августа 2012 года.
20. Gerhard's Homepage (https://web.archive.org/web/20120818124157/http://www.rfidblog.org.uk/research.html#relay). www.rfidblog.org.uk. Дата обращения: 19 сентября 2019. Архивировано из оригинала (http://www.rfidblog.org.uk/research.html#relay) 18 августа 2012 года.
21. *Kasper, Timo; Dario Carluccio, Christof Paar.* An embedded system for practical security analysis of contactless smartcards (http://www.crypto.rub.de/imperia/md/content/texte/publications/conferences/embedded_system.pdf) (англ.) // Springer LNCS : journal. — Workshop in Information Security Theory and Practices 2007, Heraklion, Crete, Greece, 2007. — May (vol. 4462). — P. 150—160. Архивировано (https://web.archive.org/web/20070721213723/http://www.crypto.rub.de/imperia/md/content/texte/publications/conferences/embedded_system.pdf) 21 июля 2007 года.

Ссылки

- Технология NFC в смартфонах и её практическое использование (http://www.ixbt.com/mobile/nfc-2013.shtml) Архивная копия (https://web.archive.org/web/20140923081606/http://www.ixbt.com/mobile/nfc-2013.shtml) от 23 сентября 2014 на Wayback Machine // IXBT.com
- ISO/IEC 18092:2004 (http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=38578&ICS1=35&ICS2=100&ICS3=10) Архивная копия (https://web.archive.org/web/20200710025206/http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=38578&ICS1=35&ICS2=100&ICS3=10) от 10 июля 2020 на Wayback Machine
- Near Future of Near Field by Joe Rayment (https://web.archive.org/web/20080603004241/http://www.theglobeandmail.com/servlet/story/RTGAM.20070911.wgtnearfielf0911/BNStory/PersonalTech) // Globe and Mail, September 11, 2007