ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

Martin Hanton

PŘÍSTUP DO ODBAVOVACÍCH SYSTÉMŮ V DOPRAVĚ S VYUŽITÍM NFC

Diplomová práce

2015

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní
d ě k a n
Konviktská 20, 110 00 Praha 1

K614 ..... Ústav aplikované informatiky v dopravě

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Bc. Martin Hanton

Kód studijního programu a studijní obor studenta:

N 3710 – ID – Inženýrská informatika v dopravě a spojích

Název tématu (česky): **Přístup do odbavovacích systémů v dopravě s využitím NFC**

Název tématu (anglicky): Use of Near Field Communication (NFC) in Fare control systems

Zásady pro vypracování

Při zpracování diplomové práce se řiďte osnovou uvedenou v následujících bodech:

- Popište a zhodnoťte technologie NFC, možnosti využití při odbavování zboží a osob.
- Zpracujte teoretický základ pro zajištění bezprčnosti v NFC systémech.
- Připravte implementaci NFC s ohledem na jeho vlastní technologická omezení. popřípadě navrhněte řešení s využitím dalších bezdrátových technologií.
- Realizujte odbavení vozidel při vstupech do areálů na základě navrženého technického řešení pro zajištění obslužnosti parkování.

Rozsah grafických prací: dle charakteru diplomové práce

Rozsah průvodní zprávy: minimálně 55 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury: Gallo, F. NFC Tags A technical introduction, applications and products [online], Rev. 1.3, 1 December 2011. Dostupné z URL: http://www.nxp.com/documents/other/R_10014.pdf

Vedoucí diplomové práce: **Ing. Marek Kalika, Ph.D.**

Datum zadání diplomové práce: **30. června 2014**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání diplomové práce: **31. května 2015**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

L. S.

doc. Dr. Ing. Tomáš Brandejský
vedoucí
Ústavu aplikované informatiky v dopravě

prof. Dr. Ing. Miroslav Svítek
děkan fakulty

Potvrzuji převzetí zadání diplomové práce.

Bc. Martin Hanton
jméno a podpis studenta

V Praze dne..... 30. června 2014

Abstrakt

Autor:	Martin Hanton
Název diplomové práce:	Přístup do odbavovacích systémů v dopravě s využitím NFC
Škola:	České vysoké učení technické v Praze
Fakulta:	Fakulta dopravní
Ústav:	Ústav aplikované informatiky v dopravě (K614)
Vedoucí bakalářské práce:	Ing. Marek Kalika, Ph.D.
Rozsah práce:	70 stran

Praha, květen 2015

Diplomová práce analyzuje možnosti využití technologie NFC v odbavovacích systémech a reaguje na jeho nedostatky kombinací NFC s dalšími technologiemi umožňujícími bezdrátovou komunikaci na delší vzdálenost. Na základě teoretického rozboru NFC a dalších technologií je v práci navržen přístupový systém, který bude realizován v místě vjezdu do podzemních garáží Nové budovy ČVUT v Dejvicích.

Klíčová slova

Near Field Communication (NFC), Bluetooth Low Energy (BLE), MIFARE DESFire EV1, přístupový systém

Abstract

Author:	Martin Hanton
Title of thesis:	Use of Near Field Communication (NFC) in Fare Control Systems
School:	Czech technical university in Prague
Faculty:	Faculty of transportation sciences
Department:	Institute of Applied Informatics in Transport (K614)
Thesis advisor:	Ing. Marek Kalika, Ph.D.
Pages:	70

Prague, May 2015

The diploma thesis analyzes the possibilities of NFC technology in fare control systems and responds to its shortcomings by combining NFC with other technologies enabling wireless communication over longer distances. Based on the theoretical analysis of NFC and other technologies, the thesis proposes access system that will be implemented at the entrance to the underground garage of the New building of CTU in Dejvice.

Keywords

Near Field Communication (NFC), Bluetooth Low Energy (BLE), MIFARE DESFire EV1, fare control system

Poděkování

Na tomto místě bych chtěl poděkovat všem, jejichž rady a připomínky se podílely na výsledné podobě této práce, zejména pak vedoucímu diplomové práce, Ing. Marku Kalikovi, Ph.D, za poskytnuté informace a konzultace v průběhu jejího zpracovávání.

Prohlášení

Já, Martin Hanton, student Fakulty dopravní ČVUT v Praze prohlašuji, že jsem svou diplomovou práci vypracoval samostatně a veškeré materiály, z nichž jsem čerpal pro svoji práci, jsou uvedeny v seznamu použitých zdrojů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne: …… Podpis: ..……

Obsah

Seznam použitých zkratek

3DES	Triple DES (viz DES)
ABS	Akrylonitrilbutadienstyren
AES	Advanced Encryption Standard
AFH	Adaptive Frequency Hopping
API	Application Programming Interface
APL	Application Layer
APS	Application Sublayer
ASCII	American Standard Code For Information Interchange
ASK	Amplitude Shift Keying
ATT	Attribute Protocol
AVCTP	Audio/Video Control Transport Protocol
AVDTP	Audio/Video Distribution Transport Protocol
BLE	Bluetooth Low Energy
BPSK	Binary Phase-Shift Keying
BT	Bluetooth
CA	Collision Avodiance
CF	Chunk Flag
CRC	Cyclic Redundancy Check
CSMA	Carrier Sense Multiple Access
DES	Data Encryption Standard
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
ECMA	European Computer Manufacturers Association
EDR	Enhanced Data Rate
EEPROM	Electrically Erasable Programmable Read-Only Memory
ETSI	European Telecommunications Standards Institute
FFD	Full Functional Device
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standard
GF	Galoisovo těleso, konečné těleso

GFSK	Gaussian Frequency Shift Keying
HCI	Host Controller Interface
HS	High Speed
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Initial Permutation, Internet Protocol
ISM	Industrial, Scientific, & Medical (radiofrekvenční pásmo)
ISO	International Standards Organization
KM	kódování Manchester
KS	Key Schedule
L2CAP	Logical Link Control and Adaptation
LAN	Local Area Network
LED	Light Emitting Diode
LMP	Link Management Protocol
LTE	Long Term Evolution (mobilní sítě 4. generace)
MAC	Media Access Control
MB	Message Begin
ME	Message End
MIME	Multipurpose Internet Mail Extensions
MLDP	Microchip's Low-energy Data Profile
MMK	modifikované Millerovo kódování
NDEF	NFC Data Exchange Protocol
NFC	Near Field Communication
NFCIP	Near Field Communication Interface and Protocol
NIST	National Institute of Standards and Technology
NWK	Network Layer
OBEX	Object Exchange Protocol
OSI	Open Systems Interconnection
P2P	Peer to Peer

PAN	Personal Area Network
PCD	Proximity Coupling Device
PDU	Protocol Data Unit
PHY	Physical Layer
PICC	Proximity Integrated Circuit Card
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PVC	Polyvinylchlorid
QPSK	Offset Quadrature Phase Shift Keying
RAM	Random Access Memory
RF	Radio Frequency
RFCOMM	Radio Frequency Communication
RFD	Reduced Functionality Device
RFID	Radio Frequency Identification
ROM	Read-Only Memory
SDP	Session Description Protocol
SE	Secure Element
SIG	Special Interest Group
SIM	Subscriber Identity Module
SMS	Short Message Service
SQL	Structured Query Language
SR	Short Record
TCP	Transmission Control Protocol
TNF	Type Name Format
UDP	User Datagram Protocol
UICC	Universal Integrated Circuit Card
UID	Unique Identifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VCD	Vicinity coupling device
ZDO	ZigBee Device Object

Úvod

Žijeme v době, která se vyznačuje nebývalou mobilitou. Objemy přepravovaných osob, věcí a informací neustále rostou. Tento růst je na jedné straně stimulem pro rozvoj společnosti, na straně druhé však vyvstává potřeba vymýšlet stále dokonalejší systémy, které by byly schopné rostoucí objemy přepravy odbavit. Platí zde jednoduché pravidlo – čím větší jsou zmíněné objemy, tím rychlejší a efektivnější musí být odbavovací proces. Naštěstí disponujeme moderními technologiemi, které nám s tímto náročným úkolem dokážou výrazně pomoci.

Využití informačních a komunikačních technologií pro řešení těchto problémů je součástí širšího konceptu označovaného souhrnným pojmem smart city. Jeho cílem je zefektivnění a zkvalitnění městských služeb za současného snížení nákladů a spotřeby vzácných zdrojů. Mezi odvětví řešená v rámci tohoto konceptu patří elektronizace státní správy, hospodaření s energií, vodou a odpady, zdravotnické služby a v neposlední řadě také řízení dopravy a logistiky. Sem spadá např. odbavování cestujících v hromadné dopravě nebo kontrola přístupu do zabezpečených areálů.

Společným jmenovatelem spojujícím vyjmenované aktivity na poli dopravy je elektronická identifikace. Její zavádění ve stále větším měřítku je dáno vzrůstajícími požadavky na zabezpečení přístupu do objektů, ať už se jedná o kancelářské budovy, vzdělávací instituce, sídla nejrůznějších úřadů nebo podzemní garáže. Zároveň je její implementace s postupujícím vývojem technologií stále jednodušší a nezřídka bývají elektronické identifikační systémy napojovány na další aplikace – například na evidenci docházky nebo zpoplatněné parkování. Rozvoj technologií je obzvláště patrný v oblasti mobilních telefonů. Současné přístroje disponující výpočetním výkonem, který byl ještě před několika desetiletími realizovatelný pouze ve špičkových superpočítačích, jsou ve spojení se stále rostoucí konektivitou velice mocným nástrojem. Není tedy divu, že se poslední dobou objevují identifikační systémy, ve kterých hrají mobilní telefony relativně velkou roli.

Implementace mobilních technologií do odbavovacího systému na bázi elektronické identifikace je rovněž tématem této diplomové práce. Konkrétně se jedná o návrh přístupového systému pro řidiče motorových vozidel (vjezd do podzemních garáží, do areálu firmy a podobně) s využitím NFC. Ne vždy je ale možné čtečky přístupových karet umístit do vhodných míst – tedy tam, odkud jsou uživatelům dobře dostupné. Nevhodné umístění čteček může být vynuceno např. stavební konstrukcí osazované budovy, v případě logistických nebo firemních areálů čtečka může být dobře dostupná pro řidiče osobních vozidel, ale pro řidiče nákladních vozidel je v nevhodné výšce. Přímému kontaktu přístupové karty a čtečky je vhodné se vyhnout také v místech, kde není žádoucí kontakt s vnějším prostředím – např.

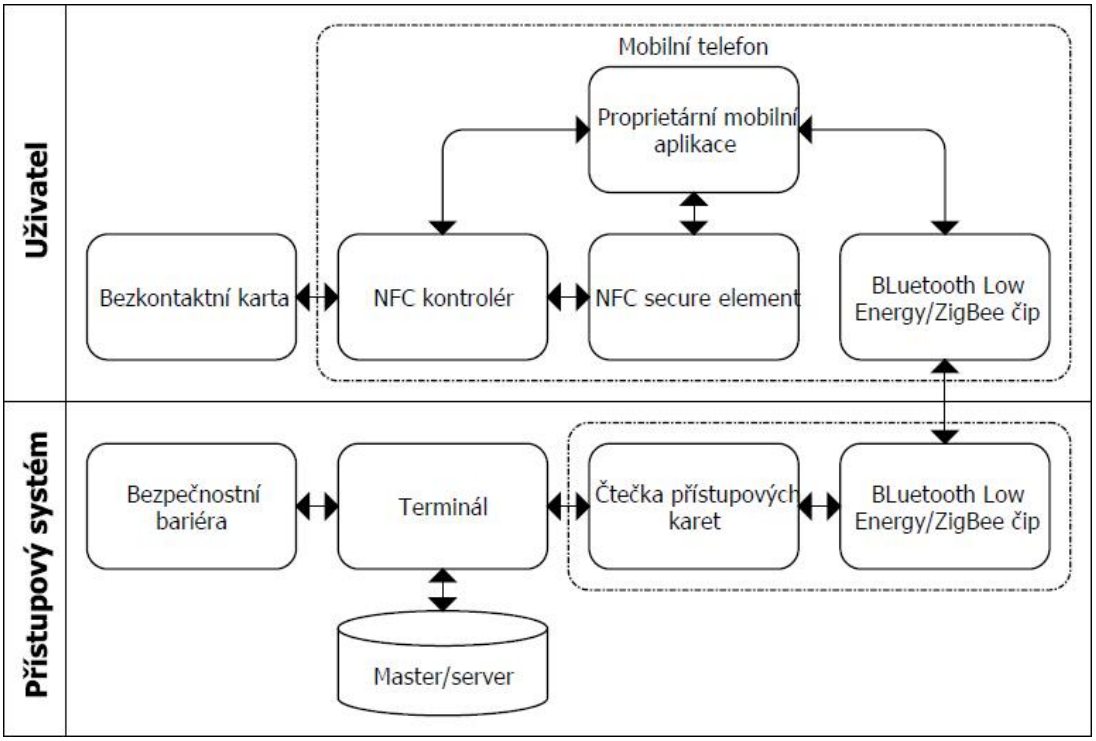
z důvodu nadměrného hluku, znečištění nebo nevhodných klimatických podmínek. Pro efektivní používání přístupového systému je proto nutné zajistit jejich dostupnost kombinací NFC s dalšími vhodnými technologiemi.

Technické řešení míst, kde jsou čtečky přístupových karet špatně dostupné z místa řidiče, je hlavní cílem této diplomové práce. Uvedený problém je zde řešen spojením mobilního telefonu a čtečky přístupových karet prostřednictvím bezdrátové komunikace, která eliminuje nutnost bezprostředního kontaktu se čtečkou. Teoretická část diplomové práce vychází z popisu užívaných technologií po hardwarové stránce – od přístupových karet a kryptografických metod přes NFC, bezdrátové technologie a jejich srovnání až po čtečku karet a návazný systém. Praktická část sestává ze dvou hlavních částí. První z nich se zabývá popisem komunikace v přístupovém systému tak, jak probíhá při používání v praxi, tj. od výměny dat mezi kartou a telefonem, popisu mobilní aplikace, která slouží jako rozhraní mezi NFC a bezdrátovou technologií, až po samotný bezdrátový přenos a komunikaci mezi čtečkou a serverem, který obsahuje informace o přístupových právech. Druhá část pojednává o nasazení navrhovaného přístupového systému v pilotním provozu. Ten bude realizován v místě vjezdu do podzemních garáží nové budovy ČVUT v dejvickém kampusu, kde je umístění čteček ovládajících bezpečnostní roletu vyřešeno nevyhovujícím způsobem. Testování a nasazení systému do ostrého provozu bude probíhat v průběhu letních prázdnin, kdy lze s výhodou využít snížené frekvence provozu v garážích.

1 Popis navrhovaného systému

Navrhovaný přístupový systém je primárně určen pro ovládání vjezdových zábran (závor, rolet apod.) z interiéru vozidla – odpadá tak přímý kontakt přístupové karty a čtečky, která je mnohdy umístěna ve větší vzdálenosti od vjezdu. Blokové schéma navrhovaného přístupového systému je na obrázku č. 1.

Prostřednictvím mobilního telefonu s NFC čipem dojde k načtení unikátního identifikačního čísla (ID) z přístupové karty (např. MIFARE DESFire EV1 4k s podporou 128bitového šifrování AES). Následně dojde k navázání zabezpečeného spojení mezi telefonem a čtečkou přístupových karet, která je vybavena speciálním modulem pro bezdrátovou komunikaci na vzdálenost v řádu jednotek až desítek metrů. ID načtené z přístupové karty telefon odešle do čtečky, přičemž vzájemnou komunikaci mezi NFC a návaznou bezdrátovou technologií zajistí navržená mobilní aplikace.



Obr. 1: Blokové schéma navrhovaného přístupového systému (zdroj: autor)

Zvolená bezdrátová technologie musí splňovat požadavky na nízkou energetickou náročnost, dostupnost technologického řešení a v neposlední řadě také na finanční únosnost. Z těchto důvodů pro bezdrátový modul přichází v úvahu technologie ZigBee, nebo Bluetooth Low Energy. V následujících kapitolách jsou obě technologie podrobně popsány a vzájemně porovnány.

Čtečka odešle přijaté ID do nadřízeného terminálu. V případě, že terminál vyhodnotí oprávněnost přijatého ID ke vstupu do dalších prostor, vyšle povel k otevření konkrétní bezpečnostní bariéry. Přístupový systém umožňuje vytvoření návaznosti na další systémy, jako je např. systém kontroly docházky, placené parkování apod.

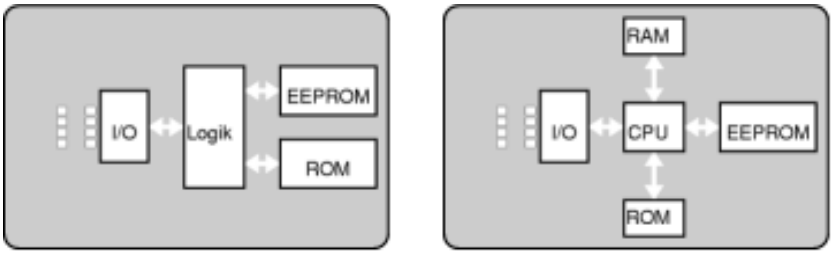
2 Čipová karta

Čipové karty jsou zpravidla plastové karty (PVC nebo ABS) obsahující integrovaný obvod, který je schopen zpracovávat data, tj. přijímat příkazy, zpracovávat je a odesílat adekvátní odpovědi. Rozměry čipových karet definuje standard ISO 7816: [1]

- **ID-1** - 85,60 mm × 53,98 mm. Nejrozšířenější formát čipových karet používaný pro široké spektrum aplikací – bankovní karty, identifikační karty (občanské a řidičské průkazy), přístupové karty aj.
- **ID-00** - 66 mm x 33 mm. Formát střední velikosti, který v praxi velké využití nenašel.
- **ID-000** - 25 mm × 15 mm. Nejmenší velikost používaná zejména pro SIM karty.

Integrované obvody v čipových kartách lze rozdělit na dva typy – paměťové čipy a mikroprocesory. Konstrukčně jednodušší karty s paměťovým čipem se využívají pro zápis a čtení informací (např. telefonní karty). K jednotlivým buňkám paměťového média se přistupuje přímo skrze rozhraní. Uložené informace je možné zabezpečit PIN kódem nebo heslem.

Naproti tomu u mikroprocesorových karet je možné k uloženým datům přistupovat pouze přes integrovaný mikroprocesor. Ten umožňuje data chránit prostřednictvím kryptografických metod, které lze využít pro implementaci služeb, jako je autentizace, šifrování, digitální podepisování apod. Kromě symetrických (DES, AES) a asymetrických (RSA) šifrovacích metod lze využít veřejného šifrovacího klíče (PKI) a hardwarových generátorů náhodných čísel. Schéma struktury obou typů karet je na obrázku č. 2.

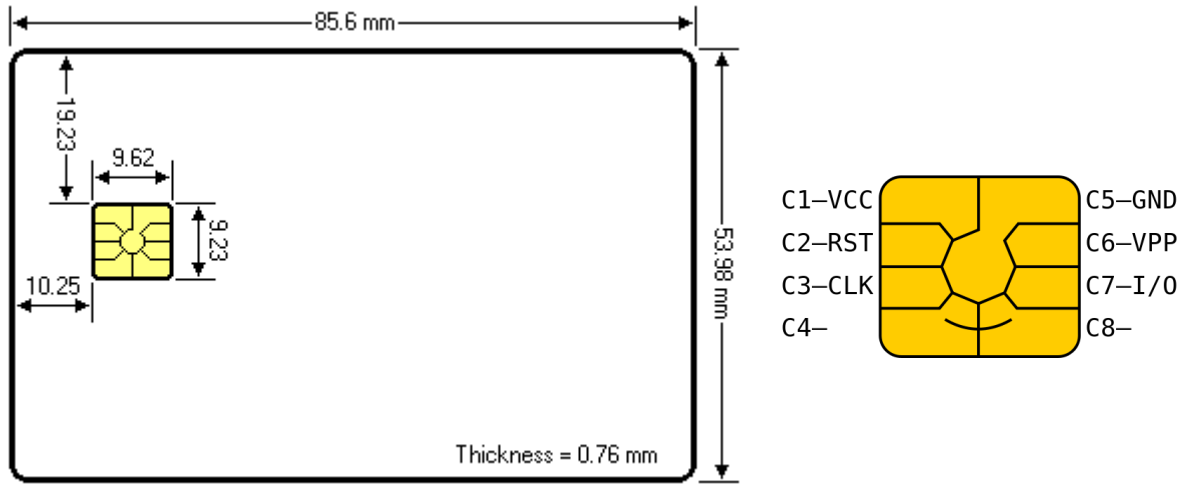


Obr. 2: Struktura čipové karty s paměťovým čipem (vlevo) a s mikroprocesorem (zdroj: [2] [3])

Blok I/O je vstupně-výstupní rozhraní čipové karty. V případě paměťových karet řídí přístup k paměťovým modulům EEPROM a ROM logický modul, v kartách s mikroprocesorem samotný mikroprocesor (např. osmibitový čip s frekvencí 5 MHz). EEPROM je ekvivalentem pevného disku v PC, ukládají se zde data aplikací a šifrovací klíče. Paměť ROM, ve které jsou kromě operačního systému uloženy také komunikační protokoly, je nepřepisovatelná – její obsah je pevně dán výrobním procesem. RAM je operační paměť, která po přerušení napájení ztrácí veškerý uložený obsah. [4]

2.1 Kontaktní a bezkontaktní čipové karty

V současné době se v praxi používají kontaktní i bezkontaktní čipové karty. Kontaktní karty mají na svém povrchu kontaktní plochu s vodivým povrchem (cca 1 cm^2), která zajišťuje komunikaci se čtečkou a napájení čipu – kartu je tedy nutné do čtečky vložit. Umístění čipu na kartě a popis jednotlivých pinů je na obrázku č. 3. Bezkontaktní karty jsou vybaveny radiovým rozhraním pracujícím na principu elektromagnetické indukce. Čtečka generuje elektromagnetické pole, které napájí čip na kartě a umožňuje vzájemnou komunikaci.



Obrázek 3: Umístění čipu na čipové kartě (vlevo), popis jednotlivých pinů čipu (C1 – napájení, C2 – reset, C3 – hodinový signál, C5 – uzemnění, C6 – programování paměti EEPROM, C7 – sériová komunikace, C4 a C8 - rezerva) (zdroj: [5] [6])

Vzhledem k tomu, že součástí navrhovaného přístupového systému je již používaná infrastruktura založená na bezkontaktních čipových kartách, budu se nadále zabývat pouze jejich bezkontaktními variantami.

2.2 Bezkontaktní čipové karty

Existuje několik typů bezkontaktních karet, které se liší podle velikosti paměti, používané frekvence, úrovně zabezpečení atd. Největší rozdíl je ale v použité technologii – typ A je založen na čipech od NXP (Philips), typ B používá čipy všech ostatních výrobců a typ C spoléhá výhradně na technologii společnosti Sony.

2.2.1 MIFARE DESFire EV1

Jak již bylo zmíněno výše, navrhovaný přístupový systém využívá technologie bezkontaktních čipových karet. Konkrétně se jedná o typ A – MIFARE DESFire EV1 s 8 kB pamětí a s podporou šifrování 128-bitového šifrování AES. Tento typ byl představen v roce 2006 a jeho výhodou je široká zpětná kompatibilita. V rámci České republiky jej implementovaly např. České dráhy pod obchodním názvem In-karta nebo pražský magistrát ve formě multiaplikační karty Opencard. Tento typ je využíván rovněž v univerzitním prostředí, mj. jako přístupová a identifikační karta také na ČVUT (viz obrázek č. 4). [7]

Obr. 4: Identifikační karta ČVUT (zdroj: [8])

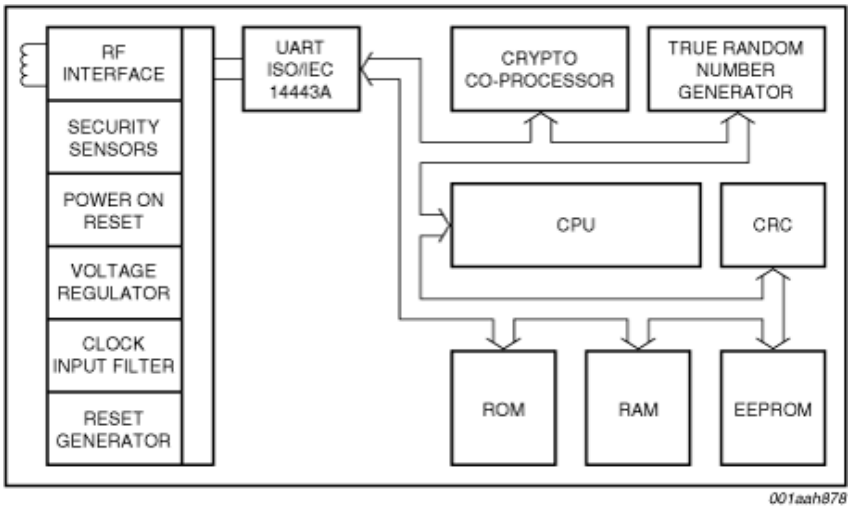
Řada čipových karet MIFARE od společnosti NXP vychází ze standardu ISO/IEC 14443. Vlastnosti typu MIFARE DESFire EV1 jsou uvedeny v tabulce č. 1. [7]

Tab. 1: Vlastnosti bezkontaktní čipové karty typu MIFARE DESFire EV1

Parametr	**Hodnota**
Maximální vzdálenost od čtečky	Až 10 cm
Frekvence	13,56 MHz
Přenosová rychlost	106, 212, 424, 848 kbps
Velikost paměti EEPROM	2, 4, 8 kB
Počet zapisovacích cyklů paměti EEPROM	500 000
Počet aplikací	až 28

Počet souborů v 1 aplikaci	až 32
Velikost UID	7 B
Podpora HW šifrování	DES, 3DES, AES

Kromě kryptografických metod uvedených v tabulce č. 1 podporuje MIFARE DESFire EV1 generování náhodných ID, šifrování dat přímo na radiofrekvenčním kanálu a autentizaci v rámci jednotlivých aplikací. Na obrázku č. 5 je blokové schéma bezkontaktní čipové karty tohoto typu.



Obr. 5: Blokové schéma struktury bezkontaktní čipové karty typu MIFARE DESFire EV1 (zdroj: [7])

2.3 Blokové šifry

Šifrovací mechanismy uvedené v tabulce č. 1 patří do kategorie tzv. blokových šifer. Jedná se o symetrické šifrování bloků pevně stanovené délky (např. 128 bitů). Při šifrování je každý blok zašifrován pomocí kryptografického algoritmu využívajícího utajený klíč. Dešifrování probíhá pomocí stejného klíče, který mezi sebou účastníci sdílí (tzv. sdílené utajení). Při použití stejného šifrovacího mechanismu na každý blok dat roste pravděpodobnost prolomení klíče. Proto je vhodné do šifrování zapojit další vstup, který do šifrování vnese nepravidelnost.

2.3.1 DES

S rozvojem výpočetní techniky vyvstala potřeba šifrovat data nejen v armádním a diplomatickém prostředí, ale také v civilních a státních organizacích. DES (Data Encryption Standard) byl prvním šifrovacím algoritmem široce používaným v civilní sféře. Počátkem 70.

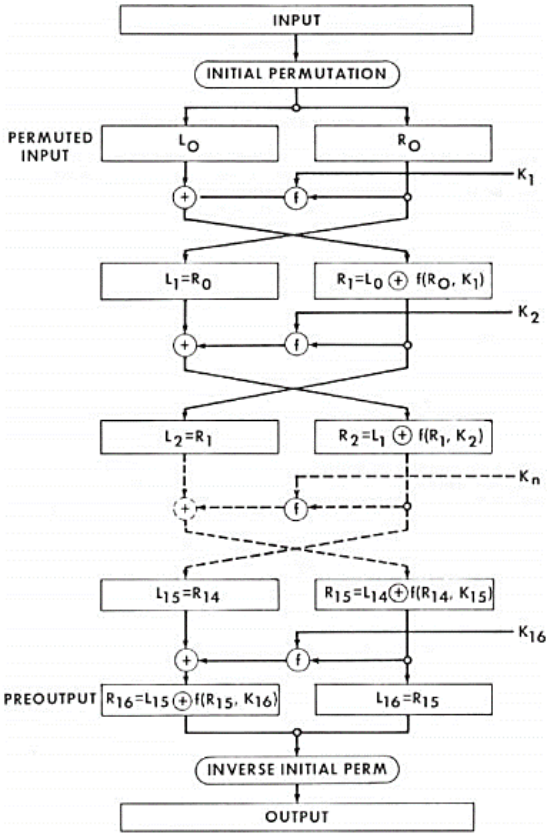
let 20. století jej vyvinula společnost IBM a v roce 1977 byl standardizován jako oficiální šifrovací metoda pro státní organizace v USA (FIPS 46), odkud se rychle rozšířil i do soukromé sféry. [9]

Šifrovací algoritmus používá klíč o délce 64 bitů (resp. 56 efektivních a 8 kontrolních bitů) a šifruje bloky dat o délce 64 bitů. Ty jsou nejprve v rámci bloku prohozeny pomocí počáteční permutace (IP) a následně rozděleny na 2 části o 32 bitech (L jako levá část a R jako pravá část). Potom probíhá 16 šifrovacích iterací podle těchto pravidel (tzv. Feistelova síť):

$$L' = R$$

$$R' = L \oplus f(R, K),$$

kde L‘ je levá a R‘ pravá strana následující iterace. Operátor $\oplus$ značí postupné sčítání bitů modulo 2, f je šifrovací funkce a K je permutace 48 bitů vybraných z 64bitového klíče (podklíč). Pozice vybraných bitů se v každé ze 16 iterací mění. Po provedení poslední iterace je na blok šifrovaných dat aplikována permutace inverzní k počáteční permutaci (IP^{-1}), což umožní použít pro dešifrování stejný algoritmus jako pro šifrování, jen s použitím podklíčů v opačném pořadí. Schéma šifrovacího algoritmu je na obrázku č. 6. [9]



Obr. 6: Schéma šifrovacího algoritmu metody DES (zdroj: [9])

V současné době je šifrovací metoda DES považována za překonanou, zejména kvůli krátkému šifrovacímu klíči a nárůstu výpočetního výkonu, který umožňuje prolomit šifru hrubou silou za méně než 24 hodin (v roce 1999 se to lidem z Electronic Frontier Foundation a Distributed Computing Technologies podařilo za 22 hodin a 15 minut). [10]

2.3.2 3DES

3DES neboli Triple DES je celkem elegantním řešením nedostatečné délky šifrovacího klíče metody DES, aniž by bylo nutné vyvíjet zcela nový šifrovací mechanismus. Spočívá v trojím aplikování šifrovacího algoritmu popsaného v předchozí části na každý blok šifrovaných dat.

Postup šifrování je následující: [11]

$$C = E_{K3}\left(D_{K2}\left(E_{K1}(P)\right)\right)$$

Nejdříve zašifrujeme otevřená data (P) metodou DES pomocí klíče K1, poté je dešifrujeme pomocí klíče K2 a nakonec opět zašifrujeme pomocí klíče K3, čímž dostaneme zašifrovaná data (C). Dešifrování probíhá opačně: [11]

$$P = D_{K1}\left(E_{K2}\left(D_{K3}(C)\right)\right)$$

3DES nabízí 3 varianty použití klíčů: [11]

1) Všechny 3 klíče jsou navzájem nezávislé.
2) K1 a K2 jsou navzájem nezávislé, K3 je shodný s K1.
3) Všechny 3 klíče jsou shodné.

Nejbezpečnější variantou je bezesporu prvně jmenovaná – když pomineme kontrolní bity, nabízí celkovou délku klíče 168 bitů. Druhá varianta pracuje s klíči o délce 112 bitů a oproti dvojímu zašifrování pomocí metody DES je navíc odolná vůči útokům typu man-in-the-middle. Třetí varianta je ekvivalentem původní metody DES – první dvě operace se navzájem vyruší a skutečná délka použitého klíče je 56 bitů. Skrze tuto variantu lze zajistit zpětnou kompatibilitu 3DES a DES, ale vzhledem k popsaným rizikům nelze její používání doporučit.

2.3.3 AES

Nástupcem DES se stala šifrovací metoda AES (Advanced Encryption Standard). Americký Národní institut pro standardizaci a technologie (National Institute of Standards and Technology, NIST) ji vybral z celkem 15 kandidátů po pěti letech testování a hodnocení. V roce 2001 se stala oficiálním standardem pro šifrování elektronické komunikace v USA (FIPS 197)

a následně se stala součástí standardu ISO/IEC 18033-3, který se zabývá bezpečnostními technikami informačních technologií. [12]

AES je založena na blokové šifře Rijndael, kterou vyvinuli dva belgičtí kryptografové – Joan Daemen a Vincent Rijmen. Jedná se o metodu, která zpracovává bloky dat o délce 128 bitů, přičemž délka klíče může být 128, 192 nebo 256 bitů. Jak je zřejmé z tabulky č. 2 [13], délka klíče určuje počet transformačních cyklů.

Tab. 2: Počet transformačních cyklů šifrovací metody AES v závislosti na délce klíče

Délka klíče [b]	Počet cyklů
128	10
192	12
256	14

AES pracuje s maticí bytů 4x4, která se označuje termínem stav. Každý sloupec, tedy 4 byty (32 bitů) je definován jako slovo. Šifrovací algoritmus začíná tzv. expanzí klíče – klíč o délce např. 128 bitů, tedy 4 slov, expanduje do rozvrhu klíčů (key schedule, KS) o délce 44 slov. První čtyři slova KS jsou shodná s původním klíčem, další 4 slova jsou odvozena pomocí logických operací s bity předchozích 4 slov atd. Tento proces pokračuje až do naplnění KS.

Poté je počáteční stav (nešifrovaný blok dat) podroben operaci XOR s prvními 4 slovy KS (což je původní klíč), načež začíná 1. transformační cyklus. Každý cyklus sestává z těchto 4 částí: [13]

1) **Záměna bytů** – náhrada každého bytu podle vyhledávací tabulky (S-boxu), odvozené z převrácených hodnot konečného tělesa GF(2^8). Toto těleso má vhodné nelineární vlastnosti, čehož lze využít k obraně před útoky založenými na pevných algebraických bodech a jejich protějších.
2) **Prohození řádků** – v tomto kroku dochází k posunu bytů na jednotlivých řádcích. První řádek zůstává nezměněn, na druhém řádku dojde k posunu všech bytů o 1 doleva. Na třetím řádku dojde k posunu bytů o 2 a na čtvrtém řádku o 3 pozice stejným směrem.
3) **Kombinování sloupců** – všechny 4 byty každého sloupce jsou modifikovány funkcí, která zajistí, že každý vstupní byte ovlivňuje všechny výstupní byty. Spolu s předchozím krokem tento krok zajistí dostatečnou náhodnost, tj. že změna jediného bitu původních otevřených dat ovlivní všechny bity zašifrovaných dat.

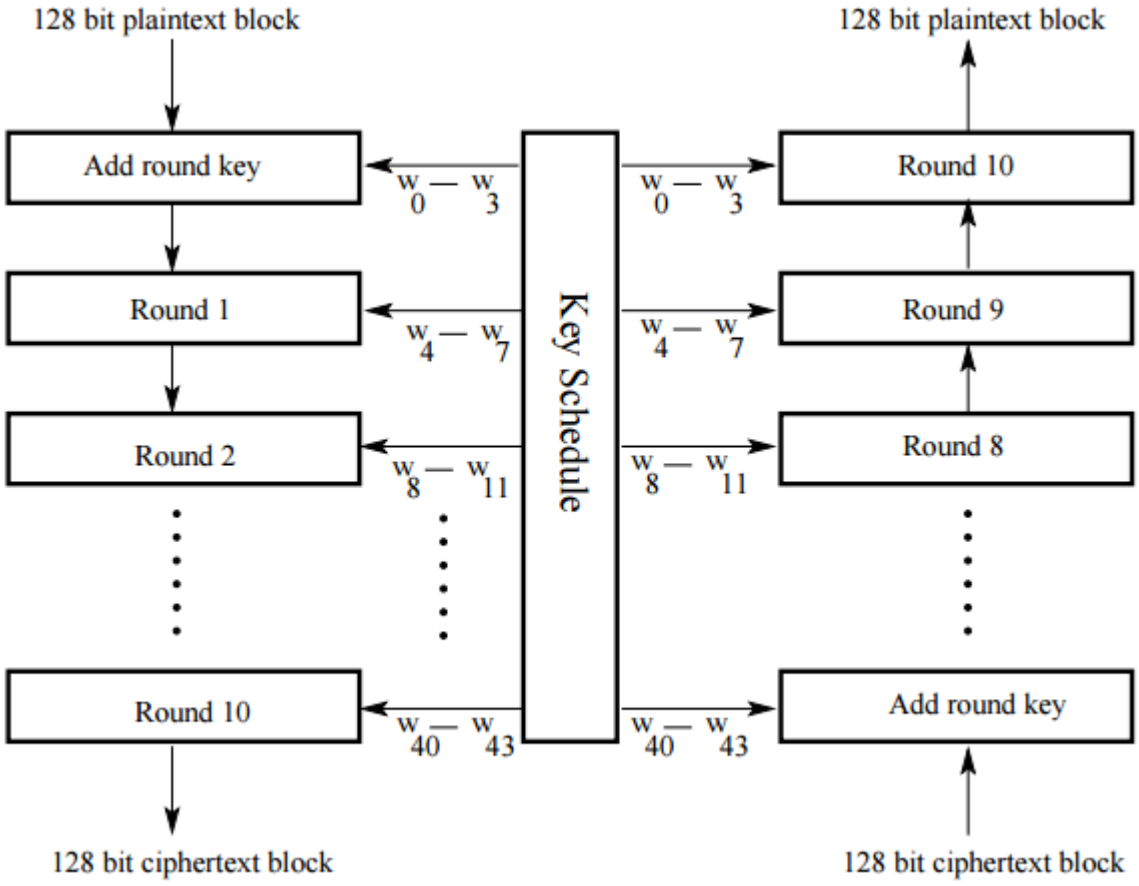
4) **Přidání podklíče** – stav je pomocí operace XOR zkombinován s podklíčem určeným pro daný cyklus, tj. pro první cyklus s pátým až osmým slovem KS, pro druhý cyklus s 9. až 12. slovem KS atd.

V posledním cyklu se vynechá krok 3 – kombinování sloupců a po přidání posledního podklíče je šifrovací algoritmus u konce. [13]

Dešifrování probíhá podobně, ale struktura jednotlivých cyklů je rozdílná: [13]

1) inverzní prohození řádků
2) inverzní záměna bytů
3) přidání podklíče
4) inverzní kombinování sloupců

Poslední dešifrovací cyklus nezahrnuje krok 4 – inverzní kombinování sloupců. Podklíče se přidávají logicky v opačném pořadí, tedy od posledního slova v KS. Schéma průběhu šifrovacího a dešifrovacího algoritmu je na obrázku č. 7.



Obr. 7: Schéma šifrovacího (vlevo) a dešifrovacího algoritmu AES (zdroj: [13])

3 Near Field Communication (NFC)

NFC je relativně nová technologie bezdrátové komunikace na krátkou vzdálenost. Je založena na radiofrekvenční identifikaci (RFID), ke komunikaci využívá indukci magnetického pole. K zahájení přenosu informací stačí, aby bylo napájeno jedno z dvojice NFC zařízení. Hlavní rozdíl oproti RFID ovšem spočívá v zaměření na jinou oblast – zatímco RFID našlo využití zejména v průmyslu, logistice a sledování zboží, NFC se soustřeďuje na služby uživatelům/zákazníkům, a to v mnoha oblastech života, např. na:

- stahování obsahu z tzv. smart plakátů
- přístup do budov
- konfigurace zařízení
- iniciace komunikace delšího rozsahu (Bluetooth, Wi-Fi)
- odbavovací systémy
- bezkontaktní platby

S rozmachem chytrých mobilních telefonů, tabletů a v poslední době též nositelné elektroniky je zřejmé, že tato technologie má velký potenciál. Zejména využití v odbavovacích systémech a finančních transakcích funguje na téměř shodném principu jako klasické bezkontaktní karty, takže je možné využít stávající infrastruktury. Použití v těchto oblastech ovšem vyžaduje vyšší úroveň zabezpečení. [14]

3.1 Základní specifikace NFC

- NFC využívá ke komunikaci indukci magnetického pole mezi dvěma anténami umístěnými v dostatečné blízkosti. Pracuje na celosvětově dostupné volné frekvenci 13,56 MHz s šířkou pásma cca 2 MHz.
- Maximální vzdálenost komunikujících NFC zařízení je 20 cm, ale v praxi komunikace probíhá do vzdálenosti 10 cm.
- Přenosová rychlost – 106, 212, nebo 424 kbps, existuje potenciál pro další zvyšování. [14]

Komunikace může probíhat ve dvou módech:

1) **Pasivní** – iniciátor komunikace generuje magnetické pole a cílové zařízení odpovídá jeho modulací. Cílové zařízení může být napájeno magnetickým polem iniciátora (pracuje jako transpondér).

2) **Aktivní** – iniciátor i cílové zařízení vzájemně komunikují střídavým generováním vlastního magnetického pole. To předpokládá napájení obou komunikujících zařízení.

Důležité je, že komunikaci iniciuje vždy aktivní zařízení, pasivní zařízení pouze odesílá odpověď na příchozí požadavek. Z toho vyplývá, že mezi sebou můžou komunikovat buď dvě aktivní NFC zařízení, nebo aktivní s pasivním zařízením – dvě pasivní NFC zařízení nejsou schopna vzájemné komunikace.

Komunikaci přes NFC lze také rozdělit do tří možných režimů: [14]

1) **Čtení/zápis** – aktivní (napájené) zařízení čte/zapisuje informace z/do pasivního NFC zařízení a následně vykonává činnost na základě získané informace (např. načtení webové stránky z přijatého URL, odeslání SMS, získání vstupenky apod.). Přenosová rychlost činí 106 kbps.
2) **Peer-to-peer** – v tomto případě probíhá komunikace mezi dvěma aktivními zařízeními. Příkladem komunikace v tomto režimu je vzájemná komunikace mezi dvěma smartphony. Přenosová rychlost dosahuje 424 kbps.
3) **Card emulation** – NFC zařízení v tomto režimu se chová jako bezkontaktní karta, takže lze využít veškerou infrastrukturu pro ně určenou – přístup do budov, odbavovací systémy, bezkontaktní platby atd.

3.2 Standardizace, kompatibilita

Ačkoli byla NFC technologie vyvinuta společnostmi Philips a Sony, jedná se o open source technologickou platformu, kterou popisuje protokol NFCIP-1 (Near Field Communication Interface and Protocol 1). Standardizace NFC je zakotvena v normách ISO 18092, ECMA 340 a ETSI TS 102 190. Tyto standardy stanoví základní parametry jako přenosové rychlosti, schémata kódování bitů, modulace, architekturu rámců a transportní protokol. Navíc je zde popsán pasivní a aktivní mód komunikace a podmínky zabraňující kolizím během inicializace. [14]

Kromě NFCIP-1 zařízení s NFC implementují rovněž protokol NFCIP-2 (definovaný normami ISO 21481, ECMA 352 a ETSI TS 102 312), který jim umožňuje výběr jednoho ze tří pracovních režimů:

- NFC data transfer (NFCIP-1)
- Proximity coupling device (PCD) → ISO 14443 (Mifare – Philips)
- Vicinity coupling device (VCD) → ISO 15693

To je důležité zejména z hlediska zpětné kompatibility s existujícími bezkontaktními systémy, zvláště s bezkontaktními kartami a čtečkami využívajícími výše zmíněné standardy pro PCD a VCD.

3.3 Kódování

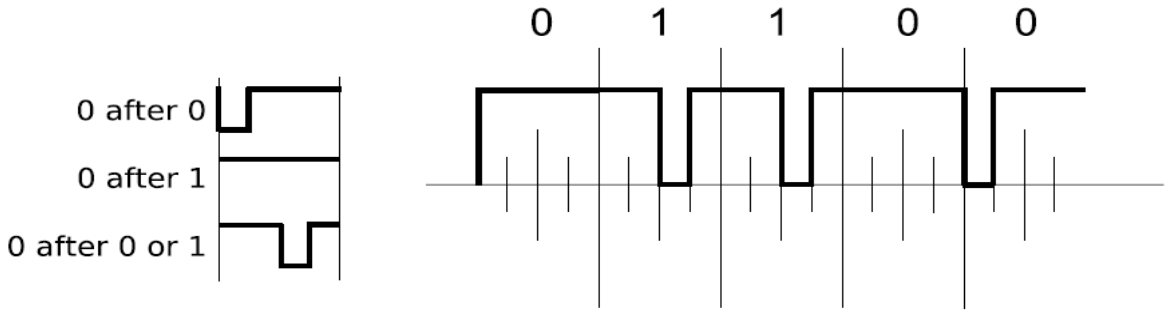
NFC využívá k přenosu dat dva typy kódování. Pro přenos dat aktivním zařízením o rychlosti 106 kbps se uplatňuje modifikované Millerovo kódování se 100% hloubkou modulace, pro všechny ostatní případy se používá kódování Manchester s 10% hloubkou modulace. Vše je shrnuto v tabulce č. 3. [14]

Tab. 3: Přehled typů kódování pro přenos dat pomocí NFC

kbps	Aktivní zařízení	Pasivní zařízení
424	Manchester, 10% ASK	Manchester, 10% ASK
212	Manchester, 10% ASK	Manchester, 10% ASK
106	Modified Miller, 100% ASK	Manchester, 10% ASK

3.3.1 Modifikované Millerovo kódování

Modifikované Millerovo kódování je charakteristické pauzami, které se vyskytují na různých pozicích v rámci periody. Princip je zřejmý z obrázku č. 8. Zatímco 1 je kódována vždy stejně, kódování 0 závisí na hodnotě předchozího bitu.

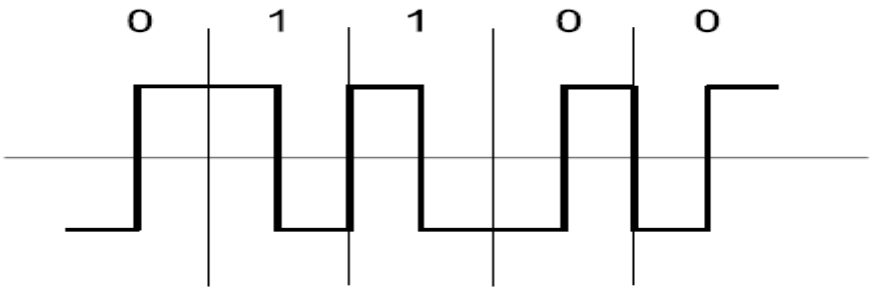


Obr. 8: Princip modifikovaného Millerova kódování (zdroj: [14])

3.3.2 Kódování Manchester

Kódování Manchester je založeno na změně úrovně signálu uprostřed periody. Přechod z nižší na vyšší úroveň reprezentuje 0, naopak přechod z vyšší na nižší úroveň představuje 1.

Uprostřed každé periody se tedy musí změnit úroveň signálu (změny úrovně na začátku periody nebereme v potaz) – viz obrázek č. 9.



Obr. 9: Princip kódování Manchester (zdroj: [14])

3.4 NFC Data Exchange Protocol (NDEF)

Zatímco specifikace NFCIP-1 definuje rozhraní a protokol pro bezdrátovou komunikaci dvou NFC zařízení, NDEF specifikuje formát zapouzdření zpráv pro vzájemnou komunikaci; jeho cílem je definice struktury dat a pravidel pro konstrukci validních **NDEF zpráv**, sestávajících z jednoho nebo více **NDEF záznamů** – jak ukazuje obrázek č. 10.

Jedná se o jednoduchý binární formát zpráv určený k zapouzdření aplikačních dat libovolného typu do jednoho celku. Data reprezentovaná jednotlivými NDEF záznamy jsou definovaná pomocí délky, typu a volitelného identifikátoru. Význam jednotlivých parametrů je následující: [15]

- **Délka** – udává velikost dat v konkrétním NDEF záznamu. Je definována polem PALYOAD_LENGTH o velikosti 1 B pro krátké zprávy a 4 B pro normální zprávy.
- **Typ** – udává druh dat přenášených konkrétním NDEF záznamem – např. URI, MIME typy, nebo dobře známé datové typy NFC. Je definován polem TNF (Type Name Format), které určuje strukturu, kódování a formát pole TYPE.
- **Volitelný identifikátor dat** – umožňuje uživatelským aplikacím identifikovat data v konkrétním NDEF záznamu (např. je možné v rámci záznamu odkazovat pomocí URI na data v jiném záznamu). NDEF samotné ale žádný linkovací mechanismus nepopisuje a nechává ho na programátorech konkrétních aplikací.

NDEF Message						
R_1 MB=1	…	R_r	…	R_s	…	R_t ME=1

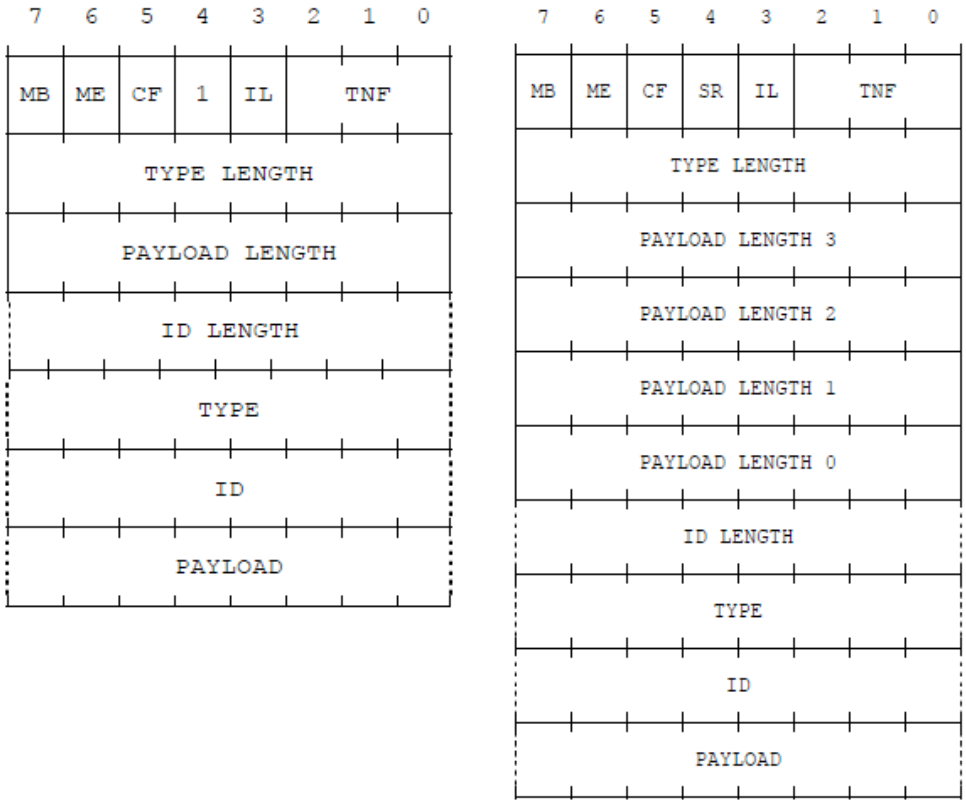
Obr. 10: Příklad NDEF zprávy se sadou záznamů (zdroj: [15])

První záznam zprávy je navíc označen příznakem MB (Message Begin – počátek zprávy), naopak poslední záznam zprávy označuje příznak ME (Message End – konec zprávy). Aplikací obou příznaků na jediný záznam dosáhneme NDEF zprávy minimální velikosti – maximální počet záznamů v NDEF zprávě není omezen.

V rámci NDEF zpráv je rovněž možné posílat tzv. **kusy záznamů** (record chunks). To je výhodné při posílání dynamicky generovaných dat o předem neznámé velikosti, protože se snižuje nutnost odchozího bufferování, a také v případě dat přesahujících povolenou velikost NDEF záznamu. NDEF zpráva nemusí obsahovat žádný kus záznamu, na druhé straně jejich počet není shora nijak omezen. První kus záznamu v pořadí je počátečním kusem záznamu následovaným nula nebo více prostředními kusy záznamů a nakonec ukončujícím kusem záznamu. Celý soubor „rozkouskovaných“ dat musí být bezpodmínečně zapouzdřen v jediné zprávě (takže počáteční ani prostřední kus záznamu nemůže mít příznak ME). [15]

3.4.1 Struktura NDEF záznamů

NDEF záznamy se liší délkou (krátký záznam 0-255 B, normální záznam max. 2^{32}-1 B), ale jinak mají standardní formát ilustrovaný níže obrázkem č. 11. V následující části jsou jednotlivá pole popsána podrobněji. [15]



Obr. 11: Struktura NDEF záznamů: krátký záznam (vlevo), normální záznam (zdroj: [15])

MB (Message Begin) – jednobitové pole, při hodnotě 1 indikuje začátek NDEF zprávy.

ME (Message End) – jednobitové pole, při hodnotě 1 indikuje konec NDEF zprávy.

CF (Chunk Flag) – jednobitové pole, hodnota 1 značí počáteční nebo prostřední kus záznamu, hodnota 0 indikuje ukončující kus záznamu.

SR (Short Record) – jednobitové pole, hodnota 1 znamená, že se jedná o krátký NDEF záznam (tzn., že pole PAYLOAD_LENGTH má velikost 8 bitů a do pole PAYLOAD se tak vejdou data o velikosti 0-255 B). Hodnota 0 znamená normální záznam.

IL (ID_LENGTH field is present) – jednobitové pole, které při nastavené 1 indikuje přítomnost pole ID_LENGTH o velikosti 1 B. Při nastavené 0 jsou pole ID_LENGTH a ID ze záznamu vynechána.

TNF (Type Name Format) – tříbitové pole, které implikuje strukturu pole TYPE; definované hodnoty pole TNF ukazuje tabulka č. 4. [15]

Tab. 4: Hodnoty pole TNF a jejich význam

Type Name Format	Hodnota
Prázdný	0x00
Dobře známý datový typ NFC	0x01
Typ médií podle RFC 2046	0x02
Absolutní URI podle RFC 3986	0x03
Externí typ NFC Fóra	0x04
Neznámý	0x05
Nezměněno	0x06
Rezervováno	0x07

Hodnota 0x00 znamená, že se záznamem není spojen žádný typ nebo data. Při nastavení této hodnoty musí být pole TYPE_LENGTH, ID_LENGTH a PAYLOAD_LENGTH nulová, což má za následek faktické vynechání polí TYPE, ID a PAYLOAD – nastavení TNF na tuto hodnotu vytvoří prázdný záznam.

Při hodnotě 0x05 musí být hodnota pole TYPE_LENGTH nulová, abychom dosáhli vynechání pole TYPE ze záznamu.

Hodnota 0x06 se nastavuje výhradně pro prostřední a ukončující kusy záznamů. Platí zde stejná podmínka nulového pole TYPE_LENGTH jako u hodnoty 0x05.

TYPE_LENGTH – bezznaménkové 8-bitové celé číslo, které specifikuje délku pole TYPE v bytech. Pro některé hodnoty TNF je vždy nulové (viz výše).

ID_LENGTH – bezznaménkové 8-bitové celé číslo, které specifikuje délku pole ID v bytech. Je součástí NDEF záznamu jedině v případě, že hodnota pole IL je 1.

PAYLOAD LENGTH – bezznaménkové 8-bitové (pro krátké záznamy) nebo 32-bitové (pro normální záznamy) celé číslo, které specifikuje délku pole PAYLOAD v bytech.

TYPE – identifikátor typu přenášených dat. Hodnota pole TYPE se musí řídit strukturou, kódováním a formátem předepsanými hodnotou pole TNF.

ID – jednoznačný identifikátor NDEF zprávy v podobě URI odkazu. Jedinečnost záznamu zaručuje generátor zpráv. Pole může být přítomno ve všech NDEF záznamech kromě prostředních a ukončujících kusů záznamů.

PAYLOAD – pole nesoucí užitečná data využitelná uživatelskými aplikacemi. Vnitřní struktura těchto dat není z hlediska NDEF brána v potaz a může být v podstatě libovolná.

3.5 Bezpečnostní hrozby pro NFC

V následující části jsou popsány základní typy útoků, které přicházejí pro technologii NFC v úvahu, a zároveň je naznačeno, jakým způsobem jim lze efektivně předcházet.

3.5.1 Odposlech

NFC jako technologie pro bezdrátovou komunikaci je už z principu zranitelná vůči odposlechu. Za předpokladu, že útočník disponuje patřičnými znalostmi a vybavením, může využít přenosu dat prostřednictvím radiových vln a pomocí antény a dekodéru odposlouchávat cizí komunikaci. Ta probíhá na krátké vzdálenosti, obvykle do 10 cm. Vzdálenost nutná pro efektivní odposlech však záleží na mnoha faktorech, jako jsou např. charakteristiky antén komunikujících NFC zařízení a útočníkovy antény, omezující vlivy v podobě bariér, úroveň šumu atd. Také záleží na energetické hladině elektromagnetického pole mezi komunikujícími zařízeními, tj. jestli komunikace probíhá v aktivním, nebo v pasivním módu. Z tohoto důvodu by bylo zavádějící uvádět konkrétní vzdálenosti nutné pro efektivní odposlouchávání, ale např. dle [16] je pro aktivní mód tato vzdálenost do 10 m, pro pasivní mód se výrazně snižuje až na cca 1 m.

Pravděpodobnost odposlechu lze snížit použitím pasivního komunikačního módu, ale jedinou zaručenou ochranou je použití zabezpečeného kanálu (viz kapitola 4.6).

3.5.2 Manipulace s daty

Kromě odposlouchávání dat se může útočník také pokusit přímo ovlivnit přenášená data. Nejjednodušším případem je **narušení přenosu dat** tak, aby příjemce nemohl komunikaci správně interpretovat. Toho lze dosáhnout vysíláním správných frekvencí používaných k přenosu dat pře NFC ve správný čas. V podstatě se jedná o DoS (Denial of Service) útok. [16]

NFC technologie ale umožňuje kontrolu elektromagnetického pole v průběhu přenášení dat, a protože energie nutná k narušení přenosu je mnohem větší, než je NFC zařízení schopné detekovat, každý pokus o útok tohoto typu by měl být bez problémů odhalen.

Pokročilejším typem útoku je **modifikace přenášených dat**. V tomto případě je cílem útoku doručit příjemci validní, ale zmanipulovaná data. Proveditelnost útoku závisí na typu použité modulace, protože dekódování signálu probíhá jinak u modifikovaného Millerova kódování (MMK) se 100% hloubkou modulace a jinak u kódování Manchester (KM) s 10% hloubkou modulace. [16]

V případě MMK dekodér sleduje, zda se v první nebo ve druhé polovině bitu objeví pauza. Aby útočník dokázal zaměnit 0 za 1 a naopak, musel by vyplnit pauzu nosnou frekvencí a vygenerovat pauzu tam, kde původně nebyla. První z těchto úkonů lze provést relativně snadno, ale druhý je uskutečnitelný jen teoreticky – muselo by dojít k vyslání signálu, který by se s původním dokonale překrýval, ale nabýval opačné hodnoty. Takže v případě MMK není útočník schopen nahradit bit s hodnotou 0 bitem s hodnotou 1, ale může nahradit bit s hodnotou 1 bitem opačné hodnoty v případě, že tomuto bitu předcházel bit stejné hodnoty.

U KM dekodér měří hodnotu signálu a porovnává je (např. 82% a 100%). V případě, že signál náleží do určeného intervalu, je vyhodnocen jako platný a dojde k jeho dekódování. Útočník by teoreticky mohl ovlivnit původní signál přidáním signálu, který by zajistil, že původních 82% by se jevilo jako 100% a naopak. Dekodér by vyhodnotil přijímaný signál jako opačný k původně vyslanému signálu. Za předpokladu, že útočník bere v potaz meze intervalu pro validaci signálu, lze tímto způsobem ovlivnit libovolný bit.

Částečnou obranou proti tomuto typu útoku je použití MMK se 100% hloubkou modulace, protože v tomto režimu není možné modifikovat každý bit. Tento režim ale předpokládá obě zařízení v aktivním režimu, což zase usnadňuje útočníkovi odposlouchávání komunikace.

Kromě kontroly elektromagnetického pole stejně jako u narušování přenosu dat lze doporučit použití zabezpečeného kanálu.

Dalším možným útokem je **vložení dat** do probíhající komunikace mezi dvěma NFC zařízeními. Tento útok je uskutečnitelný pouze v případě dlouhé doby potřebné k odeslání odpovědi – útočník toho může využít k odeslání falešné odpovědi dříve než komunikující zařízení. Předpokladem úspěšného útoku je odvysílání kompletní falešné odpovědi dříve, než začne odpovídat regulérní zařízení, jinak by došlo k narušení přenosu a data by byla poškozena. [16]

Zamezit vložení nepatřičných dat do vzájemné komunikace je možné odpovídáním bez zpoždění, příp. hlídáním času, po který má být komunikační kanál otevřen – při zahájení komunikace dříve než ve stanovený čas by bylo zřejmé, že se jedná o útok. Třetí možností je opět použití zabezpečeného kanálu.

3.5.3 Man-in-the-Middle

Princip tohoto typu útoku spočívá v narušení komunikace mezi dvěma zařízeními tak, aby ani jedno z nich narušení nezaznamenalo. Komunikující strany mají za to, že vzájemně komunikují mezi sebou, ale ve skutečnosti jejich komunikace končí „v půli cesty“, kde je odposlouchávána, modifikována a případně přeposílána dál útočníkem. Takto může být narušen i proces tvorby zabezpečené komunikace skrze sdílené utajení.

Vzhledem k tomu, že NFC zařízení komunikují bezdrátově na velmi blízkou vzdálenost, je provedení útoku typu Man-in-the-Middle nereálné. Útočník by musel odposlouchávat komunikaci a zároveň zabezpečit, aby se původní odvysílané zprávy nedostaly k zamýšleným příjemcům, aniž by to komunikující strany zaznamenaly. S přihlédnutím k možné kontrole elektromagnetického pole při komunikaci a principu čekání na odpověď je velice nepravděpodobné, že by ani jedna strana nezaznamenala útočníkovu aktivitu a nedošlo by tak k přerušení komunikačního protokolu. [16]

3.6 NFC Secure Channel

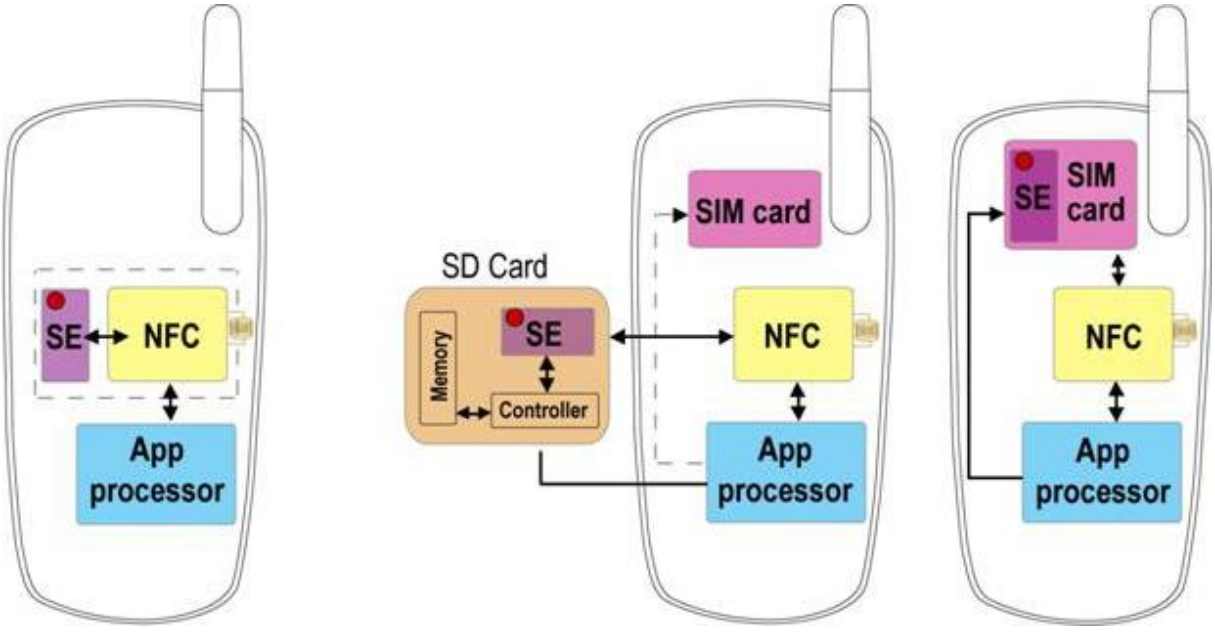
V předchozích odstavcích byl jako forma obrany proti různým útokům několikrát zmíněn zabezpečený kanál. Jeho použití je univerzální a zároveň nejefektivnější obranou proti nežádoucím zásahům třetích stran do probíhající komunikace. Předpokladem pro vytvoření zabezpečeného kanálu je to, aby byl v mobilním telefonu mimo NFC čip implementován tzv. secure element. Ten slouží jako úložiště veškerých zabezpečených dat, jako jsou důvěrné informace o platebních, věrnostních, nebo identifikačních kartách sloužících např. pro přístup

do budov. Každá karta, resp. aplikace, je zabezpečena vlastním klíčem, aby se zamezilo přístupu neoprávněné čtečky k nerelevantním aplikacím. V secure elementu jsou rovněž uloženy veškeré šifrovací klíče a také v něm probíhají všechny kryptografické operace. [17]

Secure element je tedy nezávislý čip, postavený mezi NFC čipem (obsluhující HW) a samotnou infrastrukturou telefonu. Sestává z non-volatilní paměti (takové, která uchovává data i po odpojení napájení), procesoru a kryptovacího koprocesoru. Běžně se lze v literatuře setkat s dělením na tři základní typy: [17]

1) **SIM karta** – jedná se o novou generaci SIM karty (tzv. UICC – Universal Integrated Circuit Card), na kterou se ukládají zabezpečená data. Protože vydavatelem SIM karet je operátor, bude rovněž řídit přístup do secure elementu, což lze považovat za velkou nevýhodu.
2) **Integrovaný secure element** – v tomto případě je secure element napevno zabudovaný v telefonu. Přístup k němu řídí uživatel – teoreticky tak k němu má přístup kdokoli, komu to uživatel povolí.
3) **Externí secure element** – zřídka využívané řešení, kdy jako secure element slouží např. speciální zabezpečená microSD karta.

Princip fungování těchto tří variant secure elementu přibližuje obrázek č. 12.

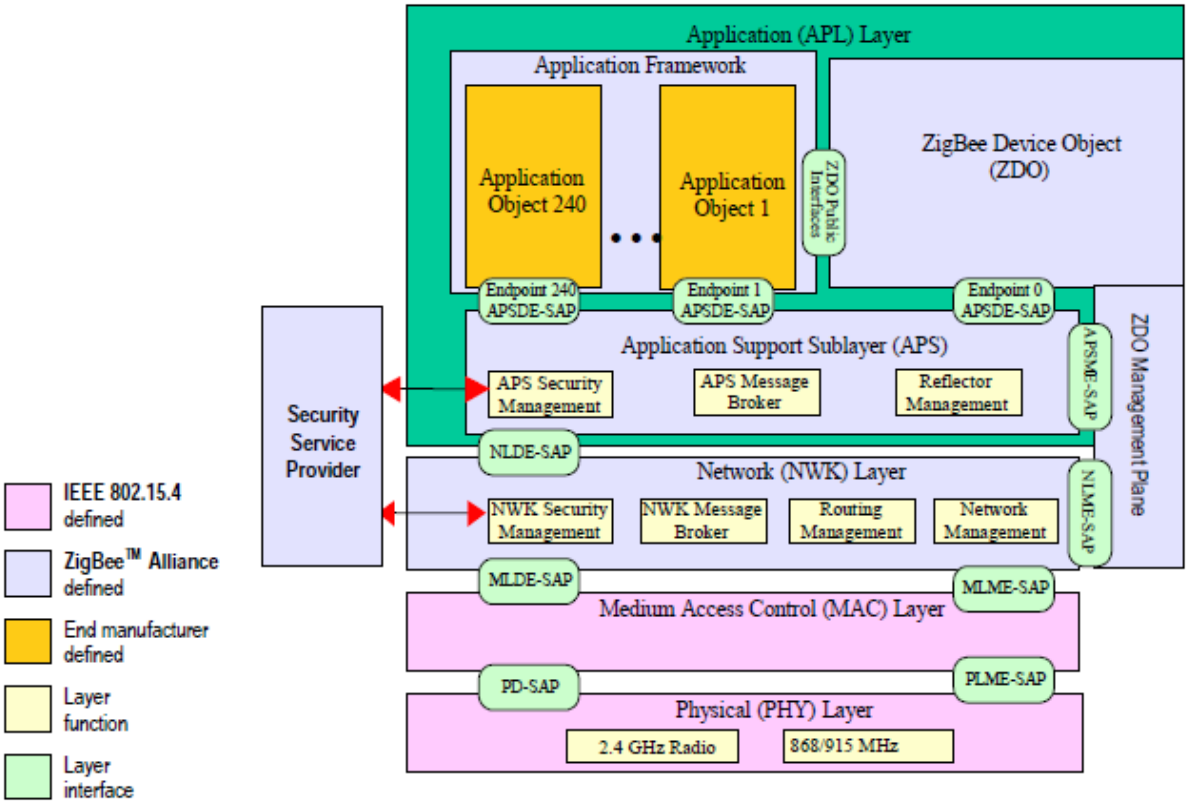


Obr. 12: Schéma umístění NFC secure elementu (SE) a zabezpečené komunikace uvnitř mobilního telefonu: integrovaný SE (vlevo), externí SE (uprostřed) a SE na SIM kartě (zdroj: [17])

4 ZigBee

ZigBee je technologie obousměrné bezdrátové komunikace, která je primárně určena pro spojení nízkovýkonových zařízení v lokálních sítích typu PAN. Její výhodou je nízká cena jednotlivých komponent a nízká spotřeba energie, což ji předurčuje k nasazení v řadě specifických situací – od průmyslových řešení a senzorových sítí přes automatizaci provozu budov a senzory zdravotního stavu až po spotřební elektroniku (spojení počítačových periferií, mobilní telefony, hry atd.). Princip multiskokového ad hoc směrování umožňuje spojení i na delší vzdálenosti bez nutnosti přímé radiové viditelnosti komunikujících zařízení.

Technologie je postavena na standardu IEEE 802.15.4, který dále rozvíjí sdružení ZigBee Alliance. Předpokládané nasazení v mikrokontrolérech s malým výkonem je důvodem snahy o co nejjednodušší implementaci protokolů, jejichž struktura tak potřebuje maximálně 30 kB programové paměti. Protokol vychází z architektury sedmivrstvého referenčního modelu OSI, z něhož však přebírá pouze nejnižší část – fyzickou vrstvu (PHY) a podvrstvu řízení přístupu k médiím (MAC). Nad nimi je síťová (NWK) a aplikační vrstva (APL), rozdělená na aplikační podvrstvu (APS), ZigBee objekt pro konkrétní zařízení (ZDO) a aplikační objekty definované různými výrobci. Vrstvovou architektura ZigBee zachycuje obrázek č. 13. [18]



Obr. 13: Vrstvová architektura ZigBee (zdroj: [18])

APS má na starosti párování zařízení podle typu poskytovaných služeb, k čemuž využívá tzv. párovacích tabulek. ZDO specifikuje roli jednotlivých zařízení v síti, vyhledává další zařízení a volí způsob zabezpečení. Jednotlivé aplikační objekty se řídí požadavky té které aplikace, která je specifikována v rámci ZigBee profilu (ZigBee profil definuje zařízení v síti a typy vzájemně vyměňovaných informací). [18]

4.1 Základní specifikace

ZigBee operuje v bezlicenčních frekvenčních pásmech pro průmyslové, vědecké a lékařské použití (ISM). ISM pásmo nesmí narušovat frekvence vyhrazené pro komunikaci, a protože jsou komunikační frekvence v různých částech světa odlišné, liší se i frekvence pro ISM pásmo. Přehled těchto frekvencí včetně přenosových rychlostí je uveden v tabulce č. 5. [19]

Tab. 5: Frekvenční pásmo ISM v různých částech světa

Oblast	Frekvence	Rychlost [kbps]
Čína	784 MHz	20
Evropa	868 MHz	20
USA, Austrálie	915 MHz	40
Ostatní oblasti	2,4 GHz	250

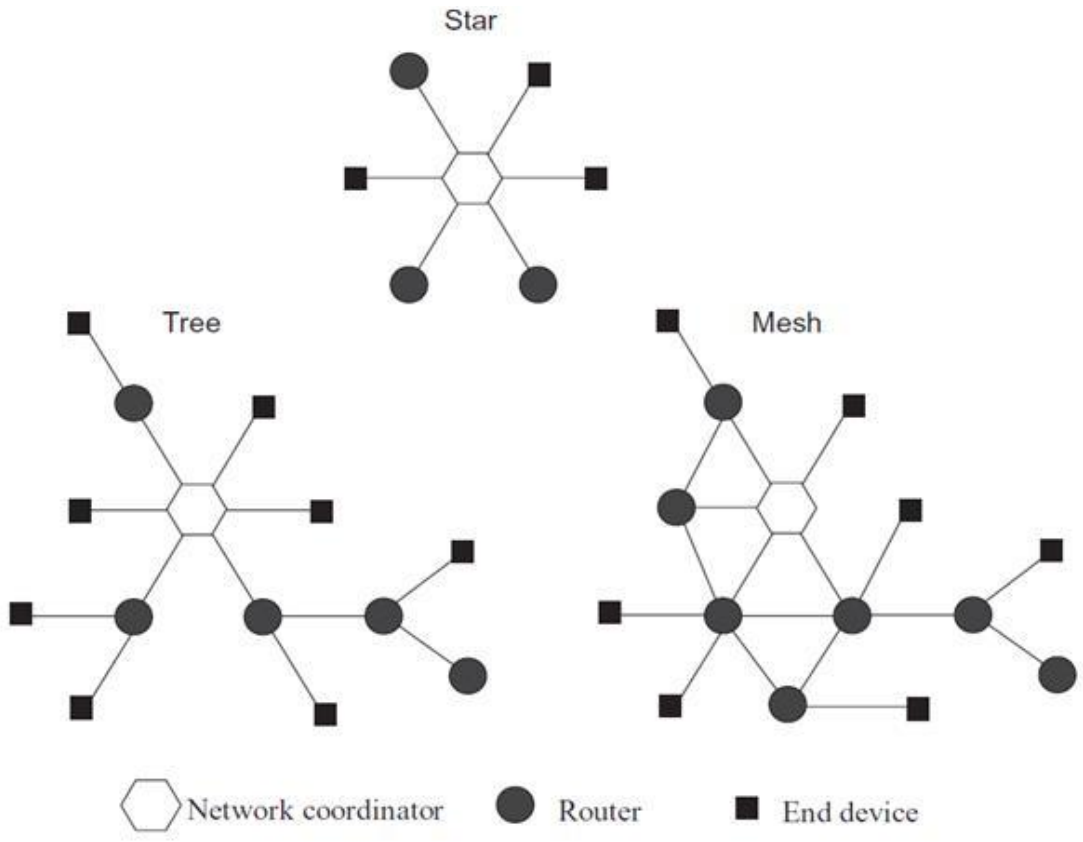
Efektivní dosah ZigBee je uvnitř budov při použití frekvence 2,4 GHz 10-20 m, při venkovním užití za předpokladu přímé viditelnosti může dosahovat teoreticky až 1500 m (v závislosti na použité frekvenci a podmínkách šíření signálu). Přístup k fyzické vrstvě se řídí metodou CSMA/CA (s výjimkou tzv. beacon signálů, které jsou odesílány v pevně daných časových okamžicích, stejně jako potvrzovací signály – podrobněji viz dále). Pro komunikaci ve frekvenčních pásmech pod 1 GHz je signál modulován metodou BPSK, v pásmu 2,4 GHz se používá OQPSK. K přenosu signálu používá ZigBee techniku přímého rozprostřeného spektra (DSSS), při níž je každý přenášený bit nahrazen pseudonáhodnou skupinou několika bitů vytvořených podle Goldových nebo Bakerových kódů. Tím dojde k rozprostření signálu do větší části spektra a signál je tím pádem odolnější vůči rušení. Výstupní výkon vysílače se pohybuje v rozmezí 0-20 dBm (1-100 mW). [18]

4.2 Topologie sítě

Síťová vrstva (NWK) standardu IEEE 802.15.4 podporuje tři typy topologií: [20]

- hvězdicovou topologii (star)
- stromovou strukturu (tree)
- síťovou topologii (mesh)

Jednotlivé typy podporovaných topologií ilustruje obrázek č. 14.



Obr. 14: Typy topologie podporované síťovou vrstvou ZigBee (zdroj: [20])

V případě hvězdicové topologie celou síť řídí centrální uzel, tzv. koordinátor. Ten má na starosti zahajování a udržování komunikace s jednotlivými koncovými zařízeními, která naopak komunikují pouze s koordinátorem.

V topologiích typu tree a mesh koordinátor zakládá síť a nastavuje její parametry. Výhodou těchto typů topologie je možnost rozšíření sítě pomocí směrovačů. V případě stromové struktury směrovače přeposílají data na základě pevně dané hierarchické struktury, kdežto v síťové topologii je realizovatelná plnohodnotná peer-to-peer (P2P) komunikace. [20]

ZigBee sítě lze dále rozdělit na dva základní druhy – na sítě s užitím tzv. beacon signálů (beacon-enabled) a na sítě bez nich (non-beacon-enabled). Beacon signály vysílá koordinátor v pravidelných časových intervalech (desítky milisekund až stovky sekund) a slouží jak k časové synchronizaci, tak k uspávání koncových zařízení. Ta se probouzí v předem definovaný čas a po dobu své aktivity komunikují s koordinátorem. Uspávání koncových zařízení šetří spotřebu elektrické energie a umožňuje jejich provoz na baterie.

V non-beacon-enabled sítích jsou koncová zařízení aktivní neustále a periodicky zjišťují, zda nejsou kontaktovány koordinátorem. Ten se naopak může probouzet pouze v požadovaný čas, což umožňuje snížit jeho spotřebu elektrické energie a případný provoz na baterie. V případě většího počtu koncových zařízení je tento typ sítě energeticky náročnější než beacon-enabled síť, ale i tak se jedná o nízkoenergetické řešení.

ZigBee dělí zařízení v sítích na tzv. plně funkční zařízení (FFD) a na zařízení s redukovanou funkčností (RFD). V FFD je implementován kompletní komunikační protokol a jejich účelem je zajištění správného fungování veškerých služeb, které jsou prostřednictvím ZigBee realizovány. RFD naproti tomu fungují jako koncová zařízení. Aby bylo možné maximálně redukovat jejich hardwarovou náročnost, implementují pouze nezbytně nutné knihovny příkazů. [18]

4.3 Datové rámce

Komunikační protokol definovaný MAC podvrstvou zahrnuje čtyři typy datových rámců, které jsou určeny pro přenos dat, řízení nebo správu sítě: [18]

- **Data Frame** – pro přenos užitečných dat
- **Acknowledgment Frame** – potvrzování komunikace na úrovni MAC
- **Beacon Frame** – vysílá koordinátor, slouží k časové synchronizaci sítě a uvádění koncových zařízení do režimu spánku
- **MAC Command Frame** – nastavení a řízení klientských zařízení v síti

Každý typ datového rámce sestává z hlavičky, která obsahuje kontrolní byte a informace o adresování, a samotné informace, specifické pro konkrétní typ rámce. Obecná struktura rámce je na obrázku č. 15.

<table>
<tr><th>Octets: 1</th><th>0/1</th><th>0/1</th><th>0/2</th><th>0/1</th><th>Variable</th></tr>
<tr><td rowspan="2">Frame control</td><td>Destination end-point</td><td>Cluster Identifier</td><td>Profile Identifier</td><td>Source endpoint</td><td rowspan="2">Frame payload</td></tr>
<tr><td colspan="4">Addressing fields</td></tr>
<tr><td colspan="5">APS header</td><td>APS payload</td></tr>
</table>

Obr. 15: Struktura rámce podle specifikace ZigBee (zdroj: [18])

Hlavička má pevně danou strukturu, adresovací informace však nemusí být zahrnuty do všech rámců. Kontrolní byte obsahuje údaje o typu rámce, způsobu adresování a zabezpečení a o požadavku na potvrzení přijetí – viz obrázek č. 16.

Bits: 0-1	2-3	4	5	6	7
Frame type	Delivery mode	Indirect address mode	Security	Ack. request	Reserved

Obr. 16: Struktura kontrolního bytu hlavičky rámce podle specifikace ZigBee (zdroj: [18])

Význam jednotlivých subpolí adresovacího pole je následující: [18]

- **Destination endpoint** – adresuje příjemce konkrétního rámce. Rámec lze adresovat vybranému ZDO, konkrétní aplikaci v konkrétním zařízení, nebo všem aktivním zařízením.
- **Cluster Identifier** – označuje příslušnost rámce ke skupině rámců, která je dále zpracovávána koordinátorem nebo jiným zařízením. Toto pole je přítomné pouze u datových rámců, příkazových rámců se netýká
- **Profile Identifier** – indikuje typ ZigBee profilu, ve kterém je daný rámec distribuován. Pole se vyskytuje u datových a potvrzovacích rámců.
- **Source endpoint** – označuje zdrojové zařízení konkrétního rámce. Původcem může být ZDO nebo konkrétní aplikace v konkrétním zařízení.

Užitečná informace následující za hlavičkou rámce se liší dle typu rámce. U datových rámců se jedná o víceméně libovolnou sekvenci bitů, která je dána potřebami aplikací z vyšší vrstvy. Příkazové rámce nesou informaci o typu příkazu a hodnotu konkrétního příkazu a potvrzovací rámce informační pole zcela vypouštějí.

4.4 Zabezpečení

ZigBee používá k zabezpečení komunikace metody založené na sdílení klíčů, ochraně rámců a managementu zařízení připojených do sítě. Nejdůležitějším z těchto principů je bezesporu zabezpečení prostřednictvím klíčů. V ZigBee sítích existují dva typy klíčů – spojový a síťový. Komunikace mezi dvěma zařízeními v rámci sítě je zabezpečena pomocí sdíleného 128bitového spojového klíče, zatímco komunikace mezi několika, příp. všemi zařízeními najednou je zabezpečena 128-bitovým síťovým klíčem sdíleným všemi zařízeními v síti.

Zařízení v ZigBee síti může získat spojový klíč trojím způsobem – distribucí klíče, vytvořením klíče na základě tzv. master klíče, anebo předinstalací (např. u výrobce). Síťový klíč je možné získat pouze distribucí nebo předinstalací (to platí i pro zmíněný master klíč).

Se síťovým klíčem může pracovat aplikační, síťová i MAC vrstva, naproti tomu s linkovým a master klíčem je oprávněna nakládat pouze APS podvrstva. [18]

5 Bluetooth Low Energy (BLE)

5.1 Technologie Bluetooth

Bluetooth je otevřený proprietární standard pro bezdrátovou komunikaci mezi dvěma a více elektronickými zařízeními. Byl vytvořen v roce 1994 společností Ericsson jako bezdrátová náhrada za sériové kabelové rozhraní RS-232. Vývoj a specifikace následně převzala skupina Bluetooth Special Interest Group (SIG), a jak je zřejmé z tabulky č. 6, její působení se dá považovat za velice úspěšné. [21]

Tab. 6: Chronologický přehled verzí Bluetooth

Verze Bluetooth	Hlavní přínosy
1.0, 1.0B	Uvedení technologie do praxe
1.1	Oprava chyb, možnost nešifrovaných kanálů,
1.2	Uvedení AFH (viz kap. 6.1.1), zvýšení rychlosti na 721 kbps
2.0 + EDR	Zvýšení rychlosti na 2,1Mbps (EDR – enhanced data rate)
2.1 + EDR	Uvedení jednoduchého bezpečného párování (viz kap. 6.1.3)
3.0 + HS	AMP – spojení přes Bluetooth, přenos dat přes Wi-Fi (až 24 Mbps)
4.0	Rozdělení na BT Classic, BT High Speed a BT Low Energy

4.1	SW vylepšení předešlé verze reflektující zavádění 4G sítí (LTE)
4.2	Zaměřeno na fenomén internetu věcí (Internet of Things, IoT)

Technologii Bluetooth definuje standard IEEE 502.15.1.Řadí se mezi osobní počítačové sítě, tzv. PAN (Personal Area Network).

5.1.1 Rádiové rozhraní

Bluetooth využívá volně dostupného pásma ISM o frekvenci 2,4 GHz (resp. 2,402-2,480 GHz), stejně jako např. Wi-Fi. K přenosu dat využívá tzv. adaptive frequency hopping (AFH), tedy přelaďování mezi 79 frekvencemi o šířce pásma 1 MHz – během jedné sekundy je provedeno až 1600 skoků. Cílem tohoto mechanismu je zvýšení odolnosti spojení vůči rušení jinými přenosy využívajícími stejné frekvence. Bluetooth může pracovat na několika výkonových úrovních (1 mW, 10 mW a 100 mW), které umožňují komunikaci na vzdálenost od 1 metru až do 100 metrů (ve volném prostoru). [22]

5.1.2 Bluetooth protokoly

Ve srovnání s Wi-Fi Bluetooth používá podobný způsob ad-hoc komunikace, ale zatímco Wi‑Fi pracuje na linkové vrstvě referenčního modelu ISO/OSI a neřeší typ přenášeného protokolu, Bluetooth pracuje i vyššími (až aplikačními) vrstvami tohoto modelu. Z toho vyplývá nutnost definovat pro každé zařízení konkrétní protokol, přes který bude probíhat vzájemná komunikace.

Existuje několik základních protokolů, jako náhradní kabelový protokol a protokol o příjmu, a také několik protokolů povinných pro každé zařízení – LMP, L2CAP a SDP. Dále jsou všeobecně podporovány protokoly HCI a RFCOMM. Podrobnější popis jednotlivých Bluetooth protokolů je uveden níže. [22]

LMP – protokol určený k řízení rádiového spojení mezi dvěma zařízeními. Je realizován pomocí řadiče.

L2CAP – slouží k multiplexnímu spojení mezi dvěma zařízeními, přičemž využívá různých protokolů vyšší úrovně. Spolehlivost zajišťuje opakovaný přenos jedním kanálem a CRC kontrola.

SDP – umožňuje Bluetooth zařízení vyhledávat služby podporované dalšími zařízeními včetně jejich parametrů (např. podporované profily), takže je zajištěna správnost vzájemného propojení.

HCI – protokol zajišťující komunikaci mezi hostitelem (PC, mobilní zařízení) a řadičem Bluetooth.

RFCOMM – radiofrekvenční komunikace sloužící jako náhrada kabelového protokolu RS-232. Souží k vytvoření virtuálního sériového datového toku.

Další široce používané protokoly jsou např. AVCTP pro přenos audio/video komunikačních příkazů skrze kanál L2CAP nebo AVDTP pro přenos zvuku do stereo sluchátek s mikrofonem. Bluetooth podporuje i některé standardy vytvořené jinými organizacemi, např. P2P protokol, TCP/IP/UDP nebo OBEX – objektově výměnný protokol.

5.1.3 Párování Bluetooth zařízení

Každé Bluetooth zařízení poskytuje na vyžádání jiným zařízením informace o názvu a třídě zařízení, seznamu poskytovaných služeb a další technické informace, jako je funkce zařízení, informace o výrobci a používaná Bluetooth specifikace. Dále je možné nakonfigurovat zařízení tak, aby odpovídalo na další specifické dotazy. Konkrétní poskytovaná služba může z bezpečnostních důvodů vyžadovat párování nebo potvrzení od majitele zařízení. Každé zařízení je jednoznačně identifikováno pomocí unikátní 48-bitové adresy, ale uživatelům se v praxi zobrazují konfigurovatelné názvy zařízení (např. výrobce a model konkrétního zařízení).

Protože služby využívající ke komunikaci Bluetooth mohou operovat se soukromými daty, případně ovládat připojená zařízení, je žádoucí poskytnout uživateli kontrolu nad připojovanými zařízeními. V určitých situacích je naopak vhodné zajistit automatické spojení bez zásahu uživatele. Tento problém řeší právě zmíněné párování – lze nastavit, aby po provedení prvního párovacího procesu nebylo párování nadále využíváno a k navázání spojení docházelo automaticky.

Samotné párování funguje na principu sdíleného utajení. Během párovacího procesu dojde k vytvoření společného klíče, který se poté uloží v obou zařízeních. Na základě tohoto klíče může být navázané spojení šifrováno a chráněno proti odposlechu. Po vymazání klíče z jednoho zařízení dojde k zániku ověřeného spojení a je nutné párovací proces opakovat.

Párovací mechanismy obecně vyžadují určitý stupeň spoluúčasti uživatele. Níže jsou popsány různé způsoby, jakými může být spoluúčast realizována: [22]

- **Dědičné párování** – pouze pro verze Bluetooth 2.0 a starší. Spočívá v zadání PIN kódu v podobě 16-bitového řetězce do obou zařízení, v případě shody kódů v obou zařízeních je spárování úspěšné.
- **Jednoduché bezpečné párování** – využívá kryptografie s veřejným klíčem a má následující režimy:
    - **Přímé párování** – nevyžaduje spolupráci uživatele, i když může být vyzván k potvrzení párovacího procesu. Využívá se u zařízení s omezenými možnostmi vstupu/výstupu (např. bezdrátová sluchátka).
    - **Numerické párování** – předpokládá přítomnost displeje na obou zařízeních, na kterých se zobrazí 6-místný číselný kód. V případě jejich shody uživatel potvrdí dokončení párovacího procesu a spojení může být navázáno.
    - **Metoda přístupového klíče** – využití pro spárování jednoho zařízení s displejem a druhého s numerickou klávesnicí, případně dvou zařízení s numerickou klávesnicí. Na klávesnici je třeba zadat 6-místný kód zobrazený na displeji druhého zařízení, respektive je třeba zadat stejný kód na obou klávesnicích.
    - **Mimopásmová metoda** – k výměně informací nutných k procesu párování využívá externích komunikačních prostředků (např. NFC).

5.2 Charakteristické vlastnosti BLE

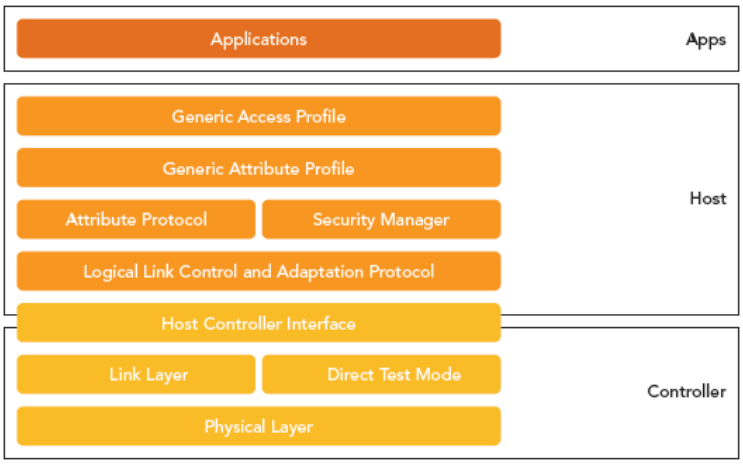
Specifikace BLE vznikla jako odpověď SIG na několik sílících trendů v oblasti konektivity, zejména na implementaci bezdrátové komunikace do zařízení, která byla tradičně propojena kabely, nebo nebyla propojena vůbec – nejvýrazněji se tento trend projevuje v oblasti přenosných zařízení (mobilní telefony, chytré hodinky, fitness náramky a další nositelná elektronika, ale i nejrůznější tagy pro komunikaci na blízkou vzdálenost). Největším problémem těchto zařízení je v současnosti jejich provoz na baterie s omezenou kapacitou, což klade nároky na nízkou energetickou náročnost bezdrátového spojení. Rozšiřování bezdrátové komunikace do množství nových zařízení s sebou nese také tlak na co nejnižší cenu.

BLE na základě těchto požadavků nabízí řešení pro jednoduché bezdrátové spojení mezi zařízeními, která vyžadují nízkou spotřebu energie a jsou dostatečně levná. Nejedná se přitom o univerzální technologii – její využití spočívá v navazování spojení k přenosu malých objemů dat na relativně krátkou vzdálenost. Tabulka č. 7 ukazuje spotřebu elektrického proudu v odlišných pracovních módech. [23]

Tab. 7: Spotřeba elektrického proudu BLE čipem (konkrétní hodnoty se liší dle vlastností spojení)

Pík	Klidový stav	Průměrný el. proud
desítky mA	desítky nA	~µA

Nízké energetické náročnosti BLE dosahuje pomocí jednoduché architektury linkové vrstvy, navržené speciálně pro navazování rychlých spojení. Většinu času BLE čipy stráví v režimu spánku, aktivní jsou jen v případě přijímání/odesílání dat. Důležitou roli hraje v BLE čipech kontrolér, který aktivuje hostitele jen v případě potřeby – vzhledem k větší energetické náročnosti hostitele oproti kontroléru to umožňuje ušetřit značné množství energie. Architektura BLE čipu je na obrázku č. 17. Další významnou vlastností BLE je přizpůsobitelná délka zpráv – odeslání delšího paketu je úspornější než odesílání několika paketů po sobě.



Obr. 17: Architektura BLE čipu (zdroj: [23])

BLE umožňuje 2 typy implementace: [23]

- **Single Mode** – nízká energetická náročnost je implementována samostatně (stand-alone).
- **Dual Mode** – nízkoenergetická funckionalita je integrována do čipů podporujících jak BLE, tak klasický Bluetooth.

Co se týče interoperability, single-mode čipy pracují pouze s dalšími single-mode nebo dual-mode zařízeními, s klasickým Bluetooth nikoli. Dual-mode čipy jsou naproti tomu interoperabilní se zařízeními s jakoukoli verzí Bluetooth technologie.

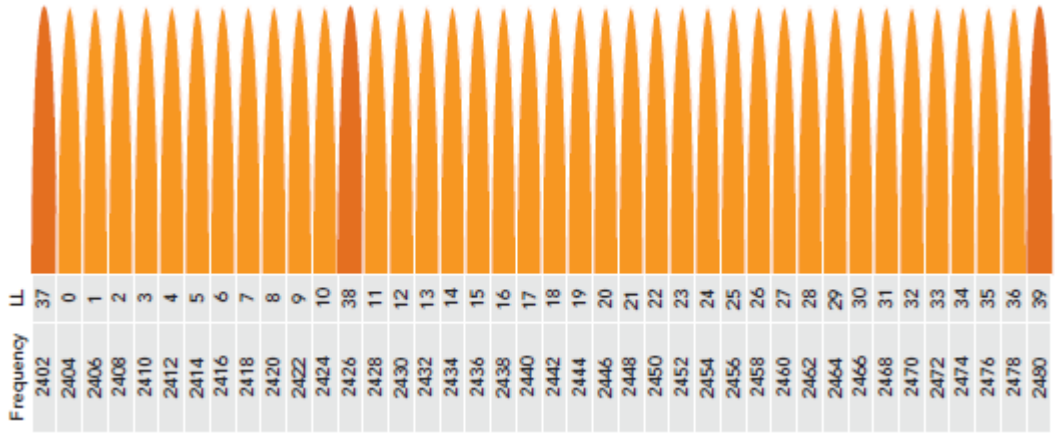
5.3 Specifikace BLE

Tabulka č. 8 [22] [23] porovnává specifikace klasického Bluetooth a BLE. Rozdíly mezi nimi jsou podrobněji popsány dále.

Tab. 8: Porovnání specifikací klasického Bluetooth a BLE

Technická specifikace	Klasické Bluetooth	BLE
Frekvence	2400-2483,5 MHz	2400-2483,5 MHz
Modulace	Frequency Hopping	Frequency Hopping
Modulační schéma	GFSK	GFSK
Modulační index	0,35	0,5
Počet kanálů	79	40
Šířka pásma	1 MHz	2 MHz
Přenosová rychlost	1-3 Mbps	1 Mbps
Propustnost	0,7-2,1 Mbps	< 0,3 Mbps
Latence	100 ms	3-6 ms
Dosah	10 m	až 60 m
Počet aktivních klientů	7	neomezeno
Zabezpečení	56 až 128-bitové	128-bitové (AES)
Robustnost	FHSS	FHSS
Přenos hlasu	Ano	Ne

Klasické Bluetooth i BLE používají stejný frekvenční rozsah a mechanismus přeladování frekvencí, ale rozdíl je v počtu používaných kanálů (79, resp. 40) a šířce jednoho pásma (1 MHz, resp. 2 MHz). Kanály BLE ilustruje obrázek č. 18. Zatímco klasické Bluetooth používá pro vyhledávání ostatních zařízení 32 kanálů (tzv. advertising channels), BLE pro tento účel používá pouze 3 kanály. Redukce počtu vyhledávacích kanálů má za následek výrazné snížení spotřeby elektrické energie – BLE stačí k vyhledání ostatních zařízení v jednom cyklu 0,6-1,2 ms, klasické Bluetooth musí být ze stejného důvodu aktivní po dobu 22,5 ms.



Obr. 18: Frekvenční kanály BLE (tmavě jsou označeny vyhledávací kanály) (zdroj: [23])

Použití tří vyhledávacích kanálů na druhou stranu snižuje robustnost technologie – roste pravděpodobnost rušení jiným spojením, které využívá stejnou frekvenci. Aby se tato pravděpodobnost snížila, byly pro vyhledávací kanály zvoleny frekvence umístěné přesně mezi kanály používané Wi-Fi technologií.

5.3.1 BLE protokol

Klasické Bluetooth operuje s devíti různými protokoly. BLE naproti tomu pracuje pouze s protokolem ATT – zjednodušenou modifikací SDP protokolu. ATT funguje sekvenčně – zpracovává najednou jen jeden požadavek. Používá architekturu klient-server, která jednoduše umožňuje klientovi číst/zapisovat informace poskytované serverem za snížené spotřeby elektrické energie. [23]

5.3.2 Datové formáty – BLE pakety

BLE pakety mají pevně danou strukturu a rozdělují se na dva typy – vyhledávací a datové pakety (advertising and data packets).

Preamble (1 octet)	Access Address (4 octets)	PDU (2 to 39 octets)	CRC (3 octets)

Obr. 19: Struktura BLE paketu (zdroj: [23])

Jak je vidět z obrázku č. 19, BLE paket se skládá z těchto částí:

- **Hlavička** – pro účely synchronizace.

- **Přístupová adresa** – slouží ke směrování každého paketu do daného připojeného zařízení v rámci fyzické vrstvy. Délka 4 B umožňuje v závislosti na počtu kombinací připojení až miliard různých zařízení.
- **PDU (Protocol Data Unit)** – jednotka přenášených dat. Může nabývat délky 2-39 B.
- **CRC (Cyclic Redundancy Check)** – zajišťuje správnost dat obsažených v PDU.

6 Porovnání BLE a ZigBee

Obě popsané technologie splňují požadavky navrhovaného systému z hlediska nízké spotřeby elektrické energie a relativně nízkých nákladů na pořízení a následný provoz. Podle tabulky č. 9 jsou si obě bezdrátové technologie podobné i dalšími technickými parametry. [18] [23]

Tab. 9: Porovnání specifikací ZigBee a Bluetooth Low Energy

Technická specifikace	ZigBee	BLE
Frekvence	784, 868, 915, 2 400 MHz	2 400 MHz
Šířka pásma	0,3; 0,6; 2 MHz	2 MHz
Přenosová rychlost	250 kbps	1 Mbps
Dosah	Až 100 m	až 60 m
Počet připojených uzlů	Až 65 000	Až 8
Typy sítí	Hvězda, síť, strom	P2P, piconet
Robustnost	Direct Spread Spectrum	Frequency Hopping

Klíčovým rozdílem mezi nimi je jejich primární určení – ZigBee se hodí pro výstavbu sítí LAN sestávajících ze senzorů a ovladačů, zatímco Bluetooth Low Energy je určena spíše pro sítě typu PAN, typicky pro spojení periferií s počítačem, případně mobilním telefonem – ať už se jedná o bezdrátová sluchátka nebo chytré hodinky.

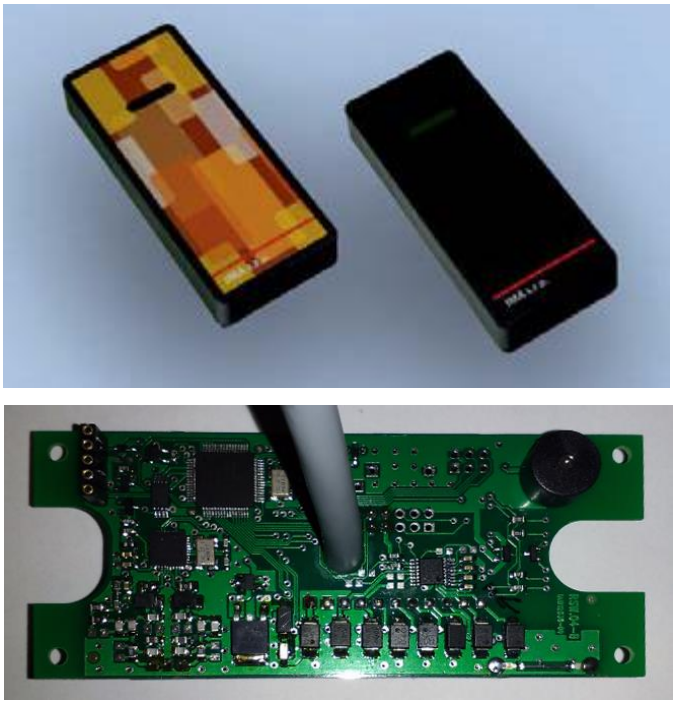
Vzhledem k architektuře celého přístupového systému, ve které je důležitým prvkem mobilní telefon, se jeví jako výhodnější varianta BLE. Technologie Bluetooth je totiž v současné době implementována v naprosté většině mobilních telefonů, zatímco konkurenční ZigBee si do nich cestu prozatím nenašla. Pro BLE mluví rovněž fakt, že spojení navazované prostřednictvím bezdrátové technologie mezi uživatelem, resp. jeho telefonem, a čtečkou karet je výhradně v režimu P2P. Protokol ZigBee umožňující stavět sítě mnohem většího rozsahu je v tomto případě zbytečně robustní.

Výše zmíněné důvody proto vedly k rozhodnutí implementovat do navrhovaného systému technologii BLE, a přizpůsobit tomu další prvky systému, zejména návrh mobilní aplikace a vybavení čteček BLE modulem.

7 Čtečka přístupových karet

V přístupovém systému, který je předmětem této práce, se jedná o nasazení čteček typu RSW.04 od společnosti IMA (Institut mikroelektronických aplikací). Tato čtečka je určena pro čtení zabezpečených informací z bezkontaktních karet vyhovujících standardu ISO/IEC 14443 (MIFARE Classic, MIFARE DESFire, FeliCA apod.). Standardní verze čtečky podporuje komunikaci ve všech třech režimech NFC (čtení/zápis, peer-to-peer, card emulation).

Konstrukčně čtečka sestává z elektroniky, která je zabudována v odolném plastovém krytu. Na přední straně krytu je okénko pro indikační LED zelené a červené barvy – diody včetně akustické signalizace jsou řízeny dle požadavků nadřazeného systému. Vnější i vnitřní část čtečky ilustruje obrázek č. 20. [24]



Obr. 20: Vnější podoba čtečky RSW.04 (nahoře) a její vnitřní elektronická část (zdroj: [24], foto dole: IMA s.r.o.)

Technické parametry čtečky typu RSW.04 shrnuje tabulka č. 10: [24]

Tab. 10: Technické parametry čtečky RSW.04

Parametr	Hodnota
Pracovní frekvence	13,56 MHz
Čtecí vzdálenost (MIFARE DESFire)	4,5 cm
Komunikační rozhraní	Wiegand, RS-232
Napájecí napětí	9-15 V
Spotřeba	120 mA (typická)
Pracovní teplota okolí	Od -25 do +60 ºC
Stupeň krytí	IP65
Materiál krytu	ABS
Rozměry	117 x 44 x 20 mm

Je zřejmé, že čtečka tohoto typu je vhodná pro umístění jak v interiérech, tak v exteriérech. Čtečka je navíc vybavena ochranou proti neoprávněné manipulaci v podobě zabudovaného tamperu.

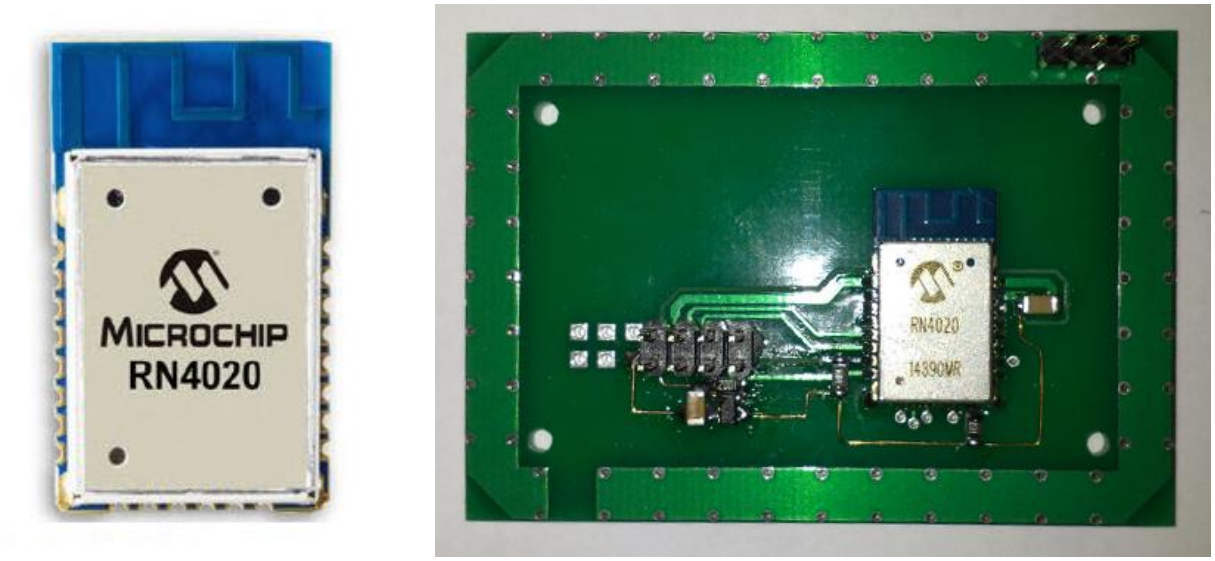
7.1 Čip RN4020

Pro účely navrhovaného přístupového systému je však nutné čtečku vybavit BLE modulem, která umožní komunikaci s mobilním telefonem na vzdálenost desítek metrů (teoreticky až 100 m, záleží na konkrétních podmínkách pro šíření signálu).

Výrobce čteček, společnost IMA, takto modifikovanou čtečku rovněž vyvíjí. Je osazena BLE modulem RN4020 (Obrázek 21 vlevo), který vyhovuje specifikaci Bluetooth ve verzi 4.1. Na ploše čipu je integrována RF anténa, frekvenční kontrolér, analogově digitální převodník a procesor zpracovávající ASCII příkazy dle API. Technické specifikace jsou uvedeny v tabulce č. 11. [25]

Tab. 11: Technické parametry BLE modulu RN4020

Parametr	Hodnota
Pracovní frekvence	2,402-2,480 MHz
Frekvenční kanály	0-39
Metoda modulace	GMSK
Přenosová rychlost	Až 1 Mbps
Operační vzdálenost	Až 100 m
Komunikační rozhraní	UART, PIO, AIO, SPI
Napájecí napětí	1,8-3,6 V
Spotřeba	12 mA (typická)
Pracovní teplota okolí	Od -30 do 85 ºC
Rozměry	11,5 x 19,5 x 2,5 mm



Obr. 21: Horní pohled na BLE modul RN4020 (vlevo), umístění modulu RN4020 na desce čtečky RSW.04 (zdroj: [25], foto vlevo: IMA s.r.o.)

Na obrázku č. 21 vpravo je snímek ilustrující napojení modulu RN4020 na desku s elektronikou čtečky typu RSW.04 (konkrétně na části s RF anténou, která je umístěna nad odvrácenou stranou desky z dolní části obrázku č. 20).

8 Přístupový systém

Čtečky bezkontaktních přístupových karet jsou součástí centrálně řízeného systému s distribucí přístupových práv v režimu semi-online. Následující části popisují jeho strukturu a použité technologie.

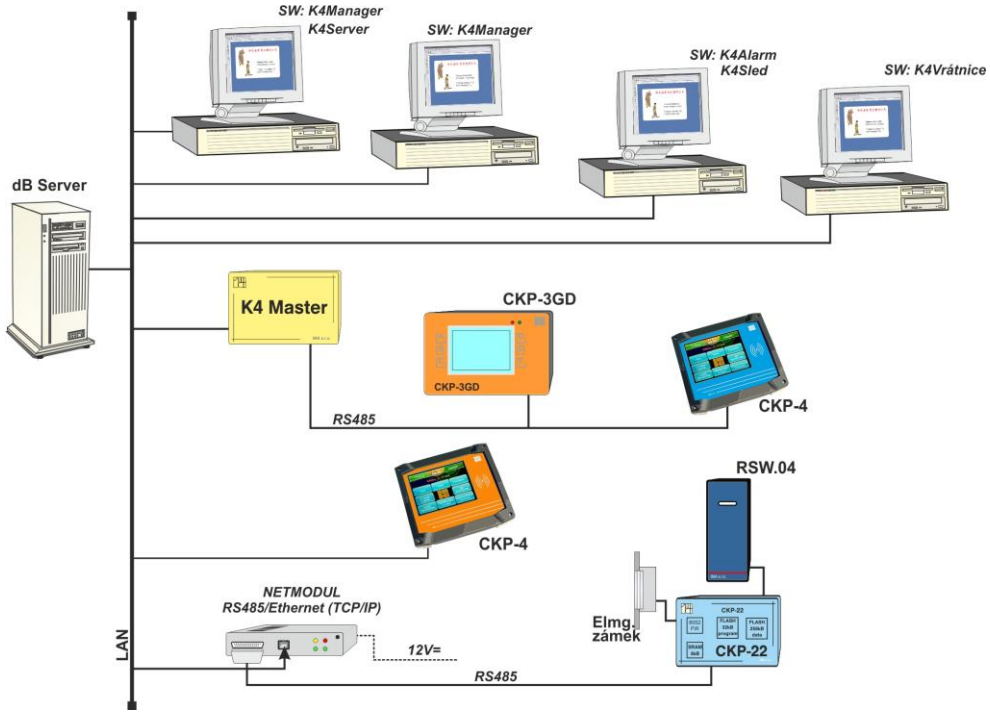
8.1 Struktura

Hlavním řídícím prvkem celého systému je centrální server napojený na databázi, která obsahuje veškeré informace o přístupových kartách v systému, tj. přístupová práva, seznam blokovaných karet (blacklist), seznam karet s univerzálními přístupovými právy apod. Databáze je spravována prostřednictvím softwarových nástrojů na správcovských klientech, které jsou přímo propojeny s databázovým serverem.

Mezi serverem a samotnou čtečkou jsou rozmístěny tzv. mastery, které dostávají aktualizované informace o přístupových právech z centrální databáze v pravidelných časových intervalech, jejichž délka se dá variabilně nastavovat. Tyto mastery jsou dále spojeny s přístupovými terminály, které můžou být trojího typu:

- Terminál s displejem a s pamětí pro informace o přístupových právech – nemusí se při každém pokusu o přístup dotazovat masteru na přístupová práva konkrétního uživatele; kromě povolení/odmítnutí přístupu lze také na displeji blíže specifikovat okolnosti příchodu/odchodu (např. přestávka, lékař aj., což je praktické při použití terminálu jako systému na evidenci docházky zaměstnanců).
- Terminál s displejem bez paměti pro informace o přístupových právech – oproti předchozímu typu se musí na přístupová práva pokaždé dotázat nadřízeného masteru, jinak je jeho funkcionalita obdobná.
- Terminál bez displeje, na který jsou napojeny čtečky bezkontaktních karet a elektromagnetické dveřní zámky – pro svou relativní jednoduchost v praxi nejčastěji nasazovaný typ terminálu, který je vhodný pro řízení přístupu do konkrétních místností, oblastí budovy nebo např. do podzemních garáží. Stejně jako terminál předchozího typu se na přístupová práva pokaždé dotazuje nadřízeného masteru. S modifikací tohoto typu terminálu, resp. na něj napojených čteček, počítá i řešení navrhované v rámci této diplomové práce.

Kvůli limitům komunikačního rozhraní je pro zabezpečení bezproblémové komunikace s jedním masterem propojeno maximálně 32 terminálů. Strukturu přístupového systému znázorňuje obrázek č. 22.



Obr. 22: Struktura přístupového systému (zdroj: IMA s.r.o.)

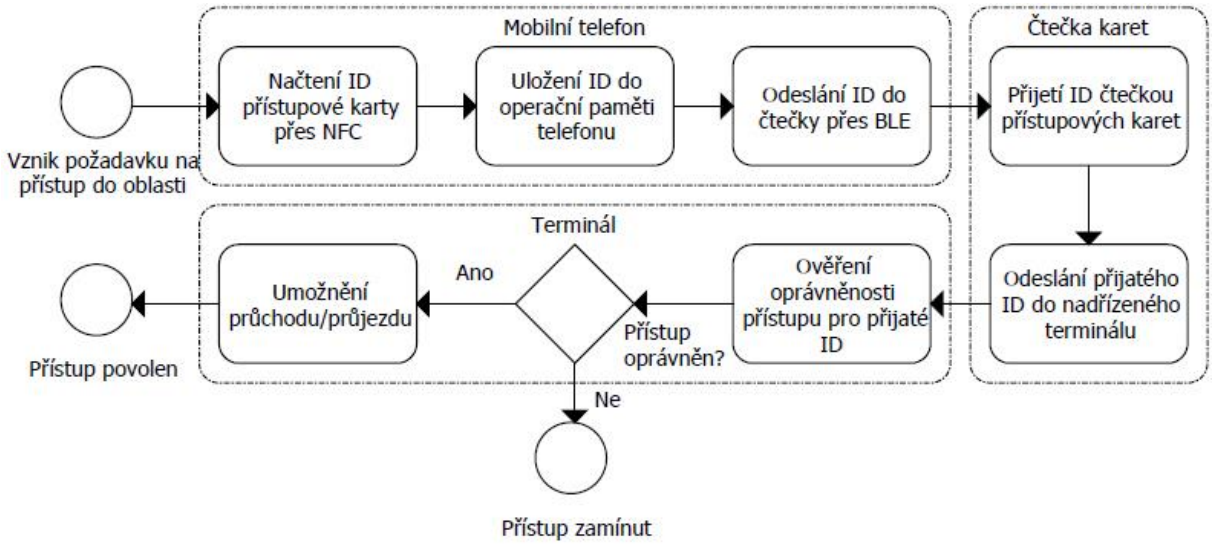
8.2 Technologie

Z technologického hlediska je systém postaven na standardních a osvědčených řešeních. Na centrálním serveru běží SQL databáze, která je se správcovskými klienty a mastery (případně přímo s terminály) spojená přes Ethernetovou LAN. Operačním systémem mezilehlých masterů je Linux a s koncovými terminály komunikují přes dvouvodičové poloduplexní sériové spojení dle standardu RS-485. Maximální délka sběrnice je až 1200 m a počet uzlů na ní je 32, jak již bylo uvedeno výše; s použitím opakovačů jich může být i více, což ale přináší zvýšené riziko kolizí. Teoretická přenosová rychlost na krátké vzdálenosti (do 10 m) činí 10 Mbps.

9 Komunikace v rámci navrhovaného systému

9.1 Procesní model komunikace

Následující ilustrace (obrázek č. 23) zachycuje procesní model komunikace probíhající v rámci navrhovaného přístupového systému. Podrobný popis jednotlivých kroků následuje v dalších kapitolách.



Obr. 23: Procesní model komunikace v rámci navrhovaného přístupového systému (zdroj: autor)

9.2 Bezkontaktní karta – mobilní telefon (NFC)

V navrhovaném přístupovém systému se předpokládá nasazení bezkontaktních karet (PICC) typu MIFARE DESFire EV1 4k s podporou 128bitového šifrování AES. Z hlediska komunikačních protokolů podle standardu ISO/IEC 14443 se jedná o typ A. Jako čtečka (PCD) bezkontaktní karty poslouží mobilní telefon s NFC čipem, který bude pracovat v režimu čtení/zápis. Mobilní telefon tedy poskytne energii pro napájení bezkontaktní karty prostřednictvím generovaného magnetického pole, přičemž karta bude odpovídat jeho modulací. Parametry komunikace, které stanoví druhá část zmíněného standardu, shrnuje tabulka č. 12. [26]

Tab. 12: Parametry komunikace pro rozhraní typu A podle ISO/IEC 14443-2

Směr komunikace	Kódování	Frekvence	Rychlost [kbps]
PCD → PICC	Modifikované Millerovo (ASK 100%)	f_c = 13,56 MHz	106
PICC → PCD	Manchester (OOK 10%)	$f_c/16$ = ~847 kHz	106

9.2.1 Inicializace

Třetí část výše zmíněného standardu, tedy ISO/IEC 14443-3, podrobně popisuje průběh inicializace včetně antikolizního mechanismu pro případ, že by se v magnetickém poli

generovaném aktivním zařízením nacházelo více kompatibilních bezkontaktních karet. Algoritmus zajistí simultánní komunikaci čtečky s více kartami, aniž by došlo ke vzájemnému rušení. Tato situace může v rámci navrhovaného systému nastat například při současném průjezdu uživatelů v opačných směrech. Inicializační proces je popsán v tabulce č. 13. [27]

Tab. 13: Příklad inicializace komunikace mezi čtečkou a kartou typu A podle ISO/IEC 14443-3

PCD	Směr komunikace	PICC
REQA (0x26)	→	
	←	PICC #1: ATQA (10000000 00000000) PICC #2: ATQA (10000010 00000000)
Čtečka vyšle příkaz REQA ve formě krátkého rámce, aby otestovala přítomnost kompatibilních bezkontaktních karet ve své blízkosti; v tomto případě se v něm nacházejí dvě – PICC #1 a PICC #2, které současně reagují odpovědí ATQA; čtečka proto zahájí první část antikolizní sekvence, tzv. cascade level 1.		
SEL (0x93), NVB (0x20)	→	
	←	PICC #1: uid0 (00001000), uid1, uid2, uid3, BCC PICC #2: CT (00010001), uid0, uid1, uid2, BCC
Čtečka odešle tzv. antikolizní příkaz, který specifikuje cascade level (hodnota SEL) a počet platných bitů UID, který čtečka dosud zachytila a případně je pro kontrolu odešle zpět k PICC (hodnota NVB – 0x20 znamená, že neodešle žádnou část UID); následně obě karty odpoví odesláním kompletních UID (PICC #1 má UID velikosti single, PICC #2 velikosti double, a protože se jedná o cascade level 1, odešle PICC #2 před svým UID navíc tzv. cascade tag; BCC je kontrolní byte UID pro daný cascade level) – je zřejmé, že první kolize nastane na pozici čtvrtého bitu.		
SEL (0x93), NVB (0x24), (0001)	→	
	←	PICC #2: (0001), uid0, uid1, uid2, BCC
Čtečka odešle další antikolizní příkaz spolu s částí UID obdrženou před kolizí doplněnou o bit hodnoty 1, hodnota NVB tedy bude 0x24; tyto 4 bity odpovídají prvním bitům UID PICC #2 (cascade level 1) – tím je vyloučena PICC#1 a PICC #2 může bez rizika kolize odeslat zbývající část svého UID (CL1).		
SEL (0x93), NVB (0x70), CT (00010001), uid0, uid1, uid2, BCC, CRC_A	→	
	←	SAK (xx1xxxxx), CRC_A

Čtečka nyní zná kompletní UID (CL1) PICC #2, příkazem tedy vybere PICC #2; karta potvrdí výběr odesláním odpovědi SAK, a protože třetí odeslaný bit má hodnotu 1, dá tím čtečce najevo, že její UID pokračuje v dalším cascade levelu (CL2); CRC_A je cyklická kontrola redundance.		
SEL (0x95), NVB (0x20)	→	
	←	uid3, uid4, uid5, uid6, BCC
SEL (0x95), NVB (0x70), uid3, uid4, uid5, uid6, BCC, CRC_A	→	
	←	SAK (xx0xxxxx), CRC_A
Čtečka zvýší úroveň casacde levelu z CL1 na CL2 (hodnota SEL se změní) a resetuje hodnotu NVB na 0x20, čímž donutí kartu odeslat své kompletní UID CL2; ta je odešle a čtečka následně příkazem vybere kartu, která potvrdí výběr odpovědí SAK, a protože třetí odeslaný bit má hodnotu 0, UID je kompletní a nepokračuje do CL3. Karta je nyní v aktivním stavu a je připravena k další komunikaci.		

Poznámka:
Hodnoty uvedené v tabulce s prefixem 0x (např. 0x95) jsou v hexadecimální soustavě, hodnoty v závorkách v soustavě binární (XX) – bit vlevo je prvním odvysílaným bitem a je tedy bitem s nejmenším významem (LSB).

V tomto okamžiku zná čtečka UID bezkontaktní karty, které je na kartě předprogramováno výrobcem a v zájmu zajištění jeho unikátnosti je chráněno proti přepisování. V současné době je toto UID v rámci ČVUT používáno jako jednoznačný identifikátor, jeho čtení však není kryptograficky chráněno. V budoucnu se předpokládá vytvoření struktury aplikací podle specifikací pro daný typ bezkontaktní karty. Identifikátor pak bude uložen na kartě v podobě souboru a bude součástí příslušné aplikace.

Po úspěšné inicializaci je karta v aktivním stavu a je připravena na komunikaci se čtečkou, v tomto případě s mobilním telefonem s aktivovaným NFC čipem v režimu čtení/zápis. Po výběru konkrétní aplikace proběhne autentizace na základě klíče přiřazeného k této aplikaci. Ta probíhá u karet typu MIFARE DESFire EV1 trojcestně (tzv. 3 pass authentication). Její průběh se dle použité kryptografické metody v některých detailech liší, princip je ale vždy stejný. Výběr aplikace a autentizace pomocí metody AES popisuje tabulka č. 14. [7]

Tab. 14: Výběr aplikace a autentizace před zahájením čtení souborových dat

PCD	Směr komunikace	PICC
0x5A (1 B), AID (3 B)	→	

	←	• Error code (1 B) • 0x00 (1 B), MAC
Komunikaci vždy iniciuje čtečka. Vyšle příkaz SelectApplication (0x5A), který obsahuje ID konkrétní aplikace o délce 3 B (AID). Pokud je požadovaná aplikace přítomna na kartě, karta potvrdí výběr odpovědí 0x00 – v opačném případě odešle čtečce chybové hlášení.		
0xAA (1 B), keyNo (1 B)	→	
	←	• Error code 0x40 (1 B) • 0xAF (1 B), ekNo (RndB) (16 B)
V dalším kroku dojde k zahájení autentizace. Čtečka vyšle příkaz AuthenticateAES, který sestává z kódu pro autentizaci metodou AES (0xAA) a vybraného klíče pro konkrétní aplikaci, případně klíče platného pro celou kartu (tzv. Master key, 0x00). Pokud vybraný klíč není uložen v paměti karty, karta odešle chybové hlášení (NO_SUCH_KEY – 0x40). V případě přijetí platného klíče karta vygeneruje náhodné číslo (RndB), zašifruje jej pomocí přijatého klíče a odešle zpět do čtečky (ekNo (RndB)). 0xAF (ADDITIONAL_FRAME) indikuje, že budou následovat další informace.		
0xAF (1 B), ekNo (RndA+RndB‘) (32 B)	→	
	←	• Error code (1 B) • 0x00 (1 B), ekNo (RndA**‘**) (16 B)
Po přijetí ekNo (RndB) čtečka provede dešifrování pomocí stejného klíče, čímž získá náhodné číslo RndB. Poté provede modifikaci RndB posunutím o 1 byte doleva – tím vznikne modifikované náhodné číslo RndB‘. Následně čtečka vygeneruje náhodné číslo RndA o stejné délce jako RndB a přidá je k RndB‘. RndA+RndB‘ je poté zašifrováno vybraným klíčem a odesláno do karty (ekNo (RndA+RndB‘)). Karta provede dešifrování přijatého řetězce a porovná získané RndB‘ s původním RndB posunutém o 1 byte doleva. V případě shody má karta jistotu, že se čtečkou sdílí stejný klíč (v opačném případě zastaví autentizační proces a odpoví chybovým hlášením). Nakonec ještě pošle čtečce modifikované číslo RndA‘, která je porovná s interně modifikovaným RndA‘ – v případě shody má i čtečka jistotu o sdílení stejného klíče (v opačném případě zastaví autentizační proces).		

Pokud autentizace proběhne úspěšně, dojde k vygenerování klíče pro probíhající relaci. V případě šifrování metodou AES je tento klíč sestaven podle tohoto principu: [7]

AES session key = RndA byte 0-3 + RndB byte 0-3 + RndA byte 6-9 + RndB byte 6-9 + RndA byte 12-15 + RndB byte 12-15

Poté může dojít k přečtení ID, které je uloženo v příslušném souboru vybrané aplikace. Průběh čtení ID popisuje tabulka č. 15. [7]

Tab. 15: Čtení souborových dat (ID) z bezkontaktní karty NFC čtečkou

PCD	Směr komunikace	PICC
0xBD (1 B), File No (1 B), Offset (3 B), Length (3 B)	→	
	←	• Error code (1 B) • 0xAF (1 B), Data (1-59 B)
Čtečka vyšle příkaz ReadData (0xBD), který specifikuje číslo souboru, ze kterého chce číst data (číslo souboru musí být v rozmezí od 0x00 do 0x1F). Dále obsahuje informaci o tzv. offsetu, který určuje startovací pozici pro čtení v souboru (0x00 00 00 až délka souboru -1) a o délce dat, která mají být přečtena (0x00 00 00 až 0xFF FF FF) – pokud je tato hodnota nastavena na 0x00 00 00, budou přečtena všechna data v daném souboru od pozice specifikované offsetem. V případě, že daná aplikace obsahuje požadovaný soubor, odpoví odesláním příslušných dat. V opačném případě dojde k odeslání chybového hlášení.		

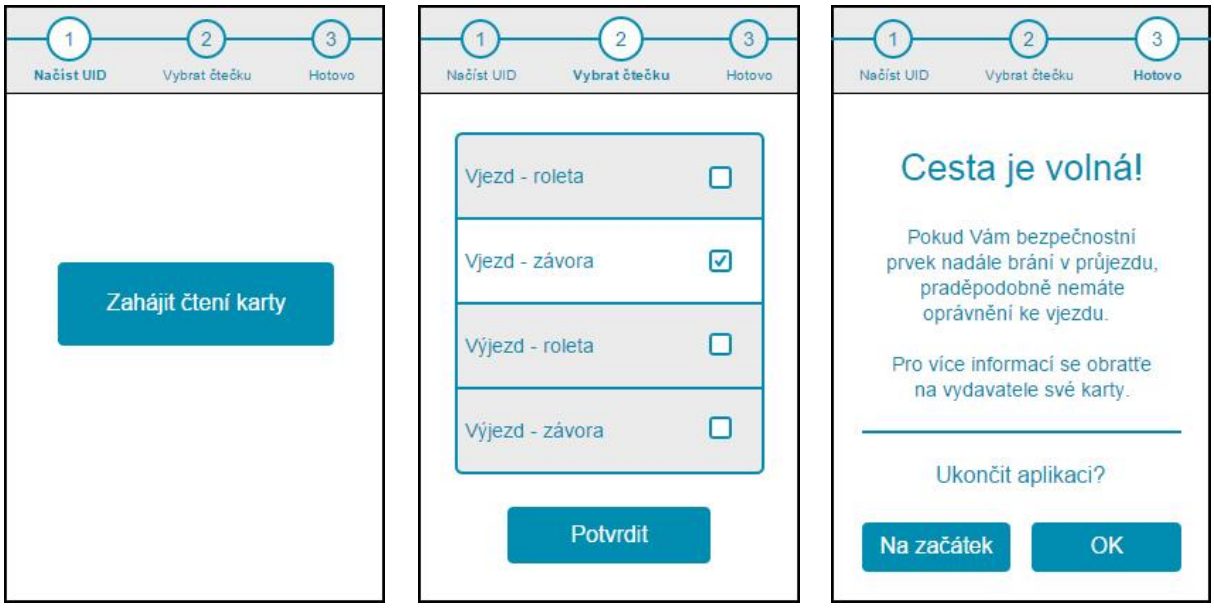
Překročí-li velikost dat odeslaných kartou v odpovědi na požadavek 59 B, čtečka po přijetí prvního rámce odešle čtečka kartě status 0xAF, který indikuje čekání na další datový rámec. Karta odešle dodatečná data ve stejné podobě jako v prvním cyklu.

9.3 Rozhraní NFC-BLE v mobilním telefonu

Unikátní ID načtené z bezkontaktní karty je dešifrováno v secure elementu NFC a je předáno dále prostřednictvím mobilní aplikace, která zajistí jeho odeslání pomocí Bluetooth Low Energy do čtečky karet napojené na přístupový systém.

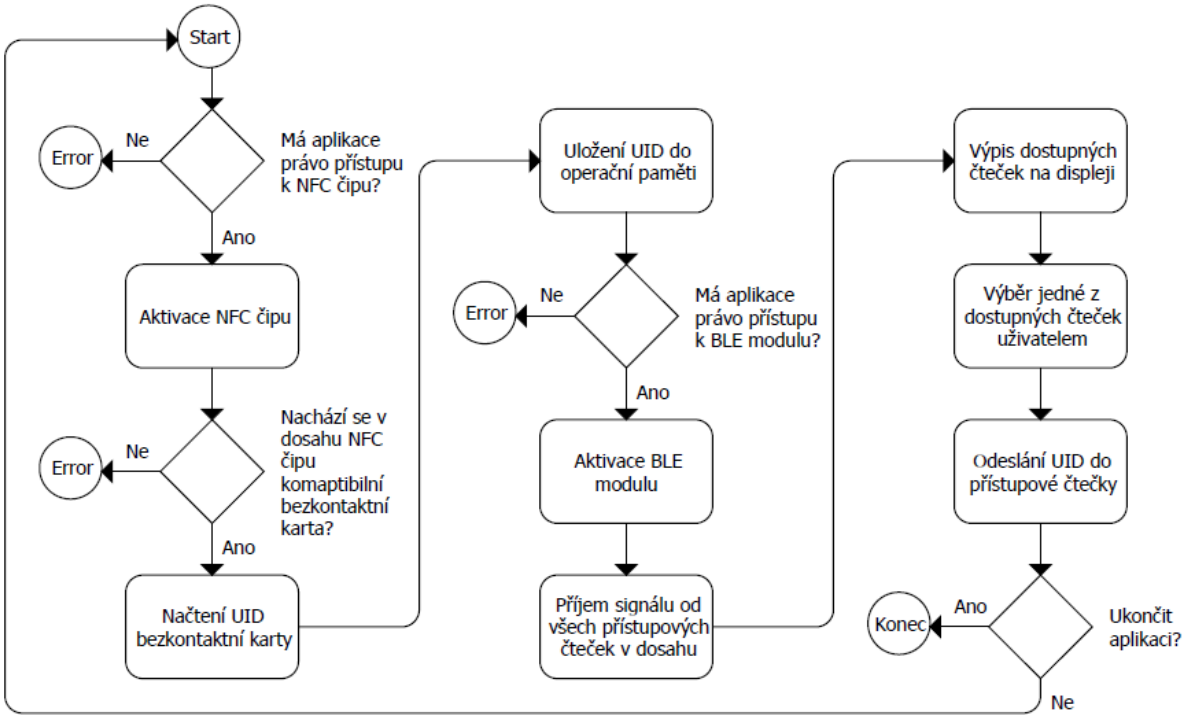
Aplikace tedy musí mít právo operovat s NFC modulem a zpracovávat jím načtené informace. Stejně tak musí mít přístup k Bluetooth modulu. Samozřejmostí pak je schopnost alokace paměti pro své operace a pro uložení načteného ID. Teoreticky je možné načtené ID zachovat v paměti telefonu, čímž by odpadla nutnost opakovaného načítání z karty, ale z hlediska bezpečnosti tato možnost využita nebude.

Z uživatelského hlediska je třeba při odbavení přístupovým systémem aplikaci v první řadě aktivovat a jejím prostřednictvím načíst pomocí NFC čipu ID bezkontaktní karty. Každá čtečka vybavená Bluetooth modulem má svou jedinečnou MAC adresu, která musí být uložena v telefonu. Vzhledem k předpokládanému použití více než jedné čtečky v dané oblasti (minimálně jedna pro každý směr) by uživatel následně zvolil jednu ze čteček, které jsou v dosahu a jejichž MAC adresy, resp. názvy, se aktuálně zobrazují na displeji telefonu. Příklad, jak by interakce uživatele s aplikací mohla vypadat, ukazuje obrázek č. 24.



Obr. 24: Ukázka uživatelského rozhraní mobilní aplikace: aktivace NFC čipu a zahájení čtení ID karty (vlevo), výběr konkrétní přístupové čtečky (uprostřed) a závěrečná nabídka na ukončení/restartování aplikace (zdroj: autor)

Poté by již došlo k navázání šifrovaného spojení mezi telefonem a čtečkou a k odeslání ID uživatelovy karty – tento krok je podrobně popsán v kapitole 10.4.



Obr. 25: Vývojový diagram popisující princip fungování mobilní aplikace (zdroj: autor)

Z funkčního hlediska je princip fungování aplikace popsán vývojovým diagramem na obrázku č. 25. Vlastní kód a samotná aplikace bude vycházet z veřejně dostupných API nejrozšířenějších mobilních operačních systémů (Android, iOS). Její realizace však překračuje rámec této diplomové práce.

9.4 Mobilní telefon-čtečka přístupových karet (BLE)

V rámci komunikace mezi čtečkou přístupových karet a mobilním telefonem přes BLE je telefon iniciátor komunikace, zatímco čtečka přístupových karet je v roli periferie. Čtečka v pravidelných časových intervalech (100-200 ms) vysílá informaci o své přítomnosti a názvu. Přenos ID uživatele zahajuje telefon připojením ke čtečce a aktivováním MLDP (Microchip's Low-energy Data Profile) – BLE profilu, který slouží k přenosu dat v podobě krátkých notifikací (maximálně 20 B, delší zprávy musí být rozděleny na úrovni uživatele). Kvůli fragmentaci dat jsou příkazy a odpovědi zapouzdřeny v rámcích, jejichž struktura je pospána v následující části.

9.4.1 Struktura rámců

- Data length (1 B) – délka přenášených dat (bez kontrolního součtu)
- Data length checksum (1 B) – (dataLength + dataLengthChecksum) = 0
- Data (1-255 B) – informace nesená daty (příkaz nebo odpověď)
- Data checksum (1 B) – (data[0] + data[1] + … + data[dataLength]) = 0x00 [28]

9.4.2 Pořadí příkazů

V navrhovaném systému se předpokládá užití standardního módu bez nutnosti zadáván PINu, pořadí příkazů tedy bude vypadat takto: [28]

1) Telefon se spojí se čtečkou a aktivuje profil MLDP
2) Instalační ID
3) Autentizace s vlastním identifikátorem
4) Potvrzení přijatého identifikátoru

Průběh komunikace popisuje tabulka č. 16. [28]

Tab. 16: Komunikace mezi mobilním telefonem a čtečkou přístupových karet přes BLE

Čtečka přístupových karet	Směr komunikace	Mobilní telefon
Installation ID (8B)	→	
	←	0x90, 0x00
V případě, že je instalační ID odeslané čtečkou shodné s ID v mobilní aplikaci, telefon jej potvrdí uvedenou odpovědí.		
3des-Enc(Random (8 B) + reader ID (4 B) + 4*0x00 (4 B); Ki) (Σ16 B)	→	
	←	3des-Dec(Random‘ (8 B) + Card number (7 B) + 4*0x00 (4 B); Ki) (Σ16 B)
Telefon uloží náhodně vygenerované číslo (Random) a zkontroluje ID čtečky. Pokud souhlasí s ID uloženým v telefonu, telefon odpoví náhodným číslem modifikovaným cyklickým posunutím původního náhodného čísla o 1 B doprava (Random‘) a ID karty. Čtyři bytová pole obsahující nuly jsou zde pro případ nutnosti zadání PINu.		
3des-Enc(reader ID (4 B) + 0x90 0x00 0x00 0x00 (4 B); Ki) (Σ8 B)	→	
	←	0x90 0x00
Posledním krokem je potvrzení přijetí ID karty.		

9.5 Přístupový systém

Posledním krokem komunikačního řetězce, který stojí za umožněním/znemožněním přístupu do dané oblasti, je ověření přístupových práv konkrétního uživatele. Čtečka odešle přijaté ID nadřízenému terminálu, který rozhodne o oprávněnosti vstupu na základě své interní databáze, která je pravidelně aktualizována ze strany serveru. Komunikace čtečky a terminálu je jednosměrná (ve směru čtečka-terminál), bezpečnostní prvek ve formě zámku/závory/rolety ovládá terminál. V případě, že je konkrétní uživatel na základě svého ID vyhodnocen jako oprávněný ke vstupu, terminál vyšle příkaz k otevření bezpečnostního prvku – v opačném případě zůstává průjezd znemožněn a z pohledu uživatele nedojde k žádné aktivitě.

10 Návrh implementace systému

Navrhovaný systém je vhodný pro umístění kdekoli, kde je klasická čtečka přístupových karet z paluby vozu hůře dostupná. To může nastat například vlivem dodatečného zavedení přístupového systému do stávajícího projektu, kde z různých důvodů není možné

optimalizovat umístění čteček pro potřeby řidičů. Může se také jednat o zabezpečenou bránu, kterou projíždí jak osobní, tak nákladní automobily a čtečka je umístěna v úrovni řidičů osobních vozů. Dalším příkladem lokality vhodné pro umístění navrhovaného systému jsou místa, která jsou zabezpečena kombinovaným systémem – vjezd je např. krytý roletou, za kterou následují bezpečnostní závory. Pokud je roleta ovládána samostatnou čtečkou, vjezd a výjezd do takto zabezpečené oblasti i z ní je o to komplikovanější. To je ostatně i případ místa, na kterém je plánován pilotní provoz celého systému. Podrobněji o něm pojednává následující kapitola.

10.1 Umístění pilotního provozu navrhovaného systému

Jako vhodná lokalita pro osazení navrhovaného systému v rámci pilotního provozu byl vytipován vjezd do podzemních garáží nové budovy ČVUT v dejvickém kampusu.

V současné době je vjezd do garáží osazen roletou, která je ovládána pomocí samostatných čteček přístupových karet. Ty jsou umístěny po stranách vjezdového koridoru – čtečka pro vjezd do garáží je připevněna na zdi před roletou, avšak na špatně dostupném místě – vpravo vzhledem k přijíždějícím vozidlům, tj. na druhé straně, než je sedadlo řidiče. Přímo naproti této čtečce je umístěna druhá čtečka, určená pro výjezd z garáží (obrázek č. 26). V případě spuštěné rolety tedy musí odjíždějící řidič roletu obejít, aby ji mohl prostřednictvím této čtečky otevřít. Roleta je přes den trvale vytažena, ale ve večerních hodinách se na noc stahuje.

Obr. 26: Umístění čteček ovládajících bezpečnostní roletu u vjezdu do podzemních garáží (foto: autor)

Kromě zmíněné rolety je vjezd do garáží zabezpečen dvojicí závor; jedna je ve směru vjezdu, druhá ve směru výjezdu z garáží. Umístění souvisejících čteček je v tomto případě logičtější – obě jsou umístěny na středovém ostrůvku (jsou tedy relativně dostupné z místa řidiče) a před závorou pro konkrétní směr (obrázek č. 27).

Obr. 27: Závory ve vjezdovém koridoru do podzemních garáží, čtečky pro jejich ovládání jsou umístěny na sloupcích uprostřed snímku (foto: autor)

10.2 Řešení systému v pilotním provozu

Návrh přístupového systému s využitím bezdrátové komunikace mezi kartou, resp. mobilním telefonem a čtečkou počítá s výměnou všech 4 čteček za typ, který je popsán v osmé kapitole. Zájemce o vjezd do garáží si prostřednictvím navržené mobilní aplikace vybere čtečku, se kterou chce navázat spojení a odešle do ní ID své přístupové karty, které předtím načetl do telefonu prostřednictvím NFC. Modelové situace běžného provozu jsou uvedeny v tabulce č. 17.

Tab. 17: Pořadí komunikace se čtečkami přístupových karet v závislosti na směru jízdy a stavu bezpečnostní rolety

Směr jízdy	Stav rolety	Pořadí komunikace se čtečkami
Do garáží	Otevřená	Závora-vjezd
Do garáží	Zavřená	Roleta-vjezd, závora-vjezd
Z garáží	Otevřená	Závora-výjezd
Z garáží	Zavřená	Roleta-výjezd, závora-výjezd

Uvedená tabulka počítá pouze s výměnou čteček, systém ovládání rolety a závor zůstane v tomto případě plně zachován. Proto je vhodné při odjezdu z garáží v případě, kdy je roleta stažená, ji nejdříve vytáhnout a teprve poté otevřít závoru – prodleva při odstraňování překážky v podobě rolety je tak alespoň zčásti využita pro otevření závory.

10.3 Návazná optimalizace přístupového systému

Je zřejmé, že stávající systém ovládání bezpečnostních prvků by se dal optimalizovat. Bylo by možné např. integrovat ovládání rolety a závor do jedné čtečky (resp. nadřízeného terminálu) pro každý směr. V případě uzavřené rolety by odeslání validního ID do čtečky vyvolalo otevření rolety a v okamžiku ukončení jejího otevírání by následně došlo k otevření závory. Tato optimalizace tedy předpokládá jednak napojení mechanismu závory, rolety a související čtečky na jeden terminál, a jednak zásah do prodlev mezi přijetím platného ID a otevřením/uzavřením jednotlivých bezpečnostních prvků.

Vzhledem ke stávající realizaci systému zpoplatněného parkování by bylo také nutné provést nezbytné úpravy v komunikaci mezi přístupovým systémem a serverem, který zpoplatněné parkování řídí.

Co se týče umístění integrovaných čteček, v úvahu přichází využití stávajících sloupků pro čtečky u závor. Důvodem je jejich logické umístění a také fakt, že roleta je přes den, tedy v době největšího provozu v garážích, trvale otevřena. Stávající čtečky by v tomto případě mohly být ponechány na svých místech jako záložní řešení, např. pro uživatele bez mobilních telefonů s potřebným vybavením (nově instalované integrované čtečky by samozřejmě nabízely možnost odbavení prostřednictvím přiložení bezkontaktní karty).

10.4 Podmínky implementace

Nasazení systému v podobě, která je popsána výše, vyžaduje specifické hardwarové vybavení. Základním předpokladem je instalace čteček přístupových karet, které jsou schopné komunikovat na vzdálenost větší, než je současných 10 cm. Konkrétně se jedná o modifikaci standardně nasazovaných čteček pomocí čipu RN4020, který je schopen bezdrátové komunikace prostřednictvím technologie Bluetooth Low Energy. Další nezbytnou součástí systému nad rámec klasických řešení přístupu pomocí bezkontaktních karet jsou mobilní telefony uživatelů vybavené technologií NFC a BLE včetně aplikace, která se stará o komunikaci mezi těmito dvěma rozhraními. Tato aplikace je nedílnou součástí navrhovaného systému a je nezbytné zajistit její distribuci všem uživatelům, kteří o ni projeví zájem.

Z hlediska minimalizace času nutného k interakci uživatelů s přístupovým systémem je žádoucí, aby měli v okamžiku vstupu/vjezdu do hlídané oblasti aktivovaný čip NFC v režimu čtení/zápis, a také Bluetooth pro komunikaci se čtečkou. Nejkomfortnějším řešením je nepřetržité ponechání zmíněných systémů v aktivním režimu, ovšem nevýhodou je v tomto

případě zbytečná – i když ne nijak zásadní – spotřeba elektrické energie. Současné mobilní telefony však umožňují poměrně pokročilé formy automatizace aktivování a deaktivování různých funkcí, např.na základě zeměpisné polohy nebo časového období v rámci dne. Protože nelze automaticky předpokládat, že jsou si uživatelé těchto možností vědomi, je vhodné je s nimi obeznámit formou krátkého školení při předání přístupové karty nebo např. informačními e-maily.

Funkčnost systému však musí být zachována i v případě, že uživatel takto vybaveným mobilním telefonem nedisponuje. V tom případě bude systém z uživatelského hlediska fungovat stejně jako klasické přístupové systémy využívající bezkontaktních karet, kdy je po přiložení karty na čtečku a vyhodnocení oprávněnosti ke vstupu umožněn, nebo znemožněn přístup do zabezpečené oblasti.

Závěr

Hlavním cílem diplomové práce byl návrh systému založeném na technologii NFC, který umožňuje kontrolu přístupu do zabezpečených oblastí, jako jsou např. logistické areály, podzemní garáže a podobné oblasti s omezeným přístupem. Možnosti takového systému se však neomezují pouze na kontrolu přístupu – na jeho základě lze vybudovat aplikace pro monitoring pohybu v dané oblasti, kontrolu docházky, sledování flotily vozidel nebo např. systémy zpoplatněného parkování. Diplomová práce se nicméně zaměřuje na konkrétní řešení spočívající v nasazení přístupového systému v místě vjezdu do podzemních garáží Nové budovy ČVUT v Dejvicích.

Technologie NFC je v práci podrobně popsána – od principů jejího fungování přes technické specifikace až po zhodnocení bezpečnostních aspektů. Rozbor NFC slouží jako teoretický základ pro samotný návrh přístupového systému, který je technologickou nadstavbou stávajícího systému postaveného na bezkontaktních přístupových kartách.

Zmíněné přístupové karty slouží jako elektronický identifikační prvek. Informace o identitě jejich uživatelů jsou prostřednictvím RFID předávány čtečkám bezkontaktních karet, jejichž úkolem je navázat s kartami zabezpečené spojení. Tato komunikace je šifrovaná – čtečka i karta provádí kryptografické operace, které zvyšují odolnost relace vůči nežádoucím zásahům třetích stran. NFC technologicky vychází z RFID, ale na rozdíl od něj umožňuje použití několika režimů bezdrátové komunikace – zařízení vybavené NFC čipem je schopné zastat roli jak čtečky, tak karty; možná je také P2P komunikace mezi dvěma aktivními (tj. napájenými) zařízeními.

V současné době jsou NFC čipy implementovány ve stále se zvyšujícím množství tzv. chytrých mobilních telefonů, které mají bezesporu podíl na rozšiřování této technologie. Diplomová práce tento fakt reflektuje a využití mobilních telefonů vybavených NFC čipy je základním předpokladem, ze kterého vychází návrh odbavovacího systému. Patřičně vybavené mobilní telefony zde figurují jako čtečky přístupových karet, které jsou zároveň schopny bezdrátové komunikace se stávajícími čtečkami napojenými na existující přístupový systém.

Účelem navrhovaného odbavovacího systému je zejména zvýšení uživatelského komfortu řidičů při interakci s přístupovým systémem. Toho je dosaženo odstraněním nutnosti přímého kontaktu přístupové karty a příslušné čtečky – ten je nahrazen bezdrátovou komunikací mezi mobilním telefonem a čtečkou, která je realizována přímo z paluby vozidla.

Aby takto navržený systém fungoval, je nezbytné NFC zkombinovat s další bezdrátovou technologií, která umožňuje komunikaci na delší vzdálenost (řádově metry až desítky metrů). Mezi další požadavky patří spolehlivá funkčnost bez ohledu na běžné klimatické podmínky, nízká energetická náročnost, a také relativně nízké náklady na implementaci. V rámci teoretické části diplomové práce jsou popsány a vzájemně porovnány dvě potencionálně vhodné technologie bezdrátové komunikace – ZigBee a Bluetooth Low Energy. Přes zřejmou podobnost v některých parametrech vycházejí obě technologie z jiných principů. ZigBee je určena zejména pro sítě typu LAN sestávajících ze senzorů a ovladačů, zatímco doménou Bluetooth Low Energy jsou primárně sítě typu PAN, určené např. pro spojení periferií s počítačem nebo mobilním telefonem. Vzhledem k architektuře navrhovaného přístupového systému, ve které je důležitým prvkem mobilní telefon, byla jako vhodnější nakonec vyhodnocena varianta Bluetooth Low Energy, a to zejména z důvodu implementace na naprosté většině současných mobilních telefonů – technologie ZigBee se dosud takového rozšíření nedočkala. Dalším důvodem pro volbu BLE je povaha bezdrátové komunikace mezi telefonem a čtečkou – jedná se výhradně o P2P komunikaci. ZigBee protokol je určený pro provoz mnohem větších sítí a pro účely navrhovaného systému je zbytečně robustní.

Po teoretickém rozboru, zhodnocení a výběru vhodných technologií byla další část práce věnována návrhu a popisu komunikačního procesu v rámci navrhovaného systému. Na straně uživatele řídí veškerou komunikaci speciálně navržená mobilní aplikace. Zahajuje čtení informací z karty pomocí NFC a načtenou informaci přeposílá čtečce prostřednictvím BLE. Komunikace mezi bezkontaktní kartou a mobilním telefonem je šifrována kryptografickou metodou 3DES, stejně jako komunikace mezi telefonem a čtečkou. Čtečky musí být vybaveny čipem pro příjem BLE signálu – v tomto případě se jedná o BLE čip typu RN4020 od společnosti Microchip. Autorem tohoto řešení je společnost IMA. Poslední částí komunikačního řetězce je předání načtené informace ze čtečky nadřízeným prvkům přístupového systému, které sestávají z terminálů, dále z tzv. masterů a hlavního serveru. Server obsahuje informace o přístupových právech všech uživatelů a v pravidelných časových intervalech je distribuuje do masterů, případně i do patřičně vybavených terminálů.

Navržená komunikace vychází ze stávajícího řešení přístupového systému na ČVUT, kde bude v rámci mých aktivit na univerzitě realizován pilotní projekt. Jak již bylo zmíněno výše, projekt spočívá v implementaci navrhovaného systému v oblasti vjezdu do podzemních garáží Nové budovy ČVUT v dejvickém kampusu. Jeho popis je zároveň poslední částí diplomové práce.

Hlavním předpokládaným přínosem navrženého systému je zjednodušení a zrychlení interakce s přístupovým systémem, což ve výsledku přinese zvýšení uživatelského komfortu. Obzvlášť patrné zlepšení by mělo nastat v místech, kde je čtečka karet z paluby vozidel špatně přístupná (např. je-li umístěna na straně spolujezdce nebo pokud je využívána řidiči osobních i nákladních vozidel a pro jednu nebo druhou kategorii řidičů je umístěna v nevyhovující výšce).

Naopak za negativa se dá považovat nutnost nahrazení čteček za jiný typ a vybavení uživatelů specificky vybavenými mobilními telefony, což přináší investiční náklady. Ty by ale s ohledem na rostoucí dostupnost potřebných technologií neměly být nepřiměřeně vysoké. Navrhovaný systém rovněž počítá se zpětnou kompatibilitou se stávajícím systémem, takže jeho nasazení uživatelům nebrání v jeho používání standardním způsobem.

Diplomová práce čerpá informace zejména ze standardů zmiňovaných technologií, ve kterých jsou popsány principy jejich fungování a technické specifikace. Konkrétní hardwarové řešení pak vychází z produktových listů jednotlivých výrobců. Vzhledem k rychlosti, s jakou se předmětná oblast vyvíjí, je převážná část informací distribuována v elektronické formě.

Popsaná technologie bude v rámci navrhovaného systému uvedena do provozu do konce roku 2015 – v případě bezproblémové implementace se očekává nasazení do konce letních prázdnin.

Seznam použitých zdrojů

[1] *Identification cards – Integrated circuit(s) cards with contacts: Part 1: Physical characteristics*. ISO/IEC JTC 1/SC 17, 2011.

[2] *Wikimedia Commons* [online]. [cit. 2015-04-01]. Dostupné z: http://upload.wikimedia.org/wikipedia/commons/7/7c/Mh_chipkarte_synchron.png

[3] *Wikimedia Commons* [online]. [cit. 2015-04-01]. Dostupné z: http://upload.wikimedia.org/wikipedia/commons/d/d1/Mh_chipkarte_asynchron.png

[4] CARDLOGIX CORPORATION,. *Smart Card & Security Basics* [online]. [cit. 2015-04-01]. Dostupné z: http://www.smartcardbasics.com/pdf/7100030_BKL_Smart-Card-Security-Basics.pdf

[5] *SB-Projects: Footprints, Smart Cards* [online]. [cit. 2015-04-01]. Dostupné z: http://www.sbprojects.com/knowledge/footprints/smart.php

[6] *Wikimedia Commons* [online]. [cit. 2015-04-01]. Dostupné z: http://commons.wikimedia.org/wiki/File:SMARTPINOUT.jpg#/media/File:SmartCardPinout.svg

[7] *MIFARE DESFire EV1 contactless multi-application IC*. NXP Semiconductors, 2011.

[8] *ČVUT v Praze: Průkaz typu STUDENT* [online]. [cit. 2015-04-01]. Dostupné z: http://intranet.cvut.cz/informace-pro-zamestnance/prukazy/student

[9] *DATA ENCRYPTION STANDARD (DES)*. U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 1999.

[10] *DES Challenge III Broken in Record 22 Hours* [online]. [cit. 2015-04-03]. Dostupné z: https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19990119_deschallenge3.html

[11] *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*. U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2012.

[12] SCHWARTZ, John. *U.S. Selects a New Encryption Technique* [online]. [cit. 2015-04-03]. Dostupné z: http://www.nytimes.com/2000/10/03/business/technology-us-selects-a-new-encryption-technique.html

[13] KAK, Avi. *AES: The Advanced Encryption Standard*. Purdue University, 2015.

[14] TRIVEDI, Kislay. *NEAR FIELD COMMUNICATION* [online]. 2011 [cit. 2015-04-05]. Dostupné z: http://www.academia.edu/1929769/NEAR_FIELD_COMMUNICATION

[15] *NFC Data Exchange Format (NDEF): Technical Specification*. NFC Forum, 2006.

[16] HASELSTEINER, Ernst a Klemens BREITFUß. *Security in Near Field Communication (NFC): Strengths and Weaknesses* [online]. 2006 [cit. 2015-04-05]. Dostupné z: http://rfidsec2013.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf

[17] *Smart Card Alliance: Securing the Stored Payment Application and Account Information* [online]. [cit. 2015-04-05]. Dostupné z: http://www.smartcardalliance.org/newsletter-200905-feature/

[18] *ZigBee Specification: ZigBee Document 053474r06, Version 1.0*. ZigBee Alliance, 2005.

[19] MAZAR, Haim. *International, regional and national regulation of SRDs* [online]. In: . [cit. 2015-04-08]. Dostupné z: http://www.itu.int/en/ITU-R/study-groups/workshops/RWP1B-SRD-UWB-14/Presentations/International,%20regional%20and%20national%20regulation%20of%20SRDs.pdf

[20] *Optical Zeitgeist Laboratory: ZigBee* [online]. [cit. 2015-04-08]. Dostupné z: http://zeitgeistlab.ca/doc/zigbee.html

[21] *RF Wireless World: Difference between Bluetooth versions* [online]. [cit. 2015-04-08]. Dostupné z: http://www.rfwireless-world.com/Terminology/difference_between_bluetooth_v1_2_v2_v2_1_v3_v4_v4_1.html

[22] *BLUETOOTH SPECIFICATION Version 4.0*. Bluetooth SIG, 2010.

[23] *Bluetooth Low Energy: Whitepaper*. LitePoint Corporation, 2012.

[24] *ČTEČKA BEZKONTAKTNÍCH KARET RSW.04: Produktový list*. IMA s.r.o., 2012.

[25] *RN4020: Bluetooth Low Energy Module*. Microchip, 2014.

[26] *Identification cards - Contactless integrated circuit(s) cards - Proximity cards: Part 2: Radio frequency power and signal interface*. ISO/IEC, 2001.

[27] *Identification cards - Contactless integrated circuit(s) cards - Proximity cards: Part 3: Initialization and anticollision*. ISO/IEC, 2001.

[28] *Description of a BLE communication in the Porter system*. IMA s.r.o., 2014.

Seznam obrázků

Seznam tabulek