

KOMUNIKACJA BLISKIEGO ZASIĘGU

KOMUNIKACJA BLISKIEGO ZASIEGU OD TEORII DO PRAKTYKI

Vedat Coskun, Kerem Ok i Busra Ozdenizci

Laboratorium NFC - Stambul, Uniwersytet ISIK, Turcja



A John Wiley & Sons, Ltd., Publikacja

To wydanie zostało opublikowane po raz pierwszy w 2012 roku
© 2012 John Wiley & Sons Ltd

Siedziba

John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, Wielka Brytania

Szczegółowe informacje na temat naszych globalnych biur redakcyjnych, obsługi klienta i sposobu ubiegania się o pozwolenie na ponowne wykorzystanie materiałów chronionych prawem autorskim w tej książce można znaleźć na naszej stronie internetowej pod adresem www.wiley.com.

Prawo autora do bycia zidentyfikowanym jako autor tej pracy zostało zapewnione zgodnie z ustawą o prawie autorskim, wzorach i patentach z 1988 r.

Wszelkie prawa zastrzeżone. Żadna część niniejszej publikacji nie może być powielana, przechowywana w systemie wyszukiwania lub przekazywana w jakiekolwiek formie lub za pomocą jakichkolwiek środków elektronicznych, mechanicznych, fotokopii, nagrywania lub w inny sposób, z wyjątkiem przypadków dozwolonych przez brytyjską ustawę o prawie autorskim, wzorach i patentach z 1988 r., bez uprzedniej zgody wydawcy.

Wiley publikuje również swoje książki w różnych formatach elektronicznych. Niektóre treści pojawiające się w wersji drukowanej mogą nie być dostępnego w książkach elektronicznych.

Oznaczenia używane przez firmy w celu wyróżnienia ich produktów są często uznawane za znaki towarowe. Wszystkie nazwy marek i produktów użyte w tej książce są nazwami handlowymi, znakami usługowymi, znakami towarowymi lub zastrzeżonymi znakami towarowymi i ich właścicielami. Wydawca nie jest powiązany z żadnym produktem ani sprzedawcą wymienionym w tej książce. Niniejsza publikacja ma na celu dostarczenie dokładnych i wiarygodnych informacji w odniesieniu do omawianego tematu. Jest ona sprzedawana przy założeniu, że wydawca nie jest zaangażowany w świadczenie profesjonalnych usług. Jeśli wymagana jest profesjonalna porada lub inna fachowa pomoc, należy skorzystać z usług kompetentnego specjalisty.

Biblioteka Kongresu Cataloging-in-Publication Data

Coskun, Vedat.

Komunikacja bliskiego zasięgu: od teorii do praktyki / Vedat Coskun, Kerem Ok i Busra Ozdenizci.

s. cm. Zawiera odniesienia bibliograficzne
i indeks. ISBN 978-1-119-97109-2 (materiał)
1. Komunikacja bliskiego zasięgu. I. Ok, Kerem. II. Ozdenizci, Busra. III. Tytuł.
TK6570.N43C67 2012
621.384-dc23

2011033663

Rekord katalogowy tej książki jest dostępny w British Library. ISBN:

9781119971092

Times 10/12pt, Aptara Inc., New Delhi, Indie

*Vedat Coskun:
Kochanym członkom mojej
rodziny; Mehmet i Fatma
Filiz & Ozgur & Arda
Mujdat & Kilinc & Muge & Selma.*

*Kerem Ok:
Mojej rodzinie, która wspierała mnie przez cały czas*

*Busra Ozdenizci:
Dla moich drogich rodziców i brata Ozana*

Zawartość

Przedmowa	xv
Podziękowania	xxiii
Lista akronimów	xxv
1 Streszczenie	1
1.1 W kierunku ery NFC	2
1.1.1 <i>Wszechobecna informatyka</i>	2
1.1.2 <i>Telefony komórkowe</i>	3
1.1.3 <i>Motywacja technologiczna NFC</i>	4
1.1.4 <i>Komunikacja bezprzewodowa, RFID i NFC</i>	4
1.2 Ewolucja NFC	4
1.2.1 <i>Wcześniejsa forma RFID: technologia kodów kreskowych</i>	4
1.2.2 <i>Technologia RFID</i>	5
1.2.3 <i>Wcześnjesze formy kart inteligentnych: Karty z paskiem magnetycznym</i>	6
1.2.4 <i>Technologia kart inteligentnych</i>	6
1.2. <i>5NFC jako nowa technologia</i>	7
1.3 NFC Essentials	7
1.3.1 <i>Inteligentne urządzenia NFC</i>	8
1.3.2 <i>Standaryzacja telefonów komórkowych z obsługą NFC</i>	8
1.3.3 <i>Ogólna architektura telefonów komórkowych z obsługą NFC</i>	10
1.3.4 <i>Interfejs i protokół komunikacji bliskiego zasięgu (NFCIP)</i>	11
1.4 Tryby pracy i podstawowe funkcje NFC	11
1.4.1 <i>Tryby pracy NFC</i>	11
1.4.2 <i>Podstawy trybu czytnika/zapisu</i>	12
1.4.3 <i>Podstawy trybu peer-to-peer</i>	13
1.4.4 <i>Podstawy trybu emulacji karty</i>	13
1.4. <i>5 Studia przypadków</i>	13
1.5 SE i zarządzanie nim	14
1.5.1 <i>Technologia Over-the-Air</i>	15
1.5.2 <i>Specyfikacja karty GlobalPlatform</i>	15
1.5.3 <i>Menedżer zaufanych usług</i>	16
1.5.4 <i>Modele zarządzania UICC</i>	16
1.5. <i>5 Wiele środowisk SE</i>	16

1.6	Rozwój aplikacji NFC	17
1.6.	<i>1JSR 257</i>	18
1.6.	<i>2JSR 177</i>	18
1.7	Bezpieczeństwo i prywatność NFC	19
1.7.	<i>IDlaczego bezpieczeństwo jest ważne?</i>	19
1.7.2	<i>Główne cele środków bezpieczeństwa</i>	20
1.7.3	<i>Podatność, zagrożenie, atak i ryzyko</i>	21
1.7.4	<i>Narzędzia i mechanizmy bezpieczeństwa</i>	21
1.7.5	<i>Bezpieczeństwo NFC</i>	22
1.7.6	<i>Prywatność, aspekty prawne i etyczne</i>	24
1.8	Ekosystem biznesowy NFC	25
1.8.1	<i>Interesariusze w ekosystemie NFC</i>	27
1.8.2	<i>Zrozumienie modeli biznesowych NFC</i>	28
1.8.3	<i>Podejście do modelu biznesowego</i>	30
1.9	Użyteczność w NFC	30
1.10	Korzyści z aplikacji NFC	31
1.10.1	<i>Przyszłe scenariusze dotyczące NFC</i>	32
1.11	NFC na całym świecie	33
1.11.1	<i>Miasta NFC</i>	33
1.11.2	<i>Próby i projekty NFC</i>	34
1.12	Stan badań naukowych nad literaturą NFC	36
1.13	Podsumowanie rozdziału	39
	Referencje	39
2	W kierunku ery NFC	41
2.1	Komputery wszechobecne i NFC	41
2.1.1	<i>Wszechobecna informatyka</i>	41
2.1.2	<i>Nowa alternatywa interfejsu komunikacyjnego dla telefonów komórkowych: Technologia NFC</i>	42
2.2	Telefony komórkowe	43
2.2.1	<i>Cechy telefonu komórkowego</i>	44
2.2.2	<i>Sieć telefonii komórkowej</i>	45
2.2.3	<i>Architektura telefonów komórkowych</i>	46
2.3	Komunikacja bezprzewodowa jako medium komunikacyjne dla technologii NFC	47
2.3.1	<i>Komunikacja bezprzewodowa, mobilna i nomadyczna</i>	48
2.3.2	<i>Technologie komunikacji bezprzewodowej i mobilnej</i>	48
2.4	Technologia RFID	50
2.4.1	<i>Wcześniejsa forma RFID: technologia kodów kreskowych</i>	51
2.4.2	<i>Kody kreskowe a znaczniki RFID</i>	53
2.4.3	<i>Podstawy technologii RFID</i>	53
2.4.4	<i>Tagi RFID jako transpondery</i>	54
2.4.5	<i>Czytniki RFID</i>	55
2.4.6	<i>Zakresy częstotliwości</i>	55
2.4.7	<i>Zasady działania technologii RFID</i>	55
2.4.8	<i>Transmisja bliskiego i dalekiego pola</i>	57
2.4.9	<i>Typowe zastosowania RFID na całym świecie</i>	58

2.5	Technologia kart inteligentnych	58
2.5.1	<i>Wcześniejsze formy kart inteligentnych: Karty z paskiem magnetycznym</i>	59
2.5.2	<i>Ewolucja kart inteligentnych</i>	60
2.5.3	<i>Rodzaje kart inteligentnych: Klasyfikacja oparta na możliwościach</i>	60
2.5.4	<i>System operacyjny kart inteligentnych (SCOS)</i>	61
2.5.5	<i>Rodzaje kart inteligentnych: Klasyfikacja oparta na mechanizmach</i>	63
2.5.6	<i>Aplikacje kart inteligentnych</i>	67
2.6	Porównanie tagów RFID i zbliżeniowych kart inteligentnych	67
2.7	Więcej o NFC	68
2.7.1	<i>Nieodłączne bezpieczeństwo i zdolność parowania NFC</i>	70
2.8	Podsumowanie rozdziału	70
	Pytania do rozdziału	71
	Odniesienia	71
3	Podstawy NFC	73
3.1	Wprowadzenie do NFC	73
3.2	Standaryzacja i rozwój telefonów komórkowych z obsługą NFC	76
3.2.1	<i>Forum NFC</i>	76
3.2.2	<i>GlobalPlatform</i>	79
3.2.3	<i>Stowarzyszenie GSM (GSMA)</i>	80
3.2.4	<i>Międzynarodowa Organizacja Normalizacyjna (ISO)/International Komisja Elektrotechniczna (IEC)</i>	80
3.2.5	<i>ECMA International</i>	81
3.2.6	<i>ETSI i ETSI Smart Card Platform (ETSI SCP)</i>	81
3.2.7	<i>Java Community Process (JCP)</i>	81
3.2.8	<i>Open Mobile Alliance (OMA)</i>	81
3.2.9	<i>Projekt partnerski trzeciej generacji (3GPP)</i>	82
3.2.10	<i>EMVCo</i>	82
3.3	Ogólne Architektura telefonów komórkowych z obsługą NFC	82
3.3.1	<i>Bezpieczny element</i>	83
3.3.2	<i>Interfejs NFC</i>	86
3.3.3	<i>Interfejs między SE a kontrolerem NFC</i>	86
3.3.4	<i>Kontroler hosta i HCI</i>	89
3.4	Warstwa fizyczna NFC	92
3.4.1	<i>ISO/IEC 14443 - Standard zbliżeniowej karty inteligentnej</i>	92
3.4.2	<i>Interfejs i protokół komunikacji bliskiego zasięgu (NFCIP)</i>	94
3.4.3	<i>Transmisja danych w warstwie radiowej</i>	96
3.5	Podstawy trybu pracy czytnika/zapisywarki	99
3.5.1	<i>Architektura stosu protokołów w trybie czytnika/zapisu</i>	100
3.5.2	<i>Typy tagów wymagane przez forum NFC</i>	101
3.5.3	<i>NDEF</i>	102
3.6	Podstawy trybu pracy peer-to-peer	108
3.6.1	<i>Architektura stosu protokołów w trybie peer-to-peer</i>	108
3.6.2	<i>LLCP</i>	109
3.7	Podstawy trybu pracy emulacji karty	111
3.7.1	<i>Architektura stosu protokołów w trybie emulacji karty</i>	111

x		Zawartość
		ć
3.	8 Podsumowanie rozdziału Pytania do rozdziału Odniesienia	112 113 113
4	Tryby pracy NFC	115
4.1	Techniki interakcji z urządzeniami mobilnymi 4.1.1 <i>Technologia NFC Technika interakcji</i>	115 117
4.2	Klasyfikacja urządzeń NFC 4.2.1 <i>Urządzenia aktywne i pasywne</i> 4.2.2 <i>Inicjator a urządzenia docelowe</i>	118 118 119
4.3	Tryb czytnika/zapisu 4.3.1 <i>Inteligentny plakat</i> 4.3.2 <i>Ogólny model użytkowania</i> 4.3.3 <i>Wiodące aplikacje</i> 4.3.4 <i>Przypadki użycia w trybie czytnika/zapisu</i> 4.3.5 <i>Korzyści z aplikacji bazowej</i>	119 120 121 123 125 127
4.4	Tryb peer-to-peer 4.4.1 <i>Ogólny model użytkowania</i> 4.4.2 <i>Wiodące aplikacje</i> 4.4.3 <i>Przypadki użycia w trybie peer-to-peer</i> 4.4.4 <i>Korzyści z aplikacji bazowej</i>	128 129 129 130 131
4.5	Tryb emulacji karty 4.5.1 <i>Ogólny model użytkowania</i> 4.5.2 <i>Wiodące aplikacje</i> 4.5.3 <i>Przypadki użycia w trybie emulacji karty</i> 4.5.4 <i>Korzyści z aplikacji bazowej</i>	131 132 133 134 135
4.6	Przegląd zalet trybów pracy	135
4.7	Studia przypadków 4.7.1 <i>Studium przypadku trybu czytnika/zapisu: Zakupy NFC</i> 4.7.2 <i>Studium przypadku trybu peer-to-peer: Plotkowanie NFC</i> 4.7.3 <i>Studium przypadku trybu emulacji karty: Sprzedaż biletów NFC</i>	136 137 141 142
4.8	Podsumowanie rozdziału Pytania do rozdziału Odniesienia	148 148 148
5	Tworzenie aplikacji NFC	151
5.1	Pierwsze kroki w tworzeniu aplikacji NFC	151
5.2	Dlaczego Java? 5.2.1 <i>Dlaczego wybraliśmy Javę?</i> 5.2.2 <i>Dlaczego Java jest faworytem?</i>	152 152 153
5.3	Konfigurowanie środowiska dla programowania Java ME i NFC	155
5.4	Wprowadzenie do programowania mobilnego 5.4.1 <i>Java ME Building Blocks</i> 5.4.2 <i>MIDlets</i> 5.4.3 <i>Pakiet javax.microedition.lcdui</i> 5.4.4 <i>Tworzenie nowego projektu MIDlet</i>	158 160 161 164 165

5.4.5	<i>Wewnątrz MIDlet Suite (MIDlet Packaging)</i>	168
5.4.6	<i>Bardziej szczegółowy interfejs użytkownika MIDlet</i>	171
5.4.	<i>7Push Registry</i>	177
5.5	Rozwój aplikacji NFC	179
5.6	Programowanie trybu czytnika/zapisu	179
5.6.1	<i>Pakiet javax.microedition.contactless</i>	181
5.6.2	<i>Pakiet javax.microedition.contactless.ndef</i>	183
5.6.3	<i>Pakiet javax.microedition.contactless.rf</i>	185
5.6.4	<i>Pakiet javax.microedition.contactless.sc</i>	185
5.6.	<i>5A Aplikacja trybu czytnika/zapisu</i>	185
5.6.6	<i>Rejestr NFC Push</i>	199
5.7	Programowanie w trybie peer-to-peer	200
5.7.1	<i>Pakiet com.nokia.nfc.p2p</i>	200
5.7.2	<i>Pakiet com.nokia.nfc.llcp</i>	201
5.7.3	<i>Aplikacja działająca w trybie peer-to-peer</i>	204
5.8	Programowanie trybu emulacji karty	211
5.8.	<i>1Uzyskanie dostępu do bezpiecznego elementu przy użyciu JSR 257</i>	212
5.8.	<i>2Uzyskanie dostępu do bezpiecznego elementu przy użyciu JSR 177</i>	212
5.9	Studium przypadku trybu czytnika/zapisu: Zakupy NFC	215
5.10	Studium przypadku trybu peer-to-peer: NFC Gossiping	223
5.11	Podsumowanie rozdziału	236
	Pytania do rozdziału	238
	Referencje	239
6	Bezpieczeństwo i prywatność NFC	241
6.1	Ogólne bezpieczeństwo	241
6.1.1	<i>Dlaczego bezpieczeństwo jest ważne?</i>	242
6.1.2	<i>Podstawowe cele środków bezpieczeństwa</i>	243
6.1.3	<i>Podatność, zagrożenie, atak i ryzyko</i>	248
6.1.4	<i>Zasady bezpieczeństwa</i>	253
6.2	Narzędzia i mechanizmy bezpieczeństwa	257
6.2.1	<i>Kryptografia</i>	257
6.2.2	<i>Kryptografia symetryczna</i>	258
6.2.3	<i>Kryptografia asymetryczna</i>	259
6.2.4	<i>Hashing</i>	261
6.2.5	<i>Kod uwierzytelniania wiadomości (MAC) i HMAC</i>	261
6.2.6	<i>Podpis cyfrowy i podpis mobilny</i>	261
6.2.7	<i>Porównanie mechanizmów bezpieczeństwa</i>	262
6.2.8	<i>Certyfikaty cyfrowe i urząd certyfikacji</i>	263
6.2.9	<i>Nie utajniaj algorytmów kryptograficznych</i>	263
6.2.10	<i>Typy kluczy: Klucz symetryczny, klucz prywatny, klucz publiczny, klucz główny i klucz sesji</i>	264
6.2.11	<i>Zarządzanie kluczami i jego znaczenie</i>	264
6.2.12	<i>WEP (Wired Equivalent Privacy) i WPA (Wi-Fi Protected Access)</i>	264
6.2.13	<i>Inne komponenty bezpieczeństwa</i>	264

6.3	Ramy bezpieczeństwa NFC	265
6.3.1	<i>Problemy z bezpieczeństwem tagów NFC</i>	266
6.3.2	<i>Problemy z bezpieczeństwem czytnika NFC</i>	268
6.3.3	<i>Kwestie bezpieczeństwa kart inteligentnych</i>	269
6.3.4	<i>Kwestie bezpieczeństwa komunikacji</i>	270
6.3.5	<i>Bezpieczeństwo oprogramowania pośredniczącego i systemu zaplecza</i>	272
6.3.6	<i>Znormalizowane protokoły bezpieczeństwa NFC</i>	272
6.4	Prywatność, aspekty prawne i etyczne	277
6.4.1	<i>To jest inny świat</i>	278
6.4.2	<i>Kilka przykładów dotyczących kwestii prywatności</i>	279
6.4.3	<i>Podsumowanie dotyczące prywatności i środków zaradczych</i>	280
6.4.4	<i>Niektóre propozycje zapewnienia prywatności na tagach</i>	280
6.4.5	<i>Co zrobić, by chronić prywatność?</i>	281
6.5	Podsumowanie rozdziału	281
	Pytania do rozdziału	282
	Odniesienia	282
7	Ekosystem biznesowy NFC	283
7.1	Ekosystem biznesowy	283
7.1.1	<i>Ogólne cechy ekosystemu biznesowego</i>	285
7.1.	<i>2 Ekosystem biznesowy NFC</i>	286
7.2	Interesariusze w ekosystemie NFC	286
7.2.1	<i>Organy normalizacyjne i inni uczestnicy</i>	287
7.2.2	<i>Producenci i dostawcy zestawów chipów NFC</i>	288
7.2.3	<i>Producenci i dostawcy bezpiecznych elementów</i>	288
7.2.4	<i>Producenci i dostawcy telefonów komórkowych</i>	290
7.2.5	<i>Producenci i dostawcy czytników</i>	290
7.2.6	<i>Operatorzy sieci komórkowych</i>	290
7.2.7	<i>Zaufani menedżerowie usług</i>	290
7.2.8	<i>Dostawcy usług</i>	292
7.2.9	<i>Sprzedawcy detaliczni</i>	293
7.2.10	<i>Klienci</i>	293
7.3	Modele biznesowe	293
7.3.1	<i>Kluczowe wskaźniki w modelach biznesowych NFC</i>	295
7.3.	<i>2 Alternatywne modele biznesowe</i>	297
7.3.3	<i>Ogólny model przepływu dochodów/wydatków</i>	300
7.4	Studium przypadku: Sprzedaż biletów NFC	301
7.5	Dodatkowa lektura: Projekt Pay-Buy-Mobile realizowany przez GSMA	304
7.6	Podsumowanie rozdziału	308
	Pytania do rozdziału	309
	Referencje	309
8	Zarządzanie bezpiecznymi elementami	311
8.1	Wprowadzenie do technologii OTA	311
8.1.1	<i>Technologia OTA i zarządzanie urządzeniami mobilnymi</i>	312
8.1.2	<i>Technologia OTA i urządzenia SE oparte na UICC</i>	313

8.2	Specyfikacja GlobalPlatform	314
8.2.1	<i>Specyfikacja karty GlobalPlatform</i>	314
8.2.2	<i>Specyfikacja wiadomości GlobalPlatform</i>	316
8.3	Zarządzanie cyklem życia SE	316
8.3.1	<i>TSM w środowisku NFC</i>	317
8.3.2	<i>Aktorzy i ich role funkcjonalne w GlobalPlatform</i>	318
8.3.3	<i>UICC Based SE: Domeny i hierarchia zabezpieczeń</i>	320
8.3.4	<i>Modele zarządzania UICC</i>	320
8.4	Wiele środowisk SE	325
8.4.1	<i>Architektura bez agregacji</i>	325
8.4.2	<i>Architektura z agregacją</i>	326
8.5	Alternatywny model zarządzania OTA oparty na TSM	326
8.6	Podsumowanie rozdziału	328
	Pytania do rozdziału	329
	Odniesienia	329
9	Miasta i testy NFC	331
9.1	Miasta NFC	331
9.1.1	<i>Miasto Oulu</i>	331
9.1.2	<i>Miasto Nicea</i>	337
9.1.3	<i>Inteligentne przestrzenie miejskie</i>	339
9.2	Testy i projekty NFC	341
9.2.1	<i>Testy płatności zbliżeniowych</i>	341
9.2.2	<i>Transport i inne próby biletowe</i>	345
9.2.3	<i>Inne próby</i>	347
9.3	Podsumowanie rozdziału	349
	Odniesienia	349
Indeks		351

Przedmowa

Komunikacja bliskiego zasięgu (NFC) jest obecnie wschodząącym i obiecującym obszarem, który będzie miał ogromny wpływ na ekosystem finansowy, a także technologię mobilną na całym świecie w ciągu zaledwie kilku lat. Producenci telefonów komórkowych, operatorzy sieci komórkowych (MNO), instytucje finansowe, takie jak banki i firmy informatyczne, prowadzą działania badawczo-rozwojowe, aby jak najbardziej zwiększyć swój udział w torcie. NFC, będąc technologią komunikacji bezprzewodowej krótkiego zasięgu, która potencjalnie ułatwia korzystanie z telefonów komórkowych miliardom ludzi na całym świecie, oferuje ogromną liczbę przypadków użycia, w tym karty kredytowe, karty debetowe, karty lojalnościowe, kluczyki samochodowe, klucze dostępu do hoteli, biur i domów, ostatecznie integrując wszystkie takie materiały w jednym telefonie komórkowym. Solidne i pełne zrozumienia NFC wymaga wiedzy w czterech obszarach: Technologia NFC; Bezpieczeństwo i prywatność NFC; Rozwój aplikacji NFC; oraz Ekosystem biznesowy NFC. Wszystkie te zagadnienia zostały omówione w niniejszej książce, która ma na celu przedstawienie wiedzy od teorii do praktyki; w tym krótkie przypadki użycia, studia przypadków, przykłady rozwoju aplikacji, a wreszcie istniejące testy z całego świata. Książka ta dostarcza informacji na temat technologii NFC, które przemawiają do potrzeb niemal wszystkich użytkowników zainteresowanych technologią NFC i jej ekosystemem.

NFC Lab - Istambuł (www.NFCLab.com)

Ta książka jest wspólnym wysiłkiem naukowców z NFC Lab - Istanbul, który jest integralną częścią Uniwersytetu Is, ik w Stambule.

NFC Lab - Istanbul uważa NFC za nową technologię, która przekształca innowacyjne pomysły w rzeczywistość dla przyszłego społeczeństwa informacyjnego i komunikacyjnego.

NFC Lab - Istanbul dąży do doskonałości badawczej w ukierunkowanych obszarach badawczych związanych z NFC. Celem laboratorium jest współpraca z operatorami sieci komórkowych, instytucjami finansowymi, agencjami rządowymi, instytutami badawczymi, zaufanymi stronami trzecimi i innymi dostawcami usług w celu ułatwienia powszechnego korzystania z aplikacji NFC.

Laboratorium jest zaangażowane w pracę nad technologią NFC z multidyscyplinarną siecią ekspertów na całym świecie. Główny zespół jest odpowiedzialny za tworzenie i utrzymywanie partnerstw biznesowych i akademickich oraz dynamicznie generuje sieci na podstawie projektów.

Nasza motywacja do napisania tej książki

My, członkowie NFC Lab - Istanbul, wykonaliśmy wiele zadań akademickich i przemysłowych w ciągu ostatnich kilku lat. Ponieważ potrzebowaliśmy informacji,

musieliszy korzystać ze źródeł internetowych, białych ksiąg,

artykuły naukowe, prace organów normalizacyjnych i tak dalej. Wiele razy informacje, które uzyskaliśmy z kilku źródeł, były ze sobą sprzeczne. Rzeczywiście, czasami uzyskane przez nas informacje były niedokładne. Ponadto źródła obejmowały różne podejścia, których nie można było łatwo porównać.

Pomimo faktu, że NFC jest dopiero rozwijającą się dziedziną, liczba nowych artykułów generowanych codziennie rośnie, a zadowalającą ilość informacji można znaleźć w Internecie. Jednak zadanie gromadzenia informacji, a następnie wyszukiwania potrzebnej wiedzy jest mączące i czasochłonne.

Kiedy praktyk z pewnym doświadczeniem w programowaniu w Javie decyduje się na dostęp do tego nowego obszaru, konieczne jest znalezienie wymaganych źródeł z różnych źródeł. Nie będzie to trywialne, ponieważ aby zbudować aplikacje NFC przy użyciu języka Java, praktyk musi zebrać rozproszone informacje, a następnie połączyć je w celu lepszego zrozumienia. Nawet w tym przypadku użytkownik byłby w stanie zebrać niewielką ilość informacji.

Niektóre podstawowe informacje istnieją w domenie publicznej, a znacznie więcej istnieje w literaturze akademickiej, która albo nie jest publicznie dostępna, albo nie jest łatwa do połączenia z informacjami publicznymi przez osoby niebędące naukowcami.

Chociaż w aktualnej literaturze istnieją pewne podstawowe informacje, inne informacje są nadal niedostępne. Na przykład, w niniejszej pracy przeprowadziliśmy szeroko zakrojoną analizę ekosystemu.

W rezultacie zdaliśmy sobie sprawę z braku i potrzeby solidnego źródła, które zawierałyby dokładne informacje i odnosiło się do wszystkich osób zaangażowanych w technologię NFC i ekosystem biznesowy NFC ze standardową zawartością.

W rzeczywistości byliśmy właściwym zespołem dla NFC. Byliśmy zadowoleni, gdy stworzyliśmy namacalne produkty, takie jak artykuły konferencyjne, artykuły w czasopismach, aplikacje, projekty naukowe, projekty komercyjne, kursy i tak dalej. Pomyśleliśmy wtedy, że warto byłoby podzielić się naszą wiedzą z innymi. Ale jak moglibyśmy to zrobić? Rozwiązaniem było napisanie książki zawierającej zbiorową wiedzę członków.

Pozytywna dyskryminacja

Ze względu na prostotę używania zaimków i pozytywną dyskryminację, zignorowaliśmy zaimki męskie w całej tej książce. W związku z tym używamy tylko *she, her i herself* i zdecydowaliśmy się zignorować *he, him, his i himself*.

NFC: Wielki sukces czy kolejna porażka?

Historia jest pełna technologicznych i ekosystemowych porażek. Jednym z przykładów jest sieć telefonii satelitarnej. Zaledwie kilka lat temu NFC było nieznane. W krótkim czasie NFC zostało wprowadzone z wielkim entuzjazmem przez kilka organizacji, w tym departamenty rządowe, ośrodki badawcze i firmy.

Oczekiwano, że wykorzystanie NFC wzrośnie w ciągu ostatnich kilku lat, ale wydaje się, że było to wielokrotnie odkładane aż do teraz. To sprawiło, że wiele osób z branży ma wątpliwości co do potencjalnego sukcesu NFC.

W rzeczywistości istnieją dwie główne przeszkody na drodze do sukcesu NFC. Pierwszą z nich jest wystarczająca technologia, a drugą porozumienie ekosystemu przez zainteresowane strony. Kwestie te są ze sobą ściśle powiązane. Gdy zaangażowane strony stają się bardziej przekonane o technicznym sukcesie nowego modelu, mają tendencję do inwestowania większych zasobów w rozwój, a wraz z pojawiением się nowych ulepszeń technicznych ekosystem staje się bardziej ugruntowany i gotowy na boom. Ponadto, gdy strona inwestuje więcej w projekt, wydaje się bardziej chętna do zawarcia umowy z innymi zaangażowanymi stronami, aby odzyskać swoje pieniądze, a tym samym zapewnić lepszy zwrot z inwestycji (ROI).

Publiczność

Niniejsza książka jest skierowana do pracowników akademickich, badaczy, studentów, przedsiębiorców, analityków biznesowych i ekosystemowych, konsultantów, praktyków, menedżerów wyższego szczebla, menedżerów produktu, kierowników projektów, analityków oprogramowania, twórców systemów i programistów, którzy zamierzają inwestować w NFC lub przynajmniej chcą mieć szeroką wiedzę na ten temat. Poniżej podano odbiorców poszczególnych rozdziałów.

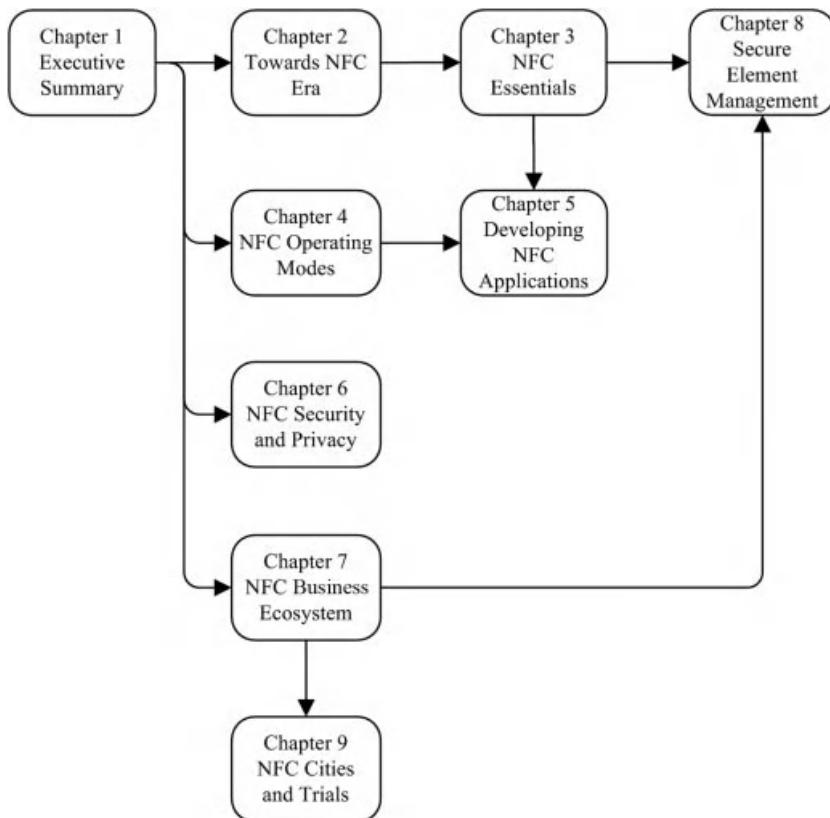
Reader Category	Chapter
Academicians	1 Executive Summary
Researchers	2 Towards NFC Era
Students	3 NFC Essentials
Entrepreneurs	4 NFC Operating Modes
Business and Ecosystem Analysts	5 Developing NFC Applications
Consultants	6 NFC Security and Privacy
Practitioners	7 NFC Business Ecosystem
Senior Managers	8 Secure Element Management
Product Managers	9 NFC Cities and Trials
Project Managers	
Software Analysts	
System Developers	
Software Developers	

Rozdział Zależności

1. *Streszczenie:* Ten rozdział nie wymaga żadnej wiedzy wstępnej.
2. *W kierunku ery NFC:* Chociaż ten rozdział nie wymaga dużej wiedzy podstawowej, zalecamy czytelnikom przeczytanie rozdziału 1, aby uzyskać ogólne zrozumienie technologii NFC. Czytelnicy tego rozdziału zapoznają się szczegółowo z podstawami technologii NFC i jej ewolucją.
3. *Podstawy NFC:* Zalecamy czytelnikom tego rozdziału przeczytanie rozdziału 1 w celu uzyskania ogólnej wiedzy na temat NFC oraz rozdziału 2 w celu szczegółowego zapoznania się z podstawowymi technologiami NFC, tak aby czytelnicy docenili techniczne i komunikacyjne podstawy trybów pracy NFC omówionych w tym rozdziale.
4. *Tryby pracy NFC:* Chociaż ten rozdział nie wymaga dużej wiedzy podstawowej, zalecamy czytelnikom przeczytanie rozdziału 1, aby uzyskać ogólne zrozumienie technologii NFC. Czytelnicy tego rozdziału zapoznają się szczegółowo z każdym trybem pracy. Będą w stanie zaprojektować aplikacje NFC w każdym trybie pracy, a także poznać korzyści płynące z zaprojektowanej aplikacji dla użytkownika.
5. *Tworzenie aplikacji NFC:* Ten rozdział wymaga ogólnych umiejętności programowania, a także podstawowej znajomości technologii Java. Czytelnicy powinni również posiadać wiedzę na temat trybów pracy NFC opisanych w rozdziale 4 i niektórych technicznych podstawa NFC opisanych w rozdziale 3. Czytelnicy tego rozdziału zdobędą podstawową wiedzę na temat programowania NFC.
6. *Bezpieczeństwo i prywatność NFC:* Chociaż ten rozdział nie wymaga dużej wiedzy podstawowej, zalecamy czytelnikom przeczytanie rozdziału 1, aby uzyskać ogólne zrozumienie technologii NFC. Czytelnicy tego rozdziału dowiedzą się o kwestiach bezpieczeństwa i prywatności technologii NFC.
7. *Ekosystem biznesowy NFC:* Chociaż ten rozdział nie wymaga dużej wiedzy podstawowej, zalecamy czytelnikom przeczytanie rozdziału 1, aby uzyskać ogólne zrozumienie technologii NFC. Czytelnicy tego rozdziału dowiedzą się o naturze ekosystemu biznesowego NFC z holistycznej perspektywy.
8. *Zarządzanie bezpiecznymi elementami:* Zalecamy czytelnikom przeczytanie Rozdziału 1, aby uzyskać ogólne zrozumienie technologii NFC, Rozdziału 3, aby dowiedzieć się o bezpiecznym elemencie i jego infrastrukturze w telefonach komórkowych NFC oraz Rozdziału 7, aby docenić znaczenie bezpiecznego elementu i koncepcji Over-the-Air (OTA) w modelach biznesowych NFC.
9. *Miasta i testy NFC:* Chociaż ten rozdział nie wymaga dużej wiedzy podstawowej, zalecamy czytelnikom przeczytanie rozdziału 1, aby uzyskać ogólne zrozumienie technologii NFC. Co więcej, odbiorcy tego rozdziału powinni również przeczytać rozdział 7. Czytelnicy tego rozdziału dowiedzą się o prowadzonych projektach, testach i wdrożeniach z całego świata oraz przeanalizują różne usługi NFC z holistycznej perspektywy. Pomoże to czytelnikom zdobyć ważną wiedzę na temat wdrożeń usług NFC na całym świecie.

Organizacja

Niniejsza książka składa się z dziewięciu rozdziałów. Są one ułożone w taki sposób, aby ułatwić czytelnikowi wybór odpowiedniego dla niego materiału. Potencjalni czytelnicy każdego rozdziału są określeni w jego treści poniżej.



Rozdział 1: Streszczenie

Niniejszy rozdział zawiera podsumowanie ekosystemu i technologii NFC. Czytelnicy tego rozdziału będą mogli uzyskać wstępную wiedzę na wysokim poziomie bez narażania się na niepotrzebne szczegóły techniczne. Czytelnicy otrzymają wystarczającą ilość informacji, aby zrozumieć, czym jest NFC w prawie wszystkich scenariuszach. Osoby, które zamierzają zająć się rozwojem systemu NFC, tworzeniem aplikacji NFC, świadczeniem usług NFC itp. będą musiały dodatkowo przeczytać powiązane rozdziały, aby uzyskać szczegółową wiedzę. Po zapoznaniu się z NFC w tym rozdziale, odbiorcy będą mogli wygodnie czytać inne rozdziały.

Odbiorcy tego rozdziału mogą dodatkowo przeczytać Rozdział 7 i Rozdział 9. Czytelnicy, którzy są zainteresowani bardziej technicznymi aspektami NFC, powinni przeczytać rozdziały 2-4, 6 i 8 w celu uzyskania dalszej wiedzy technicznej. Potencjalni członkowie zespołów opracowujących aplikacje NFC

Zachęcamy również do przeczytania rozdziału 5.

Rozdział 2: W kierunku ery NFC

Ten rozdział zawiera podstawową wiedzę na temat wszechobecnych komputerów, telefonów komórkowych, identyfikacji radiowej, kart inteligentnych i technologii NFC. Chociaż ten rozdział nie

wymaga dużej wiedzy podstawowej, zalecamy czytelnikom przeczytanie rozdziału 1, aby uzyskać ogólną wiedzę na temat technologii NFC w celu lepszego zrozumienia. Rozdział ten skierowany jest do czytelników wszystkich kategorii.

Czytelnicy tego rozdziału będą mogli poznać i docenić koncepcję NFC, a także łatwiej zrozumieć inne rozdziały. Zachęcamy odbiorców tego rozdziału do przeczytania również rozdziałów 7 i 9. Czytelnicy, którzy są zainteresowani bardziej technicznymi aspektami NFC, powinni przeczytać rozdziały 3, 4, 6 i 8, aby uzyskać dalsze techniczne zrozumienie. Rozdział 5 należy przeczytać, jeśli zamierzają być częścią zespołu opracowującego aplikacje NFC.

Rozdział 3: Podstawy NFC

Ten rozdział zawiera ogromną ilość informacji na temat technologii NFC w celu zapewnienia solidnego i pełnego zrozumienia. Obejmuje to wystarczającą wiedzę na temat urządzeń NFC i ich możliwości, telefonów komórkowych obsługujących NFC i ich szczegółów architektonicznych oraz organów normalizacyjnych w rozwoju telefonów komórkowych obsługujących NFC, cech warstwy częstotliwości radiowej NFC, a także podstaw technicznych i architektur komunikacyjnych każdego trybu pracy. Potencjalnymi czytelnikami tego rozdziału są naukowcy, badacze, studenci, praktycy, menedżerowie produktów i twórcy systemów.

Czytelnicy tego rozdziału zapoznają się szczegółowo z architekturą komunikacji każdego z trybów pracy NFC oraz innymi istotnymi kwestiami technicznymi. Wiedza ta pomoże czytelnikowi lepiej zrozumieć dalsze koncepcje technologii NFC, a także opracować systemy oparte na NFC.

Rozdział 4: Tryby działania NFC

Ten rozdział składa się głównie z trybów pracy NFC, w tym opisów, podstaw, przypadków użycia, ogólnych modeli użytkowania i korzyści każdego trybu pracy. Rozdział ten skierowany jest do czytelników wszystkich kategorii.

Czytelnicy tego rozdziału zapoznają się szczegółowo z każdym trybem pracy. Będą w stanie zaprojektować aplikacje NFC w każdym trybie pracy, a także poznać korzyści płynące z zaprojektowanej aplikacji dla użytkownika. Nasi czytelnicy mogą przeczytać rozdział 5, w którym omówiono programowanie aplikacji NFC w każdym trybie pracy. Czytelnicy, którzy są zainteresowani bardziej technicznymi aspektami NFC, powinni przeczytać rozdziały 6 i 8 w celu uzyskania dalszej wiedzy technicznej.

Rozdział 5: Tworzenie aplikacji NFC

Niniejszy rozdział przedstawia wszystkie informacje niezbędne do tworzenia aplikacji NFC. Na początku przedstawiono ogólne informacje dotyczące projektowania projektów NFC i zarządzania zespołem aplikacji. Ze względu na liczbę pozytywnych funkcji, dostępność interfejsów programowania aplikacji i duże doświadczenie na rynku, Java jest używana jako technologia programistyczna. Potencjalnymi czytelnikami tego rozdziału są akademicy, badacze, studenci, praktycy, kierownicy projektów, analitycy oprogramowania, programiści systemów i programiści.

Czytelnicy tego rozdziału zdobędą podstawową wiedzę w zakresie programowania NFC, a nabycie umiejętności programowania NFC w technologii Java pomogą użytkownikom łatwiej tworzyć aplikacje oparte na NFC w innych językach i platformach programistycznych. Nasi czytelnicy to

Zachęcamy również do przeczytania rozdziałów 7 i 9. Czytelnicy zainteresowani pogłębieniem wiedzy technicznej powinni przeczytać rozdziały 6 i 8.

Rozdział 6: Bezpieczeństwo i prywatność NFC

Niniejszy rozdział przedstawia wstępna wiedzę na temat bezpieczeństwa; podatności, zagrożeń, ataków i ryzyka; kryptografii; kwestii bezpieczeństwa NFC i mechanizmów zapobiegawczych w celu radzenia sobie z ryzykiem. Treść jest przeznaczona zarówno dla osób na wyższych lub kierowniczych, jak i niższych lub technicznych poziomach. Potencjalnymi czytelnikami są akademicy, badacze, studenci, konsultanci, praktycy, kierownicy projektów, analitycy oprogramowania, twórcy systemów i programiści.

Czytelnicy tego rozdziału zapoznają się szczegółowo z kwestiami bezpieczeństwa i prywatności dotyczącymi technologii NFC. Dzięki temu będą w stanie zaprojektować bezpieczne i interoperacyjne systemy i usługi oparte na NFC w każdym trybie pracy. Czytelnicy, którzy są zainteresowani uzyskaniem dalszej wiedzy technicznej, powinni przeczytać rozdział 8.

Rozdział 7: Ekosystem biznesowy NFC

Rozdział ten obejmuje ekosystem biznesowy NFC, w tym kompleksową analizę ekosystemu, ogólne role, punkty widzenia różnych stowarzyszeń, alternatywne modele biznesowe z czynnikami napędzającymi oraz studium przypadku. Potencjalnymi czytelnikami tego rozdziału są akademicy, badacze, studenci, przedsiębiorcy, analitycy biznesowi i ekosystemowi, konsultanci, praktycy, menedżerowie wyższego szczebla, menedżerowie produktu i kierownicy projektów.

Czytelnicy tego rozdziału poznają naturę ekosystemu biznesowego NFC i zrozumieją wymagania biznesowe uczestniczących w nim interesariuszy. Będą w stanie ocenić i zaprojektować usługi NFC ze zrównoważonymi modelami biznesowymi. Czytelnicy mogą również przeczytać rozdział 9, który przedstawia rzeczywiste testy NFC na całym świecie w różnych środowiskach biznesowych.

Rozdział 8: Bezpieczne zarządzanie elementami

Rozdział ten składa się głównie z technologii NFC, w tym podstaw technologii OTA, przeglądu specyfikacji GlobalPlatform, bezpiecznego elementu opartego na uniwersalnej karcie zintegrowanej (UICC) i jego architektury domeny bezpieczeństwa, różnych modeli zarządzania bezpiecznymi elementami opartymi na UICC, zarządzania wieloma bezpiecznymi elementami w jednym telefonie komórkowym NFC oraz alternatywnego modelu zarządzania OTA. Potencjalnymi czytelnikami tego rozdziału są pracownicy naukowi, badacze, studenci, praktycy, menedżerowie produktów, kierownicy projektów i twórcy systemów.

Czytelnicy tego rozdziału zdobędą szeroką wiedzę na temat technologii OTA; bezpiecznych elementów opartych na UICC i zarządzania ich cyklem życia za pomocą technologii OTA, a także alternatywnego modelu zarządzania OTA.

Rozdział 9: Miasta i testy NFC

Rozdział ten składa się z miast NFC, uruchomionych testów NFC i projektów, które do tej pory zostały opracowane na całym świecie. Potencjalnymi czytelnikami tego rozdziału są

studenci, przedsiębiorcy, analitycy biznesowi i ekosystemowi, konsultanci, praktycy, menedżerowie wyższego szczebla, menedżerowie produktu i kierownicy projektów.

Rozdział rozpoczyna się od opisu miast NFC, które są najpopularniejszymi implementacjami technologii NFC. Celem miast NFC może być testowanie implementacji lub nawet faktyczne wykorzystanie ich na określonej arenie. Miasta NFC testują głównie społeczny aspekt technologii NFC w porównaniu z testami i projektami. Kwestie użyteczności wraz z problemami związanymi z technologią można łatwo uzyskać w sposób ciągły poprzez testy w miastach NFC. W przypadku testów i projektów NFC, aspekt biznesowy aplikacji lub ekosystemu NFC jest testowany bardziej niż aspekt społeczny.

Apel o opinie i pomoc

Jest to jeden z pionierskich materiałów na temat technologii NFC, zapewniający tak obszerną zawartość. Jednym z wyzwań, przed którymi stanęliśmy, jest to, że ulepszenia są stale wprowadzane, niemal wykładowczo. W związku z tym książka będzie musiała zostać zaktualizowana w ciągu kilku lat. Zamierzamy aktualizować tę książkę, często ją ulepszając. Naszą motywacją jest umieszczenie tej książki w centrum ekosystemu NFC na świecie. Oprócz pracy, którą zamierzamy wykonać, będziemy wdzięczni za wszelkie opinie, dodatkowe materiały pomocnicze lub informacje, które mogą pomóc w ulepszeniu przyszłych wydań dla potencjalnych czytelników.

Będziemy wdzięczni za komentarze takie jak

- Wszelkie błędy, które wprowadziliśmy, lub ewentualnie ignorowanie niektórych faktów;
- Wszelkie brakujące, ale ważne punkty, które użytkownik uważa za istotne;
- Każdy brakujący, ale ważny wkład w technologię i ekosystem NFC, który mamy zignorowany;
- Propozycje nowych rozdziałów lub dodatkowych materiałów, które powinny zostać dodane do przyszłych wydań.

Aby uzyskać więcej informacji, odwiedź towarzyszącą stronę internetową - www.wiley.com/go/coskun

Wszelkie takie wiadomości e-mail należy kierować na adres: info@nfc-book.com. Wszelkie inne materiały można przesyłać na adres:

Vedad Coskun
ISIK University
Sile 34980
Stambuł Turcja

Podziękowania

Jesteśmy wdzięczni za wsparcie Uniwersytetu ISIK dla NFC Lab - Istanbul; w szczególności Prof. Dr. Siddik Binboga Yarman, Przewodniczącemu Rady Powierniczej; Prof. Dr. Nafiye Gunec Kiyak, Rektorowi; Aziz Genc, Sekretarzowi Generalnemu. Jesteśmy również wdzięczni prof. dr Erdalowi Cayirci, który udzielił wsparcia dla tej książki.

Lista akronimów

3DES	Potrójny DES
3G	Trzecia generacja
3GPP	3rd Generation Partnership
Project AC	Alternating Current
AES	Advanced Encryption Standard
AMS	Application Management
Software (oprogramowanie do zarządzania aplikacjami)	
	ANSI American National Standards
Institute APDU	Application Protocol Data Unit (Jednostka danych protokołu aplikacji)
API	Application Programming Interface
	APS Application Provider Security
Domain ASK	Amplitude Shift Keying (kluczowanie z przesunięciem amplitudy)
	BPSK Binary Phase Shift
Keying BS	Base Station
CA	Urząd certyfikacji
	CASD Controlling Authority Security
Domain CDC	Connected Device
Configuration	(Konfiguracja podłączonego urządzenia)
Bank wydający karty	CIBC Card
CLDCC	Connected Limited Device
Configuration CLF	Contactless Front-end
	CSMA Carrier Sense Multiple
Access DC	Direct Current
DES	Standard szyfrowania danych
	DoS Denial of Service
DSP	Digital Signal Processor
EAN	European Article Number
	ECC Elliptic Curve
Cryptography	(Kryptografia Krzywych Eliptycznych)
	ECMA Europejskie Stowarzyszenie
Producentów Komputerów	EDGE Zaawansowane dane dla ewolucji GSM
EMV	Europay, Mastercard i Visa
EPC TM	Elektroniczny kod produktu

ETSI Europejski Instytut Norm
Telekomunikacyjnych FIPS Federalny Standard
Przetwarzania Informacji

GPRS General Packet Radio
System GPS Global Positioning System

GSM	Global System for Mobile
Communications	Stowarzyszenie GSM
	Graficzny interfejs użytkownika
HCP	Protokół kontrolera hosta
HCIHost	Controller Interface
	HDLCHigh-Level Data Link
Control	
Kod uwierzytelniania wiadomości	oparty na
HMACHash	HSPAHigh Speed Packet Access
WEJŚCIE/WYJŚCIE	Wejście/wyjście
	ICIntegrated Circuit
ICAO	Organizacja Międzynarodowego Lotnictwa Cywilnego
ICT	Technologie informacyjne i komunikacyjne
IDPS	System wykrywania i zapobiegania włamaniom
IEC	Międzynarodowa Komisja
Elektrotechniczna IFF	Identyfikuj przyjaciela lub wroga
Domena zabezpieczeń	ISDIssuer
ISO	International Organization of Standardization
ITU	International Telecommunication Union
J2EE	Java™ 2 Enterprise Edition
J2ME	Java™ 2 Micro
Edition	J2SEJava™ 2 Standard
Edition	JADJava Application
Descriptor	JARJava Archive
JCPJava	Community Process
JCVM	Wirtualna maszyna
JavaCard	
	JCRMIIJavaCard Remote Method
Invocation	JISJapoński standard przemysłowy
JLS	Specyfikacja języka Java
JSP	Java Community Process
JSR	Żądania specyfikacji Java
JVM	Wirtualna maszyna Javy
KDFKey	Derivation Function
KMAKey	Management Authority
KVM	Kilobyte Virtual Machine
	LLCPLogical Link Control
Protocol MAC	Kod uwierzytelniania wiadomości
	MIDPMobile Information Device
Profile MIM	Man in the Middle
MMS	Multimedia Messaging Service
MNO	Network Operator MULTOS
	Multi-application Operating System
MVNO	Virtual Network Operator
NDEFNFC	Data Exchange Format
NFC	Komunikacja bliskiego zasięgu
NFCIP	Interfejs i protokół komunikacji bliskiego zasięgu

NFCIP-1	Interfejs i protokół komunikacji bliskiego zasięgu-1
NFCIP-2	Interfejs i protokół komunikacji bliskiego zasięgu-2
OMAOpen	Mobile Alliance
SYSTEM OPERACYJNY	System operacyjny
OTA	Over-the-Air
PC	Komputer osobisty
PCDProximity	Coupling
Device PDA	Personal Digital Assistant
(osobisty	asystent cyfrowy)
PICCProximity	Integrated
Circuit Card PIN	Personal Identification
Number PKI	Public Key Infrastructure
POS	Punkt sprzedaży
PSK	Phase Shift Keying
Jakość usług	QoS
Częstotliwość	radiowa
RFID	Radio Frequency
Identification RoI	Return of
Investment	
RTD	RSTResetowanie mikroprocesora
SATSIM	Definicja typu rekordu
SCOS	Smart Card Operating System
SCPSSmart	Card Platform
SCPSecure	Channel Protocol
SDK	Software
Development Kit SE	Secure Element
SEP	Protokół bezpiecznej wymiany
SIM	Moduł identyfikacji abonenta
SMC	Secure Memory Card
SMS	Usluga przesyłania krótkich wiadomości tekstowych
SSD	Supplementary Security
Domain SSL	Secure Sockets Layer
STEP	Secure Trusted Environment
Provisioning SWP	Single Wire Protocol
TLS	Bezpieczeństwo warstwy transportowej
TNF	Nazwa typu Format
TSMT	Zaufany
menedżer usług TT	PT Zaufana
UICC	strona trzecia
UMTS	Uniwersalna karta z układem scalonym
System UPC	Universal Mobile Telecommunication
URI	Uniwersalny kod produktu
USIM	Jednolity identyfikator zasobów
identyfikacji abonenta	Uniwersalny moduł
wirtualna	
VPN	Wirtualna sieć prywatna
WEP	Równoważna Prywatność
Przewodowa	

WI	Interfejs przewodowy
Wi-Fi	Bezprzewodowa łączność
	WiMAX Worldwide Interoperability for
Microwave Access WLAN	Bezprzewodowa sieć
lokalna	
WPA	Wi-Fi Protected Access
	WPAN Bezprzewodowa sieć
osobista WWAN	Bezprzewodowe sieci
rozległe	

1

Streszczenie

Near Field Communication (NFC) to nowa technologia i ekosystem, który pojawił się w ciągu ostatniej dekady. Technologia NFC to technologia komunikacji bezprzewodowej krótkiego zasięgu, wysokiej częstotliwości, niskiej przepustowości i między dwoma urządzeniami obsługującymi NFC. Komunikacja między urządzeniami NFC odbywa się na wysokiej częstotliwości 13,56 MHz, która pierwotnie była wykorzystywana przez identyfikację radiową (RFID). Choć RFID jest w stanie odbierać i nadawać na odległość większą niż kilka metrów, NFC ogranicza się do bardzo bliskiej odległości. Obecnie integracja technologii NFC z telefonami komórkowymi jest uważana za najbardziej praktyczne rozwiązanie, ponieważ prawie każdy ma je przy sobie.

Technologia NFC umożliwia komunikację między telefonem komórkowym z obsługą NFC na jednym końcu, a innym telefonem komórkowym z obsługą NFC, czytnikiem NFC lub tagiem NFC na drugim końcu. Potencjalne aplikacje i usługi wykorzystujące technologię NFC obejmują e-płatności, e-bilety, usługi lojalnościowe, identyfikację, kontrolę dostępu, dystrybucję treści, inteligentną reklamę, transfer danych/pieniądzy i usługi społecznościowe. Ze względu na możliwość zastosowania w szerokim zakresie obszarów i obiecujące możliwości tworzenia wartości dodanej, technologia ta przyciągnęła wielu naukowców, badaczy, organizacji i firm komercyjnych.

Zmiany lub ulepszenia RFID w celu wyeksponowania technologii NFC można opisać następująco:

- Komunikacja krótkiego zasięgu, podczas gdy RFID może wykorzystywać daleki zasięg, szczególnie w przypadku aktywnych tagów, które zawierają wbudowaną energię.
- Używanie tylko tagów pasywnych (w rzeczywistości występuje tylko w trybie czytnika/zapisu), podczas gdy zarówno aktywne, jak i w RFID możliwe są tagi pasywne.
- Bezpieczna wymiana danych dzięki komunikacji krótkiego zasięgu.
- Niejawne dopasowanie par, które wyrażają chęć nawiązania komunikacji NFC przez zbliżając się do siebie.
- Zainteresowanie firm integracją wielu usług, takich jak płatności debetowe i kredytowe karty, lojalność, identyfikacja, kontrola dostępu i tak dalej, ze względu na bezpieczną komunikację i niejawne dopasowanie, jak opisano w poprzednim punkcie.

Wykorzystanie technologii jest obecnie w fazie pilotażowej w wielu krajach. Kwestie użyteczności i przyjęcia technologii są badane przez wielu naukowców i organizacje przemysłowe. Wiele urządzeń mobilnych

© 2012 John Wiley & Sons, Ltd. Opublikowano 2012 przez John Wiley & Sons, Ltd.

producentów telefonów wprowadziło już na rynek swoje telefony komórkowe obsługujące technologię NFC. W miarę rozpowszechniania się telefonów komórkowych z obsługą NFC i uruchamiania usług komercyjnych, ludzie będą mogli płacić za towary i usługi, uzyskiwać dostęp do pokoi hotelowych lub mieszkań, aktualizować swoje informacje w sieciach społecznościowych, przesyłać swoje dane zdrowotne do szpitalnych systemów monitorowania z domu i korzystać z wielu innych usług za pomocą swoich telefonów z obsługą NFC.

Sukces technologii NFC wiąże się również z postępem w innych dziedzinach. Technologia Over-the-Air (OTA) pomiędzy uczestnikami ekosystemu jest zdecydowanie warunkiem wstępny do zadowalającej obsługi systemów NFC. Bezpieczny element (SE) jest również wymagany do przechowywania cennych informacji cyfrowych i bezpiecznego jednoczesnego wykonywania wielu usług NFC na tej samej karcie inteligentnej. Zależność od innych technologii jest jednym z wyzwań, przed którymi stoi obecnie NFC.

Kolejnym ważnym wyzwaniem są potencjalni interesariusze w ekosystemie NFC. NFC ma złożone i dynamiczne środowisko z dużą liczbą uczestniczących organizacji. Rozpoznaly one już możliwe wartości dodane, a każda ze stron stara się zmaksymalizować wartość swojego udziału. Własność i zarządzanie SE jest dominującym czynnikiem w uzyskaniu większego udziału, ponieważ każda transakcja musi korzystać z niektórych aplikacji zainstalowanych na SE, a właściciel zawsze może zażądać wyższego udziału. Obecnie operatorzy sieci komórkowych (MNO) są właścicielami i wydają UICC jako SE w telefonach komórkowych, a alternatywne własności SE są negocjowane między MNO, organizacjami finansowymi, a nawet producentami kart inteligentnych.

Należy pamiętać, że ten rozdział jest streszczeniem książki i dlatego odniesienia znajdują się na końcu powiązanych rozdziałów.

1.1 W kierunku ery NFC

NFC to technologia, która upraszcza i zabezpiecza interakcję z automatyką wszechobecną wokół nas. Koncepcja NFC opiera się na synergii kilku technologii, w tym komunikacji bezprzewodowej, urządzeń mobilnych, aplikacji mobilnych i kart inteligentnych. Programowanie po stronie serwera, usługi sieciowe i technologie XML również przyczyniają się do szybkiej poprawy i rozpowszechnienia technologii NFC. Wiele codziennych aplikacji, takich jak karty kredytowe, kluczyki samochodowe i karty dostępu do pokoi hotelowych, prawdopodobnie przestanie istnieć, ponieważ telefon komórkowy z obsługą NFC wystarczy, aby zapewnić wszystkie ich funkcje.

Obecnie NFC jest jednym z czynników umożliwiających wszechobecne przetwarzanie danych. Dlatego też pochodzenie tego pomysłu jest ściśle związane z wszechobecną informatyką. Aby zrozumieć związek NFC i wszechobecnego przetwarzania, musimy zacząć od historii wszechobecnego przetwarzania.

1.1.1 Wszechobecna informatyka

Istotą współczesnych komputerów są zautomatyzowane obliczenia i programowalność. Historia nowoczesnych komputerów obejmuje pracę pionierów na przestrzeni prawie dwustu lat. Komputery osobiste (PC) są ważnym krokiem po wczesnych komputerach, zmieniając sposób interakcji użytkownika z komputerami poprzez wykorzystanie klawiatur i monitorów do wprowadzania i wyprowadzania danych zamiast kart dziurkowanych, kabli itp. Mysz również zmieniła sposób interakcji ludzi i komputerów, ponieważ umożliwiła użytkownikom wprowadzanie danych przestrzennych do komputera. Ręka przyzwyczaiła się do trzymania myszy, a palec wskazujący przyzwyczaił się do jej klikania. Ruchy

urządzenia wskazującego są odzwierciedlane na ekranie przez ruchy kurSORA, tworząC prosty i intuicyjny sposób poruszania się po graficznym interfejsie użytkownika (GUI) komputera.

Ekrany dotykowe radykalnie zmieniły formę interakcji. Usunęły potrzebę stosowania wcześniejszych urządzeń wejściowych, a interakcja była wykonywana poprzez bezpośrednie dotknięcie ekranu, nowego urządzenia wejściowego. W międzyczasie wprowadzono telefony komórkowe, początkowo do komunikacji głosowej. Wczesne formy telefonów komórkowych zawierały klawiaturę. Telefony komórkowe z ekranami dotykowymi można uznać za najnowocześniejszą technologię, ponieważ ten sam ekran jest używany zarówno jako jednostka wejściowa, jak i wyjściowa, umożliwiając użytkownikowi bardziej intuicyjne działanie.

Wszehobecna informatyka to najwyższy poziom interakcji między ludźmi a komputerami, w którym urządzenia komputerowe są całkowicie zintegrowane z codziennym życiem i otaczającymi je przedmiotami oraz są proste w użyciu. Ubiquitous computing to model, w którym ludzie nie projektują swoich działań zgodnie z maszynami, z których muszą korzystać; zamiast tego maszyny dostosowują się do ludzkich potrzeb. Ostatecznie głównym celem jest to, aby ludzie korzystający z maszyn nie mieli zmieniać swoich normalnych zachowań, a także nawet nie zauważą, że wykonują czynności z pomocą maszyn.

1.1.2 Telefony komórkowe

Telefon komórkowy to urządzenie elektroniczne, które służy głównie do wykonywania połączeń głosowych, gdy użytkownik jest mobilny. Użytkownik telefonu komórkowego musi być zarejestrowany w sieci telefonii komórkowej, w której usługa jest świadczona przez MNO. Połączenie może być wykonane lub odebrane z dowolnego innego telefonu, który jest członkiem tej samej lub innej sieci telefonii komórkowej, sieci stacjonarnej, a nawet sieci internetowej. Telefony komórkowe obsługują motto "zawsze i wszędzie". Telefony komórkowe są również określane jako telefony komórkowe.

Telefony komórkowe są bardzo wygodne w użyciu i poręczne. Dlatego też, oprócz możliwości wykonywania połączeń głosowych, dołączono do nich ogromną liczbę dodatkowych usług, a wiele nowych usług, takich jak technologia NFC, jest wciąż w przygotowaniu. Obecnie obsługiwane usługi komunikacyjne telefonów komórkowych można przeglądać w oparciu o to, czy są to usługi przewodowe czy bezprzewodowe. Telefony komórkowe zawierają również ogromną ilość zintegrowanych usług.

Synchronizacja USB i PC to najważniejsze usługi przewodowe. Telefony są podłączone do komputerów, aby umożliwić transfer danych, synchronizację itp.

Z drugiej strony ilość usług bezprzewodowych jest znacznie większa. Komunikacja GSM jest oczywiście podstawową usługą świadczoną przez telefon komórkowy. W rzeczywistości była to usługa, którą zapewniały pionierskie telefony. Później wprowadzono usługę krótkich wiadomości tekstowych (SMS). Usługa wiadomości multimedialnych (MMS) mogła zostać włączona dopiero po osiągnięciu wysokiej szybkości transmisji danych między stacjami bazowymi a telefonami komórkowymi. Ponadto użytkownicy mogą korzystać z mobilnych usług radiowych i telewizyjnych za pomocą telefonów komórkowych. Usługi lokalizacyjne, w szczególności Globalny System Pozycjonowania (GPS), umożliwiły telefonom korzystanie z aplikacji takich jak nawigacja i interakcja z medianami społecznościowymi. Jedną z dodatkowych możliwości komunikacji z telefonami komórkowymi jest kilka usług peer-to-peer, takich jak podczerwień, Bluetooth i wreszcie NFC. Podczerwień wymaga linii wzroku, NFC wymaga bardzo bliskiej interakcji, a mianowicie dotykania, a Bluetooth wymaga komunikacji w niewielkiej odległości. Łączność Wi-Fi umożliwiła telefonom komórkowym dostęp do Internetu przy niskiej przepustowości. Poczta elektroniczna (e-mail) umożliwiła użytkownikom dostęp do ich skrynek odbiorczych lub wysyłanie wiadomości e-mail podczas korzystania z telefonu

komórkowego.

Przechowywanie danych kontaktowych i komunikacyjnych to najważniejsze usługi zintegrowane, ponieważ upraszczają one Globalny System Łączności Ruchomej (GSM). Istnieją inne zintegrowane usługi, które nie są związane z GSM, przynajmniej nie bezpośrednio. Zamiast tego, głównym celem tych usług jest

Usługi mają na celu wyeliminowanie dodatkowych urządzeń i zintegrowanie wszystkich w jednym urządzeniu. Kalkulator jest jedną z prymitywnych funkcji i eliminuje fizyczną potrzebę posiadania kalkulatora. Gry to funkcja, którą większość ludzi lubi mieć w swoich telefonach komórkowych. Robienie zdjęć i filmów, a nawet ich edycja za pomocą dodatkowych aplikacji są proste w użyciu, dzięki czemu dodatkowe kamery lub rejestratory wideo nie są wymagane. Odtwarzanie muzyki i wideo to dwie kolejne atrakcyjne funkcje. Co więcej, funkcja zegara i alarmu wyeliminowała potrzebę noszenia zegarków.

Niektóre z głównych usług bezprzewodowych oferowanych obecnie przez telefony komórkowe to nawigacja GPS, bezprzewodowe usługi internetowe, GSM, Bluetooth, Wi-Fi i technologie NFC.

1.1.3 Motywacja technologiczna NFC

Główną motywacją dla NFC jest integracja osobistych i prywatnych informacji, takich jak dane kart kredytowych lub debetowych w telefonach komórkowych. Dlatego bezpieczeństwo jest najważniejszym problemem, a zasięg komunikacji bezprzewodowej zapewniany nawet przez technologię RFID jest uważany za zbyt długi. Mechanizmy takie jak ekranowanie są niezbędne, aby zapobiec podsłuchiwaniu prywatnych informacji przez nieupoważnione osoby, ponieważ nawet niezasilane, pasywne tagi mogą być odczytywane z odległości ponad 10 m. W tym miejscu pojawia się NFC.

1.1.4 Komunikacja bezprzewodowa, RFID i NFC

Komunikacja bezprzewodowa odnosi się do przesyłania danych bez użycia kabli. Gdy komunikacja jest niemożliwa i niepraktyczna w przypadku użycia kabli, rozwiązaniem jest komunikacja bezprzewodowa. Zasięg komunikacji może ważyć się od kilku centymetrów do wielu kilometrów. Komunikacja bezprzewodowa jest zasadniczo mobilna, a komunikacja mobilna jest zasadniczo bezprzewodowa. Odróżniają również komunikację nomadyczną od mobilnej. Urządzenia, które umożliwiają komunikację nomadyczną, mogą w danym momencie wykonywać zarówno komunikację bezprzewodową, jak i przewodową. Przykładem komunikacji nomadycznej jest laptop. Bezpośrednią konsekwencją komunikacji bezprzewodowej jest mobilność. Mobilność pozwoliła ludziom być elastycznymi, ponieważ można do nich dotrzeć w dowolnym miejscu. Oczywiście jest, że mobilność zwiększyła produktywność, ponieważ komunikacja mobilna umożliwiła ludziom dostęp w dowolnym miejscu i czasie. Ma to duży wpływ na nasze codzienne życie. Ludzie stają się osiągalni nie tylko w celach komercyjnych, ale także ze względów społecznych. Obecnie dostępne usługi komunikacji mobilnej obsługujące mobilność to GSM, Bluetooth, Wi-Fi, WiMAX i ZigBee.

1.2 Ewolucja NFC

NFC można traktować jako rozszerzenie RFID, które wykorzystuje również interfejsy technologii kart inteligentnych. Aby zrozumieć technologię NFC, musimy mieć krótką wiedzę na temat prekursorów technologii NFC: kodu kreskowego jako wcześniejszej formy technologii RFID, RFID i karty z paskiem magnetycznym jako wcześniejszej formy kart inteligentnych i technologii kart inteligentnych.

1.2.1 Wcześniejsza forma RFID: technologia kodów kreskowych

Kod kreskowy jest wizualną reprezentacją danych obiektu, do którego jest dołączony.

Informacje na kodach kreskowych są skanowane przez czytniki kodów kreskowych i przesyłane do urządzeń komputerowych podłączonych do czytników. Następnie urządzenie przetwarza informacje.

Wczesne kody kreskowe reprezentują dane poprzez zmianę szerokości i odstępów między równoległymi liniami i są określane jako liniowe lub jednowymiarowe (1D). Ze względu na wykorzystaną przestrzeń, minimalną grubość każdego paska i ograniczenia orientacji, maksymalny adresowalny kod 1D nie jest wysoki. W przeciwieństwie do ograniczonej liczby dostępnych kodów 1D, później wyewoluowały dwuwymiarowe (2D) kody kreskowe, które mają większą pojemność do przechowywania danych. Przykładowo, kody kreskowe 2D na pudelku z lekami mogą zawierać określone informacje identyfikacyjne dla tego pudelka, dzięki czemu można śledzić każdego konkretnego pacjenta i każdy konkretny lek.

Niektóre z głównych przykładów liniowych kodów kreskowych to UPC (Universal Product Code) i EAN13 (European Article Number). Przykładem kodu kreskowego 2D jest również kod QR (Quick Response).

1.2.2 *Technologia RFID*

RFID to technologia wykorzystująca komunikację za pośrednictwem fal radiowych do wymiany danych między czytnikiem RFID a elektronicznym tagiem RFID (etykieta), tradycyjnie przymocowanym do obiektu, głównie w celu identyfikacji i śledzenia. Transmisja danych wynika z fal elektromagnetycznych, które mogą mieć różne zakresy w zależności od częstotliwości i pola magnetycznego.

Tagi RFID to małe układy scalone, które mogą pomieścić małe aplikacje, a także niewielką ilość danych. Istnieją dwa rodzaje tagów RFID: pasywne i aktywne. Tagi pasywne nie mają wewnętrznego zasilania, mają wbudowany układ scalony i antenę. Są one zasilane sygnałem przychodzącym z pola o częstotliwości radiowej (RF). Etykiety pasywne mają praktyczne odległości odczytu od około 10 cm do kilku metrów, w zależności od wybranej konstrukcji i rozmiaru RF i anteny. W przeciwieństwie do pasywnych tagów RFID, aktywne tagi RFID mają własne wewnętrzne źródło zasilania, które służy do zasilania wszelkich układów scalonych generujących sygnał wychodzący. Aktywne tagi są zazwyczaj znacznie bardziej niezawodne niż tagi pasywne ze względu na możliwość prowadzenia sesji z czytnikiem na większych odległościach. Główną wadą tagów RFID w porównaniu z papierowymi kodami kreskowymi jest ich wyższa cena.

Zarówno kody kreskowe, jak i znaczniki RFID mogą być kopiowane, jednak na różne sposoby. Kody kreskowe mogą być dystrybuowane elektronicznie, co umożliwia ich drukowanie i wyświetlanie na urządzeniu cyfrowym, takim jak komputer lub telefon komórkowy. Obraz kodu kreskowego można wysłać pocztą elektroniczną do dużej liczby osób, a wszyscy odbiorcy mogą natychmiast wydrukować kod kreskowy na zwykłym papierze. Zawartość tagów RFID może być również rozpowszechniana elektronicznie. Jednak do każdej kopii wymagany jest cyfrowy chip zamiast papieru. W porównaniu z kodami kreskowymi, produkcja oryginału i kopii jest droższa. Znacznik RFID ma dużą pojemność danych, a każdy pojedynczy znacznik ma unikalny kod, który jest podobny do kodów kreskowych 2D. Unikalność tagów RFID zapewnia możliwość śledzenia produktu, gdy przemieszcza się on z jednej lokalizacji do drugiej.

RFID była stosunkowo wczesną technologią i do tej pory opracowano wiele aplikacji RFID. Niektóre z tych zastosowań są następujące:

- *Kontrola zapasów:* Większość aplikacji RFID służy do zarządzania aktywami. Sklepy detaliczne używają tagów RFID na swoich produktach do kontrolowania zakupów, zmniejszania zapasów itp.
- *Drogi płatne:* Aktywne znaczniki RFID są przymocowane do pojazdów, dzięki czemu podczas podróży pojazdu

Koszt opłaty można łatwo odliczyć od rachunku właściciela.

- *Transport publiczny*: Wiele miast korzysta z systemów płatności RFID w transporcie publicznym, aby ułatwić dokonywanie płatności.
- *Paszporty*: Umieszczanie znaczników RFID w paszportach stało się powszechnym procesem, aby zapobiec ich podrabianie. Informacje takie jak zdjęcie właściciela, odcisk palca, adres, niektóre prywatne dane itp. są osadzone w tagu, dzięki czemu modyfikacja i nielegalne użycie jest trudniejsze niż przy użyciu samego drukowanego materiału.

1.2.3 Wcześniejsze formy kart inteligentnych: Karty z paskiem magnetycznym

Karta z paskiem magnetycznym to karta zawierająca cyfrową pamięć, do której dane są ładowane na etapie produkcji. Pasek składa się z małych cząsteczek magnetycznych w żywicy. Tradycyjnie jest to element tylko do odczytu. Jest on odczytywany poprzez fizyczny kontakt poprzez przeciagnięcie karty obok urządzenia z magnetyczną głowicą odczytującą. Obecnie paski magnetyczne są najczęściej używane na bankowych kartach debetowych i kredytowych, kartach lojalnościowych, biletach lotniczych i kartach pokładowych.

1.2.4 Technologia kart inteligentnych

Karta inteligentna to przedmiot zawierający wbudowany układ scalony ze zintegrowaną pamięcią, który najczęściej obejmuje bezpieczny mikrokontroler lub równoważne inteligentne urządzenie. Pod względem mechanizmu karty inteligentne można podzielić na trzy grupy: stykowe i bezstykowe karty inteligentne oraz modele hybrydowe.

Karty inteligentne nie zawierają żadnego źródła zasilania; dlatego energia jest dostarczana przez urządzenie zewnętrzne lub czytnik, z którym karta wchodzi w interakcję. Karty stykowe otrzymują wymaganą energię poprzez fizyczny kontakt, podczas gdy karty bezstykowe otrzymują energię poprzez pole elektromagnetyczne.

Stykowa karta inteligentna komunikuje się z czytnikiem kart poprzez bezpośredni kontakt fizyczny, podczas gdy bezstykowa karta inteligentna wykorzystuje w tym samym celu interfejs RF. Stykowe karty inteligentne zawierają mikromoduł zawierający pojedynczą krzemową kartę IC z pamięcią i mikroprocesorem. Zewnętrzne urządzenie zapewnia bezpośrednie połączenie elektryczne z przewodzącą płytka stykową po włożeniu do niej stykowej karty inteligentnej. Transmisja poleceń, danych i informacji o stanie karty odbywa się przez te fizyczne punkty styku.

W przypadku bezstykowych kart inteligentnych komunikacja odbywa się tylko wtedy, gdy urządzenia znajdują się w bliskiej odległości. Jednym z powodów jest zwiększenie bezpieczeństwa komunikacji, a innym umożliwienie wyższego transferu energii z urządzenia aktywnego (urządzenia z wbudowanym źródłem zasilania) do urządzenia pasywnego. Gdy bezstykowa karta inteligentna znajdzie się w zasięgu pola elektromagnetycznego czytnika kart inteligentnych, czytnik kart wysyła sygnał elektromagnetyczny, a karta inteligentna jest zasilana przez ten sygnał. Gdy karta inteligentna jest zasilana, może odpowiedzieć na żądanie czytnika.

Trzy główne bezstykowe karty inteligentne to ISO/IEC 10536 Close Coupling Smart Cards, ISO/IEC 14443 Proximity Coupling Smart Cards i ISO/IEC 15693 Vicinity Coupling Smart Cards. Karty inteligentne ze sprzężeniem bliskim działają w odległości do 1 cm, a karty inteligentne ze sprzężeniem zbliżeniowym działają w odległości mniejszej niż 10 cm (mniej niż 4 cala) przy częstotliwości 13,56 MHz. Karty inteligentne ze sprzężeniem bliskim działają w zasięgu do 1 m przy częstotliwości 13,56 MHz, takie jak te używane w

Popularnymi kartami są zbliżeniowe karty inteligentne, które umożliwiają szeroki zakres zastosowań w wielu dziedzinach, od zdrowia po rozrywkę. Pojawiły się różne technologie zbliżeniowych kart inteligentnych; jednak tylko kilka z nich stało się standardem ISO/IEC 14443, który zapewnia również interfejs dla transakcji NFC w zależności od trybu pracy. Obecnie najbardziej znany i konkurencyjnymi zbliżeniowymi kartami inteligentnymi są MIFARE, Calypso i FeliCa.

(i) *MIFARE*

MIFARE to dobrze znany i szeroko stosowany system zbliżeniowych kart inteligentnych 13,56 MHz, który jest rozwijany i jest własnością NXP Semiconductors, która jest spółką wydzieloną z Philips Semiconductors. MIFARE jest standardem ISO/IEC 14443 typu A. Obecnie MIFARE jest używany w ponad 80% wszystkich zbliżeniowych kart inteligentnych na świecie.

(ii) *Calypso*

Calypso to międzynarodowy standard biletu elektronicznego dla bezdotykowej karty elektronicznej z mikroprocesorem, pierwotnie zaprojektowany przez grupę europejskich operatorów tranzytowych z Belgii, Niemiec, Francji, Włoch i Portugalii. Zapewnia wiele źródeł kompatybilnych produktów i umożliwia interoperacyjność między kilkoma operatorami transportu na tym samym obszarze.

(iii) *FeliCa*

FeliCa to bezstykowy, zbliżeniowy, szybki system kart inteligentnych 13,56 MHz firmy Sony, stosowany głównie w kartach pieniądza elektronicznego. FeliCa nie stała się jednak standardem ISO/IEC.

1.2.5 *NFC jako nowa technologia*

NFC działa między dwoma urządzeniami w bardzo krótkim zasięgu komunikacji. Komunikacja NFC wykorzystuje widmo 13,56 MHz, podobnie jak w przypadku RFID. Obecnie dostępne prędkości transferu danych to 106, 212 i 424 kb/s. Technologia NFC działa w różnych trybach operacyjnych: czytnik/zapis, peer-to-peer i emulacja karty, gdzie komunikacja odbywa się między telefonem komórkowym NFC po jednej stronie, a pasywnym tagiem RFID (tagiem NFC), telefonem komórkowym NFC lub czytnikiem NFC po drugiej stronie. Technologia NFC została porównana z innymi technologiami pod względem szybkości przesyłania danych w rozdziale 2, rysunek 2.23. Jedną z głównych właściwości technologii NFC jest jej ukryte bezpieczeństwo ze względu na niewielką odległość komunikacji. Bliskość dwóch urządzeń sprawia, że prawdopodobieństwo przechwycenia sygnału jest bardzo niskie. Inną właściwością NFC jest możliwość automatycznego parowania. Aplikacja zainstalowana na urządzeniu mobilnym jest automatycznie uruchamiana po znalezieniu pasującej pary.

1.3 Podstawy NFC

Ponieważ podstawy wykorzystywanej technologii zostały przedstawione powyżej, możemy teraz przedstawić istotne szczegóły techniczne NFC. Aby to zrobić, struktura NFC i urządzenia NFC (tag NFC, czytnik NFC i telefon komórkowy NFC) muszą zostać wyjaśnione wystarczająco szczegółowo. Komunikacja opiera się na istniejących standardach, a urządzenia trzymają się tych standardów, aby zapewnić płynną aktywację. W związku z tym dostarczymy również informacji na temat organów normalizacyjnych, które sterują technologią NFC.

1.3.1 Inteligentne urządzenia NFC

Urządzenia NFC są działającymi komponentami NFC. NFC jest dostępne przy użyciu trzech urządzeń NFC: telefonu komórkowego NFC, czytnika NFC i tagu NFC.

- *Telefon komórkowy z obsługą NFC*: Telefony komórkowe z obsługą NFC, które są również określane jako telefony komórkowe NFC, są najważniejszymi urządzeniami NFC. Obecnie integracja technologii NFC z telefonami komórkowymi (wprowadzając w ten sposób telefony komórkowe z obsługą NFC) stwarza dużą szansę na łatwość użytkowania i akceptację ekosystemu NFC.
- *Czytnik NFC*: Czytnik NFC jest w stanie przesyłać dane z komponentem NFC. Czytnik Najczęstszym przykładem jest bezstykowy terminal POS (Point of Sale), który może wykonywać płatności bezstykowe z obsługą NFC po dotknięciu urządzenia NFC do czytnika NFC.
- *Tag NFC*: Tag NFC to w rzeczywistości tag RFID, który nie ma zintegrowanego źródła zasilania.

NFC działa w bardzo intuicyjny sposób. Dwa urządzenia NFC natychmiast rozpoczynają komunikację, gdy zostaną dotknięte. Dotknięcie jest traktowane jako warunek uruchomienia komunikacji NFC. Jest to ważna cecha technologii NFC. W przypadku NFC aplikacja NFC jest zaprojektowana w taki sposób, że gdy telefon komórkowy dotyka jakiegoś elementu NFC z oczekiwana formą danych, uruchamia się. W związku z tym użytkownik nie musi wchodzić w interakcję z urządzeniem mobilnym po dotknięciu jednego odpowiedniego urządzenia NFC, którym może być tag NFC, czytnik NFC lub inny telefon komórkowy z obsługą NFC. Jest to bardzo przydatna właściwość komunikacji NFC, która zapewnia wszechobecne przetwarzanie danych.

Dla każdej sesji komunikacji NFC, strona, która rozpoczyna lub inicjuje komunikację nazywana jest inicjatorem, podczas gdy urządzenie, które odpowiada na żądania inicjatora nazywane jest celem. Ten przypadek jest analogiczny do dobrze znanej architektury klient-serwer. Należy pamiętać, że w komunikacji klient-serwer klient inicjuje komunikację, a serwer odpowiada. Nie inaczej jest w przypadku komunikacji NFC.

W podejściu urządzenia aktywnego/pasywego, gdy komponent NFC ma wbudowane źródło zasilania, może generować własne pole RF i naturalnie inicjuje i prowadzi komunikację. Takie urządzenie nazywane jest urządzeniem aktywnym. Z drugiej strony, jeśli nie ma wbudowanego źródła zasilania, nazywane jest urządzeniem pasywnym i może reagować tylko na urządzenie aktywne.

Inicjator zawsze musi być urządzeniem aktywnym, ponieważ wymaga źródła zasilania do zainicjowania komunikacji. Obiekt docelowy może być natomiast urządzeniem aktywnym lub pasywnym. Jeśli cel jest urządzeniem aktywnym, wykorzystuje własne źródło zasilania, aby odpowiedzieć; jeśli jest urządzeniem pasywnym, wykorzystuje energię wytwarzaną przez pole elektromagnetyczne generowane przez inicjator, który jest urządzeniem aktywnym.

Rozważmy tag NFC, który jest urządzeniem o niskim koszcie i małej pojemności. Nie zawiera on żadnego źródła zasilania i potrzebuje zewnętrznego źródła zasilania do wykonania jakiejkolwiek czynności. W związku z tym tag NFC jest zawsze urządzeniem pasywnym i zawsze jest celem, ponieważ założenia nie zawiera żadnego źródła energii. Przechowuje dane, które mogą być odczytane przez aktywne urządzenie.

1.3.2 Standaryzacja telefonów komórkowych z obsługą NFC

Technologia NFC została opracowana wspólnie przez firmy Philips⁷ i Sony pod koniec 2002 roku na potrzeby komunikacji bezstykowej. Europejska organizacja ECMA International przyjęła tę technologię jako standard w grudniu 2002 roku.

2002. Międzynarodowa Organizacja Normalizacyjna (ISO) i Międzynarodowa Komisja Elektrotechniczna (IEC) przyjęły technologię NFC w grudniu 2003 roku. W 2004 roku Nokia, Philips i Sony założyły NFC Forum w celu promowania tej technologii. Standardy technologii NFC są uznawane przez ISO/IEC (Międzynarodowa Organizacja Normalizacyjna/Międzynarodowa Komisja Elektrotechniczna), ETSI (Europejski Instytut Norm Telekomunikacyjnych) i ECMA (Europejskie Stowarzyszenie Producentów Komputerów).

NFC to wspólna przygoda różnych technologii. Karty inteligentne, telefony komórkowe, czytniki kart, komunikacja krótkiego zasięgu, bezpieczna komunikacja, systemy transakcyjne i płatnicze to najważniejsze wiodące technologie. Ponieważ w grę wchodzi kilka technologii, powiązane organy organizacyjne zapewnili odpowiednie standardy. Mamy nadzieję, że zintegrowana forma tych standardów zdefiniuje wspólną wizję bezpiecznego, a jednocześnie funkcjonalnego użytkowania i transakcji. Interoperacyjny zestaw standardów jest niezbędny dla udanego ekosystemu NFC. Najbardziej dominującymi organizacjami standaryzacyjnymi są:

(i) *Forum NFC*

NFC Forum to stowarzyszenie zajmujące się określaniem standardów NFC opartych na normach ISO/IEC. NFC Forum zostało założone w celu umożliwienia technologii NFC i rozpowszechnienia jej na całym świecie. NFC Forum jest stowarzyszeniem branżowym non-profit utworzonym w celu poprawy wykorzystania bezprzewodowej interakcji krótkiego zasięgu NFC w elektronice użytkowej, urządzeniach mobilnych i komputerach PC. NFC Forum promuje wdrażanie i standaryzację technologii NFC w celu zapewnienia interoperacyjności między urządzeniami i usługami. Misją NFC Forum jest promowanie wykorzystania technologii NFC poprzez opracowywanie specyfikacji, zapewnianie interoperacyjności między urządzeniami i usługami oraz edukowanie rynku w zakresie technologii NFC.

Do tej pory NFC Forum ustandaryzowało dwa tryby pracy (tryb czytnika/zapisu i tryb peer-to-peer). Specyfikacje Record Type Definition (RTD) i NFC Data Exchange Format (NDEF) są dostarczane przez NFC Forum dla komunikacji w trybie czytnika/zapisu. W trybie peer-to-peer, Logical Link Control Protocol (LLCP) jest używany do łączenia aplikacji opartej na peer-to-peer z warstwą RF. Z drugiej strony tryb emulacji karty zapewnia możliwość obsługi kart inteligentnych w telefonach komórkowych.

Kolejną ważną zmianą wprowadzoną przez NFC Forum jest znak towarowy "N-Mark", który jest uniwersalnym symbolem NFC, dzięki czemu konsumenci mogą łatwo zidentyfikować, gdzie mogą być używane ich urządzenia obsługujące NFC.

(ii) *GlobalPlatform*

GlobalPlatform to międzybranżowe stowarzyszenie non-profit, które identyfikuje, rozwija i publikuje specyfikacje ułatwiające bezpieczne i interoperacyjne wdrażanie i zarządzanie wieloma wbudowanymi aplikacjami na bezpiecznych kartach inteligentnych. Celem specyfikacji GlobalPlatform jest zapewnienie interoperacyjności w zakresie zarządzania zawartością kart inteligentnych, zarządzania kartami inteligentnymi bez żadnych zależności od sprzętu, producentów lub aplikacji.

(iii) *GSM Association (GSMA)*

GSMA jest stowarzyszeniem operatorów telefonii komórkowej i powiązanych z nimi firm zajmujących się wspieraniem standaryzacji, wdrażania i promocji GSM. GSMA reprezentuje interesy światowej branży komunikacji mobilnej. GSMA koncentruje się na inicjowaniu, inkubowaniu i tworzeniu nowych możliwości dla swoich członków, a wszystko to w celu napędzania rozwoju branży komunikacji mobilnej.

(iv) ISO/IEC

ISO jest największym na świecie twórcą i wydawcą międzynarodowych standardów. Jest to organizacja pozarządowa, która tworzy pomożczy między sektorem publicznym i prywatnym. IEC jest międzynarodową organizacją non-profit, która przygotowuje i publikuje międzynarodowe standardy dla wszystkich technologii elektrycznych, elektronicznych i pokrewnych. ISO i IEC współpracują ze sobą w celu zapewnienia światowych standardów.

(v) ECMA International

ECMA International jest międzynarodową organizacją non-profit zajmującą się standaryzacją systemów informatycznych i komunikacyjnych. Badania ECMA obejmują urządzenia mobilne i NFC.

(vi) ETSI i ETSI Smart Card Platform (ETSI SCP)

ETSI jest organizacją non-profit zrzeszającą ponad 700 członków. ETSI opracowuje globalne standardy dla technologii informacyjnych i komunikacyjnych (ICT), w tym technologii stacjonarnych/mobilnych, radiowych, nadawczych i internetowych. ETSI SCP zajmuje się specyfikacjami modułów identyfikacji abonenta (SIM), które umożliwiały kartom SIM przenoszenie aplikacji NFC lub pełnienie innych ról w telefonach NFC.

(vii) Java Community Process (JCP)

JCP odpowiada za rozwój technologii Java, która jest ważnym kandydatem do zastosowań NFC. Jako otwarta, integracyjna organizacja aktywnych członków i osób niebędących członkami, kieruje przede wszystkim rozwojem i zatwierdzaniem specyfikacji technicznych Java.

(viii) Open Mobile Alliance (OMA)

OMA opracowuje otwarte standardy dla branży telefonii komórkowej. Członkami OMA jest wiele firm, w tym wiodący na świecie operatorzy komórkowi, dostawcy urządzeń i sieci, firmy informatyczne oraz dostawcy treści i usług.

(ix) Projekt partnerski trzeciej generacji (3GPP)

3GPP to współpraca między grupami stowarzyszeń telekomunikacyjnych w celu stworzenia globalnie stosowanej specyfikacji systemu telefonii komórkowej trzeciej generacji (3G). Specyfikacje 3GPP oparte są na rozwiniętych specyfikacjach GSM.

(x) EMVCo

EMVCo ma na celu zapewnienie globalnej interoperacyjności między kartami chipowymi i terminalami na całym świecie, niezależnie od producenta, instytucji finansowej lub wydawcy karty. Specyfikacje EMV 2000 są otwartym zestawem standardów dla systemów płatności opartych na kartach chipowych na całym świecie i dążą do współpracy w zakresie standardów płatności mobilnych.

1.3.3 Ogólna architektura telefonów komórkowych z obsługą NFC

Urządzenia mobilne zintegrowane z technologią NFC zawierają specyficzne dla NFC układy scalone, takie jak SE i interfejs NFC (patrz rozdział 3, rysunek 3.7). Interfejs NFC składa się z analogowo-cyfrowego front-endu zwanego NFC Contactless Front-end (NFC CLF), anteny NFC i kontrolera NFC umożliwiającego komunikację NFC. Kontroler NFC umożliwia komunikację NFC telefonu komórkowego z zewnętrznym urządzeniem NFC. Telefon komórkowy z obsługą NFC wymaga SE do przeprowadzania bezpiecznych transakcji z zewnętrznymi urządzeniami NFC. SE zapewnia bezpieczne środowisko dla powiązanych programów i danych. Umożliwia przechowywanie poufnych danych użytkownika. Umożliwia również bezpieczne przechowywanie i wykonywanie usług obsługujących NFC, takich jak

płatności zbliżeniowych. Zdefiniowano już różne standardy komunikacji NFC między dwoma urządzeniami obsługującymi NFC oraz transferu danych w telefonie komórkowym NFC, takie jak Single Wire Protocol (SWP) lub NFC Wired Interface (NFC-WI).

Kontroler hosta można zidentyfikować jako serce każdego telefonu komórkowego. Interfejs kontrolera hosta (HCI) tworzy pomost między kontrolerem NFC a kontrolerem hosta. HCI to logiczny interfejs, który umożliwia interfejsowi NFC, w tym front-endowi, bezpośrednią komunikację z procesorem aplikacji i wieloma SE w urządzeniach mobilnych.

1.3.4 Interfejs i protokół komunikacji bliskiego zasięgu (NFCIP)

W warstwie fizycznej interfejs i protokół komunikacji bliskiego zasięgu (NFCIP) jest standaryzowany w dwóch formach: NFCIP-1, który definiuje tryby komunikacji NFC w warstwie RF i inne cechy techniczne warstwy RF, oraz NFCIP-2, który obsługuje przełączanie trybów poprzez wykrywanie i wybieranie jednego trybu komunikacji.

(i) Interfejs i protokół komunikacji bliskiego zasięgu-1 (NFCIP-1)

Standard NFCIP-1 definiuje dwa tryby komunikacji: aktywny i pasywny. Definiuje również pole RF, interfejs sygnału komunikacyjnego RF i ogólny przepływ protokołu. Ponadto definiuje protokół transportowy, w tym aktywację protokołu, protokół wymiany danych z architekturą ramki i obliczaniem kodu wykrywania błędów (CRC dla obu trybów komunikacji przy każdej szybkości transmisji danych) oraz metody dezaktywacji protokołu.

(ii) Interfejs i protokół komunikacji bliskiego zasięgu-2 (NFCIP-2)

Standard NFCIP-2 określa mechanizm wyboru trybu komunikacji i nie zakłoca żadnej trwającej komunikacji na częstotliwości 13,56 MHz dla urządzeń wdrażających NFCIP-1, ISO/IEC 14443 i ISO/IEC 15693.

1.4 Tryby pracy i podstawowe funkcje NFC

Należy pamiętać, że w NFC istnieją trzy główne inteligentne urządzenia: telefony komórkowe z obsługą NFC, czytniki NFC i tagi NFC. Komunikacja NFC odbywa się między dwoma urządzeniami NFC z pewnymi prawidłowymi kombinacjami. Na przykład, telefon komórkowy może komunikować się z czytnikiem NFC.

Ponieważ NFC występuje w bardzo bliskim zasięgu, bardzo często zdarza się, że komunikujące się urządzenia dotykają się nawzajem. Z tego powodu proces ten nazywany jest paradygmatem dotykania. Świadomość użytkownika jest zdecydowanie niezbędna do wykonania NFC. Użytkownik najpierw wchodzi w interakcję z inteligentnym obiektem (czyli tagiem NFC, czytnikiem NFC lub innym urządzeniem mobilnym NFC) za pomocą telefonu komórkowego (patrz rozdział 4, rysunek 4.3). Po dotknięciu urządzenie mobilne może wykorzystać otrzymane dane i skorzystać z usług mobilnych, takich jak otwarcie strony internetowej, nawiązanie połączenia z usługą internetową itp.

1.4.1 Tryby pracy NFC

Jak już wspomniano, dostępne są trzy tryby pracy: czytnik/zapis, peer-to-peer i emulacja karty. Tryb czytnika/zapisu umożliwia jednemu telefonowi NFC wymianę danych z jednym tagiem NFC. Tryb peer-to-peer umożliwia dwóm telefonom komórkowym z obsługą NFC wymianę danych między sobą.

inne. W trybie emulacji karty telefon komórkowy może być używany jako karta inteligentna do interakcji z czytnikiem NFC. Każdy tryb pracy ma inną infrastrukturę techniczną, a także korzyści dla użytkowników.

(i) *Tryb czytnika/zapisu*

Ten tryb zapewnia komunikację telefonu komórkowego NFC z tagiem NFC. Celem komunikacji jest odczyt lub zapis danych z lub do tagu przez telefon komórkowy. Tryb ten można podzielić na dwa różne tryby: tryb czytnika i tryb zapisu. W trybie czytnika telefon komórkowy odczytuje dane z tagu NFC, natomiast w trybie zapisu telefon komórkowy zapisuje dane do tagu NFC.

(ii) *Tryb peer-to-peer*

Dwa telefony komórkowe NFC korzystające z tego trybu wymieniają między sobą dowolne dane. Ponieważ oba telefony komórkowe mają zintegrowane zasilanie, każdy z nich zużywa własną energię, będąc w trybie aktywnym w tym trybie. Dwukierunkowa komunikacja półduplekowa jest wykonywana w tym trybie podobnie jak w innych trybach, co oznacza, że gdy jedno urządzenie nadaje, drugie musi nasłuchiwać i może rozpoczęć transmisję danych po zakończeniu pierwszego.

(iii) *Tryb emulacji karty*

Tryb ten zapewnia możliwość działania telefonu komórkowego NFC jako zbliżeniowej karty intelligentnej. Niektóre przykłady emulowanych zbliżeniowych kart intelligentnych to karty kredytowe, karty debetowe, karty lojalnościowe itp. Jeden telefon komórkowy NFC może nawet przechowywać wiele aplikacji bezstykowych kart intelligentnych jednocześnie. Tryb emulacji karty jest ważnym trybem, ponieważ umożliwia płatności i aplikacje biletowe i jest kompatybilny z istniejącą infrastrukturą kart intelligentnych.

1.4.2 Podstawy trybu czytnika/zapisu

Jak już wspomniano, architektura techniczna każdego z trybów jest inna. Standardy i specyfikacje wykorzystywane przez każdy z trybów również mogą się różnić. W trybie czytnika/zapisu aktywny telefon komórkowy złączoną funkcją NFC inicjuje komunikację bezprzewodową i może odczytywać i zmieniać dane przechowywane w tagach NFC. Po pierwsze, interfejs RF używany w tym trybie jest zgodny ze schematami ISO/IEC 14443 typu A, typu B i FeliCa, które są bezstykowymi interfejsami kart intelligentnych (patrz rozdział 3, rysunek 3.24). Aplikacje działające w trybie czytnika/zapisu zwykle nie potrzebują bezpiecznego obszaru w telefonie komórkowym z obsługą NFC; proces polega jedynie na odczytywaniu danych przechowywanych w tagu i zapisywaniu danych na tagu.

W tym trybie operacyjnym NFC Forum wykonało różne specyfikacje i standardy w zakresie typów tagów, działania typów tagów i formatu wymiany danych między urządzeniami. Telefon komórkowy z obsługą NFC jest w stanie odczytywać typy tagów zatwierdzone przez NFC Forum. Cztery typy tagów zostały zdefiniowane przez NFC Forum i są oznaczone jako Typ 1, Typ 2, Typ 3 i Typ 4. Każdy typ tagu ma inny format i pojemność. Formaty tagów NFC są oparte na ISO 14443 typ A, ISO 14443 typ B lub Sony FeliCa.

Innym ważnym standardem jest NDEF. NDEF to format danych służący do wymiany informacji między dwoma urządzeniami NFC, a mianowicie między aktywnym urządzeniem mobilnym NFC a pasywnym tagiem lub aktywnym urządzeniem mobilnym NFC a aktywnym urządzeniem mobilnym NFC.

NDEF to binarny format komunikatów zaprojektowany do hermetyzacji jednego lub więcej ładunków zdefiniowanych przez aplikację w pojedynczej konstrukcji komunikatu.

Komunikat NDEF zawiera jeden lub więcej NDEF

rekordy i te rekordy mogą być łączone w łańcuchy w celu obsługi większych ładunków. Różne typy rekordów dla formatu wiadomości NDEF są zdefiniowane przez NFC Forum dla konkretnych przypadków; inteligentne plakaty, URI, podpis cyfrowy i tekst.

Typy rekordów zdefiniowane dla inteligentnych plakatów są najczęściej używane. Na przykład, dzięki zdefiniowanym typom rekordów inteligentnych plakatów, adresy URL, wiadomości SMS lub numery telefonów mogą być umieszczane na tagu zatwierdzonym przez Forum NFC. Po dotknięciu tagu urządzeniem NFC, informacje te mogą zostać odczytane i przetworzone. Inteligentny plakat zawiera dane, które uruchomią aplikację w urządzeniu, taką jak uruchomienie przeglądarki w celu wyświetlenia strony internetowej, wysłanie wiadomości SMS do usługi premium w celu otrzymania dzwonka itp.

1.4.3 Podstawy trybu peer-to-peer

W trybie peer-to-peer dwa telefony komórkowe z obsługą NFC nawiązują dwukierunkowe połaczenie na poziomie łączą w celu wymiany informacji, jak pokazano w rozdziale 3, rysunek 3.29. Mogą one wymieniać się wirtualnymi wizytówkami, zdjęciami cyfrowymi i innymi rodzajami danych lub wykonywać parowanie Bluetooth itd. Interfejs komunikacji radiowej trybu pracy peer-to-peer jest standaryzowany przez ISO/IEC 18092 jako NFCIP-1. W tym trybie używana jest również wiadomość NDEF, która jest odbierana przez LLCP, który jest również zdefiniowany przez NFC Forum. Format danych jest taki sam jak w trybie czytnika/zapisu.

LLCP jako protokół warstwy łączą danych obsługuje komunikację peer-to-peer między dwoma urządzeniami obsługującymi NFC, co jest niezbędne dla każdej aplikacji NFC, która obejmuje komunikację dwukierunkową. Specyfikacja LLCP definiuje pięć głównych usług: transport bezpołączeniowy, transport zorientowany na połaczenie, aktywację-nadzór-dezaktywację łączą, asynchroniczną zrównoważoną komunikację i multipleksowanie protokołów.

1.4.4 Podstawy trybu emulacji karty

W trybie emulacji karty telefon komórkowy z obsługą NFC działa jak karta inteligentna. Telefon komórkowy z obsługą NFC emuluje kartę inteligentną ISO 14443 lub chip karty inteligentnej zintegrowany z telefonem komórkowym jest podłączony do anteny modułu NFC. Gdy użytkownik przyłoży telefon komórkowy do czytnika NFC, czytnik NFC zainicjuje komunikację. Ten tryb pracy jest przydatny do bezpiecznych transakcji, takich jak płatności zbliżeniowe, aplikacje biletowe i kontrola dostępu.

Jak przedstawiono w rozdziale 3, rysunek 3.32, gdy czytnik NFC wchodzi w interakcję z urządzeniem NFC, urządzenie NFC działa jak standardowa karta inteligentna, a zatem czytnik NFC wchodzi w interakcję z SE i jego aplikacjami. Tylko tryb emulacji karty efektywnie wykorzystuje SE i bezpiecznie wykonuje funkcje.

1.4.5 Studia przypadków

Na końcu rozdziału 4 przedstawiamy następujące trzy studia przypadków, aby dokładnie wyjaśnić trzy tryby pracy i ich zastosowania:

1. System zakupów z obsługą NFC umożliwia użytkownikom robienie zakupów online w dowolnym miejscu, bez ograniczeń geograficznych. Ten przypadek użycia wykorzystuje tryb czytnika/zapisu.

2. Aplikacja plotkowania oparta na NFC działa w taki sam sposób jak plotkowanie i rozpowszechnia informacje między stronami. Ten przypadek użycia wykorzystuje tryb peer-to-peer.
3. Aplikacja do sprzedaży biletów do kina umożliwia dokonywanie płatności. Ten przypadek użycia wykorzystuje tryb emulacji karty.

W każdym przypadku użycia początkowo podany jest opis przypadku. Następnie podawane są diagramy przypadków użycia, diagramy aktywności i ogólne modele użycia. Pierwszy i drugi przypadek użycia są również zaimplementowane w Javie w rozdziale 5. Kody mogą być uruchamiane w emulatorze lub telefonie komórkowym po pomyślnej implementacji. Środowisko ekosystemu i modele biznesowe trzeciego przypadku użycia są analizowane w rozdziale 7.

1.5 SE i zarządzanie nim

Aby zapewnić bezpieczne przechowywanie i wykonywanie aplikacji obsługujących NFC, niezbędny jest SE. SE jest w rzeczywistości połączeniem sprzętu, oprogramowania, interfejsów i protokołów. Ponieważ bezpieczne funkcje są zapewniane głównie w trybie emulacji karty, SE jest również najczęściej używany w tym trybie. Gdy SE jest używany we właściwy sposób, to znaczy zgodnie z przewidzianymi standardami, użytkownicy i dostawcy usług mają pewność co do bezpieczeństwa całego procesu. Obecnie rozwijane są różne alternatywy SE, ale najpopularniejsze z nich to (patrz rozdział 3, rysunek 3.10):

- Sprzęt wbudowany;
- Bezpieczna karta pamięci (SMC);
- Uniwersalna karta z układem scalonym (UICC).

(i) *Sprzęt wbudowany*

Wbudowany SE jest nieusuwalnym komponentem w telefonie komórkowym. Ten chip jest wbudowany w telefon komórkowy na etapie produkcji i musi zostać spersonalizowany po dostarczeniu urządzenia do użytkownika końcowego. Wbudowany chip SE nie może być oczywiście przenoszony do innych telefonów komórkowych. Musi on zostać wymieniony i spersonalizowany za każdym razem, gdy telefon komórkowy jest używany przez innego użytkownika. SE nowego telefonu komórkowego musi być spersonalizowany dla użytkownika.

(ii) *SMC*

Wymieniony SMC składa się z pamięci, wbudowanego elementu karty inteligentnej i kontrolera karty inteligentnej. Innymi słowy, jest to połączenie karty pamięci i karty inteligentnej. Dzięki wymienionej właściwości i pamięci o dużej pojemności, SE oparty na SMC może obsługiwać dużą liczbę aplikacji i nie musi być ponownie wydawany, gdy klient kupuje nowy telefon komórkowy.

(iii) *UICC*

UICC to fizyczna karta inteligentna, na której zaimplementowany jest moduł tożsamości abonenta (SIM) lub uniwersalny moduł tożsamości abonenta (USIM). Dlatego jest powszechnie znany jako SIM lub USIM. SE oparty na UICC to wymieniona karta inteligentna używana w terminalach mobilnych w sieciach GSM i UMTS.

SE oparty na UICC zapewnia idealne środowisko dla aplikacji NFC. Jest osobisty, bezpieczny, przenośny i łatwy do zdalnego zarządzania za pośrednictwem technologii OTA. Posiadacz karty może mieć pewność, że transakcje są wykonywane z zachowaniem ochrony jego danych osobowych. Ma odpowiednią strukturę karty opartą na specyfikacji karty GlobalPlatform, która umożliwia wiele domen bezpieczeństwa dla różnych aplikacji na tej samej karcie inteligentnej. Dzięki wykorzystaniu OTA, nowe aplikacje NFC mogą być zdalnie instalowane na UICC, personalizowane, a cykl życia SE może być łatwo zarządzany. W związku z tym użytkownik nie musi fizycznie dotykać urządzenia mobilnego z obsługą NFC do systemu, aby wykonać którykolwiek z wymienionych procesów.

1.5.1 *Technologia Over-the-Air*

OTA to standard wymiany aplikacji i informacji związanych z aplikacjami za pośrednictwem bezprzewodowych mediów komunikacyjnych. Ułatwiając platformę OTA, można wprowadzać nowe usługi; SE mogą być dostępne, manipulowane i modyfikowane w szybki i opłacalny sposób za pośrednictwem platformy OTA. W oparciu o uzgodniony ekosystem, usługa OTA może być świadczona przez MNO lub inny zaufany podmiot.

Obecnie karty UICC są produkowane, przekazywane użytkownikowi, a tym samym są własnością OSK w sposób doraźny. OSK kontrolują i zarządzają UICC oraz wykorzystują funkcje OTA dostarczane przez tego samego OSK do zarządzania UICC. W związku z tym funkcje OTA są uważane za część głównych funkcji OSK, a także za część zarządzania urządzeniami mobilnymi.

1.5.2 *Specyfikacja karty GlobalPlatform*

Należy pamiętać, że specyfikacja karty GlobalPlatform zawiera szczegóły karty inteligentnej. W oparciu o standardy zdefiniowane przez GlobalPlatform, logiczne i fizyczne komponenty karty inteligentnej mają na celu zapewnienie interoperacyjności aplikacji i bezpieczeństwa w środowisku kontrolowanym przez emitenta.

Domeny bezpieczeństwa są niezwykle ważne, aby karty inteligentne oparte na platformie GlobalPlatform zapewniały wystarczający poziom bezpieczeństwa. W rzeczywistości domeny bezpieczeństwa są reprezentantami władz poza kartą. Umożliwiają one zarządzanie aplikacjami w bezpieczny sposób, zapewniając pełną separację kluczy kryptograficznych, a domeny bezpieczeństwa można podzielić na kategorie, odzwierciedlając różne typy władz poza kartą rozpoznawanych przez kartę:

- Emitent Security Domain (ISD) jest przedstawicielem wydawcy karty na karcie. Ten komponent reprezentuje obszar emitenta na karcie, który kontroluje aplikacje emitenta.
 - Supplementary Security Domain (SSD) jest przedstawicielem aplikacji na karcie dostawców i wydawców kart. Ten komponent umożliwia dostawcom aplikacji współdzielenie i wykorzystywanie terytorium na karcie bez ryzyka naruszenia zarządzania kartą lub jakąkolwiek aplikacją na karcie.
 - Controlling Authority Security Domain (CASD) jest w rzeczywistości podtypem SSD. Domena

Rolą organu kontrolującego jest egzekwowanie polityki bezpieczeństwa dla wszystkich aplikacji na karcie.

1.5.3 Zaufany menedżer usług

Aby wdrożyć aplikacje i usługi NFC na SE użytkownika, dostawcy usług i MNO mają różne wymagania. Aby stworzyć i zarządzać zaufanym środowiskiem oraz umożliwić podmiotom bezpieczną komunikację między sobą, wymagany jest dodatkowy zaufany podmiot; Trusted Service Manager (TSM), który jest niezależną stroną obsługującą inne podmioty ekosystemu NFC zgodnie z wymaganiami. TSM zapewnia poziom zaufania i poufności między głównymi uczestnikami systemu, takimi jak dostawcy usług i MNO podczas zarządzania cyklem życia aplikacji.

1.5.4 Modele zarządzania UICC

Standardy kart inteligentnych GlobalPlatform definiują proces zarządzania zawartością karty jako obejmujący kilka działań: ładowanie początkowego zestawu kluczy domeny bezpieczeństwa, kodowanie aplikacji przez stronę trzecią, ładowanie aplikacji, personalizację i tak dalej.

GlobalPlatform definiuje trzy modele zarządzania zawartością kart: tryb prosty, tryb delegowany i tryb autoryzowany. Modele te obejmują ładowanie aplikacji i procesy personalizacji na SE. Tryb prosty jest modelem całkowicie skoncentrowanym na wydawcy karty, podczas gdy tryb delegowany i tryb autoryzowany są modelami bardziej skoncentrowanymi na TSM. Specyfikacja komunikatów GlobalPlatform obsługuje wszystkie modele wdrażania.

(i) Tryb prosty przy użyciu platformy MNO OTA

W trybie prostym dostawca usług deleguje pełne zarządzanie swoją aplikacją obsługującą NFC do TSM. TSM zarządza domeną bezpieczeństwa w imieniu usługodawcy. MNO jest upoważniony do wykonywania funkcji zarządzania zawartością karty, a mianowicie ładowania, instalowania, aktywowania i usuwania aplikacji na SE. TSM zarządza jedynie procesami blokowania, odblokowywania i personalizacji aplikacji przy użyciu własnego serwera OTA i sieci MNO.

(ii) Tryb delegowany z pełną delegacją do TSM

Przypadek delegowanego zarządzania można opisać jako ładowanie skoncentrowane na TSM. W tym przypadku MNO nie jest już odpowiedzialny za ładowanie, instalowanie, aktywowanie lub usuwanie aplikacji. Zarządzanie zawartością karty jest wykonywane przez TSM przy wstępnej autoryzacji ze strony MNO. W niektórych przypadkach dostawca usług może potrzebować zarządzać własnym procesem personalizacji aplikacji, aby zapobiec manipulowaniu kluczami aplikacji lub danymi aplikacji przez osoby trzecie.

(iii) Tryb autoryzowany z pełną delegacją do TSM

Wdrożenie autoryzowanego zarządzania jest całkowicie zorganizowane wokół opcji centralnego ładowania TSM. TSM posiada aplikacje dostawcy usług i jest w stanie zarządzać zawartością karty bez autoryzacji (lub konieczności użycia tokena) od MNO. Podobnie jak w trybie delegowanym, dostawca usług może zarządzać własną personalizacją aplikacji zamiast delegować ją do TSM.

1.5.5 Wiele środowisk SE

Można również zauważyć, że pojedynczy telefon komórkowy z obsługą NFC może obsługiwać wiele SE. Na przykład, telefon komórkowy może zawierać wbudowany sprzęt lub SMC, który jest zintegrowany z NFC.

przez producenta podczas procesu produkcji, wraz z SE opartym na UICC, który jest osadzany przez MNO przed przekazaniem telefonu komórkowego klientowi. Wiele problemów może pojawić się, gdy wiele SE znajduje się na tym samym telefonie komórkowym z obsługą NFC. Jeden z problemów może pojawić się podczas wdrażania aplikacji w trybie emulacji karty. Czytnik NFC musi zainicjować komunikację tylko z jednym SE na telefonie komórkowym z obsługą NFC. Innym problemem jest zarządzanie wieloma SE w tym samym czasie. Według GlobalPlatform możliwe są dwa modele biznesowe: architektura bez agregacji i architektura z agregacją:

- *Architektura bez agregacji*: Kontroler NFC może być używany tylko przez jeden SE w danym czasie, a zatem tylko jeden SE może być aktywny w danym czasie. SE jest aktywowany przez użytkownika, dzięki czemu aktywowany SE jest w stanie wykonywać transakcje zbliżeniowe z obsługą NFC. Użytkownik jest odpowiedzialny za wybór właściwego SE w tym modelu.
- *Architektura z agregacją*: Wszystkie SE hostowane w telefonach komórkowych z obsługą NFC są aktywne na w tym samym czasie. Każda aplikacja na dowolnym SE może wykonywać transakcje zbliżeniowe NFC w dowolnym momencie. Oczywiście każdy SE może zawierać jedną lub więcej aplikacji. Aplikacja powinna być wybierana przez zewnętrzny czytnik NFC.

1.6 Rozwój aplikacji NFC

Tworzenie aplikacji NFC jest ważną częścią technologii NFC. Aby opracować aplikacje NFC, wymagane jest pełne zrozumienie technologii NFC i trybów pracy. Istnieją dwa różne typy aplikacji w usługach NFC. Pierwszym z nich jest aplikacja graficznego interfejsu użytkownika (GUI), która istnieje we wszystkich aplikacjach trybu operacyjnego. Aplikacja GUI zapewnia interfejs, który pozwala użytkownikowi na interakcję z urządzeniem mobilnym. Zapewnia również możliwość odczytu i zapisu z i do komponentów NFC. Drugim typem jest aplikacja SE, która jest potrzebna do zapewnienia bezpiecznego i zaufanego środowiska dla aplikacji wymagających bezpieczeństwa (np. karty kredytowej). Na rynku dostępne są różne narzędzia programistyczne przeznaczone dla różnych telefonów komórkowych. Niektóre z tych narzędzi programistycznych to:

- Android SDK (Software Development Kit) dla telefonów komórkowych z systemem Android;
- Qt SDK dla telefonów komórkowych z systemem Symbian 3;
- Seria 40 Nokia 6212 NFC SDK dla urządzeń Nokia 6212.

Java jest dobrze znanym językiem programowania obiektowego i może być używana w różnych środowiskach, od komputerów PC po lodówki i od serwerów po telefony komórkowe. Java, w kontekście NFC, dostarczyła jeden z pierwszych interfejsów API (Application Programming Interfaces). W rozdziale 5 przedstawiliśmy informacje na temat tworzenia aplikacji NFC przy użyciu języka Java. Wnioski wyciągnięte z rozdziału 5 pomogą użytkownikom tworzyć aplikacje oparte na NFC również na innych platformach programistycznych.

Java udostępnia dwa interfejsy API dla rozwoju NFC: JSR 257 (Contactless Communication API) i JSR 177 (Security and Trust Services API). JSR 257 umożliwia głównie programowanie aplikacji w trybie czytnika/zapisu, podczas gdy JSR 177 i niektóre klasy w JSR 257 zapewniają dostęp do SE w celu implementacji projektów w trybie

Tabela 1.1 Pakiety JSR 257

Pakiet	Opis
javax.microedition.contactless	Zapewnia wspólne funkcje dla wszystkich celów bezstykowych takie jak wykrywanie celu
javax.microedition.contactless.ndef	Zapewnia funkcjonalność wymiany sformatowanych danych NFC Forum
javax.microedition.contactless.rf	Umożliwia komunikację z tagami RFID, które zawierają dane z tagami RFID
javax.microedition.contactless.sc	Umożliwia komunikację z kartami inteligentnymi ISO14443-4
javax.microedition.contactless.visual	Umożliwia komunikację z tagami wizualnymi

programowanie, wymagane są własne interfejsy API, ponieważ ten tryb nie jest obsługiwany przez standardowe interfejsy API Java.

1.6.1 JSR 257

Ten interfejs API zapewnia interfejs programowania aplikacji, który umożliwia aplikacjom dostęp do tagów RFID, kart inteligentnych i tagów wizualnych (kodów kreskowych). Dla każdego typu celu zdefiniowano różne pakiety, a aplikacja korzystająca z tego interfejsu API może wykrywać cele zbliżeniowe w pobliżu, powiadamiać aplikacje o wykryciu i wykonywać operacje zbliżeniowe. Kilka klas w tym API umożliwia również dostęp do SE przy użyciu połączenia ISO 14443. Tabela 1.1 podsumowuje pakiety w JSR 257.

1.6.2 JSR 177

Ten interfejs API definiuje opcjonalne pakiety do obsługi komunikacji kart inteligentnych i operacji bezpieczeństwa. Usługi podpisu cyfrowego, zarządzanie poświadczeniami użytkownika, operacje kryptograficzne i inne mogą być implementowane za pomocą tego API. Umożliwia telefonom komórkowym dostęp do kart inteligentnych przy użyciu protokołów APDU (Application Protocol Data Unit) i JavaCard Remote Method Invocation (RMI). JSR 177 składa się z czterech opcjonalnych pakietów (podsumowanych w tabeli 1.2), które również składają się z różnych pakietów i klas.

Tabela 1.2 Pakiety JSR 177

Pakiet opcjonalny	Opis
SATSA-APDUE	Umożliwia komunikację z kartami inteligentnymi przy użyciu protokołu na podstawie APDU
SATSA-JCRMIE	Umożliwia komunikację z kartami inteligentnymi przy użyciu JavaCard
Protokół RMI	
SATSA-PKIE	umożliwia kartom inteligentnym zarządzanie podpisami cyfrowymi i certyfikaty
SATSA-CRYPTO	Przeprowadza operacje kryptograficzne, takie jak skróty wiadomości

Tryb peer-to-peer nie jest obsługiwany przez standardowe interfejsy API Java; istnieją jednak rozszerzenia interfejsu API komunikacji zbliżeniowej, które umożliwiają programowanie w trybie peer-to-peer. Są to zazwyczaj interfejsy API specyficzne dla urządzeń mobilnych, a mianowicie zastrzeżone interfejsy API.

Rejestr Push jest kolejnym ważnym tematem w NFC i może zwiększyć użyteczność aplikacji. Zazwyczaj aplikacje mogą być uruchamiane przez użytkownika z menu telefonu komórkowego. Jednak aplikacja może również działać bez żadnego działania użytkownika, ale z funkcją "Push". Na przykład, aplikacja może zostać uruchomiona za pomocą pakietu sieciowego otrzymanego przez przychodząą wiadomość SMS. Rejestr Push po prostu utrzymuje listę połączeń przychodzących i automatycznie uruchamia aplikacje na podstawie otrzymanych połączeń. W przypadku NFC umożliwia uruchamianie aplikacji za pomocą połączenia NFC.

Aby aktywować usługę rejestrów push, aplikacja powinna być zarejestrowana do uruchamiania z określonym połączeniem. Możliwe są dwa rodzaje rejestracji: dynamiczna i statyczna. W przypadku rejestracji statycznej aplikacja jest rejestrowana dla rejestrów push podczas instalowania jej na urządzeniu mobilnym. Z drugiej strony, rejestracja dynamiczna jest wykonywana przy pierwszym uruchomieniu aplikacji.

Rejestracje dynamiczne i statyczne mają swoje zalety i wady. Rejestracja statyczna umożliwia łatwą rejestrację połączenia push bez działania użytkownika na etapie instalacji. Jeśli jednak w urządzeniu znajduje się wpis rejestrów push powodujący konflikt, aplikacja nie może zostać zainstalowana. Z drugiej strony, dynamiczna rejestracja eliminuje ten problem. Jedną z wad dynamicznej rejestracji jest to, że aby zapisać wpis rejestrów push, pierwsze wykonanie aplikacji musi zostać wykonane z akcją użytkownika.

1.7 Bezpieczeństwo i prywatność NFC

Chociaż telefon komórkowy jest prawie identyczny z komputerem PC pod względem technicznym, różni się, ponieważ jest bardziej osobistym przedmiotem i najczęściej noszonym przez ludzi w życiu codziennym. Użytkownicy zazwyczaj wierzą, że ich telefony komórkowe są ważną częścią ich życia i zazwyczaj poddają je fizycznemu nadzorowi. Jednak telefon komórkowy jest nadal narażony na ataki fizyczne, takie jak kradzież, oraz techniczne ataki bezprzewodowe przy użyciu technologii komunikacyjnych Bluetooth lub WI-FI. Zintegrowana funkcja NFC nakłada również pewne dodatkowe zagrożenia na telefony komórkowe.

1.7.1 Dlaczego bezpieczeństwo jest ważne?

Usługa jest użyteczna tylko wtedy, gdy jest zarówno funkcjonalna, jak i wystarczająco bezpieczna. Użytkownik początkowo dba o funkcjonalność, a dopiero później zauważa znaczenie bezpieczeństwa. Podsumowując, użytkownik chętnie korzysta z usługi tylko wtedy, gdy jest ona funkcjonalna i jednocześnie bezpieczna. Niedoskonałości techniczne i przeszkody związane z bezpieczeństwem są potencjalnie niepokojące dla użytkowników.

Kilkadziesiąt lat temu ludzie nie byli świadomi znaczenia bezpieczeństwa usług. Gdy zaczęły pojawiać się złośliwe działania, zarówno ludzie, jak i firmy zaczęli dostrzegać znaczenie bezpieczeństwa, ale dopiero po tym, jak koszty szkód stały się znaczne. Hakerzy zauważali również, że oprócz dumy z uzyskania nielegalnego dostępu do zasobów i wyrządzenia szkód, mogą również zyskać finansowo.

Istnieją pewne oczywiste powody, dla których zagrożenie bezpieczeństwa wzrosło tak bardzo w ostatnim czasie. Przedstawiono trzy punkty widzenia.

Punkt widzenia hakerów:

- Mogą otrzymać nagrodę finansową.
- Mogą zaspokoić swoje ego.
- Mogą nawet stać się sławni, gdy wykonają niezwykle udane akcje.

Punkt widzenia użytkowników:

- Liczba użytkowników Internetu wzrasta wykładniczo; w związku z tym możliwości złośliwych działań również rosną. Jeden haker może wypróbować tę samą metodę, aby zhakować wiele potencjalnych ofiar.
- Ilość aktywów finansowych wzrosła, co skutkuje większą nagrodą finansową dla hakerów.

Techniczny punkt widzenia:

- Organizacje tradycyjnie ignorują bezpieczeństwo na początkowym etapie tworzenia oprogramowania. Jednym z powodów jest utrzymanie wydatków w ramach budżetu, a bezpieczeństwo wydaje się najbardziej oczywistym obszarem, w którym można obniżyć koszty. Skutkuje to niepowodzeniem w zakresie bezpieczeństwa systemu, nawet jeśli w późniejszym czasie zostanie włożony ogromny wysiłek, ponieważ nie jest łatwo zintegrować bezpieczeństwo, jeśli zostanie ono zignorowane w fazie projektowania.

Teraz nadszedł czas, aby dokonać projekcji znaczenia bezpieczeństwa w ekosystemie NFC. Główne powody, dla których NFC jest kuszącym celem, są następujące:

- NFC to nowa technologia zintegrowana z telefonami komórkowymi.
- Prawie każdy posiada telefon komórkowy.
- NFC jest mocno promowane przez dostawców usług, operatorów sieci komórkowych i banki.
- NFC ma potencjalnie duży rynek finansowy, co jest kuszące dla hakerów.

1.7.2 Główne cele środków bezpieczeństwa

Wymagania bezpieczeństwa każdego systemu są różne; różne są też ich priorytety. Niektóre priorytetowo traktują udostępnianie informacji tylko jednej lub kilku osobom, podczas gdy inne wymagają zachowania niezmienionej zawartości danych aplikacji przez nielegalne strony.

Najczęstsze wymagania bezpieczeństwa można wymienić w następujący sposób:

- Tajność zapewnia, że informacje są dostępne tylko dla osób z autoryzowanym dostępem.
- Uwierzytelnianie zatwierdza tożsamość osoby, procesu lub urządzenia na podstawie dostarczonych danych informacji.
- Autoryzacja pozwala na różne działania na obiekcie (pliku, aplikacji lub maszynie) przez podmiot (użytkownika) po uwierzytelnieniu.
- Brak zaprzeczenia strony uniemożliwia nadawcy zaprzeczenie wysłania wiadomości do strony odbiornika, aby sędzia mógł udowodnić sprawę.
- Dostępność zapewnia, że system poprawnie i w pełni odpowiada na żądania użytkowników autoryzowanych użytkowników w danym momencie.

- Integralność danych zapewnia, że otrzymane informacje są dokładnie takie same jak wysłane, a tym samym potwierdza, że nie zostały przypadkowo lub złośliwie zmodyfikowane, zmienione lub zniszczone.
- Odpowiedzialność gwarantuje prześledzenie wszystkich działań wraz z aktorem, który je wykonał.
wykonuje.

1.7.3 Podatność, zagrożenie, atak i ryzyko

Aby złośliwe działanie mogło spowodować uszkodzenie zabezpieczonego systemu, początkowo system powinien być podatny na ataki. W tym sensie podatność jest słabością systemu, która pozwala atakującemu na wykonanie pewnych działań zagrażających bezpieczeństwu informacji.

Zagrożenie to potencjalne niebezpieczeństwo, które może przynieść nieuczciwą korzyść nieautoryzowanemu użytkownikowi lub wyrządzić szkodę, wykorzystując lukę w zabezpieczeniach.

Celowa próba wykonania nieautoryzowanego dostępu do informacji przez intruzów nazywana jest atakiem.

Ataki są klasyfikowane jako aktywne lub pasywne. Jeśli atak nie modyfikuje ani nie usuwa zasobu, jest klasyfikowany jako pasywny, w przeciwnym razie jest klasyfikowany jako atak aktywny.

Potencjalna szkoda, która może powstać po zrealizowaniu jakiegoś zagrożenia, jest dalej definiowana jako ryzyko.

1.7.4 Narzędzia i mechanizmy bezpieczeństwa

Aby spełnić wymagania bezpieczeństwa, kryptografia jest najczęściej stosowaną techniką. Większość mechanizmów bezpieczeństwa opiera się na kryptografii. Kryptografia jest wykorzystywana do zapewnienia bezpiecznego kanału, przechowywania informacji o hasłach na dysku twardym, cyfrowego podpisywania transakcji finansowych itp.

Kryptografia jest również wykorzystywana do wielu celów, takich jak ukrywanie treści danych przed nieautoryzowaną stroną trzecią lub zapobieganie nielegalnej modyfikacji niektórych przesyłanych danych. Poniżej przedstawiono podstawowe usługi świadczone przez kryptografię:

- Przechowywane lub wymieniane informacje nie są ujawniane nieupoważnionym stronom.
- Zawartość przechowywanych lub wymienianych danych nie może zostać zmieniona przez osoby nieupoważnione, lub zostanie to zauważone, jeśli wystąpi.
- Gdy dane są tworzone lub wysyłane przez jakąś stronę, strona ta nie może zaprzeczyć tworzeniu lub wysyłaniu danych.
oni.

W kryptografii oryginalne dane (tekst jawnny) są początkowo szyfrowane przy użyciu klucza szyfrującego w celu utworzenia zmodyfikowanej formy tekstu jawnego, zwanej szyfrogramem. Dane mogą być po prostu przechowywane lub przesyłane do odbiorcy. Odbiorca odszyfrowuje dane za pomocą klucza deszyfrującego w celu odtworzenia oryginalnej wiadomości.

Idea zapewnienia tajemnicy przy użyciu kryptografii polega na możliwości wysłania wiadomości w zakodowanej formie zwanej szyfrogramem, tak aby komunikacja między nadawcą a odbiorcą była nadal możliwa i mogła być wykonywana przy użyciu kanałów publicznych, takich jak Internet.

1.7.5 Bezpieczeństwo NFC

Podobnie jak w przypadku wszystkich systemów informatycznych, systemy oparte na NFC są narażone na ataki, które zagrażają bezpieczeństwu systemu i prywatności użytkownika. Każdy tryb pracy NFC ma inną architekturę. W związku z tym ataki i mechanizmy obronne zależą głównie od różnych przypadków użycia. Kiedy systemy oparte na NFC są analizowane z punktu widzenia bezpieczeństwa, powinniśmy osobno rozważyć kwestie bezpieczeństwa związane z tagiem NFC, czytnikiem NFC, kartą inteligentną, komunikacją i systemami zaplecza.

1.7.5.1 Kwestie bezpieczeństwa tagów NFC

Należy pamiętać, że tag NFC działa w trybie czytnika/zapisu. W tym trybie tradycyjnie urządzenie mobilne NFC wchodzi w interakcję z tagiem NFC. Aby spełnić ogólne wymagania bezpieczeństwa, należy zabezpieczyć bezpieczeństwo danych na tagu NFC, a także bezpieczeństwo komunikacji między urządzeniami NFC. Pamiętając, że tag NFC jest w rzeczywistości tagiem RFID, możemy wykorzystać wiedzę zgromadzoną przy użyciu tagów RFID do obsługi bezpieczeństwa tego samego tagu w NFC. Tradycyjnie, poniżej przedstawiono kwestie bezpieczeństwa związane z NFC lub tagiem RFID:

(i) *Klonowanie znaczników*

Atakujący może próbować sklonować lub stworzyć dokładną kopię ważnego tagu. Aby wprowadzić mechanizmy zapobiegawcze do systemu, w y m a g a n e są aplikacje wymagające dużej mocy obliczeniowej, co zwiększa koszt tanich tagów. Oczywiście jest to niewykonalne i niedopuszczalne, ponieważ głównym celem jest umożliwienie korzystania z tanich tagów NFC.

(ii) *Zmiany zawartości tagów*

Atakujący może próbować zmodyfikować tag NFC, aby zmienić jego zawartość. W ten sposób możliwe staje się przeprowadzenie kilku ataków:

- Ataki typu spoofing

Atak spoofingowy polega na dostarczeniu użytkownikowi fałszywych informacji, które wydają się ważne, a zatem prawdopodobnie zostaną zaakceptowane przez użytkownika. W wyniku ataku spoofingowego użytkownik może wprowadzić do tagu fałszywą nazwę domeny, numer telefonu lub fałszywe informacje dotyczące identyfikacji jakiejś osoby, przedmiotu lub działania.

- Manipulowanie danymi znaczników

Zawartość tagu może zostać zmieniona przez atakującego w złośliwym celu.

- Atak typu odmowa usługi (DOS).

Ataki DoS mają na celu zniszczenie relacji między klientem a dostawcą usług. Głównym sposobem na osiągnięcie tego celu jest wyczerpanie zasobów systemu poprzez zmuszenie go do wykonania niepotrzebnych i nielegalnych działań. Powoduje to zmniejszenie i ostatecznie wyczerpanie źródła zasilania serwera.

(iii) *Zastępowanie i ukrywanie tagów*

Tag NFC może zostać zastąpiony złośliwym tagiem, tak aby ten ostatni wykonywał nielegalne działania zgodnie ze swoim przeznaczeniem. Umieszczenie złośliwego tagu na oryginalnym tagu lub zastąpienie oryginalnego tagu złośliwym tagiem nazywane jest ukrywaniem tagu i wystarczy, aby system działał zgodnie z życzeniem atakującego.

1.7.5.2 Problemy z bezpieczeństwem czytnika NFC

Należy pamiętać, że tryb emulacji karty obejmuje interakcję telefonu komórkowego z czytnikiem NFC. W związku z tym w tym trybie chodzi o bezpieczeństwo czytnika. Czytnik NFC jest podobny do czytnika RFID; dlatego obawy dotyczące bezpieczeństwa są podobne. Tego rodzaju podobieństwa są ważne i uspokajające, ponieważ potencjalne problemy zostały do tej pory w większości rozwiązane.

1.7.5.3 Kwestie bezpieczeństwa kart inteligentnych

Karty inteligentne w telefonie komórkowym są najczęściej używane przez aplikacje działające w trybie emulacji karty w ekosystemie NFC. W związku z tym bezpieczeństwo karty inteligentnej jest głównym problemem w tym trybie. Ataki na karty inteligentne można podzielić na dwie grupy: ataki inwazyjne i ataki typu side channel.

1.7.5.4 Kwestie bezpieczeństwa komunikacji

We wszystkich trybach pracy technologii NFC oczywiste jest, że wykorzystywana jest komunikacja krótkiego zasięgu. Atakujący z ulepszonymi urządzeniami radiowymi mogą komunikować się z bezstykowymi kartami inteligentnymi w promieniu kilku metrów. Dlatego ataki i zagrożenia podczas komunikacji są ważne we wszystkich trybach.

- *Podsłuchiwanie:* Nieupoważniona osoba może użyć anteny w celu zarejestrowania komunikacji między urządzeniami NFC.
- *Uszkodzenie danych:* Oprócz podsłuchiwania, atakujący może próbować modyfikować przesypane dane.
- *Modyfikacja danych:* Atakujący może próbować zmodyfikować lub usunąć cenne informacje poprzez inter- z wyjątkiem komunikacji.
- *Wstawianie danych:* Dane mogą być wstawiane do wiadomości wymienianych między dwoma urządzeniami NFC urządzenia. Atakujący musi być wystarczająco szybki, aby wysłać dane przed prawidłową odpowiedzią. Wstawienie danych powiedzie się tylko wtedy, gdy wstawione dane mogą zostać przesłane przed odpowiedzią oryginalnego urządzenia. Jeśli oba strumienie danych nalożą się na siebie, dane zostaną uszkodzone.
- *Atak Man-in-the-Middle:* Ataki te są przeprowadzane przez nieznane strony w sieci komunikacyjnej.
 - którzy przekazują informacje tam i z powrotem, sprawiając jednocześnie wrażenie, że są drugą stroną.
 - *Atak przekaźnikowy:* Atakujący wykorzystuje komunikację bezprzewodową, aby pożyczyć dane od ofiary.
 - do innego tagu. Oznacza to, że atakujący wstawia wiadomości do danych wymienianych między dwoma urządzeniami.
 - *Atak powtórkowy:* Prawidłowy sygnał NFC jest przechwytywany, a jego dane są najpierw rejestrowane; jest to później przesyłane do czytnika w celu ich "odtworzenia". Ponieważ dane wydają się prawidłowe, czytnik akceptuje je, chyba że zastosowano odpowiednie mechanizmy zapobiegawcze.

1.7.5.5 Bezpieczeństwo oprogramowania pośredniczącego i systemu zaplecza

System oparty na NFC zawiera czytniki NFC, telefony komórkowe NFC i tagi NFC w kategoriach technicznych. Kompletny system NFC obejmuje serwery do przechowywania danych i zarządzania nimi, takie jak serwery bankowe, kredytowe i inne.

oprogramowanie pośredniczące kart, podsystemy uwierzytelniania itd. W związku z tym bezpieczeństwo systemu NFC nie jest kompletne, jeśli nie zostanie zapewnione bezpieczeństwo wszystkich komponentów systemu. Kwestie bezpieczeństwa oprogramowania pośredniczącego i systemów zaplecza nie wchodzą w zakres tej książki. Jednak czytelnik powinien być świadomy faktu, że oprogramowanie pośredniczące i systemy zaplecza powinny być bezpieczne.

1.7.5.6 Znormalizowane protokoly bezpieczeństwa NFC

Wszystkie protokoły bezpieczeństwa związane z NFC są standaryzowane w ECMA 385 jako NFC-SEC i w ECMA 386 jako NFC-SEC-01. Protokoły te dotyczą kwestii bezpieczeństwa NFCIP-1, ponieważ NFCIP-1 nie zapewnia żadnych zabezpieczeń. NFC-SEC zapewnia standard bezpieczeństwa dla komunikacji peer-to-peer NFC. Oprócz NFCIP-1, NFC-SEC jest promowany w celu dodania funkcji bezpieczeństwa.

1.7.6 Prywatność, aspekty prawne i etyczne

Informacje, które są dobrowolnie udostępniane, ale później są kradzione lub niewłaściwie wykorzystywane, są obecnie ważną kwestią. Prywatność wymaga odpowiedniego wykorzystania informacji. Kiedy coś jest prywatne dla danej osoby, zwykle oznacza to, że jest to uważane za z natury i osobiste wyjątkowe. Prywatność jest szersza niż bezpieczeństwo i obejmuje koncepcje odpowiedniego wykorzystania i ochrony informacji.

Kilka dekad temu uważano, że jest to era informacji. Obecnie uważa się, że jest to era zarządzania informacjami. Powód tej różnicy jest oczywisty: dane i informacje są wszędzie. Ważniejsze jest pozyskiwanie użytecznych informacji niż ich tworzenie.

Ogromna ilość danych jest generowana w różny sposób na całym świecie. Dane są gromadzone na całym świecie za pomocą czujników, aplikacji i innych urządzeń zbierających dane. Bezprzewodowe węzły czujników i kamery to dwa przykłady urządzeń zbierających dane. Kiedy dzwonisz do kogoś lub nawet nosisz telefon komórkowy bez celowego korzystania z niego, kupujesz coś nawet za gotówkę lub klikasz na stronę internetową w przeglądarce, wiele danych jest rejestrowanych. Dlatego generowanie danych nie jest już problemem. Problemem jest to, jak te dane wykorzystać.

Prawdę jest, że ludzie nie lubią być nagrywani, gdy wchodzą do budynku, idą drogą, spotykają się z przyjaciółmi w kawiarni itp. Niefortunne jest to, że trend ten nie ulegnie zmianie, nawet jeśli można go tymczasowo spowolnić. Jeszcze bardziej irytujące jest to, że przechwycone dane są wykorzystywane do działań naruszających prywatność użytkowników.

Zasady muszą zostać zmienione na całym świecie, ponieważ obecnie tak łatwo jest wykorzystywać informacje zebrane o ludziach nawet bez ich zgody.

1.7.6.1 Co zrobić, aby chronić prywatność

Prawdę jest, że komunikacja bezprzewodowa podlega większej liczbie zagrożeń bezpieczeństwa w porównaniu z medianami przewodowymi. Prawdę jest również, że urządzenia mobilne mają niższą zdolność przetwarzania ze względu na wyższy koszt sprzętu, co skutkuje podatnością na wykonywanie usług zaimplementowanych w celu budowania środków bezpieczeństwa.

Innym faktem jest to, że firmy tradycyjnie dbały o bezpieczeństwo produktów znacznie

mniej niż o ich funkcjonalność. Dlatego początkowo ludzie byli zazębiańi, gdy kupowali nowe aplikacje,

Ale potem napotkali szkody, ponieważ luki w zabezpieczeniach zostały nadużyte przez złośliwe działania. W związku z tym znacznie wzrosła podejrzliwość opinii publicznej wobec nowej technologii.

Ponieważ opinia publiczna stała się bardziej podejrzliwa wobec systemów mobilnych i bezprzewodowych, RFID również spotkał się z publicznym sprzeciwem. Dlatego też RFID z czasem spotkało się ze strachem i odrzuceniem.

W przypadku RFID klienci skarzyli się, że nie zostali poinformowani przez firmy o tym, że wbudowały one znaczniki RFID w swoje produkty. Nawet jeśli zostali poinformowani, nie powiedziano im o wszystkich zagrożeniach. Dlatego też ludzie byli wściekli, gdy w końcu poznali fakty. Możliwy jest wyciek poufnych danych znajdujących się na tagu, zwłaszcza jeśli dana osoba nie jest świadoma istnienia tagu.

Ponieważ NFC jest dopiero rozwijającą się technologią, gromadzenie, przechowywanie i wykorzystywanie wrażliwych danych prywatnych jest również przedmiotem publicznego zainteresowania. Cenne dane prywatne, takie jak informacje o kartach płatniczych i dane osobowe, są zagrożone, jeśli nie zostaną podjęte odpowiednie środki.

Aby uspokoić obawy opinii publicznej, należy przekazać potencjalnym klientom szczegółowe informacje, a także wszystkie zagrożenia, a także zastosować odpowiednie środki bezpieczeństwa. Aby osiągnąć zaufanie użytkowników, istnieje wyraźna potrzeba skutecznych narzędzi, które wspierają użytkowników w ochronie ich prywatności. Wymagane może być również wspieranie przepisów dotyczących ochrony danych, innych pomiarów prawnych i mechanizmów audytu. W ten sposób użytkownicy aplikacji NFC mogą być przekonani, że aplikacje te nie będą nadużywać ich danych osobowych i prywatności.

1.8 Ekosystem biznesowy NFC

Do tej pory wprowadzono wiele ulepszeń technologicznych. Niektóre historyczne przykłady obejmują odbiorniki radiowe, telewizory, kanały telewizji kablowej, kanały telewizji satelitarnej, telefony, telefony komórkowe i telefony satelitarne. Niektóre z tych technologii zostały z powodzeniem zaakceptowane, podczas gdy inne po prostu zniknęły. Istnieją różne powody akceptacji lub odrzucenia takich technologii. Podstawowym wymogiem szerokiego zastosowania takiej technologii jest oczywiście sukces techniczny. Bez wystarczającego poziomu technicznego żadne urządzenie techniczne nie może być używane.

Kolejnym czynnikiem wpływającym na sukces technologii jest akceptacja społeczna. Jeśli ludzie uznają ją za wystarczająco użyteczną, są skłonni za nią zapłacić. Gdy więcej osób płaci za urządzenia, firmy uzyskują większy dochód i zapewniają dalsze inwestycje w celu ulepszenia technologii. W miarę ulepszania technologii cena jednostkowa jest obniżana, co sprawia, że więcej osób chce posiadać urządzenie. Cykl ten prowadzi cenę produktu do rozsądnego poziomu, dzięki czemu nowa technologia ostatecznie odnosi sukces.

Jak widać z ostatniego akapitu, dominujący czynnik sukcesu modelu jest w rzeczywistości bardziej finansowy niż technologiczny. Motywacje ekonomiczne umożliwiają osiągnięcie wystarczalności technicznej przez pewien czas. Przeanalizowaliśmy już zaangażowanie użytkownika w ten proces. Z perspektywy inwestora zwrot z inwestycji (RoI) jest główną motywacją firm. Firmy zawsze żądają krótkich ram czasowych, w których mogą odzyskać swoje pieniądze.

Prawdą jest, że w przypadku korzystania z dowolnego urządzenia technologicznego zaangażowanych jest więcej niż jedna firma. Weźmy na przykład transmisję telewizyjną. Istnieją producenci, firmy kablowe, firmy reklamowe, firmy infrastrukturalne i wiele innych. Każda firma stara się zmaksymalizować swój zysk, zmniejszając w ten sposób swój

RoI tak bardzo, jak to możliwe. Możemy zilustrować aspekt finansowy za pomocą tortu. Rozmiar tortu zależy od liczby użytkowników, którzy są skłonni zapłacić za produkty i usługi. Następnie określany jest udział każdej firmy. Każda firma stara się uzyskać jak najwięcej. Jeśli wynikowa konfiguracja podziału jest zdrowa, wówczas system

działa. W przeciwnieństwie do tego, jeśli jakakolwiek duża firma nie może otrzymać wystarczającej ilości pieniędzy, jej RoI zbytnio wzrasta, a zatem firma ta nie inwestuje żadnych pieniędzy. Ponownie posłużymy się przykładem telewizora. Jeśli producent telewizorów próbuje uzyskać większość pieniędzy poprzez zwiększenie kosztów telewizorów, ludzie przestaną kupować telewizory, a zatem nikt nie wygra. Inną alternatywą jest to, że jeśli dostawca usług kanałowych zażąda zbyt dużo pieniędzy, ludzie przestaną kupować telewizory, ponieważ nie będą już chcieli z nich korzystać. W związku z tym dobre porozumienie w sprawie tego, kto co otrzyma i w jaki sposób, definiuje sukces wyniku.

Nie inaczej jest w przypadku technologii NFC. Historia sukcesu zostanie napisana dopiero wtedy, gdy gracze uzgodnią sposób podziału zysków, który nie został jeszcze ustalony.

Prawdą jest, że ekosystem NFC zapewnia zachęcający udział finansowy wszystkim powiązanym partnerom. NFC tworzy nowe środowisko biznesowe i duży łańcuch wartości. Udziały finansowe zaostrajają apetyt wielu firm.

Potencjał technologii NFC w zakresie możliwości biznesowych (zwłaszcza w branży mobilnych usług finansowych) wywołał ogromne podekscytowanie w wielu organizacjach. Ponieważ technologia NFC składa się z kilku komponentów, przekracza granice wielu organizacji z różnych sektorów biznesowych.

Wiodące firmy, które mogą być entuzjastycznie nastawione do powstającego ekosystemu, to operatorzy sieci komórkowych, usługi bankowe i płatnicze, producenci produktów, w tym producenci telefonów komórkowych, twórcy oprogramowania i inni sprzedawcy, w tym operatorzy transportu i sprzedawcy detaliczni.

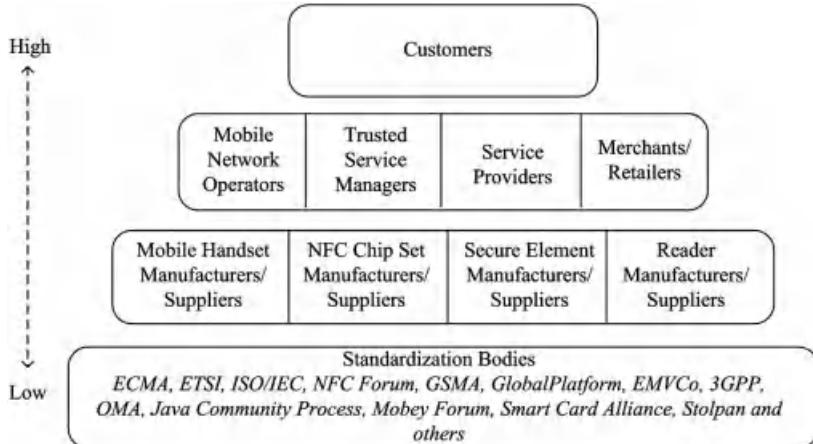
Niektóre firmy na całym świecie starają się czerpać wszelkie możliwe zyski z ekosystemu NFC. Na przykład niektórzy operatorzy MNO próbują ominąć banki, aby uzyskać całą wartość dodaną. To samo dotyczy niektórych banków. Niektórzy producenci telefonów komórkowych próbują stworzyć odpowiednie modele, aby nie potrzebować żadnych MNO ani banków do ułatwiania usług NFC. Jest to jednak dość rozczarowujące. Firmy powinny zrozumieć, że żadna pojedyncza firma nie może uzyskać całego zysku. Pieniądze do podziału można zwiększyć tylko wtedy, gdy wszystkie powiązane sektory uzgodnią model podziału, który zadowoli wszystkie firmy. W przeciwnym razie pieniądze do podziału będą tylko niewielką kwotą.

Start NFC był wolniejszy niż oczekiwano. Powód tego nie jest techniczny. Najważniejszym powodem jest brak wspólnego zrozumienia i wizji technologii NFC wśród uczestniczących organizacji i branż. W związku z tym nie udało się jeszcze stworzyć wzajemnie korzystnego modelu biznesowego. Głównymi przyczynami braku wspólnego zrozumienia i wizji są:

- Zysk, który zostanie podzielony, jest ogromny. Dlatego każda firma chce mieć w nim duży udział.
- Wszystkie strony są potężnymi firmami, więc zakładają, że inne strony są zobowiązane do podążać za ich żądaniemi.
- Różne rozwiązania techniczne i infrastruktury dla konkretnej usługi obsługującej NFC to. Ponieważ każda ze stron proponuje model, który przynosi jej więcej korzyści niż innym. Na przykład operatorzy sieci komórkowych proponują modele oparte na kartach SIM, ponieważ mogą kontrolować karty SIM, a zatem mogą uzyskać większy zysk, jeśli ten model zostanie zastosowany. Nikt nie próbuje znaleźć rozwiązań, które mogłyby uszczęśliwić wszystkie strony.

Aby osiągnąć uczciwy, a jednocześnie rentowny model biznesowy, niezbędna jest

interoperacyjność, kompatybilność i standaryzacja uzgodnionego modelu technologii NFC.
Ważne jest również uzyskanie akceptacji klientów.



Rysunek 1.1 Interesariusze w ekosystemie NFC.

1.8.1 Interesariusze w ekosystemie NFC

W każdy projekt NFC potencjalnie zaangażowanych jest wielu interesariuszy, w zależności od rodzaju świadczonych usług. Niektóre z potencjalnie wiodących usług to inteligentne plakaty, płatności, sprzedaż biletów i przetwarzanie mediów społecznościowych. Rodzaj używanej usługi definiuje potencjalnych graczy, szczegóły dotyczące potrzeby współpracy między tymi graczami, pieniądze do podziału i tak dalej.

Jak pokazano na rysunku 1.1, możemy zbadać podmioty uczestniczące w ekosystemie NFC na czterech poziomach. Na najniższym poziomie istnieją organy normalizacyjne, których celem jest opracowanie globalnych, interoperacyjnych standardów dla NFC i zależnych od niej technologii, takich jak karty inteligentne i telefony komórkowe. Poziom ten może być postrzegany jako podstawowy dla technologii NFC i jej ekosystemu. Kolejny poziom obejmuje producentów i dostawców sprzętu (tj. telefonów komórkowych, zestawów chipów NFC, SE, czytników NFC). Są oni odpowiedzialni za produkcję i sprzedaż produktów zgodnych ze standardami umożliwiającymi korzystanie z systemów opartych na NFC. Weźmy na przykład pod uwagę producentów i dostawców SE. Muszą oni dostarczać odpowiednie SE odpowiednim klientom. Wbudowany sprzęt i bezpieczne karty pamięci oparte na SE muszą być produkowane dla producentów telefonów komórkowych lub innych sprzedawców detalicznych, a SE oparte na UICC dla MNO. Producenci i dostawcy UICC są zakontraktowani i zmuszeni do dostarczania wymaganego sprzętu UICC do MNO. W ten sposób mają bezpośredni związek z MNO, który również definiuje wymagania dla UICC i wydaje SE.

Główni gracze istnieją na kolejnym poziomie. Są to podmioty, które realizują aplikacje i usługi NFC w bezpiecznym, zaufanym środowisku. Można je opisać w następujący sposób:

- Operatorzy MNO tradycyjnie zapewniają właścicielom telefonów komórkowych dostęp do sieci komunikacyjnej i danych. W rzeczywistości są oni obecnie odpowiedzialni za - a nawet mają przywilej - dostarczania wszelkiego rodzaju usług mobilnych swoim abonentom. W międzyczasie MNO mogą dostarczać i utrzymywać infrastrukturę sieciową, która umożliwia bezpieczne rozwiązania OTA w celu zapewnienia zdalnego zarządzania i konserwacji aplikacji przechowywanych na SE.

- TSM jest wymagany do tworzenia i zarządzania zaufanym środowiskiem wśród podmiotów ekosystemu NFC. TSM generalnie oferuje pojedynczy punkt kontaktu z MNO dla dostawców usług, takich jak instytucje finansowe, banki, władze tranzytowe, sprzedawcy detaliczni i inni, którzy chcą dostarczać płatności, bilety lub aplikacje lojalnościowe klientom z telefonami komórkowymi obsługującymi NFC.
- Dostawca usług wdraża i zarządza usługą na urządzeniach mobilnych swoich klientów. Klienci. Dostawcą usług może być instytucja finansowa, bank, organ transportowy lub inna organizacja.
- W kontekście ekosystemu NFC kupcy i sprzedawcy detaliczni są interesariuszami, którzy akceptują usługi zbliżeniowych płatności mobilnych.

Podmioty te mają bezpośrednie relacje z użytkownikami końcowymi jako klientami na najwyższym poziomie. Klienci są zawsze głównymi interesariuszami w każdej firmie i są w centrum uwagi dostawców usług; powód tego jest oczywisty. Klienci będą utrzymywać firmę tylko wtedy, gdy ich potrzeby zostaną zaspokojone. Wszystkie działania marketingowe zawsze koncentrują się na nich.

Jak już wspomniano, od 2005 r. na całym świecie wdrożono kilka testów NFC; a operatorzy, banki i emitenci SE mają ambicję zwiększenia swoich przychodów dzięki usługom NFC. Zwłaszcza w branży europejskiej banki i operatorzy sieci komórkowych konkurują ze sobą, dlatego można zaobserwować różne modele biznesowe i podejścia do włączania usług NFC. Na przykład w Austrii niektórzy operatorzy sieci komórkowych uzyskali licencje bankowe, dzięki czemu mogą świadczyć usługi finansowe i bankowe. Model wirtualnego operatora sieci komórkowej (MVNO) zyskał popularność w ostatnich latach. Operatorzy MVNO pozwalają operatorom MNO i firmom nietelekomunikacyjnym uczestniczyć w usługach mobilnych. Na przykład w Holandii bank o nazwie Rabobank zaczął działać jako MVNO, współpracując z MNO w celu świadczenia usług mobilnych z usługami finansowymi dla swoich klientów. Taki model MVNO tworzy model korzystny dla obu stron dzięki współpracy z MNO; model ten szybko rozwija się w krajach takich jak Hiszpania, Włochy i Portugalia, a ostatnio także w Turcji. MVNO mogą zwiększyć świadomość swojej marki, kanały dystrybucji i bazę klientów, aby zapewnić swoim klientom usługi o wartości dodanej. Z drugiej strony, MNO mogą zwiększyć przepustowość swojej sieci, infrastrukturę IT i portfolio usług, dodać nowy strumień przychodów i tak dalej.

1.8.2 Zrozumienie modeli biznesowych NFC

W modelach biznesowych NFC problemy, które należy rozwiązać, są głównie związane z biznesem, a nie z technologią lub infrastrukturą. Modele biznesowe są ważne, aby zapewnić wartość wszystkim zainteresowanym stronom. Niektóre modele biznesowe nie zachęcają do silnej współpracy między wszystkimi organami; jednak w NFC jest to koniecznością.

Obecnie istnieje wszechobecna niepewność co do tego, który model biznesowy jest najlepszy; która firma wykona dokładnie jaką działalność i kto zapłaci komu za jaką usługę, a ostatecznie ile zysku zostanie zarobione lub podzielone przez któregokolwiek z interesariuszy. Ze względu na nowatorstwo technologii NFC, nadal nie ma porozumienia ani wspólnej wizji modelu biznesowego, który w wystarczającym stopniu zadowalałby wszystkich interesariuszy. W rzeczywistości opublikowano wiele propozycji i specyfikacji modeli biznesowych, a różne projekty są wdrażane w ramach ogromnej liczby testów na całym świecie, zwłaszcza w zakresie mobilnych usług finansowych ze względu na wysoki stopień złożoności ekosystemu i infrastruktury technologicznej. NFC Forum,

GSMA i EMVCo to niektóre z ważnych stowarzyszeń, które intensywnie pracują nad ekosystemem NFC i modelami biznesowymi, a także nad podstawową infrastrukturą technologiczną. Podsumowując, konieczne jest zharmonizowanie interesów wszystkich uczestników w tworzeniu zrównoważonych modeli biznesowych. W przeciwnym razie powstaną sprzeczne, niewykonalne i nieinteroperacyjne rozwiązania. a tym samym technologia nie będzie mogła zostać ulepszona.

Istnieje kilka kluczowych pytań, które pomagają nam zrozumieć środowisko biznesowe aplikacji i usług obsługujących NFC. Pytania te są następujące:

- Kto będzie emitował i posiadał kontrolę nad SE?
- Kto będzie zarządzał cyklem życia platformy SE?
- Czyja platforma OTA będzie używana do zarządzania platformą SE?

W odniesieniu do tych pytań zidentyfikowaliśmy trzy główne kwestie, które określają alternatywne modele biznesowe dla NFC: emitent SE, menedżer platformy i dostawca OTA. Kwestie te można również określić jako funkcjonalne role i obowiązki, które muszą być obsługiwane przez pojedynczy podmiot lub wiele podmiotów w modelu biznesowym NFC.

(i) *SE Emittent*

Emitent SE to podmiot, który emittuje i jest właścicielem SE. Obecnie w prawie wszystkich przypadkach OSK lub dostawcy usług (np. banki) pełnią jednocześnie rolę emitenta SE. W idealnym przypadku emitent SE powinien być niezależnym podmiotem, ale obecnie tak nie jest. Jeśli SE oparty na UICC jest używany w modelu biznesowym, MNO ponosi odpowiedzialność za wystawcę SE, ponieważ SE jest przekazywany użytkownikowi, gdy dostarczana jest karta SIM zawierająca SE. W przypadku korzystania z SE opartego na sprzęcie wbudowanym, rolę tę pełni podmiot, który przekazuje użytkownikowi telefon komórkowy. Jeśli telefon komórkowy jest przekazywany aktualnemu klientowi operatora sieci komórkowej, na przykład w kontekście kampanii, to operator sieci komórkowej jest wydawcą karty. Jeśli telefon komórkowy został zakupiony przez użytkownika od sprzedawcy detalicznego lub dostawcy usług, wystawcą karty może być teoretycznie każdy niezależny partner, taki jak sprzedawca detaliczny, dostawca usług lub inny.

(ii) *Menedżer platformy*

Drugą ważną kwestią jest kontrola i zarządzanie platformą SE. Menedżer platformy jest właścicielem kluczy kryptograficznych, które są używane do kontrolowania SE w jego cyklu życia. Menedżer platformy umożliwia autoryzowanym dostawcom usług instalowanie aplikacji na SE, najlepiej przy użyciu infrastruktury OTA.

Model biznesowy jest prostszy, gdy emitent SE i menedżer platformy są tym samym podmiotem. Inną opcją jest powierzenie roli menedżera platformy podmiotowi innemu niż emitent SE. Podmiotem tym może być TSM jako niezależna, neutralna strona. Aby zrealizować tę opcję, TSM i emitent SE muszą wcześniej uzgodnić model biznesowy. Umowa może obejmować szczegóły od infrastruktury technicznej po podział przychodów. TSM może obsługiwać wszystkie funkcje zarządzania SE za pomocą własnej platformy OTA lub łącza OTA MNO, co jest trzecią ważną kwestią omówioną poniżej.

(iii) *Dostawca OTA*

Ostatnią ważną kwestią jest zapewnienie platformy OTA. Zapewnienie elastycznego i interoperacyjnego rozwiązania OTA jest kluczowym wymogiem w ekosystemie NFC. Umożliwia bezpieczną komunikację bezprzewodową między dwiema stronami

końcowymi oraz zapewnia transmisję i odbiór informacji związanych z aplikacją w systemie komunikacji bezprzewodowej. OTA

umożliwia zdalne pobieranie, instalację i zarządzanie aplikacjami, takimi jak aktualizacja, aktywacja lub dezaktywacja aplikacji przechowywanej w SE.

1.8.3 Podejścia do modelu biznesowego

Obecnie dostępne modele biznesowe to warianty skoncentrowane na MNO, rozproszone i skoncentrowane na TSM:

(i) Model biznesowy zorientowany na MNO

W modelu biznesowym skoncentrowanym na MNO, MNO wydaje SE i działa jednocześnie jako wydawca SE, menedżer platformy i dostawca OTA. Nie ma innego niezależnego zaufanego podmiotu; MNO wykonuje wszystkie funkcje TSM, jest właścicielem i zarządza cyklem życia SE przy użyciu własnej platformy OTA. OSK wykonuje również procesy ładowania, instalacji i personalizacji, a także tworzenia domen bezpieczeństwa w SE. Dostawcy usług muszą płacić OSK, aby ich aplikacje mogły działać na SE, a nawet udostępniać OSK swoje dane personalizacyjne.

(ii) Rozproszony model biznesowy

W rozproszonym modelu biznesowym usługi zarządzania platformą są dystrybuowane między emitentem SE a dostawcą usług. Może istnieć oddzielna infrastruktura TSM, a brak infrastruktury jest również inną opcją. W rzeczywistości wybór zależy od możliwości TSM podmiotu. Jeśli dostawca usług nie ma możliwości TSM, musi zawrzeć umowę z istniejącym TSM. Obecnie dostawcy usług wolą współpracować z zaufanymi stronami trzecimi niż dokonywać wysokich inwestycji w celu zbudowania infrastruktury OTA w swoich organizacjach.

(iii) Model biznesowy zorientowany na TSM

W przypadku usług NFC model biznesowy oparty na jednym TSM jest w rzeczywistości najlepszą opcją i jednocześnie mniej złożonym modelem biznesowym. Operatorzy MNO i dostawcy usług, którzy chcą uczestniczyć w tym konkretnym ekosystemie usług NFC, muszą podpisać umowę z istniejącym na rynku TSM. TSM pełni rolę menedżera platformy całkowicie w imieniu dostawców usług; odbywa się to poprzez realizację procesów ładowania, instalacji i personalizacji za pośrednictwem własnej platformy OTA. Liczba TSM może wzrosnąć w zależności od dostępnych usług i umów między podmiotami w ekosystemie NFC. Na przykład usługi płatnicze i transportowe z obsługą NFC mogą korzystać z tej samej platformy TSM, jak również z różnych platform TSM.

Aby stworzyć zrównoważony model, naprawdę ważne jest stworzenie modelu biznesowego korzystnego dla wszystkich zainteresowanych stron na rynku z wieloma dodatkowymi przychodami i możliwościami marketingowymi. Aby z powodzeniem rozwijać wszelkiego rodzaju modele biznesowe, niezbędne jest **zrozumienie wymagań biznesowych** wszystkich zainteresowanych stron, zwłaszcza operatorów sieci komórkowych i dostawców usług, oraz zbudowanie zaufania między nimi. Następnie można uzyskać bezpieczny i prosty ekosystem.

1.9 Użyteczność w NFC

Technologia NFC została uznana przez NFC Forum za łatwą w użyciu i prostą. Aby korzystać z NFC, wszystko co użytkownik musi zrobić, to trzymać urządzenia obsługujące NFC razem. W ten sposób użytkownicy mogą

dostęp do usług, nawiązywanie połączeń, dokonywanie płatności lub korzystanie z biletów [1]. Do tej pory tylko kilka badań przeprowadziło analizę użyteczności NFC w celu zmierzenia sukcesu prób. Poniżej podsumowujemy niektóre badania dotyczące użyteczności NFC.

W [2] zbadano subiektywną użyteczność głosowania w samorządzie studenckim i porównano ją ze scenariuszem głosowania internetowego. Głosowanie NFC uzyskało wyższą użyteczność niż głosowanie internetowe z wynikiem 82,75, podczas gdy głosowanie internetowe uzyskało wynik 78,50 na 100. Wyniki testu użyteczności wykazały, że technologia NFC ma potencjał do zwiększenia użyteczności systemów. W rezultacie pojawienie się telefonów komórkowych i usług kompatybilnych z NFC przyniesie nowe możliwości, które ułatwią nam życie. W kontekście głosowania, NFC zapewniło praktyczne i łatwe w użyciu środowisko.

W innym badaniu [3] przeprowadzono również testy użyteczności NFC w celu określenia, w jaki sposób systemy oparte na NFC mogą zostać wykorzystane do poprawy przepływu pracy i użyteczności rozwiązań mobilnych.

Badanie wykazało, że NFC może usprawnić mobilne przepływy pracy poprzez rozwiązywanie różnych powiązanych problemów. W przypadkach pilotażowych technologia NFC poradziła sobie z następującymi problemami:

- Dostęp do informacji, aplikacji i instrukcji w terenie w czasie rzeczywistym;
- Aktualizacja danych w czasie rzeczywistym;
- Usuwanie błędów ludzkich;
- Zmniejszenie obciążenia pamięci użytkowników;
- Tworzenie możliwości weryfikacji obecności osób w różnych lokalizacjach.

Badanie wykazało, że rozwiązania oparte na NFC są łatwe w użyciu, ale mała i ograniczona klawiatura urządzeń mobilnych powoduje trudności w projektowaniu modeli. Rozwiązania oparte na NFC powinny uwzględnić miejsce tagów, łatwość korzystania z aplikacji i ilość wprowadzanego tekstu. Badanie wykazało, że przyjazność dla użytkownika została wzięta pod uwagę w pilotażach, ale nie zawsze miała wpływ na wrażenia użytkownika.

Inne badanie dotyczące doświadczeń użytkowników i scenariuszy akceptacji aplikacji NFC [4] wykazało, że prosta technologia NFC musi pokonać alternatywne technologie pod względem doświadczenia użytkownika i kryteriów wydajności, zwłaszcza gdy obie technologie zapewniają prawie takie same funkcje dla użytkownika końcowego.

1.10 Korzyści z aplikacji NFC

Liczne aplikacje NFC są projektowane, prototypowane i rozwijane do tej pory. Dostawcy usług są chętni do oferowania usług opartych na NFC, jednak czasami nie decydują, którą usługę zaoferować. W badaniu [5] przeanalizowano większość aplikacji NFC w literaturze i podkreślono korzyści płynące z tych aplikacji z perspektywy użytkowników. Ponadto w badaniu przedstawiono możliwe przyszłe scenariusze użytkowania w oparciu o odkryte korzyści.

Badanie początkowo wykazało, że każdy tryb pracy zapewnia użytkownikom inne korzyści [5]. W związku z tym przeanalizowano aplikacje w oparciu o używany tryb pracy.

W trybie czytnika/zapisu dane przechowywane w tagu NFC są odczytywane przez telefon komórkowy z obsługą NFC, a następnie wykorzystywane do przetwarzania dalszych operacji. Przesypane dane mogą być dowolnym typem tekstu, takim jak adres internetowy, dane zdarzenia lub inne dane. Po operacji transferu dane mogą być wykorzystywane do wielu celów (np. do wyświetlania informacji na ekranie urządzenia mobilnego w podróży).

Ponadto, w oparciu o projekt aplikacji, tryb ten jest w stanie zapewnić mobilność i zasięgu.

zmnieszyć wysiłek fizyczny. Rosnąca moc obliczeniowa i bezprzewodowy dostęp do Internetu w urządzeniach mobilnych również pomogły w tej kwestii i uczyniły ten tryb bardziej atrakcyjnym. Na przykład pacjenci mogą przesyłać swoje informacje medyczne za pomocą technologii NFC z domu, a osoby starsze mogą zamawiać posiłki z domu. Klienci mogą robić zakupy z domu, dotykając swoimi urządzeniami mobilnymi tagów NFC umieszczonych na broszurach.

Powstaje znacznie więcej aplikacji wykorzystujących tryb czytnika/zapisu niż inne tryby. Najważniejszym powodem takiego rozwoju jest to, że istnieje tak wiele interesujących i łatwych do wdrożenia scenariuszy przypadków użycia, które można opracować w trybie czytnika/zapisu. Ponadto rozwój i wdrażanie aplikacji w trybie czytnika/zapisu jest stosunkowo łatwiejsze niż w przypadku innych trybów.

Tryb peer-to-peer jest rzadki w porównaniu z innymi trybami, które są badane głównie pod kątem parowania urządzeń, sieci społecznościowych i operacji przesyłania plików. Tryb peer-to-peer zapewnia łatwą wymianę danych między dwoma urządzeniami i umożliwia niektóre przypadki sieci społecznościowych (np. aktualizowanie informacji o obecności w sieciach społecznościowych).

W badaniu stwierdzono, że tryb emulacji karty dotyczy głównie eliminacji potrzeby posiadania fizycznego obiektu. Na przykład korzystanie z telefonu komórkowego eliminuje potrzebę noszenia przy sobie karty kredytowej, debetowej, a nawet gotówki. Zamiast tego użytkownik dokonuje płatności za pomocą telefonu komórkowego. Korzystanie z NFC eliminuje potrzebę noszenia fizycznego klucza i bezstykowego inteligentnego klucza. Ponieważ NFC może być używane do wchodzenia do pomieszczeń zamiast kluczy elektronicznych, zapewnia kontrolę dostępu. Co więcej, tryb emulacji karty jest używany podczas realizacji biletów i kuponów mobilnych. W rzeczywistości te dwa procesy pozwoliły również wyeliminować fizyczne obiekty (papierowe bilety, kupon itp.). Najważniejszymi cechami trybu emulacji karty są eliminacja fizycznych obiektów i zapewnienie kontroli dostępu. W badaniu stwierdzono również, że dostępne na rynku aplikacje są w większości opracowywane przy użyciu trybu emulacji kart.

1.10.1 Przyszłe scenariusze dotyczące NFC

Główne zalety trybu czytnika/zapisu to zwiększenie mobilności i zmniejszenie wysiłku fizycznego. Korzyści te są zgodne z właściwością mobilności telefonu komórkowego, która z kolei ogólnie zmniejsza wysiłek fizyczny. Na przykład dzwonienie do kogoś zapewnia mobilność i eliminuje potrzebę komunikowania się twarzą w twarz. Co więcej, wraz z wykorzystaniem usług mobilnych, aplikacje e-mail są opracowywane dla telefonów komórkowych i umożliwiają użytkownikom czytanie i pisanie wiadomości e-mail bez żadnych ograniczeń geograficznych. Badanie wykazało, że większość rzeczywistych scenariuszy można dostosować do aplikacji tego trybu. Projekty aplikacji powinny obejmować przesyłanie danych z tagu NFC do telefonu komórkowego i wyświetlanie ich użytkownikowi. Ponadto telefony komórkowe mogą wykonywać dodatkowe przetwarzanie przesyłanych danych (np. mogą przechowywać dane w telefonie komórkowym i przesyłać je do dowolnego serwera w Internecie).

Zauważono, że główną zaletą trybu peer-to-peer jest łatwa wymiana danych. Wymiana danych między dwoma urządzeniami NFC zapewnia możliwość bezpiecznego przesyłania krytycznych danych i interakcji społecznych. Ponieważ urządzenia NFC mogą przesyłać dane w odległości do 4 cm, wymiana krytycznych danych może być jednym z kluczowych przyszłych zastosowań tego trybu.

W [5] stwierdzono, że głównym celem trybu emulacji karty jest ścisłe powiązanie telefonu komórkowego z jego użytkownikami. Można to uznać za wyzwanie dla mobilności

telefonów komórkowych, jednak ludzie noszą telefony komórkowe ~~zasięgu~~ przez większość czasu i

Sprzężenie telefonów komórkowych z ludzkim ciałem faktycznie pasuje do korzystania z telefonów komórkowych. W niedalekiej przyszłości może pojawić się możliwość noszenia telefonów komórkowych z obsługą NFC nie tylko w celu uzyskania mobilności, ale także w celu wykonywania codziennych czynności. Karty kredytowe, klucze i bilety będą wbudowane w telefony komórkowe. W związku z tym pojawi się więcej możliwości integracji przedmiotów codziennego użytku z telefonami komórkowymi obsługującymi technologię NFC. Oprócz obecnych obszarów zastosowań, wiele przedmiotów, takich jak karty identyfikacyjne, paszporty, odciski palców i prawa jazdy, może być przechowywanych w telefonach komórkowych i wykorzystywanych dzięki NFC. W miarę jak telefon komórkowy staje się częścią codziennego życia człowieka, mogą pojawić się dodatkowe możliwości. Jedną z nich będzie wykorzystanie telefonów komórkowych z obsługą NFC jako obszaru pamięci dla danych użytkowników. Jednym z najbardziej konkretnych przykładów takiego zastosowania jest przechowywanie informacji o pacjencie użytkownika w telefonie komórkowym z obsługą NFC.

1.11 NFC na całym świecie

Do tej pory podjęto wiele prób wdrożenia technologii NFC. Niektóre modele są opracowywane przez uniwersytety, inne przez firmy, a jeszcze inne przez wspólne wysiłki uniwersytetów i firm. Wiele modeli jest tylko teoretycznych, niektóre nie mogą być używane z powodu brakujących funkcji, ale inne są w pełni rozwinięte.

Miasto NFC opisuje obszar, w którym używanych jest kilka aplikacji NFC. Celem miasta NFC może być testowanie implementacji lub nawet faktyczne korzystanie z niej. Miasta NFC są ważne dla doskonalenia technologii NFC, ponieważ są rzeczywistą areną umiarkowanej wielkości mediów użytkowych.

W testach i projektach NFC testowane są aplikacje i ekosystem NFC; dlatego kwestie użyteczności wraz z problemami technologii można uzyskać poprzez testy w początkowej fazie miast NFC. Technologia NFC, aplikacje i kwestie użyteczności mogą być testowane w tej fazie. Podczas okresu testowego jednym z celów jest ocena możliwości zastosowania technologii NFC. Nie jest to jednak jedyny powód tego wysiłku. Jednym z głównych celów jest przetestowanie kwestii związanych z ekosystemem NFC. Użyteczność ekosystemu NFC jest co najmniej tak samo ważna jak stosowność techniczna, ponieważ model nie może być używany, gdy nie ma zgody między zaangażowanymi podmiotami.

1.11.1 Miasta NFC

1.11.1.1 Miasto Oulu

Miasto Oulu zostało wykorzystane jako poligon doświadczalny dla projektu SmartTouch. Projekt trwał od 2006 do końca 2008 roku i badał rolę NFC w życiu miasta, domu, dobrobycie i zdrowiu, rozrywce, technologii i biznesie. Obywatele mieszkający w Oulu mieli okazję przetestować komercyjne i publiczne usługi NFC jako pierwi użytkownicy technologii w szerokim aspekcie. Główne aplikacje, które zostały przetestowane to:

- Zamawianie posiłków dla osób starszych;
- Proces frekwencji uczniów w szkole średniej;
- Proces frekwencji w szkole podstawowej z wykorzystaniem NFC;
- Miejskie biegi na orientację dla szkół;
- Inteligentne parkowanie dzięki wyeliminowaniu monet i biletów parkingowych;

- Pobieranie wiadomości i filmów z inteligentnych plakatów w kinach;
- Szybkie zamawianie lunchu w restauracjach i uzyskiwanie kuponów;
- Sprzedaż biletów autobusowych;
- Zarządzanie czasem pracy i dziennik kierowców;
- Zarządzanie blokadami w publicznych halach sportowych;
- Tagi informacyjne w środowisku miejskim;
- Koncepcja sklepu przyszłości;
- Glukometr z obsługą NFC.

1.11.1.2 Miasto Nicea

Zakłada się, że Nicea będzie pierwszym miastem NFC w Europie z komercyjnym wdrożeniem NFC przez każdego francuskiego MNO. Projekty są prowadzone głównie w zakresie podróży, m-turystyki, opieki zdrowotnej, wspomaganego życia, m-płatności, m-kultury, m-administracji, m-edukacji i sprawiedliwego handlu. Wdrożone w Nicei projekty obejmują wszystkie tryby pracy: czytnik/zapis, peer-to-peer i emulację kart. Również aplikacje są przechowywane i wdrażane na jednej karcie SIM. Projekty są rozwijane we Francji, Maroku, Rosji i na Haiti w ramach różnych partnerstw i umów.

Projekty te obejmowały również Uniwersytet w Nicei, który był gospodarzem ważnego projektu pilotażowego NFC w latach 2010-2011. Celem projektu Nice Future Campus jest zastąpienie fizycznej legitymacji studenckiej telefonami komórkowymi z obsługą NFC i umożliwienie korzystania z wielu aplikacji na jednej karcie SIM. Student korzystający z tego projektu był w stanie płacić, zarządzać biletami i kuponami, dzielić się opiniami na temat książek, uzyskiwać informacje kontekstowe, komunikować się ze znajomymi i wiele więcej za pomocą telefonu komórkowego z obsługą NFC na terenie kampusu. Główne zastosowania technologii NFC dotyczyły płatności, biletów do restauracji uniwersyteckiej, dostępu do biblioteki, kontroli dostępu, usług opartych na lokalizacji, sieci społecznościowych i usług informacyjnych.

1.11.1.3 Inteligentne przestrzenie miejskie

Smart Urban Spaces (SUS) to wspólny europejski projekt koncentrujący się na projektowaniu i wdrażaniu usług kontekstowych i usług e-miasta opartych na NFC z najnowszymi technologiami mobilnymi i wszechobecnymi. SUS to trzyletni projekt trwający od połowy 2009 do połowy 2012 roku i obejmujący cztery kraje: Finlandię, Francję, Hiszpanię i Grecję. Oulu, Helsinki, Caen, Walencja i Sewilla to tylko niektóre z miast biorących udział w projekcie. W projekt SUS zaangażowanych jest wiele organizacji ze wszystkich czterech krajów. Głównym celem projektu SUS jest zapewnienie ram dla przyjęcia usług e-miasta, analiza techniczna i operacyjna usług, analiza interoperacyjności i testowanie innych kwestii poprzez pilotaże i próby. Usługi e-miasta uwzględnione w projektach SUS można skategoryzować jako transport, rodzina i społeczność, rozrywka, kultura i sport, narzędzia użytkowe, edukacja i nauka, ekosystem miejski NFC i inne specyficzne usługi.

1.11.2 Testy i projekty NFC

Na całym świecie prowadzono różne testy i projekty NFC. Aplikacje płatnicze i biletowe są prawdopodobnie najbardziej znanyimi i obiecującymi codziennymi zastosowaniami technologii NFC, a także najbardziej złożonymi z punktu widzenia ekosystemu. Dlatego też

i projekty próbne są wdrażane w tej dziedzinie zastosowań. Niektóre z tych projektów zostały zakończone lub rozszerzone na inne domeny aplikacji z rosnącą liczbą uczestniczących podmiotów lub są nadal kontynuowane. Niektóre z tych prób i projektów są następujące:

- *Payez Mobile Project*: Jest to wspólna inicjatywa rozpoczęta w listopadzie 2007 roku. Jest to pilotażowa usługa płatności mobilnych wdrożona z udziałem około 1000 testerów i 500 sprzedawców detalicznych w Caen i Strasburgu. Globalnym celem uczestników tej próby jest stworzenie wspólnej wizji, rozwiązania biznesowego dla banków i MNO w domenie aplikacji płatności zbliżeniowych.
- *C1000 NFC Pilot z Rabo Mobile w Holandii*: Rabobank z siedzibą w Holandii Rabo Mobile (pierwotna nazwa Rabo Mobi) stał się pierwszym bankiem w Europie, który wprowadził bankowość mobilną i tanie usługi telefoniczne w inny sposób. Jest to MVNO, który jest w pełni własnością Rabobanku. Rabo Mobile zainicjowało nowy pilot NFC o nazwie "Płać telefonem komórkowym w C1000" w Holandii. C1000 to jedna z największych holenderskich sieci supermarketów. W ciągu 6 miesięcy wdrożono szereg aplikacji obsługujących NFC w sklepach detalicznych C1000, w tym płatności mobilne i usługi lojalnościowe. Ponadto klienci mogą przynosić puste butelki i otrzymywać paragony rabatowe do wykorzystania przy kasie z automatów do butelek, które znajdują się w supermarketie lub mogą otrzymać zwrot pieniędzy na swoje konta Rabobank.
- *Doświadczenie na stadionie NFC w Manchesterze*: Manchester City Football Club i Orange UK udostępniła aplikację do sprzedaży biletów z obsługą NFC. Kibice mogą używać swoich telefonów komórkowych z obsługą NFC, aby dotknąć czytników NFC przy bramach stadionu i wejść przez bramki, aby łatwo uczestniczyć w meczach domowych.
- *Próby Bouygues Telecom w Paryżu*: Największy francuski operator telekomunikacyjny Bouygues Telecom, RATP i Firma SNCF, która jest dostawcą zbliżeniowych kart przejazdowych Navigo, przeprowadziła w Paryżu 3-miesięczny test biletów tranzytowych z obsługą NFC. Celem tej próby było umożliwienie użytkownikom płacenia za przejazd przy bramkach lub czytnikach w autobusach, które akceptują aplikację biletową Navigo, za pomocą telefonów komórkowych z obsługą NFC.
- *O2 Wallet*: Telefonica O2, jako jeden z największych MNO, ogłosiła w listopadzie O2 Wallet 2007 i przeprowadził 6-miesięczny test z różnymi dostawcami usług. Program pilotażowy O2 Wallet otwiera drogę do szerokiego wykorzystania telefonów komórkowych jako kart Oyster do podróżowania po Londynie, płacenia za zakupy kartą Barclaycard lub wstępu na imprezy. Aplikacja ta eliminuje potrzebę noszenia przez użytkowników inteligentnych kart Oyster w swoich portfelach. Użytkownicy mogą płacić za swoje podróże za pośrednictwem aplikacji Oyster, po prostu dotykając swoich telefonów komórkowych do czytników Oyster NFC na stacjach londyńskiego metra, w autobusach i tramwajach.
- *London Fashion Week*: Jeden z największych MNO w Europie, Telefonica O2, zorganizował i przeprowadziła małą próbę podczas London Fashion Week, który jest kluczowym wydarzeniem dla projektantów w Londynie, aby pokazać swoje projekty nabywcom mody na całym świecie. Celem tej próby było zapewnienie nabywcom mody możliwości natychmiastowego wyrażenia opinii na temat kolekcji projektanta Emilio de la Morena. Ten test wiadomości z obsługą NFC został przeprowadzony z ograniczoną liczbą użytkowników.
- *Pass and Fly na lotnisku w Nicei*: Pass and Fly był wspólnym projektem portu lotniczego

Nicea-Lazurowe Wybrzeże

i Air France we współpracy z Amadeus i IER. Pilotaż został uruchomiony w kwietniu 2009 roku i trwał 6 miesięcy na lotnisku Nicea-Lazurowe Wybrzeże. Celem pilotażu było umożliwienie pasażerom pobierania cyfrowych kart pokładowych na ich telefony komórkowe przy użyciu technologii NFC.

1.12 Stan badań naukowych nad literaturą NFC

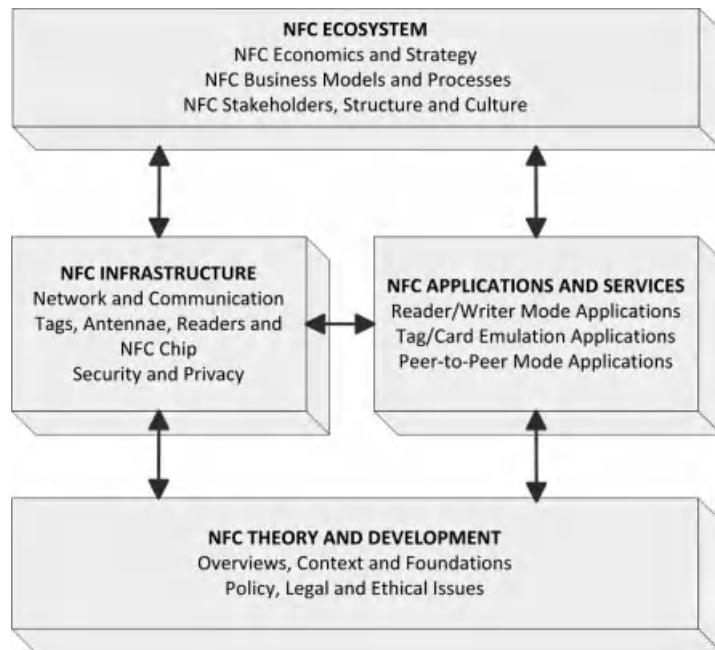
Obecnie NFC stało się atrakcyjnym obszarem badawczym dla wielu naukowców ze względu na jego gwałtowny wzrost i obiecujące zastosowania oraz powiązane usługi. Ze względu na swój charakter, duża część badań nad NFC może być reprezentowana jako badania z zakresu design science, które mają na celu zaproponowanie innowacyjnego artefaktu projektowego i mają znaczenie dla problemu i rygorystyczny charakter. Badanie dotyczące NFC [6] zawiera rygorystyczny przegląd literatury na temat NFC. W ciągu ostatnich kilku lat nastąpił znaczny wzrost liczby prac badawczych i działań dotyczących NFC. Jednak lepsze zrozumienie obecnego stanu obszaru badawczego NFC poprzez akademicki przegląd literatury jest konieczne, aby utrzymać postęp wiedzy w badaniach nad NFC i zidentyfikować lukę między teorią a praktyką.

Przeprowadzone badanie opiera się na artykułach w czasopismach i głównie materiałach konferencyjnych. Badanie nie obejmuje prac magisterskich, doktorskich, podręczników, niepublikowanych dokumentów roboczych, białych ksiąg, artykułów redakcyjnych, raportów prasowych i recenzji książek. Naukowcy i praktycy często korzystają z czasopism w celu pozyskiwania informacji i rozpowszechniania nowych wyników badań, dlatego większość istniejących przeglądów literatury wyklucza również artykuły z konferencji. Nie wyklucza się jednak artykułów konferencyjnych, które zapewniają "wysoki poziom badań, zarówno pod względem szerokości, jak i zakresu" po czasopismach.

(i) *Ramy badawcze NFC*

Zgodnie z badaniem zaproponowano ramy badawcze NFC, które obejmują zorientowaną na treść klasyfikację literatury NFC. Ramy te klasyfikują literaturę akademicką NFC w czterech głównych kategoriach i oznaczają dwukierunkowe relacje między kategoriami: Teoria i rozwój NFC, infrastruktura NFC, zastosowania i usługi NFC oraz ekosystem NFC (patrz rysunek 1.2). Większość artykułów dotyczących badań nad NFC można uznać za badania z zakresu nauk projektowych, które zapewniają innowacyjny, celowy artefakt projektowy w postaci konstruktu, modelu, metody lub instancji. Artefakt projektowy musi rozwiązać konkretny problem lub opracować rozwiązania oparte na technologii. Poziom Teorii i Rozwoju NFC jest podstawowym poziomem ram rewizji NFC. Obejmuje on badania związane z rozwojem technologii i aplikacji NFC; "Przeglądy, kontekst i podstawy" obejmuje ogólne wprowadzenia, oceny, przeglądy dotyczące NFC, podstawy i standardy technologii NFC, analizę wydajności i pomiary oraz nowe wytyczne dotyczące rozwoju aplikacji lub usług obsługujących NFC, a "Polityka, kwestie prawne i etyczne" obejmuje kwestie bezpieczeństwa i prywatności, regulacje i wymogi prawne. Artykuły w tej kategorii koncentrują się na kwestiach behawioralnych i naukach behawioralnych, które mają na celu opracowanie i uzasadnienie teorii, a nie opracowanie artefaktu projektowego. Artykuły dotyczące tego poziomu wpływają na wyższe poziomy, które koncentrują się na nauce projektowania w badaniach NFC.

Poziom infrastruktury NFC to poziom pośredni, który obejmuje badania związane z kwestiami "sieci i komunikacji" (np. aspekt danych, nowe protokoły komunikacyjne i transakcje OTA), kwestie sprzętowe związane z "tagami, anteną, czytnikiem i chipem NFC", kwestie "bezpieczeństwa i prywatności" (np. analiza podatności, dostępność, poufność, integralność, uwierzytelnianie, autoryzacja i niezaprzeczalność), które koncentrują się na opracowywaniu artefaktów projektowych, a nie na kwestiach behawioralnych. Warstwa ta jest pozycjonowana z wcześniej zdefiniowaną działalnością związaną z istniejącą infrastrukturą technologiczną, aplikacjami i istniejącym ekosystemem. Proponowane ramy pokazują bezpośrednie powiązania NFC



Rysunek 1.2 Ramy klasyfikacji dla badań nad NFC.

Infrastruktura z innymi kategoriami. Co więcej, badania związane z infrastrukturą NFC ułatwiają zaspokajanie nowych potrzeb biznesowych.

Aplikacje i usługi NFC to kolejny poziom pośredni, na który wpływ mają pozostałe trzy kategorie. Artykuły w tej kategorii przedstawiają przestrzeń problemową lub nowe potrzeby biznesowe. Technologia NFC obejmuje szeroki zakres zastosowań, które zapewniają rzeczywiste wdrożenia lub prototypy z rygorystycznymi ocenami artefaktów projektowych, takich jak eksperymenty, testy, badania terenowe itp. Artykuły w tej kategorii są również pogrupowane według trybów pracy aplikacji: "Aplikacje w trybie czytnika/zapisu", "Aplikacje w trybie emulacji karty" i "Aplikacje w trybie peer-to-peer". Rzeczywiście, w literaturze dotyczącej NFC można znaleźć artefakty projektowe, które proponują aplikacje lub usługi działające w dwóch lub więcej trybach.

Ekosystem NFC jest najwyższym poziomem ram badawczych NFC. Poziom ten jest częścią przestrzeni problemowej lub środowiska badań NFC, a ulepszenia lub zmiany w środkowych i podstawowych warstwach mają znaczący wpływ na ekosystem NFC. Artykuły w tej kategorii są pogrupowane w kategorie "Ekonomia i strategia NFC", "Modele biznesowe i procesy NFC" oraz "Interesariusze, struktura i kultura NFC". Pierwsze dwie grupy dotyczą wymagań biznesowych, analizy i zarządzania technologią NFC. Trzecia grupa zajmuje się społecznymi aspektami technologii NFC, takimi jak role, cechy i możliwości (np. akceptacja użytkownika, użyteczność, przyjęcie, niezawodność i łatwość zarządzania) interesariuszy (np. operatorów sieci komórkowych, dostawców usług i użytkowników końcowych) oraz kultura usług obsługujących NFC. Interesariusze odgrywają kluczową rolę w ułatwianiu badań i rozwoju NFC. W ekosystemie NFC, cele, zadania, problemy i

Szanse definiują potrzeby biznesowe tak, jak są one postrzegane przez interesariuszy. Postrzeganie to jest kształtowane przez role, możliwości i cechy interesariuszy oceniane w kontekście ekonomii i strategii, struktury i kultury oraz modeli i procesów biznesowych.

(ii) *Ocena przeglądu akademickiego*

NFC jako nowy wyłaniający się obszar badawczy przyciągnął uwagę zarówno praktyków, jak i naukowców. Jak wspomniano wcześniej, akademicka działalność badawcza w obszarze NFC znacznie wzrosła od 2006 roku. Niniejszy przegląd literatury ma na celu rzucenie światła na obecny stan badań nad NFC. Wyniki schematu klasyfikacji NFC mają kilka ważnych implikacji:

- Istnieje wyraźna potrzebawiększej liczby publikacji w czasopismach, aby zapewnić powiązane z biznesem i rygorystyczne artykuły badawcze na temat technologii NFC.
- Nic dziwnego, że większość prac naukowych dotyczy aplikacji i usług NFC, zwłaszcza działających w trybie czytnika/zapisu. Powodem takiego zainteresowania tym trybem jest to, że rozwój i wdrażanie takich usług lub aplikacji jest znacznie łatwiejsze niż rozwój aplikacji działających w innych trybach. Niestety istnieje tylko kilka prac badawczych na temat "aplikacji w trybie Peer-to-Peer".
- Kolejna duża część artykułów dotyczy infrastruktury NFC. Nasz przegląd pokazuje, jak ważne jest ponowne skupienie się na kwestiach technicznych nowej technologii, a nie na kwestiach związanych z realizacją ekonomii, wartości biznesowych lub strategii rozwoju, rozpowszechniania i marketingu NFC. Należy przeprowadzić bardziej szczegółowe badania nad kwestiami biznesowymi i ekoniemią technologii NFC.
- Podczas opracowywania usługi NFC należy również wziąć pod uwagę ekosystem i środowisko biznesowe tej usługi NFC. Takie nowe aplikacje mogą przynieść nowe modele biznesowe i procesy z nowymi graczami. W szczególności możliwości, cechy i role interesariuszy muszą zostać ocenione i zmodyfikowane w razie potrzeby, aby spełnić wymagania nowych modeli biznesowych i procesów. Interesującym obszarem do zbadania mogą być różnice kulturowe dotyczące przyjmowania technologii NFC.
- Problemy polityczne, etyczne i prawne, które można nazwać kwestiami behawioralnymi, były innymi ważnymi i wymagającymi obszarami badawczymi dla rozwoju nowej, wschodzącej technologii. Jednakże, trudno jest znaleźć artykuły zajmujące się polityką publiczną i problemami prawnymi (np. problemami podatkowymi, zaufaniem, oszustwami, kwestiami prywatności w Internecie i prywatności finansowej). Powinno to skłonić naukowców do zbadania tego obszaru.
- Obecnie wydaje się, że najpopularniejszymi obszarami badawczymi związanymi z NFC są rozwój nowych aplikacji obsługujących NFC i rozwój infrastruktury NFC. W związku z tym, badania nad NFC mogą być w większości określane jako badania naukowe w zakresie projektowania, które proponują innowacyjne artefakty i zapewniają użyteczność dla odpowiednich problemów biznesowych. W międzyczasie użyteczność i wydajność proponowanego artefaktu musi zostać wykazana za pomocą dobrze zdefiniowanych metod. Większość artykułów wykorzystuje bardziej opisowe (np. scenariusze i przypadki użycia w celu wykazania ich użyteczności) lub analityczne (np. analiza architektury) metody podczas opracowywania aplikacji lub usługi, zamiast przeprowadzać metody eksperymentalne i testowe. W niektórych artykułach przeprowadzane są nieodpowiednie oceny projektu lub obserwowane są implikacje proponowanych artefaktów projektowych. Zamiast oceny za pomocą scenariuszy lub przypadków użycia, badania terenowe, kontrolowane eksperymenty lub symulacje będą bardziej przydatne do rygorystycznego reprezentowania proponowanego artefaktu.

(iii) *Dalsze badania nad NFC*

Przegląd literatury przedstawiony w [6] ma na celu zapewnienie całościowego przeglądu i kompleksowej podstawy do zrozumienia badań nad NFC. Oprócz ocen zaproponowano pewne akademickie pytania badawcze do dalszych badań w dziedzinie NFC:

- Czy istnieją polityki publiczne, regulacje i normy prawne dotyczące rozwoju i przyjęcia technologii NFC na poziomie indywidualnym i korporacyjnym?
- W jaki sposób opracowywane są wymagane standardy NFC z punktu widzenia polityki, przepisów i prawa?
- Jaki jest wpływ na przyjęcie i akceptację aplikacji NFC po stronie użytkownika?
- Jakie są możliwe konsekwencje różnic kulturowych dla przyjęcia technologii NFC i nowych możliwości biznesowych?
- W jaki sposób można ocenić rozwój technologii NFC jako narzędzi technologii informacyjnej pod względem wyników ekonomicznych i zasad podejmowania decyzji ekonomicznych?

1.13 Podsumowanie rozdziału

NFC jako obiecujący obszar badań i rozwoju przyciągnął uwagę zarówno naukowców, jak i praktyków w ciągu ostatniej dekady. Technologia NFC ma na celu uproszczenie codziennego życia ludzi za pomocą prostego dotyku, a w bardzo niedalekiej przyszłości ludzie będą mogli korzystać z wielu usług za pomocą swoich telefonów komórkowych NFC. Będą mogli kupować towary i usługi, uzyskiwać dostęp do pokoi hotelowych, mieszkań lub samochodów, konfigurować ustawienia Wi-Fi i Bluetooth, przesyłać dane dotyczące zdrowia do szpitalnych systemów monitorowania i tak dalej.

Podstawowe warstwy technologii NFC są zgodne z globalnie przyjętymi standardami ISO, ETSI, ECMA i tak dalej, a także specyfikacjami pionierów branży. NFC Forum jest najważniejszym stowarzyszeniem w rozwoju tej technologii.

Chociaż obecnie dostępne są interoperacyjne zestawy standardów i specyfikacji, nadal brakuje powszechnego zrozumienia potrzeby współpracy. Ponieważ zyski na rynku są bardzo duże, firmy chcą się nimi dzielić. Powoduje to silną rywalizację między operatorami sieci komórkowych, instytucjami finansowymi, władzami transportowymi, firmami IT i tak dalej, co wpływa na postęp ekosystemu NFC i modeli biznesowych. Do tej pory na całym świecie przeprowadzono różne testy NFC i badania użyteczności, zwłaszcza w dziedzinie płatności i usług biletowych. Niektóre z nich doprowadziły do komercyjnego uruchomienia, podczas gdy inne nie, ze względu na brak możliwości wygenerowania spójnych modeli biznesowych.

Rozdział ten stanowi dobre wprowadzenie do technologii NFC z różnych perspektyw, w tym technicznej, biznesowej, użyteczności itp. Przedstawiono w nim również cenne badania akademickie dotyczące korzyści płynących z zastosowań NFC oraz stan badań akademickich w literaturze dotyczącej NFC.

Referencje

- [1] NFC Forum, <http://www.nfc-forum.org/> (dostęp: 10 lipca 2011 r.).
- [2] Ok, K., Coskun, V., and Aydin, M. N. Usability of Mobile Voting with NFC Technology. Proceedings of IASTED International Conference on Software Engineering, Innsbruck, Austria, 16-18 lutego 2010, s. 151-158.
- [3] Jaring, P., Tōrmänen, V., Siira, E., and Matinmikko, T. Improving Mobile Solution Workflows and Usability Using Near Field Communication Technology. Proceedings of the 2007 European Conference on Ambient Intelligence, Darmstadt, Germany, 7-10 November 2007, pp. 358-373.

- [4] Franssila, H. User Experiences and Acceptance Scenarios of NFC Applications in Security Service Field Work. Proceedings of the 2010 Second International Workshop on Near Field Communication, Monaco, 20-22 April 2010, pp. 39-44.
- [5] Ok, K., Coskun, V., Aydin, M. N., and Ozdenizci, B. Current Benefits and Future Directions of NFC Services. Proceedings of 2010 International Conference on Education and Management Technology (ICEMT), Kair, Egipt, 2-4 listopada 2010, s. 334-338.
- [6] Ozdenizci, B., Aydin, M. N., Coskun, V., and Ok, K. NFC Research Framework: A Literature Review and Future Research Directions. Proceedings of 14th International Business Information Management Association Conference on Global Business Transformation through Innovation and Knowledge Management, Istambuł, Turcja, 23-24 czerwca 2010, s. 2672-2685.

2

W kierunku ery NFC

Near Field Communication (NFC) to technologia, która upraszcza i zabezpiecza interakcję z otaczającymi nas urządzeniami obsługującymi NFC. Integruje ona technologię identyfikacji radiowej (RFID) i bezstykowy interfejs kart inteligentnych z telefonami komórkowymi. Koncepcja NFC wynika z synergii kilku technologii, w tym komunikacji bezprzewodowej, urządzeń mobilnych, aplikacji mobilnych, komunikacji RFID i kart inteligentnych. Programowanie po stronie serwera, usługi sieciowe i technologie XML również przyczyniają się do szybkiej poprawy i rozprzestrzeniania się NFC, umożliwiając usługi online przez Internet. Wiele znanych przedmiotów, takich jak karty kredytowe, kluczyki samochodowe i karty dostępu do pokoi hotelowych, ostatecznie przestanie istnieć, ponieważ telefon komórkowy z obsługą NFC wystarczy, aby zapewnić wszystkie ich funkcje.

Technologia NFC już się pojawiła i jest coraz powszechniej stosowana. Widać to wyraźnie podczas lektury tej książki, która wyjaśnia NFC przy użyciu kompleksowego podejścia, od koncepcji i komponentów technologicznych po obszary zastosowań i kwestie proceduralne. W tym rozdziale rozpoczynamy od krótkiej historii, która wyjaśnia, w jaki sposób wszystkie wspomniane powyżej technologie utorowały drogę do rozwoju NFC.

2.1 Ubiquitous Computing i NFC

Obecnie NFC jest jednym z czynników umożliwiających wszechobecne przetwarzanie danych. Dlatego też pochodzenie tego pomysłu jest ściśle związane z wszechobecną informatyką. Aby zrozumieć tło NFC, musimy zacząć od historii wszechobecnej informatyki.

2.1.1 Wszechobecny Computing

Zautomatyzowane obliczenia i programowalność są istotą współczesnych komputerów, a tym samym wszechobecnej informatyki. Historia współczesnych komputerów obejmuje prace pionierów na przestrzeni prawie dwustu lat, takie jak krośno tekstylne, dziurkowane karty papierowe Josepha Marie Jacquarda, które zaowocowały krosnem Jacquarda, w pełni programowalny komputer mechaniczny Charlesa Babbage'a w latach trzydziestych XIX wieku, zapis danych na nośniku do odczytu maszynowego Hermana Holleritha pod koniec lat osiemdziesiątych XIX wieku, formalizacja koncepcji algorytmów i obliczeń.

z maszyną Turinga Alana Turinga w latach 30. i pierwszymi komputerami elektronicznymi w połowie XX wieku, które wymagały dużych pomieszczeń pełnych urządzeń.

Komputery osobiste to ważny krok, który nastąpił po tych wydarzeniach, zmieniając sposób interakcji użytkownika z komputerami poprzez użycie klawiatur i monitorów do wprowadzania i wyprowadzania danych. Mysz jeszcze bardziej poprawiła interakcję między ludźmi a komputerami, ponieważ umożliwiła użytkownikom wprowadzanie danych przestrzennych do komputera. Ręka przyzwyczaiła się do trzymania myszy, a palec wskazujący przyzwyczaił się do jej klikania. Myszy trójwymiarowe (3D), joysticki i drążki wskazujące były innymi formami używanymi do wprowadzania danych. Ruchy urządzenia wskazującego są odzwierciedlane na ekranie przez ruchy kurSORA, tworząc prosty i intuicyjny sposób poruszania się po GUI komputera.

Ekrany dotykowe radykalnie zmieniły również formę interakcji. Zmniejszyły zainteresowanie wszystkimi wcześniejszymi urządzeniami wejściowymi, ponieważ ręce mogły poruszać się bardziej swobodnie na nowym urządzeniu wejściowym komputera. W międzyczasie wprowadzono telefony komórkowe, początkowo do komunikacji głosowej. Wczesne formy zawierały klawiaturę, z mniejszą liczbą klawiszy niż zwykłe klawiatury, ponieważ zwykłe klawiatury nie zmieściłyby się na tak małej powierzchni. Telefony komórkowe z ekranami dotyковymi można uznać za najnowocześniejszą technologię, ponieważ ten sam ekran jest używany zarówno jako jednostka wejściowa, jak i wyjściowa.

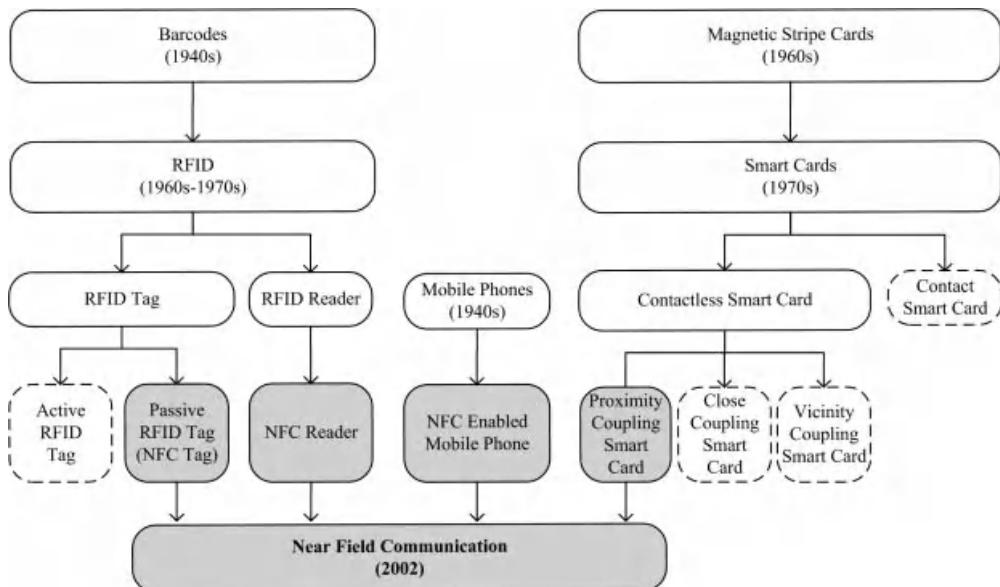
Wszechobecna informatyka odnosi się do kolejnego poziomu interakcji między ludźmi a komputerami, w którym urządzenia komputerowe są całkowicie zintegrowane z codziennym życiem i otaczającymi je przedmiotami. Ubiquitous computing to model, w którym ludzie nie projektują swoich działań zgodnie z maszynami, z których muszą korzystać; zamiast tego maszyny zmieniają swoje formy, aby dostosować się do ludzkich potrzeb. Ostatecznie głównym celem jest to, aby ludzie korzystający z maszyn nie mieli zmieniać swoich codziennych zachowań, a także nawet nie zauważyli, że wykonują czynności z pomocą maszyn.

2.1.2 Nowa alternatywa interfejsu komunikacyjnego dla telefonów komórkowych: Technologia NFC

Podobnie jak w przypadku nowoczesnych komputerów i interfejsów, rosnąca mobilność urządzeń komputerowych zapewniana przez komunikację mobilną jest również ważnym krokiem w rozwoju wszechobecnych możliwości obliczeniowych i NFC. Telefony komórkowe miały już kilka opcji komunikacji ze środowiskiem zewnętrznym przed wprowadzeniem NFC. Kiedy początkowo wprowadzono telefony komórkowe, ich głównym celem było umożliwienie komunikacji głosowej (a ostatnio transmisji danych) między telefonami komórkowymi. Komunikacja GSM umożliwiła funkcjonalność telefonów komórkowych dla kilku usług, takich jak komunikacja głosowa, Short Messaging Service (SMS), Multimedia Messaging Service (MMS) i ograniczony dostęp do Internetu. Jedną z natychmiastowych opcji komunikacji telefonów komórkowych z innymi urządzeniami był przewodowy transfer danych z komputerami.

Technologia Bluetooth została wprowadzona później w celu stworzenia sieci osobistych, które łączą urządzenia peryferyjne z urządzeniami komputerowymi, w tym telefonami komórkowymi. Bluetooth stał się bardzo popularny na początku XXI wieku. Prawdopodobnie najczęściej używaną funkcją Bluetooth jest wymiana danych między telefonami komórkowymi oraz między telefonem komórkowym a innym urządzeniem obsługującym Bluetooth, takim jak komputer. Bluetooth umożliwia komunikację między urządzeniami znajdującymi się w pobliżu. Jednak bezpieczne transakcje nie mogą być przeprowadzane za pomocą tej technologii, ponieważ jest ona przeznaczona do komunikacji

bezprzewodowej w promieniu kilkudziesięciu metrów, co pozwala złośliwym urządzeniom w pobliżu na podsłuchiwanie komunikacji między węzłami Bluetooth.



Rysunek 2.1 Ewolucja technologii NFC.

Główną motywacją dla wizji NFC jest integracja osobistych i prywatnych informacji, takich jak dane kart kredytowych lub debetowych w telefonach komórkowych. Ze względu na wrażliwość wymienianych informacji, bezpieczeństwo jest najważniejszym problemem, a zasięg komunikacji bezprzewodowej zapewniany nawet przez technologię RFID jest uważany za zbyt długi. Ekranowanie jest konieczne, aby zapobiec podsłuchiwaniu prywatnych informacji przez osoby nieupoważnione, ponieważ nawet niezasilane, pasywne tagi mogą być odczytywane z odległości ponad 10 m. W tym miejscu pojawia się NFC.

NFC działa między dwoma kompatybilnymi urządzeniami w bardzo krótkim zasięgu komunikacji. Komunikacja jest wykonywana przez telefon komórkowy NFC z jednej strony i tag NFC (pasywny tag RFID), czytnik NFC lub telefon komórkowy NFC z drugiej strony. RFID jest w stanie odbierać i przesyłać dane z odległości większej niż kilka metrów i ma szeroki zakres zastosowań. Jednak NFC jest ograniczona do bardzo bliskiej odległości i jest również przeznaczona do bezpiecznego przesyłania danych. Obecnie integracja technologii NFC z telefonami komórkowymi jest uważana za najbardziej praktyczne rozwiązanie dla NFC, ponieważ prawie każdy ma przy sobie telefon komórkowy.

Ewolucję technologii NFC zilustrowano na rysunku 2.1. Zasadniczo NFC wykorzystuje technologię RFID, a także jest kompatybilna z bezstykowymi interfejsami kart inteligentnych. Szare obszary na rysunku 2.1 to rozwój technologiczny, który bezpośrednio wspiera środowisko NFC. Technologie, które umożliwiają ewolucję NFC, zostały pokróćce omówione w tym rozdziale. Zapoznanie się z technologicznym tłem NFC będzie pomocne dla czytelnika w zrozumieniu kolejnych rozdziałów.

2.2 Telefony komórkowe

Telefon komórkowy to urządzenie elektroniczne, które służy przede wszystkim do wykonywania połączeń telefonicznych, gdy użytkownik jest w ruchu. Telefony komórkowe są po prostu nazywane telefonami komórkowymi. Użytkownik telefonu komórkowego

musi być zarejestrowany w sieci telefonii komórkowej, w której usługa jest świadczona przez operatora sieci komórkowej (MNO). Połączenie można wykonać lub odebrać z dowolnego innego telefonu, który jest członkiem tej samej lub innej sieci telefonii komórkowej, sieci stacjonarnej, a nawet Internetu. Telefony komórkowe obsługują motto "zawsze i wszędzie".

2.2.1 Cechy telefonu komórkowego

Telefony komórkowe są bardzo wygodne w użyciu i poręczne. Dlatego też, oprócz możliwości wykonywania połączeń telefonicznych, jest do nich dołączona ogromna ilość dodatkowych usług, a wiele nowych przyszłych usług jest wciąż w drodze. Niektóre z obecnie obsługiwanych usług są następujące:

Uslugi łączności przewodowej

- USB;
- Synchronizacja z komputerem.

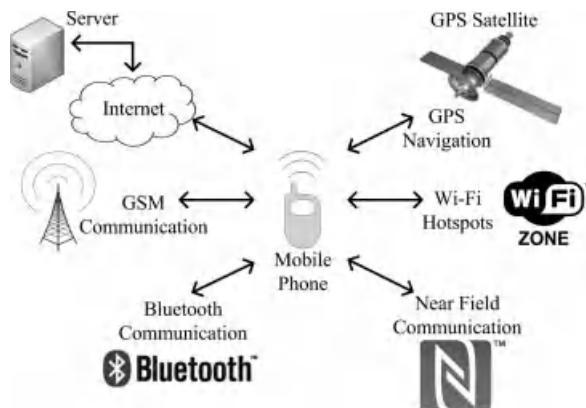
Uslugi komunikacji bezprzewodowej

- Komunikacja GSM;
- SMS (Short Messaging Service lub wiadomości tekstowe);
- MMS (Multimedia Messaging Service);
- Odbiornik radiowy RDS;
- Nawigacja za pomocą globalnego systemu pozycjonowania (GPS);
- Komunikacja bezprzewodowa krótkiego zasięgu: podczerwień, Bluetooth, NFC itp;
- Łączność Wi-Fi;
- Poczta elektroniczna;
- Dostęp do Internetu.

Uslugi zintegrowane

- Przechowywanie danych kontaktowych i komunikacyjnych;
- Planowanie;
- Kalkulator;
- Gry;
- Zdjęcia;
- Odtwarzanie muzyki (MP3) i wideo (MP4);
- Alarmy;
- Nagrywanie notatki;
- Funkcje osobistego asystenta cyfrowego (PDA);
- Kamera (nagrywanie wideo);
- Bezpieczna karta pamięci (SMC, MSD, SD itd.).

Rysunek 2.2 przedstawia główne usługi bezprzewodowe obsługiwane obecnie przez telefony komórkowe: Nawigacja GPS, bezprzewodowe usługi internetowe, GSM, Bluetooth, Wi-Fi i technologie NFC. Technologia GPS, jako oparta na przestrzeni kosmicznej technologia globalnej nawigacji satelitarnej, jest jedną z najpopularniejszych usług wykorzystywanych przez telefony komórkowe. Zapewnia niezawodne informacje o lokalizacji w niemal każdych warunkach pogodowych.

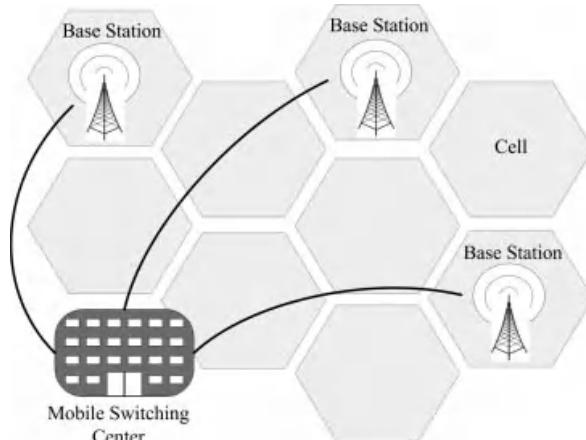


Rysunek 2.2 Główne usługi bezprzewodowe oferowane przez telefony komórkowe.

w każdych warunkach i o każdej porze na całym świecie. Ponieważ wiele osób korzysta z inteligentnych telefonów komórkowych lub urządzeń PDA, a systemy nawigacyjne mogą działać na tych urządzeniach, zapotrzebowanie na systemy nawigacyjne i ich wykorzystanie rośnie. Bezprzewodowe usługi internetowe mogą być włączane na różne sposoby; poprzez Wi-Fi, sieci komórkowe itp. Technologie bezprzewodowe GSM, Bluetooth i Wi-Fi zostały przedstawione w sekcji 2.3.2.

2.2.2 Telefon komórkowy Sieć

Sieć telefonii komórkowej składa się z MNO, stacji bazowych (BS), mobilnego centrum przełączania (MSC) i telefonów komórkowych (patrz rysunek 2.3). Telefon komórkowy wysyła sygnał radiowy, który jest przechwytywany przez pobliską stację bazową, jeśli taka istnieje. Jeśli sygnał zostanie przechwycony przez BS, telefon komórkowy może uzyskać dostęp do sieci, w przeciwnym razie użytkownik zostanie poinformowany, że telefon komórkowy jest poza siecią.



Rysunek 2.3 Sieć telefonii komórkowej.

zasięg. Telefon komórkowy znajdujący się w zasięgu sieci za pośrednictwem dowolnego BS może następnie otrzymać dowolną usługę żądaną przez użytkownika. W przypadku połączenia telefonicznego z innym telefonem komórkowym, żądany telefon musi znajdować się w obszarze zasięgu tego samego lub innego BS, w przeciwnym razie połączenie nie może zostać przetworzone. Obwód, który jest budowany w locie między dwoma telefonami komórkowymi, może obejmować naziemne odnogi komunikacyjne oprócz odnóg komunikacji mobilnej.

Każdy BS obejmuje, a tym samym utrzymuje pierwszy (i ostatni, w zależności od kierunku połączenia) etap komunikacji między telefonem komórkowym a siecią telefonii komórkowej. Obszar obsługiwany przez każdy BS nazywany jest komórką. Rozmiar komórek technicznie zależy od zasięgu odbioru i nadawania, lub który zależy głównie od mocy BS. Mniejsze komórki są używane w obszarach, w których istnieje duże zapotrzebowanie, czyli głównie w zatłoczonych obszarach miejskich, i odwrotnie, w celu zapewnienia dobrej jakości usług (QoS).

W telekomunikacji komórkowej przekazanie (handoff) to proces przenoszenia trwającego połączenia lub sesji danych z jednego kanału sieci rdzeniowej do innego. W komunikacji satelitarnej odnosi się do procesu przekazywania odpowiedzialności za kontrolę satelitarną z jednej stacji naziemnej do drugiej.

Gdy telefon komórkowy jest w ruchu podczas połączenia, połączenie jest utrzymywane przez BS komórki, do której telefon został przeniesiony. Jeśli telefon komórkowy znajduje się poza obszarem zasięgu BS lub innymi słowy poza komórką podczas rozmowy i nie ma zasięgu BS w tej lokalizacji, połączenie nie może zostać utrzymane, więc połączenie zostaje przerwane. Istnieją algorytmy umożliwiające kontynuowanie rozmowy z wysoką jakością, tak aby osoby na obu końcach rozmowy nie były świadome faktu, że nastąpiło przekazanie podczas przejścia komórki.

2.2.3 Architektura telefonu komórkowego

Urządzenie mobilne składa się z kilku komponentów, z których każdy spełnia określona potrzebę:

- Mikrofon przechytuje głos do konwersji z trybu analogowego na cyfrowy.
- Wyświetlacz pokazuje informacje o połączeniach, telefonie, sygnale i sieci.
- Mechanizm wejściowy umożliwia użytkownikowi interakcję z telefonem. Dwa najpopularniejsze mechanizmy wejściowe mechanizmami są klawiatury i ekrany dotykowe.
- Bateria wielokrotnego ładowania zasila telefon komórkowy.
- Karta Universal Subscriber Identity Module (USIM) umożliwia dostęp do sieci, która jest zarządzana przez OSK.
- Antena umożliwia odbiór i transmisję sygnałów między telefonem komórkowym a BS.
- Cyfrowy procesor sygnału (DSP) pobiera sygnał cyfrowy i przetwarza go w celu dalszego wykorzystania.
- Mikroprocesor koordynuje prawie wszystkie funkcje na płycie.
- Jednostka pamięci przechowuje wszystkie rodzaje danych, takie jak numery telefonów, zapisy rozmów, i informacje o wiadomościach.
- Karta USIM działa jak karta inteligentna, która przechowuje informacje o tożsamości abonenta. Przechowuje ona dane abonenta, dane bezpieczeństwa umożliwiające dostęp do zabezpieczonych usług oraz

pamięć do przechowywania danych osobowych, takich jak numery telefonów.

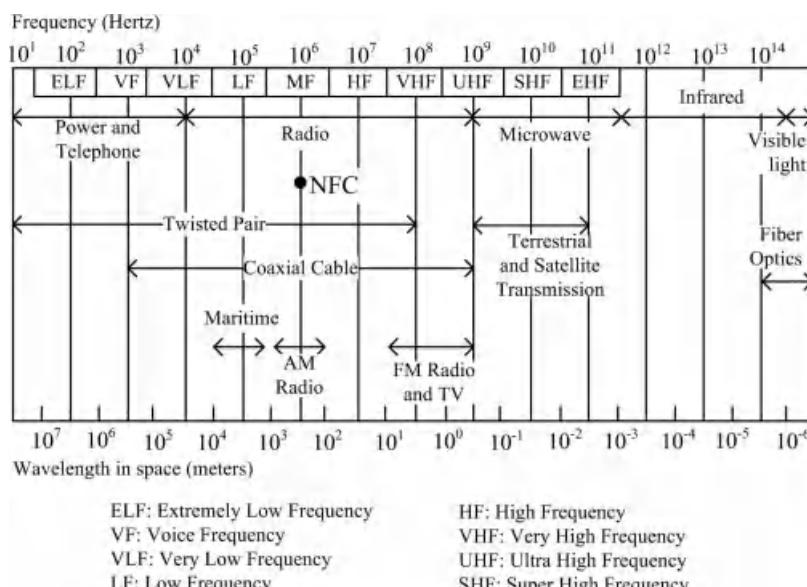
Karta USIM zawiera mikroprocesor, który zawiera wymagane informacje i klucze dostępu w celu uzyskania dostępu do sieci telefonii komórkowej zarządzanej przez MNO.

Powodem dostarczenia mobilnej karty USIM zamiast osadzania jej w urządzeniu mobilnym jest zapewnienie użytkownikowi elastyczności i przenośności. Użytkownik może po prostu przełączyć USIM z telefonu komórkowego na inny, będąc w stanie połączyć się z tym samym operatorem sieci komórkowej bez żadnych dodatkowych procedur.

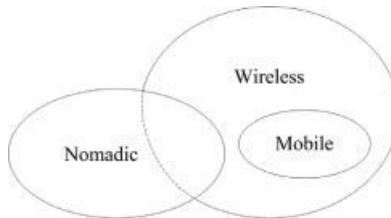
USIM jest zarządzany przez mobilny system operacyjny. Obecnie istnieje szeroki zakres opcji, a udział w rynku systemów operacyjnych różni się w miarę upływu czasu.

2.3 Komunikacja bezprzewodowa jako medium komunikacyjne dla technologii NFC

Komunikacja bezprzewodowa odnosi się do przesyłania danych bez użycia kabli. Gdy komunikacja jest niemożliwa i niepraktyczna przy użyciu przewodów lub kabli, preferowana jest komunikacja bezprzewodowa. Zasięg może ważyć się od kilku centymetrów do wielu kilometrów. Urządzenia do komunikacji bezprzewodowej obejmują różne typy stacjonarnych, mobilnych i przenośnych radiotelefonów dwukierunkowych, telefonów komórkowych, urządzeń PDA, GPS, bezprzewodowych myszy komputerowych, klawiatur, zestawów słuchawkowych, telewizji satelitarnej i telefonów bezprzewodowych i umożliwiają komunikację bez konieczności fizycznego połączenia z siecią. Komunikacja bezprzewodowa wprowadza wyzwania, które są nieco bardziej trudne do pokonania w porównaniu z komunikacją przewodową, takie jak zakłócenia, tłumienie, zawodność, wyższe koszty i niższe bezpieczeństwo. Termin "bezprzewodowy" odnosi się do transmisji danych za pośrednictwem fal elektromagnetycznych, który wykorzystuje widmo elektromagnetyczne przedstawione na rysunku 2.4.



Rysunek 2.4 Widmo elektromagnetyczne na potrzeby komunikacji.



Rysunek 2.5 Komunikacja bezprzewodowa, mobilna i nomadyczna.

2.3.1 Komunikacja bezprzewodowa, mobilna i nomadyczna

Łączność bezprzewodowa jest zasadniczo mobilna, a łączność mobilna jest zasadniczo bezprzewodowa przynajmniej w jednym łączu, jak pokazano na rysunku 2.5. Przykładem komunikacji bezprzewodowej, ale nie mobilnej, jest komputer stacjonarny, który wykorzystuje komunikację bezprzewodową do łączenia się z bezprzewodową siecią lokalną (WLAN). Rozróżniamy również komunikację nomadyczną od mobilnej. W komunikacji nomadycznej węzeł porusza się pomiędzy komunikacjami, ale nie porusza się podczas komunikacji. Przykładem komunikacji nomadycznej jest laptop. Jeśli mobilność nie jest potrzebna podczas komunikacji, można użyć komunikacji bezprzewodowej lub przewodowej, chociaż laptop można przenieść w dowolne miejsce na świecie. Zdolność do bycia mobilnym podczas komunikacji może być zapewniona tylko przez medium bezprzewodowe.

Kompleksowa komunikacja między dwoma urządzeniami bezprzewodowymi nie wymaga całkowicie bezprzewodowej ścieżki. Infrastruktura przewodowa może być wykorzystana do uzupełnienia ścieżki. Tylko pierwszy etap komunikacji między użytkownikiem mobilnym a jednym terminaliem sieci musi być bezprzewodowy, podczas gdy pozostała część może nadal opierać się na połączeniach przewodowych, a tym samym na sieci przewodowej. Taka architektura nazywana jest siecią komórkową lub infrastrukturalną siecią bezprzewodową. Alternatywnie, gdy wszystkie łączą się bezprzewodowe i nie ma wstępnie zaprojektowanej infrastruktury, architektura jest klasyfikowana jako sieć bezprzewodowa ad hoc lub bez infrastruktury. Jeśli weźmiemy pod uwagę na przykład sieć GSM, telefon komórkowy wykonuje komunikację bezprzewodową z BS, do którego jest podłączony, ale większość pozostałej komunikacji między BS a serwerami sieciowymi wykorzystuje następnie komunikację przewodową. Dlatego GSM opiera się na architekturze komórkowej. W przypadku bezprzewodowej sieci czujników, węzły czujników bezprzewodowych budują sieć bezprzewodową między sobą, a także ze zlewem, tworząc w ten sposób sieć ad hoc.

2.3.2 Komunikacja bezprzewodowa i mobilna Technologie

Najbardziej oczywistą zaletą komunikacji bezprzewodowej jest mobilność, która rzeczywiście ma duży wpływ na nasze codzienne życie. Komunikacja mobilna wspiera nie tylko produktywność i elastyczność organizacji, ale także życie społeczne jednostek, ponieważ ludzie mogą pozostawać w stałym kontakcie ze swoimi sieciami społecznościowymi. Powszechnie stosowane technologie bezprzewodowe obejmują GSM, Bluetooth, Wi-Fi, WiMAX i ZigBee:

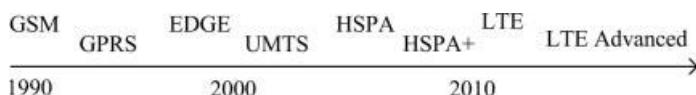
(i) Globalny system łączności komórkowej (GSM)

GSM jest jedną z powszechnie stosowanych technologii komunikacji mobilnej. GSM

W kierunku ery

NFC Wykorzystuje dwukierunkowe, pełnodupleksowe połączenie między dwoma urządzeniami.

Jest to system zorientowany na połączenia



Rysunek 2.6 Ewolucja technologii GSM.

który zapewnia wysoce niezawodne funkcje i znacznie zmniejsza zużycie energii przez terminal w porównaniu z wcześniejszymi generacjami komunikacji mobilnej.

Na rysunku 2.6 przedstawiono ewolucję usług GSM w zależności od daty ich wprowadzenia na rynek. Jest to największa różnorodność spośród wszystkich technologii bezprzewodowych. Ewolucja zaczyna się od 2G GSM i General Packet Radio System (GPRS) do 3G Enhanced Data for GSM Evolution (EDGE), Universal Mobile Telecommunication System (UMTS) i High Speed Packet Access (HSPA).

Istnieje kilka cech, które sprawiają, że GSM jest tak popularny wśród operatorów i ich klientów. Umożliwia obsługę danych, w tym wiadomości SMS i przeglądanie stron internetowych, wyraźną jakość glosu i roaming międzynarodowy z usługami dostępnymi w ponad 200 krajach. Więcej szczegółowych informacji można znaleźć na stronie internetowej (<http://www.gsm.org>).

(ii) *Bluetooth*

Bluetooth jest przykładem bezprzewodowej sieci osobistej (WPAN) opartej na IEEE Standard 802.15. Jest to otwarty standard technologii bezprzewodowej. Każde urządzenie obsługujące Bluetooth może połączyć się z innym urządzeniem obsługującym Bluetooth w pobliżu za pomocą technologii radiowej zwanej widmem rozproszonym z przeskakiem częstotliwości. Wykorzystuje ona pasmo częstotliwości radiowej krótkiego zasięgu (RF) 2,4 GHz.

Urządzenia obsługujące technologię Bluetooth mogą komunikować się za pomocą pikosieci krótkiego zasięgu. Pikosieci pozwalają jednemu urządzeniu nadziranemu na podłączenie do siedmiu aktywnych urządzeń podrzędnych. Gdy urządzenie z obsługą Bluetooth znajdzie się w zasięgu radiowym, pikosieci są tworzone automatycznie. Dzięki temu można łatwo łączyć się w dowolnym miejscu.

Najczęściej używane aplikacje Bluetooth to przesyłanie danych między telefonem komórkowym a urządzeniem obsługującym Bluetooth, urządzenia wejściowe i wyjściowe komunikujące się z komputerem oraz zestaw słuchawkowy telefonu komórkowego komunikujący się z bazą telefonu komórkowego. Obecnie Bluetooth jest zarządzany przez Bluetooth Special Interest Group. Więcej szczegółowych informacji można znaleźć na stronie internetowej (<http://bluetooth.com>).

(iii) *Wi-Fi*

Wi-Fi jest jedną z popularnych technologii bezprzewodowych i jest supersetem standardu IEEE 802.11, który dotyczy bezprzewodowych sieci lokalnych (WLAN). Znak towarowy Wi-Fi jest własnością Wi-Fi Alliance. Wi-Fi to bezprzewodowa wersja sieci Ethernet. Wykorzystuje częstotliwości radiowe podobne do Bluetooth, ale o większej mocy. W rzeczywistości skutkuje to lepszym i szybszym połączeniem w dużym zasięgu.

Obecnie z Wi-Fi można korzystać wszędzie. Jest ono zainstalowane w wielu komputerach PC, odtwarzaczach MP3, smartfonach, drukarkach, konsolach do gier wideo i laptopach. Urządzenia te mogą łatwo łączyć się z Internetem, ponieważ znajdują się w zasięgu sieci bezprzewodowej podłączonej do Internetu. Wielkość zasięgu zależy od liczby połączonych ze sobą punktów dostępowych. Więcej szczegółowych informacji można znaleźć na stronie internetowej (<http://www.wi-fi.org>).

(iv) *WiMAX*

NFC WiMAX (Worldwide Interoperability for Microwave Access) to protokół telekomunikacyjny zapewniający stacjonarny i w pełni mobilny dostęp do Internetu. WiMAX Forum opisuje

Tabela 2.1 Przegląd niektórych technologii bezprzewodowych

Technologia bezprzewodowa	Częstotliwość pracy	Szybkość transmisji danych	Zakres działania
UMTS	900, 1800, 1900 MHz	2 Mb/s	Szeroki zakres
EDGE	900, 1800, 1900 MHz	160 kb/s	Szeroki zakres
GPRS	900, 1800, 1900 MHz	160 kb/s	Szeroki zakres
802.16 WiMAX	10-66 GHz	134 Mb/s	1-3 mil
Wi-Fi 802.11b/g	2,4 GHz	54 Mb/s	100 m
802.11a Wi-Fi	5 GHz	54 Mb/s	100 m
802.15.1 Bluetooth 2.0	2,4 GHz	3 Mb/s	10 m
802.15.4 ZigBee	2,4 GHz	250 kb/s	70 m
NFC	13,56 MHz	106, 212, 424 kb/s	0-4 cm
RFID	125-134 kHz (LF) 13,56 MHz (HF) 400-930 MHz (UF) 2,5 GHz i 5 GHz (mikrofalówka)	1-200 kb/s	20 cm dla pasywnych 400 cm dla aktywnych

WiMAX jako "oparta na standardach technologia umożliwiająca dostarczanie bezprzewodowego dostępu szerokopasmowego ostatniej mili jako alternatywy dla kabli i DSL". Więcej szczegółowych informacji można znaleźć na stronie internetowej (<http://www.wimax.com>).

(v) ZigBee

ZigBee to standard bezprzewodowej sieci kratowej. Jest to technologia o niskim koszcie, niskim poborze mocy i niskiej szybkości oparta na standardzie IEEE 802.15.4 (Low Rate Wireless Personal Area Networks). ZigBee jest prostsza i tańsza niż inne technologie WPAN, takie jak Bluetooth. ZigBee umożliwia aplikacje i usługi, takie jak zdalne sterowanie, kontrola drzwi i kontrola oświetlenia, które wymagają niskiej szybkości transmisji danych i długiego czasu pracy baterii. Dzięki niezawodnej wydajności bezprzewodowej i pracy na baterii, ZigBee zapewnia użytkownikom swobodę i elastyczność. Więcej szczegółowych informacji można znaleźć na stronie internetowej (<http://www.zigbee.org>).

Tabela 2.1 zawiera krótkie podsumowanie popularnych technologii bezprzewodowych - zgodnie z ich częstotliwością roboczą, zasięgiem działania i szybkością transmisji danych - obecnie używanych na całym świecie oraz integrację dwóch innych technologii bezprzewodowych w tym kontekście. Te dwie inne główne technologie bezprzewodowe to RFID i NFC, które są rozszerzeniem RFID krótkiego zasięgu. Szczegóły technologii RFID zostały wyjaśnione w następnej sekcji.

W tabeli 2.1 technologie GPRS, EDGE i UMTS reprezentują bezprzewodowe sieci rozległe (WWAN). Po tych technologiach następuje WLAN z różnymi częstotliwościami roboczymi i zasięgiem. Następnie pojawiają się technologie bezprzewodowych sieci osobistych (WPAN), takie jak ZigBee i Bluetooth. NFC ma najkrótszy zasięg komunikacji w porównaniu z innymi technologiami.

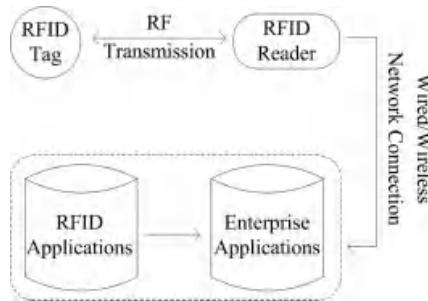
2.4 Technologia RFID

RFID to technologia komunikacyjna służąca do wymiany danych między czytnikiem RFID

W kierunku ery

a elektronicznym znacznikiem RFID (etykietą) za pomocą fal radiowych (patrz rysunek 2.7).

Etykiety te są tradycyjnie



Rysunek 2.7 Architektura systemu RFID.

przymocowane do obiektu, głównie w celu identyfikacji i śledzenia. Transmisja danych wynika z fal elektromagnetycznych, które mogą mieć różne zakresy w zależności od częstotliwości i pola magnetycznego. Czytniki RFID mogą odczytywać/zapisywać dane z/do tagów RFID.

Połączenie między czytnikami RFID a aplikacją hosta RFID wykorzystuje sieci przewodowe lub bezprzewodowe. W systemie zaplecza aplikacja RFID ma przypisane określone informacje. Tagi RFID zazwyczaj zawierają układ scalony (IC) i antenę. Układ scalony zapewnia przechowywanie i przetwarzanie danych, modulowanie i demodulowanie sygnału RF oraz inne funkcje. Antena umożliwia odbiór i transmisję sygnału. Tagi, czytniki i szczegóły transmisji dotyczące komponentów systemu RFID zostały wyjaśnione w dalszej części tej sekcji.

System IFF (Identify Friend or Foe) był pierwszym powszechnym zastosowaniem technologii RFID podczas II wojny światowej, używanym do odróżniania przyjaznych samolotów od wrogich. Komercyjne wykorzystanie technologii RFID sięga lat 60. i 70. ubiegłego wieku w systemach otwierania drzwi za pomocą klucza. Postęp technologiczny w wielu różnych dziedzinach (np. komputery, radio, radar, zarządzanie łańcuchem dostaw, transport, zarządzanie jakością i inżynierią) sprawił, że technologia RFID stała się bardziej przydatna w zarządzaniu aktywami, płatnościami, biletach, śledzeniu zwierząt gospodarskich i transporcie.

2.4.1 Wcześniejsza forma RFID: technologia kodów kreskowych

Kod kreskowy to sposób reprezentowania danych, które można odczytać za pomocą urządzenia optycznego lub skanera. Kody kreskowe zawierają dane o obiekcie, do którego są dołączone. Kody kreskowe są skanowane przez skanery optyczne zwane czytnikami kodów kreskowych. Wczesne kody kreskowe reprezentują dane poprzez różne szerokości i odstępów między równoległymi liniami. Są one określane jako liniowe lub jednowymiarowe (1D) kody kreskowe. Później ewoluowały one w prostokąty, kropki, sześciokąty i inne wzory geometryczne w dwóch wymiarach. Chociaż dwuwymiarowe kody kreskowe (2D) wykorzystują różne symbole inne niż paski, nadal nazywane są kodami kreskowymi.

Kody kreskowe mają niewielką pojemność, a ich produkcja jest łatwa i tania. Zakres liniowych kodów kreskowych jest niski, ale zakres kodów 2D jest znacznie wyższy. Liniowe kody kreskowe są zwykle używane do identyfikacji grupy produktów, takich jak batoniki określonej marki, ale nie są używane do identyfikacji każdego konkretnego batonika. Dlatego wszystkie batoniki tej samej marki zawierają ten sam kod kreskowy, nawet w różnych domach towarowych, różnych miastach i krajach. Kody kreskowe 2D mają większą pojemność do przechowywania danych niż liniowe kody kreskowe, dlatego

NFC mogą zawierać unikalną wartość klucza dla każdego produktu.



Rysunek 2.8 Przykład kodu kreskowego UPC-A.

określony przedmiot. Na przykład, kody kreskowe 2D w pudełku z lekami mogą zawierać konkretne dane identyfikacyjne tego pudełka, dzięki czemu pacjenci i leki mogą być śledzone ze scentralizowanej bazy danych. Niektóre z głównych przykładów liniowych kodów kreskowych to UPC (uniwersalny kod produktu) i EAN-13 (europejski numer artykułu). Kod kreskowy QR (Quick Response) jest przykładem kodu kreskowego 2D.

(i) *Kod kreskowy UPC-A*

Kod kreskowy UPC umożliwia unikalną identyfikację produktu i jego producenta. UPC-A jest dobrze znany typem UPC i jest 12-cyfrowym kodem, jak pokazano na rysunku 2.8. Pierwsze sześć cyfr reprezentuje znak systemu liczbowego i producenta oznaczonego produktu. Kolejne pięć cyfr jednoznacznie identyfikuje produkt, a dwunasta cyfra to znak kontrolny.

UPC koduje 12 cyfr dziesiętnych jako SLLLLLMRRRRRE. S odnosi się do początku, który jest prefiksem, a E odnosi się do końca, który jest znakiem sprawdzania błędów. S i E stanowią wzorzec bitowy 101. Znak M, który znajduje się w środku, to wzorzec bitowy 01 010. S, M i E to paski zabezpieczające kodu kreskowego UPC. L (po lewej) i R (po prawej) to cyfry reprezentowane przez siedmiobitowy kod. Kod UPC koduje 84 cyfry i 11 cyfr jako paski ochronne.

(ii) *Kod kreskowy EAN-13*

Kod kreskowy EAN-13 odnosi się do kodu kreskowego European Article Number-13, który obecnie został przemianowany na International Article Number. Wykorzystuje on 13 cyfr składających się z 12 cyfr danych i cyfry kontrolnej. Kody kreskowe EAN-13 są używane na całym świecie do oznaczania produktów często sprzedawanych w punktach sprzedaży detalicznej. Numery zakodowane w kodach kreskowych EAN-13 to numery identyfikacyjne produktów, w tym kody kraju, producenta i produktu. Przykładowy kod kreskowy EAN-13 pokazano na rysunku 2.9.

(iii) *Kod kreskowy QR*

Kod kreskowy QR Code został zaprojektowany przez japońską firmę Denso. Jest to matryca ogólnego przeznaczenia 2D przeznaczona do szybkiego skanowania informacji. Symbol kodu kreskowego QR ma kształt kwadratu i posiada ciemne i jasne kwadraty w trzech rogach symbolu, co umożliwia ich łatwą identyfikację. Przykładowy kod kreskowy QR pokazano na rysunku 2.10.



Rysunek 2.9 Przykład kodu kreskowego EAN-13.



Rysunek 2.10 Przykład kodu kreskowego QR Code.

2.4.2 Kody kreskowe a znaczniki RFID

Ważne jest, aby powiedzieć, że tagi RFID mogą być identyfikowane jako uzupełnienie, ale nie substytut kodów kreskowych. Oba mają różne zalety i wady.

Rozważmy najpierw kody kreskowe. Kody kreskowe są drukowane na papierze lub naklejkach, które muszą być widoczne. Ponieważ do tworzenia kodów kreskowych używa się papieru lub naklejek, można je łatwo generować i dystrybuować. Skaner kodów kreskowych służy do łatwego odczytu naklejki. Kody kreskowe są jednak nieodpowiednie w niektórych zastosowaniach. Mogą łatwo ulec uszkodzeniu lub zużyciu i mogą być nieodpowiednie do zastosowań wymagających wysokiego poziomu bezpieczeństwa. Skaner kodów kreskowych odbija światło na czarnych paskach kodu kreskowego, a odczytane dane są konwertowane na ich numeryczny odpowiednik do dalszego przetwarzania. Umieszczenie skanera na kodzie kreskowym i zeskanowanie każdego elementu jest nieco trudnym procesem.

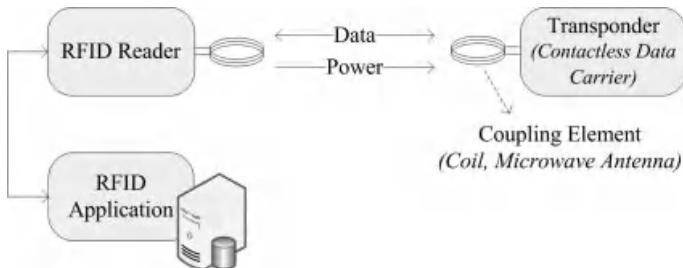
W przypadku systemów RFID, tagi RFID nie mają żadnych problemów z widocznością. Fale radiowe mogą z łatwością pobierać dane przechowywane w tagach RFID; nie ma wymogu linii wzroku do odczytu i pobierania danych. Dane przechowywane w tagu mogą być szyfrowane, aby zapobiec złośliwemu koplowaniu. W ten sposób tagi RFID zapewniają większe bezpieczeństwo niż kody kreskowe. Jednak główną wadą tagów RFID jest ich koszt.

Inną ważną kwestią jest to, że pojemność danych tagu RFID jest wystarczająco duża, aby każdy pojedynczy tag mógł dostarczyć unikalny kod i unikalne znaczenie. W związku z tym, dzięki unikalności tagów RFID, każdy pojedynczy produkt może być po prostu śledzony, gdy przemieszcza się z jednej lokalizacji do drugiej. Śledzenie produktów jest ważną cechą tagów RFID. Jest to bardzo przydatne w przypadku kradzieży lub utraty produktu.

2.4.3 Podstawy technologii RFID

Kilka organizacji jest zaangażowanych w rozwój i definiowanie technologii RFID, takich jak koncepcje sprzętowe, środowisko aplikacji itp. Różne organizacje biorą udział w standaryzacji, takie jak Międzynarodowa Organizacja Normalizacyjna (ISO), EPCglobal Inc., Europejski Instytut Norm Telekomunikacyjnych (ETSI) i Federalna Komisja Łączności (FCC) [1].

System RFID składa się z dwóch głównych elementów: transpondera i czytnika [2]. Transponder to komponent, który znajduje się na produkcie lub obiekcie, który ma zostać zidentyfikowany, oraz



Rysunek 2.11 Główne komponenty systemu RFID.

Czytnik jest elementem, który odczytuje dane z transpondera lub odczytuje/zapisuje dane z/do transpondera (patrz rysunek 2.11):

- Transponder składa się z elementu sprzęgającego i układu scalonego, który przechowuje rzeczywiste dane. Transponder jest w rzeczywistości tagiem RFID. Transponder może być pasywny lub aktywny. Gdy transponder znajduje się w zasięgu czytnika RFID, jest zasilany przez przychodzące sygnały.
- Czytnik zazwyczaj zawiera nadajnik-odbiornik (lub moduł wysokiej częstotliwości) z dekoderem, który służy do interpretacji danych, jednostki sterującej i anteny. Wiele czytników RFID jest wyposażonych w dodatkowy interfejs umożliwiający przekazywanie odebranych danych do innego systemu.

2.4.4 Tagi RFID jako transpondery

Jak wspomniano, tagi RFID to małe układy scalone z elementami sprzęgającymi. Mają one wystarczającą zdolność do przechowywania dużych ilości danych. Są one podzielone na dwie główne grupy: tagi pasywne, które nie mają zasilania oraz tagi aktywne, które mają własne zasilanie.

2.4.4.1 Pasywne znaczniki RFID

Pasywne tagi RFID mają wbudowany układ scalony i antenę, ale nie mają wewnętrznego źródła zasilania. Przychodzące sygnały RF zapewniają wystarczającą moc do uruchomienia układu scalonego w tagu i przesłania odpowiedzi. Ze względu na brak wbudowanego zasilacza lub baterii, pasywne tagi RFID są dość małe. Jeśli chodzi o rozmiar, mogą one mieć wielkość od znaczka pocztowego do karty pocztowej. Ponadto mogą być odczytywane tylko z niewielkich odległości, które wahają się od około 10 cm do kilku metrów. Zasięg ten zależy od wybranej częstotliwości radiowej, konstrukcji anteny i rozmiaru. Pasywne tagi RFID są przydatne tylko w ograniczonym zestawie zastosowań, ponieważ nie mają wewnętrznego źródła zasilania i mogą być odczytywane tylko z niewielkich odległości. Pasywny tag pozostaje czytelny przez bardzo długi czas; nawet po sprzedaży produktu komercyjnego zawierającego pasywny tag RFID. Znaczniki te są bardzo tanie w produkcji.

2.4.4.2 Aktywne znaczniki RFID

Podobnie, aktywne tagi RFID również posiadają układ scalony i antenę. Jednak w przeciwieństwie do pasywnych tagów RFID, aktywne tagi RFID mają własne wbudowane źródło zasilania. Jest ono wykorzystywane do zasilania układu scalonego w tagu w celu

Tabela 2.2 Porównanie tagów aktywnych i pasywnych

Parametry	Aktywne tagi	Tagi pasywne
Źródło zasilania	Wbudowane źródło zasilania	Moc z pola RF
Bateria	Tak	Nie
Siła sygnału do tagu	Bardzo niski	Bardzo wysoka
Zakres działania	Daleki zasięg	Do kilku metrów
Pojemność przechowywania danych	Wysoki	Niski
Koszt produkcji	Drogie	Tani

z czytnikiem RFID. Mogą nadawać przy wyższych poziomach mocy i są bardziej niezawodne niż tagi pasywne. Znaczniki te mogą być również skuteczne w środowiskach o trudnym dostępie do fal radiowych, takich jak woda, kontenery transportowe i pojazdy na duże odległości.

Aktywne tagi RFID mają znacznie większy zasięg i większy rozmiar pamięci niż pasywne tagi RFID. Aktywny tag RFID jest zazwyczaj droższy i fizycznie większy niż pasywny tag RFID. Mają one możliwość przechowywania dodatkowych informacji wysyłanych przez czytnik RFID. Niektóre aktywne tagi RFID mogą być zintegrowane z czujnikami, takimi jak czujniki temperatury, wilgotności, wstrząsów/wibracji, światła i atmosfery. Charakterystyczne właściwości aktywnych i pasywnych tagów RFID zostały porównane w tabeli 2.2.

2.4.5 Czytniki RFID

Czytnik RFID to urządzenie, które służy do odpytywania tagu RFID. Jak wspomniano wcześniej, zawiera on nadajnik-odbiornik, jednostkę sterującą i antenę. Antena emisuje fale radiowe, a czytnik przechwytuje dane przesypane przez tag i dostarcza je do infrastruktury w celu dalszego przetwarzania, na przykład pobierania treści powiązanych z numerem identyfikacyjnym na tagu. Czytniki mogą odczytywać pojedyncze częstotliwości, podczas gdy czytniki wieloprotokołowe mogą odczytywać spektrum większości dostępnych pasm.

2.4.6 Częstotliwość Zakresy

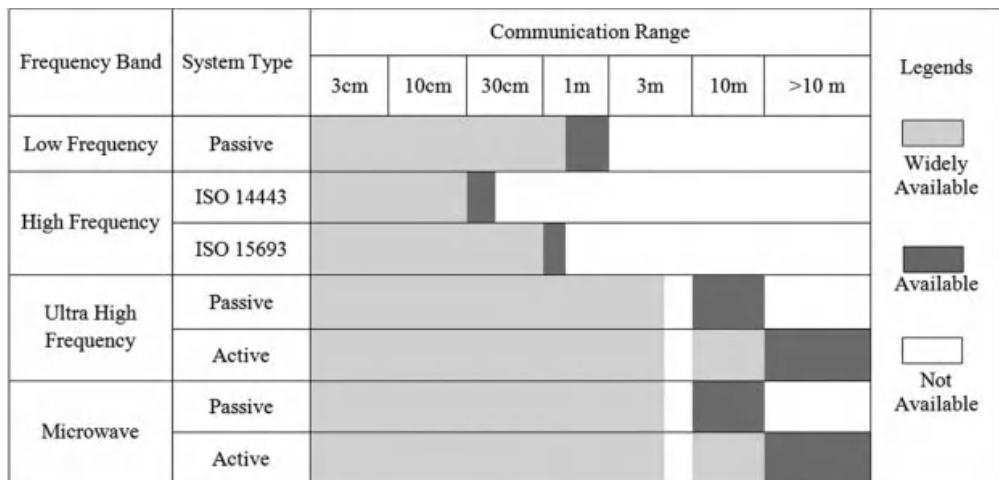
RFID wykorzystuje częstotliwości od 300 kHz do 3 GHz; dokładny zakres zależy od przepisów obowiązujących w danym kraju. Tagi aktywne nadają tylko na wyższych częstotliwościach RF, podczas gdy tagi pasywne nadają na wszystkich częstotliwościach. Rysunek 2.12 przedstawia zakres komunikacji dla różnych pasm częstotliwości i typów systemów.

2.4.7 Zasady działania technologii RFID

Najważniejsze zasady działania technologii RFID to sprzężenie indukcyjne i sprzężenie zwrotne:

2.4.7.1 Sprzężenie indukcyjne

Zgodnie z [2], transponder sprzężony indukcyjnie składa się z elektronicznego urządzenia przenoszącego dane, zwykle pojedynczego mikroukładu i cewki o dużej powierzchni, która działa jak antena.

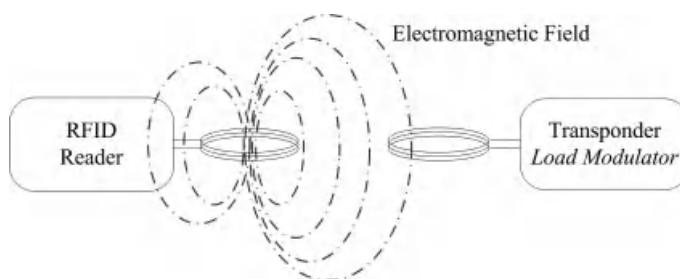


Rysunek 2.12 Zasięg komunikacji systemu RFID [3].

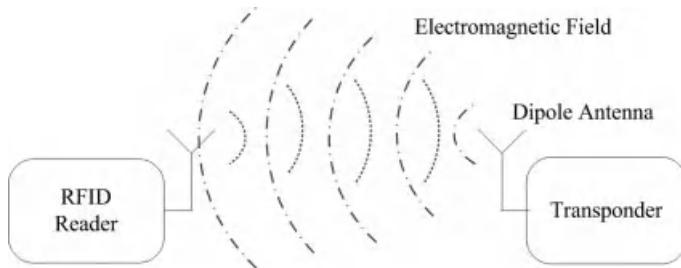
Transpondery lub tagi sprężone indukcyjnie są zazwyczaj tagami pasywnymi, które nie mają wewnętrznego źródła zasilania. W związku z tym mogą być używane tylko w bliskim polu. Oznacza to, że cała energia dla wbudowanego mikroprocesora w tagu musi być dostarczona przez czytnik RFID, aby mikroprocesor mógł działać.

W tym celu antena czytnika RFID generuje pole elektromagnetyczne o wysokiej częstotliwości. Pole to przenika przez przekrój cewki anteny i obszar wokół cewki. Długość fali zakresu częstotliwości jest kilkakrotnie większa niż odległość między anteną czytnika RFID a pasywnym tagiem RFID. To pole elektromagnetyczne można również zidentyfikować jako proste zmienne pole magnetyczne.

Gdy tag RFID zostanie umieszczony w polu elektromagnetycznym czytnika RFID, transponder pobiera energię z tego pola magnetycznego (patrz rysunek 2.13). Ten pobór mocy można opisać jako spadek napięcia na rezystancji wewnętrznej w antenie czytnika RFID poprzez prąd zasilający antenę czytnika RFID. Tak więc włączanie i wyłączanie rezystancji obciążenia (lub modulatora obciążenia) w antenie transpondera powoduje zmiany napięcia w antenie czytnika RFID. Jeśli włączanie i wyłączanie modulatora obciążenia jest kontrolowane przez dane, to



Rysunek 2.13 Sprzężenie indukcyjne.



Rysunek 2.14 Sprzężenie wsteczne.

Dane te mogą być przesyłane z tagu RFID do czytnika RFID. Ten rodzaj transferu danych nazywany jest modulacją obciążenia.

2.4.7.2 Sprzężenie wsteczne

Rozważmy pole elektromagnetyczne technologii RADAR [2]. Fale elektromagnetyczne uderzają w obiekty, a te je odbijają. Obiekty te mają duży przekrój odbicia, który jest miarą skuteczności odbijania fal przez obiekt.

W typowym systemie RFID pole elektromagnetyczne rozchodzi się na zewnątrz od anteny czytnika RFID. Niewielka część tego pola jest redukowana ze względu na wolną przestrzeń. Pozostała część pola dociera do anteny transpondera lub tagu RFID. Antena dostarcza napięcie o wysokiej częstotliwości. Po wyprostowaniu przez diody, moc ta może być wykorzystana do włączenia napięcia w celu dezaktywacji lub aktywacji trybu oszczędzania energii.

W przypadku sprzężenia zwrotnego część przychodzącej energii radiowej jest odbijana przez antenę transpondera, jak pokazano na rysunku 2.14. Na przekrój *odbicia* anteny transpondera można wpływać poprzez zmianę obciążenia podłączonego do anteny. Aby przesłać dane z tagu RFID do czytnika RFID, rezystor obciążenia podłączony równolegle do anteny tagu jest włączany i wyłączany w czasie przesyłanych danych. W ten sposób siła sygnału odbitego od transpondera może być modulowana. Nazywa się to *modulacją rozproszenia wstecznego*.

Sygnal z transpondera jest wypromienowywany w wolną przestrzeń. Część tego sygnału jest odbierana przez antenę czytnika RFID. Odbity sygnał trafia więc w kierunku wstecznym do anteny czytnika RFID. Można go oddzielić za pomocą *sprzęgacza kierunkowego*.

2.4.8 Bliskie pole a dalekie pole Transmisja

Istnieją dwa różne podejścia projektowe RFID do przesyłania energii z czytnika do tagu: indukcja magnetyczna i przechwytywanie fal elektromagnetycznych. Dwa projekty wykorzystują te podejścia i są nazywane bliskim i dalekim polem [1]:

- *RFID bliskiego zasięgu*

Technologia RFID bliskiego pola wykorzystuje indukcję magnetyczną między czytnikiem a transponderem. Podczas gdy RFID generuje pole magnetyczne w swojej lokalizacji, przepuszcza prąd zmienny przez cewkę odczytującą. Jeśli znacznik RFID z mniejszą cewką zostanie umieszczony w zasięgu czytnika, to

Pojawia się na nim zmienne napięcie, a na pole magnetyczne wpływają dane zapisane w tagu. Napięcie jest prostowane i zasila tag. Gdy jest zasilany, dane są wysyłane z powrotem do czytnika za pomocą modulacji obciążenia.

- *RFID dalekiego zasięgu*

Znaczniki wykorzystujące zasady dalekiego pola działają powyżej 100 MHz, zazwyczaj w zakresie 865–915 MHz do 2,45 GHz. Wykorzystują one zasadę działania sprzężenia zwrotnego. W dalekim polu sygnał czytnika jest odbijany i modulowany do zmiennej różnicy potencjałów w celu transmisji danych. Zasięg systemu jest ograniczony transmisją energii wysyłanej przez czytnik. Ze względu na postęp w produkcji półprzewodników, energia wymagana do zasilania tagu stale maleje. Możliwy maksymalny zasięg odpowiednio wzrasta.

2.4.9 Typowe zastosowania RFID w całym świecie

Aplikacje RFID zostały wdrożone na całym świecie, w tym:

- *Śledzenie żetonów w kasynach:* Niektóre kasyna umieszczają znaczniki RFID na swoich żetonach o wysokiej wartości, aby śledzić i wykrywać podrobione żetony, śledzić nawyki obstawiania poszczególnych graczy, przyspieszyć liczenie żetonów i określić błędy w liczeniu popełniane przez krupierów.
- *Identyfikacja zwierząt:* Używanie tagów RFID dla zwierząt jest jednym z najstarszych zastosowań RFID.

RFID zapewnia zarządzanie identyfikacją zwierząt na dużych rancach i w trudnym terenie. Wszczepialna odmiana znacznika RFID jest również używana do identyfikacji zwierząt.

- *Systemy inwentaryzacji:* Technologia RFID umożliwia szybkie i łatwe zarządzanie zapasami dla

firm. Umożliwia również śledzenie redukcji braków magazynowych, zwiększenie sprzedaży produktów, a także redukcję kosztów pracy, uproszczenie procesów biznesowych i zmniejszenie niedokładności zapasów.

- *Szpitalne sale operacyjne:* Korzystanie z czytnika RFID i jednorazowych gazików ze znacznikami RFID oraz Towels ma na celu poprawę bezpieczeństwa pacjentów i wydajności operacyjnej w szpitalach.

- *Ośrodki narciarskie:* Wiele ośrodków narciarskich zastosowało tagi RFID, aby zapewnić narciarzom dostęp bez użycia rąk

do wyciągów narciarskich. Umożliwia gromadzenie informacji, takich jak pokonane stopy w pionie i liczba jazdów, które mogą być również udostępnione użytkownikowi online.

- *Implanty dla ludzi:* Wszczepialne chipy RFID zaprojektowane do znakowania zwierząt są również wykorzystywane u ludzi.

2.5 Technologia Smart Card

Karta inteligentna zawiera wbudowany układ scalony, który może być jednostką pamięci z bezpiecznym mikrokontrolerem lub bez niego. Typowy system kart inteligentnych obejmuje karty, czytniki i system zaplecza. Karta inteligentna łączy się z czytnikiem za pomocą bezpośredniego kontaktu fizycznego (kontaktowa karta inteligentna) lub za pomocą zdalnego bezstykowego interfejsu RF (bezstykowa karta inteligentna). Czytnik łączy się z systemem zaplecza, który przechowuje i zarządza informacjami.

Motywacją dla kart inteligentnych jest to, że istnieje wyraźna potrzeba przenośnego zapisu wniosków, a zapisy te wymagają aktualizacji w czasie. Ważne jest również

bezpieczeństwo tych zapisów, zwłaszcza poufność i integralność. Karty intelligentne są obiecującymi rozwiązaniami w zakresie wydajnego przetwarzania i przesyłania danych oraz zapewniania bezpiecznych środowisk dla wielu aplikacji. Pod względem możliwości karty intelligentne dzielą się na dwie grupy: oparte na pamięci i mikroprocesorach (patrz sekcja 2.5.3). Karty intelligentne z wbudowanym bezpiecznym

Mikrokontroler może przechowywać dużą ilość danych i wykonywać własne funkcje na karcie, takie jak operacje związane z bezpieczeństwem i wzajemnym uwierzytelnianiem. Te karty inteligentne mogą intelligentnie współpracować z czytnikiem kart intelligentnych. Karty te mają własny system operacyjny (patrz sekcja 2.5.4). Podobnie, pod względem mechanizmu działania, karty intelligentne są podzielone na trzy grupy: stykowe, bezstykowe i hybrydowe karty intelligentne. Szczegóły dotyczące ogólnych funkcji i interfejsów zostały wyjaśnione w sekcji 2.5.5.

Karta intelligentna powinna być oczywiście zgodna z międzynarodowymi standardami. Istnieje wiele standardów i specyfikacji, które są istotne dla implementacji kart intelligentnych, a niektóre z nich są istotne dla aplikacji branżowych. Pełne organy normalizacyjne i specyfikacje kart intelligentnych to normy ISO/IEC, specyfikacje EMV 2000, federalny standard przetwarzania informacji 201 (FIPS 201), inne federalne standardy przetwarzania informacji, normy American National Standards Institute (ANSI), specyfikacje GlobalPlatform, specyfikacje Common Criteria (CC), Międzynarodowa Organizacja Lotnictwa Cywilnego (ICAO), Międzynarodowe Stowarzyszenie Linii Lotniczych i Transportu (IATA), G-8 Health Standards, The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191) Standards, Global System for Mobile Communication (GSM) Standards, Personal Computer/Smart Card (PC/SC) Workgroup Open Specifications, Open Card TM Framework, American Public Transportation Association's Contactless Fare Media System (CFMS) Standard oraz Biometric Standards [4].

2.5.1 Wcześniejsze formy kart intelligentnych: Pasek magnetyczny Karty

Proces dołączania paska magnetycznego do plastikowej karty został wynaleziony przez IBM w latach 60. ubiegłego wieku. Pasek magnetyczny to czarny lub brązowy pasek umieszczony zazwyczaj na karcie kredytowej lub na odwrocie biletu lotniczego lub karty tranzytowej. Pasek składa się z małekich częsteczek magnetycznych w żywicy. Częsteczki mogą być nakładane bezpośrednio na kartę lub mogą być wykonane w postaci paska na plastikowym podkładzie, który jest nakładany na kartę. Karty z paskiem magnetycznym umożliwiają przechowywanie danych. Karty te można odczytać poprzez fizyczny kontakt, przesuwając kartę na zewnętrznym urządzeniu, które ma magnetyczną głowicę odczytującą, jak pokazano na rysunku 2.15. Obecnie paski magnetyczne są najczęściej widoczne na finansowych kartach debetowych lub kredytowych, biletach lotniczych i kartach pokładowych.



Rysunek 2.15 Karta z paskiem magnetycznym.

Materiał użyty do produkcji częstek określa koercję paska. Koercja jest miarą trudności kodowania informacji na pasku magnetycznym. Miara koercji jest regulowana przez materiał użyty do wytworzenia częstek. Na przykład paski o niskiej koercji mogą wykorzystywać tlenek żelaza, a paski o wysokiej koercji mogą wykorzystywać ferryt baru. Zaletą wysokiej koercji jest to, że trudniej jest zakodować informacje na pasku. W związku z tym trudniej jest usunąć informacje z karty, więc problemy z przypadkowym usunięciem są wyeliminowane.

2.5.2 Ewolucja inteligentnych kart

Karty inteligentne zostały wynalezione w latach 70. ubiegłego wieku. Po raz pierwszy masowo wykorzystano je do płatności telefonicznych w latach 80-tych. W międzyczasie wprowadzono mikroprocesorowe karty inteligentne. Mikroprocesory zostały zintegrowane z kartami debetowymi w latach 90-tych. Systemy elektronicznych portmonetek oparte na kartach inteligentnych, które przechowują wartości na karcie i nie wymagają łączności sieciowej, zaczęły być używane w Europie od połowy lat 90-tych. Jedno z głównych ulepszeń w technologii kart inteligentnych miało miejsce w latach 90-tych; wprowadzono karty SIM oparte na kartach inteligentnych i zaczęto ich używać w środowiskach telefonów komórkowych opartych na GSM w Europie. Wykorzystanie kart inteligentnych wzrosło wraz z powszechnością telefonów komórkowych w Europie. W 1993 r. międzynarodowe marki płatnicze Europay, MasterCard i Visa (EMV) podjęły współpracę w celu opracowania nowych specyfikacji dla kart inteligentnych w celu wykorzystania ich w płatnościach zarówno jako karty debetowej, jak i kredytowej. Pierwsza wersja specyfikacji EMV, która jest skrótem od specyfikacji Europay, MasterCard i Visa, została wydana w 1994 roku. EMVCo zaktualizowało specyfikację w 2000 roku. Specyfikacja została ostatnio zaktualizowana w 2004 roku. Z wyjątkiem niektórych krajów, nastąpił znaczny postęp we wdrażaniu sprzętu zgodnego z EMV w punktach sprzedaży (POS), a także w wydawaniu kart debetowych i kredytowych przy użyciu specyfikacji EMV. W tym czasie zazwyczaj krajowe stowarzyszenie płatnicze każdego kraju było koordynowane przez MasterCard International, Visa International, American Express lub JCB. Wspólnie planowali i wdrażali systemy EMV, biorąc pod uwagę różnych interesariuszy. Wraz z wprowadzeniem specyfikacji i systemów EMV w całej Europie, płatności za pomocą systemów zbliżeniowych kart inteligentnych uległy znacznej poprawie. Z perspektywy technologii bezstykowych kart inteligentnych, głównym postępem było porozumienie Visa i MasterCard w latach 2004-2006 w celu wdrożenia płatności bezstykowych i aplikacji biletowych, takich jak transport masowy i opłaty za autostrady w USA. Wraz z wprowadzeniem bezstykowych kart inteligentnych, takich jak zbliżeniowa karta inteligentna MIFARE firmy Philips, aplikacje bezstykowych kart inteligentnych zaczęły mieć znaczny udział w rynku w Europie i Stanach Zjednoczonych.

2.5.3 Rodzaje kart inteligentnych: Klasyfikacja oparta na możliwościach

Karty inteligentne to plastikowe karty z wbudowanym mikroprocesorem i pamięcią. Niektóre karty inteligentne mają tylko nieprogramowalną pamięć, a zatem mają ograniczone możliwości. Karty inteligentne wyposażone w mikroprocesory mają różne funkcje. Karty inteligentne, pod względem ich możliwości, można podzielić na dwie główne grupy: karty inteligentne oparte na pamięci i karty inteligentne oparte na mikroprocesorach.

2.5.3.1 Karty inteligentne oparte na pamięci

Karty inteligentne oparte na pamięci mogą przechowywać wszelkiego rodzaju dane, w tym finansowe, osobiste i inne specjalne informacje. Nie mają one jednak możliwości



Rysunek 2.16 Przykładowa mikroprocesorowa karta inteligentna.

komunikują się z urządzeniem zewnętrznym, takim jak czytnik kart, przy użyciu protokołów synchronicznych do manipulowania danymi na karcie. Karty te są szeroko stosowane jako przedpłacone karty telefoniczne.

2.5.3.2 Karty inteligentne oparte na mikroprocesorach

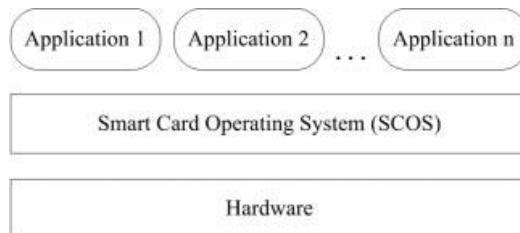
Karty inteligentne oparte na mikroprocesorach mają możliwości dynamicznego przetwarzania danych na karcie. Posiadają mikroprocesor oraz pamięć. Przykładową kartę mikroprocesorową pokazano na rysunku 2.16. Mikroprocesor na karcie zarządza alokacją pamięci i zarządzaniem danymi. Karty inteligentne oparte na mikroprocesorach są porównywalne z małymi komputerami, bez wewnętrznego źródła zasilania. Te karty inteligentne mają system operacyjny (OS), a mianowicie Smart Card Operating System (SCOS), umożliwiający zarządzanie danymi na karcie inteligentnej i pozwalający kartom inteligentnym być wielofunkcyjnymi. Mogą one przechowywać i przetwarzać informacje oraz wykonywać złożone obliczenia na przechowywanych danych. Mogą rejestrować, modyfikować i przetwarzać dane w przeciwnieństwie do kart inteligentnych opartych na pamięci. Ponadto karty inteligentne oparte na mikroprocesorach mają możliwość przechowywania dużej ilości danych w porównaniu z kartami pamięci.

2.5.4 System operacyjny kart inteligentnych (SCOS)

Do końca lat 90. bardzo trudno było mieć więcej niż jedną aplikację działającą na karcie inteligentnej ze względu na ograniczenia pamięci układów scalonych. Wraz z rozwojem SCOS, możliwe stało się wdrożenie kilku aplikacji, uruchamianie ich jednocześnie i ładowanie nowych w trakcie aktywnego życia karty. Obecnie SCOS umożliwiają bardziej dynamiczne platformy z wieloma aplikacjami i są uważane za naprawdę inteligentny i potężny bezpieczny obiekt obliczeniowy dla wielu nowych domen aplikacji.

Obecnie każda karta inteligentna ma swój własny SCOS, który można zdefiniować jako zestaw instrukcji osadzonych w pamięci ROM karty inteligentnej. SCOS są ogólnie podzielone na dwie kategorie

[5]: SCOS ogólnego przeznaczenia, który ma ogólny zestaw poleceń, w którym różne sekwencje obejmują większość aplikacji; oraz dedykowany SCOS, który ma polecenia zaprojektowane dla określonych aplikacji i może zawierać tylko powiązane aplikacje (np. inteligentną kartę płatniczą, która



Rysunek 2.17 Architektura kart inteligentnych [6].

została zaprojektowana do obsługi wyłącznie transakcji płatniczych). Architektura kart inteligentnych została przedstawiona na rysunku 2.17.

Podstawowe funkcje SCOS obejmują:

- Zarządzanie wymianą między kartą inteligentną a urządzeniem zewnętrznym, takim jak terminal POS.
- Zarządzanie danymi przechowywanymi w pamięci.
- Kontrola dostępu do informacji i funkcji.
- Zarządzanie bezpieczeństwem karty inteligentnej, zwłaszcza pod względem integralności danych.
- Zarządzanie cyklem życia karty inteligentnej od jej personalizacji do użytkowania i zakończenia.

Na wcześniejszym etapie ewolucji SCOS aplikacja lub usługa na karcie inteligentnej była napisana dla konkretnego systemu operacyjnego. W związku z tym wydawca karty musiał porozumieć się z konkretnym twórcą aplikacji, a także z systemem operacyjnym. Było to kosztowne i nieelastyczne rozwiązanie. Konsumenti musieli nosić różne karty inteligentne dla każdej usługi. Obecnie trend zmierza w kierunku otwartego systemu operacyjnego, który obsługuje wiele aplikacji działających na jednej karcie inteligentnej. Obecnie najbardziej znany system operacyjny, który mają większą ekspozycję na rynku, są MULTOS i JavaCard OS [5,6].

2.5.4.1 MULTOS

MULTOS (Multi-application Operating System) to system operacyjny dla kart inteligentnych, który jest jednym z idealnych rozwiązań OS z ulepszonymi funkcjami bezpieczeństwa. MULTOS jest kontrolowany przez przemysłowe konsorcjum MULTOS, które obejmuje podmioty od producentów chipów i krzemów kart inteligentnych po dostawców systemów zarządzania kartami i personalizacji.

MULTOS ma na celu zapewnienie standardowego bezpiecznego SCOS, który mógłby zostać zaimplementowany na dowolnym chipie krzemowym i wykonywać dowolną aplikację karty inteligentnej (np. płatności, tożsamość, bilety). W związku z tym różne aplikacje mogą być uruchamiane i działać na tej samej karcie inteligentnej niezależnie i bezpiecznie. Zapewnia to połączenie różnych aplikacji od różnych dostawców i wszystkie mogą istnieć niezależnie od siebie.

Jedną z kluczowych różnic MULTOS w porównaniu z innymi SCOS jest to, że jest on specjalnie zaprojektowany do bezpiecznych aplikacji. Implementuje on Secure Trusted

Environment Provisioning (STEP), który jest opatentowanym ^{zasięgu} mechanizmem. STEP umożliwia produkcję, wydawanie i dynamiczne aktualizacje inteligentnych kart MULTOS pod kontrolą wydawcy karty, co jest możliwe dzięki MULTOS Key Management Authority (KMA). KMA zapewnia wydawcom kart wymaganą kryptografię.

dane, aby wydawcy kart mogli przejąć kontrolę nad kartą inteligentną i wygenerować certyfikaty uprawnień do zarządzania aplikacjami.

2.5.4.2 JavaCard OS

Kolejnym nowym trendem w SCOS jest system operacyjny JavaCard. JavaCard umożliwia uruchamianie aplikacji (lub appletów) napisanych w języku JavaCard (podzbiór języka programowania Java) na kartach inteligentnych. Technologia ta jest standaryzowana przez Sun Microsystems i JavaCard Forum.

JavaCard zapewnia bezpieczną, interoperacyjną i wieloaplikacyjną platformę dla kart inteligentnych, wykorzystując zalety języka Java: programowanie obiektowe, ponowne wykorzystanie istniejących środowisk programistycznych, język silnie typowany, kilka poziomów kontroli dostępu do metod i zmiennych oraz interoperacyjność. Oznacza to, że aplikacje oparte na JavaCard OS mogą być używane na kartach inteligentnych dowolnego producenta, które obsługują JavaCard OS. JavaCard OS daje programistom niezależność od architektury.

Kolejną zaletą systemu operacyjnego JavaCard jest to, że umożliwia on późniejsze wydawanie aplikacji. Pozwala to na uaktualnianie i aktualizowanie aplikacji na karcie inteligentnej po dostarczeniu karty do użytkownika końcowego, gdy jest to konieczne. JavaCard OS posiada maszynę wirtualną JavaCard Virtual Machine (JCVM), która umożliwia uruchamianie aplikacji napisanych w języku programowania Java. Część JCVM działa poza kartą jako konwerter, a inna część działa na karcie jako interpreter kodu bajtowego. W związku z tym w JavaCard wiele zadań nie jest wykonywanych podczas wykonywania, ale jest przekazywanych do części maszyny wirtualnej poza kartą (np. ładowanie klas, weryfikacja kodów bajtowych, rozwiązywanie powiązań i optymalizacja).

2.5.5 Rodzaje kart inteligentnych: Klasyfikacja oparta na mechanizmach

Karty inteligentne dzielą się na trzy główne grupy pod względem mechanizmu komunikacji z urządzeniami zewnętrznymi: stykowe karty inteligentne, bezstykowe karty inteligentne i modele hybrydowe.

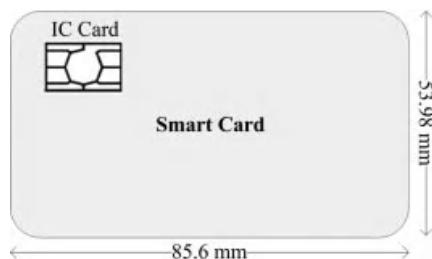
2.5.5.1 Kontakt Smart Cards

Stykowe karty inteligentne są osadzone w mikro module zawierającym pojedynczą krzemową "kartę IC" (lub kartę chipową) z pamięcią i mikroprocesorem. Ta karta IC jest przewodzącą płytą stykową o długości około 1 cm^2 ($0,16 \text{ cala}^2$) umieszczoną na powierzchni karty inteligentnej, która jest zazwyczaj pozłacana. Urządzenie zewnętrzne zapewnia bezpośrednie połączenie elektryczne z przewodzącą płytą stykową po włożeniu do niej stykowej karty inteligentnej. Transmisja poleceń, danych i informacji o stanie karty odbywa się za pośrednictwem tych fizycznych punktów styku.

Karty nie zawierają żadnego źródła zasilania; dlatego energia jest dostarczana przez urządzenie zewnętrzne, z którym karta wchodzi w interakcję. Te urządzenia zewnętrzne są używane jako medium komunikacyjne między stykową kartą inteligentną a hostem. Urządzeniem zewnętrznym może być komputer, terminal POS lub urządzenie mobilne. Stykowe karty inteligentne współpracujące z urządzeniami POS są wykorzystywane do celów płatniczych. Wymiary stykowej karty inteligentnej do celów płatniczych są znormalizowane jako

$85,6 \text{ mm} \times 53,98 \text{ mm} \times 0,76 \text{ mm}$, podobnie jak obecne karty bankowe (patrz rysunek

2.18). Karty te posiadają również pasek magnetyczny. W rzeczywistości karty IC używane w kontaktowych kartach inteligentnych do celów płatniczych są takie same jak te używane w modułach identyfikacji abonenta (SIM) w kartach płatniczych.

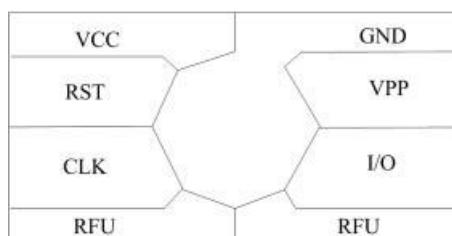


Rys. 2.18 Standardowe wymiary finansowych stykowych kart inteligentnych.

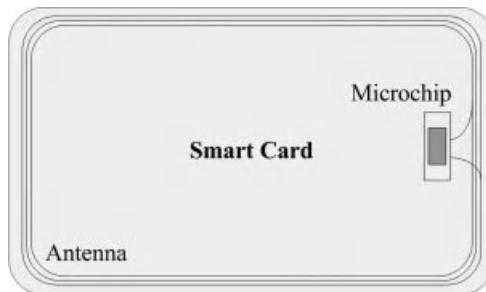
telefony komórkowe. Są one inaczej zaprogramowane i osadzone w innym kawałku PVC. Karty te współpracują z zewnętrznymi czytnikami, takimi jak telefony komórkowe. Fizyczny kształt modułów SIM z kartami IC może różnić się od kart bankowych i zazwyczaj są one mniejsze. Stykowe karty inteligentne mogą być używane poprzez włożenie ich do czytnika.

Normy związane ze stykowymi kartami inteligentnymi to ISO/IEC 7810 i głównie ISO/IEC 7816. Określają one fizyczny kształt i charakterystykę stykowych kart inteligentnych, pozycje i kształty złączy elektrycznych, charakterystykę elektryczną, protokoły komunikacyjne, w tym polecenia wymieniane z kartą, oraz podstawową funkcjonalność. Zgodnie z normą ISO/IEC 7816, karta IC ma na swojej powierzchni osiem poziaczanych styków elektrycznych (patrz rysunek 2.19): VCC (napięcie zasilania), RST (reset mikroprocesora), CLK (sygnał zegarowy), GND (masa), VPP (napięcie programowania lub zapisu) oraz I/O (linia wejścia/wyjścia szeregowego). Tylko styki I/O i GND są obowiązkowe na typowej karcie inteligentnej; pozostałe są opcjonalne. Dwa styki są zarezerwowane do wykorzystania w przyszłości (RFU). Wykorzystanie ścieżek komunikacyjnych od C1 do C8 to [4,7]:

- C1: VCC to napięcie zasilania, które napędza chipy i zazwyczaj wynosi 5 V. Można przewidzieć chipy, które pozwalają na niższe zużycie energii.
- C2: RST to linia sygnału resetowania, która inicjuje stan układu scalonego po włączeniu zasilania.
- C3: CLK jest sygnałem zegarowym, który steruje logiką ICC i jest również używany jako sygnał odniesienia dla łącza komunikacji szeregowej. Linia ta kontroluje prędkość działania i zapewnia wspólne ramy dla komunikacji danych między urządzeniem interfejsu (IFD) a układem scalonym (ICC).
- C4: RFU.
- C5: GND odnosi się do linii sygnału masy, która zapewnia wspólną masę elektryczną między IFD a ICC.



Rysunek 2.19 Pola stykowe na karcie IC.



Rysunek 2.20 Bezstykowa karta inteligentna.

- C6: VPP to połączenie zasilania lub wejście napięcia programowania, które jest używane dla sygnału wysokiego napięcia, który jest niezbędny do zaprogramowania pamięci EEPROM. Do późnych lat 80-tych konieczne było zastosowanie zewnętrznego napięcia do programowania i kasowania pamięci EEPROM, ponieważ mikrokontrolery używane w tym czasie nie miały pomp ładowających. Jednak od początku lat 90. standardową praktyką jest generowanie tego napięcia bezpośrednio z układu scalonego za pomocą pompy ładowającej, więc ten styk nie jest już używany. Styk C6 nie może być wykorzystywany do żadnej innej funkcji, w przeciwnym razie byłby sprzeczny ze standardem ISO. C6 znajduje się dokładnie pośrodku między stykiem GND i I/O, więc C6 nie jest ani używany, ani eliminowany.
- C7: I/O to szeregowe złącze wejścia/wyjścia, które zapewnia kanał komunikacji półdupleksowej. między czytnikiem kart a kartą inteligentną. Ta linia sygnałowa jest używana do komunikacji i wysyłania poleceń do chipa w karcie inteligentnej. Protokoły używane do komunikacji z kartą inteligentną są określane jako T0 i T1.
- C8: RFU.

2.5.5.2 Bezstykowe karty inteligentne

Bezstykowa karta inteligentna to rodzaj karty inteligentnej, która jest przetwarzana bez konieczności kontaktu z urządzeniem zewnętrznym. Jest to połączenie wbudowanego mikroprocesora (lub układu scalonego) i anteny, która umożliwia śledzenie karty (patrz rysunek 2.20). Antena ta składa się z kilku przewodów. W bezstykowych kartach inteligentnych informacje są przechowywane w mikrochipie, który ma bezpieczny mikrokontroler i pamięć wewnętrzną. W przeciwieństwie do stykowej karty inteligentnej, zasilanie bezstykowej karty inteligentnej odbywa się za pomocą wbudowanej anteny na karcie inteligentnej. Wymiana danych między kartą inteligentną a urządzeniem zewnętrznym, takim jak czytnik kart inteligentnych, odbywa się za pomocą tej anteny. Pola elektromagnetyczne zapewniają zasilanie karty, a także wymianę danych z urządzeniem zewnętrznym.

Bezstykowe karty inteligentne umożliwiają bezpieczne przechowywanie danych i zarządzanie nimi. Zapewniają również dostęp do danych przechowywanych na karcie; wykonują funkcje na karcie, takie jak umożliwienie wzajemnego uwierzytelniania. Mogą łatwo i bezpiecznie współpracować z zewnętrznym czytnikiem zbliżeniowym.

Komunikacja bezstykowa może być realizowana tylko z urządzeniami znajdującymi się w bliskiej odległości. Czytniki z możliwością odczytu RFID są oznaczone specjalnym symbolem, jak pokazano na rysunku 2.21. Zarówno urządzenie zewnętrzne, jak i bezstykowa karta inteligentna mają antenę i komunikują się za pomocą technologii RF z

NFC Szybkością transmisji danych 106-848 kb/s. Większość kart bezstykowych pobiera również zasilanie dla mikroprocesora z tego sygnału elektromagnetycznego.



Rysunek 2.21 Symbol uniwersalnego czytnika zbliżeniowych kart inteligentnych.

Gdy bezstykowa karta inteligentna znajdzie się w polu elektromagnetycznym czytnika kart, rozpoczyna się transfer energii z czytnika kart do mikroprocesora na karcie intelligentnej. Mikroprocesor jest zasilany sygnałem przychodzący z czytnika kart. Gdy mikroprocesor jest zasilany, nawiązywana jest komunikacja bezprzewodowa między kartą intelligentną a czytnikiem kart w celu przesyłania danych.

Technologia bezstykowych kart intelligentnych jest wykorzystywana w aplikacjach, które przetwarzają prywatne informacje, takie jak dane zdrowotne i dane tożsamości, które mają być chronione. Jest również wykorzystywana w aplikacjach, w których wymagane są szybkie i bezpieczne transakcje, takie jak płatności za przejazd, paszporty elektroniczne i kontrola wizowa. Bezstykowe karty intelligentne są często używane do transakcji bez użycia rąk. Aplikacje korzystające z bezstykowych kart intelligentnych muszą obsługiwać wiele funkcji bezpieczeństwa, takich jak wzajemne uwierzytelnianie, silne bezpieczeństwo informacji dzięki dynamicznym kluczom kryptograficznym, silne bezpieczeństwo urządzeń bezstykowych i prywatność poszczególnych informacji. Technologia bezstykowych kart intelligentnych jest dostępna w różnych formach, takich jak karty plastikowe, zegarki, breloki do kluczy, dokumenty, telefony komórkowe i inne urządzenia mobilne lub słuchawki.

Obecnie istnieją trzy różne główne standardy dla bezstykowych kart intelligentnych oparte na szerokim zakresie klasyfikacji: ISO/IEC 10536, ISO/IEC 14443 i ISO/IEC 15693:

(i) *ISO/IEC 10536 - Karty intelligentne z bliskim sprzężeniem*

Norma ISO/IEC 10536 zatytułowana "Identification Cards - Contactless Integrated Circuit Cards" (Karty identyfikacyjne - bezstykowe karty z układem scalonym) opisuje strukturę i parametry operacyjne bezstykowych kart intelligentnych z bliskim sprzężeniem. Karty te działają w odległości do 1 cm. Norma ta składa się z czterech części: charakterystyka fizyczna, wymiary i lokalizacja obszarów sprzężenia, sygnał elektryczny i procedury resetowania oraz reakcja na reset i protokoły transmisji.

(ii) *ISO/IEC 14443 - Karty intelligentne ze sprzężeniem zbliżeniowym*

Norma ISO/IEC 14443 zatytułowana "Identification Cards - Proximity Integrated Circuit Cards" opisuje metodę działania i parametry operacyjne bezstykowych kart intelligentnych ze złączem zbliżeniowym. Zgodnie z tą normą zbliżeniowa karta intelligentna działa w odległości mniejszej niż 10 cm przy częstotliwości 13,56 MHz. Szczegóły tego standardu wyjaśniono w rozdziale 3.

(iii) *ISO/IEC 15693 - Karty intelligentne ze złączem Vicinity Coupling*

Norma ISO/IEC 15693 zatytułowana "Identification Cards - Contactless Integrated Circuit Cards - Vicinity Cards" opisuje sposób działania i parametry operacyjne bezstykowych kart intelligentnych ze sprzężeniem zbliżeniowym. Te karty intelligentne działają w zasięgu do 1 m przy częstotliwości 13,56 MHz, podobnie jak te używane w systemach kontroli dostępu. Standard ten składa się z czterech części: charakterystyki fizycznej, inicjalizacji interfejsu radiowego, protokołów antykolizyjnych i protokołu transmisji.

Tabela 2.3 Niektóre nowe zastosowania kart inteligentnych

Obszary zastosowań	Przykłady
<i>Finanse</i>	Elektroniczne portmonetki zastępujące monety przy drobnych zakupach Kredytowe i debetowe karty płatnicze
<i>Komunikacja</i>	Karty SIM GSM, które są popularne do bezpiecznej komunikacji
<i>Identyfikacja i fizyczna kontrola dostępu</i>	Karty dostępu dla pracowników z zabezpieczonymi identyfikatorami i hasłami Legitymacje studenckie lub karty kampusowe, które mogą mieć różne zastosowania, takie jak uwierzytelnianie, elektroniczna portmonetka, karta biblioteczna i karta na posiłki.
<i>Transport</i>	Systemy pobierania opłat za transport zbiorowy Prawa jazdy Elektroniczne systemy poboru opłat
<i>Lojalność konsumentów</i>	Karty członkowskie lub lojalnościowe do systemów śledzenia nagród dla
<i>Zdrowie</i>	Karty zdrowia do przechowywania ubezpieczenia i danych medycznych użytkownika w nagłych wypadkach

2.5.5.3 Modele hybrydowe

Ponadto można zobaczyć hybrydowe modele kart inteligentnych, takie jak karty z dwoma interfejsami i karty hybrydowe:

- Karta z podwójnym interfejsem ma zarówno interfejs stykowy, jak i bezstykowy, który zawiera tylko jeden chip. Taki model umożliwia dostęp do tego samego chipa zarówno przez interfejs stykowy, jak i bezstykowy z wysokim poziomem bezpieczeństwa.
- Karta hybrydowa zawiera dwa chipy. Jeden z tych chipów jest używany do interfejsu stykowego, a drugi Drugi jest używany do interfejsu bezstykowego. Chipy te są niezależne i nie są ze sobą połączone.

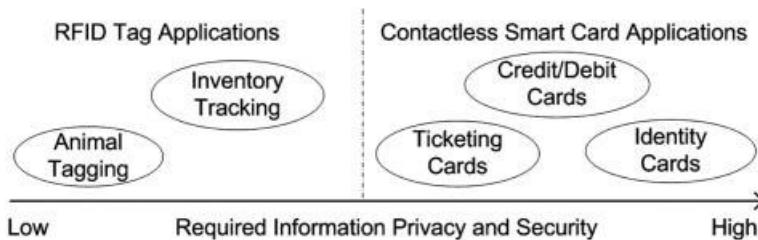
2.5.6 Karta inteligentna Aplikacje

Pierwszymi kartami inteligentnymi były przedpłacone karty telefoniczne wdrożone w Europie w połowie lat 80-tych. Były to proste karty inteligentne z pamięcią. Obecnie niektóre z głównych obszarów zastosowań kart inteligentnych opartych na mikroprocesorach to finanse, komunikacja, identyfikacja i fizyczna kontrola dostępu, transport, lojalność i opieka zdrowotna. Karta inteligentna może przenosić aplikacje z więcej niż jednego obszaru, np. łącząc na tej samej karcie fizyczne zabezpieczenia dostępu, aplikacje finansowe i lojalnościowe. Niektóre główne obszary zastosowań kart inteligentnych i ich przykłady przedstawiono w tabeli 2.3.

2.6 Porównanie tagów RFID i inteligentnych kart zbliżeniowych

Obecnie wiele aplikacji wykorzystuje technologię RF do automatycznej identyfikacji obiektów i osób. Zastosowania te obejmują śledzenie zwierząt i produktów w celu umożliwienia szybkich płatności i bezpiecznej identyfikacji osób. Wszystkie te aplikacje wykorzystują fale radiowe, aby umożliwić bezprzewodową komunikację i transfer danych.

Aplikacje te różnią się jednak wykorzystywana technologią RF w zależności od wymagań aplikacji [8]. Zgodnie z ogólną definicją, technologia RFID wykorzystuje znaczniki RFID w aplikacjach, które identyfikują lub śledzą obiekty, podczas gdy bezstykowe karty inteligentne



Rysunek 2.22 Znacznik RFID a aplikacje bezstykowych kart inteligentnych.

wykorzystuje zbliżeniowe karty inteligentne w aplikacjach, które identyfikują ludzi lub przechowują informacje finansowe i osobiste.

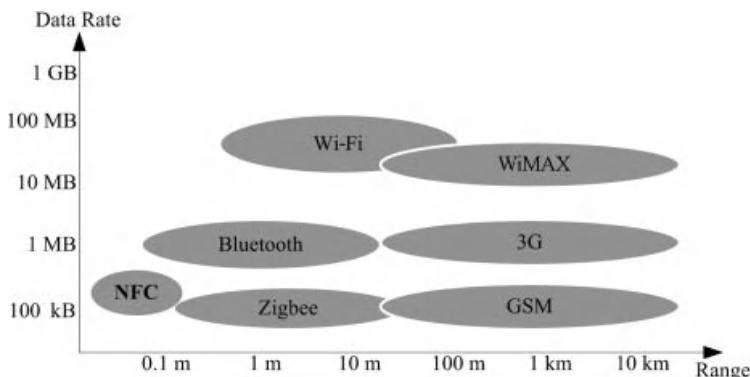
Jak już wspomniano, znaczniki RFID są głównymi komponentami systemów RFID. Są one proste, tanie i jednorazowe. Są one wykorzystywane w różnych projektach, takich jak identyfikacja zwierząt i logistyczne śledzenie towarów, a także zastępują drukowane kody kreskowe w sklepach detalicznych. Tagi RFID zawierają układ scalony, który zazwyczaj przechowuje dane statyczne oraz antenę, która umożliwia chipowi przesyłanie przechowywanych danych do czytnika. Gdy tag znajdzie się w zasięgu czytnika RFID, dane przechowywane na tagu są przesyłane do czytnika. Dane na tagu lub przesyłane między tagiem a czytnikiem nie są zabezpieczone ani uwierzytelniane. W ten sposób każdy czytnik wykorzystujący odpowiedni sygnał RF może uzyskać zawartość tagu RFID. Typowe tagi RFID mogą być łatwo odczytywane z odległości od kilku centymetrów do kilku metrów, co umożliwia łatwe śledzenie obiektów w zależności od używanego typu tagu.

Podobnie jak znaczniki RFID, bezstykowe karty inteligentne również intelligentnie współpracują z urządzeniem zewnętrznym przy użyciu technologii RF. Jednak bezstykowe karty inteligentne są używane w aplikacjach, które wymagają wysokiego poziomu bezpieczeństwa w celu ochrony poufnych informacji i przeprowadzania bezpiecznych transakcji. Jak już wspomniano, bezstykowa karta inteligentna zawiera bezpieczny mikrokontroler i pamięć wewnętrzną. Ma również możliwość wykonywania złożonych funkcji (np. szyfrowania lub innych funkcji bezpieczeństwa) oraz bezpiecznego zarządzania, przechowywania i zapewniania dostępu do danych na karcie. Aplikacje wymagające wysokiego poziomu bezpieczeństwa (np. aplikacje płatnicze, identyfikatory rządowe, paszporty elektroniczne) wykorzystują technologię bezstykowych kart inteligentnych. W takich zastosowaniach preferowana jest zazwyczaj odległość około 10 cm (4 cale). Aplikacje, które wymagają większych odległości odczytu, mogą wykorzystywać inne rodzaje technologii bezstykowych, takie jak zbliżeniowe bezstykowe karty inteligentne. Aplikacje wykorzystujące bezstykowe karty inteligentne zapewniają integralność i poufność danych oraz prywatność przechowywanych lub przesyłanych informacji. W porównaniu z tagami RFID, technologia bezstykowych kart inteligentnych jest idealnym rozwiązaniem dla aplikacji wymagających bezpieczeństwa i prywatności.

Aplikacje często mają różne wymagania i możliwości w zakresie korzystania z technologii RF. Rysunek 2.22 podsumowuje rodzaje technologii wykorzystywanych w niektórych kluczowych zastosowaniach oraz poziom ochrony informacji, jaki zapewniają. Na przykład, w aplikacjach śledzenia zapasów i znakowania zwierząt, tagi RFID przechowują informacje, takie jak numer identyfikacyjny lub kod elektroniczny, który nie ma wysokiej czułości. Dlatego nie wymagają one wysokiego poziomu bezpieczeństwa i prywatności w porównaniu z aplikacjami bezstykowych kart inteligentnych.

2.7 Więcej na NFC

Technologia NFC została opracowana wspólnie przez firmy Philips⁷ i Sony pod koniec 2002 roku na potrzeby komunikacji bezstykowej. Europejskie stowarzyszenie ECMA (European Computer Manufacturers Association) International



Rysunek 2.23 Porównanie technologii bezprzewodowych w oparciu o zasięg i szybkość wymiany danych.

przyjęła tę technologię jako standard w grudniu 2002 roku. Międzynarodowa Organizacja Normalizacyjna (ISO) i Międzynarodowa Komisja Elektrotechniczna (IEC) przyjęły technologię NFC w grudniu 2003 roku. W 2004 roku Nokia, Philips i Sony założyły NFC Forum w celu promowania tej technologii. Standardy technologii NFC są uznawane przez ISO/IEC (Międzynarodową Organizację Normalizacyjną/Międzynarodową Komisję Elektrotechniczną), ETSI (Europejski Instytut Norm Telekomunikacyjnych) i ECMA. Inne organizacje uczestniczące w standaryzacji technologii NFC i urządzeń NFC zostały szczegółowo omówione w rozdziale 3.

NFC to dwukierunkowa technologia komunikacji bezprzewodowej krótkiego zasięgu. Komunikacja odbywa się między dwoma urządzeniami zgodnymi z NFC w odległości kilku centymetrów. Wykorzystywany jest sygnał 13,56 MHz o przepustowości nie większej niż 424 kbps. Technologia NFC działa w różnych trybach operacyjnych: czytnik/zapis, peer-to-peer i emulacja karty, w których komunikacja odbywa się odpowiednio między urządzeniem mobilnym NFC po jednej stronie a pasywnym tagiem RFID (tagiem NFC), urządzeniem mobilnym NFC lub czytnikiem NFC po drugiej stronie. Każdy tryb pracy wykorzystuje różne interfejsy komunikacyjne (tj. interfejsy ISO/IEC 14443, FeliCa, NFCIP-1) w warstwie RF, a także ma różne wymagania techniczne, operacyjne i projektowe, które zostały wyraźnie przedstawione w rozdziale 3.

Technologia NFC jest porównywana z innymi technologiami [9] pod względem szybkości przesyłania danych na rysunku 2.23 oraz pod względem bezpieczeństwa, personalizacji, elastyczności i zużycia energii w tabeli 2.4.

W technologii NFC urządzenie generuje pole fal radiowych o niskiej częstotliwości w paśmie 13,56 MHz. Gdy inne urządzenie NFC zbliży się na tyle, by zetknąć się z tym polem, następuje magnetyczne sprzężenie indukcyjne.

Tabela 2.4 Porównanie NFC z innymi technologiami bezprzewodowymi [10]

Parametr	RFID	Bluetooth	ZigBee	NFC
Bezpieczeństwo	Wysoki	Niski	Niski	Wysoki
Personalizacja	Wysoki	Średni	Niski	Wysoki
Elastyczność	Niski	Wysoki	Wysoki	Wysoki
Zużycie energii	Nie	Wysoki	Średni	Niski

przesyła energię i dane z jednego urządzenia do drugiego. Urządzenie NFC z wewnętrznym zasilaniem jest uważane za aktywne, podczas gdy urządzenie bez wewnętrznego zasilania, takie jak karta inteligentna, jest uważane za pasywne. Sprzężenie indukcyjne powoduje, że urządzenie pasywne pochłania energię z urządzenia aktywnego, gdy znajdzie się wystarczająco blisko. Po włączeniu zasilania urządzenie pasywne może komunikować się i wymieniać dane z drugim urządzeniem.

Do tej pory na całym świecie przeprowadzono wiele testów NFC, zwłaszcza w dziedzinie płatności. We wszystkich testach stwierdzono, że wraz z rozwojem technologii NFC telefon komórkowy stanie się bezpieczniejszy, wygodniejszy, szybszy i bardziej modny. Technologia NFC pozwala ludziom zintegrować karty, których używają na co dzień, takie jak karty lojalnościowe i kredytowe, z ich telefonami komórkowymi. Oprócz integracji kart z urządzeniami mobilnymi, technologia NFC wprowadza innowacje do komunikacji mobilnej. Umożliwia ona dwóm użytkownikom łatwą komunikację i wymianę danych poprzez zetknięcie ze sobą dwóch telefonów komórkowych. Co więcej, technologia NFC daje telefonom komórkowym możliwość korzystania z czytników NFC, dzięki czemu NFC może być przez nie odczytywane. Rosnąca moc obliczeniowa telefonów komórkowych, dostęp do Internetu i wiele innych funkcji zyskują dzięki tej funkcji czytnika, która doprowadzi do powstania nowych i innowacyjnych usług. Prawdą jest, że technologia NFC upraszcza transakcje, zapewnia łatwe dostarczanie treści i umożliwia udostępnianie informacji. Jednocześnie stwarza nowe możliwości dla różnych interesariuszy; operatorzy telefonii komórkowej, banki, operatorzy transportu i sprzedawcy prawdopodobnie będą mieli szybsze transakcje, mniej obsługi gotówki i nowe usługi operatora.

2.7.1 Nieodłączne funkcje bezpieczeństwa i parowania NFC

Jedną z głównych właściwości technologii NFC jest jej ukryte bezpieczeństwo ze względu na niewielką odległość komunikacji. Bliskość dwóch urządzeń sprawia, że prawdopodobieństwo przechwycenia sygnału jest bardzo niskie. Inną właściwością NFC jest możliwość niejawnego parowania. Aplikacja zainstalowana na urządzeniu mobilnym jest automatycznie uruchamiana po znalezieniu pasującej pary. Rozważmy aplikację, która odczytuje zdarzenia koncertowe z tagu NFC. Aplikacja ta może zostać zaprogramowana tak, aby uruchamiała się natychmiast i automatycznie po dotknięciu telefonu komórkowego tagiem NFC, który zawiera informacje o wydarzeniu. Może ona wykonywać całe przetwarzanie, dopóki nie będzie wymagana interwencja użytkownika. Jeśli interwencja użytkownika nie jest potrzebna zgodnie z wbudowanym algorytmem, aplikacja może zakończyć swoje procesy i wyjść. W takim przypadku użytkownik może nawet nie zauważyc, że aplikacja została uruchomiona, przetworzona i zakończona. Ten rodzaj przetwarzania nie jest odpowiedni dla usług wymagających bezpieczeństwa. Na przykład w przypadku płatności, interwencja użytkownika jest niezbędna, a płatność nie może być kontynuowana bez zgody użytkownika i bez wprowadzenia szczegółów, takich jak hasło płatności. Automatyczne uruchamianie aplikacji NFC umożliwia automatyczne parowanie powiązanych komponentów NFC, co nie jest prawdą w przypadku Bluetooth. Użytkownik pokazuje zamiar automatycznego parowania, zbliżając swoje urządzenie do drugiego urządzenia. Aby pokazać intencję w komunikacji peer-to-peer, dwóch użytkowników musi zbliżyć do siebie swoje urządzenia. Tak więc parowanie dwóch urządzeń NFC jest zupełnie inne niż procesy wymagane w Bluetooth. Należy pamiętać, że parowanie urządzeń w Bluetooth obejmuje wyszukiwanie, oczekiwanie, parowanie i autoryzację.

2.8 Rozdział Podsumowanie

Wszechobecna informatyka odnosi się do kolejnego poziomu interakcji między ludźmi a

NFC komputerami, w którym urządzenia komputerowe są całkowicie zintegrowane z naszym codziennym życiem. NFC jest głównie

uważana za ważny krok w kierunku wszechobecnej informatyki. NFC wykorzystuje paradygmat dotykowy do interakcji. Użytkownicy muszą dotknąć swoich telefonów komórkowych do czytnika lub tagu w celu nawiązania połączenia. NFC jest rozszerzeniem technologii RFID i jest kompatybilne z interfejsami technologii bezstykowych kart inteligentnych.

Technologia RFID jest wykorzystywana do znakowania i identyfikacji obiektów na dużych odległościach. System RFID zazwyczaj składa się z dwóch głównych elementów: transpondera, który jest umieszczany na obiekcie, który ma zostać zidentyfikowany; oraz czytnika, który ma możliwość odczytu i/lub zapisu. Transponderami są zazwyczaj tagi RFID (pasywne lub aktywne).

Technologia bezstykowych kart inteligentnych wykorzystuje bezstykowe karty intelligentne, które muszą chronić prywatne informacje, a także wykonywać szybkie i bezpieczne transakcje. Niektóre przykłady kart inteligentnych to weryfikacja tożsamości, karty płatnicze i paszporty elektroniczne. Główne standardy dla bezstykowych kart inteligentnych to ISO/IEC 10536 dla kart zbliżeniowych, ISO/IEC 14443 dla kart zbliżeniowych oraz ISO/IEC 15693 dla kart zbliżeniowych.

Technologia NFC została zdefiniowana przez NFC Forum założone przez firmy Nokia, Philips i Sony, które umożliwiają komunikację w oparciu o technologię RFID i infrastrukturę ISO/IEC 14443. Działa w trzech trybach (czytnik/zapis, peer-to-peer i emulacja karty) z częstotliwością radiową 13,56 MHz, gdzie komunikacja odbywa się z jednej strony między telefonem komórkowym z funkcją NFC, a z drugiej strony odpowiednio pasywnym tagiem RFID, urządzeniem NFC lub czytnikiem NFC.

Głównymi właściwościami technologii NFC są automatyczne parowanie i ukryte bezpieczeństwo dzięki możliwości komunikacji na krótkich dystansach. W porównaniu z innymi technologiami bezprzewodowymi, pozwala ona na przesyłanie danych z niską prędkością na bardzo bliskie odległości. Jest bardziej zorientowana na człowieka, łatwa, szybka i zapewnia wysoki poziom bezpieczeństwa i prywatności.

Rozdział Pytania

1. Wyjaśnij wszechobecne komputery i ich związek z NFC.
2. Jakie są podobieństwa i różnice między kodem QR a technologią RFID?
3. Wyjaśnij różnicę między aktywnymi i pasywnymi tagami RFID.
4. Jakie są różnice między transmisją bliskiego i dalekiego pola w odniesieniu do transferu energii między urządzeniem aktywnym i pasywnym?
5. Jakie są różnice między kartami intelligentnymi opartymi na pamięci i mikroprocesorze?
6. Jakie są różnice między kartami mikroprocesorowymi a komputerami PC?
7. Przed jakimi wyzwaniami stoi mobilny system operacyjny, a przed jakimi nie stoi system operacyjny dla komputerów PC?
8. Narysuj symbol uniwersalnego czytnika bezstykowych kart intelligentnych.
9. Jakie są różnice między kartami zbliżeniowymi a kartami intelligentnymi ze sprzężeniem zbliżeniowym?
10. Jakie są różnice między tagami RFID a zbliżeniowymi kartami intelligentnymi?
11. Jakie są najważniejsze integralne właściwości technologii NFC?

Referencje

- [1] Resarsch, F. (2010) *Ubiquitous Computing, Developing and Evaluating Near Field Communication Applications*, Gabler, ISBN: 978-3-8349-2167-3.
- [2] Finkenzeller, K. (2010) *RFID Handbook. Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification*, Wiley, ISBN: 978-0-470-54910-3.

W kierunku ery

NFC Frequency Identification and Near-Field Communication, John Wiley & Sons, Ltd, ISBN: 978-0-470-69506-

7.

- [3] Dressen, D. (2004) Rozważania na temat wyboru technologii RFID. *Atmel Applications Journal*, 3, 45-47.

- [4] Smart Card Alliance, <http://www.smartcardalliance.org/> (dostęp: 10 lipca 2011 r.).
- [5] Cardwerk, <http://www.cardwerk.com/smartcards/> (dostęp: 10 lipca 2011 r.).
- [6] Sauveron, D. (2009) Multiapplication smart card: W kierunku otwartej karty inteligentnej? *Information Security Technical Report*, **14**(2), 70-78.
- [7] Leng, X. (2009) Smart card applications and security. *Information Security Technical Report*, **14**(2), 36-45.
- [8] Smart Card Alliance, *Tagi RFID i technologia bezstykowych kart inteligentnych: Porównanie i zestawienie zastosowań i możliwości.* Dostępny pod adresem: http://www.hidglobal.com/documents/tagsVsSmartcards_wp_en.pdf (dostęp 10 lipca 2011).
- [9] NFC Forum, <http://www.nfc-forum.org/> (dostęp: 10 lipca 2011 r.).
- [10] Chang, Y. et al. (2010) NCASH: Spersonalizowane środowisko inteligentnego domu z obsługą telefonu NFC, *Cybernetics and Systems*, **41**(2), 123-145.

3

Podstawy NFC

Jesteśmy teraz gotowi, aby zapewnić czytelnikowi dogłębny wgląd w techniczne podstawy NFC. Najpierw przedstawiamy podstawową strukturę NFC i jej urządzenia (tag NFC, czytnik NFC i telefon komórkowy z obsługą NFC). Ważne jest również zrozumienie organów normalizacyjnych, które sterują technologią NFC. Różne organy normalizacyjne składają się z różnych typów podmiotów w ekosystemie NFC. Producenci urządzeń mobilnych i kart inteligentnych, banki i operatorzy sieci komórkowych (MNO) należą do głównych interesariuszy, którzy wpływają na wysiłki standaryzacyjne NFC.

W tym rozdziale opracowano architekturę komunikacji i podstawowe elementy każdego trybu pracy (czytnik/zapis, peer-to-peer i emulacja karty) oraz warstwy częstotliwości radiowej (RF) technologii NFC. NFC Forum prawie zakończyło standaryzację komunikacji między poziomem aplikacji a warstwą RF w trybach pracy czytnik/zapis i peer-to-peer. W trybie emulacji karty infrastruktura techniczna jest jednak zupełnie inna niż w pozostałych dwóch trybach, a proces standaryzacji nie został jeszcze zakończony. Tryb ten domyślnie daje możliwość obsługi kart inteligentnych telefonom komórkowym NFC posiadającym bezpieczne środowisko.

3.1 Wprowadzenie do NFC

NFC występuje między dwoma urządzeniami NFC w bliskim zasięgu (w odległości kilku centymetrów). Te dwa urządzenia NFC mogą działać w kilku trybach. Tryby NFC rozróżnia się na podstawie tego, czy każde urządzenie ma wbudowane źródło zasilania, dzięki czemu

może generować własne pole RF, czy też jedno z nich pobiera energię z pola RF generowanego przez drugie. Pod względem mocy, jeśli urządzenie generuje własne pole RF, nazywane jest urządzeniem aktywnym; w przeciwnym razie nazywane jest urządzeniem pasywnym. Alternatywnie urządzenia mogą być klasyfikowane w oparciu o algorytmiczny

punkt widzenia; jeśli urządzenie aktywnie prowadzi sesję komunikacyjną, na przykład prosiąc o numer karty kredytowej lub przekazując partnerowi pewne informacje w oparciu o intelligentne decyzje, zwiększa się, że jest to urządzenie aktywne. Jeśli jednak odpowiada na zapytanie, przyjmuje się, że jest urządzeniem pasywnym. Zasadniczo oba punkty widzenia (klasyfikacja urządzeń na podstawie ich wewnętrznego źródła zasilania lub zastosowanego algorytmu) są w większości zgodne. Gdy urządzenie ma wbudowane źródło zasilania, naturalnie inicjuje i prowadzi komunikację. Z drugiej strony, jeśli nie ma żadnego

Tabela 3.1 Aktywny vs. pasywny tryb komunikacji

Urządzenie A	Urządzenie B	Opis	Tryb komunikacji
Aktywny	Aktywny	Pole RF jest generowane przez oba urządzenia	Tryb aktywny
Aktywny	Pasywny	Pole RF jest generowane tylko przez urządzenie A	Tryb pasywny
Pasywny	Aktywny	Pole RF jest generowane tylko przez urządzenie B	Tryb pasywny

wbudowane źródło zasilania, może reagować tylko na urządzenie aktywne. W tej książce określamy urządzenie jako aktywne, gdy ma ono własne wbudowane źródło zasilania; w przeciwnym razie określamy je jako urządzenie pasywne.

Podobnie, tryby pracy zdefiniowane w protokole NFC są również klasyfikowane jako aktywne i pasywne tryby komunikacji. W trybie aktywnej komunikacji oba urządzenia generują własne pole RF w celu wymiany danych (patrz Tabela 3.1). W trybie komunikacji pasywnej tylko jedno urządzenie generuje pole RF, podczas gdy drugie wykorzystuje modulację obciążenia do przesyłania danych; zostało to już wyjaśnione w rozdziale 2.

Ponadto istnieją dwie różne role, które urządzenie może odgrywać w NFC, co można zilustrować jako koncepcję "żądania i odpowiedzi", jak pokazano na rysunku 3.1. Inicjator wysyła komunikat żądania do celu, a cel odpowiada, wysyłając komunikat z powrotem do inicjatora. W tym przypadku rolą inicjatora jest rozpoczęcie komunikacji. Rolą obiektu docelowego jest odpowiadanie na żądania pochodzące od inicjatora.

Tabela 3.2 przedstawia możliwe kombinacje ról inicjatora/celu w odniesieniu do ról aktywnego/pasywnego urządzenia. Urządzenie aktywne może działać zarówno jako inicjator, jak i cel. Jednak urządzenie pasywne nie może być inicjatorem.

Jak już wspomniano w rozdziale 2, NFC występuje między dwoma urządzeniami NFC. Urządzenia te mogą odgrywać rolę inicjatora lub celu, a także być urządzeniami aktywnymi lub pasywnymi. Tabela 3.3 przedstawia możliwe style interakcji między urządzeniami NFC, które są telefonami komórkowymi z obsługą NFC, tagami NFC i czytnikami NFC:

(i) Telefony komórkowe z obsługą NFC

Telefony komórkowe z obsługą NFC są również określane jako telefony komórkowe NFC. Obecnie integracja technologii NFC w telefonach komórkowych NFC stwarza dużą szansę na pokazanie łatwości użytkowania i akceptacji ekosystemu NFC. Wiele modeli telefonów komórkowych NFC jest już dostępnych na rynku. Telefony komórkowe umożliwiają bezpieczne przechowywanie danych, a zatem mogą zachowywać się jak bezpieczne karty inteligentne. Korzystając z tej funkcji, NFC umożliwia korzystanie z aplikacji obsługujących NFC, które wymagają bezpiecznej implementacji, takich jak płatności, sprzedaż biletów, aplikacje lojalnościowe i kontrola dostępu.

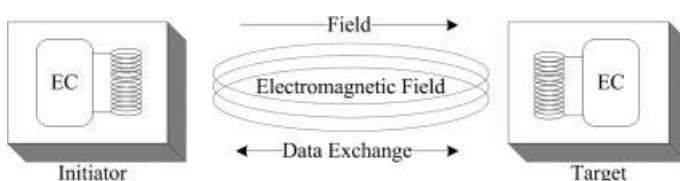
**Rysunek 3.1** Urządzenie inicjujące i docelowe.

Tabela 3.2 Możliwe kombinacje urządzenia aktywnego/pasywnego z urządzeniem inicjującym/docelowym

Rola urządzenia	Aktywne urządzenie	Urządzenie pasywne
Inicjator	Możliwe	Niemogliwe
Cel	Możliwe	Możliwe

(ii) *Tagi NFC*

Tag NFC jest w rzeczywistości pasywnym tagiem RFID. Obecnie tylko niewielka ilość danych może być przechowywana na tagu NFC. Aby zasilić tag NFC, użytkownik dotyka do niego aktywnego urządzenia, takiego jak telefon komórkowy NFC lub czytnik NFC. Gdy aktywne urządzenie wytwarza sygnał RF, energia jest zużywana przez tag NFC, dzięki czemu uruchamia się on natychmiast, a dane są przesyłane z powrotem, ponieważ wstępnie załadowany algorytm jest do tego zaprojektowany.

Będąc urządzeniem pasywnym, tag NFC może komunikować się tylko z aktywnym urządzeniem NFC (telefonem komórkowym NFC lub czytnikiem NFC); dwa tagi nie mogą komunikować się ze sobą, ponieważ w tagach NFC nie ma źródła zasilania umożliwiającego komunikację. Tagi NFC mogą być używane w aplikacjach, które wymagają niewielkich możliwości, takich jak inteligentne plakaty. Tagi NFC mogą zawierać dowolny typ danych, ale ograniczenie rozmiaru nie może zostać przekroczone. NFC Forum jako organ standaryzacyjny zdefiniował cztery typy tagów NFC (Typ 1, Typ 2, Typ 3 i Typ 4). Szczegóły dotyczące zatwierdzonych przez NFC Forum typów tagów i typów rekordów zostaną wyjaśnione w sekcji 3.5.

(iii) *Czytniki NFC*

Czytnik NFC jest zawsze aktywnym urządzeniem i jest w stanie dwukierunkowo przesyłać informacje z innym urządzeniem NFC. Czytnik NFC może występować w jednej z dwóch form: wewnętrznej i zewnętrznej. Wewnętrzny czytnik NFC może być zintegrowany z telefonem komórkowym obsługującym NFC, dzięki czemu po dotknięciu tagu NFC telefon komórkowy NFC może odczytywać/zapisywać dane z/do tagu. W ten sposób interakcja między telefonem komórkowym NFC (z wbudowanym czytnikiem NFC) a tagiem NFC jest odpowiednio interakcją między urządzeniami aktywnymi i pasywnymi.

W przypadku interakcji między dwoma telefonami komórkowymi NFC, tworzona jest między nimi komunikacja na poziomie łącza. Czytnik NFC wbudowany w telefon komórkowy NFC jest zawsze aktywny i generuje własne pole RF, chyba że telefon komórkowy NFC znajduje się w trybie czuwania lub samolotowym. Zewnętrzny czytnik NFC jest zwykle używany do odczytu danych z telefonu komórkowego NFC (patrz rysunek 3.2). Najczęstszym przykładem zewnętrznego czytnika NFC jest bezstykowy terminal POS, który może wykonywać płatności bezstykowe z obsługą NFC po dotknięciu urządzenia NFC do czytnika NFC.

Tabela 3.3 Style interakcji urządzeń NFC

Urządzenie inicjujące	Urządzenie docelowe
NFC	mobileNFC tag

NFC

Czytnik

mobileNFC

mobile

NFCNFC mobile



Rysunek 3.2 Telefon komórkowy NFC i czytnik NFC.

3.2 Standaryzacja i rozwój telefonów komórkowych z obsługą NFC

Technologia NFC korzysta z różnych elementów, takich jak karty inteligentne, telefony komórkowe, czytniki kart, systemy płatności itp. Wszystkie te elementy muszą uzyskać akredytację od szeregu organów zarządzających, które są odpowiedzialne za bezpieczeństwo i interoperacyjność różnych urządzeń NFC. Ponieważ telefony komórkowe stały się najlepszym rozwiązaniem dla technologii NFC, szczególnie dla bezpiecznych transakcji, różne organy normalizacyjne określiły, w jaki sposób technologia NFC powinna być zintegrowana z telefonami komórkowymi i innymi powiązanymi urządzeniami. Niektóre inne organy zdefiniowały architektury i standardy bezpieczeństwa, a także technologie pomocnicze dla telefonów komórkowych z obsługą NFC, takie jak karty inteligentne do transakcji NFC. Wspólną wizją wszystkich organów normalizacyjnych jest zwiększenie łatwości dostępu, interoperacyjności i bezpieczeństwa technologii NFC. Rysunek 3.3 przedstawia podsumowanie organów normalizacyjnych, które odgrywają rolę w rozwoju technologii NFC, a rysunek 3.4 przedstawia "ogólny obraz" telefonów komórkowych i organów je wspierających.

3.2.1 Forum NFC

NFC Forum to stowarzyszenie branżowe non-profit, które zostało założone w celu umożliwienia technologii NFC i rozpowszechnienia jej na całym świecie. NFC Forum to sojusz mający na celu określenie standardów NFC opartych na normach ISO/IEC. Początki tej organizacji sięgają 2004 roku, kiedy to wiele dużych firm, w tym Nokia, Philips i Sony, zawarło sojusz na rzecz zaawansowanego wykorzystania technologii RFID w zastosowaniach konsumenckich. Forum NFC obejmowało później takie firmy jak Visa, MasterCard, Samsung, Microsoft i Motorola.

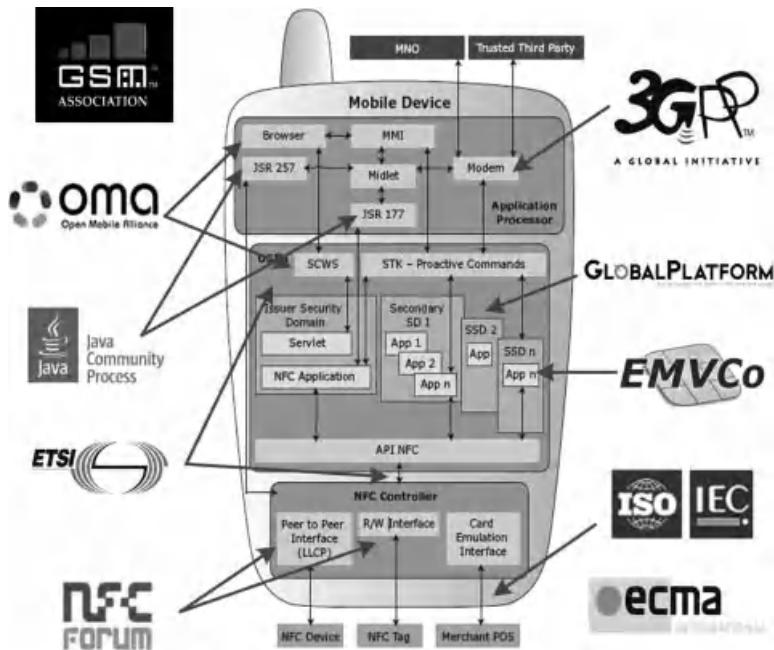
NFC Forum koncentruje się na poprawie wykorzystania bezprzewodowej interakcji krótkiego zasięgu za pośrednictwem technologii NFC w elektronice użytkowej, urządzeniach mobilnych i komputerach PC. Misją NFC Forum jest promowanie wykorzystania technologii NFC poprzez opracowywanie specyfikacji, zapewnianie interoperacyjności

Organization	Standards or Activities Governed within NFC Ecosystem			Responsibility
	Only Mobile Phones	Supportive Technologies	NFC Technology	
GSMA	✓	✓		Engages in technical, commercial and public policy initiatives to ensure that mobile services are interoperable worldwide
OMA	✓	✓		Develops specifications for mobile service enablers to promote interoperability
JCP		✓	✓	Establishes specifications for the development of Java technology on mobile phones
ETSI and its Smart Card Platform	✓	✓		Develops globally interoperable standards and handles SIM specifications
3GPP	✓	✓		Develops globally applicable technical specifications for the third generation GSM
EMVCo		✓	✓	Provides specifications to ensure interoperability of smart card based payment systems as well as mobile payment standards worldwide
GlobalPlatform		✓	✓	Provides open and interoperable infrastructure and standards for transactions performed on smart cards
NFC Forum	✓	✓	✓	Develops specifications for NFC devices that are based on ISO/IEC 18092 contactless interface ensuring interoperability among devices and services
ISO/IEC	✓	✓	✓	Provides worldwide international standards for business, government and society
ECMA International	✓	✓	✓	Provides international standards and technical reports for information communication

Rysunek 3.3 Lista organów normalizacyjnych w ekosystemie NFC.

między urządzeniami i usługami oraz edukowanie rynku w zakresie technologii NFC [1]. Celami NFC Forum są:

- Opracowanie specyfikacji NFC, które definiują modułową architekturę dla urządzeń NFC.
- Zdefiniowanie protokołów dla interoperacyjnej wymiany danych i dostarczania usług niezależnych od urządzenia.
- Definiowanie protokołów wykrywania urządzeń i ich możliwości.



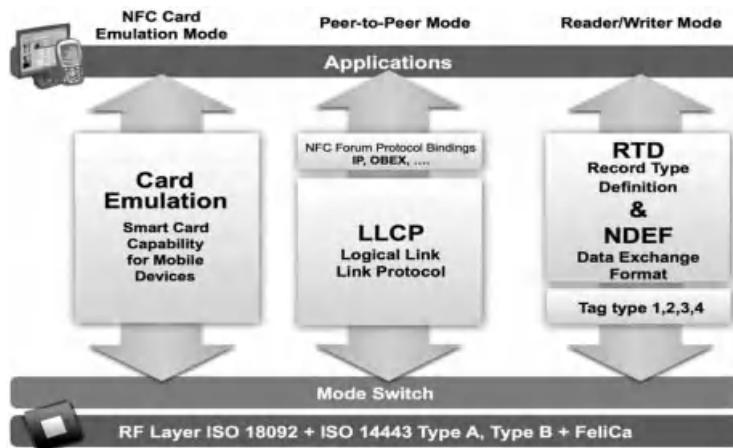
Rysunek 3.4 Standardy i organy standaryzacyjne NFC mobile. Powielono za zgodą GSMA. Wszelkie prawa zastrzeżone.

- Zachęcanie dostawców technologii do opracowywania i wdrażania produktów obsługujących technologię NFC w oparciu o wspólny zestaw specyfikacji.
- Ustanowienie programu certyfikacji zapewniającego zgodność produktów z wymaganiami NFC Forum specyfikacje.
- Promowanie globalnego wykorzystania technologii NFC poprzez edukowanie konsumentów i użytkowników korporacyjnych w zakresie zastosowań i korzyści technologii NFC.

NFC Forum ustandaryzowało tylko dwa tryby pracy (reader/writer i peer-to-peer) od warstwy aplikacji do warstwy RF (patrz rysunek 3.5). Jak wspomniano w tabeli 3.4, w trybie czytnika/zapisu używane są specyfikacje Record Type Definition (RTD) i NFC Data Exchange Format (NDEF). W trybie peer-to-peer, Logical Link Control Protocol (LLCP) jest używany do połączenia aplikacji opartej na peer-to-peer z warstwą RF, podczas gdy tryb emulacji karty zapewnia możliwość obsługi kart inteligentnych w telefonach komórkowych. Szczegóły z rysunku 3.5 zostaną pokróćce omówione dla każdego trybu pracy w tym rozdziale. Więcej szczegółów na temat tych specyfikacji można znaleźć na stronie internetowej NFC Forum (<http://www.nfc-forum.org>).

Kolejną ważną zmianą wprowadzoną przez NFC Forum jest znak towarowy "N-Mark", który jest uniwersalnym symbolem NFC (patrz rysunek 3.6), dzięki czemu konsumenti mogą łatwo zidentyfikować, gdzie mogą być używane ich urządzenia obsługujące NFC. N-Mark ma dwa znaczenia [1]:

- Istnienie znaku N-Mark na aktywnym urządzeniu oznacza, że przeszło ono testy certyfikacyjne NFC Forum. Po uzyskaniu certyfikatu produkt może zawierać znak N-Mark. The



Rysunek 3.5 Architektura techniczna NFC Forum. Powielono za zgodą NFC Forum.

N-Mark na produkcie jest punktem styku dla interakcji NFC. Obecnie tylko członkowie NFC Forum mogą certyfikować swoje urządzenia.

- Znak N na plakatach, znakach, plakietkach, etykietach itp. oznacza, że usługi NFC są dostępne w określonej lokalizacji, co jest ważne dla klientów. Wskazuje, gdzie znajduje się punkt dotykowy na urządzeniu docelowym, aby włączyć usługi NFC. N-Mark może być swobodnie używany na tagach i innych nośnikach po otrzymaniu licencji N-Mark.

3.2.2 GlobalPlatform

GlobalPlatform reprezentuje interesy branży kart inteligentnych, wydawców kart i sprzedawców. Jest to międzybranżowe stowarzyszenie non-profit, które identyfikuje, opracowuje i publikuje specyfikacje ułatwiające bezpieczne i interoperacyjne wdrażanie i zarządzanie wieloma kartami intelligentnymi.

Tabela 3.4 Przegląd specyfikacji NFC Forum

Specyfikacja	Przeznaczenie
NFC Data Exchange Format (NDEF)	Wspólny format danych dla urządzeń i tagów
NFC Record Type Definition (RTD) pomiędzy	Standardowe typy rekordów używane w wiadomościach
Smart Poster RTD	urządzenia/tagi Doplakatów zawierających tagi NFC z tekstem, dźwiękiem lub innymi danymi
Tekst RTD	Dla rekordów zawierających zwykły tekst
Uniform Resource Identifier (URI) internetowego	W przypadku rekordów odnoszących się do zasobu
Connection Handover	Okręśl sposob nawiązywania połączenia z innymi technologiami bezprzewodowymi.
Typy znaczników NFC 1-4 Działanie przez Forum NFC Protokół kontroli łączna logicznego (LLCP) Obsługujesz działanie P2P dla aplikacji NFC	Definiuje typy znaczników zatwierdzone



Rysunek 3.6 Znak towarowy N-Mark dla urządzeń NFC.

wbudowanych aplikacji na bezpiecznych kartach inteligentnych. Celem specyfikacji GlobalPlatform jest zapewnienie interoperacyjności w zakresie zarządzania zawartością kart inteligentnych, zarządzania kartami inteligentnymi bez żadnych zależności od sprzętu, producentów lub aplikacji. Specyfikacje GlobalPlatform dotyczą kart, terminali kart i globalnego zarządzania systemami wykorzystującymi karty inteligentne. Więcej szczegółowych informacji można znaleźć na stronie internetowej (<http://www.globalplatform.org>).

3.2.3 GSM Association (GSMA)

GSMA jest stowarzyszeniem operatorów telefonii komórkowej i ściśle powiązanych z nimi firm, których celem jest wspieranie standaryzacji, wdrażania i promowania technologii GSM (Global System for Mobile). W rzeczywistości GSMA reprezentuje interesy wszystkich organizacji w branży komunikacji mobilnej. GSMA zrzesza ponad 800 światowych operatorów komórkowych i ponad 200 dodatkowych firm w ramach ekosystemu mobilnego. Firmy te to producenci telefonów, oprogramowania, dostawcy sprzętu, firmy internetowe oraz organizacje medialne i rozrywkowe. GSMA koncentruje się na innowacjach i tworzeniu nowych możliwości biznesowych dla swoich członków. Głównym celem GSMA jest umożliwienie ciągłego rozwoju branży komunikacji mobilnej.

GSMA współpracuje również z wieloma operatorami sieci komórkowych w celu opracowania wspólnej wizji mobilnych usług NFC poprzez promowanie rozwoju stabilnego i wydajnego ekosystemu, aby zapobiec fragmentacji rynku. Ponadto GSMA przeprowadziła analizę interfejsu UICC do chipu NFC (Host Controller Interface, HCI), środowiska wykonawczego UICC, udostępniania Over-the-Air (OTA) i bezpieczeństwa mobilnych urządzeń NFC.

Wytyczne GSMA mają na celu zapewnienie wizji MNO dla mobilnych rozwiązań NFC poprzez identyfikację opcji technicznych i dostarczenie zaleceń. GSMA prowadzi projekt NFC, którego celem jest zdefiniowanie technicznych wytycznych dotyczących wykorzystania NFC w telefonach komórkowych. GSMA przewiduje płatności, bilety transportu publicznego i usługi lojalnościowe jako obszary zastosowań dla GSM z obsługą NFC. Więcej szczegółowych informacji można znaleźć na stronie internetowej (<http://www.gsm.org>).

3.2.4 Międzynarodowa Organizacja Normalizacyjna (ISO)/Międzynarodowa Komisja Elektrotechniczna (IEC)

ISO jest największym na świecie twórcą i wydawcą międzynarodowych standardów. Jest to sieć instytutów normalizacyjnych na całym świecie. Jest to organizacja pozarządowa, która stanowi pomost między sektorem publicznym i prywatnym. IEC jest organizacją non-profit

Międzynarodowa organizacja zapewniająca międzynarodowe standardy dla wszystkich technologii elektrycznych, elektronicznych i innych powiązanych.

ISO i IEC współpracują ze sobą w celu dostarczania zainteresowanym stronom informacji na temat normalizacji, standardów i powiązanych kwestii. Zapewniają światowe standardy, aby rozwój i wytwarzanie produktów i usług było bardziej wydajne i bezpieczniejsze, zapewniając bezpieczeństwo konsumentom i użytkownikom oraz upraszczając życie poprzez dostarczanie rozwiązań typowych problemów. Więcej szczegółowych informacji można znaleźć na stronie internetowej (<http://www.standardsinfo.net>).

3.2.5 ECMA International

ECMA International jest międzynarodową, pozarządową organizacją non-profit zajmującą się standaryzacją systemów informatycznych i komunikacyjnych. Organizacja powstała w 1961 roku w celu standaryzacji systemów komputerowych. Jest to prywatna organizacja członkowska. Członkostwo jest otwarte dla firm dowolnej wielkości, które opracowują, produkują lub sprzedają systemy komputerowe i komunikacyjne. Badania ECMA obejmują urządzenia mobilne i NFC. Więcej szczegółowych informacji można znaleźć na stronie internetowej (<http://www.ecma-international.org>).

3.2.6 ETSI i ETSI Smart Card Platform (ETSI SCP)

Europejski Instytut Norm Telekomunikacyjnych (ETSI) jest organizacją non-profit zrzeszającą ponad 700 organizacji członkowskich z ponad 60 krajów na 5 kontynentach na całym świecie. ETSI opracowuje globalnie interoperacyjne i obowiązujące standardy dla technologii informacyjnych i komunikacyjnych (ICT), w tym technologii stacjonarnych, mobilnych, radiowych, nadawczych i internetowych.

Z drugiej strony, ETSI SCP zajmuje się specyfikacjami modułów identyfikacji abonenta (SIM), które obejmują przyjęcie wszelkich zmian sprzętowych i czasami programowych w kartach SIM, które umożliwiły kartom przenoszenie aplikacji NFC lub pełnienie innych ról w telefonach NFC. Więcej szczegółowych informacji można znaleźć na stronie internetowej (<http://www.etsi.org>).

3.2.7 Java Community Process (JCP)

JCP odpowiada za rozwój technologii Java. Organizacja ta przede wszystkim kieruje rozwojem i zatwierdzaniem specyfikacji technicznych Java. JCP przyjęła już dwie ważne specyfikacje API dotyczące telefonów komórkowych dla urządzeń NFC [Contactless Communications API (JSR257) i Secure and Trust Service API (SATSA, JSR177)], które zostaną szczegółowo wyjaśnione w rozdziale 5. Więcej szczegółowych informacji można znaleźć na stronie internetowej (<http://jcp.org>).

3.2.8 Open Mobile Alliance (OMA)

OMA opracowuje otwarte standardy dla branży telefonii komórkowej. Została utworzona w czerwcu 2002 roku przez około 200 firm, w tym wiodących operatorów sieci komórkowych, dostawców urządzeń mobilnych i sieci, firmy informatyczne oraz dostawców treści i usług.

OMA wspiera rozwój specyfikacji usług mobilnych i tworzenie interoperacyjnych usług mobilnych typu end-to-end. Specyfikacje dotyczą ogólnie architektury usług i otwartych interfejsów, które są całkowicie niezależne od bazowych sieci i platform bezprzewodowych. Więcej szczegółowych informacji można znaleźć na stronie internetowej (<http://www.openmobilealliance.org>).

3.2.9 Projekt partnerski trzeciej generacji (3GPP)

3GPP to organizacja, która powstała w wyniku współpracy stowarzyszeń telekomunikacyjnych. Jej celem jest stworzenie globalnie stosowanych specyfikacji systemu telefonii komórkowej trzeciej generacji (3G) w ramach projektu *International Mobile Telecommunications 2000* Międzynarodowego Związku Telekomunikacyjnego (ITU). Specyfikacje 3GPP są oparte na specyfikacjach GSM. Więcej szczegółowych informacji można znaleźć na stronie internetowej (<http://www.3gpp.org>).

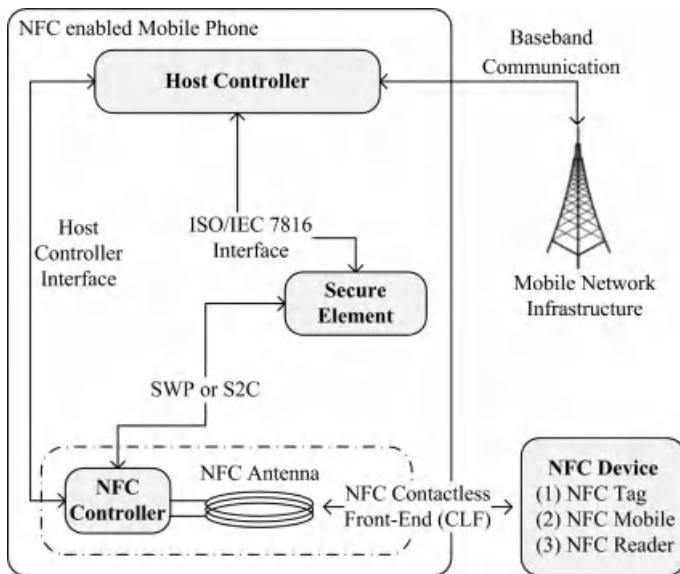
3.2.10 EMVCo

Specyfikacje *EMV 2000* są otwartym standardowym zestawem specyfikacji dla systemów płatności opartych na kartach chipowych i dążą do współpracy w zakresie standardów płatności mobilnych na całym świecie. EMVCo, należące do American Express, JCB, MasterCard i Visa, zarządza, utrzymuje i ulepsza specyfikacje EMV w celu zapewnienia globalnej interoperacyjności między kartami chipowymi i terminalami na całym świecie, niezależnie od producenta, instytucji finansowej lub wydawcy karty. EMVCo opracowuje również cenne specyfikacje dotyczące infrastruktury systemów płatności obsługujących technologię NFC w bezpiecznym środowisku. Więcej szczegółowych informacji można znaleźć na stronie internetowej (<http://www.emvco.com>).

3.3 Ogólna architektura telefonów komórkowych z obsługą NFC

Urządzenie mobilne zintegrowane z technologią NFC składa się zazwyczaj z różnych układów scalonych (IC), SE i interfejsu NFC (patrz rysunek 3.7). Interfejs NFC składa się z bezstykowego, analogowo-cyfrowego interfejsu zwanego NFC Contactless Front-end (NFC CLF), anteny NFC i układu scalonego zwanego kontrolerem NFC, który umożliwia transakcje NFC. Oprócz kontrolera NFC, telefon komórkowy z obsługą NFC ma co najmniej jeden SE, który jest podłączony do kontrolera NFC w celu wykonywania bezpiecznych transakcji zbliżeniowych z zewnętrznymi urządzeniami NFC. SE zapewnia dynamiczne i bezpieczne środowisko dla programów i danych. Umożliwia bezpieczne przechowywanie cennych i prywatnych danych, takich jak informacje o karcie kredytowej użytkownika, oraz bezpieczne wykonywanie usług obsługujących NFC, takich jak płatności zbliżeniowe. Ponadto, więcej niż jeden SE może być bezpośrednio podłączony do kontrolera NFC. Obsługiwane wspólne interfejsy między SE a kontrolerem NFC to Single Wire Protocol (SWP) i NFC Wired Interface (NFC-WI). SE może być dostępny i kontrolowany z kontrolera hosta wewnętrznie, jak również z pola RF zewnętrznie.

Kontroler hosta (kontroler pasma podstawowego) jest sercem każdego telefonu komórkowego. Interfejs kontrolera hosta (HCI) tworzy pomost między kontrolerem NFC a kontrolerem hosta. Interfejs ISO/IEC 7816 obsługuje połączenie SE z kontrolerem hosta. Kontroler hosta ustawia tryby pracy kontrolera NFC za pośrednictwem HCI, przetwarza wysyłane i odbierane dane oraz ustania połączenie między kontrolerem NFC a SE. Ponadto utrzymuje interfejs komunikacyjny, urządzenia peryferyjne i interfejs użytkownika.



Rysunek 3.7 Architektura techniczna telefonu komórkowego z obsługą NFC.

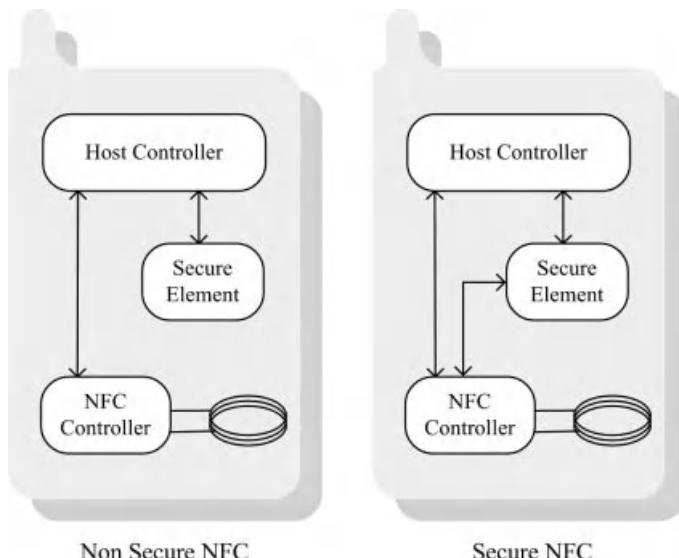
3.3.1 Bezpieczny element

Usługi NFC muszą zapewniać użytkowników i usługodawców, że transakcja odbywa się w chronionym środowisku. Ochrona ta jest osiągana poprzez wykorzystanie SE, który zapewnia mechanizmy bezpieczeństwa wymagane do obsługi różnych modeli biznesowych. SE to połączenie sprzętu, oprogramowania, interfejsów i protokołów wbudowanych w telefon komórkowy, które umożliwia bezpieczne przechowywanie danych.

SE jak zwykle musi mieć system operacyjny. System operacyjny (np. MULTOS, JavaCard OS) obsługuje bezpieczne wykonywanie aplikacji i bezpieczne przechowywanie danych aplikacji. System operacyjny może również obsługiwać bezpieczne ładowanie aplikacji. Jeśli aplikacje obsługujące NFC są zapisywane i wykonywane w pamięci kontrolera hosta telefonu komórkowego obsługującego NFC, aplikacje te nie są chronione przed niezamierzonym usunięciem lub celową manipulacją zapisanymi danymi w pamięci.

Przesyłają one jedynie dane między telefonami komórkowymi obsługującymi technologię NFC lub zbierają informacje z inteligentnych plakatów. W przypadku bezdotykowej sprzedaży biletów, płatności i innych podobnych zastosowań, bezpieczeństwo jest ważną kwestią. Aplikacje te wykorzystują cenne dane, a przechowywanie cennych, prywatnych informacji (np. informacji o karcie kredytowej) w niezabezpieczonej pamięci jest niedopuszczalne. Dane mogą być przesyłane za pośrednictwem interfejs GSM stronie trzeciej, która może niewłaściwie wykorzystać te informacje.

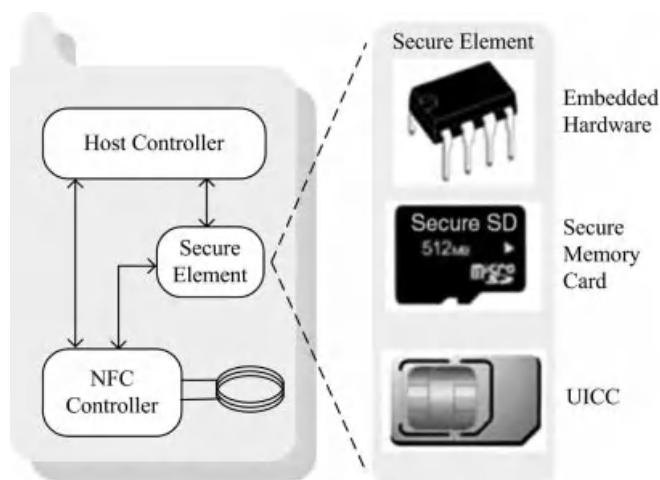
Aby rozwiązać ten problem, odpowiednie aplikacje NFC muszą być wykonywane i zapisywane w pamięci SE telefonu komórkowego z obsługą NFC (patrz rysunek 3.8). Różne moduły mogą służyć jako SE, takie jak uniwersalne karty scalone (UICC) (tj. karty SIM), karty pamięci lub wbudowany sprzęt. SE jest niezbędny do różnych zastosowań, takich jak płatności, sprzedaż biletów, aplikacje rządowe i inne, w których bezpieczne uwierzytelnianie i zaufane środowisko są jednymi z warunków wstępnych.



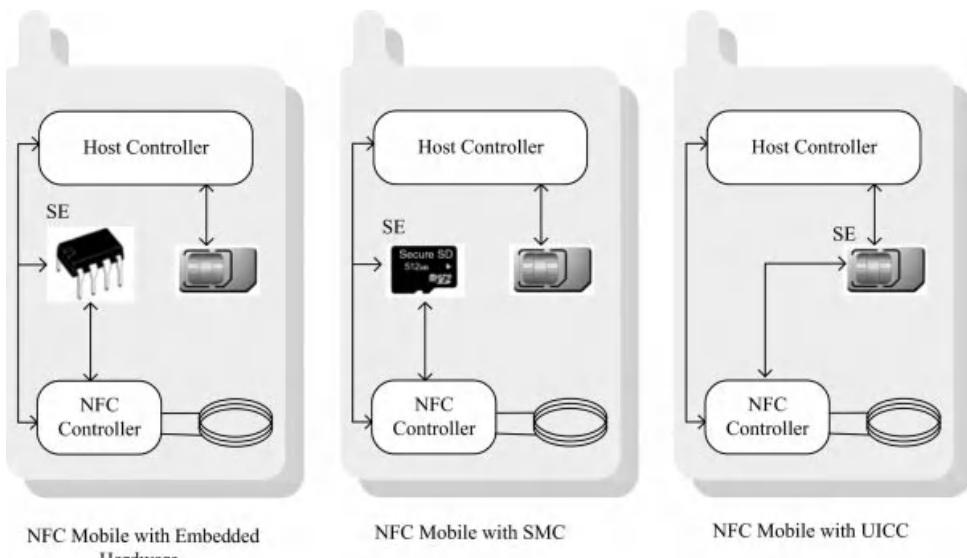
Rysunek 3.8 Niezabezpieczone vs. bezpieczne NFC [2].

Do tej pory w branży wprowadzono różne rozwiązania SE umożliwiające korzystanie z systemów opartych na NFC. Obecnie najbardziej preferowanymi i używanymi opcjami SE dla telefonu komórkowego z obsługą NFC są (patrz rysunek 3.9 i rysunek 3.10):

- *Sprzęt wbudowany* w urządzenie mobilne jako integralna, niewymieniona część urządzenia.
- *Secure Memory Card (SMC)* jako bezpieczny obszar pamięci w wymienionej karcie inteligentnej.
- *UICC* jako fizyczna karta inteligentna i być może najbardziej popularna.



Rysunek 3.9 Alternatywne elementy bezpieczeństwa [2].



Rysunek 3.10 Różne modele projektowe dla bezpiecznego NFC [2].

(i) *Sprzęt wbudowany*

Ta alternatywa SE to karta inteligentna przylutowana do telefonu komórkowego, której nie można usunąć. W związku z tym poziom bezpieczeństwa zapewniany przez ten SE jest tak wysoki, jak w przypadku karty intelligentnej. Ten chip jest wbudowany w telefon komórkowy na etapie produkcji i musi zostać spersonalizowany po dostarczeniu urządzenia do użytkownika końcowego. Przylutowany do słuchawki, chip SE oczywiście nie może zostać przeniesiony do innego telefonu komórkowego. Musi on być personalizowany za każdym razem, gdy telefon komórkowy jest używany przez innego użytkownika. Chociaż wbudowany sprzęt oparty na SE jest zgodny ze wszystkimi standardami kart intelligentnych, komunikacja w telefonie komórkowym nie została jeszcze ustandaryzowana.

(ii) *SMC*

Wymienny SMC składa się z pamięci, wbudowanego elementu karty intelligentnej i kontrolera karty intelligentnej. Innymi słowy, jest to połączenie karty pamięci i karty intelligentnej. Tym samym SMC zapewnia taki sam wysoki poziom bezpieczeństwa jak karta intelligentna i jest zgodny z większością głównych standardów, interfejsów i środowisk dla kart intelligentnych (np. EMV, GlobalPlatform, ISO/IEC 7816, JavaCard). Dzięki wymiennym właściwościom i pamięci o dużej pojemności, SE oparta na SMC może obsługiwać dużą liczbę aplikacji i nie musi być ponownie wydawana, gdy klient kupuje nowy telefon komórkowy. SE oparta na SMC można łatwo włożyć do nowego urządzenia.

(iii) *UICC*

UICC to fizyczna karta intelligentna, na której zaimplementowana jest karta SIM lub USIM. Dlatego jest powszechnie znany jako karta SIM lub USIM. SE oparty na UICC jest zgodny ze wszystkimi standardami kart intelligentnych i może obsługiwać wiele aplikacji wydanych przez różnych dostawców aplikacji. UICC zapewnia integralność i bezpieczeństwo wszystkich rodzajów danych osobowych. UICC może obsługiwać aplikacje GSM/UMTS, takie jak aplikacje SIM/USIM, takie jak

a także aplikacje nietelekomunikacyjne, takie jak płatności, lojalność, sprzedaż biletów, e-paszporty itp.

Obecnie urządzenia SE oparte na UICC stanowią idealne środowisko dla aplikacji NFC. Są one osobiste, bezpieczne, przenośne i łatwe do zdalnego zarządzania za pomocą technologii OTA (patrz rozdział 8). Posiadacze kart mogą być pewni, że transakcje są wykonywane z ochroną ich danych osobowych. Dostawcy usług, którzy wdrażają aplikacje obsługujące NFC, nie ryzykują utraty klientów, gdy posiadacze kart zmieniają telefony.

3.3.2 Interfejs NFC

Interfejs NFC składa się z bezdotykowego, analogowo-cyfrowego interfejsu zwanego NFC Contactless Front-end (NFC CLF), anteny NFC i układu scalonego zwanego kontrolerem NFC, aby umożliwić transakcje NFC, jak pokazano na rysunku 3.11.

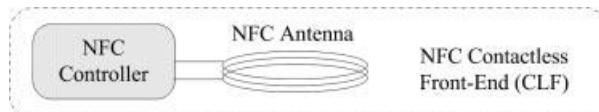
Kontroler NFC umożliwia połączenie NFC w telefonie komórkowym. Działa on jako modulator i demodulator pomiędzy analogowym sygnałem RF a anteną NFC. Aby podłączyć antenę NFC do kontrolera NFC, zwykle potrzebnych jest kilka pasywnych komponentów, takich jak kondensatory, rezystory i cewki indukcyjne. Kontroler NFC obsługuje zarówno aktywną, jak i pasywną komunikację z różnymi typami modulacji. Zazwyczaj kontroler NFC jest zgodny z protokołem NFCIP-1 (tryb peer-to-peer) oraz z innymi dwoma trybami pracy (tryb czytnika/zapisu i emulacji karty). Często obsługiwane są również inne protokoły RFID, takie jak ISO/IEC 15693.

NFC CLF jest analogowym front-endem kontrolera NFC. Interfejs logiczny NFC CLF definiuje protokół na szczeblu warstwy łączącej dane, a także sposób przesyłania wiadomości między SE a NFC CLF. Jest on teoretycznie niezależny od podstawowego interfejsu (tj. interfejsu fizycznego i interfejsu łączącego dane), który przenosi komunikaty.

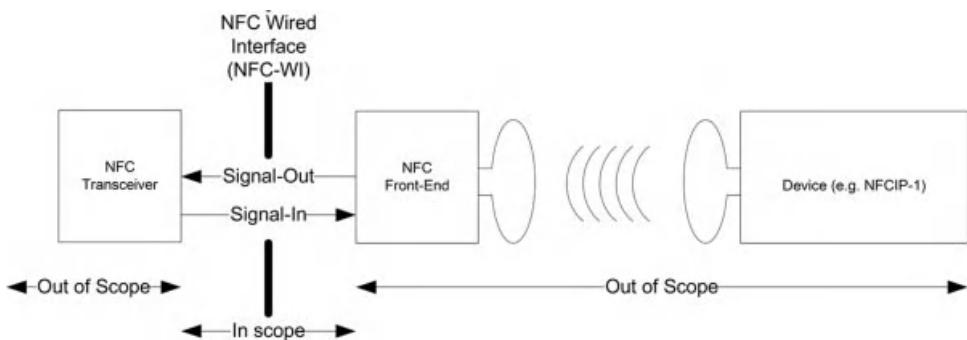
Wszystkie modele SE mają interfejs między SE a kontrolerem NFC, a także między kontrolerem hosta a kontrolerem NFC. Dane przesyłane za pośrednictwem interfejsu bezstykowego są bezpośrednio przekazywane przez kontroler NFC do SE i odwrotnie. Kontroler hosta (tj. niezabezpieczona część systemu) nie jest zaangażowany w transakcję.

3.3.3 Interfejs między SE a kontrolerem NFC

Istnieją różne opcje techniczne projektowania interfejsu między SE a kontrolerem NFC. Najbardziej obiecujące są dwie opcje: NFC-WI i SWP. Najważniejszą różnicą między nimi jest to, że SWP wykorzystuje jedną fizyczną linię, podczas gdy NFC-WI wykorzystuje dwie linie. Warto wspomnieć, że nie są to alternatywy dla siebie nawzajem, ale opcje do wykorzystania w niektórych miejscach.



Rysunek 3.11 Interfejs NFC.



Rysunek 3.12 Architektura NFC-WI [3].

(i) *NFC-WI*

NFC-WI (zwany również S2C) to cyfrowy interfejs przewodowy ustandaryzowany przez ECMA 373, ISO/IEC 28361, a także ETSI TS 102 541. SE jest zdefiniowany jako nadajnik-odbiornik, a kontroler NFC jest zdefiniowany jako front-end w tym protokole. SE jest połączony z kontrolerem NFC za pomocą dwóch przewodów [3]. NFC-WI definiuje przewody Signal-In (SIGIN) i Signal-Out (SIGOUT) między transceiverem a front-endem, jak pokazano na rysunku 3.12. W standardzie [3] transceiver jest jednostką, która steruje przewodem SIGIN i odbiera na przewodzie SIGOUT. Front-end jest jednostką, która steruje przewodem SIGOUT i odbiera na przewodzie SIGIN.

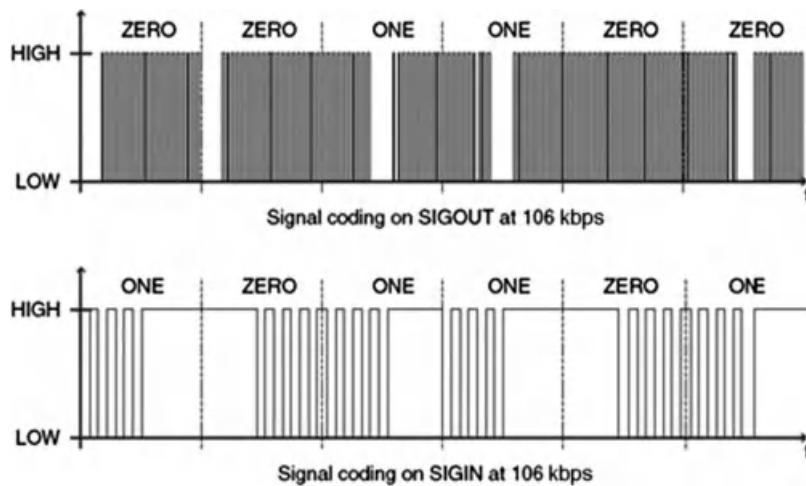
Ten cyfrowy interfejs przewodowy przenosi dwa sygnały binarne, które są zdefiniowane jako HIGH i LOW. Oba przesyłają sygnały modulacji między kontrolerem NFC a SE i są cyfrowo odbierane lub wysyłane przez interfejs RF. Transceiver steruje przewodem SIGIN sygnałem binarnym HIGH lub LOW. Front-end odbiera sygnał binarny znajdujący się na przewodzie SIGIN. Front-end steruje przewodem SIGOUT sygnałem binarnym HIGH lub LOW. Urządzenie nadawczo-odbiorcze odbiera sygnał binarny znajdujący się na przewodzie SIGOUT.

Trzy szybkości transmisji obsługiwane przez NFC-WI to 106, 212 i 424 kb/s. Przy prędkości 106 kb/s (patrz rysunek 3.13) strumień danych z kontrolera NFC do urządzenia nadawczo-odbiorczego (SIGIN) przenosi kombinację AND zmodyfikowanych danych zakodowanych bitem Millera z częstotliwością 13,56 MHz. W przeciwnym kierunku (SIGIN) strumień danych jest kodowany w systemie Manchester, a następnie odwracany przez logiczną operację OR z częstotliwością 848 kHz. Przy prędkościach 212 i 424 kb/s strumień danych z kontrolera NFC do nadajnika-odbiornika (SIGIN) jest kodowany w systemie Manchester, a następnie odwracany przez logiczną operację XOR z częstotliwością 13,56 MHz. Odpowiada to modulacji PSK (Phase Shift Keying) sygnału zegara. W przeciwnym kierunku (SIGIN) strumień danych jest ponownie kodowany w systemie Manchester.

NFC-WI jest w pełni zgodny i bezpośrednio sprzężony ze wszystkimi trybami, typami i szybkościami transmisji danych ISO/IEC 18092 i ISO/IEC 14443 i nie wymaga dodatkowej adaptacji ani konwersji protokołu. Jest to niezawodna koncepcja, którą można natychmiast wdrożyć.

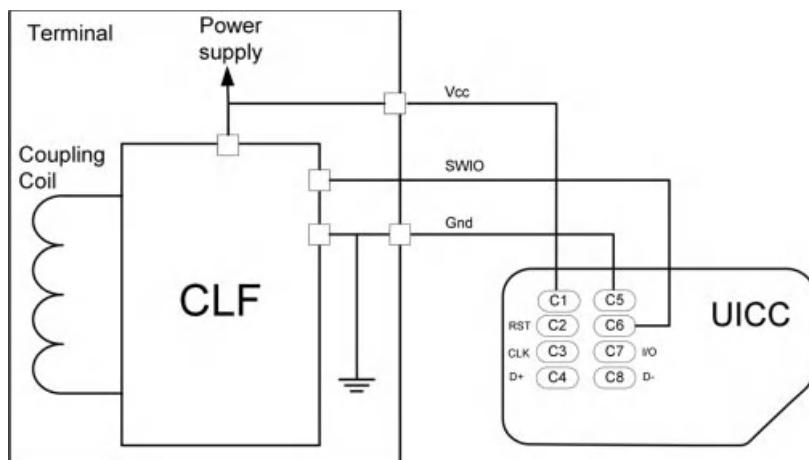
(ii) *SWP*

Kolejną opcją interfejsu fizycznego jest SWP, który definiuje jednoprzewodowe połączenie między SE a kontrolerem NFC w telefonie komórkowym, w przeciwieństwie do NFC-WI

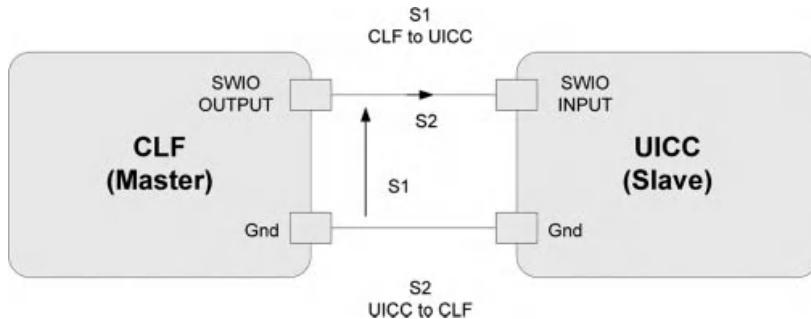


Rysunek 3.13 Transmisja sygnałów modulacji kontrolera NFC z prędkością 106 kb/s [2].

połączenie dwuprzewodowe. SWP jest standaryzowany przez ETSI TS 102 613. SWP jest cyfrowym protokołem pełnodupleksowym [4]. Szybkość transmisji danych jest skalowalna od 212 kb/s do 1,6 Mb/s dla odległości mniejszej niż 10 cm. Interfejs SWP to zorientowany bitowo protokół komunikacji punkt-punkt między SE a kontrolerem NFC, jak pokazano na rysunku 3.14. Zasada działania jest podobna do zasady działania urządzenia nadzawanego i podzawanego; kontroler NFC jest porównywalny z urządzeniem nadzawanym, a SE jest porównywalny z urządzeniem podzawanym.



Rysunek 3.14 Fizyczne łącze CLF-UICC (architektura SWP). © Europejski Instytut Norm Telekomunikacyjnych 2008. Dalsze wykorzystanie, modyfikacja, redystrybucja są surowo zabronione. Normy ETSI są dostępne na stronie <http://pda.etsi.org/pda/>.



Rysunek 3.15 Transmisja danych SWP. © Europejski Instytut Norm Telekomunikacyjnych 2008. Dalsze wykorzystanie, modyfikacja, redystrybucja są surowo zabronione. Standardy ETSI są dostępne na stronie <http://pda.etsi.org/pda/>.

Funkcja SWP jest przeznaczona głównie dla kart UICC w telefonach komórkowych, ponieważ tylko jedna ze standardowych ośmiu ścieżek stykowych jest dostępna dla funkcji SWP. Występuje tu szczególny przypadek, jak pokazano na rysunku 3.14, w którym napięcie (Vcc) karty UICC nie jest dostarczane bezpośrednio przez telefon komórkowy, ale przez interfejs NFC. Jest to konieczne do bezstykowej transmisji danych z SE, nawet gdy bateria jest wyczerpana. Jeśli interfejs NFC znajduje się w pobliżu czytnika NFC, pole czytnika dostarcza energię do SE za pośrednictwem interfejsu NFC. Należy pamiętać, że telefon komórkowy NFC działa w tym przypadku w trybie pasywnym.

W ten sposób kontroler NFC i SE mogą być używane w trybie emulacji karty. Dzięki temu aplikacje działające w trybie emulacji karty, które wymagają wysokiego poziomu bezpieczeństwa operacyjnego i funkcjonalności zbliżeniowej, nie są już zależne od stanu naładowania akumulatora.

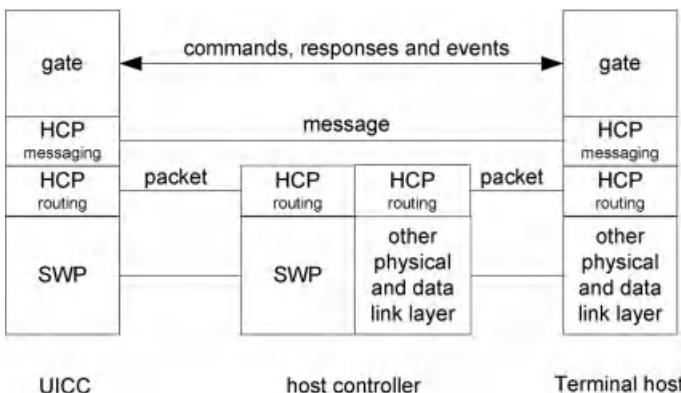
Przesypane dane są reprezentowane przez binarne stany napięcia (S1) i prądu (S2) na pojedynczym przewodzie (patrz rysunek 3.15). Transmisja danych z interfejsu NFC do SE odbywa się za pomocą sygnału modulującego S1. W odwrotnym kierunku dane są przesypane za pomocą sygnału modulującego S2.

Na szczeblu fizycznego zaimplementowano zorientowaną bitowo warstwę dostępu i kontroli medium (MAC) opartą na HDLC (High-Level Data Link Control). Protokół HDLC jest używany do kontrolowania transmisji danych między interfejsem NFC a SE. Protokół HDLC jest standaryzowany jako ISO/IEC 13239, który jest jednym z najstarszych protokołów komunikacyjnych. Zapewnia wydajne wykrywanie i korekcję błędów, synchronizację znaków i kontrolę przepływu.

SWP przenosi krótkie pakiety (ładunek mniejszy niż 30 bajtów) do warstwy aplikacji i umożliwia kierowanie wiadomości do różnych komponentów w telefonie komórkowym. Korzystanie z krótkich pakietów i potokowania umożliwia komunikację z niskim opóźnieniem między SE a interfejsem NFC. Wykorzystuje technikę tunelowania, dzięki czemu każda ramka może zostać zamknięta w ramce SWP z/do SE [5].

3.3.4 Kontroler hosta i HCI

HCI to interfejs logiczny, który umożliwia interfejsowi NFC bezpośrednią komunikację z procesorem aplikacji i wieloma SE. HCI może być wykorzystywany w różnych urządzeniach elektronicznych



Rysunek 3.16 Stos HCP w sieci hosta. © Europejski Instytut Norm Telekomunikacyjnych 2008. Dalsze wykorzystanie, modyfikacja, redystrybucja są surowo zabronione. Normy ETSI są dostępne na stronie <http://pda.etsi.org/pda/>. UWAGA: Dla przejrzystości pokazano tylko dwie bramki. Kontroler hosta posiada również bramki do łączenia się przez HCP z innymi hostami.

takich jak urządzenia mobilne, PDA i urządzenia periferyjne PC. W przypadku telefonów komórkowych z obsługą NFC umożliwia szybszą integrację funkcji NFC. HCI jest standaryzowany w ETSI TS 102 622 [6].

HCI definiuje interfejs pomiędzy jednostkami logicznymi zwanymi *hostami*, które obsługują jedną lub więcej usług. Zgodnie z terminologią ETSI, sieć dwóch lub więcej hostów nazywana jest *siecią hosta*; a jeden z hostów, który jest również odpowiedzialny za zarządzanie siecią hosta, nazywany jest kontrolerem *hosta*. W sieci hosta o topologii gwiazdy wszystkie hosty są podłączone do kontrolera hosta. HCI składa się z trzech komponentów: kolekcji bramek, które wymieniają polecenia, odpowiedzi i zdarzenia; mechanizmu przesyłania komunikatów Host Controller Protocol (HCP); oraz mechanizmu routingu HCP, który w razie potrzeby może opcjonalnie segmentować komunikaty (patrz rysunek 3.16).

Warstwy łączące danych HCP muszą być wolne od błędów, aby można było zaufać kolejności wysyłanych i odbieranych danych. Warstwa łącząca danych powinna również umożliwiać kontrolę przepływu danych, fragmentować pakiety warstwy wyższej do maksymalnego rozmiaru i zgłaszać rozmiar każdego odebranego pakietu do warstwy wyższej.

(i) Bramki

Brama stanowi punkt wejścia dla usług działających na hoście. HCP umożliwia bramom z kilku hostów wymianę wiadomości. Istnieją dwa rodzaje bram: bramy zarządzające, które obsługują zarządzanie siecią, oraz bramy ogólne.

Każdy typ bramy ma identyfikator bramy, który jest unikalny (wartości od "10" do "FF") lub nie (wartości od "00" do "0F"). Każdy host musi mieć kilka wstępnie zdefiniowanych bram, w tym administrację, zarządzanie tożsamością, zarządzanie łączami i bramy pętli zwrotnej.

(ii) Rury

Bramy komunikują się ze sobą za pośrednictwem logicznych kanałów komunikacyjnych zwanych potokami. Istnieją dwa rodzaje potoków: statyczne i dynamiczne. Rury statyczne nie muszą być tworzone i nie mogą być usuwane; jednak rury dynamiczne mogą być tworzone i usuwane. Stan potoku może być otwarty



Rysunek 3.17 Pakiety HCP. © Europejski Instytut Norm Telekomunikacyjnych 2008. Dalsze wykorzystanie, modyfikacja, redystrybucja są surowo zabronione. Standardy ETSI są dostępne na stronie <http://pda.etsi.org/pda/>.

pozostaje trwała, nawet jeśli host zostanie wyłączony i włączony lub zostanie usunięty z sieci.

Długość identyfikatora potoku (pID) wynosi 7 bitów. Jest on używany w nagłówku pakietów HCP dla informacji o routingu. Identyfikatory dynamicznych potoków są dynamicznie definiowane przez kontroler hosta, podczas gdy identyfikatory statycznych potoków są predefiniowane.

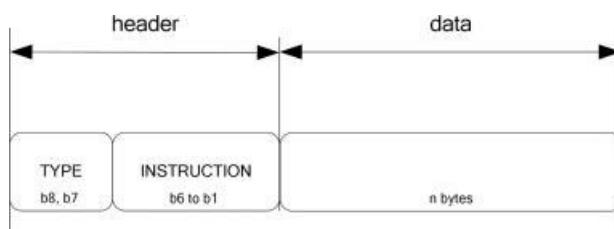
(iii) Pakiety HCP

Pakiety HCP są wymieniane między hostami a kontrolerem hosta (patrz rysunek 3.17) i zawierają następujące segmenty:

- CB jest wartością łańcuchową, która przyjmuje wartość "1" dla ostatniego pakietu pofragmentowanej wiadomości lub wartość "0" dla pakietu, który należy do pofragmentowanej wiadomości.
- pID to identyfikator potoku.
- Wiadomość zawiera jedną instrukcję i opcjonalne dane, jak pokazano na rysunku 3.18. TYPE określa typ instrukcji. INSTRUKCJA może być polecienniem (TYPE = 0), zdarzeniem (TYPE = 1) lub odpowiedzią na polecenie (TYPE = 2).

(iv) Rejestry

Rejestry są identyfikatorami o długości 1 bajta i są używane do definiowania unikalnych parametrów związanych z każdą bramką. Host jest odpowiedzialny za zarządzanie swoimi rejestrami. Dla każdej rury tworzona jest nowa instancja rejestru i ustawiane są parametry rejestru. Gdy potok jest usuwany z sieci, jego instancja rejestru jest również usuwana.



Rysunek 3.18 Struktura komunikatu HCP. © Europejski Instytut Norm Telekomunikacyjnych 2008. Dalsze wykorzystanie, modyfikacja, redystrybucja są surowo zabronione. Standardy ETSI są dostępne na stronie <http://pda.etsi.org/pda/>.

(v) *Procedury HCI*

- Następujące procedury są zdefiniowane w ETSI TS 102 622:
- *Tworzenie potoku*, które opisuje, w jaki sposób host żąda dynamicznego utworzenia potoku między jedną ze swoich bramek a bramką na innym hoście.
 - *Dostęp do rejestru*, który określa, w jaki sposób host może odczytywać/zapisywać parametry w rejestrze innego hosta.
 - *Wykrywanie hosta i bramy*, które definiuje sposób, w jaki host wykrywa inne hosty w sieci hosta, a także bramy.
 - *Inicjalizacja sesji*, która określa, w jaki sposób host może wykrywać zmiany w mechanizmach odzyskiwania.
 - *Testowanie pętli zwrotnej*, które definiuje sposób, w jaki host może zweryfikować łączność potoku z innym hostem.

3.4 Warstwa fizyczna NFC

Technologia NFC opiera się na technologii RFID w zakresie zbliżeniowym przy częstotliwości 13,56 MHz. NFC przesyła dane z prędkością do 424 kb/s. Komunikacja między dwoma urządzeniami NFC jest znormalizowana w normie ISO/IEC 18092 jako NFCIP-1. Standard ten definiuje tylko komunikację między urządzeniami zarówno dla aktywnych, jak i pasywnych trybów komunikacji. Jednak warstwa RF NFC jest superszczególnie standardowymi protokołami, który jest również kompatybilny ze standardem ISO/IEC 14443 (tj. standardem bezstykowej zbliżeniowej karty inteligentnej) i standardem JIS X 6319 jako FeliCa (tj. innym standardem bezstykowej zbliżeniowej karty inteligentnej firmy Sony), a także standardem ISO/IEC 15693 (tj. standardem bezstykowej zbliżeniowej karty inteligentnej). Te interfejsy kart inteligentnych podobnie działają na częstotliwości 13,56 MHz od czytnika kart do karty inteligentnej z różnymi szybkościami transmisji danych i zakresami komunikacji. Tabela 3.5 zawiera krótkie podsumowanie i porównanie interfejsów komunikacyjnych ISO/IEC 14443, ISO/IEC 15693 i ISO/IEC 18092. W tej sekcji podano podstawową wiedzę na temat interfejsów komunikacji zbliżeniowej wykorzystywanych przez technologię NFC, a następnie wyjaśniono funkcje transmisji danych warstwy RF.

3.4.1 ISO/IEC 14443 - Standard zbliżeniowych kart inteligentnych

Jak opisano w normie ISO/IEC 14443, transakcje zbliżeniowe opierają się na sprzężeniu elektromagnetycznym między kartą zbliżeniową a czytnikiem RFID, który wykorzystuje wbudowany mikrokontroler (w tym własny procesor i jeden z kilku rodzajów pamięci) oraz antenę pętli magnetyczną, która działa na częstotliwości 13,56 MHz. Norma ISO/IEC 14443 umożliwia transakcje bezstykowe między czytnikiem a kartą zbliżeniową używaną do identyfikacji. Zazwyczaj taka karta zbliżeniowa wykorzystuje

Tabela 3.5 Podsumowanie standardów interfejsów komunikacyjnych

	Parametry	ISO/IEC 18092	ISO/IEC 14443	ISO/IEC 15693
Tryb card	pracy	Peer-to-peer	Reader-to-	Reader-to-
pasywny	Reader-to-card	Tryb komunikacji	Aktywny i	
Zasięg	Bliskość	Bliskość	106, 212, 424 kb/s	106
	Vicinity	Szybkość	kb/s	26 kb/s
				≤ 26 kb/s

Tabela 3.6 Części normy ISO/IEC 14443

Nazwa części	Zawartość
Część 1- Charakterystyka fizyczna bezstykowych kart inteligentnych (PICC)	Okręsia cechy fizyczne bezstykowej karty inteligentnej, wymienia kilka wymagań i testów, które należy przeprowadzić na poziomie karty w celu skonstruowania karty i anteny itp.
Część 2 - Interfejs zasilania i sygnału RF	Definiuje moc RF i interfejs sygnału, schematy sygnalizacji typu A i typu B, a także określa sposób zasilania karty przez pole RF itp.
Część 3 - Inicjalizacja i ochrona przed kolizją	Definiuje protokoły inicjalizacji i protokoły antykolizyjne dla typu A i typu B, a także polecenia antykolizyjne, odpowiedzi, ramki danych i taktowanie.
Część 4 - wysokiego poziomu dla	Protokół transmisjiOkręsila protokoły transmisji danych
	Typ A i typ B, które są protokołami opcjonalnymi, dzięki czemu karty zbliżeniowe mogą być projektowane z obsługą lub bez obsługi protokołów części 4

Standardowy format karty kredytowej zdefiniowany przez ISO/IEC 7810 ID-1, ale możliwe są również inne formaty - takie jak tokeny lub breloki do kluczy. ISO/IEC 14443 używa terminów PICC (Proximity Integrated Circuit Card) i PCD (Proximity Coupling Device) do opisania komponentów biorących udział w transakcji. PCD odnosi się do czytnika kart zbliżeniowych, podczas gdy PICC odnosi się do karty zbliżeniowej.

Norma ISO/IEC 14443 zawiera cztery główne części (patrz tabela 3.6): charakterystyka fizyczna jest wyjaśniona w pierwszej części, moc RF i interfejs sygnału są wyjaśnione w drugiej części, inicjalizacja i protokoły antykolizyjne stanowią trzecią część, a protokół transmisji jest zdefiniowany w czwartej części [2]. Definiuje również dwie główne karty zbliżeniowe, a mianowicie typ A i typ B.

3.4.1.1 Główne zasady działania ISO/IEC 14443

Zbliżeniowe karty inteligentne działające na częstotliwości 13,56 MHz są zasilane i komunikują się z czytnikiem poprzez indukcyjne sprzężenie anteny czytnika z anteną karty. Zmienne pole magnetyczne jest wytwarzane przez sinusoidalny prąd przepływający przez pętlę anteny czytnika. Gdy karta wchodzi w zmienne pole magnetyczne generowane przez czytnik, w antenie pętli karty indukowany jest prąd zmienny (AC). Układ scalony PICC zawiera prostownik i zasila regulator do konwersji prądu przemiennego na prąd stały (DC) w celu zasilania układu scalonego. Czytnik moduluje amplitudę pola RF w celu wysłania informacji do karty. Układ scalony zawiera demodulator do konwersji modulacji amplitudy na sygnały cyfrowe. Układ scalony zawiera również obwód ekstrakcji zegara, który wytwarza cyfrowy sygnał zegarowy 13,56 MHz do użytku w układzie scalonym. Dane z czytnika są taktowane, dekodowane i przetwarzane przez układ scalony. Układ scalony komunikuje się z czytnikiem poprzez modulację obciążenia anteny karty i obciążenia anteny czytnika. ISO/IEC 14443 PICC wykorzystuje podnośną 847,5 kHz do modulacji obciążenia, co pozwala czytnikowi odfiltrować częstotliwość podnośną z anteny czytnika i zdekodować dane.

3.4.1.2 Główne technologie zbliżeniowych kart inteligentnych

Do tej pory pojawiły się różne technologie zbliżeniowych kart inteligentnych, jednak tylko kilka z nich jest zgodnych ze standardem ISO/IEC 14443. Obecnie najbardziej znany i konkurencyjnymi zbliżeniowymi kartami inteligentnymi są MIFARE, Calypso i FeliCa:

(i) *MIFARE*

MIFARE to dobrze znany i szeroko stosowany system zbliżeniowych kart inteligentnych 13,56 MHz, który jest rozwijany i jest własnością NXP Semiconductors, która jest spółką spin-off Philips Semiconductors. MIFARE to standard ISO/IEC 14443 typu A. Od 2011 roku MIFARE jest używany w ponad 80% wszystkich bezstykowych kart inteligentnych na świecie. Rodzina MIFARE obejmuje różne typy kart, takie jak Ultralight, Standard, Desfire, Classic, Plus i SmartMX [7]. Karty MIFARE Classic mają różne rozmiary pamięci. Karty inteligentne oparte na MIFARE są wykorzystywane w coraz szerszym zakresie zastosowań, głównie w biletach transportu publicznego, a także w zarządzaniu dostępem, płatnościami elektronicznymi, opłatach drogowych i aplikacjach lojalnościowych.

(ii) *FeliCa*

FeliCa to bezstykowy, zbliżeniowy, szybki system kart inteligentnych 13,56 MHz firmy Sony, stosowany głównie w elektronicznych kartach pieniężnych [8]. Nazwa FeliCa pochodzi od słowa "felicity", co sugeruje, że technologia ta uczyńi nasze codzienne życie wygodniejszym i przyjemniejszym. Sony złożyło wniosek o standaryzację FeliCa do ISO/IEC 14443 jako standardu typu C, ale nie udało się. FeliCa ostatecznie nie stała się standardem ISO/IEC. FeliCa jest obecnie zgodna jedynie z japońskim standardem przemysłowym (JIS) X 6319 część 4, który definiuje szybkie karty zbliżeniowe.

(iii) *Calypso*

Calypso to kolejny przykład zbliżeniowej karty inteligentnej, która jest również międzynarodowym standardem transportu publicznego [9]. Został on pierwotnie zaprojektowany przez grupę europejskich operatorów tranzytowych z Belgii, Niemiec, Francji, Włoch i Portugalii. Umożliwia interoperacyjność między kilkoma operatorami transportu na tym samym obszarze. Calypso zostało stworzone w 1993 roku przez partnerstwo pomiędzy operatorem tranzytowym RATP i Innovatron Group. Stworzenie tej technologii zostało opatentowane, aby umożliwić egzekwowanie technicznej interoperacyjności i finansowanie rozwoju poprzez otwarty system licencji. Zarówno norma ISO/IEC 14443 Typ B, jak i europejska norma EN 1545, która definiuje dane biletowe dla kart inteligentnych, są bezpośrednimi rezultatami tej pracy.

3.4.2 Interfejs i protokół komunikacji bliskiego zasięgu (NFCIP)

NFCIP jest standaryzowany w dwóch formach: NFCIP-1, który definiuje tryby komunikacji NFC w warstwie RF i inne cechy techniczne warstwy RF; oraz NFCIP-2, który obsługuje przełączanie trybów poprzez wykrywanie i wybieranie jednego z trybów komunikacji.

3.4.2.1 NFCIP-1

NFCIP-1 jest standaryzowany w normach ISO/IEC 18092, ECMA 340 i ETSI TS 102 190. Standard ten definiuje dwa tryby komunikacji: aktywny i pasywny. Definiuje również pole RF, interfejs sygnału komunikacyjnego RF i ogólny przepływ protokołu, warunki inicjalizacji dla interfejsu komunikacyjnego.

szczegółowo obsługiwane szybkości transmisji danych 106, 212 i 424 kb/s. Ponadto definiuje protokół transportowy, w tym aktywację protokołu, protokół wymiany danych z architekturą ramki i obliczaniem kodu wykrywającego błędy (CRC dla obu trybów komunikacji przy każdej szybkości transmisji danych) oraz metody dezaktywacji protokołu [10].

Częstotliwość nośna pola RF wynosi 13,56 MHz. Minimalne niemodulowane pole RF jest oznaczone symbolem H_{\min} i ma wartość skutecną 1,5 A/m. Maksymalne niemodulowane pole RF jest oznaczone przez H_{\max} i ma wartość 7,5 A/m rms. To pole RF musi być modulowane podczas komunikacji.

Jak wspomniano wcześniej dla trybu aktywnej komunikacji, zarówno inicjator, jak i cel używają własnego pola RF, aby umożliwić komunikację. Inicjator rozpoczyna komunikację NFCIP-1, podczas gdy cel odpowiada na polecenie inicjatora w trybie aktywnej komunikacji przy użyciu samodzielnego wygenerowanej modulacji samodzielnego wygenerowanego pola RF. Obiekt docelowy jest zasilany przez sprzężenie indukcyjne i jest w stanie wysyłać i odbierać dane. W trybie komunikacji pasywnej inicjator generuje pole RF i rozpoczyna komunikację. Obiekt docelowy odpowiada na polecenie inicjatora w trybie komunikacji pasywnej przy użyciu schematu modulacji obciążenia opisanego w rozdziale 2.

Schemat komunikacji przez interfejs RF w aktywnych i pasywnych trybach komunikacji obejmuje schematy modulacji, prędkość transferu i kodowanie bitów. Dodatkowo obejmuje rozpoczęcie komunikacji, zakończenie komunikacji, reprezentację bitów i bajtów, ramkowanie i wykrywanie błędów, wykrywanie pojedynczego urządzenia, wybór protokołu i parametrów, wymianę danych i usunięcie wyboru urządzeń NFCIP-1.

Wszystkie urządzenia NFCIP-1 mają możliwość komunikacji z prędkością 106, 212 lub 424 kb/s i mogą przełączać się na inną prędkość transferu lub pozostać przy tej samej prędkości transferu. Prędkość transferu inicjatora do celu i prędkość transferu celu do inicjatora nie muszą być takie same podczas transakcji. Zmiana prędkości transferu podczas sesji transakcji może być wykonana za pomocą procedury zmiany parametrów. Tryb (aktywny lub pasywny) nie może zostać zmieniony w ramach jednej sesji transakcji. Transakcja jest rozpoczynana przez inicjalizację urządzenia i kończona przez de-selekcję urządzenia (lub jej odpowiednik).

3.4.2.2 NFCIP-2

NFCIP-2 to standard określony w normach ISO/IEC 21481, ECMA 352 i ETSI TS 102 312. Standard określa mechanizm wyboru trybu komunikacji i został zaprojektowany tak, aby nie zakłócać żadnej trwającej komunikacji na częstotliwości 13,56 MHz dla urządzeń wdrażających ISO/IEC 18092 (tj. NFCIP-1), ISO/IEC 14443 (np. MIFARE) lub ISO/IEC 15693 (np. dalekiego zasięgu).

komunikacja w pobliżu, tagi RFID) [11]. Chociaż wszystkie normy ISO/IEC 18092, ISO/IEC 14443 i ISO/IEC 15693 określają częstotliwość roboczą 13,56 MHz, mogą one określać różne tryby komunikacji. Są one zdefiniowane jako tryby komunikacji NFC, PCD, PICC i VCD. Osiaga się to za pomocą wielodostępu z detekcją nośnej (CSMA), dlatego urządzenie NFCIP-2 nie aktywuje swojego pola RF, gdy wykryje zewnętrzne RF, które przekracza określony próg [11].

Urządzenia zgodne z NFCIP-2 muszą implementować funkcje urządzenia łączającego zblizeniowo (ISO/IEC 14443), urządzenia łączającego w pobliżu (ISO/IEC 15693) oraz funkcje inicjatora i celu zdefiniowane w ECMA-340. Dzięki temu urządzenie NFC są kompatybilne z istniejącymi komercyjnie wdrożonymi systemami FeliCa i MIFARE. Kompatybilność nie jest jednak osiągana

po stronie emulacji kart inteligentnych dla standardów ISO/IEC 14443 Typ B i ISO/IEC 15936, chociaż odczyt i edycja są możliwe [5].

3.4.3 Transmisja danych w warstwie RF

Tryb czytnika/zapisu umożliwia połoczenie danych tylko z prędkością 106 kb/s i opiera się na interfejsie RF, który jest zgodny ze schematami ISO/IEC 14443 (typ A, typ B) i FeliCa. W trybie peer-to-peer interfejs RF, który umożliwia wszystkie połączenia danych, takie jak 106, 212 i 424 kb/s, jest oparty na standardzie ISO/IEC 18092 (NFCIP-1). W trybie emulacji karty interfejs RF jest oparty na standardzie ISO/IEC 14443 (typ A, typ B) i FeliCa. Typ B jest szczególnie używany do wysoce bezpiecznych transakcji, takich jak zbliżeniowe płatności mobilne i sprzedaż biletów. W tej sekcji wyjaśniono techniki modulacji i kodowania stosowane przez NFC.

(i) Modulacja

Podobnie jak standardy RFID 14443 i FeliCa, NFC wykorzystuje sprzężenie indukcyjne. Częstotliwość robocza wynosi 13,56 MHz, a powszechnie stosowana szybkość transmisji to 106 kb/s (częściowo także 212 kb/s i 424 kb/s). Schematy modulacji używane przez NFC to ASK (Amplitude Shift Keying) z różną głębokością modulacji (100% lub 10%) i modulacją obciążenia:

- W przypadku transmisji danych z urządzeniem inicjującym do urządzenia docelowego, takiego jak telefon komórkowy z obsługą NFC w trybie emulacji karty, urządzenie docelowe wykorzystuje sygnał nośny 13,56 MHz urządzenia inicjującego jako źródło energii. Schemat modulacji urządzenia inicjującego to modulacja ASK. W trybie peer-to-peer oba kierunki są modulowane i kodowane jak w urządzeniu inicjującym. Wymagana jest jednak mniejsza moc, ponieważ oba aktywne urządzenia NFC korzystają z własnego zasilania, generują własne pole RF, a sygnał nośny jest wyłączany po zakończeniu transmisji.
- W przypadku transmisji danych z urządzenia docelowego do urządzenia inicjującego, ze względu na sprzężenie cewek urządzeń inicjującego i docelowego, pasywne urządzenie docelowe wpływa również na aktywne urządzenie inicjujące. Zmiana impedancji urządzenia docelowego powoduje zmiany amplitudy lub fazy napięcia antenowego urządzenia inicjującego, co jest wykrywane przez urządzenie inicjujące. Technika ta nazywana jest modulacją obciążenia. Modulacja obciążenia jest przeprowadzana w trybie nasłuchu przy użyciu nośnej pomocniczej o częstotliwości 848 kHz, która jest modulowana przez pasmo podstawowe i zmienia impedancję urządzenia docelowego.

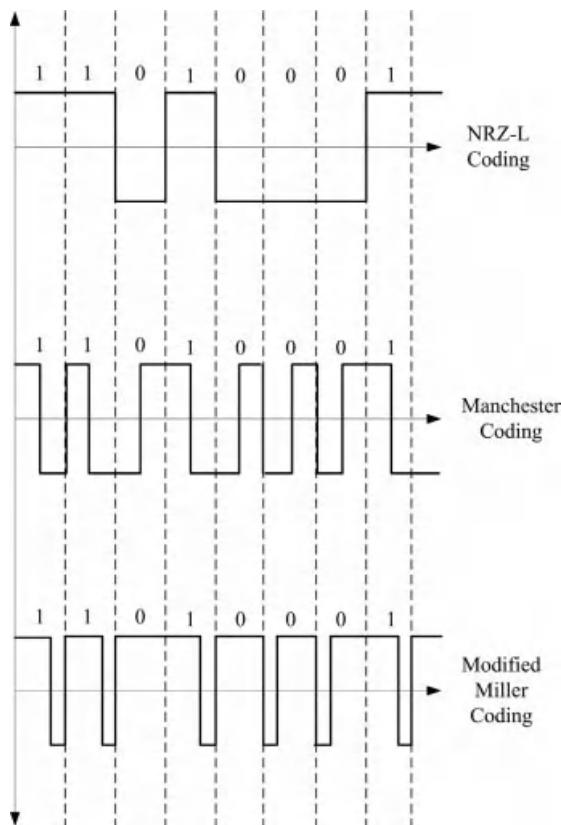
(ii) Kodowanie

NFC wykorzystuje trzy różne techniki kodowania do przesyłania danych: NRZ-L, Manchester i zmodyfikowane kodowanie Millera (patrz rysunek 3.19):

- W kodowaniu NRZ-L: stan wysoki podczas trwania jednego bitu odnosi się do logiki 1, a stan niski odnosi się do logiki 0.
- W kodowaniu Manchester: przy logice 1, pierwsza połowa bitu jest ustawniona na stan wysoki, a druga połowa tego bitu jest ustawniona na stan niski. Przy logice 0 pierwsza połowa bitu jest ustawniona na stan niski, a druga połowa na stan wysoki.
- W zmodyfikowanym kodowaniu Millera: przy logice 1 niski impuls występuje po połowie czasu trwania bitu. Przy logice 0 niski impuls występuje na początku bitu. Jeśli logika 0 występuje po logice 1, żaden impuls nie występuje przy logice 0, stąd sygnał pozostaje wysoki.

W schematach kodowania Manchester i Modified Miller pojedynczy bit danych jest

wysyłany w ustalonej szczerbinie czasowej. Ta szczerbina czasowa jest podzielona na dwie połowy, zwane półbitami. W kodowaniu Millera kodowane jest 0

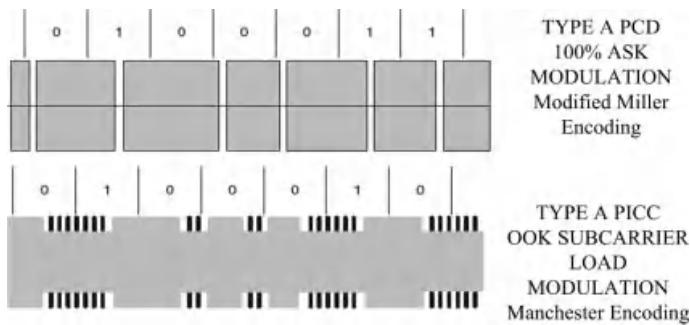


Rysunek 3.19 Kodowanie z NFC to kodowanie NRZ-L, kodowanie Manchester lub zmodyfikowane kodowanie Miller.

z przerwą w pierwszej połowie bitu i bez przerwy w drugiej połowie bitu. Cyfra 1 jest kodowana bez pauzy w pierwszym bicie, ale z pauzą w drugim półbicie. W zmodyfikowanym kodowaniu Millera obowiązują dodatkowe zasady kodowania zer. W przypadku 1, po którym następuje 0, dwa kolejne półbitły miałyby pauzę. Zmodyfikowane kodowanie Millera pozwala tego uniknąć, kodując 0, które następuje bezpośrednio po 1, dwoma półbitami bez pauzy. W kodowaniu Manchester sytuacja jest prawie taka sama, ale zamiast pauzy w pierwszym lub drugim półbicie, cały półbit jest albo pauzowany, albo modulowany. Oprócz schematu kodowania, siła modulacji zależy również od szybkości transmisji. Dla 106 kbaud stosowana jest modulacja 100%. Oznacza to, że podczas pauzy sygnał RF wynosi zero. Podczas pauzy nie jest wysyłany żaden sygnał RF. W przypadku szybkości transmisji większej niż 106 kbaud stosowany jest 10% współczynnik modulacji. Ta różnica w sile modulacji jest bardzo ważna z punktu widzenia bezpieczeństwa i zostanie opisana później w sekcji dotyczącej bezpieczeństwa [12].

3.4.3.1 ISO/IEC 14443 typ A

Sygnalizacja typu A wykorzystuje 100% modulację ASK pola RF do komunikacji z czytnika (PCD) do karty (PICC) z zakodowanymi danymi Modified Miller. Komunikacja



Rysunek 3.20 Podsumowanie interfejsu ISO/IEC 14443 typu A [2].

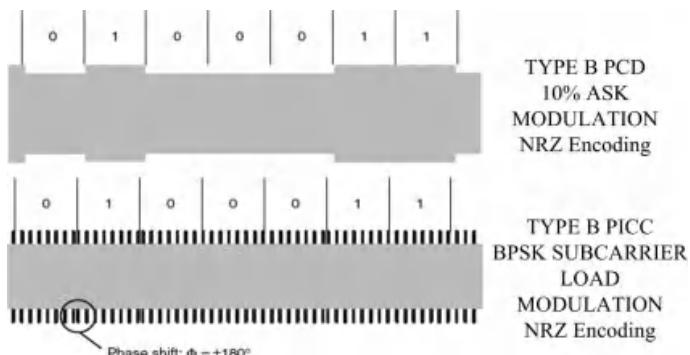
z karty do czytnika wykorzystuje podnośną OOK (podnośna 847,5 kHz) modulację obciążenia z zakodowanymi danymi Manchester. W sygnalizacji typu A pole RF jest wyłączane na krótkie okresy czasu, gdy czytnik nadaje (patrz rysunek 3.20).

3.4.3.2 ISO/IEC 14443 typ B

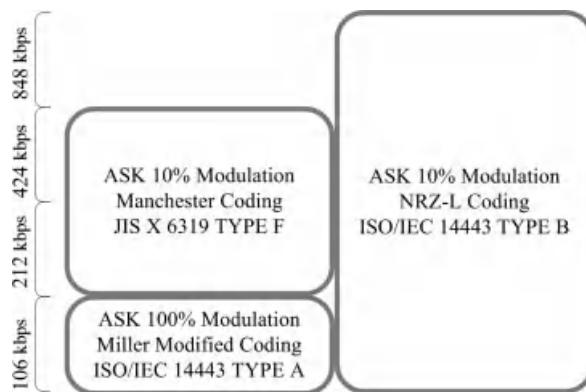
Sygnalizacja typu B wykorzystuje 10% modulację ASK pola RF do komunikacji z czytnika (PCD) do karty (PICC) z zakodowanymi danymi NRZ-L. Komunikacja z karty do czytnika wykorzystuje modulację podnośnej BPSK (Binary Phase Shift Keying) podnośnej 847,5 kHz z danymi zakodowanymi w standardzie NRZ-L (patrz rysunek 3.21).

3.4.3.3 JIS X 6319 typ F

Innym ważnym standardem, który jest dostarczany przez Japoński Standard Przemysłowy jest JIS X 6319 Typ F. JIS X 6319 wykorzystuje kodowanie Manchester w obu kierunkach transferu. Szerokość pasma potrzebna do przenoszenia danych jest dwukrotnie większa niż częstotliwość danych. Technologia ta jest standaryzowana tylko dla prędkości 212 kb/s i 424 kb/s [5].



Rysunek 3.21 Podsumowanie interfejsu ISO/IEC14443 typu B [2].



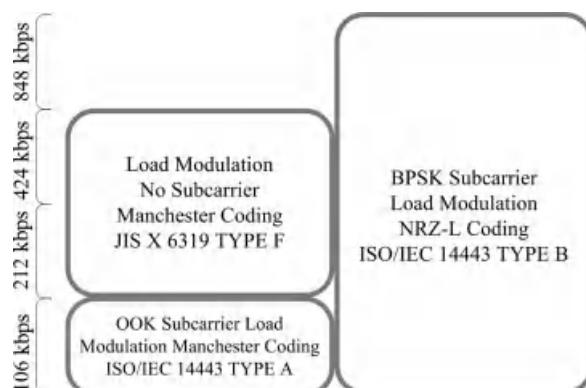
Rysunek 3.22 Kodowanie i modulacja od PCD do PICC [5].

3.4.3.4 Podsumowanie

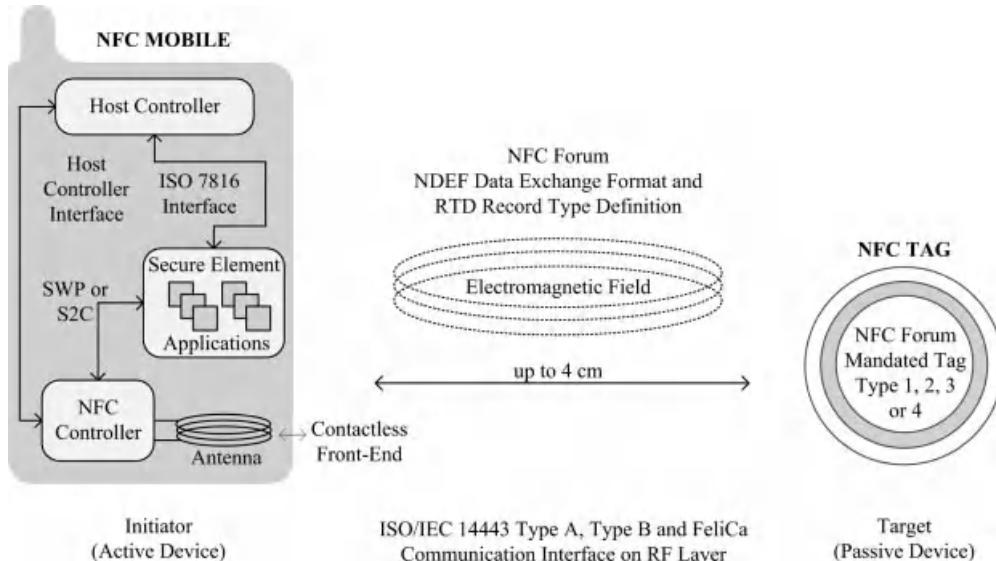
ISO/IEC 18092 (NFCIP-1) jest połączeniem ISO/IEC 14443 Typ A i JIS X 6319 Typ A. F. Wysoka prędkość ISO/IEC 14443 typu A została znormalizowana od 2005 roku, ale nie została zintegrowana z NFCIP-1. W związku z tym NFCIP-1 nie definiuje kodowania i modulacji opartych na ISO/IEC 14443 typ A większych niż 106 kb/s (patrz rysunki 3.22 i 3.23). W przypadku szybkich transferów danych z PICC do PCD i odwrotnie, używany jest typ B.

3.5 Podstawy trybu pracy czytnika/zapisywarki

W trybie czytnika/zapisu aktywny telefon komórkowy z obsługą NFC inicjuje komunikację bezprzewodową i może odczytywać oraz zmieniać dane przechowywane w tagach NFC. W tym trybie pracy telefon komórkowy z obsługą NFC jest w stanie odczytywać typy tagów zatwierdzone przez NFC Forum, takie jak inteligentne tagi plakatowe NFC. Umożliwia to użytkownikowi telefonu komórkowego pobranie danych przechowywanych w tagu i podjęcie odpowiednich działań.



Rysunek 3.23 Kodowanie i modulacja od PICC do PCD [5].



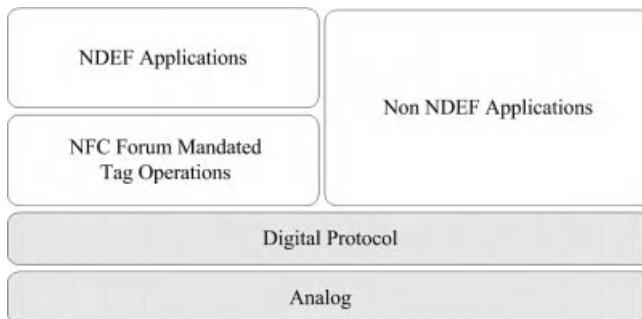
Rysunek 3.24 Architektura komunikacji w trybie czytnika/zapisu.

Jak pokazano na rysunku 3.24, interfejs RF trybu czytnika/zapisu jest zgodny ze schematami ISO/IEC 14443 typu A, typu B i FeliCa. Forum NFC ustandaryzowało typy tagów, działanie typów tagów i format wymiany danych między komponentami. Tryb pracy czytnika/zapisu zwykle nie wymaga bezpiecznego obszaru, SE innymi słowy, telefonu komórkowego z obsługą NFC. Proces polega jedynie na odczytywaniu danych przechowywanych w tagu pasywnym i zapisywaniu danych do tagu pasywnego. Architektura stosu protokołów trybu pracy czytnika/zapisu, NDEF i typy rekordów zostały wyjaśnione w sekcjach 3.5.1 i 3.5.2.

3.5.1 Architektura stosu protokołów trybu czytnika/zapisu

Rysunek 3.25 przedstawia użyteczną ilustrację stosu protokołów dla trybu czytnika/zapisu. Urządzenie NFC działające w trybie czytnika/zapisu posiada następujące elementy stosu protokołów:

- Protokoły analogowe i cyfrowe to niższe protokoły, które zostały wyjaśnione w rozdziale 3.4. Analogowy jest związany z charakterystyką RF urządzeń NFC i określa zasięg działania urządzeń. Protokoły cyfrowe odnoszą się do cyfrowych aspektów standardów ISO/IEC 18092 (patrz rozdział 3.4.2.1) i ISO/IEC 14443 (patrz rozdział 3.4.1) i definiują bloki konstrukcyjne komunikacji. Istnieje również inna ważna specyfikacja NFC Forum na tym poziomie, która jest specyfikacją działań NFC [13]. Specyfikacja ta definiuje wymagane działania, które konfiguruują komunikację w sposób interoperacyjny w oparciu o specyfikację protokołu cyfrowego, takie jak cykle odpytywania, kiedy należy wykonać wykrywanie kolizji.
 - Operacje na znacznikach oznaczają polecenia i instrukcje używane przez urządzenia NFC do obsługi NFC
- Tagi zatwierdzone przez forum, które są typu 1, typu 2, typu 3 i typu 4. Umożliwiają one odczyt i



Rysunek 3.25 Stos protokołów trybu pracy czytnika/zapisu.

operacje zapisu przy użyciu formatu danych NDEF i RTD (tj. inteligentny plakat, URI RTD) z/do tagu.

- Aplikacje NDEF są oparte na specyfikacjach NDEF, takich jak inteligentny plakat i odczyt informacji o produkcie z inteligentnych ulotek zakupowych obsługujących technologię NFC.
- Aplikacje inne niż NDEF to aplikacje specyficzne dla dostawcy, takie jak elektroniczne saldo portmonetki i czytnik biletów zbliżeniowych, które nie są oparte na specyfikacjach NDEF.

3.5.2 Typy tagów wymagane przez forum NFC

Cztery typy tagów zostały zdefiniowane przez NFC Forum i otrzymały oznaczenia od 1 do 4. Każdy typ tagu ma inny format i pojemność. Formaty tagów NFC są oparte na normach ISO/IEC 14443 typ A, ISO/IEC 14443 typ B lub Sony FeliCa. Poniżej wymieniono różne definicje typów tagów NFC, a w tabeli 3.7 przedstawiono ich porównanie.

- *Tag typu 1:* Tag NFC typu 1 jest oparty na standardzie ISO/IEC 14443 typu A. Te tagi NFC można zarówno odczytywać, jak i zapisywać. Dane na tych tagach mogą być również modyfikowane, a użytkownicy mogą skonfigurować tag tak, aby był tylko do odczytu, gdy jest to wymagane. Dostępność pamięci wynosi do 1 kB, co wystarcza do przechowywania adresu URL strony internetowej lub podobnej niewielkiej ilości danych. Rozmiar pamięci można rozszerzyć do 2 kB. Prędkość komunikacji tego tagu NFC wynosi 106 kbps. Ze względu na swoją prostotę, ten typ tagu jest opłacalny i może być używany w wielu aplikacjach NFC.
- *Tag typu 2:* Znacznik NFC typu 2 jest również oparty na standardzie ISO/IEC 14443 typu A. Te tagi NFC mogą być zarówno odczytywane, jak i zapisywane, a użytkownicy mogą skonfigurować tag tak, aby był tylko do odczytu, gdy jest to wymagane. Rozmiar pamięci tego typu tagu można rozszerzyć do 2 kB. Podobnie prędkość komunikacji wynosi 106 kb/s.
- *Znacznik typu 3:* Znacznik NFC typu 3 jest oparty na interfejsie bezstykowej karty inteligentnej Sony FeliCa. Jest to ma obecnie pojemność pamięci 2 kB, a prędkość transmisji danych wynosi 212 kb/s. Ten typ tagu jest bardziej odpowiedni dla złożonych aplikacji. Jest on jednak droższy w porównaniu z innymi typami tagów.
- *Tag typu 4:* Znacznik NFC typu 4 jest kompatybilny zarówno z ISO14443 typu A, jak i typu B. standardy. Te tagi NFC są wstępnie konfigurowane na etapie produkcji i mogą być

zapisywane lub tylko do odczytu; a typ jest definiowany na etapie produkcji. Typ

Tabela 3.7 Podsumowanie typów tagów NFC Forum

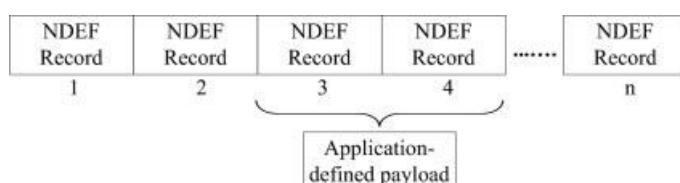
Parametr	Typ 1	Typ 2	Typ 3	Typ 4
Na podstawie Nazwa chipa	ISO/IEC 14443 Topaz typu A	ISO/IEC 14443 Typ A MIFARE	FeliCa	ISO/IEC 14443 Typ A, Typ B DESFIRE, SmartMX-
JCOPRozmiar pamięci 64 kB		1 kB	Do 2 kB	Do 1 MB
Szybkość transmisji danych (kb/s)	106		106	212
Bezpieczeństwo	16- lub 32-bitowy podpis cyfrowy		Niezabezpieczony 16- lub 32-bitowy podpis cyfrowy	Zmienna
Dostarczone	przez Innovision Research and Technology	Philips/NXP	Sony	Kilka
Cena jednostkowa	Niski	Niska	Wysoka	Średnia/Wysoka
Przypadki użycia	Tagi małą pamięcią dla pojedynczej aplikacji		Elastyczne tagi z większą pamięcią oferujące możliwości wielu aplikacji	

Pojemność pamięci może wynosić do 32 kB, a prędkość komunikacji wynosi od 106 do 424 kb/s.

3.5.3 NDEF

Specyfikacja NDEF jest standardem zdefiniowanym przez NFC Forum [14]. NDEF to format danych służący do wymiany informacji między urządzeniami NFC; mianowicie między aktywnym urządzeniem NFC a pasywnym tagiem lub dwoma aktywnymi urządzeniami NFC. Wiadomość NDEF jest wymieniana, gdy urządzenie NFC znajduje się w pobliżu tagu zatwierzonego przez NFC Forum, wiadomość NDEF jest odbierana z tagu zatwierzonego przez NFC Forum, a także przez LLCP NFC Forum (patrz sekcja 3.6). Format danych jest taki sam w obu przypadkach.

NDEF to binarny format komunikatu, który zawiera jeden lub więcej ładunków zdefiniowanych przez aplikację w pojedynczym komunikacie, jak pokazano na rysunku 3.26. Komunikat NDEF zawiera jeden lub więcej rekordów NDEF. Każdy rekord składa się z ładunku o rozmiarze do 2^{32} - 1 oktetów. Rekordy mogą być łączone w łańcuchy w celu obsługi większych ładunków.



Rysunek 3.26 Struktura NDEF.



Rysunek 3.27 Komunikat NDEF z zestawem rekordów. Powielono za zgodą NFC Forum.

W komunikacie NDEF pierwszy rekord jest oznaczony flagą MB (Message Begin), a ostatni rekord jest oznaczony flagą ME (Message End) (patrz rysunek 3.27). Minimalna długość komunikatu to jeden rekord, co osiąga się poprzez ustawienie zarówno flagi MB, jak i ME w tym samym rekordzie. Maksymalna liczba rekordów NDEF, które mogą być przenoszone w wiadomości, jest nieograniczona.

Nagłówek wiadomości zaczyna się od lewej (head) do prawej (tail). Pierwszy zestaw flag (MB) jest określany przez indeks 1, a ostatni (ME) jest określany przez indeks t. Tak więc indeksy rekordów logicznych są w kolejności: $t > s > r > 1$ (patrz rysunek 3.27).

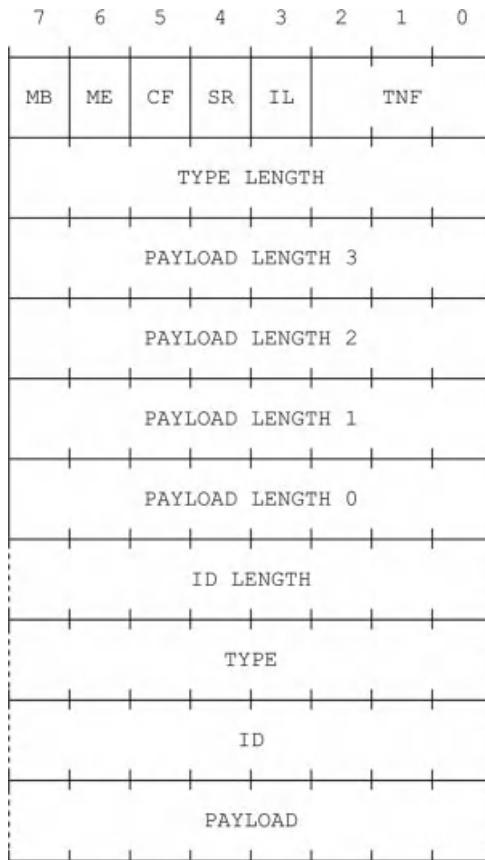
Rekord jest jednostką przenoszącą ładunek w komunikacie NDEF. Każdy rekord NDEF zawiera trzy parametry opisujące jego ładunek: długość ładunku, typ ładunku i opcjonalny identyfikator ładunku. Cele korzystania z tych parametrów są następujące:

- *Długość ładunku* wskazuje całkowitą liczbę oktetów w ładunku.
- *Identyfikator typu ładunku* wskazuje typ ładunku. NDEF obsługuje identyfikatory URI, MIME konstrukcje typu nośnika i format typu specyficzny dla NFC jako identyfikatory typu. Wskazując typ ładunku, możliwe jest wysłanie ładunku do odpowiedniej aplikacji.
- *Opcjonalny identyfikator ładunku* umożliwia aplikacjom użytkownika identyfikację przenoszonego ładunku w rekordzie NDEF.

Rekordy NDEF są rekordami o zmiennej długości i wspólnym formacie przedstawionym na rysunku 3.28. Każde pole w rekordzie ma inne cechy. Szczegóły każdego rekordu można znaleźć w specyfikacjach. Najważniejsze z nich to pole TNF (Type Name Format) i pole TYPE. Wartość pola TNF wskazuje strukturę wartości pola TYPE. Pole TYPE opisuje typ ładunku. TNF obejmuje 3-bitowe pole, a możliwe wartości pola TNF są wymienione w tabeli 3.8.

Różne typy rekordów dla formatu wiadomości NDEF są zdefiniowane przez NFC Forum [15]. Pole *typu rekordu* zawiera nazwę typu rekordu jako *nazwę typu rekordu*. Nazwy typów rekordów są używane przez aplikacje NDEF do identyfikacji semantycznej i struktury zawartości rekordu. Nazwy typów rekordów mogą być określone w kilku formatach w polu TNF nagłówka rekordu NDEF. Nazwy typów rekordów mogą być typami mediów MIME, bezwzględnymi identyfikatorami URI, zewnętrznymi nazwami typów NFC Forum lub dobrze znanimi nazwami typów NFC. Każda definicja typu rekordu jest identyfikowana przez nazwę typu rekordu:

- *NFC Forum Well-known Type*: Jest to gesty format przeznaczony dla znaczników i tworzenia prymitywów lub wspólnych typów. Jest on identyfikowany wewnątrz komunikatu NDEF poprzez ustawienie pola TNF rekordu na wartość 0×01 . NFC Forum Well-known Type to URN z identyfikatorem przestrzeni nazw "nfc" (NID). Ciąg znaków specyficzny dla przestrzeni nazw (NSS) znanego typu forum NFC



Rysunek 3.28 Rekord NDEF. Powielono za zgodą NFC Forum.

jest poprzedzony prefiksem "wkt:" (patrz Tabela 3.9). Gdy jest zakodowany w komunikacie NDEF, musi być zapisany jako względna konstrukcja-URI, w której prefiks NID i "wkt:" są odrzucane. Na przykład, "urn:nfc:wkt:very-complicated-type" jako NFC Forum Well-known Type będzie zakodowany jako "very-complicated-type". Dwa główne typy są następujące:

- Typ globalny NFC Forum: NFC Forum definiuje i zarządza tym typem. Typy globalne NFC Forum zaczynają się od dużej litery w zestawie znaków, który można znaleźć w specyfikacji RTD. Na przykład "A", "Trip-to-Istanbul".
- Typ lokalny NFC Forum: Typy lokalne NFC Forum zaczynają się od małej litery w zestawie znaków lub od liczby w zestawie znaków, które można znaleźć w specyfikacji RTD. Na przykład "2", "a", "trip". Typ lokalny forum NFC może być ponownie wykorzystany przez inną aplikację w innym kontekście i z inną zawartością.
- *NFC Forum External Type*: Nazwa typu zewnętrznego jest identyfikowana wewnątrz komunikatu NDEF.

poprzez ustawienie pola TNF lub rekordu na wartość 0×04 . Typ zewnętrzny forum NFC to URN z identyfikatorem NID "nfc". Część NSS jest poprzedzona przedrostkiem "ext:". Przykładem może być

Tabela 3.8 Możliwe wartości pola TNF

Typ	Nazwa	Format (TNF)	Wartość
NFC Forum Well-Known			Puste0 × 00
Typ			Type0 × 01
Bezwzględny			nośnika0 × 02
NFC Forum External			URI0 × 03
Bez			Type0 × 04
			Nieznany0 × 05
			zmian0 × 06
			Zarezerwowane0 × 07

być "urn:nfc:ext:yourcompany.com:f". Podobnie jak w przypadku dobrze znanych typów NFC Forum, kodowanie binarne typu zewnętrznego NFC Forum odrzuca prefiks NID i NSS "ext:".

NFC Forum definiuje różne typy rekordów dla określonych przypadków: inteligentne plakaty, URI, podpis cyfrowy i tekst. Te RTD można znaleźć szczegółowo na stronie internetowej NFC Forum. Poniżej znajduje się krótki opis każdego z nich:

(i) *URI RTD*

Usługa URI RTD definiuje rekord, który ma być używany z NDEF do pobierania URI przechowywanego na tagu NFC lub do przesyłania URI z jednego urządzenia NFC do drugiego [16]. Znanym typem rekordu URI jest "U" (0 × 55 w reprezentacji binarnej NDEF). Struktura rekordu URI została przedstawiona w tabeli 3.10. Istnieje 256 kodów identyfikatorów URI, których szczegóły można znaleźć w specyfikacji URI RTD NFC Forum. Niektóre przykłady kodów identyfikatorów URI przedstawiono w tabeli 3.11. Pole URI jest zdefiniowane przez kodowanie UTF-8, które w specyfikacjach jest również nazywane kodowaniem binarnym NFC.

Tabele 3.12 i 3.13 podają przykłady przechowywania różnych identyfikatorów URI w tagach. Tabela 3.12 przedstawia prosty przykład uruchomienia strony internetowej NFC Lab - Istanbul "http://www.nfclab.com", gdzie pole identyfikatora URI ma wartość 0 × 01. Jeśli zawartość tego pola wynosi 0 × 02, a zawartość pola URI brzmi "nfclab.com", wynikowy URI to "https:// www.nfclab.com". Tabela 3.13 dotyczy przechowywania adresu e-mail w tagu. Zawartość pola URI brzmi "info@nfclab.com"; wynikowy URI to "mailto:info@nfclab.com".

Tabela 3.9 Przykłady dobrze znanych typów rekordów NDEF

Typ rekordu NDEF	Opis	Odniesienie URI
Sp	Inteligentny plakat	urn:nfc:wkt:Sp
T	Tekst	urn:nfc:wkt:T
U	URI	urn:nfc:wkt:U
Sig	Podpis	urn:nfc:wkt:Sig

Tabela 3.10 Zawartość rekordu URI

Nazwa	Wartość	Opis
Kod identyfikatora URI Pole URI	Kod identyfikatora URI Dane zakodowane w formacie UTF-8	Kod identyfikatora URI (256 kodów) Pozostała część identyfikatora URI lub cały identyfikator URI (jeśli kod identyfikatora to 0 × 00)

Tabela 3.11 Kilka przykładów kodów identyfikatorów URI

Dziesiętny	Szesnastkowy	Typ protokołu
	00 × 00	Niedostępne. Pole URI zawiera nieskrócony identyfikator URI
1	0 × 01	http://www.
2	0 × 02	https://www.
5	0 × 05	tel:
6	0 × 06	mailto:
8	0 × 08	ftp://ftp.

Tabela 3.12 Przechowywanie adresu URL

Przesunięcie	Treść	Wyjaśnienie
0	0 × D1	SR = 1, TNF = 0 × 01 (Forum NFC Well-Known Type), ME = 1, MB = 1
1	0 × 01	Długość typu rekordu (1 bajt)
2	0 × 0B	Długość ładunku (11 bajtów)
3	0 × 55	Typ rekordu URI ("U")
4	0 × 01	Kod identyfikatora URI jako "http://www".
5	0 × 6e 0 × 63 0 × 6c 0 × 61 0 × 62 0 × 2e 0 × 63 0 × 6f 0 × 6d	Ciąg znaków "nfclab.com" w UTF-8

Tabela 3.13 Przechowywanie adresu e-mail

Przesunięcie	Treść	Wyjaśnienie
0	0 × D1	SR = 1, TNF = 0 × 01 (Forum NFC Well-Known Type), ME = 1, MB = 1
1	0 × 01	Długość typu rekordu (1 bajt)
2	0 × 10	Długość ładunku (16 bajtów)
3	0 × 55	Typ rekordu URI ("U")
4	0 × 06	Kod identyfikatora URI jako "mailto:"
5	0 × 69 0 × 6e 0 × 66 0 × 6f 0 × 40 0 × 6e 0 × 66 0 × 63 0 × 6c 0 × 61 0 × 62 0 × 2e 0 × 63 0 × 6f 0 × 6d	Ciąg znaków "info@nfclab.com" w UTF-8

Tabela 3.14 Przykład URI na inteligentnym plakacie

Przesunięcie	Treść	Długość	Wyjaśnienie
0	0 × D1	1	Nagłówek NDEF, TNF = 0 × 01 (znany typ), SR = 1, MB = 1, ME = 1
1	0 × 02	1	Długość nazwy rekordu (2 bajty)
2	0 × 12	1	Długość danych inteligentnego plakatu (18 bajtów)
3	"Sp"	2	Nazwa rekordu
5	0 × D1	1	Nagłówek NDEF, TNF = 0 × 01 (znany typ), SR = 1, MB = 1, ME = 1
6	0 × 01	1	Długość nazwy rekordu (1 bajt)
7	0 × 0A	1	Długość ładunku URI (11 bajtów)
8	"U"	1	Typ rekordu: "U"
9	0 × 01	1	Skrót: "http://www".
10	"nfclab.com"	10	Sam identyfikator URI

(ii) Smart Poster RTD

Smart Poster RTD definiuje znany typ NFC Forum Well-Known Type dotyczący umieszczania adresów URL, SMS-ów i numerów telefonów na tagu zatwierdzonym przez NFC Forum oraz sposobu ich przesyłania między urządzeniami [17]. Inteligentne plakaty są popularnymi przypadkami użycia aplikacji obsługujących NFC. Pomysł polega na tym, że obiekt można uczynić "inteligentnym", tak aby mógł przechowywać dodatkowe informacje w postaci tagu zatwierzonego przez NFC Forum. Po dotknięciu tagu urządzeniem NFC, informacje te mogą zostać odczytane i przetworzone. Inteligentny plakat zawiera dane, które uruchomią aplikację w urządzeniu, taką jak uruchomienie przeglądarki w celu wyświetlenia strony internetowej, wysłanie wiadomości SMS do usługi premium w celu otrzymania dzwonka itp.

Koncepcja inteligentnego plakatu opiera się głównie na identyfikatorach URI, które stały się standardem odwoływanego się do informacji w Internecie. URI są bardzo potężne i jak już wspomniano, mogą reprezentować wszystko, od unikalnych identyfikatorów i adresów internetowych po wiadomości SMS, połączenia telefoniczne i tak dalej.

Zawartość ładunku inteligentnego plakatu to komunikat NDEF. Treść tego komunikatu składa się z kilku rekordów NDEF. Najważniejsze z nich są następujące:

- Rekord *tytułu* dla usługi.
- URI, który jest rdzeniem inteligentnego plakatu.
- Rejestr działań opisujący, w jaki sposób należy traktować usługę.
- Rekord ikony, który odnosi się do jednego lub wielu rekordów obrazów (ikon) typu MIME w ramach inteligentnego plakatu.
- Rekord rozmiaru służący do określania rozmiaru odniesień URI, które mają zewnętrzną jednostkę (np. przez URL).
- Rekord typu do zadeklarowania typu MIME odniesienia URI, które ma podmiot zewnętrzny (np. za pośrednictwem adresu URL).

Jak pokazano w tabeli 3.14, treść tej wiadomości reprezentuje adres internetowy NFC Lab-Istanbul, więc gdy użytkownik dotknie tagu na tym inteligentnym plakacie, uruchomi przeglądarkę na urządzeniu NFC i wyświetli stronę internetową NFC Lab Istanbul.

(iii) Signature RTD

Rekord podpisu zawiera podpis cyfrowy powiązany z jednym lub większą liczbą rekordów w wiadomości NDEF [18]. Podpis może być wykorzystany do weryfikacji

całego komunikatu NDEF poprzez ich podpisanie. Cyfrowe podpisywanie danych NDEF jest godną zaufania metodą dostarczania informacji o pochodzeniu danych NDEF w tagu i urządzeniu NFC zatwierdzonym przez NFC Forum. Umożliwia to weryfikację autentyczności i integralności danych w komunikacie NDEF. Celem nie jest zdefiniowanie lub nakazanie określonego PKI lub systemu certyfikacji, ani zdefiniowanie nowego algorytmu do użytku z podpisem RTD.

Znanym typem NFC Forum dla rekordu podpisu jest "Sig", który ma wymiary 0×53 , 0×69 , 0×67 w kodowaniu UTF-8. Zawartość ładunku rekordu podpisu jest następująca:

- *Wersja*, która odnosi się do wersji specyfikacji.
- *Podpis*, który zawiera rzeczywisty podpis lub odniesienie do lokalizacji podpisu.
- Łańcuch *certyfikatów* zawierający opcjonalne i obowiązkowe pola.

Rekord podpisu może być używany w wiadomości NDEF, a także w innych typach danych. Szczegółowe informacje na temat signature record można znaleźć na stronie internetowej NFC Forum.

(iv) *Tekst RTD*

Rekord tekstowy zawiera dowolny zwykły tekst [19]. Rekord tekstowy może pojawić się jako jedyny rekord w komunikacie NDEF, ale w tym przypadku zachowanie jest niezdefiniowane i aplikacja powinna sobie z tym poradzić. Zazwyczaj rekord tekstowy powinien być używany w połączeniu z innymi typami rekordów w celu dostarczenia tekstu objaśniającego. Znanym typem NFC Forum dla rekordu tekstu jest "T", czyli 0×54 w kodowaniu UTF-8. W typach rekordów tekstowych tekst może być zakodowany w UTF-8 lub UTF-16, co jest zdefiniowane przez bajt statusu w rekordzie tekstu. Rekord tekstowy składa się zazwyczaj z nagłówka rekordu NDEF, ładunku i rzeczywistego tekstu w formacie UTF. W ładunku, bajt statusu definiuje strukturę kodowania.

3.6 Podstawy trybu pracy peer-to-peer

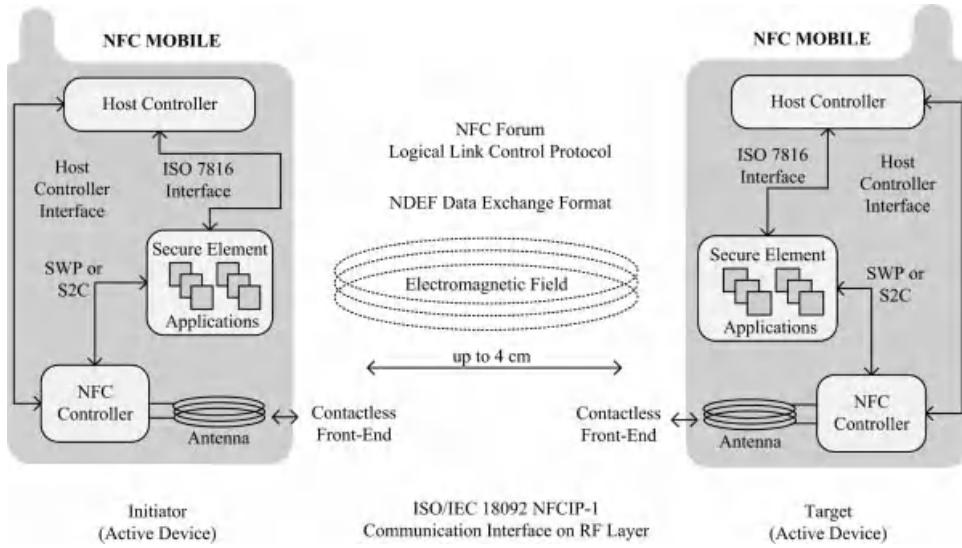
W trybie peer-to-peer dwa telefony komórkowe z obsługą NFC nawiązują dwukierunkowe połaczenie w celu wymiany informacji, jak pokazano na rysunku 3.29. Mogą one wymieniać się wirtualnymi wizytówkami, zdjęciami cyfrowymi i innymi rodzajami danych. Interfejs komunikacji radiowej w trybie peer-to-peer jest standaryzowany przez normę ISO/IEC 18092 jako NFCIP-1.

3.6.1 Architektura stosu protokołów w trybie peer-to-peer

Zgodnie ze specyfikacją NFC Forum, urządzenie NFC działające w trybie peer-to-peer posiada następujące elementy stosu protokołów (patrz rysunek 3.30):

- Protokoły analogowe i cyfrowe są protokołami niższej warstwy ustandaryzowanymi przez NFCIP-1.
- LLCP umożliwia przesyłanie jednostek informacji warstwy wyższej między dwoma urządzeniami NFC (zob. następną sekcję).
- Wiązania protokołów zapewniają standardowe powiązania z protokołami NFC Forum i umożliwiają interoperacyjność.
- możliwość korzystania z zarejestrowanych protokołów.

- Protokoły NFC Forum to te, które NFC Forum definiuje jako wiążące dla LLCP, takie jak OBEX i IP.

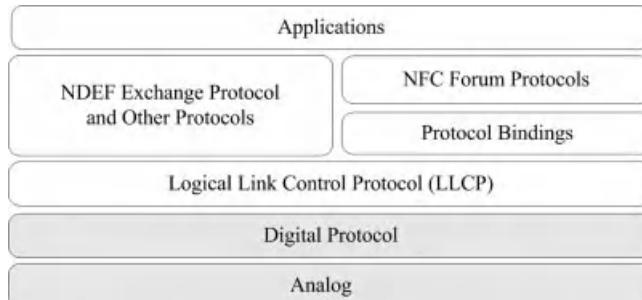


Rysunek 3.29 Architektura komunikacji w trybie pracy peer-to-peer.

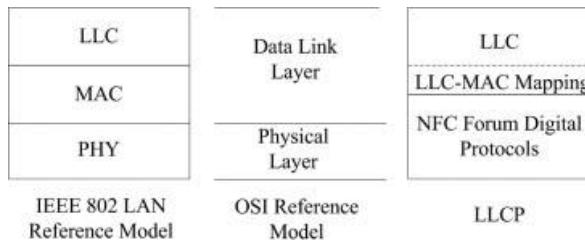
- Prosty protokół wymiany NDEF umożliwia wymianę komunikatów NDEF. Możliwe jest również uruchamianie innych protokołów w warstwie łącza danych zapewnianej przez LLCP.
 - Aplikacje mogą działać w oparciu o prosty protokół wymiany NDEF, inne protokoły lub NFC.
- Protokoły forum. Przykładowe zastosowania to drukowanie z kamery, wymiana wizytówek itp.

3.6.2 LLCP

LLCP definiuje protokół łącza danych OSI do obsługi komunikacji peer-to-peer między dwoma urządzeniami obsługującymi NFC. LLCP jest niezbędny dla każdej aplikacji NFC, która obejmuje komunikację dwukierunkową (patrz rysunek 3.31) [20].



Rysunek 3.30 Stos protokołów w trybie pracy peer-to-peer.



Rysunek 3.31 Związek między LLCP a modelem referencyjnym OSI. Powielono za zgodą NFC Forum.

LLCP zapewnia solidną podstawę dla aplikacji peer-to-peer. Ulepsza również podstawowe funkcje zapewniane przez protokół NFCIP-1. Protokół NFCIP-1 zapewnia SAR (Segmentation and Reassembly) Level 1 Capability, a także kontrolę przepływu danych w zależności od zasady "Go and Wait" typowej dla protokołów półduplekowych. Ponadto protokół NFCIP-1 umożliwia obsługę błędów za pomocą ramki potwierdzenia (ACK) i ramki negatywnego potwierdzenia (NACK) oraz zapewnia uporządkowany przepływ danych. Zapewnia warstwę łączą, która jest niezawodna i wolna od błędów [5].

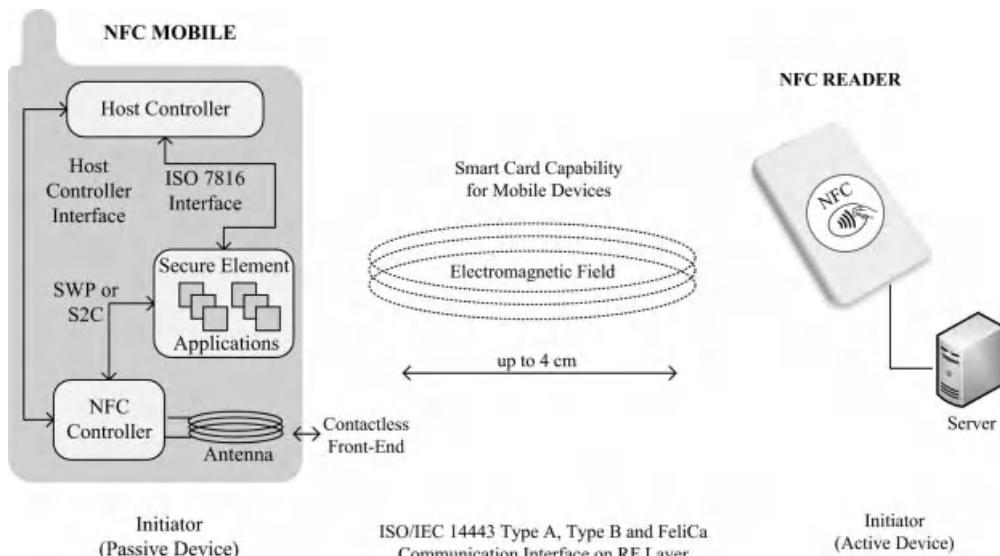
LLCP zapewnia pięć ważnych usług: transport bezpołączeniowy; transfer zorientowany na połaczenie; aktywację, nadzór i dezaktywację łączą; asynchroniczną zrównoważoną komunikację; oraz multipleksowanie protokołów. Zostały one opisane poniżej [20]:

- *Transport bezpołączeniowy:* Transport bezpołączeniowy zapewnia niepotwierdzoną usługę transmisji danych. Ten tryb transportu może być używany, jeśli wyższe warstwy protokołu implementują własne mechanizmy kontroli przepływu. Dlatego warstwy te nie muszą polegać na mechanizmie kontroli przepływu warstwy łączą danych.
 - *Transport zorientowany na połaczenie:* Ten tryb zapewnia usługę transmisji danych z seą gwarantowane dostarczanie jednostek danych usługi. Transmisja danych jest kontrolowana przez protokół okna przesuwnego.
 - *Aktywacja, nadzór i dezaktywacja łączą:* LLCP określa, w jaki sposób dwa urządzenia NFC Forum
- w zasięgu komunikacji rozpoznają kompatybilne implementacje LLCP, ustanawiają łącze LLCP, nadzorują połączenie ze zdalnym urządzeniem równorzędnym i dezaktywują łącze na żądanie.
- *Zrównoważona komunikacja asynchroniczna:* Typowe MAC NFC działają w trybie normalnej odpowiedzi

Tryb, w którym tylko master, zwany inicjatorem, może wysyłać dane do celu i żądać danych od tagu. LLCP umożliwia asynchroniczny tryb zrównoważony (ABM) między punktami końcowymi usługi w dwóch urządzeniach równorzędnych za pomocą mechanizmu symetrii. Korzystając z ABM, punkty końcowe usługi mogą inicjować, nadzorować, odzyskiwać po błędach i wysyłać informacje w dowolnym momencie.

- *Multipleksowanie protokołów:* LLCP jest w stanie pomieścić kilka instancji protokołów wyższego poziomu.
- protokołów w tym samym czasie.

Szczegółowe informacje na temat protokołu LLCP, architektury i procedur można znaleźć w specyfikacji LLCP NFC Forum na stronie internetowej NFC Forum.



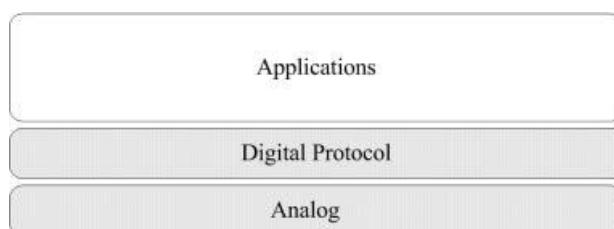
Rysunek 3.32 Architektura komunikacji w trybie emulacji karty.

3.7 Podstawowy tryb pracy emulacji karty

W trybie emulacji karty telefon komórkowy z obsługą NFC działa jak karta inteligentna. Telefon komórkowy z obsługą NFC emuluje kartę inteligentną ISO 14443 lub chip karty intelligentnej zintegrowany z telefonem komórkowym jest podłączony do anteny modułu NFC. Gdy użytkownik zbliża swój telefon komórkowy do czytnika NFC, czytnik NFC inicjuje komunikację. Architektura komunikacji w tym trybie została zilustrowana na rysunku 3.32.

3.7.1 Architektura stosu protokołów w trybie emulacji karty

Urządzenia NFC działające w trybie emulacji karty wykorzystują podobny protokół cyfrowy i techniki analogowe jak karty inteligentne i są całkowicie zgodne ze standardami kart intelligentnych (patrz rysunek 3.33). Tryb emulacji karty obejmuje zastrzeżone aplikacje kart zbliżeniowych, takie jak płatności, bilety i kontrola dostępu. Aplikacje te są oparte na interfejsach komunikacyjnych ISO/IEC 14443 typu A, typu B i FeliCa.



Rysunek 3.33 Stos protokołów w trybie emulacji karty.

Jak pokazano na rysunku 3.32, gdy czytnik NFC wchodzi w interakcję z telefonem komórkowym NFC, telefon komórkowy NFC zachowuje się jak standardowa karta inteligentna, a zatem czytnik NFC wchodzi w interakcję z aplikacjami płatniczymi na SE. Tylko tryb emulacji karty efektywnie i bezpiecznie wykorzystuje SE do wykonywania funkcji wymagających wysokiego poziomu bezpieczeństwa.

Istnieją różne badania i specyfikacje dotyczące zdalnego zarządzania zawartością SE za pośrednictwem technologii Over the Air (OTA), które zostały omówione w rozdziale 8.

3.8 Rozdział Podsumowanie

NFC występuje między dwoma inteligentnymi urządzeniami NFC, które mogą odgrywać rolę inicjatora lub celu. Te urządzenia NFC to telefon komórkowy z obsługą NFC, tag NFC i czytnik NFC. Telefon komórkowy z obsługą NFC jest głównym urządzeniem transakcji NFC, które występuje w każdym typie interakcji.

W celu rozwoju technologii NFC w telefonach komórkowych różne organy normalizacyjne zapewniają otwarte specyfikacje i standardy w celu zwiększenia łatwości dostępu, interoperacyjności i bezpieczeństwa technologii NFC, a także technologii telefonów komórkowych. Wiodące organizacje to NFC Forum, GSMA, GlobalPlatform, OMA i EMVCo. Telefony komórkowe z obsługą NFC mają złożoną architekturę, w tym interfejs NFC, który jest głównym elementem urządzeń NFC, SE z różnymi alternatywami, kontroler hosta i interfejs kontrolera hosta.

NFC działa na częstotliwości 13,56 MHz i przesyła dane z prędkością do 424 kb/s. Komunikacja między dwoma urządzeniami NFC jest ustandaryzowana w normie ISO/IEC 18092 jako NFCIP-1, która obejmuje tylko komunikację między urządzeniami, komunikację peer-to-peer oraz aktywne/pasywne tryby komunikacji czytnik/zapis. Jednak warstwa RF komunikacji NFC jest również zgodna ze standardem ISO/IEC 14443 (tj. standardem zbliżeniowych kart inteligentnych), japońskim standardem JIS X 6319 jako FeliCa (tj. innym standardem zbliżeniowych kart inteligentnych firmy Sony) oraz standardem ISO/IEC 15693 (tj. standardem zbliżeniowych kart inteligentnych). Te interfejsy kart inteligentnych działają na częstotliwości 13,56 MHz z różnymi szybkościami transmisji danych, zakresami komunikacji, a także różnymi funkcjami modulacji i kodowania.

ISO/IEC 14443 jest głównym standardem, który zapewnia zbliżeniowy interfejs komunikacyjny dla transakcji z obsługą NFC, które odbywają się w trybie komunikacji pasywnej. ISO/IEC 14443 ma dwie główne formy: TYP A (np. karty inteligentne MIFARE) i TYP B (np. karty inteligentne Calypso). FeliCa to kolejny ważny interfejs zbliżeniowych kart inteligentnych 13,56 MHz, który jest również kompatybilny z warstwą RF NFC.

NFC może występować w trzech stylach interakcji: między telefonem komórkowym z obsługą NFC a tagiem NFC, między telefonem komórkowym z obsługą NFC a czytnikiem NFC oraz między dwoma telefonami komórkowymi z obsługą NFC. W związku z tymi interakcjami technologia NFC oferuje trzy tryby pracy: tryb pracy czytnika/zapisu, tryb pracy peer-to-peer i tryb pracy emulacji karty. W tym rozdziale omówiono podstawowe zasady komunikacji w każdym z tych trybów. NFC Forum ustandaryzowało wszystkie warstwy od poziomu aplikacji do warstwy RF trybu czytnika/zapisu i trybu peer-to-peer.

W trybie czytnika/zapisu aktywny telefon komórkowy z obsługą NFC inicjuje komunikację bezprzewodową, a następnie odczytuje i/lub zmienia dane zapisane w tagu NFC. W tym trybie telefon komórkowy z obsługą NFC może odczytywać typy tagów zatwierdzone przez NFC Forum. Jest on zgodny z interfejsem komunikacyjnym ISO/IEC 14443 typu A, typu B i FeliCa w warstwie RF. NFC Forum ustandaryzowało typy tagów wymagane przez NFC Forum, a także NFC Data

Format wymiany (NDEF) i różne typy rekordów od warstwy aplikacji do warstwy RF. W przypadku trybu peer-to-peer komunikacja odbywa się między dwoma aktywnymi telefonami komórkowymi NFC. Jeden z telefonów komórkowych inicjuje komunikację, a następnie nawiązywana jest między nimi komunikacja na poziomie łączka. Do komunikacji w warstwie RF wykorzystywany jest standard ISO/IEC18092 NFCIP-1. NFC Forum ustandaryzowało LLCP od warstwy aplikacji do warstwy fizycznej. Tryb emulacji karty umożliwia transakcje wymagające bezpieczeństwa i prywatności z NFC. Daje on możliwość korzystania z kart inteligentnych w telefonach komórkowych i wykorzystuje normy ISO/IEC 14443 Typ A, Typ B i FeliCa. Koncepcja SE jest ważną kwestią w tym trybie do przechowywania i przetwarzania cennych danych i aplikacji.

Rozdział Pytania

1. Dlaczego dwa pasywne urządzenia nie mogą nawiązać komunikacji NFC?
2. Jakie są organy normalizacyjne związane z technologią NFC?
3. Jaki jest ostateczny cel NFC Forum?
4. Jaki jest ostateczny cel GlobalPlatform?
5. Czym jest interfejs NFC? Wyjaśnij jego elementy.
6. Wymień i wyjaśnij alternatywy bezpiecznych elementów (SE).
7. Jakie są różnice między interfejsem przewodowym NFC (NFC-WI) a protokołem jednoprzewodowym (SWP)? Wyjaśnij.
8. Jaka jest różnica między ISO/IEC 14443 a ISO/IEC 15693 pod względem trybu pracy i zakresu?
9. Jakie są główne implementacje zbliżeniowych kart inteligentnych?
10. Jakie jest zastosowanie NFCIP-1?
11. Jakie jest zastosowanie NFCIP-2?
12. Jakie są różnice między tagami typu 1, typu 2, typu 3 i typu 4?
13. Wyjaśnij podstawową strukturę NDEF.
14. Jakie jest znaczenie RTD i jakie są możliwe przypadki jego użycia?
15. Jaki jest dobrze znany typ rekordu NDEF? Podaj kilka przykładów.
16. Co to jest protokół warstwy łączka logicznego (LLCP)? Wyjaśnij jego związek z modelem referencyjnym OSI.
17. Wyjaśnij bezpołączeniowe i zorientowane na połączenia usługi transportowe LLCP.
18. Wyjaśnij znaczenie bezpiecznego elementu w trybie emulacji karty.

Referencje

- [1] NFC Forum, <http://www.nfc-forum.org/> (dostęp: 10 lipca 2011 r.).
- [2] Finkenzeller, K. (2010) *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*, John Wiley & Sons, Lts, ISBN: 978-0-470-69506-7.
- [3] ECMA International (2006) *ECMA 373: Near Field Communication Wired Interface (NFC-WI)*, czerwiec 2006. Dostępny pod adresem: <http://www.ecma-international.org/memento/TC47-M.htm> (dostęp 10 lipca 2011 r.).
- [4] ETSI TS (2008) ETSI TS 102 613, Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Charakterystyka warstwy fizycznej i warstwy łączka danych. Specyfikacja techniczna, wrzesień 2008.
- [5] Tuikka, T. i Isomursu, M. (red.) (2009) *Touch the Future with a Smart Touch*, VTT Tiedotteita - Research Notes 2492, Espoo, Finlandia, 2009. Dostępny pod adresem: www.vtt.fi/inf/pdf/tiedotteet/2009/T2492.pdf (dostęp 10 lipca 2011).

- [6] ETSI TS (2008) *ETSI TS 102 622, Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI)*, Specyfikacja techniczna, luty 2008.
- [7] MIFARE, <http://www.MIFARE.net/products/MIFARE-smart card-ic-s/> (dostęp: 10 lipca 2011 r.).
- [8] FELICA, <http://www.sony.net/Products/felica/> (dostęp: 10 lipca 2011 r.).
- [9] Calypso, <http://www.calypsonet-asso.org/index.php> (dostęp: 10 lipca 2011 r.).
- [10] ECMA International (2004) *ECMA 340: Near Field Communication Interface and Protocol (NFCIP-1)*, grudzień 2004. Dostępny pod adresem: <http://www.ecma-international.org/memento/TC47-M.htm> (dostęp 10 lipca 2011 r.).
- [11] ECMA International (2010) *ECMA 352: Near Field Communication Interface and Protocol (NFCIP-2)*, czerwiec 2 0 1 0 . Dostępny pod adresem: <http://www.ecma-international.org/memento/TC47-M.htm> (dostęp 10 lipca 2011 r.).
- [12] Haselsteiner, E. i Breitfuß, K. *Security in Near Field Communication (NFC)*, Philips Semiconductors. Dostępne pod adresem: <http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf> (dostęp 10 lipca 2011 r.).
- [13] NFC Forum, *NFC Activity Specification*, Specyfikacja techniczna, wersja 1.0, listopad 2010 r.
- [14] NFC Forum, *NFC Data Exchange Format (NDEF)*, Specyfikacja techniczna, wersja 1.0, lipiec 2006 r.
- [15] NFC Forum, *Record Type Definition (RTD)*, Specyfikacja techniczna, wersja 1.0, lipiec 2006.
- [16] NFC Forum, *URI Record Type Definition*, Specyfikacja techniczna, wersja 1.0, lipiec 2006 r.
- [17] NFC Forum, *Smart Poster Record Type Definition*, Specyfikacja techniczna, wersja 1.1, lipiec 2006.
- [18] NFC Forum, *Signature Record Type Definition*, Specyfikacja techniczna, wersja 1.0, listopad 2010 r.
- [19] NFC Forum, *Text Record Type Definition*, Specyfikacja techniczna, wersja 1.0, lipiec 2006.
- [20] NFC Forum, *Logical Link Control Protocol*, Specyfikacja techniczna, wersja 1.0, grudzień 2009 r.

4

Tryby pracy NFC

Istnieją trzy główne urządzenia w NFC; mianowicie telefony komórkowe z obsługą NFC, czytniki NFC i tagi NFC. Dostępne są różne kombinacje tych urządzeń do interakcji mobilnej. Na przykład, telefon komórkowy może komunikować się z czytnikiem NFC, innym telefonem komórkowym lub tagiem NFC. Należy pamiętać, że komunikacja jest tutaj działaniem parami, to znaczy, że tylko dwa urządzenia NFC mogą wchodzić ze sobą w interakcje w tym samym czasie.

Należy również pamiętać, że trzy istniejące tryby pracy to tryb czytnika/zapisu, peer-to-peer i emulacji karty. Tryb czytnika/zapisu umożliwia urządzeniom mobilnym z obsługą NFC wymianę danych z tagami NFC zatwierdzonymi przez NFC Forum. Tryb peer-to-peer umożliwia dwóm urządzeniom mobilnym z obsługą NFC wymianę danych między sobą. W trybie emulacji karty użytkownik wchodzi w interakcję z czytnikiem NFC, aby używać swojego telefonu komórkowego jako karty inteligentnej, takiej jak karta kredytowa. Każdy tryb pracy ma różne scenariusze przypadków użycia i każdy zapewnia różne podstawowe korzyści dla użytkowników.

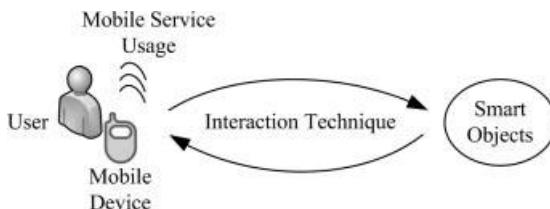
Równolegle do rozważań projektowych i implementacji technologii, komunikacja między urządzeniami musi odbywać się w bardzo bliskiej odległości. Aby zapewnić udaną komunikację, bardzo powszechnie jest dotykanie komunikujących się urządzeń. Z tego powodu proces ten nazywany jest paradygmatem dotykowym.

Niniejszy rozdział początkowo opisuje szczegóły technik interakcji mobilnych, w tym interakcji technologii NFC. Następnie podkreślono szczegóły trybów pracy NFC, scenariusze przypadków użycia i podstawowe korzyści każdego trybu pracy NFC. Na koniec przedstawiono analizy studiów przypadków w celu szczegółowego opisania korzystania z usług NFC.

4.1 Interakcja mobilna Techniki

Urządzenia mobilne są wykorzystywane do świadczenia usług mobilnych, takich jak połączenia telefoniczne, wymiana krótkich wiadomości tekstowych (SMS), korzystanie z Internetu, usług sieciowych itp. W prostym korzystaniu z usług mobilnych zaangażowane są trzy ważne komponenty:

- *Użytkownik* korzystający z urządzenia mobilnego.
- *Urządzenie mobilne*, które jest narzędziem używanym przez użytkownika.
- *Usługa mobilna* uruchamiana za pośrednictwem urządzenia mobilnego.



Rysunek 4.1 Interakcja mobilna.

Są to minimalne wymagania dotyczące wykonywania usług mobilnych. Jednakże, gdy urządzenia mobilne są używane do interakcji z inteligentnymi obiektami w środowisku, dołączane są dodatkowe komponenty. Pierwszym z nich jest inteligentny obiekt, z którym urządzenie mobilne wchodzi w interakcję. Dodatkowo, gdy użytkownik wchodzi w interakcję z inteligentnym obiektem, używana jest *technika interakcji*, która jest paradylematem komunikacji między inteligentnym obiektem a użytkownikiem za pośrednictwem urządzenia mobilnego. Dostępne techniki interakcji wykorzystywane przez urządzenia mobilne, zwane *technikami interakcji mobilnej*, to dotykanie, wskazywanie i skanowanie. W związku z tym interakcja mobilna składa się z pięciu elementów, którymi są użytkownik, urządzenie mobilne, usługa mobilna, inteligentny obiekt i technika interakcji (rysunek 4.1).

Inteligentne obiekty występują w różnych formach i zazwyczaj składają się z czujników. Tagi NFC, tagi RFID i kody kreskowe to kilka przykładów inteligentnych obiektów. Użytkownik korzysta z jednej z technik interakcji mobilnej podczas interakcji z inteligentnym obiektem za pośrednictwem urządzenia mobilnego. Zdefiniujemy tutaj dostępne techniki interakcji mobilnej, a następnie podamy szczegóły interakcji NFC:

(i) Dotykanie

Dotykanie, jak sama nazwa wskazuje, odbywa się poprzez dotknięcie urządzenia mobilnego do inteligentnego obiektu. Dotykanie może również odnosić się do komunikacji z inteligentnym obiektem w bardzo bliskiej odległości. Typowy zasięg wahaj się od 0 do 10 cm [1].

Aby użytkownik mógł wchodzić w interakcję z inteligentnym obiektem za pomocą techniki interakcji dotykowej, użytkownik, urządzenie mobilne i inteligentny obiekt muszą znajdować się bardzo blisko siebie. Dotykanie jest bardzo naturalną, intuicyjną i najbardziej użyteczną techniką interakcji, ponieważ wszystko, co użytkownik musi zrobić, to fizycznie dotknąć urządzenia mobilnego do inteligentnego obiektu.

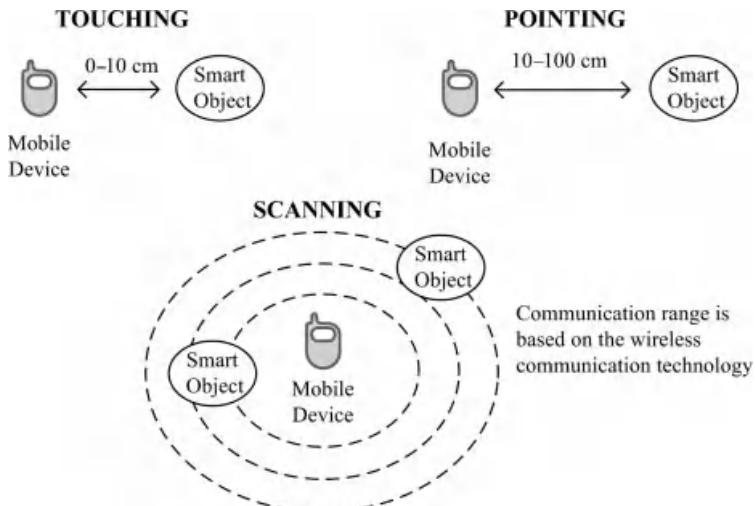
Dobrze znanymi przykładami dotykania są aplikacje technologii RFID, które komunikują się w bardzo bliskim zasięgu. Ponieważ NFC opiera się na technologii RFID, a użytkownik musi dotknąć swojego urządzenia mobilnego do inteligentnego obiektu, NFC również wykorzystuje technikę interakcji dotykowej.

(ii) Wskazywanie

Technika interakcji polegająca na wskazywaniu jest analogiczna do wskazywania obiektu. W przypadku interakcji mobilnej kierujemy nasze urządzenie mobilne na inteligentny obiekt z pewnej odległości. Przykłady tego rodzaju interakcji można zobaczyć w znacznikach wizualnych i kamerach opartych na wskazywaniu. Odczytywanie kodów QR (Quick Response) [2] jest jednym z przykładów tej techniki interakcji.

Kod QR (który jest również opisany w rozdziale 2) jest podobny do kodu kreskowego i jest specyficzny kodem matrycowym, który można odczytać za pomocą czytników kodów kreskowych QR lub telefonów komórkowych

wyposażonych w aparat fotograficzny. Różnica między kodem QR a kodem kreskowym polega na tym, że ponieważ kod QR jest dwuwymiarowym matrycowym kodem kreskowym, może przechowywać znacznie więcej informacji niż kod kreskowy. W kodzie QR można zapisać dowolny rodzaj informacji, takich jak tekst, adres URL lub inne dane.



Rysunek 4.2 Techniki interakcji mobilnej.

Interakcja ta zachodzi zazwyczaj w odległości od 10 cm do 100 cm. Interakcje, które występują poza tym zakresem, nie są już określane jako wskazywanie [1].

(iii) Skanowanie

Technika interakcji skanowania zazwyczaj obejmuje wykrywanie inteligentnych obiektów w środowisku przy użyciu technologii komunikacji bezprzewodowej. Najlepszym praktycznym przykładem jest technologia Bluetooth. Jedną z zalet tej techniki jest to, że użytkownik nie musi być świadomy dokładnej lokalizacji inteligentnego obiektu; urządzenie po prostu wyszukuje inteligentne obiekty w zasięgu. Po wykryciu dowolnego obiektu użytkownik może wchodzić w interakcje z wykrytym inteligentnym obiektem za pomocą swojego urządzenia mobilnego [1].

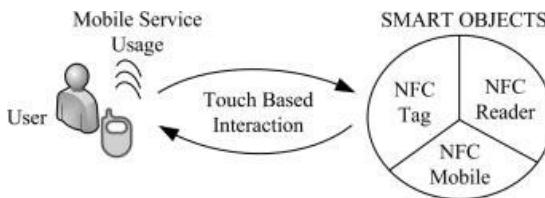
Trzy techniki interakcji przedstawiono na rysunku 4.2. Różnice między technikami interakcji podano w tabeli 4.1.

4.1.1 Technologia NFC Interakcja Technika

Jak zdefiniowano wcześniej, technologia NFC wymaga zetknięcia dwóch kompatybilnych urządzeń NFC na odległość kilku centymetrów. Świadomość użytkownika jest niezbędna do nawiązania komunikacji NFC.

Tabela 4.1 Techniki interakcji mobilnej

Technika interakcji mobilnej	Zasięg komunikacji	Świadomość
inteligentnego obiektu Dotykanie	Od 0 do 10 cm	cm
Skanowanie oparte	Wskazywanie Od 10 do 100 cm na komunikacji bezprzewodowej ak technologii	Tak Br



Rysunek 4.3 Interakcja technologii NFC.

Technika interakcji technologii NFC opiera się na dotyku, jak pokazano na rysunku 4.3. Użytkownik najpierw wchodzi w interakcję z inteligentnym obiektem (tagiem NFC, czytnikiem NFC lub innym telefonem komórkowym obsługującym NFC) za pomocą swojego telefonu komórkowego. Po dotknięciu urządzenie mobilne może korzystać z otrzymanych danych, a tym samym może dodatkowo korzystać z usług mobilnych, takich jak otwieranie strony internetowej, nawiązywanie połączenia z usługą internetową itp.

4.2 Klasyfikacja urządzeń NFC

NFC działa w bardzo intuicyjny sposób. Dwa urządzenia NFC natychmiast rozpoczynają komunikację, gdy zostaną dotknięte. Dotknięcie jest traktowane jako warunek wyzwalający komunikację NFC. Ten prosty model jest w rzeczywistości jedną z ważnych właściwości technologii NFC. Aplikacja na urządzeniu komputerowym może zostać uruchomiona przez użytkownika lub inną inicjatywą aplikacji. W przypadku urządzeń mobilnych, jednym z typowych scenariuszy może być sytuacja, w której użytkownik otwiera menu, wybiera element skrótu, naciska OK i tak dalej. W przypadku NFC jest to banalnie proste. Aplikacja NFC została zaprojektowana w taki sposób, że gdy telefon komórkowy dotyka jakiegoś urządzenia NFC z oczekiwana formą danych, natychmiast się uruchamia. W związku z tym użytkownik nie musi już wchodzić w interakcję z urządzeniem mobilnym, a jedynie dotyka jednego odpowiedniego urządzenia NFC, którym może być tag NFC, czytnik NFC lub inny telefon komórkowy. Możliwe są również bardziej wyrafinowane scenariusze. Rozważmy, że na tym samym telefonie komórkowym dostępne są dwie lub więcej aplikacji NFC. Gdy użytkownik dotyka innego urządzenia NFC, uruchamia się aplikacja zaprojektowana do interakcji z dotknietym obiektem, ale nie inne aplikacje. Biorąc pod uwagę wymagania wszechobecnego przetwarzania, jest to bardzo przydatna właściwość komunikacji NFC.

Możemy sklasyfikować urządzenia NFC w komunikacji w oparciu o dwa parametry. Pierwszym parametrem jest zasilanie, które skutkuje urządzeniami aktywnymi i pasywnymi. Drugi to inicjowanie komunikacji, które prowadzi do urządzeń inicjujących i docelowych.

4.2.1 Aktywne i pasywne urządzenia

Definicje urządzeń aktywnych i pasywnych są ważne dla zrozumienia komunikacji NFC. Urządzenie aktywne to takie, które jest zasilane przez jakieś źródło energii - takie jak bateria - dzięki czemu generuje własne pole elektromagnetyczne. Z drugiej strony, urządzenie pasywne to takie, które nie ma żadnego zintegrowanego źródła zasilania. Zasadą natury jest, że każda aktywność wymaga energii; dlatego nawet urządzenie pasywne wymaga pewnej mocy, aby działać zgodnie z wcześniejszym programem. W komunikacji NFC energia jest dostarczana przez drugą (aktywną) stronę dla urządzenia pasywnego. Podsumowując, urządzenie aktywne zasila urządzenie pasywne poprzez wytworzenie pola elektromagnetycznego.

Tabela 4.2 Kombinacje urządzeń NFC

Urządzenia	Inicjator	Cel
Aktywny		✓
Pasywny	X	

4.2.2 Urządzenia inicjujące a docelowe

NFC zawsze występuje między dwiema stronami, więc jedna strona nazywana jest inicjatorem, a druga strona nazywana jest celem. Inicjator jest tym, który inicjuje komunikację; cel odpowiada na żądanie złożone przez inicjatora. Ten przypadek jest analogiczny do dobrze znanej architektury klient-serwer. Należy pamiętać, że w komunikacji klient-serwer klient inicjuje komunikację, a serwer odpowiada. W komunikacji NFC nie jest inaczej.

Inicjator oczywiście zawsze musi być urządzeniem aktywnym, ponieważ wymaga źródła zasilania do zainicjowania komunikacji. Z drugiej strony, cel może być urządzeniem aktywnym lub pasywnym. Jeśli cel jest urządzeniem aktywnym, wykorzystuje własne źródło zasilania, aby odpowiedzieć; jeśli jest urządzeniem pasywnym, wykorzystuje energię wytwarzaną przez pole elektromagnetyczne generowane przez inicjator, który jest urządzeniem aktywnym.

Tag RFID lub tag NFC jest urządzeniem o niskim koszcie i małej pojemności. W związku z tym nie zawiera żadnego źródła zasilania i potrzebuje zewnętrznego źródła zasilania, aby wykonać jakąkolwiek czynność. Tak więc tag NFC jest zawsze urządzeniem pasywnym, ponieważ z założenia nie zawiera żadnego źródła energii. Zawiera dane, które mogą być odczytane przez aktywne urządzenie NFC. Z tego samego powodu może być tylko celem, a nie inicjatorem.

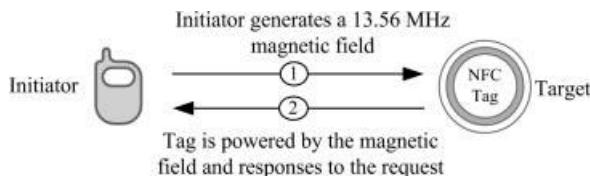
Podsumowując, NFC występuje między jednym inicjatorem NFC a jednym celem NFC. Urządzenie aktywne może pełnić dowolną rolę, podczas gdy urządzenie pasywne może być tylko celem (patrz Tabela 4.2). Inicjator wysyła żądania do celu, a cel odpowiada na te żądania, tak jak w architekturze klient-serwer.

4.3 Tryb Reader/Writer

Tryb czytnika/zapisu dotyczy komunikacji telefonu komórkowego obsługującego technologię NFC z tagiem NFC w celu odczytu lub zapisu danych z lub do tych tagów. Wewnętrznie definiuje dwa różne tryby: tryb czytnika i tryb zapisu.

W trybie czytnika inicjator odczytuje dane z tagu NFC, który już zawiera żądane dane. Wspomniany tutaj tag NFC jest jednym z typów tagów zatwierdzonych przez Forum NFC, jak opisano w rozdziale 3. Oprócz wymogu, aby tag NFC zawierał już żądane dane, składa się on również z programu, który zwraca żądane dane do inicjatora.

W trybie zapisu telefon komórkowy działa jako inicjator i zapisuje dane w tagu. Jeśli tag zawiera już jakieś dane przed procesem zapisu, zostaną one nadpisane. Algorytm może być nawet zaprojektowany w taki sposób, że inicjator będzie aktualizował, modyfikując również wcześniej istniejące dane. Chociaż nie jest to powszechna opcja, czytnik NFC, oprócz telefonu komórkowego, może być również używany do odczytu danych z tagu. Możemy nawet wyobrazić sobie czytnik NFC



Rysunek 4.4 Tryb czytnika/zapisu.

który zapisuje dane w tagu NFC. Maksymalna możliwa szybkość transmisji danych w tym trybie wynosi 106 kb/s. Schematyczne przedstawienie trybu czytnika/zapisu przedstawiono na rysunku 4.4.

Telefon komórkowy może wykonać różne działania po odczytaniu danych z tagu. Jeśli tag przechowuje na przykład dane rejestru push, wówczas aplikacja, która została wcześniej zainstalowana na telefonie komórkowym, może zostać uruchomiona automatycznie. Należy pamiętać, że rekord rejestru push służy do automatycznego uruchamiania aplikacji na urządzeniu mobilnym. Jeśli tag przechowuje adres URL, można uruchomić przeglądarkę internetową i wyświetlić odebraną stronę internetową.

Funkcje telefonów komórkowych, takie jak moc obliczeniowa, funkcje audio/video i dostęp do Internetu wraz z trybem czytnika/zapisu, zapewniają wiele możliwości zarówno użytkownikom, jak i dostawcom usług. Użytkownik może kupić bilet do kina po otwarciu aplikacji mobilnej lub strony internetowej, dotykając swoim urządzeniem mobilnym inteligentnego plakatu. Aplikacje w tym trybie są niezliczone i mogą być bardzo innowacyjne.

4.3.1 Inteligentny plakat

Termin "inteligentny plakat" odnosi się do materiałów reklamowych lub plakatów wyposażonych w tagi NFC. Znaczniki te mogą zawierać różne rodzaje danych, takie jak adres URL, kupon, SMS itp. (patrz rysunek 4.5). Inteligentne plakaty są najczęstszym obszarem użytkowania trybu czytnika/nagrywarki i należy podkreślić niektóre kwestie związane z inteligentnymi plakatami:



Rysunek 4.5 Przypadek użycia inteligentnego plakatu.

(i) *Gdzie dotknąć*

Najważniejszą kwestią w inteligentnych plakatach jest świadomość użytkownika dotycząca punktu dotyku. Inteligentny plakat powinien być zaprojektowany w taki sposób, aby użytkownik nie tracił czasu na szukanie znacznika. Można to osiągnąć za pomocą różnych środków:

- Znak kierujący: W pobliżu znacznika można umieścić znak tekstowy, taki jak "Dotknij tutaj" i/lub dodatkowy obraz oznaczający punkt dotknięcia.
- Obraz telefonu komórkowego: Obraz telefonu komórkowego na lub obok znacznika może być pomocny w oznaczeniu punktu dotyku.
- N-Mark: Logo N-Mark może być używane do oznaczania tagu NFC [3]. Jednak użytkownicy końcowi mogą nie być świadomi znaczenia znaku N-Mark. Dlatego uważamy, że logo N-Mark powinno być dodatkowym elementem i może być używane oprócz dwóch powyższych opcji. Należy pamiętać, że logo N-Mark jest ważnym osiągnięciem, które zostało wprowadzone przez NFC Forum i ma być uniwersalnym symbolem NFC.

(ii) *Świadomość zawartości tagów*

Ponieważ cyfrowa zawartość tagu nie może być odczytana wizualnie, pojawia się pytanie, w jaki sposób umożliwić użytkownikowi odgadnięcie zawartości tagu. Rozwiązanie jest w rzeczywistości dość proste: wstawić materiał reklamowy lub informacje opisowe w pobliżu tagu. Na przykład, jeśli inteligentny plakat reklamuje kupon rabatowy, a na inteligentnym plakacie znajduje się tylko jeden tag, łatwo jest zrozumieć, że tag zawiera kupon. Jeśli jednak na tym samym inteligentnym plakacie znajduje się wiele tagów, tekst opisowy lub obraz powinien być umieszczony obok każdego tagu. Tekst opisowy powinien być krótki (jedno lub kilka słów) i powinien być łatwy do zrozumienia. Przykładowe teksty to "Info", "Dokonaj rezerwacji" i "Oferta dnia".

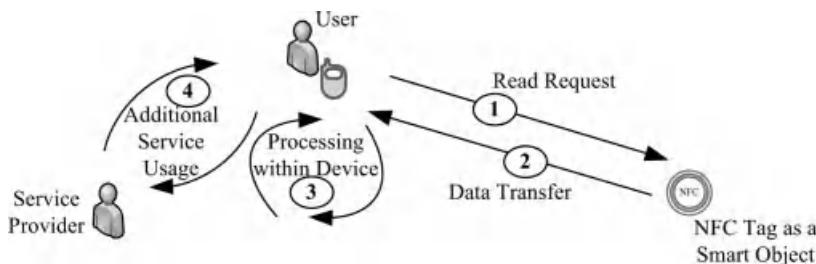
(iii) *Wiarygodność*

Inną ważną kwestią związaną z inteligentnym plakatem jest jego wiarygodność. Termin "wiarygodność" w kontekście inteligentnego plakatu odnosi się do "pewności, że inteligentny plakat zachowuje się zgodnie z oczekiwaniami". Kiedy użytkownik widzi inteligentny plakat, musi zaufać oryginalności, integralności i niezawodności dostawcy inteligentnego plakatu. Wtedy użytkownik będzie miał pewność, że plakat nie zaszkodzi urządzeniu mobilnemu w żaden sposób, na przykład nie spowoduje zainstalowania niezamówionej aplikacji. Aby osiągnąć wiarygodność, najprostszym sposobem jest użycie oryginalnego materiału logo dostawcy. W celu zdobycia zaufania można również wykorzystać różne opcje w zależności od świadczonej usługi.

4.3.2 Ogólne zastosowanie Model

Korzystanie z usługi w każdym trybie pracy NFC różni się, ponieważ interakcje z inteligentnymi obiektami są różne i zapewniają różne scenariusze użytkowania. W trybie czytnika/zapisu użytkownik wchodzi w interakcję z tagiem NFC i używa swojego telefonu komórkowego jako czytnika/zapisu. W tym przypadku usługodawca jest właściwym właścicielem tagu NFC. Jest on jednak tylko pośrednio włączony w proces. Dlatego interakcja NFC odbywa się w trybie offline w odniesieniu do usługodawcy, podczas gdy korzystanie z usługi odbywa się w trybie online, gdy telefon komórkowy wchodzi w interakcję z serwerem po użyciu informacji przechowywanych w tagu NFC. Należy pamiętać, że informacje na tagu są prawdopodobnie informacjami, które zostaną wykorzystane do uzyskania dostępu do serwera dostarczonego przez usługodawcę, takiego jak adres URL strony, informacje o rezerwacji lub dane usługi internetowej sprzedawy biletów. W innym scenariuszu tag NFC

przechowuje adres URL, dzięki czemu powiązana strona internetowa może zostać uruchomiona przez przeglądarkę w telefonie komórkowym.

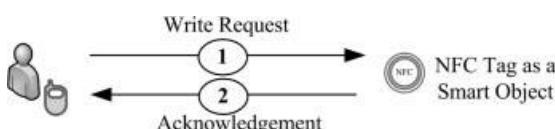


Rysunek 4.6 Ogólny model użytkowania trybu czytnika.

odebrany zostanie adres URL. W jeszcze innym przykładzie znacznik może zawierać informacje o usłudze sieciowej, dzięki czemu aplikacja na telefonie komórkowym może uruchomić usługę sieciową świadczoną przez usługodawcę.

Każdy tryb pracy ma swoją własną charakterystykę, dzięki czemu możliwe jest zdefiniowanie innego modelu użytkowania dla każdego trybu pracy. Ogólne modele użytkowania definiują te cechy, które każdy tryb pracy wykonuje obowiązkowo wraz z zasadą użytkowania technologii. Modele te zostały wyjaśnione w tym rozdziale, aby szczegółowo wyjaśnić korzystanie z każdego trybu pracy. Rysunki 4.6 i 4.7 przedstawiają ogólny model użytkowania odpowiednio dla trybu czytnika i trybu zapisu:

1. *Żądanie odczytu*: Użytkownik żąda danych, dotykając swoim telefonem komórkowym tagu NFC, który może być osadzony w różnych elementach, takich jak inteligentny plakat, pudełko produktu itp.
2. *Transfer danych*: Dane znajdujące się w tagu są przesyłane do telefonu komórkowego.
3. *Przetwarzanie przez urządzenie mobilne*: Gdy dane są przesyłane do telefonu komórkowego, mogą być wykorzystywane do kilku celów, takich jak wypychanie aplikacji, wyświetlanie danych użytkownikowi lub przetwarzanie danych w aplikacji do dodatkowych celów.
4. *Korzystanie z dodatkowych usług*: Ten krok jest opcjonalny i wykorzystuje zaawansowane możliwości telefonu komórkowego, a głównie wiąże się z łącznością z Internetem. Gdy dane są przechowywane w telefonie komórkowym, można je wykorzystać do dalszych operacji za pośrednictwem Internetu, takich jak łączenie się z dostawcą usług za pomocą usługi internetowej.
5. *Żądanie zapisu*: Użytkownik żąda zapisu danych na tagu NFC, dotykając go telefonem komórkowym.
6. *Transfer danych*: Tag NFC odpowiada danymi potwierdzenia, aby poinformować użytkownika o powodzeniu operacji.



Rysunek 4.7 Ogólny model użytkowania trybu zapisu.

4.3.3 Wiodące aplikacje

Istnieją charakterystyczne różnice między trybami pracy NFC, dzięki czemu każdy tryb zapewnia różne przypadki użycia. Na przykład istnieje wiele możliwości wykorzystania trybu czytnika/zapisu. Przesyłane dane mogą być tekstem, adresem URL, identyfikacją produktu lub innym rodzajem danych. Po operacji transferu, dane mogą być wykorzystywane do wielu celów przez telefon komórkowy zgodnie z projektem.

W tym trybie możliwa jest ogromna liczba scenariuszy. Firmy lub specjalisi mogą być skłonni do projektowania projektów w tym trybie ze względu na elastyczność różnych typów danych, które mogą być przechowywane na tagu NFC, a także elastyczność w sposobie wykorzystania tych informacji. W związku z tym szeroki zakres zastosowań w dziedzinie zdrowia, edukacji i rozrywki może być potencjalnie generowany przy użyciu trybu czytnika / zapisu.

4.3.3.1 Gromadzenie informacji

Zdecydowanie najważniejszym przypadkiem użycia trybu czytnika/nagrywarki jest gromadzenie informacji. Większość aplikacji do gromadzenia informacji obejmuje inteligentne aplikacje plakatowe. W swojej pierwotnej formie gromadzenie informacji obejmuje odczytywanie informacji z tagu NFC, a następnie przechowywanie lub wyświetlanie ich na telefonie komórkowym. Istnieją dwie opcje przechowywania danych:

- Rzeczywiste dane mogą być przechowywane na tagu;
- Znacznik zawiera adres URL strony internetowej, która zawiera rzeczywiste dane.

Zaletą przechowywania danych na tagu jest to, że odbiór przez telefon komórkowy jest łatwy i szybki w przypadku małych ilości; zaletą korzystania z serwera jest to, że może on zawierać większe ilości danych. Przechowywanie danych na serwerze ma jeszcze jedną zaletę: dane mogą być łatwo aktualizowane w odniesieniu do modyfikacji wszystkich tagów NFC, które zawierają nieaktualne dane. Gdy dane mają być przechowywane na zdalnym serwerze, korzystanie z usługi internetowej zapewnia również wygodne i nowoczesne rozwiązanie. Aby korzystać z usługi internetowej, na urządzeniu mobilnym należy zainstalować odpowiednią aplikację, która może z niej korzystać.

Jeśli ilość danych jest niewielka i statyczna, rozsądniej jest osadzić dane w tagu, ponieważ nie będzie potrzeby aktualizowania danych w tagach. Jeśli jednak usługodawca jest skłonny zapewnić dodatkowe usługi dynamiczne, które mogą być zmieniane lub aktualizowane w czasie, lepszym rozwiązaniem jest skłonienie użytkownika do połączenia się z serwerem usługodawcy.

(i) *Harmonogram pobierania*

Ten przypadek umożliwia użytkownikom pobieranie rozkładów jazdy (np. rozkładów jazdy autobusów) na telefon komórkowy za pośrednictwem inteligentnych plakatów. Jak wspomniano powyżej, rozkłady jazdy mogą być zapisywane w tagu, gdy ilość danych jest niewielka i statyczna, więc nie zmienia się często. Jeśli zmieniają się często, informacje powinny być zapisywane na stronie internetowej, która jest dostępna w przeglądarkach mobilnych lub w serwerze bazy danych, który jest dostępny za pośrednictwem klienta usługi internetowej. Harmonogramami można łatwo zarządzać, jeśli informacje są przechowywane w zasobie internetowym.

(ii) *Informacje o produkcie*

Ten przypadek użycia umożliwia użytkownikom zbieranie informacji o produkcie z

tagu, który jest osadzony na opakowaniu produktu. ~~Najlepszy~~ Przykład specyfikacje techniczne lub informacje o zawartości

produkту mogą być przesyłane do telefonów komórkowych natychmiast po odczytaniu etykiety. Można go również wdrożyć z dodatkowymi opcjami korzystania z Internetu, aby zapewnić dodatkowe specyfikacje, komentarze użytkowników na temat produktu, przedziały cenowe i wiele więcej. Korzystanie z Internetu w tym przypadku jest niezbędne, ponieważ dodatkowe dane wymagają dużej ilości pamięci, która jest większa niż pojemność tagu.

(iii) *Historia produktu*

Ten przypadek użycia umożliwia odczytanie historii produktu za pomocą dołączonego do niego tagu NFC. Na przykład, gdy klient kupuje wołowinę w supermarkecie, można odczytać informacje o produkcji wołowiny, takie jak rasa i wiek krowy, lokalizacja gospodarstwa i rzeźnia, w której została wyprodukowana.

4.3.3.2 Marketing zdalny

Zdalny marketing to kolejny fajny przypadek użycia w trybie czytnika/nagrywarki, który umożliwia rezerwacje i zakupy online.

(i) *Rezerwacja i zakup online*

Rezerwacji i zakupu biletów na spektakle, takie jak kino i teatr, można dokonać online za pomocą inteligentnych plakatów. Znacznik NFC zawiera podsumowanie informacji o występie, które mogą być statyczne. Informacje o harmonogramie mogą być dynamiczne i przechowywane na serwerze. Po połączeniu się z serwerem, użytkownik może dokonać rezerwacji lub zakupu biletu.

(ii) *Oferty specjalne online*

Specjalne oferty, takie jak zniżki w centrach handlowych, sklepach lub na produkty, a także informacje o kampaniach można uzyskać, dotykając urządzeniem mobilnym tagu NFC na inteligentnym plakacie.

(iii) *Zdalne zakupy*

Przypadek użycia zdalnych zakupów można wdrożyć na kilka sposobów, aby umożliwić zakupy online. Weźmy pod uwagę, że wszystkie towary są dostarczane z tagiem NFC dołączonym do ich opakowań. Po spożyciu produktu użytkownik może dotknąć urządzeniem mobilnym tagu na opakowaniu produktu i dodać go do listy zakupów. Następnie użytkownik będzie mógł zamówić listę zakupów online.

4.3.3.3 Mobilne serwisy społecznościowe

(i) *Sieci społecznościowe*

Ogólnie rzeczą biorąc, wszystkie przypadki sieci społecznościowych w trybie czytnika/zapisu obejmują aktualizację informacji o obecności w sieciach społecznościowych. W takim przypadku tagi NFC mogą dostarczać rekord rejestrów push wraz z dodatkowym rekordem informacji o aktualizacji. Należy pamiętać, że rekord rejestrów push jest używany do automatycznego uruchamiania aplikacji na urządzeniu mobilnym. Aktualizacja obecności w serwisach społecznościowych może stać się jedną z ważnych aplikacji w trybie czytnika/nagrywarki. Na przykład w aplikacjach społecznościowych użytkownicy mogą dotykać tagów NFC, które są osadzone przy wejściu do miejsca rozrywki lub instytucji edukacyjnej, aby zaktualizować status lub informacje o lokalizacji podczas wchodzenia lub wychodzenia z miejsca. Informacje o aktualizacji statusu mogą wyglądać następująco:

Wstąpiłem na Uniwersytet ISIK.

(ii) *Usługi oparte na lokalizacji*

Usługi oparte na lokalizacji mogą być wdrażane w różnych kontekstach. Jako usługa dla, powiedzmy, turystów, użytkownicy mogą otrzymywać informacje o najbliższym punkcie kasowym lub centrum informacji turystycznej, a także informacje o mieście, przewodnik turystyczny, mapę miasta lub inne informacje z inteligentnych plakatów. Innymi przykładami w tym kontekście są nawigacje oparte na NFC, rekomendacje wydarzeń społecznościowych i reklamy mobilne oparte na lokalizacji.

Istnieje ogromna liczba przypadków użycia i aplikacji w trybie czytnika/zapisu. Powyżej podaliśmy przypadki użycia, aby pokazać, co mogą zapewnić aplikacje trybu czytnika/zapisu.

4.3.4 Przypadki użycia w trybie Reader/Writer

W tej sekcji przedstawiono krótkie przypadki użycia trybu czytnika/zapisu, aby przedstawić ideę trybu pracy.

4.3.4.1 Gromadzenie informacji

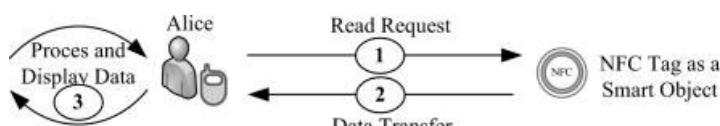
Alice miała za sobą długi dzień na uniwersytecie i była bardzo zmęczona. Siedziała teraz w stolówce. Chciała wiedzieć, gdzie jest następny autobus z uniwersytetu do miasta, ale nie chciała iść na przystanek. Wtedy zobaczyła na ścianie kawiarni elegancki plakat *p r z e d s t a w i a j ą c y* uniwersyteckie autobusy wahadłowe. Zdała sobie sprawę, że może sprawdzić rozkład jazdy autobusów wahadłowych na plakacie. Przyłożyła swój telefon komórkowy z funkcją NFC do znacznika na inteligentnym plakacie.

W tym przypadku istnieją trzy różne opcje modelowania usług NFC:

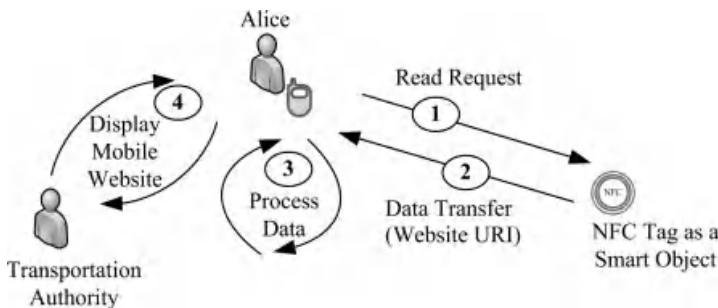
1. Tag NFC przechowuje informacje o harmonogramie.
2. Tag NFC przechowuje adres URL strony internetowej, dzięki czemu strona internetowa przechowuje informacje o harmonogramie.
3. Tag NFC przechowuje dane rejestru push i dodatkowe dane usługi do przetwarzania przez aplikację mobilną (np. aplikacja mobilna zapewnia różne usługi, a dane te umożliwiają aplikacji dostarczanie danych harmonogramu), a serwer przechowuje informacje o harmonogramie, do których można uzyskać dostęp za pośrednictwem usług internetowych.

(i) *Przypadek użycia 1*

1. *Żądanie odczytu*: Alice żąda danych rozkładu jazdy autobusów, dotykając tagu swoim telefonem komórkowym (patrz rysunek 4.8).
2. *Transfer danych*: Dane rozkładu jazdy autobusów znajdujące się w tagu są przesyłane do telefonu komórkowego Alice.



Rysunek 4.8 Przykładowy model użycia zbierania informacji o harmonogramie z tagu NFC.



Rysunek 4.9 Przykładowy model użytkowania gromadzenia informacji o harmonogramie z mobilnej strony internetowej.

3. *Przetwarzanie i wyświetlanie danych:* Telefon komórkowy Alice przetwarza dane i wyświetla informacje o harmonogramie.

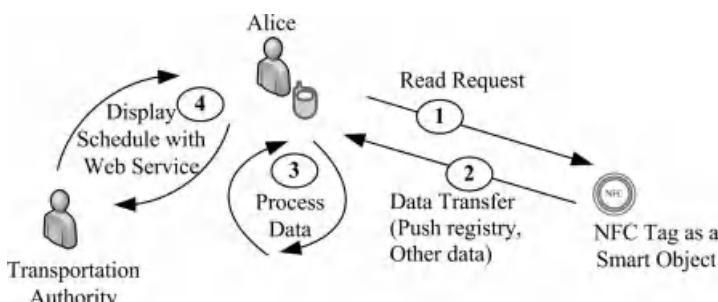
Uwaga: Aby wyświetlić dane bez dodatkowej aplikacji, dane muszą być sformatowane w określony sposób, który telefon komórkowy może zinterpretować za pomocą własnych aplikacji systemu operacyjnego.

(ii) *Przypadek użycia2*

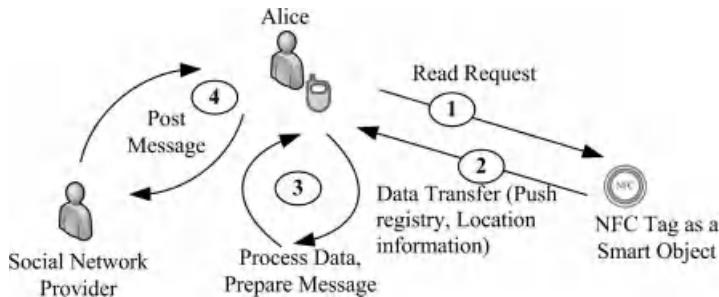
1. *Żądanie odczytu:* Alice żąda danych rozkładu jazdy autobusów, dotykając tagu swoim telefonem komórkowym (patrz rysunek 4.9).
2. *Transfer danych:* Adres URL strony internetowej w tagu jest przesyłany do telefonu komórkowego Alice.
3. *Przetwarzanie danych:* Telefon komórkowy Alice przetwarza dane i odkrywa, że jest to adres URL.
4. *Wyświetlanie strony mobilnej:* Telefon komórkowy Alice uruchamia stronę internetową za pomocą przeglądarki i wyświetla informacje o harmonogramie.

(iii) *Przypadek użycia3*

1. *Żądanie odczytu:* Alice żąda danych rozkładu jazdy autobusów, dotykając tagu swoim telefonem komórkowym (patrz rysunek 4.10).
2. *Transfer danych:* Rejestr Push i dodatkowe dane wymagane do przetworzenia przez aplikację (jeśli istnieją) w tagu są przesyłane do telefonu komórkowego Alice. Dane rejestru Push zostaną wykorzystane do automatycznego uruchomienia aplikacji w telefonie komórkowym. Ponadto aplikacja może wymagać dodatkowych danych (w oparciu o jej projekt), aby wyświetlić użytkownikowi wymagany harmonogram.



Rysunek 4.10 Przykładowy model użycia zbierania informacji o harmonogramie za pośrednictwem usługi sieciowej.



Rysunek 4.11 Przykładowy model użytkowania aktualizacji informacji o obecności w sieci społecznościowej.

- Przetwarzanie danych:** Telefon komórkowy Alice przetwarza dane, uruchamia aplikację i przesyła dodatkowe wymagane dane (jeśli takie istnieją) do aplikacji.
- Wyświetlanie harmonogramu za pomocą usługi sieciowej:** Aplikacja odbiera informacje o harmonogramie od usługodawcy za pośrednictwem usługi internetowej i wyświetla informacje o harmonogramie.

Po zapoznaniu się z rozkładem jazdy autobusu Alice poczuła się komfortowo. Unikała czekania na przystanku autobusowym i odpoczywała w stołówce do czasu odjazdu autobusu.

4.3.4.2 Mobile Social

Alice poszła do niedawno otwartej restauracji ze swoim chłopakiem Bobem. Po kilku minutach zobaczyła znak NFC w pobliżu stolika, który zapewniał mechanizm aktualizacji informacji o obecności w jej sieci społecznościowej. Chciała poinformować znajomych o restauracji.

- Żądanie odczytu:** Alice dotyka swojego telefonu komórkowego do tagu, aby zaktualizować informacje o statusie w swojej sieci społecznościowej (patrz rysunek 4.11).
- Transfer danych:** Dane rejestru Push i informacje o lokalizacji w tagu są przesyłane do telefonu komórkowego. Dane rejestru Push są wykorzystywane do automatycznego uruchamiania aplikacji.
- Przetwórz dane, przygotuj wiadomość:** Aplikacja przetwarza dane, uruchamia aplikację (jeśli nie jest jeszcze uruchomiona) i prosi Alice o potwierdzenie opublikowania komunikatu "I'm now in Sunday Restaurant". Alice dodaje również komentarz "Musisz zobaczyć tę restaurację, chwalebne...".
- Opublikowanie wiadomości:** Alice wysyła wiadomość do swojego dostawcy sieci społecznościowej za pośrednictwem aplikacji mobilnej.

W ciągu kilku minut jej najlepsza przyjaciółka, Julia, skomentowała jej post. Alice była bardzo zadowolona, że mogła podzielić się wiadomościami o restauracji ze swoimi przyjaciółmi.

4.3.5 Aplikacja bazowa Korzyści

Każdy tryb pracy NFC zapewnia różne możliwości zastosowania. Każdy przypadek użycia

zapewnia użytkownikom różne korzyści. W tej sekcji podano szczegółowe informacje na temat tych podstawowych korzyści aplikacji w trybie czytnika/zapisu.

Ogólnie rzecz biorąc, telefon komórkowy i jego aplikacje zapewniają mobilność; a to z kolei generalnie zmniejsza zapotrzebowanie na wysiłek fizyczny. Na przykład wykonanie telefonu do kogoś na odległość zapewnia mobilność i eliminuje potrzebę komunikowania się twarzą w twarz. Powoduje to wzrost mobilności i zmniejszenie wysiłku fizycznego. Co więcej, rosnąca moc obliczeniowa i bezprzewodowy dostęp do Internetu w urządzeniach mobilnych umożliwiają użytkownikom komunikowanie się z innymi w podróży i pokonywanie ograniczeń geograficznych. Tryb ten ma również wpływ na wzrost wykorzystania telefonów komórkowych.

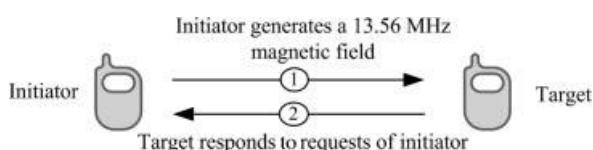
Omówimy teraz kilka przypadków użycia, aby pokazać, w jaki sposób tryb czytnika/zapisu zapewnia te korzyści. W przypadku inteligentnego plakatu, gdy użytkownik doryka swoim telefonem tagu na inteligentnym plakacie, wcześniej zapisane dane są przesyłane z tagu do urządzenia mobilnego. Założymy, że te informacje to numer biura pracownika działu. Korzystając z przesłanych informacji, użytkownik może łatwo znaleźć biuro pracownika, eliminując potrzebę zapamiętywania numeru biura, który jest nadal wyświetlany na ekranie urządzenia mobilnego. Procesy te zapewniają użytkownikowi mobilność. Użytkownik może znaleźć swoją drogę, podczas gdy wymagane informacje mogą być nadal odczytywane z ekranu. Eliminuje to również potrzebę drukowania tych informacji.

Rozważmy przypadek zdalnych zakupów, w którym ludzie mogą zamawiać produkty za pomocą tagów osadzonych na opakowaniach produktów. Najpierw użytkownik wybiera żądany przedmiot, dotykając telefonem komórkowym tagu NFC na opakowaniu, a następnie składa zamówienie. W szczególności starsi użytkownicy będą mogli łatwo robić zakupy z domu, co skutkuje zmniejszonym wysiłkiem fizycznym. Jeśli przyjrzymy się już o p r a c o w a n y m rozwiązaniom, możemy z łatwością wyobrazić sobie wiele innych zastosowań trybu czytnika/zapisu. Opracowywanie i wdrażanie aplikacji trybu czytnika/zapisu jest stosunkowo łatwe w porównaniu z innymi aplikacjami trybu operacyjnego. Istnieje również wiele interesujących i łatwych do wdrożenia scenariuszy przypadków użycia, które mogą być opracowany w tym trybie.

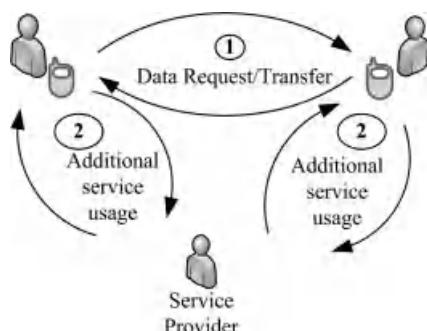
4.4 Tryb peer-to-peer

Tryb peer-to-peer umożliwia dwóm urządzeniom mobilnym obsługującym technologię NFC wymianę informacji, takich jak dane kontaktowe, wiadomości tekstowe lub innego rodzaju dane. Tryb ten ma dwie standardowe opcje: NFCIP-1 i LLCP, które zostały już opisane w rozdziale 3. NFCIP-1 wykorzystuje paradygmat inicjator-ceł, w którym inicjator i urządzenia docelowe są definiowane przed rozpoczęciem komunikacji. Jednak w komunikacji LLCP urządzenia są identyczne. Po początkowym uzgodnieniu, decyzja jest podejmowana przez aplikację działającą w warstwie aplikacji.

Ze względu na wbudowane zasilanie telefonów komórkowych, oba urządzenia są w trybie aktywnym podczas komunikacji w trybie peer-to-peer. Dane są przesyłane przez dwukierunkowy kanał półduplexowy, co oznacza, że gdy jedno urządzenie nadaje, drugie musi nasłuchiwać i powinno rozpocząć transmisję danych po zakończeniu pierwszego. Maksymalna możliwa szybkość transmisji danych w tym trybie wynosi 424 kb/s. Schematyczną reprezentację trybu peer-to-peer przedstawiono na rysunku 4.12.



Rysunek 4.12 Tryb peer-to-peer.



Rysunek 4.13 Ogólny model użytkowania trybu peer-to-peer.

4.4.1 Ogólne zastosowanie Model

W trybie peer-to-peer użytkownicy komunikują się ze sobą za pomocą telefonów komórkowych obsługujących technologię NFC. W tym trybie zazwyczaj żaden dostawca usług nie jest wykorzystywany w procesie, co oznacza, że użytkownicy nie komunikują się z nim. Jeśli użytkownicy zamierzają korzystać z jakichkolwiek usług w Internecie, dostawca usług może również zostać włączony do procesu. Rysunek 4.13 przedstawia ogólny model użytkowania trybu peer-to-peer.

1. *Wymiana danych*: Dwóch użytkowników wymienia dane za pośrednictwem telefonów komórkowych.
2. *Dodatkowe wykorzystanie usług*: Gdy dane są udostępniane między telefonami komórkowymi, dane te mogą być opcjonalnie wykorzystywane do dodatkowych celów, takich jak zapisanie otrzymanej wizytówki w bazie danych przez Internet po udanym udostępnieniu lub rozpoczęcie znajomości w sieci społecznościowej.

4.4.2 Wiodące aplikacje

W tej sekcji skupiamy się na głównych aplikacjach, które korzystają z trybu peer-to-peer.

4.4.2.1 Wymiana danych

Wymiana danych jest ważnym przypadkiem użycia tego trybu (patrz rysunek 4.14).

(i) *Wymiana prywatnych danych*

Krytyczne informacje mogą być bezpiecznie przechowywane w urządzeniu mobilnym i mogą być dalej wymieniane z innymi upoważnionymi osobami za pomocą trybu peer-to-peer. Ponieważ komunikacja odbywa się na odległość kilku centymetrów, użytkownicy będą czuli się pewnie, udostępniając prywatne i ważne dane za pomocą technologii NFC. W przypadku ustalenia wyższego poziomu wymagań bezpieczeństwa, należy również zapewnić dodatkowe środki bezpieczeństwa (patrz rozdział 6).

(ii) *Przelew pienięży*

Dwóch użytkowników może wymieniać pieniądze między portfelami przechowywanymi w ich telefonach komórkowych NFC. Prezenty, kupony i bilety mogą być również zaimplementowane jako obiekty wymienne.



Rysunek 4.14 Dwóch użytkowników wymienia się informacjami kontaktowymi.

4.4.2.2 Sieci społecznościowe

Sieci społecznościowe w trybie peer-to-peer obejmują przypadki użycia, w których ludzie wymieniają się swoimi informacjami społecznymi. Dobrym przykładem jest nawiązywanie znajomości w sieciach społecznościowych. Wymiana wizytówek to kolejny przykład.

4.4.2.3 Parowanie urządzeń

Można sparować dwa urządzenia obsługujące technologię NFC, takie jak zestawy słuchawkowe, urządzenia samochodowe, komponenty komputerowe itp.

4.4.3 Przypadki użycia w trybie peer-to-peer

(i) Wymiana danych

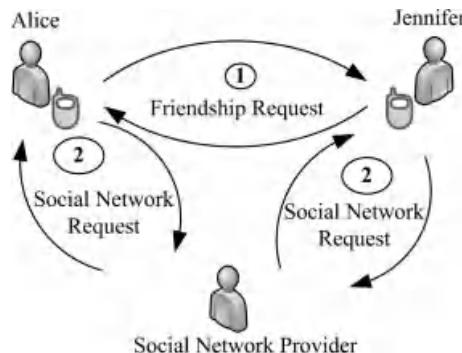
Alice jadła lunch w uniwersyteckiej stołówce. Inna studentka, Jennifer, zapytała, czy może usiąść obok niej. Wcześniej prawie ze sobą nie rozmawiali. Zjadły razem lunch i w międzyczasie rozmawiali. Alice zapytała, czy może uzyskać dane kontaktowe Jennifer. Jennifer wyjęła swój telefon komórkowy, a Alice zobaczyła, że jest to również telefon komórkowy z obsługą NFC.

1. *Przesyłanie wizytówek:* Alice i Jennifer zbliżają do siebie swoje telefony komórkowe. Telefon komórkowy Alice prosi o udostępnienie wizytówek, a Jennifer to akceptuje. Następnie następuje proces udostępniania (patrz rysunek 4.15).

Zarówno Alice, jak i Jennifer otrzymały swoje dane kontaktowe, dzięki czemu będą mogły komunikować się ze sobą w przyszłości.



Rysunek 4.15 Przykładowy model użytkowania wymiany danych.



Rysunek 4.16 Przykładowy model korzystania z sieci społecznościowych.

(ii) Sieci społecznościowe

Alice i Jennifer kontynuowały rozmowę w oczekiwaniu na kolejny wykład. Jennifer wspominała Alice o zabawnym filmiku, który widziała na swoim portalu społecznościowym, a który Alice również widziała poprzedniego dnia. Jennifer uciekszyła się, że Alice również korzysta z tego samego portalu społecznościowego i zasugerowała zaprzyjaźnienie się na ich portalu społecznościowym.

1. *Prośba o przyjaźń:* Alice i Jennifer proszą o przyjaźń w sieci społecznościowej, dotykając swoich urządzeń mobilnych (patrz rysunek 4.16).
2. *Prośba z sieci społecznościowej:* Aplikacja mobilna Alice przesyła prośbę o przyjaźń, a aplikacja mobilna Jennifer przesyła prośbę o akceptację przyjaźni do serwisu społecznościowego, a następnie zostają przyjaciółmi w serwisie.

Alice i Jennifer cieszą się, że zostały przyjaciółkami na portalu społecznościowym. Od teraz będą mogły łatwo się komunikować.

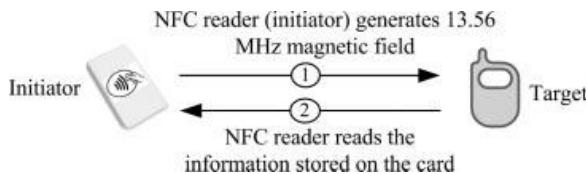
4.4.4 Aplikacja bazowa Korzyści

Liczba aplikacji opracowanych przy użyciu trybu peer-to-peer jest jak dotąd mniejsza niż w przypadku innych trybów pracy. Tryb peer-to-peer jest zwykle używany do parowania urządzeń, tworzenia sieci i przesyłania plików. Parowanie urządzeń Bluetooth, wymiana wizytówek i nawiązywanie nowych znajomości w sieciach internetowych to możliwe implementacje tego trybu. Tryb peer-to-peer zapewnia łatwą wymianę danych między dwoma urządzeniami.

Łatwa wymiana danych pomiędzy dwoma urządzeniami kompatybilnymi z NFC zapewnia możliwość bezpiecznej wymiany prywatnych danych. Urządzenia NFC mogą przesyłać dane na odległość kilku centymetrów, więc wymiana prywatnych i ważnych danych może być jednym z kluczowych przyszłych zastosowań tego trybu.

4.5 Tryb emulacji karty

Tryb emulacji karty zapewnia możliwość działania urządzenia mobilnego z obsługą NFC jako zbliżeniowej karty inteligentnej. Urządzenia mobilne mogą nawet przechowywać wiele zbliżeniowych kart inteligentnych



Rysunek 4.17 Tryb emulacji karty.

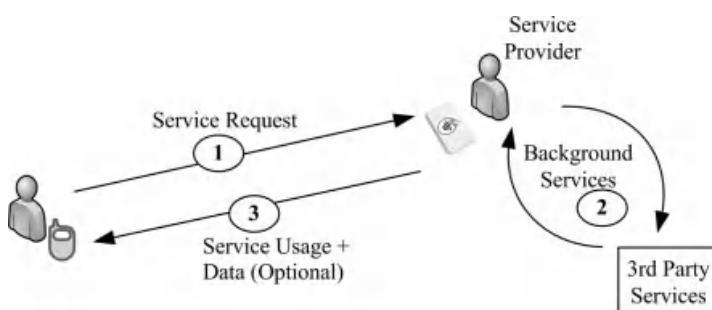
aplikacje na karcie inteligentnej. Przykładami emulowanych zbliżeniowych kart inteligentnych są karty kredytowe, debetowe i lojalnościowe.

W tym trybie pracy telefon komórkowy z obsługą NFC nie generuje własnego pola RF; zamiast tego czytnik NFC tworzy to pole. Obecnie obsługiwane interfejsy komunikacyjne dla trybu emulacji karty to ISO/IEC 14443 Typ A i Typ B oraz FeliCa. Tryb emulacji karty jest ważnym trybem, ponieważ umożliwia płatności i aplikacje biletowe i jest kompatybilny z istniejącą infrastrukturą kart inteligentnych. Schematyczne przedstawienie trybu emulacji karty przedstawiono na rysunku 4.17.

4.5.1 Ogólne zastosowanie Model

W trybie emulacji karty użytkownik wchodzi w interakcję z czytnikiem NFC, zazwyczaj używając swojego telefonu komórkowego jako karty inteligentnej. Czytnik NFC jest własnością dostawcy usług, który może być również połączony do Internetu. W tym trybie pracy użytkownik łączy się z dostawcą usług za pośrednictwem czytnika NFC, być może bez powiadomiania dostawcy usług. Rysunek 4.18 przedstawia model użytkowania trybu emulacji karty.

1. *Żądanie usługi*: Użytkownik wysyła żądanie do usługodawcy poprzez przyłożenie telefonu komórkowego do czytnika NFC. Wymagane dane są przesyłane z telefonu komórkowego do usługodawcy za pośrednictwem czytnika NFC.
2. *Usługi zaplecza*: Dostawca usług uruchamia wymaganą usługę zaplecza po uzyskaniu wymaganych danych z urządzenia mobilnego użytkownika. Przykładami takich usług są autoryzacja kart kredytowych i validacja biletów.
3. *Korzystanie z usługi*: Dostawca usługi zwraca użytkownikowi usługę, taką jak wystawienie biletu, który został już zakupiony za pomocą karty płatniczej, autoryzacja płatności itd.



Rysunek 4.18 Ogólny model użytkowania trybu emulacji karty.

Usługodawca może również opcjonalnie wysyłać dane do urządzenia mobilnego użytkownika, takie jak kupon, bilet, paragon itp.

4.5.2 Wiodące aplikacje

W tej sekcji przedstawiono główne implementacje trybu emulacji karty.

(i) Płatność

Istnieją różne rodzaje zastosowań płatności NFC. Nie ma wątpliwości, że najważniejszymi aplikacjami płatniczymi są karty kredytowe i debetowe, które mogą być uruchamiane przez czytniki NFC. Istnieją również inne możliwości płatności NFC, takie jak przechowywanie i używanie voucherów, korzystanie z kart podarunkowych itp.

(ii) Lojalność

Punkty lojalnościowe można zdobywać w punktach płatności, a następnie wykorzystywać je do robienia darmowych zakupów lub otrzymywania prezentów. Ponadto kupony pobierane za pośrednictwem inteligentnych plakatów w trybie czytnika/zapisu mogą być dalej wykorzystywane przez czytniki NFC korzystające z tego trybu pracy.

(iii) Sprzedaż biletów

Przypadki użycia związane z biletami mogą być wdrażane w różnych formach. Użytkownicy mogą przechowywać różne rodzaje biletów, takie jak bilety teatralne, autobusowe i lotnicze, które zostały wcześniej pobrane za pomocą inteligentnych plakatów lub w inny sposób. Bilety te mogą być następnie wykorzystywane w bramkach obrotowych lub punktach walidacji w trybie emulacji karty. Przedpłacone lub miesięczne karty biletowe mogą być również przechowywane i używane.

(iv) Kontrola dostępu

Przypadki użycia kontroli dostępu umożliwiają użytkownikom przechowywanie obiektów kontroli dostępu w urządzeniach mobilnych. Przykłady takich przypadków obejmują elektroniczne klucze do samochodów, budynków, bezpiecznych obszarów i pokoi hotelowych. Zameldowanie w hotelu to interesujący przypadek użycia, który umożliwia otrzymanie klucza do pokoju za pośrednictwem technologii OTA przed przybyciem do hotelu i bezpośrednim zameldowaniem się w pokoju. W tym przypadku nie ma więc powodu, aby spędzać czas w recepcji po przyjeździe.

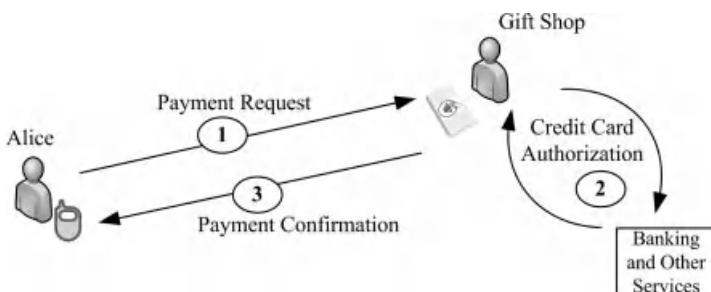
(v) Usługi identyfikacyjne

Innym interesującym przypadkiem użycia tego trybu jest przechowywanie informacji opartych na tożsamości na urządzeniach mobilnych i umożliwienie autoryzowanemu personelowi dostępu do nich. Przykładem tego typu usługi jest przechowywanie danych pacjenta. Historia pacjenta może być przechowywana na urządzeniu mobilnym, a użytkownik może następnie zezwolić lekarzowi na dostęp do tych danych za pośrednictwem czytnika NFC. Zwiększa to prywatność użytkownika, ponieważ niepożądane osoby trzecie, takie jak firmy ubezpieczeniowe, nie będą miały dostępu do informacji o pacjencie. W tej kategorii można opracować jeszcze bardziej interesujące aplikacje, takie jak integracja krajowych kart identyfikacyjnych, paszportów, odcisków palców i praw jazdy z telefonami komórkowymi.

(vi) Inteligentne środowisko

Przypadek inteligentnego środowiska odnosi się do wykorzystania technologii NFC w inteligentnych środowiskach (inteligentny dom, biuro itp.). Najczęstszym przykładem jest zarządzanie inteligentnymi środowiskami za pomocą wstępnie skonfigurowanych danych w telefonie komórkowym. W tym przypadku, gdy użytkownik

wchodzi do inteligentnego środowiska, określone ustawienia inteligentnego środowiska (np. poziom jasności, wybór utworu) można dostosować za pomocą urządzenia mobilnego. Można go również zintegrować z mechanizmem kontroli dostępu, dzięki czemu gdy użytkownik otworzy drzwi za pomocą klucza elektronicznego NFC, można aktywować spersonalizowane inteligentne środowisko.



Rysunek 4.19 Przykładowy model użytkowania płatności kartą kredytową.

4.5.3 Przypadki użycia w trybie emulacji karty

W tej sekcji przedstawiono i szczegółowo zilustrowano przypadki użycia płatności kartą kredytową i sprzedaży biletów.

(i) Płatność kartą kredytową

Alicja z radością znalazła w centrum handlowym prezent na urodziny Boba. Zaniosła go do kasjera, który zaprosił, jakiej metody płatności zamierza użyć. Alice zauważała znak NFC i poinformowała kasjera, że zapłaci kartą kredytową NFC.

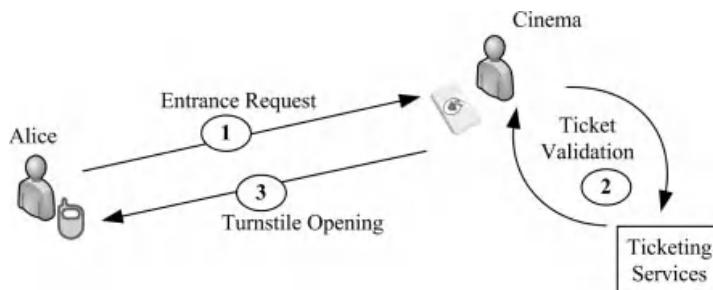
- 1. Żądanie płatności:** Alice żąda płatności NFC, dotykając swojego telefonu komórkowego do czytnika NFC (patrz rysunek 4.19). Czytnik NFC odczytuje wymagane dane karty kredytowej i przetwarza je. Telefon komórkowy może być postrzegany jako inicjator w tym procesie, jednak urządzeniem wytwarzającym pole magnetyczne jest czytnik NFC, a zatem czytnik NFC jest urządzeniem inicjującym. Czynność dotykowa użytkownika może być postrzegana jako czynność wyzwalająca.
- 2. Autoryzacja karty kredytowej:** Czytnik NFC wysyła informacje o karcie do usług bankowych w celu autoryzacji karty kredytowej. Usługa autoryzacji odpowiada na żądanie transakcji.
- 3. Potwierdzenie płatności:** Telefon komórkowy jest następnie powiadamiany o transakcji. Alice z przyjemnością zapłaciła swoim telefonem komórkowym.

(ii) Sprzedaż biletów

Alice dała Bobowi prezent urodzinowy. Wybrali się razem na film. Alice wcześniej zarezerwowała miejsca, a bilety były zapisane w jej telefonie komórkowym. Kiedy dotarli do kina, weszli bezpośrednio do środka, nie czekając w kolejce po bilety. Następnie podeszli do kołowrotów. Alice cieszyła się, że ma telefon komórkowy z funkcją NFC i była szczęśliwa, że zarezerwowała za jego pomocą bilety.

- 1. Żądanie wejścia:** Alice prosi o wejście do teatru, dotykając swojego telefonu komórkowego do czytnika NFC. Czytnik NFC odczytuje wymagane dane biletu przechowywane w bezpiecznym elemencie i przetwarza je (patrz rysunek 4.20).
- 2. Walidacja biletu:** Czytnik NFC wysyła informacje o biletie do serwera biletowego w celu jego walidacji. Alternatywnie, walidacja może być również przeprowadzona w trybie offline za pośrednictwem aplikacji na czytniku NFC.
- 3. Otwarcie bramki obrotowej:** Po zatwierdzeniu biletu system otwiera bramkę obrotową, aby Alice i Bob mogli przez nią przejść.

Alice i Bob nie musieli czekać w kolejce i nie spóźnili się do kina.



Rysunek 4.20 Przykładowy model użytkowania sprzedaży biletów.

4.5.4 Aplikacja bazowa Korzyści

Wcześniej stwierdziliśmy, że telefony komórkowe zapewniają użytkownikom mobilność w trybie czytnika/zapisu. Jednak tryb emulacji karty nie wspiera mobilności; jego celem jest ścisłe powiązanie telefonu komórkowego z jego użytkownikiem. Mamy na myśli to, że korzystanie z telefonu komórkowego w trybie emulacji karty nie wpływa na mobilność użytkownika, ponieważ użytkownik jest już mobilny, nawet jeśli nosi karty kredytowe do wykonywania tych samych funkcji. Tryb emulacji karty eliminuje jedynie potrzebę noszenia kart. Ludzie noszą ze sobą telefony komórkowe przez większość czasu, więc połączenie telefonów komórkowych z ludzkim ciałem pasuje do ich zastosowania. Można oczekwać, że w niedalekiej przyszłości ludzie będą nosić telefony komórkowe z obsługą NFC nie tylko w celu uzyskania mobilności, ale także w celu wykonywania codziennych funkcji. Wszystkie karty kredytowe, klucze, bilety itp. będą prawdopodobnie wbudowane w telefony komórkowe. W związku z tym w przyszłości pojawi się więcej możliwości integracji przedmiotów codziennego użytku z telefonami komórkowymi obsługującymi technologię NFC.

Podsumowując, dominującą cechą trybu emulacji karty jest wyeliminowanie potrzeby posiadania fizycznego obiektu. Kilka przykładów może zilustrować tę cechę. W aplikacjach płatniczych korzystanie z telefonu komórkowego eliminuje potrzebę noszenia przy sobie stykowych i bezstykowych kart kredytowych, kart debetowych i gotówki. Co więcej, w aplikacjach biletowych, telefon komórkowy z obsługą NFC eliminuje fizyczne przedmioty, eliminując potrzebę noszenia biletów papierowych lub elektronicznych. W aplikacji kontroli dostępu lub klucza elektronicznego, użycie NFC eliminuje potrzebę noszenia fizycznego klucza lub bezstykowego klucza inteligentnego. Ponieważ służy do wchodzenia do pomieszczeń bez użycia kluczy elektronicznych, zapewnia również kontrolę dostępu. W rezultacie najważniejszymi zaletami aplikacji w trybie emulacji karty jest eliminacja obiektów fizycznych i zapewnienie kontroli dostępu.

Jesteśmy w stanie wyeliminować potrzebę noszenia fizycznych przedmiotów poprzez osadzenie tych informacji w telefonach komórkowych obsługujących technologię NFC. Obecnie karty kredytowe, bilety, klucze i kupony są używane z telefonami komórkowymi obsługującymi NFC, ale wciąż istnieje wiele ekscytujących opcji użytkowania. W telefonach komórkowych będziemy mogli przechowywać wiele obiektów, takich jak karty identyfikacyjne, paszporty, odciski palców i prawa jazdy. Większość z tych przyszłych opcji rozwoju wciąż wymaga rozwiązania, ale wszystkie mają duży potencjał do zrealizowania.

4.6 Przegląd korzyści płynących z obsługi Tryby

Korzyści płynące z każdego trybu pracy podano w powyższej sekcji dotyczącej każdego

trybu. Tabela 4.3 podsumowuje korzyści płynące z każdego trybu ~~zasięgu~~.

Tabela 4.3 Korzyści z każdego trybu pracy

Tryb czytnika/zapisu	Tryb Peer-to-Peer	Tryb emulacji karty
- Zwiększa mobilność	- Łatwa wymiana danych	- Eliminacja obiektów fizycznych
- Zmniejsza wysiłek fizyczny	- Parowanie urządzeń	- Kontrola dostępu
- Możliwość dostosowania do wielu scenariuszy		
- Łatwy do wdrożenia		

Podsumowując, najważniejszym trybem NFC jest tryb emulacji karty, ponieważ NFC zapewnia dwa duże ulepszenia w tym trybie: eliminację fizycznego obiektu i zapewnienie kontroli dostępu za pomocą urządzenia mobilnego. Dostępne na rynku aplikacje (płatności, klucze elektroniczne, bilety itp.) zazwyczaj korzystają z trybu emulacji karty. Tryb emulacji karty jest obecnie najbardziej obiecującym trybem technologii NFC [4].

Ważnym punktem, który należy porównać w trybach pracy, jest dostęp do usługodawcy. Komunikacja z usługodawcą odbywa się na różne sposoby w każdym z trybów. W trybach czytnika/zapisu i peer-to-peer telefon komórkowy wykonuje połączenie za pomocą funkcji dostępu do Internetu telefonu komórkowego, podczas gdy jest ono wykonywane przez czytnik NFC w trybie emulacji karty. W związku z tym użytkownik nie jest świadomym połączenia z dostawcą usług w trybie emulacji karty, ponieważ połączenie jest nawiązywane płynnie przez czytnik, a użytkownik nie podejmuje żadnych działań, aby osobiście nawiązać połączenie. Jednak w innych trybach użytkownik jest świadomym, że otrzymuje usługę, ponieważ usługa jest wizualizowana w telefonie komórkowym (w przeglądarce, aplikacji itp.) i najczęściej wymaga również zatwierdzenia. Podsumowanie interakcji z dostawcami usług przedstawiono w tabeli 4.4.

4.7 Przypadek Studia

Przedstawiamy trzy studia przypadków, aby zilustrować wszystkie trzy tryby działania i ich zastosowania. Pierwszy przypadek to system zakupów z obsługą NFC, który umożliwia użytkownikom robienie zakupów online bez żadnych ograniczeń geograficznych. W tym przypadku wykorzystywany jest tryb czytnika/zapisu. Drugi przypadek to aplikacja plotkarska oparta na NFC, która działa w taki sam sposób jak plotkowanie i rozpowszechnianie informacji między rówieśnikami w trybie peer-to-peer. Trzeci przypadek to aplikacja do sprzedaży biletów do kina, która umożliwia również dokonywanie płatności za pomocą trybu emulacji karty.

Dla każdego studium przypadku opis przypadku jest podany jako pierwszy. Następnie przedstawiono diagramy przypadków użycia, diagramy aktywności i ogólne modele użycia. Programowanie aplikacji dla pierwszych dwóch przypadków podano w rozdziale 5. Przypadki te są otwartymi aplikacjami NFC, co oznacza

Tabela 4.4 Interakcja z dostawcą usług

Tryby pracy	Inicjator	Cel	Łączenie z dostawcą usług	Świadomość dostawcy usług
Czytelnik/napisarz	Urządzenie mobilne	Znacznik NFC	Przez Internet	Tak
Emulacja karty	Czytnik NFC	Urządzenie mobilne	Poprzez czytnik NFC	Nie

Peer-to-peer	Urządzenie mobilne	Urządzenie mobilne	Przez Internet	Tak
--------------	-----------------------	-----------------------	----------------	-----

że przypadki nie muszą obejmować wielu podmiotów i ekosystemu NFC. Użytkownicy mogą korzystać z tych aplikacji po pomyślnym wdrożeniu i instalacji. Jednak trzecie studium przypadku jest bezpieczną aplikacją NFC i obejmuje wiele podmiotów w swojej strukturze. Analizujemy środowisko ekosystemu i modele biznesowe tego studium przypadku na końcu rozdziału 7, ale nie przedstawiamy jego programowania.

4.7.1 Studium przypadku trybu czytnika/zapisu: NFC Zakupy

(i) Wprowadzenie do sprawy

ROSCAXT to sieć supermarketów działająca w wielu miastach. Obecnie oferuje zarówno zakupy na rynku, jak i zakupy online za pośrednictwem swojej strony internetowej. Głównym zamiarem ROSCAXT jest obniżenie kosztów na rynku poprzez zwiększenie zakupów online; w ten sposób będą w stanie obniżyć swoje koszty i zwiększyć przychody. Są jednak niezadowoleni z niskiego poziomu penetracji rynku internetowego przez użytkowników i chcą zaoferować użytkownikom łatwiejsze zakupy dzięki nowym i innowacyjnym technologiom. Użytkownicy powinni również dobrze się bawić na nowej stronie internetowej, aby regularnie robili na niej zakupy.

(ii) Integracja technologii NFC z biznesem

Zdając sobie sprawę z tego, że NFC jest nową i innowacyjną technologią, która zapewnia użytkownikom łatwe i przyjemne doświadczenie, kierownictwo firmy pomyślało, że dobrze byłoby uruchomić zakupy online za pomocą NFC, aby firma miała szansę wyprzedzić konkurencję. Postanowili opracować aplikację na urządzenia mobilne, aby korzystać z zakupów online z obsługą NFC. Rozpoczęli projekt o nazwie "Zakupy NFC" i pozwolili swojemu działowi IT zbudować system obsługujący NFC.

Po przeprowadzeniu analizy wykonalności, dział IT zdecydował się na udostępnienie użytkownikom zakupów NFC poprzez dystrybucję katalogów zakupowych z obsługą NFC. W katalogu produkty są drukowane wraz z ich opisem i ceną. Dodatkowo na stronie każdego produktu znajduje się tag NFC. Użytkownicy będą mogli robić zakupy online, dotykając tagów w katalogu za pomocą swoich telefonów komórkowych i zamawiając online bez żadnych ograniczeń geograficznych.

(iii) Rozwój systemu

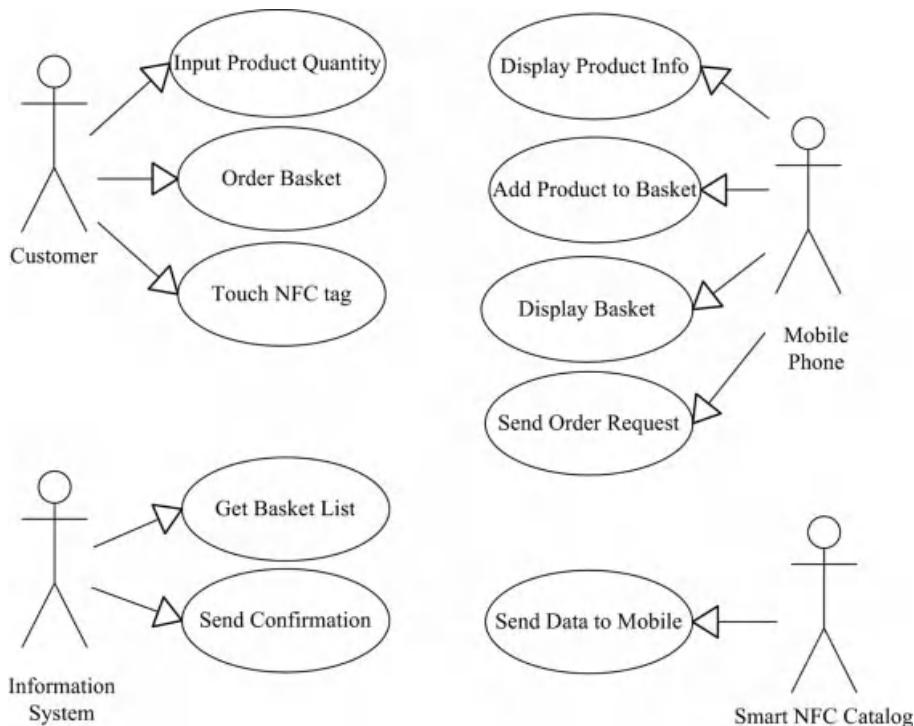
W celu opracowania NFC Shopping wykonywane są następujące kroki:

1. Opis przypadku użycia;
2. Diagram przypadków użycia;
3. Diagram aktywności;
4. Dane w znaczniku;
5. Zastosowanie ogólnego modelu użytkowania trybu czytnika/zapisu do przypadku użycia.

(iv) Opis przypadku użycia

To był pracowity dzień dla Alice. Musi gotować dla swoich gości i musi kupić składniki, ale niestety nie ma czasu na zakupy. Przypomina sobie, że otrzymała już nowy katalog marketu. Na katalogu znajdowało się logo NFC, więc Alice postanawia wypróbować tę nową usługę. Ma przy sobie katalog i telefon komórkowy. Na pierwszej stronie czyta opis, jak robić zakupy za pomocą telefonu komórkowego z obsługą NFC. Znajduje pierwszy produkt, który chce kupić i dotyka go telefonem komórkowym. Następnie uruchamiana jest aplikacja i wybrany produkt jest dodawany do koszyka. Alice dotyka telefonem komórkowym towarów jeden po

drugim i dodaje je do koszyka. W koszyku znajdowały się tylko żagle



Rysunek 4.21 Diagram przypadków użycia NFC Shopping.

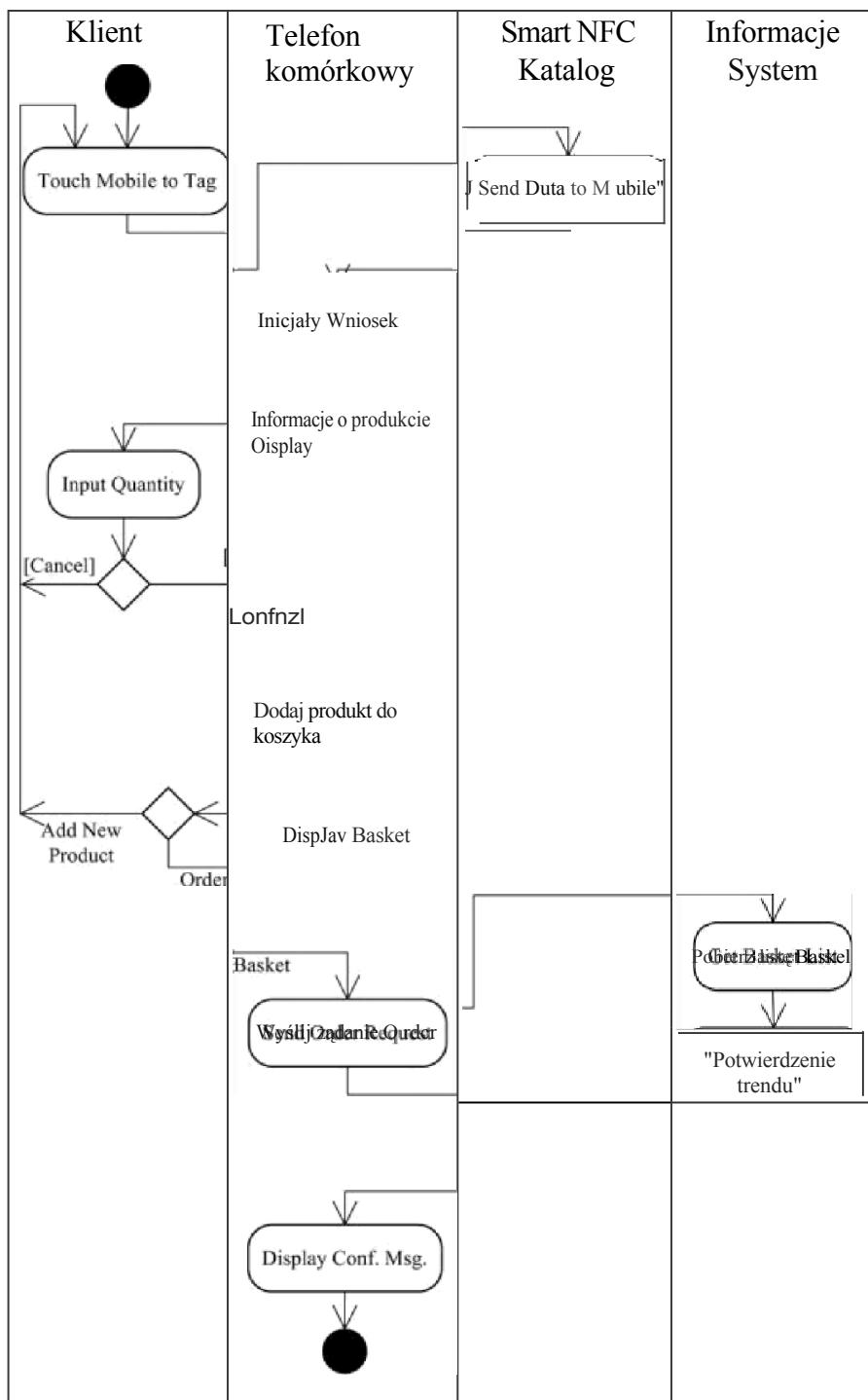
pozostała jedna czynność do wykonania: zamówienie produktów. Zamówiła swój koszyk bez wychodzenia z aplikacji i to był koniec procesu.

(v) *Diagram przypadków użycia*

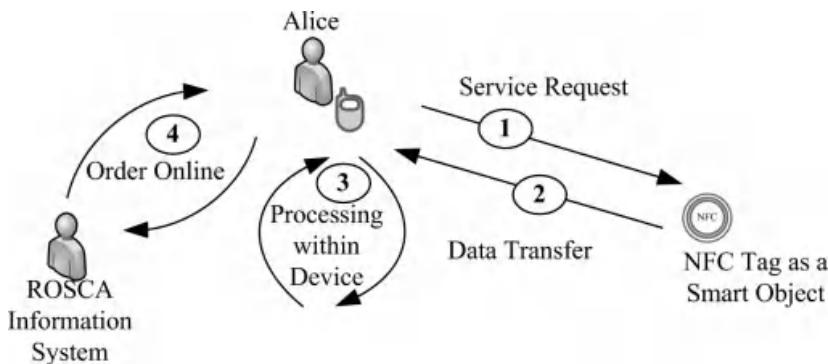
W diagramach przypadków użycia pokazujemy głównie, które funkcje aplikacji są wykonywane przez którego aktora. W naszym konkretnym systemie uwzględniamy czterech aktorów, a mianowicie klienta, telefon komórkowy klienta, katalog NFC i system zaplecza. Klient jest jednym z głównych aktorów, który komunikuje się za pomocą telefonu komórkowego. Wybiera również produkt, dotykając telefonem komórkowym powiązanego tagu i wprowadza wymaganą ilość do aplikacji. Gdy koszyk jest gotowy, użytkownik zamawia go przez Internet. Telefon komórkowy wykonuje faktyczne przetwarzanie, a także komunikację z tagami NFC. System informatyczny wykonuje wymagane operacje na serwerze zaplecza, takie jak przetwarzanie koszyka i wysyłanie odpowiedzi potwierdzającej do telefonu komórkowego. Z drugiej strony tag NFC wysyła tylko zapisane dane do urządzenia mobilnego. Schemat przypadku użycia przedstawiono na rysunku 4.21.

(vi) *Diagram aktywności*

Jak wspomniano powyżej, w obecny system zaangażowane są cztery podmioty. Diagram aktywności przedstawiony na rysunku 4.22 pokazuje działania krok po kroku, działania czterech podmiotów, a także komunikację z innymi podmiotami.



Rysunek 4.22 Diagram aktywności w przypadku zakupów NFC.



Rysunek 4.23 Model użytkowania w przypadku zakupów NFC.

(vii) *Dane w znaczniku*

Aby wdrożyć usługę, wymagane dane powinny zostać przesłane z tagu NFC do urządzenia mobilnego:

- *Wpis rejestr push:* Służy do automatycznego uruchamiania aplikacji mobilnej, gdy użytkownik dotknie tagu.
- *Identyfikacja produktu:* Jest to klucz główny dla każdego produktu. Dane te zostaną wysłane do serwera informacyjnego po zamówieniu koszyka wraz z żądanymi ilościami. System informacyjny będzie w stanie zidentyfikować żądane produkty przy użyciu tych danych. Należy pamiętać, że użytkownik wprowadzi żądaną ilość produktu.
- *Informacje o produkcie:* Służą do wyświetlania użytkownikowi krótkiego opisu produktu.
- *Cena produktu:* Służą do wyświetlania ceny produktu użytkownikowi.

(viii) *Ogólny model korzystania z zakupów NFC*

W tym rozdziale przedstawiliśmy już ogólne modele użytkowania trybów pracy. Ogólny model użycia trybu operacyjnego zapewnia model, który prawie pasuje do użycia wszystkich aplikacji w tym samym trybie operacyjnym. Przypadek użycia NFC Shopping wykorzystuje tryb czytnika/zapisu, a jego użycie w ramach ogólnego modelu użytkowania trybu czytnika/zapisu przedstawiono poniżej (patrz rysunek 4.23).

1. *Żądanie usługi:* Alice dotyka swojego telefonu komórkowego do tagu w inteligentnym katalogu NFC.
2. *Transfer danych:* Rejestr Push, identyfikacja produktu, informacje o produkcie i cena produktu są przesyłane do telefonu komórkowego.
3. *Przetwarzanie przez urządzenie mobilne:* Aplikacja jest uruchamiana za pomocą danych rejestr push (jeśli nie została jeszcze uruchomiona). Następnie telefon komórkowy wykonuje wymagane przetwarzanie, takie jak wyświetlanie użytkownikowi informacji o produkcie, proszenie użytkownika o wprowadzenie danych, dodawanie produktu do koszyka itd.
4. *Zamówienie online:* Alice zamawia bieżący koszyk, a telefon komórkowy komunikuje się z serwerem supermarketu za pośrednictwem usługi mobilnego Internetu lub usługi Wi-Fi. Serwer potwierdza to żądanie i wysyła wiadomość potwierdzającą pomyślne otrzymanie wymaganych danych.

4.7.2 Studium przypadku trybu peer-to-peer: NFC Gossiping

(i) Wprowadzenie do sprawy

Plotkowanie jest interakcją społeczną, a mianowicie bezczynną rozmową głównie na tematy prywatne. Jest to jedna z najczęstszych metod dzielenia się informacjami między ludźmi. Choć plotkowanie czasami odnosi się do dzielenia się błędnymi informacjami między ludźmi, w tym przypadku odnosimy się do plotkowania jako bezczynnej rozmowy w celu rozpowszechniania informacji.

Celem przypadku plotkowania jest ustanowienie cyfrowej usługi plotkowania, aby ludzie mogli rozpowszechniać informacje wśród innych peer-to-peer. Technologia NFC zapewnia tutaj ważną infrastrukturę, ponieważ komunikacja odbywa się na niewielką odległość i wymaga rzeczywistego dotyku. Podobnie jak w klasycznym plotkowaniu, dwie osoby muszą znajdować się wystarczająco blisko siebie w plotkowaniu NFC. Informacje nie są jednak wiedzą ukrytą, jak w przypadku klasycznego plotkowania, ale znajdują się w pamięci telefonu komórkowego.

(ii) Rozwój systemu

W celu opracowania wymaganego plotkowania NFC wykonywane są następujące kroki:

1. Opis przypadku użycia;
2. Diagram przypadków użycia;
3. Diagram aktywności;
4. Struktura danych plotek;
5. Zastosowanie ogólnego modelu użytkowania trybu peer-to-peer do przypadku użycia.

(iii) Opis przypadku użycia

Alice była na kampusie i siedziała w stołówce. Przypomniała sobie, że słyszała o czymś, co wydarzyło się wczoraj między Joe i Jennifer. Stworzyła wiadomość, wpisując ją do aplikacji plotkarskiej i zapisała ją. Później zobaczyła Boba i chciała podzielić się z nim tą plotką. Wybrała wiadomość do udostępnienia i zbliżyła swój telefon komórkowy do telefonu Boba. Bob odebrał wiadomość, przeczytał ją i zapisał na swoim telefonie komórkowym.

Jak widać w przypadku użycia, plotkowanie NFC jest prawie identyczne z klasycznym plotkowaniem. Nowe plotki mogą być tworzone, a plotki mogą być wymieniane z innymi za pomocą technologii NFC. Ponieważ technologia ta umożliwia przesyłanie danych w promieniu kilku centymetrów, pasuje ona do idei klasycznego plotkowania.

(iv) Diagram przypadków użycia

Nasz system obejmuje użytkownika, telefon komórkowy użytkownika i zdalny telefon komórkowy jako aktorów. Użytkownik jest tym, który czyta przychodzące plotki i tworzy nowe. Telefon komórkowy użytkownika wykonuje niezbędne funkcje komunikacji NFC, takie jak udostępnianie plotek zdalnemu telefonowi komórkowemu, wyświetlanie otrzymanych plotek i przechowywanie plotek. Diagram przypadków użycia dla plotkowania NFC przedstawiono na rysunku 4.24.

(v) Diagram aktywności

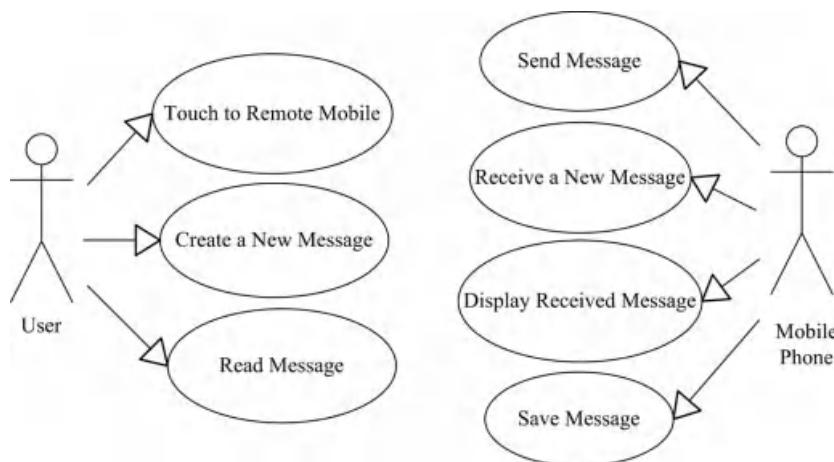
Diagram aktywności przedstawia krok po kroku czynności i działania uczestników (patrz rysunki 4.25 i 4.26).

(vi) Struktura danych plotek

Aby wdrożyć wymaganą usługę, dane plotek powinny być przechowywane w pamięci urządzenia mobilnego. Następujące dane muszą być przechowywane w celu wykonania niezbędnych funkcji:

- *Wiadomość plotkarska:* Jest to rzeczywista wiadomość, która zostanie wysłana do urządzeń równorzędnych.
- *Nazwa grupy:* Zawiera zdefiniowane nazwy grup.

Domyślnie w aplikacji zdefiniowana jest grupa "publiczna". Kolejne grupy mogą być definiowane przez użytkownika.



Rysunek 4.24 Diagram przypadków użycia plotkowania NFC.

– *Grupa wiadomości*: Przechowuje odpowiednią grupę każdej wiadomości. Ponieważ każda wiadomość zostanie udostępniona następnej osobie zgodnie z jej grupą, dane grupy są wymagane.

(vii) Ogólny model użytkowania plotek NFC

Opisany przypadek użycia pasuje do ogólnego modelu użytkowania trybu peer-to-peer (patrz rysunek 4.27). Chociaż w ogólnym modelu użytkowania trybu peer-to-peer istnieje opcjonalna faza korzystania z usług, nie jest ona wymagana w przypadku plotkowania. Nie ma potrzeby korzystania z dodatkowych usług z Internetu, więc wymiana wiadomości będzie odbywać się tylko lokalnie.

1. *Plotkujące przesyłanie wiadomości*: Alice przekazuje Bobowi wiadomość, którą chce udostępnić.

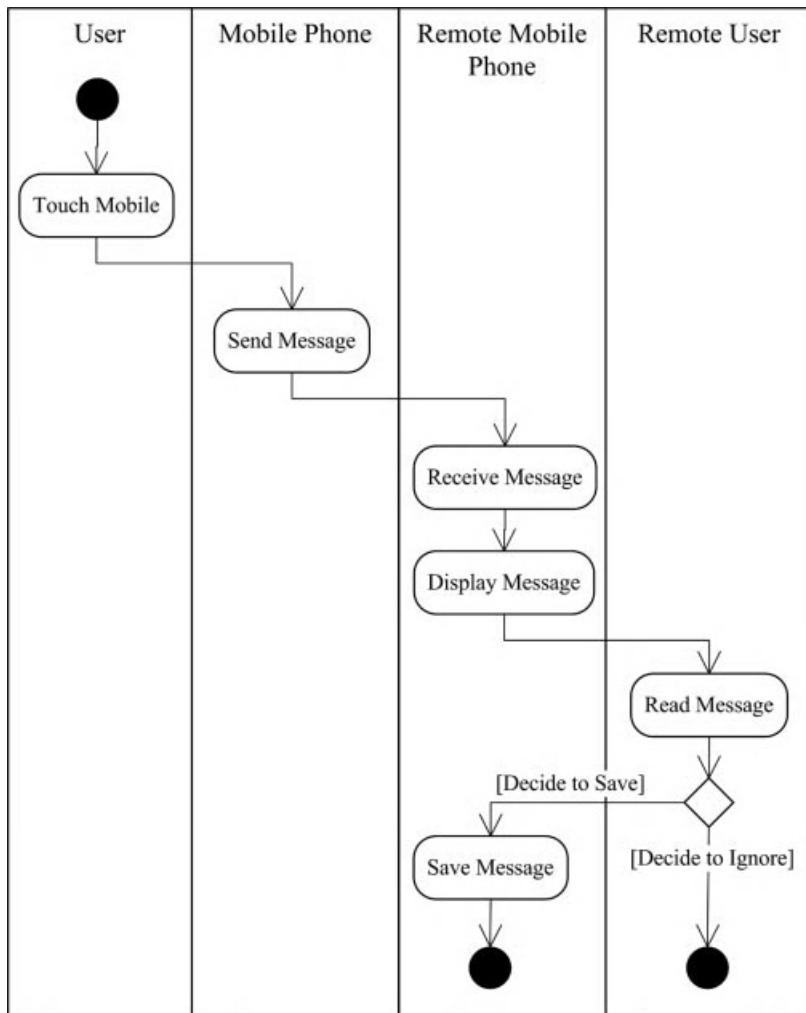
4.7.3 Studium przypadku trybu emulacji karty: NFC Sprzedaż biletów

(i) Wprowadzenie do sprawy

ROSCAXINE to firma kinowa działająca w wielu miastach. W przypadku tradycyjnej metody klient może kupić bilet w kiosku, płacąc kartą kredytową. Aby zapłacić, klient przesuwa kartę kredytową w automacie kiosku. Urządzenie drukuje papierowy bilet dla użytkownika. Przy wejściu do sali kinowej czytnik kodów kreskowych odczytuje kod kreskowy umieszczony na wydrukowanym bilecie i otwiera bramkę obrotową. Inną opcją jest zakup biletu w kasie. Klient może zapłacić gotówką lub kartą kredytową. Następnie bilet jest drukowany przez kasjera i wydawany klientowi.

Głównym celem ROSCAXINE jest zwiększenie świadomości marki poprzez promowanie nowych produktów wśród użytkowników. Chcą czerpać korzyści z nowo powstającej technologii NFC.

Po analizie stwierdzili, że technologia NFC zapewnia użytkownikom łatwe i pozytywne doświadczenia. Nie mieli żadnych zastrzeżeń co do osadzenia technologii NFC w swoich projektach biznesowych.



Rysunek 4.25 Diagram aktywności plotkowania NFC.

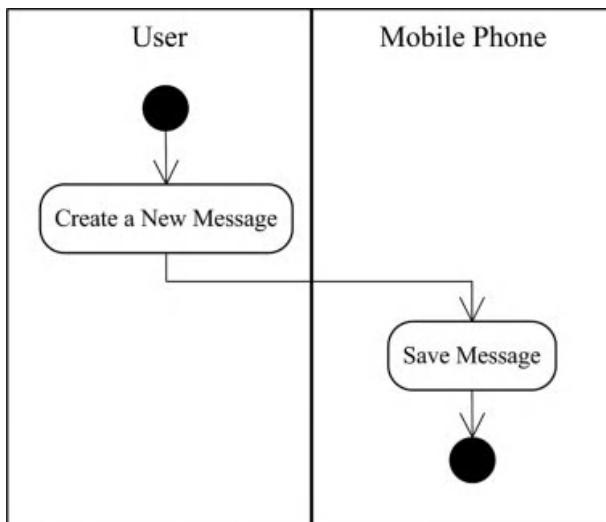
(ii) Rozwój systemu

Aby opracować wymagany projekt sprzedaży biletów NFC, wykonamy następujące kroki:

1. Opis przypadku użycia;
2. Diagram przypadków użycia;
3. Diagram aktywności;
4. Zastosowanie ogólnego modelu użytkowania trybu emulacji karty do przypadku użycia.

(iii) Opis przypadku użycia

Bob był w domu, gdy zadzwonił jego telefon komórkowy. Dzwoniła Alice i zaproponowała wyjście do kina. Alice i Bob udali się do kina po bilety. Alice podeszła do kiosku, aby kupić bilety i dowiedziała się, że ROSCAXINE właśnie zintegrował technologię NFC.



Rysunek 4.26 Diagram aktywności plotkowania NFC.

w automatach kioskowych. Wybrała film, godzinę i miejsca, a następnie zapłaciła za bilety za pomocą telefonu komórkowego z obsługą NFC, dotykając telefonu komórkowego do czytnika wbudowanego w kiosk. Po potwierdzeniu płatności dotknęła kolejnego tagu, aby przenieść bilety na swój telefon komórkowy. Był to prosty proces. Następnie Alice i Bob podeszli do bramki obrotowej przy wejściu do kina. Alice przyłożyła swój telefon komórkowy do czytnika na kołowniku, po czym kołownik się otworzył.

(iv) *Diagram przypadków użycia*

Nasz system obejmuje użytkownika, telefon komórkowy użytkownika, kiosk, bramkę obrotową i zdalne systemy zaplecza jako aktorów. Użytkownik jest aktorem, który inicjuje proces. Kiosk odczytuje informacje o karcie kredytowej na telefonie komórkowym oraz tworzy i wysyła bilety za pośrednictwem OTA. Czytnik przy kołowniku odczytuje bilet i otwiera kołownik. Proces systemu zaplecza jest wymagany do operacji płatności i sprzedaży biletów. Schemat przypadków użycia dla sprzedaży biletów NFC przedstawiono na rysunku 4.28.

(v) *Diagram aktywności*

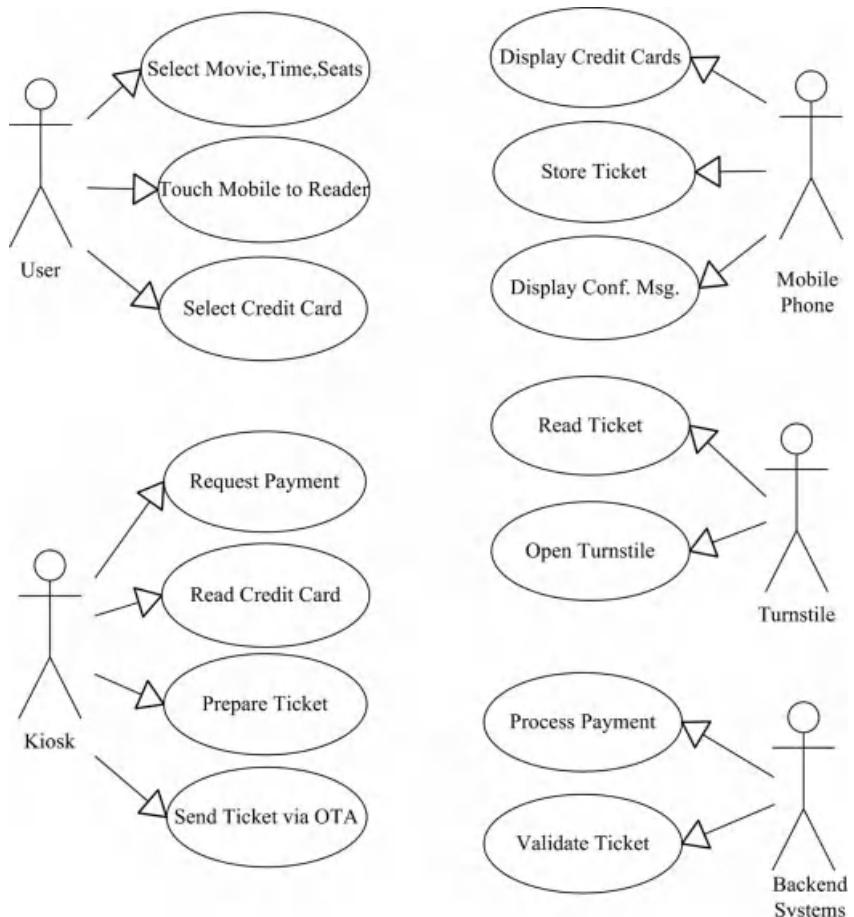
Diagram aktywności przedstawia krok po kroku czynności i działania uczestników (patrz rysunki 4.29 i 4.30).

(vi) *Ogólny model użytkowania sprzedawy biletów NFC*

Ogólny model użytkowania trybu emulacji karty został opisany we wcześniejszych sekcjach. Przypadek użycia biletu NFC obejmuje dwie aplikacje emulacji karty. W związku z tym podane



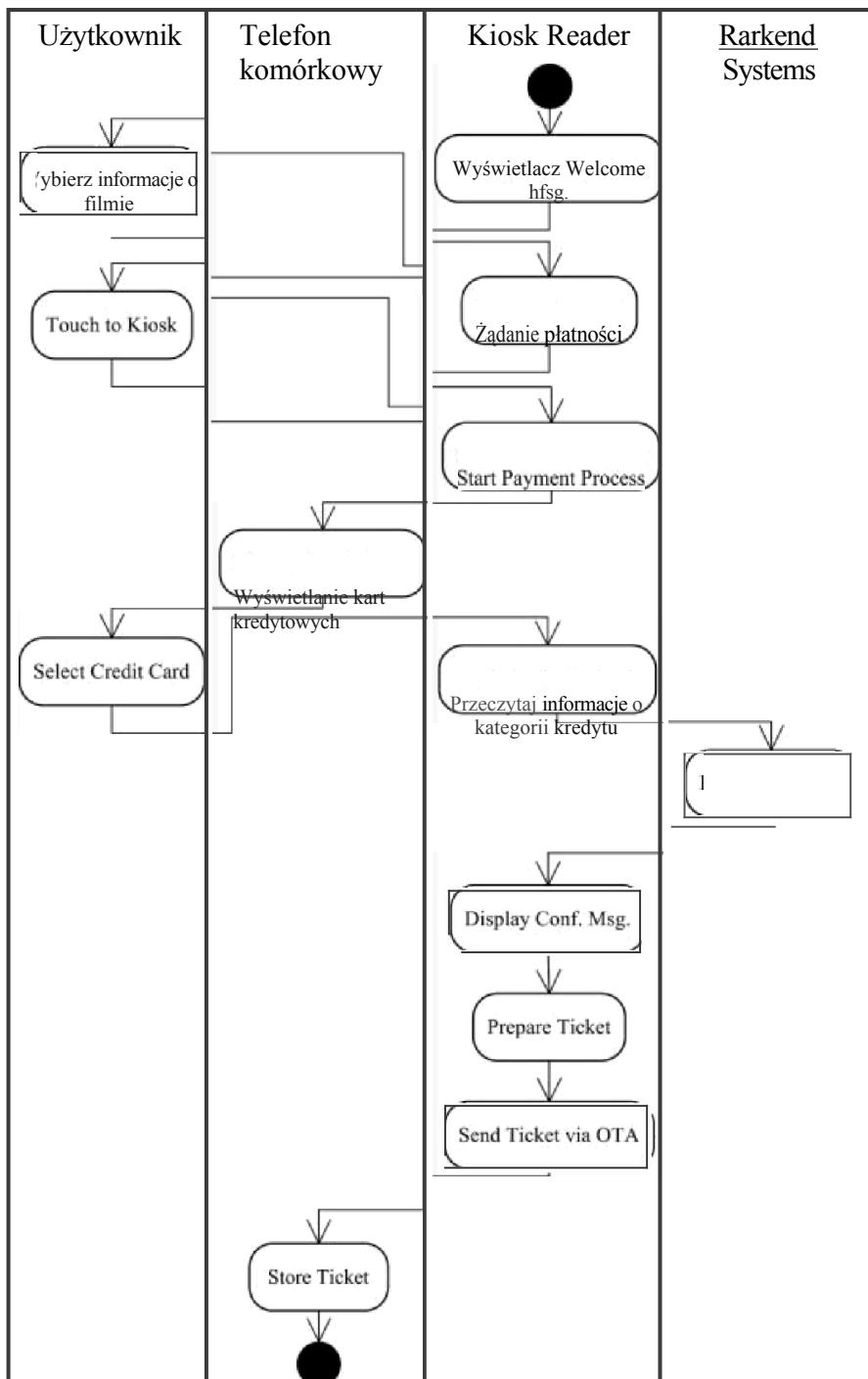
Rysunek 4.27 Model użytkowania w przypadku plotkowania NFC.



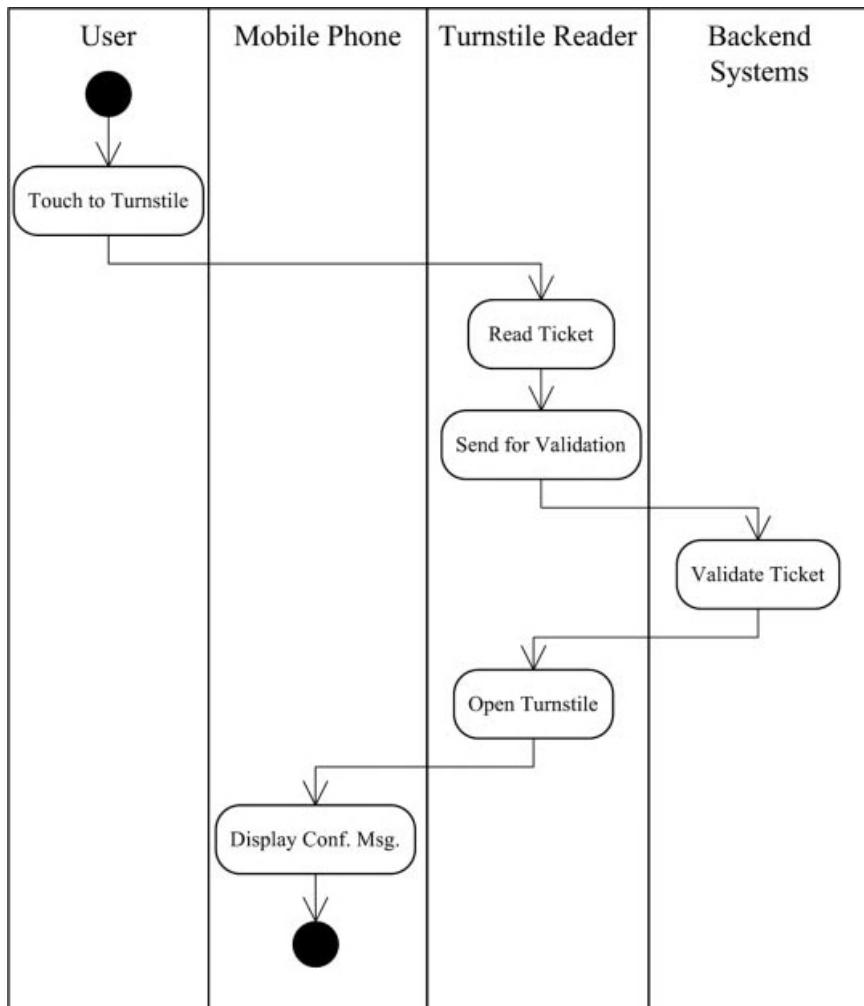
Rysunek 4.28 Diagram przypadków użycia sprzedaży biletów NFC.

Model użytkowania sprzedaży biletów NFC obejmuje dwukrotnie ogólny model użytkowania. Przypadek użycia sprzedaży biletów NFC pasuje do ogólnego modelu użytkowania trybu emulacji karty (patrz rysunek 4.31).

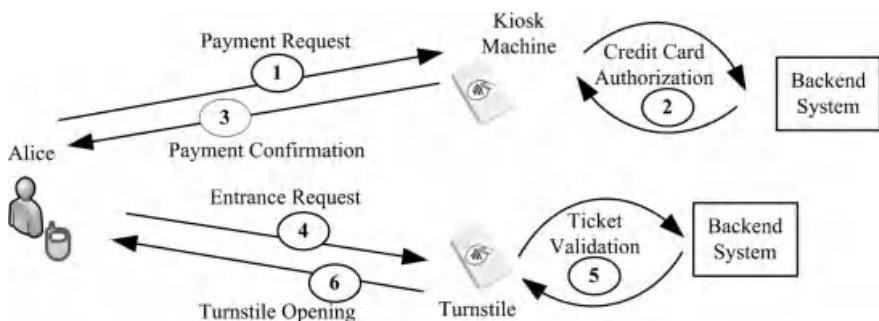
1. *Żądanie płatności:* Alice żąda płatności, dotykając swojego telefonu komórkowego do czytnika w kiosku. Czytnik NFC odczytuje wymagane dane karty kredytowej.
2. *Autoryzacja karty kredytowej:* Czytnik wysyła informacje o karcie kredytowej do systemu informatycznego backendu w celu autoryzacji karty kredytowej.
3. *Potwierdzenie płatności:* Telefon komórkowy jest powiadamiany o transakcji, a bilet jest wysyłany do urządzenia za pośrednictwem OTA.
4. *Żądanie wejścia:* Alice prosi o wejście do kina, dotykając swojego telefonu komórkowego do czytnika przy bramce obrotowej. Czytnik NFC odczytuje bilet i przetwarza go.
5. *Walidacja biletu:* Czytnik NFC wysyła informacje o bilecie do systemu zaplecza w celu jego walidacji.
6. *Otwarcie kołowrotu:* Gdy bilet zostanie skasowany, bramka obrotowa zostanie otwarta.



Rysunek 4.29 Schemat działań związanych z biletami NFC.



Rysunek 4.30 Schemat działań związanych z biletami NFC.



Rysunek 4.31 Model użytkowania w przypadku sprzedaży biletów NFC.

4.8 Rozdział Podsumowanie

Istnieją trzy techniki interakcji w komunikacji mobilnej: dotykanie, wskazywanie i skanowanie. Interakcja NFC jest techniką interakcji opartą na dotyku, ponieważ występuje, gdy dwa urządzenia znajdujące się w odległości kilku centymetrów są po prostu dotykane. Aby wykonać interakcję NFC, użytkownik musi posiadać telefon komórkowy z obsługą NFC i powinien wchodzić w interakcję z tagiem NFC, czytnikiem NFC lub innym telefonem komórkowym z obsługą NFC.

W technologii NFC zdefiniowano trzy różne tryby pracy: tryb czytnika/zapisu, tryb peer-to-peer i tryb emulacji karty. Wykorzystanie każdego trybu można zdefiniować za pomocą ogólnych modeli użytkowania. Co więcej, każdy tryb zapewnia użytkownikom inne korzyści. Aplikacje w trybie czytnika/zapisu mogą zwiększyć mobilność użytkownika i zmniejszyć wysiłek fizyczny. Z drugiej strony, aplikacje w trybie emulacji karty nie promują mobilności telefonów komórkowych; jednak ściśle łączą użytkowników z telefonami komórkowymi. Zalety tego trybu obejmują eliminację obiektów fizycznych i zapewnienie kontroli dostępu. Aplikacje w trybie peer-to-peer są przydatne do łatwej wymiany danych między użytkownikami i zapewniają łatwe parowanie urządzeń.

Projektowanie inteligentnych plakatów to kolejny ważny obszar, na który zwrócono uwagę w tym rozdziale. Użytkownicy powinni być świadomi punktu dotyku na inteligentnym plakacie, w przeciwnym razie będą musieli przeszukiwać inteligentny plakat, co zmniejszy użyteczność. Świadomość zawartości tagów i wiarygodność plakatu to kolejne ważne kwestie, które należy wziąć pod uwagę.

W tym rozdziale rozważono przypadki użycia NFC pod względem trybów pracy. Krótkie przypadki użycia i ogólne modele użytkowania daly podstawowy projekt aplikacji. Szczegółowe przypadki użycia obejmowały wymagania dotyczące projektowania aplikacji i charakterystyki trybów pracy.

Rozdział Pytania

1. Na czym polega technika interakcji NFC? Jakie są podstawowe właściwości tej techniki?
2. Jakie są różnice między urządzeniami aktywnymi i pasywnymi?
3. W jaki sposób role inicjatora i celu wpływają na tryb komunikacji NFC?
4. Czy urządzenie pasywne może być inicjatorem w NFC? Dlaczego?
5. Zdefiniuj inteligentny plakat i wyjaśnij jego zastosowanie. Którego trybu pracy używają zazwyczaj aplikacje typu smart poster?
6. Nazwij i podaj szczegóły jednego przypadku użycia, który wykorzystuje tryb czytnika/zapisu.
7. Wymień i podaj szczegóły jednego przypadku użycia, który wykorzystuje tryb peer-to-peer.
8. Wymień i podaj szczegóły jednego przypadku użycia, który wykorzystuje tryb emulacji karty.
9. Opisz korzyści płynące z zastosowania trybu czytnika/zapisu.
10. Opisz podstawowe korzyści aplikacji trybu peer-to-peer.
11. Opisz korzyści płynące z zastosowania trybu emulacji karty.
12. Który tryb NFC jest najbardziej obiecujący dla organizacji finansowych? Dlaczego?
13. Który tryb NFC jest najbardziej obiecujący dla operatorów sieci komórkowych? Dlaczego?
14. Który tryb NFC jest używany w aplikacjach społecznościowych? Podaj szczegóły.

Referencje

- [1] Rukzio, E., Callaghan, V., Leichtenstern, K., and Schmidt, A. (2006) *An Experimental Comparison of Physical Mobile Interaction Techniques: Touching, Pointing and Scanning*. Proceedings of Eighth International

- [2] QR Code, <http://www.qrcode.com/> (dostęp: 10 lipca 2011 r.).
- [3] NFC Forum N-Mark for Tags and Media Frequently Asked Questions, <http://www.nfc-forum.org/resources/N-Mark/> (dostęp 10 lipca 2011 r.).
- [4] Ok, K., Coskun, V., Aydin, M.N., and Ozdenizci, B. (2010) *Current Benefits and Future Directions of NFC Services*. Proceedings of 2010 International Conference on Education and Management Technology (ICEMT), Kair, Egipt, 2-4 listopada 2010, s. 334-338.

5

Tworzenie aplikacji NFC

Ten rozdział dotyczy tworzenia aplikacji NFC dla telefonów komórkowych. Większość właściwości telefonów komórkowych różni się od właściwości innych urządzeń, takich jak rozmiar monitora, styl klaviatury itp. Dlatego kody muszą uwzględniać właściwości urządzenia docelowego, w którym aplikacja będzie instalowana i używana. Aplikację można opracować, biorąc pod uwagę zestaw SDK (Software Development Kit) urządzenia docelowego, ale wymaga to dalszych wysiłków w celu przetestowania jej niezależnie od urządzenia docelowego. Jedną z opcji jest przeniesienie aplikacji na urządzenie docelowe natychmiast po jej jednorazowym napisaniu, co nie jest praktyczne. Żadna aplikacja nie może być opracowana bezbłędnie za pierwszym razem; jest to szczególnie prawdziwe w przypadku aplikacji mobilnych. Jeśli chodzi o aplikację mobilną NFC, transfer jest jeszcze bardziej niepraktyczny. Dlatego oprócz SDK, do tworzenia aplikacji mobilnych należy użyć symulatora mobilnego, który obsługuje urządzenie docelowe. Gdy aplikacja zostanie przetestowana w symulatorze, po usunięciu wszystkich błędów i będzie wolna od błędów, można ją przenieść na docelowy telefon komórkowy.

Istnieją różne platformy i języki programowania NFC. Dla telefonów komórkowych z systemem operacyjnym Android, Android SDK [1] jest używany do rozwoju NFC. Istnieje również inny interfejs API (Application Programming Interface) w Qt SDK [2], który zapewnia obsługę technologii NFC dla urządzeń z systemem Symbian³. Co więcej, Java jest głównym środowiskiem programistycznym, które może być używane w większości telefonów komórkowych. Interfejsy API technologii Java związane z NFC mogą być również wykorzystywane do tworzenia aplikacji NFC. Istnieją również inne platformy do tworzenia aplikacji NFC, a w przyszłości mogą pojawić się dodatkowe platformy.

W tym rozdziale używamy technologii Java, aby wyjaśnić tworzenie aplikacji NFC. Zakłada się, że czytelnicy mają podstawową wiedzę na temat technologii Java, a także możliwość pisania programów Java przy użyciu, na przykład, J2SE. Dodatkowo, niektóre treści programistyczne Java METM (JavaTM 2 Micro Edition) są podane w sekcji 5.4 dla tych, którzy nie są z nimi zaznajomieni. Istota tego rozdziału, tworzenie aplikacji NFC, jest podana po wprowadzeniu do Java ME, więc czytelnicy posiadający wiedzę na temat programowania Java ME mogą przejść do sekcji 5.5.

5.1 Pierwsze kroki w rozwoju aplikacji NFC

Tworzenie aplikacji NFC nie jest trywialne; jest to jedna z najważniejszych części wdrażania usług NFC dla klientów. Istnieją dwa rodzaje aplikacji NFC, które należy wziąć pod uwagę

Komunikacja bliskiego zasięgu: Od teorii do praktyki, wydanie pierwsze. Vedat Coskun, Kerem Ok i Busra Ozdenici.

© 2012 John Wiley & Sons, Ltd. Opublikowano 2012 przez John Wiley & Sons, Ltd.

na etapie rozwoju. Jeden typ to aplikacja GUI (Graphical User Interface), która musi być obecna we wszystkich aplikacjach trybu operacyjnego i zapewnia zarówno GUI dla użytkownika, jak i możliwość odczytu komponentów NFC. Drugi typ to aplikacja Secure Element (SE), która jest potrzebna do zapewnienia bezpiecznego i zaufanego środowiska dla aplikacji wymagających bezpieczeństwa, takich jak płatności, bilety i uwierzytelnianie w SE.

Aplikacje działające w trybie Reader/Writer i peer-to-peer zazwyczaj składają się tylko z aplikacji GUI, ponieważ te tryby pracy nie wymagają żadnych bezpiecznych operacji. W języku Java MIDlety są aplikacjami Java działającymi na telefonie komórkowym i zapewniają określone właściwości.

Z drugiej strony, aplikacje SE są używane w aplikacjach trybu emulacji kart. Aplikacje w trybie emulacji karty składają się zarówno z komponentów GUI, jak i SE. Aplikacje te współpracują z czytnikami NFC i MIDletami zainstalowanymi na telefonie komórkowym. W języku Java aplety są aplikacjami JavaCard działającymi na SE lub kartach inteligentnych.

Na rynku dostępne są różne narzędzia programistyczne, a użytkownik może wybrać odpowiednie narzędzie programistyczne dla docelowego telefonu komórkowego, ponieważ aplikacje są zależne od telefonu komórkowego. Na przykład dla telefonu komórkowego z systemem Android, aplikacja powinna zostać opracowana przy użyciu Android SDK, który można pobrać ze strony <http://developer.android.com/>. W przypadku telefonu komórkowego z systemem Symbian® 3, aplikacja powinna zostać opracowana przy użyciu Qt SDK. Ten SDK można pobrać ze strony <http://qt.nokia.com/>.

Zestawy SDK zapewniają również symulatory telefonów komórkowych. Wewnątrz symulatora można tworzyć i edytować tagi. Po zakończeniu fazy tworzenia aplikacji, powinna ona zostać przeniesiona na rzeczywiste urządzenia mobilne i przetestowana w środowisku czasu rzeczywistego. Aplikacje mogą być instalowane na telefonie komórkowym poprzez połączenie go do komputera za pomocą połączenia przewodowego lub Bluetooth lub alternatywnie mogą być instalowane online za pośrednictwem zasobów internetowych.

Dwa JSR (Java Specification Requests) zostały opracowane w ramach platformy Java w celu umożliwienia aplikacji opartych na NFC. JSR 257 (Contactless Communication API) służy głównie do programowania w trybie czytnika/zapisu, a JSR 177 (Security and Trust Services API) do programowania w trybie emulacji karty. JSR 257 dotyczy głównie wykrywania obiektów zbliżeniowych w pobliżu, powiadamiania aplikacji o wykryciu i wykonywania operacji na tagach. JSR 177 obsługuje komunikację z aplikacjami kart inteligentnych, a także zapewnia podpisywanie podpisów cyfrowych na poziomie aplikacji, zarządzanie poświadczeniami użytkownika i operacje kryptograficzne.

5.2 Dlaczego Java?

5.2.1 Dlaczego wybraliśmy Java?

Aby łatwo tworzyć aplikacje NFC na dowolnej platformie, język programowania NFC powinien zapewniać podstawy programowania NFC i powinien służyć jako podstawa dla czytników. Obecnie dostępne są różne platformy do tworzenia aplikacji NFC. W przyszłości mogą pojawić się nowe.

Jako język programowania wybraliśmy Javę, ponieważ jest ona powszechnie używana i jest dobrze znanym językiem programowania. Dostarczył również jeden z pierwszych interfejsów API w technologii NFC. Nokia 6212 i Nokia 6131 NFC SDK to platformy programistyczne, które są w stanie współpracować z JSR 257 i 177, które zapewniają programowanie NFC w Javie. Chociaż telefony te są przestarzałe, główną funkcją tego rozdziału jest przekazanie podstawowej wiedzy na temat programowania NFC. Zdobyte

umiejętności programowania NFC w technologii Java pomogą użytkownikom łatwo rozwijać NFC

w innych językach programowania dla różnych telefonów komórkowych przy użyciu różnych zestawów SDK.

5.2.2 Dlaczego Java jest faworytem ?

Dlaczego Java stała się faworytem? Zdecydowanie pomogły afirmatywne właściwości Javy. Niezależność od platformy, a także bycie powszechną technologią na wszystkich platformach sprawiły, że stała się korzystna. Jeśli chcesz napisać samodzielna aplikację na komputery osobiste, możesz użyć Javy. Jeśli chcesz wyeksportować ją na serwer WWW, nadal możesz używać Javy. Jeśli chcesz zaimplementować programy na wbudowanym sprzęcie w lodówkach, Java nadal może być używana. Tworzenie aplikacji mobilnych jest nadal możliwe przy użyciu Javy. Dlatego ta sama technologia z niewielkimi różnicami jest wystarczająca na wszystkich platformach. Bez Javy programista aplikacji musi uczyć się różnych technologii dla różnych środowisk.

JavaTM to technologia programowania obiektowego, która została zaprojektowana przede wszystkim jako obiektowa i niezależna od platformy. Została wprowadzona przez Sun Microsystems w 1995 roku i jest znakiem towarowym tej firmy. Każdy, kto chce zaimplementować środowisko uruchomieniowe Java, musi uzyskać pozwolenie od firmy Sun i przejść kompleksowy zestaw testów zgodności. Składnia i semantyka samego języka Java zostały opisane w specjalnym dokumencie zatytułowanym The Java Language Specification (JLS). Więcej szczegółów można znaleźć na stronie <http://java.sun.com/docs/books/jls/index.html>.

Programy Java są zapisywane w plikach z rozszerzeniem .java. Programy Java nie są konwertowane na kody maszynowe, zamiast tego są wykonywane na interpreterach online. Dostępne interpretery różnią się w zależności od platformy wykonawczej. Konwertery na komputerach osobistych określane są jako Java Virtual Machines (JVM), podczas gdy na telefonach komórkowych nazywane są Kilobyte Virtual Machines (KVM). Przed uruchomieniem programu Java z rozszerzeniem .java, należy go skompilować i przekonwertować na kod bajtowy z rozszerzeniem .class przy użyciu kompilatora Java. Programy kodu bajtowego Java są wykonywane na wierzchu maszyny wirtualnej.

Ogromną zaletą tego języka programowania jest to, że programy Java są niezależne od platformy. Oznacza to, że kody Java mogą być uruchamiane na dowolnym sprzęcie i dowolnym systemie operacyjnym, o ile dostępna jest kompatybilna maszyna wirtualna Java.

Główne właściwości technologii Java są następujące:

- *Niezależność od platformy i przenośność (napisz raz, uruchom wszędzie)*: Kod bajtowy Java jest interpretowany przez maszynę wirtualną. W związku z tym aplikacja Java może być wykonywana na dowolnym urządzeniu, które zawiera wymaganą maszynę wirtualną, niezależnie od systemu operacyjnego i sprzętu. Obecnie większość urządzeń mobilnych posiada wymaganą maszynę wirtualną. Podczas opracowywania aplikacji dla szerokiej gamy urządzeń mobilnych, jedno opracowanie dla wielu urządzeń skutkuje ogromnymi oszczędnościami produkcyjnymi.
- *Solidność*: Nawet jeśli aplikacja Java ulegnie awarii, pozostaje ona w maszynie wirtualnej i nie ulega awarii.
wypływać na inne aplikacje lub ważne dane na urządzeniu. Ponadto aplikacja Java ma automatyczne zarządzanie pamięcią i zbieranie śmieci.
- *Bezpieczeństwo*: Technologia Java zapewnia bezpieczne środowisko dzięki menedżerowi zabezpieczeń i API bezpieczeństwa. Kryptograficzna funkcjonalność technologii i integracja infrastruktury klucza publicznego (PKI) umożliwiają tworzenie bezpiecznych aplikacji.

Uwierzytelnianie i kontrola dostępu chronią aplikacje przed nieautoryzowanym dostępem.

- *Zorientowany obiektowo:* Java jest językiem obiektowym, w którym model języka programowania jest zorganizowany wokół obiektów, a nie akcji.
- *Szerokie zastosowanie na zapleczu:* Klienci Java mogą łatwo współpracować z aplikacją Java na zapleczu serwery.
- *Obsługa wielowątkowości:* Aplikacja wielowątkowa jest niezbędna w przypadku niektórych specyficznych problemów; jest to również zapewnione przez Javę.
- *Świadomość sieci:* Aplikacje Java są świadome sieci (aplikacje są dynamicznie (może wymieniać dane z serwerem przy użyciu dowolnej technologii, takiej jak GSM, CDMA, TDMA itp. oraz za pośrednictwem dowolnego protokołu sieciowego, takiego jak TCP/IP, WAP, i-mode itp.)

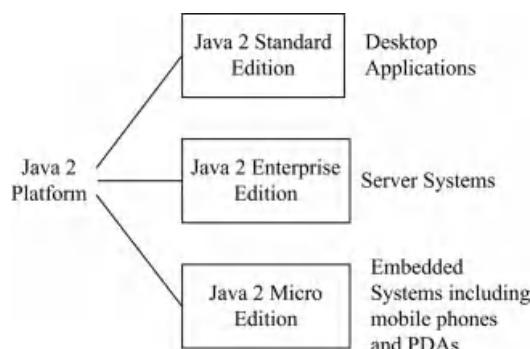
Jednak zalety techniczne nie są jedynymi czynnikami decydującymi o sukcesie danej technologii. Równie ważne są wartości biznesowe. W szczególności zdolność dostawcy do rozwiązywania problemów społeczności programistów i użytkowników ma kluczowe znaczenie dla przyjęcia technologii. Przyjrzymy się teraz, jak społeczność Java™ wpływa na ewolucję technologii.

Technologia Java składa się z następujących trzech elementów, których połączenie tworzy platformę Java:

- Standardy języka programowania Java, które definiują zasady pisania programów Java.
- JVM do wykonywania programów Java, które są napisane zgodnie ze standardem języka Java.
- Rozbudowany zestaw interfejsów API, które obsługują szeroką gamę źródeł potrzebnych programiście.

Platforma Java została zaprojektowana tak, aby była dostępna dla szerokiej gamy sprzętu, od telefonów komórkowych i kart inteligentnych po serwery aplikacji internetowych i serwery korporacyjne. Platforma Java występuje w trzech formach (patrz rysunek 5.1):

- *Java 2 Standard Edition (J2SE)* jest przeznaczona dla komputerów stacjonarnych [3].
- *Java 2 Enterprise Edition (J2EE)* jest przeznaczona dla większej liczby platform, takich jak aplikacji dla wielu użytkowników lub aplikacji korporacyjnych. Opiera się na J2SE i dodaje interfejsy API do obliczeń po stronie serwera [4].
- *Java 2 Micro Edition (J2ME)* została zaprojektowana z myślą o technologiach i specyfikacjach wykorzystywanych w małych przedsiębiorstwach. urządzeniu takie jak telefony komórkowe i osobiste asystenty cyfrowe (PDA) [5].



Rysunek 5.1 Platforma Java 2.

W tym rozdziale główny nacisk położono na interfejsy API technologii Java związane z NFC. Specyfikacje API Java, w tym konfiguracje i profile Java ME, zostały opracowane w ramach Java Community Process (JCP). JCP stara się zapewnić, że technologia Java jest rozwijana zgodnie z konsensusem społeczności, aby uniknąć fragmentacji branży. JCP skupia wiodących graczy w odpowiednich branżach w celu uzgodnienia wspólnej specyfikacji, zgodnie z którą wszyscy mogą projektować swoje produkty [6]. Każda konfiguracja lub profil zaczyna się jako JSR, który opisuje zakres prac, które zostaną wykonane i zarys obszarów, które zostaną objęte [7]. Grupa ekspertów jest gromadzona w celu stworzenia specyfikacji, która jest następnie poddawana wewnętrznemu głosowaniu i rewizji przed udostępnieniem wyników do publicznego przeglądu. Po publicznym przeglądzie i ewentualnej ostatniej rewizji powstaje ostateczny projekt, a JSR zostaje ukończony. Aktualną listę JSR, w tym tych, które zostały ukończone, można znaleźć na stronie internetowej JCP pod adresem <http://jcp.org/jsr/all/>.

5.3 Konfiguracja środowiska dla programowania Java ME i NFC

W tej sekcji wyjaśnimy, jak skonfigurować środowisko do tworzenia aplikacji NFC, które będzie używane w całej tej książce.

W celu tworzenia aplikacji Java, JDK (Java Development Kit) powinien być zainstalowany w systemie.

Odpowiednie środowisko do tworzenia aplikacji NFC wymaga trzech komponentów:

- Java ME.
- Symulator urządzenia mobilnego oraz komponentów NFC.
- Rozszerzenia NFC.

Istnieje kilka dostępnych środowisk programistycznych MIDP, a także różne symulatory dla różnych platform sprzętowych. Series 40 Nokia 6212 NFC SDK [8] jest używany jako symulator telefonu komórkowego ze zintegrowanymi rozszerzeniami NFC. Series 40 Nokia 6212 NFC SDK zapewnia środowisko programistyczne i testowe NFC dla urządzeń Nokia 6212 NFC. Ponadto do pisania kodów dla urządzeń mobilnych wymagane jest zintegrowane środowisko programistyczne (IDE) z wymaganymi dodatkami dla środowiska NFC. Na rynku dostępne są różne IDE Java, a użytkownik może wybrać dowolne, które zawiera wymagane komponenty. W tej książce użyliśmy środowiska programistycznego Eclipse wraz z dodatkiem Eclipse ME, aby zapewnić wsparcie dla tworzenia aplikacji mobilnych. Użyty przez nas pakiet NFC SDK jest kompatybilny zarówno z Eclipse, jak i Netbeans IDE [8].

(i) Nokia 6212 NFC SDK z serii 40

Aplikacje NFC są opracowywane dla określonych platform telefonów komórkowych. Musimy pamiętać, że NFC jest stosunkowo nową technologią i nie wszystkie telefony komórkowe obsługują NFC. Niektóre początkowe telefony komórkowe zostały wprowadzone przez wiodących producentów, takich jak Nokia, a liczba dostępnych modeli rośnie z dnia na dzień. W tej książce używamy Nokii 6212 jako platformy testowej dla aplikacji NFC. Seria 40 Nokia 6212 NFC SDK to implementacja klasycznego urządzenia Nokia 6212, które również posiada łączność NFC. To oprogramowanie emulatora ma wbudowany menedżer NFC i symulator urządzenia Nokia 6212 classic. Emulator umożliwia programistom testowanie i uruchamianie aplikacji MIDP.

jak również aplikacje obsługujące NFC. Za pomocą menedżera NFC można tworzyć i symulować nowe tagi; ponadto można je również edytować i zapisywać do wykorzystania w przyszłości. Tag może być dołączony do symulatora telefonu komórkowego i może się z nim komunikować. Co więcej, interfejs pozwala obsługiwany czytnikom NFC na łatwe łączenie się z emulatorem. SDK może być używany jako samodzielny SDK lub alternatywnie może być zintegrowany z obslugiwany IDE, takim jak Eclipse lub Netbeans. Zestaw SDK Nokia 6212 NFC Series 40 można pobrać ze strony <http://www.forum.nokia.com/>.

(ii) *Eclipse*

Projekty Eclipse są rozwijane przez Eclipse Foundation, która jest społecznością open source. Fundacja Eclipse jest korporacją non-profit, wspieraną przez członków, która obsługuje projekty Eclipse. Eclipse zapewnia różne IDE, które obejmują środowiska wykonawcze, języki statyczne i dynamiczne, frameworki po stronie serwera, modelowanie i raportowanie biznesowe oraz systemy wbudowane i mobilne. W tej książce użyjemy jednego z IDE Fundacji Eclipse, a mianowicie Eclipse IDE for Java Developers do tworzenia aplikacji MIDlet. IDE można pobrać bezpłatnie ze strony <http://www.eclipse.org/downloads/>. Więcej informacji na temat Eclipse Foundation i Eclipse IDE można znaleźć na stronie <http://www.eclipse.org/> [9].

(iii) *Eclipse ME*

Eclipse ME to wtyczka do Eclipse IDE umożliwiająca tworzenie MIDletów. Wtyczka Eclipse ME umożliwia tworzenie MIDletów poprzez połączenie z bezprzewodowymi zestawami narzędzi.

Aby zainstalować Eclipse ME, należy pomyślnie zainstalować zarówno Eclipse IDE, jak i odpowiedni zestaw narzędzi bezprzewodowych, który jest przeznaczony dla docelowego telefonu komórkowego. Zestaw SDK Nokia 6212 NFC Series 40 zawiera zestaw narzędzi bezprzewodowych, więc nie trzeba instalować go osobno. Najnowszą wtyczkę Eclipse ME można pobrać ze strony <http://eclipseme.org/> [5, 10].

(iv) *Instalacja*

Instalację platform należy przeprowadzić w następującej kolejności:

1. *Instalacja pakietu Nokia 6212 NFC SDK Series 40*

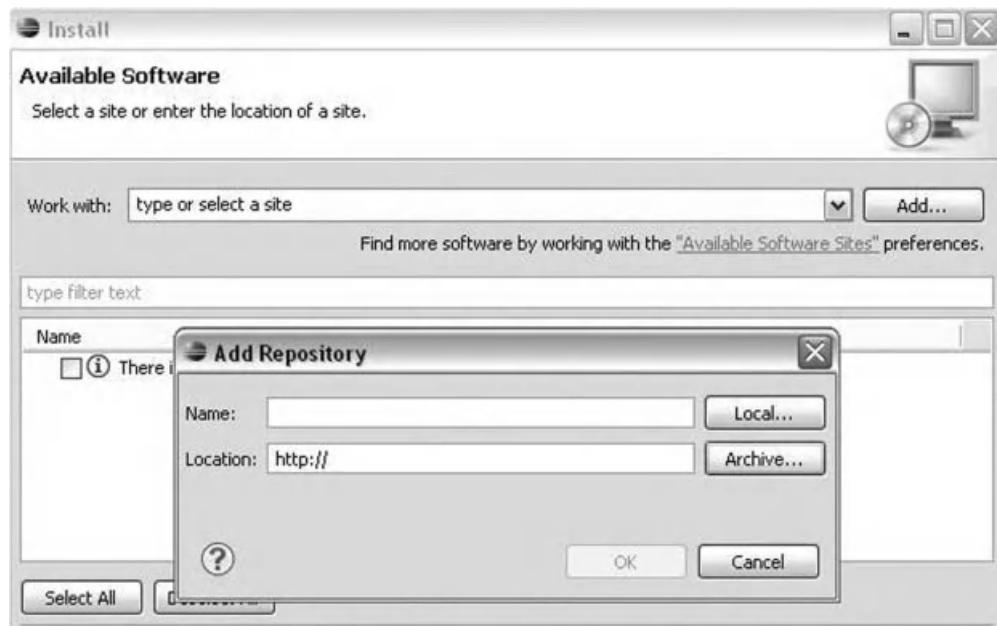
- a. Rozpakuj pobrane archiwum Nokia 6212 NFC SDK Series 40 do folderu.
- b. Uruchom plik instalacyjny i postępuj zgodnie z instrukcjami. Zainstalowany zostanie emulator Nokia 6212 NFC, menedżer NFC i wymagane pliki.

2. *Instalacja Eclipse IDE*

Rozpakuj pobrane archiwum Eclipse IDE do folderu. Po rozpakowaniu zobaczysz folder o nazwie "eclipse". W folderze tym znajduje się plik wykonywalny `eclipse.exe`. Pozostaje tylko uruchomić plik `eclipse.exe`, aby uruchomić aplikację Eclipse. Oczywiście opcjonalnie można utworzyć skrót na pulpicie, aby uprościć ten proces.

3. *Instalacja Eclipse ME*

- a. Uruchom Eclipse IDE.
- b. Z menu "Pomoc" w Eclipse wybierz "Zainstaluj nowe oprogramowanie".
- c. Wybierz "Dodaj", a następnie "Archiwizuj" w oknie dialogowym (Rysunek 5.2).
- d. Wybierz pobrany plik archiwum Eclipse ME i kliknij "OK".
- e. Pakiet instalacyjny Eclipse ME zostanie wyświetlony w oknie dialogowym. Kliknij pole wyboru obok niego, a następnie kliknij "Next" (Rysunek 5.3).
- f. Przeczytaj i zaakceptuj "Umowę licencyjną", kliknij "Zakończ" i poczekaj, aż Eclipse zainstaluje pakiet.

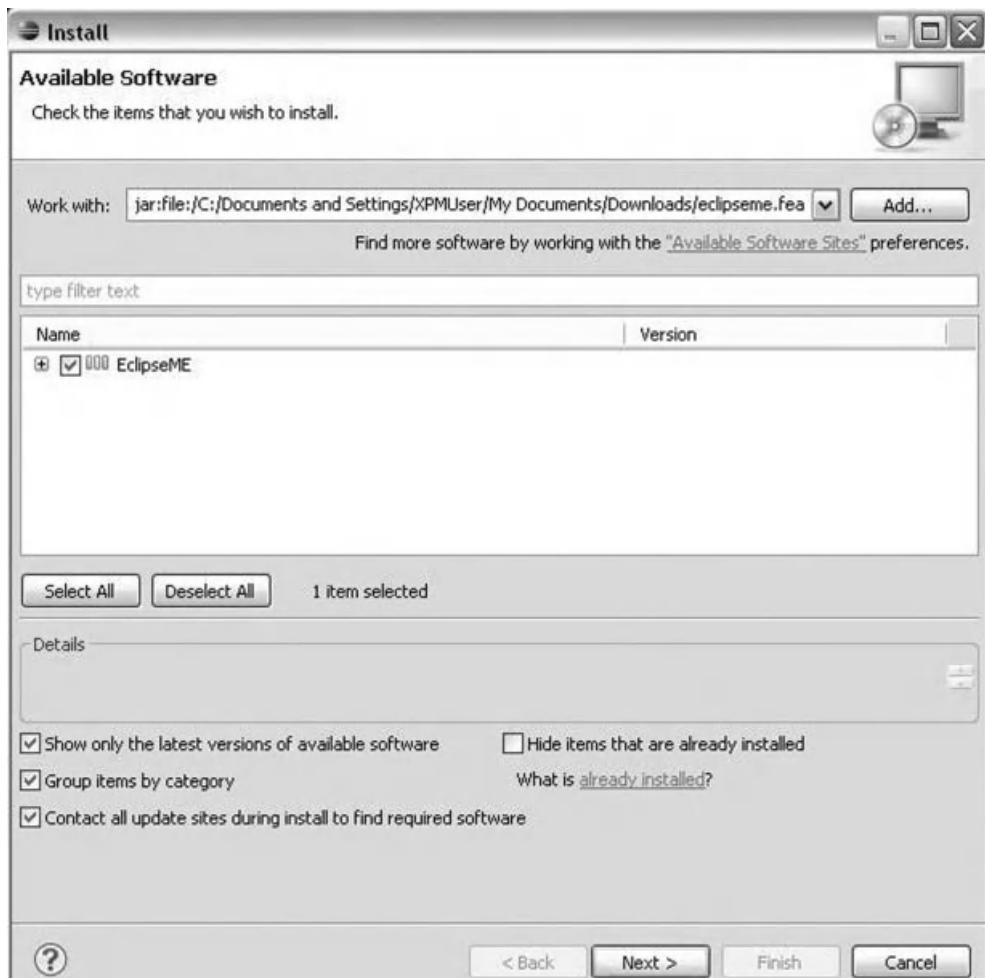


Rysunek 5.2 Ekran instalacji SDK-1.

4. *Konfiguracja Nokia 6212 NFC SDK Series 40 z Eclipse*
 - a. Uruchom Eclipse IDE, jeśli już go zamknąłeś.
 - b. Z menu "Okno" wybierz "Preferencje".
 - c. W lewej kolumnie rozwiń "Java" i kliknij "Debug".
 - d. Odznacz wszystkie opcje w sekcji "Wstrzymaj wykonanie".
 - e. W sekcji "Komunikacja" ustaw "Limit czasu debugera" i "Limit czasu uruchamiania" na 20 000 (ms).
 - f. W lewej kolumnie rozwiń "J2ME" i kliknij "Device Management".
 - g. Kliknij "Importuj", a następnie wybierz "Przeglądaj" (rysunek 5.4).
 - h. Wybierz katalog główny folderu instalacyjnego Series 40 Nokia 6212 NFC SDK, na przykład "C:\Nokia\Devices\S40_Nokia_6212_NFC_SDK", a następnie kliknij "OK".
 - i. Kliknij "Odśwież", aby Eclipse wyszukał urządzenia w wybranym folderze (rysunek 5.5).
 - j. Po znalezieniu zestawu Nokia 6212 NFC SDK Series 40 i wyświetleniu go w sekcji "Urządzenia", kliknij pole wyboru pod "Importuj" i kliknij "Zakończ" (rysunek 5.6).
 - k. Na koniec kliknij "OK", aby zastosować ustawienia i zamknąć okno "Preferencje".

Po pomyślnym zainstalowaniu i skonfigurowaniu aplikacji, jesteś gotowy do tworzenia MIDletów Java ME, w tym aplikacji NFC.

Jeśli korzystasz z systemu Windows Vista lub Windows 7, powinieneś ustawić zgodność "emulator.exe" w "C:\Nokia\Devices\S40_Nokia_6212_NFC_SDK\bin" na Windows XP.

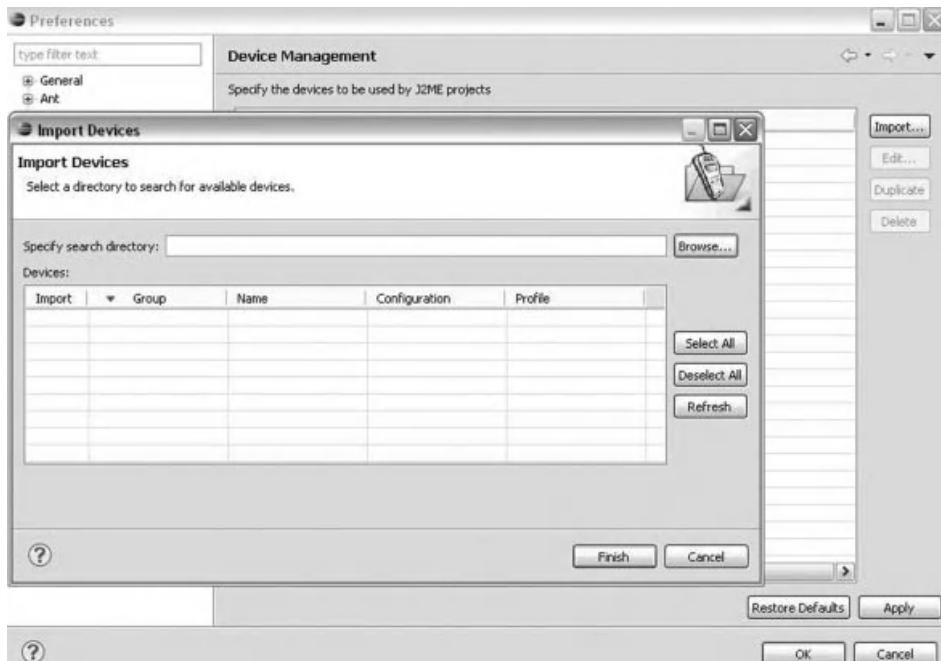


Rysunek 5.3 Ekran instalacji SDK-2.

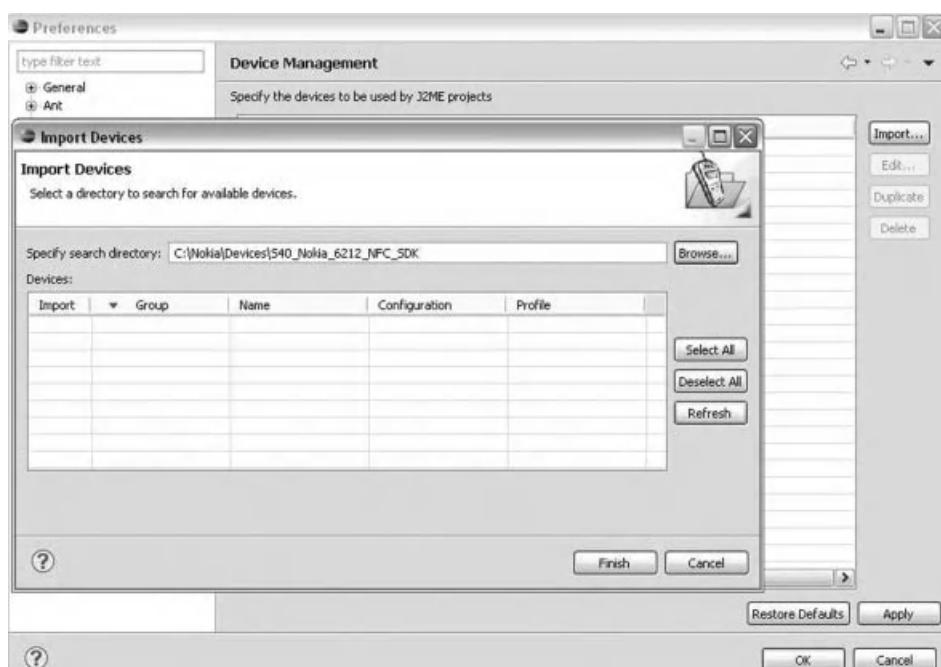
Alternatywnie, można użyć innego zestawu narzędzi bezprzewodowych (np. Sun Java Wireless Toolkit) jako mobilnego środowiska emulacji dla rozwoju MIDlet. Preferowany jest zestaw Nokia 6212 NFC SDK z serii 40, ponieważ będzie on również używany w programowaniu NFC w tej książce.

5.4 Wprowadzenie do programowania mobilnego

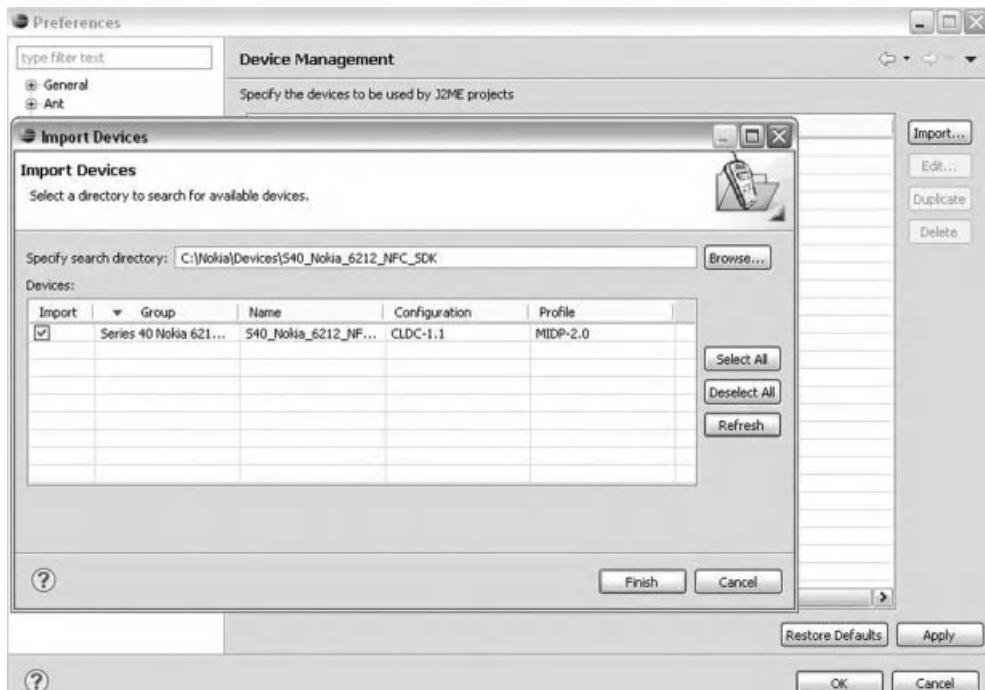
Ta sekcja zawiera krótkie wprowadzenie do Java ME dla programistów Java, którzy zamierają pisać aplikacje dla telefonów komórkowych lub PDA. Urządzenia te mają wspólną cechę: mają ograniczone zasoby pamięci i moc obliczeniową w stosunku do zwykłych komputerów. Dlatego też programy pisane dla urządzeń mobilnych są mniej wydajne w zakresie wejścia, wyjścia i przetwarzania. Aby przezwyciężyć ograniczenia wydajności, aplikacje mobilne powinny być projektowane i wdrażane z większą starannością.



Rysunek 5.4 Ekran instalacji SDK-3.



Rysunek 5.5 Ekran instalacji SDK-4.

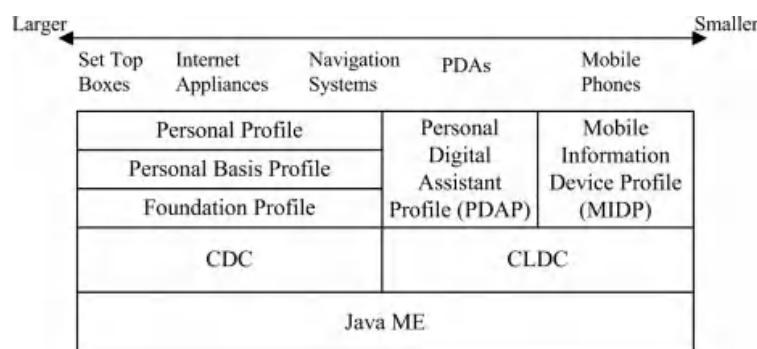


Rysunek 5.6 Ekran instalacji SDK-5.

5.4.1 Java ME Building Blocks

Technologia Java ME opiera się na konfiguracjach, profilach i opcjonalnych pakietach (patrz rysunek 5.7) [5]:

- *Konfiguracja* zawiera podstawowy zestaw interfejsów API i możliwości maszyny wirtualnej, które mogą być używane z urządzeniem o określonej wydajności sprzętowej.



Rysunek 5.7 Konfiguracje i profile Java ME.

Tabela 5.1 Konfiguracje CLDC i CDC

Nr JSR.	Nazwa JSR	URL
30	Connected Limited Device Configuration (CLDC) 1.0	http://jcp.org/jsr/detail/30.jsp
139	Connected Limited Device Configuration (CLDC) 1.1	http://jcp.org/jsr/detail/139.jsp
36	Konfiguracja podłączonego urządzenia (CDC) 1.0.1	http://jcp.org/jsr/detail/36.jsp
218	Konfiguracja podłączonego urządzenia (CDC) 1.1	http://jcp.org/jsr/detail/36.jsp

- *Profile* dodają bardziej specyficzne interfejsy API niż konfiguracje. Profil to zestaw interfejsów API, które obsługują węższy zakres urządzeń.
- *Pakiet opcjonalny* zapewnia funkcjonalność, która nie jest zawarta w określonej konfiguracji lub profil.

Konfiguracja definiuje podstawowe środowisko uruchomieniowe Java ME, które obejmuje:

- Maszyna wirtualna (która jest bardziej ograniczona niż J2SE VM);
- Zestaw podstawowych klas (wywodzących się głównie z klas J2SE).

Każda konfiguracja jest przeznaczona dla określonej rodziny urządzeń o podobnych możliwościach. Platforma Java ME została dalej podzielona na dwie konfiguracje, jedną dla stosunkowo mniej wydajnych urządzeń mobilnych, a drugą dla bardziej wydajnych urządzeń mobilnych, takich jak smartfony. Konfiguracja dla małych urządzeń, takich jak telefony komórkowe, nazywana jest Connected Limited Device Configuration (CLDC), a konfiguracja dla bardziej wydajnych urządzeń nazywana jest Connected Device Configuration (CDC). Niektóre dostępne konfiguracje podano w tabeli 5.1.

CLDC jest skierowany do urządzeń o ograniczonych zasobach, takich jak ograniczona moc obliczeniowa, pamięć i grafika. Oprócz CLDC i CDC opisano różne profile, które składają się z kilku interfejsów API i definiują完备ne środowiska aplikacji. Profil Mobile Information Device Profile (MIDP) jest takim profilem i jest szeroko stosowany w Java ME, który jest oparty na CLDC. MIDP umożliwia pisanie aplikacji i usług dla urządzeń mobilnych, w tym telefonów komórkowych. Aplikacje te są dostępne do pobrania i zapewniają możliwość połączenia z siecią.

Profil rozszerza konfigurację (która może być CDC lub CLDC, jak wspomniano powyżej), dodając klasy specyficzne dla domeny, aby zapewnić funkcjonalność brakującą w używanej konfiguracji. Każde urządzenie musi obsługiwać co najmniej jedną konfigurację. Nie każde urządzenie obsługuje każdy profil i nie każdy profil obsługuje każde urządzenie. Niektóre dostępne profile podano w tabeli 5.2.

W przypadku rozwoju MIDP, który jest podstawowym profilem rozwoju dla urządzeń mobilnych, początkowo należy utworzyć MIDlet. MIDlety są również wymagane przy tworzeniu aplikacji NFC, ponieważ aplikacje NFC działają na telefonach komórkowych i są oparte na profilu MID. Przykłady MIDletów są wprowadzane i rozwijane w kolejnych sekcjach.

5.4.2 MIDlety

Aby rozpocząć programowanie MIDletów, musimy najpierw poznać następujące definicje [11]:

Tabela 5.2 Profile Java

Nr JSR.	Nazwa JSR	URL
37	Profil mobilnego urządzenia informacyjnego 1.0	http://jcp.org/jsr/detail/37.jsp
118	Profil mobilnego urządzenia informacyjnego 2.0	http://jcp.org/jsr/detail/118.jsp
271	Profil mobilnego urządzenia informacyjnego 3.0	http://jcp.org/jsr/detail/271.jsp
75	PDA Profile 1.0	http://jcp.org/jsr/detail/75.jsp
46	Foundation Profile 1.0	http://jcp.org/jsr/detail/46.jsp
219	Foundation Profile 1.1	http://jcp.org/jsr/detail/219.jsp
129	Personal Basis Profile 1.0	http://jcp.org/jsr/detail/129.jsp
217	Personal Basis Profile 1.1	http://jcp.org/jsr/detail/217.jsp
62	Profil osobisty 1.0	http://jcp.org/jsr/detail/62.jsp

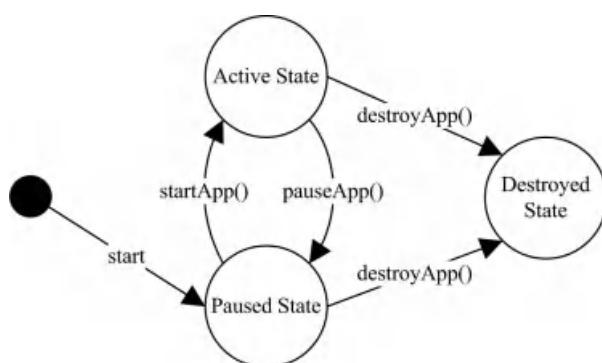
- *Oprogramowanie zarządzające aplikacją (AMS)* jest częścią oprogramowania środowiska operacyjnego urządzenia, które zarządza i kontroluje MIDlet. Pobiera właściwości z deskryptora aplikacji i kieruje MIDletem poprzez zmiany stanu.
- *MIDlet* to aplikacja MIDP na urządzeniu, która została zdefiniowana wcześniej. Wysyła również sygnał do oprogramowania do zarządzania aplikacjami o procesie.
- *Stany MIDletów* to stany, które może posiadać MIDlet.

5.4.2.1 Stany MIDlet

W celu ułatwienia zarządzania MIDletami, MIDlet może przechodzić w różne stany kontrolowane przez AMS. Każdy MIDlet rozszerza i zastępuje te stany.

Istnieją trzy prawidłowe stany MIDlet (patrz rysunek 5.8):

- *Stan wstrzymania:* MIDlet jest wstrzymany w tym stanie. Nie jest on zakończony; powinien jednak zwolnić zasoby uzyskane w stanie aktywnym. MIDlet jest zwykle wstrzymywany, gdy telefon musi wykonać proces o wyższym priorytecie, taki jak połączenie przychodzące. MIDlet może przejść do stanu wstrzymania poprzez wywołanie metody `pauseApp()`, gdy znajduje się w stanie aktywnym. Ponadto



Rysunek 5.8 Stany MIDletów.

Gdy MIDlet rozpoczyna wykonywanie, tworzy nową instancję MIDletu, a AMS umieszcza go w stanie wstrzymania.

- *Stan aktywny:* MIDlet działa normalnie w tym stanie. MIDLET może zmienić swój stan do aktywnego poprzez wywołanie metody `startApp`, jeśli jest w stanie wstrzymania.
- *Stan zniszczenia:* MIDlet zostaje zakończony w tym stanie i zwalnia swoje zasoby. A MIDlet może przełączyć się do stanu zniszczenia ze stanu wstrzymania lub aktywności poprzez wywołanie funkcji `destroyApp`.

Jak opisaliśmy wcześniej, aplikacja MIDP jest MIDletem. W Java ME każda aplikacja MIDlet musi rozszerzać abstrakcyjną klasę MIDlet, która znajduje się w pakiecie `javax.microedition.midlet`.

5.4.2.2 Klasa MIDlet

Klasa `MIDlet` definiuje aplikacje MIDP i interakcje między aplikacją a środowiskiem, w którym aplikacja działa. Klasa znajduje się w folderze `javax.microedition.midlet package`.

Aplikacje muszą rozszerzyć tę klasę, aby AMS mógł kontrolować MIDlet i pobierać właściwości z deskryptora aplikacji oraz żądać zmian stanu w celu uruchomienia, wstrzymania lub zniszczenia MIDletu.

MIDlet musi nadpisać następujące trzy metody abstrakcyjnej klasy MIDlet: `startApp`, `pauseApp` i `destroyApp`. Każda metoda umożliwia zmianę stanu (patrz rysunek 5.8).

- *startApp () :* Metoda ta sygnalizuje MIDletowi, że wszedł w stan aktywny. W stanie aktywnym MIDlet może posiadać pewne zasoby. Metoda ta może być wywołana tylko wtedy, gdy MIDlet jest w stanie wstrzymania.
- *pauseApp () :* Metoda ta sygnalizuje MIDletowi przejście w stan wstrzymania. W stanie wstrzymania MIDlet musi zwolnić współdzielone zasoby. Metoda ta może być wywołana tylko wtedy, gdy MIDlet jest w stanie aktywnym.
- *destroyApp(boolean unconditional) :* Ta metoda sygnalizuje MIDletowi, aby zakończył aplikację. MIDlet musi zwolnić wszystkie zasoby i powinien zapisać wymagane dane przed zakończeniem. Metoda ta może zostać wywołana, gdy MIDlet znajduje się w stanie wstrzymania lub aktywności.

Parametr `boolean` w metodzie `destroyApp` jest używany w celu umożliwienia MIDletowi żądania kontynuacji, jeśli nie chce on zostać zniszczony. Jeśli wartość parametru wynosi `true`, MIDlet musi zwolnić wszystkie posiadane zasoby. Jeśli parametr ma wartość `false`, MIDlet może kontynuować działanie, rzucając wyjątek. Jednym z powodów żądania kontynuacji jest na przykład to, że aplikacja nadal zapisuje dane.

Inne ważne metody w klasie `MIDlet` są następujące:

- *notifyDestroyed()*: MIDlet wysyła powiadomienie do AMS, że został przełączony w stan zniszczony.
- *notifyPaused()*: MIDlet wysyła powiadomienie do AMS, że został przełączony do stanu

wstrzymania

stan.

resumeRequest(): MIDlet prosi AMS o wznowienie poprzez ponowne uruchomienie.

- *String getAppProperty(String key)*: Ta metoda umożliwia aplikacji otrzymanie właściwości MIDletu z deskryptora aplikacji i pliku manifestu. Parametr key jest nazwą właściwości, która ma zostać odebrana.

5.4.3 Pakiet javax.microedition.lcdui

`javax.microedition.lcdui` jest ważnym pakietem dla aplikacji MIDlet. Pakiet ten zapewnia implementację interfejsów użytkownika. Jest to również ważny pakiet dla rozwoju NFC, ponieważ interfejsy użytkownika są wymagane w aplikacjach NFC.

Głównym elementem interfejsu użytkownika w telefonie komórkowym jest ekran. Ekran emuluje obiekty graficzne i wyświetla je użytkownikowi. Aplikacje mobilne mogą wyświetlać jeden obiekt ekranu na raz. Gdy bieżący ekran ma zostać przełączony na inny, wymagane argumenty muszą zostać przekazane do następnego ekranu.

Istnieje wiele przydatnych klas zdefiniowanych w tym pakiecie; niektóre ważne klasy podano poniżej. Pełna lista klas i ich definicji jest dostępna online pod adresem <http://java.sun.com/javame>.

5.4.3.1 Polecenie klasy

Klasa `Command` reprezentuje polecenie, które ma zostać wykonane w aplikacji głównie przez działanie użytkownika. Każde polecenie ma typ, który definiuje intencję polecenia. Na przykład polecenie `OK` kieruje użytkownika do potwierdzenia pytania tak/nie lub przesłania odpowiedzi na pytanie. Dostępne typy poleceń wymieniono w tabeli 5.3. Należy pamiętać, że akcje poleceń nie są implementowane automatycznie i powinny zostać zaimplementowane w metodzie `commandAction`. Ponadto każde polecenie ma priorytet nadany przez użytkownika, który opisuje znaczenie polecenia. Aplikacja wykorzystuje priorytet poleceń w celu umieszczenia ich na ekranie. Polecenia o wyższym priorytecie są najczęściej umieszczane na ekranie, dzięki czemu użytkownik

Tabela 5.3 Dostępne typy poleceń Java ME

Typ polecenia	Opis
SCREENA	Nieokreślone polecenie, które dotyczy zawartości ekranu lub nawigacji między ekranami.
BACK	Powrót do poprzedniego ekranu CANCELD odrzuca wszystko, co zostało wprowadzone do bieżącego ekranu bez podejmowania żadnych działań. Polecenie to może również spowodować powrót do poprzedniego lub wcześniejszego ekranu
Potwierdzająca odpowiedź OKA	na obiekt na bieżącym ekranie
Żądanie pomocy	HELPA przez użytkownika STOPA żądanie zatrzymania bieżącej operacji EXITA Żądanie wyjścia z aplikacji ITEMSpecific implementacja do elementów ekranu lub elementów wyboru. Może być używany do tworzenia kontekstowych opcji menu

można bezpośrednio wybrać ich wykonanie; jednak polecenia o niższym priorytecie są umieszczane w menu, które można wyświetlić po naciśnięciu przycisku programowalnego i wybrać w drugiej czynności. W numeracji priorytetów niższe liczby całkowite oznaczają wyższą ważność i odwrotnie.

Każde polecenie składa się z etykiety, typu i priorytetu. Typ i priorytet są już opisane. Etykiety są wyświetlane użytkownikowi w celu wyrażenia treści polecenia. Etykieta powinna składać się tylko z kilku słów, ponieważ musi zajmować niewielki obszar na ekranie. Polecenie można skonstruować w następujący sposób:

```
Command(String label, int commandType, int priority)
```

Przykładowe polecenie można utworzyć w następujący sposób:

```
Command command = new Command("Back", Command.BACK, 0);
```

5.4.4 Tworzenie nowego projektu MIDlet

Aby utworzyć nową aplikację mobilną za pomocą Eclipse IDE, kliknij "New Project" w menu "File"; po czym zostanie wyświetlony kreator "New Project". Wybierz "J2ME Midlet Suite" i nadaj nazwę swojemu projektowi. Jeśli tworzysz aplikację NFC, upewnij się, że jako urządzenie emulatora wybrano "S40 Nokia 6212 NFC SDK". Po utworzeniu projektu, utwórz nowy "J2ME Midlet" w swoim projekcie.

(i) *Rozpoczęcie pracy z prostym MIDletem*

```
/*
 * Prosty MIDlet, który zawiera formularz i wydruki
 * String do wyświetlenia
 */
import javax.microedition.lcdui.*;
import javax.microedition.midlet.*;

public class Hello extends MIDlet implements CommandListener
{
    private Form mainForm;
    private Command exitCommand;

    public Hello(){

        // instancja obiektu formularza
        mainForm = new Form("My MIDlet");

        // dodaj wiadomość tekstową
        mainForm.append(new StringItem(null, "This is my first
MIDlet"));

        // instancja polecenia exitCommand
        exitCommand=new Command("Exit", Command.EXIT, 0);

        // dodanie polecenia exitCommand do obiektu formularza
        mainForm.addCommand(exitCommand);
    }
}
```

```
/*
 * skonfigurować odbiornik poleceń tak, aby
 * urządzenie nasłuchuje poleceń użytkownika
 */
mainForm.setCommandListener(this);

}

public void startApp(){

    // wyświetlenie formularza na ekranie
    Display.getDisplay(this).setCurrent(mainForm);
}

public void pauseApp(){

}

public void destroyApp(boolean unconditional){

    // powiadomienie o operacji
    zniszczenia notifyDestroyed();
}

public void commandAction(Command command, Displayable
    displayable){

    // jeśli użytkownik naciśnie
    exitCommand if (command ==
    exitCommand){
        destroyApp(true);
        // zniszczyć aplikację
    }
}
} // koniec MIDletu
```

(ii) *Uruchamianie MIDletu*

Po zaimplementowaniu MIDletu, kliknij prawym przyciskiem myszy na nazwę projektu w "Package Explorer", rozwiń "J2ME" i kliknij "Create Package". Następnie kliknij prawym przyciskiem myszy na MIDlet i kliknij "Run As - Emulated J2ME Midlet".

W tym pierwszym przykładzie tworzony jest prosty MIDlet, który wyświetla na ekranie obiekt Form i otrzymuje od użytkownika polecenie "Exit". Zrzut ekranu MIDletu można zobaczyć na rysunku 5.9.

(iii) *Wyjaśnienie kodu*

Do MIDletu importowane są dwie klasy:

```
import javax.microedition.lcdui.* ;
import javax.microedition.midlet.* ;
```

javax.microedition.lcdui jest wymagany do tworzenia obiektów ekranowych, wyświetlania ich i pobierania poleceń od użytkownika.
javax.microedition.midlet jest wymagany



Rysunek 5.9 Ekran Hello MIDlet.

dla wszystkich MIDletów, ponieważ pozwala menedżerowi aplikacji kontrolować MIDlet. Co więcej, trzy metody, które należy zaimplementować w tej klasie abstrakcyjnej to: `startApp`, `pauseApp` i `destroyApp`.

MIDlet implementuje interfejs `CommandListener` z pakietu `lcdui`:

```
public class Hello extends MIDlet implements CommandListener {}
```

Interfejs `CommandListener` umożliwia aplikacji nasłuchiwanie poleceń od użytkownika. Gdy wystąpi zdarzenie polecenia, automatycznie wywołuje metodę `commandAction`.

Tworzony jest obiekt `Form` o nazwie `mainForm` i obiekt `Command` o nazwie `exitCommand`:

```
private Form mainForm;  
private Command exitCommand;
```

Formularz może zawierać pojedynczy element wyświetlania lub kombinację różnych elementów wyświetlania, takich jak elementy łańcuchowe, pola tekstowe i inne obiekty wyświetlania. Gdy użytkownik wybierze polecenie `exitCommand`, MIDlet zostanie zniszczony, a tym samym aplikacja zostanie zamknięta.

Jak zapewne pamiętają programiści Javy, konstruktor jest wykonywany, gdy odpowiadająca mu wartość zostanie utworzony obiekt tej klasy. Jednak zawartość aplikacji nie zostanie wyświetlona na telefonie komórkowym, dopóki metoda `startApp` nie zostanie wywołana przez menedżera aplikacji. W części konstruktora, jak widać w poniższym kodzie, początkowo tworzony jest obiekt `Form` i dodawany jest do niego element `string`. Następnie tworzona jest instancja polecenia i dodawana do `mainForm` za pomocą metody `addCommand`. Metoda ta po prostu dodaje obiekt polecenia do obiektu `Form`. Na koniec do obiektu formularza implementowana jest metoda `setCommandListener`. Słuchacz umożliwia formularzowi nasłuchiwanie poleceń od użytkownika. Pozwala to na automatyczne wywołanie metody `commandAction`, gdy tylko zostanie odebrane polecenie użytkownika.

```
public Hello() {
    mainForm = new Form("My MIDlet");
    mainForm.append("This is my first MIDlet");
    exitCommand = new Command("Exit", Command.EXIT, 0);
    mainForm.addCommand(exitCommand);
    mainForm.setCommandListener(this);
}
```

Następnie implementowana jest metoda `startApp`, a ekran jest ustawiany na wyświetlanie obiektu Form za pomocą następującej linii kodu:

```
Display.getDisplay(this).setCurrent(mainForm);
```

`getDisplay` jest statyczną metodą klasy `Display`, dlatego można ją wywołać, używając nazwy klasy, czyli `Display`, zamiast nazwy odniesienia do obiektu jako prefiksu. Wywołanie `setCurrent(mainForm)` ustawia `mainForm` jako bieżący formularz do wyświetlenia.

Gdy aplikacja jest niszczona, menedżer aplikacji jest powiadamiany o operacji niszczenia za pomocą `notifyDestroyed`, jak widać w następujących liniach kodu:

```
public void destroyApp(boolean unconditional) {
    notifyDestroyed();
}
```

Metoda `commandAction` jest wywoływana przez aplikację automatycznie po otrzymaniu polecenia od użytkownika:

```
public void commandAction(Command command, Displayable
displayable){}
```

Metoda ta otrzymuje dwa argumenty. `Command` pobiera żądanie użytkownika, dzięki czemu aplikacja określa, którą operację wykonać. W kolejnych liniach kodu polecenie użytkownika jest sprawdzane, jeśli otrzymano `exitCommand`. Aplikacja jest niszczona, a menedżer aplikacji jest powiadamiany o operacji niszczenia.

```
if (command == exitCommand){
    destroyApp(true);
    notifyDestroyed();
}
```

Z drugiej strony, `displayable` pobiera odniesienie do aktualnie wyświetlonego obiektu na ekranie. Jeśli to samo polecenie jest zdefiniowane w kilku obiektach ekranu w aplikacji, można je obsłużyć w metodzie `commandAction` za pomocą parametru `displayable`.

5.4.5 Wewnątrz pakietu MIDlet Suite (pakiet MIDlet)

Aby wdrożyć MIDlet na urządzeniu mobilnym, należy utworzyć pakiet MIDlet, który składa się z:

- Java Archive File (JAR) zawierający:
 - Klasy Java dla MIDletów;
 - Pliki zasobów (obrazy itp.) używane przez MIDlety;
 - Plik manifestu opisujący zawartość pliku JAR.
- Plik deskryptora aplikacji Java (JAD).

Plik JAR składa się głównie z klas java, które są potrzebne w MIDletach. Pliki JAR są zazwyczaj automatycznie tworzone przez używane IDE; dlatego też działania użytkownika nie są wymagane.

(i) *Plik manifestu JAR*

Plik manifestu JAR definiuje atrybuty, które są używane przez AMS do identyfikacji właściwości MIDletów. Plik JAD może również zawierać te same atrybuty. W takim przypadku używane są atrybuty w pliku JAD. Atrybuty w pliku manifestu JAR są używane tylko wtedy, gdy te atrybuty nie są zawarte w pliku JAD. Atrybut w pliku manifestu JAR nie może pojawić się więcej niż raz.

Najczęściej używane atrybuty dla plików manifestu JAD i JAR są następujące:

- *MIDlet-Name*: Nazwa pakietu MIDlet.
- *MIDlet-Version*: Numer wersji pakietu MIDlet. Numery wersji muszą być sformatowane jako X.X[X]. Część [X] nie jest obowiązkowa, a jeśli pozostanie pusta, zostanie automatycznie ustawiona na zero jako ".0". Każda część numeru wersji może mieć maksymalnie dwie cyfry od 0 do 99. Jeśli znacznik MIDlet-Version pozostanie pusty, jest on uważany za nowszą wersję pakietu MIDlet.
- *MIDlet-Vendor*: Nazwa organizacji dostarczającej pakiet MIDlet.
- *MIDlet-Icon*: Ikona reprezentująca pakiet MIDletów. Powinna to być rozróżniająca wielkość liter bezwzględna nazwa pliku obrazu PNG w pliku JAR.
- *MIDlet-Description*: Opis pakietu MIDlet.
- *MIDlet-Info-URL*: Adres URL do dalszego opisu pakietu MIDlet.
- *MIDlet-<n>*: Definicja MIDletów w pakiecie. Trzy wpisy muszą być zawarte i oddzielone przecinkami, które są nazwą MIDletu, ikoną MIDletu (jeśli istnieje) i klasą MIDletu. Liczba zaczyna się od 1 i dla każdego MIDletu wzrasta kolejno.
- *MIDlet-Jar-URL*: Adres URL pliku JAR. Można używać bezwzględnych i względnych adresów URL. Względny adres URL rozpoczyna się od folderu zawierającego deskryptor aplikacji.
- *MIDlet-Jar-Size*: Rozmiar pliku JAR w bajtach.
- *MIDlet-Data-Size*: Minimalna liczba bajtów trwałych danych wymaganych przez MIDlet.
- *MicroEdition-Profile*: Profil J2ME (na przykład "MIDP-2.0").
- *MicroEdition-Configuration*: J2ME Configuration (na przykład "CLDC-1.0"). Istnieją również dodatkowe atrybuty. Szczegółowe informacje na temat wszystkich atrybutów i dodatkowe informacje można znaleźć na stronie <http://java.sun.com/javame>.

Istnieją trzy atrybuty, które muszą być zawarte w pliku manifestu JAR:

- MIDlet-Name
- Wersja MIDlet
- MIDlet-Vendor

Następujące trzy atrybuty muszą być zawarte w manifeście JAR lub pliku JAD:

- *MIDlet-<n>* (dla każdego MIDletu)
- *MicroEdition-Profile*

Tabela 5.4 Obowiązkowe atrybuty dla plików manifestu JAD i JAR

Nazwa atrybutu	Manifest JAR	JAD	Jeden z plików
MIDlet-Name	Obowiązkowe	Obowiązkowe	
Wersja MIDlet	Obowiązkowe	Obowiązkowe	
MIDlet-Vendor	Obowiązkowe	Obowiązkowe	
<i>MIDlet-<n></i>			Obowiązkowe
MIDlet-Jar-URL	Obowiązkowe		
MIDlet-Jar-Size	Obowiązkowe		
MicroEdition-Profile			Obowiązkowe
MicroEdition-Configuration			Obowiązkowe

- MicroEdition-Configuration

Plik manifestu może zawierać także inne atrybuty, ale nie są one obowiązkowe.

(ii) Plik JAD

Plik JAD jest używany przez MIDlet dla atrybutów specyficznych dla konfiguracji. AMS zarządza MIDletami za pomocą pliku JAD wraz z plikiem manifestu JAR. Pozwala to również na dostarczanie atrybutów do MIDletów bez modyfikowania pliku JAR. Rozszerzenie pliku JAD to "jad".

Następujące pięć atrybutów musi być zawarte w pliku JAD, jednak plik JAD może zawierać również inne opcjonalne atrybuty:

- MIDlet-Name
- Wersja MIDlet
- MIDlet-Vendor
- MIDlet-Jar-URL
- MIDlet-Jar-Size

Jak wynika z tabeli 5.4, istnieją trzy wspólne obowiązkowe atrybuty (MIDlet- Name,

MIDlet-Version, MIDlet-Vendor) dla obu plików. Atrybuty te jednoznacznie identyfikują aplikację i muszą być zduplikowane w obu plikach. Jeśli wartości tych atrybutów nie są takie same w obu plikach, plik JAR nie może zostać zainstalowany.

Inne atrybuty nie muszą być zduplikowane w obu plikach. Jeśli jednak jest zduplikowany, należy pamiętać, że zostanie użyty ten, który znajduje się w pliku JAD, a drugi może zostać zignorowany. Należy pamiętać, że metoda `getAppProperty` odbiera właściwości aplikacji z plików manifestu JAD i JAR. Metoda ta najpierw przeszukuje plik JAD. Jeśli nie może

znajdzie określony atrybut w tym pliku, a następnie przeszuka plik manifestu JAR. Przykładowa zawartość pliku JAD jest podana poniżej:

```

MIDlet-Name: Hello
Midlet MIDlet-Version:
1.0.0
MIDlet-Vendor: My Vendor Name
MIDlet-1: Hello,,Hello
MicroEdition-Profile: MIDP-
2.0
MicroEdition-Configuration: CLDC-
1.1 MIDlet-Jar-URL: Hello.jar
MIDlet-Jar-Size: 1219

```



Rysunek 5.10 Ekrany MIDletów UIMIDlet.

5.4.6 Bardziej szczegółowy interfejs użytkownika MIDlet

Przedstawiamy teraz MIDlet, który jest bardziej szczegółowym przykładem pokazującym, jak korzystać z pól tekstowych, list i pól tekstowych. Jak widać na zrzutach ekranu aplikacji (rysunek 5.10), aplikacja ta demonstruje użycie niektórych interfejsów użytkownika, takich jak menu listy, pola tekstowe, pola tekstowe, a także słuchacze poleceń. Lewy górny ekran na rysunku 5.10 przedstawia główny ekran MIDletu. Składa się on z niejawnego menu listy, które przekierowuje użytkownika do różnych menu poprzez wybór. Wybór "Form" wyświetla użytkownikowi formularz składający się z pól tekstowych. Wybór "TextBox" wyświetla użytkownikowi pole tekstowe, a wybór "List" wyświetla użytkownikowi menu z wieloma listami. Akcje poleceń są stosowane tylko do wyświetlania menu; dalsza implementacja nie jest wykonywana, ponieważ nie jest to w zakresie tego MIDletu. Różne akcje zostaną podane w sekcji 5.5.

(i) Kod źródłowy aplikacji

```
import javax.microedition.lcdui.* ;
import javax.microedition.midlet.* ;

public class UIMIDlet extends MIDlet implements
    CommandListener {
```

```
// utworzenie obiektu
wyświetlacza private Display
screen;

/*
 * utworzyć dwie listy, jedną dla menu głównego i jedną
 * dla menu wielokrotnego wyboru
 */
private List listMenu, listMultiple;

// utworzenie pola
tekstowego private TextBox
bodyText;

// utworzenie
formularza private
Form mainForm;

// tworzenie pól tekstowych
private TextField toField, subjectField,
ccField, bccField;
/*
 * tworzenie poleceń powrotu do menu głównego
 * i wyjście z MIDletu
 */

private Command backCommand = new
Command("Back", Command.BACK, 0);
private Command exitCommand = new
Command("Exit", Command.EXIT, 1);

public UIMIDlet(){

    // utworzenie listy do wyświetlenia w menu głównym
    listMenu = new List("My List", Choice.IMPLICIT);
    listMenu.append("Simple Form", null);
    listMenu.append("Simple TextBox", null);
    listMenu.append("Simple List", null);
    listMenu.addCommand(exitCommand);
    listMenu.setCommandListener(this);
}

public void startApp(){

    screen = Display.getDisplay(this);
    mainMenu();
}

public void pauseApp(){

}

public void destroyApp(boolean unconditional) {
```

```
    notifyDestroyed();
}

void mainMenu() {
    // ustaw bieżący ekran na listę listMenu
    screen.setCurrent(listMenu);
}

public void commandAction(Command command,
                           Displayable displayable) {

    String label = command.getLabel();

    // zniszcz, jeśli użytkownik naciśnie
    polecenie Exit if
    (label.equals("Exit")) {
        destroyApp(true);
    }else if (label.equals("Back")) {

        // pokaż menu główne, jeśli użytkownik
        naciśnie polecenie Wstecz mainMenu();
    }else {

        /*
         * jeśli nic powyżej się nie wydarzyło, to użytkownik
         * wybrał elementu na ekranie głównym
         */
        switch(((List) screen.getCurrent())
               .getSelectedIndex()){

            case 0:
                emailHeader();
                break;
            case 1:
                emailBody();
                break;
            case 2:
                emailOptions();
                break;
        }
    }
}

/*
 * utworzyć formularz do komponowania podstawowych
 * informacje nagłówka wiadomości e-mail i
 * wyświetlać
 */
public void emailHeader() {

    mainForm = new Form("E-mail Header");
}
```

```
toField = new TextField("To:", "", 32,  
    TextField.EMAILADDR);  
  
subjectField = new TextField("Subject:", "",  
    32, TextField.ANY);  
  
ccField = new TextField("Cc:", "", 32,  
    TextField.EMAILADDR);  
  
bccField = new TextField("Bcc:", "", 32,  
    TextField.EMAILADDR);  
mainForm.append(toField);  
mainForm.append(subjectField);  
mainForm.append(ccField);  
mainForm.append(bccField);  
mainForm.addCommand(backCommand);  
mainForm.addCommand(exitCommand);  
mainForm.setCommandListener(this);  
screen.setCurrent(mainForm);  
}  
  
/*  
 * utworzyć pole tekstowe do tworzenia treści  
 * e-mail i wyświetlić go  
 */  
public void emailBody() {  
  
    bodyText = new TextBox("E-mail Body:", "",  
        255, TextField.ANY);  
    bodyText.addCommand(backCommand);  
    bodyText.addCommand(exitCommand);  
    bodyText.setCommandListener(this);  
    screen.setCurrent(bodyText);  
}  
  
/*  
 * utworzyć listę wielokrotnego wyboru dla  
 * wybieranie opcji poczty e-mail i wyświetlanie jej  
 */  
public void emailOptions() {  
  
    listMultiple = new List("Choose E-mail  
        Options", Choice.MULTIPLE);  
    listMultiple.append("Request Read Receipt",  
        null);  
    listMultiple.append("Request Delivery  
        Receipt", null);  
    listMultiple.append("Save to Sent Items",  
        null);
```

```
    listMultiple.addCommand(backCommand);
    listMultiple.addCommand(exitCommand);
    listMultiple.setCommandListener(this);
    screen.setCurrent(listMultiple);
}
}
```

(ii) Wyjaśnienie kodu

Na samym początku aplikacji poniższe linie kodu tworzą odpowiednie obiekty interfejsu użytkownika:

```
prywatny ekran wyświetlacza;
private List listMenu, listMultiple;
private TextBox bodyText;
private Form mainForm;
private TextField toField, subjectField, ccField, bccField;
private Command backCommand = new Command("Back", Command.BACK, 0);
private Command exitCommand = new Command("Exit", Command.EXIT, 1);
```

Te obiekty interfejsu obejmują:

- Obiekt *Display* do obsługi wyświetlania ekranu.
- Dwa obiekty *List*, które wyświetlają listy na dwóch różnych ekranach.
- Obiekt *TextBox* do wyświetlania pola tekstowego użytkownikowi.
- Obiekt *Form*, który będzie zawierał obiekty *TextField* i polecenia.
- Obiekty *TextField* do pobierania danych wejściowych od użytkownika wewnątrz obiektu *Form*.
- Dwa *polecenia*, aby uzyskać polecenie użytkownika; jedno do powrotu do menu głównego i jedno do wyjścia z aplikacji.

W części konstruktora, obiekt *ListMenu* jest inicjowany z typem wyboru *IMPLICIT*. Do listy dodawane są trzy elementy, a użytkownik może wybrać jeden z nich. Każdemu elementowi automatycznie nadawana jest wartość indeksu, począwszy od 0. Gdy użytkownik wybierze element, wywoływana jest metoda *commandAction*. Nie ma potrzeby dodawania dodatkowego polecenia wyboru, ponieważ klawisz wyboru na urządzeniach mobilnych zostanie automatycznie ustawiony na wybór elementu.

```
public UIMIDlet() {
    listMenu = new List("My List", Choice.IMPLICIT);
    listMenu.append("Simple Form", null);
    listMenu.append("Simple TextBox", null);
    listMenu.append("Simple List", null);
    listMenu.addCommand(exitCommand);
    listMenu.setCommandListener(this);
}
```

List to kolejna klasa w pakiecie *javax.microedition.lcdui*. Gdy wyświetlany jest obiekt *List*, użytkownik może wejść z nim w interakcję, wybierając jedną z dostępnych opcji. Operacja *wyboru* na elemencie listy różni się w zależności od urządzenia. W urządzeniach, które mają dedykowany klawisz wyboru, operacja wyboru jest zaimplementowana za pomocą tego klawisza.

Tabela 5.5 Dostępne typy list Java ME

Typ listy	Opis
EXCLUSIVE	Można wybrać tylko jeden element na raz
MULTIPLE	Można wybrać dowolną liczbę elementów jednocześnie
IMPLICIT	Obecnie skoncentrowany element jest wybierany po wydaniu polecenia

Obiekty listy mogą być tworzone z typami wyboru EXCLUSIVE, MULTIPLE i IMPLICIT (patrz tabela 5.5).

Wewnątrz metody `startApp` wywoływana jest metoda `mainMenu`, która ustawi bieżący ekran na obiekt listy `listMenu`.

```
public void startApp(){
    screen = Display.getDisplay(this);
    mainMenu();
}

void mainMenu() {
    screen.setCurrent(listMenu);
}
```

`listMenu` jest listą wyświetlaną na ekranie głównym. Ponieważ menu główne jest wywoływanie z wielu części aplikacji, tworzona jest specjalna metoda do wyświetlania menu głównego, która jest wywoływana za każdym razem, gdy menu główne musi zostać wyświetlone.

Jak widzieliśmy wcześniej, gdy użytkownik naciśnie przycisk, wywoływana jest metoda `commandAction`. W tym przykładzie istnieją trzy opcje, które użytkownik może wybrać:

1. Zamknij aplikację.
2. Wróć (do menu głównego).
3. Wybierz opcję z menu głównego.

W metodzie `commandAction` polecenie użytkownika jest odbierane poprzez zapisanie etykiety przycisku komendy do łańcucha znaków. Należy pamiętać, że przycisk jest tworzony z etykietą. Etykieta `exitCommand` jest ustawiana na "Exit", a etykieta `backCommand` na "Back". Aplikacja wychodzi, gdy ciąg "label" jest równy "Exit" i wyświetla menu główne, gdy ciąg "label" jest równy "Back".

```
public void commandAction(Command command, Displayable
displayable) {
    String label = command.getLabel();
    if (label.equals("Exit"))
    {
        destroyApp(true);
    }
    else if (label.equals("Back"))
    {
        mainMenu();
    }
    inny
    {
        switch(((List) screen.getCurrent()).getSelectedIndex())
```

```

    {
        case      0:      emailHeader();
        b r e a k ;   case 1: emailBody();
        break;           case      2:
        emailOptions(); break;
    }
}

```

Wreszcie, jeśli etykieta wybranego polecenia nie jest równa "Back" lub "Exit", oznacza to, że użytkownik wybrał opcję z menu głównego. Wybór użytkownika jest uzyskiwany za pomocą indeksu wybranej listy bieżącego ekranu, a odpowiednia metoda jest wywoływana przez MIDlet.

W metodzie `emailHeader` tworzony jest nowy formularz, do którego dodawane są pola tekstowe związane z nagłówkiem wiadomości e-mail i poleceniami.

W metodzie `emailBody` tworzony jest pole tekstowe dla treści wiadomości e-mail, a do wyświetlanego obiektu dodawane są polecenia.

W metodzie `emailOptions` tworzona jest nowa lista wielokrotnego wyboru i dodawane są do niej elementy listy. Dodawane są również dwa polecenia umożliwiające powrót do menu głównego i wyjście z aplikacji.

5.4.7 Push Registry

`PushRegistry` jest klasą zdefiniowaną w pakiecie `javax.microedition.io`. Zwykle MIDlety mogą być wykonywane, gdy użytkownik uruchomi je z menu urządzenia mobilnego. Alternatywnie, MIDlet może zostać wywołany za pomocą funkcji "Push", bez jakiejkolwiek interakcji z użytkownikiem. Na przykład, aplikacja może zostać uruchomiona przez pakiet sieciowy otrzymany przez przychodząca usługę Short Messaging Service (SMS).

`PushRegistry` po prostu utrzymuje listę połączeń przychodzących i mapuje ciągi połączeń sieciowych na nazwy klas. AMS nasłuchiwał przychodzącej aktywności sieciowej i powiadomień. Gdy do AMS dotrze powiadomienie dla zarejestrowanego MIDletu, AMS uruchamia MIDlet za pomocą metody `startApp`.

`PushRegistry` może być zaimplementowany na dwa sposoby:

- *Rejestracja statyczna*: Aplikacja może zarejestrować rekord push z wpisem w pliku JAD.
- *Rejestracja dynamiczna*: Aplikacja może zarejestrować rekord push dynamicznie poprzez wywołanie funkcji `registerConnection` w MIDletie.

(i) Rejestracja statyczna

Aby zadeklarować połączenie push statycznie, atrybut `MIDlet-Push-<n>` musi być określony w pliku JAD lub pliku manifestu JAR.

`MIDlet-Push-<n>: <ConnectionURL>, <MIDletClassName>, <AllowedSender>`

- *MIDlet-Push-<n>*: Nazwa atrybutu dla rejestracji Push. `<n>` zaczyna się od 1 i wzrasta kolejno.
- *ConnectionURL*: Ciąg połączenia używany w metodzie `Connector.open`. Gdy to połączenie zostanie nawiązane, MIDlet zostanie wypchnięty.

- *MIDletClassName*: MIDlet, który zostanie wypchnięty. MIDlet powinien być również zarejestrowany w deskryptorze lub pliku manifestu. Wymagana rejestracja powinna być dokonana za pomocą atrybutu MIDlet -<n>.
- *AllowedSender*: Filtr, który włącza lub ogranicza nadawców pchających MIDlet. Wpisy w tym polu powinny być zgodne z wymaganym formatem adresowania. To pole może zawierać:
 - Dowolne adresy IPv4 i IPv6 w nawiasach kwadratowych
 - "*" znak pasujący do dowolnego źródła
 - znak "?", aby dopasować dowolny pojedynczy znak

W części *AllowedSender* można użyć symboli wieloznacznych, na przykład "193.255.146.*", aby dopasować podsieć. Numery portów nie mogą być filtrowane w tym atrybutie.

Jeśli dwa pakiety MIDlet mają to samo statyczne połaczenie push i jeden z nich jest już zainstalowany na urządzeniu mobilnym, użytkownik powinien odinstalować pierwszy pakiet, aby pomyślnie zainstalować drugi pakiet, ponieważ więcej niż jeden MIDlet nie może zarejestrować tego samego połączenia push.

Przykładowa statyczna rejestracja wpisu rejestru push powinna wyglądać następująco:

`MIDlet-1: MyGame, , example.games.MyGame`

`MIDlet-Push-1: datagram://:50000, example.games.MyGame, *`

(ii) Dynamiczna rejestracja

Podobnie jak w przypadku rejestracji statycznej, aby zaimplementować wpis rejestru push, należy ustawić trzy elementy. Elementy te powinny być ustawione jako parametry w metodzie `PushRegistry.registerConnection`.

Poniższy przykład dynamicznie rejestruje połaczenie rejestru push w taki sam sposób, jak w przypadku rejestracji statycznej:

```
PushRegistry.registerConnection("datagram://:50000",
"example.games.MyGame", )*
```

Aby usunąć dynamiczny wpis rejestru push, należy usunąć powiązany pakiet MIDlet lub wyrejestrować wpis za pomocą metody `PushRegistry.unregisterConnection` w klasie `PushRegistry`. Więcej informacji na temat rejestru push można znaleźć na powiązanej stronie internetowej <http://java.sun.com/javame/>.

Rejestracje dynamiczne i statyczne mają swoje zalety i wady. Rejestracja statyczna umożliwia łatwą rejestrację połączenia push bez interakcji użytkownika. Jeśli jednak w urządzeniu znajduje się wpis rejestru push powodujący konflikt, aplikacja nie może zostać zainstalowana. Z drugiej strony, dynamiczna rejestracja eliminuje ten problem, a aplikacja jest instalowana niezależnie od wpisów rejestru push w telefonie komórkowym. Jednak w przypadku dynamicznej rejestracji wpis push jest zapisywany przy pierwszym uruchomieniu aplikacji.

W tej sekcji przedstawiliśmy krótkie wprowadzenie do Java ME. Aby uzyskać więcej informacji, zachęcamy czytelników do przeczytania konkretnych książek na temat Java ME i korzystania z zasobów internetowych, takich jak:

- Ogólne informacje na temat Java ME

<http://java.sun.com/javame/>

- Konfiguracja podłączonego ograniczonego urządzenia

<http://java.sun.com/products/cldc/>

- Profil mobilnego urządzenia informacyjnego

- <http://java.sun.com/products/midp/>
- *Dokumentacja techniczna Java ME*
<http://java.sun.com/j2me/docs/>
 - *Strona dla programistów Java*
<http://developer.java.sun.com>

5.5 Rozwój aplikacji NFC

W tej sekcji zaczynamy mówić o programowaniu NFC. Do tworzenia aplikacji NFC wymagane są dwa interfejsy API, a mianowicie JSR 257 i JSR 177. JSR 257 zapewnia zasoby do programowania aplikacji w trybie czytnika / zapisu, podczas gdy JSR 177 i niektóre klasy w JSR 257 zapewniają dostęp do SE. Do programowania w trybie peer-to-peer wymagane są własne interfejsy API, ponieważ ten tryb nie jest obsługiwany przez standardowe interfejsy API Java.

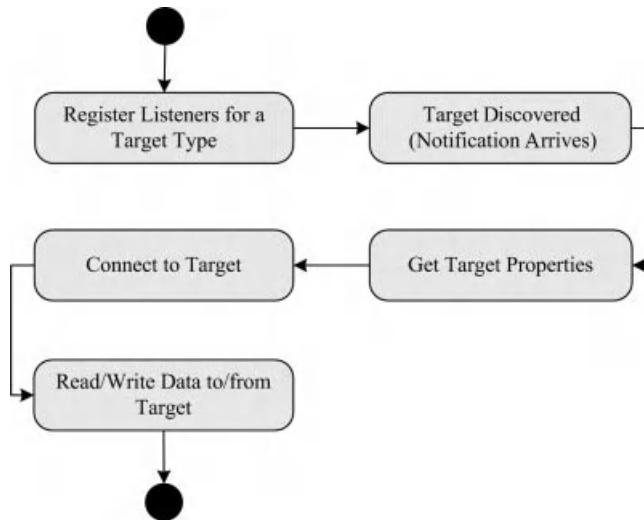
- *JSR 257 (Contactless Communication API)*: Ten interfejs API opisuje komunikację bezstykową i rejestr push w NFC. Zapewnia interfejs programowania aplikacji, który umożliwia aplikacjom dostęp do tagów RFID, kart inteligentnych i tagów wizualnych (kodów kreskowych). Dla każdego typu celu zdefiniowano różne pakiety, a aplikacja korzystająca z tego interfejsu API może wykrywać cele bezstykowe, a następnie łączyć się z celem za pomocą odpowiedniego pakietu opartego na typie celu [12].
 - *JSR 177 (Security and Trust Services API, SATSA)*: Ten interfejs API zapewnia dostęp do kart inteligentnych
 - i zapewnia operacje bezpieczeństwa ukierunkowane na SE przy użyciu protokołów APDU (Application Protocol Data Unit) i JavaCard RMI (Remote Method Invocation) [13].
 - JSR 177 vs. JSR 257 (różnica w dostępie do kart inteligentnych):
 - Obie umożliwiają aplikacjom dostęp do kart inteligentnych.
 - JSR257 umożliwia dostęp do karty inteligentnej z połączeniem ISO14443.
 - JSR177 umożliwia dostęp do karty inteligentnej za pomocą APDUConnection lub JavacardRMI – .
- Połączenie.

5.6 Programowanie trybu czytnika/zapisu

Interfejs API komunikacji bezstykowej (JSR 257) [12] zapewnia interfejs programowania aplikacji, który umożliwia aplikacjom dostęp do tagów RFID, kart inteligentnych i tagów wizualnych. Aplikacja korzystająca z tego interfejsu API może wykrywać cele bezstykowe, a następnie łączyć się z nimi za pomocą odpowiedniego pakietu opartego na typie celu.

W przypadku trybu czytnika/zapisu, JSR 257 umożliwia wykrywanie bezstykowych tagów RFID i łączenie ich z telefonami komórkowymi obsługującymi NFC. Pakiety związane z trybem czytnika/zapisu są omówione w tej sekcji. Na przykład użytkownik może otworzyć stronę internetową, dotykając swoim urządzeniem mobilnym tagu zawierającego adres URL strony na inteligentnym plakacie. Aplikacja najpierw wykryje cel, następnie połączy się z celem za pomocą powiązanego pakietu i odczyta zawartość celu. Na koniec aplikacja może zachowywać się tak, jak została zaprogramowana.

Aby komunikować się z celem, urządzenie mobilne musi najpierw zarejestrować słuchaczy dla określonego typu celu (np. typy tagów sformatowanych przez NFC Forum) przy użyciu instancji klasy `DiscoveryManager` i metody `addTargetListener`. Gdy określony cel zostanie wykryty w pobliżu, powiadomienie dociera do metody



Rysunek 5.11 Przebieg procesu komunikacji bezstykowej.

interfejsu `TargetListener`. Właściwości urządzenia, które są potrzebne do nawiązania połączenia, są również przesyłane do metody `targetDetected`. Po nawiązaniu połączenia z obiektem docelowym urządzenie może wykonywać operacje odczytu i zapisu na obiekcie docelowym. Procesy te zostały przedstawione na rysunku 5.11.

Istnieje pięć pakietów zdefiniowanych w JSR 257 API. Do pracy z tym API wymagana jest wersja 1.1 CLDC.

Z tabeli 5.6 wynika, że pakiety wyróżniają się różnymi typami docelowymi, z wyjątkiem pakietu `javax.microedition.contactless`. Pakiet ten jest zawarty we wszystkich

Tabela 5.6 Pakiety JSR 257

Pakiet	Opis	Obsługiwany cel
<code>javax.microedition.contactless</code>	Zapewnia wspólne funkcje dla wszystkie cele zbliżeniowe, takie jak wykrywanie celu	Wspólny
<code>javax.microedition.contactless.ndef</code>	Zapewnia funkcjonalność do wymiany Dane sformatowane przez NFC Forum z tagami RFID	NDEF_TAG
<code>javax.microedition.contactless.rf</code>	Umożliwia komunikację z RFID znaczniki zawierające dane niesformatowane przez Forum NFC	RFID_TAG
<code>javax.microedition.contactless.sc</code> zewnętrznym	Umożliwia komunikację z smart cards	ISO14443_CARD VISUAL_TAG
<code>javax.microedition.contactless.</code> odczytu danych na	visualZapewnia funkcjonalność tagi wizualne i generowanie obrazów tagów wizualnych	

aplikacje, które implementują interfejs API komunikacji zbliżeniowej niezależnie od urządzenia docelowego. Dodatkowo, jeden z pozostałych pakietów jest wykorzystywany w aplikacji w zależności od typu urządzenia docelowego.

Typ docelowy NDEF_TAG definiuje tag, który zawiera dane sformatowane przez NFC Forum. RFID_TAG to ogólny tag RFID, który zawiera dane w zastrzeżonym formacie. ISO14443_CARD definiuje karty inteligentne zgodne z ISO14443-4, do których można uzyskać dostęp za pomocą poleceń APDU zdefiniowanych w ISO7816-4. Z drugiej strony VISUAL_TAG jest ogólnym tagiem wizualnym.

W kolejnych sekcjach opisano najpierw wspólny pakiet dla wszystkich typów docelowych, `javax.microedition.contactless`. Następnie opisano pozostałe dwa pakiety dla typów NDEF_TAG i RFID_TAG oraz podano przykłady kodu.

5.6.1 Pakiet `javax.microedition.contactless`

Pakiet ten zawiera wspólne klasy i interfejsy, które mogą być używane wraz ze wszystkimi typami docelowymi. Jest to również punkt wyjścia dla interfejsu API JSR 257. Główną funkcją pakietu jest wykrywanie zbliżeniowych obiektów docelowych. Aplikacja może otrzymywać powiadomienia, gdy nowe cele zostaną wykryte w pobliżu i może nawiązać połączenie z konkretnym celem, które jest zdefiniowane w pakietach specyficznych dla celu.

Pakiet składa się z trzech klas, z których jedna jest klasą wyjątków, oraz trzech interfejsów (patrz Tabela 5.7).

(i) Klasa `DiscoveryManager`

Klasa `DiscoveryManager` jest sercem tego pakietu. Umożliwia ona wykrywanie celów w pobliżu, zarządzanie różnymi nasłuchiwanymi i wiele więcej. Zwraca również listę typów celów obsługiwanych przez implementację API za pomocą metody `getSupportedTargetTypes`. Możliwe typy celów zostaną podane w klasie `TargetType`.

Metoda `addTargetListener` służy do dodawania odbiornika dla określonego typu celu, aby otrzymywać powiadomienia, gdy cel jest dostępny w pobliżu. Należy pamiętać, że dla każdego typu celu można zarejestrować tylko jednego słuchacza. Jeśli dla danego typu celu zostanie zarejestrowany inny słuchacz, zostanie zgłoszony wyjątek `IllegalStateException`. Metoda `removeTargetListener` usunie określonego słuchacza. Metoda `getProperty` odbiera właściwości celu po jego wykryciu.

(ii) Klasa `TargetType`

Kolejną klasą w pakiecie `javax.microedition.contactless` jest `TargetType`, która zbiera obsługiwane typy docelowe. Dostępne interfejsy połączenia z fizycznym celem można zebrać za pomocą metody `getConnectionNames` w interfejsie `TargetProperties`.

Tabela 5.7 Pakiet `javax.microedition.contactless`

Klasy	<code>DiscoveryManager</code> <code>TargetType</code>
Interfejsy	<code>TagConnection</code> <code>TargetListener</code> <code>TargetProperties</code>
Wyjątek	Wyjątek <code>ContactlessException</code>

Tabela 5.8 Obsługiwane typy celów w JSR 257

Typ celu	Opis	Interfejs komunikacyjny
14443-4 compliant	NDEF_TAGNFC Dane sformatowane przez forum zawierające znacznik	NDEFTagConnection z pakietu javax.microedition.contactless.ndef
	RFID_TAGGeneral Znacznik RFID PlainTagConnection od javax.microedition.contactless.rf pakiet	
	ISO14443_CARDISO karty inteligentne	ISO14443Connection z pakietu javax.microedition.contactless.sc
	VISUAL_TAG Ogólny tag wizualny	VisualTagConnection od javax.microedition.contactless Pakiet.visual

Obecnie w tym interfejsie API zaimplementowane są cztery różne typy celów, jak pokazano w tabeli 5.8. Należy pamiętać, że w przyszłości mogą pojawić się dodatkowe implementacje typów docelowych.

(iii) *Interfejs TagConnection*

TagConnection to interfejs znacznika w tym interfejsie API, który zapewnia połączenia tagów RFID, połączenia tagów NDEF i połączenia kart intelligentnych. Należy pamiętać, że interfejs znacznika w rzeczywistości nie definiuje żadnych komponentów, takich jak atrybuty lub metody. Zamiast tego jest używany do oznaczania klas. Połączenia inne niż znaczniki wizualne muszą rozszerzać ten interfejs. Następujące trzy interfejsy dziedziczą interfejs TagConnection:

- NDEFTagConnection dla typów docelowych NDEF_TAG
- PlainTagConnection dla typów docelowych RFID_TAG
- ISO14443Connection dla typów docelowych ISO14443_CARD

(iv) *Interfejs TargetListener*

TargetListener to ważny interfejs, który wszystkie aplikacje muszą zaimplementować, aby otrzymywać powiadomienia o wykryciu celu zbliżeniowego przez urządzenie mobilne. Metoda targetDetected w tym interfejsie jest wywoływana automatycznie po wykryciu celu zbliżeniowego.

Jeśli aplikacja ustawi słuchacza za pomocą metody addTargetListener, otrzyma powiadomienie, gdy określony cel zostanie wykryty i otrzyma wszystkie informacje o celu.

(v) *Interfejs TargetProperties*

Za pomocą interfejsu TargetProperties można zbierać informacje o wykrytym celu. Metoda getConnectionNames zwraca nazwę interfejsu (np. NDEFTagConnection), który jest potrzebny do komunikacji z celem. Metoda getProperty umożliwia aplikacji odpytywanie określonych właściwości celu. Metoda getUid zwraca unikalny identyfikator obiektu docelowego. Metoda getUrl zwraca adres URL w celu utworzenia połączenia z celem. Wreszcie, has targetType sprawdza, czy wykryty cel jest określonego typu.

(vi) *Interfejs TransactionListener*

Interfejs ten został opisany w sekcji 5.8.

(vii) *Wyjątek ContactlessException*

Ten wyjątek jest zgłoszany w przypadku próby wykonania nieobsługiwanej operacji.

Powody rzucenia tego wyjątku są następujące:

- Wywołanie nieobsługiwanej metody przez API;
- Wywołanie nieobsługiwanej metody przez cel;
- Nieobsługiwane użycie interfejsu API.

Wyjątek może być skonstruowany z komunikatem o szczegółach wyjątku lub bez niego:

- public ContactlessException()
- public ContactlessException(java.lang.String message)

5.6.2 Pakiet javax.microedition.contactless.ndef

Pakiet ten zapewnia funkcjonalność wymiany danych w formacie NDEF z obiektemi zbliżeniowymi. Aby pracować z tym pakietem, cel musi zawierać dane w formacie NDEF. Ponadto deweloper nie musi znać fizycznego typu obiektu docelowego, aby wymieniać komunikaty i rekordy NDEF.

Aby otrzymać powiadomienie, gdy cel zostanie wykryty z danymi w formacie NDEF, należy ustawić NDEFRecordListener za pomocą metody addNDEFRecordListener, która znajduje się w klasie DiscoveryManager.

Klasy i interfejsy znajdujące się w tym pakiecie są podane w tabeli 5.9.

(i) Klasa NDEFMessage

Klasa ta zazwyczaj reprezentuje komunikat NDEF. Komunikat NDEF składa się z rekordów NDEF, a manipulacja rekordami (odczyt, dodawanie, usuwanie, aktualizacja) jest zapewniona przez tę klasę. Metody getRecord i getRecords umożliwiają odczyt rekordów z komunikatu. Metoda getNumberOfRecords zwraca liczbę rekordów w wiadomości. Metoda insertRecord pozwala na dodanie rekordu do wiadomości. Metoda removeRecord umożliwia usunięcie rekordu z określonym indeksem.

Dla tej klasy można użyć trzech różnych konstruktorów:

- public NDEFMessage ()
- public NDEFMessage (NDEFRecord [] records)
- public NDEFMessage (byte[] data, int offset)

(ii) Klasa NDEFRecord

Klasa NDEFRecord reprezentuje rekord NDEF i umożliwia operacje na rekordach NDEF. Metoda getId zwraca identyfikator ładunku rekordu. Metoda getPayload zwraca ładunek rekordu jako tablicę bajtów. Metoda getRecordType zwraca

Tabela 5.9 Pakiet javax.microedition.contactless.ndef

Klasy	NDEFMessage NDEFRecord NDEFRecordType
Interfejsy	NDEFRecordListener NDEFTagConnection

typ rekordu. Metoda `appendPayload` dodaje określony ładunek na końcu ładunku rekordu.

W tej klasie istnieją dwa różne konstruktory:

- `public NDEFRecord (NDEFRecordType recordType, byte[] id, byte[] payload)`
- `public NDEFRecord (byte[] data, int offset)`

(iii) *Klasa NDEFRecordType*

Klasa `NDEFRecordType` reprezentuje typ rekordu poprzez przechowywanie jego nazwy i formatu. Format nazwy typu rekordu, jak sama nazwa wskazuje, określa strukturę i format nazwy typu rekordu.

Metoda `getFormat` zwraca format nazwy typu rekordu NDEF. Istnieje sześć możliwych formatów nazw typów rekordów (patrz poniżej). Inna metoda w tej klasie, `equals`, porównuje dwie nazwy typów rekordów. Metoda `getName` zwraca nazwę rekordu NDEF bez żadnych przedrostków. Zwykle nazwy NFC Forum RTD i nazwy zewnętrznych typów rekordów zawierają prefiks (`urn:nfc:wkt:` i `urn:nfc:ext:`). Jednak metoda `getName` nie zwraca tych prefiksów.

• PUSTY

Puste rekordy są identyfikowane przez ten identyfikator. Nazwa typu rekordu w formacie `EMPTY` może być prawidłowa tylko wtedy, gdy ma wartość `null`. Dwie nazwy typu rekordu `EMPTY` są równe, jeśli obie mają wartość `null`, w przeciwnym razie nie są równe. Wartość tej nazwy typu rekordu wynosi 0.

• NFC_FORUM_RTD

Jest to identyfikator formatu nazwy typu rekordu dla NFC Forum RTD, takich jak NFC Text RTD, NFC URI RTD i NFC Smart Poster RTD. Dwie nazwy typu rekordu `NFC_FORUM_RTD` są równe, jeśli wszystkie znaki są równe, a porównanie uwzględnia wielkość liter. Wartość tej nazwy typu rekordu wynosi 1.

• MIME

Jest to identyfikator formatu nazwy typu rekordu dla typów MIME. Dwie nazwy typu rekordu `MIME` są równe, jeśli wszystkie znaki są równe w sposób niewrażliwy na wielkość liter aż do pierwszego znaku `";"`. Wartość tej nazwy typu rekordu wynosi 2.

• URI

Jest to identyfikator formatu nazwy typu rekordu dla typów URI. Dwie nazwy typu rekordu `URI` są równe, jeśli wszystkie znaki są równe. Należy pamiętać, że w porównaniu rozróżniana jest wielkość liter. Zastrzeżone znaki muszą być kodowane przy użyciu kodowania procentowego. Cyfry szesnastkowe powinny być pisane wielkimi literami, a części hosta powinny być pisane małymi literami. Wartość tej nazwy typu rekordu to 3.

• EXTERNAL_RTD

Jest to specyficzny identyfikator formatu nazwy typu rekordu dla nazw typów zewnętrznych NFC Forum. Dwie nazwy typu rekordu `EXTERNAL_RTD` są równe, jeśli wszystkie znaki są równe. Porównanie nie uwzględnia wielkości liter. Wartość tej nazwy typu rekordu wynosi 4.

• NIEZNANY

Jeśli typ ładunku jest nieznany, identyfikatorem formatu nazwy typu rekordu dla tego rekordu jest `UNKNOWN`. Dwie nazwy typu rekordu `UNKNOWN` są równe, jeśli obie mają wartość `null`, w przeciwnym razie nie są równe. Wartość tej nazwy typu rekordu to 5.

(iv) *Interfejs NDEFRecordListener*

Interfejs ten zapewnia powiadomienie aplikacji, gdy rekordy NDEF zostaną usunięte z obiektów docelowych. Aplikacja może jednak tylko odczytywać dane (co oznacza, że

ma dostęp tylko do odczytu) i nie może ich modyfikować ani usuwać

W tym interfejsie zdefiniowana jest metoda `recordDetected`, która jest wywoływana automatycznie przez platformę w celu powiadomienia urządzenia o wykryciu typu rekordu NDEF z obiektu docelowego. Aplikacja wykonuje wymagane działania i ostatecznie dostarcza dane z parametrem `NDEFMessage`.

(v) *Interfejs NDEFTagConnection*

Interfejs `NDEFTagConnection` dziedziczy po interfejsie `TagConnection` w sekcji `javax.microedition.contactless`, jak opisano wcześniej.

Interfejs ten umożliwia wymianę danych z tagami i zbliżeniowymi kartami intelligentnymi. Dane są sformatowane na forum NFC i muszą być przechowywane w obiekcie `NDEFMessage`, który składa się z `NDEFRecords`. Aplikacja może odczytywać/zapisywać dane z/do celu bezstykowego. Nie musi znać typu fizycznego urządzenia docelowego, a jedynie musi wiedzieć, czy typ urządzenia docelowego składa się z danych sformatowanych przez forum NFC.

Aby otworzyć połaczenie z bezstykowym obiektem docelowym, należy go najpierw wykryć i powiadomić za pomocą powiadomienia `targetDetected` z interfejsu `TargetListener`. Następnie identyfikator URI używany do otwarcia połączenia można uzyskać za pomocą interfejsu `TargetProperties`.

5.6.3 Pakiet `javax.microedition.contactless.rf`

Pakiet ten udostępnia interfejs `PlainTagConnection` umożliwiający dostęp do tagów RFID. Jak opisano wcześniej, interfejs `PlainTagConnection` dziedziczy interfejs `TagConnection`. Może być używany z obiektami RFID, które nie zawierają danych sformatowanych przez NFC Forum.

5.6.4 Pakiet `javax.microedition.contactless.sc`

Pakiet ten udostępnia interfejs `ISO14443Connection` umożliwiający dostęp do obiektów docelowych bezstykowych kart intelligentnych zgodnych z normą ISO 14443-4. Należy pamiętać, że bezstykowy interfejs zbliżeniowy ISO/IEC 14443 został już opisany w rozdziale 3. Interfejs `ISO14443Connection` dziedziczy po interfejsie `TagConnection`. Komunikacja opiera się na poleceniach APDU po wykryciu obiektu docelowego. Numer slotu potrzebny do otwarcia połączenia z zewnętrzną kartą intelligentną można uzyskać za pomocą metody `getProperty` z interfejsu `TargetProperties`.

Do tej pory opisaliśmy części związane z trybem czytnika / zapisu interfejsu API komunikacji bezstykowej (JSR 257). Istnieje jeszcze jeden pakiet w tym API, którym jest `javax.microedition.contactless.visual`. Pakiet ten zapewnia komunikację z tagami wizualnymi (kodami kreskowymi), ale wykracza poza zakres tej książki. Części tego API związane z trybem emulacji kart są opisane w sekcji 5.8.

W tej książce przedstawiliśmy tylko krótkie wprowadzenie do tego interfejsu API. Aby uzyskać pełną specyfikację klas, interfejsów i metod, zapoznaj się z `Contactless Communication API`.

5.6.5 Aplikacja w trybie czytnika/zapisu

Udostępniamy przykład, który demonstruje, jak odczytywać rekordy danych ze znaczników w formacie NDEF i jak zapisywać rekordy danych w formacie NDEF do znaczników. Ta aplikacja zawiera dwie dodatkowe klasy: klasę `Read` do odczytu ze znaczników i klasę `Write` do zapisu danych do znaczników. Jak



Rysunek 5.12 Ekrany MIDletu NFCReadWriteMIDlet.

W ramach programowania NFC tworzona jest metoda `targetDetected`, która jest automatycznie wywoływana po wykryciu nowego celu.

Aplikacja zawiera trzy przyciski na ekranie głównym. Dwa przyciski służą do odczytu i zapisu danych z/do tagu, a trzeci służy do wyjścia z aplikacji. Główny ekran MIDletu jest pokazany w lewym górnym rogu rysunku 5.12. Po naciśnięciu przycisku "Read NDEF" wyświetlany jest ekran w prawym górnym rogu. Gdy aplikacja wykryje cel w pobliżu, wyświetlany jest ekran w lewym środkowym rogu rysunku 5.12. Jeśli użytkownik naciśnie przycisk

Po naciśnięciu przycisku "Write NDEF" wyświetlony zostanie ekran po prawej stronie. Po wykryciu celu aplikacja zapisuje żądane dane w znaczniku, jak pokazano na dolnym ekranie na rysunku 5.12.

(i) *Kod źródłowy aplikacji*

```
import java.io.IOException;
import javax.microedition.contactless.*;
import javax.microedition.contactless.ndef.*;
; import javax.microedition.io.Connector;
import javax.microedition.lcdui.*;
import javax.microedition.midlet.*;

public class NFCReadWriteMIDlet extends MIDlet
    implements CommandListener, TargetListener {

    private Display screen;

    private Form mainForm;

    private StringItem screenText = new
        StringItem(null, "Wybierz akcję z menu");
    private String screenString = "";

    /*
     *dane te zostaną zapisane w tagu NFC przez
     *konwersja na tablicę bajtów
     */
    private String payloadString = "Te dane
        zostaną zapisane w tagu";

    /*
     *dwie zmienne logiczne, które przełączają się na true
     *z poleceniem użytkownika i jest używany do decyduowania
     *czy uruchomić funkcję odczytu czy zapisu
     */
    private boolean readTag = false;
    private boolean writeTag = false;

    /*
     *wartość logiczna, która zmienia wartość na true, jeśli
     *typ docelowy to tag NDEF. Jest on używany do informowania
     *użytkownika, jeśli typ docelowy nie jest tagiem NDEF
     */
    private boolean ndefMessage=false;

    private Command readCommand = new Command("Read
        NDEF", Command.OK, 1);
    private Polecenie writeCommand = new
```

```
        Command("Write NDEF", Command.OK, 1);
private Command exitCommand = new
        Command("Exit", Command.EXIT, 0);

// obiekt połączenia dla typów znaczników
NDEF private NDEFTagConnection conn =
null;

/*
 *Obiekt TargetProperties jest tworzony w celu gromadzenia
 *właściwości dla celów bezkontaktowych
 */
private TargetProperties[] target;

public NFCReadWriteMIDlet() {

    mainForm = new Form("NFC Read/Write");
    mainForm.append(screenText);
    mainForm.addCommand(readCommand);
    mainForm.addCommand(writeCommand);
    mainForm.addCommand(exitCommand);
    mainForm.setCommandListener(this);

    /*
     *Obiekt klasy DiscoveryManager jest tworzony w celu
     *Odkryj cele dla płatności zbliżeniowych
     * komunikacja i instancja klasy to
     * pobierane przez metodę getInstance()
     */

    DiscoveryManager dm = DiscoveryManager.
        getInstance();

    // słuchacz dodany dla typów znaczników
    NDEF_TAG try {
        dm.addTargetListener(this,
            TargetType.NDEF_TAG);
    }catch (ContactlessException ce) {
        screenText.setText("Błąd podczas dodawania
            słuchaczy: " + ce.getMessage());
    }
}

protected void startApp() {

    screen = Display.getDisplay(this);
    screen.setCurrent(mainForm);
}

protected void destroyApp(boolean unconditional) {

    try {
```

```
        if (conn != null) {
            conn.close();
        }
    }catch (Exception e) {
        screenText.setText(" Błąd: " +
            e.getMessage());
    }

    notifyDestroyed();
}

protected void pauseApp() {

}

public void commandAction(Command command,
    Displayable displayable) {

    String label = command.getLabel();

    if (label.equals("Exit")) {
        destroyApp(true);
    }

    /*
     *jeśli użytkownik naciśnie przycisk Read NDEF,
     *zmienna readTag ma wartość true
     */
    if (label.equals("Read NDEF")){
        writeTag = false;
        readTag = true;
        screenText.setText("Please touch a tag to
            read");
    }

    /*
     *jeśli użytkownik naciśnie przycisk Write NDEF,
     *zmienna writeTag jest ustawiona na true
     */
    if (label.equals("Write NDEF")){
        readTag = false;
        writeTag = true;
        screenText.setText("Please touch a tag to
            write");
    }

    /*
     *metoda targetDetected jest wywoływaną automatycznie
     *przez platformę po wykryciu celu
    }
}
```

```
/*
public void targetDetected(TargetProperties[]
    prop) {

    /*
     * zmienna docelowa otrzymuje właściwości
     * wykryty cel
     */
    target = prop;

    /*
     * gdy cel zostanie wykryty i jeśli użytkownik już
     * nacisnął przycisk "Czytaj NDEF", nowy wątek to
     * utworzona dla metody Read, która będzie przetwarzać
     * operacja odczytu tagu
     */
    if (readTag) {
        Read read = new Read();
        new Thread(read).start();
    }

    /*
     * gdy cel zostanie wykryty i jeśli użytkownik już
     * nacisnął przycisk "Write NDEF", nowy wątek jest
     * utworzona dla metody Write, która będzie przetwarzać
     * operacja zapisu do tagu
     */
    else if (writeTag) {
        Write write = new Write();
        new Thread(write).start();
    } else {
        screenText.setText("Wybierz akcję z menu");
    }
}

/*
 * ta metoda jest używana do zamknięcia połączenia z
 * cel
*/
public void closeConnection(NDEFTagConnection
    conn){
    try {
        if (conn != null) {
            conn.close();
        }
    } catch (IOException e) {
    }
}
```

```
/*
 * Wątek odczytu jest uruchamiany, gdy przycisk Read NDEF jest
 * włączony.
 * Trafienie i odkrycie nowego celu
 */
public class Read implements Runnable {

    public void run() {

        /*
         * Zmienna "ndefMessage" jest ustawiona na false. Jeśli
         * typ docelowy jest NDEF_TAG i jest ustawiony na
         * true w następujących wierszach
         */
        ndefMessage = false;

        for (int i = 0; i < target.length; i++) {

            /*
             * jeśli typem docelowym jest NDEF_TAG, przetwarzanie
             * kontynuuje
             */
            if (target[i].hasTargetType
                (TargetType.NDEF_TAG)) {

                ndefMessage = true;
                try {

                    /*
                     * Pobierz adres url dla bieżącego celu NDEF_TAG
                     * aby się z nim połączyć
                     */
                    String url = target[i].getUrl
                        (Class.forName("javax.microedition.
                            contactless.ndef.NDEFTagConnection"));

                    conn = (NDEFTagConnection)
                        Connector.open(url);

                    // odczyt sformatowanych danych z
                    // docelowego komunikatu NDEFMessage =
                    conn.readNDEF();

                    if (message != null) {

                        // zapisywanie rekordów NDEF do tablicy
                        "records" NDEFRecord[] records =
                            message.
                                getRecords();

                    /*
                     * zapisać "unikalny identyfikator
                     * target" i liczba rekordów do
                     */
                }
            }
        }
    }
}
```

```
/*screenString" nazwany ciąg znaków, który
*zostanie wyświetlona na ekranie
*/
screenString = "Tag UID: " +
    target[i].getUid() + "\n" +
    records.length + " records exist on
    target";

for (int j=0; j<records.length; j++) {

/*
*dla każdego rekordu, zapisz rekord
*numer, nazwa rekordu, rekord
*format(wartość) i ładunek rekordu
*do "screenString"
*/
screenString += "\n\nRecord Number "
    + j + "\nRecord type: " +
    records[j].getRecordType().
    getName() + "\nRecord Format: " +
    records[j].getRecordType().
    getFormat() + "\nRecord Payload: "
    + new String(records[j].
    getPayload());
}

// wyświetla ciąg znaków na ekranie
screenText.setText(screenString);

} else {
    screenText.setText("Tag UID: " +
        target[i].getUid() + "\nNo saved
        NDEF Messages in the target");
}
} catch (ContactlessException e) {
    screenText.setText("Błąd: " +
        e.getMessage());
} catch (IOException e) {
    screenText.setText("Błąd: " +
        e.getMessage());
} catch (Exception e) {
    screenText.setText("Błąd: " +
        e.getMessage());
}
} // koniec klauzuli if
} // koniec pętli for

if(!ndefMessage){screenText.setText("Target
type is not an
znacznik w formacie NDEF");}
```

```
}

    closeConnection(conn);
} // koniec konstruktora wątku Read
} // koniec wątku Read

/*
 * Wątek zapisu jest uruchamiany po naciśnięciu przycisku Write
 NDEF
 * trafienie i odkrycie nowego celu
 */
public class Write implements Runnable {

    public void run() {

        ndefMessage = false;

        for (int i = 0; i < target.length; i++) {

            if (target[i].hasTargetType
                (TargetType.NDEF_TAG)) {

                ndefMessage = true;
                try {

                    String url = target[i].getUrl
                        (Class.forName("javax.microedition.
                        contactless.ndef.NDEFTagConnection"));
                    conn = (NDEFTagConnection)
                        Connector.open(url);

                    /*
                     * Tworzy sformatowany obiekt typu rekord
                     * z NFC_FORUM_RTD
                     */
                    NDEFRecordType recordType = new
                    NDEFRecordType(NDEFRecordType.
                    NFC_FORUM_RTD, "urn:nfc:wkt:T");

                    /*
                     * nowy rekord NDEFRecord z określonym
                     * identyfikator typu rekordu i ładunek
                     * są tworzone
                     */
                    NDEFRecord newRecord = new NDEFRecord(
                        recordType, null,
                        payloadString.getBytes());

                    /*
                     * tworzy "newRecord" o nazwie
                     * NDEFRecord do tablicy NDEFRecord.
                     */
                }
            }
        }
    }
}
```

```
*Aby zapisać więcej niż jeden rekord
*do tagowania, wiele rekordów może być
*utworzony i zapisany w tablicy
*/
NDEFRecord[] newRecordArray = new
    NDEFRecord[]{newRecord};

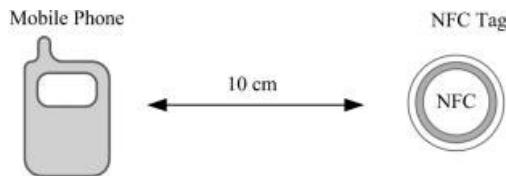
/*
 *Tworzy nowy komunikat NDEF z rozszerzeniem
 * rekord(y) w tablicy NDEFRecord i
 * zapisuje go w tagu
 */
NDEFMessage newMessage = new
    NDEFMessage(newRecordArray);
conn.writeNDEF(newMessage);
screenText.setText(" ---Dane są
zapisywane
do tagu---");
}catch (ContactlessException e) {
    e.printStackTrace();
    screenText.setText("Błąd: " +
        e.getMessage());
}catch (IOException e) {
    e.printStackTrace();
    screenText.setText("Error: " +
        e.getMessage());
} catch (Wyjątek e) {e.printStackTrace();
    screenText.setText("Błąd: " +
        e.getMessage());
}
}
}// koniec klauzuli if
}// koniec pętli for

if(!ndefMessage){screenText.setText("Target
type is not an
znacznik w formacie NDEF");
}

closeConnection(conn);
}// koniec konstruktora wątku zapisu
}// koniec wątku zapisu
}// koniec MIDletu
```

(ii) *Wyjaśnienie Kodeksu*

W bardzo podstawowym wyjaśnieniu, słuchacz dla celów jest rejestrowany przy użyciu metody addTar- getListener podczas uruchamiania aplikacji. Użytkownik może nacisnąć przycisk "Read NDEF"; jednak urządzenie mobilne nie może wykryć celu, ponieważ cel nie znajduje się w pobliżu, jak pokazano na rysunku 5.13.



Target is not in the proximity and the mobile phone cannot detect it

Rysunek 5.13 Znacznik nie znajduje się w pobliżu.

Gdy cel znajdzie się w pobliżu (rysunek 5.14), telefon komórkowy wykrywa cel. Następnie platforma automatycznie wywołuje metodę `targetDetected`. Metoda ta uruchamia wątek `Read`. Wewnątrz wątku nawiązywane jest połączenie z celem i odczytywane są z niego dane.

Teraz opiszemy szczegółowo części MIDletu związane z programowaniem NFC.

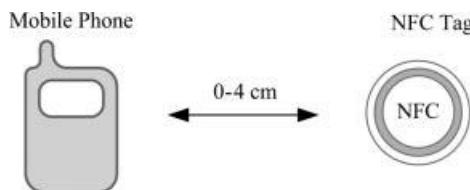
Jak opisano wcześniej, `DiscoveryManager` jest klasą zawartą w pakiecie `javax.microedition.contactless`, która umożliwia aplikacji wykrywanie obiektów zbliżeniowych. Obiekt typu `DiscoveryManager` jest tworzony jako `dm`. Odbiornik docelowy dla tego obiektu jest dodawany za pomocą metody `addTargetListener`, aby otrzymywać powiadomienie, gdy w pobliżu zostanie wykryty cel bezstykowy.

```
DiscoveryManager dm = DiscoveryManager.getInstance();
try {
    dm.addTargetListener(this, TargetType.NDEF_TAG);
} catch (ContactlessException ce) {
    screenText.setText("Błąd podczas dodawania nasłuchujących: " +
        ce.getMessage());
}
```

Nagłówek metody `addTargetListener` pokazano poniżej:

```
addTargetListener(TargetListener listener, TargetType targetType)
```

Jak widać w kodzie MIDletu, słuchacz docelowy jest dodawany w celu wykrycia określonego typu docelowego `NDEF_TAG`.



Target is in the proximity and the mobile phone detects it

Rysunek 5.14 Znacznik w pobliżu.

Metoda `targetDetected` jest wywoływana automatycznie po wykryciu celu w pobliżu. Metoda ta pobiera parametr `TargetProperties`, jak widać w poniższych liniach kodu, i odbiera właściwości wykrytych celów. Po wykryciu nowego celu, właściwości celu są przekazywane do metody `targetDetected`, a właściwości są zapisywane w tablicy celów, jak zdefiniowano wcześniej.

```
private TargetProperties[] target;

public void targetDetected(TargetProperties[] prop) {
    target = prop;
    ...
}
```

Klauzula if-else w metodzie `targetDetected` określa, czy uruchomić wątek `Read` czy `Write` za pomocą zmiennych `boolean readTag` i `writeTag`. Te zmienne logiczne są ustawiane w metodzie `commandAction` po naciśnięciu przez użytkownika przycisku "Read" lub "Write". Jeśli użytkownik wybierze menu "Read NDEF", aby odczytać dane z tagu, zmienna `readTag` zostanie ustawiona na `true`, a zmienna `writeTag` na `false` i odwrotnie w menu "Write NDEF". Klasa `Read` pobiera wiadomość NDEF z celu i drukuje każdy rekord w wiadomości na ekranie. Z drugiej strony, `klassWrite` zapisuje predefiniowany ciąg znaków do tagu jako komunikat NDEF.

5.6.5.1 Czytaj klasę

Klasa `Read` służy do odczytu danych ze znaczników sformatowanych w NDEF. Najpierw ustawia zmienną logiczną `ndefMessage` na `false`, która zostanie ustawiona na `true`, jeśli celem jest `NDEF_TAG`. Zmienna ta jest używana w dalszej części tej klasy do wyświetlanego ostrzeżenia, jeśli typem docelowym nie jest `NDEF_TAG`.

Cel jest sprawdzany za pomocą metody `hasTargetType`, jeśli jest to `NDEF_TAG`. Metoda ta jest jedną z metod zdefiniowanych w interfejsie `TargetProperties`.

```
if(target[i].hasTargetType(TargetType.NDEF_TAG))
```

Gdy cel zostanie zidentyfikowany jako `NDEF_TAG`, aplikacja przechodzi do klauzuli try-catch. Początkowo definiowany jest ciąg o nazwie `url` i ustawiany na adres URL wykrytego celu, który jest potrzebny do połączenia się z celem.

```
url = target[i].getUrl(Class.forName("javax.microedition.contactless.  
ndef.NDEFTagConnection"));
```

Adres URL celu jest uzyskiwany za pomocą metody `getUrl`, która jest zdefiniowana w interfejsie `TargetProperties`. Użycie metody `getUrl` jest następujące:

```
public java.lang.String getUrl(java.lang.Class connectionName)  
conn = (NDEFTagConnection) Connector.open(url);
```

Połączenie z adresem URL jest otwierane za pomocą metody `open`, która jest zdefiniowana w klasie `javax.microedition.io.Connector`. Ponieważ dostęp do danych w formacie NDEF można uzyskać za pomocą `NDEFTagConnection`, parametr w metodzie `getUrl` jest ustawiony na `NDEFTagConnection`.

Po skonfigurowaniu połączenia tworzony jest komunikat NDEFMessage, a rekordy NDEF są odczytywane z tagu za pomocą metody readNDEF, która jest zdefiniowana w interfejsie NDEFTagConnection.

```
NDEFMessage message = conn.readNDEF();
```

Jeśli w tagu znajduje się jakikolwiek komunikat NDEF, tworzona jest nowa tablica NDEFRecord, records, a rekordy są zapisywane w tej tablicy.

```
NDEFRecord[] records = message.getRecords();
```

Istnieją dwa możliwe konstruktory dla NDEFRecord (podane w poprzedniej sekcji). Z drugiej strony, metoda getRecords w klasie NDEFMessage zwraca wszystkie rekordy NDEF w komunikacie NDEF. Użycie tej metody jest następujące:

```
public NDEFRecord[] getRecords()
```

Po zapisaniu wszystkich rekordów NDEF pozostaje tylko przetworzyć dane.

Ponieważ aplikacja zapisała już wszystkie rekordy NDEF w tablicy rekordów, najpierw drukowany jest unikalny identyfikator wykrytego celu, aby pokazać kilka przykładów użycia API. Unikalny identyfikator dotyczy właściwości celu, a metoda getUserId zdefiniowana w interfejsie TargetProperties zwraca unikalny identyfikator wykrytego celu. W aplikacji unikalny identyfikator celu wraz z liczbą rekordów jest zapisywany w ciągu znaków, jak pokazano poniżej:

```
screenString="Tag UID: " + target[i].getUserId() + "\n" +
records.length + " rekordy istnieją w celu";
```

Teraz nadszedł czas, aby wyświetlić rekordy w tagu. Aby wydrukować wszystkie rekordy, musimy wydrukować rekordy w pętli. Możemy zrobić wiele rzeczy używając rekordów z metodami zdefiniowanymi w klasach NDEFMessage i NDEFRecord.

W podanym przykładzie zastosowania dane przedstawione w tabeli 5.10 są drukowane na ekranie.

`getRecordType` to metoda, która jest zdefiniowana w klasie NDEFRecord i zwraca wartość

`NDEFRecordType`, który zawiera informacje o typie i formacie danych.

Funkcja `getRecordType().getName()` zwraca nazwę rekordu NDEF bez żadnych przedrostków. Z drugiej strony, `getRecordType().getFormat()` zwraca format nazwy typu rekordu. Dostępne opcje formatu są zdefiniowane w klasie NDEFRecordType w poprzedniej sekcji. Jako przykład, `NFC_FORUM_RTD` zwraca wartość 1.

Aby wydrukować ładunek danych, używana jest metoda `getPayload`, która jest zdefiniowana w klasie NDEFRecord. Metoda ta zwraca ładunek w rekordzie NDEF jako tablicę bajtów.

Tabela 5.10 Dane drukowane w NFCReadWriteMIDlet

Dane	Wydrukowane przez
Numer rekordu	zmienna j w pętli for
Typ rekordu	<code>getRecordType().getName()</code>
Format rekordu	<code>getRecordType().getFormat()</code>
Ładunek rekordu	<code>getPayload()</code>

W tym przykładzie wszystkie dane zebrane z tagu są zapisywane w łańcuchu o nazwie `screenString`. Ostatnią rzeczą do zrobienia jest wydrukowanie łańcucha na ekranie. `Uid` tagu, liczba rekordów w tagu, numer rekordu, typ rekordu, format rekordu i ładunek wszystkich rekordów mają być wyświetlane na ekranie.

5.6.5.2 Write Class

Klasa `Write` służy do zapisywania danych do tagów w formacie NDEF. Wszystko jest takie samo jak w przypadku klasy

Czytaj klasę do momentu odczytania danych.

Po skonfigurowaniu połączenia z tagiem za pomocą `Connector.open(url)`, tworzony jest obiekt `NDEFRecordType` o nazwie `recordType`. Zawiera on format i nazwę rekordu. W naszym przykładzie wartości formatu i nazwy to odpowiednio `NFC_FORUM_RTD` i `urn:nfc:wkt:T`:

```
NDEFRecordType recordType = new
NDEFRecordType(NDEFRecordType.NFC_FORUM_RTD, "urn:nfc:wkt:T");
```

`NDEFRecordType` jest następnie używany do utworzenia nowego obiektu `NDEFRecord` o nazwie `newRecord`

z określonym typem rekordu, identyfikatorem i ładunkiem:

```
NDEFRecord newRecord= new NDEFRecord(recordType, null,
payloadString.getBytes());
```

Następujący konstruktor jest używany dla `NDEFRecord`:

```
NDEFRecord(NDEFRecordType recordType, byte[] id, byte[] payload)
```

Jak opisano w poprzedniej sekcji, komunikat `NDEFMessage` można utworzyć na trzy sposoby. Utworzymy go za pomocą tablicy `NDEFRecord` w następujący sposób:

```
NDEFMessage(NDEFRecord[] records)
```

Utworzony rekord `NDEFRecord` o nazwie `newRecord` jest zapisywany w nowym rekordzie `NDEFRecord`

w celu skonstruowania komunikatu `NDEFMessage`:

```
NDEFRecord[] newRecordArray = new NDEFRecord[] {newRecord};
```

Następnie tworzony jest nowy komunikat `NDEFMessage` z następującym kodem:

```
NDEFMessage newMessage = new NDEFMessage(newRecordArray);
```

W przykładowym MIDlecie, jeden rekord jest zapisywany do tagu; jednakże, wiele rekordów może być również przetwarzanych poprzez zapisanie wielu rekordów do tablicy `NDEFRecord` w następujący sposób:

```
NDEFRecord[] newRecordArray = new NDEFRecord[] {newRecord1,
newRecord2,...};
```

Ostatnią rzeczą do zrobienia jest zapisanie `NDEFMessage` do tagu:

```
conn.writeNDEF(newMessage);
```

Ważne jest również, aby zamknąć połączenie z celem zbliżeniowym po zakończeniu wymaganych operacji:

```
conn.close();
```

5.6.6 Rejestr NFC Push

Przypomnijmy z wcześniejszych rozdziałów, że rejestr push po prostu utrzymuje listę połączeń przychodzących i mapuje ciągi połączeń sieciowych na nazwy klas w celu ich automatycznego uruchamiania. W przypadku NFC rejestr push jest ważnym tematem; ma na celu poprawę użyteczności aplikacji poprzez automatyczne uruchamianie aplikacji za pomocą połączenia NFC.

W trybie czytnika/nagrywarki, gdy cel zawiera żądzany rekord NDEF, aplikacja zarejestrowana dla tego rekordu może zostać uruchomiona automatycznie, więc użytkownicy nie muszą uruchamiać aplikacji ręcznie. Aby uruchomić aplikację za pomocą rejestrów push, obiekty docelowe muszą mieć rekordy NDEF sformatowane przez NFC Forum.

Nazwa i format nazwy typu rekordu są używane do dopasowania żądanej aplikacji do odpowiedniego rekordu NDEF. Należy pamiętać, że jedna unikalna para nazwy i formatu może być dopasowana tylko do jednej aplikacji. Co więcej, używany jest pierwszy rekord na urządzeniu docelowym, który pasuje do wpisu rejestrów push w telefonie.

Załóżmy, że w pobliżu wykryto cel zbliżeniowy. Najpierw AMS sprawdza dostępne wpisy rejestrów push. Jeśli istnieje wpis o pasującej nazwie i formacie nazwy typu rekordu, aplikacja we wpisie jest wykonywana. W przeciwnym razie, jeśli istnieje słuchacz dla rekordu NDEF (NDEFRecordListener), powiadomienie jest wysyłane do tego słuchacza. Gdy aplikacja jest uruchamiana z wpisem rejestrów push, aplikacja powinna automatycznie zarejestrować słuchacza rekordów NDEF, aby dalej otrzymywać powiadomienia o wykrytych rekordach NDEF.

5.6.6.1 NDEF Push Record Format

Format rekordu push NDEF musi być utworzony w następujący sposób:

NDEF push record format = "ndef:" + record_type_format + "?name=" + record_type_string

Zmienna record_type_format może być przypisana do jednej z następujących czterech dostępnych wartości:

record_type_format= "rtt" | "external_rtt" | "mime" | "uri"

Zmienna record_type_string może mieć wiele wartości:

record_type_string= w pełni kwalifikowana nazwa typu rekordu

Przykładowe rekordy NDEF push znajdują się w tabeli 5.11.

Jak opisano wcześniej, rejestr push może być zaimplementowany na dwa sposoby: rejestracja dynamiczna i rejestracja statyczna.

`javax.microedition.io.PushRegistry`

Tabela 5.11 Przykładowe rekordy NDEF push

Rekord NDEF push	Opis
<code>ndef:rtt?name=urn:nfc:wkt:</code>	SpRecord, aby zarejestrować aplikację, gdy cel zawierający Smart Poster RTD jest wykrywany
<code>ndef:mime?</code> do uruchomienia, gdy	<code>name=text/x-uriRecord</code> , aby zarejestrować aplikację cel zawierający adres URL jest wykrywany
<code>ndef:ext?name=urn:nfc:ext:example.com:</code> adresem URL jest wykrywany.	<code>fRecord</code> w celu zarejestrowania aplikacji, gdy cel z

`.registerConnection` powinna być używana do dynamicznej rejestracji. Istnieją inne przydatne metody w klasie `PushRegistry`, takie jak wyrejestrowanie połączenia lub uzyskanie listy zarejestrowanych połączeń push. Pełna specyfikacja znajduje się w specyfikacji `javax.microedition.io.PushRegistry`.

Przykładowe połączenie rejestru push z mobilnej aplikacji Java wygląda następująco:

```
PushRegistry.registerConnection("ndef:rtd?name=urn:nfc:wkt:T",
    "MyMobileApplication", "*");
```

5.7 Programowanie w trybie peer-to-peer

Wcześniej wspomniano, że tryb peer-to-peer wykonuje komunikację na poziomie łączą między urządzeniami. Nie jest on obsługiwany przez standardowe interfejsy API Java; istnieją jednak różne rozszerzenia interfejsu API komunikacji zbliżeniowej, które umożliwiają programowanie w trybie peer-to-peer. Są to zazwyczaj interfejsy API specyficzne dla urządzeń mobilnych, a mianowicie zastrzeżone interfejsy API. Te interfejsy API można znaleźć na stronach internetowych deweloperów dla określonych urządzeń.

Rozszerzenia API JSR 257 są dostępne dla urządzeń mobilnych Nokia 6212 [14]. Rozszerzenia te zapewniają dodatkowe funkcje, w tym obsługę trybu peer-to-peer. Podsumowanie rozszerzeń API Nokia 6212 JSR 257 podano w tabeli 5.12.

Jak widać w tabeli 5.12, pakiet `com.nokia.llcp` i pakiet `com.nokia.nfc.p2p` zapewniają interfejsy do programowania trybu peer-to-peer przy użyciu LLCP (Logical Link Control Protocol) i NFCIP-1 (Near Field Communication Interface and Protocol-1). Większość funkcji aplikacji trybu peer-to-peer nie może być testowana wraz z SDK, ponieważ potrzebne są dwa urządzenia mobilne, a SDK zapewnia jedną instancję urządzenia mobilnego. Z tego powodu aplikacje powinny być ładowane na telefony komórkowe i testowane na nich.

5.7.1 Pakiet `com.nokia.nfc.p2p`

Pakiet ten zawiera jeden interfejs; `NFCIPConnection`, który zapewnia komunikację między dwoma urządzeniami NFCIP.

Tabela 5.12 Przegląd implementacji Nokia 6212 Classic JSR 257

Nazwa pakietu	Opis
<code>com.innovision.rf.Zapewnia</code>	interfejs umożliwiający dostęp do tagów Innovision Jewel
<code>com.nokia.nfc.llcp</code>	Zapewnia interfejs umożliwiający komunikację ze zdalnymi urządzeniami przy użyciu funkcji
	LLCP
<code>com.nokia.nfc.nxp.desfire</code>	Zapewnja interfejs połączenia i klasy narzędziowe, które mogą być używane, gdy Dostęp do kart MIFARE DESFire
<code>com.nokia.nfc.nxp.mfstd</code>	Zapewnja interfejs dostępu do karty MIFARE Standard
<code>com.nokia.nfc.nxp.simpletag</code>	Zapewnja interfejs dostępu do karty SimpleTag
<code>com.nokia.nfc.p2p</code>	Zapewnja interfejs do komunikacji z urządzeniami NFCIP-1
<code>com.sony.felica</code>	Zapewnja interfejs dostępu do tagu NFC Forum Type 3

Tabela 5.13 Stałe wartości pól
dla NFCIPConnection

Nazwa	Wartość
MAX_LEN	65 524
MODE_INITIATOR	1
MODE_TARGET	2

5.7.1.1 Interfejs NFCIPConnection

Interfejs NFCIPConnection umożliwia komunikację między dwoma urządzeniami przy użyciu NFCIP-1. Podczas komunikacji jedno urządzenie staje się inicjatorem, a drugie urządzeniem docelowym. Komunikacja odbywa się zgodnie z paradigmatem inicjator-ceł, w którym gdy jedno urządzenie wysyła dane, drugie musi nasłuchiwać. Połączenie jest otwierane za pomocą metody Connector.open i na tym etapie określany jest tryb połączenia urządzeń.

Ciąg połączenia musi być sformatowany w następujący sposób:

*NFCIP Connection String = "nfc:rf;type=nfcip;mode=" + target (+ ";timeout=" +
+
timeout)*

- Tryb połączenia może być jednego z dwóch typów:
target = "inicjator" | "cel"
- Limit czasu jest opcjonalny i definiuje wartość limitu czasu dla oczekującego urządzenia docelowego w milisekundach
(1000 ms = 1 s):
timeout = wartość całkowita

Metody wysyłania i odbierania są używane do wysyłania i odbierania danych do/z urządzenia zdalnego w bajtach. Urządzenie inicjujące powinno najpierw wysłać dane, a następnie poczekać na ich odebranie. Po otrzymaniu danych może wysłać je ponownie itd. Z drugiej strony, urządzenie docelowe powinno najpierw poczekać na odebranie danych, a następnie je wysłać.

Za pomocą metody getMode można uzyskać tryb połączenia urządzenia, który zwraca MODE_TARGET lub MODE_INITIATOR. Stałe wartości pól urządzeń docelowych i inicjujących podano w tabeli 5.13. Ponadto metoda getUID zwraca identyfikator uid drugiego urządzenia NFC w bajtach. Stała MAX_LEN w tabeli 5.13 określa maksymalną ilość bajtów, które można wysłać w jednym wywołaniu.

5.7.2 Pakiet com.nokia.nfc.llcp

LLCP API zapewnia interfejs dla MIDletów w celu komunikacji ze zdalnymi urządzeniami za pomocą LLCP.

Pakiet ten zawiera klasę LLCPManager, która służy do zarządzania elementami nasłuchującymi związanymi z LLCP. Pakiet zawiera również cztery interfejsy, jak podano w tabeli 5.14.

Oba typy transportu LLCP są obsługiwane w tym pakiecie. Należy pamiętać, że typ 1 zapewnia bezpośredniowy transport danych, który jest zawodny i bez sesji. Z drugiej strony, typ 2 zapewnia transport danych zorientowany na połączenie, który jest niezawodny i

Tabela 5.14 Pakiet com.nokia.nfc.llcp

Klasy	Interfejsy
LLCPManager	ErrorRecoveryListener
	LLCPConnection
	LLCPConnectionListener
	LLCPLinkListener

transport, połączenia mają oddzielne kanały. Jednak w transporcie typu 1 połączenia są specyficzne dla identyfikatora usługi, a pierwsza przychodząca ramka danych otworzy połączenie. Oba typy transportu są obsługiwane w tym API. Listener jest konfigurowany za pomocą metody `startListening` w klasie `LLCPManager` i tutaj również wybierany jest typ transportu. Komunikacja przy użyciu typu transportu odbywa się za pomocą interfejsu `LLCPConnection`.

Nashuchiwacze działań na łączach LLCP są dodawane i usuwane za pomocą klasy `LLCPManager`, a powiadomienia są odbierane przez interfejs `LLCPLinkListener`. Po ustanowieniu łącza można otworzyć komunikację z obiektem docelowym za pomocą metody `Connector.open`. Gdy połączenie jest skonfigurowane, dane mogą być wysyłane i odbierane za pomocą metod `wysyłania` i `odbierania` w interfejsie `LLCPConnection`.

Format URI połączenia LLCP jest standardowy i musi być sformatowany w następujący sposób: `LLCP Connection String = "nfc:llcp;type=" + transport_type + ";sid=" + service_id + ";uid=" + uid`

- Zmienna `Transport_type` może być jednego z dwóch typów:
`transport_type = "1" | "2"`
- Zmienna `service_id` może mieć różne wartości całkowite od 0 do 62:
`service_id = liczba całkowita (0-62)`
- Zmienna `uid` może mieć różne ciągi szesnastkowe:
`uid = szesnastkowy ciąg znaków uid zdalnego urządzenia LLCP`

(i) Klasa `LLCPManager`

Klasa `LLCPManager` służy do zarządzania nashuchami związanymi z LLCP. Korzystając z metod tej klasy, urządzenie mogą dodawać i usuwać nashuchywaczy, uruchamiać i zatrzymywać nashuchiwanie połączeń przychodzących. Implementuje ona również nashuchiwanie zdarzeń związanych z odzyskiwaniem błędów LLCP.

Metody `addLinkListener` i `removeLinkListener` dodają i usuwają `LLCPLinkListener`, dzięki czemu urządzenie może być powiadamiane o łączach LLCP.

Metody `startListening` i `stopListening` służą do uruchamiania i zatrzymywania nashuchiwanego połączeń. Po otwarciu połączenia automatycznie wywoływana jest metoda `connectionOpened` z interfejsu `LLCPConnectionListener`.

Ponadto dwie metody, `addErrorRecoveryListener` i `removeErrorRecoveryListener` dodają i usuwają `ErrorRecoveryListener` w celu otrzymywania powiadomień o zdarzeniach związanych z odzyskiwaniem błędów LLCP.

(ii) Interfejs `ErrorRecoveryListener`

Interfejs ten służy do wysyłania powiadomień do aplikacji o odzyskaniu łącza LLCP po błędzie. Gdy status odzyskiwania zostanie zmieniony, wywoływana jest funkcja `recoveryStatus(int)`

Tabela 5.15 Stałe wartości pól dla metody recoveryStatus

Nazwa	Wartość
RECOVERY_STARTED	1
RECOVERY_FAILED	2
RECOVERY_SUCCESSFUL	3

przez platformę w celu powiadomienia o zmianie. Możliwe wartości statusu dla metody recoveryStatus podano w tabeli 5.15.

(iii) *Interfejs LLCPConnection*

Interfejs ten służy do komunikacji z innym urządzeniem LLCP. Głównymi metodami interfejsu są send i receive, które służą do wysyłania i odbierania danych. Wartości związane z połączeniem mogą być zbierane przez metody tej klasy. getTransportType zwraca typ transportu połączenia w bajtach. Metoda getUID zwraca identyfikator zdalnego urządzenia w postaci ciągu znaków.

Jak opisano wcześniej, należy wybrać jeden z dwóch różnych typów transportu. Możliwe wartości typów transportu i maksymalnej długości danych, które można przesyłać w jednym połączeniu, podano w tabeli 5.16.

(iv) *Interfejs LLCPConnectionListener*

Interfejs ten jest używany do powiadamiania o otwarciu połączenia LLCP. Metoda connectionOpened jest wywoływana automatycznie przez platformę po otwarciu połączenia.

(v) *Interfejs LLCPLinkListener*

Interfejs ten zapewnia mechanizm powiadamiania o ustanowieniu lub utracie połączenia z obiektem docelowym. Metoda linkEstablished, jak sama nazwa wskazuje, jest wywoływana, gdy połączenie zostanie ustanowione, a metoda linkLost jest wywoływana, gdy połączenie zostanie utracone. Obie metody są wywoływane automatycznie, a identyfikator zdalnego urządzenia jest wysyłany do metody linkEstablished.

(vi) *Push Registry w LLCP*

Wymagana aplikacja może zostać uruchomiona automatycznie za pomocą wpisu rejestrzu push i wyzwalacza drugiego urządzenia. Jednak niektóre parametry muszą być podane w URI rejestracji push.

LLCP Push registry="llcp-type" + transport_type + ":?sid=" + service_id

Tabela 5.16 Stałe wartości pól dla LLCPConnection

Nazwa	Wartość
MAX_DATA_LEN	65 521
TYPE_1	1
TYPE_2	2

Jak wspomniano wcześniej, pakiety związane z trybem peer-to-peer to `com.nokia.nfc.llcp` i `com.nokia.nfc.p2p`. Wprowadziliśmy te dwa pakiety w tej sekcji. Inne pakiety wprowadzają różne typy połączeń związanych z kartami inteligentnymi i tagami, które nie zostały tutaj omówione. Aby dowiedzieć się więcej o tych pakietach i uzyskać bardziej szczegółowe informacje na temat dwóch omawianych pakietów, należy zapoznać się z JSR 257 Nokia Extensions [14].

5.7.3 Aplikacja działająca w trybie peer-to-peer

W tej sekcji przedstawiamy przykładowy MIDlet, który umożliwia komunikację peer-to-peer między dwoma telefonami komórkowymi przy użyciu interfejsu komunikacyjnego NFCIP-1. W tej aplikacji dwóch użytkowników może wysyłać i odbierać wiadomości do siebie nawzajem.

Po pierwszym uruchomieniu MIDlet znajduje się w stanie odczytu, co oznacza, że oczekuje na połączenie od inicjatora. Użytkownikowi wyświetlany jest również formularz ekranu głównego, jak widać na lewym górnym ekranie na rysunku 5.15. Po nawiązaniu połączenia z inicjatorem jest on gotowy do odebrania wiadomości. Należy pamiętać, że w komunikacji NFCIP cel musi najpierw otrzymać komunikat



Rysunek 5.15 Ekrany MIDletów P2PExample.

a następnie wysłać i ponownie odebrać. Jeśli użytkownik chce wysłać wiadomość, wpisuje ją w polu tekstowym widocznym na lewym górnym ekranie, a następnie naciska przycisk "Wyślij wiadomość". W tym przypadku stan aplikacji jest w stanie zapisu, a aplikacja próbuje nawiązać połączenie z urządzeniem docelowym (dolny ekran na rysunku 5.15). Po znalezieniu urządzenia w stanie odczytu następuje wymiana wiadomości.

MIDlet składa się głównie z interfejsu użytkownika, wątku i zmieniacza stanu. Zmieniacz stanu umożliwia MIDletowi przełączanie się ze stanu odczytu do stanu zapisu i odwrotnie. Wątek wykonuje konfigurację połączenia NFCIP-1 i wymianę komunikatów. Po wymianie wiadomości oba urządzenia drukują wymienioną wiadomość na ekranie.

(i) *Kod źródłowy aplikacji*

```
import java.io.IOException;
import javax.microedition.io.Connector;
import javax.microedition.lcdui.*;
import javax.microedition.midlet.*;
import com.nokia.nfc.p2p.NFCIPConnection;

public class P2PExample extends MIDlet
    implements Runnable, CommandListener {

    /**
     * ciąg połączenia używany przez inicjatora i
     * urządzenia docelowe
     */
    private static final String INITIATOR =
        "nfc:rf;type=nfcip;mode=initiator";
    private static final String TARGET =
        "nfc:rf;type=nfcip;mode=target";

    private StringItem screenText = new
        StringItem(null, "Napisz nową wiadomość do
send\n");

    private Display screen;
    private Form mainForm;
    private TextBox chatTextBox;

    private Command writeCommand = new Command("New
Message", Command.SCREEN, 1);
    private Command sendCommand=new
        Command("Wyślij wiadomość", Command.SCREEN,
        1);
    private Command cancelCommand=new
        Command("Cancel", Command.CANCEL, 0);
    private Command exitCommand=new Command("Exit",
        Command.EXIT, 0);
```

```
/*
 *określa, czy aplikacja jest w trakcie odczytu
 *stan lub stan pisemny
 */
boolean readState = true;

public P2PExample() throws IOException {

    mainForm = new Form("Formularz");
    mainForm.append(screenText);
    mainForm.addCommand(writeCommand);
    mainForm.addCommand(exitCommand);
    mainForm.setCommandListener(this);
}

protected void startApp(){

    screen = Display.getDisplay(this);
    screen.setCurrent(mainForm);

    /*
     *nowy wątek jest uruchamiany podczas startu w celu
     *aby otrzymywać połączenia przychodzące i wiadomości pod adresem
     *ekran główny
    */

    Thread thread = new Thread(this);
    thread.start();
}

protected void pauseApp() {

}

protected void destroyApp(boolean unconditional){

    notifyDestroyed();
}

public void commandAction(Command command,
    Displayable displayable) {

    String label = command.getLabel();

    if (label.equals("Exit")) {
        destroyApp(true);
    }else if(label.equals("Nowa wiadomość")) {
        chatMenu();
    }
}
```

```
        }else if(label.equals("Wyślij wiadomość")) {
            changeState();
        }else if (label.equals("Anuluj")) {
            screen.setCurrent(mainForm);
        }
    }
// wyświetla pole tekstowe do napisania
wiadomości public void chatMenu() {

    chatTextBox = new TextBox("Tekst do
        napisania", null, 255, TextField.ANY);
    chatTextBox.addCommand(sendCommand);
    chatTextBox.addCommand(cancelCommand);
    chatTextBox.setCommandListener(this);
    screen.setCurrent(chatTextBox);
}
// metoda zmiany wartości readState
public void changeState() {

/*
 *if readState is true(MIDlet jest w stanie read
 *state) i MIDlet wywołał tę metodę (użytkownik
 *wciśnięty przycisk "Wyślij wiadomość"), readState to
 *ustawiona na false w celu przełączenia na zapis
 *i nawiązać połączenie z celem.
 */
if(readState){
    readState = false;

    Alert sendAlert = new
        Alert("Wysyłanie wiadomości...",
            "Proszę dotknąć", null,
            AlertType.INFO);
    sendAlert.addCommand(cancelCommand);
    sendAlert.setTimeout(10000);
    sendAlert.setCommandListener(this);
    screen.setCurrent(sendAlert);
}

/*
 *jeśli readState ma wartość false (użytkownik pomyślnie
 *wysłał wiadomość), jest ustawiana z powrotem na true
 *(stan odczytu), więc MIDlet ustawia z powrotem na
 *stan odczytu.
 */
else{
    readState = true;
    screen.setCurrent(mainForm);
}
```

```
/*
 *wreszcie nowy wątek rozpoczęty pod koniec
 *metoda w celu aktywacji nowych
 *wartości readState
 */
Thread thread = new Thread(this);
thread.start();
}
/*
*wątek, który wykonuje połączenie NFCIP
*konfiguracja i wiadomość Exchange
*/
public void run() {

/*
 *conn jest ustawione na null, aby zresetować połączenie
 *w każdym uruchomionym wątku
 */
conn = null;

if (readState) {

/*
 *jeśli readState ma wartość true, urządzenie czeka, aż
 *inicjator otwiera połączenie
 */

while (readState) {
try {
conn = (NFCIPConnection)
Connector.open(TARGET);

/*
 *po nawiązaniu połączenia,
 *cel otrzymuje pierwszą wiadomość
 *od inicjatora
 */
byte[] data = conn.receive();

/*
 *target wysyła bezsensowną wiadomość do
 *inicjatora, ponieważ inicjatorem jest
 *oczekiwanie na odpowiedź
 */
conn.send("-1".getBytes());

// zapisanie odebranej wiadomości na ekranie
mainForm.append("Odebrano: " + new
String(data) + "\n");
}
}
```

```
// zamknięcie bieżącego połączenia
conn.close();
} catch (Exception e) {
    screenText.setText("Błąd połączenia
                      : " + e.getMessage());
}
}
} else {

/*
 * jeśli readState ma wartość false, urządzenie próbuje
 * otworzyć połączenie z urządzeniem docelowym
 * i czeka, aż urządzenie zostanie znalezione lub
 * odwołany
 */
while (!readState) {
    try {
        conn = (NFCIPConnection)
            Connector.open(INITIATOR);

    /*
     * gdy połączenie jest skonfigurowane, inicjator
     * wysyła pierwszą wiadomość do celu
     */
    conn.send(chatTextBox.getString().
               getBytes());

    /*
     * inicjator czeka i odbiera
     * odpowiedź od celu
     */
    conn.receive();

    // zapisanie wysłanej wiadomości na ekranie
    mainForm.append("Sent: " +
                    chatTextBox.getString() +"\n");

    // wyświetlenie głównego formularza na ekranie
    screen.setCurrent(mainForm);

    // zamknięcie bieżącego połączenia
    conn.close();

    /*
     * wywołać metodę changeState() w celu
     * zmiany stanu odczytu na true
     */
    changeState();
} catch (Exception e) {
```

```
        screenText.setText ("Błąd połączenia  
        : " + e.getMessage () );  
    }  
}  
}  
}  
}
```

(ii) Wyjaśnienie kodu

Opiszymy teraz części MIDletu związane z programowaniem NFC. Dwa końcowe ciągi są zdefiniowane jako INITIATOR i TARGET. Są to ciągi połączeń, które będą używane do nawiązywania połączenia. Jak widać w ciągu, tryby urządzeń (inicjator lub cel) są również określone.

```
private static final String  
    INITIATOR="nfc:rf;type=nfcip;mode=initiator";  
private static final String  
TARGET="nfc:rf;type=nfcip;mode=target";
```

Tryb pracy peer-to-peer wykorzystuje transmisję półduplekową. W związku z tym jeden z partnerów jest w trybie wysyłania, a drugi w trybie odbierania w danym momencie. Urządzenie wysyłające jest w roli inicjatora dla tej komunikacji, a urządzenie odbierające jest w roli docelowej. Aby poradzić sobie z tą sytuacją, zdefiniowano zmienną logiczną `readState`. Ponieważ w przykładzie zastosowano programowanie wielowątkowe, ten sam kod jest wykonywany przez oba urządzenia. W związku z tym, gdy wartość `readState` jest prawdziwa dla jednego urządzenia, powinna być fałszywa dla drugiego. Metoda `changeState` obsługuje przełączanie między stanami odczytu i zapisu, a tym samym powoduje, że urządzenie staje się inicjatorem lub celem.

```
public void changeState(){  
    ...  
}
```

Metoda `changeState` jest wywoływana dwukrotnie w MIDletie:

- Metoda `commandAction` składa się z wywołania metody `changeState`. Gdy użytkownik wpisuje tekst w polu tekstowym i naciska przycisk "Send Message" w celu wysłania tekstu do urządzenia docelowego, wywoływana jest metoda `commandAction`, po czym urządzenie zmienia swój stan na stan zapisu w celu wykonania akcji wysyłania.
- Po wysłaniu komunikatu MIDlet musi znajdować się w stanie odczytu, aby nasłuchiwać komunikatów przychodzących ze zdalnego urządzenia. Jednak obecnie znajduje się w stanie zapisu, a zmiana stanu jest wykonywana przez wywołanie metody `changeState`.

Programowanie komunikacji peer-to-peer odbywa się w wątku. Obiekt połączenia NFCIP `conn` jest ustawiony na wartość null (co zapewnia ustanowienie nowego połączenia, jeśli

MIDlet nie uruchamia wątku za pierwszym razem), a następnie wątek jest dzielony na dwie części, jedną dla stanu odczytu i jedną dla stanu zapisu.

```
public void run() {  
    ...  
}
```

Urządzenia zarówno w stanie odczytu, jak i zapisu wykonują podobne czynności; jednak obiekt NFCIPConnection jest ustawiony inaczej. Jeśli MIDlet jest w stanie odczytu, jest ustawiony na TARGET; w przeciwnym razie jest ustawiony na INITIATOR.

```
conn = (NFCIPConnection) Connector.open(TARGET);  
conn = (NFCIPConnection) Connector.open(INITIATOR);
```

MIDlet w stanie odczytu najpierw odbiera dane za pomocą metody receive i ustawia tablicę bajtów danych na odebrane dane. Należy pamiętać, że receive jest metodą zdefiniowaną przez interfejs NFCIPConnection i używaną do odbierania danych z innego urządzenia NFC. byte[] data = conn.receive();

Następnie urządzenie docelowe wysyła dane do inicjatora, ponieważ inicjator oczekuje na odpowiedź. W tym przykładzie urządzenie docelowe wysłało "-1" do inicjatora w celu powiadomienia o operacji odbioru. Aplikacja rozumie znaczenie "-1", ponieważ jest zaprogramowana w ten sposób. Metoda wysyłania jest również zdefiniowana przez interfejs NFCIPConnection i służy do wysyłania danych do innego urządzenia NFC.
conn.send("-1".getBytes());

Jedyną pozostałą rzeczą do zrobienia dla urządzenia docelowego jest wydrukowanie otrzymanej wiadomości na ekranie, a następnie zamknięcie połączenia. Nie ma potrzeby zmiany jego stanu, ponieważ nadal znajduje się ono w stanie odczytu.

```
mainForm.append("Otrzymano: " + new String(data) + "\n");  
conn.close();
```

Z drugiej strony, po nawiązaniu połączenia, urządzenie inicjujące najpierw wysyła dane do urządzenia zdalonego i czeka na odpowiedź. Po otrzymaniu odpowiedzi wyświetla dane na ekranie po przełączeniu ekranu na mainForm. Należy zauważyć, że powodem zmiany ekranu jest to, że alert był nadal wyświetlany. Następnie MIDlet zamknie połączenie. Wreszcie, urządzenie inicjujące musi zmienić swój stan ze stanu zapisu na stan odczytu, a zatem wywołuje w tym celu metodę changeState.

```
conn.send(chatTextBox.getString().getBytes());  
conn.receive();  
mainForm.append("Wysłano: " + chatTextBox.getString() + "\n");  
screen.setCurrent(mainForm);  
conn.close();  
changeState();
```

W tym przykładzie zademonstrowano komunikację peer-to-peer. Pokazaliśmy, jak skonfigurować komunikację ze zdalnym urządzeniem oraz jak wysyłać i odbierać wiadomości za pomocą komunikacji NFCIP-1.

5.8 Programowanie trybu emulacji karty

Dostęp do SE można zaprogramować za pomocą JSR 257 lub JSR 177.

5.8.1 Dostęp do bezpiecznego elementu przy użyciu JSR 257

APDUConnection i JavaCardRMIConnection umożliwiają dostęp do kart inteligentnych w JSR 177 API, które zostaną opisane w kolejnych sekcjach. W JSR 257 interfejs Transaction- Listener może być używany do uzyskiwania dostępu do SE.

Gdy wystąpi aktywność między SE a zewnętrznym czytnikiem, MIDlet otrzymuje powiadomienie za pomocą interfejsu TransactionListener, jeśli nasłuchuje SE. Aby otrzymywać powiadomienia, aplikacje muszą zaimplementować ten interfejs, a także zarejestrować słuchacza transakcji za pomocą metody addTransactionListener klasy DiscoveryManager.

Metoda externalReaderDetected jest również zdefiniowana w tym interfejsie, który jest wywoływanego automatycznie przez platformę w celu powiadomienia aplikacji o wystąpieniu zdarzenia na SE. Możliwą przyczyną jest zmiana w SE, a aplikacja może podjąć wymagane działanie (np. wyświetlić pozostałe kredyty na ekranie).

5.8.2 Dostęp do bezpiecznego elementu przy użyciu JSR 177

Security and Trust Services API (SATSA) (JSR 177) [13] definiuje opcjonalne pakiety do obsługi komunikacji kart inteligentnych i operacji bezpieczeństwa. Za pomocą tego interfejsu API można zaimplementować certyfikaty cyfrowe, podpisy cyfrowe i wiele więcej.

Jak opisano we wcześniejszych rozdziałach, SE mogą mieć różne formy. Najważniejszą korzystną opcję SE jest karta inteligentna, a JSR 177 zapewnia środowisko programistyczne. Komunikacja karty inteligentnej z tym API może być zaimplementowana przy użyciu protokołu APDU lub protokołu JavaCard RMI.

Tryb emulacji karty został opracowany głównie w celu zapewnienia aplikacji, które nakładają wysokie ograniczenia bezpieczeństwa, takie jak karty kredytowe. Ten interfejs API obsługuje wymagane operacje bezpieczeństwa, w tym usługi podpisu cyfrowego, zarządzanie poświadczeniami użytkownika, operacje kryptograficzne i przechowywanie kluczy kryptograficznych.

5.8.2.1 Zawartość pakietów opcjonalnych

W tym interfejsie API zdefiniowano cztery opcjonalne pakiety, które składają się z różnych pakietów i klas:

(i) Opcjonalny pakiet SATSA-APDU

Opcjonalny pakiet SATSA-APDU służy do komunikacji z kartami inteligentnymi przy użyciu protokołu opartego na APDU. Ten opcjonalny pakiet zawiera następujące elementy:

- Klasa wyjątku UnsupportedOperationException w pakiecie java.lang
- Pakiet javax.microedition.apdu

(ii) Opcjonalny pakiet SATSA-JCRMI

Opcjonalny pakiet SATSA-JCRMI służy do komunikacji z kartami inteligentnymi przy użyciu protokołu JavaCard RMI. Ten opcjonalny pakiet zawiera następujące elementy:

- Pakiet javax.microedition.jcrmi
- Podzbiór pakietu java.rmi
- Podzbiór pakietu javacard.framework

- Podzbior pakietu javacard.framework.service
- Podzbior pakietu javacard.security
- Klasa wyjątku UnsupportedOperationException w pakiecie java.lang

(iii) *Opcjonalny pakiet SATSA-PKI*

Opcjonalny pakiet SATSA-PKI umożliwia kartom inteligentnym zarządzanie podpisami cyfrowymi i certyfikatami. Ten opcjonalny pakiet zawiera następujące elementy:

- pakiet javax.microedition.pki
- Pakiet javax.microedition.securityservice

(iv) *Opcjonalny pakiet SATSA-CRYPTO*

Opcjonalny pakiet SATSA-CRYPTO zapewnia operacje kryptograficzne, takie jak skróty wiadomości i podpisy cyfrowe w celu zwiększenia bezpieczeństwa. Ten opcjonalny pakiet zawiera następujące elementy:

- Pakiet java.security
- Pakiet java.security.spec
- pakiet javax.crypto
- Pakiet javax.crypto.spec
- Klasa wyjątku IllegalStateException w pakiecie java.lang

5.8.2.2 Szczegóły pakietów opcjonalnych

(i) *Opcjonalny pakiet SATSA-APDU*

Pakiet ten umożliwia aplikacjom dostęp do kart inteligentnych za pomocą APDU. APDU to jednostka komunikacyjna (komunikat) reprezentowana przez bajty. Pakiet ten umożliwia aplikacji na rezydentnej karcie inteligentnej wymianę tych komunikatów APDU z aplikacją na karcie. Polecenia APDU powinny być zgodne z formatem określonym w normie ISO7816-4.

W APDU występują dwa rodzaje komunikatów: APDU poleceń i APDU odpowiedzi. Oznacza to, że aplikacja MIDP może zarówno wysyłać polecenia do aplikacji karty inteligentnej, jak i odbierać od niej polecenia.

Połączenia z kartą inteligentną są nawiązywane przy użyciu Generic Connection Framework. Wywołanie metody Connector.open zwróci połączenie APDU, które zostanie użyte do połączenia z aplikacją karty. Aplikacja karty inteligentnej jest identyfikowana przez identyfikator aplikacji (AID).

Ciąg połączenia APDU musi być sformatowany w następujący sposób:

APDU Connection String= "apdu:" + slot_number + ";target=" + target

- *slot_number* wskazuje numer slotu, przez który aplikacja karty będzie się komunikować.

• *target* jest wartością AID lub ciągiem "SAT". Jeśli komunikowana aplikacja karty inteligentnej to (U)SIM Application Toolkit [(U)SAT], wartość powinna być ciągiem "SAT". W przeciwnym razie wartość powinna być wartością AID. AID jest reprezentowany przez 5-16 bajtów heksadecymalnych, a każda wartość bajtu jest oddzielona znakiem ". ". Należy również pamiętać, że jeśli aplikacja karty inteligentnej jest (U)SAT, komunikacja musi odbywać się za pośrednictwem kanału 0.

Na przykład, poniższy kod spróbuje nawiązać połączenie z celem o identyfikatorze AID A0.0.0.67.4.7.1F.3.2C.3 z gniazda 0:

```
String url = "apdu:0;target=A0.0.0.67.4.7.1F.3.2C.3";
```

```
Połączenie APDUConection =  
(APDUConection)Connector.open(url);
```

Jeśli określony slot, karta lub aplikacja karty w określonym slacie nie istnieje, połączenie zgłosi wyjątek ConnectionNotFoundException.

Co więcej, dostępne sloty kart można zebrać za pomocą metody getProperty z parametrem "microedition.smartcardslots". Jeśli slot jest wymienialny na zimno, to "C", jeśli

gniazdo można wymieniać podczas pracy, wówczas do numeru gniazda dodawany jest symbol "H".

Metoda exchangeAPDU służy do wysyłania i odbierania komunikatów pomiędzy aplikacjami MIDP i smart card. Komunikaty są pobierane za pomocą tablicy bajtów. W poniższym przykładzie kodu tablica bajtów o nazwie apdu jest wysyłana do aplikacji karty, a odpowiedź jest zapisywana w tablicy bajtów odpowiedzi po jej otrzymaniu:

```
byte[] response = connection.exchangeAPDU(apdu);
```

(ii) *Opcjonalny pakiet SATSA-JCRMI*

Pakiet ten umożliwia komunikację z kartą inteligentną przy użyciu protokołu JavaCard Remote Method Invocation (JCRMI). Pozwala aplikacjom, które nie znajdują się na karcie inteligentnej, komunikować się z aplikacjami na karcie inteligentnej. Aby to osiągnąć, aplikacje używają odgałęzień do komunikacji ze zdalnymi obiektami na karcie inteligentnej. Stub może być postrzegany jako proxy dla zdalnego obiektu. Gdy aplikacja wywołuje metodę na odgałęzieniu, ta operacja wywołania jest przekazywana do karty inteligentnej, a wyniki są zwracane do aplikacji po wykonaniu wymaganych operacji na karcie inteligentnej.

Gniazda kart inteligentnych można wykryć w taki sam sposób, jak opisano w pakiecie SATSA- APDU. Połączenie w SATSA-JCRMI jest również zaimplementowane w podobny sposób. Ciąg połączenia JCRMI musi być sformatowany w następujący sposób:

```
JCRMI Connection String="jcrmi:" + slot_number + ";AID=" +  
AID Poniższy kod pokazuje przykład połączenia JCRMI:  
String url = "jcrmi:0;AID= A0.0.0.67.4.7.1F.3.2C.3";  
JavaCardRMIConection  
connection=(JavaCardRMIConection)Connector.open(url);  
Counter counter = (Counter) connection.getInitialReference();
```

Po skonfigurowaniu połączenia, za pomocą metody getInitialReference można pobrać obiekt skrótowy dla zdalnego odniesienia. Odniesienie to umożliwia aplikacji wywoływanie metod na zdalnym obiekcie poprzez wywołanie go na instancji.

(iii) *Opcjonalny pakiet SATSA-PKI*

Pakiet ten umożliwia aplikacjom zarządzanie podpisami cyfrowymi i certyfikatami. Aplikacje mogą podpisywać wiadomości kluczem prywatnym w celu spełnienia wymagań uwierzytelniania i niezaprzecalności. Aplikacja może również wykonywać żądania rejestracji certyfikatów oraz dodawać/usuwać certyfikaty do/z magazynu certyfikatów przy użyciu opcjonalnego pakietu SATSA-PKI.

(iv) *Opcjonalny pakiet SATSA-CRYPTO*

Pakiet ten umożliwia aplikacjom zarządzanie funkcjami kryptograficznymi. Obejmuje skróty wiadomości i podpisy cyfrowe w celu zapewnienia integralności danych, szyfry do szyfrowania i odszyfrowywania danych. Głównym celem tego

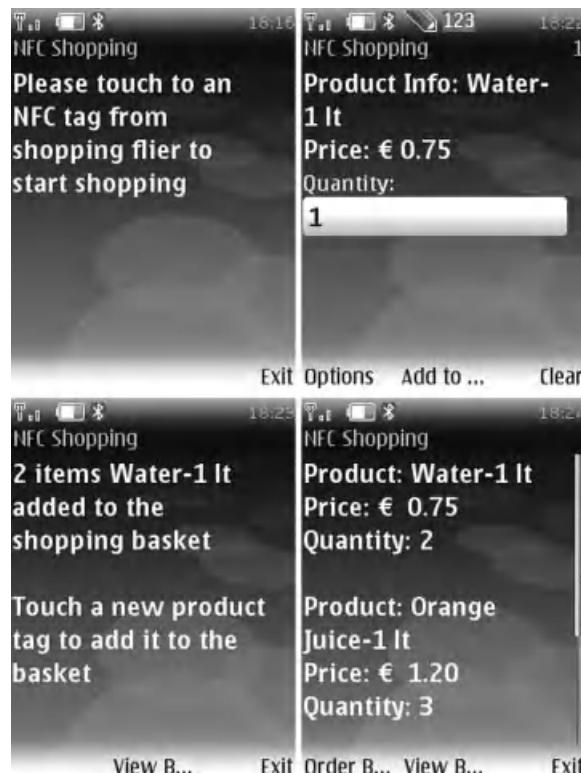
pakietu jest ochrona bezpieczeństwa i prywatności danych w aplikacji.

SE. Należy pamiętać, że pakiet SATSA-CRYPTO jest podzbiorem Java Cryptography Extension platformy J2SE.

5.9 Studium przypadku trybu czytnika/zapisu: Zakupy NFC

Pod koniec rozdziału 4 opisano i przedstawiono trzy przypadki użycia wraz z ich wymaganiami projektowymi i ogólnymi modelami użytkowania. W tej sekcji wdrażamy dwa pierwsze przypadki użycia. Środowisko ekosystemu i modele biznesowe trzeciego przypadku użycia są analizowane na końcu rozdziału 7.

Jak opisano w rozdziale 4, tryb czytnika/zapisu zapewnia wiele możliwości dla użytkowników i deweloperów. W tym trybie można zaimplementować wiele rzeczywistych scenariuszy. W tym przypadku zaimplementowaliśmy scenariusz zakupów online, aby pokazać NFC w akcji. Aplikacja nie zawiera skomplikowanych operacji, ponieważ naszym celem nie jest wprowadzenie zaawansowanych algorytmów programowania, a jedynie przedstawienie programowania NFC i idei stojącej za trybem pracy w rzeczywistym scenariuszu. Do celów produkcyjnych do aplikacji należy dodać wiele funkcji, takich jak łatwy w użyciu i dobrze wyglądający interfejs użytkownika, więcej funkcji zakupowych (usuwanie produktu, czytanie komentarzy o produkcie online itp.) oraz inne usługi dla klientów.



Rysunek 5.16 Ekrany MIDletu zakupów NFC.

Pamiętamy z przypadku użycia w rozdziale 4, że zakupy NFC zapewniają użytkownikom możliwość robienia zakupów poprzez wyeliminowanie ograniczeń geograficznych. Użytkownik dodaje produkty do koszyka po prostu dotykając telefonem tagów w katalogach zakupów obsługujących technologię NFC. Zrzuty ekranu aplikacji przedstawiono na rysunku 5.16.

Gdy użytkownik uruchomi aplikację, aplikacja czeka na rozpoczęcie interakcji NFC, jak widać na lewym górnym ekranie na rysunku 5.16. Gdy żądany tag zostanie wykryty w pobliżu, dane z tagu są przesyłane do telefonu komórkowego, a informacje o produkcie są wyświetlane użytkownikowi, a następnie żądana jest żądana ilość (prawy górny ekran na rysunku 5.16). Gdy użytkownik potwierdzi dodanie produktu do koszyka, produkt jest dodawany do koszyka, a użytkownikowi wyświetlany jest komunikat potwierdzający (lewy dolny ekran na rysunku 5.16). Kroki te są powtarzane, dopóki użytkownik nie zdecyduje się złożyć zamówienia w koszyku. Użytkownik może również wyświetlić aktualny koszyk, naciskając przycisk "Wyświetl koszyk" (prawy dolny ekran na rysunku 5.16).

(i) *Kod źródłowy aplikacji*

```
import java.io.IOException;
import java.util.Vector;
import javax.microedition.contactless.*;
import javax.microedition.contactless.ndef.*;
; import javax.microedition.io.Connector;
import javax.microedition.lcdui.*;
import javax.microedition.midlet.*;

public class ShoppingMain extends
    MIDlet implements Runnable,
    CommandListener, TargetListener {

    private NDEFTagConnection conn = null;

    private TargetProperties[] target;

    private Display screen;
    private Form mainForm, addProductForm;

    private StringItem screenText = new
        StringItem(null, "Dotknij tagu NFC z ulotki
zakupowej, aby rozpocząć zakupy");

    private String screenString, productinfo,
        productprice, productid;

    private int productquantity;
    private double totalbasketprice=0;

    private Vector basketprices = new Vector();
    private Vector basketinfo = new Vector();
    private Vector basketquantity = new Vector();
    private Vector basketids = new Vector();
```

```
private TextField quantityTextField;

private boolean ndefMessage=false;

private Command addToBasketCommand = new
    Command("Dodaj do koszyka", Command.SCREEN, 1);
private Command viewBasketCommand = new
    Command("View Basket", Command.SCREEN, 1);
private Command orderBasketCommand = new
    Command("Order Basket", Command.SCREEN, 1);
private Command cancelCommand = new
    Command("Anuluj", Command.CANCEL, 0);
private Command exitCommand = new
    Command("Exit", Command.EXIT, 0);

public ShoppingMain() {

    createMenu();

    DiscoveryManager dm = DiscoveryManager.
        getInstance();

    try {
        dm.addTargetListener(this,
            TargetType.NDEF_TAG);
    }catch (ContactlessException ce) {
        screenText.setText("Błąd podczas
            dodawania słuchaczy: " +
            ce.getMessage());
    }

}

protected void startApp() {

    screen = Display.getDisplay(this);
    screen.setCurrent(mainForm);
}

protected void pauseApp() {

}

protected void destroyApp(boolean unconditional)
{

    try {
        if (conn != null) {
            conn.close();
        }
    }catch (Exception e) {
```

```
        screenText.setText(" Błąd: " +
            e.getMessage());
    }

    notifyDestroyed();
}

public void commandAction(Command command,
    Displayable displayable) {

    String label = command.getLabel();

    if (label.equals("Exit")) {
        destroyApp(true);
    } else if (label.equals("Anuluj")) {
        screenText.setText("Dotknij urządzenia NFC
            tag z ulotki zakupowej, aby rozpocząć zakupy");
        screen.setCurrent(mainForm);
    } else if (label.equals("Dodaj do koszyka")) {
        addToBasket();
    } else if (label.equals("View Basket")) {
        viewBasket();
    } else if (label.equals("Koszyk zamówień")) {
        orderBasket();
    }
}

public void targetDetected(TargetProperties[] prop) {

    target = prop;

    Thread thread = new Thread(this);
    thread.start();
}

public void closeConnection(NDEFTagConnection conn){
    try {
        if (conn != null) {
            conn.close();
        }
    } catch (IOException e) {
    }
}

public void createMenu(){

    mainForm = new Form("Zakupy NFC");
    mainForm.append(screenText);
```

```
        mainForm.addCommand(exitCommand);
        mainForm.setCommandListener(this);
    }

    public void addToBasket(){

        mainForm.addCommand(viewBasketCommand);
        productquantity = Integer.parseInt(
            quantityTextField.getString());
        basketinfo.addElement(productinfo);
        basketprices.addElement(productprice);
        basketquantity.addElement(
            Integer.toString(productquantity));
        basketids.addElement(productid);
        totalbasketprice += productquantity *
            Double.parseDouble(productprice);
        screenText.setText(productquantity + " items "
            + productinfo + "dodano do koszyka" +
            "dotknij nowego tagu produktu, aby dodać
            go do koszyka");
        screen.setCurrent(mainForm);
    }

    public void addProduct(){

        quantityTextField = new TextField("Quantity:",
            "1", 2, TextField.NUMERIC);
        addProductForm = new Form("NFC Shopping");
        addProductForm.append("Informacje o produkcie: " +
            productinfo + "\nPrice: €      " + productprice);
        addProductForm.append(quantityTextField);
        addProductForm.addCommand(addToBasketCommand);
        addProductForm.addCommand(cancelCommand);
        addProductForm.addCommand(exitCommand);
        addProductForm.setCommandListener(this);
        screen.setCurrent(addProductForm);
    }

    public void viewBasket(){

        screenString = "";
        for(int i=0;i<basketprices.size();i++){
            screenString += "Product: " + (String)
                basketinfo.elementAt(i);
            screenString += "\nPrice: €      " + (String)
                basketprices.elementAt(i);
            screenString += "\nQuantity: " + (String)
                basketquantity.elementAt(i) + "\n\n";
        }
        screenString+="Cena całkowita: €" +
    }
```

```
totalbasketprice + "\n\nDotknij tagu nowego
produkту, aby dodać go do koszyka";
screenText.setText(screenString);
mainForm.addCommand(orderBasketCommand);
}

public void orderBasket(){

/*
 * wątek usługi sieciowej powinien zostać zaimplementowany
 * tutaj
 */
}

public void run() {

ndefMessage=false;
for (int i = 0; i <target.length; i++) {

if (target[i].hasTargetType
(TargetType.NDEF_TAG)) {

ndefMessage = true;
try {

String url = target[i].getUrl
(Class.forName("javax.microedition.
contactless.ndef.NDEFTagConnection"));
conn = (NDEFTagConnection)
Connector.open(url);
NDEFMessage message = conn.readNDEF();
if (message != null) {

NDEFRecord[] records =
message.getRecords();
productid = new
String(records[0].getPayload());
productinfo = new
String(records[1].getPayload());
productprice = new
String(records[2].getPayload());
addProduct();
} else {
screenText.setText("Nie ma żadnych
zapisanych komunikatów NDEF w
celu");
}
} catch (ContactlessException e) {
screenText.setText("Błąd: " +
e.getMessage());
} catch (IOException e) {
```

```
        screenText.setText("Błąd: " +
            e.getMessage());
    }catch (Exception e) {
        screenText.setText("Błąd: " +
            e.getMessage());
    }
} // koniec klauzuli if
} // koniec pętli for

if(!ndefMessage){screenText.setText("Target
type is not an
Znacznik w formacie NDEF");
}

closeConnection(conn);
} // koniec konstruktora wątku Read
} // koniec MIDletu
```

(ii) *Zrozumienie kodu*

Jak opisano w przykładzie trybu czytnika/zapisu, w konstruktorze tworzony jest nowy obiekt DiscoveryManager i konfigurowany jest docelowy nasłuch dla NDEF_TAG (dane sformatowane przez NFC Forum).

```
DiscoveryManager dm = DiscoveryManager.getInstance();
try {
    dm.addTargetListener(this, TargetType.NDEF_TAG);
}catch (ContactlessException ce) {
    screenText.setText("Błąd podczas dodawania nasłuchujących: " +
        ce.getMessage());
}
```

Gdy cel zostanie wykryty, jego właściwości zostaną zapisane w obiekcie TargetProperties.

```
public void targetDetected(TargetProperties[] prop) {
    target = prop;
    Thread thread = new Thread(this);
    thread.start();
}
```

Po wykryciu tagu NFC w pobliżu i przesłaniu rekordów z tagu do telefonu komórkowego, wywoływana jest metoda addProduct. Metoda ta wyświetla informacje o produkcie przesłane z tagu i prosi użytkownika o wprowadzenie żądanej ilości (prawy górny ekran na rysunku 5.16). Użytkownik może zarówno wprowadzić ilość, jak i potwierdzić dodanie produktu do koszyka, lub alternatywnie dotknąć innego tagu NFC, aby anulować operację.

```
public void addProduct(){
    quantityTextField = new TextField("Quantity:", "1", 2,
        TextField.NUMERIC);
    addProductForm = new Form("NFC Shopping");
```

```

    addProductForm.append("Informacje o produkcie: " + productinfo +
        "\nPrice: €      " + productprice);
    addProductForm.append(quantityTextField);
    addProductForm.addCommand(addToBasketCommand);
    addProductForm.addCommand(cancelCommand);
    addProductForm.addCommand(exitCommand);
    addProductForm.setCommandListerner(this);
    screen.setCurrent(addProductForm);
}

```

Metoda `addToBasket` dodaje produkt do koszyka, co jest potwierdzane przez metodę `addProduct`.

```

public void addToBasket(){
    mainForm.addCommand(viewBasketCommand);
    productquantity =
    Integer.parseInt(quantityTextField.getString());
    basketinfo.addElement(productinfo);
    basketprices.addElement(productprice);
    basketquantity.addElement(Integer.toString(productquantity));
    basketids.addElement(productid);
    totalbasketprice += productquantity*
        Double.parseDouble(productprice);
    screenText.setText(productquantity + " items " + productinfo +
        " dodany do koszyka" + "\n\nDotknij tagu nowego
produktu
        aby dodać go do koszyka");
    screen.setCurrent(mainForm);
}

```

W celu przechowywania informacji o produktach dodawanych do koszyka, w aplikacji tworzone są cztery wektory:

- `basketPrices`: aby zachować cenę jednostkową każdego produktu;
- `basketInfo`: przechowywanie informacji o każdym produkcie;
- `basketQuantities`: aby zachować zamówioną ilość każdego produktu;
- `basketIds`: aby zachować identyfikację każdego produktu.

Wektory te, z wyjątkiem `basketIds`, są używane do wyświetlania użytkownikowi informacji o koszyku. Identyfikatory koszyka są potrzebne tylko do wysłania identyfikacji produktów w koszyku do systemu zaplecza supermarketu. Ponadto ilość każdego produktu jest wyświetlana użytkownikowi i wysyłana do supermarketu. Ponadto zmienna całkowita, `totalBasketPrice`, przechowuje całkowitą cenę koszyka.

Metoda `viewBasket` służy do wyświetlania bieżących produktów w koszyku wraz z ich informacjami, ceną jednostkową i ilością, jak widać na prawym dolnym ekranie na rysunku 5.16. Łączna cena produktów w bieżącym koszyku jest wyświetlana użytkownikowi. Użytkownik może zamówić koszyk za pomocą polecenia "Zamów koszyk" lub może nadal dodawać inne produkty do koszyka, dotykając znacznika nowego produktu.

```

public void viewBasket(){
    screenString = "";

```

```
for(int i=0; i<basketPrices.size(); i++){
    screenString += "Product: " +
    (String)basketInfo.elementAt(i);
    screenString += "\nPrice: €      "
    +
    (String)basketPrices.elementAt(i);
    screenString += "\nQuantity: " +
    (String)basketQuantities.elementAt(i) + "\n\n";
}
screenString += "Cena całkowita: €      " + totalBasketPrice +
    "Dotknij nowego tagu produktu, aby dodać go do koszyka";
screenText.setText(screenString);
mainForm.addCommand(orderBasketCommand);
}
```

Metoda `run` rozpoczyna się, gdy wątek jest uruchamiany w bieżącym MIDlecie. Jest to główna część wykonawcza programu NFC. Po prostu nawiązuje połączenie z celem za pomocą `NDEFTagConnection`. Połączenie zostało już opisane w sekcji 5.6.5, więc tutaj opiszemy je tylko pokrótko.

```
public void run() {
    ...
}
```

Po nawiązaniu połączenia wiadomość NDEF w tagu jest odczytywana, a wszystkie rekordy w wiadomości są zapisywane w tablicy `rekordów`. Następnie identyfikator produktu, informacje o produkcie i cena produktu są zapisywane w odpowiednich zmiennych. Należy pamiętać, że dane w tagu są uporządkowane w tej samej kolejności. Pierwszy rekord odpowiada identyfikacji produktu, drugi rekord odpowiada informacjom o produkcie, a trzeci rekord odpowiada cenie produktu. Ostatnią rzeczą do zrobienia jest wywołanie metody `addProduct` w celu dodania powiązanych produktów do koszyka.

Kod usługi sieciowej w tym przypadku pozostaje niezaimplementowany dla uproszczenia. Chcemy jeszcze raz podkreślić, że celem tej sekcji jest pokazanie NFC w akcji, a nie wdrożenie produktu przemysłowego.

5.10 Studium przypadku trybu peer-to-peer: NFC Gossiping

W tej aplikacji zaimplementowano przypadek plotkowania NFC opisany pod koniec rozdziału 4. Przypomnijmy, że przypadek plotkowania NFC umożliwia użytkownikom tworzenie nowych plotek lub otrzymywanie ich od znajomych. Użytkownik po prostu dotyka swojego urządzenia mobilnego do urządzenia mobilnego znajomego, aby wymienić (wysłać lub odebrać) plotkę. Zrzuty ekranu aplikacji przedstawiono na rysunku 5.17.

Gdy użytkownik uruchamia aplikację po raz pierwszy, wyświetlane jest menu główne z dwiema opcjami: "Udostępnij plotkę" i "Utwórz nową plotkę", jak widać na lewym górnym ekranie na rysunku 5.17. Gdy użytkownik chce utworzyć nową plotkę, wyświetlane jest pole tekstowe (prawy górny ekran na rysunku 5.17). Użytkownik może zapisać plotkę lub anulować i powrócić do ekranu głównego. Gdy użytkownik wejdzie do menu "Udostępnij plotkę" z ekranu głównego, wszystkie zapisane plotki zostaną wyświetlone na ekranie. Użytkownik może udostępnić jedną z nich, naciskając przycisk "Udostępnij" (ekran w lewym dolnym i prawym dolnym rogu).



Rysunek 5.17 Ekrany MIDletów plotkujących NFC.

Gdy zdalne urządzenie otrzyma plotkę, może ją zapisać. Nie możemy podać tych ekranów tutaj, ponieważ emulator nie może zarządzać komunikacją peer-to-peer. Dlatego też operacje te mogą być wykonywane tylko na prawdziwym telefonie komórkowym.

(i) *Kod źródłowy aplikacji*

```
import java.io.IOException;
import javax.microedition.io.Connector;
import javax.microedition.lcdui.*;
import javax.microedition.midlet.*;
import javax.microedition.rms.*;
import com.nokia.nfc.llcp.*;

public class NFCGossiping extends MIDlet
    implements CommandListener,
    LLCPConnectionListener, LLCPLinkListener {

    // Obiekt LLCPManager
    private LLCPManager llcpManager;
```

```
// Obiekty połączenia LLCP
private LLCPConnection inConnection;
private LLCPConnection outConnection;

/*
 * identyfikator usługi, który ma być używany w
 * ciąg połączenia
 */
private static final byte SID=11;

/*
 * typ transportu, który ma być używany w
 * ciąg połączenia
 */
private static final byte
TYPE=LLCPConnection.TYPE_2;

/*
 * łańcuch uid przechowujący ciąg szesnastkowy
 * identyfikatora UID zdalnego urządzenia LLCP i będzie
 * może być użyty w łańcuchu połączenia
 */
private String uid = "";

/*
 *isReading jest używany przez urządzenie, które
 *jest w stanie odczytu. Odpowiada on następującym ciągiem znaków
 *w celu powiadomienia urządzenia wysyłającego
 */
private String isReading = "-1";

private StringItem screenText = new
StringItem(null,"");

/*
 *tablice bajtów przechowujące przesyłane plotki
 *i otrzymywane plotki
 */
private byte[] sendData = null,
receiveData = null;

/*
 * określa, czy aplikacja jest w trybie odczytu lub
 * stan zapisu
 */
private boolean readState=true;

// magazyn rekordów używany do przechowywania
plotek private RecordStore rs = null;
```

```
// ciąg znaków, który będzie używany dla magazynu
rekordów private static final String
RECORD_STORE = "GOSSIPSS";

private Display screen;
private Form mainForm = null;
private List mainList = null, gossipList = null;
private TextBox newGossipTextBox = null;

private Command saveIncomingGossipCommand=new
    Command("Store Gossip", Command.SCREEN, 1);
private Polecenie saveGossipCommand = new
    Command("Save Gossip", Command.SCREEN, 1);
private Command shareGossipCommand = new
    Command("Share Gossip", Command.SCREEN, 1);
private Command mainMenuCommand = new
    Command("Main Menu", Command.SCREEN, 1);
private Command cancelCommand = new
    Command("Anuluj", Command.CANCEL, 0);
private Command exitCommand = new
    Command("Exit", Command.EXIT, 0);

public NFCGossiping() throws IOException {

    /*
     *ta funkcja (zaimplementowana poniżej) tworzy
     * formularz i listą, która będzie używana w
     * interfejsy użytkownika
     */
    createMenu();
    screen = Display.getDisplay(this);

    // słuchacze dodani dla obiektu LLCPManager
    llcpManager = LLCPManager.getInstance();
    llcpManager.addLinkListener(this);
    llcpManager.startListening(TYPE, SID, this);
}

protected void startApp() throws
    MIDletStateChangeException {

    displayMainMenu();
    /*
     *ta funkcja (zaimplementowana poniżej) jest wywoływana
     *podczas uruchamiania i wyświetla mainList użytkownikowi
     */
}

protected void pauseApp() {
```

```
}

protected void destroyApp(boolean unconditional) {

    /*
     *gdy aplikacja zostanie zniszczona, llcpmanager
     *przystaje nasłuchiwać i połączenia są zamykane
     */
    llcpManager.stopListening(TYPE, SID, this);
    llcpManager.removeLinkListener(this);
    closeLCPConnection(inConnection);
    closeLCPConnection(outConnection);
    inConnection = null;
    outConnection = null;
    notifyDestroyed();
}

public void commandAction(Command command,
    Displayable displayable) {

    String label = command.getLabel();
    if (label.equals("Exit")) {
        destroyApp(true);
    }else if(label.equals("Save Gossip")) {
        saveGossip();
    }else if (label.equals("Anuluj")) {
        displayMainMenu();
    }else if (label.equals("Store Gossip")) {
        createNewGossip(new String(receiveData));
    }else if (label.equals("Menu główne")) {
        displayMainMenu();
    }else {
        Lista down = (Lista)screen.getCurrent();
        if(screen.getCurrent() == gossipList)
            sendMessage(getGossip(down.
                getSelectedIndex())+1));
    }else{
        switch(down.getSelectedIndex()) {
            case 0:
                processGossips();
                break;

            case 1:
                createNewGossip("");
                break;
        }
    }
}
```

```
public void displayMainMenu(){  
  
    screen.setCurrent(mainList);  
}  
  
// formularz i lista są tworzone do późniejszego  
użycia public void createMenu(){  
  
    mainForm = new Form("NFC Gossiping");  
    mainForm.append(screenText);  
    mainForm.addCommand(mainMenuCommand);  
    mainForm.addCommand(exitCommand);  
    mainForm.setCommandListener(this);  
  
    mainList = new List("NFC Gossiping",  
        Choice.IMPLICIT);  
    mainList.append("Udostępnij plotkę", null);  
    mainList.append("Utwórz nową plotkę", null);  
    mainList.addCommand(exitCommand);  
    mainList.setCommandListener(this);  
}  
  
/*  
 * wyświetla pole tekstowe do wpisania nowej plotki.  
 * Służy również do edytowania i zapisywania przychodzących  
 * wiadomości.  
 * gossip przy użyciu parametru String newgossip  
 */  
public void createNewGossip(String newgossip) {  
  
    newGossipTextBox = new TextBox("Tekst do  
        napisania", newgossip, 255,  
        TextField.ANY);  
    newGossipTextBox.addCommand  
        (saveGossipCommand);  
  
    newGossipTextBox.addCommand(cancelCommand);  
    newGossipTextBox.setCommandListener(this);  
    screen.setCurrent(newGossipTextBox);  
}  
  
public String getGossip(int index) {  
  
    String gossip="";  
    openRecordStore();  
    try{  
  
        byte[] recData = new  
            byte[rs.getRecordSize(index)];  
        int len = rs.getRecord(index, recData, 0);  
        gossip= new String(recData, 0, len);  
    }  
}
```

```
        catch (wyjątek e){
            e.printStackTrace();
        }
        closeRecordStore();
        return gossip;
    }

/*
 *Wyświetla listę wszystkich rekordów w RecordStore.
 *Dodaje opcję udostępniania, aby udostępnić plotkę z listy
 */
public void processGossips() {

    openRecordStore();
    try{
        gossipList = new List("Gossips",
            Choice.IMPLICIT);
        for (int i=1; i <= rs.getNumRecords(); i++){
            byte[] recData = new
                byte[rs.getRecordSize(i)];
            int len = rs.getRecord(i, recData, 0);
            gossipList.append(new String(recData, 0,
                len), null);
        }
    }
    catch (wyjątek e){
        e.printStackTrace();
    }
    gossipList.setSelectCommand
        (shareGossipCommand);
    gossipList.addCommand(mainMenuCommand);
    gossipList.addCommand(exitCommand);
    gossipList.setCommandListener(this);
    screen.setCurrent(gossipList);
    closeRecordStore();
}

/*
 *Pobiera plotkę z pola tekstowego, które jest
 * utworzony w metodzie createNewGossip i zapisuje
 * do sklepu z płytami.
 */
public void saveGossip(){

    openRecordStore();
    byte[] record = newGossipTextBox.
        getString().getBytes();
    try{
        rs.addRecord(record, 0, record.length);
    }
}
```

```
        catch (wyjątek e){
            e.printStackTrace();
        }
        closeRecordStore();
        screenText.setText("Plotka została
zapisana: " +
                newGossipTextBox.getString());
        screen.setCurrent(mainForm);
    }

    // otwiera połączenie z RecordStore
    public void openRecordStore(){
        try{
            rs = RecordStore.openRecordStore
                (RECORD_STORE, true );
        }
        catch (wyjątek e){
            e.printStackTrace();
        }
    }

    // zamyka połączenie z RecordStore
    public void closeRecordStore(){
        try{
            rs.closeRecordStore();
        }

        catch (wyjątek e){
            e.printStackTrace();
        }
    }

    /*
     *ta metoda zapisuje plotkę do bajtu sendData
     *która ma zostać udostępniona. To również
     *zmienia readState na false w celu
     *wysłać wiadomość. Zostanie utworzony nowy alert
     *ostrzeżenie użytkownika przed dotknięciem zdalnego urządzenia
     */
    public void sendMessage(String gossip) {

        readState = false;
        sendData = gossip.getBytes();

        Alert sendAlert = new Alert("Sending
Gossip...", "Please Touch", null,
        AlertType.INFO);
        sendAlert.addCommand(cancelCommand);
        sendAlert.setTimeout(10000);
        sendAlert.setCommandListener(this);
        screen.setCurrent(sendAlert);
```

```
}

/*
*gdy urządzenie pomyślnie wyśle wiadomość,
* wywołuje tę metodę, aby zmienić swój stan na
* readState
*/
public void readMessage() {

    sendData = null;
    receiveData = null;
    readState = true;
}

/*
*Ta metoda jest wywoływana, gdy łącze jest
*z urządzeniem zdalnym.
*Należy pamiętać, że urządzenie nie jest w stanie odczytu
*/

public void linkEstablished(String uid) {

    receiveData = null;
    this.uid=uid;

    ProcessSend sendThread = new ProcessSend();
    new Thread(sendThread).start();
}

/*
*jest wywoływana, gdy połączenie zostanie utracone z
*urządzeniem zdalne
*/
public void linkLost() {

    closeLLCPConnection(outConnection);
    closeLLCPConnection(inConnection);
    outConnection = null;
    inConnection = null;
}

/*
*ta metoda jest wywoływana, gdy połączenie jest
*otwarte za pomocą urządzenia zdalonego. Należy pamiętać, że
*urządzenie jest w stanie odczytu
*/

public void connectionOpened(LLCPConnection
    connection) {
```

```
if (inConnection == null) {  
    inConnection = connection;  
    ProcessReceive receiveThread = new  
        ProcessReceive();  
    new Thread(receiveThread).start();  
} else  
    closeLLCPConnection(connection);  
}  
  
// metoda zamykająca połączenie LLCPConnection  
public void  
closeLLCPConnection(LLCPConnection  
connection) {  
  
    if (connection != null) {  
        try {  
            connection.close();  
        } catch (IOException e) {  
            screenText.setText("Błąd zamykania  
połączenia : " + e.getMessage());  
        }  
    }  
}  
  
/*  
 * gdy połączenie zostało otwarte za pomocą  
 * urządzenie inicjujące, urządzenie w odczycie  
 * state wywołuje tę metodę, wysyłając komunikat "isReading"  
 * (-1) do urządzenia zapisującego i czeka  
 * dla rzeczywistych danych przychodzących.  
 */  
  
public class ProcessReceive implements Runnable {  
  
    public void run() {  
        try {  
            if(readState) {  
  
                inConnection.send(isReading.getBytes());  
                byte[] data = inConnection.receive();  
                processReceivedData(data);  
            }  
        }  
        catch (wyjątek e) {  
            screenText.setText("Błąd obsługi połączenia  
przychodzącego:" + e.getMessage());  
        }  
    }  
}
```

```
*po odebraniu danych z urządzenia zdalnego,
*jest przetwarzany w tej metodzie. Jeśli urządzenie
*jest w stanie odczytu, drukuje plotkę do
*ekran. Jeśli urządzenie nie jest w stanie odczytu,
*(oznacza to, że urządzenie odbiera "-1"
*z urządzenia zdalnego), wówczas wiadomość jest wysyłana
*/
private synchronized void
processReceivedData(byte[] data) {

    if(receiveData == null) {
        receiveData = data;
    } else
        powrót;

    if(readState) {
        if(!new String(receiveData).
           equals(isReading)) {
            screenText.setText("Otrzymano plotkę: "
                + new String(receiveData) + "\n");
            mainForm.addCommand
                (saveIncomingGossipCommand);
            screen.setCurrent(mainForm);
        }
    } else {
        if(sendData != null) {
            screenText.setText("Plotka została
                pomyślnie wysłana");
            screen.setCurrent(mainForm);
            readMessage();
        }
    }
}

/*
*po ustanowieniu połączenia ze zdalnym
*urządzenie, program wywołuje tę metodę. To
*otwiera połączenie ze zdalnym
*i wysyła dane plotki.
*/
public class ProcessSend implements Runnable {

    public void run() {
        try {
            outConnection = (LLCPConnection)
                Connector.open("nfc:llcp?type=" + TYPE
                    + ";sid=" + SID + ";uid=" +
                    uid); if(!readState) {
```

```
        outConnection.send(sendData);
        byte[] data = outConnection.receive();
        if(new String(data).equals(isReading))
            processReceivedData(data);
    }
}
catch (IOException e) {
    screenText.setText("Błąd obsługi
        połączenia wychodzącego : " +
        e.getMessage());
}
}
```

(ii) *W wyjaśnieniu kodu*

Szczegóły aplikacji są teraz opisane. Aplikacja wykorzystuje RecordStore do przechowywania plotek w urządzeniu mobilnym, jednak tylko część NFC zostanie tutaj szczegółowo opisana. Interfejsy API RecordStore i ich opisy można znaleźć na powiązanych stronach pod adresem <http://java.sun.com/>.

Poniższy kod, w części konstruktora, tworzy nową instancję menedżera LLCP. Następnie dodawany jest słuchacz łączca, który będzie powiadamiany o zdarzeniach związanych z łączem LLCP oraz słuchacz, który rozpoczęcie nasłuchiwanie połączeń. Aby rozpocząć nasłuchiwanie połączeń, jako parametry należy podać typ transportu połączenia i identyfikator usługi. *TYPE* i *SID* są zdefiniowane jako zmienne statyczne. Należy pamiętać, że istnieja dwa możliwe typy transportu w komunikacji LLCP.

```
llcpManager = LLCPManager.getInstance();
llcpManager.addLinkListener(this);
llcpManager.startListening(TYPE, SID, this);
```

Interakcja NFC rozpoczyna się, gdy użytkownik wybierze jedną z istniejących plotek do udostępnienia. W takim przypadku urządzenie mobilne wchodzi w stan zapisu, co oznacza, że to ono wyśle plotkę. Z drugiej strony, interakcja NFC może być również rozpoczęta przez zdalne urządzenie. W tym przypadku urządzenie jest w stanie odczytu i to ono będzie odbierać plotki.

5.10.1.1 Pisanie plotek

Gdy użytkownik chce udostępnić plotkę, wywoływana jest metoda sendMessage z parametrem string. Parametr ten składa się z treści plotki, która zostanie udostępniona. Udostępniona plotka jest uzyskiwana przy użyciu wartości indeksu listy plotek, która jest używana do uzyskania dostępu do magazynu rekordów. Wartość indeksu listy plotek jest wysyłana do metody getGossip, a ta zwraca odpowiednią plotką z magazynu rekordów. W metodzie sendMessage wartość readState urządzenia jest ustawiana na false, a zawartość plotki jest zapisywana w tablicy bajtów sendData, jak pokazano w poniższym kodzie.

```
readState = false;  
sendData = gossip.getBytes();
```

Następnie urządzenie rozpoczyna oczekивание на nawiązanie połączenia z urządzeniem zdalnym. Po nawiązaniu połączenia automatycznie wywoływana jest metoda linkEstablished. W tej metodzie tablica bajtów receiveData jest ustawiana na wartość null, aby wyczyścić poprzednie plotki, jeśli takie istnieją. Ponadto identyfikator uid zdalnego urządzenia LLCP jest zapisywany w łańcuchu uid, który będzie używany podczas połączenia. Następnie uruchamiany jest nowy wątek w celu wymiany wiadomości, jak pokazano w poniższym kodzie.

```
receiveData = null;
this.uid = uid;
ProcessSend sendThread = new ProcessSend();
new Thread(sendThread).start();
```

W klasie ProcessSend otwierane jest nowe połączenie LLCP z ciągami TYPE, SID i uid. Ponieważ stan odczytu urządzenia jest fałszywy, wysyła ono tablicę bajtów sendData do urządzenia zdalnego i czeka na wiadomość przychodząą. Po nadejściu wiadomości ze zdalnego urządzenia sprawdza, czy otrzymane dane są równe ciągowi isReading. Należy pamiętać, że ciąg ten jest początkowo ustawiony na "-1". Jeśli odebrane dane są równe "-1", wywołuje metodę processReceivedData, jak pokazano w poniższym kodzie.

```
outConnection = (LLCPConnection)
Connector.open("nfc:llcp;type="
+
    TYPE + ";sid=" + SID + ";uid=" + uid);
if(!readState) {
    outConnection.send(sendData);
    byte[] data = outConnection.receive();
    if(new String(data).equals(isReading))
        processReceivedData(data);
}
```

Gdy wywoływana jest metoda processReceivedData, ponieważ urządzenie jest w stanie zapisu, uruchamia ona inną część kodu i ustawia tekst bieżącego ekranu. Wywołuje również metodę readMessage w celu przejścia do stanu odczytu.

```
if(readState) {
    ...
} else {
    if(sendData != null) {
        screenText.setText("Plotka została pomyślnie wysłana");
        screen.setCurrent(mainForm);
        readMessage();
    }
}
```

5.10.1.2 Czytanie plotek

Gdy użytkownik chce uzyskać plotkę, urządzenie zdalne powinno być w stanie zapisu, a użytkownik powinien dotknąć swojego urządzenia mobilnego do urządzenia zdalnego. Gdy tak się stanie, metoda connecOpened jest wywoływana automatycznie przez urządzenie czytające (urządzenie, które jest w stanie odczytu).

state). W tej metodzie tworzony jest nowy wątek z klasy `ProcessReceive`, jak pokazano w poniższym kodzie.

```
if (inConnection == null) {
    inConnection = connection;
    ProcessReceive receiveThread = new ProcessReceive();
    new Thread(receiveThread).start();
} else
    closeLLCPConnection(connection);
```

Klasa `ProcessReceive` zapisuje przychodząca wiadomość w tablicy bajtów i wysyła "-1" do urządzenia zdalnego. Aby obsłużyć zapisaną wiadomość przychodzącą, wysyła tablicę bajtów do metody `processReceivedData`.

```
inConnection.send(isReading.getBytes());
byte[] data = inConnection.receive();
processReceivedData(data);
```

Ponieważ urządzenie jest w stanie odczytu, uruchamia część kodu `if`. W tej części po prostu zapisuje przychodząca wiadomość na ekranie. Dodaje również polecenie, które umożliwia użytkownikowi zapisanie przychodzącej plotki, jak widać w poniższym kodzie.

```
if(readState) {
    if(!new String(receiveData).equals(isReading)) {
        screenText.setText("Otrzymano plotkę: " + new String(receiveData)
            + "\n");
        mainForm.addCommand(saveIncomingGossipCommand);
        screen.setCurrent(mainForm);
    }
} else {
    ...
}
```

Gdy użytkownik naciśnie polecenie zapisu, aplikacja wywołuje metodę `createNewGossip`. Aplikacja wyświetla również otrzymaną wiadomość w polu tekstowym, aby użytkownik mógł ją edytować przed zapisaniem.

Jak opisano wcześniej, aplikacja ta umożliwia cyfrową usługę plotkowania, dzięki czemu ludzie mogą rozpowszechniać plotki peer-to-peer. Może tworzyć, przechowywać i udostępniać plotki. Należy zauważyć, że zaawansowana implementacja nie jest tutaj omawiana, ponieważ idea tych przypadków użycia jest pokazanie NFC w akcji, a nie wdrażanie aplikacji użytkownika końcowego.

5.11 Podsumowanie rozdziału

W tym rozdziale opisano rozwój aplikacji NFC. Ponieważ Java jest powszechnie używana i dobrze znana, uważałyśmy, że poznanie rozwoju aplikacji nowej technologii za pomocą interfejsów API Java pomoże czytelnikom lepiej ją zrozumieć.

Użyliśmy Eclipse IDE jako podstawy do programowania mobilnego. Seria 40 Nokia 6212 NFC SDK jest również używana do tworzenia aplikacji NFC i środowiska testowego. Nokia 6212 NFC SDK jest kompatybilny z Eclipse IDE oraz platformą Netbeans. Istnieją jednak

Tabela 5.17 Przegląd interfejsów API JSR 257

Pakiet	Opis Interfejsy	, klasy, wyjątki
javax.microedition.contactless	Zapewnia wspólne funkcje dla wszystkich celów zbliżeniowych, takie jak wykrywanie celu	TagConnection Interface TargetListener Interface TargetProperties Interface TransactionListener Interface DiscoveryManager Class TargetType Class ContactlessException
javax.microedition.contactless.ndef	Zapewnia funkcjonalność dla wymiana danych sformatowanych przez NFC Forum z tagami RFID	NDEFRecordListener Interface NDEFTagConnection Interface NDEFMessage Class NDEFRecord Class NDEFRecordType Class PlainTagConnection Interface
javax.microedition.contactless.rf	Umożliwia komunikację z Tagi RFID zawierające dane niesformatowane przez NFC Forum	ISO14443Interface połączenia
javax.microedition.contactless.sc	Umożliwia komunikację z Karty inteligentne ISO14443-4	

również inne środowiska programistyczne NFC. Dla urządzeń z systemem Android dostępne jest Android SDK, a dla urządzeń z systemem Symbian 3, Qt Connectivity API zapewnia obsługę programowania NFC. Istnieją również inne środowiska programistyczne.

Najpierw przedstawiono wprowadzenie do J2ME, aby czytelnicy mogli zdobyć podstawową wiedzę na temat programowania aplikacji mobilnych. Następnie opisano tworzenie aplikacji NFC za pomocą dwóch pakietów Java (JSR 257 i JSR 177 API). JSR 257 umożliwia głównie programowanie w trybie czytnika / zapisu; jednak niektóre klasy w pakiecie są również używane do uzyskiwania dostępu do SE. Pakiety związane z NFC w JSR 257 API są podsumowane w tabeli 5.17.

Dzięki temu interfejsowi API aplikacja może otrzymywać powiadomienia o wykryciu celów w pobliżu i może nawiązać połączenie z konkretnym celem. Pakiet javax.microedition.contactless zawiera wspólne klasy i interfejsy, które mogą być używane wraz ze wszystkimi typami celów. Pakiet ten musi być zawarty we wszystkich aplikacjach, które implementują JSR 257. Oprócz tego pakietu należy użyć drugiego pakietu w oparciu o typ docelowy. Pakiet javax.microedition.contactless.ndef umożliwia urządzeniom mobilnym wymianę danych w formacie NDEF z bezstykowymi urządzeniami docelowymi. Pakiet javax.microedition.

Pakiet .contactless.rf może być używany do celów RFID, które nie zawierają danych w formacie NFC Forum. Wreszcie, pakiet javax.microedition.contactless.sc zapewnia interfejs ISO14443Connection do uzyskiwania dostępu do celów bezstykowych kart inteligentnych zgodnych z ISO 14443-4.

Aby nasłuchiwać aktywności na SE przy użyciu JSR 257, aplikacje muszą zaimplementować interfejs TransactionListener, a także zarejestrować detektor transakcji za pomocą metody addTransactionListener klasy

DiscoveryManager. Metoda externalReaderDetected jest wywoływana automatycznie w celu powiadomienia aplikacji o wystąpieniu zdarzenia na SE.

Z drugiej strony, JSR 177 API zapewnia komunikację z SE. Tryb emulacji karty została opracowany głównie dla aplikacji, które implementują wysokie ograniczenia bezpieczeństwa. Ten interfejs API umożliwia również operacje bezpieczeństwa, zapewniając certyfikaty cyfrowe, podpisy cyfrowe i operacje kryptograficzne. Komunikacja kart intelligentnych z tym API może być zaimplementowana przy użyciu protokołu APDU lub protokołu JavaCard RMI.

Do programowania w trybie peer-to-peer nie są dostarczane standardowe interfejsy API, więc należy używać własnych pakietów. Te własne pakiety można znaleźć w rozszerzeniach API Nokia 6212 JSR 257. LLCP i NFCIP-1 są objęte programowaniem w trybie peer-to-peer.

Na końcu rozdziału zaimplementowano dwa przypadki użycia, aby pokazać NFC w akcji i zilustrować tryby pracy w rzeczywistym scenariuszu.

Pytania do rozdziału

1. Jakie rodzaje aplikacji są potrzebne dla NFC?
2. Jakiego rodzaju aplikacje są wymagane dla każdego trybu pracy?
3. Jakie elementy składają się na platformę Java?
4. Definiowanie oprogramowania do zarządzania aplikacjami.
5. Opisz stany MIDletu i metody, które obsługują zmiany stanu. Które z tych metod muszą być zaimplementowane w MIDletie?
6. Który pakiet umożliwia MIDletowi implementację interfejsów użytkownika?
7. Jakie pliki są zawarte w pakiecie MIDlet?
8. Jakie atrybuty muszą być zawarte w plikach manifestów JAD i JAR?
9. Definiowanie rejestru push. Jak MIDlet może zarejestrować rekord push?
10. Podaj przykład statycznego wpisu rejestru push.
11. Wymień JSR opracowane dla programowania NFC.
12. Jakie typy celów są obsługiwane w interfejsie API komunikacji zbliżeniowej?
13. Podaj procesy aplikacji działającej w trybie czytnika/zapisu, która odczytuje dane z tagu NFC.
14. W jaki sposób aplikacja w trybie czytnika/zapisu wykrywa cel i jak otrzymuje powiadomienie za pomocą interfejsu API JSR 257?
15. Co oznacza typ docelowy NDEF_TAG?
16. Których pakietów z JSR 257 można użyć do zaimplementowania aplikacji działającej w trybie czytnika/zapisu, która komunikuje się z typem docelowym NDEF_TAG?
17. Która klasa reprezentuje wiadomość NDEF w JSR 257?
18. Wymień formaty nazw typów rekordów i zdefiniuj trzy z nich.
19. Jak można używać rejestru push w trybie czytnika/zapisu?
20. Podaj przykład wpisu połączenia rejestru push, który umożliwia uruchomienie aplikacji po wykryciu znacznika.
21. Które protokoły mogą implementować aplikację w trybie peer-to-peer?
22. Podaj przykłady ciągów połączeń NFCIP i LLCP.
23. Opisz komunikację dwóch urządzeń w połączeniu NFCIP.
24. Opisz komunikację dwóch urządzeń w połączeniu LLCP.
25. Jakie są sposoby uzyskiwania dostępu do SE za pomocą aplikacji?
26. Jakie podstawowe funkcje zapewnia JSR 177?
27. Podaj przykłady ciągów połączeń APDU i JCRMI.

Referencje

- [1] Android SDK, <http://developer.android.com/sdk/> (dostęp: 10 lipca 2011 r.).
- [2] Qt SDK, <http://qt.nokia.com/> (dostęp: 10 lipca 2011 r.).
- [3] Java Platform, Standard Edition (Java SE), <http://www.oracle.com/technetwork/java/javase/> (dostęp: 10 lipca 2011 r.).
- [4] Java Platform, Enterprise Edition (Java EE), <http://www.oracle.com/technetwork/java/javaee/> (dostęp: 10 lipca 2011 r.).
- [5] Java Platform, Micro Edition (Java ME), <http://www.oracle.com/technetwork/java/javame/> (dostęp: 10 lipca 2011 r.).
- [6] Java Community Process (JCP), <http://jcp.org/> (dostęp: 10 lipca 2011 r.).
- [7] Java Specification Requests (JSR), <http://www.jcp.org/en/jsr/> (dostęp: 10 lipca 2011 r.).
- [8] Seria 40 Nokia 6212 NFC SDK, http://www.developer.nokia.com/info/sw.nokia.com/id/5bcae40-d2b2-4595-b5b5-4833d6a4cda1/S40_Nokia_6212_NFC_SDK.html (dostęp 10 lipca 2011).
- [9] Społeczność open source Fundacji Eclipse, <http://www.eclipse.org/> (dostęp: 10 lipca 2011 r.).
- [10] Eclipse, <http://eclipseme.org/> (dostęp: 10 lipca 2011 r.).
- [11] Mobile Information Device Profile (MIDP); JSR 118, <http://java.sun.com/products/midp/> (dostęp: 10 lipca 2011 r.).
- [12] JSR 257: Contactless Communication API, <http://www.jcp.org/en/jsr/detail?id=257> (dostęp: 10 lipca 2011 r.).
- [13] JSR 177: Security and Trust Services API for J2METM, <http://jcp.org/en/jsr/detail?id=177> (dostęp: 10 lipca 2011 r.).
- [14] Nokia 6212 Classic JSR-257 Implementation, można znaleźć w Series 40 Nokia 6212 NFC SDK, http://www.developer.nokia.com/info/sw.nokia.com/id/5bcae40-d2b2-4595-b5b5-4833d6a4cda1/S40_Nokia_6212_NFC_SDK.html (dostęp 10 lipca 2011 r.).

6

Bezpieczeństwo i prywatność NFC

Chociaż telefon komórkowy jest prawie identyczny z komputerem osobistym (PC) pod względem technicznym, różni się tym, że jest bardziej osobistym przedmiotem i jest noszony przez ludzi przez cały czas. Użytkownicy zazwyczaj uważają, że ich telefony komórkowe są ważną częścią ich życia i zazwyczaj mają je pod fizycznym nadzorem. Jednak nasz telefon komórkowy jest zawsze narażony na ataki fizyczne, takie jak kradzież, oraz techniczne ataki bezprzewodowe przy użyciu technologii komunikacyjnych Bluetooth lub Wi-Fi. Zintegrowana funkcja NFC nakłada również pewne dodatkowe zagrożenia na telefony komórkowe.

Niniejszy rozdział zawiera szczegółowe informacje dotyczące bezpieczeństwa i prywatności w technologii NFC. Rozpoczynamy od wprowadzenia ogólnych informacji i definicji dotyczących bezpieczeństwa, jego zasad, narzędzi i mechanizmów, a następnie kontynuujemy, określając szczegóły dotyczące bezpieczeństwa NFC, kwestii prywatności, problemów i ich rozwiązań. Biorąc pod uwagę, że czytelnik może nie mieć szczegółowej wiedzy na ten temat, staramy się w szczególności przekazać wiedzę wprowadzającą na temat bezpieczeństwa i prywatności.

6.1 Bezpieczeństwo w Ogólne

Bezpieczeństwo to stopień ochrony przed celowym lub przypadkowym niewłaściwym użyciem lub działaniem. Jeśli złośliwe działanie w jakiś sposób wykorzystuje słabość, może spowodować uszkodzenie systemu. Złośliwe działanie może być wywołane przez przeciwnika, którego celem może być uzyskanie pewnych korzyści, utrudnienie prawidłowego funkcjonowania atakowanego systemu lub spowodowanie nieprawidłowego działania systemu lub wycieku niektórych informacji.

Bezpieczny dostęp do systemu wymaga zastosowania podstawowych procesów uwierzytelniania, autoryzacji i niezaprzecjalności. Uwierzytelnianie zapewnia, że osoba, która próbuje uzyskać dostęp do systemu, jest naprawdę tym, za kogo się podaje. Na przykład w przypadku klienta próbującego uzyskać dostęp do konta za pomocą strony internetowej banku, uwierzytelnianie jest procesem potwierdzania tożsamości klienta.

Uwierzytelnianie zasadniczo weryfikuje - lub unieważnia - deklarowaną tożsamość użytkownika. Autoryzacja to zezwolenie na wykonanie określonego zestawu działań przez uwierzytelnionego użytkownika.

W związku z tym uwierzytelniony użytkownik może wykonać dowolną czynność z zestawu dozwolonych działań, ale nie może wykonać żadnego działania, na które nie ma pozwolenia.

Niezaprzecjalność jest silniejszą wersją uwierzytelniania. Biorąc pod uwagę poprzedni przykład banku, serwer internetowy może uwierzytelić klienta przy użyciu hasła, które jest znane tylko przez

Komunikacja bliskiego zasięgu: Od teorii do praktyki, wydanie pierwsze. Vedat Coskun, Kerem Ok i Busra Ozdenizci.

© 2012 John Wiley & Sons, Ltd. Opublikowano 2012 przez John Wiley & Sons, Ltd.

użytkownika i serwera. Serwer WWW nie może jednak udowodnić tożsamości użytkownika, chyba że dane uwierzytelniające są znane tylko użytkownikowi. Rozróżnienie między uwierzytelnianiem a niezaprzecjalnością zostanie wyjaśnione w dalszej części tego rozdziału.

Bezpieczeństwo zajmuje się głównie takimi kwestiami, jak poufność (tajność) jako ochrona danych przed nieautoryzowanymi użytkownikami i wykorzystaniem, integralność jako ochrona danych przed modyfikacją przez nieautoryzowanych użytkowników oraz dostępność, aby umożliwić dostęp autoryzowanym użytkownikom w dowolnym czasie i warunkach.

Poufność polega na zachowaniu dostępu do treści danych tylko dla upoważnionych użytkowników i w autoryzowany sposób. Istnieją dwie podkategorie poufności, a mianowicie tajemnica i prywatność. Poufność zapewnia, że prywatne informacje nie są dostępne, nie są udostępniane ani ujawniane nieautoryzowanemu użytkownikowi. Po tym, jak autoryzowany użytkownik uzyska dostęp do tajnych danych, prywatność zapewnia, że dane nie zostaną wykorzystane w niezamierzonym celu przez właściciela. Prywatność pośrednio ogranicza późniejszy transfer danych przez autoryzowanego użytkownika do nieautoryzowanego użytkownika. Tajemnica dotyczy dostępu do danych tylko przez upoważnione osoby, podczas gdy prywatność dotyczy niewłaściwego wykorzystania danych przez upoważnionych użytkowników. Tajemnica umożliwia dostęp do danych tylko uwierzytelnionym osobom. Prywatność polega na umożliwieniu wykorzystania danych zgodnie z przeznaczeniem dopiero po uzyskaniu dostępu do danych przez uwierzytelnionego użytkownika, zapobiegając w ten sposób wykorzystaniu danych do niezamierzonych celów.

Integralność to pewność, że dane nie zostały zmodyfikowane lub usunięte przez nieautoryzowanego użytkownika lub w niezamierzony sposób. Mówiąc o danych na jakimś urządzeniu pamięci masowej, integralność może zostać naruszona zarówno przez problemy techniczne, jak i w wyniku złośliwego lub przypadkowego działania. Wiedząc, że problemy techniczne nie stanowią problemu dla bezpieczeństwa, złośliwe lub przypadkowe działania wszystkich użytkowników muszą być odpowiednio traktowane. Integralność danych przesyłanych między nadawcą a odbiorcą w Internecie również podlega temu samemu problemowi. Dane mogą ulec uszkodzeniu podczas przesyłania, przez co wysłane i odebrane wiadomości mogą się nie zgadzać lub wysłana wiadomość może nawet nie dotrzeć do odbiorcy. Gdy przyczyną problemu jest jakaś złośliwa aktywność, mechanizmy bezpieczeństwa są odpowiedzialne za radzenie sobie z tym problemem.

W oparciu o opisane koncepcje bezpieczeństwa, zapewnienie bezpieczeństwa w przypadku NFC jest krytyczne, ponieważ NFC jest najczęściej wykorzystywane do celów płatności i sprzedaży biletów.

6.1.1 Dlaczego bezpieczeństwo jest ważne?

Gdy użytkownik chce skorzystać z usługi, takiej jak narzędzie do zarządzania informacjami, jego głównym celem jest uwolnienie się od problemów związanych z korzystaniem z usługi. Kolejną motywacją może być uzyskanie jak największej wydajności. Funkcjonalność i wydajność razem stanowią sumę nabytej usługi.

Dwa negatywne parametry, które potencjalnie mogą wpływać na poziom wykorzystania usług, to braki techniczne i problemy związane z bezpieczeństwem. Różnica między bezpieczeństwem a niedociągnięciami technicznymi polega na tym, że bezpieczeństwo uwzględnia działania ludzi i inteligentnych maszyn próbujących spowodować zniszczenie, podczas gdy problemy techniczne nie są wywoływanie przez problemy z bezpieczeństwem.

Bezpieczeństwo stało się ważną kwestią w ostatniej dekadzie z następujących powodów:

- Z punktu widzenia hakera istnieje teraz więcej możliwości finansowych. Haker może zarabiać na złośliwych działaniach.
- Z technicznego punktu widzenia:

- Liczba użytkowników Internetu rośnie wykładniczo; dlatego też media do złośliwych działań stają się wygodniejsze. Jeden haker może wypróbować tę samą metodę, aby zhakować wiele potencjalnych ofiar.
- Trudno jest osadzić środki bezpieczeństwa w nowych aplikacjach ze względu na wysoki poziom rozwoju.
koszty w obszarze IT i rosnące zapotrzebowanie na nowe aplikacje. Ponadto zaprojektowanie reszty aplikacji jest znacznie łatwiejsze niż wbudowanie funkcji bezpieczeństwa. Wynika to z faktu, że projektowanie wbudowanej architektury bezpieczeństwa wymaga więcej czasu i pieniędzy.
- Z punktu widzenia dewelopera, potencjalni nabywcy cenią sobie funkcjonalność, więcej niż bezpieczeństwo. Chociaż zauważenie funkcji bezpieczeństwa wymaga specjalistycznej wiedzy, użytkownicy z łatwością zauważają inne funkcje, takie jak interfejs użytkownika.

Bezpieczeństwo jest również ważną kwestią w ekosystemie NFC. Główne powody można wymienić jako:

- NFC to popularna technologia zintegrowana z telefonami komórkowymi.
- Każdy posiada telefon komórkowy, a ludzie martwią się o rzeczy związane z nimi samymi.
- NFC jest mocno promowane przez dostawców usług.
- NFC potencjalnie ma duży rynek finansowy, co jest wymagającym powodem dla hakerów.

6.1.2 Główne cele środków bezpieczeństwa

Każdy system ma swoje własne wymagania dotyczące bezpieczeństwa. Niektóre wymagają, aby informacje były dostępne tylko dla jednej lub więcej osób, podczas gdy inne wymagają zachowania niezmienionej zawartości przez nielegalne strony. W tej sekcji przedstawimy ważne wymagania bezpieczeństwa, które są stosowane w prawie wszystkich systemach. Nie wszystkie systemy wymagają wszystkich środków bezpieczeństwa. Niektóre wymagają jedynie uwierzytelniania, podczas gdy inne wymagają integralności. Najpierw wymienimy wszystkie środki i użyjemy ich definicji w dalszych podrozdziałach.

6.1.2.1 Tajność/poufność

Tajność to zapewnienie, że informacje są dostępne tylko dla upoważnionej strony (osoby, procesu lub urządzenia). Tajność wymaga ukrycia treści informacji, tradycyjnie poprzez szyfrowanie, tak aby tylko upoważnione strony mogły uzyskać do niej dostęp za pomocą tajnego klucza.

6.1.2.2 Uwierzytelnianie

Uwierzytelnianie to potwierdzanie tożsamości osoby, procesu lub urządzenia. Uwierzytelnianie można przeprowadzić na kilka sposobów. Załóżmy na przykład, że zaprosiłeś przyjaciela na posiłek, ale nie chcesz zepsuć sobie wieczoru, otwierając drzwi komuś innemu, gdy ktoś do nich zapuka. Z tego powodu możesz uzgodnić metodę pukania do drzwi, tak aby twój przyjaciel zapukał do twoich drzwi na przykład trzy razy. W związku z tym informacje, które wymieniłeś ze swoim przyjacielem, są kluczem, którego nikt inny nie zna. Ponieważ ty i twój przyjaciel jesteście jedyną parą osób znających tajne informacje do uwierzytelniania, będziesz mieć pewność, czy osoba pukająca do twoich drzwi jest twoim

szłyfr symetryczny, który zostanie opisany w sekcji 6.2; tajne informacje są znane obu partnerom i nikomu innemu.

(i) *Uwierzytelnianie oznacza*

Do uwierzytelnienia można użyć wielu metod, takich jak żądanie hasła, dotknięcie karty identyfikacyjnej RFID do czytnika kart RFID, przyciśnięcie palców do skanera, gdzie odcisk palca jest sprawdzany z bazy danych, lub przyłożenie pisma ręcznego do tego samego skanera. Różne sposoby uwierzytelniania można sklasyfikować w następujący sposób:

- Coś, co zna: hasło.
- Coś, co posiada: karta inteligentna, token OTP, klucz fizyczny lub słuchawka NFC.
- Coś, czym jest: fizjologiczne/statyczne dane biometryczne, takie jak odcisk palca, głos, siatkówka oka lub tęczówka oka.
- Coś, co robi: biometria behawioralna/dynamiczna, taka jak pismo odreżne, pisanie na klawiaturze lub rytm chodzenia.

(ii) *Obecne schematy uwierzytelniania*

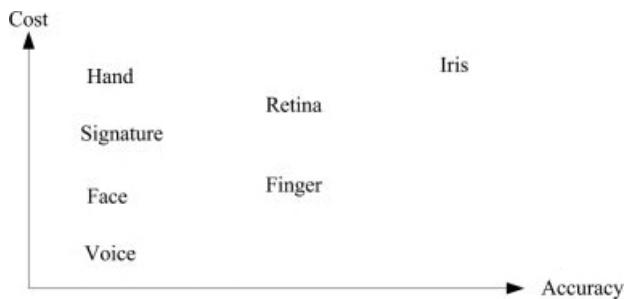
Zawsze toczy się walka między hakerami a dostawcami zabezpieczeń. Celem dostawców zabezpieczeń jest stworzenie mechanizmów bezpieczeństwa, które zapewnią wysoki stopień ochrony i wystarczający poziom funkcjonalności w tym samym czasie; celem hakerów jest ominięcie tych mechanizmów.

Mogą istnieć kompromisy między różnymi mechanizmami bezpieczeństwa. Na przykład podpis cyfrowy jest obecnie najsilniejszym sposobem uwierzytelniania, ale korzystanie z podpisu cyfrowego jest bardziej kosztowne niż hasło jednorazowe. Banki nie nalegają, a jedynie wspierają użycie podpisu cyfrowego; nalegają jednak na użycie hasła jednorazowego. Poniżej przedstawiono obecnie używane przez banki opcje uwierzytelniania:

- *Jednorazowe hasło przez SMS*: Serwer banku wysyła hasło na zarejestrowany wcześniej telefon komórkowy. Użytkownik otrzymuje hasło za pomocą telefonu komórkowego i wpisuje je na stronie internetowej. W związku z tym zakłada się, że bieżący użytkownik jest faktycznie zamierzonym użytkownikiem.
- *Token generujący hasło jednorazowe*: Użytkownik wywołuje token otrzymany wcześniej od banku w celu wygenerowania hasła jednorazowego i wpisuje je na stronie internetowej. W związku z tym zakłada się, że bieżący użytkownik jest faktycznie zamierzonym użytkownikiem.
- *Oprogramowanie do generowania haseł jednorazowych*: Przypadek jest podobny do poprzedniego, z tą różnicą, że aplikacja generatora haseł jednorazowych jest instalowana i wywoływana na telefonie komórkowym zamiast tokena.
- *Podpis mobilny*: Użytkownik otrzymuje podpis cyfrowy od zaufanego urzędu certyfikacji, dzięki czemu może podpisać każdą transakcję, której zażąda. Podpis mobilny zapewnia również mechanizmy bezpieczeństwa inne niż uwierzytelnianie.

(iii) *Uwierzytelnianie biometryczne*

System biometryczny uwierzytelnia użytkownika na podstawie cech fizycznych (biometrycznych). Metryki mogą obejmować cechy statyczne, takie jak siatkówka oka, odcisk palca lub cechy dynamiczne, takie jak wzór głosu. Zakłada się, że użycie skanera siatkówki oka lub analizatora odcisków palców zapewnia wyższy poziom bezpieczeństwa niż użycie hasła. Jednak bezpieczne hasło, które jest wystarczająco długie i złożone oraz często aktualizowane, zapewnia wystarczające bezpieczeństwo. W porównaniu ze schematami opartymi na kryptografii, metody biometryczne nie są jeszcze wystarczająco dojrzałe i nadal są zbyt kosztowne. Niektóre z powodów, dla których drogie mechanizmy są nadal rozwijane, są następujące:



Rysunek 6.1 Względny koszt i dokładność systemu biometrycznego.

- Trudno jest zaufać użytkownikowi, ponieważ może on wprowadzić pewne istotne dane podczas tworzenia hasła, modyfikując jedynie, na przykład, datę urodzenia.
 - Trudno jest zaufać użytkownikowi, nawet jeśli jego hasło jest złożone, ponieważ prawdopodobieństwo, że użytkownik zapisze gdzieś hasło, jest bardzo wysokie.
 - Zasada wielowarstwości dyktuje, że powinniśmy wstawiać różne mechanizmy sprawdzania bezpieczeństwa w różnych punktach. Hasło biometryczne jest czym innym niż zwykłe hasło, a sprawdzanie informacji biometrycznych w jednym punkcie kontrolnym po haśle we wcześniejszym punkcie zapewnia lepsze bezpieczeństwo niż dwa mechanizmy sprawdzania hasła.
 - Wraz ze wzrostem możliwości obliczeniowych hakerzy będą w stanie złamać złożone hasła w ciągu zaledwie kilku sekund, które użytkownik może obsłużyć w swoim mózgu. Dlatego dobrze jest mieć zamiennik na ten przyszły czas.
 - Wraz ze wzrostem wykorzystania haseł biometrycznych, badania nad poprawą ich skuteczności będą się nasilać i staną się one bardziej skuteczne.
- System biometryczny może opierać się zarówno na właściwościach statycznych, jak i dynamicznych. Niektóre przykłady metodologii statycznej to cechy twarzy, odcisk palca, DNA, geometria dłoni, tęczówka i wzór siatkówki. Niektóre przykłady metodologii dynamicznej to rytm pisania, głos i podpis. Rysunek 6.1 przedstawia względny koszt i dokładność systemu biometrycznego.

(iv) *Jak działają systemy biometryczne?*

Rozważmy fotografię. Staromodne, klasyczne aparaty analogowe wykorzystywały analogowe klisze fotograficzne i przechowywały dokładne informacje. Następnie pojawiła się fotografia cyfrowa. Nie wszystkie aparaty cyfrowe mają jednak taką samą rozdzielcość. Rozważmy trzy aparaty cyfrowe z 1, 2 i 3 megapikselami. Gdy każdy z nich jest używany do nagrywania tej samej klatki, używają różnych rozmiarów plików ze względu na różną rozdzielcość, którą obsługują. Nawet jeśli nagrywają ten sam obszar, rozmiar pliku i zawartość, którą wygenerują, będą się różnić. W związku z tym nie przechowują one rzeczywistych informacji, ale ich reprezentację. Ich zakres kolorów również może być inny. Jeśli używają 16-, 24- i 32-bitowych schematów kolorów, przechowują różne informacje o kolorze dla każdego bitu. W związku z tym reprezentacja rzeczywistego piksela na świecie będzie inna dla każdej kamery. Porównując trzy pliki z trzema zdjęciami wykonanymi przez różne kamery, trudno jest zdecydować, czy zrobione zdjęcia reprezentują tę samą rzeczywistą klatkę, czy nie.

System biometryczny działa podobnie. Informacje biometryczne przechowywane w fazie rejestracji są w rzeczywistości cyfrową reprezentacją rzeczywistych danych, takich jak informacje o tęczówce, geometrii dłoni lub odcisku palca. Oczywiście sposób reprezentacji rzeczywistych danych wpływa na współczynnik powodzenia ogólnych algorytmów. Dlatego też różne proponowane algorytmy mają różne współczynniki sukcesu. System najpierw przechowuje cyfrową reprezentację rzeczywistych danych (faza rejestracji) w bazie danych, a następnie cyfrowa reprezentacja bieżącego użytkownika jest porównywana z przechowywanymi danymi (faza weryfikacji) w bazie danych. Kroki te są analogiczne do mechanizmu uwierzytelniania opartego na hasłach. Różnica polega na tym, że w uwierzytelnianiu opartym na haście nie ma różnic między prawdziwym hasłem a jego reprezentacją, ponieważ proces jest wykonywany natychmiast przy użyciu symboli. Jednak w systemie biometrycznym mogą występować nawet różnice między różnymi zapisami tych samych informacji, takich jak informacje o geometrii tej samej ręki ze względu na zmianę kąta i warunków oświetleniowych lub pewne różnice w algorytmie. W związku z tym podobieństwo jest określane za pomocą pewnego progu; jeśli podobieństwo jest powyżej pewnego wskaźnika, użytkownik jest uwierzytelniany, w przeciwnym razie użytkownik jest odrzucany.

6.1.2.3 Wzajemne uwierzytelnianie

Uwierzytelnianie spełnia tylko zapewnienie jednej strony dla strony uwierzytelniającej. Rozważmy stronę internetową, która żąda od użytkownika identyfikacji i hasła w celu umożliwienia dalszej funkcjonalności. Gdy użytkownik wprowadzi te informacje, serwer uwierzytelni się, ale użytkownik nie będzie w stanie zrozumieć, czy strona internetowa należy do rzeczywistego serwera bankowego, czy komputera hakera, który imituje aplikację serwera bankowego. W rezultacie użytkownik nie może być pewien, czy tajne informacje zostały wysłane na serwer banku, czy też na stronę hakerską. Problem ten można rozwiązać za pomocą techniki wzajemnego uwierzytelniania, w której obie strony uwierzytelniają się nawzajem. W przypadku, gdy istnieje możliwość phishingu, wzajemne uwierzytelnianie jest niezbędne.

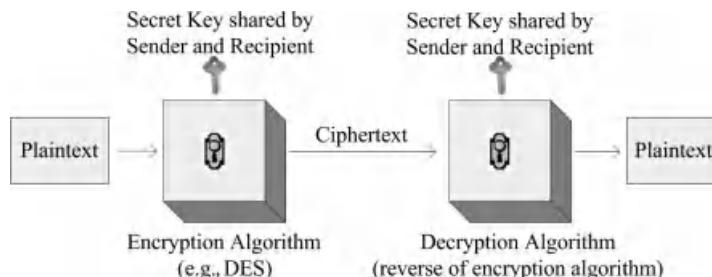
6.1.2.4 Autoryzacja

Po uwierzytelnieniu, autoryzacja pozwala na różne działania na obiekcie (pliku, aplikacji lub maszynie) przez podmiot (użytkownika). Na przykład profesor musi zostać uwierzytelniony przed wykonaniem jakichkolwiek operacji wstawiania, aktualizacji lub usuwania ocen studentów. Każdy student jest uprawniony do przeglądania swoich ocen. Natomiast ocena żadnego studenta nie jest widoczna dla żadnego innego studenta. Podobnie, jeden profesor może być w stanie pracować nad ocenami swoich kursów, ale nie innych. Prawa autoryzacji mogą się nawet różnić w zależności od warunków, takich jak czas. Na przykład, profesor może nie być w stanie modyfikować ocen po określonym czasie, takim jak koniec semestru.

6.1.2.5 Niezaprzeczalność

Niezaprzeczalność jest silniejszym wymogiem niż uwierzytelnianie. Uwierzytelnianie opiera się na pewnych tajnych informacjach, kluczu lub haśmie (patrz rysunek 6.2). Gdy jeden z partnerów korzysta z tajnych informacji, kontrahent będzie w stanie uwierzytelić drugiego. Jednym z ograniczeń uwierzytelniania jest to, że żadna ze stron nie może udowodnić, że

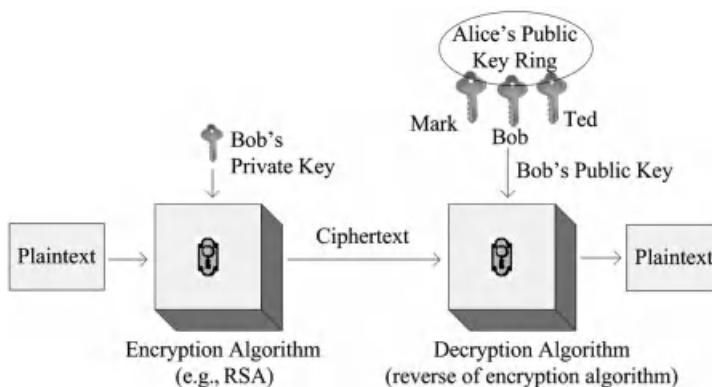
~~Przykrość NEC~~
konfidenca jest osobą trzecią, co jest możliwe tylko dzięki technikom niezaprzeczalności.
Zapewnienie niezaprzeczalności jest trudniejsze. A



Rysunek 6.2 Schemat uwierzytelniania.

Tajny klucz współdzielony przez parę partnerów nie jest wystarczający, ponieważ strona trzecia nie może być pewna, która strona użyła klucza. Jednym z dodatkowych wymogów niezaprzeczalności jest to, że strona trzecia, innymi słowy arbiter, musi znać klucz lub pewne ważne informacje na jego temat (patrz rysunek 6.3).

Rozważmy przykład. Bank posiada stronę internetową, która wymaga od użytkowników wprowadzenia hasła. W tym przypadku hasło użytkownika jest znane zarówno bankowi, jak i użytkownikowi. Gdy użytkownik zostanie poproszony o wprowadzenie hasła i wprowadzi je poprawnie, bank potwierdzi jego hasło. Założymy, że użytkownik zlecił przelew pieniężny za pomocą strony internetowej, a przelew jest wykonywany przez serwer internetowy banku. Bank jest pewien, że użytkownik zlecił przelew, ponieważ tylko on i bank znają hasło. Jednak bank nie może tego udowodnić, ponieważ sam również zna klucz. Pracownik banku, który ma dostęp do hasła, mógł użyć klucza. W związku z tym wymagany jest zupełnie inny rodzaj projektu klucza, generowania, zarządzania i systemu użytkowania. Tylko użytkownik powinien znać klucz. Jedyną rzeczą, którą może zrobić zarówno bank, jak i sędzia, jest weryfikacja klucza. Wymagany jest tutaj klucz asymetryczny, współczesny lub publiczny. W kryptografii symetrycznej tylko użytkownik posiada klucz prywatny. Sędzia posiada klucz publiczny, który może być użyty do weryfikacji użycia klucza prywatnego. Właściciel klucza publicznego (bank i sędzia) nie może uzyskać dostępu do konta bez użycia klucza prywatnego. Tak więc, gdy użytkownik wykonał przelew pieniężny w tym przypadku, nie może zaprzeczyć operacji.



Rysunek 6.3 Schemat niezaprzeczalności.

Tabela 6.1 Miary czasu przestoju

% Dostępność	9s	Przestój
90.0000	1	36.5 d
99.0000	2	3.65 d
99.9000	3	8.76 h
99.9900	4	52 min
99.9990	5	5 min
99.9999	6	31 s

6.1.2.6 Dostępność

Dostępność polega na zapewnieniu, że system reaguje poprawnie i całkowicie na żądania autoryzowanego użytkownika w danym momencie. W sensie technicznym dostępność to stosunek czasu, w którym system działa zgodnie z oczekiwaniami, do całkowitego czasu. Rozważmy system, który jest używany przez 1 godzinę dziennie; miałyby on dostępność 23/24. Typowe wartości dostępności są określane w postaci dziesiętnej (np. 0,9583). Aby wyrazić dostępność aplikacji, używana jest metryka znana jako dziewiątki. Dziewiątki odpowiadają liczbie dziewiątek w wartości procentowej dostępności. Na przykład "cztery dziewiątki" odpowiadają dostępności 0,9999 (lub 99,99%) (patrz Tabela 6.1). Czas przestoju to kolejna notacja, która pokazuje okres niedostępności systemu w notacji dziewiątek.

$$A = MTBF/(MTBF + MTTR)$$

MTBF = średni czas między awariami

MTTR = średni czas naprawy

6.1.2.7 Integralność danych

Integralność to pewność, że otrzymane informacje są dokładnie takie same jak wysłane. Oznacza to, że informacje nie zostały przypadkowo lub złośliwie zmodyfikowane lub usunięte podczas jakiejkolwiek operacji, takiej jak przechowywanie lub przesyłanie. Dane posiadające integralność są identyczne z oryginałem.

6.1.2.8 Odpowiedzialność

Wykonane działania związane z bezpieczeństwem muszą być w stanie prześledzić wstecz do inicjatora, gdy jest to wymagane przez oficera bezpieczeństwa lub aplikację. Odpowiedzialność faktycznie wiąże się z innymi wymaganiami, takimi jak niezaprzecalność i rejestrowanie aktywności.

6.1.3 Podatność, zagrożenie, atak i ryzyko

6.1.3.1 Podatność

Podatność to słaby punkt zabezpieczeń, który może zostać wykorzystany przez atakującego. Na przykład, system może być podatny na nieautoryzowaną manipulację danymi, ponieważ nie weryfikuje

Parameters	Availability	Confidentiality	Integrity
Hardware	Not available when the hardware or its components are stolen or broken		
Software	Not available when the software is modified or deleted so that it cannot function at all	Confidentiality is violated when software is modified to help hackers	Functions improperly generate unexpected results when the software is modified
Data	Not available when the data are modified or deleted	Confidentiality is violated when data are read by unauthorized parties	False data results in inappropriate results when existing data are modified, deleted or even fake data are generated
Packages	Not available when the packages are modified or deleted on the way to the receiver	Confidentiality is violated when packages are read by unauthorized parties	False data results in inappropriate results when a package content is a modified, deleted or even a fake package is generated

Rysunek 6.4 Analiza zagrożeń.

tożsamości użytkownika przed zezwoleniem na dostęp. Słabym punktem może być błąd projektowy, błąd implementacji lub wada jakiejś procedury.

Podatność to połączenie trzech elementów: wady systemu, możliwości dostępu atakującego w celu wykorzystania wady oraz możliwości atakującego do wykorzystania wady. Jeśli w systemie istnieje luka, atakujący może zainicjować atak w celu jej wykorzystania. Ryzyko jest więc (możliwą) szkodą.

6.1.3.2 Zagrożenie

Potencjalne niebezpieczeństwo, które może przynieść nieuczciwą korzyść nieupoważnionym osobom lub wyrządzić szkodę poprzez wykorzystanie słabości, nazywane jest zagrożeniem. Zagrożenia mogą być zamierzone lub niezamierzone. Zamierzone zagrożenia mają na celu celowe uzyskanie nieuczciwych korzyści lub wyrządzenie szkody; niezamierzone zagrożenia zazwyczaj występują przypadkowo i nie mają na celu celowego wyrządzenia szkody. Przykładami zagrożeń niezamierzonych są błędy ludzkie, takie jak błędy projektowe oprogramowania, sprzętu i wprowadzania danych oraz błędy techniczne, takie jak awarie systemu komputerowego i pożary. Zagrożenia, które niszczą dostępność, poufność i integralność, zostały skategoryzowane na rysunku 6.4.

6.1.3.3 Atak

Atak to celowa próba odczytania, zmodyfikowania, usunięcia, wyłączenia lub uzyskania nieautoryzowanego dostępu do informacji przez intruzów. Atak można sklasyfikować jako aktywny lub pasywny. Działania

Próby odczytania informacji bez wpływu na zasoby systemu nazywane są atakami pasywnymi, podczas gdy działania zmieniające zasoby systemu nazywane są atakami aktywnymi.

Ataki pasywne są wymierzone w poufność, a typowe przykłady to ukryty kanał, analiza przepływu ruchu, rekonesans, podsłuchiwanie pakietów, podsłuchiwanie, backdoor i rejestrowanie kluczy. Wykrycie ataku pasywnego jest bardzo trudne, ponieważ podczas ataku dane nie ulegają zmianie. Szyfrowanie jest oczywistym wyborem, aby zapobiec atakom pasywnym. W przypadku ataków pasywnych nacisk kładziony jest na zapobieganie, bez wykrywania.

Aktywne ataki są wymierzone w integralność, a typowe przykłady to maskarada, innymi słowy spoofing, atak Denial of Service (DoS), rozproszony atak DoS (DDoS), atak z odbiciem, atak wzmacniający, atak Man in the Middle (MIM), atak replay, modyfikacja wiadomości i atak salami. Ataki mogą być inicjowane przez osobę z wewnętrz, która jest autoryzowanym użytkownikiem i może uzyskać dostęp do zasobów systemowych. Jednak po uzyskaniu dostępu do danych wykorzystuje je w sposób niezatwierdzony przez osoby, które udzielili autoryzacji. Atak może być również zainicjowany przez osobę z zewnątrz, która jest osobą nieupoważnioną lub nielegalną.

Istnieją różne rodzaje ataków. Te rodzaje ataków są opracowywane przez hakerów równolegle z technologią. Niektóre z głównych ataków są następujące:

(i) *Podsłuchiwanie*

Podsłuchiwanie, innymi słowy sniffing, jest aktem nieautoryzowanego tajnego przechwytywania prywatnej komunikacji w czasie rzeczywistym. Termin podsłuch wywodzi się z praktyki słuchania rozmowy w fizycznym sąsiedztwie.

(ii) *Inżynieria społeczna*

Inżynieria społeczna polega na manipulowaniu ludźmi; haker jest nieautoryzowany i próbuje uzyskać informacje. Niektóre techniki polegają na oszukiwaniu, podczas gdy inne obejmują ostre metody, takie jak grożenie użytkownikowi.

(iii) *Phishing*

Phishing to proces polegający na próbie zdobycia informacji, takich jak nazwy użytkownika lub hasła, poprzez maskaradę. Phishing zazwyczaj wykorzystuje wiadomości e-mail lub komunikatory internetowe i często przekonuje użytkowników do wprowadzenia danych osobowych, takich jak hasło do fałszywej strony internetowej. Phishing można również sklasyfikować jako przykład techniki inżynierii społecznej.

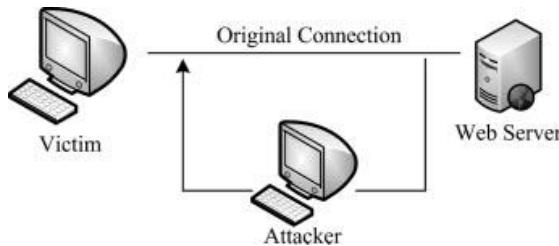
(iv) *Wyciek*

Wyciek, innymi słowy ukryty kanał, polega na zbieraniu niewielkiej ilości danych z każdego pakietu, a następnie łączeniu tych drobnych fragmentów w dłuższą serię. Następnie zebrane dane mogą zostać wykorzystane przez intrusa do pewnych celów, które są sprzeczne z poufnością. Na przykład, weźmy pod uwagę MNO, który przyznaje punkty bonusowe w oparciu o ilość rozmów, które mogą być następnie wykorzystane do uzyskania darmowych przedmiotów ze sklepu. Twój znajomy jest klientem tego OSK i pozwala ci wykorzystać punkty bonusowe z jej telefonu komórkowego, a także podaje twoje imię i nazwisko oraz inne informacje OSK. Od tego momentu możesz zdobywać i wykorzystywać punkty bonusowe za każdą minutę spędzoną przez Twoją znajomą na telefonie komórkowym. Po każdej miesięcznej fakturze na kwotę X euro znajomy otrzymuje X punktów bonusowych. Problemem w tym przypadku jest wyciek informacji, ponieważ otrzymując punkty bonusowe i fakturę od znajomego, otrzymujesz informacje o jego okresie rozmów.

(v) *Atak MIM*

Stojąc pomiędzy dwoma legalnymi użytkownikami systemu, atakujący może

odebrać pakiet od nadawcy (patrz rysunek 6.5). Następnie ~~zasięga~~ przekazuje go odbiorcy i wykorzystuje uzyskane informacje. Założymy, że rozmawiają ze sobą dwie kobiety. Kiedy



Rysunek 6.5 Atak typu "man in the middle".

Jeśli rozmawiają twarzą w twarz, oboje są pewni swojej tożsamości. Jeśli wstawimy inne medium komunikacyjne do czatowania, takie jak linia telefoniczna, dane mowy są ewentualnie konwertowane do formatu cyfrowego i przenoszone przez niektóre serwery pośredniczące. W takim przypadku możliwe jest, że strona trzecia odbiera dane z serwera nadawcy i wysyła je do serwera odbiorcy, a oba serwery mogą być nieświadome serwera pośredniczącego. Ten scenariusz jest w rzeczywistości studium przypadku dobrze znanego algorytmu, zwanego atakiem MIM. Opracowano nowe mechanizmy zapobiegania atakom MIM; jednak ulepszone mechanizmy ataku są następnie generowane przez hakerów.

(vi) *Atak powtórkowy*

Atak typu replay ma miejsce, gdy prawidłowa transmisja danych jest złośliwie powtarzana po wystąpieniu pierwotnej transmisji. Jest to przeprowadzane albo przez inicjatora, albo przez przeciwnika, który przechwytuje dane i przesyła je ponownie. Przykładem niebezpiecznego ataku typu replay jest transakcja przelewu pieniędzy między dwoma kontami.

(vii) *Atak przekaźnikowy*

Atak przekaźnikowy polega na przekazaniu wiadomości, która ma zostać wymieniona między nadawcą a odbiorcą. Jest on powiązany z atakami MIM i replay. Głównym sposobem uniknięcia ataku typu relay jest różnicowanie sesji wymiany danych. Istnieje kilka przykładów zapobiegania:

- Nadawca wstawia znacznik czasu do każdej wysyłanej wiadomości. Odbiorca zauważa przekazaną wiadomość, ponieważ czas odbioru wiadomości i znacznik czasu osadzony w wiadomości będą się różnić. Synchronizacja czasu powinna być realizowana przy użyciu bezpiecznego protokołu.
- Odbiorca wysyła jednorazowy token do nadawcy, a legalny nadawca używa wstępnie ustalonego algorytmu do przekształcenia tokena i wysłania wyniku do odbiorcy, np. obliczając funkcję skrótu tokena.

(viii) *Pharming*

Pharming ma na celu przekierowanie ruchu na stronie internetowej na fałszywy serwer. Niektóre możliwe sposoby przeprowadzenia ataku typu pharming to:

- Informacje mogą być nielegalnie modyfikowane na komputerze ofiary. Gdy użytkownik próbuje uzyskać dostęp do serwera, zostaje przekierowany na fałszywy serwer. Fizyczna próba wejścia do biura, uzyskania dostępu do komputera i zmodyfikowania adresu na skrócie to jeden z przykładów. Modyfikacja adresu za stroną banku w Ulubionych to jedna z opcji. Gdy użytkownik wybierze bank z Ulubionych, uzyska dostęp do fałszywego serwera. Inną opcję jest zmiana lokalnych wpisów DNS systemu operacyjnego. Co więcej, złośliwe oprogramowanie może wykonywać te czynności automatycznie.

- Komponenty sieciowe mogą zostać zmodyfikowane w celu przekierowania przychodzącego pakietu do fałszywego serwera. W takim przypadku na komputerze ofiary nie będzie żadnego śladu. W tym celu wystarczy zmienić tablicę routingu routera na drodze między komputerem ofiary a rzeczywistym serwerem WWW.

(ix) *Atak typu spoofing*

Atak spoofingowy polega na podszywaniu się pod inną osobę i uzyskiwaniu w ten sposób nielegalnej przewagi. Niektóre przykłady to:

- *Podszywanie się pod adres URL*: Odtwarzana jest legalna strona internetowa, która wydaje się identyczna z oryginalną. Użytkownicy mogą zostać oszukani i myśleć, że są połączeni z zaufaną witryną. W ten sposób hakerzy mogą uzyskać nazwy użytkowników i hasła.
- *SMS spoofing*: Wysyłanie wiadomości SMS podszywając się pod kogoś innego.
- *Podszywanie się pod e-mail*: Wysyłanie wiadomości e-mail podszywając się pod kogoś innego.
- *Podszywanie się pod adres IP*: Wysyłanie pakietu poprzez maskaradę przy użyciu fałszywego adresu IP.

(x) *Atak DoS*

Atak DoS polega na uczynieniu zasobu niedostępnym dla jego docelowych użytkowników. Jedną z powszechnych metod jest gromadzenie ogromnej ilości żądań do maszyny docelowej, tak że nie może ona już odpowiadać na legalny ruch lub odpowiada tak wolno, że usługa nie może być uznana za skutecznie dostępną. Ataki DoS są wdrażane w celu zmuszenia docelowego komputera do wyłączenia lub wyczerpania jego zasobów, tak aby nie mógł już świadczyć zamierzonych usług.

6.1.3.4 Ryzyko

Zagrożenie to możliwe niebezpieczeństwo, które może wyrządzić szkodę poprzez wykorzystanie słabości, podczas gdy potencjalna szkoda, która może powstać po zrealizowaniu jakiegoś zagrożenia, nazywana jest ryzykiem. Zagrożenie może mieć niskie prawdopodobieństwo wystąpienia, ale może mieć poważne konsekwencje, gdy się wydarzy. Na przykład prawdopodobieństwo wystąpienia trzęsienia ziemi może być bardzo niskie, ale w przypadku fabryki samochodów trzęsienie ziemi może całkowicie zniszczyć fabrykę, a firma może nawet zbankrutować, jeśli nie podejmie środków przed wystąpieniem zagrożenia.

Nie możemy zaakceptować dużego ryzyka, nawet jeśli prawdopodobieństwo jego realizacji jest niewielkie. Musimy zwiększyć bezpieczeństwo do punktu, w którym nasze ryzyko jest pod kontrolą i tolerowane. Rozwiążaniem jest zarządzanie ryzykiem.

Ryzyko jest definiowane jako funkcja trzech zmiennych:

- Potencjalny wpływ możliwej szkody, jaką spowoduje zagrożenie (koszt).
- Prawdopodobieństwo wystąpienia ataku (P_{attack}).
- Prawdopodobieństwo powodzenia ataku ($P_{success}$).

Tak

więc:

$$\text{Ryzyko} = (\text{Koszt}) * (P_{attack}) * (P_{success})$$

Z równania wynika, że prawdopodobieństwo ryzyka pozostaje wysokie, gdy koszt jest wysoki, nawet jeśli prawdopodobieństwo jest niskie. Podobny wynik można obliczyć, gdy koszt jest umiarkowany, ale prawdopodobieństwo jest wysokie. W każdym przypadku menedżer ryzyka powinien wziąć pod uwagę wszystkie składniki równania.

Rozważając możliwość ataku wirusa, przyjmijmy, że podane są następujące wartości:

- Oczekiwany koszt wirusa dla firmy wynosi 10 000 EUR.
- Prawdopodobieństwo ataku wirusa wynosi 40%.
- Prawdopodobieństwo powodzenia ataku wynosi 80%.

Możemy obliczyć ryzyko jako:

$$\text{Ryzyko} = 10\,000 * 0,40 * 0,80 = 3200 \text{ €}$$

Podsumowując, możemy użyć jednego przykładu, aby pokazać związek między podatnością, zagrożeniem, atakiem i ryzykiem. Gdy w domu pozostawione jest otwarte okno, stanowi ono słaby punkt domu. Biorąc pod uwagę, że złodzieje mogą próbować włamać się do domów w regionie, zagrożenie polega na tym, że złodzieje mogą wejść do domu. Gdy konkretny złodziej próbuje wejść do domu, jego działanie jest atakiem. Jeśli złodziejowi uda się wejść do domu, istnieje ryzyko, że cała biżuteria może zostać skradziona.

6.1.4 Zasady bezpieczeństwa

6.1.4.1 Kompromis w bezpieczeństwie: Bezpieczeństwo a funkcjonalność i wydajność

Funkcjonalność to to, co produkt oferuje lub zapewnia swojemu użytkownikowi. Wydajność to ilość oferowanej pracy. Funkcjonalność i wydajność razem to suma tego, co i w jakim stopniu system informacyjny wykonuje dla użytkownika lub potencjalnego klienta oferowanego produktu.

Bezpieczeństwo to stopień ochrony przed złośliwymi działaniami, które mogą w jakiś sposób wyrządzić szkodę. Bezpieczny system to taki, który wykonuje funkcje systemu i jednocześnie zapobiega wszelkim działaniom niewłaściwego użycia.

Usługa powinna zapewniać równowagę między łatwością użytkowania a bezpieczeństwem. Jako prosty przykład, gdy hasło jest łatwe do zapamiętania, użytkownik jest zadowolony, ponieważ nie poświęca zbyt wiele wysiłku, próbując je zapamiętać. Jednak takie hasło nie zapewnia dużego bezpieczeństwa. Bezpieczeństwo wzrasta, gdy hasło staje się bardziej złożone, ale w takim przypadku hasło staje się problemem dla użytkownika, ponieważ zapamiętanie go staje się trudniejsze.

(i) Punkt widzenia użytkownika podczas instalacji komponentów zabezpieczeń

Kiedy definicje funkcjonalności, wydajności i bezpieczeństwa są oceniane razem, wydaje się, że bezpieczeństwo pomaga poprawić funkcjonalność i wydajność. Nie jest to jednak takie banalne. Rozważ korzystanie z oprogramowania antywirusowego. Jeśli wirus rozprzestrzeni się na komputerze, komputer ulegnie degradacji. Oznacza to mniejszą wydajność, mniejszą funkcjonalność lub nawet brak wydajności.

Korzystanie z oprogramowania antywirusowego ma jednak swoje wady. Pierwszą z nich jest koszt oprogramowania. Kolejną jest spadek wydajności komputera ze względu na wykorzystanie procesora i pamięci przez oprogramowanie podczas jego wykonywania. Dlatego oprogramowanie antywirusowe jest używane w celu zwiększenia funkcjonalności i wydajności, ale powoduje spadek obu. Jakie są inne alternatywy?

- Jeśli nie korzystasz z oprogramowania antywirusowego:
 - W najlepszym przypadku nie dojdzie do udanego ataku.
 - Wirus przeprowadza udany atak. W rezultacie utracisz wydajność, przydatne dane, zainstalowane aplikacje, a nawet komputer.

- Jeśli korzystasz z oprogramowania antywirusowego:
 - Nie dochodzi do ataku, ale trzeba zakupić oprogramowanie antywirusowe, a komputer traci wydajność z powodu wykonywania oprogramowania.
 - Atak wirusa zakończy się sukcesem, jednak nie będzie on skuteczny. Zaoszczędzisz funkcjonalność, wydajność, dane i potencjalnie pieniądze, ponieważ zachowałeś dane, aplikacje, system operacyjny i sam komputer.

(ii) *Punkt widzenia dewelopera na instalację komponentów bezpieczeństwa*

Kiedy opracowywana jest nowa aplikacja, firma zawsze stara się (i zwykle musi) zaprezentować produkt końcowy tak wcześnie, jak to możliwe w celach marketingowych. Zawsze istnieje możliwość, że konkurencja wkrótce zaoferuje podobny produkt na rynku. Jednak wbudowanie komponentów bezpieczeństwa w produkt jest zawsze żmudnym i kosztownym procesem. W związku z tym, gdy decyzję pozostawia się firmie, wydaje się ona odkładać większość pomiarów bezpieczeństwa na później, co skutkuje wysokim ryzykiem.

Z szerszego punktu widzenia, kompromis jest pomiędzy poziomem bezpieczeństwa, szybkością wykonywania aplikacji, funkcjonalnością systemu i dodatkowymi kosztami środków bezpieczeństwa.

6.1.4.2 Czy możliwe jest idealne bezpieczeństwo?

Perfekcja w bezpieczeństwie jest niemożliwa. Żaden system nie jest w 100% bezpieczny. Konieczne jest osiągnięcie równowagi między zwiększeniem bezpieczeństwa systemu a jego funkcjonalnością. Wiedząc, że użytkownik bardziej ceni sobie funkcjonalność niż bezpieczeństwo, trudno jest zbudować bardzo bezpieczny system.

Możemy powiedzieć, że system jest całkowicie bezpieczny, jeśli cała moc obliczeniowa na świecie jest używana w nieskończoność, system nie może zostać złamany. System jest obliczeniowo bezpieczny, nawet jeśli używany jest ograniczony czas (ale bardzo duży) i ograniczona moc komputera (ale bardzo duża), system nie może zostać złamany. W tym przypadku możemy również powiedzieć, że złamanie systemu jest niewykonalne, ponieważ intruz zużyłby zbyt dużo czasu. Rozważmy atak na mechanizm bezpieczeństwa karty kredytowej. Jeśli system zabezpieczeń jest bezpieczny obliczeniowo, próba złamania systemu jest niewykonalna, ponieważ nawet jeśli zabezpieczenia karty zostaną złamane, zajmie to kilka stuleci, a karta kredytowa nie będzie już w użyciu.

Po zaakceptowaniu niemożności doskonałego bezpieczeństwa jako prawdy, nadal konieczne jest utrzymanie wysokiego poziomu bezpieczeństwa systemu. Wraz z wprowadzeniem nowoczesnych kryptosystemów, a następnie odpowiednich implementacji, możliwe jest budowanie systemów, które są wystarczająco bezpieczne.

Bezpieczeństwo systemu zależy od dwóch parametrów:

- Siła algorytmów kryptograficznych, która musi być badana przez naukowców i specjalistów ds. bezpieczeństwa, ale nie przez osoby, które korzystają z zapewnionego bezpieczeństwa.
- Nie możemy ignorować roli użytkownika. Jest on odpowiedzialny za przechowywanie hasła lub klucza przypisany do niej. Nie jest to trywialna sprawa. Jeśli hasło jest łatwe do zapamiętania, hakerowi łatwo jest je znaleźć w ciągu kilku sekund za pomocą ogólnodostępnych programów z Internetu. Zwiększenie złożoności hasła wydaje się być rozwiązaniem pozwalającym przezwyciężyć ten problem.

hakerów. Jednak osadzenie niektórych złożonych liter w haśle, takich jak "?-;* /&%+", sprawia, że hasło jest trudne do zapamiętania, a zatem może zostać zapisane gdzieś przez użytkownika, co umożliwia hakerowi jego znalezienie.

Dlatego też, gdy widzisz na stronie internetowej banku frazę "%100 bezpieczny", to, co twierdzą, że oferują, to tylko algorytm kryptograficzny. Całkowite bezpieczeństwo zawsze zależy od odpowiednika, takiego jak budowanie i utrzymywanie hasła w tajemnicy, tak aby haker lub narzędzie hakerskie nie mogły do niego dotrzeć ani go wygenerować.

6.1.4.3 Hakerzy są zawsze o krok do przodu

Oprogramowanie antywirusowe zapobiega dostępowi nowych wirusów dopiero po ich wygenerowaniu przez haka. Antywirus jest generowany po pojawienniu się powiązanego wirusa. Hakerzy są zawsze o krok do przodu, co wydaje się niesprawiedliwe, ale niestety jest prawdą. Istnieją ku temu ważne powody. Używając analogii do zamku:

- Istnieje więcej niż jedna słaba ściana zamku i trudno jest naprawić je wszystkie. Nawet jeśli to zrobimy, wcześniejsze stosunkowo mocne części staną się od tego momentu słabsze. Musimy wzmacnić również te części. Spowoduje to niekończącą się sekwencję wysiłków.
- Trudno zgadnąć, w jaki sposób hakerzy zaatakują słabsze części. Istnieje tak wiele opcji że naprawdę nie jest łatwo technicznie zaspokoić każdą możliwość.
- Należy również wziąć pod uwagę koszty. Próba naprawy wielu części ściany jest kosztowna.

6.1.4.4 Zachowaj prostotę

Rozważmy mechanizmy bezpieczeństwa zbudowane dla dużej organizacji. Kampus jest ogromny, są tam tysiące pracowników i odwiedzających, a zapewnienie mechanizmów bezpieczeństwa nie jest łatwe. Natychmiastowe opcje, które może rozważyć menedżer ds. bezpieczeństwa, to wykorzystanie wielu pracowników ochrony, punktów kontrolnych, kart dostępu, haseł, kompleksowych ścisłych zasad i broszur pomocniczych, w tym dyrektyw dla pracowników ochrony i personelu. Oczywiście może to doprowadzić do niepowodzenia, ponieważ po wprowadzeniu dużej złożoności do systemu może on również nie działać prawidłowo. Na przykład pracownicy ochrony będą mieli trudności ze sprawdzeniem szczegółów zasad z broszur; będą mieli spory co do stosowania surowych zasad. Pracownicy mogą również czuć się bardzo niekomfortowo z tymi zasadami i mogą narzekać.

Dlaczego złożoność osłabia bezpieczeństwo:

- Dyscyplina bezpieczeństwa jest z natury złożona i należy wziąć pod uwagę wiele parametrów. Jeśli procedury stają się złożone, trudniej jest odkryć ich słabe punkty.
- Jeśli procedury bezpieczeństwa są złożone, trudniej jest zweryfikować ich poprawność i kompletność;
W związku z tym istnieje duże prawdopodobieństwo, że niektóre luki zostały już pominięte.
- W przypadku zaobserwowania problemu w mechanizmie bezpieczeństwa, trudniej jest zidentyfikować jego przyczynę.

Rozwiązań jest prostota. Proste zasady z jasnymi definicjami pozwalające na wystarczającą inicjatywę upoważnionym pracownikom ochrony zapewniają lepsze bezpieczeństwo.

6.1.4.5 Wzmocnij najsłabsze ogniwo

System najprawdopodobniej zawiedzie w najsłabszym ogniwie, a atakujący zaatakuje również najsłabsze ogniwo. Kiedy zamierzasz zwiększyć bezpieczeństwo systemu, mądrze jest skoncentrować się na najsłabszym ogniwie. Wykorzystanie zasobów do wzmacniania innych punktów nie pomoże, ponieważ system najprawdopodobniej zostanie uszkodzony w najsłabszym ogniwie.

6.1.4.6 Nie ufaj użytkownikom

Kiedy ludzie dokonują wyborów, mają tendencję do podejmowania najgorszych decyzji dotyczących bezpieczeństwa. Powód tego jest oczywisty. Użytkownicy zawsze preferują funkcjonalność i zakładają, że bezpieczeństwo oznacza spędzanie czasu bez żadnych korzyści.

6.1.4.7 Przypisywanie najniższych uprawnień

Podmiotowi (użytkownikowi lub aplikacji) należy nadać tylko niezbędne prawa i uprawnienia do wykonania zadania bez dodatkowych i niepotrzebnych uprawnień. Ograniczenie uprawnień podmiotu potencjalnie ogranicza ilość szkód, które mogą zostać wyrządzone. Zasada ta pomaga organizacji chronić swoje zasoby.

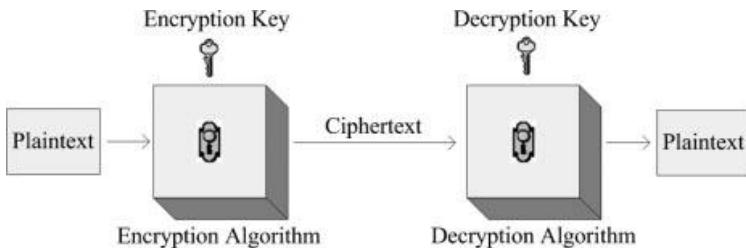
Zasada najmniejszego przywileju wymaga, aby każdy podmiot miał dostęp tylko do tych obiektów, które są zdecydowanie niezbędne dla jego funkcjonalności. Rozważmy użytkownika, który musi wykonać kopię zapasową danych, ale nie musi ich modyfikować. W związku z tym użytkownik musi mieć tylko możliwość wykonania kopii zapasowej, ale nie może mieć możliwości aktualizacji danych. W związku z tym wszelkie inne działania, które nie są istotne dla tworzenia kopii zapasowych, muszą zostać zablokowane.

6.1.4.8 Obrona w głąb

Obrona w głąb ma na celu opóźnienie działania atakującego zamiast stosowania mechanizmów zapobiegawczych. W międzyczasie można podjąć dodatkowe środki ostrożności i zapobiec dalszym szkodom wyrządzonym przez atakującego. Zamiast pokonywać atakującego za pomocą pojedynczej i silnej linii obrony, obrona w głąb ma na celu zmuszenie atakującego do utraty impetu przez pewien okres czasu. Gdy atakujący straci impet, można zareagować na jego słabe punkty.

6.1.4.9 Warstwowe zabezpieczenia

Środkiem uwierzytelniania jest coś, co użytkownik zna, ma, jest i robi. Weźmy pod uwagę firmę, która każe swoim pracownikom okazywać kartę identyfikacyjną przy głównym wejściu. Próbując zwiększyć bezpieczeństwo systemu, lepiej jest dodać inne mechanizmy, takie jak skaner siatkówki oka lub hasło przy wejściu do działu. Bezpieczeństwo warstwowe polega na stosowaniu różnych mechanizmów ochrony zasobów i danych informatycznych.



Rysunek 6.6 Proces szyfrowania i deszyfrowania.

broniąc się przed napastnikiem metodami wykorzystującymi tę samą strategię, zabezpieczenia warstwowe wykorzystują różne typy mechanizmów. Na przykład karta identyfikacyjna może być używana przy głównym wejściu, metody biometryczne mogą być używane przy wejściu do centrali, a klawiatura wymagająca wprowadzenia hasła może być używana przy wejściu do centrum obliczeniowego.

6.2 Narzędzia bezpieczeństwa i mechanizmy

Większość mechanizmów bezpieczeństwa opiera się na kryptografii. Kryptografia jest używana do zapewniania bezpiecznych kanałów, przechowywania informacji o hasłach na dysku twardym, cyfrowego podpisywania transakcji finansowych i tak dalej.

6.2.1 Kryptografia

Kryptografia to praktyka ukrywania informacji poprzez zmianę ich formy w nieoczywisty tekst. Podstawowe usługi świadczone przez kryptografię to:

- Zdolność do przechowywania informacji w formie, która nie jest łatwa do ujawnienia oryginalnych informacji.
- Możliwość bezpiecznej wymiany informacji między uczestnikami.

Kryptografia polega na szyfrowaniu oryginalnych danych (wiadomości) przy użyciu klucza szyfrującego, przechowywaniu lub przesyłaniu zaszyfrowanych danych (syfrogramu) do odbiorcy i odszyfrowywaniu syfrogramu przy użyciu klucza deszyfrującego do oryginalnej wiadomości (patrz rysunek 6.6).

Ideą kryptografii jest możliwość wysłania wiadomości w zakodowanej formie zwanej syfrogramem, tak aby komunikacja między nadawcą a odbiorcą była nadal możliwa i odbywała się za pomocą kanałów publicznych, takich jak Internet. W międzyczasie intruz nie ma pojęcia o rzeczywistej treści, czyli zwykłym tekście wiadomości.

Kryptografia tradycyjnie była wykonywana przy użyciu kryptografii symetrycznej, w której zarówno nadawca, jak i odbiorca dzielą ten sam tajny klucz. W 1976 roku wprowadzono nową formę kryptografii, kryptografię asymetryczną, wraz z pierwszym przykładem algorytmu RSA, w którym nadawca i odbiorca posiadają różne, ale pasujące do siebie pary kluczy. Hashing, jako inna forma algorytmu kryptograficznego, nie używa żadnego klucza. Zapewnia on głównie integralność przesyłanej wiadomości, ale nie uwierzytelnianie ani poufność. Algorytmy Hashing [np. Hash-based Message Authentication Code (HMAC)], które wykorzystują klucze, zapewniają również uwierzytelnianie.

6.2.2 Kryptografia symetryczna

Kryptografia symetryczna, znana również jako kryptografia tradycyjna i kryptografia z kluczem tajnym, wykorzystuje jeden wspólny klucz zarówno do procesu szyfrowania, jak i deszyfrowania. Jest ona określana jako:

- *Tradycyjna kryptografia*, ponieważ składa się ze stosunkowo starszego mechanizmu w porównaniu z nowoczesną kryptografią.
- *Kryptografia klucza tajnego*, ponieważ klucz współdzielony między nadawcą a odbiorcą musi być
 - być utrzymywane w tajemnicy przed osobami trzecimi.
- *Kryptografia symetryczna*, ponieważ:
 - Algorytmy szyfrowania i deszyfrowania są identyczne (symetryczne).
 - Ten sam klucz jest używany zarówno do szyfrowania, jak i deszyfrowania.

Kryptografia z kluczem symetrycznym jest używana w celu zapewnienia tajności, uwierzytelnienia i integralności, co oznacza, że klucz musi być utrzymywany w tajemnicy. Ponieważ ten sam klucz jest używany zarówno do szyfrowania, jak i deszyfrowania, klucz jest symbolizowany przez K bez użycia żadnego indeksu dolnego. Dwa ważne wymagania dotyczące bezpiecznego korzystania z szyfrowania symetrycznego to:

- Wymagany jest silny algorytm szyfrowania.
- Tajny klucz powinien być utrzymywany w tajemnicy przez nadawcę i odbiorcę. Ujawnienie klucza komukolwiek strony trzecie skutkuje niespełnieniem wymogów bezpieczeństwa, takich jak uwierzytelnianie.

Algorytmy kryptosystemów symetrycznych opierają się głównie na substytucji, permutacji i schematach hybrydowych. Zastępowanie polega na zastępowaniu części tekstu jawnego niektórymi danymi z alfa-beta. Permutacja polega na zamianie części tekstu jawnego między sobą. Schematy hybrydowe polegają na wykonywaniu obu metod jedna po drugiej.

Wcześniejszego przykłady kryptosystemu symetrycznego, na przykład algorytm Cezara, przenoszą tekst jawnego po jednej literze na raz i są nazywane szyframi strumieniowymi. Nowsze algorytmy symetryczne, takie jak Data Encryption Standard (DES), Triple DES (3DES) i Advanced Encryption Standard (AES), szyfrują tekst jawnego w określonych długościach i są nazywane szyframi blokowymi.

(i) DES

DES to symetryczny szyfr blokowy wykorzystujący klucz współdzielony, który został przyjęty jako standard w 1976 roku. Algorytm był początkowo kontrowersyjny ze względu na elementy projektu, które nie zostały upubliczniione, stosunkowo krótką długość klucza i możliwość backdoora Agencji Bezpieczeństwa Narodowego (NSA). DES jest obecnie uważany za mało bezpieczny w wielu zastosowaniach. Wynika to głównie z faktu, że 56-bitowy rozmiar klucza jest zbyt mały, a wielu już złamało system.

(ii) 3DES

Po wprowadzeniu DES moc obliczeniowa wzrosła na całym świecie, a atakujący korzystający z nowych komputerów odnieśli sukces w atakach siłowych. Jednym z głównych powodów był rozmiar klucza. 3DES zapewnia metodę zwiększania rozmiaru klucza praktycznie bez projektowania nowego algorytmu. Dlatego też uważa się, że algorytm DES jest stosunkowo bezpieczny tylko w formie 3DES. Jest to zmodyfikowana wersja DES, w której algorytm szyfrowania DES jest stosowany trzy

(iii) *AES*

W ostatnich latach szyfr 3DES został zastąpiony przez AES.

6.2.3 Kryptografia asymetryczna

W kryptografii asymetrycznej używane są dwa różne klucze: klucz publiczny używany do szyfrowania i klucz prywatny używany do deszyfrowania i odwrotnie. Publiczny klucz szyfrowania jest udostępniany wszystkim lub każdemu członkowi zamkniętej grupy, podczas gdy prywatny klucz deszyfrowania jest znany tylko odbiorcy. Wiadomości są szyfrowane za pomocą klucza publicznego i mogą być odszyfrowane tylko za pomocą klucza prywatnego. Znajomość klucza prywatnego nie pomaga w tworzeniu odpowiedniego klucza publicznego i odwrotnie. Klucz prywatny jest oznaczany jako K_R , a klucz publiczny jako K_U .

Kryptografia asymetryczna jest określana jako:

- *Nowoczesna kryptografia*, ponieważ składa się ze stosunkowo nowszego mechanizmu w porównaniu z tradycyjną kryptografią.
- *Kryptografia klucza publicznego*, ponieważ klucz szyfrowania (i czasami deszyfrowania) jest tworzony publiczna i nie ma potrzeby utrzymywania jej w tajemnicy.
- *Kryptografia asymetryczna*, ponieważ:
 - Algorytmy szyfrowania i deszyfrowania są różne (nie symetryczne).
 - Klucz szyfrowania nie może być użyty do odszyfrowania i odwrotnie.

Kryptografia symetryczna wymaga wymiany kluczy między stronami przed rozpoczęciem szyfrowania. Fizyczny transfer klucza wydaje się wystarczająco bezpieczny. Jeśli klucz jest utrzymywany przez obie strony w całkowitej tajemnicy, można go następnie wykorzystać do wymiany zaszyfrowanych wiadomości. Oczywiście jest, że fizyczna wymiana kluczy nie jest trywialnym procesem. Kryptografia klucza publicznego rozwiązuje tę kwestię i inne wady.

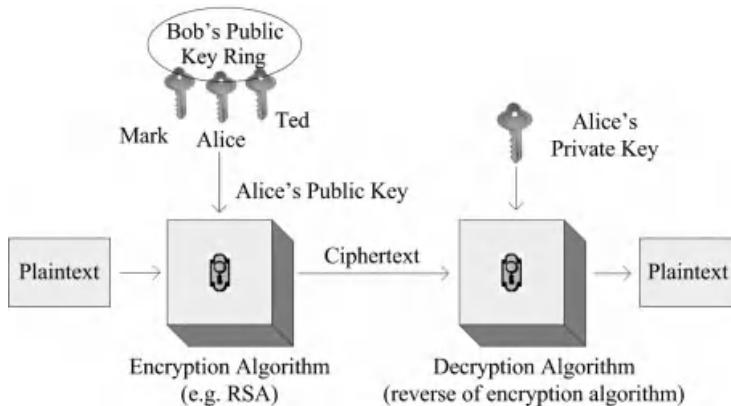
Kryptografia klucza publicznego może być również wykorzystywana do bezpiecznej wymiany symetrycznych kluczy kryptograficznych między dwiema stronami. Jednym z wyróżniających się przykładów jest wymiana kluczy Diffiego-Hellmanna. Była to pierwsza metoda ustanawiania tajnego klucza za pośrednictwem kanału publicznego.

Kryptografia asymetryczna może być wykorzystywana do spełnienia różnych wymagań bezpieczeństwa:

- *Szyfrowanie kluczem publicznym*: Wiadomość zaszyfrowana kluczem publicznym wcześniej określonego odbiorcy może zostać odszyfrowana tylko przez tego odbiorcę, ale przez nikogo innego. Ten przypadek jest wykorzystywany do zapewnienia poufności.
- *Podpis cyfrowy*: Wiadomość podpisana kluczem prywatnym może być zweryfikowana przez każdego, kto posiada klucz publiczny. Jeśli użycie klucza publicznego skutkuje pomyślnym odszyfrowaniem, dowodzi to, że zaszyfrowany dokument został utworzony przez właściciela klucza prywatnego. Zasadniczo wymaga to oczywiście zachowania klucza prywatnego nadawcy w tajemnicy.

Do lat 70-tych XX wieku znane były tylko algorytmy symetryczne, a co za tym idzie, możliwe było spełnienie tylko niektórych wymagań, takich jak tajność i integralność danych.

~~Zymaność NEC~~ strony, niezwykle ważne wymagania, takie jak niezaprzeczalność, nie mogły zostać spełnione. Odkrycie algorytmów klucza publicznego zrewolucjonizowało kryptografię. Gdyby kryptografia klucza publicznego nie została wprowadzona,



Rysunek 6.7 Schemat RSA A: użycie klucza publicznego do szyfrowania i klucza prywatnego do deszyfrowania.

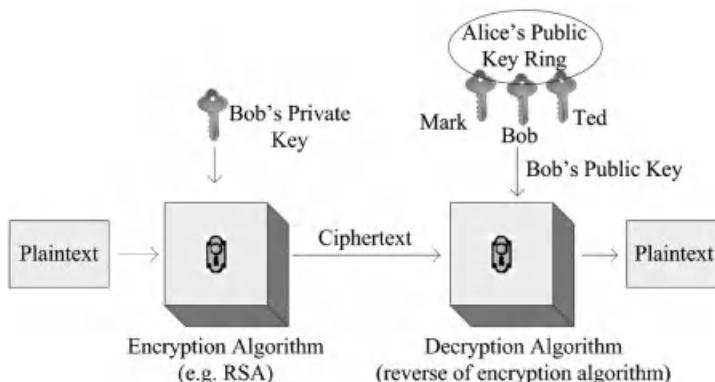
Obecne korzystanie z witryn bankowych, cyfrowych przelewów pieniężnych i tak dalej nie byłoby możliwe. Najważniejsze algorytmy to:

(i) *RSA*

Algorytm RSA jest pierwszą publicznie znaną kryptografią klucza publicznego (patrz rysunki 6.7 i 6.8). Był to znaczący postęp w kryptografii. Obecnie RSA jest szeroko stosowany w protokołach handlu elektronicznego. Uważa się, że jest bezpieczny, gdy używane są wystarczająco długie klucze, a protokół użytkowania jest doskonały.

(ii) *Kryptografia krzywych eliptycznych*

Zdecydowana większość usług wykorzystujących kryptografię klucza publicznego do szyfrowania i podpisów cyfrowych wykorzystuje algorytm RSA. Obecnie pojawił się konkurencyjny system stanowiący wyzwanie dla RSA o nazwie Elliptic Curve Cryptography (ECC). W porównaniu z RSA, główną zaletą ECC jest to, że wymaga mniejszego rozmiaru bitu dla tego samego poziomu bezpieczeństwa. W związku z tym ECC zmniejsza narzut przetwarzania. ECC jest zasadniczo bardziej skomplikowana.



Rysunek 6.8 Schemat RSA B: użycie klucza prywatnego do szyfrowania i klucza publicznego do deszyfrowania.

do wyjaśnienia i przetworzenia niż RSA. Wymagana jest technika matematyczna oparta na wykorzystaniu konstrukcji matematycznej znanej jako krzywa eliptyczna.

6.2.4 Hashing

Hashing zapewnia integralność informacji poprzez tworzenie wartości skrótu danych wejściowych. Integralność zapewniana przez hashowanie nie jest jednak tak silna, jak integralność zapewniana przez podpis cyfrowy. Po pierwsze, nie wszystkie algorytmy hashujące zapewniają równy poziom zaufania. Rozważmy algorytm haszujący wykorzystujący 1 bit wartości haszującej, tak że wartość haszująca dowolnej wiadomości wynosi 0 lub 1. W takim przypadku atak brute force ma 50% szans powodzenia nawet przy pierwszej próbie. Najwyraźniej nie jest to godny zaufania algorytm haszujący. Wraz ze wzrostem rozmiaru wartości skrótu wzrasta odporność systemu. Algorytm użyty do tego celu jest oczywiście ważny i zmienia poziom zaufania. Nie będziemy podawać szczegółów na ten temat, ale ważne jest, aby pamiętać, że słaby algorytm haszujący rozczałrowuje użytkownika.

6.2.5 Kod uwierzytelniania wiadomości (MAC) i HMAC

Aby mieć pewność co do tożsamości nadawcy wiadomości i jej treści, jedną z opcji jest zaszyfrowanie całej wiadomości, a następnie jej wysłanie. W zależności od rodzaju zastosowanego algorytmu kryptograficznego (tj. symetrycznego lub asymetrycznego), poufność, integralność danych, uwierzytelnianie itp. mogą być spełnione. Problem polega na tym, że fazy szyfrowania i deszyfrowania wymagają czasu, co nie jest korzystne w niektórych przypadkach. W tym celu można wygenerować MAC za pomocą algorytmu mieszącego, który jest szybszy niż szyfrowanie. Algorytm MAC wprowadza tajny klucz i wiadomość, a następnie generuje MAC. Wartość MAC może być później wykorzystana do zapewnienia integralności danych, a także autentyczności wiadomości.

HMAC jest ulepszoną wersją algorytmu MAC. MAC nie używa żadnego klucza, podczas gdy HMAC używa tajnego klucza współdzielonego zarówno przez nadawcę, jak i odbiorcę. MAC zapewnia integralność danych, ale nie autentyczność, ponieważ algorytm MAC jest publiczny. Z kolei HMAC zapewnia również uwierzytelnianie, ponieważ tylko nadawca i odbiorca znają tajny klucz. Należy również zauważać, że ponieważ obaj użytkownicy posiadają klucz, niezaprzeczalność nie jest spełniona. Obecnie dostępne popularne algorytmy HMAC to MD5, SHA-1 i SHA-2. Bezpieczeństwo HMAC zależy od powodzenia zastosowanego algorytmu kryptograficznego, rozmiaru danych wyjściowych oraz rozmiaru i jakości klucza kryptograficznego.

6.2.6 Podpis cyfrowy i podpis mobilny

Podpis cyfrowy zapewnia uwierzytelnienie i niezaprzeczalność użytkownika oraz integralność dokumentu. Przeanalizujmy przyczyny takiego stanu rzeczy. Po pierwsze, należy pamiętać, że kriptografia asymetryczna może być stosowana w dwóch scenariuszach. W pierwszym scenariuszu każdy może użyć klucza publicznego do zaszyfrowania wiadomości i wysłania jej do odbiorcy. Następnie odbiorca, który posiada klucz prywatny, używa tego klucza do odszyfrowania szyfrogramu. W drugim scenariuszu klucz prywatny jest znany tylko nadawcy, a nadawca używa tego klucza do utworzenia szyfrogramu. Klucz publiczny jest znany wszystkim i może być użyty przez każdego do

Pierwszy scenariusz zapewnia integralność i tajność, podczas gdy drugi scenariusz zapewnia integralność, uwierzytelnianie i niezaprzecjalność.

Scenariusz 1 przewiduje:

- Integralność, ponieważ jeśli szyfrogram zostanie w jakiś sposób zmodyfikowany po drodze, zmodyfikowanej wersji szyfrogramu nie można później odszyfrować za pomocą klucza prywatnego.
- Tajność, ponieważ nikt inny niż odbiorca nie może odszyfrować szyfrogramu, ponieważ prywatny jest znany tylko przez odbiorcę.

Scenariusz 2 przewiduje:

- Integralność, ponieważ jeśli szyfrogram zostanie w jakiś sposób zmodyfikowany po drodze, zmodyfikowanej wersji szyfrogramu nie można później odszyfrować za pomocą klucza publicznego.
- Uwierzytelnianie, ponieważ nikt inny niż nadawca nie może utworzyć szyfrogramu, ponieważ Klucz prywatny jest znany tylko nadawcy, a odszyfrowanie szyfrogramu zapewnia odbiorcę o tym fakcie.
- Niezaprzecjalność, ponieważ szyfrowanie wiadomości kluczem prywatnym udowadnia, że tylko osoba nadawca i nikt inny nie jest w stanie wysłać zaszyfrowanej wersji wiadomości.

Może być mylące, że zarówno podpis cyfrowy, jak i MAC zapewniają integralność. Użytkownik może zastanawiać się, który z nich wybrać, gdy chce zapewnić integralność danych. Zauważymy już, że nie wszystkie algorytmy haszujące lub MAC są równie obiecujące. Istnieje różnica między algorytmami haszowania i podpisu cyfrowego. Zasadniczo algorytmy podpisu cyfrowego zapewniają lepszą integralność niż algorytmy haszujące. Powodem jest fakt, że każda konkretna wartość hash odpowiada więcej niż jednej możliwej wartości wejściowej, a haker zawsze ma szansę na uzyskanie dostępu. Nie jest to prawdą w przypadku podpisów cyfrowych. Tylko przypadkowo i rzadko podpis reprezentuje jakąkolwiek treść wiadomości.

6.2.7 Porównanie mechanizmów bezpieczeństwa

Najprostszym algorytmem sprawdzania błędów jest kodowanie bitów parzystości, ponieważ wykorzystuje on 1 bit do sprawdzania błędów, co jest najmniejszą ilością danych, jaką może przechowywać. Trywialnie można powiedzieć, że jest to najmniej skuteczna opcja. Rozważmy algorytm RSA. Gdy używany jest krótszy rozmiar klucza, taki jak 256 lub 512 bitów, bezpieczeństwo jest mniejsze w porównaniu z dłuższymi kluczami, takimi jak 1024 lub 2048 bitów.

Pamiętajmy, że mamy wymagania bezpieczeństwa i narzędzi kryptograficzne, które je spełniają. Mogłyby być prościej, gdyby istniał jeden mechanizm dla każdego z nich, ale niestety tak nie jest. Hashing może być używany do integralności dokumentu; MAC może być używany do integralności dokumentu i uwierzytelniania nadawcy; kryptografia symetryczna może być używana do uwierzytelniania nadawcy i odbiorcy, a także integralności dokumentu; podpis cyfrowy może być używany do uwierzytelniania nadawcy, niezaprzecjalności i integralności dokumentu. Nieznajomość szczegółów algorytmów może prowadzić do nieporozumień. Aby wybrać odpowiedni, powinniśmy je szczegółowo

przeanalizować.

Hashowanie wykorzystuje funkcje jednokierunkowe, tworząc w ten sposób mniejszą wartość skrótu w porównaniu z wiadomością. Oczywistymi zaletami haszowania i MAC w porównaniu z algorytmami symetrycznymi i asymetrycznymi jest to, że algorytmy haszujące działają znacznie szybciej i mają mniejsze rozmiary.

rozmiar, co skutkuje lepszym przechowywaniem. Wadą jest to, że dobrze znany paradoks urodzin jest podatnością tego rodzaju algorytmów, przez co są one mniej bezpieczne niż inne opcje.

Kryptografia symetryczna zapewnia poufność i uwierzytelnianie wiadomości (uwierzytelnianie nadawcy wraz z integralnością dokumentu). Algorytmy symetryczne działają szybciej niż algorytmy oparte na haszowaniu, ale wolniej niż algorytmy asymetryczne.

Kryptografia asymetryczna z szyfrowaniem kluczem prywatnym zapewnia poufność, uwierzytelnianie wiadomości i niezaprzecjalność nadawcy i odbiorcy. Gdy do szyfrowania używany jest klucz publiczny, spełnione są tylko warunki uwierzytelniania wiadomości i niezaprzecjalności odbiorcy. Poufność nie jest jednak spełniona, ponieważ klucz publiczny jest znany przez wszystkich.

Kryptografia asymetryczna działa znacznie wolniej niż algorytmy symetryczne i nie nadaje się do szyfrowania masowego. Dlatego w przypadkach, w których wymagana jest wysoka wydajność, należy stosować pewne schematy hybrydowe. Na przykład, aby zapewnić bezpieczny kanał, najpierw należy zapewnić autoryzację przy użyciu kryptografii asymetrycznej, a następnie wykonać kryptografię symetryczną przy użyciu klucza sesji, który jest generowany tylko dla tej sesji.

6.2.8 Certyfikaty cyfrowe i certyfikat Authority

Certyfikat cyfrowy jest w rzeczywistości podpisem cyfrowym odpowiedniej osoby lub organizacji (np. tożsamość, okres ważności) ze zintegrowanym kluczem publicznym. Certyfikat może być wykorzystany do zweryfikowania, czy klucz publiczny należy do właściciela certyfikatu. Podpis jest tradycyjnie wydawany przez zaufany podmiot, czyli urząd certyfikacji (CA).

6.2.9 Nie utrzymuj algorytmów kryptograficznych w tajemnicy

Załóżmy, że opracowałeś algorytm kryptograficzny, który może być użyty do spełnienia pewnych wymagań bezpieczeństwa. Wydaje się oczywiste, że utrzymanie algorytmu w tajemnicy przed samym sobą czyni go tajnym. Na pierwszy rzut oka system kryptograficzny wykorzystujący algorytm wydaje się wystarczająco bezpieczny. Nie jest to jednak rzeczywistość. Zwyczajem jest publikowanie algorytmów kryptograficznych, głównie w środowisku akademickim, takim jak konferencje lub czasopisma, aby zainteresowane strony mogły natychmiast rozpocząć analizę algorytmu w nadziei na znalezienie słabości, a następnie opublikowanie wyników swoich badań.

W rzeczywistości istnieją trzy przypadki do rozważenia:

- Znaleziona luka jest tak duża, że niemożliwe jest jej wypełnienie i w konsekwencji algorytm zostaje odrzucony.
- Znaleziona zostaje jedna lub więcej mniejszych luk, które mogą zostać naprawione przez twórcę algorytmu lub
 - Naprawy mogą być nawet sugerowane przez naukowca, który znalazł lukę.
- Nie znaleziono żadnego słabego punktu, więc algorytm jest wystarczająco doskonały, aby można go było wykorzystać do dostarczania pewnych wzgórzy bezpieczeństwa.

Ponieważ wszystkie algorytmy są upubliczniane, silne algorytmy są poddawane kontroli, a słabe algorytmy są odsuwane na bok. Wykorzystanie doświadczenia naukowców, praktyków i profesjonalistów ostatecznie doprowadzi do odrzucenia algorytmu lub

dostrajenia go, aż stanie się wystarczająco bezpieczny. Czasami system szyfrowania działa przez dziesięciolecia. Prywatne lub zastrzeżone algorytmy nie pomagają w zwiększeniu bezpieczeństwa. Często ci, którzy analizują zastrzeżone systemy kryptograficzne, to ci sami ludzie, którzy je zaprojektowali i w ich najlepszym interesie jest, aby nie znaleźć wady.

Profesjonalni kryptografowie i amatorzy recenzują algorytm z różnych punktów widzenia i jest to pewny sposób na odkrycie, czy algorytm szyfrowania jest godny zaufania. Producenci, którzy nie korzystają z systemu wzajemnej weryfikacji, są zwykle marginalizowani i tracą biznes, ponieważ opinia publiczna im nie ufa. Upublicznienie algorytmu zasługuje na pomoc ze strony świata bezpieczeństwa. Prywatne lub zastrzeżone algorytmy w większości przypadków nie są wystarczająco bezpieczne, ponieważ tylko kilka osób przyczyniło się do ich powstania. Ważne jest jednak, aby stwierdzić, że bezpieczeństwo systemu szyfrowania powinno opierać się na bezpieczeństwie klucza, a nie algorytmu.

6.2.10 Typy kluczy: Klucz symetryczny, Klucz prywatny, Klucz publiczny, Klucz główny, i Klucz sesji

Klucze są nazywane zgodnie z algorytmami, których dotyczą lub celami, do których są używane. Klucze używane w kriptografii symetrycznej są określane jako symetryczne (oznaczane przez K). Algorytmy asymetryczne wykorzystują pary kluczy prywatnych i publicznych (oznaczane odpowiednio jako K_R i K_U).

W przypadku szyfrowania danych masowych najpierw generowany jest klucz symetryczny, a następnie do szyfrowania i deszyfrowania używany jest algorytm symetryczny. Algorytm symetryczny jest preferowany ze względu na większą szybkość szyfrowania i deszyfrowania. Jeśli współdzielony tajny klucz jest używany we wszystkich sesjach, wówczas atakujący ma możliwość wyodrębnienia klucza ze względu na dużą ilość tego samego użycia klucza. Z tego powodu generowany jest klucz symetryczny, w którym pary kluczy prywatnych i publicznych są używane w celu zwiększenia bezpieczeństwa algorytmu.

6.2.11 Zarządzanie kluczami i jego znaczenie

Zaskakujące może być to, że wszystkie schematy uwierzytelniania i podpisu cyfrowego, które zależą od algorytmów "co dana osoba wie", opierają się na jednym haśle. Kompletny schemat bezpieczeństwa można po prostu złamać poprzez niewłaściwe wyodrębnienie hasła przez osoby nieupoważnione. Na przykład, gdy otrzymasz hasło z banku, aby uzyskać dostęp do swojego konta bankowego, wszystkie twoje pieniądze mogą zostać przelane na inne konto przez nieupoważnioną osobę, jeśli będziesz nieostrożny i zanotujesz swoje hasło. Zabezpieczenia warstwowe mają na celu przewyciężenie tego problemu poprzez wprowadzenie dodatkowych punktów uwierzytelniania, ale nie trywializują znaczenia zabezpieczania kluczy lub haseł.

6.2.12 WEP (Wired Equivalent Privacy) i WPA (Wi-Fi Protected Access).

WEP został wprowadzony jako część protokołu 802.11 w 1997 roku w celu zapewnienia poufności, ale doświadczenie pokazało, że jest on podatny na podsłuchiwanie. Zidentyfikowano kilka słabych punktów. Później Wi-Fi Alliance wprowadziło WPA, a następnie WPA2, aby przewyciążyć napotkane problemy.

6.2.13 Inne składniki bezpieczeństwa

(i) Polityka bezpieczeństwa

Polityka bezpieczeństwa zawiera szczegółowe informacje na temat procedur i parametrów konfiguracyjnych organizacji w celu spełnienia wymagań, ewentualnie określonych przez kierownictwo i osoby odpowiedzialne za IT.

(ii) *Firewall*

Firewall jest tradycyjnie używany do blokowania nieautoryzowanego dostępu, jednocześnie umożliwiając autoryzowaną komunikację. Firewall wykorzystuje reguły, aby zdecydować, jak zachować się w przypadku każdego rodzaju żądania komunikacji. Zapory sieciowe mogą być oprogramowaniem zainstalowanym na komputerze lub mogą być zintegrowane ze sprzętem.

(iii) *System wykrywania i zapobiegania włamaniom (IDPS)*

System wykrywania włamań (IDS) to zintegrowane urządzenie lub aplikacja, która monitoruje aktywność sieciową pod kątem złośliwych działań lub naruszeń zasad. IDPS koncentruje się głównie na wykrywaniu możliwych incydentów, rejestrowaniu powiązanych informacji, próbach ich powstrzymania i raportowaniu.

(iv) *Bezpieczeństwo fizyczne*

Bezpieczeństwo fizyczne obejmuje środki mające na celu uniemożliwienie atakującym dostęp do zasobu i składa się z mechanizmów odpornych na złośliwe działania. Przykładami takich mechanizmów są zamki, ogrodzenia, strażnicy, bramki obrotowe.

(v) *Bezpieczny kanał*

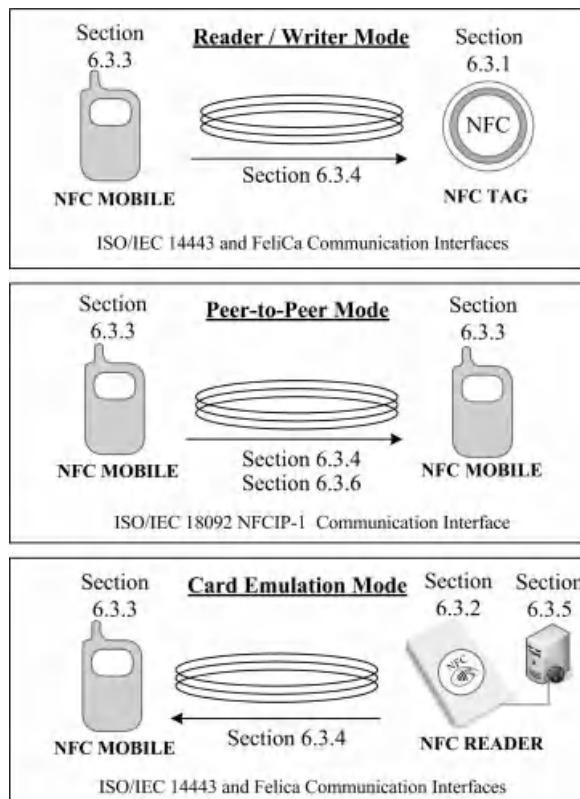
Bezpieczny kanał to medium komunikacyjne między dwiema stronami, dzięki któremu podczas wymiany danych spełnione są wymogi bezpieczeństwa, takie jak tajność i integralność danych. Oczywistą techniką tworzenia bezpiecznego kanału jest użycie środków kryptograficznych. Ustanowienie bezpiecznego kanału między dwoma urządzeniami jest najlepszym podejściem do ochrony przed atakiem. Bezpieczny kanał można zbudować przy użyciu podpisów cyfrowych i infrastruktury klucza publicznego. Secure Sockets Layer (SSL) i jego następca, Transport Layer Security (TLS) to metody używane obecnie do tworzenia bezpiecznych kanałów.

6.3 Bezpieczeństwo NFC Framework

Podobnie jak w przypadku wszystkich systemów informatycznych, systemy oparte na NFC są narażone na ataki, które zagrażają bezpieczeństwu systemu i prywatności użytkownika. Jak omówiono w rozdziale 3, różne tryby pracy NFC wykorzystują różne protokoły komunikacyjne. Niektóre zagrożenia bezpieczeństwa, usługi i mechanizmy są podobne, podczas gdy niektóre kwestie są unikalne dla każdego trybu pracy. Tutaj przeanalizujemy kwestie bezpieczeństwa związane z systemami opartymi na NFC w zależności od ich trybu pracy. Tryb czytnika/zapisu składa się głównie z zagrożeń i usług opartych na strukturze RFID, podczas gdy tryb peer-to-peer jest inny. Tryb emulacji karty obejmuje zagrożenia i usługi podobne do systemów bezstykowych kart inteligentnych, a także inne kwestie związane z trybem pracy.

Gdy systemy oparte na NFC są analizowane z punktu widzenia bezpieczeństwa, komponenty systemu uwzględniające wszystkie trzy tryby pracy można wymienić jako (patrz rysunek 6.9):

- Kwestie bezpieczeństwa związane z tagiem NFC (sekcja 6.3.1);
- Kwestie bezpieczeństwa związane z czytnikiem NFC (sekcja 6.3.2);
- Kwestie bezpieczeństwa związane z kartą inteligentną (sekcja 6.3.3);
- Kwestie bezpieczeństwa związane z komunikacją (sekcja 6.3.4);
- Kwestie bezpieczeństwa związane z oprogramowaniem pośredniczącym i systemami zaplecza (sekcja 6.3.5);



Rysunek 6.9 Ramy bezpieczeństwa NFC.

6.3.1 Kwestie bezpieczeństwa tagów NFC

Dwa urządzenia NFC zaangażowane w tryb czytnika/zapisu to tag NFC po jednej stronie i telefon komórkowy NFC po drugiej. W związku z tym zapewnienie bezpieczeństwa systemu NFC powinno uwzględniać bezpieczeństwo tagu NFC, a także bezpieczeństwo komunikacji między urządzeniami NFC. Należy pamiętać, że tag NFC jest w rzeczywistości tagiem RFID z odpowiednimi obawami dotyczącymi bezpieczeństwa. Dlatego w pierwszej kolejności powinniśmy omówić kwestie bezpieczeństwa i możliwe ataki na pasywne tagi RFID.

6.3.1.1 Atakowanie tagów NFC

W tej sekcji przeanalizujemy tag NFC, gdy znajduje się on w trybie gotowości. Ataki występujące podczas komunikacji między tagiem NFC a telefonem komórkowym NFC zostaną przeanalizowane w sekcji 6.3.4.

Powszechnie ataki na tagi NFC można podzielić na następujące kategorie:

- Klonowanie tagów i podszywanie się pod nie;
- Zmiany zawartości znaczników;
- Zastępowanie i ukrywanie tagów.



Rysunek 6.10 Przykład złośliwego znacznika.

(i) *Klonowanie tagów i podszywanie się pod tagi*

Z punktu widzenia technologii RFID, najtrudniejszymi zagrożeniami bezpieczeństwa w komercyjnych zastosowaniach RFID są klonowanie tagów i podszywanie się pod nie. Społeczność badawcza zajmuje się tymi zagrożeniami głównie poprzez próby utrudnienia klonowania tagów za pomocą kryptograficznych protokołów uwierzytelniania tagów. Podstawowe trudności w tych badaniach dotyczą kompromisów między kosztem tagów, poziomem bezpieczeństwa i wydajnością pod względem szybkości odczytu i odległości. Ochrona pasywnych tagów RFID przed klonowaniem stanowi obecnie wyzwanie.

Klonowanie tagów ma taki sam wpływ jak ataki przekaźnikowe, z tą dużą zaletą dla atakującego, że tag RFID może być ponownie użyty bez konieczności wykorzystywania ofiary do każdego pojedynczego ataku. Należy zauważyć, że atak przekaźnikowy jest wykonywany podczas komunikacji NFC, podczas gdy klonowanie jest wykonywane przed rozpoczęciem komunikacji. Dlatego technicznie łatwiej jest wykonać klonowanie tagów.

(ii) *Zmiany zawartości tagów*

Zawartość tagów może zostać zmieniona przez różne ataki:

- *Ataki typu spoofing*

Atak spoofingowy polega na dostarczeniu użytkownikowi fałszywych informacji, które wydają się prawidłowe. Ataki spoofingowe zazwyczaj obejmują fałszywą nazwę domeny, numer telefonu lub fałszywe informacje dotyczące identyfikacji jakiejś osoby, przedmiotu lub działania [8]. Przykładem spoofingu w systemie RFID jest nadawanie nieprawidłowego elektronicznego kodu produktuTM (EPCTM). Niektóre z możliwych ataków spoofingowych to:

- *URI spoofing*: Zasadniczo atak ten nadużywa inteligentnych plakatów i ukrywa prawdziwe URI, aby wykorzystać słabość GUI telefonów komórkowych. W ten sposób użytkownicy są nakłaniani do wykonywania szkodliwych operacji.
- *Podszywanie się pod adres URL*: Falszywy, niewinnie wyglądający adres URL jest przechowywany na tytule inteligentnego plakatu, podczas gdy rzeczywisty i złośliwy adres URL jest przechowywany w tagu NFC (patrz rysunek 6.10). Użytkownicy zazwyczaj nie zauważają rzeczywistego URI po przeczytaniu tagu. Zakładają, że używany jest adres URL na inteligentnym plakacie.
- *Fałszowanie połączeń telefonicznych*: Fałszywy numer telefonu jest przechowywany w inteligentnym plakacie, podczas gdy numer o podwyższonej opłacie, taki jak 0900xxxxxxxx, jest przechowywany w rekordzie URI. W związku z tym możliwy wpływ ataku jest wysoki. Ten rodzaj ataku jest prawdopodobny, ponieważ atakujący czerpie z niego korzyści finansowe.
- *Fałszowanie wiadomości SMS*: Fałszywy numer telefonu i wiadomość są przechowywane na inteligentnym plakacie, podczas gdy podany jest inny numer

które wiążą się z pewnymi kosztami. Jest to mniej prawdopodobne, ponieważ użytkownik musi potwierdzić wiadomość SMS na czystym ekranie.

- *Manipulowanie danymi znaczników*

W zależności od charakteru etykiety, cena, numer magazynowy i wszelkie inne dane na etykiecie mogą być modyfikowane lub manipulowane. Na przykład, zmieniając dane dotyczące ceny na tagu, haker może uzyskać znaczną zniżkę. Inne zmiany danych na tagu mogą być również wykorzystane do oszukania użytkownika.

- *Atak DOS*

Ataki DoS mogą być wykorzystywane do udaremnenia relacji między klientem a dostawcą usług. Na przykład złośliwy znacznik zawierający zniekształcony komunikat NDEF, który jest używany w usłudze, może spowodować awarię telefonów komórkowych i ponowne uruchomienie za każdym razem, gdy usługa jest używana. Użytkownicy w końcu przestaną korzystać z usługi, aby uniknąć awarii.

(iii) *Zastępowanie i ukrywanie tagów*

Przyklejenie złośliwego tagu na oryginalnym tagu lub zastąpienie oryginalnego tagu złośliwym tagiem wystarczy, aby system działał zgodnie z życzeniem atakującego. W przypadku przyklejenia nowego tagu, możliwe jest wyłączenie starego tagu. Inną metodą ataku na pasywne tagi jest złamanie zabezpieczenia przed zapisem i nadpisanie go złośliwymi danymi.

6.3.1.2 Mechanizmy obronne

Tagi NFC mogą być chronione poprzez podpisywanie ich za pomocą technik podpisu, takich jak szyfrowanie. Jednak tylko podpisanie danych tagu nadal nie zapobiega klonowaniu.

6.3.2 Problemy z bezpieczeństwem czytnika NFC

Czytnik NFC to ważne urządzenie NFC, które umożliwia głównie aplikacje w trybie emulacji karty, składające się z telefonu komórkowego z obsługą NFC po jednej stronie i czytnika po drugiej. Czytnik NFC jest podobny do czytnika RFID, więc kwestie bezpieczeństwa są takie same. Główne metody ataku na czytniki NFC to ich usunięcie lub zniszczenie oraz podszywanie się pod nie [1]:

- *Usuwanie lub zniszczenie czytników NFC:* Podobnie jak w przypadku czytników RFID, czytniki NFC również mogą zostać zniszczone lub usunięte. Czytniki NFC mogą zostać skradzione, zwłaszcza gdy są umieszczone w nienadzorowanych miejscach. Czytnik NFC może zawierać krytyczne informacje, takie jak klucze kryptograficzne, które mogą być celem ataku. Wpływ skradzionego czytnika NFC jest znaczący, ponieważ jego potencjalna manipulacja może umożliwić złośliwym atakującym uzyskanie dostępu nie tylko do telefonów komórkowych z obsługą NFC, ale także do systemu zaplecza, w którym można ułatwić manipulację danymi.
- *Podszywanie się:* Gdy komunikacja NFC jest nieuwierzyteliona, atakujący mogą łatwo podszywać się pod inne osoby.

ataki polegające na podrobieniu tożsamości legalnego czytnika w celu uzyskania poufnych informacji, a także modyfikacji danych na tagach. Wykonalność tych ataków zależy od środków bezpieczeństwa służących do uwierzytelniania czytnika. Na przykład, jeśli dane uwierzytelniające są przechowywane na czytniku, skradziony czytnik może dostarczyć dane uwierzytelniające niezbędne do uzyskania dostępu do tagów RFID i

6.3.3 Kwestie bezpieczeństwa na karcie Smart

Jak już wspomniano, karty inteligentne są zwykle używane jako bezpieczny element (SE) na urządzeniach mobilnych z obsługą NFC. Jak zwykle, mogą istnieć luki w zabezpieczeniach kart inteligentnych urządzeń mobilnych NFC. W tej sekcji opisujemy ataki i środki zaradcze przeprowadzane na kartach inteligentnych. Ataki są analizowane w dwóch grupach: ataki inwazyjne i ataki typu side channel. Ataki, które zostaną tutaj opisane, dotyczą zarówno styczowych, jak i bezstykowych kart inteligentnych.

(i) Ataki inwazyjne

Ataki inwazyjne wymagają fizycznego usunięcia lub zaatakowania mikroprocesora karty intelligentnej. Ataki te zazwyczaj wymagają bardzo drogiego sprzętu, dużej wiedzy specjalistycznej i dużych inwestycji. Środki zaradcze, które można wdrożyć w celu zapobiegania atakom inwazyjnym, obejmują [2]:

- *Projekt:* Projekt układu scalonego może obejmować takie środki zaradcze, jak logika kleju, zaciemniona logika i ukryte magistrale, które utrudniają inżynierię wstępna. Pamięć nieulotna, magistrale i układy logiczne mogą być zakodowane, aby uniemożliwić inżynierię wstępna oprogramowania wbudowanego lub technik projektowania układów scalonych poprzez sondowanie.
- *Cechy krzemu:* Niektóre układy scalone zawierają ekran, który jest dodatkową warstwą metalu nad funkcjonalnymi warstwami metalu, która działa w celu uniemożliwienia wizualnego i fizycznego dostępu do powierzchni chipa. Funkcje tego rodzaju mogą być stosowane na całym chipie lub na określonych wrażliwych częściach chipa.
- *Detektory anomalii:* W kartach inteligentnych występują zazwyczaj różne rodzaje detektorów anomalii. Służą one do wykrywania nietypowych warunków środowiskowych, takich jak zdarzenia w napięciu i zegarze dostarczany do karty. Karta inteligentna zazwyczaj resetuje się lub wykonuje nieskończoną pętlę, dopóki nienormalny stan nie zostanie usunięty.

(ii) Ataki bocznym kanałem

Jedną z metod atakowania kart inteligentnych jest obserwowanie kanału bocznego podczas przetwarzania informacji. Oznacza to, że atakujący stara się uzyskać informacje, obserwując, jak zmienia się charakterystyka karty intelligentnej podczas przetwarzania różnych informacji. Oto kilka przykładów ataków typu side channel [2]:

- *Analiza czasu:* Najprostszą formą analizy kanałów bocznych jest po prostu obserwowanie czasu wykonywania danego procesu i wyciąganie wniosków z tych obserwacji. Czas trwania procesu może być źródłem informacji o przetwarzanych danych. Na przykład; jeśli cyfry osobistego numeru identyfikacyjnego (PIN) są sprawdzane indywidualnie i zwracany jest wynik negatywny w przypadku napotkania nieprawidłowej cyfry, atakujący może wykorzystać długość czasu, aby określić, ile cyfr odgadniętego kodu PIN jest prawidłowych.
- *Prosta analiza kanału bocznego:* Innym sposobem jest obserwacja zużycia energii przez kartę intelligentną w czasie poprzez obserwację zmian napięcia na szeregowo połączonym rezystorze. Ilość zużywanej energii zależy od rodzaju wykonywanej instrukcji i manipulowanych danych.
- *Atak indukujący błąd:* Inną metodą ataku na kartę intelligentną jest próba wprowadzenia błędu podczas jej normalnego funkcjonowania, takiego jak zmiana szyfrogramu utworzonego przez algorytm kryptograficzny. Pozwoliłoby to na uzyskanie informacji o używanym kluczu.

Środki zaradcze, które można wdrożyć w celu zapobiegania atakom typu side channel obejmują:

- *Stale wykonanie:* Algorytmy można zaimplementować w taki sposób, że te same operacje będą wykonywane w tej samej kolejności, niezależnie od używanych danych i wartości kluczy. Uniemożliwia to atakującemu przeprowadzenie analizy czasu i prostej analizy kanału bocznego.
- *Losowe opóźnienia:* Analiza różnicowego kanału bocznego wymaga wykonania tych samych operacji. w tej samej kolejności, niezależnie od wartości danych i kluczy. Funkcje, które nie robią nic poza pętlą przez losowy czas, mogą być zawarte w implementacjach, tak aby atakujący był zobowiązany do synchronizacji przejęć a posteriori.
- *Randomizacja:* Analiza różnicowa kanału bocznego wymaga również, aby istniała korelacja między manipulowanymi danymi a obserwowanym kanałem bocznym. Osiąga się to poprzez manipulowanie danymi w taki sposób, że wartość prezentowana w pamięci jest zawsze maskowana losową wartością. Następnie maska ta jest usuwana na końcu algorytmu w celu uzyskania szyfrogramu.

6.3.4 Kwestie bezpieczeństwa komunikacji na stronie

We wszystkich trybach pracy technologii NFC oczywiste jest, że wykorzystywana jest komunikacja krótkiego zasięgu. Atakujący z ulepszonymi urządzeniami radiowymi mogą komunikować się z bezstykowymi kartami intelligentnymi w promieniu kilku metrów. Dlatego ataki i zagrożenia podczas komunikacji są ważne we wszystkich trybach.

6.3.4.1 Ataki na komunikację

(i) Podsłuchiwanie

W podsłuchiwaniu nieupoważniona osoba używa anteny w celu rejestrowania komunikacji między legalnymi urządzeniami [7]. Bezprzewodowy charakter RFID sprawia, że podsłuch jest jednym z najpoważniejszych zagrożeń. Ten rodzaj ataku może być przeprowadzony zarówno w kierunku od tagu do czytnika, jak i od czytnika do tagu. Sygnał, który zostanie podsłuchany, zależy również od lokalizacji podsłuchującego w odniesieniu do tagu RFID i czytnika, a także od możliwych środków zaradczych zastosowanych w celu pogorszenia sygnału radiowego.

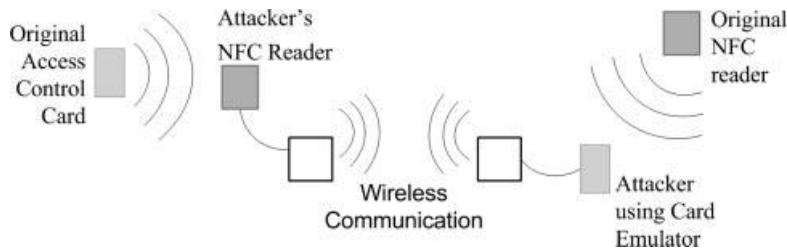
• Zasięg podsłuchu

Komunikacja w NFC zawsze odbywa się między dwoma urządzeniami znajdującymi się w bliskiej odległości. Głównym pytaniem jest to, jak blisko musi znajdować się atakujący, aby odebrać użyteczny sygnał RF. Niestety, nie ma dokładnej odpowiedzi na to pytanie. Powodem tego jest ogromna liczba parametrów, które wpływają na ten problem.

Dodatkowo ważny jest tryb pracy, w którym odbywa się komunikacja. Oznacza to, czy nadawca generuje własne pole RF, czy też korzysta z pola RF generowanego przez inne urządzenie. Znacznie trudniej jest podsłuchiwać urządzenie pasywne, które wykorzystuje pole RF generowane przez urządzenie aktywne. Powód jest oczywisty: aktywne urządzenie generuje sygnał o stosunkowo większym zasięgu.

(ii) Uszkodzenie danych

Atakujący może również próbować modyfikować dane NFC. W najprostszym przypadku atakujący może próbować wygenerować atak DoS, jak wyjaśniono wcześniej.



Rysunek 6.11 Atak przekaźnikowy.

(iii) *Modyfikacja danych*

W przypadku modyfikacji danych atakujący chce zmodyfikować lub usunąć cenne informacje poprzez przechwycenie komunikacji.

(iv) *Wstawianie danych*

Atakujący może również chcieć wstawić jakiś kod do wymienianych danych. Jest to możliwe tylko w przypadku, gdy odpowiadające urządzenie czeka bardzo długo na odpowiedź. Wtedy atakujący może wysłać dane z powrotem do nadawcy wcześniej niż prawidłowy odbiorca. Wstawienie zakończy się sukcesem, jeśli wstawione dane zostaną przesłane, zanim oryginalne urządzenie zacznie odpowiadać. Jeśli oba strumienie danych nałożą się na siebie, dane zostaną uszkodzone.

(v) *Atak MIM*

Atak MIM wykorzystuje wzajemne zaufanie strony trzeciej lub jednoczesne podszywanie się pod obie strony dwukierunkowego zaufania, jak pokazano na rysunku 6.5. Atakujący MIM są nieznanymi stronami w komunikacji, które przekazują informacje tam i z powrotem, sprawiając jednocześnie wrażenie, że są drugą stroną.

Ponieważ RFID i NFC wykorzystują media bezprzewodowe, łatwiej jest przeprowadzić atak MIM, co zmusza osoby odpowiedzialne za bezpieczeństwo do stworzenia silniejszych środków zapobiegawczych. Środki fizyczne i administracyjne są jednym z zestawów opcji, a innym jest rozwiązanie kryptograficzne. Parametry, które należy wziąć pod uwagę w przypadku NFC są następujące:

- Właściwość bliskiego pola komunikacji;
- Generowana moc RF;
- Zasięg do tagu NFC.

(vi) *Atak przekaźnikowy*

Karty zgodne z normą ISO/IEC 14443 są podatne na ataki typu relay. Ofiara jest nieświadoma tego ataku, jeśli nie są przestrzegane odpowiednie środki ostrożności. Rysunek 6.11 przedstawia prostą konfigurację ataku przekaźnikowego. Atakujący wykorzystuje komunikację bezprzewodową, aby pożyczyć dane z tagu ofiary do innego tagu. Oznacza to, że atakujący wstawia wiadomości do danych wymienianych między dwoma urządzeniami. Jest to możliwe tylko wtedy, gdy urządzenie odpowiadające potrzebuje czasu przed wysłaniem żądania, aby działanie przekaźnikowe mogło zostać wykonane w tym czasie. Jeśli oba strumienie danych nakładają się na siebie, dane zostaną uszkodzone.

(vii) *Atak powtórkowy*

Przechwycenie ważnego sygnału NFC, nagranie go w celu późniejszego wykorzystania i przesłanie do czytnika nazywa się atakiem typu replay. Ponieważ dane wyglądają na prawidłowe, czytnik najprawdopodobniej je zaakceptuje. Istnieją pewne mechanizmy zapobiegające atakom typu replay. Przykładem jest użycie numeru sekwencyjnego lub ograniczeń czasowych. Należy pamiętać, że atak typu relay jest przeprowadzany online, podczas gdy atak typu replay jest przeprowadzany offline.

6.3.4.2 Obrona komunikacji

(i) Podsłuchiwanie

Dane przesyłane w trybie pasywnym są znacznie trudniejsze do podsłuchania w porównaniu z trybami aktywnymi. Samo korzystanie z trybu pasywnego prawdopodobnie nie jest wystarczające dla większości aplikacji, które przesyłają wrażliwe dane. Jedynym faktycznym rozwiązaniem zapobiegającym atakowi podsłuchowemu jest ustanowienie bezpiecznego kanału.

(ii) Uszkodzenie danych

Urządzenia NFC mogą przeciwdziałać temu atakowi, ponieważ mogą sprawdzać pole RF podczas przesyłania danych. Urządzenie NFC może łatwo wykryć ten rodzaj ataku, ponieważ wymagana moc do uszkodzenia danych jest znacznie wysoka.

(iii) Modyfikacja danych

Ochronę przed modyfikacją danych można osiągnąć na różne sposoby. Używając 106 kbaud w trybie aktywnym, atakujący nie może zmodyfikować wszystkich danych przesyłanych przez łącze RF. Oznacza to, że w obu kierunkach aktywny tryb komunikacji musi zapobiegać modyfikacji danych. Ponadto ochrona przed modyfikacją nie jest doskonała, ponieważ nawet niektóre bity mogą być modyfikowane przy 106 kbaud.

(iv) Wstawianie danych

Istnieją trzy możliwe środki zaradcze na wstawianie danych. Jednym z nich jest to, że respondent odpowiada bez opóźnienia. W tym przypadku atakujący nie może być szybszy niż prawidłowy respondent. Atakujący może być tak szybki, jak prawidłowe urządzenie, jednak jeśli dwa urządzenia odpowiedzą w tym samym czasie, nie zostaną odebrane prawidłowe dane. Drugim możliwym środkiem zaradczym jest to, że prawidłowy respondent może nasłuchiwać kanału. Wtedy urządzenie może wykryć atakującego, który chce wprowadzić dane. Trzecią opcją jest zbudowanie bezpiecznego kanału między dwoma urządzeniami.

(v) Atak MIM

Aby zapobiec atakowi MIM, aktywna strona powinna nasłuchiwać pola RF podczas wysyłania danych, aby móc wykryć wszelkie zakłócenia spowodowane przez potencjalnego atakującego.

6.3.5 Oprogramowanie pośredniczące i system zaplecza Bezpieczeństwo

Pod względem technicznym system oparty na NFC obejmuje czytniki NFC, telefony

komórkowe NFC i tagi NFC. Jednak kompletny system NFC obejmuje serwery do przechowywania danych i zarządzania nimi, takie jak serwery bankowe, oprogramowanie pośredniczące kart kredytowych, podsystemy uwierzytelniania itp. W związku z tym bezpieczeństwo systemu NFC nie jest kompletne, chyba że zapewnione jest bezpieczeństwo wszystkich komponentów całego systemu. Bezpieczeństwo oprogramowania pośredniczącego i systemów zaplecza nie wchodzi w zakres tej książki. Czytelnik powinien

mieć świadomość, że oprogramowanie pośredniczące i systemy zaplecza powinny być bezpieczne. Bazy danych mogą być niezwykle wrażliwe, jeśli zawierają cenne informacje, takie jak numery kart kredytowych. Firmy mogą nawet stracić zaufanie konsumentów, jeśli nie zapobiegą szkodom lub szybko ich nie naprawią. Istnieje wiele doniesień o firmach, które ucierpiały z powodu poważnych niepowodzeń w postaci utraty klientów z powodu awarii związanego z IT.

6.3.6 Znormalizowane zabezpieczenia NFC Protokoły

Protokoły bezpieczeństwa NFCIP-1 są standaryzowane w ECMA 385 jako NFC-SEC i ECMA 386 jako NFC-SEC-01. Te protokoły bezpieczeństwa są używane w trybie pracy peer-to-peer.

Tabela 6.2 Podsumowanie świadczonych usług bezpieczeństwa [3]

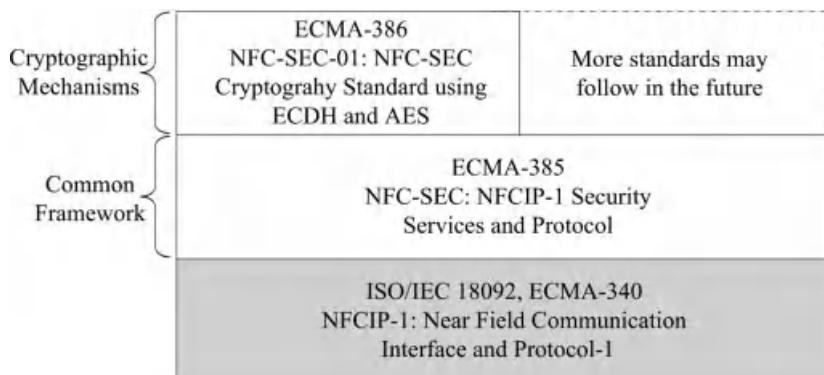
Protokół	Usługi bezpieczeństwa
NFC-SEC	Podsłuch, modyfikacja danych
NFC-SEC-01 SSE	<ul style="list-style-type: none"> - Wymiana klucza z krzywą eliptyczną Diffiego-Hellmana (ECDH) (192 bity) - Tworzenie i potwierdzanie kluczy (AES 128 bitów) SCH - Szyfrowanie danych (AES 128 bitów) - Integralność danych (AES 128 bitów)

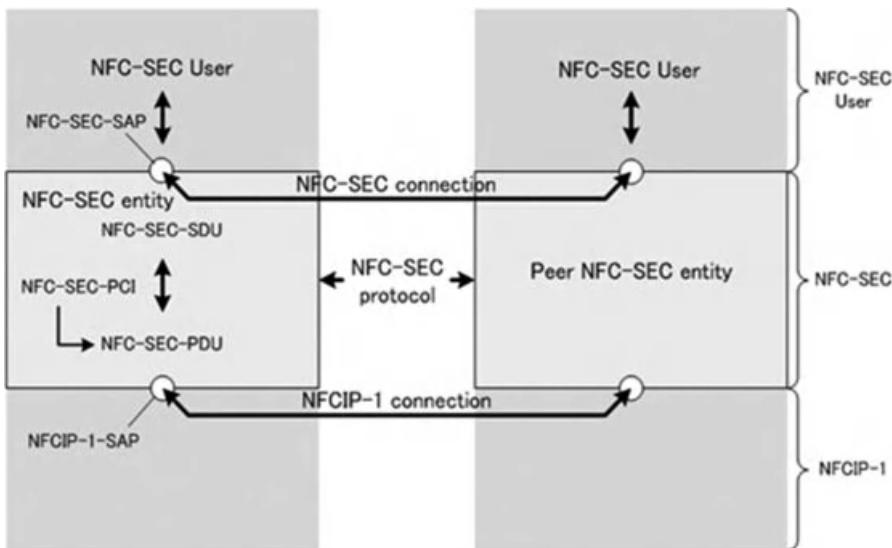
6.3.6.1 NFC-SEC: Usługi i protokół bezpieczeństwa NFCIP-1 - ECMA 385

NFC-SEC zapewnia standard bezpieczeństwa dla komunikacji peer-to-peer NFC, który nie obejmuje trybu czytnika/zapisu i emulacji karty. Należy pamiętać, że zwiększone usługi bezpieczeństwa zawsze zmniejszają wydajność zapewnianą użytkownikowi. Niemniej jednak NFC-SEC zapewnia dobrą równowagę między bezpieczeństwem a wydajnością.

NFCIP-1 nie zapewnia żadnych zabezpieczeń. Na szczytzie NFCIP-1 promowany jest NFC-SEC, aby zapewnić mu możliwości bezpieczeństwa. Protokoły zawarte w NFC-SEC są zdefiniowane tak, aby mogły być używane na protokole NFCIP-1. NFC-SEC definiuje stos protokołów, który umożliwia niezależne od aplikacji funkcje szyfrowania w warstwie łączna danych. Aplikacje korzystające z trybu peer-to-peer nie wymagają specyficznych dla aplikacji mechanizmów szyfrowania dla usług bezpieczeństwa dostarczanych przez komponenty NFC. Przypadek ten jest podobny do korzystania z IPsec i ignorowania usług bezpieczeństwa w wyższych warstwach.

NFC-SEC składa się z dwóch różnych protokołów (patrz Tabela 6.2). Podstawowy NFC-SEC to standard usług i protokołów bezpieczeństwa. Jest on określony w ECMA-385 [3]. Jego główne usługi to ochrona przed podsłuchem i modyfikacją danych. Wspólne ramy są uzupełnione przez ECMA-386 NFC-SEC-01; NFC-SEC Cryptography Standard using ECDH and AES [4]. Określa on mechanizmy kryptograficzne, które wykorzystują protokół ECDH do uzgadniania kluczy i algorytm AES do szyfrowania i integralności danych. W przyszłości może pojawić się więcej standardów kryptograficznych, a każdy z nich ma być identyfikowany przez identyfikator protokołu (PID) (patrz rysunek 6.12).

**Rysunek 6.12** Architektura standardów NFC-SEC [5].



Rysunek 6.13 Architektura NFC-SEC [3].

6.3.6.2 NFC-SEC i jego architektura

Architektura NFC-SEC wykorzystuje model referencyjny OSI określony w ISO/IEC 7498-1 i architekturę bezpieczeństwa ISO 7498-2 (patrz rysunek 6.13). Użytkownicy NFC-SEC wywołują usługi NFC-SEC i uzyskują do nich dostęp za pośrednictwem punktów dostępu do usług NFC-SEC (NFC-SEC-SAP). Podmioty NFC-SEC otrzymują jednostki danych usługi NFC-SEC (NFC-SEC-SDU), które są określone jako żądania od użytkowników NFC-SEC i zwracają im jednostki NFC-SEC-SDU (potwierdzenia). Podmioty NFC-SEC, które są podglądane, wymieniają NFC-SEC-PDU (jednostki danych protokołu) zgodnie z protokołem NFC-SEC. Podmioty NFC-SEC, które są wzajemnie podporządkowane, komunikują się ze sobą, uzyskując dostęp do usługi danych NFCIP-1 za pośrednictwem punktów dostępu do usług NFCIP-1 (NFCIP-1-SAP). Podmioty NFC-SEC mogą wysyłać i odbierać jednostki NFC-SEC-PDU. Typowa jednostka NFC-SEC-PDU zawiera informacje kontrolne protokołu NFC-SEC (NFC-SEC-PCI) i pojedynczą jednostkę NFC-SEC-SDU.

Struktura NFC-SEC-PDU jest pokazana na rysunku 6.14. Obejmuje on protokół bezpiecznej wymiany (SEP), PID i ładunek NFC-SEC.

Tabela 6.3 przedstawia możliwe opcje NFC-SEC-PDU wraz z ich kodami i opisami. Zdefiniowano cztery podstawowe kroki, jak pokazano na rysunku 6.15. Etapy "uzgodnienia klucza", po którym następuje "potwierdzenie klucza", są fazami ustanawiania klucza i są wymagane zarówno dla SSE, jak i SCH. "Zabezpieczenie PDU" zapewnia faktyczne szyfrowanie i ochronę danych, wymagane tylko przez SCH. Wreszcie, zarówno SSE, jak i SCH kończą się etapem protokołu "Zakończenie".

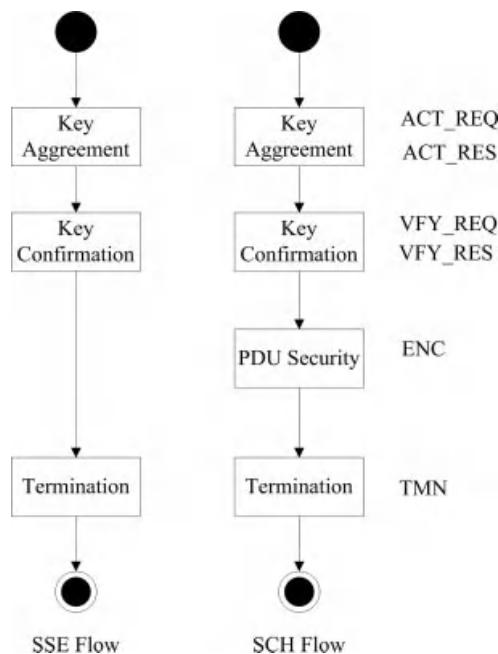


Rysunek 6.14 Struktura PDU NFC-SEC [3].

Tabela 6.3 Typy i opis PDU [3]

NFC-SEC-PDU		
Nazwa	Kod	Opis
ACT_REQ	0000	Żądanie aktywacji w celu zamówienia nowej usługi
ACT_RES	0001	Odpowiedź aktywacyjna na zaakceptowanie żądania usługi
VFY_REQ	0010	Żądanie weryfikacji w celu przesłania wartości kontrolnych dla
VFY_RES	0011	weryfikacja współdzielonego sekretu nadawcy Odpowiedź weryfikacyjna w celu przesłania wartości kontrolnych dla
ENC	0100	weryfikacja współdzielonego hasła odbiorcy Szyfrowanie pakietów w celu bezpiecznej wymiany danych
TMN	0110	Zakończ żądanie zakończenia usługi
BŁĄD	1111	Wskazanie błędu

- *Uzgadnianie klucza:* Podmioty Peered NFC-SEC ustanawiają wspólny klucz tajny przy użyciu ACT_REQ (PDU żądania aktywacji) i ACT_RES (PDU odpowiedzi na aktywację).
- *Potwierdzenie klucza:* Podmioty NFC-SEC weryfikują swój uzgodniony wspólny klucz tajny za pomocą VFY_REQ (PDU żądania weryfikacji) i VFY_RES (PDU odpowiedzi na weryfikację).
- *Bezpieczeństwo PDU:* Podmioty Peered NFC-SEC chronią swoje mechanizmy wymiany danych za pomocą
ENC (zaszyfrowany pakiet PDU). Protokół zapewnia również integralność sekwencji w oparciu o



chronione numery sekwencyjne. Dodatkowo protokół ten zapewnia poufność, integralność danych i uwierzytelnianie pochodzenia.

- **Zakończenie:** Podmioty Peered NFC-SEC mogą zakończyć swoją sesję za pomocą TMN (terminate

PDU). Gdy NFCIP-1 zostanie zwolniony lub odznaczony, lub urządzenie NFC zostanie wyłączone, sesja również zostanie zakończona.

6.3.6.3 Mechanizmy NFC-SEC-01 wykorzystujące ECDH i AES

Aby umożliwić bezpieczną komunikację między urządzeniami NFC, które nie współdzielą żadnych wspólnych tajnych danych, zanim zaczną się ze sobą komunikować, do ustanowienia wspólnego sekretu między tymi urządzeniami wykorzystywana jest kriptografia klucza publicznego, a dokładniej schemat wymiany kluczy ECDH. Ten wspólny sekret jest używany do ustanowienia SSE i SCH.

NFC-SEC-01 jest standaryzowany w ECMA 386, który określa mechanizmy kryptograficzne wykorzystujące protokół ECDH do uzgadniania kluczy oraz algorytm AES do szyfrowania i integralności danych [4]. Standard ECMA 386 określa mechanizmy SSE i SCH, które są zdefiniowane w ECMA 385. NFC-SEC-01 zapewnia głównie następujące funkcje:

- Treść wiadomości z regułami konkatenacji dla kluczy i innych pól;
- Kluczowe prymitywy;
- Wymagania dotyczące liczb losowych;
- Reguły konwersji i transformacji;
- Algorytmy i metody kryptograficzne.

Określone funkcje Key Derivation Function (KDF), potwierdzania klucza, szyfrowania danych i integralności danych są oparte na AES. Poufność danych jest zapewniana przez AES z kluczem o długości 128 bitów w trybie CTR, który jest bezpieczny i odpowiedni dla ograniczonej przepustowości komunikacji, ponieważ nie jest wymagane wypełnianie.

Dwa KDF są określone w ECMA 386. Pierwszy z nich dotyczy SSE, który jest kluczem głównym MKSSE służącym do weryfikacji klucza dla bezpiecznego kanału. Druga funkcja dotyczy SCH, która wprowadza trzy klucze: klucz główny dla SSE (MKSCH); klucz szyfrowania dla SCH (KESCH); oraz klucz ochrony integralności dla SCH (KISCH). Użycie kluczy opisano w tabeli 6.4.

Gdy klucz jest uzyskiwany po procesach KDF, podmioty NFC-SEC sprawdzają, czy rzeczywiście mają ten sam klucz. Aby wykonać ten proces potwierdzenia klucza, każdy podmiot generuje klucz

Tabela 6.4 Podsumowanie użycia kluczy [4]

Klucz	Użycie klucza
MKSSE	Weryfikacja klucza dla bezpiecznego kanału
MKSCHKlucz główny dla SSE używany jako wspólny sekret	przekazywany do wyższej warstwy jako weryfikacja klucza
KESCH	Szyfrowanie pakietów danych przesyłanych przez SCH
KISCH	Zabezpieczenie integralności pakietów danych przesyłanych przez SCH

Tabela 6.5 Protokoły bezpieczeństwa i ich standardy referencyjne [5]

Protokół	Części protokołu	Standardy odniesienia
NFC-SEC	Ramy	ISO/IEC 11770-1
	Model podstawowy	ISO/IEC 7498-1
	Architektura zabezpieczeń	ISO 7498-2
	Konwencje definiowania usług OSI	ISO/IEC 10731
NFC-SEC-01	Specyfikacje ogólne	ISO/IEC 15946-1
	Zarządzanie kluczami przy użyciu techniki asymetrycznej	ISO/IEC 11770-3
	Szyfry 10116	blokowe ISO/IEC 18033-3 i ISO/IEC
	Kryptografia klucza	1363 i FIPS 186-2
	Generowanie bitów liczb losowych	ISO/IEC 18031

(zwanego MacTag), a następnie wysyła go do swojej jednostki równorzędnej. Podmioty weryfikują znacznik potwierdzenia klucza po otrzymaniu klucza.

6.3.6.4 Uwierzytelnianie podmiotów i ataki MIM

Mechanizm ten nie chroni przed atakami MIM, ponieważ nie można zapewnić uwierzytelnienia podmiotu, gdy równorzędne urządzenia NFC nie udostępniają wcześniej żadnego sekretu [4]. Praktyczne ryzyko ataków MIM jest uważane za niskie w docelowych przypadkach użycia ze względu na niewielką odległość roboczą i specyficzne właściwości RF NFC. Użytkownicy powinni być świadomi i uważnie oceniać potencjalną podatność planowanych wdrożeń.

6.3.6.5 Podsumowanie standardów bezpieczeństwa NFC

Protokoły NFC-SEC i NFC-SEC-01 są oparte na niektórych międzynarodowych standardach, jak pokazano w tabeli 6.5.

6.4 Aspekty prywatności, prawne i etyczne

Prywatność to właściwe wykorzystanie informacji. Gdy niektóre informacje są prywatne dla danej osoby, oznacza to, że są one dla niej szczególne. Prywatność jest terminem szerszym niż bezpieczeństwo, co oznacza, że prywatność może zostać naruszona nawet wtedy, gdy spełnionych jest wiele wymogów bezpieczeństwa.

Zastanówmy się przez chwilę nad uwierzytelnianiem. Kiedy ktoś, powiedzmy Alicja, podaje swój numer telefonu Bobowi, zakłada, że Bob zachowa ten numer w tajemnicy. Jednak Bob przekazuje numer telefonu Alicji Lizie bez pytania jej o zgodę. Może to doprowadzić do niezręcznej sytuacji. Powodem jest to, że Alicja może po prostu nie chcieć podać swojego numeru telefonu Lizie. Jest to rzeczywiście bardzo częsty przykład niewłaściwego wykorzystania informacji.

Prywatność ma kilka wymiarów. Jednym z nich jest ochrona danych osobowych, określana jako prywatność informacyjna lub ochrona danych. Jako osoby fizyczne nie chcemy, aby informacje o nas samych były udostępniane innym, nawet jeśli początkowe

ujawnienie odbywa się za naszą zgodą.



Rysunek 6.16 Główne kwestie związane z prywatnością.

zatwierdzenie. Podobnie jest z prywatnymi informacjami, którymi dzielimy się z naszymi bliskimi przyjaciółmi z początkowym ostrzeżeniem: "Powiem ci coś, ale najpierw musisz mi obiecać, że nie powiesz nikomu innemu!".

Ujawnienie niektórych informacji o ludziach może być uważane za naruszenie prywatności w niektórych krajach, ale może być bardziej akceptalne w innych. Prywatność może być również dobrowolnie poświęcana, głównie dla postrzeganych korzyści. Konstytucje lub prawa różnych krajów mają różne poziomy wsparcia w kwestiach prywatności, a także mogą istnieć przepisy ograniczające stopień prywatności ze względu na interes publiczny. Jednym z podstawowych sposobów wspierania prywatności może być zachowanie poufności rozmów prowadzonych przez osoby korzystające z telefonów komórkowych.

Kwestie prywatności można dalej podzielić na cztery kategorie: nieobserwowalność, brak powiązań, pseudonimowość i anonimowość (patrz rysunek 6.16):

- Zgodnie z normą ISO 99, nieobserwowalność to stan, w którym elementy będące przedmiotem zainteresowania są nieodróżnialne od innych elementów będących przedmiotem zainteresowania (np. podmiotów, wiadomości, zdarzeń, działań).
- Zgodnie z normą ISO 99, brak powiązań ma miejsce, gdy dwa lub więcej elementów systemu jest przedmiotem zainteresowania, z perspektywy atakującego, nie są ani bardziej, ani mniej powiązane po obserwacji niż przed uzyskaniem wiedzy przez atakującego.
- Pseudonimowość oznacza nieznane lub niezadeklarowane źródło, które jest stanem pomyłki ukryta tożsamość.
- Zgodnie z normą ISO 99 anonimowość to stan, w którym nie można nikogo zidentyfikować ani zauważyć.

Osoby, które mają bezpośredni lub późniejszy dostęp do prywatnych informacji, mogą nie być godne zaufania; prywatność jest zapewniana za pomocą anonimowości. Korzystanie z pseudo tożsamości, niepowiązanych informacji oraz nieobserwowalnych zachowań i relacji to najczęściej stosowane metody zapewniania anonimowości, a co za tym idzie prywatności.

6.4.1 To jest inny świat

Kilka dekad temu uważano, że świat znajduje się w erze informacji. Obecnie uważa się, że mamy do czynienia z erą zarządzania informacją. Powód tej różnicy jest oczywisty: dane i informacje są obecnie wszędzie. Ważniejsze jest pozyskiwanie użytecznych informacji niż ich tworzenie.

Dane będą zbierane ze wszystkich możliwych punktów przy użyciu wszystkich możliwych czujników i urządzeń zbierających dane. Bezprzewodowe węzły czujników, tagi NFC i kamery to tylko kilka przykładów urządzeń zbierających dane. Kiedy dzwonisz do kogoś lub nawet nosisz telefon komórkowy bez jego używania, nawet kupujesz coś za gotówkę lub klikasz na stronę internetową w przeglądarce, rejestrowana jest ogromna ilość

6.4.2 Kilka przykładów dotyczących prywatności Kwestie

Najprostszym rozwiązaniem fizycznej kontroli dostępu jest zatrudnienie strażników przy drzwiach do wszystkich wrażliwych obszarów. Jednak strażnicy są kosztowni, popełniają błędy i nie lubią prowadzić ścieżek audytu. Wprowadzono karty dostępu w postaci kart z paskiem magnetycznym. Systemy te wykorzystują komputerowy backend, dzięki czemu karty mogą być unieważniane i usuwane z systemu, a tożsamość, lokalizacja i czas są przechowywane. Jednak nielegalnie przechwycone karty z paskiem magnetycznym mogą zostać wykorzystane przez hakera i niestety nielegalny dostęp będzie w tym przypadku łatwiejszy niż przy użyciu strażników. Do rozwiązania tych problemów wykorzystano technologie RFID i zbliżeniowych kart inteligentnych. Karty te są aktywnymi implementacjami RFID, co oznacza, że mają wbudowany

źródło zasilania.

Rozważmy następującą teoretyczną sytuację, która wykorzystuje tagi i narusza prywatność użytkownika. Użytkownik kupuje sweter z tagiem RFID. Po przejściu przez stanowisko kasowe przedmiot jest skanowany, a użytkownik płaci za niego kartą kredytową. Kilka tygodni później zakładasz sweter w tym samym sklepie, w którym go kupiłeś. Pod warunkiem, że tag nadal działa, po wejściu do sklepu czytnik w drzwiach rozpoznaje numer identyfikacyjny i dopasowuje go do imienia i nazwiska oraz informacji o karcie kredytowej.

Istnieją różne przypadki RFID na całym świecie, które podkreślają kwestie bezpieczeństwa i prywatności:

(i) Sprawa Benetton

Jednym z przykładów, który wywołał negatywną reakcję opinii publicznej, była sprawa Benetton, która doprowadziła firmę do wycofania planów osadzania tagów RFID w swoich produktach. W 2003 roku firma Philips ogłosiła, że będzie dostarczać tagi RFID firmie Benetton. Gdy obrońcy prywatności dowiedzieli się o tym planie, wezwali do bojkotu firmy. W obliczu tego publicznego oburzenia, Benetton wycofał się i ogłosił, że poszczególne elementy odzieży nie będą posiadały tagów RFID.

(ii) Metro Group

Metro Group utworzyła eksperymentalny punkt sprzedaży o nazwie Future Store, aby przetestować nowe technologie i koncepcje, w tym technologię RFID. Etykiety RFID zostały dołączone do każdego opakowania produktu. Znaczniki te zawierały unikalny identyfikator, który został zaprogramowany w fabryce podczas fazy produkcji. Czytniki przymocowane do półek monitorowały aktualną ilość produktów dla każdej marki.

Aby zaspokoić obawy dotyczące prywatności, sklep udostępnił kioski dezaktywacyjne do dezaktywacji tagów, gdy klient chciał to zrobić przed zakupem produktu. Firma dołączyła tagi RFID do swoich kart lojalnościowych, ale nie poinformowała o tym klientów. Doprowadziło to do protestów, a następnie Metro Group zaprzestała stosowania tagów RFID na kartach lojalnościowych. Metro Group kontynuuje swoją inicjatywę Future Store, ale zajmuje się kwestiami prywatności w znacznie większym stopniu.

(iii) Wal-Mart

Wal-Mart to duża sieć handlowa, która chciała zachęcić swoich dostawców do zintegrowania RFID z ich łańcuchami dostaw. Celem było automatyczne skanowanie palet z towarami, gdy wchodzą one lub wychodzą z magazynu, oszczędzając w ten sposób czas i inne zasoby.

(iv) Paszporty RFID

Tagi RFID zaczęły być wykorzystywane w nowych paszportach do celów

prywatności NFC twierzytelniania i integralności. Hasło z obsługą RFID jest również jednym z przypadków użycia technologii NFC. Kwestie bezpieczeństwa i prywatności związane z paszportami RFID istnieją również w przypadku haseł z obsługą NFC.

Wiele krajów, w tym USA, Turcja i niektóre inne kraje europejskie, faktycznie wdrożyły te znaczniki w ostatnich latach. Tagi RFID w paszportach są wykorzystywane do aktualizacji zabezpieczeń i ochrony przed fałszerstwami. Jednak ten dodatek do paszportów wywołał ogromną debatę wśród ekspertów ds. bezpieczeństwa i prywatności oraz zwolenników bezpieczeństwa narodowego. Nowy projekt paszportu integruje znacznik RFID w paszporcie zgodnie ze specyfikacjami formatu ISO 14443A i 14443B. Paszporty są czytelne w promieniu 10 cm, a znacznik zawiera identyczną kopię informacji, które są już wydrukowane w paszporcie, w tym zdjęcie i inne informacje biometryczne, takie jak odciski palców i podpisy. Dzięki temu dodatkowi zmiana skradzionego lub zgubionego paszportu stała się znacznie bardziej trudna. Chip przechowuje informacje biometryczne danej osoby, co zwiększa możliwości straży granicznej i organów wydających paszporty.

agencje, aby potwierdzić czyjś paszport.

Jedną z głównych obaw związanych z paszportami RFID jest skimming, czyli możliwość odczytywania informacji zawartych w paszporcie. Istnieje obawa, że przestępcy będą w stanie wyłowić konkretne osoby z tłumu i potencjalnie namierzyć je w celu porwania lub rabunku.

Nawet jeśli informacje są zaszyfrowane, paszport może zostać zidentyfikowany zgodnie z krajem, który go wydał. Aby zapobiec problemom, gdy więcej niż jeden tag znajduje się w zasięgu czytnika, każdy tag posiada identyfikator antykolizyjny. Ten unikalny identyfikator pozwala czytnikowi odróżnić jeden tag od drugiego. RFID w paszportach rozwiązuje również problem zgodności z normami i kwestię polityczną dotyczącą postrzeganej potrzeby zwiększenia bezpieczeństwa paszportów. Należy zachować szczególną ostrożność, gdy urządzenie zabezpieczające jest używane w czymś tak ważnym jak paszport.

6.4.3 Podsumowanie dotyczące prywatności i środków zaradczych

Istnieją pewne problemy związane z technologią RFID, a także przesadzone i wprowadzające w błąd informacje. Wiele informacji dotyczących RFID zostało opublikowanych w odniesieniu do jej potencjalnych możliwości tajnego śledzenia. Te spekulacje i błędne informacje sprawiły, że ludzie są nieufni wobec RFID.

Trudno jest ocenić, jak powszechnie są obawy konsumentów. Niewielka liczba konsumentów, którzy pasjonują się konkretną kwestią, może mieć duży głos. Nawet niewielka liczba osób, których obawy nie zostały rozwiązane w zadowalający sposób, może doprowadzić do zatrzymania inicjatywy RFID. Z poprzednich przykładów można wyciągnąć następujące wnioski:

- Pierwszym krokiem jest zrozumienie punktu widzenia konsumentów w odniesieniu do tagów RFID. Spróbuj uzyskać informacje zwrotne od konsumentów.
- Zademonstrowanie kroków podejmowanych w celu ochrony prywatności konsumentów i zapewnienia kontroli nad w ręce konsumentów. Upewnij się, że wiadomość dotrze do odbiorców.

6.4.4 Niektóre propozycje dotyczące zapewnienia prywatności w tagach

Tutaj przedstawimy niektóre mechanizmy prywatności dotyczące korzystania z tagów NFC.

(i) Wyłącznik awaryjny

Zawartość tagów NFC może zostać wyczyszczona, przez co nie będzie można z nich korzystać. Problem pojawi się, gdy dane na tagach NFC są wymagane po opuszczeniu

~~prywatność NFC~~ Sklep: Jeśli klient z jakiegoś powodu chce zwrócić przedmiot do sklepu, dobrze byłoby, gdyby tag był nadal czytelny. Niektóre potencjalne problemy [6] to:

- Sklepy mogą chcieć, aby produkty miały czytelne etykiety na wypadek, gdyby zostały zwrócone jako wadliwe.
- Produkty mogą wymagać odczytu, aby można je było skategoryzować do celów recyklingu po pewnym okresie użytkowania produktu przez klienta.
- Sklepy mogą wydawać paragony z wbudowanymi tagami, aby móc potwierdzić szczegóły zakupu, gdy produkt zostanie zwrócony.
- Przedmioty kolekcjonerskie, takie jak karty baseballowe i płyty CD, mogą mieć tagi RFID, aby umożliwić właścicielom lepsze zarządzanie zapasami.
- Półka w lodówce lub spiżarni może być w stanie stwierdzić, kiedy upłynął termin ważności jakiegoś produktu spożywczego lub leku.

(ii) *Podejście klatki Faradaya*

Tag NFC może być chroniony za pomocą pojemnika wykonanego z metalu, który jest nieprzenikalny dla sygnałów radiowych; nazywa się to klatką Faradaya.

(iii) *Aktywne zagłuszanie*

Klient może mieć przy sobie urządzenie emitujące sygnały radiowe. Może ono blokować lub zakłócać działanie pobliskich czytników RFID. Jest to kosztowne rozwiązanie.

(iv) *Inteligentne podejście RFID*

Tagi NFC mogą być inteligentniejsze dzięki motywacji do ochrony prywatności. Wymagałoby to oczywiście zastosowania metod kryptograficznych i wiązałoby się z wyższymi kosztami niż w przypadku zwykłych tagów. Zaproponowano trzy przypadki inteligentnych tagów:

- Metoda blokady Hash;
- Metoda ponownego szyfrowania (w kilku formach);
- Ciche chodzenie po drzewach.

6.4.5 Co zrobić, aby chronić prywatność

Społeczeństwo konfrontuje się z systemami RFID, ponieważ wykorzystują one stosunkowo nową i nieznaną technologię, której funkcjonalność, ograniczenia i ryzyko nie są w pełni zrozumiałe. Podobnie jak w przypadku innych nowych technologii, RFID spotyka się ze strachem i odrzuceniem.

Korzystanie z technologii RFID wywołuje poważne zastrzeżenia ze strony obrońców prywatności konsumentów. Dotyczy to w szczególności sytuacji, w których właściciel przedmiotu nie jest informowany o istnieniu tagu, który może zostać odczytany na odległość w sposób niezauważony. Istnieje możliwość wycieku wrażliwych danych, jeśli dana osoba nie posiada odpowiedniej wiedzy.

W przypadku NFC, przy powszechnym korzystaniu z telefonów komórkowych NFC i aplikacji NFC, gromadzenie danych, a także przechowywanie cennych danych prywatnych (np. informacje o karcie kredytowej, informacje o tożsamości, dane dostępu) wzrośnie. Dla konsumenta bardziej skomplikowane stanie się zarządzanie i nadzorowanie gromadzonych i przechowywanych danych. W związku z tym prywatność nabiera szczególnego znaczenia.

Użytkownicy aplikacji NFC powinni być przekonani, że aplikacje te nie będą nadużywać ich danych osobowych i prywatności. Aby osiągnąć zaufanie użytkowników, istnieje wyraźna potrzeba skutecznych narzędzi, które wspierają użytkowników w ochronie ich prywatności. Wymagane może być również wspieranie przepisów dotyczących ochrony danych, innych pomiarów prawnych i mechanizmów audytu.

6.5 Rozdział Podsumowanie

NFC nie tylko stwarza nowe luki w zabezpieczeniach, ale także prowadzi do obaw o

prywatność użytkowników. Rozważmy przypadek, w którym osobiste dane zdrowotne są zapisywane na serwerach szpitalnych, dzięki czemu

Informacje te mogą być wykorzystywane zarówno przez zarząd szpitala, jak i firmy ubezpieczeniowe. Być może otrzymałeś powiadomienia od swojej firmy ubezpieczeniowej, informujące o anulowaniu części polisy z powodu jakiejś choroby, której doświadczyłeś. Sytuacja ta jest zdecydowanie korzystna dla firm ubezpieczeniowych. Jeśli dane zdrowotne mają być przechowywane w lokalnej bazie danych na osobistym telefonie komórkowym z obsługą NFC i mają być usuwane ze szpitalnej bazy danych, obawy o prywatność użytkownika mogą być bardziej zaspokojone.

NFC jest nową, rozwijającą się branżą i jest wiele do zrobienia w tej dziedzinie. Istnieje potrzeba wysoce znormalizowanych, interoperacyjnych mechanizmów na całym świecie. Ponieważ NFC jest technologią komunikacji bezprzewodowej i wiąże się z przechowywaniem i wymianą prywatnych i ważnych danych, kwestie bezpieczeństwa i prywatności muszą być jasno określone.

Rozdział Pytania

1. Wyjaśnij poufność, integralność danych, uwierzytelnianie i autoryzację.
2. Dlaczego idealne bezpieczeństwo nie jest możliwe?
3. Dlaczego hakerzy są o krok do przodu?
4. Dlaczego złożoność osłabia bezpieczeństwo?
5. Jak można zastosować atak typu pharming na użytkownika? Podaj dwa przykłady.
6. Wyjaśnij podatność, zagrożenie, atak i ryzyko, podając przykład.
7. Jakie są różnice między zabezpieczeniami kryptografii symetrycznej i asymetrycznej?
8. Wyjaśnij ataki klonowania tagów na tagi NFC, podając przykłady.
9. Czym jest atak podsłuchowy w kontekście bezpieczeństwa NFC?
10. Czym jest atak typu man in the middle w kontekście bezpieczeństwa NFC?
11. Jaka jest różnica między atakami typu relay i replay?
12. Czym są protokoły NFC-SEC i NFC-SEC-01? Wyjaśnij usługi bezpieczeństwa zapewniane przez te protokoły.
13. Jakie są główne obawy dotyczące prywatności, które należy uwzględnić przy projektowaniu aplikacji NFC?

Referencje

- [1] Mitrokotsa, A. et al. (2009) Classification of RFID attacks. *Information Systems Frontiers*, **12**(5), 491-505
- [2] Leng, X. (2009) Smart card applications and security. *Information Security Technical Report*, **14**(2), 36-45
- [3] ECMA International (2010) *ECMA 385: NFC-SEC: NFCIP-1 Security Services and Protocol*, czerwiec 2010 r., <http://www.ecma-international.org/memento/TC47-M.htm> (dostęp 10 lipca 2011 r.).
- [4] ECMA International (2010) *ECMA 386: NFC-SEC-01: NFC-SEC Cryptographic Standard using ECDH and AES*, czerwiec 2010 r., <http://www.ecma-international.org/memento/TC47-M.htm> (dostęp: 10 lipca 2011 r.).
- [5] ECMA International (2008) *NFC-SEC*, Biała Księga, grudzień 2008. Dostępna pod adresem: <http://www.ecma-international.org/activities/Communications/tc47-2008-089.pdf> (dostęp 10 lipca 2011 r.).
- [6] Juels, A. et al. *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*. Dostępny pod adresem: <http://citeseex.ist.psu.edu/viewdoc/download?doi=10.1.1.1.7036&rep=rep1&type=pdf> (dostęp 10 lipca 2011).
- [7] Haselsteiner, E. i Breitfuß, K. *Security in Near Field Communication (NFC)*, Philips Semiconductors, dostępne pod adresem: <http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf> (dostęp 10 lipca 2011 r.).
- [8] Mulliner, C. (2008) *Attacking NFC Mobile Phones*, EUSecWest 2008. Dostępny pod adresem: http://www.mulliner.org/nfc/feed/collin_mulliner_eusecwest08_attacking_nfc_phones.pdf (dostęp 10 lipca 2011).

7

Ekosystem biznesowy NFC

Niniejszy rozdział ma na celu ustanowienie solidnych podstaw dla biznesowego aspektu NFC. Faktem jest, że badania w literaturze NFC są rzadkie, a terminologia używana do dyskusji na tematy biznesowe jest obecnie zbyt niedojrzała. Istnieje potrzeba wyjaśnienia podstawowych pojęć charakteryzujących NFC i jej środowisko biznesowe. W tym rozdziale wyartykułowało te charakterystyczne pojęcia i opracowano koncepcyjną podstawę dla NFC w kontekście ekosystemu.

Po pierwsze, niniejszy rozdział poszukuje odpowiedzi na pytania "Co oznacza ekosystem w ogóle?" i "Co oznacza ekosystem w kontekście NFC?". Następnie przeprowadzono kompleksową analizę środowiska biznesowego NFC. Dominujący interesariusze, obowiązki i ogólne role, które mogą służyć jako punkt odniesienia do prezentacji modeli biznesowych, są badane z uwzględnieniem punktów widzenia różnych stowarzyszeń.

Rozwój modelu biznesowego zasługuje na dogłębną dyskusję w zakresie czynników i wyzwań biznesowych, krytycznych kwestii wpływających na modelowanie biznesowe oraz realnych scenariuszy biznesowych z względem w branżę. Niniejszy rozdział ma na celu przedstawienie głównych czynników napędzających modele biznesowe, zaproponowanie trzech alternatywnych modeli biznesowych oraz wyjaśnienie, w jaki sposób i dlaczego systemy oparte na NFC są złożone. Pod koniec tego rozdziału przeanalizowano również przypadek użycia biletów NFC omówiony w rozdziale 4 z perspektywy ekosystemu, a także przedstawiono propozycję modelu biznesowego od jednego z pionierów branży.

7.1 Ekosystem biznesowy

Pojęcie ekosystemu jest zakorzenione w różnych naukach, takich jak biologia, socjologia, zarządzanie i ekonomia. Można nadać mu znaczenie jako społeczności żywych organizmów na określonym obszarze z powietrzem, wodą, światłem słonecznym i innymi zasobami. W rzeczywistości definicja ta opisuje ekosystem w kontekście biologicznym. W zależności od kontekstu, w którym ekosystem jest używany, w literaturze wprowadzono kilka definicji i wyrażeń. Niektóre z przedstawionych tutaj przykładów i koncepcji ekosystemów zostały omówione wcześniej [1-3].

Na przykład ekosystem przemysłowy jest proponowany w celu podkreślenia znaczenia zrównoważonego rozwoju we wszystkich rodzajach działalności przemysłowej. Innym przykładem jest ekosystem społeczny, który jest definiowany jako "każda organizacja jest w pełni uczestniczącą stroną, która zarówno wpływa, jak i jest pod wpływem ekosystemu społecznego składającego się ze wszystkich powiązanych firm, konsumentów i konsumentów".

© 2012 John Wiley & Sons, Ltd. Opublikowano 2012 przez John Wiley & Sons, Ltd.

dostawców, a także instytucji gospodarczych, kulturalnych i prawnych" [1]. W rzeczywistości współprzeźność między podmiotami jest podkreślana w [1] jako jedna z głównych cech ekosystemu społecznego.

Naszym ostatnim przykładem jest ekosystem biznesowy, który jest zasadniczo centralnym punktem tego rozdziału. Różni autorzy mają wiele sugestii i określeń dotyczących ekosystemu biznesowego. Można go po prostu zidentyfikować jako środowisko współdziałających organizacji i jednostek. Zgodnie z sugestiami Jamesa F. Moore'a, ekosystem biznesowy obejmuje klientów, wiodących producentów, konkurentów i innych interesariuszy [2]. Kluczowymi podmiotami ekosystemu biznesowego są wiodące firmy, które są "kluczowymi gatunkami" i mają silny wpływ na procesy współewolucyjne.

Moore opisuje cykl życia ekosystemu biznesowego w czterech etapach: narodziny, ekspansja, przywództwo i samoodnowienie lub śmierć. Na etapie narodzin ekosystem biznesowy musi zrobić coś więcej niż tylko spełnić oczekiwania klientów. Na etapie ekspansji testowany jest potencjał skalowania koncepcji biznesowej. Na etapie przywództwa ekosystem biznesowy osiąga stabilność i wysoką rentowność. Ostatni etap jest spowodowany zagrożeniem ze strony powstających nowych ekosystemów. Inną ważną kwestią wskazaną przez Moore'a jest to, że główną różnicą między systemami ekologicznymi i społecznymi jest rola świadomego wyboru. W systemach ekologicznych zwierzęta mogą wybierać swoje siedliska, partnerów i zachowania. W systemach ekonomicznych decydenci, menedżerowie i inwestorzy spędzają dużo czasu na zrozumieniu sytuacji, podejmowaniu decyzji i rozważaniu możliwych wyników różnych wyborów.

Z drugiej strony, ekosystem biznesowy może być również oceniany z perspektywy środowiska biologicznego. Rozważmy dogłębnie ekosystem biologiczny, w którym każdy gatunek odgrywa ważną rolę. Jeśli nastąpi znacząca zmiana w ilości któregokolwiek gatunku, ekosystem może doświadczyć poważnych problemów. Aby wszystkie gatunki żyły w harmonii, gdy nowe gatunki wchodzą do ekosystemu, muszą dostosować się do warunków fizycznych panujących w środowisku. Co więcej, środowisko musi mieć odpowiedni rodzaj i wystarczającą ilość pożywienia dla wszystkich istniejących gatunków, aby mogły one rosnąć i rozmnażać się w ekosystemie. Inną ważną kwestią jest to, że liczba zgonów nie powinna przekraczać liczby narodzin w dłuższej perspektywie, w przeciwnym razie może to doprowadzić do eliminacji gatunku. Jest to konieczne dla przetrwania ekosystemu. Gdy liczba zgonów przewyższa liczbę narodzin, gatunki w ekosystemie z czasem zaczynają się wyczerpywać. Może się to również zdarzyć, gdy nowy gatunek wejdzie do ekosystemu; nowy gatunek może zacząć zjadąć niektóre gatunki w niekontrolowany sposób. Krótko mówiąc, równowaga w ekosystemie zostaje naruszona, a jeśli ekosystem jest zdrowy, wszystkie gatunki mogą się rozwijać; jeśli ekosystem jest niezdrowy, wszystkie gatunki głęboko cierpią.

Podobnie, w ekosystemie biznesowym wszystkie uczestniczące podmioty muszą dostosować się do sytuacji i okoliczności rynkowych. Podmioty, które nie potrafią się dostosować i nie radzą sobie z konkurencją, są wykluczane z ekosystemu w krótkim okresie. Ponadto podmioty zaangażowane w ekosystem muszą produkować z pomocą dostawców zasobów i stale dostarczać wartość klientom. Konkurencja między istniejącymi podmiotami musi być kontynuowana, gdy nowi partnerzy lub podmioty wchodzą do ekosystemu biznesowego. Ekosystem biznesowy może być również bardziej doceniany i realizowany z perspektywy ekosystemu biologicznego.

Inne badanie koncentruje się na krytycznych czynnikach sukcesu ekosystemu biznesowego, które mogą również zapewnić przydatne zrozumienie dla ekosystemu biznesowego NFC. Pierwszym czynnikiem jest produktywność, która jest bardzo podstawowym czynnikiem i definiuje sukces każdego rodzaju działalności. W kontekście NFC można to określić jako udane wdrożenie technologii i aplikacji NFC, ponieważ będzie to oznaczało

wyjaśnione później. Drugim czynnikiem jest odporność ekosystemu biznesowego. Odporność w naturalnym ekosystemie wyraża zdolność do przetrwania, gdy wstrząsy z wewnątrz lub z zewnątrz ekosystemu grożą (np. bezprecedensowe ruchy na rynku NFC lub wprowadzenie lepszych technologii na rynek), aby go zniszczyć. W rzeczywistości solidność w życiu biznesowym oznacza czerpanie przewagi konkurencyjnej z wielu źródeł i zdolność do adaptacji, gdy zmienia się środowisko. Wreszcie, ekosystem biznesowy powinien mieć zdolność do tworzenia nisz i możliwości dla nowych firm (np. organ transportowy odgrywający rolę zaufanego menedżera usług (TSM) jako neutralną kluczową rolę). Wymaga to zmiany nastawienia interesariuszy i innych uczestników ekosystemu z protekcjonistycznego na nastawione na współpracę.

7.1.1 Ogólne cechy ekosystemu biznesowego

Zgodnie z [1-3] przedstawiono niektóre główne cechy typowego ekosystemu biznesowego. Wykazano, że ekosystem biznesowy rozwija się poprzez złożoność, samoorganizację, wyłanianie się, współevolucję i adaptację, które są również istotne w przypadku ekosystemu biznesowego NFC. Terminy te zostały pokrótko wyjaśnione poniżej:

- *Złożoność*: Ekosystem biznesowy sam w sobie jest złożonym środowiskiem. Złożoność może być definiowana z różnych perspektyw. Według [1] złożony system to taki, którego właściwości nie są w pełni wyjaśnione przez zrozumienie jego części. Zrozumienie dynamiki ekosystemu biznesowego, wymagań, uczestniczących podmiotów i ich ról w ekosystemie jest naprawdę złożoną kwestią, którą należy się zająć.
- *Samoorganizacja*: Samoorganizacja jest procesem, w którym "powstają nowe struktury lub cechy".
w systemie bez interwencji zewnętrznego lub wewnętrznego kontrolera". Samoorganizacja jest procesem ciągłym, ponieważ nigdy nie zakończy się ostatecznym rezultatem. To "ja" się organizuje. Brak zewnętrznego lub wewnętrznego kontrolera jest kluczem do samoorganizacji. Tworzenie ekosystemu biznesowego jest procesem, w którym uczestnicy gromadzą się dobrowolnie i bez zewnętrznego lub wewnętrznego lidera. Cele są ustalane w lokalnych interakcjach, gdzie organizacje negocują i tworzą nowy porządek.
- *Pojawienie się*: Zgodnie z [1, 3], emergencja jest procesem, który tworzy nowy porządek wraz z samoorganizacją. Potencjał do tworzenia nowego porządku jest najważniejszą cechą złożonych, ewoluujących systemów. Pojawienie się jest również identyfikowane jako "mechanizm generujący niespodzianki zależny od łączności" przez Casti [3]. Ważne jest, aby pamiętać, że ekosystem biznesowy jest zawsze czymś więcej niż sumą jego części. Oznacza to, że wynik interakcji między różnymi jednostkami jest czymś, czego nie może wytworzyć tylko jeden podmiot.
- *Współevolucja*: Koewolucja w ekosystemach biznesowych może być opisana jako ewolucja jednego ekosystemu w drugi.
firma wpływająca na rozwój innych firm. Po prostu są to wzajemne zmiany organizacji zaangażowanych w ekosystem. Weźmy na przykład branżę NFC. Kiedy producenci chipów NFC produkują bardziej wydajne chipy, producenci czytników NFC szybko wykorzystują nowe możliwości. Strategiczne ruchy firmy wpływają na ruchy i postawy innych firm na rynku.
- *Adaptacja*: Ekosystem biznesowy powinien również dostosowywać się do zewnętrznych zmian środowiskowych
i ograniczenia, na przykład ograniczenia rządowe i prawne dotyczące procedur płatności mobilnych z obsługą NFC. Kiedy zmienia się środowisko, ekosystem biznesowy

dostosowuje się do zmienionych warunków poprzez wyłamanie się, ~~zasięgu~~, współewolucję i samoorganizację.

7.1.2 *Ekosystem biznesowy NFC*

Z punktu widzenia ekosystemu, branża NFC to nowe, wschodzące środowisko biznesowe i duży łańcuch wartości obejmujący kilka branż i organizacji. Główne branże, które odgrywają ważną rolę w ekosystemie NFC, to operatorzy sieci komórkowych (MNO), firmy bankowe i płatnicze, półprzewodniki i urządzenia elektroniczne, w tym producenci telefonów komórkowych, twórcy oprogramowania i inni handlowcy, w tym operatorzy transportu i sprzedawcy detaliczni. Potencjał technologii NFC w zakresie możliwości biznesowych (zwłaszcza w branży mobilnych usług finansowych) wywarł wrażenie na wielu organizacjach. Ponieważ technologia NFC składa się z kilku komponentów, przekracza granice wielu organizacji z różnych sektorów biznesowych. Wszystkie strony zgodziły się już, że technologia NFC nie może być dostarczona przez jedną firmę, która mogłaby opracować całą technologię, w tym wymagania infrastrukturalne i usługowe. NFC Forum, zrzeszające obecnie ponad 900 członków, jest jedną z głównych organizacji na świecie, której celem jest koordynacja wszystkich uczestniczących instytucji w rozwoju projektów opartych na NFC poprzez oferowanie interoperacyjnych specyfikacji technologicznych. Według uczestników i obserwatorów technologii, start NFC był wolniejszy niż oczekiwano. Głównym powodem tego powolnego startu jest brak wspólnego zrozumienia i wizji technologii NFC wśród uczestniczących organizacji i branż. W związku z tym nie udało się jeszcze stworzyć wzajemnie korzystnego modelu biznesowego. Główne przyczyny tego braku

Wspólne zrozumienie i wizja zostały podsumowane poniżej:

- Zysk, który zostanie podzielony, jest ogromny.
- Uczestniczące organizacje są potężnymi firmami, dlatego uważają, że wszystkie inne strony musi podążyć za ich potrzebami.
- Dla każdej usługi obsługującej NFC istnieją różne rozwiązania techniczne i infrastruktury. Stąd, Każdy podmiot może zaproponować inny model, który przyniesie mu więcej korzyści niż inne. Na przykład operatorzy sieci komórkowych proponują modele oparte na kartach SIM, ponieważ mogą kontrolować karty UICC, a zatem mogą uzyskać większe zyski, jeśli ten model jest używany.

Aby osiągnąć dobry model biznesowy, niezbędna jest interoperacyjność, kompatybilność i standaryzacja przyjętego modelu technologii NFC. Ważne jest również, aby stymulować współpracę partnerów w ekosystemie, a także umożliwić akceptację klientów. Obecnie wykonuje się ogólną pracę nad organizacją wkładu i interesów wszystkich podmiotów oraz lepszym zarządzaniem całym ekosystemem.

Niniejszy rozdział w zwięzły sposób omówi interesariuszy ekosystemu biznesowego NFC oraz modele biznesowe. Będzie to korzystne dla czytelnika, aby zobaczyć szerszy obraz i zrozumieć złożoność technologii w międzyczasie.

7.2 **Interesariusze w ekosystemie NFC**

NFC ma szeroką gamę interesariuszy lub podmiotów, w zależności od rodzaju świadczonych usług, takich jak inteligentne plakaty, płatności, sprzedaż biletów itp. Rodzaj usługi obsługiwanej przez NFC określa złożoność pod względem stosowanego modelu biznesowego, zaangażowanych interesariuszy, odpowiedniego modelu współpracy, modelu przychodów między graczami i tak dalej. NFC to nowa technologia i konieczne jest wykonanie czegoś więcej niż tylko uzasadnienie potrzeb i oczekiwania klientów.



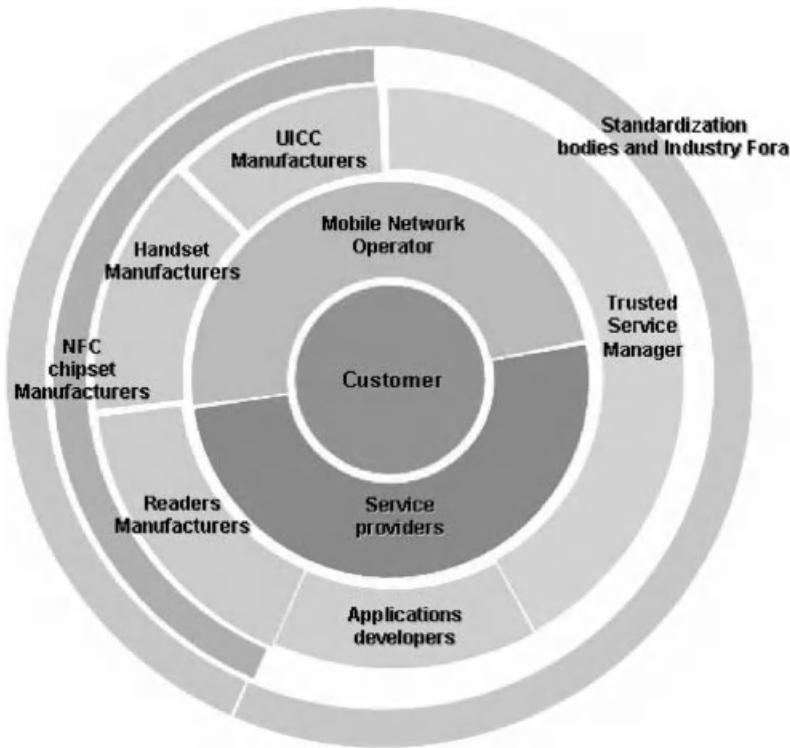
Rysunek 7.1 Widok ekosystemu NFC według NFC Forum. Powielono za zgodą NFC Forum.

Obecnie mobilne usługi finansowe stanowią najbardziej obiecujące możliwości w kontekście NFC. Mają one również największą złożoność zarówno pod względem technologicznym, jak i biznesowym w odniesieniu do innych usług NFC, takich jak inteligentne usługi plakatowe, sieci społecznościowe, gry itp. Organizacje standaryzacyjne definiują różne spojrzenia na ekosystem NFC. Przedstawiamy dwa przykłady tych poglądów. NFC Forum identyfikuje ekosystem NFC w zależności od i w odniesieniu do portfolio swoich członków (patrz rysunek 7.1). Z drugiej strony GSMA opisuje i wizualizuje ekosystem z subiektywnego punktu widzenia MNO (patrz rysunek 7.2). Jednak kluczowi gracze w ekosystemie NFC są w większości tacy sami w obu modelach.

W zależności od różnych podejść przedstawionych przez organizacje, niniejsza sekcja analizuje i identyfikuje głównych interesariuszy (patrz rysunek 7.3), ich role i obowiązki, aby dać wgląd w branżę NFC.

7.2.1 *Organy normalizacyjne i inni uczestnicy*

Jak już wspomniano w rozdziale 3, w ekosystemie NFC istnieją różne organy normalizacyjne i organizacje o stosunkowo różnych misjach, celach biznesowych i interesach, takie jak NFC Forum, GlobalPlatform, GSMA i EMVCo. Niektóre z tych celów biznesowych pokrywają się ze sobą, ale istnieje również wiele sprzecznych celów. Główne organy normalizacyjne ekosystemu NFC zostały już przedstawione w rozdziale 3. Organy te mają na celu opracowanie



Rysunek 7.2 Widok ekosystemu NFC według GSMA. Powielono za zgodą GSMA. Wszelkie prawa zastrzeżone.

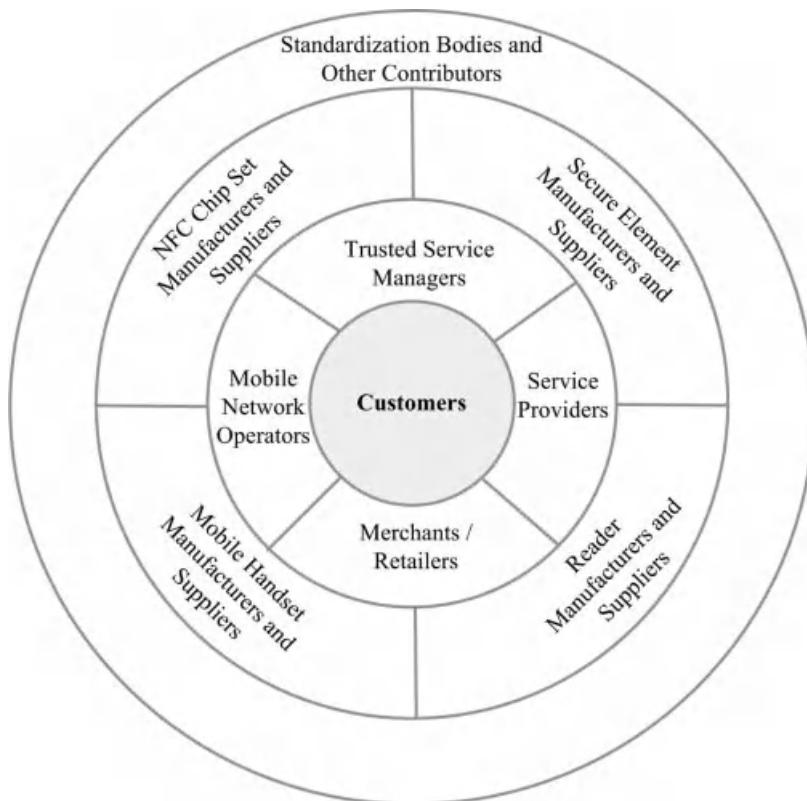
globalne i interoperacyjne standardy dla NFC, zależnych od niej technologii, takich jak karty inteligentne i telefony komórkowe. Tabela 7.1 opisuje inne pomniejsze stowarzyszenia, które również mają korzystny wpływ na rozwój NFC.

7.2.2 *Producenci i dostawcy zestawów chipów NFC*

Producenci i dostawcy zestawów chipów NFC dostarczają zgodne ze standardami zestawy chipów NFC i inny powiązany sprzęt do integracji technologii NFC w telefonach komórkowych. NXP Semicon-ductors, jako współwynalazca technologii NFC wraz z Sony, jest nadal ważnym producentem i dostawcą zestawów chipów NFC w ekosystemie biznesowym NFC. Pierwotnie została założona przez firmę Philips i sprzedana konsorcjum w 2006 roku. Firma produkuje i sprzedaje zestawy chipów NFC, a także bezstykowe karty inteligentne MIFARE, które są powszechnie używane przez różne systemy tranzystowe na całym świecie.

7.2.3 *Producenci i dostawcy bezpiecznych elementów*

Jak już opisano w rozdziale 3, Secure Element (SE) odgrywa kluczową rolę w systemach opartych na NFC, zwłaszcza w aplikacjach korzystających z trybu emulacji karty. Producenci i dostawcy SE



Rysunek 7.3 Interesariusze w ekosystemie NFC.

Tabela 7.1 Inni aktywni współtwórcy technologii NFC

Nazwa organizacji	Odpowiedzialność
NXP Semiconductors	Współwynalazca technologii NFC wraz z Sony, uczestniczy w
projektie	i wspiera rozwój NFC
Mobey Forum	Nienastawione na zysk, globalne forum branży finansowej, które zachęca do korzystania z technologii mobilnych w usługach finansowych.
Firmy płatnicze (American Express, Discover, MasterCard, Visa)	Zapewnia specyfikacje dotyczące płatności mobilnych, a także kwestie bezpieczeństwa i kwalifikacji funkcjonalności aplikacji.
Smart Card Alliance	Stowarzyszenie non-profit, które działa na rzecz stymulowania zrozumienia, przyjęcie i powszechnego zastosowanie technologii kart inteligentnych StolpanAssociation, które przyczynia się do ustanowienia otwartego, interoperacyjnego środowiska usług NFC

potrzeba zapewnienia SE zgodnych ze standardami. Urządzenia wbudowane i SE oparte na Secure Memory Card (SMC) są produkowane dla producentów telefonów komórkowych lub innych sprzedawców detalicznych, a SE oparte na UICC dla MNO. Producenci i dostawcy UICC są kontraktowani i zmuszani do dostarczania wymaganego sprzętu UICC do MNO. Mają oni bezpośrednie relacje z MNO, którzy również definiują wymagania dla UICC i wydają SE. Tak więc ogólnie systemy oparte na NFC wykorzystujące SE oparte na UICC są bardziej modelami biznesowymi ukierunkowanymi na MNO.

7.2.4 Producenci i dostawcy telefonów komórkowych

Rolą producentów i dostawców telefonów komórkowych jest zapewnienie standaryzowanych telefonów komórkowych z obsługą NFC poprzez włączenie zestawu chipów NFC i SE dla aplikacji i usług obsługujących NFC. Producenci telefonów komórkowych chcą oczywiście uczynić swoje telefony bardziej atrakcyjnymi dla klientów. Ponadto producenci telefonów komórkowych mogą uzyskać przewagę konkurencyjną, oferując telefony komórkowe obsługujące płatności i inne atrakcyjne aplikacje. Innowacyjne aplikacje mobilne dają producentom możliwość przyciągnięcia nowych klientów i stworzenia dodatkowych partnerstw biznesowych.

7.2.5 Producenci i dostawcy czytników

Rolą producenta czytników jest dostarczanie czytników obsługujących NFC dla sprzedawców, detalistów i innych stron, które chcą stosować aplikacje obsługujące NFC w swoich sklepach, takie jak płatności, bilety i aplikacje transportowe. Czytniki te są podobne do terminali POS (Point of Sale) używanych w zbliżeniowych transakcjach płatniczych dokonywanych za pomocą zbliżeniowych kart płatniczych.

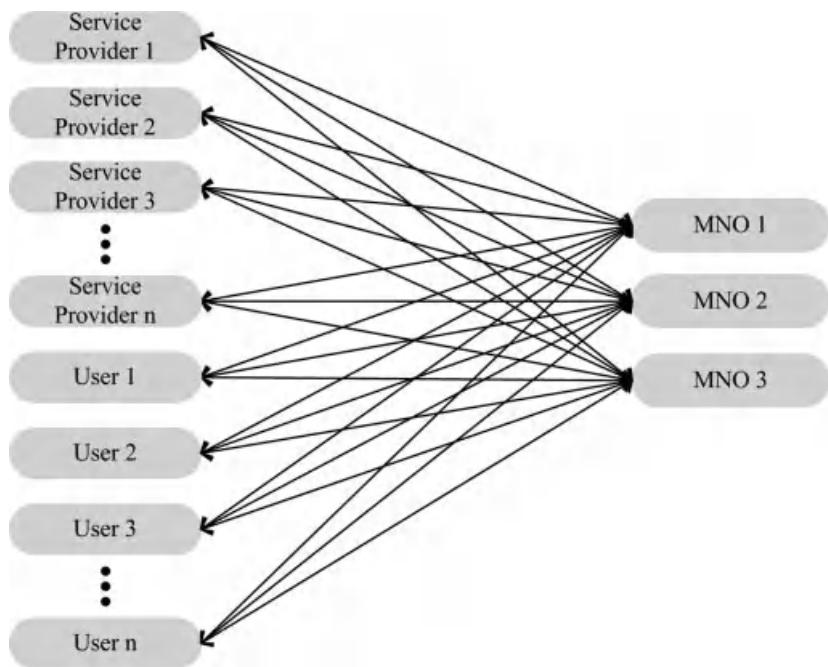
7.2.6 Operatorzy sieci komórkowych

Operatorzy MNO tradycyjnie zapewniają komunikację i sieć danych właścicielom telefonów komórkowych. W rzeczywistości są oni obecnie odpowiedzialni za - a nawet mają przywilej - dostarczania wszelkiego rodzaju usług mobilnych swoim abonentom. MNO mogą dostarczać i utrzymywać infrastrukturę sieciową, która umożliwia bezpieczne rozwiązania Over the Air (OTA) w celu zapewnienia zdalnego zarządzania i konserwacji aplikacji przechowywanych na SE.

OSK odgrywają ważną rolę w definiowaniu modeli biznesowych. Kwestie własności SE i dostarczania platform OTA mają bezpośredni wpływ na modele biznesowe NFC. Obecnie operatorzy sieci komórkowych starają się uzyskać duży udział w rynku i do tej pory w większości testów i projektów znajdują się w centrum środowiska biznesowego, kontrolując cykl życia SE i zarządzając platformami SE za pomocą własnych rozwiązań OTA. Jak zwykle, w tych testach najczęściej używane są SE oparte na UICC. W związku z tym klienci tego modelu biznesowego muszą być abonentami danego MNO. Takie środowisko tworzy zależność od jednego MNO, ponieważ dostawca usług nie współpracuje z żadnym innym MNO.

7.2.7 Zaufani menedżerowie usług

TSM jest wymagany do tworzenia i zarządzania zaufanym środowiskiem pomiędzy podmiotami ekosystemu NFC, głównie pomiędzy dostawcami usług i MNO. Integracja



Rysunek 7.4 Chaotyczny charakter środowiska biznesowego bez TSM.

umożliwia bezpieczną komunikację i ochronę interesów każdego podmiotu, a także zmniejsza złożoność modeli biznesowych.

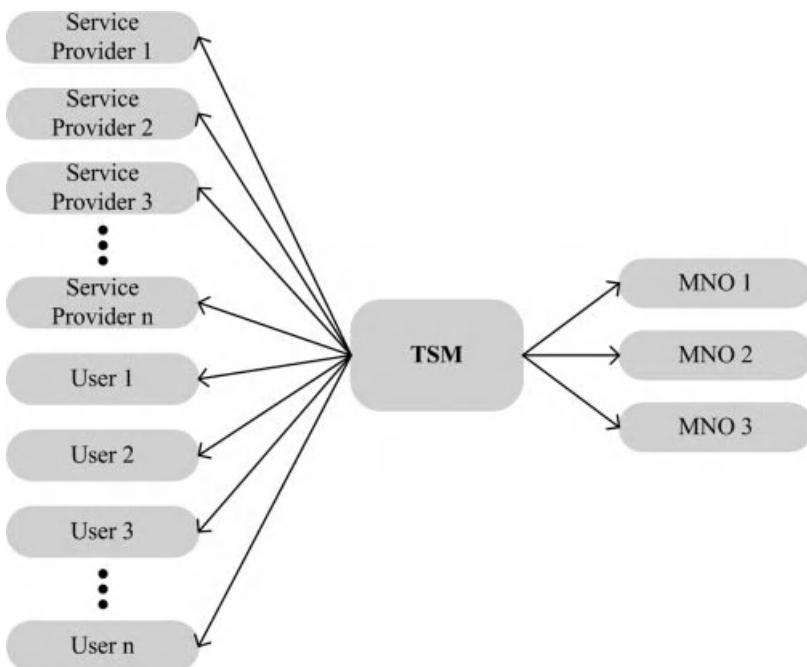
Z drugiej strony, aby zapewnić prostotę, gracze muszą być ze sobą w kontakcie, co tworzy złożone środowisko komunikacyjne, gdy nie jest używany TSM (patrz rysunek 7.4).

Alternatywnie, TSM odgrywa rolę centralnego organu w takim systemie i eliminuje złożoność (patrz rysunek 7.5). TSM generalnie oferuje pojedynczy punkt kontaktu z MNO dla dostawców usług, takich jak instytucje finansowe, banki, władze tranzytowe, przedstawcy detaliczni i inni, którzy chcą zapewnić klientom płatności NFC, bilety, usługi lojalnościowe itp. TSM jest również w stanie zapewnić własną platformę OTA i rozwiązania biznesowe. Umożliwia to wysyłanie i ładowanie aplikacji obsługujących NFC za pośrednictwem własnego łącza OTA do SE i jednocześnie zarządzanie cyklem życia SE.

Zwłaszcza w dużych systemach opartych na NFC, korzystanie z TSM jako centralny i neutralny zaufany podmiot jest korzystne.

Nie jest to jednak ani zdrowa, ani zrównoważona sytuacja. Role TSM muszą zostać zdefiniowane i uzgodnione między dostawcami usług i operatorami sieci komórkowych w celu zapewnienia klientom skutecznych usług mobilnych NFC. Rola TSM staje się ważna zwłaszcza w przypadku korzystania z mobilnych usług finansowych. MasterCard i Visa, będąc głównymi markami płatniczymi, a tym samym dostawcami usług, mają ścisłe wymagania dla organizacji, które chcą działać jako TSM. Opublikowano już wiele specyfikacji i standardów dotyczących roli TSM w mobilnych usługach finansowych.

CASSIS International, jako jeden z ważnych dostawców infrastruktury i platformy TSM, został założony przez zespół wizjonerskich przedsiębiorców i weteranów kart inteligentnych. CASSIS OTA



Rysunek 7.5 Rola TSM.

Platformy zapewniają zarządzanie SE, kluczami dla wszystkich rodzajów aplikacji obsługujących NFC oraz usługami płatniczymi. CASSIS ma silne partnerstwo biznesowe z wieloma wiodącymi bankami, operatorami sieci komórkowych i operatorami tranzytowymi w obszarach takich jak Azja i Pacyfik, Europa i USA. Dobrym przykładem jest partnerstwo biznesowe z Interbank Card Center (BKM), organizacją, która umożliwia transakcje kartami kredytowymi w różnych bankach w Turcji. Obecnie BKM stara się być TSM tureckiego sektora bankowego w domenie mobilnych usług finansowych z obsługą NFC i zaprasza wszystkie tureckie banki, które chcą wdrożyć usługi płatnicze z obsługą NFC, do stworzenia wspólnej wizji. CASSIS zapewnia rozwiązania biznesowe TSM i infrastrukturę umożliwiającą BKM bycie pierwszym międzybankowym krajowym TSM w Turcji. BKM uzgodnił z niektórymi bankami i operatorami sieci komórkowych świadczenie tej usługi.

7.2.8 Dostawcy usług

Dostawca usług to podmiot, który chce wdrożyć usługę na urządzeniu mobilnym klienta, a także zarządzać nią. Dostawcą usług może być instytucja finansowa, bank, organ transportowy lub inna organizacja. Dostawca usług może jednocześnie pełnić rolę dewelopera, właściciela i dostawcy aplikacji.

Ze względu na obecną atrakcyjność usług płatności mobilnych, instytucje finansowe lub banki (np. Visa, MasterCard, HSBC, ING Bank) są głównymi dostawcami usług w ekosystemie biznesowym NFC. Dostawcy ci są odpowiedzialni za oferowanie swoim klientom nowych i zróżnicowanych zaufanych usług płatniczych oraz zwiększanie wolumenów transakcji kredytowych i debetowych.

a także ulepszyć swoje marki. Z ich punktu widzenia uważa się, że technologia NFC jako nowa forma płatności może zwiększyć liczbę płatności dokonywanych kartami kredytowymi dzięki powszechnemu korzystaniu z telefonów komórkowych obsługujących technologię NFC.

7.2.9 Sprzedawcy detaliczni

W kontekście ekosystemu NFC, sprzedawcy i detaliści są interesariuszami, którzy akceptują zbliżeniowe usługi płatności mobilnych. Sprzedawcy mają możliwość przyspieszenia płatności w punktach sprzedaży. Są oni właścicielami systemu bezstykowych urządzeń POS i sieci finansowych określonego banku lub instytucji finansowej. Mikropłatności oferują natychmiastowe korzyści dla sprzedawców, takie jak wydajność operacyjna dzięki szybszym transakcjom i mniejszym wymaganiom dotyczącym obsługi gotówki, niższym kosztom pracy i zwiększonej wygodzie klientów w tym samym czasie. Mikropłatności mogą również pomóc sprzedawcom nawiązać silniejsze relacje z klientami i zwiększyć ich lojalność.

Sprzedawcy, podobnie jak banki, mogą oferować swoim klientom własne usługi lojalnościowe. Mogą również oferować swoje karty podarunkowe, a także programy lojalnościowe, ponieważ karty kredytowe i debetowe klientów są zawsze dostępne w ich telefonach komórkowych. Co więcej, sprzedawcy mogą oferować zaawansowane mobilne programy marketingowe i promocyjne, dostarczając klientom lub członkom wiadomości wpływające na ich zachowanie w celu korzystania z płatności mobilnych. Zgodnie z wynikami pilotów i innych badań niektórych pilotów płatności mobilnych z obsługą NFC zaobserwowano, że promocje mobilne i kupony były atrakcyjnymi opcjami i miały pozytywny wpływ na zachowania konsumentów.

7.2.10 Klienci

Klient jest inicjatorem usługi NFC poprzez dotknięcie swojego telefonu komórkowego do inteligentnego obiektu NFC. Klienci są zawsze głównymi interesariuszami w każdej firmie i znajdują się w centrum uwagi dostawców usług. Powód tego jest oczywisty. Klienci utrzymają firmę tylko wtedy, gdy ich potrzeby zostaną zaspokojone. Wszystkie działania marketingowe zawsze koncentrują się na nich. Konsumenti w sklepach detalicznych, bankach, na lotniskach, w teatrach, hotelach, szpitalach lub korzystający z transportu publicznego stanowią trzon tej branży, która chce czerpać korzyści finansowe z aplikacji i usług NFC.

7.3 Modele biznesowe

Kiedy nowa usługa ma być promowana, oczywiste jest, że istnieje wiele kwestii do załatwienia i problemów do rozwiązania. Większość z nich ma charakter biznesowy i wiąże się ze stosunkowo niewielką liczbą elementów technologicznych i infrastrukturalnych. Aby zaproponować nową usługę, bardzo ważne jest opracowanie niezbędnych i odpowiednich modeli biznesowych i procesów. W modelach biznesowych ważne jest dostarczanie wartości wszystkim zainteresowanym stronom. Niektóre modele biznesowe nie zachęcają do współpracy między wszystkimi organami; jednak w NFC jest to niezbędne.

Nowe kanały usług i koncepcje prowadzą do nowych wymagań biznesowych, tak jak w przypadku NFC. Aby zbudować skuteczny model biznesowy, wymagana jest odpowiednia analiza klientów i branży. Dobrym przykładem analizy wymagań biznesowych NFC jest Mobey Forum [4]. Mobey Forum proponuje szereg wymagań (tj. wymagania początkowe,

operacyjne, użytkowe i zewnętrzne), które należy wziąć pod uwagę przy tworzeniu modeli biznesowych.

Initial Requirements	Operational Requirements	Usability Requirements	External Requirements
<ul style="list-style-type: none">• Business Case• Transparency of Ecosystem• Mass market potential• Life cycle management• Open Standards• Added new value• Service adaptability	<ul style="list-style-type: none">• Business sustainability• Retain business control• Branding• Clarification of roles• Risk management• Consumer freedom to change service providers	<ul style="list-style-type: none">• International usage• Service integrity• Service availability• Ease of enrolment• Clear customer service• Service scope	<ul style="list-style-type: none">• Legal requirements• Seamless audit trail• Security demands• Customer authentication & transaction non-repudiation

Rysunek 7.6 Wymagania dotyczące modelu biznesowego [5]. Powielono za zgodą Mobey Forum.

Rysunek 7.6 podsumowuje te wymagania w czterech kategoriach. Początkowo wymagania zostały zidentyfikowane oddziennie dla konsumentów i dla każdej branży w ekosystemie NFC. Następnie okazało się, że wymagania różnych sektorów są w rzeczywistości bardzo podobne i utworzono listę wspólnych wymagań (patrz rysunek 7.6).

Rozważmy wymóg uzasadnienia biznesowego w tworzeniu modelu biznesowego. Zarówno konsumenti, jak i branże muszą mieć własne powody i cele, aby zainicjować usługę lub projekt NFC lub uczestniczyć w środowisku biznesowym NFC. Jeśli chodzi o branżę, na przykład dostawców usług transportowych, nowe możliwości biznesowe i oszczędności kosztów są dobrymi argumentami biznesowymi przemawiającymi za uczestnictwem w środowisku NFC. Wraz z zastąpieniem obecnych procesów w transporcie, mogą pojawić się nowe źródła przychodów dla MNO, klientów i innych dostawców usług. W przypadku klientów, na każdego konsumenta wchodzącego do tego ekosystemu i zaczynającego korzystać z technologii NFC mogą wpływać pewne czynniki motywujące i czynniki napędzające. Uzasadnienie biznesowe dla klientów umożliwia im zaakceptowanie tej nowej technologii i korzystanie z niej.

Ekosystem NFC obejmuje szeroką gamę aplikacji i usług od ogromnej liczby dostawców usług z wielu sektorów. Wszyscy uczestnicy ekosystemu reprezentują różne wymagania biznesowe i interesy. W związku z tym większość usług NFC skutkuje różnymi modelami współpracy w kontekście biznesowym. Różne rzeczywiste przypadki współpracy zostały przedstawione w rozdziale 9.

Obecnie istnieje ogromna niepewność co do tego, który model biznesowy jest najlepszy, która firma wykona dokładnie jaką czynność i kto zapłaci komu za jaką usługę, a także ile zysku ma zostać zarobione i podzielone między wszystkich interesariuszy. Ze względu na nowatorski charakter technologii NFC, nadal nie ma zgody co do modelu biznesowego, który w wystarczającym stopniu satysfakcjonowałby wszystkich interesariuszy. Opublikowano wiele propozycji i specyfikacji modeli biznesowych oraz przeprowadzono różne projekty i testy na całym świecie, zwłaszcza w zakresie mobilnych usług finansowych ze względu na wysoki stopień złożoności ekosystemu i infrastruktury technologicznej. NFC Forum, GlobalPlatform, GSMA i EMVCo to niektóre z ważnych stowarzyszeń, które intensywnie pracują nad ekosystemem NFC, modelami biznesowymi i podstawową infrastrukturą technologiczną.

Krótko mówiąc, konieczne jest zharmonizowanie interesów wszystkich uczestników w tworzeniu modeli biznesowych. Bez tego powstaną sprzeczne i nieinteroperacyjne rozwiązania, a tym samym technologia nie będzie miała szansy na ulepszenie. W następnej sekcji omówiono główne kwestie techniczne

Przedstawiono i opisano kwestie i obawy, które kształtują modele biznesowe oraz obowiązki interesariuszy.

7.3.1 Kluczowe wskaźniki w modelach biznesowych NFC

Do tej pory rynek przyjął kilka opcji SE, które są obsługiwane w różnych segmentach rynku i w różnych modelach telefonów. Obecnie istnieją trzy popularne modele (tj. wbudowany sprzęt, SMC i UICC). Te trzy alternatywy SE zostały omówione i przedstawione w szczegółach technicznych w rozdziale 3. Jak już wiadomo, telefony komórkowe potrzebują SE do bezpiecznego przechowywania i przetwarzania poufnych danych oraz ułatwiania aplikacji wymagających prywatności. Niektóre pytania, które są ważne dla modeli biznesowych NFC to:

- Kto będzie emitował i posiadał kontrolę nad SE?
- Kto będzie zarządzał cyklem życia platformy SE?
- Czyja platforma OTA będzie używana do zarządzania platformą SE?

Odnosząc się do tych pytań, w tej sekcji identyfikujemy trzy główne kwestie, które określają alternatywy modelu biznesowego dla NFC: emitent SE, menedżer platformy i dostawca OTA. Kwestie te można również określić jako funkcjonalne role i obowiązki, które muszą być obsługiwane przez pojedynczy podmiot lub wiele podmiotów w modelu biznesowym NFC.

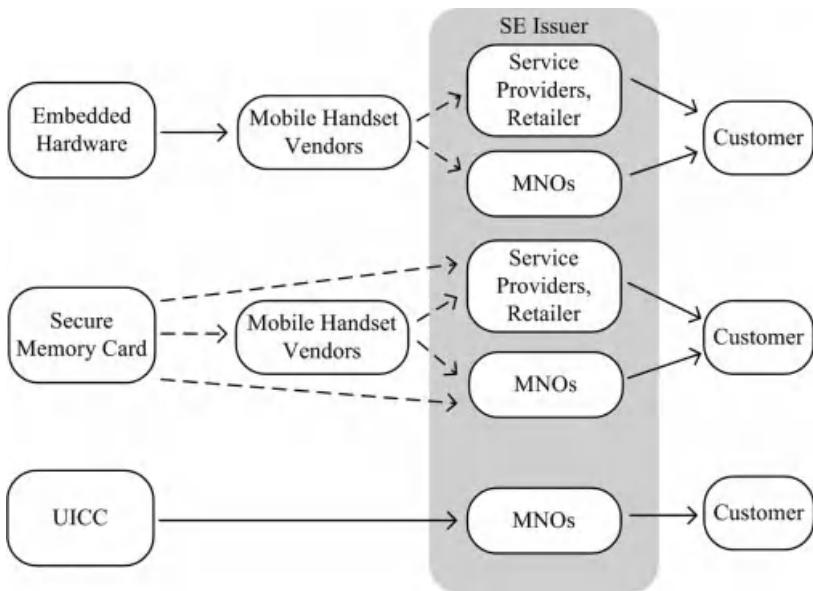
(i) *SE Emittent*

Emitent SE jest podmiotem, który wydaje i posiada kontrolę nad SE, który jest dostarczany do użytkownika końcowego. Rola emitenta SE jest pełniona przez różne podmioty w zależności od rodzaju używanego SE. W idealnym przypadku wystawca SE powinien być niezależnym podmiotem, ale nie jest tak w rzeczywistych przypadkach lub implementacjach. Obecnie nie jest zaskakujące, że OSK lub dostawcy usług (np. banki) jednocześnie odgrywają rolę wystawcy SE.

Rysunek 7.7 ilustruje alternatywy emitenta SE w zależności od modeli SE. Jeśli w modelu biznesowym wykorzystywany jest SE oparty na UICC, OSK ponosi odpowiedzialność za wystawcę SE, ponieważ OSK dystrybuują UICC. Jeśli używany jest wbudowany SE oparty na sprzęcie, rolę tę odgrywa podmiot, który przekazuje telefon komórkowy użytkownikowi. Jeśli telefon komórkowy jest dostarczany aktualnemu klientowi przez MNO w ramach kampanii, MNO jest wystawcą karty. Jeśli telefon komórkowy został zakupiony przez użytkownika od sprzedawcy detalicznego lub dostawcy usług, wystawcą karty może być teoretycznie dowolny niezależny partner, taki jak sprzedawca detaliczny, dostawca usług lub inny. Jeśli używany jest SE oparty na SMC, może on zostać wydany przez MNO, dostawcę usług lub sprzedawcę detalicznego.

(ii) *Menedżer platformy*

Drugą ważną kwestią jest kontrolowanie i zarządzanie platformą SE. Menedżer platformy jest właścicielem kluczy kryptograficznych używanych do kontrolowania SE w jego cyklu życia. Wszystkie SE posiadają klucz główny, który jest generowany podczas procesu personalizacji SE. Klucz główny jest unikalną wartością w celu zapewnienia mechanizmów bezpieczeństwa, takich jak tajność, uwierzytelnianie, integralność danych i niezaprzeczalność. Aktor będący właścicielem klucza głównego ma pełną kontrolę nad SE, a klucz ten może zostać zmieniony wyłącznie przez menedżera platformy. Menedżer platformy umożliwia autoryzowanym dostawcom usług instalowanie aplikacji na SE, najlepiej przy użyciu infrastruktury OTA.



Rysunek 7.7 Modele emitentów bezpiecznych elementów [6]. Powielono za zgodą Mobey Forum.

Menedżer platformy może użyć klucza głównego, aby podzielić platformę pamięci masowej (tj. SE) na bezpieczne domeny zgodnie z wymaganiami i przekazać kontrolę nad każdą bezpieczną domeną powiązanemu dostawcy usług, umożliwiając w ten sposób dostawcy zarządzanie cyklem życia aplikacji. Dostawcy usług mogą zarządzać cyklami życia swoich aplikacji. Menedżer platformy może również w razie potrzeby wyłączyć platformę lub jej część (tj. domenę bezpieczeństwa). Menedżer platformy nie ma dostępu do informacji specyficznych dla aplikacji, ponieważ po zarezerwowaniu określonej bezpiecznej domeny dla dostawcy usług, dostawca ma nad nią pełną kontrolę.

Rolę menedżera platformy może pełnić emitent SE lub inny zaufany, niezależny podmiot. Należy pamiętać, że obecnie możliwe są różne modele, a rolę menedżera platformy mogą pełnić różne organizacje. Rozważmy przypadek, w którym używany jest SE oparty na UICC, a MNO odgrywa zwykle rolę emitenta SE. Rola menedżera platformy może być pełniona przez tego MNO w tym samym czasie, a MNO jest właścicielem klucza głównego, a tym samym kontroluje cykl życia UICC. Dostawcy usług muszą zawierać umowy biznesowe z MNO w celu wdrażania aplikacji, a model biznesowy staje się całkowicie skoncentrowany na MNO.

W rzeczywistości model biznesowy jest prostszy, gdy emitent SE i menedżer platformy są tym samym podmiotem. Delegowanie roli menedżera platformy (tj. przekazywanie klucza głównego SE) innej stronie niż emitent SE jest jeszcze jedną opcją. Podmiotem tym może być TSM jako niezależna strona neutralna. Aby zrealizować tę opcję, TSM i wystawca SE powinni wcześniej uzgodnić model biznesowy. Umowa może obejmować szczegóły od infrastruktury technicznej po podział przychodów. TSM może obsługiwać wszystkie funkcje zarządzania SE za pomocą własnej platformy OTA lub łącza OTA MNO.

Mobey Forum zaproponowało trzy modele biznesowe w zależności od własności SE opartych na UICC. Mogą one być własnością jednej organizacji lub współwłasnością, emitowane przez jedną organizację lub współemitowane, zarządzane przez jedną organizację lub współzarządzane. Modele te to: model koncepcji hotelu, model koncepcji wynajmu budynku i model koncepcji własności. W modelu koncepcyjnym hotelu, SE i wszystkie powiązane obiekty, takie jak klucze i zarządzanie domeną bezpieczeństwa, są własnością, są kontrolowane i zarządzane przez jeden podmiot, taki jak właściciel hotelu, który jest jednocześnie emitentem SE. W przypadku koncepcji budynku na wynajem, SE jest emitowany i stanowi własność jednej organizacji, ale jest zarządzany przez stronę trzecią, taką jak TSM. Emitent SE jako właściciel budynku może zdecydować się na zatrudnienie strony trzeciej do zarządzania i organizowania usług w budynku (tj. SE). W modelu koncepcji własności, jedna lub więcej organizacji kontroluje proces wydawania SE, a każdy interesariusz, który posiada przestrzeń w SE, może uczestniczyć w zarządzaniu cyklem życia SE. Szczegółowe informacje na temat modeli operacyjnych i biznesowych Mobey Forum można znaleźć w innym miejscu [4].

(iii) *Dostawca OTA*

Ostatnią kwestią jest zapewnienie platformy OTA. Zapewnienie elastycznego i interoperacyjnego rozwiązania OTA jest kluczowym wymogiem w ekosystemie NFC. Szczegóły techniczne technologii OTA zostały przedstawione w rozdziale 8. Umożliwia ona bezpieczną komunikację bezprzewodową między dwiema stronami końcowymi oraz zapewnia transmisję i odbiór informacji związanych z aplikacją w systemie komunikacji bezprzewodowej. Technologia OTA umożliwia zdalne pobieranie, instalowanie i zarządzanie aplikacjami, takimi jak aktualizowanie, aktywowanie lub dezaktywowanie aplikacji przechowywanych w SE. Dlatego dostawcy OTA również odgrywają kluczową rolę.

Obecnie niektórzy MNO na całym świecie są w stanie dostarczać rozwiązania OTA przy użyciu swojej obecnej infrastruktury technologicznej. Kiedy MNO działają jako menedżerowie platform, używają własnego łącza OTA do zarządzania cyklem życia SE.

Możliwe jest jednak również utworzenie wymaganej infrastruktury przez inne podmioty (np. dostawców usług, TSM). Podmioty te mogą świadczyć usługi OTA niezależnie od emitentów SE lub menedżerów platform. Idealnym i najbardziej odpowiednim przypadkiem jest skorzystanie z rozwiązania OTA TSM i uczynienie TSM liderem platformy. TSM, jako neutralna strona między MNO a dostawcami usług, w pełni zarządza SE za pomocą własnego łącza OTA. Podział przychodów stanie się sprawiedliwy, a interesy zostaną zharmonizowane.

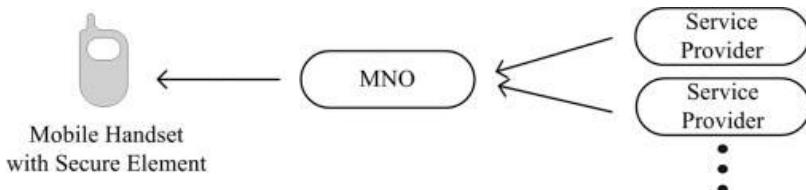
7.3.2 *Alternatywne modele biznesowe*

Ta sekcja zawiera podstawową wiedzę i zrozumienie modeli biznesowych proponowanych i stosowanych dotychczas w branży. Przedstawiamy niektóre modele współpracy, które zostały omówione, zbadane w literaturze lub zastosowane w praktyce. Obecnie dostępne modele to modele biznesowe skoncentrowane na MNO, rozproszone i skoncentrowane na TSM. W sekcji 7.5 przedstawiono udany przykład projektu GSMA wraz z jego modelami biznesowymi.

(i) *Model biznesowy ukierunkowany na MNO*

W modelu biznesowym skoncentrowanym na MNO, MNO wydaje SE i działa jako wydawca SE, menedżer platformy i dostawca OTA. Nie ma niezależnego zaufanego

NFC podmiotu. W związku z tym MNO wykonuje wszystkie funkcje TSM; jest właścicielem i zarządza ładowaniem, instalacją i



Rysunek 7.8 Model biznesowy ukierunkowany na MNO.

procesy personalizacji, a także tworzenie domen bezpieczeństwa w SE. Dostawcy usług muszą udostępniać swoje dane personalizacyjne MNO.

Rysunek 7.8 przedstawia przypadek, w którym na rynku istnieje tylko jeden MNO dla określonej usługi, takiej jak płatność. Wszyscy dostawcy usług (tj. banki) podpisują umowy biznesowe z jedynym OSK na rynku. W rzeczywistości liczba zaangażowanych OSK może wzrosnąć dla tego konkretnego środowiska usług. Dostawca usług musi współpracować z innymi MNO i wydanymi przez nich SE. Kiedy nowy MNO wchodzi do branży dla tej usługi, oczywiście usługodawca może podpisać umowę biznesową z tym MNO, aby dotrzeć do wszystkich potencjalnych klientów na rynku.

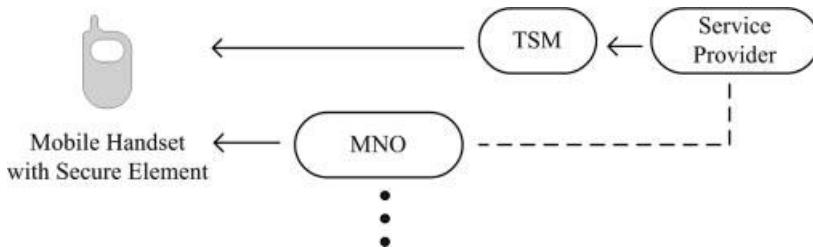
(ii) Rozproszony model biznesowy

W rozproszonym modelu biznesowym usługi zarządzania platformą są dystrybuowane wśród emitentów SE i dostawców usług. Może istnieć oddzielny podmiot TSM, a korzystanie z infrastruktury MNO OTA jest również inną opcją.

Jeśli dostawca usług nie ma możliwości TSM, musi zawrzeć umowę z istniejącym TSM. Ponadto dostawca usług musi udostępnić TSM dane związane z aplikacjami. Obecnie dostawcy usług wolą współpracować z zaufanymi stronami trzecimi niż dokonywać wysokich inwestycji w celu zbudowania platformy TSM w swoich organizacjach. Dlatego w rozproszonym modelu biznesowym zakładamy, że każdy z nich zawiera umowę z istniejącym TSM, a ta zaufana strona trzecia (TTP) wykonuje wszystkie funkcje TSM w imieniu usługodawcy.

W tym modelu rolę emitenta SE pełni głównie MNO, który wykonuje ładowanie i instalację aplikacji na używanym SE. Używana alternatywa SE nie musi być tylko SE opartym na UICC. OSK może również wykonywać procesy blokowania, odblokowywania i usuwania, a także tworzenia domeny bezpieczeństwa na karcie. Do tych procesów OSK wykorzystuje własną infrastrukturę platformy OTA. Dostawca usług wykonuje procesy przygotowania danych i personalizacji na platformie SE. Dostawca usług może korzystać z infrastruktury OTA MNO lub OTA TSM. W rzeczywistości w tym modelu rola dostawcy OTA zmienia się w zależności od umowy biznesowej między MNO a dostawcą usług. Jednak w obu przypadkach platforma SE jest zarządzana przez dwa podmioty, jak pokazano na rysunku 7.9.

Rozproszony model biznesowy jest najbardziej preferowanym, ale nie najbardziej odpowiednim rozwiązańem biznesowym. Model ten w rzeczywistości tworzy w ekosystemie sytuację korzystną dla obu stron. Ma on jednak pewne ograniczenia po stronie klienta, w zależności od opcji SE. W przypadku SE opartych na UICC, usługa NFC może być oferowana tylko ograniczonej liczbie klientów dostawców usług, którzy muszą być jednocześnie abonentami danego MNO. Aby dotrzeć do większej liczby klientów, usługodawca musi podpisać i uzgodnić umowę z innymi MNO na rynku, co stwarza inne komplikacje.



Rysunek 7.9 Rozproszony model biznesowy.

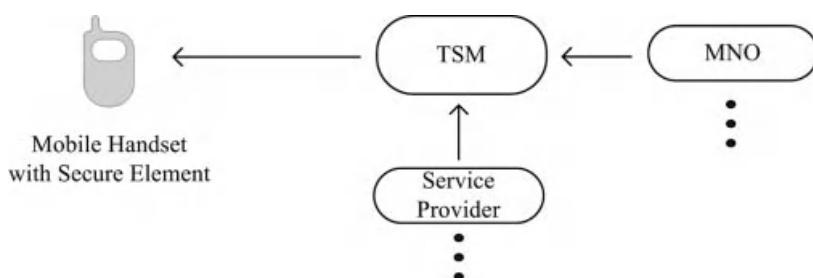
(iii) *Model biznesowy zorientowany na TSM*

W przypadku usługi NFC pojedynczy model biznesowy skoncentrowany na TSM jest w rzeczywistości najlepszą opcją i jednocześnie mniej złożoną (rysunek 7.10). Zaangażowanie TTP jako TSM dla konkretnej usługi NFC zmniejsza złożoność środowiska w porównaniu z innymi modelami. Zapewnia również sprawiedliwy podział przychodów między MNO i dostawcami usług. W międzyczasie szeroki zakres użytkowników korzysta z usług NFC świadczonych przez różnych dostawców usług.

Liczba TSM może wzrosnąć w zależności od dostępnych usług i uzgodnień podmiotów w ekosystemie NFC. Na przykład usługi płatnicze i transportowe z obsługą NFC mogą korzystać z tych samych lub różnych platform TSM. OSK i dostawcy usług, którzy chcą uczestniczyć w ekosystemie NFC, muszą podpisać i uzgodnić z TSM. Wszystkie podmioty powinny udostępniać wymagane dane autoryzowanemu TSM w ekosystemie. TSM pełni rolę menedżera platformy całkowicie w imieniu dostawców usług, realizując procesy ładowania, instalacji i personalizacji za pośrednictwem własnej platformy OTA.

(iv) *Podsumowanie modeli biznesowych*

Rysunek 7.11 podsumowuje wszystkie możliwe kombinacje trzech modeli biznesowych omówionych powyżej. We wszystkich zdefiniowanych modelach biznesowych wszystkie opcje SE - UICC, SMC i wbudowane SE oparte na sprzęcie - mogą być wydawane i zarządzane. W przypadku modelu biznesowego skoncentrowanego na MNO, wszystkie kluczowe wskaźniki są obsługiwane przez MNO. W przypadku rozprozonego modelu biznesowego zarządzanie platformą jest wykonywane przez MNO i dostawcę usług. Podczas zarządzania platformą używana platforma OTA może się różnić w zależności od umowy biznesowej między dostawcą usług a OSK.



Rysunek 7.10 Model biznesowy skoncentrowany na TSM.

SE Option	SE Issued By	Platform Management				Business Model	
		Application Loading and Installation		Data Preparation and Personalization			
		Installation	OTA Provider	Personalization	OTA Provider		
All*	MNO	MNO	MNO	MNO	MNO	MNO Centric	
All*	MNO	MNO	MNO	Service Provider	MNO	Distributed	
All*	MNO	MNO	MNO	Service Provider	TSM	Distributed	
All*	MNO	Service Provider	TSM	Service Provider	TSM	TSM Centric	
SMC, Embedded Hardware	Service Provider or Retailer	Service Provider	TSM	Service Provider	TSM	TSM Centric	

**All" refers to embedded hardware, SMC or UICC based SEs

Rysunek 7.11 Podsumowanie alternatywnych modeli biznesowych.

W modelu biznesowym skoncentrowanym na TSM, TSM ma pełne uprawnienia do zarządzania platformą i dostarczania OTA we wszystkich fazach. W rzeczywistości tożsamość strony wydającej SE i używanej opcji SE nie jest ważna. Autoryzacja zarządzania SE jest udzielana centralnemu TSM.

Jak już wspomniano, dostawcy usług i inni sprzedawcy detaliczni mogą jedynie wydawać SMC i sprzęt wbudowany w telefony komórkowe. Przykładem jest Akbank w Turcji, który wdrożył usługę mikropłatności Visa payWave z obsługą NFC bez zależności od MNO na rynku z dobrze wykwalifikowanym TSM.

Według Mobey Forum, wydaje się mało prawdopodobne, aby operatorzy MNO pozwolili stronie trzeciej na przejęcie roli zarządzania platformą SE opartych na UICC. W rzeczywistości przez dłuższy czas OSK z pewnością w pełni lub częściowo przejmą rolę zarządzania platformą (tj. zarządzania cyklem życia SE) w modelach biznesowych, w których wykorzystywane są SE oparte na UICC, a OSK będą jedynymi podmiotami, które je wydają. Ponieważ SE oparte na SMC są bardziej niezależne od MNO i mogą być stosowane we wszystkich modelach biznesowych, uważały, że będą one preferowane i częściej wykorzystywane przez dostawców usług w najbliższej przyszłości.

W niektórych scenariuszach, takich jak sprzedaż biletów i kuponów, które obejmują dodatkowych dostawców usług innych niż banki i instytucje finansowe, złożoność ekosystemu wzrasta. W optymalnym ekosystemie każdy dostawca usług i MNO musi podpisać umowę biznesową z jednym lub kilkoma centralizowanymi menedżerami platform, aby jego aplikacja została przesłana do SE. Dzięki temu konsumenci mają dostęp do wszystkich dostępnych usług i mogą włączać i wyłączać dowolną usługę, którą wybiorą, mogą również w dowolnym momencie przełączyć się na innego operatora i łatwo uzyskać dostęp do określonej usługi.

7.3.3 Ogólny model przepływu dochodów/wydatków

Jeśli chodzi o aspekt przychodów i wydatków modelu biznesowego, Mobey Forum przeprowadziło ogólną analizę modelu przychodów w [4]. W celu rozszerzenia tej analizy

Stakeholders	Revenue	Expenditure
Customer	<ul style="list-style-type: none"> Gaining coupons and other benefits from financial and loyalty services 	<ul style="list-style-type: none"> NFC enabled mobile phone Removable secure element; UICC, SMC Monthly subscription fees to service providers, and other bills
Service Providers	<ul style="list-style-type: none"> Monthly fees paid by customers as well as merchants, retailers 	<ul style="list-style-type: none"> Application development and other application related backend services Maintenance services for applications Customer care services
Mobile Network Operators	<ul style="list-style-type: none"> Monthly fees paid by its subscribers 	<ul style="list-style-type: none"> New UICC issuances Mobile network services OTA management services depending on business model Billing subscribers Customer care services
Merchants / Retailers	<ul style="list-style-type: none"> Increased sales (due to new customers or customer retention) 	<ul style="list-style-type: none"> Customer care services Bank fees and other
Trusted Service Managers	<ul style="list-style-type: none"> Fees paid by MNOs, service providers depending on business model 	<ul style="list-style-type: none"> TSM infrastructure services OTA management solutions depending on business model Customer care services

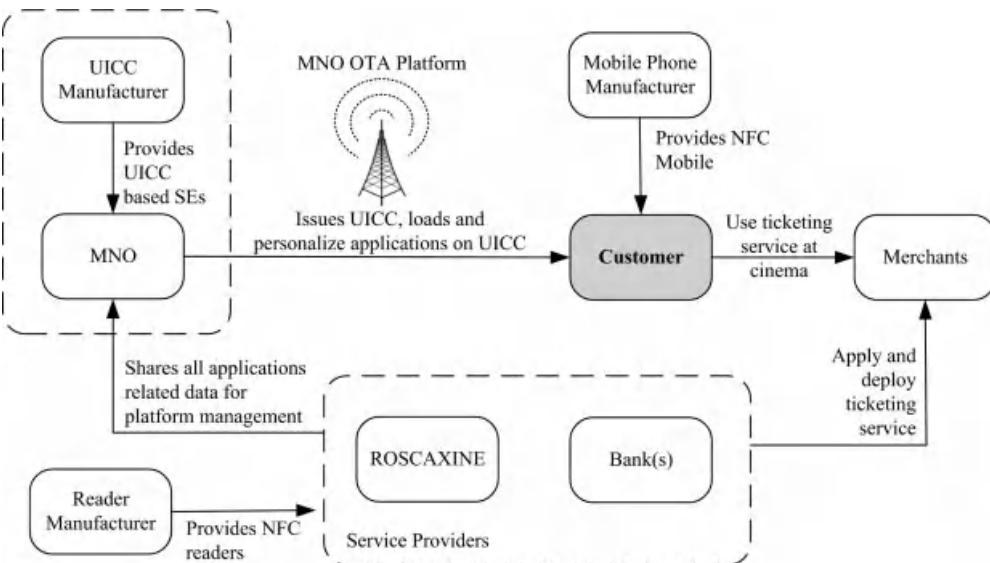
Rysunek 7.12 Ogólny przepływ przychodów/wydatków między interesariuszami NFC.

Z perspektywy, użyteczne zrozumienie prostych przepływów pieniężnych wśród interesariuszy NFC podsumowano na rysunku 7.12.

7.4 Studium przypadku: Sprzedaż biletów NFC

Niniejsza sekcja ma na celu przedstawienie i opisanie studium przypadku użycia usługi sprzedawy biletów w kinie z obsługą NFC. Ten przypadek użycia jest również omawiany i oceniany w rozdziale 4 z innego punktu widzenia. Jak już wspomniano, sprzedaż biletów jest usługą działającą w trybie emulacji karty. Kwestie operacyjne i zasady działania usługi sprzedawy biletów do kina zostały krótko przedstawione i zilustrowane w rozdziale 4.

Ta sekcja wyraża i ocenia środowisko biznesowe usługi sprzedawy biletów NFC w oczekiwaniu na proponowane modele biznesowe w sekcji 7.3. Usługi działające w trybach czytnika/zapisu i peer-to-peer mają bardziej odrębne środowisko biznesowe niż usługi działające w trybie emulacji karty. Usługi działające w trybie czytnika/zapisu i trybie peer-to-peer generalnie wykonują



Rysunek 7.13 Środowisko biznesowe MNO centric NFC ticketing case.

nie wymagają złożonego i bezpiecznego środowiska do zastosowania na telefonie komórkowym użytkownika z obsługą NFC. Aplikacje działające w trybie emulacji karty obejmują szeroki zakres alternatyw infrastruktury technicznej, aplikacje te muszą być bezpiecznie pobrane na SE telefonu komórkowego użytkownika, a domeny bezpieczeństwa i inne klucze muszą być generowane na SE. Następnie zarządzanie cyklem życia platformy SE i aplikacji na niej musi być stale wykonywane przez autoryzowane podmioty za pośrednictwem odpowiedniego rozwiązania OTA. Środowiska biznesowe takich usług obejmują różnych interesariuszy i współpracę biznesową.

Przypomnijmy, że w naszym przypadku użycia firma kinowa ROSCAXINE decyduje się wdrożyć usługę sprzedaży biletów NFC przy użyciu kas w swoich strefach rozrywki. Użytkownicy mogą wybrać film i dokonać rezerwacji miejsca, informując o tym kasjera w kasie. Użytkownik najpierw dотyka czytnika zbliżeniowego NFC POS, aby zapłacić za bilety, a następnie otrzymuje bilety. Bilety są przechowywane na urządzeniu mobilnym, dzięki czemu po dotknięciu czytnika NFC przy bramce obrotowej użytkownik może łatwo wejść do sali kinowej.

W niniejszym studium przypadku zastosowano usługę sprzedaży biletów NFC przy użyciu trzech różnych wariantów modelu biznesowego. Każda alternatywa różni się wybraną opcją SE i kluczowymi wskaźnikami zdefiniowanymi w sekcji 7.3.1. Większość omówionych modeli na rysunku 7.11 jest bardziej wizualizowana w tym studium przypadku, a mocne i słabe strony interesariuszy są krótko przedstawione.

(i) Przypadek 1: Model biznesowy ukierunkowany na MNO

Rysunek 7.13 przedstawia środowisko biznesowe w przypadku sprzedaży biletów NFC w centrum sieci MNO oraz relacje podmiotów zaangażowanych w ekosystem. W typowym przypadku sprzedaży biletów istnieją dwie główne fazy: płatność i sprzedaż biletów. Jak zwykle, dostawcą usług jest bank, który zapewnia usługę płatności z obsługą NFC w celu uzyskania biletu, oraz firma biletowa, taka jak ROSCAXINE, która zapewnia bilet elektroniczny dla użytkownika.

Rozważmy, że ROSCAXINE decyduje się na świadczenie usługi sprzedaży biletów NFC we współpracy z konkretnym MNO na rynku i wykorzystuje SE oparte na UICC, aby umożliwić tę usługę. ROSCAXINE uzgadnia i podpisuje umowy biznesowe z OSK. OSK może mieć również podpisane umowy z bankami, które świadczą usługi płatnicze. Ponieważ używany jest SE oparty na UICC, właścicielem i wydawcą karty jest MNO.

Na etapie umowy biznesowej wszystkie podmioty decydują o infrastrukturze technicznej usługi biletowej, która zostanie wdrożona na karcie UICC dla klientów, a także decydują o przychodach, które będą dzielone.

Aplikacje biletowe ROSCAXINE i aplikacje płatnicze banku są przechowywane na UICC klienta. Ponieważ MNO odgrywa rolę zarządzającą całą platformą, procesy ładowania i personalizacji aplikacji są wykonywane przez MNO przy użyciu własnego łącza OTA. Tak więc, aby świadczyć usługi OTA, nie ma potrzeby dodatkowych inwestycji dla dostawców usług; MNO może korzystać z istniejącej infrastruktury.

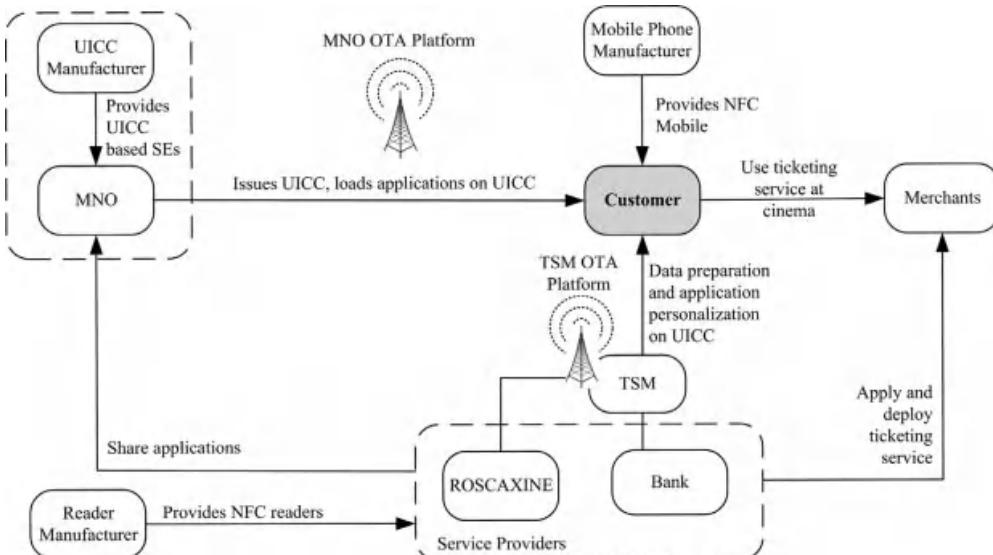
W takim modelu biznesowym przychody są dzielone głównie między MNO a dostawcami usług. Głównym ograniczeniem tej usługi jest ograniczona grupa docelowa, która z niej korzysta. Tylko abonenci tego MNO i członkowie uzgodnionych banków mogą korzystać z tej usługi bez dodatkowych kosztów (np. kosztów członkostwa itp.). Jeśli ROSCAXINE chce dotrzeć do większej liczby klientów, powinien podpisać umowy biznesowe z innymi MNO na rynku i korzystać z ich SE opartych na UICC i sieci OTA. Następnie abonenci innych operatorów, którzy są już członkami uzgodnionego banku, mogą również korzystać z tej usługi.

(ii) *Przypadek 2: Rozproszony model biznesowy*

Załóżmy ponownie, że ROSCAXINE decyduje się na świadczenie usługi sprzedaży biletów NFC wspólnie z konkretnym MNO na rynku i wykorzystuje SE oparte na UICC, aby umożliwić tę usługę. Jak zwykle, SE oparte na UICC są wydawane i posiadane tylko przez MNO w celu ładowania i instalacji aplikacji w tym scenariuszu. Proces zarządzania platformą jest jednak współdzielony przez MNO i dostawców usług, co kształtuje rozproszony model biznesowy.

Rysunek 7.14 przedstawia relacje między zaangażowanymi podmiotami w rozproszonym modelu biznesowym sprzedaży biletów NFC, gdy używana jest alternatywna SE oparta na UICC. Po pierwsze, ROSCAXINE uzgadnia i podpisuje umowy biznesowe z MNO. Wybiera infrastrukturę techniczną usługi sprzedaży biletów, gdy używany jest SE oparty na UICC i model zarządzania platformą rozproszoną. Fazy ładowania i instalacji aplikacji biletowych i płatniczych są wykonywane przez MNO na SE za pośrednictwem kanałów OTA MNO. Dostawca usług jest odpowiedzialny za fazę personalizacji aplikacji na UICC. Zazwyczaj nie posiadają oni żadnych istniejących rozwiązań biznesowych TSM. W związku z tym powinni oni nawiązać partnerstwo biznesowe z TSM w branży w tym samym czasie.

Podsumowując, model ten jest również zależny od MNO. Przychody są dzielone głównie między MNO i dostawców usług. Główną korzyść uzyskują dostawcy usług. Ten rozproszony model zapewnia dostawcom usług większą kontrolę nad ich aplikacjami na SE użytkownika, a oni wykonują usługę za pomocą swojej platformy TSM OTA w tym samym czasie. Głównym ograniczeniem tej usługi jest ponownie ograniczona liczba klientów docelowych, którzy korzystają z tej usługi, co zostało omówione w pierwszym przypadku użycia. Tylko abonenci danego MNO i jednocześnie członkowie uzgodnionego banku (banków) mogą korzystać z tej usługi bez żadnych dodatkowych kosztów.



Rysunek 7.14 Środowisko biznesowe rozproszonej sprzedaży biletów NFC.

(iii) Przypadek 3: Model biznesowy skoncentrowany na TSM

Załóżmy, że SE oparty na SMC jest używany w telefonie komórkowym użytkownika z obsługą NFC w tym ostatnim scenariuszu (patrz rysunek 7.15). Dostawcy usług ładują aplikację biletową i usługi płatnicze na SMC. ROSCAXINE i bank korzystają z jednej platformy TSM OTA i wykonują procesy ładowania, instalacji i personalizacji aplikacji całkowicie przy użyciu infrastruktury TSM OTA, która zapewnia niezależność od operatorów MNO. Zarządzanie platformą jest wykonywane przez TSM.

Zaletą tego modelu jest jego niezależność od operatorów MNO. Wszyscy klienci banku mogą korzystać z tej usługi poprzez uzyskanie wydanego SMC. Jeśli ROSCAXINE chce dotrzeć do większej liczby klientów, może uzgodnić i współpracować z innymi bankami, które chcą wdrożyć usługę płatności na SE opartych na SMC do sprzedaży biletów NFC w strefach rozrywki ROSCAXINE.

7.5 Dodatkowa lektura: Projekt Pay-Buy-Mobile realizowany przez GSMA

Projekt Pay-Buy-Mobile został uruchomiony przez GSMA w lutym 2007 roku podczas Mobile World Congress. Projekt ten został również opublikowany jako biała księga o nazwie "Pay-Buy-Mobile Business Opportunity Analysis", która jest publicznie dostępna na oficjalnej stronie internetowej GSMA [7]. Głównym celem projektu jest stworzenie wspólnej globalnej wizji usług płatności mobilnych z obsługą NFC i osiągnięcie interoperacyjności. Ponad 60 MNO (Vodafone, Orange, Turkcell itp.) wspiera ten projekt, dlatego proponowane modele biznesowe są oczywiście bardziej ukierunkowane na MNO. Przeprowadzono wiele programów pilotowych i testów Pay-Buy-Mobile NFC w celu wzmacniania partnerów rynkowych NFC. Testy przeprowadzono w wielu krajach, takich jak Australia, Kanada, Francja, Japonia, Korea, Malezja, Norwegia, Filipiny, Hiszpania, Tajwan, Turcja i USA.

Pay-Buy-Mobile to usługa płatności mobilnych z obsługą NFC, która jest wykonywana na SE opartych na UICC. Nie trzeba dodawać, że GSMA promuje ideę, że UICC jest

NFC najlepiej odpowiednim SE dla telefonów komórkowych z obsługą NFC. Są one uniwersalne (tj. globalnie stosowane w ponad 80% telefonów komórkowych).

Tabela 7.2 Modele biznesowe i rola TSM w systemie Pay-Buy-Mobile

Model biznesowy Platforma	TSM dostarczana przez
Model zorientowany na MNO	OSK
Model niezależnego podmiotu	Zaufana strona trzecia
Model centryczny CIB	CIB
Model	łączony MNO-CIB-zaufana strona trzecia

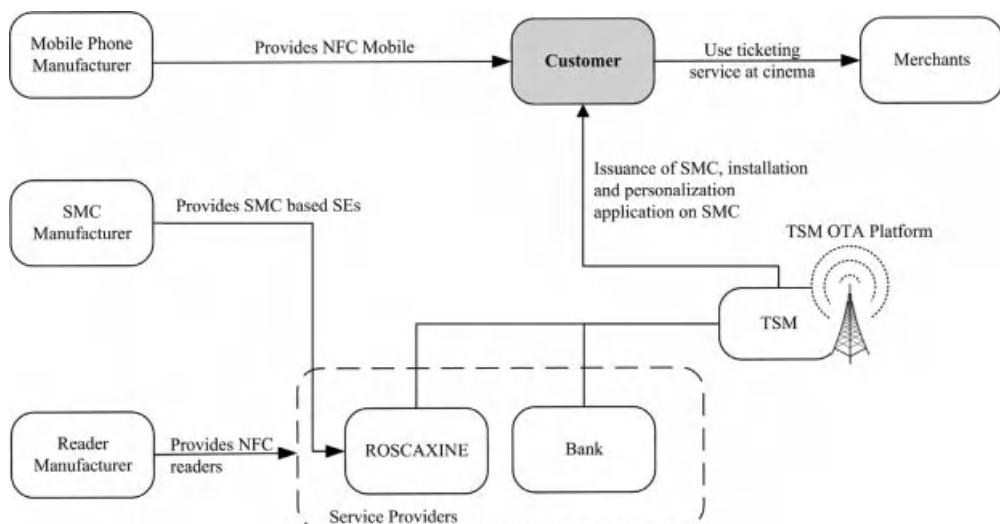
telefony komórkowe), przenośne, ustandaryzowane i umożliwiają dynamiczne zdalne zarządzanie poprzez funkcję OTA, jak wyjaśniono w rozdziale 8.

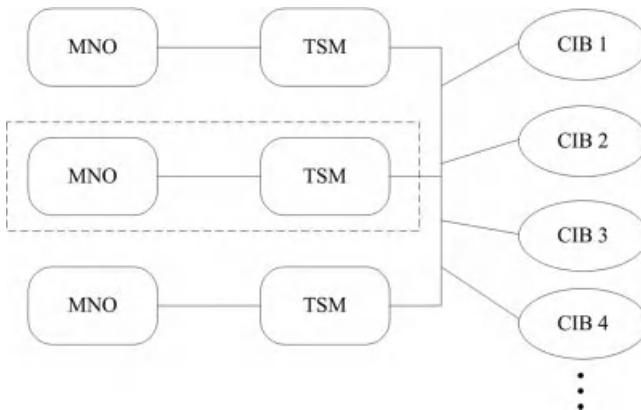
Głównymi uczestnikami Pay-Buy-Mobile są TSM, MNO i banki wydające karty (CIB). TSM jest łącznikiem między CIB a MNO. Banki CIB jako dostawcy usług umożliwiają ogólną obsługę płatności i są odpowiedzialne za obsługę klienta, wydawanie aplikacji płatniczych i danych personalizacyjnych klienta, a także ustanowienie formalnej umowy z klientem na usługę płatności z obsługą NFC.

Nie tylko łączy pojedynczy CIB z pojedynczym MNO, ale jest także zintegrowanym punktem pomiędzy wieloma CIB i wieloma MNO. Możliwe jest również posiadanie wielu TSM w ekosystemie Pay-Buy-Mobile, a także połączenie MNO i CIB pełniących rolę TSM na rynku. Projekt Pay-Buy-Mobile proponuje cztery modele biznesowe, jak pokazano w tabeli 7.2. Podmioty uczestniczące w ekosystemie Pay-Buy-Mobile mogą wybrać najbardziej odpowiedni model biznesowy, aby zaspokoić swoje potrzeby rynkowe.

(i) Model skoncentrowany na MNO

W tym modelu MNO tworzy i integruje możliwości TSM w ramach swojej infrastruktury sieciowej i oferuje bezpieczną i otwartą platformę TSM dla CIB, jak pokazano na rysunku 7.16. MNO może zapewnić elastyczność w dostosowywaniu świadczenia usług dla usług mobilnych z obsługą NFC.

**Rysunek 7.15** Środowisko biznesowe w przypadku sprzedaży biletów NFC z wykorzystaniem TSM.



Rysunek 7.16 Model centralny MNO. Powielono za zgodą GSMA. Wszelkie prawa zastrzeżone.

Operatorzy MNO powinni dokonać dużych inwestycji w stworzenie infrastruktury TSM, jeśli jeszcze jej nie posiadają. Z drugiej strony, CIB powinny zapewnić infrastrukturę płatniczą obsługującą NFC, aby umożliwić Pay-Buy-Mobile. W porównaniu z pozostałymi trzema modelami biznesowymi Pay-Buy-Mobile, CIB muszą dokonać stosunkowo niewielkiej inwestycji w budowę infrastruktury Pay-Buy-Mobile, znacząca część pracy jest wykonywana przez MNO. Jednak każdy CIB na rynku musi zawrzeć umowę biznesową, a także współpracować z każdym MNO w celu realizacji usługi Pay-Buy-Mobile.

(ii) *Model niezależnego podmiotu*

W tym modelu TTP jest oddzielony od wszystkich innych podmiotów, a zatem jest niezależny od wszystkich innych graczy i wykonuje funkcje TSM. Stroną trzecią jest organizacja dostarczająca wyłącznie rozwiązania biznesowe TSM na rynku, która działa jako pojedynczy i neutralny punkt kontaktowy między MNO a CIB.

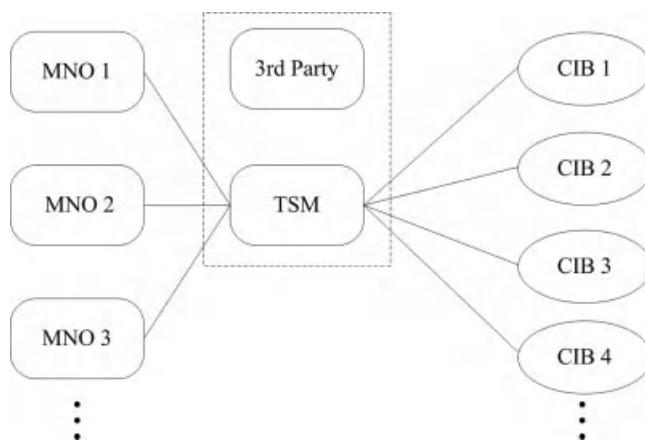
TSM wykonuje ogólne zarządzanie domenami bezpieczeństwa na UICC w oparciu o SE użytkownika. Model ten zmniejsza ogólną złożoność ekosystemu Pay-Buy-Mobile, zapewniając zintegrowany interfejs między MNO i CIB. Model ten eliminuje potrzebę inwestowania w infrastrukturę TSM zarówno dla MNO, jak i CIB. Aby ułatwić ten model, każdy MNO i CIB na rynku musi zawrzeć umowę biznesową ze stroną trzecią, jak pokazano na rysunku 7.17.

(iii) *Model skoncentrowany na CIB*

W modelu skoncentrowanym na CIB, CIB wykonuje wszystkie funkcje TSM i współpracuje z uczestniczącymi MNO na rynku, jak pokazano na rysunku 7.18. CIB musi dokonać dużej inwestycji w budowę platformy TSM, ponieważ wiąże się to z dodatkowymi wysokimi kosztami dla CIB. Dla małych CIB inwestycja ta może stanowić barierę wejścia na rynek płatności mobilnych z obsługą NFC. Z punktu widzenia operatorów sieci komórkowych, nadal dostarczają oni SE oparte na UICC.

(iv) *Model łączony*.

W modelu łączonym rolę TSM może odgrywać dowolna kombinacja MNO, CIB i niezależnego podmiotu TTP. Na przykład, jak pokazano na rysunku 7.19, uczestniczący OSK i CIB mogą wspólnie utworzyć infrastrukturę TSM, aby obsługiwać swoich klientów. Inwestycje są dzielone między początkowych założycieli infrastruktury TSM.

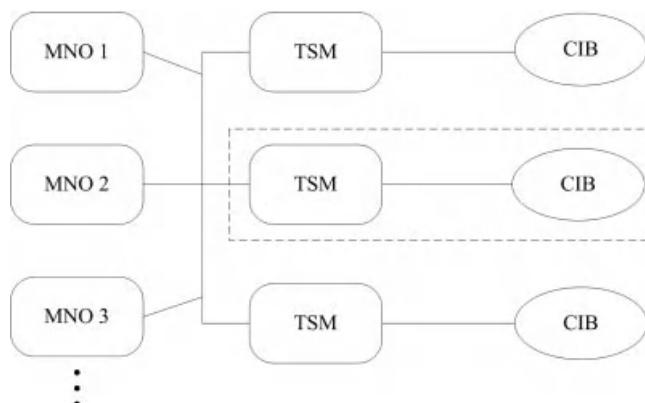


Rysunek 7.17 Model niezależnego podmiotu. Powielono za zgodą GSMA. Wszelkie prawa zastrzeżone.

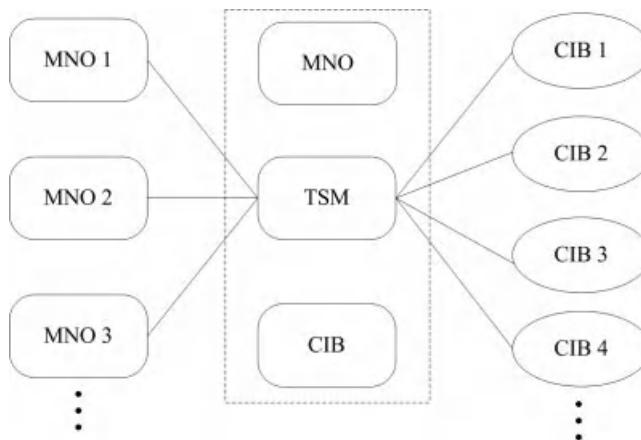
Po utworzeniu platformy TSM nowi partnerzy, tacy jak MNO lub CIB, mogą dołączyć do sieci biznesowej.

Aby stworzyć zrównoważony model, naprawdę ważne jest stworzenie modelu biznesowego korzystnego dla wszystkich interesariuszy na rynku, z wieloma dodatkowymi przychodami i możliwościami marketingowymi. Projekt Pay-Buy-Mobile uruchamia wiele usług mobilnych opartych na UICC z obsługą NFC. Według GSMA, UICC jest głównym komponentem w rozwiązywaniu biznesowym płatności. Zapewnia bezpieczny i elastyczny kanał do przeprowadzania mobilnych transakcji płatniczych z obsługą NFC.

Kolejnym ważnym elementem są firmy bankowe. GSMA zaprosiła społeczności usług finansowych do współpracy z MNO w celu osiągnięcia wspólnej wizji w projekcie Pay-Buy-Mobile. OSK i banki muszą uzgodnić wzajemnie korzystne i akceptowalne modele biznesowe. Aby pomyślnie przejść do przodu ze wszystkimi rodzajami modeli biznesowych, zrozumienie



Rysunek 7.18 Model centryczny CIB. Powielono za zgodą GSMA. Wszelkie prawa zastrzeżone.



Rysunek 7.19 Model łączony. Powielono za zgodą GSMA. Wszelkie prawa zastrzeżone.

Wymagania biznesowe MNO i banku oraz ustanowienie zaufania między nimi jest wymagane.

7.6 Podsumowanie rozdziału

Termin ekosystem ma różne znaczenia w różnych dziedzinach, takich jak biologia, socjologia, ekonomia i biznes. Jeden z najlepszych opisów ekosystemu biznesowego został podany przez Jamesa F. Moore'a, który definiuje go jako środowisko współdziałających organizacji i osób, które ma swój własny cykl życia. Ekosystem biznesowy może być również oceniany z perspektywy środowiska biologicznego. W ekosystemie biznesowym wszystkie uczestniczące podmioty muszą dostosować się do sytuacji i okoliczności rynkowych. Podmioty, które nie są w stanie dostosować się i poradzić sobie z konkurencją, są w krótkim czasie wykluczane z ekosystemu. Ciągłe wytwarzanie i dostarczanie wartości klientom jest wymagane do przetrwania ekosystemu. Jeśli ekosystem jest zdrowy, wszystkie podmioty mogą odnieść sukces.

Jednym z ważnych aspektów, które należy wziąć pod uwagę przy zrozumieniu technologii NFC, jest jej ekosystem biznesowy. Branża NFC ma nowy, wyłaniający się ekosystem biznesowy i łańcuch wartości obejmujący kilka branż i organizacji. Gracze to głównie organy normalizacyjne i inne podmioty przyczyniające się do rozwoju technologii NFC, takie jak producenci i dostawcy zestawów chipów NFC, producenci i dostawcy telefonów komórkowych, producenci i dostawcy czytników, producenci i dostawcy bezpiecznych elementów, operatorzy sieci komórkowych, TSM, dostawcy usług, sprzedawcy lub detaliści i wreszcie klienci.

Aby wdrożyć ekosystem, bardzo ważne jest opracowanie i przetworzenie odpowiednich modeli biznesowych. Niektóre modele biznesowe nie zachęcają do współpracy wszystkich podmiotów, jednak ekosystem NFC wymaga współpracy różnych interesariuszy i branż. Modele biznesowe muszą zostać opracowane w celu zapewnienia zysków wszystkim zainteresowanym stronom. Możliwe są trzy główne modele współpracy: MNO-centryczne, rozproszone i TSM-centryczne modele biznesowe. Definiując modele biznesowe NFC, należy zająć się trzema kluczowymi kwestiami: kto będzie emitentem SE w zależności od

alternatywę SE, kto będzie zarządzał cyklem życia SE i będzie menedżerem platformy, i wreszcie, kto będzie dostawcą OTA.

Opublikowano wiele propozycji modeli biznesowych i specyfikacji, a różne projekty zostały wdrożone w ramach testów na całym świecie, zwłaszcza w przypadku mobilnych usług finansowych ze względu na wysoki stopień złożoności ekosystemu i infrastruktury technologicznej. NFC Forum, GlobalPlatform, GSMA i EMVCo to niektóre z ważnych stowarzyszeń. GSMA przeprowadziło cenny projekt o nazwie Pay-Buy-Mobile, w którym uczestniczy ponad 60 uczestniczących i wspierających MNO. Przeprowadzono wiele pilotów i testów Pay-Buy-Mobile NFC w celu wzmacniania rynku NFC w wielu krajach. Projekt ten proponuje cztery modele biznesowe, w których uczestniczące podmioty mogą wybrać najbardziej odpowiedni. Te cztery modele to: Model skoncentrowany na MNO, model skoncentrowany na niezależnym podmiocie, model skoncentrowany na CIB oraz model kombinowany.

Ze względu na nowatorski charakter technologii NFC, wciąż nie ma wspólnej wizji modelu biznesowego, który satysfakcyjowałby wszystkich interesariuszy. Istnieje wszechobecna niepewność co do tego, który podmiot wykona dokładnie co, kto komu zapłaci, a także ile zysku osiągnie każdy z interesariuszy. Istotne jest, aby infrastruktura technologiczna i bezpieczny element używany w telefonach komórkowych, dostawca platformy OTA i infrastruktura TSM kształtyły modele biznesowe i obowiązki interesariuszy w ekosystemie NFC. Zrozumienie wymagań biznesowych i potrzeb rynkowych wszystkich interesariuszy, a także budowanie zaufania między nimi to kluczowe kwestie dla rozwoju ekosystemu NFC.

Pytania do rozdziału

1. Czym jest ekosystem biznesowy? Wyjaśnij.
2. Wymień i wyjaśnij ogólne cechy ekosystemu biznesowego.
3. Wymień głównych interesariuszy ekosystemu biznesowego NFC.
4. Jakie jest znaczenie TSM w ekosystemie biznesowym NFC?
5. Czy sugerujesz korzystanie z centralnego TSM w ekosystemie NFC? Jakie są korzyści porównawcze?
6. Jakie są główne wskaźniki modelowania biznesowego w ekosystemie NFC?
7. Porównanie zalet i wad modelu biznesowego MNO pod względem przychodów i wydatków.
8. Porównanie zalet i wad rozproszonego modelu biznesowego pod względem przychodów i wydatków.
9. Porównanie zalet i wad modelu biznesowego TSM pod względem przychodów i wydatków.
10. Jaka jest najbardziej krytyczna decyzja w ekosystemie NFC dotycząca trybu emulacji karty NFC?

Referencje

- [1] Peltoniemi, M. i Vuori, E. (2004) *Business Ecosystem as the New Approach to Complex Adaptive Business Environments*. Proceedings of Frontiers of E-Business Research, 2004.
- [2] Moore, J. (1993) Drapieżniki i ofiary: Nowa ekologia konkurencji *Harvard Business Review*, 71(3), 75-86.
- [3] Casti, J.L. (1997) *Would-be Worlds: How Simulation Is Changing the Frontiers of Science*, John Wiley & Sons, Ltd, New York, ISBN: 978-0471196938.

- [4] Mobey Forum Enrollment Task Force (2008) *Best Practices for Mobile Financial Services*, MOBEY Forum, 2008. Dostępny pod adresem: <http://www.mobeyforum.org/content/download/460/2768/file/Best%20Practices%20for%20MFS%20Enrolment%20Business%20model%20analysis%20final.pdf> (dostęp 10 lipca 2011 r.).
- [5] Mobey Forum Enrollment Task Force (2008) *Best Practices for Mobile Financial Services*, Table 4.1, MOBEY Forum, 2008. Dostępne pod adresem: <http://www.mobeyforum.org/content/download/460/2768/file/Best%20Practices%20for%20MFS%20Enrolment%20Business%20model%20analysis%20final.pdf> (dostęp 10 lipca 2011 r.).
- [6] Mobey Forum Enrollment Task Force (2008) *Best Practices for Mobile Financial Services*, Figure 6.2, MOBEY Forum, 2008. Dostępny pod adresem: <http://www.mobeyforum.org/content/download/460/2768/file/Best%20Practices%20for%20MFS%20Enrolment%20Business%20model%20analysis%20final.pdf> (dostęp 10 lipca 2011 r.).
- [7] GSMA (2007) *Pay-Buy Mobile Business Opportunity Analysis*, wersja 1.0, listopad 2007, biała księga. Dostępny pod adresem: http://www.gsmworld.com/documents/gsma_nfc_tech_guide_vs1.pdf (dostęp 10 lipca 2011 r.).

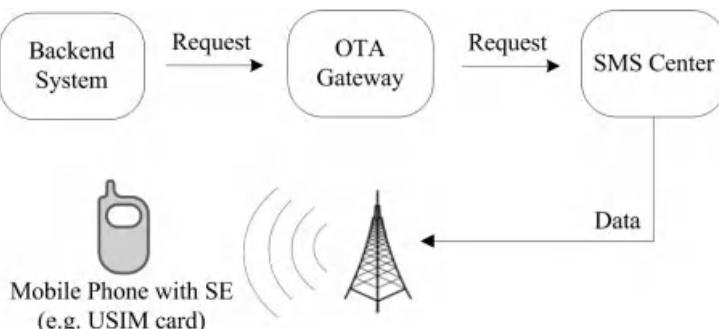
8

Zarządzanie bezpiecznymi elementami

Ekosystem NFC jest niezwykle dynamiczny. Aplikacje obsługujące NFC są często tworzone, pobierane przez telefon komórkowy z obsługą NFC, instalowane na telefonach komórkowych lub Secure Element (SE), konfigurowane i utrzymywane przez powiązane podmioty ekosystemu. Jak omówiono w rozdziale 3, obecnie najlepszą alternatywą dla zarządzania SE, w tym instalacji aplikacji i zdalnego zarządzania, jest użycie uniwersalnej karty z układem scalonym (UICC). UICC zapewnia odpowiednią strukturę karty opartą na specyfikacji karty GlobalPlatform, która umożliwia wiele domen bezpieczeństwa dla różnych aplikacji na tej samej karcie. Każda domena bezpieczeństwa jest w rzeczywistości bezpieczną przestrzenią dla aplikacji NFC, w której przechowywany jest również unikalny klucz bezpieczeństwa aplikacji w celu kontrolowania dostępu do bezpiecznej domeny przez autoryzowaną stronę. Telefony komórkowe obsługujące NFC z odpowiednimi SE mogą być dostępne za pośrednictwem technologii Over-the-Air (OTA), która jest obiecującym i skutecznym sposobem dotarcia do telefonu niezależnie od lokalizacji użytkownika. Korzystanie z OTA umożliwia zdальną instalację, personalizację i zarządzanie cyklem życia aplikacji NFC w SE. Oznacza to, że użytkownik nie musi fizycznie dotykać swojego urządzenia mobilnego z obsługą NFC do systemu, aby wykonać którykolwiek z wymienionych procesów. Ta sekcja koncentruje się na zarządzaniu SE i roli technologii OTA. Przedstawiono również modele wdrażania OTA w SE opartych na UICC oraz zarządzanie wieloma środowiskami SE zgodnie ze specyfikacjami GlobalPlatform.

8.1 Wprowadzenie do technologii OTA

System operacyjny kontrolujący SE w urządzeniu mobilnym musi umożliwiać instalację, personalizację i zarządzanie wieloma aplikacjami - z których każda może być dostarczana przez różnych dostawców - za pośrednictwem technologii OTA. OTA to standard transmisji i odbioru aplikacji oraz informacji związanych z aplikacjami za pośrednictwem mediów komunikacji bezprzewodowej. Korzystając z platformy OTA, można wprowadzać nowe usługi i modyfikować zawartość SE w szybki i opłacalny sposób. Usługa OTA może być świadczona przez operatora sieci komórkowej (MNO) lub inny zaufany podmiot, w zależności od uzgodnionego ekosystemu.



Rysunek 8.1 Podstawowa architektura OTA.

8.1.1 Technologia OTA i zarządzanie urządzeniami mobilnymi

Obecnie karty USIM (Universal Subscriber Identity Module) są przekazywane użytkownikom usług telefonii komórkowej przez operatorów MNO, którzy są ich właścicielami. OSK kontrolują i zarządzają USIM, a niektórzy z nich używają technologii OTA do zarządzania USIM. Obecnie OSK, którzy stworzyli wymaganą infrastrukturę OTA, mają możliwość zdalnej konfiguracji pojedynczego urządzenia mobilnego, całej floty urządzeń mobilnych lub dowolnego zestawu urządzeń mobilnych zdefiniowanych przez IT. Mogą wysyłać aktualizacje oprogramowania i systemu operacyjnego (OS); zdalnie blokować urządzenie w celu ochrony aplikacji i danych, gdy zostanie ono na przykład zgubione lub skradzione; zdalnie rozwiązywać problemy z urządzeniem; i wykonywać inne podobne usługi.

Podstawową architekturę technologii OTA przedstawiono na rysunku 8.1. Zazwyczaj OTA opiera się na architekturze klient-serwer składającej się z systemu zaplecza jako serwera i karty inteligentnej w telefonie komórkowym jako klienta. System zaplecza wysyła żądania, którymi może być operator obsługi klienta do systemu rozliczeniowego, dostawcy treści itp. Żądania te mogą być akcjami, takimi jak aktywacja, dezaktywacja, ładowanie i modyfikacja. Żądania są wysyłane do bramy OTA, która przekształca je w krótkie wiadomości. Następnie te krótkie wiadomości są wysyłane do centrum krótkich wiadomości tekstowych (SMS) przez dostawcę OTA, który przekazuje je do odpowiedniej karty inteligentnej. Polecenia OTA są zazwyczaj wysyłane jako wiadomości SMS. Polecenia te są wykonywane na karcie inteligentnej.

Karty inteligentne zapewniają bezpieczny dostęp użytkownika i są używane głównie jako karty SIM (Subscriber Identification Module) w standardzie GSM. Karta SIM jest głównym elementem ekosystemu GSM, torującym drogę do usług o wartości dodanej. Karty SIM oferują rozszerzone funkcje, takie jak zaawansowane menu, wcześniej zarejestrowane numery do szybkiego wybierania oraz możliwość wysyłania wiadomości SMS w celu przeszukiwania bazy danych, przeprowadzania bezpiecznych transakcji itp. Wraz z rozwojem kart SIM, UICC stały się cennymi kartami inteligentnymi, umożliwiającymi korzystanie z ulepszonych usług, takich jak technologia NFC i zarządzanie OTA.

Technologia OTA niesie ze sobą różne korzyści dla interesariuszy na rynku. Jeśli chodzi o operatorów MNO, ponieważ są oni również wydawcami kart SIM, technologia OTA zapewnia większą efektywność kosztową, zdalne zarządzanie kartami SIM, a tym samym zwiększa wartość inwestycji. Użytkownicy nie muszą fizycznie nigdzie chodzić, aby aktywować lub aktualizować jakiekolwiek usługi. Karty inteligentne w urządzeniach mobilnych nie są już statycznymi komponentami. Mogą przechowywać więcej informacji i mają większą wartość dla użytkownika.

Wykorzystując te zalety, OTA może zaoferować użytkownikom ogromną liczbę równolegkich usług o wartości dodanej. Ponadto technologia OTA pozwala autoryzowanym stronom trzecim zachować kontrolę nad informacjami pobranymi na karty inteligentne. Technologia OTA umożliwia operatorom wybór usług, które są do dyspozycji klienta. Są właścicielami treści, a tym samym klientami.

Z punktu widzenia użytkowników są oni w stanie wybrać usługi, które chcą mieć na swoim spersonalizowanym telefonie. Co więcej, mogą to robić bez względu na miejsce i czas. Mogą pobierać usługi i aktualizować swoje karty inteligentne, gdy są mobilni. Aplikacje (tj. doładowanie subskrypcji prepaid, zmiana zestawu parametrów subskrypcji) można wykonać za pomocą OTA, gdy są mobilni, zamiast zabierać telefon do obsługi klienta. Ta zwiększona jakość usług zapewnia wygodę użytkownikowi i umożliwia kontrolę nad parametrami jego subskrypcji.

8.1.2 *Technologia OTA i urządzenia SE oparte na UICC*

Jak już wspomniano, UICC stał się najpopularniejszym sposobem promowania systemów opartych na NFC przy użyciu technologii OTA. Dzięki technologii OTA nowe aplikacje NFC mogą być dostarczane do UICC, a następnie łatwo nimi zarządzać. Technologia OTA przyczynia się do rozwoju NFC poprzez uelastycznenie i ułatwienie zarządzania aplikacjami NFC w SE. Nowi uczestnicy mogą płynnie uruchamiać swoje aplikacje, a istniejący uczestnicy mogą aktualizować swoje aplikacje w miarę udostępniania nowych wersji. Ponieważ zarządzanie odbywa się za pośrednictwem OTA, konsument nie musi fizycznie odwiedzać sklepu ani podłączać telefonu do stacji dokującej, aby zaktualizować dostępne aplikacje.

Jeśli chodzi o technologię NFC, niezbędne usługi OTA obejmują aktywację i dezaktywację SE, zdalne zarządzanie usługami, zdalne zarządzanie cyklem życia aplikacji NFC na SE.

Wraz z pojawiением się nowych usług obsługujących NFC, zakwaterowanie i zdalne zarządzanie aplikacjami na urządzeniach mobilnych stało się ważnym zagadnieniem. Różne stowarzyszenia intensywnie pracują nad zdalnym zarządzaniem usługami (tj. instalacją, personalizacją, aktualizacją, zakończeniem) i zdalnym zarządzaniem cyklem życia (tj. blokowaniem, odblokowywaniem, ponownym wydawaniem karty, resetowaniem kodu PIN, zmianą, aktualizacją parametrów) SE za pośrednictwem OTA.

W systemach NFC, w których UICC został wybrany jako SE, uczestnicy ekosystemu mają tę zaletę, że mogą korzystać z już istniejącej infrastruktury dostępnej do zarządzania kartami SIM. Operatorzy sieci komórkowych już teraz zajmują się zakupem, dystrybucją, konfiguracją, zarządzaniem i aktualizacją UICC.

Rozważmy przypadek, w którym po wydaniu karty UICC użytkownikowi, użytkownik żąda nowej aplikacji NFC. Jeśli w tej sytuacji zostanie użyta technologia OTA, wydawca SE utworzy bezpieczną przestrzeń (bezpieczną domenę) na UICC dla nowej aplikacji NFC i przypisze unikalny klucz bezpieczeństwa do domeny bezpieczeństwa. Proces ten może być łatwo i bezpiecznie przeprowadzony przez MNO przy użyciu jego platformy OTA. Aplikacja i jej dane mogą być pobierane za pomocą OTA lub alternatywnie mogą być kopiowane z wstępnie załadowanej instancji aplikacji na UICC.

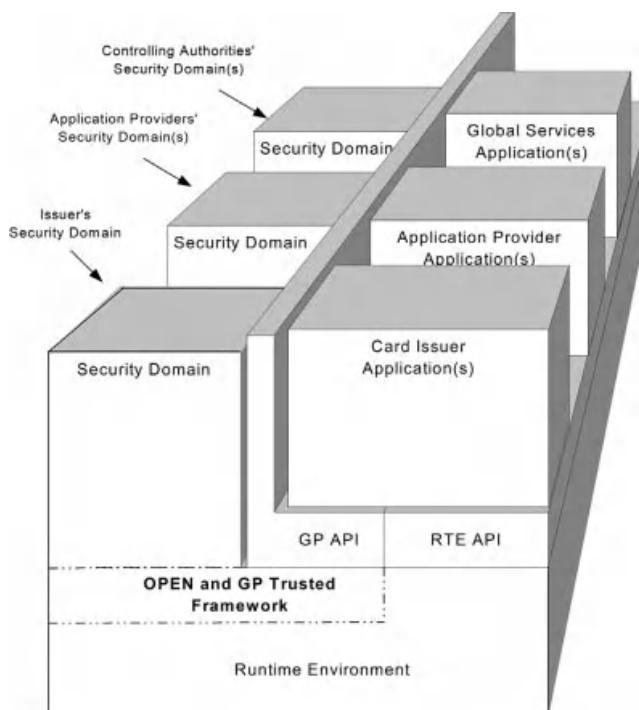
Ponadto możliwe jest zablokowanie lub usunięcie usług obsługujących NFC na UICC, gdy jest to wymagane z jakiegoś powodu. Jest to istotna funkcja, szczególnie w przypadku aplikacji kart kredytowych, gdy telefon komórkowy został zgubiony lub skradziony. MNO może w ten sposób zablokować lub usunąć wszystkie usługi w imieniu dostawców usług NFC.

8.2 GlobalPlatform Specyfikacje

Jak już wspomniano w rozdziale 3, GlobalPlatform jest organizacją członkowską obejmującą ponad 50 organizacji, począwszy od branży płatności i komunikacji, a skończywszy na sektorze rządowym i społeczności sprzedawców. Zaangażowane firmy są pionierami w promowaniu globalnej infrastruktury do wdrażania kart inteligentnych we wszystkich możliwych branżach. Czują się odpowiedzialne za promowanie interoperacyjnych specyfikacji technicznych niezbędnych do obsługi kart inteligentnych i odpowiedniego zarządzania systemem kart inteligentnych dla wydawców kart. GlobalPlatform zapewnia specyfikację karty, która jest obecnie akceptowana jako właściwy model karty i oferuje bezpieczne i elastyczne zarządzanie zawartością karty w wielu aplikacjach (tj. ładowanie, instalacja, ekstradycja, aktualizacja rejestru i usuwanie zawartości karty) podczas cyklu życia karty.

8.2.1 Karta GlobalPlatform Specyfikacja

Niniejsza sekcja ma na celu podkreślenie głównych właściwości specyfikacji kart GlobalPlatform [1]. Zgodnie ze specyfikacją karty GlobalPlatform, karta inteligentna składa się z szeregu logicznych i fizycznych komponentów, które mają na celu zapewnienie interoperacyjności aplikacji i bezpieczeństwa w środowisku kontrolowanym przez emitenta. Specyfikację karty inteligentnej przedstawiono na rysunku 8.2. Środowisko Run Time Environment (RTE), środowisko GP Environment (OPEN) i GP Trusted Framework, jako



Rysunek 8.2 Architektura karty GlobalPlatform. Powielone za zgodą GlobalPlatform.

Komponenty komunikacyjne znajdują się nad mikroprocesorem karty inteligentnej. Pozostała część karty inteligentnej jest podzielona na jedną lub więcej usług wydawcy karty, dostawcy aplikacji i usług globalnych, a także na ich domeny bezpieczeństwa.

GlobalPlatform ma działać na dowolnej bezpiecznej karcie RTE z wieloma aplikacjami; w t e n s p o s ó b GlobalPlatform nie narzuca konkretnej technologii RTE. RTE składa się z trzech głównych komponentów: Smart Card Operating System (SCOS), maszyny wirtualnej (VM) i interfejsu programowania aplikacji (API). RTE jest odpowiedzialny za zapewnienie neutralnego sprzętowo API dla aplikacji, a także bezpiecznej przestrzeni do przechowywania i wykonywania aplikacji. Maszyna wirtualna działa jako interpreter między SCOS a aplikacjami. RTE zapewnia interfejs API RTE, który obejmuje zestaw usług wykorzystywanych przez aplikacje kart inteligentnych, takich jak komunikacja między aplikacjami i bezpieczna izolacja aplikacji. Karty GlobalPlatform mogą zawierać jeden lub więcej zaufanych framework'ów, które zapewniają usługi komunikacji między aplikacjami. Zaufane struktury mają specjalny status; są częścią lub mają rozszerzenia RTE karty.

OPEN udostępnia GP API dla aplikacji. GP API odpowiada za wysyłanie poleceń, wybór aplikacji, (opcjonalne) zarządzanie kanałami logicznymi i usługi zarządzania zawartością karty (np. blokowanie, aktualizowanie). GlobalPlatform udostępnia specyfikacje API dla MULTOS oraz JavaCard. Szczegóły GP API dla kart JavaCard i MULTOS można znaleźć w specyfikacji GlobalPlatform.

Domeny bezpieczeństwa są niezwykle ważne dla kart opartych na GlobalPlatform. Domeny bezpieczeństwa działają jako przedstawiciele władz poza kartą. Umożliwiają one bezpieczne zarządzanie aplikacjami poprzez zapewnienie pełnej separacji kluczy kryptograficznych, a także posiadanych aplikacji i danych między wydawcami kart a pozostałymi domenami bezpieczeństwa, które są własnością powiązanych dostawców aplikacji. Istnieją trzy główne kategorie domen bezpieczeństwa odzwierciedlające różne typy organów pozakartowych rozpoznawanych przez kartę:

- Emitent Security Domain (ISD) jest głównym i obowiązkowym przedstawicielem wydawcy karty na karcie. Ta domena bezpieczeństwa reprezentuje terytorium wydawcy na karcie i kontroluje aplikacje wydawcy.
- Dodatkowa domena bezpieczeństwa (SSD) lub domena bezpieczeństwa dostawcy aplikacji (APSD)
jest przedstawicielem na karcie dostawców aplikacji i wydawców kart lub ich agentów. Mechanizm ten umożliwia dostawcom aplikacji współdzielenie i wykorzystywanie pewnej przestrzeni na karcie bez ryzyka naruszenia zarządzania kartą lub jakąkolwiek aplikacją na karcie. Ta domena bezpieczeństwa deleguje niektóre możliwości zarządzania treścią do zaufanych dostawców aplikacji. Oszczędza to czas wydawcy karty w odniesieniu do dodatkowych zadań administracyjnych.
- Controlling Authority Security Domain (CASD) to specjalny typ dysku SSD. Rolą domeny Organ kontrolujący ma za zadanie egzekwować politykę bezpieczeństwa dla wszystkich aplikacji, które mają być lub są już załadowane na kartę. Organ kontrolujący używa również tego typu domeny bezpieczeństwa jako swojego przedstawiciela na karcie.

Domeny bezpieczeństwa obsługują różne usługi bezpieczeństwa, takie jak obsługa kluczy, szyfrowanie, deszyfrowanie, generowanie podpisu cyfrowego i weryfikacja dla aplikacji ich dostawców (tj. wydawcy kart, dostawcy aplikacji lub organu kontrolnego). Każda domena bezpieczeństwa jest ustanawiana w imieniu konkretnego wydawcy karty, dostawcy aplikacji lub organu kontrolnego. Gdy te podmioty spoza karty używają kluczy specyficznych dla domeny, które są całkowicie odizolowane od siebie, aplikacje wchodzą w interakcję z powiązaną domeną bezpieczeństwa za pośrednictwem interfejsu API GP.

Menedżer kart jest głównym komponentem kart GlobalPlatform, który działa jako centralny administrator karty GlobalPlatform. Można go postrzegać jako połączenie trzech podmiotów: OPEN, ISD i Cardholder Verification Method Services, które są jedną z ważnych globalnych aplikacji usługowych.

Głównym celem GlobalPlatform jest zapewnienie bezpieczeństwa i integralności RTE, OPEN, ISD, SSD i aplikacji do zarządzania cyklem życia karty inteligentnej. Integralność danych, dostępność zasobów, poufność i mechanizmy uwierzytelniania są w pełni obsługiwane na kartach opartych na GlobalPlatform poprzez treść specyfikacji.

GlobalPlatform został zaprojektowany tak, aby zapewnić maksymalną elastyczność wydawcy karty, jak również jego partnerom biznesowym w zakresie zarządzania treścią karty. Ze względu na tę elastyczność, wydawca karty może delegować lub autoryzować funkcje zarządzania treścią karty do dostawcy usług, co zostanie omówione w następnej sekcji. Szczegóły dotyczące specyfikacji kart można znaleźć na stronie GlobalPlatform.

8.2.2 *GlobalPlatform Messaging Specyfikacja*

Specyfikacja komunikatów GlobalPlatform definiuje zestaw standardowych komunikatów do wymiany danych między podmiotami w środowisku kart inteligentnych [2]. Specyfikacja ta ma również zastosowanie do wszystkich SE (tj. wbudowanego sprzętu, SMC i UICC) w telefonach komórkowych NFC. Specyfikacja jest wykorzystywana w celu zapewnienia standardowej infrastruktury i uniknięcia zastrzeżonych rozwiązań, a tym samym do płynnej wymiany informacji, promowania standardowych interakcji między graczami, a także ułatwienia łatwej integracji nowych graczy w ekosystemie kart inteligentnych. Zapewnia interoperacyjność na trzech głównych poziomach: dane biznesowe (tj. wspólne słownictwo), proces biznesowy (tj. rola, obowiązki, proces i ograniczenia) oraz wymiana danych (tj. struktura danych, integralność i bezpieczeństwo informacji, obsługa błędów itp.). Szczegóły dotyczące specyfikacji komunikatów [3] można znaleźć na stronie internetowej GlobalPlatform.

8.3 Zarządzanie cyklem życia SE

Zarządzanie cyklem życia SE w telefonie komórkowym NFC rozpoczyna się po wydaniu SE użytkownikowi. Cykl życia można zidentyfikować za pomocą dwóch faz, a mianowicie *procesu instalacji i personalizacji* oraz *procesu zdalnego zarządzania*. Proces zdalnego zarządzania rozpoczyna się po instalacji i personalizacji aplikacji NFC. Początkowo posiadacz karty - jako użytkownik - pobiera aplikację NFC, tworzona jest powiązana domena bezpieczeństwa wraz z jej kluczami, a aplikacja jest instalowana na SE. Następnie można przeprowadzić zdalny proces personalizacji i zdalnie zarządzać nową aplikacją (tj. aktualizować ją, usuwać, odnawiać).

Ponieważ procesy instalacji, personalizacji i zdalnego zarządzania mogą być wykonywane na wszystkich opcjach SE (tj. wbudowanym sprzęcie, bezpiecznej karcie pamięci, UICC), ustanowienie nowych domen bezpieczeństwa na każdym typie SE wymaga innej infrastruktury technologicznej. Obecnie dostęp do SE opartych na sprzęcie wbudowanym i bezpiecznej karcie pamięci (SMC) można uzyskać tylko przez OTA za pośrednictwem proxy midlet. Połączenie to wymaga zainicjowania komunikacji po stronie telefonu komórkowego i ustanowienia bezpiecznego połączenia http przy użyciu komunikacji GPRS lub 3G.

Jak już wspomniano, SE oparte na UICC zapewniają doskonałą okazję do szerokiego wsparcia klienta za pośrednictwem OTA. W tym rozdziale zarządzanie cyklem życia SE opartych na UICC jest głównie

objęte. GlobalPlatform określa trzy modele procesu instalacji i personalizacji aplikacji NFC na UICC: tryb prosty, tryb delegowany i tryb autoryzowany. Modele te mogą być również stosowane dla innych opcji SE z różnymi infrastrukturami i wymaganiami. Inne szczegóły dotyczące zarządzania zawartością karty i konfiguracji UICC można znaleźć w specyfikacji karty GlobalPlatform. Ta sekcja pokrótkę obejmuje wymaganą wiedzę podstawową, taką jak znaczenie Trusted Service Managers (TSM), role i podmioty zdefiniowane przez GlobalPlatform, strukturę UICC w zależności od GlobalPlatform, a także modele zarządzania GlobalPlatform dla procesu instalacji i personalizacji aplikacji.

8.3.1 TSM w środowisku NFC

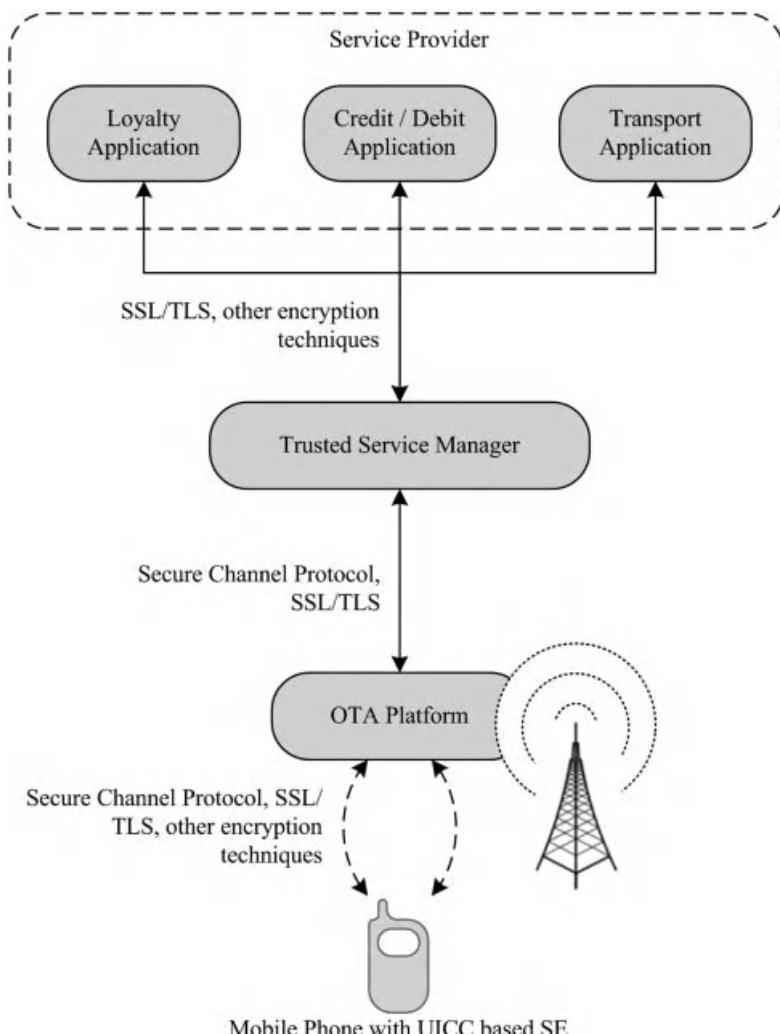
Ekosystem NFC jest z natury złożonym środowiskiem. Składa się z różnych graczy, od producentów komponentów NFC po konsumentów. Szczegółowa analiza biznesowa ekosystemu NFC została już omówiona w rozdziale 7. Jak wyszczególniono tam, głównymi uczestnikami ekosystemu są dostawcy sprzętu, dostawcy usług (np. bankowe podmioty finansowe, organy tranzytowe, detaliści, którzy chcą wdrażać i zarządzać usługami na SE użytkowników), wydawcy kart (lub wydawcy SE), MNO i dostawcy platform OTA. W większości prototypów i testów usług NFC, MNO wydają SE, a niektóre z nich są również właścicielami i zarządzają platformą OTA. Możliwe jest jednak również, że wydawanie SE, a także dostarczanie OTA może być wykonywane przez zaufane podmioty inne niż OSK.

Aby wdrożyć aplikacje i usługi NFC w SE użytkowników, dostawcy usług i MNO mają różne wymagania. Aby stworzyć i zarządzać zaufanym środowiskiem oraz umożliwić podmiotom bezpieczną komunikację między sobą, wymagany jest dodatkowy zaufany podmiot. TSM jest niezależną stroną obsługującą inne podmioty ekosystemu NFC zgodnie z wymaganiami. Zapewnia poziom zaufania i bezpieczeństwa między głównymi uczestnikami systemu, takimi jak dostawcy usług i operatorzy sieci MNO, podczas zarządzania cyklem życia aplikacji.

Jeśli TSM nie istnieje w ekosystemie, każdy gracz musi komunikować się bezpośrednio z każdym innym graczem, aby skutecznie zarządzać zawartością kart, co tworzy złożony i niepewny system. Zamiast tego TSM odgrywa rolę centralnego organu w systemie. Alternatywnie, funkcje zarządzania zawartością karty mogą być ustanowione albo przez podejście skoncentrowane na wydawcy karty, które wykorzystuje platformę OTA wydawcy karty, albo przez podejście skoncentrowane na niezależnym TSM, które wykorzystuje platformę OTA TSM. Cechy architektoniczne i techniczne niezależnego wdrożenia OTA i zarządzania zawartością karty zgodnie z tym scenariuszem zostaną omówione w następnej sekcji.

Rozważmy teraz aplikacje płatnicze z obsługą NFC działające na UICC. Z natury jest to bardzo złożony i dynamiczny świat. Obecnie na całym świecie istnieją różne modele współpracy w ekosystemie płatności mobilnych. W tym modelu wymagana jest współpraca między instytucjami finansowymi, MNO i innymi interesariuszami w ekosystemie płatności mobilnych, a także TSM, który musi odgrywać centralną rolę między MNO a dostawcami usług. Na przykład TSM może dostarczyć informacje o rachunku płatniczym użytkownika po otrzymaniu ich od instytucji finansowej za pośrednictwem OTA do UICC; oznacza to, że użytkownik może używać swojego telefonu komórkowego jako wirtualnej karty kredytowej lub debetowej (patrz rysunek 8.3). Platforma OTA TSM lub MNO może być używana w zależności od modelu wdrożenia, jak przedstawiono w następnej sekcji.

Jak już wspomniano, podstawową funkcją TSM jest zapewnienie bezpieczeństwa między podmiotami ekosystemu. GlobalPlatform zdefiniował protokół bezpiecznego kanału (SCP), który zapewnia bezpieczną funkcjonalność komunikacji i przechowywania wrażliwych danych między TSM a SE z ekosystemu.



Rysunek 8.3 Środowisko NFC i mechanizmy bezpieczeństwa.

telefon komórkowy. Różne typy SCP (np. SCP01, SCP02) są zdefiniowane w specyfikacji karty GlobalPlatform [1]. SCP jest używany przez TSM, gdy próbuje dotrzeć do domen bezpieczeństwa na UICC za pośrednictwem OTA, jak przedstawiono w modelach wdrażania w następnej sekcji. TSM wykorzystuje również inne mechanizmy bezpieczeństwa, takie jak infrastruktura klucza publicznego (PKI), wirtualna sieć prywatna (VPN) i techniki szyfrowania Secure Sockets Layer (SSL)/Transport Layer Security (TLS).

8.3.2 Aktorzy i ich role funkcjonalne w GlobalPlatform

GlobalPlatform definiuje pięć głównych podmiotów w ekosystemie NFC: dostawcę usług, dostawcę kart SIM, MNO, TSM i organ kontrolny. GlobalPlatform definiuje również różne role, którymi są

przyjęte przez tych aktorów. Każdy aktor może pełnić jedną lub więcej ról. Role zdefiniowane przez GlobalPlatform [2] są następujące:

- *Właściciel aplikacji* to osoba, która utrzymuje specyfikacje związane z aplikacją.
 - *Programista aplikacji* to osoba, która projektuje i wdraża kod aplikacji.
 - *Dostawca aplikacji* jest tym, który dostarcza komponent do załadowania aplikacji (tj., kod aplikacji, dane aplikacji, klucze aplikacji i/lub certyfikaty oraz dane należące do konkretnego posiadacza karty) na kartę.
 - *Program obsługujący karty* wykonuje funkcje personalizacji wstępnej; ładowanie początkowych zabezpieczeń emitenta domenę, domenę zabezpieczeń organu kontrolującego oraz, jeśli istnieją, dodatkowe domeny zabezpieczeń dostawcy aplikacji.
 - *Producent kart* to podmiot, który produkuje karty zgodnie z wymaganiami wydawca karty.
 - *Producent układów scalonych (IC)* to podmiot, który wytwarza płytki zawierające chipy z określona konfiguracją ROM.
 - *Platform* jest osobą odpowiedzialną za rozwój GlobalPlatform zgodnie ze specyfikacjami dostarczonymi przez konsorcjum GlobalPlatform.
 - *Właściciel platformy* definiuje i utrzymuje specyfikacje systemu operacyjnego platformy karty.
 - *Wydawca karty* jest tym, który ponosi ostateczną odpowiedzialność za SE. Jest to jedyny organ aby umożliwić ładowanie, instalację, usuwanie, dodawanie i personalizację aplikacji. Ponadto wydawca karty może delegować te czynności stronie trzeciej, takiej jak dostawca aplikacji, za pośrednictwem menedżera SSD.
 - *Loader* ładuje aplikacje i dane personalizacyjne na karty specyficzne dla wydawcy karty zgodnie z instrukcjami dostawcy aplikacji, przestrzegając zasad i procedur bezpieczeństwa określonych przez wydawcę karty.
 - *Menedżer SSD* zarządza domenami zabezpieczeń na karcie. Przechowuje on SCP (tj., SCP02 i SCP80) klucze i certyfikaty należące do bezpiecznej domeny i umożliwia bezpieczną komunikację z bezpieczną domeną, którą zarządza. SCP02 to symetryczny protokół bezpiecznego kanału umożliwiający przesyłanie wiadomości skryptowych, które można odbierać bezpośrednio za pośrednictwem interfejsów stykowych i bezstykowych. SCP80 to protokół bezpiecznego kanału OTA umożliwiający bezpośredni dostęp do domeny bezpieczeństwa z platformy OTA za pośrednictwem sieci GSM. Menedżer SSD ma możliwość ładowania, instalowania, ekstradykcji i personalizacji aplikacji w imieniu dostawcy usług. Jego rolą nie jest zarządzanie aplikacjami na karcie inteligentnej, ale dostarczanie i pośredniczenie w bezpiecznej domenie w celu zarządzania zawartością karty i wykonywania usług kryptograficznych.
 - *Collator i decollator* to osoby, które dokonują zestawienia (agregacji danych) osób. Dane alizacyjne od wszystkich dostawców usług dla posiadacza karty po załadowaniu aplikacji przez program ładujący. Wykonuje funkcję dekorelacji w celu zwrócenia informacji do wydawcy karty i odpowiednich dostawców aplikacji.
 - *Organ kontrolny* jest najważniejszym i najbardziej wymaganym podmiotem dla zachowania poufności.
- ładowanie i personalizacja aplikacji. Podmiotem tym może być urząd certyfikacji lub sprzedawca karty SIM. Klucze i certyfikaty organu kontrolującego są ładowane do bezpiecznej domeny organu kontrolującego (CASD) na karcie UICC przez producenta karty podczas procesu produkcji UICC. Organ kontrolujący zapewnia podpisy bloków

danych pliku ładowania zgodnie z własną polityką bezpieczeństwa w zakresie integralności i autentyczności źródła. Podmiot organu kontrolującego musi być zaufaną stroną dla podmiotu obsługującego platformę OTA, a także dla podmiotu wykonującego personalizację aplikacji na UICC.

8.3.3 UICC Based SE: Domeny bezpieczeństwa i hierarchia

Jak już wspomniano, obecnie SE oparty na UICC wykorzystuje strukturę kart opartą na GlobalPlatform jako architekturę referencyjną do obsługi systemów opartych na NFC. UICC może hostować wiele różnych aplikacji należących do wydawcy karty lub innych stron, z których każda definiuje i kontroluje własną aplikację. UICC ma oddzielną domenę bezpieczeństwa dla każdej aplikacji lub dla każdego dostawcy aplikacji zarządzanego przez wydawcę aplikacji i opartego na wykorzystaniu tajnych kluczy administracyjnych. SCOS na karcie implementuje zaporę sieciową, która uniemożliwia aplikacjom dostęp do danych lub udostępnianie ich między sobą.

Każdy SE oparty na UICC zgodny z GlobalPlatform jest dostarczany z jednym ISD i opcją dla pojedynczego lub wielu dysków SSD. Te dyski SSD mogą być domenami bezpieczeństwa TSM lub domenami bezpieczeństwa dostawcy usług, takimi jak karty kredytowe, transport, bilety i aplikacje lojalnościowe. Obszary aplikacji i przechowywania danych TSM i dostawców usług są oddzielone i odizolowane od siebie. Dodatkowo, każdy SE oparty na UICC ma tylko jeden CASD. Architektura ta umożliwia wydawcom kart, dostawcom usług i TSM zarządzanie kluczami i weryfikację aplikacji podczas ładowania aplikacji i procesów personalizacji.

W obszarze ISD UICC wydawca karty (głównie MNO) przechowuje klucze do udostępniania OTA, zarządzania zawartością karty i zarządzania domeną bezpieczeństwa. ISD jest tworzony podczas procesu produkcyjnego, a klucz do zarządzania zawartością karty jest następnie bezpiecznie przesyłany od producenta do MNO. Zgodnie ze specyfikacjami GlobalPlatform, ISD musi autoryzować tworzenie dowolnych dysków SSD, tak aby tylko ISD miał uprawnienia do tworzenia dysków SSD. Ponadto tylko ISD może przypisać autoryzowane lub delegowane uprawnienia do zarządzania.

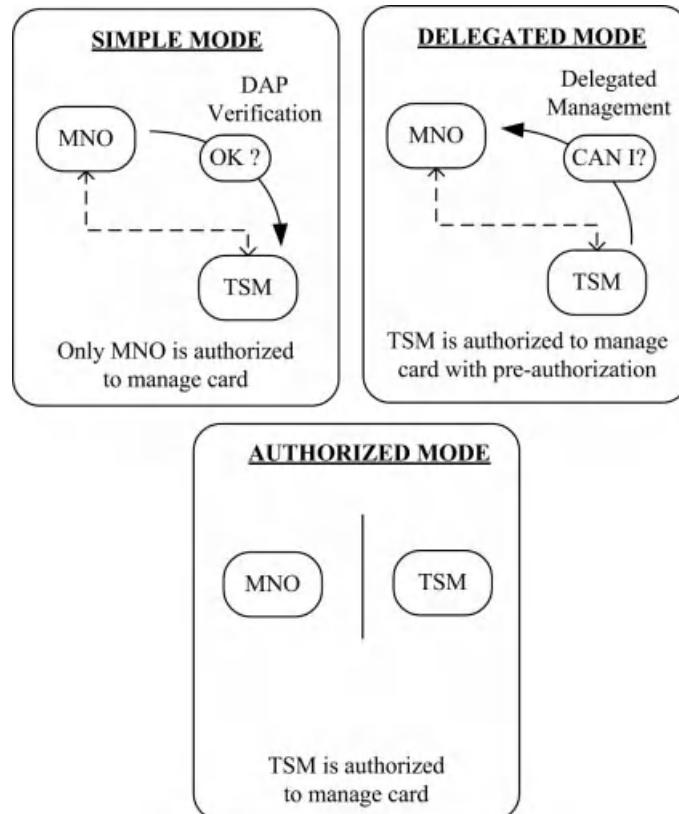
8.3.4 Zarządzanie UICC Modele

Zgodnie ze specyfikacją GlobalPlatform [2] proces zarządzania zawartością karty obejmuje następujące działania: poufne ładowanie początkowego zestawu kluczy domeny bezpieczeństwa strony trzeciej, ładowanie aplikacji i personalizację. GlobalPlatform proponuje trzy modele zarządzania zawartością karty: tryb prosty, tryb delegowany i tryb autoryzowany dla SE, jak pokazano na rysunku 8.4. Modele te obejmują ładowanie aplikacji i procesy personalizacji na kartach UICC. Tryb prosty jest modelem skoncentrowanym na wydawcy karty, podczas gdy tryb delegowany i tryb autoryzowany są modelami bardziej skoncentrowanymi na TSM (patrz rozdział 7). Specyfikacja komunikatów GlobalPlatform obsługuje wszystkie modele wdrażania [2, 3]. Zasadnicze szczegóły techniczne i architektoniczne tych trybów podano poniżej.

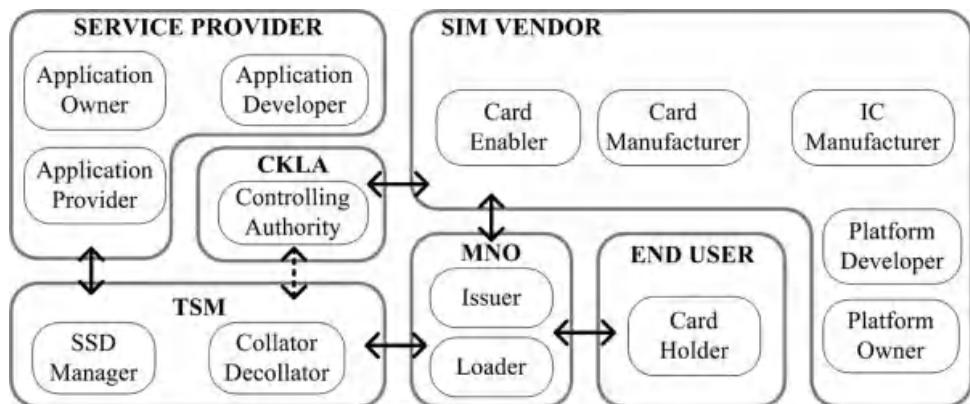
(i) Tryb prosty przy użyciu platformy MNO OTA

W trybie prostym dostawca usług deleguje pełne zarządzanie swoją aplikacją obsługującą NFC do TSM. TSM zarządza domeną bezpieczeństwa w imieniu usługodawcy. MNO jest upoważniony do wykonywania funkcji zarządzania zawartością karty, tj. ładowania, instalowania, aktywowania i usuwania aplikacji na SE. TSM zarządza jedynie procesami blokowania, odblokowywania i personalizacji aplikacji przy użyciu własnego serwera OTA i sieci MNO.

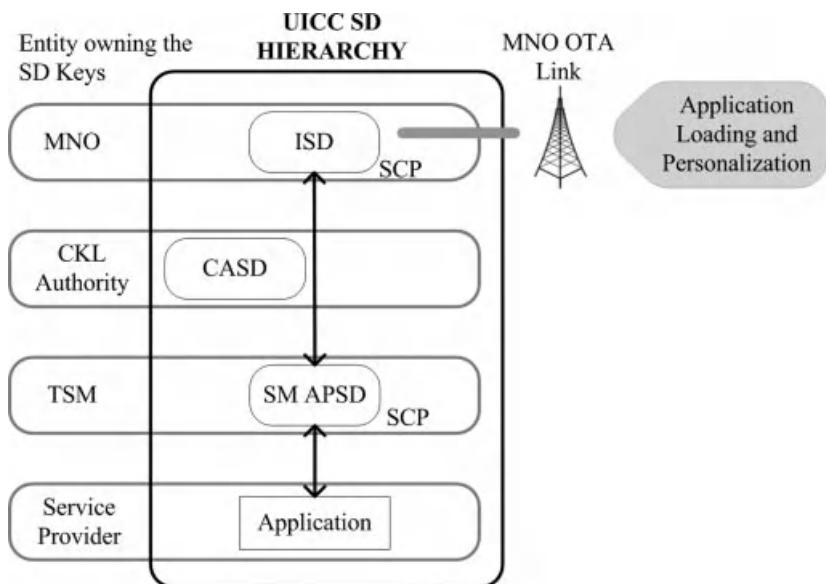
Jak widać na rysunku 8.5, MNO pełni rolę ładowarki. TSM może jednak monitorować ładowanie aplikacji, dostarczając sygnaturę Data Authentication Pattern (DAP) do MNO. Weryfikacja DAP służy do uwierzytelniania i sprawdzania integralności aplikacji załadowanej na UICC.



Rysunek 8.4 Modele zarządzania aplikacjami. Powielone za zgodą GlobalPlatform.



Rysunek 8.5 Role aktorów w trybie prostym przy użyciu platformy MNO OTA. Powielono za zgodą GlobalPlatform.



Rysunek 8.6 Tryb prosty wykorzystujący platformę MNO OTA na UICC. Powielono za zgodą GlobalPlatform.

Jak pokazano na rysunku 8.6, każdy aktor ma własną domenę bezpieczeństwa na UICC w celu obsługi usług bezpieczeństwa, takich jak obsługa kluczy, szyfrowanie, deszyfrowanie, generowanie podpisu cyfrowego i weryfikacja aplikacji należących do tego aktora. Proces ładowania zawartości umożliwia podmiotowi spoza karty (z reprezentacją na karcie za pośrednictwem bezpiecznej domeny) dodawanie zawartości do karty.

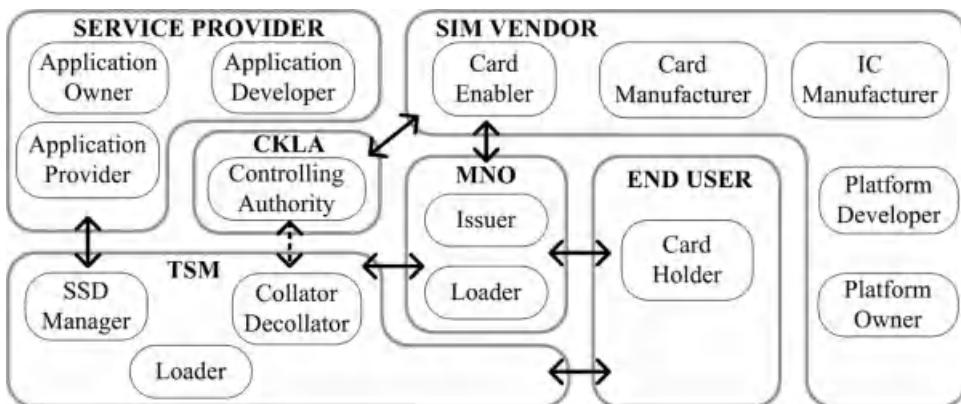
MNO ma ISD na bezpiecznym UICC; organ ładujący klucze poufne (CKLA) ma bezpieczną domenę organu kontrolującego (CASD). TSM umożliwia połączenie między dostawcą usług a MNO za pośrednictwem SCP na karcie i ma domenę bezpieczeństwa dostawcy aplikacji w trybie prostym (SM APSD), która ustanawia aplikację dostawcy usług.

TSM wykorzystuje platformę MNO OTA do tworzenia SM APSD. Klucze SM APSD są tworzone i pobierane przez TSM w celu zarządzania aplikacjami w sposób poufnny. Platforma TSM OTA nie jest całkowicie zaangażowana w tryb prosty.

(ii) *Tryb delegowany z pełną delegacją do TSM*

Przypadek delegowanego zarządzania można opisać jako ładowanie centralne TSM. W tym przypadku MNO nie jest już odpowiedzialny za ładowanie, instalowanie, aktywowanie lub usuwanie aplikacji (patrz rysunek 8.7). Zarządzanie zawartością karty jest wykonywane przez TSM ze wstępna autoryzacją ze strony MNO. W niektórych przypadkach dostawca usług może potrzebować zarządzać własnym procesem personalizacji aplikacji, aby zapobiec manipulowaniu przez osoby trzecie kluczami aplikacji lub danymi aplikacji, które są cenne dla jego klientów.

Uprawnienie do zarządzania delegowanego umożliwia delegowane ładowanie, instalację, ekstradycję, aktualizację i usuwanie. Dostawca usług deleguje pełne zarządzanie swoją aplikacją do TSM, a TSM jest odpowiedzialny za utworzenie swojego APSD i zarządzanie nim.



Rysunek 8.7 Role aktorów w trybie delegowanym z pełną delegacją do TSM. Powielono za zgodą GlobalPlatform.

ładowanie aplikacji i proces personalizacji. TSM będzie korzystać z własnej platformy OTA. MNO musi dostarczyć token zarządzania do TSM w celu wykonania wstępnie autoryzowanej akcji zarządzania zawartością karty. Ten token zarządzania może być również identyfikowany jako *token ładowania*, który jest podpisem cyfrowym wykonywanym wyłącznie przez wydawcę karty. W przypadku blokowania/odblokowywania aplikacji i personalizacji nie ma potrzeby delegowania tokena zarządzania; TSM może działać bez tokena. Podobnie klucze APSD są tworzone i pobierane przez TSM w sposób poufny.

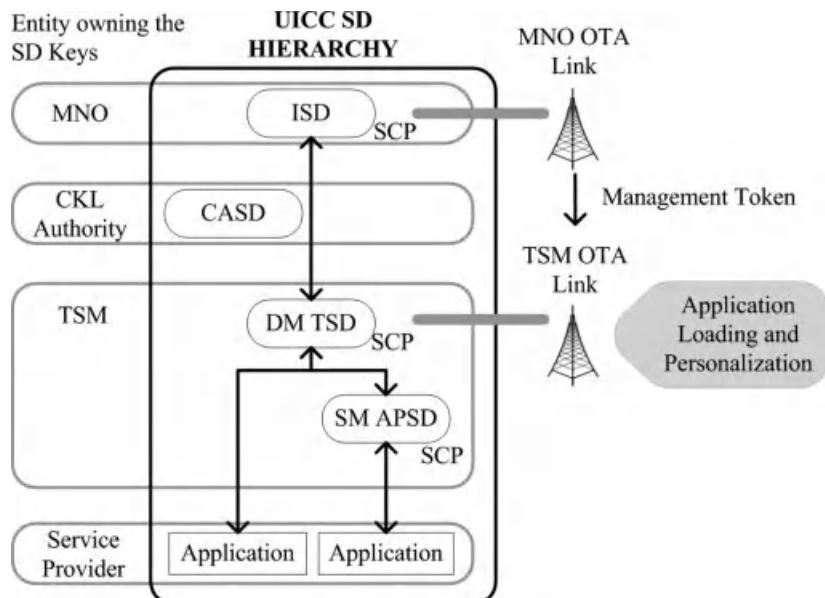
Delegowane zarządzanie upoważnia wydawców kart do korzystania z mechanizmu preautoryzacji. W ten sposób wydawcy kart są chronieni przed nieautoryzowanymi zmianami i odrzucają odpowiedzialność za zarządzanie aplikacjami poza ich bezpośrednim zainteresowaniem. Jednocześnie dostawcy usług mają zapewnioną elastyczność w zarządzaniu własnymi aplikacjami.

Jak widać na rysunku 8.8, MNO ma własną domenę bezpieczeństwa jako ISD na karcie UICC, a CKLA ma CASD. TSM umożliwia ustanowienie połączenia między dostawcą usług a MNO za pośrednictwem SCP na UICC. W trybie delegowanym TSM tworzy własną domenę bezpieczeństwa TSM (TSD) na UICC z preautoryzacją dostarczoną przez wydawcę karty. Aplikację dostawcy usług można załadować na dwa sposoby: można ją załadować bezpośrednio na TSD w trybie delegowanym (DM TSD) lub na dedykowanym APSD w trybie prostym (SM APSD), który jest przypisany do aplikacji.

(iii) Tryb autoryzowany z pełną delegacją do TSM

Wdrożenie autoryzowanego zarządzania jest całkowicie zorganizowane wokół opcji centralnego ładowania TSM. TSM posiada aplikacje dostawcy usług i jest w stanie zarządzać zawartością karty bez autoryzacji (lub konieczności użycia tokena) od MNO. Podobnie jak w trybie delegowanym, dostawca usług może zarządzać własną personalizacją aplikacji zamiast delegować ją do TSM. OSK nie ma powiązań z użytkownikiem końcowym, a także nie pełni już roli ładowarki, jak pokazano na rysunku 8.9.

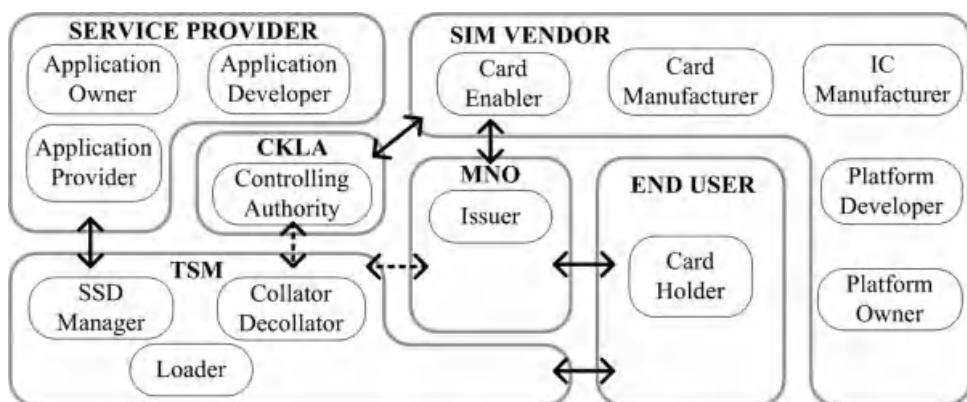
W tym trybie dostawca usług deleguje zarządzanie zawartością karty swojej aplikacji do TSM, a TSM korzysta z własnej platformy OTA. W związku z tym TSM ma pełną elastyczność w zakresie tworzenia domeny bezpieczeństwa jako TSD trybu autoryzowanego (AM TSD) i ładowania



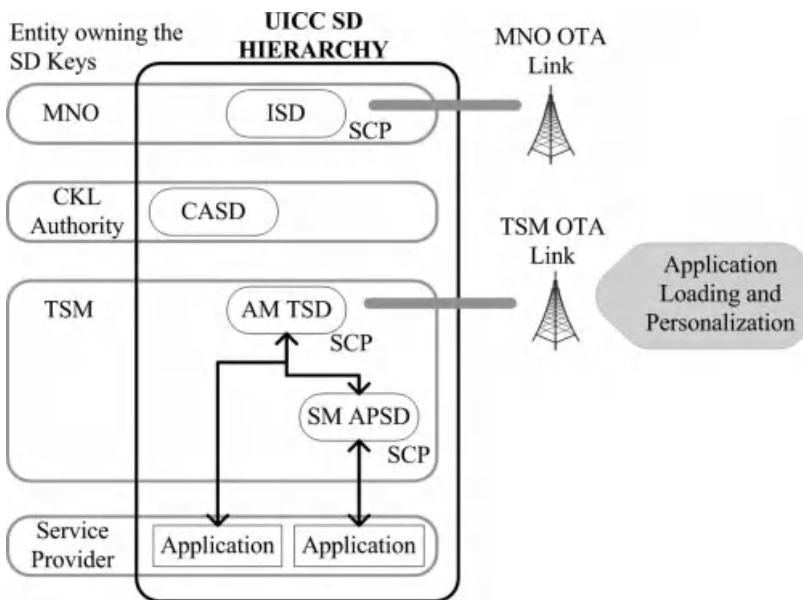
Rysunek 8.8 Tryb delegowany z pełną delegacją do TSM na UICC. Powielono za zgodą GlobalPlatform.

aplikacji bez autoryzacji MNO. Klucze APSD są tworzone i pobierane przez TSM w sposób poufny.

Jak widać na rysunku 8.10, TSM tworzy własną domenę bezpieczeństwa na UICC. Aplikacja dostawcy usług może być ładowana bezpośrednio w ramach AM TSD lub alternatywnie dla każdej aplikacji można przypisać dedykowany i oddzielny APSD trybu prostego (SM APSD). Podczas ładowania aplikacji i procesów personalizacji nie ma połączenia ani łącza komunikacyjnego z MNO i jego platformą OTA.



Rysunek 8.9 Role aktorów w trybie autoryzowanym z pełną delegacją do TSM. Powielono za zgodą GlobalPlatform.



Rysunek 8.10 Tryb autoryzowany z pełną delegacją do TSM na UICC. Powielono za zgodą GlobalPlatform.

8.4 Wiele środowisk SE

Można również zauważyć, że telefon komórkowy z obsługą NFC może obsługiwać wiele SE. Na przykład telefon komórkowy może zawierać wbudowany sprzęt lub SMC wraz z SE opartym na UICC, który jest wbudowany przez MNO przed przekazaniem telefonu komórkowego klientowi. Tak więc każdy wydawca SE może oferować portfolio aplikacji i usług świadczonych przez różnych dostawców usług na odpowiednim SE.

Wiele problemów może pojawić się, gdy wiele SE znajduje się na tym samym telefonie komórkowym z obsługą NFC; szczególnie najważniejszy z nich może wystąpić podczas wdrażania aplikacji w trybie emulacji karty. Czytnik NFC musi zainicjować komunikację tylko z jednym SE na telefonie komórkowym obsługującym NFC. Innym problemem jest zarządzanie wieloma SE w tym samym czasie. GlobalPlatform wykonał cenną pracę nad potencjalnymi konsekwencjami zarządzania wieloma SE w tym samym telefonie komórkowym. Dokument GlobalPlatform [4] podaje szczegóły zarządzania wieloma SE w jednym telefonie komórkowym w celu dostarczania aplikacji i usług NFC. Podsumowując dokument [4], można wykonać dwa modele biznesowe: architekturę bez agregacji i architekturę z agregacją. Każdy model ma swoje własne wymagania; jednak te modele biznesowe należy rozpatrywać bardziej pod kątem kompatybilności i interoperacyjności.

8.4.1 Architektura bez agregacji

Zgodnie z tym modelem, jeśli wiele SE jest hostowanych na tym samym telefonie komórkowym z obsługą NFC, dostępność usług między aplikacjami znajdującymi się na różnych SE może się różnić w zależności od

możliwości SE, takie jak infrastruktura i poziom bezpieczeństwa SE, możliwość wyłączenia zasilania itp. Dostępność usług może się również różnić w zależności od poziomu obsługi klienta zapewnianego przez emitentów SE i dostawców usług.

W tym modelu kontroler NFC może być używany tylko przez jeden SE w danym czasie. Z tego powodu tylko jeden SE może być aktywny w danym momencie. Gdy u ż y w a n y jest model "bez agregacji", SE jest aktywowany przez użytkownika, dzięki czemu aktywowany SE może wykonywać transakcje zbliżeniowe z obsługą NFC. Wybór SE zależy oczywiście od usługi, która ma być używana, i należy wybrać SE, który zawiera powiązaną aplikację; użytkownik jest odpowiedzialny za wybór właściwego SE w tym trybie. Jeśli użytkownik chce korzystać z aplikacji NFC hostowanej w aktualnie nieaktywnym SE, musi przełączyć aktywny SE. Kolejnym ważnym wymogiem jest mechanizm zapory sieciowej pomiędzy SE. Firewall zapewnia, że informacje z SE nie mogą zostać pobrane przez inny SE bez autoryzacji wystawcy SE.

Wyboru aktywnego SE można dokonać za pośrednictwem menu telefonu komórkowego za zgodą użytkownika. Menu wyświetla informacje związane tylko z SE i nie są wyświetlane żadne informacje o aplikacjach w SE. Po wybraniu SE można wyświetlić listę aplikacji. Interfejs ten musi być tak dynamiczny, aby po załadowaniu nowej aplikacji do SE lub usunięciu aplikacji, lista wszystkich bieżących aplikacji w SE była pobierana z SE i wyświetlana użytkownikowi.

Ponadto status aplikacji NFC (tj. aktywacja lub dezaktywacja) na aktywnym SE może być również kontrolowany przez użytkownika. Na przykład, użytkownik może aktywować jedną lub wiele aplikacji kart kredytowych obsługujących NFC na SE. Ponadto użytkownik może aktywować i nadać priorytet tym aplikacjom znajdującym się na SE przed przedstawieniem telefonu komórkowego czytnikowi.

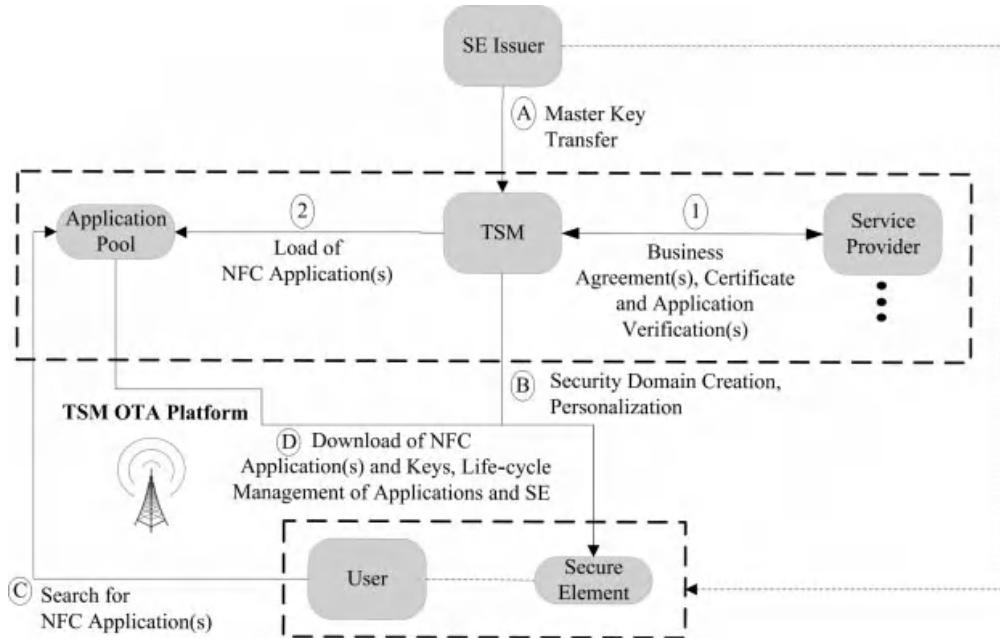
8.4.2 Architektura z agregacją

W modelu "z agregacją" wszystkie SE hostowane w telefonie komórkowym z obsługą NFC są aktywne w tym samym czasie. Każda aplikacja na dowolnym SE może wykonywać transakcje zbliżeniowe NFC w dowolnym momencie. Tak więc lista wszystkich aplikacji NFC na wszystkich SE w telefonie komórkowym powinna być wyświetlana użytkownikowi jednocześnie. Oczywiście każdy SE może zawierać jedną lub więcej aplikacji.

Nadal możliwe jest kontrolowanie stanu aplikacji NFC na pojedynczym SE lub na wielu SE. Status aplikacji NFC jest kontrolowany przez użytkownika, a aplikacja powinna być wybierana przez zewnętrzny czytnik. Zewnętrzny czytnik wysyła żądanie wyboru do aktywnej aplikacji, a to żądanie wyboru jest bezpośrednio przekazywane do odpowiedniego SE, w którym znajduje się aktywna aplikacja. Czytnik otrzymuje pojedynczą odpowiedź od odpowiedniej aplikacji.

8.5 Alternatywny model zarządzania OTA oparty na TSM

Obecnie w branży NFC istnieje szeroki zakres konkurencji między partnerami biznesowymi, dlatego modele biznesowe, z których korzystają, różnią się w zależności od możliwości biznesowych. OSK odgrywają ważną rolę jako wydawcy UICC, a nawet mogą działać jak menedżer kart. OSK posiada istotne klucze na karcie. W związku z tym dostawcy usług i inne podmioty, takie jak TSM, są głównie zależne od wydawców kart. Niniejsza sekcja przedstawia alternatywny model, w którym żaden z podmiotów nie jest zależny od jednego podmiotu i który korzysta z roli TSM w zakresie wiarygodności. Model ten jest w rzeczywistości rozszerzeniem autoryzowanego modelu GlobalPlatform, w którym



Rysunek 8.11 Alternatywne zarządzanie OTA aplikacjami NFC w oparciu o TSM.

Pełna delegacja jest przyznawana TSM, ale może być również stosowana do wszystkich opcji SE, takich jak sprzęt wbudowany, SMC i UICC.

TSM ma możliwość tworzenia i zarządzania zaufanym środowiskiem za pomocą własnej platformy OTA zarówno dla użytkowników, jak i dostawców usług. Zapewnienie interoperacyjnej i elastycznej platformy OTA jest jednym z kluczowych wymagań w systemach NFC. W celu zapewnienia bezpieczniejszego i wydajniejszego zarządzania cyklem życia aplikacji NFC i SE, proponowana jest nowa infrastruktura; infrastruktura puli aplikacji, która jest kontrolowana przez TSM. Proponowana pula aplikacji zapewnia centralną lokalizację lub bazę danych do przechowywania aplikacji; może to być również sklep z aplikacjami online. Aplikacje mogą być ładowane przez dostawców usług do tej puli aplikacji i mogą być oferowane użytkownikom w dowolnym momencie.

Jak pokazano na rysunku 8.11, gdy dostawcy usług decydują się na dystrybucję aplikacji obsługującej NFC, muszą początkowo zawrzeć umowy biznesowe z TSM na rynku.

Następnie TSM sprawdza i, jeśli jest ważny, zatwierdza aplikację wraz z jej certyfikatami (Krok 1), po czym aplikacje mogą być ładowane i publikowane w puli aplikacji TSM (Krok 2). Podczas gdy TSM obsługuje dostawców usług i wymagania rynkowe, może również bezpiecznie kontrolować i zarządzać cyklem życia SE. Jak widać na rysunku 8.11, TSM żąda klucza głównego SE od wystawcy SE (krok A). Jak już wspomniano, klucz główny jest kluczem unikalnym i istnieje we wszystkich SE. Umożliwia on właścielowi tworzenie domen bezpieczeństwa na SE, kontrolowanie każdej domeny bezpieczeństwa i personalizowanie SE (krok B). W proponowanym modelu TSM działa jako właściciel klucza głównego jako zaufana strona między podmiotami. TSM żąda tego klucza do obsługi funkcji SE od wystawcy SE, który może być OSK lub innym podmiotem w zależności od opcja SE (jak omówiono w rozdziale 7).

Użytkownik, który chce korzystać z jednej z tych aplikacji NFC, może wyszukać aplikację z bazy danych aplikacji TSM (krok C). TSM może łatwo zarządzać tymi aplikacjami; może je aktualizować i personalizować za pośrednictwem OTA na UICC użytkownika (krok D). Ponadto taki mechanizm umożliwia zapobieganie aplikacjom podobnym do spamu, a prywatne i wrażliwe informacje są zabezpieczone na UICC użytkownika.

8.6 Rozdział Podsumowanie

Karty UICC stały się najpopularniejszym sposobem promowania systemów opartych na NFC, które obsługują technologię OTA. Technologia OTA jest zawsze dostępna i łatwa w zarządzaniu, oferując klientom usługi o wartości dodanej. Dzięki technologii OTA aplikacje obsługujące NFC mogą być dostarczane do UICC, a także mogą być łatwo aktualizowane i zarządzane. Po stronie użytkownika OTA zapewnia wiele korzyści zarówno użytkownikom, jak i ich UICC. Po stronie biznesowej i technicznej istnieje złożona struktura. GlobalPlatform starał się zapewnić standardy i specyfikacje dla odpowiedniego, interoperacyjnego zarządzania systemem kart inteligentnych i zaoferował bezpieczną i elastyczną funkcjonalność zarządzania zawartością karty w wielu aplikacjach podczas cyklu życia karty.

GlobalPlatform zaoferował architekturę kart i modele wdrażania OTA na tej architekturze kart, która ma również zastosowanie do SE opartego na UICC. Zgodnie z architekturą kart inteligentnych, karta składa się z szeregu logicznych i fizycznych komponentów: mikroprocesorów, RTE, OPEN, GP Trusted Framework, API, obszarów składających się z jednej lub więcej usług od wydawcy karty, dostawcy aplikacji i usług globalnych oraz domen bezpieczeństwa (tj. ISD, APSD i CASD). Domeny bezpieczeństwa są ważną częścią karty, która obsługuje usługi bezpieczeństwa, takie jak obsługa kluczy, szyfrowanie, deszyfrowanie, generowanie podpisu cyfrowego i weryfikacja dla aplikacji ich dostawców. Każda domena bezpieczeństwa jest ustanawiana w imieniu wydawcy karty, dostawcy aplikacji lub organu kontrolnego.

Każdy UICC zgodny z GlobalPlatform jest dostarczany z jednym ISD i opcją dla wielu domen bezpieczeństwa TSM lub domen bezpieczeństwa dostawcy aplikacji (lub dostawcy usług) (takich jak karty kredytowe, transport, bilety, aplikacje lojalnościowe). Obszary przechowywania danych każdego dostawcy usług i TSM są od siebie odizolowane, podobnie jak ich aplikacje. Ponadto każdy SE oparty na UICC ma tylko jeden CASD. Architektura ta umożliwia wydawcom kart, dostawcom usług i TSM zarządzanie kluczami i weryfikację aplikacji podczas ładowania aplikacji i procesów personalizacji.

Według GlobalPlatform, pofne zarządzanie zawartością karty jest początkowym kluczowym zestawem ładowania domeny bezpieczeństwa strony trzeciej, ładowania aplikacji i personalizacji. GlobalPlatform proponuje trzy modele zarządzania zawartością karty na kartach UICC: tryb prosty, który jest modelem całkowicie skoncentrowanym na wydawcy karty; tryb delegowany i tryb autoryzowany są modelami bardziej skoncentrowanymi na TSM.

W trybie prostym dostawca usług deleguje pełne zarządzanie swoją aplikacją obsługującą NFC do TSM. TSM zarządza procesami blokowania, odblokowywania i personalizacji aplikacji przy użyciu własnego serwera OTA, ale sieci MNO. OSK jest upoważniony do wykonywania funkcji zarządzania zawartością karty. W trybie delegowanym MNO musi dostarczyć TSM cyfrowy znak jako token dla wstępnie autoryzowanej akcji zarządzania zawartością karty. TSM może jednak nadal wykonywać blokowanie/odblokowywanie aplikacji i proces personalizacji bez tokena. W trybie autoryzowanym wdrożenie jest całkowicie zorganizowane wokół TSM. TSM posiada aplikacje dostawcy usług i jest w stanie zarządzać zawartością karty za pomocą własnej platformy OTA, bez autoryzacji lub

Inną ważną kwestią jest wiele środowisk SE na jednym urządzeniu mobilnym z obsługą NFC. Każdy SE obsługuje jedną lub więcej aplikacji NFC, które są dostarczane przez różnych dostawców usług. Podczas gdy wiele SE znajduje się w tym samym telefonie, należy wziąć pod uwagę dwie kwestie: działanie czytnika zewnętrznego z aplikacją na SE i zarządzanie wieloma SE w tym samym czasie. Mobilna grupa zadaniowa GlobalPlatform przeprowadziła analizę potencjalnych konsekwencji zarządzania wieloma SE w tym samym telefonie; można zastosować dwa modele biznesowe: architekturę bez agregacji i architekturę z agregacją. W przypadku modelu architektury bez agregacji, tylko jeden SE jest aktywowany przez użytkownika i jest widoczny dla czytelnika. W związku z tym aktywowany SE jest w stanie wykonywać transakcje zbliżeniowe. W przypadku architektury z modelem agregacji, wszystkie SE hostowane w telefonie komórkowym z obsługą NFC są aktywne w tym samym czasie. Każdy model z odrębnymi wymaganiem musi być bardziej przemyślany pod względem kompatybilności i interoperacyjności.

Wraz z rozwojem technologii NFC i UICC, a także z nowymi uczestnikami ekosystemu NFC i modelami współpracy, mogą pojawić się nowe modele wdrażania. Może pojawić się ulepszony autoryzowany model, a TSM mogą dominować w systemach opartych na NFC z własnymi elastycznymi i interoperacyjnymi platformami OTA, co wyeliminuje zależność od wydawców kart i operatorów sieci. Z drugiej strony może to spowodować, że TSM będzie w przyszłości jedynym organem publikującym lub sprzedającym karty UICC.

Rozdział Pytania

1. Jaka jest rola technologii OTA w zarządzaniu urządzeniami mobilnymi?
2. Jakie jest znaczenie technologii OTA w ekosystemie NFC?
3. Jaka jest rola i znaczenie TSM w ekosystemie NFC?
4. Co to jest domena bezpieczeństwa? Wyjaśnij architekturę bezpiecznego elementu opartego na UICC.
5. Wyjaśnij związek między zarządzaniem zawartością karty a wdrażaniem OTA.
6. Wyjaśnij znaczenie specyfikacji GlobalPlatform i modeli wdrażania OTA.
7. Szczegółowe informacje na temat prostego trybu korzystania z platformy MNO OTA.
8. Podać szczegóły trybu delegowanego z pełną delegacją do TSM.
9. Podaj szczegóły autoryzowanego trybu z pełną delegacją do TSM.
10. Czy możliwe jest hostowanie wielu bezpiecznych elementów na jednym telefonie komórkowym NFC? W jaki sposób?

Referencje

- [1] GlobalPlatform (2006) *GlobalPlatform Card Specification Version 2.2*, marzec 2006, <http://www.globalplatform.org/specificationscard.asp> (dostęp 10 lipca 2011 r.).
- [2] GlobalPlatform (2009) *GlobalPlatform's Proposition for NFC Mobile: Secure Element Management and Messaging*, Biała Ksiega, kwiecień 2009. Dostępny pod adresem: http://www.globalplatform.org/documents/GlobalPlatform_NFC_Mobile_White_Paper.pdf (dostęp 10 lipca 2011).
- [3] GlobalPlatform (2011) *GlobalPlatform System, Messaging Specification for Management of Mobile NFC-Services, Version 1.0*, luty 2011, <http://www.globalplatform.org/specificationscard.asp> (dostęp: 10 lipca 2011 r.).
- [4] GlobalPlatform Mobile Task Force (2010) *Requirements for NFC Mobile: Management of Multiple Secure Elements Version 1.0*, GlobalPlatform, luty 2010. Dostępne pod adresem: http://www.globalplatform.org/documents/whitepapers/GlobalPlatform_Requirements_Secure_Elements.pdf (dostęp 10 lipca 2011 r.).

9

Miasta i testy NFC

Podjęto wiele prób wdrożenia i wykorzystania technologii NFC. Niektóre modele zostały opracowane przez uniwersytety, inne przez firmy, a jeszcze inne jako wspólny wysiłek uniwersytetów i firm. Wiele modeli jest tylko teoretycznych, niektóre zostały wdrożone, ale nie mogą być używane z powodu brakujących elementów, a inne zostały w pełni opracowane (np. w celu przetwarzania kont bankowych). Miasto NFC zazwyczaj opisuje miasto, w którym używana jest jedna lub więcej aplikacji NFC. Celem miasta NFC jest przetestowanie lub użycie jednej lub więcej implementacji. Miasta NFC są ważne dla doskonalenia technologii NFC, ponieważ są rzeczywistą areną umiarkowanej wielkości mediów użytkowych. W testach i projektach NFC testowana jest aplikacja lub ekosystem NFC; w ten sposób kwestie użyteczności wraz z problemami związanymi z technologią można uzyskać poprzez testy w początkowej fazie miast NFC. Podezas okresu testowego jednym z celów jest ocena możliwości zastosowania i wykorzystania technologii NFC. Jednym z głównych celów jest przetestowanie kwestii związanych z ekosystemem NFC. Użyteczność ekosystemu NFC jest co najmniej tak samo ważna jak stosowność techniczna, ponieważ model nie może być używany, gdy nie ma zgody między zaangażowanymi stronami.

9.1 NFC Miasta

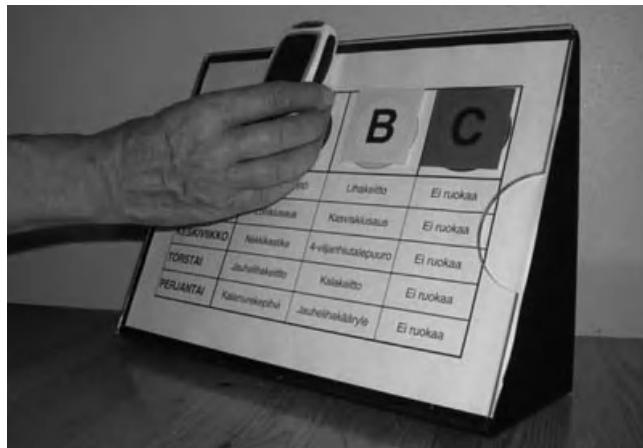
Przeanalizowaliśmy trzy wiodące miasta NFC, a mianowicie Oulu, Niceę i Smart Urban Spaces.

9.1.1 Miasto Oulu

Oulu zostało wykorzystane jako poligon doświadczalny dla projektu SmartTouch. W projekcie SmartTouch uczestniczyło 22 partnerów z 8 krajów europejskich. Wśród partnerów znalazło się 9 dużych organizacji przemysłowych, 5 firm, 4 organizacje badawcze i 2 organizacje publiczne. Projekt był koordynowany przez Fińskie Centrum Badań Technicznych VTT. Dzięki temu projektowi Oulu stało się pionierskim miastem, które następnie zostało członkiem NFC Forum.

Projekt trwał od 2006 do końca 2008 roku i badał rolę NFC w życiu miejskim, domowym, wellness i zdrowotnym, rozrywkowym, technologicznym i biznesowym. Obywatele mieszkający w Oulu mieli możliwość przetestowania komercyjnych i publicznych usług NFC w ramach projektu.

© 2012 John Wiley & Sons, Ltd. Opublikowano 2012 przez John Wiley & Sons, Ltd.



Rysunek 9.1 Zamawianie posiłków dla osób starszych [1].

pierwszych użytkowników technologii obejmującej ten szeroki zakres. Aplikacje, testy i pilotaże, które zostały przetestowane w ramach tego projektu, są następujące [1, 2]:

(i) *Zamawianie posiłków dla osób starszych*

Usługa ta umożliwiła starszym klientom zamawianie posiłków poprzez dotykanie etykiet posiłków, zamiast wykonywania połączeń telefonicznych. Motywacją dla projektu było zmniejszenie wysiłku ludzi.

Podczas fazy pilotażowej użytkownicy dotykali znaczników preferowanych pozycji w codziennym menu za pomocą swoich telefonów komórkowych z obsługą NFC. Scenariusz został przedstawiony na rysunku 9.1. Posiłki były następnie dostarczane do domu przez personel firmy spożywczej. Po dotknięciu znacznika przez użytkownika usługa Oulu Meal Service przyjmowała zamówienie i przygotowywała posiłek. Następnie firma logistyczna dostarczała jedzenie. Pracownicy logistyki również korzystali z telefonów komórkowych z obsługą NFC i zgłaszały status posiłku na początku rundy dostawy, po udanej dostawie i wreszcie po zakończeniu całego procesu. Pracownicy zaplecza kontrolowali cały proces, zbierając w czasie rzeczywistym informacje o statusie posiłku, ponieważ informacje te były przesyłane online do serwerów zaplecza.

W fazie pilotażowej wzięło udział dziewięciu użytkowników; średni wiek uczestników wynosił

76.6. Wdrożenie testowe wykazało, że interakcja z technologią NFC była dość łatwa dla osób starszych, ale niektóre z nich doświadczyły problemów w korzystaniu z telefonu komórkowego. W szczególności korzystanie z klawiatury telefonu komórkowego było trudne dla niektórych uczestników ze względu na pogorszenie ich wzroku i zdolności motorycznych. Niektórzy z uczestników skarzyli się na mały rozmiar klawiszy na klawiaturach: jest to w rzeczywistości powszechny problem telefonów komórkowych i nie jest bezpośrednio związany z technologią NFC.

Spośród kilku opcji menu, właściwy punkt dotyku był wymagany do zamówienia odpowiedniego elementu. Doświadczenie pokazało, że było to dość łatwe dla użytkowników. W rezultacie technika interakcji oparta na dotyku wydaje się być łatwa do dostosowania dla wszystkich użytkowników.

Najważniejszym odkryciem badania było to, że pięciu z dziewięciu uczestników stwierdziło, że wolą zamawiać posiłki za pomocą NFC niż d z w o n i ć, aby zamówić posiłki na odległość. Pozostali uczestnicy nadal preferowali starą metodę



Rysunek 9.2 Uczeń loguje się do klasy [1]. Sfotografowany przez Juha Sarkkinen, Miasto Oulu, Projekt Smart Touch.

metoda [3]. Aby obejrzeć film demonstracyjny, zachęcamy czytelników do odwiedzenia strony <http://www.ouka.fi/video/smart/elderly/>.

(ii) *Nadzór obecności NFC dla szkół średnich*

Celem projektu było monitorowanie frekwencji uczniów szkół średnich dla ich rodziców. Wyeliminowało to potrzebę zaznaczania nieobecności przez nauczycieli, co oszczędza czas, pozwalając na więcej czasu na nauczanie.

Gdy uczeń przychodzi na zajęcia, dotyczy znacznika, który jest przymocowany do biurka nauczyciela; baza danych na serwerze zaplecza jest natychmiast aktualizowana o obecności ucznia-użytkownika. W rezultacie uczeń jest oznaczany jako nieobecny, jeśli nie wykona żadnej akcji logowania przed upływem określonego terminu. W przypadku spóźnienia, system odpowiednio rejestruje sytuację. W przypadku uzasadnionego usprawiedliwienia nieobecności, takiego jak choroba, nauczyciele aktualizują dane dla tej sytuacji (patrz rysunki 9.2 i 9.3).

Inną ważną właściwością systemu było informowanie rodziców i administratorów o frekwencji uczniów, które odbywa się w czasie rzeczywistym. Projekt pilotażowy został przeprowadzony z udziałem 113 uczniów z 5 klas ósmoklasistów w 2008 roku i trwał 8 tygodni [4]. Aby obejrzeć film demonstracyjny, zachęcamy czytelników do odwiedzenia strony <http://www.ouka.fi/video/smart/school/>.

(iii) *Nadzór nad frekwencją w szkole podstawowej z wykorzystaniem NFC*

Przypadki użycia tego projektu są dość podobne do poprzedniego. W tym projekcie frekwencja uczniów szkoły podstawowej jest rejestrowana w celu zapewnienia rodzicom informacji o ich dzieciach w czasie rzeczywistym. W klasie każdy uczeń ma kartę intelligentną, na której zapisane jest jego imię i nazwisko oraz dane identyfikacyjne. Nauczyciel posiada telefon komórkowy obsługujący technologię NFC z zainstalowaną aplikacją do rejestracji obecności. Gdy uczeń dotknie swoją kartą telefonu komórkowego nauczyciela, akcja wejścia lub wyjścia, znacznik czasu i identyfikacja ucznia są zapisywane w systemie zaplecza. Rodzice mogą monitorować frekwencję swoich dzieci online lub otrzymywać powiadomienia SMS-em zgodnie z własnymi preferencjami.

Pilotaż tego projektu rozpoczął się w 2008 roku i trwał 14 tygodni. W pilotażu wzięło udział 27 uczniów w wieku od 6 do 7 lat. Jedna klasa składała się z



Rysunek 9.3 Zaakceptowane informacje o obecności [1]. Zdjęcie wykonane przez Juha Sarkkinen, The City of Oulu, Smart Touch Project.

20 uczniów, a w klasie umieszczono aktywny czytnik. Druga klasa składała się z siedmiu uczniów, a jako czytnik NFC wykorzystano telefon komórkowy nauczyciela obsługujący technologię NFC (patrz rysunek 9.4). W ramach pilotażu przetestowano również użyteczność technologii NFC i aspekty bezpieczeństwa kontroli obecności wśród dzieci [4]. Aby obejrzeć film demonstracyjny, zachęcamy do odwiedzenia strony <http://www.ouka.fi/video/smart/school2/>.

(iv) Niesamowite NFC

Amazing NFC to projekt miejskich biegów na orientację dla szkół realizowany w Oulu. Jego celem jest nauczenie uczniów rzeczy niezbędnych w szkole i życiu codziennym, takich jak informacje o pożyczkach studenckich lub informacje o historii miasta. Przeprowadzane są dwa różne rodzaje biegów na orientację: trasa survivalowa i trasa kulturowo-historyczna. Tor przetrwania



Rysunek 9.4 Nauczyciel loguje uczniów za pomocą telefonu komórkowego z obsługą NFC [1]. Zdjęcie wykonane przez Juha Sarkkinen, Miasto Oulu, Projekt Smart Touch.



Rysunek 9.5 Uczeń uprawiający biegi na orientację [1]. Sfotografowany przez Juha Sarkkinen, Miasto Oulu, Projekt Smart Touch.

umożliwia uczniom poznanie urzędów i instytucji w Oulu. Ścieżka kulturalna pomaga uczniom uzyskać informacje na temat kultury i historii Oulu.

Gdy uczeń rozpoczyna bieg na orientację, definiowany jest punkt startowy. Gdy uczeń dotrze do tego punktu, dotyka znalezionej znacznika i otrzymuje pytanie za pośrednictwem mobilnej strony internetowej. Pytanie może być zadane za pomocą tekstu, wideo lub audio. Gdy uczeń odpowie poprawnie, otrzymuje następny punkt kontrolny (patrz rysunek 9.5).

Faza pilotażowa tego projektu rozpoczęła się w 2008 roku od ścieżki przetrwania, a następnie ścieżki kulturowej. W fazie pilotażowej wykorzystano około 400 studentów. Jednak ścieżka kulturowa była ograniczona przez słabą dostępność urządzeń końcowych NFC od dostawcy [4]. Film demonstracyjny można obejrzeć na stronie <http://www.ouka.fi/video/smart/amazing/>.

(v) *Inteligentne parkowanie z NFC*

Projekt ten umożliwił kontrolę parkowania za pomocą technologii NFC, eliminując monety i bilety parkingowe. Co więcej, płacono tylko za rzeczywisty czas parkowania, a nie za predefiniowane okresy, co zmniejszyło opłaty za parkowanie.

Aby zainicjować rejestrację i płatność za parkowanie, użytkownik najpierw dotyka swoim telefonem komórkowym tagu NFC na przedniej szybie, a następnie tagu w strefie parkowania. Alternatywnie, może wybrać strefę parkowania z aplikacji w telefonie komórkowym. Po zakończeniu parkowania użytkownik dotyka tylko znacznika umieszczonego na przedniej szybie lub w strefie parkowania, jak pokazano na rysunku 9.6. Pracownicy ruchu drogowego zostali również wyposażeni w telefony komórkowe z obsługą NFC, a gdy pracownicy dotknęli znacznika na zaparkowanym samochodzie, aplikacja na telefonie komórkowym sprawdziła status zaparkowanego samochodu.

Badanie pilotażowe rozpoczęło się pod koniec 2007 roku i trwało około 3 miesięcy. W fazie pilotażowej wzięło udział około 55 losowo wybranych uczestników [5]. Film demonstracyjny można obejrzeć na stronie <http://www.ouka.fi/video/smart/parking/>.

(vi) *NFC w kinie*

Projekt Oulu NFC w teatrze został zaplanowany przez teatr w Oulu i Kanresta, dostawcę usług restauracyjnych. TeliaSonera i MSG Software dostarczyły rozwiązania techniczne. Użytkownicy otrzymywali bilety do teatru z punktu sprzedaży w teatrze za pomocą telefonu komórkowego z obsługą NFC.



Rysunek 9.6 Inteligentne parkowanie w akcji [1]. Zdjęcie wykonane przez Juha Sarkkinen, Miasto Oulu, Projekt Smart Touch.

lub bezprzewodowo za pośrednictwem systemu zaplecza TeliaSonera. W restauracji teatralnej użytkownicy mogli pobierać wiadomości za pośrednictwem inteligentnych plakatów. Użytkownicy mogli również pobierać filmy na swoje telefony komórkowe za pośrednictwem inteligentnych plakatów (patrz rysunek 9.7).

Pilotaż tego projektu został przeprowadzony w 2007 roku i trwał około 6 tygodni. Ogółem w badaniach pilotowych wzięło udział 158 osób, a usługa była pilotowana podczas dziewięciu wydarzeń. Celem pilotazu było sprawdzenie, w jaki sposób technologia NFC może być wykorzystywana podczas imprez rozrywkowych [6]. Zachęcamy czytelników do odwiedzenia strony <http://www.ouka.fi/video/smart/theatre/> w celu obejrzenia filmu demonstracyjnego.

(vii) *NFC w restauracji*

W tym projekcie użytkownicy mogą szybko zamówić lunch za pomocą telefonów komórkowych z obsługą NFC. Klient najpierw dotyka tagu NFC umieszczonego na stole, a następnie dotyka jednego z tagów na liście menu i składa zamówienie. Następnie system pośredniczący TeliaSonera odbiera zamówienie i dostarcza je do systemu kasowego i kuchni restauracji.



Rysunek 9.7 Inteligentny plakat NFC [1]. Sfotografowany przez Juha Sarkkinen, Miasto Oulu, Projekt Smart Touch.

Z systemem zintegrowany jest również system kuponów, a klienci mogą korzystać z elektronicznych kuponów obiadowych. Po złożeniu zamówienia za pomocą kuponu jest on natychmiast usuwany z urządzenia. Projekt ma na celu zapewnienie większej przepustowości i przychodów w godzinach szczytu. Eliminuje również kupy papierowe. Informacje o potrawach i napojach w menu były również dostępne za pośrednictwem znaczników na plakatach i stołach [2].

Inne projekty realizowane w ramach projektu SmartTouch [1] to:

- Sprzedaż biletów autobusowych;
- Zarządzanie czasem pracy i dziennik kierowców;
- Zarządzanie zamkami w publicznej hali sportowej;
- Tagi informacyjne w środowisku miejskim;
- Koncepcja sklepu przyszłości;
- Glukometr z obsługą NFC.

Aby zapoznać się z pełną listą projektów i ich szczegółami, zachęcamy do odwiedzenia strony <http://www.vtt.fi/inf/pdf/tiedotteet/2009/T2492.pdf>.

9.1.2 Miasto Nicea

Zakłada się, że Nicea jest pierwszym miastem NFC w Europie z komercyjnym wdrożeniem

NFC przez każdego francuskiego operatora sieci komórkowej (MNO). Trzy tysiące telefonów NFC zostało wprowadzonych na rynek w 2010 roku, z głównym naciskiem na usługi transportowe i płatnicze. Sukces miasta Nicea został osiągnięty dzięki pracom MBDS, laboratorium informatyki i innowacji Uniwersytetu Nicea Sophia Antipolis we Francji (www.mbdss-fr.org) wraz z międzynarodowymi partnerami. Projekty dotyczyły głównie podróży, m-turystyki, opieki zdrowotnej, życia wspomaganego, m-płatności, m-kultury, m-administracji, m-edukacji i sprawiedliwego handlu. Wdrożone w Nicei projekty obejmują wszystkie tryby pracy (czytnik/zapis, peer-to-peer i emulacja karty). Aplikacje są przechowywane i wdrażane na jednej karcie SIM. Projekty są rozwijane we Francji, Maroku, Rosji i na Haiti z różnymi partnerstwo i późniejsze umowy.

Projekty te połączyły siły z Uniwersytetem w Nicei, który w latach 2010-2011 był gospodarzem ważnego projektu pilotażowego NFC (Nice Future Campus). Celem projektu Nice Future Campus jest zastąpienie fizycznych kart identyfikacyjnych studentów telefonami komórkowymi obsługującymi technologię NFC. Wdrożone projekty w mieście Nicea zostały przedstawione poniżej wraz z krótkimi opisami [13].

(i) Kampus Nice Future

Projekt Nice Future Campus został wdrożony we Francji w latach 2010-2011. Niektórzy z zaangażowanych partnerów to Extelia, Orange, Mobile Distillery i Uniwersytet w Nicei Sophia Antipolis.

Głównym celem projektu jest zastąpienie fizycznych kart identyfikacyjnych studentów telefonami komórkowymi z obsługą NFC i umożliwienie korzystania z wielu aplikacji na jednej karcie SIM. W projekcie wykorzystywane są wszystkie trzy tryby operacyjne i wdrożono dwa programy pilotażowe. Projekt składa się z wielu aplikacji z różnych kategorii, w tym płatności, transportu, biblioteki, administracji, sprzedaży biletów i życia społecznego studentów. Student w tym projekcie

Projekt był w stanie płacić, zarządzać biletami i kuponami, dzielić się opiniami na temat książki, uzyskiwać informacje kontekstowe, komunikować się ze znajomymi i wiele więcej za pomocą telefonu komórkowego z obsługą NFC [13].

W projekcie Nice Future Campus karta uniwersytecka z obsługą NFC może być używana do:

- Płatność;
- Bilet do restauracji uniwersyteckiej;
- Dostęp do biblioteki;
- Kontrola dostępu.

W ramach projektu Nice Future Campus, w kontekście usług opartych na lokalizacji student może:

- Zobacz ścieżkę do następnego kursu;
- Znajdź dane miejsce;
- Znajdź lokalizację książki w bibliotece.

W kontekście usług związanych z sieciami społecznościowymi student może:

- Zostaw wiadomość kontekstową na Facebooku;
- Zostaw wiadomość o książce na Facebooku.

W kontekście usług informacyjnych student może:

- Uzyskaj informacje kontekstowe dotyczące kampusu;
- Uzyskaj informacje o ogłoszeniach studentów, ofertach pracy i danych kontaktowych na dany temat.

W kontekście usług bibliotecznych student może:

- Zobacz rekomendacje nauczycieli dotyczące książki;
- Zobacz oceny książki dostarczone przez uczniów;
- Przeczytaj komentarze innych uczniów na temat książki;
- Zostaw komentarz na temat książki;
- Oceń książkę.

Stworzono platformę internetową, dzięki której uczeń może sprawdzać wydarzenia za pomocą

na tej platformie, kupować bilety i udostępniać wydarzenia w sieciach społecznościowych. Również za pomocą telefonu komórkowego z obsługą NFC student może:

- Zobacz bilety;
- Użyj biletów.

(ii) *REVE*

Projekt REVE został wdrożony w ramach projektu Nice Future Campus w Astrachaniu w 2010 roku. Studenci mogli uzyskać rekomendacje dotyczące książek, dotykając swoimi telefonami komórkowymi książek oznaczonych tagami NFC w bibliotece. Platformy społecznościowe, takie jak Facebook i Twitter, zostały również zintegrowane z systemem w celu budowania "przyjaciół lub obserwujących" stopień naukowy, książkę lub profesora.

(iii) *TAP'nFlouss*

Projekt ten został wdrożony w Maroku w latach 2009-2011 i umożliwia użytkownikom pobieranie pieniędzy z bankomatów za pomocą telefonów komórkowych obsługujących technologię NFC. Projekt został opracowany we współpracy z Omnidata, NCR i M2T, a dodatki NFC zostały wykorzystane do zapewnienia funkcji NFC w telefonach Bluetooth [13].

(iv) *MBDS*

Projekt został wdrożony w Nicei, Grasse, Hiszpanii, Tunezji, Egipcie i Astrachaniu w latach 2009-2010. Projekt umożliwia przekształcenie miejsc kultury w miastach w muzea. Wykorzystywane jest tagowanie NFC i 2D, a uczestnicy używają swoich

telefonów komórkowych do odkrywania kulturowych, tematycznych, rodzinnych i historycznych ścieżek w miastach [13].

Aplikacje są opracowywane dla telefonów z GPS, które mają system operacyjny Android i naklejkę NFC, aby uzyskać funkcję NFC.

Wdrożenia są następujące:

- Park naukowy Sophia Antipolis (Francja) w 2008 roku;
- Historyczny kampus Valrose Uniwersytetu w Nicei (Francja) w 2009 r;
- Menton i Grasse (Francja), Sidi Bou Said (Tunezja), Cyfrowe Muzeum Kremla w Astrachaniu (Rosja) oraz park naukowy Sophia Antipolis w ramach projektu Sophia Zen.

w 2011 roku.

(v) *TICKET TAP*

Projekt został wdrożony we Francji w 2008 roku. Wirtualne kupony i bilety są zarządzane za pomocą platformy Cassis OTA (Over the Air). Projekt ten został również wykorzystany w projekcie Nice Future Campus w 2010 r. oraz w projekcie IMAJEANS dotyczącym marketingu ulicznego i marketingu w punktach sprzedaży, który ma zostać wdrożony w Nicei [13].

(vi) *CAMPUS NOVA*

Projekt został wdrożony we Francji w 2008 roku we współpracy z bankiem Credit Agricole. Był to pierwszy francuski projekt płatności mobilnych NFC, który umożliwił 30 studentom korzystanie z telefonów komórkowych do dokonywania płatności. Studenci mogli płacić za pomocą swoich telefonów komórkowych, a także używać ich do kontroli dostępu w salach lekcyjnych. Projekt ten pomógł również we wdrożeniu nowych projektów płatniczych we Francji, takich jak Nice Future Campus [13].

(vii) *CAP ROUGE NIMERIK*

Projekt został wdrożony na Haiti w 2008 roku w celu śledzenia worków z kawą do celów zarządzania z obszarów wiejskich na Haiti do fabryki w Nicei. W tym celu w workach z kawą umieszczono tagi NFC. Projekt został wdrożony z dużymi partnerami, takimi jak Malango (producent kawy z Francji), Solutions (producent oprogramowania na Haiti), Voila (Haiti MNO) i Alcatel Lucent (do umieszczenia WiMAX) [13].

(viii) *RoboDOMO*

Projekt został wdrożony we Francji w 2006 roku i jest realizowany do 2012 roku przez Microsoft, Covea Tech i szpital w Nicei. Robot firmy Robosoft został zbudowany wokół obiektów komunikacyjnych w celu monitorowania osób starszych w domu. Kontrola dostarczania leków, zarządzanie osobami pracującymi z osobami starszymi w domu i wizyty opieki domowej to tylko niektóre z wdrożonych usług [13].

(ix) *MOSTRA*

Projekt MOSTRA został wdrożony w 2005 i 2006 roku we współpracy z firmami Amadeus i Renault. Celem tego projektu jest wykorzystanie telefonów komórkowych z obsługą NFC jako obiektu kontroli dostępu w samochodach i hotelach, a także przechowywanie wirtualnych voucherów w urządzeniu mobilnym. Projekt ten umożliwił również przeprowadzenie eksperymentu z wykorzystaniem wirtualnej karty pokładowej NFC na lotnisku w Nicei w 2009 roku [13].

9.1.3 Inteligentne przestrzenie miejskie

Smart Urban Spaces to wspólny europejski projekt skupiający się na projektowaniu i wdrażaniu usług kontekstowych i usług e-miasta opartych na NFC z wykorzystaniem najnowszych technologii mobilnych i wszechobecnych. W ramach projektu prototypowane

są aplikacje i usługi NFC oraz badane są kwestie interoperacyjności.

Smart Urban Spaces to 3-letni projekt realizowany od połowy 2009 do połowy 2012 roku, w który zaangażowane są Finlandia, Francja, Hiszpania i Grecja. Oulu, Helsinki, Caen, Walencja i Sewilla to tylko niektóre z nich.

zaangażowanych miast. W projekt zaangażowanych jest wiele organizacji z czterech uczestniczących krajów. Organizacje te obejmują dostawców usług, twórców oprogramowania, uniwersytety, dostawców chipów i kart SIM, MNO i dostawców systemów. Projekt jest jednym z największych wysiłków w Europie w zakresie tworzenia usług miejskich w całej UE [8-11].

Głównymi celami projektu są:

- Ramy wdrażania usług e-miasta;
- Analiza techniczna i operacyjna usług;
- Testy pilotażowe i próbne w celu przetestowania aplikacji i usług;
- Analiza interoperacyjności;
- Określenie zestawu europejskich zaleceń i standardów miejskich;
- Zbudowanie sieci miast europejskich w celu wymiany doświadczeń w zakresie usług mobilnych i kontekstowych.

Usługi e-miasta zawarte w projekcie można podzielić na następujące kategorie:

- Transport;
- Rodzina i społeczność;
- Czas wolny, kultura i sport;
- Narzędzia użytkowe;
- Edukacja i uczenie się;
- Ekosystem miejski NFC;
- Inne usługi specjalne.

Niektóre z tych projektów zostały pokrótko omówione poniżej.

(i) *Bilet mobilny w transporcie publicznym*

W ramach tej usługi usługi biletowe zostaną przekształcone w bilety NFC. Telefony NFC zostaną uwzględnione w ogólnym planie rozwoju systemu taryfowego i biletowego dla obszaru metropolitalnego Helsinek w 2014 r. przez Helsinki Region Transport. Pierwszym krokiem była wymiana 700 000 kart podróżnych na standardowe karty oparte na technologii RFID. Czytniki kart w pojazdach zostały przekształcone w czytniki zgodne z telefonami NFC.

(ii) *Technologia NFC w ośrodkach opieki dziennej*

Dzięki temu projektowi personel przedszkola może monitorować obecność dzieci, w tym czas przybycia i wyjścia, za pomocą technologii NFC. Mogą również zamawiać posiłki, korzystając z listy obecnych dzieci.

(iii) *Uslugi kart miejskich w Oulu*

Karty miejskie Oulu są kompatybilne z NFC i wyposażone w dwuwymiarowe kody. Dzięki temu projektowi bilety mogą być sprawdzane z karty za pomocą telefonu komórkowego.

(iv) *Inteligentne znaki w Hernesaari*

W Hernesaari tagi prowadzą użytkowników do i z Hernesaari za pomocą inteligentnych znaków. Dotknietcie tagu otwiera informacje w formacie tekstowym, obrazkowym, audio lub wideo, a następnie użytkownik może być prowadzony za pomocą tych informacji.

(v) *Ścieżki miejskie*

W tym projekcie znaczniki NFC są używane przez turystów, aby zapewnić im dobre wrażenia w mieście w ograniczonym czasie. Cyfrowe tagowanie służy do prowadzenia użytkowników z mapą turystyczną na telefonie komórkowym.

(vi) *Bukiet usług*

Celem tej usługi jest zapewnienie użytkownikom wielu usług w ramach jednej platformy. W tym celu karta miejska Oulu jest używana w różnych podmiotach usługowych do świadczenia wielu usług, takich jak płatności, bilety na wydarzenia i bilety transportowe.

(vii) *Nauka*

W celu wspierania nauki prowadzonych jest kilka projektów. Cele tych projektów obejmują:

- Poprawa uczenia się poprzez wzrost motywacji w szkole;
- Dodanie poczucia wspólnoty poprzez dzielenie się i komentowanie zdobytych informacji;
- Poprawa komunikacji między szkołą a rodzicami.

Prowadzone są również inne projekty, w tym inteligentny sport, mobilna matematyka,

wielofunkcyjne oznakowane miasta, interoperacyjne legitymacje studenckie, sieci społecznościowe i rozwiązania NFC dla pracowników mobilnych w sektorze publicznym. Projekty wdrażają również następujące rozwiązania problemów technicznych:

- Subskrypcja usług;
- Rezygnacja z subskrypcji usług;
- Udostępnianie aplikacji;
- Płatność kartą kredytową;
- Wiele kart płatniczych;
- Płatność e-portmonetką;
- Kontrola dostępu i sprzedaż biletów;
- Wymiana biletów;
- Blokowanie i odblokowywanie aplikacji;
- Usuwanie aplikacji;
- Utrata telefonu;
- Tworzenie i edycja profili.

9.2 Testy NFC i projekty

Jak już wspomniano, na całym świecie przeprowadzono różne testy i projekty NFC. Aplikacje płatnicze i biletowe są prawdopodobnie najbardziej znanyimi i obiecującymi codziennymi zastosowaniami technologii NFC, a także najbardziej złożonymi z punktu widzenia ekosystemu. Dlatego większość testów i projektów próbnych jest wdrażana w tej domenie aplikacji. Oprócz miast NFC, niniejsza sekcja stara się przedstawić i zilustrować różne projekty NFC w różnych krajach. Niektóre z tych projektów zostały zakończone lub rozszerzone na różne domeny aplikacji z rosnącą liczbą uczestniczących podmiotów lub nadal są kontynuowane.

9.2.1 Płatności zbliżeniowe Próby

(i) *Pilotaż płatności Visa payWave w Malezji*

Krótki, ale udany przypadek pochodzi z Malezji, która została uruchomiona w kwietniu 2006 roku. MNO Maxis Communications, Maybank, który jest największym bankiem i grupą finansową w Malezji, oraz Visa współpracowały w celu wdrożenia płatności NFC w Malezji. Jest to pierwszy na świecie pilotaż płatności mobilnych Visa payWave. Został on wdrożony w stolicy Malezji, Kuala Lumpur, z udziałem

200 uczestników. Uczestnicy zostali wybrani spośród posiadaczy kart Maybank Visa i abonentów sieci komórkowej Maxis. Innymi dostawcami, którzy wzięli udział w tym programie pilotażowym byli Vivotech dla terminali lub czytników zbliżeniowych z obsługą NFC oraz NXP Semiconductors dla zestawów chipów NFC i wbudowanych sprzętowych bezpiecznych elementów (SE) dla telefonów komórkowych. Ten test płatności odegrał dużą rolę w komercyjnym wprowadzeniu usług NFC w Malezji w kwietniu 2009 roku [7,14].

(ii) *Testy HSBC w USA*

Inny przypadek pochodzi od globalnej firmy świadczącej usługi bankowe i finansowe. HSBC uruchomił pilotażowy program płatności mobilnych z obsługą NFC we współpracy z MasterCard w styczniu 2007 roku w USA. Pilotaż ten trwa 6 miesięcy i testował wykorzystanie telefonów komórkowych z obsługą NFC w płatnościach. Usługa płatności była używana tam, gdzie akceptowane były płatności zbliżeniowe kartą kredytową i MasterCard PayPass. Około 36 000 sprzedawców zaakceptowało w tym czasie opcję płatności MasterCard PayPass. Ponad 200 pracowników banków w Nowym Jorku, Chicago i kilku innych dużych miastach USA skorzystało z procesu instalacji i personalizacji OTA, aby pobrać informacje o karcie kredytowej HSBC na swoje telefony komórkowe z obsługą NFC. Aplikacja i platforma TSM zostały dostarczone przez Vivotech. Telefony komórkowe Nokia 3220 z obsługą NFC były używane z wbudowanym oprogramowaniem sprzętowym. Te SE i zestawy chipów NFC zostały dostarczone przez NXP Semiconductors [7,14].

(iii) *Projekt Payez Mobile*

Projekt Payez Mobile jest wspólną inicjatywą rozpoczętą w listopadzie 2007 roku [12, 13]. Jest to szeroko zakrojony pilotaż usługi płatności mobilnych wdrożony z udziałem około 1000 testerów i 500 sprzedawców detalicznych w Caen i Strasburgu. W projekt zaangażowanych jest czterech operatorów MNO (tj. Bouygues Telecom, NRJ Mobile, Orange i SFR), osiem wiodących francuskich banków (tj. BNP Paribas, Crédit Agricole, LCL, Crédit Mutuel, CIC, Groupe Caisse d'Epargne, La Banque Postale i Socie'te' Gé'ne'r'ale), Visa i MasterCard. Projekt ten łączy możliwości wymienionych organizacji, a także wykorzystuje technologie opracowane w ramach projektu ITEA SmartTouch.

Usługa płatności zbliżeniowych świadczona przez Payez Mobile jest w pełni kompatybilna z istniejącymi międzynarodowymi specyfikacjami Visa i MasterCard. Co więcej, aplikacje MasterCard i Visa mogą być hostowane jednocześnie w tym samym SE. Globalnym celem uczestników testu Payez Mobile jest stworzenie wspólnej wizji,

a mianowicie rozwiązania biznesowego dla banków i MNO w domenie aplikacji płatności zbliżeniowych. Z technicznego punktu widzenia eksperyment Payez Mobile

opiera się na połączeniu czterech kwestii. Pierwszą kwestią jest to, że aplikacje płatnicze dostarczane przez banki są instalowane na SE telefonu komórkowego z obsługą wielu aplikacji opartych na UICC. Drugą kwestią jest to, że technologia NFC jest używana tylko do obsługi usługi płatności z urządzenia mobilnego obsługującego

NFC do terminala sprzedawcy. Trzecią kwestią jest to, że protokół Single Wire Protocol (SWP) jest używany do zarządzania komunikacją z SE opartym na UICC z interfejsu NFC. Wreszcie, do zdalnego wdrażania wielu aplikacji wymagane są zaawansowane mechanizmy OTA. Dostawcami SE opartych na UICC i bezpiecznych

platform OTA są Gemalto i Obertur Card Systems. Ponadto, telefony komórkowe z obsługą NFC używane w projekcie to Motorola L7, Sagem My700 i LG L600V.

Ta usługa zbliżeniowych płatności mobilnych wykorzystuje istniejącą infrastrukturę kart bankowych. Metody płatności są zdefiniowane przez Payez Mobile. Pierwsza metoda dotyczy kwot poniżej 20 euro, dzięki czemu klienci mogą płacić bez

metoda dotyczy kwot przekraczających 20 euro, w przypadku których wymagany jest kod PIN. W przypadku tych metod każdy bank może wdrożyć jedną lub więcej aplikacji płatniczych obsługujących NFC, które można załadować i zainstalować na UICC telefonu komórkowego klienta obsługującego NFC.

To rozwiązanie płatnicze jest odpowiednie dla wszystkich kwot i zostało przetestowane wśród osób w każdym wieku. Według Association Europeenne Payez Mobile, do końca 2008 roku badania wykazały, że większość klientów uważa to rozwiązanie płatnicze za "wysoce praktyczne", "łatwe" i "atrakcyjne". Ponad 90% wszystkich klientów wyraziło "zadowolenie" z tego rozwiązania, a 59% stwierdziło, że będzie korzystać z tej usługi, gdy stanie się ona dostępna. Ponadto 82% sprzedawców jest zadowolonych z tej usługi płatniczej i docenia szybkość mobilnych płatności zbliżeniowych. Aby uzyskać więcej informacji na temat projektu Payez Mobile, specyfikacji i demonstracji, zachęcamy czytelników do odwiedzenia strony <http://www.payezmobile.com> [12].

(iv) *Pilotaż C1000 NFC z Rabo Mobile w Holandii*

Holenderski Rabobank stał się pierwszym bankiem w Europie, który wprowadził bankowość mobilną i usługi tanich połączeń telefonicznych w inny sposób dzięki Rabo Mobile. Jest to wirtualny operator sieci komórkowej (MVNO), który jest w pełni własnością Rabobanku. Ta nowa usługa zmienia obecną strategię z "chodzenia do banku w godzinach otwarcia" na "bank dostępny zawsze i wszędzie". Rabobank oferuje swoim klientom przejrzystą i wydajną obsługę klienta dzięki Rabo Mobile. Partnerami w ramach tego programu są firma multimedialna Talpa i MNO Orange dostarczający usługę sieci komórkowej [7].

Początkowo Rabo Mobile koncentruje się na klientach bankowości internetowej Rabobank. Opracowywane są również różne produkty i usługi dla różnych grup klientów, takich jak małe i średnie przedsiębiorstwa. Jest to nowy i innowacyjny sposób, który łączy tradycyjną bankowość i bankowość internetową z szybko rozwijającym się biznesem operatorów komórkowych.

W sierpniu 2007 r. Rabo Mobile zainicjowało nowy program pilotażowy NFC o nazwie "Płać telefonem komórkowym w C1000" w Holandii. C1000 jest jedną z największych holenderskich sieci supermarketów. W ciągu 6 miesięcy wdrożono szereg aplikacji obsługujących NFC w sklepach detalicznych C1000, w tym płatności mobilne i usługi lojalnościowe. Około 100 klientów supermarketu C1000 i Rabobank wzięło udział w pilotażu w małym miasteczku Molenaarsgraaf. Klienci korzystali z telefonów komórkowych Samsung obsługujących technologię NFC i płacili za zakupy po prostu dotykając telefonu do czytnika NFC przy kasie. Następnie wprowadzali swój kod PIN do terminala POS i finalizowali transakcję. Jest to dobry przykład bezstykowej aplikacji debetowej online w Europie, która umożliwia korzystanie z istniejącego systemu PIN za pomocą telefonu komórkowego. Co więcej, klienci mogą zwrócić puste butelki i otrzymać paragony rabatowe do wykorzystania przy kasie w automatach z butelkami, które znajdują się w supermarkecie, lub otrzymać zwrot pieniędzy na konto Rabobank.

Zgodnie z wynikami uzyskanymi przez sprzedawcę detalicznego C1000 i współorganizatora badania Schuitema, około 68% użytkowników stwierdziło, że preferuje płatności mobilne. Pozostali stwierdzili, że nie ma znaczenia, z jakiej formy płatności korzystają. Co więcej, około połowa użytkowników stwierdziła, że kupiłaby telefon komórkowy z obsługą NFC, gdyby więcej usług NFC było szeroko dostępnych, w tym płatności. Ponad 70% użytkowników stwierdziło, że chce wprowadzać kod PIN w celu sfinalizowania transakcji, nawet w przypadku zakupów o niskiej wartości. Jednak około 78% użytkowników nie chce płacić dodatkowych kilku eurocentów za transakcję w przypadku płatności NFC [7].

(v) *Testy EZ-Link i StarHub w Singapurze*

Spółka zależna urzędu transportu lądowego, EZ-Link, przetwarza ponad 4 miliony transakcji finansowych dziennie w Singapurze i wydaje miliony kart. W październiku 2007 r. EZ-Link wraz z operatorem MNO StarHub rozpoczął 6-miesięczny okres próbny sprzedaży biletów w technologii NFC. W trakcie trwania testów użyto około 20 000 terminali, które akceptowały singapurską portmonetkę tranzytową EZ-Link. Terminale te znajdowały się głównie w pociągach i autobusach, ale można je również znaleźć w niektórych sklepach detalicznych, restauracjach i automatach do sprzedaży [7].

Test StarHub i EZ-Link Singapore był pierwszym na świecie testem NFC FeliCa zapewniającym sprzedaż biletów, a także usługi inteligentnych plakatów. Użytkownicy mogą dotykać tagów umieszczonych na inteligentnych plakatach, aby pobrać adresy URL, kupony lub inne treści promocyjne. Użytkownicy mogą również sprawdzić saldo swojej portmonetki, historię transakcji i inne szczegóły za pomocą urządzenia mobilnego.

Pozostałymi partnerami w tym teście biletów tranzytowych byli Vivotech jako dostawca czytników NFC oraz NXP Semiconductors jako dostawca zestawów chipów NFC do telefonów komórkowych. Test został przeprowadzony z udziałem ponad 800 użytkowników, którzy korzystali ze specjalnie zaprojektowanych telefonów komórkowych z obsługą NFC dostarczonych przez Sony z wbudowanymi układami FeliCa SE.

Zgodnie z wynikami badania, jeśli technologia zostanie zaoferowana, 23% respondentów ankiety przeprowadzonej po zakończeniu badania stwierdziło, że byłoby "bardzo prawdopodobne" przyjęcie tej technologii. Kolejne 45% respondentów stwierdziło, że "prawdopodobnie" przyjęłyby tę technologię. Innym ważnym wynikiem jest to, że około 83% użytkowników korzystało z telefonów podczas testów, aby płacić za przejazdy, a około 70% użytkowników sprawdzało historię swoich transakcji [7].

(vi) *Test Pay-Buy-Mobile w Australii*

Pilotaż Pay-Buy-Mobile (patrz Rozdział 7) został przeprowadzony w Australii z udziałem największego australijskiego MNO Telstra, National Australia Bank i Visa (payWave). Pilotaż został uruchomiony w sierpniu 2008 roku i trwał 3 miesiące. W tym niewielkim pilotażu wzięło udział około 500 użytkowników i 12 akceptantów. Użytkownicy pochodzili głównie z personelu Telstra i National Australia Bank.

Telstra dostarczyła i wydała użytkownikom karty SIM. Aplikacja płatnicza National Australia Bank i Visa została zainstalowana na kartach SIM telefonów komórkowych Sagem my700X z obsługą NFC. Innymi dostawcami byli Inside Contactless dla zestawów chipów NFC w telefonach komórkowych, Vivotech dla czytników NFC w sklepach oraz Cassis International dla rozwiązań biznesowych TSM. Dzięki temu pilotażowi użytkownicy mogli dotykać czytników NFC przy zakupach za 35 USD lub mniej. Zgodnie z wynikami Telstra, około 95% uczestników testu stwierdziło, że "prawdopodobnie" lub "bardzo prawdopodobnie" skorzysta z technologii NFC w przyszłości [7].

(vii) *Próba ING Banku w Rumunii*

Holenderski bank ING i MasterCard (PayPass) testowały opłacalność technologii NFC w systemach płatności mobilnych za zakupy o niskiej wartości w Rumunii. Test rozpoczął się w listopadzie 2008 roku i trwał 7 miesięcy. Próba objęła wielu MNO w Rumunii i tylko jedną platformę TSM dostarczoną przez Venyon.

Test ten był jednym z pierwszych, który umożliwił użytkownikom doładowanie i sprawdzenie salda konta zbliżeniowego MasterCard PayPass za pośrednictwem OTA

ze specjalnym kodem. Próba ta była również pierwszą dla ING Banku i MasterCard w Rumunii. Przy projekcie współpracowali z dostawcą technologii płatniczych Collis, dostawcą platformy usług OTA dla płatności NFC Venyon i tajwańską firmą NFC Toro [7].

Terminale płatnicze z obsługą NFC zostały zainstalowane w około 11 sklepach, w tym w restauracjach typu fast food, kinach i kioskach. Około 360 klientów banku wzięło udział w testach z telefonami komórkowymi Nokia 6212 obsługującymi NFC, które mają wbudowane SE, gdzie zainstalowano aplikację płatniczą.

(viii) *Cep-T Cuzdan Launch w Turcji.*

Kolejny dobry przypadek uruchomienia NFC pochodzi z Turcji. Garanti Bank, Yapı Kredi Bank i MNO Turkcell współpracowały w ramach usługi portfela mobilnego z obsługą NFC. Usługa została uruchomiona komercyjnie w 2011 roku [7].

Turkcell wprowadził na rynek telefon z systemem Android obsługujący technologię NFC (U8650NFC Sonic) pod nazwą Turkcell T20. Turkcell wstępnie ładuje oprogramowanie portfela mobilnego do telefonu komórkowego, który obsługuje również więcej niż jedną aplikację wydaną przez bank. Telefon obsługuje standard protokołu single wire, umożliwiając przechowywanie bezpiecznych aplikacji na kartach SIM. Turkcell obsługuje również elastyczne anteny portfela mobilnego dla telefonów komórkowych, które nie mają funkcji NFC.

Turkcell służy również jako TSM do pobierania i zarządzania bezpiecznymi aplikacjami w swoim portfelu. Platforma TSM została zbudowana we własnym zakresie. Obecnie dostępne są dwie aplikacje płatnicze z dwóch największych prywatnych banków w Turcji.

9.2.2 Transport lub inne próby biletowe

(i) *Bilet komunikacji miejskiej NFC z RMV w Hanau*

RMV (Rhein-Main-Verkehrsverbund) jest jednym z największych regionalnych zarządów transportu publicznego w Europie, który świadczy usługi transportowe dla pięciu milionów mieszkańców w kraju związkowym Hess w Niemczech. Nokia i Vodafone, jako jeden z największych operatorów MNO, wraz z władzami transportu publicznego dla większego obszaru Frankfurtu, RMV, przeprowadziły wspólny projekt w domenie usług biletowych transportu z obsługą NFC. Próba rozpoczęła się na początku 2005 roku i objęła około 200 użytkowników [7].

W tej próbie klienci RMV korzystali z telefonów komórkowych Nokia 3220 z obsługą NFC, które mają inteligentną powłokę NFC, w której przechowywane są bilety, aby uzyskać dostęp do lokalnej sieci autobusowej w Hanau, mieście niedaleko Frankfurtu. Aplikacja RMV do sprzedaży biletów elektronicznych jest bezpiecznie przechowywana na zintegrowanym kontrolerze kart inteligentnych w telefonie komórkowym.

Zgodnie z pierwszymi wynikami ankiety, telefony komórkowe z obsługą NFC są postrzegane jako bardziej atrakcyjne i innowacyjne niż karty inteligentne. Przeprowadzono wiele projektów pilotażowych z innymi operatorami i stronami trzecimi. Usługa rozszerzyła się na szersze zastosowania, w tym domeny aplikacji informacyjnych, lojalnościowych i płatniczych z rosnącą liczbą użytkowników. Obecnie sprzedaż biletów NFC z RMV jest dostępna komercyjnie z programami lojalnościowymi. Na przykład telefony komórkowe Nokia z obsługą NFC mogą być również używane jako karta bonusowa o nazwie "RMV ErlebnisCard".

(ii) *Doświadczenie stadionu NFC w Manchesterze*

MNO Orange UK przeprowadził test usług sprzedaży biletów bezstykowych z klubem piłkarskim Manchester City. Ta niewielka próba została uruchomiona w sierpniu 2006 roku z udziałem około 20 użytkowników, którzy posiadali ważne bilety sezonowe. Wykorzystano telefony komórkowe Nokia 3220 z obsługą NFC i wbudowanym sprzętowym SE. Manchester City Football Club i Orange UK dostarczyły aplikację do sprzedaży biletów na te urządzenia. Uczestniczący kibice

mogli używać swoich telefonów komórkowych z obsługą NFC, aby dotknąć czytników NFC przy bramkach stadionu piłkarskiego Manchester City i łatwo wejść do kołowrotów [7].

(iii) Próby Bouygues Telecom w Paryżu

Największy francuski MNO Bouygues Telecom przeprowadził w Paryżu 3-miesięczny test sprzedaży biletów tranzytowych z obsługą NFC. Próba ta rozpoczęła się w listopadzie 2006 roku. Wzięło w nim udział około 50 użytkowników. Głównymi dostawcami usług byli RATP (Régie Autonome des Transports Parisiens) i SNCF (Société Nationale des Chemins de fer Français), którzy są dostawcami bezstykowych kart tranzytowych Navigo. Dostarczyli oni aplikację biletową z obsługą NFC, która została załadowana i zainstalowana na karcie SIM użytkownika. Celem tej próby jest umożliwienie użytkownikom płacenia za bilety przy bramkach lub w czytnikach w autobusach, które akceptują aplikację biletową Navigo za pomocą ich telefonów komórkowych z obsługą NFC.

Użytkownicy mogli również doładowywać swoje karty za pośrednictwem mobilnego Internetu. Bouygues Telecom dostarczył telefon komórkowy z obsługą NFC od japońskiego producenta telefonów komórkowych, NEC, który został specjalnie zaprojektowany do testów. Innymi zaangażowanymi dostawcami byli Axalto/Gemalto jako dostawca SE opartego na karcie SIM oraz Inside Contactless jako dostawca zestawu chipów NFC. Ta pierwsza próba przeprowadzona przez Bouygues Telecom doprowadziła do kolejnych pilotażowych rozwiązań w zakresie biletów tranzytowych i płatności we Francji [7].

(iv) Portfel O2

Telefonica O2, jako jeden z największych MNO, ogłosiła O2 Wallet w listopadzie 2007 roku i przeprowadziła 6-miesięczny test we współpracy z różnymi dostawcami usług, a mianowicie: TfL (Transport for London), TranSys, który obsługuje inteligentną kartę Oyster dla TfL, Venyon dla rozwiązań biznesowych TSM, Barclaycard, Visa Europe (payWave), Nokia, Giesecke & Devrient dla zarządzania danymi, Innovision dla inteligentnych tagów plakatowych, NXP Semiconductors, Inside Contactless, Consult Hyperion dla doradztwa i AEG Europe. O2 Wallet obejmował wiele usług, od biletów transportowych po inteligentne aplikacje plakatowe, i był pierwszym w Wielkiej Brytanii pilotażem NFC na dużą skalę [7,15].

Pilotaż O2 Wallet utorował drogę do szerokiego wykorzystania telefonów komórkowych jako kart Oyster do podrózowania po Londynie, płacenia za zakupy kartą Barclaycard i dostępu do wydarzeń. W pilotażu wzięło udział około 500 abonentów sieci komórkowej O2, którzy zostali wyposażeni w telefony komórkowe Nokia 6131 z obsługą NFC. W programie pilotażowym wykorzystano wbudowane urządzenia SE. Użytkownik musi jedynie przechowywać aplikację Oyster z obsługą NFC na swoim telefonie komórkowym i wstępnie załadować swoją aplikację. Aplikacja ta eliminuje potrzebę noszenia przez użytkowników inteligentnych kart Oyster w portfelach. Użytkownicy mogą płacić za swoje koszty podróży za pośrednictwem aplikacji Oyster, po prostu dotykając swoich telefonów komórkowych do czytników Oyster NFC na stacjach metra w Londynie oraz w autobusach i tramwajach (patrz rysunek 9.8). Jeśli telefon użytkownika zadzwoni podczas dokonywania transakcji, może on odebrać połączenie. Połączenie lub wiadomość tekstowa nie koliduje z usługą NFC.

Oprócz wstępnie załadowanej aplikacji do sprzedaży biletów w O2 Wallet, dostawcy usług umożliwiają płatności, inteligentne plakaty i aplikacje kontroli dostępu. Usługa płatności jest dostarczana przez Barclaycard, który wprowadził pierwszą kartę kredytową w Wielkiej Brytanii i Visa payWave dla O2 Wallet. Użytkownicy mogli dokonywać płatności za pomocą aplikacji płatniczej Barclaycard zainstalowanej na ich telefonach komórkowych. Ta aplikacja płatnicza może być używana u około 5000 sprzedawców, w tym Books Etc., Chop'd, Coffee Republic, EAT i Krispy Kreme.

Użytkownicy mogą również dotykać inteligentnych plakatów, aby zbierać

informacje o restauracjach i innych lokalizacjach. Znaczniki na inteligentnych plakatach służą jako skróty do usług dostępnych za pośrednictwem telefonu komórkowego. Na przykład, gdy użytkownik dotknie znacznika na inteligentnym plakacie, może automatycznie wybrać numer, wysłać wiadomość tekstową lub wyświetlić stronę internetową zawierającą informacje



Rysunek 9.8 Portfel O2 [1]. Zdjęcie wykonane przez Juha Sarkkinen, Miasto Oulu, Projekt Smart Touch.

o wydarzeniu itd. Kolejną ważną usługą O2 Wallet jest kontrola dostępu. Użytkownicy mogą uzyskać dostęp i wejść do strefy VIP obiektów rozrywkowych O2 za pomocą telefonu komórkowego z obsługą NFC.

Zgodnie z wynikami ankiet przeprowadzonych po pilotażu O2 Wallet, ponad połowa uczestników stwierdziła, że gdyby usługi zbliżeniowe były dostępne, korzystaliby z nich na swoich telefonach komórkowych. Około 90% uczestników było zadowolonych z technologii NFC i ponownie zdecydowana większość stwierdziła, że dotykanie telefonów komórkowych jest wygodniejsze niż korzystanie z kart inteligentnych Oyster. Obecnie trwają intensywne prace nad rozszerzeniem usług O2 Wallet. Pilotaże i testy prowadzą O2 Wallet do komercyjnego uruchomienia.

(v) *Testy Orange w Hiszpanii*

W kwietniu 2008 r. w Malagna rozpoczęto kolejną próbę systemu biletowego. Była to niewielka próba, w której testowano pobieranie opłat w autobusach z udziałem około 50 użytkowników. Partnerami w tym pilotażu byli EMT jako dostawca usług pobierania opłat tranzytowych oraz France Telecom-Orange Spain jako MNO. Telefony komórkowe z obsługą NFC dostarczone przez Sony to Sony Ericsson Z750i. Aplikacja była przechowywana na kartach SIM i została dostarczona przez Oberthur Technologies. Był to pierwszy pilotażowy projekt NFC w Orange Spain w dziedzinie aplikacji biletowych opartych na NFC [7].

9.2.3 Inne próby

(i) *Próby podczas Londyńskiego Tygodnia Mody*

Atrakcyjny i innowacyjny przypadek został wdrożony przez jednego z największych MNO, Telefonica O2, w Wielkiej Brytanii. O2 zorganizowała i przeprowadziła małą próbę w lutym 2008 roku podczas London Fashion Week, który jest kluczowym wydarzeniem dla projektantów w Londynie, aby pokazać swoje projekty nabywcom mody z całego świata. Celem tej próby było zapewnienie nabywcom mody możliwości natychmiastowego wyrażenia opinii na temat kolekcji Emilio de la Morena. Ten test wiadomości z obsługą NFC został przeprowadzony z ograniczoną liczbą kupujących lub użytkowników.

Aby umożliwić przeprowadzenie tej próby, wykorzystano inteligentne plakaty z tagami NFC do automatycznego wysyłania wiadomości tekstowych do Emilio de la Morena. Ponadto kupujący modę byli wyposażeni w telefony komórkowe Nokia 6131 z obsługą NFC, a gdy kupujący dotknął tagów NFC umieszczonych na inteligentnych plakatach za pomocą telefonu komórkowego, zarejestrował swoje opinie i zainteresowania określonym projektem kolekcji jesienno-zimowej Emilio de la Morena. Wiadomość tekstowa była następnie automatycznie wysyłana do projektanta [7].

(ii) *Pilot Pass and Fly na lotnisku w Nicei*

Pass and Fly był wspólnym projektem portu lotniczego Nicea-Lazurowe Wybrzeże i Air France we współpracy z Amadeus i IER. Pilotaż został uruchomiony w kwietniu 2009 roku na lotnisku Nicea-Lazurowe Wybrzeże i trwał 6 miesięcy. Celem pilotażu było umożliwienie pasażerom pobierania cyfrowych kart pokładowych na telefony komórkowe przy użyciu technologii NFC. Firma Amadeus opracowała aplikacje dla telefonów komórkowych, systemu kontroli odlotów i czytników lotniskowych w celu udostępniania i wyświetlania informacji istotnych dla procesu wejścia pasażera na pokład. Firma IER dostarczyła kabiny i czytniki NFC zintegrowane z infrastrukturą lotniska i podłączone do systemu zarządzania pasażerami Air France. Air France dostarczyła elektroniczne karty pokładowe [7].

Członkowie programu Club Airport Premier (CAP) na lotnisku w Nicei oraz programu lojalnościowego Air France dla osób często podróżujących wzięli udział w programie pilotażowym Pass and Fly. Korzystali oni z telefonów komórkowych Nokia 6212 z obsługą NFC lub naklejek NFC, aby otrzymać elektroniczną kartę pokładową i zbierać punkty lojalnościowe. Aplikacje zostały załadowane na telefony komórkowe Nokia 6212 z obsługą NFC, które wykorzystują wbudowany sprzęt oparty na SE.

Karty pokładowe były zgodne z formatem Międzynarodowego Zrzeszenia Przewoźników Powietrznych. Aplikacja NFC umożliwiała również użytkownikom zdobywanie punktów w programie lojalnościowym dla osób często podróżujących. Aby umożliwić pobranie aplikacji, pasażer musiał najpierw dokonać odprawy przez Internet przed udaniem się na lotnisko.

Po zakończeniu procesu odprawy użytkownik przyłożył swój telefon komórkowy do czytnika NFC Pass and Fly. Urządzenie zidentyfikowało pasażerkę i wyszukało informacje o jej programie lojalnościowym i karcie pokładowej. Cyfrowa karta pokładowa w formacie IATA została wysłana na telefon komórkowy użytkownika. Ponadto, punkty programu lojalnościowego Nice Airport CAP zostały automatycznie naliczone. W związku z tym członkowie programu lojalnościowego nie musieli udawać się do oddzielnego kiosku, aby otrzymać punkty.

Następnie użytkownik ponownie przyłożył swój telefon komórkowy do drugiego czytnika NFC w punkcie kontroli bezpieczeństwa. Terminal ten wyświetlał kartę pokładową w formie elektronicznej dla pracowników ochrony. Przy bramce do wejścia na pokład personel linii lotniczych musiał jedynie sprawdzić dane identyfikacyjne pasażera. Czytnik NFC sprawdzał kartę pokładową po raz trzeci, a terminal drukował kupon z przydziałem miejsca. Pass and Fly to jeden z pierwszych innowacyjnych pilotów w branży lotniczej. Ta nowa infrastruktura z obsługą NFC i przepływem informacji przyspiesza korzystanie z lotniska przez podróżnych, oszczędzając czas i koszty.

(iii) *Frekwencja studentów w londyńskim college'u*

Aplikacje płatnicze i biletowe z obsługą NFC są obecnie bardzo popularne. Dodatkowo, frekwencja i inne aplikacje do zarządzania pracownikami mogą być zaimplementowane jako jedna z usług NFC za pośrednictwem telefonów komórkowych. Dobry test ma miejsce w Newham College w Wielkiej Brytanii. Próba

ta rozpoczęła się w styczniu 2010 roku i nadal trwa [7].

zasięgu

Zgodnie z testem, Newham College rozdał telefony komórkowe Nokia 6212 z obsługą NFC czterem nauczycielom, którzy dotykają tych telefonów komórkowych do kart identyfikacyjnych około 120 uczniów zamiast rejestrować się każdego dnia. Nauczyciele logują się

sami, dotykając swoich telefonów do tagów po przybyciu do klasy. Dane dotyczące obecności są przechwytywane i wysyłane z telefonów komórkowych obsługujących technologię NFC do "systemu rejestracji czasu pracy" dostarczanego przez fińską firmę Reslink.

Uczelnia korzysta z "systemu czasu i obecności", aby zaoszczędzić czas i koszty związane z papierową robotą przy rejestrowaniu obecności na początku każdych zajęć i ograniczyć papierową robotę dla administratorów. Karty identyfikacyjne uczniów na potrzeby pilotażu zostały zmodyfikowane za pomocą bezdotykowych naklejek zawierających numery identyfikacyjne, dzięki czemu gdy nauczyciele dotykają ich, identyfikacja ucznia jest przesyłana do telefonu komórkowego nauczyciela. Jeśli ta próba zakończy się sukcesem, może doprowadzić do rozszerzenia programu na 300 nauczycieli i 16 000 studentów.

9.3 Rozdział Podsumowanie

Obecnie prowadzonych jest wiele prób i projektów mających na celu wdrożenie technologii NFC. Niektóre modele są opracowywane przez uniwersytety, firmy, a także jako wspólny wysiłek uniwersytetów i firm. Dzięki tym próbom i projektom uczestniczące podmioty starają się zrozumieć naturę technologii NFC zarówno pod względem społecznym, jak i biznesowym.

Miasta NFC to najpopularniejsze implementacje technologii NFC. Celem miasta NFC może być albo przetestowanie implementacji, albo nawet faktyczne wykorzystanie jej na określonej arenie. Miasta NFC są wykorzystywane głównie do testowania społecznego aspektu technologii NFC w porównaniu z testami i projektami. Kwestie użyteczności wraz z problemami związanymi z technologią są uzyskiwane w sposób ciągły poprzez testy w miastach NFC. W przypadku testów i projektów NFC, aspekt biznesowy aplikacji lub ekosystemu NFC jest testowany bardziej niż aspekt społeczny. W tym rozdziale pokrótko przedstawiliśmy wszystkie miasta NFC (miasto Oulu, miasto Nicea i inteligentne przestrzenie miejskie) oraz niektóre ważne wdrożenia technologii NFC na całym świecie.

Referencje

- [1] Tuikka, T. i Isomursu, M. (red.) (2009) *Touch the Future with a Smart Touch*, VTT Tiedotteita - Research Notes 2492, Espoo, Finlandia, 2009. Dostępny pod adresem: www.vtt.fi/inf/pdf/tiedotteet/2009/T2492.pdf (dostęp 10 lipca 2011).
- [2] Smart Touch City of Oulu - Usługi dzięki technologii NFC. Dostępny pod adresem: ttuki.vtt.fi/smarttouch/www/kuvat/December08_Newsletter.pdf (dostęp 10 lipca 2011).
- [3] Haïkio®, J., Wallin, A., and Isomursu, M. (2009) *Touch the Future with a Smart Touch*, Section 5.2.2, VTT Tiedotteita - Research Notes 2492, Editors: Tuikka, T., Isomursu, M., Espoo, Finlandia, 2009. Dostępny pod adresem: www.vtt.fi/inf/pdf/tiedotteet/2009/T2492.pdf (dostęp 10 lipca 2011 r.).
- [4] Rouru-Kuivala, O. (2009) *Touch the Future with a Smart Touch*, Section 5.2.3, VTT Tiedotteita - Re- search Notes 2492, Editors: Tuikka, T., Isomursu, M., Espoo, Finlandia, 2009. Dostępny pod adresem: www.vtt.fi/inf/pdf/tiedotteet/2009/T2492.pdf (dostęp 10 lipca 2011 r.).
- [5] Rouru-Kuivala, O. (2009) *Touch the Future with a Smart Touch*, Section 5.1.2, VTT Tiedotteita - Re- search Notes 2492, Editors: Tuikka, T., Isomursu, M., Espoo, Finlandia, 2009. Dostępny pod adresem: www.vtt.fi/inf/pdf/tiedotteet/2009/T2492.pdf (dostęp 10 lipca 2011 r.).
- [6] Rouru-Kuivala, O. (2009) *Touch the Future with a Smart Touch*, Section 5.4.1, VTT Tiedotteita - Re- search Notes 2492, Editors: Tuikka, T., Isomursu, M., Espoo, Finlandia, 2009. Dostępny pod adresem: www.vtt.fi/inf/pdf/tiedotteet/2009/T2492.pdf (dostęp 10 lipca 2011 r.).
- [7] NFC Times, Project Map, <http://www.nfcetimes.com/nfc-projects> (dostęp 10 lipca 2011 r.).
- [8] Smart Urban Spaces, <http://www.smarturbanspaces.org/> (dostęp: 10 lipca 2011 r.).
- [9] Smart Urban Spaces - City of Oulu, <http://www.ouka.fi/sus/english/> (dostęp: 10 lipca 2011 r.).

- [10] Research Notes, 2011 Third International Workshop on Near Field Communication, Hagenberg, Austria, 22 lutego 2011 r.
- [11] Research Notes, WIMA NFC 2011 - 5th Global NFC Applications Products & Services Congress, Monaco, Francja, 19-21 kwietnia 2011 r.
- [12] Payez Mobile, <http://www.payezmobile.com> (dostęp: 10 lipca 2011 r.).
- [13] Miranda, S. and Pastorelly, N. (2011) *NFC Mobiquitous Information Service Prototyping at the University of Nice Sophia Antipolis and Multi-mode NFC Application Proposal*. Proceedings of 2011 Third International Workshop on Near Field Communication, Hagenberg, Austria, 22 lutego 2011, s. 3-8.
- [14] Mobey Forum Enrollment Task Force (2008) *Best Practices for Mobile Financial Services*, Mobey Forum, 2008, dostępnepod adresem:
<http://www.mobeyforum.org/content/download/460/2768/file/Best%20Practices%20for%20MFS.%20Enrolment%20Business%20model%20analysis%20final.pdf> (dostęp 10 lipca 2011 r.).
- [15] O2 News Centre, <http://mediacentre.o2.co.uk> (dostęp: 10 lipca 2011 r.).

Indeks

- 3DES, *patrz* potrójny DES
3GPP, *patrz* 3rd Generation Partnership Project 3rd Generation Partnership Project (3GPP), 10, 82
odpowiedzialność, 21, 248
aktywny tryb komunikacji, 8, 73-4, 118
urządzenie aktywne, 8, 73-4, 118
zaawansowany standard szyfrowania (AES), 258 AES, *zob.* zaawansowany standard szyfrowania AM TSD, *zob.* tryb autoryzowany TSD
AMS, *patrz* anonimowość oprogramowania do zarządzania aplikacjami, 278
APDU, *patrz* jednostka danych protokołu aplikacji Połączenie APDU, 213-14
aplet, 152
obudowa aplikacji, *patrz* pula aplikacji
program ładujący aplikacje, 319
oprogramowanie do zarządzania aplikacjami (AMS), 162
pula aplikacji, 326-8
jednostka danych protokołu aplikacji (APDU), 213-14
domena bezpieczeństwa dostawcy aplikacji (APSD), 315, 320
dostawca aplikacji, *zob.* dostawca usług APSD, *zob.* bezpieczeństwo dostawcy aplikacji domena kryptografia asymetryczna, 259-61 kryptografia krzywych eliptycznych, 260-261 Rivest, Shamir i Adleman, 260
zrównoważona komunikacja asynchroniczna, LLCP, 110
atak, 21, 249-52
Odmowa usługi, 22, 252, 268
podsluch, 23, 250, 270, 272
fałszowanie wiadomości e-mail, 252
Podsywanie się pod adres IP, 252
wyciek, 250
Man in the Middle Attack, 23, 250-251, 271, 272
farmacja, 251-2
phishing, 250
fałszowanie połączeń telefonicznych, 267
atak przekaźnikowy, 23, 251, 271
atak powtórkowy, 23, 251, 271
SMS spoofing, 252, 267-8
inżynieria społeczna, 250
atak typu spoofing, 22, 252, 267-8
URI spoofing, 267
Podsywanie się pod adresy URL, 252, 267
atakowanie NFC, 23, 270-272
uszkodzenie danych, 23, 270 wstawianie danych, 23, 271 modyfikacja danych, 23, 271
podsluch, 23, 250, 270, 272
MIM Attack, 23, 250-251, 271-2
atak przekaźnikowy, 23, 251, 271
atak powtórkowy, 23, 251, 271
atakowanie czytników NFC, 23, 268
atakowanie tagów NFC, 22, 267-8
manipulowanie danymi znaczników, 22, 268 spoofing, *zob.* ataki spoofingowe

- atakowanie tagów NFC (*ciąg dalszy*) klonowanie tagów, 22, 267 ukrywanie znaczników, 22, 268 podszywanie się pod tag, 267 wymiana tagów, 22, 268 atakowanie kart inteligentnych, 23, 269-70 atak inwazyjny, 269 atak kanałem bocznym, 269 uwierzytelnianie, 20, 243-6 uwierzytelnianie biometryczne, 244-6 autoryzacja, 20, 246 tryb autoryzowany, 16, 323-4 TSD w trybie autoryzowanym (AM TSD), 323-4 dostępność, 20, 248 zabezpieczenia systemu zaplecza, 23-4, 272 kod kreskowy, 4-5, 51-3 jednowymiarowy kod kreskowy, 5, 51 dwuwymiarowy kod kreskowy, 5, 51-2 stacja bazowa, 45-6 uwierzytelnianie biometryczne, 244-6 bluetooth, 49 ekosystem biznesowy, 25-6, 283-6 modelowanie biznesowe, 293-5 modele biznesowe, ekosystem NFC, 30, 297-300 rozproszone, 30, 298 MNO centric, 30, 297-8 TSM centric, 30, 299 Calypso, 7, 94 zarządzanie zawartością kart, 316-24 tryb emulacji karty, *patrz* tryb pracy emulacji karty programowanie trybu emulacji karty, 211-15 tryb pracy emulacji karty, 12-13, 111-12, 131-5, 211-15 korzyści z aplikacji, 135 aplikacje, 133 ogólny model użytkowania, 132-3 programowanie, 211-15 architektura stosu protokołów, 111-12 operator kart, 319 wydawca kart, 319 bank wydający karty (CIB), 304-5 menedżer kart, 316 producent kart, 319 CASD, *patrz* domena bezpieczeństwa organu kontrolującego CDC, *patrz* konfiguracja podłączonego urządzenia, organ centralny, 317 organ wydający zaświadczenia, 263 miasta, 33-4, 331-41 Miasto Nicea, 34, 337-9 Miasto Oulu, 33-4, 331-7 Smart Urban Spaces, 34, 339-41 Miasto Nicea, 34, 337-9 Miasto Oulu, 33-4, 331-7 CLDC, *patrz* konfiguracja podłączonego ograniczonego urządzenia karty inteligentne ze sprzężeniem ściślym, 6, 66 kolator, 319 bezstykowe karty inteligentne, standaryzacja, 6-7, 66 ISO/IEC 10536, 66 ISO/IEC 14443, 6-7, 66, 92-4 ISO/IEC 15693, 66 Pakiet com.nokia.nfc.llcp, 201 Pakiet com.nokia.nfc.p2p, 200 Interfejs ErrorRecoveryListener, 202-3 Interfejs LLCPConnection, 203 Interfejs LLCPConnectionListener, 203 Interfejs LLCPLinkListener, 203 Klasa LLCPManager, 202 Klasa poleceń, 164-5 typy poleceń, 164 poufność, 243 konfiguracja podłączonego urządzenia (CDC), 161 ograniczona konfiguracja podłączonego urządzenia (CLDC), 161 transport zorientowany na połaczenie, LLCP, 110 transport bezpołączeniowy, LLCP, 110 stykowe karty inteligentne, 6, 63-5 interfejs API komunikacji bezstykowej, *zob.* JSR 257 bezstykowe karty inteligentne, 6-7, 65-8 Wyjątek ContactlessException, 183 organ kontrolny, 319 domena bezpieczeństwa organu kontrolującego (CASD), 15, 315, 320 ukryty kanał, *zob.* wyciek

- kryptografia, 21, 257
asymetryczna, 259-61
nowoczesna, 259-61
klucz publiczny, 259-61
klucz tajny, 258-
9 symetryczny,
258-9 tradycyjny,
258-9
klienci, 293
- DAP, *patrz* wzorzec uwierzytelniania danych wzorzec uwierzytelniania danych (DAP), 320 uszkodzenie danych, 23, 270, 272 standard szyfrowania danych (DES), 258 wstawianie danych, 23, 271-2 integralność danych, 21, 248 modyfikacja danych, 23, 271-2 dekollatory, 319 tryb delegowany, 16, 322-3 tryb delegowany TSD (DM TSD), 322-3 odmowa usługi, 22, 252, 268 DES, *patrz* standard szyfrowania danych certyfikat cyfrowy, 263 podpis cyfrowy, 261-2 klasa DiscoveryManager, 181 rozproszony model biznesowy, 298 DM TSD, *zob.* tryb delegowany TSD DoS, *zob.* odmowa usługi karty inteligentne z podwójnym interfejsem, 67
- EAN, *patrz* europejski numer artykułu EAN-13, 5, 52 podsłuchiwanie, 23, 250, 270, 272 ECC, *zob.* kryptografia krzywych eliptycznych ECDH, *patrz* elliptic curve diffie - hellman Eclipse IDE, 156 Instalacja Eclipse, 155-8 Eclipse ME, 156 ECMA International, 10, 81 ekosystem, 283-5 EDGE, *patrz* rozszerzone dane dla ewolucji gsm widmo elektromagnetyczne, 47 Kryptografia krzywych eliptycznych (ECC), 260-261 krzywa eliptyczna diffie - hellman (ECDH), 276 fałszowanie wiadomości e-mail, 252 sprzęt wbudowany, 14, 85 EMVCo, 10, 82 enhanced data for gsm evolution (EDGE), 48-9 uwierzytelnianie podmiotu, 277 Interfejs ErrorRecoveryListener, 202-3 ETSI, 10, 81 ETSI SCP, *patrz* platforma kart inteligentnych ETSI Platforma kart inteligentnych ETSI, 10, 81 europejski numer artykułu (EAN), 5, 52 Kod kreskowy EAN-13, 5, 52 transmisja dalekiego pola, 57-8 FeliCa, 7, 94, 98 firewall, 265 role funkcjonalne, GlobalPlatform, 319 ogólny pakietowy system radiowy (GPRS), 48-9 globalny system telefonii komórkowej (GSM), 48-9 GlobalPlatform, 9, 79-80, 314-16 specyfikacja karty, 15, 314-16 specyfikacja przesyłania wiadomości, 316 Specyfikacja karty GlobalPlatform, 15, 314-16 domena zabezpieczeń dostawcy aplikacji, 315, 320 domena bezpieczeństwa organu kontrolującego, 15, 315, 320 Środowisko GP, 314-15 Zaufane ramy GP, 314-15 domena zabezpieczeń emitenta, 15, 315, 320 OPEN, 314-15 środowisko uruchomieniowe, 314-15 dodatkowa domena bezpieczeństwa, 15, 315, 320 maszyna wirtualna, 315 Role funkcjonalne GlobalPlatform, *zob.* role funkcjonalne Specyfikacja komunikatów GlobalPlatform, 316 Środowisko GP, *patrz* OPEN Zaufane ramy GP, 314-15 GPRS, *patrz* ogólny pakietowy system radiowy GSM, *patrz* globalny system telefonii komórkowej GSM Association (GSMA), 9, 80 GSMA, *patrz* GSM Association

- kod uwierzytelniania wiadomości oparty na skrócie (HMAC), 261
haszowanie, 261
HCI, *patrz* interfejs kontrolera hosta
HCP, *patrz* protokół kontrolera hosta
HDLC, *patrz* wysokopoziomowa kontrola łącza danych Program Hello, 165-8
szybki dostęp pakietowy (HSPA), 48-9
kontrola łącza danych wysokiego poziomu (HDLC), 89
HMAC, *patrz* kod uwierzytelniania wiadomości oparty na skrócie kontroler hosta, 10-11, 89-90
interfejs kontrolera hosta (HCI), 10-11, 89-92
bramki, 90
Pakiety HCP, 91
rury, 90-91
procedury, 92
rejestry, 91
protokół kontrolera hosta (HCP), 90
sieć hosta, 90
HSPA, *patrz* szybki dostęp pakietowy hybrydowe karty inteligentne, 67
- Producent układów scalonych, 319
IDPS, *patrz* System wykrywania i zapobiegania włamaniom
IEC, *patrz* Międzynarodowa Komisja Elektrotechniczna
podsywanie się, 268 nieodłączne
bezpieczeństwo, 70
inicjator, 8, 74, 119
instalacja, *patrz* Instalacja Eclipse
Międzynarodowa Komisja Elektrotechniczna (IEC), 10, 80-81
Międzynarodowa Organizacja Normalizacyjna (ISO), 10, 80-81
System wykrywania i zapobiegania włamaniom (IDPS), 265
atak inwazyjny, 269
Podsywanie się pod adres IP, 252
ISD, *zob.* domena zabezpieczeń emitenta
ISO, *patrz* Międzynarodowa Organizacja Normalizacyjna
ISO/IEC 10536, 66
- ISO/IEC 14443, 6-7, 66, 92-4
transmisja danych, 97-8
zasady działania, 93
Typ A, 94, 97-8
Typ B, 94, 97-8
ISO/IEC 15693, 66
ISO/IEC 18092, 11, 94-5
ISO/IEC 21481, 11, 94-5
ISO/IEC 7816, 63-5
domena bezpieczeństwa emitenta (ISD), 15, 315, 320
- J2EE, *patrz* Java 2 enterprise edition J2ME, *patrz* Java 2 micro edition J2SE, *patrz* Java 2 standard edition JAD, *patrz* Java application descriptor
japoński standard przemysłowy (JIS) X 6319, 94, 98
transmisja danych, 98
Plik manifestu JAR, 169
JAR, *patrz* plik archiwum Java
Java 2 enterprise edition (J2EE), 154
Java 2 micro edition (J2ME), 154
Java 2 standard edition (J2SE), 154
Java application descriptor (JAD), 170
Java archive file (JAR), 169-70
Java Community Process (JCP), 10, 81
Specyfikacja języka Java (JLS), 153
Platforma Java, 152-5
enterprise edition, 154
micro edition, 154
standard edition, 154
Ządanie specyfikacji Java (JSR), 155
Technologia Java, 153-5
Maszyna wirtualna Java (JVM), 153
JavaCard, 63
system operacyjny, 63
maszyna wirtualna, 63
System operacyjny JavaCard (JavaCard OS), 63
JavaCard OS, *patrz* system operacyjny JavaCard JavaCard RMI (JCRMI), 214
Maszyna wirtualna JavaCard (JavaCard VM), 63
Maszyna wirtualna JavaCard, *patrz* pakiet javax.microedition.contactless, 181
Wyjątek ContactlessException, 183
Klasa DiscoveryManager, 181

- Interfejs TagConnection, 182
- Interfejs TargetListener, 182 Interfejs TargetProperties, 182 Klasa TargetType, 181-2
- pakiet javax.microedition.contactless.ndef, 183
 - Klasa NDEFMessage, 183 Klasa NDEFRecord, 183-4 Interfejs NDEFRecordListener, 184-5 Klasa NDEFRecordType, 184
- pakiet javax.microedition.contactless.rf, 185
- Pakiet javax.microedition.contactless.sc, 185
- Pakiet
 - javax.microedition.contactless.visua l, 185
- Pakiet javax.microedition.io, 177
 - Klasa PushRegistry, 177-8
- Pakiet javax.microedition.lcdui, 164 Klasa poleceń, 164-5
 - Typy poleceń, 164 Pakiet
- javax.microedition.midlet, 161
 - Klasa MIDlet, 163-4
- JCP, *patrz* Java Community
- Process Połączenie JCRMI, 214
- JCRMI, *patrz* JavaCard RMI
- JLS, *patrz* specyfikacja języka Java
- JSR, *patrz* żądanie specyfikacji języka Java JSR 177, 18, 179, 212-15
 - JSR 257, 18, 179-200
- Rozszerzenia API JSR 257, 200-204 JVM, *zob.* wirtualna maszyna Javy
- KDF, *zob.* funkcja wyprowadzania klucza funkcja wyprowadzania klucza (KDF), 276 zarządzanie kluczami, 264
 - kluczowy organ zarządzający (KMA), 62-3
 - kluczowe wskaźniki, modelowanie
- biznesowe NFC, 295-7
 - dostawca usług bezprzewodowych, 29-30, 297
 - menedżer platformy, 29, 295-7
 - emitent SE, 29, 295
- typy kluczy,
 - bezpieczeństwo, 264
 - klucz publiczny, 264

- kilobajtowa maszyna wirtualna (KVM), 153 KMA, *zob.* organ zarządzania kluczami KVM, *zob.* kilobajtowa maszyna wirtualna 271, 272
- zabezpieczenia token zarządzania, 323
- warstwowe, 256-7 plik manifestu, *patrz* plik manifestu
- wyciek, 250 JAR manipulowanie danymi znaczników, 22, 268 karty
- najmniejszy przywilej, 256 inteligentne oparte na pamięci, 60-61
- zarządzanie cyklem życia, 316-24 handlowcy, 293
- aktywacja łącza, LLCP, *patrz* aktywacja kod uwierzytelniania wiadomości (MAC), 261
- łącza, LLCP
- aktywacja łącza, LLCP, 110
- dezaktywacja łącza, LLCP, 110
- nadzór łącza, LLCP, 110 typy
- list, Java ME, 176
- asynchroniczne
- zrównoważone LLCP
- komunikacja, *patrz* asynchroniczna
- komunikacja zrównoważona, LLCP
- Transport zorientowany na połaczenie LLCP, *patrz* transport zorientowany na połaczenie LLCP
- Transport bezpołączeniowy LLCP, *patrz* transport bezpołączeniowy, LLCP
- Dezaktywacja łącza LLCP, *patrz* dezaktywacja łącza, LLCP
- Nadzór łącza LLCP, *patrz* nadzór łącza, LLCP
- multipleksowanie protokołów LLCP, *patrz* multipleksowanie protokołów, LLCP
- Rejestr push LLCP, 203-4
- LLCP, *patrz* protokół kontroli łącza logicznego LLCPConnection interface, 203 LLCPConnectionListener interface, 203 LLCPLinkListener interface, 203
- LLCPManager class, 202
- token lądowania, *patrz* token zarządzania
- protokół kontroli łącza logicznego (LLCP), 109-10
- MAC, *patrz* kod uwierzytelniania wiadomości
- karty z paskiem magnetycznym, 6, 59-60
- Man in the Middle Attack, 23, 250-251,

- mikroprocesorowe karty inteligentne,
61 bezpieczeństwo oprogramowania
pośredniczącego, 23-4, 272 MIDlet,
152
Klasa MIDlet, 163-4
Opakowanie MIDlet, 168-
70 Stany MIDlet, 162-4
 stan aktywny, 163
 stan zniszczenia,
 163 stan
 wstrzymania, 162
Pakiet MIDlet, 168-70
MIFARE, 7, 94, 97-8
MIM, *patrz* Man in the Middle
Attack MNO, *patrz* operator sieci
komórkowej MNO centric business
model, 297-8
Mobey Forum, 289
 modele biznesowe,
 297
 wymagania dotyczące modelu
biznesowego, 293-4 Wymagania dotyczące
modelu biznesowego Mobey Forum,
 293-4
Modele biznesowe Mobey Forum,
297 komunikacja mobilna, 48-50
producenci telefonów komórkowych, 290
mobilne techniki interakcji, 115-18
 wskazując, 116-17
 skanowanie, 117
 dotykanie, 116
operator sieci komórkowej (MNO),
290 architektura telefonu
komórkowego, 46-7
sieć telefonii komórkowej, 45-
 6 stacja bazowa, 45-6
 mobilne centrum przełączania, 45-6
 telefon komórkowy, 3-4, 43-5
 programowanie mobilne, 158-79
 podpis mobilny, 261-2
 mobilne centrum przełączania,
 45-6
operator wirtualnej sieci komórkowej
 (MVNO), 28
nowoczesna kryptografia, *zob.*
 kryptografia asymetryczna
MULTOS, 62-3
 organ zarządzania kluczami (KMA), 62-
3 wzajemne uwierzytelnianie, 246
MVNO, *zob.* operator wirtualnej sieci
komórkowej
N Mark, 78-9, 121
Komunikat NDEF, 102-3

- Format rekordu push NDEF, 199-200 NFC, *patrz* format wymiany danych NFC Klasa NDEFMessage, 183 Klasa NDEFRecord, 183-4 Interfejs NDEFRecordListener, 184-5 Klasa NDEFRecordType, 184 Interfejs NDEFTagConnection, 185 Interfejs i protokół komunikacji bliskiego zasięgu-1 (NFCIP-1), 11, 94-5 Interfejs i protokół komunikacji bliskiego zasięgu-2 (NFCIP-2), 11, 95-6 komunikacja bliskiego zasięgu (NFC), 1-39, 42-3, 68-70 antena, 10-11, 82, 86 front-end bezstykowy, 10-11, 82, 86 kontroler, 10-11, 82, 86 interfejs, 10-11, 82, 86 telefon komórkowy, 8, 75 czytnik, 8, 75 bezpieczny element, 14, 83-6 znacznik, 8, 75 transmisja bliskiego pola, 57-8 NFC, *patrz* komunikacja bliskiego zasięgu Antena NFC, 10-11, 82, 86 Rozwój aplikacji NFC, 17-19, 151-239 programowanie trybu emulacji karty, 211-15 programowanie trybu peer-to-peer, 200-211 programowanie trybu czytnika/zapisu, 179-200 Producenci zestawów chipów NFC, 288 Miasta NFC, *patrz* miasta NFC CLF, *patrz* NFC contactless front-end NFC contactless front-end (NFC CLF), 10-11, 82, 86 Kontroler NFC, 10-11, 82, 86 Format wymiany danych NFC (NDEF), 102-8 ładunek zdefiniowany przez aplikację, 102-3 komunikat, 102-3 rekord, 102-3 Ekosystem NFC, 25-30, 286-304 kluczowe wskaźniki, 29-30, 295-7 interesariusze, 27-8, 286-93

- Telefony komórkowe z obsługą NFC, 8, 75
architektura, 10-11, 82-92
standaryzacja, 8-10, 76-82,
287-8
- Zatwierdzone przez NFC Forum typy tagów, 101-2 Typ 1, 101
Typ 2, 101
Typ 3, 101
Typ 4, 101-2
- Typ rekordu NFC Forum, 103-8 typ zewnętrzny, 104-5
typ globalny, 104
typ lokalny, 104
dobrze znany typ, 103-4, 105-8
- NFC Forum dobrze znany typ, 103-4, 105-8
podpis, 107-8
inteligentny
plakat, 107 tekst,
108
URI, 105
- Forum NFC, 9, 76-9
- Przypadek plotkowania NFC, 141-2, 215-23 projekt, 141-2
programowanie, 215-23
- Interfejs NFC, 10-11, 82, 86
- Telefony komórkowe z obsługą NFC, *patrz* Telefony komórkowe z obsługą NFC
- Tryby pracy NFC, 11-12, 128-35
emulacja karty, 12, 14, 131-5
peer-to-peer, 12, 14, 128-31
reader/writer, 12-13, 119-28
- Programowanie NFC, *patrz* Tworzenie aplikacji NFC
- Rejestr push NFC, 199-200
- Czytnik NFC, 8, 75
- Bezpieczeństwo NFC, 22-4, 265-77 system backend, 23-4, 272 komunikacja, 23, 270-272 framework, 265
czytelnicy, 23, 268
karta inteligentna, 23, 269-70
tagi, 22, 266-8
- Etui na zakupy NFC, 137-40, 215-23
projekt, 137-40
programowanie, 215-23
- Znacznik NFC, 8, 75
- Projekt etui na bilety NFC, 142-5
ekosystem, 301-4
Testy NFC, *zob.*
testy
- Interfejs przewodowy NFC (NFC-WI), 10-11, 82,
87
- Program NFCGossiping, 223-36 Usługi i protokół bezpieczeństwa NFCIP-1 (NFC-SEC), 24, 273-6
architektura, 274
protokół, 274
- NFCIP-1, *patrz* Interfejs i protokół komunikacji bliskiego zasięgu-1
- NFCIP-2, *patrz* Interfejs i protokół komunikacji bliskiego zasięgu-2
- Interfejs NFCIPConnection, 201 Interfejs NFCIPConnection, 201 Program NFCReadWriteMIDlet, 185-98
Architektura NFC-SEC, 274
Standard kryptograficzny NFC-SEC (NFC-SEC-01), 24, 276-7
- Protokół NFC-SEC, 274
- NFC-SEC, *zob.* usługi i protokół bezpieczeństwa NFCIP-1 (NFC-SEC)
- NFC-SEC-01, *patrz* standard kryptograficzny NFC-SEC
- NFC-WI, *patrz* interfejs przewodowy NFC, komunikacja nomadyczna, 48
niezaprzecjalność, 20, 246-7
- Portfel O2, 35, 346-7
- OMA, *patrz* Open Mobile Alliance jednowymiarowy kod kreskowy, 5, 51
Open Mobile Alliance (OMA), 10, 81
OPEN, 314-15
pakiety opcjonalne, JSR 177, 212-15 SATSA-APDU, 213-14
SATSA-CRYPTO, 214-15
SATSA-JCRMI, 214
SATSA-PKI, 214
Wdrożenie OTA, 316-24
- Bramka OTA, 312
- Dostawca OTA, *patrz* dostawca over-the-air
Technologia OTA, *patrz* technologia over-the-air
dostawca usług over-the-air (dostawca OTA), 29-30, 297

- technologia over-the-air (technologia OTA), 15, 311-13
menedżer kart, 316
brama, 312
dostawca, 297, 311-12
- Program P2PExample, 204-11
możliwość parowania, 70
pasywny tryb komunikacji, 8, 73-4, 118
urządzenie pasywne, 8, 73-4, 118
Projekt Pay-Buy-Mobile, 304-8
Projekt Payez Mobile, 35, 342-3
PCD, *zob.* urządzenie zbliżeniowe w trybie peer-to-peer, *zob.* peer-to-peer
 tryb pracy
programowanie trybu peer-to-peer, 200-211
tryb pracy peer-to-peer, 12-13,
 108-11, 128-31, 200-211
 korzyści z zastosowania, 131
 zastosowania, 129-30
 ogólny model użytkowania, 129
 programowanie, 200-211
 architektura stosu protokołów, 108-9
farmacja, 251-2
phishing, 250
fałszowanie połączeń telefonicznych, 267
PICC, *patrz* platforma deweloperska kart z układem scalonym zbliżeniowym, 319
zarządzanie platformą, *patrz* bezpieczne zarządzanie elementami, zarządzanie zawartością karty
menedżer platformy, 29, 295-7
właściciel platformy, 319
paradygmat wskazywania, 116-17
prywatność, 24-5, 277-81
 anonimowość, 278
 pseudonimowość, 278
 niepołączalność, 278
 nieobserwowałość, 278
mechanizmy ochrony prywatności, 280-281
klucz prywatny, 264, 259
program
 Hello, 165-8
 NFCGossiping, 223-36
 NFCReadWriteMIDlet, 185-98
- Przykład P2PE, 204-11
ShoppingMain, 215-23
UIMIDlet, 171-7
multipleksowanie protokołów, LLCP, 110
zbliżeniowe karty inteligentne, 6-7, 66,
 92-4
 Calypso, 7, 94
 FeliCa, 7, 94, 98
 MIFARE, 7, 94, 97-8
 Typ A, 94, 97-8 Typ B, 94, 97-8
zbliżeniowe urządzenie sprzągające (PCD), 93 karty intelligentne ze sprzężeniem zbliżeniowym, *zob.*
 zbliżeniowe bezstykowe karty inteligentne
 zbliżeniowa karta z układem scalonym (PICC), 93 pseudonimowość, 278
 klucz publiczny, 264, 259
 kryptografia klucza publicznego, *zob.*
 kryptografia asymetryczna
 szyfrowanie klucza publicznego, 259-61 rejestr push, 177-8
 rejestracja dynamiczna, 178
 LLCP Push Registry, 203-4
 NFC Push Registry, 199-200
 rejestracja statyczna, 177-8
 rejestr wypychania, LLCP, *patrz* rejestr wypychania LLCP rejestr wypychania, NFC, *patrz* rejestr wypychania NFC klasa PushRegistry, 177-8
- Kod kreskowy QR, *patrz* kod kreskowy szybkiego reagowania Kod kreskowy szybkiego reagowania (QR), 5, 52
- identyfikacja radiowa (RFID), 5-6, 50-58
 zastosowanie, 58
 sprzężenie zwrotne, 57
 modulacja rozproszenia wstecznego, 57
 element sprzągający, 53-4
 łącznik kierunkowy, 57
 transmisja dalekiego pola, 57-8
 zakresy częstotliwości, 55
 sprzężenie indukcyjne, 55-7
 modulacja obciążenia, 55-7
 transmisja bliskiego pola, 57-8
 czytnik, 5, 55
 tag, 5, 54-5, 67-8

- transceiver, 53-5
 - transponder, 53-5
 - producenci czytników, 290
 - tryb pracy czytnika/zapisu, 12-13, 99-108, 119-28, 179-200
 - korzyści z zastosowania, 127-8
 - zastosowania, 123-5
 - ogólny model użytkowania, 121-2
 - programowanie, 179-200
 - architektura stosu protokołów, 100-101
 - tryb czytnika/zapisu, *zob.* tryb czytnika/zapisu
 - tryb pracy
 - programowanie trybu czytnika/zapisu, 179-200
 - definicja typu zapisu (RTD), 78-9, 105-8
 - atak przekaźnika, 23, 251, 271
 - atak powtórkowy, 23, 251, 271
 - sprzedawcy detaliczni, *zob.* kupcy
 - RFID, *patrz* identyfikacja radiowa
 - Zastosowanie RFID, 5-6, 58
 - Sprzężenie zwrotne RFID, 57
 - Modulacja rozproszenia wstecznego RFID, 57
 - Element sprzągający RFID, 53-4
 - Zakresy częstotliwości RFID, 55
 - Sprzężenie indukcyjne RFID, 55-7
 - Modulacja obciążenia RFID, 55-7
 - Czytnik RFID, 5, 55
 - Znacznik RFID, 5, 54-5, 67-8
 - Technologia RFID, *patrz* identyfikacja radiowa
 - Nadajnik-odbiornik RFID, 53-5
 - Transponder RFID, 53-5
 - ryzyko, 21, 252-3
 - Rivest, Shamir i Adleman (RSA), 260
 - RSA, *patrz* Rivest, Shamir i Adleman
 - RTD, *patrz* definicja typu rekordu
 - RTE, *patrz* środowisko uruchomieniowe środowiska uruchomieniowe (RTE), 314-15
-
- SATSA API, *patrz* JSR
 - 177 SATSA-APDU, 213-14
 - SATSA-CRYPTO, 214-15
 - SATSA-JCRMI, 214
 - SATSA-PKI, 214
 - paradygmat skanowania, 117
 - SCOS (system operacyjny kart intelligentnych) SCP (protokół bezpiecznego kanału)

Instalacja SDK, *patrz* instalacja Eclipse SE, *patrz* bezpieczny element Emitent SE, *zob.* emitent bezpiecznego elementu Zarządzanie SE, *zob.* bezpieczny element tajemnica zarządzania, 20, 243 kryptografia z kluczem tajnym, *zob.* kryptografia symetryczna bezpieczny kanał, 265 protokół bezpiecznego kanału (SCP), 317-18 wystawca bezpiecznych elementów (SE issuer), 29, 295 zarządzanie bezpiecznymi elementami (SE zarządzanie), 311-29 producenci bezpiecznych elementów, 288-90 bezpieczny element (SE), 14, 83-6 sprzęt wbudowany, 14, 85 wiele bezpiecznych elementów, 16-17, 325-6 zabezpieczona karta pamięci, 14, 85 uniwersalna karta z układem scalonym, 14, 85 protokół bezpiecznej wymiany (SEP), 274 domena bezpieczeństwa, karta inteligentna, 15, 315, 320 dostawca aplikacji, 315, 320 organ kontrolny, 15, 315, 320 emitent, 15, 315, 320 uzupełniający, 15, 315, 320 środki bezpieczeństwa, 243-248 odpowiedzialność, 21, 248 uwierzytelnianie, 20, 243-6 autoryzacja, 20, 246 dostępność, 20, 248 poufność, 243 integralność danych, 21, 248 wzajemne uwierzytelnianie, 246 niezaprzeczalność, 20, 246-7

tajemnica, 20, 243 secure memory card (SMC), 14, 85 secure sockets layer (SSL), 317-18 Security and Trust Services API, *patrz* JSR 177 polityka bezpieczeństwa, 264 SEP, *zob.* dostawcy usług protokołu bezpiecznej wymiany, 292-3 Program ShoppingMain, 215-23 atak kanałem bocznym, 269 SIM, *patrz* moduł identyfikacji abonenta tryb prosty, 16, 320-322 tryb prosty APSD (SM APSD), 320-322

- protokół jednoprzewodowy (SWP), 10-11, 82, 87-9
SM APSD, *patrz* tryb prosty karty inteligentnej APSD, 6-7, 58-7
 aplikacje, 67
 zblíženiowe karty inteligentne, 6, 66
 stykowe karty inteligentne, 6, 63-5
 bezstykowe karty inteligentne, 6-7, 65-8
 karty inteligentne z podwójnym interfejsem, 67
 hybrydowe karty inteligentne, 67
 karty z paskiem magnetycznym, 6, 59-60
 karty inteligentne z pamięcią, 60-61
 karty inteligentne z mikroprocesorem, 61
 system operacyjny, 61-3
 zblíženiowe karty inteligentne, 6-7, 66, 92-4
 karty inteligentne ze sprzężeniem zblíženiowym, 6-7, 66, 92-4
 karty inteligentne ze sprzężeniem sąsiedzkim, 6, 66
 Smart Card Alliance, 289
aplikacje kart inteligentnych, 67
zarządzanie zawartością kart
 inteligentnych, *patrz* zarządzanie zawartością kart
Wydawca kart inteligentnych, *patrz* wydawca kart inteligentnych
Producent kart inteligentnych, *patrz* producent kart inteligentnych
 producent
system operacyjny kart inteligentnych (SCOS), 61-3
inteligentny plakat, 107, 120-121
Smart Urban Spaces, 34, 339-41
SMC, *patrz* bezpieczna karta pamięci SMS spoofing, 252, 267-8
sniffing, *patrz* podsłuchiwanie inżynieria społeczna, 250
spoofing, *patrz* ataki spoofingowe ataki spoofingowe, 22, 252, 267-8
 fałszowanie wiadomości e-mail, 252
 Podsywając się pod adres IP, 252
 fałszowanie połączeń telefonicznych, 267
 SMS spoofing, 252, 267-8
 URI spoofing, 267
 Podsywając się pod adresy URL, 252, 267
SSD, *patrz* dodatkowa domena zabezpieczeń Menedżer SSD, *patrz* dodatkowe zabezpieczenia menedżer domeny SSL, *patrz* bezpieczna warstwa gniazd

- interesariusze, ekosystem NFC, 27-8, 286-93
klienci, 293
kupcy/detaliści, 293
producenci telefonów komórkowych, 290
operator sieci komórkowej, 290
Producenci zestawów chipów NFC, 288
producenci czytników, 290
producenci bezpiecznych elementów, 288-90
dostawcy usług, 292-3
organy normalizacyjne, 8-10, 76-82, 287-288
zaufany menedżer usług, 16, 290-292
organy normalizacyjne, 8-10, 76-82, 287-8
Stolpan, 289
moduł tożsamości abonenta (SIM), 14, 85
dodatkowa domena bezpieczeństwa (SSD), 15,
315, 320
menedżer dodatkowej domeny
zabezpieczeń (menedżer SSD), 315, 319
SWP, *zob.* protokół
jednoprzewodowy
kryptografii
symetrycznej, 258-9
zaawansowany standard
szyfrowania, 259 standard
szyfrowania danych, 258
potrójny DES, 258
klucz symetryczny, 263
- klonowanie znaczników, 22, 267
ukrywanie znaczników, 22, 268
podsywanie się pod tag, 267
zastępowanie tagów, 22,
268 interfejs
TagConnection, 182
target, 8, 74, 119
interfejs TargetListener,
182 interfejs
TargetProperties, 182
- klasa TargetType, 181-2
zagrożenie, 21, 249
TLS, *patrz* bezpieczeństwo
warstwy transportowej TNF, *patrz*
format nazwy typu paradygmat
dotykania, 116
kryptografia tradycyjna, *zob.* kryptografia
symetryczna
Interfejs TransactionListener, 212, 237
zabezpieczenia warstwy transportowej
(TLS), 317-18 próby, 34-5, 341-9
potrójny DES (3DES), 258
zaufany menedżer usług (TSM), 16, 290-292

- zaufana strona trzecia, *patrz* zaufany menedżer usług
- TSD, *zob.* domena bezpieczeństwa
- TSM TSM, *zob.* zaufany menedżer usług TSM centryczny model biznesowy, 299 TSM domena bezpieczeństwa (TSD), 323 TTP, *zob.* zaufany menedżer usług dwuwymiarowy kod kreskowy, 5, 51-2 Type Name Format (TNF), 103, 105
- wszechobecne komputery, 2-3, 41-3
- UICC, *patrz* uniwersalna karta układu scalonego Modele zarządzania UICC, 16, 320-324
- tryb autoryzowany TSD, 16, 323-4
 - TSD w trybie delegowanym, 16, 322-3
 - tryb prosty APSD, 16, 320-322
- Program UIMIDlet, 171-7
- UMTS, *patrz* uniwersalny telefon komórkowy
- system telekomunikacyjny
 - uniwersalna karta z układem scalonym (UICC), 14, 85
- uniwersalny system telefonii komórkowej (UMTS), 48-9
- uniwersalny kod produktu (UPC), 5, 52
- uniwersalny moduł identyfikacji abonenta (USIM), 14, 85
- niepołączalność, 278
- nieobserwowność, 278
- UPC, *patrz* uniwersalny kod produktu
- Kod kreskowy UPC-A, 52
- URI spoofing, 267
- URL spoofing, 252, 267
- użyteczność, 30-31
- USIM, *patrz* uniwersalny moduł identyfikacji abonenta
- karty inteligentne ze sprzężeniem sąsiedzkim, 6, 66 maszyna wirtualna, 315
- VM, *zob.* luka w zabezpieczeniach maszyny wirtualnej, 21, 248-9
- WEP, *patrz* równoważna prywatność sieci przewodowej Wi-Fi, 49
- Dostęp chroniony Wi-Fi (WPA), 264 Wi-Max, 49-50
- komunikacja przewodowa, 44
- WEP, 264 komunikacja bezprzewodowa, 4, 44, 47-50 bezprzewodowa sieć lokalna (WLAN), 49 bezprzewodowa sieć osobista (WPAN), 49
- bezprzewodowa sieć rozległa (WWAN), 50
- WLAN, *patrz* bezprzewodowa sieć lokalna
- WPA, *patrz* dostęp chroniony Wi-Fi
- WPAN, *zob.* bezprzewodowa sieć osobista
- WWAN, *zob.* bezprzewodowa sieć rozległa
- ZigBee, 50