Technologia NFC omówienie.

Wykorzystane materiały

http://elektronikab2b.pl/technika/3480-nfc-potencjal-perspektywy-i-zagrozenia
http://www.elektroonline.pl/a/5911,Technologia-NFC-Platnosci-i-nie-tylko,,Telekomunikacja
http://en.wikipedia.org/wiki/Near_field_communication
http://docs.oracle.com/javame/dev-tools/jme-sdk-3.0.5/developer-guide/contactless.htm
http://www.oracle.com/technetwork/articles/javame/nfc-140183.html
http://www.mgsm.pl/pl/
http://www.nfc-forum.org

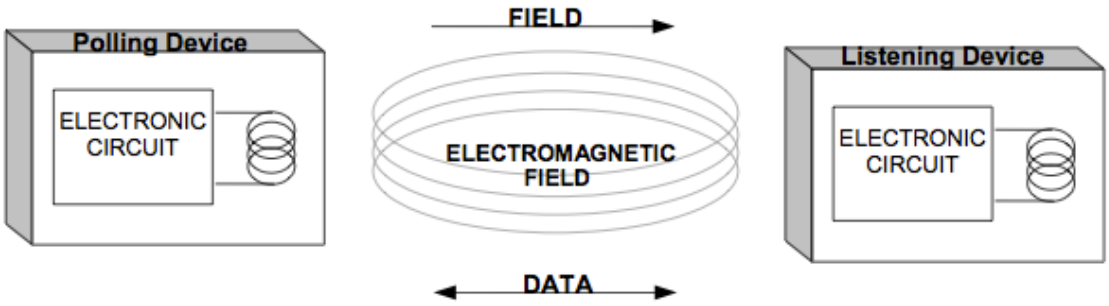
Odnośniki aktualne 18.02.2013

Co to jest NFC

Near Field Communication - NFC to technologia zapewniająca wygodny i bezpieczny transfer danych cyfrowych wysokoczęstotliwościową drogą radiową na niewielkie odległości po to, aby łączyć ze sobą nowoczesne urządzenia elektroniczne oraz będąca platformą technologiczną do realizacji wielu usług i obsługi płatności. Technologia ta jest prostym rozszerzeniem ISO/IEC 14443. Najważniejszą cechą NFC jest bezprzewodowa komunikacja pomiędzy urządzeniami znajdującymi się w odległości maksymalnie do 20 cm. Rozróżnia się dwa tryby pracy. Pierwszy z nich nazywany jest aktywnym i charakteryzuje urządzenie zdolne do samodzielnego emitowania pola elektromagnetycznego stosowanego podczas wymiany danych. Drugi tryb określany jest mianem pasywnego, gdyż nie umożliwia on wytwarzania własnego sygnału radiowego i bazuje na energii pozyskanej z modułu pracującego w trybie aktywnym. Kolejną różnicą pomiędzy tymi trybami jest zasilanie – układy aktywne wymagają go, natomiast pasywne – nie. Co więcej, sposób transmisji danych (kodowanie oraz modulacja) uzależnione są od zastosowanego trybu.

Zasada działania

NFC działa na zasadzie indukcji magnetycznej gdzie dwie kołowe anteny są umieszczone w swoim polu bliskim. Używa ogólnie dostępnej częstotliwości 13.56 MHz, z szerokością pasma 14 kHz. Możliwe prędkości przesyłu to: 106, 212, 424 lub 848 kbit/s.



Rys. 1: Schemat działania

Prędkość transferu	Modulacja	Kod sygnału
106 kb/s	100% ASK	Modyfikowany kod Millera
212 kb/s	8-30% ASK	Kod Manchester
424 kb/s	8-30% ASK	Kod Manchester
848 kb/s	8-30% ASK	Kod Manchester

Tabela 1: Prędkości sygnałów a wykorzystane kody sygnałów

Zgodnie ze standardem, technologia NFC może być używana w trzech różnych trybach protokołu:

- **Read/Write** – w tym trybie urządzenia NFC odczytują informacje z elektronicznych tagów; przykładem może być "inteligentny" kiosk lub plakat, gdzie interaktywny kontent stanowi wartość dodaną do ekspozycji statycznej,
- **Peer-to-Peer** – w tym trybie dwa urządzenia NFC wymieniają dane, np. dwa telefony synchronizujące książkę adresową lub multimedia,
- **Card Emulation** – tryb, w którym urządzenia działają jak tradycyjne "inteligentne karty" (karty chipowe), wykorzystywany jest w e-biletach i płatnościach bezstykowych; obecnie jest to najpopularniejszy tryb stosowania NFC.

Komunikacja bliskiego zasięgu oparta jest na koncepcji zapytań i odpowiedzi. Oznacza to, że jedno urządzenie wysyła pytanie (nazywane jest wtedy inicjatorem – ang. initiator), a drugie urządzenie (nazywane docelowym – ang. target device) odsyła odpowiedź po uprzednim odebraniu tego pytania. Niemożliwe jest wysyłanie jakichkolwiek danych bez wcześniejszego otrzymania zapytania od układu inicjującego. Warto zauważyć, że komunikacja w technologii NFC nie jest ograniczona do pary urządzeń, gdyż inicjator może nawiązać połączenie z wieloma urządzeniami docelowymi. Po rozpoczęciu komunikacji wszystkie urządzenia docelowe są aktywowane w tym samym czasie, więc należy określić, które z nich ma brać udział w wymianie danych. Pozostałe urządzenia (pominięte w procesie nawiązywania połączenia) zignorują dane przesyłane przez inicjator i odpowie tylko

wybrany moduł. Taka organizacja komunikacji wyklucza możliwość wysłania wiadomości do więcej niż jednego urządzenia jednocześnie, ale umożliwia sekwencyjną komunikację z dowolną liczbą urządzeń.

Urządzenie aktywne przesyła dane z wykorzystaniem modulacji ASK (Amplitude Shift Keying). Oznacza to, że częstotliwość nośna jest modulowana strumieniem danych stosownie do wybranego schematu kodowania. Dane transmitowane z prędkością 106 kbps są kodowane z użyciem zmodyfikowanego algorytmu Millera, natomiast dla większych prędkości zastosowanie znajduje kodowanie Manchester. W obu przypadkach pojedynczy bit jest przesyłany w ustalonym slocie czasowym, który jest dzielony na dwie połówki zwana półbitami. Jeden półbit zawiera kodowany bit, natomiast drugi pauzę. Zmodyfikowany algorytm Millera wprowadza dodatkowe reguły dotyczące kodowania logicznego zera następującego bezpośrednio po jedynce. Odbywa się to przez zastosowanie dwóch półbitów bez pauzy. W tradycyjnym kodowaniu Millera w takiej sytuacji dwa następujące po sobie półbity byłyby pauzą.

Kodowanie w systemie Manchester wykorzystuje podobną zasadę, z tym że pojedynczy bit złożony jest zawsze z pauzy oraz sygnału. Kolejność ich wystąpienia decyduje o tym, czy przesyłana jest jedynka, czy zero. Innym aspektem decydującym o postaci sygnału radiowego jest prędkość transmisji. Jeżeli wynosi ona 106kbps, to stosowana jest modulacja o głębokości 100%, co odpowiada wygaszeniu sygnału radiowego w czasie trwania pauzy. Przy większych prędkościach transmisji stosowana jest modulacja o głębokości 10%, w której sygnał nie jest wygaszany podczas pauzy i jego amplituda stanowi 82% wartości szczytowej. Rozwiązanie to jest stosowane w trybie pasywnym razem z kodowaniem Manchester, z tym że modulowanie częstotliwości nośnej 13,56MHz następuje przy prędkość transmisji większej niż 106kbps (w innym przypadku modulacji podlega podnośna).

Jak już zostało wspomniane wcześniej wyróżniamy dwa tryby pracy urządzeń NFC:

- Tryb pasywny: Inicjujące urządzenie wytwarza pole elektromagnetyczne a docelowe urządzenia odpowiada modulując to pole. W trybie tym urządzenie docelowe jest zasilane mocą pola elektromagnetycznego urządzenia inicjującego, dzięki czemu urządzenie docelowe działa jako transponder.

Rys. 2:Tryb pasywny

- Tryb aktywny: Oba urządzenia: inicjujące i docelowe komunikują się przez naprzemienne generowania swojego sygnału. Urządzenie wyłącza swoje pole elektromagnetyczne, gdy czeka na dane. W tym trybie oba urządzenia zwykle potrzebują zasilania.

Rys. 3: Tryb aktywny

Zastosowanie

Technologia NFC ma wiele rodzajów zastosowań. Podobnie jak to było w przypadku technologii optycznego skanowania (takich jak QR kody), NFC upowszechniła się najpierw wśród pionierskich użytkowników i entuzjastów nowoczesnych technologii, ale zyskuje też popularność jako "wyposażenie dodatkowe" i alternatywa dla standardowych kanałów komunikacyjnych. Materiały reklamowe i sprzedaż e-biletów są dwoma oczywistymi przykładami użycia technologii w sposób już przyjęty i praktykowany. Technologia NFC przyciąga także uwagę rynku medycznego, zainteresowanego w szczególności wykorzystaniem smartfonów jako urządzeń diagnostycznych.

Do najbardziej znanych zastosowań NFC należy przede wszystkim obsługa pasywnych znaczników bezprzewodowych (tokenów). Znacznikiem takim może być karta bezprzewodowa (Smart Card), etykieta RFID, breloczek do kluczy lub może zostać wbudowana bezpośrednio w urządzenie. Jednak ze względu na brak fizycznego złącza w znaczniku, rozwiązanie to nie zastępuje komunikacji bezprzewodowej, gdyż do znacznika nie można podłączyć np. mikrokontrolera, który odbierałby i wysyłał dane. Co więcej, ze względu na dostępną niewielką ilość energii pochodzącej z indukcji pola elektromagnetycznego tokeny charakteryzują się małą mocą obliczeniową. Ograniczenia te sprawiają, że ich rola redukuje się do przechowywania danych, które mogą zostać odczytane przez aktywne urządzenie NFC. Rozwiązanie to nadaje się przede wszystkim do przechowywania różnych informacji użytkowych np.: dla produktów podstawowe dane takie jak data produkcji, okres upływu przydatności produktu, czy odnośniki do kontaktu z pomocą techniczną bądź dokumentacją techniczną produktu. Producenci smartfonów wyposażonych w tą technologię dołączają do zestawów naklejki z odpowiednimi tagami umożliwiające poprzez położenie automatyczną zmianę ustawień profilowych w zależności od zdefiniowanego otoczenia np. wkładamy telefon w samochodzie do chwytaka z naklejoną naklejką a telefon zmienia ustawienia rozmów i włącza nawigację GPS.

Rys. 4: Token NFC

Wyróżniane są cztery rodzaje tagów:

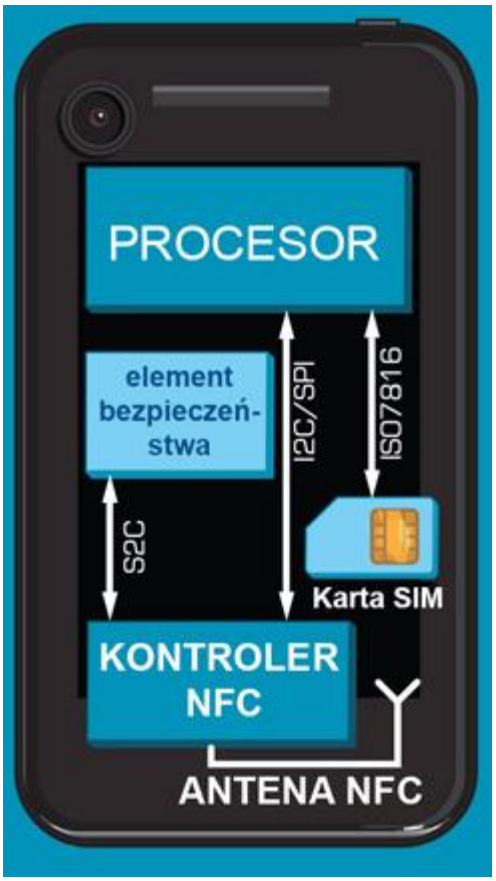
- Tag 1 Type:
  - Standard ISO14443A
  - 96 bajtów co jest więcej niż wystarczające do przechowywania adresu URL strony internetowej lub inne małych ilości danych. Jednak rozmiar pamięci posiada możliwość rozbudowy do 2 kilobajtów.
  - Szybkość komunikacji tego znacznika NFC wynosi 106 kbit / s. W wyniku tej prostoty znacznik jest opłacalny i nadaje się do wielu zastosowań NFC.
- Tag 2 Type:
  - Standard ISO14443A.
  - Podstawowa wielkość pamięci tego typu słowa to tylko 48 bajtów. Jednak rozmiar pamięci posiada możliwość rozbudowy do 2 kilobajtów.
  - Szybkość komunikacji tego znacznika NFC wynosi 106 kbit / s.
- Tag 3 Type:
  - Znacznik 3 typu NFC na podstawie technologii Sony Felicia
  - Rozmiar pamięci to 2 kilobajty.
  - Szybkość komunikacji tego znacznika NFC wynosi 212 kbit / s.
  - Wykorzystywany do bardziej złożonych aplikacji. Jego koszt jest przez to wyższy
- Tag 4 Type:
  - Standard ISO14443A oraz ISO14443B.
  - Rozmiar pamięci to 32 kilobajty.
  - Szybkość komunikacji tego znacznika NFC wynosi pomiędzy 106 kbit / s a 424 kbit / s.

Z definicji NFC różnych typów znaczników, można zauważyć, że znaczniki typu 1 i 2 różnią się od znaczników typu 3 i 4, pojemnością i możliwością wykorzystania.
Znaczniki typu 1 i typu 2 mogą działać w dwóch stanach odczytu / zapisu lub tylko do odczytu. Typ 3

i Typ 4 są znacznikami tylko do odczytu, dane są wprowadzane podczas produkcji lub przy użyciu specjalnej nagrywarki tagów.

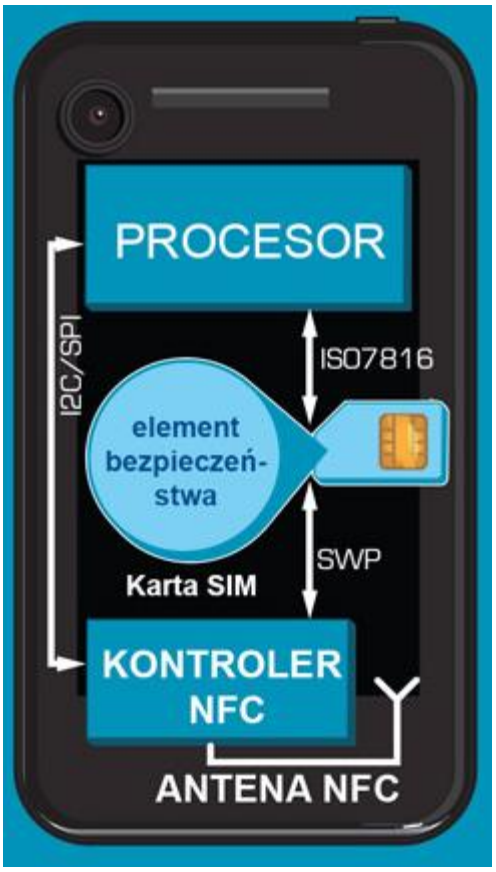
Inną możliwością zastosowania technologii NFC są płatności za pomocą urządzenia posiadającego odpowiedni moduł. Rolę urządzenia płatniczego może pełnić karta lub telefon komórkowy. W tym przypadku konieczne jest użycie bardziej złożonego urządzenia z rozszerzonym interfejsem – sam odczyt danych nie jest wystarczający. Do poprawnej pracy systemu niezbędna jest możliwość zasilania urządzenia pieniędzmi. Architektura sprzętowa produktów NFC, różni się w zależności od celu w jakim powstaje konkretne urządzenie. Główna różnica polega na rozmieszczeniu elementu bezpieczeństwa. W niektórych przypadkach, elementy te, są instalowane oddzielnie, w innych natomiast są implementowane w karcie SIM.

Obecnie najczęściej stosowanym na rynku rozwiązaniem są urządzenia , gdzie nie ma potrzeby integrowania elementu zabezpieczającego z kartą SIM. Innymi słowy integracja technologii NFC może być wykonywana na etapie produkcji urządzeń przez producentów elementów półprzewodnikowych lub producentów telefonów komórkowych bez konieczności współpracy z operatorami sieci komórkowych, co znacznie usprawnia cały proces. Jednak pojawia się tu pewna niedogodność, ponieważ brak integracji zabezpieczenia NFC z kartą SIM nie pozwala na ich komunikację i np. wysyłanie danych do serwerów bankowych, co limituje użyteczność protokołu przy operowaniu finansami w czasie rzeczywistym. W przypadku zaistnienia potrzeby takiej komunikacji konieczny jest dedykowany protokół. Dzięki takiemu rozwiązaniu możliwa jest ekstremalna kompleksowość w projektowaniu sprzętu, ale wiąże się to z koniecznością aktualizacji oprogramowania elementu zabezpieczającego.



Rys. 5: Karta SIM niezależna od elementu zabezpieczającego

Drugie rozwiązanie w którym znajduje się integrujący element zabezpieczający w karcie SIM jest z kolei preferowane przez operatorów sieci komórkowych. Kontroler NFC komunikuje się tu z kartą SIM używając protokołu SWP (Single Wire Protocol), zdolnego do pełno-dupleksowej komunikacji opartej na podstawowych właściwościach napięcia i modulacji. Aplikacje i programy przechowywane w elemencie bezpieczeństwa mogą być aktualizowane i modyfikowane przez interfejsy komunikacji bezprzewodowej, ale częstość i skuteczność takich aktualizacji zależeć będzie w większym stopniu od operatorów komórkowych niż od producentów oprogramowania.



Rys. 6: Element zabezpieczający zintegrowany z kartą SIM

Dokumentacja i standardy ISO

Technologia NFC wykorzystuje istniejące standardy komunikacji zbliżeniowej takie jak:

- ISO/IEC 14443 - podstawowy standard protokołów transmisji danych i parametrów łącza radiowego.
- ISO/IEC 18092 / ECMA-340- podstawowy standard protokołów transmisji danych i parametrów łącza radiowego (NFCIP-1).
- ISO/IEC 21481 / ECMA-352- podstawowy standard protokołów transmisji danych i parametrów łącza radiowego (NFCIP-2).
- JIS X 6319-4 – FeliCa - podstawowy standard protokołów transmisji danych i parametrów łącza radiowego.
- ISO/IEC 15693 – Vicinity – wynik pracy NFC Forum.
- ISO 23917 Protocol Test Methods
- ISO 22536 RF Interface Test Methods

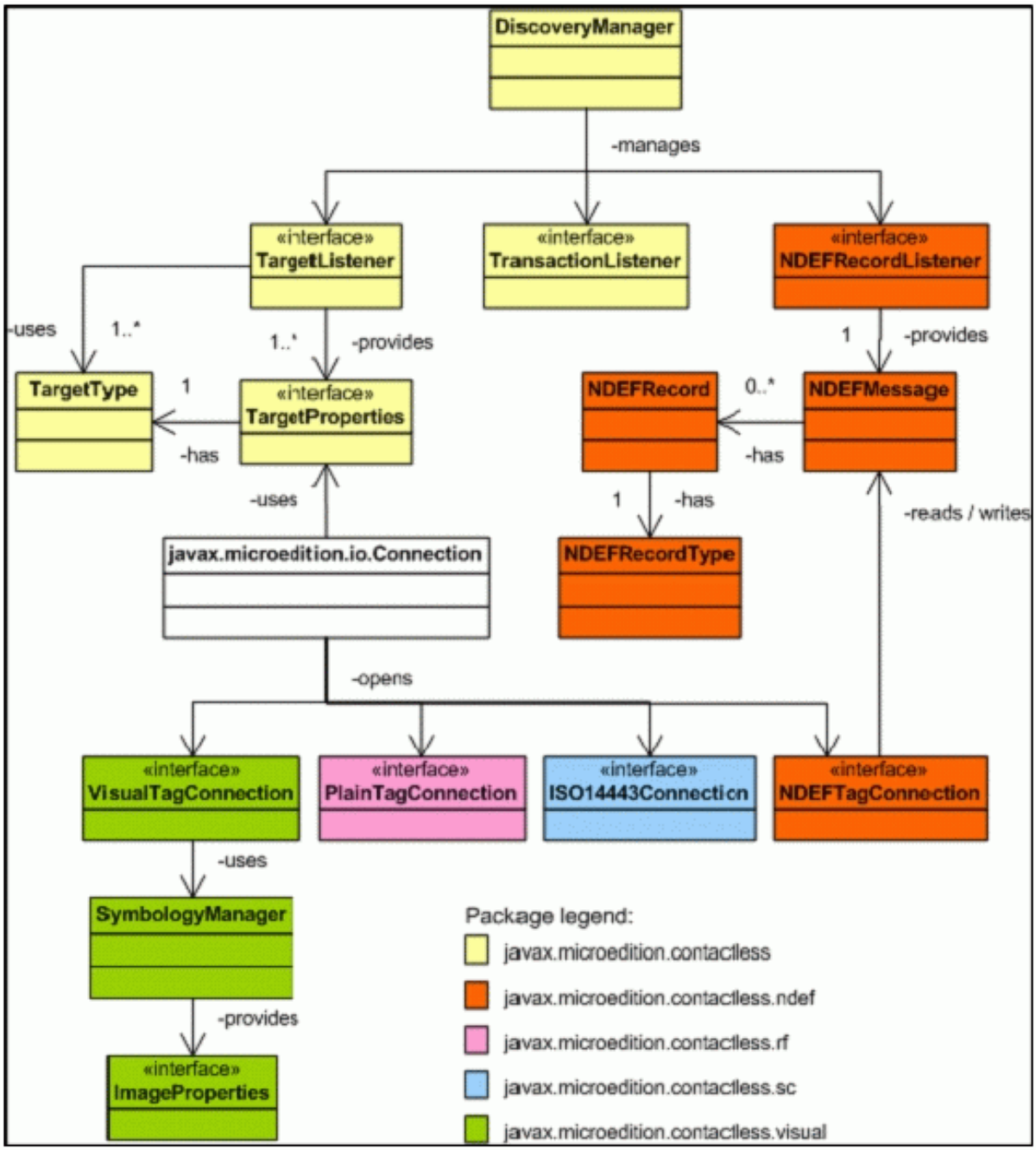
Dodatkowe specyfikacje można znaleźć również na stronie: http://www.nfc-forum.org

API dla urządzeń NFC

Na rynku występuje coraz więcej oprogramowania umożliwiającego pisanie aplikacji dla urządzeń NFC. Jednym z najpopularniejszych jest wykorzystanie Java ME wraz z pakietem JSR 257: Contactless Communication API (http://www.jcp.org/en/jsr/detail?id=257).

Java Package	Interfaces	Classes	Exceptions
javax.microedition.contactless A **mandatory** package that contains all the target discovery and classes common to all targets	TagConnection TargetListener TargetProperties TransactionListener	DiscoveryManager TargetType	ContactlessException
javax.microedition.contactless.ndef An optional package for communicating with NDEF formatted data tags	NDEFRecordListener NDEFTagConnection	NDEFMessage NDEFRecord NDEFRecordType	
javax.microedition.contactless.rf An optional package for communicating with RFID (no NDEF formatted data) tags	PlainTagConnection		
javax.microedition.contactless.sc An optional package for communicating with external smartcards	ISO14443Connection		
javax.microedition.contactless.visual An optional package for reading and generating visual tags	ImageProperties VisualTagConnection	SymbologyManager	VisualTagCodingExc

Tabela 2: Java ME Implementation



Rys. 7: Biblioteka specyfikacji JSR-257

Bezpieczeństwo

Technologia NFC do komunikacji wykorzystuje fale radiowe, co wiąże się z możliwością przechwycenia danych wymienianych między urządzeniami przez nieautoryzowaną jednostkę. Włamywacz może użyć anteny, aby przechwycić przesyłany sygnał radiowy i w sposób eksperymentalny lub na podstawie dostępnej literatury ustalić, jakie dane są przesyłane. Do tego celu nie jest wymagany skomplikowany sprzęt. Ponieważ nie jest możliwe udaremnienie przechwytywania sygnału radiowego, jedynym wyjściem z tej sytuacji jest ustanowienie bezpiecznego, szyfrowanego kanału na czas trwania połączenia. Czyni to ukradzione dane bezużytecznymi dla urządzeń nieposiadających klucza szyfrującego.

Dobrym rozwiązaniem są algorytmy takie jak Diffi e-Hellmann bazujący na RSA czy ASE, które umożliwiają wymianę danych z zachowaniem dużej pewności i ich weryfikacji. Oprócz przechwytywania sygnału istnieją inne zagrożenia dla bezpieczeństwa wymienianych danych. Następnym przykładem jest zniekształcanie transmisji polegające na wysłaniu silnego sygnału radiowego, zakłócającego normalną pracę urządzeń. Działanie to sprowadza się do wygenerowania fali elektromagnetycznej o odpowiednio dobranym widmie częstotliwościowym w odpowiednim czasie. Czas transmisji danych oraz wymagane do tego widmo mogą zostać wyznaczone, jeżeli znany jest sposób kodowania oraz rodzaj użytej modulacji. Atak ten nie należy do skomplikowanych i nie powoduje co prawda przechwycenia poufnych danych, ale może doprowadzić do zablokowania usługi (Denial of Service). Jest on jednakże wykrywalny ze względu na obecność silnego pola elektromagnetycznego towarzyszącego takiej operacji. Po wykryciu ataku urządzenia mogą zaprzestać komunikacji.

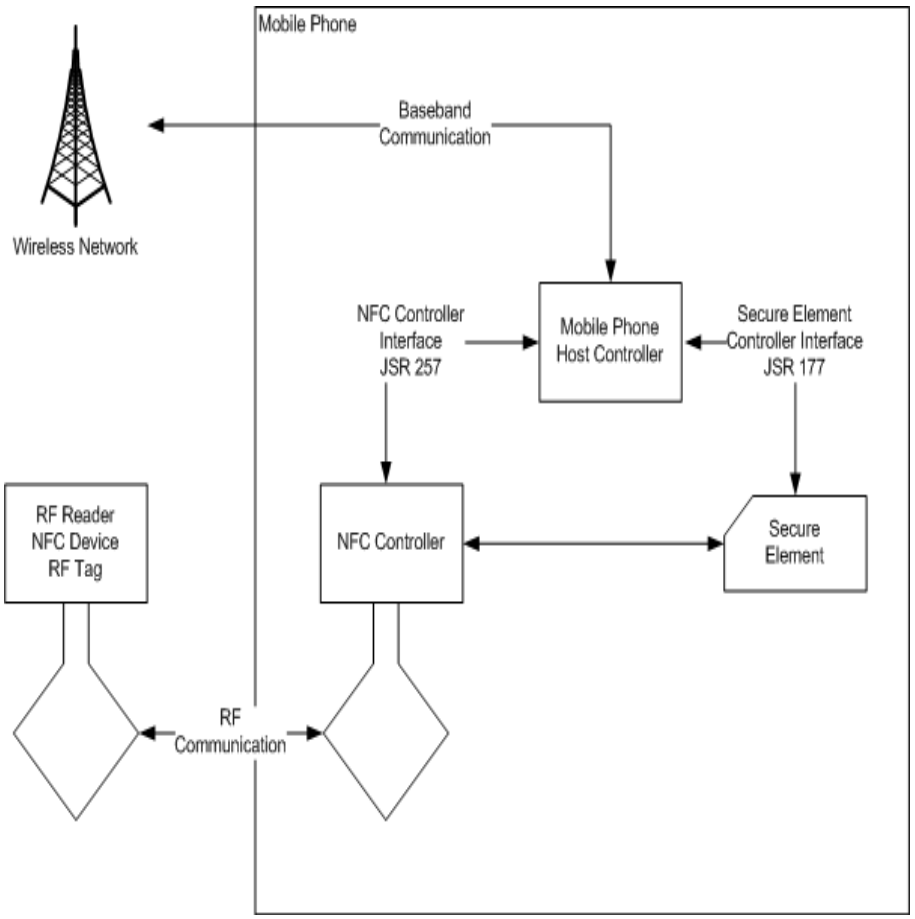
Inną możliwością agresji na system komunikacji bliskiego zasięgu jest modyfikacja przesyłanych danych. Sprowadza się to do wygenerowania takiego sygnału radiowego, dla którego pracujące urządzenie otrzyma prawidłowe dane (w sensie braku błędów transmisji), jednakże inne od wysłanych przez autoryzowanego użytkownika. Wyjściem z tej sytuacji ponownie staje się omówiony wcześniej bezpieczny i szyfrowany kanał komunikacyjny. Oprócz tego nadajnik powinien kontrolować natężenie pola elektromagnetycznego w czasie transmisji i zaprzestać nadawania po stwierdzeniu, że nastąpiła próba ataku. Oprócz zmiany transmitowanych danych lub ich uszkodzenia istnieje jeszcze metoda polegająca na wstawianiu prawidłowej wiadomości w czasie przerwy pomiędzy zapytaniem inicjatora a odpowiedzią urządzenia docelowego. Jest to możliwe tylko w przypadku, gdy odpowiedź przychodzi po bardzo długim czasie. Umożliwia to włamywaczowi szybszą reakcję i wysłanie odpowiedzi, zanim zrobi to właściwe urządzenie. Przeciwdziałanie takim atakom sprowadza się do wybrania jednego z trzech mechanizmów. Pierwszym z nich jest wspominany bezpieczny kanał. Oprócz tego urządzenie inicjujące może dokonywać nasłuchu kanału w czasie przetwarzania danych przez układ docelowy i na podstawie obecności sygnału radiowego w otwartym kanale stwierdzić włamanie. Ostatnią z możliwości jest takie przygotowanie urządzenia docelowego, aby odpowiadało ono natychmiast – włamywacz nigdy nie będzie szybszy od prawidłowego urządzenia.

Do uzyskania najwyższego poziomu bezpieczeństwa potrzebny jest sprzętowy moduł bezpieczeństwa – Secure Element. Obecnie SE może być dostępny w trzech różnych formach: wbudowany w telefon, na karcie SIM, umieszczony na zewnętrznej karcie pamięci SD. Zasada działania jest następująca: urządzenie/telefon pełni rolę czytnika SmartCard. Używane są dwie aplikacje. Aplikacja JME na

telefonie komórkowym pełniąca oferująca interfejs użytkownika oraz aplikacja JavaCard na elemencie SE. JSR177 stanowi interfejs pomiędzy aplikacjami.

Interfejs JSR177:

- Określa interfejs komunikacji z aplikacjami na karcie smart card za pomocą protokołu APDU.
- Określa API Java Card RMI - pozwala JME wywoływać metody obiektów Java Card,
- Wspiera podpis elektroniczny z poziomu aplikacji – bez weryfikacji.
- Pozwala na podstawowe zarządzanie poświadczeniami użytkownika.
- Opisuje podzbiór API kryptograficznego J2SE – weryfikacja podpisu, szyfrowanie, odszyfrowywanie, funkcje skrótu.



Rys. 8: Secure element

NFC vs Bluetooth

	NFC	Bluetooth V2.1	Bluetooth V4.0
RFID compatible	ISO 18000-3	active	active
Standardization body	ISO/IEC	Bluetooth SIG	Bluetooth SIG
Network Standard	ISO 13157 etc.	IEEE 802.15.1	IEEE 802.15.1
Network Type	Point-to-point	WPAN	WPAN
Cryptography	not with RFID	available	available
Range	< 0.2 m	~10 m (class 2)	~1 m (class 3)
Frequency	13.56 MHz	2.4-2.5 GHz	2.4-2.5 GHz
Bit rate	424 kbit/s	2.1 Mbit/s	~200 kbit/s
Set-up time	< 0.1 s	< 6 s	< 1 s
Power consumption	< 15mA (read)	varies with class	< 15 mA (xmit)

Tabela 3: Porównanie NFC i Bluetooth

Urządzenia obsługujące NFC

Liczba telefonów i urządzeń z NFC stale się powiększa. Należą do nich między innymi następujące urządzenia:

Acer
- Acer CloudMobile
- Acer Liquid Express E320
- Acer Liquid Glow

Alcatel
- Alcatel OT 818
- Alcatel OT 818D
- Alcatel OT 828
- Alcatel OT 922

Asus
- Asus Google Nexus 7
- Asus Google Nexus 7 32GB
- Asus PadFone 2

BenQ
- BenQ T60

BlackBerry
- BlackBerry 9350 Curve
- BlackBerry 9360 Curve
- BlackBerry 9370 Curve
- BlackBerry 9790 Bold
- BlackBerry 9900 Bold
- BlackBerry 9930 Bold
- BlackBerry Porsche Design P9981
- BlackBerry Q10
- BlackBerry Z10

Fly
- Fly IQ285 Turbo

Gigabyte
- Gigabyte Orange San Diego
- Gigabyte Orange Santa Clara

HTC
- HTC Butterfly
- HTC Desire V
- HTC Desire VC
- HTC Droid DNA
- HTC Droid Incredible
- HTC Droid Incredible 2
- HTC Droid Incredible 4G LTE
- HTC Elation
- HTC EVO 4G LTE
- HTC Explorer
- HTC Incredible S
- HTC J

- HTC J butterfly
- HTC J ISW13HT
- HTC One SV
- HTC One VX
- HTC One X
- HTC One X+
- HTC One XL
- HTC Salsa
- HTC Status
- HTC Wildfire S
- HTC Windows Phone 8X

Huawei

- Huawei Ascend G600
- Huawei Sonic

Lenovo

- Lenovo K800

LG

- LG Escape
- LG L600v
- LG Nexus 4
- LG Optimus 3D Cube
- LG Optimus 3D Max
- LG Optimus 4X HD
- LG Optimus Elite
- LG Optimus G
- LG Optimus G E973
- LG Optimus G Pro
- LG Optimus L7
- LG Optimus L9
- LG Optimus LTE 2
- LG Optimus Vu II
- LG P692
- LG P768
- LG P769
- LG P895
- LG Prada 3.0
- LG Spectrum 2
- LG Splendor
- LG Swift L5
- LG Swift L5 Dual
- LG T530
- LG Viper

Motorola

- Motorola Droid RAZR HD
- Motorola Droid RAZR M
- Motorola Droid RAZR Maxx HD
- Motorola Electrify M
- Motorola Photon Q 4G LTE
- Motorola RAZR HD

- Motorola RAZR i
- Motorola RAZR M

Nokia

- Nokia 600
- Nokia 603
- Nokia 6131 NFC
- Nokia 6212 Classic
- Nokia 6216 Classic
- Nokia 700
- Nokia 701
- Nokia 808 Pure View
- Nokia Astound
- Nokia C7
- Nokia Lumia 610 NFC
- Nokia Lumia 620
- Nokia Lumia 810
- Nokia Lumia 820
- Nokia Lumia 822
- Nokia Lumia 920
- Nokia Lumia 920T
- Nokia N9
- Nokia N9 64GB
- Nokia Oro

Panasonic

- Panasonic Eluga
- Panasonic Eluga Power
- Panasonic P-04D

Pantech

- Pantech Discover
- Pantech Vega No 6
- Pantech Vega R3

Sagem

- Sagem Cosy Phone
- Sagem my700X
- Sagem my700X ContactLess

Samsung

- Samsung ATIV S
- Samsung ATIV Tab
- Samsung Epic 4G Touch
- Samsung Galaxy Ace 2
- Samsung Galaxy Exhibit
- Samsung Galaxy Express
- Samsung Galaxy Fame
- Samsung Galaxy Fame Duos
- Samsung Galaxy II Skyrocket
- Samsung Galaxy mini 2
- Samsung Galaxy Nexus
- Samsung Galaxy Nexus Telus
- Samsung Galaxy Note

- Samsung Galaxy Note II
- Samsung Galaxy Note SC-05D
- Samsung Galaxy Note SGH-i717
- Samsung Galaxy Pop SHV-E220
- Samsung Galaxy Premier i9260
- Samsung Galaxy R Style
- Samsung Galaxy S Advance
- Samsung Galaxy S II
- Samsung Galaxy S II HD LTE
- Samsung Galaxy S II LTE
- Samsung Galaxy S II Plus
- Samsung Galaxy S II T-Mobile
- Samsung Galaxy S II WiMAX ISW11SC
- Samsung Galaxy S III
- Samsung Galaxy S III GT-i9305
- Samsung Galaxy S III mini
- Samsung Galaxy S III SC-06D
- Samsung Galaxy Tab 7.7
- Samsung Google Nexus 10
- Samsung GT-i8250
- Samsung GT-i9023 Google Nexus S
- Samsung GT-i9103 Galaxy S II
- Samsung GT-S5230N
- Samsung GT-S5380 Wave Y
- Samsung GT-S5780
- Samsung GT-S7250 Wave M
- Samsung Nexus S
- Samsung Nexus S 4G
- Samsung SCH-i515
- Samsung SGH-i535
- Samsung SGH-i747
- Samsung SGH-T989
- Samsung SGH-T999
- Samsung SGH-X700
- Samsung SHV-E270S
- Samsung SPH-L710
- Samsung Victory 4G LTE
- Samsung Wave Y La Fleur

SKY

- SKY Vega LTE
- SKY Vega LTE M

Sonim

- Sonim XP1301 Core

Sony

- Sony Xperia acro S
- Sony Xperia AX SO-01E
- Sony Xperia NX SO-02D
- Sony Xperia P
- Sony Xperia S

- Sony Xperia SL
- Sony Xperia sola
- Sony Xperia T HSPA
- Sony Xperia T LTE
- Sony Xperia Tablet Z SO-03E
- Sony Xperia TX
- Sony Xperia V
- Sony Xperia Z
- Sony Xperia ZL

VERTU

- VERTU Ti

ZTE

- ZTE Blade II
- ZTE Era
- ZTE Flash
- ZTE Grand Era
- ZTE Grand X IN
- ZTE Kis
- ZTE Mimosa X
- ZTE Orbit

Inne

- Oppo Find 5
- Xolo X900
- YotaPhone