Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Možnosti využití technologií RFID a NFC

Bc. Adam Urválek

Vedoucí práce: Ing. Jiří Vaněk, Ph.D.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Adam Urválek

Podnikání a administrativa

Název práce

Možnosti využití technologií RFID a NFC

Název anglicky

Possibilities of using technologies RFID and NFC

Cíle práce

Hlavním cílem práce je charakterizovat a zhodnotit vybrané bezdrátové technologie se zaměřením na RFID a NFC. Jejich bezpečnost, možnosti a využití v dnešní době a v budoucnosti.

Dílčí cíle práce jsou:

- Princip a charakteristika vybraných technologií a jejich zhodnocení
- Možnosti implementace daných technologií
- Hodnocení a závěr práce

Metodika

V části „Přehled řešené problematiky“ bude provedeno hodnocení a charakteristika vybraných bezdrátových technologií. Bude vysvětlen princip jejich funkce, možnosti zabezpečení a jejich využití. Následně bude uveden přehled a hodnocení zařízení, které dané technologie využívají.

Vlastní řešení bude spočívat v ověření zabezpečení technologií RFID a NFC. Možnosti klonování čipových a platebních karet, které tyto technologie využívají. Výsledky řešení budou shrnuty v závěru práce.

Doporučený rozsah práce

50 – 60 stran

Klíčová slova

NFC, RFID, smartphone, čip, karta, čtečka

Doporučené zdroje informací

Amal Graafstra. RFID Toys: Cool Projects for Home, Office and Entertainment. Nakladatelství Wiley Publishing, 2006. ISBN: 0471771961.

Bill Glover, Himanshu V Bhatt. RFID Essentials (Theory in Practice (O'Reilly)). Nakladatelství O'Reilly Media, 2006. ISBN: 0596009445.

Gerard O´Regan. Brief History of Computing. Nakladatelství Springer, 2012. ISBN: 1447123581.

Pužmanová, Rita. Bezpečnost bezdrátové komunikace. Nakladetelství Computer press, 2005. ISBN: 9788025107911.

Tom Igoe. Getting Started with RFID: Identify Objects in the Physical World with Arduino. Nakladatelství Maker Media, 2012. ISBN: 1449324185.

Předběžný termín obhajoby

2016/17 ZS – PEF

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 8. 11. 2015

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2015

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 06. 11. 2016

Čestné prohlášení

Prohlašuji, že svou diplomovou práci Možnosti využití technologií RFID a NFC jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30. 11. 2016 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Jiřímu Vaňkovi, Ph.D., za odborné rady a vedení v průběhu mé diplomové práce.

Možnosti využití technologií RFID a NFC

Souhrn

Diplomová práce představuje dvě vybrané bezdrátové technologie, které jsou široce využívány v běžném životě a v průmyslových odvětví. V práci jsou vysvětleny principy jednotlivých bezdrátových technologií a jejich možnosti využití. Představena jsou zařízení, které tyto technologie využívají a možnosti implementace v budoucnosti. Práce je zaměřena na technologie NFC (Near Field Communication) a RFID (Radio Frequency Identification – radiofrekvenční identifikace). NFC jako mladší z těchto dvou technologií je stále častěji využívána pro komunikaci a zejména také jako prostředek platby. RFID technologie je široce využívána pro identifikaci osob a docházkové systémy, ACS (Access Control System – Systém kontroly vstupu). Práce uvádí problematiku spojenou s identifikací včetně legislativních a normativních aspektů. Bezpečnost RFID a NFC technologie je široce rozebrána a zkoumána z pohledu možnosti jejího prolomení. Praktická část zpracovává možnosti kopírování RFID čipů v praxi za pomoci dnes běžně dostupného softwaru a hardwaru. V rámci praktické části bude navrhnuto řešení docházkového a přístupového systému identifikace zaměstnanců pro fiktivní firmu s ohledem na náklady a úroveň bezpečnosti. V závěru práce jsou shrnuty doporučení, bezpečnostní výhody a nevýhody jednotlivých navrhovaných systémů a samotných technologií.

Klíčová slova: NFC, RFID, smartphone, čip, karta, čtečka

Possibilities of using technologies RFID and NFC

Summary

The thesis presents two wireless technologies widely used in both everyday life and industrial area. Their working principles and utilization methods are explained, as well as devices which use these technologies and the possibilities of future implementation. The focus is on NFC (Near Field Communication) and RFID (Radio Frequency Identification). NFC is latter of the two, and it has become often used for communication and payments. RFID technology is widely used for personal identification and attendance systems, ACS (Access Control System). The thesis takes up the subject of identification from legislative and normative aspects. The RFID and NFC safety breach possibility is thoroughly discussed and analyzed. The practical part elaborates RFID chip copying possibilities using commonly available software and hardware. In the same part, there will be an employee identification access control system draft for a fictional company, considering cost and safety. In the conclusion, there are recommendations, safety advantages and disadvantages of each suggested systems and the technologies themselves.

Keywords: NFC, RFID, smartphone, chip, card, reader

Obsah

1 Úvod ... 8

2 Cíl práce a metodika ... 9

2.1 Cíl práce ... 9
2.2 Metodika ... 9

3 Teoretická východiska ... 10

3.1 Bezdrátové technologie ... 10
3.2 Radio Frequency Identification ... 11
3.2.1 Historie ... 11
3.2.2 Technologie ... 12
3.2.3 Legislativa a standardizace ... 13
3.2.4 Zařízení a oblasti využívající RFID ... 16
3.2.5 RFID Tag ... 17
3.2.6 Zabezpečení RFID ... 19
3.3 Near Field Communication ... 22
3.3.1 Historie ... 23
3.3.2 Technologie ... 24
3.3.3 Režimy přenosu ... 24
3.3.4 Standardy ISO/IEC ... 26
3.3.5 Zařízení využívající NFC ... 29
3.3.6 NFC Tag ... 30
3.3.7 Využití NFC ... 32
3.3.8 Bezpečnost NFC ... 32

4 Vlastní práce ... 35

4.1 Kopírování RFID čipů ... 35
4.1.1 Jednofrekvenční kopírovací zařízení 125 kHz ... 36
4.1.2 Multifrekvenční kopírovací zařízení ... 37
4.1.3 Zařízení pro kopírování UID 125 kHz ... 38
4.1.4 Zařízení ACR 122U ... 39
4.1.5 Možnosti zvýšení ochrany ... 41
4.2 Návrh projektu realizace přístupového systému ... 42
4.2.1 Základní charakteristika projektu ... 43
4.2.2 Přístupový systém EMmarin 125 kHz ... 44
4.2.3 Biometrický přístupový systém ... 48
4.3 Využívání a vývoj RFID ... 50
4.4 Zabezpečení bezkontaktních karet ... 56
4.4.1 Čtení informací z karty VISA a MasterCard ... 57
4.4.2 Rizika zneužití získaných dat ... 61

5 Výsledky a diskuse ... 62

5.1 Kopírování RFID čipů ... 62
5.2 Přístupové systémy ... 62
5.3 Zabezpečení bezkontaktních karet ... 63

6 Závěr ... 64

7 Seznam použitých zdrojů 66

Seznam obrázků

Obrázek č. 1. Oficiální logo NFC. 23
Obrázek č. 2. Nové oficiální logo NFC. 23
Obrázek č. 3. X-Ray snímek NFC Tagu. 30
Obrázek č. 4. Jednofrekvenční kopírovací zařízení 125 kHz. 36
Obrázek č. 5. Multifrekvenční kopírovací zařízení a podporované frekvence. 37
Obrázek č. 6. Zařízení pro kopírování UID 125 kHz. 38
Obrázek č. 7. Zařízení ACR 122U. 39
Obrázek č. 8. Speciální obal karty. 42
Obrázek č. 9. Mapa areálu firmy s legendou. 44
Obrázek č. 10. Číslo VISA karty po načtení informací. 57
Obrázek č. 11. Historie transakcí karty VISA. 57
Obrázek č. 12. Informace o kartě VISA. 58
Obrázek č. 13. Číslo MasterCard karty po načtení informací. 58
Obrázek č. 14. Historie transakcí karty MasterCard. 59
Obrázek č. 15. Informace o kartě MasterCard. 60

Seznam tabulek

Tabulka č. 1. Rozpočet turniketového systému pro vrátnici a parkoviště. 46
Tabulka č. 2. Rozpočet docházkového systému EMmarin. 47
Tabulka č. 3. Rozpočet turniketového biometrického systému pro vrátnici. 48
Tabulka č. 4. Rozpočet biometrického docházkového systému. 49
Tabulka č. 5. Využití RFID pro identifikaci osob v letech. 50
Tabulka č. 6. Využití RFID v závislosti na velikosti podniku. 51
Tabulka č. 7. Využití RFID dle účelu s ohledem na odvětví v %. 52
Tabulka č. 8. Využití RFID v EU v závislosti na velikosti podniku 54

Seznam grafů

Graf č. 1. Využití RFID pro identifikaci osob dle velikosti podniku. 51
Graf č. 2. RFID a způsoby jeho použití v jednotlivých zemích EU. 53
Graf č. 3. Podniky využívající RFID v České republice. 54
Graf č. 4. Podniky využívající RFID v rámci EU. 55

1 Úvod

Diplomová práce se zabývá bezdrátovými technologiemi a způsoby jejich komunikace. Za jednu z největších změn poslední doby můžeme považovat technologický nástup chytrých telefonů, které v sobě bezdrátové technologie ukrývají. Technologický pokrok nám nabízí stále větší možnosti implementace. Hlavně díky minimalizaci součástek, ke které v posledních letech došlo. Proto je možné, aby jedno zařízení disponovalo třemi nebo čtyřmi bezdrátovými technologiemi současně. Výrazným faktorem je stále klesající cena zařízení, které ho tak činí dostupnějším pro širokou veřejnost a podniky. To umožnilo proniknout těmto technologiím do běžně dostupných zařízení, jako jsou „chytré“ televize, kde jsme před několika lety tuto možnost nepředpokládali. Práce je zaměřena na technologie NFC (Near Field Communication) a RFID (Radio Frequency Identification – radiofrekvenční identifikace). NFC je již běžnou součástí platebních karet a drobné elektroniky. Není tedy překvapením, že je stále častěji diskutována bezpečnost této technologie a to především v oblasti bankovnictví. Práce představuje případná rizika, která plynou z používání technologie NFC pro bezkontaktní platbu. V posledních letech došlo k nárůstu potřeby identifikace, kde je využívána právě technologie RFID. Nejedná se pouze o identifikaci osob, ale lze ji využít v daleko širší oblasti. Jedná se především o identifikaci výrobků, ale i zvířat. Identifikace osob však stále zaujímá největší oblast využití. Moderní osobní doklady využívají této technologie pro zjednodušení procesu identifikace, proto je využívána takřka všude, kde je nutné ověřit identitu. Využití najdeme ve většině docházkových systémů, ACS (Access Control System – Systém kontroly vstupu). Pro každodenní bezproblémový provoz musí být technologie funkční a bezpečná. Právě bezpečnost je důležitým faktorem, který nesmíme opomínat. Jak se technologie vyvíjí a rozšiřuje se pole využití, vyvíjí se i způsoby prolomení zabezpečení a možnosti útoků. V případech, kde omezení vstupu na základě oprávnění hraje hlavní roli, je bezpečnost na prvním místě. Růst kriminality pomohl této technologii proniknout do oblasti zabezpečení výrobků. Mnoho obchodních řetězců tak chrání svoje výrobky právě RFID čipy. K tomuto masivnímu rozšíření došlo právě díky klesajícím nákladům na zřízení a provoz této ochrany. Hrozba krádeže není eliminována úplně, ale technologie snižuje riziko odcizení zboží. V budoucnosti lze očekávat využití i v dalších odvětvích a lze očekávat progresivní vývoj těchto technologií.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem této práce je charakterizovat a zhodnotit vybrané bezdrátové technologie, jejich možnosti, bezpečnost a využití v dnešní době a budoucnosti se zaměřením na NFC (Near Field Communication) a RFID (Radio Frequency Identification – radiofrekvenční identifikace). RFID technologie bude zkoumána zejména v oblasti bezpečnosti a možnosti kopírování RFID čipů.

2.2 Metodika

Dílčí cíle práce jsou:

- přehled, charakteristika a hodnocení vybraných bezdrátových technologií

- přehled typů zařízení, která dané technologie využívají

- technologie NFC a RFID jejich bezpečnost a možnosti využití

V první části práce bude provedeno hodnocení dvou vybraných bezdrátových technologií se zaměřením na jejich technologii, komunikaci a její parametry. Následně bude uveden přehled vybraných zařízení, která bezdrátové technologie využívají. Podrobně bude řešena problematika technologií NFC a RFID, na kterou se práce zaměří.

Vlastní řešení bude spočívat v ověření možnosti kopírovat RFID čipy. Za použití dostupných zařízení bude otestována možnost vytvoření kopie a její následné použití v praxi. Pro kopírování bylo vybráno několik zařízení. Z přenosných zařízení jedno multifrekvenční a jedno určeno přímo pro kopírování čipů s pracovní frekvencí 125 kHz. Dále byla vybrána dvě zařízení pracující se softwarem na připojeném počítači. Bude testováno několik různých typů RFID čipů. Přístupové karty do objektu a karty využívané například jako elektronické peněženky. Dosažené výsledky budou hodnoceny v diskuzi a v závěru práce.

3 Teoretická východiska

3.1 Bezdrátové technologie

Základem bezdrátových technologii je spojení dvou subjektů bez použití spojovacího materiálu. Díky tomu není nutné použití kabelů a bezdrátové spojení je zachováno i za pohybu daného zařízení. Tento typ technologií nabízí srovnatelný ekvivalent k sítím drátovým, pokud pomineme přenosovou rychlost. První bezdrátový přenos je datován k roku 1895. Italský vědec Guglielmo Marconi dokázal přenést informaci na vzdálenost přibližně dvou kilometrů. Za další milník v historii bezdrátové komunikace lze považovat rok 1901. Toho roku byl uskutečněn první transatlantický přenos. Na zemi byla komunikace zajištěna zejména telegrafem, proto hlavní využití bezdrátové technologie souviselo s námořnictvem. Na začátku byla informace přenášeno Morseovou abecedou až do roku 1904. Tento rok došlo k uskutečnění prvního bezdrátového přenosu hlasu. Amplitudová modulace (AM) neměla dobrou kvalitu a byla vystřídána kvalitnější frekvenční modulací (FM). Frekvenční modulace se poprvé objevila roku 1934. Poté se začala rozvíjet analogová radiotelefonie. Již v roce 1961 byl odzkoušen první buňkový analogový telefonní systém. Koncem osmdesátých let 20. století se poprvé objevily digitální radiotelefonní systémy. Koncem 20. století došlo k obrovskému nárůstu digitálních systémů. Z tohoto důvodu zastaralá analogová technologie postupně upadala. Dalším významným milníkem v historii bezdrátové technologie je rok 1971. Toho roku byl na Havajské univerzitě zprovozněn bezdrátový spoj ALOHNET. Tento spoj umožňoval spojení sedmi počítačů rozmístěných na pěti různých ostrovech. Komerční využití datujeme k počátku osmdesátých let minulého století. Mezi prvními byly například firmy IBM a Motorola, které vyvinuly na sobě nezávislá řešení, která umožnovala digitální přenos dat. V té době byla přenosová rychlost několik kilobitů za sekundu. První komerční automatizovaná telefonní síť byla spuštěna v japonském Tokiu roku 1979. Největší rozvoj zaznamenaly bezdrátové technologie koncem devadesátých let 20. století. Vlivem technického pokroku bylo možné využít i pásmo UHF a také mikrovlnou oblast. Tedy použít frekvence nad 1 GHz. [1]

3.2 Radio Frequency Identification

Radio Frequency Identification zkráceně RFID je jednou ze starších bezdrátových komunikačních technologií. Oproti modernějším technologiím nedisponuje velkou přenosovou rychlostí. Dosah také není srovnatelný s Bluetooth a WiFi. Přesto tato technologie i dnes nalézá své využití a pravděpodobně bude ještě dlouho využívána. Zejména pro svoji jednoduchost a bezproblémový provoz.

3.2.1 Historie

Historie RFID není přesně datována. Za její počátek lze považovat druhou světovou válku. V této době se tato technologie objevila ve vojenském identifikačním systému letadel. Tento systém s názvem IFF (Identification Friend or Foe) měl za úkol identifikovat letadlo jako přátelské nebo jako nepřítele. Právě s objevením radaru a jeho začátku používání se naskytl problém s identifikací letadel. Po zavedení IFF se tento problém eliminoval a bylo tím docíleno zefektivnění radaru samotného. V praxi to znamenalo vyslání dotazu z radaru směrem k detekovanému letounu, který obsahoval transpondér. Po zpracování dotazu transpondér odeslal informaci zpět k vysílači a potvrdil, že se jedná o přátelský letoun. Již v té době bylo možné signál odeslat aktivním a pasivním způsobem. Pasivní způsob je dnes nejvíce rozšířeným a jeho princip spočívá v odražení původního přijatého signálu. Odražený signál byl upraven o informaci, že se jedná o přátelský letoun. Další možností byla komunikace mezi dvěma aktivními zařízeními. Po přijetí signálu z radaru byla odpověď realizována vysílačem umístěným přímo v letadle. Vysílač umístěný v letadle mohl svojí odpověď předávat již na jiné frekvenci. Tak došlo k ověření, že se jedná o přátelský letoun. Dalšímu výzkumu a vývoji této technologie docházelo během šedesátých let 20. století. Později byl vyvinut jednoduchý systém pro kontrolu zboží v obchodech. Díky jedno bitovému RFID čipu bylo možné určit, zda bylo zboží zaplaceno nebo je předmětem krádeže a neprošlo přes kasu. V sedmdesátých letech 20. století se poprvé objevuje pasivní transpondér obsahující identifikační číslo ve své paměti. Paralelně s pasivními RFID čipy byl vyvíjen systém pro kontrolu pohybu radioaktivního materiálu. Tato technologie byla složena z brány, která představovala RFID čtecí zařízení a transpondéru, který byl umístěn ve vozidle. V okamžiku kdy se vozidlo dostalo do dosahu brány, byl signál z brány přenesen do transpondéru, který zpětně odeslal požadované informace. Dodnes tento princip nalezneme v podobě mýtných bran po celém světě. Dalším historickým milníkem jsou osmdesátá léta. V této době nalézá technologie uplatnění i v zemědělství a to především pro potřeby

identifikace zvířat. Pro identifikaci zvířat byl již plně aplikován pasivní RFID transpondér. V této době také došlo ke standardizaci pracovní frekvence na 125 kHz. Počátkem devadesátých let byl započat vývoj RFID čipu, který by umožnil sledovat přepravované zboží po celém světě. Standardní čárový kód byl doplněn o EPC (Electronic product code), který umožňoval monitorovat pohyb zboží. [8]

3.2.2 Technologie

Standardní radiofrekvenční systém se skládá ze dvou částí. Jde o čtecí zařízení, jinak také čtečku a o transpondér neboli Tag. Technologie využívá elektromagnetických vln, které jsou využity pro přenos dat. Čtecí zařízení vysílá do svého okolí za pomoci antény elektromagnetické vlnění na nosném kmitočtu radiových vln. Pokud se do elektromagnetického pole vloží RFID Tag, jeho anténa je schopna přijmout vlnu na základě rezonance. Po vložení Tagu do elektromagnetického pole čtečky je využita energie pole pro napájení integrovaných obvodů, které díky modulaci ASK (Amplitude Shift Keying) mohou přenášet data. Poté jsou vhodně upraveny vlastnosti elektromagnetického pole. Zpětně získaná data čtečkou jsou v podobě binárního kódu a to prostřednictvím obvodu PLL (Phase Locked Loop). Takto přijatý kód je poté zpracován v mikrokontroléru, kde dojde k porovnání známých kódu v paměti. Pokud je nalezena shoda a kód se jeví jako známý, nastane předem nastavená akce, jako otevření dveří apod. Dnes používaná frekvence je 125 kHz. Tato pracovní frekvence bývá označována jako nízkofrekvenční (low frequency). Další v poslední době stále více využívanou vyšší frekvencí (high frequency) je 13,56 MHz. Obě tyto frekvence jsou nejčastěji využívány pro čtecí zařízení s omezeným dosahem do 25 centimetrů. Pokud je nutné použití většího dosahu je nutné použít frekvence 433,92 MHz nebo 868 MHz. Tyto ultra vysoké frekvence (ultra high frequency) nalezneme zejména v aktivních systémech, jako jsou speciální dálkové ovladače. Díky standardizaci se frekvence takřka na celém světě nemění a díky tomu je zaručena vysoká univerzalita a kompatibilita. V ČR se o správu těchto frekvencí stará ČTÚ (Český telekomunikační úřad). Úřad vydal všeobecné oprávnění č. VO-R/10/05.2014-3, které slouží pro využívání rádiových kmitočtů. [7]

3.2.3 Legislativa a standardizace

Pro RFID technologii jsou definovány určité povinnosti vyplývající ze zákonů nebo norem. Aby bylo možné globální kompatibilní využití, je nutné zajistit do jisté míry standardizaci technologie. Hlavním bodem standardizace je normalizace pracovních frekvencí a s tím spojená kompatibilita jednotlivých typů čipových technologií.

3.2.3.1 Legislativa

Systémy pro kontrolu vstupu a identifikaci osob musí splňovat dané podmínky plynoucí z norem a platných legislativních dokumentů. Tyto systémy jsou realizovány za použití určitého hardwaru a proto i hardware musí splňovat požadavky legislativních dokumentů obecného charakteru. Stejně tak to platí u zákonů, které se týkají přímo konkrétní řešené problematiky.

- Nařízení vlády č. 17/2003 Sb., zde jsou stanoveny technické požadavky na elektrická zařízení nízkého napětí. [9]
- Nařízení vlády č. 88/2010 Sb., stanovuje vybrané výrobky k posuzování shody, ve znění pozdějších předpisů. [10]
- Nařízení vlády č. 490/2009 Sb., zde se mění některé zákony v souvislosti s přijetím nařízení Evropského parlamentu a Rady, kterým se stanoví požadavky na akreditaci a dozor nad trhem, týkající se uvádění výrobků na trh. [11]
- Nařízení vlády č. 616/2006 Sb., upravuje technické požadavky na výrobky z hlediska jejich elektromagnetické kompatibility. [12]

3.2.3.2 Ochrana osobních údajů

V České republice se ochranou osobních dat zabývá Úřad pro ochranu osobních údajů. Byl zaveden na základě zákona č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů. Technologie RFID využívána pro identifikaci osob musí být schopna zajistit bezpečnost uložených dat. Jsou-li během identifikace součástí i citlivá data je nevyhnutelné zajisti jejich bezpečnost splněním požadavků stanovených zákonem. Zákon upravuje podmínky, za kterých je možné ukládat a dále zpracovávat osobní údaje. Dále upravuje postup při jejich likvidaci. Základním předpokladem pro provoz identifikačního systému, je souhlas osoby, u které bude docházek k ukládání dat. V zákonu je také obsažena oznamovací povinnost. To znamená povinnost oznámit proces zpracovávání osobních údajů bez ohledu na systém zpracování Úřadu pro ochranu osobních údajů. [13]

3.2.3.3 Standardizace

Pro bezproblémový a spolehlivý provoz je nutná jistá míra standardizace. Bez normalizace výroby zařízení určených pro RFID by nebylo možné zaručit plnou kompatibilitu. Vybrané normy budou blíže specifikovány v následujících podkapitolách.

3.2.3.3.1 ISO/IEC 7810 Identification cards - physical characteristics

V této normě nalezneme specifikaci pro velikost jednotlivých karet včetně jejich tvaru. Norma specifikuje rovněž spolehlivost funkce karet při jejich vystavení nestandardnímu prostředí. Obsahuje 4 základní definice karet:

- ID-1 – karta se zaoblenými rohy s poloměrem 2,88 – 3,48 milimetrů. Rozměr byl definován na 85,60 x 53,98 mm. Jde o nejrozšířenější formát používaných karet. Tento typ nalezneme ve firmách pro identifikaci zaměstnanců, nebo jako karty městské hromadné dopravy, permanentky apod.
- ID-2 – rozměr je definován na 105 x 74 milimetrů shodně s formátem A7. Jejich zastoupení není veliké a pomalu se od nich přechází na menší a lépe skladné karty ID-1. Tento typ karty je v současné době velice rozšířen v evropské unii. Hlavním využitím jsou identifikační karty pro občany.
- ID-3 – rozměr stanoven na 125 x 88 milimetrů odpovídá formátu B7. Tento typ je využit pro cestovní pasy.

- ID-000 – s rozměry 25 x 15 milimetrů se jedná o nejmenší kartu definovanou tímto standardem. Tvar karty je upraven 3 mm zkosením jednoho rohu. Využita je hlavně jako SIM karta do mobilních telefonů starší generace. [15]

3.2.3.3.2 ISO/IEC 7816

Řada norem nesoucí označení ISO/IEC 7816 stanovuje využití karet s integrovanými obvody s přenosem informací přes fyzický kontakt za účelem identifikace. Norma obsahuje popis fyzikálních parametrů integrovaného obvodu. Mimo jiné také stanovuje přípustné limity expozice okolních jevů. Jedná se především o X-Ray paprsky, elektromagnetické pole a ultrafialové záření. Obsahuje teplotní limity okolního prostředí pro zajištění správné funkčnosti. Součástí je i definice velikosti kontaktního pole, číslování nebo materiálu, z kterého je kontaktní pole vyrobeno. Norma definuje rovněž přenosové protokoly. [14]

3.2.3.3.3 ISO/IEC 14443

Mezinárodní standard používaný pro standardizaci bezkontaktních identifikačních karet. Norma je složena ze čtyř částí:

- ISO / IEC 14443-1: 2008 Část 1: Fyzikální vlastnosti.
- ISO / IEC 14443-2: 2010 Část 2: Napájení EM polem a signální rozhraní.
- ISO / IEC 14443-3: 2011 Část 3: Inicializace a antikolize.
- ISO / IEC 14443-4: 2008 Část 4: Přenosový protokol.

Můžeme se setkat i s označením ISO/IEC 14443 A a ISO/IEC 14443 B. Toto rozdělení vzniklo na základě neshod mezi výrobci. Hlavním rozdílem je způsob použité modulace v kódování a protokolech. Více o této normě bude pojednáno v kapitole 3.3.4.2. Tento standard mimo jiné zavádí termíny PCD: Proximity Coupling Device jinak bezkontaktní čtečka. Dalším termínem je PICC: Proximity Integrated Circuit Cards což je bezkontaktní čipová karta.

3.2.3.3.4 ČSN ETSI EN 302291

Norma s názvem Elektromagnetická kompatibilita a radiové spektrum – Zařízení krátkého dosahu (SRD – Shord Range Devices). Norma je určená pro zařízení komunikující v blízkém dosahu s induktivním přenosem na pracovní frekvenci 13,56 MHz. Jsou zde definovány minimální nutné vlastnosti pro dosažení optimální funkčnosti s použitím dostupného spektra volných frekvencí. Zařízení, která jsou určena pro datovou komunikaci v blízkém dosahu

a s induktivním přenosem, odpovídají definici pro zařízení krátkého dosahu. Pro vysílače a přijímače datové komunikace blízkého dosahu na pracovní frekvenci 13,56 MHz je tato norma závazná. Norma mimo jiné obsahuje definice pro pevné stanice, pohyblivé a přenosné zařízení. Pro zajištění kompatibility nejen elektromagnetické, ale také kompatibility pro systémy ACS (Access Control System – Systém kontroly vstupu) jsou použity tyto normy:

- ČSN EN 61000-6-1 Elektromagnetická kompatibilita – Kmenové normy – Odolnost – Prostředí obytné, obchodní a lehkého průmyslu.
- ČSN EN 61000-6-3 Elektromagnetická kompatibilita – Kmenové normy – Emise – Prostředí obytné, obchodní a lehkého průmyslu.

3.2.3.3.5 Normy aplikační

Pro konkrétní využití technologie RFID v odlišných odvětvích jsou zavedeny normy upravující konkrétní aplikace technologie.

- ČSN EN 50 133 – Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích.
- ČSN EN 60839-11-1 – Poplachové a elektronické bezpečnostní systémy - Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty.
- ČSN ISO 18 186 – Kontejnery – Systém RFID Tagů nákladních zásilek.
- ČSN ISO 17 366 – Aplikace RFID v dodavatelském řetězci – Obaly výrobků.
- ČSN ISO 17 367 – Aplikace RFID v dodavatelském řetězci – Označování výrobků.
- ČSN EN 48 17 – Letectví a kosmonautika – Pasivní UHF RFID Tagy, určené pro letecké použití.
- ISO 11 784 a ISO 11 785 – Radiofrekvenční identifikace zvířat.
- ČSN EN 60950-1 Zařízení informační technologie – Bezpečnost – Všeobecné požadavky.

3.2.4 Zařízení a oblasti využívající RFID

Jako základní zařízení můžeme definovat čtečku a RFID Tag. Aplikaci zařízení lze využít v široké oblasti odvětví. Tato kapitola představuje vybrané odvětví, kde se můžeme s RFID setkat. V zemědělství je RFID používán pro identifikaci zvířat ale i pro identifikaci potravin. Můžeme se setkat s identifikací užitkových zvířat, ryb, holubů a dalších zvířat. Meziroční nárůst v tomto odvětví je přibližně 30 %. Zvířata jsou opatřována RFID Tagy zejména z důvodu automatizace, logistiky, ochrany proti krádeži, kontrolu nemocí apod. Prostřednictvím tohoto systému lze do Tagu ukládat i informace o očkování jednotlivých

zvířat. V Americe se identifikace skotu stala povinností a je nařízena vládním protokolem pro elektronickou identifikaci skotu. Pro Evropskou unii je nařízení o identifikaci platné pro nové chovy koz a ovcí. V zemědělství jsou mimo zvířat označovány speciální RFID etiketou také přepravní boxy. Díky tomuto označení je možné sledovat trasu zboží od zemědělce až ke konečnému spotřebiteli a tím i ověřit jeho čerstvost. Ve strategických bodech trasy jsou rozmístěna čtecí zařízení, které monitorují pohyb zboží až ke spotřebiteli. V logistice nalézá tato technologie významné postavení. Každý produkt od své výroby až po doručení ke konečnému spotřebiteli urazí komplikovanou distribuční cestu. Technologií RFID je zjednodušen proces příjmu zboží na sklad, jeho pohyb na skladě, vyskladnění a předání pro distribuci. Oproti čárovým kódům, kde je nutná přímá viditelnost mezi kódem a čtecím zařízením, je u RFID možné načítat několik tisíc čipů během vteřiny a jednotlivé čipy nemusí být přímo viditelné. Proto je možné v jeden okamžik načíst zboží, které je zabaleno na paletě. Firmy implementují tuto technologii také pro eliminaci chyb na straně obsluhy a pro zpřesnění celkové evidence výrobků. Velkou výhodou je nízká cena komponentů a to je i důvod proč firmy upouštějí stále častěji od systému čárových kódů. Další výhodou je možnost dodatečného zapisování informací během pohybu zboží. Podobně jako v zemědělství je zboží na strategických místech načteno a případně je do čipu připsán údaj o aktuální poloze zboží. Systémy postaveny na RFID technologii mají také velkou odolnost. Vysoká odolnost proti vlivům okolního prostředí, jako jsou například vlhkost a teplota, zaručuje dlouhou životnost. Při použití speciálních čipů a čtecích zařízení je vzdálenost pro čtení a zápis dat až 15 metrů u pasivních RFID Tagů. RFID je také velice často použita pro identifikaci osob. Světově je využívána v osobních identifikačních kartách, jako jsou cestovní pasy nebo občanské průkazy a jejich obdoby. Velké množství firem si vybralo tuto technologii pro řízení přístupu do areálu firmy a pro identifikaci osob a moderní docházkový systém, který bude popsán a řešen v praktické části práce. Velice časté je využití RFID karet jako elektronické peněženky pro městskou hromadnou dopravu.

3.2.5 RFID Tag

Díky velké expanzi této technologie je dnes na trhu mnoho výrobců, kteří nabízejí RFID zařízení. Díky tomu je na trhu k dostání mnoho variant RFID čipů a čteček, které nabízejí odlišné parametry. Následující podkapitoly představují základní rozdělení RFID Tagů a vybrané typy.

3.2.5.1 Rozdělení RFID Tagů

Jako základní rozdělení lze uvést Tag pasivní a aktivní. Pasivní Tagy neobsahují vlastní zdroj napájení a jsou napájeny pomocí elektromagnetické indukce a cívky v nich umístěné. Oproti tomu jsou aktivní Tagy vybaveny vlastním napájením, a tedy je jejich dosah větší. Dle typu přenosu dat lze RFID Tagy rozdělit do dvou kategorií:

- Read Tag – Tag určený pouze pro čtení. U této skupiny Tagů není možný zápis do paměti. Identifikační data jsou uložena pomocí paměti ROM (Read only memory). Data jsou uložena do paměti již během jejich výroby a poté je nelze již měnit. Pro přenos dat je zde využit simplexní přenos.
- Read/Write Tag – Tag určený pro čtení i zápis dat. Jejich využití nalezneme v náročnějších aplikacích. Možnost číst a zapisovat data umožňuje použitá paměť EEPROM (Electrically Erasable Programmable Read Only Memory). Jedná se o elektricky smazatelnou programovatelnou paměť ROM. Přenos dat je u této paměti realizován poloduplexně.

3.2.5.1.1 Pracovní frekvence RFID Tagu

- 125 - 134 kHz – LW RFID (low frequency - nízkofrekvenční Tagy). Tento typ je vhodný zejména pro pasivní systémy. Využíván pro systémy řízení kontroly vstupu.
- 13,56 MHz – HF RFID (high frequency – vysokofrekvenční Tagy). Stejně jako u předešlé skupiny Tagů jsou vhodné pro využití v pasivních systémech. V současné době se jedná o nejvíce používané Tagy.
- 433,92 MHz – UHF RFID (ultra high frequency – ultra vysokofrekvenční Tagy). Jsou vhodné pro velkou vzdálenost. Využívány jsou v aktivních systémech.
- 860 - 960 MHz – UHF RFID. Vhodné na velkou vzdálenost a pro aktivní systémy.
- 2,45 – 5,8 GHz – MICROWAVE (mikrovlny). Podobně jako UHF RFID, je tato frekvence vhodná pro velkou přenosovou vzdálenost a zejména pro aktivní systémy. [21]

3.2.5.1.2 Vzhled RFID Tagu

- Karty – standardizovány v ISO/IEC 7810. Nejčastěji se setkáme s kartou typu ID-1 v podobě občanských průkazů, zaměstnaneckých, věrnostních a permanentních karet.
- Přívěšky – v podobě klíčenek slouží především pro osobní využití. Bývají zajímavě tvarovány a lze je opatřit například gravírováním pro snadnou identifikaci.
- Samolepky – často v podobě štítků, které jsou využívány v logistice pro identifikaci zboží zejména pro jejich nízké pořizovací náklady. Často bývají doplněny o čárový kód.
- Skleněné Tagy – využívány především pro identifikaci zvířat v zemědělství. Zde se výrobci zaměřují na malé rozměry a velkou čtecí vzdálenost. Celý Tag je zapouzdřen ve skleněném obalu a díky tomu je možné ho aplikovat pod kůži zvířat.
- Speciální Tagy – na trhu jsou k dostání speciální RFID Tagy různých tvarů a rozměrů. Lze se setkat s náramky, přívěšky na krk a podobně. Speciální Tagy, které lze umístit na kovové plochy, obsahují odstínění okolního prostředí. RFID čip lze dnes umístit v podstatě do jakéhokoliv pouzdra.

3.2.6 Zabezpečení RFID

Zabezpečení je důležitou součástí každé komunikační technologie. Tato kapitola představuje metody šifrování používané v RFID a vybrané typy karet, které toto šifrování využívají.

3.2.6.1 Metody šifrování

- DES (Data Encryption Standard) – Jedná se již o starší a překonanou metodu zabezpečení. Je založena na symetricky blokované šifře za využití klíče o délce 64 bitů. Efektivně je využíváno pouze 56 bitů. Zůstatkových 8 bitů je využito pro kontrolní součty. Takto krátké šifrování je možné překonat do 24 hodin.
- 3DES – tato metoda šifrování může být označována také jako TDES a Triple DES. Základem je předchozí metoda šifrování DES. Délka klíče je rozšířena na 168 bitů. Vzhledem k tomuto prodloužení délky klíče je zaručena větší bezpečnost. Nicméně díky velkým výpočetním kapacitám dnešních zařízení je možné tuto šifru překonat v poměrně krátké době.

- AES (Advanced Encryption Standard) – stejně jako u předchozích metod je i zde použita symetrická bloková šifra. Na rozdíl od 3DES je rychlost zpracování několikanásobně větší. V současné době je stále využívána, protože její překonání je velice obtížné a zdlouhavé. V Americe byla tato metoda schválena jako bezpečná pro šifrování utajovaných dokumentů.
- CRYPTO-1 – základem je symetrická proudová šifra. Šifra byla vytvořena primárně pro potřeby karty typu MiFare classic. Přináší velmi rychlé šifrování, ale bohužel nízkou bezpečnost. Algoritmus zpracování šifry byl odhalen a karta tak ztratila svoje zabezpečení. Typu MiFare Classic a jejímu zabezpečení bude věnována pozornost v praktické části práce.
- PKE (Public Key Encryption) – pro šifrování je u této metody použit veřejný šifrovací klíč. Jedná se o asymetrické šifrovací algoritmy. Jsou zde použity dva klíče. Veřejný jinak také primární, který je určen k dešifrování soukromé zprávy. Druhý klíč je soukromý, který zprostředkovává zašifrování zprávy pro příjemce. Je zde jistá matematická podobnost klíčů, ale jsou navrhnuté tak, aby bez znalosti veřejného klíče nebylo možné zjistit klíč soukromý a naopak.

3.2.6.2 Výrobci a typy karet

Dnešní trh nabízí mnoho typů karet od různých výrobců a s různým stupněm zabezpečení. V této podkapitole jsou představeny vybrané karty od dvou největších výrobců.

- EM Microelectronic - Marin SA – Švýcarská společnost, která se věnuje výrobě miniaturních integrovaných obvodů se zaměřením na minimální napětí a energetickou spotřebu. RFID čipy tohoto výrobce jsou velice rozšířeny i přes jejich minimální stupeň zabezpečení, které do jisté míry kompenzuje jejich nízká cena. Technologie EM Marine využívá pro komunikaci pracovní frekvenci 125 kHz. V praxi se setkáme s označením EM a čtyřmi číslicemi. První široce užívaná karta měla označení EM4001. Dnes je vyráběna karta s označením EM4200. V této kartě je integrovaný obvod CMOS (Complementary Metal – Oxide – Semiconductor), který je určený pouze pro čtení. Součástí karty je i paměť ROM (Read - Only Memory), ve které je již během výroby pomocí laseru uloženo unikátní 128 bitové UID (Unique Identification). Jedná se o unikátní číslo karty. Je zde využita modulace OOK (On-Off Keying), za jejíž pomoci je zpět do čtecího zařízení odesíláno unikátní

číslo obsažené v paměti ROM. I přes velké rozšíření těchto karet bohužel nenabízí velký stupeň bezpečnosti. Tomuto problému bude věnována pozornost v praktické části. Pro nedostatečné zabezpečení je tato technologie využívána tam, kde není kladen velký důraz na bezpečnost. Nalezneme ji v zemědělství, kde je využita pro identifikaci zvířat, ale i v systémech řízení přístupu. V současné době tento typ karet vyrábí samozřejmě mnoho výrobců. [20]

- NXP Semiconductors – Společnost zabývající se výrobou RFID čipů s historickým názvem Philips Semiconductors. Tato společnost je špičkou ve svém oboru. Je výrobcem několika čipů jako HITAG, NTAG, ICODE a UCODE. [16]

  - HITAG – technologie využívána především v systémech pro řízení vstupu. Dnes se setkáme s technologií HITAG 2, která se stala nástupcem původní technologie HITAG. Technologie využívá jako pracovní frekvenci 125 kHz. Pro přenos dat využívá poloduplexní přenos s využitím šifrování. Nabízí dva typy kódování přenosu Manchaster a Biphase. Obsahuje 256 bitovou paměť s možností ochrany proti čtení i zápisu. Při přenosu je využita modulace ASK. Podobně jako u EM Marine je zde paměť ROM, ve které je uloženo 32 bitové unikátní číslo. Paměť může být šifrována za pomoci 48 bitového klíče. [17]

  - MiFare Classic - karta již využívá pracovní frekvenci 13,56 MHz. Čím spadá do řady high frequency (vysoká frekvence). Tato karta je označována také jako Smart Card (chytrá karta). Vyráběna je ve čtyřech řadách MiFare Classic, DESFire, Plus, Ultralight. Řada Classic využívá šifrování CRYPTO-1 a její zabezpečení bude testováno v praktické části. Čipy těchto karet jsou označovány přívlastkem S50 a S70. Rozdíl spočívá ve velikosti paměti. U S50 je paměť 1 kB (1K). U S70 byla paměť navýšena na 4 kB (4K). V současné době se vyrábí pouze MiFare Classic S70. Vzhledem k nedostačující bezpečnosti dochází k nahrazování tohoto typu další kartou z řady, s názvem DESFire. Využívány jsou především jako zaměstnanecké karty, elektronické jízdenky v hromadné dopravě a pro mýtné brány. [19]

- MiFare DESFire – po prolomení šifrování CRYPTO-1, které je využito u předešlé kary MiFare Classic se společnost NXP rozhodla pro vývoj nové technologie s názvem DESFire. Tento typ nabízel další bezpečnostní prvky a tím pozvedl stupeň zabezpečení. K jejímu překonání došlo v roce 2011. Ještě před tím, ale byla společností vydána technologie s označením DESFire EV1. Tato technologie je stále považována za bezpečnou, protože zatím nebyla překonána. S tím jsou spojené i vyšší náklady na její pořízení. [19]

- SmartMX2 – poměrně mladá technologie, která v sobě ukrývá vysoký stupeň zabezpečení. Pro komunikaci je využito duální rozhraní. Tato funkční platforma je určena pro bezpečné a rychlé datové transakce. Komunikaci lze realizovat kontaktně i bezkontaktně. Technologie přináší pokročilé možnosti v oblasti zabezpečení a velký výkon za podpory silných kryptografických koprocesorů, které pracují s minimálními nároky na energii. Pro šifrování jsou využity 3DES a AES. Technologie je kompatibilní se standardem ISO/IEC 7816 a také ISO/IEC 14443A. [18]

3.3 Near Field Communication

NFC neboli Near Field Communication je jako všechny bezdrátové technologie určena pro bezdrátovou komunikaci. Ke komunikaci dochází přiblížením dvou zařízení k sobě na krátkou vzdálenost v řádu centimetrů. Z tohoto důvodu lze provádět bezkontaktní platební transakce nebo propojit dvě zařízení pouhým dotekem. Oproti jiným komunikačním technologiím je přenosová rychlost opravdu malá. Rychlost přenosu se pohybuje v řádu Kb/s. Výhodou této technologie je její jednoduchost. S ohledem na rychlost přenosu je určena pouze pro výměnu malých dat. Technologie je založena podobně, jako starší výše zmíněná RFID, na principu pasivních prvků. Pro komunikaci je využita elektromagnetická indukce, která zajišťuje napájení obvodů v přijímači.

Obrázek č. 1. Oficiální logo NFC.

Zdroj: <http://rapidnfc.com/imgs/n_mark_info.png>

V lednu roku 2016 NFC Forum představilo nové logo doplněné o text, jak můžete vidět na obrázku č. 2.

Obrázek č. 2. Nové oficiální logo NFC.

Zdroj: < http://www.nfcmix.com/img/cms/nfc-logo1.png>

3.3.1 Historie

Near Field communication pochází ze starší technologie RFID. Můžeme říci, že NFC je jistou podskupinou RFID s kratším komunikačním rozsahem pro podporu bezpečnosti. Společnosti SONY, Nokia a Philips vytvořili společně v roce 2004 NFC Forum. Zaměření již zmíněného sdružení spočívalo v podpoře zabezpečení a snadnosti použití technologie NFC. Jednalo se o neziskové sdružení. Členy byli převážně výrobci a vývojáři. Zpočátku byl počet členů přibližně 200, ale jak rostla popularita technologie, počet členů neustále narůstal. [3]
Cílem sdružení bylo mimo jiné připravit normy a informovat o nich podniky. To umožňovalo, aby jakékoliv zařízení podporující NFC navázalo bezproblémové spojení s dalším zařízením. Firmy, které chtěly NFC technologie do svých zařízení implementovat, musely splňovat dané

standardy. Dva roky od založení, tedy v roce 2006 byla vydána první technologická dokumentace k technologii NFC. První pokusy implementace se objevovaly v letech 2007 a 2008. Z důvodu malé podpory zejména v oblasti bankovnictví a v oblasti osobní dopravy, nezaznamenala technologie velký úspěch. Jednou z překážek, byla jistě již velmi rozšířená a funkční technologie RFID. Pro dopravce by přechod na novou technologii znamenalo nákup nových čtecích zařízení a s tím spojené finanční náklady, protože NFC pracuje na jiné frekvenci. Ve stejném roce, kdy byla vydána technologická dokumentace, byla vytvořena specifikace pro tzv. chytrý plakát. Šlo o plakáty obsahující informaci v čipu. Po načtení čipu mohl uživatel nalézt informace o autorovy, jeho životopis nebo informace o díle samotném.
Prvním kompatibilním telefonem byla Nokia 6131. Po uvedení telefonu na trh, ostatní výrobci postupně začínali své přístroje touto technologií doplňovat také. Jako další přišel na trh roku 2010 mobilní telefon Nexus S od společnosti Samsung. Ve stejné době se NFC objevilo v bankovnictví a to zejména pro realizaci bezkontaktní platby za použití bezkontaktních platebních karet. [2]

3.3.2 Technologie

NFC pracuje stejně jako starší technologie RFID na principu pasivních prvků. Jedná se o radiový přenos dat. Přenos je omezen pouze na krátké vzdálenosti a hlavním prvkem je zde elektromagnetická indukce. Zdroj vysíláním vytváří elektromagnetické pole, které je po vložení pasivního zařízení do jeho dosahu, schopné napájet jeho obvody. Pasivní zařízení z tohoto důvodu nepotřebuje žádné napájení. Zde je možné shledat rozdíl mezi technologií Bluetooth a WiFi, které využívají pro přenos radiové vlny. NFC technologie pracuje na frekvenci 13,56 MHz. Frekvence byla zvolena tak, aby nezasahovala do pásma jiných, již dostupných technologií. Přenos je definován podílem 1/128 nosného kmitočtu. Můžeme se setkat i s podílem 1/64 a 1/32. Vzdálenostní limit pro přenos je maximálně 10 cm, avšak pro bezpečnou a bezproblémovou komunikace se uvažuje vzdálenost do 4 cm. [4]

3.3.3 Režimy přenosu

Způsob komunikace lze rozdělit do třech režimů. Jednotlivé režimy jsou určeny pro různé typy komunikace. Rozlišujeme tedy připojení mezi aktivním a pasivním NFC čipem. Pro vzájemnou komunikaci byl vytvořen jednotný formát NDEF (NFC Data Exchange Format). Starší standardy, které byly použity pro přenášení dat technologií RFID, podporovaly pouze přenos identifikačních dat. Bylo nutné přidání standardu, který by dokázal přenášet jakákoliv data. Proto NFC Forum vytvořilo standard NDEF. Tento formát definoval zapouzdření zpráv

pro výměnu dat mezi jednotlivými zařízeními podporující NFC. Standard umožnil přenos dat mezi dvěma aktivními zařízeními, ale i mezi aktivním a pasivním zařízením.

3.3.3.1 Peer – to – peer

Přenos peer – to – peer probíhá mezi dvěma aktivními zařízeními a umožňuje vzájemnou výměnu dat. Obě zařízení jsou tedy schopné přijímat i vysílat informace. Nelze však současně vysílat i přijímat informaci, protože komunikace probíhá v half-duplexním režimu. Přenosový režim umožňuje odesílat data velice rychle v řádu milisekund a s přenosovou rychlostí až 424 Kb/s.

3.3.3.2 Read / Write

Režim Read / Write neboli Čtení / Zápis je založen především na čtení a zápisu dat z nebo do pasivního NFC čipu (transpondéru). Tento režim nalezneme při realizaci bezkontaktní platby. Celý proces přenosu mezi kartou a čtečkou je šifrován a přenosová rychlost je 106 Kb/s. Tento typ přenosu koresponduje se standardem ISO/EIC 14443 a FeliCa. Standard FeliCa je nejrozšířenější v Japonsku a jeho výrobcem je SONY. Pokud nastane situace, že se ve čtecím poli nalézá více karet, díky anti-koliznímu algoritmu dojde k vybrání pouze jedné karty. V tomto režimu čtečka pracuje jako aktivní zařízení. Pokud je na čipu uložená informace, pak se čtečka zachová dle přečtené informace z čipu bez potřeby zásahu uživatele.

3.3.3.3 Card emulation

Režim Card emulation umožňuje, aby se i aktivní zařízení chovalo jako pasivní. Tento typ přenosu nalezneme především v chytrých mobilních telefonech. Kdy se zařízení jeví jako pasivní a čeká, dokud čtečka nezačne iniciovat čtení. Tento režim je opakem přenosového režimu Read / Write. A proto je možné mít v NFC zařízení několik emulovaných karet, například karty platební, karty pro městskou hromadnou dopravu apod. V takovém případě čtečka detekuje několik karet a na základě požadavku čtečky je vybrána správná karta. Pokud dojde k situaci, že je na výběr ze dvou platebních karet, výběr karty se provede na základě preference uživatele. Pokud nejsou preference nastaveny, musí pak uživatel konkrétní kartu vybrat sám. Pro čtečku je takové zařízení stejné jako pasivní NFC Tag a nedokáže tedy rozpoznat, zda se jedná o mobilní zařízení nebo klasickou bezkontaktní kartu.

3.3.4 Standardy ISO/IEC

Standardy zaručují plnou kompatibilitu všech NFC zařízení mezi sebou. Na základě těchto standardů jsou tedy konstruovány NFC čipy s absolutní kompatibilitou pro všechna NFC zařízení. V následující kapitole si tyto standardy více představíme.

3.3.4.1 ISO/IEC 7816-4

Tento mezinárodní standard definuje organizaci, příkazy a ochranu pro výměnu dat u karet. Konkrétně upravuje tyto oblasti:

- příkazy a odpovědi, které jsou mezi dvěma zařízeními vyměňovány,
- možnosti získávání elementů dat a objektů v kartách,
- strukturální a historický obsah bajtů sloužící k popisu operačních vlastností karet,
- strukturu pro aplikace a data v kartě, které jsou vidět během zpracování v interface,
- metody přístupu k datům na kartě,
- bezpečnost řídící přístupová práva k datům na kartě,
- prostředky a mechanismus pro adresaci a identifikaci aplikace v kartách,
- metodologii pro bezpečnou výměnu dat,
- přístupové metody k algoritmům zpracovávaných kartou.

Ve standardu ovšem nenajdeme specifikace pro vnitřní implementaci karty. Fyzické rozhraní karty není závislé na tomto standardu. Použijeme-li kartu, která obsahuje několik fyzických rozhraní a může je využívat současně, vzájemné vztahy mezi interface nejsou řešeny pomocí tohoto standardu. [5]

3.3.4.2 ISO/IEC 14443

Mezinárodní standard skládající se ze 4 částí pro čipové karty pracující s frekvencí 13,56 MHz. Zde jsou zahrnuty karty obsahující anténu a pracující pouze na krátkou vzdálenost. Standard definuje modulaci a přenosové protokoly mezi kartou a čtečkou k vytvoření fungujících karet pro realizaci bezkontaktních plateb.

- ISO / IEC 14443-1: 2008 Část 1:
    - První část standardu definuje fyzickou vrstvu PICC (Proximity Integrated Circuit Card). Jedná se o karty s integrovaným obvodem.

- ISO / IEC 14443-1: 2008 Část 2:
    - V této části standardu je specifikována charakteristika polí, které jsou poskytovány pro napájení a obousměrnou komunikaci čtečkou karet PCD (Proximity Coupling Device) a kartou s integrovaným obvodem (PICC).

- ISO / IEC 14443-1: 2008 Část 3:
    - Třetí část standardizuje způsob dotazování pro PICC, která vstoupí do pole PCD. Nalezneme zde i standardizaci pro formáty bajtů, rámce a časování použité během první, iniciační fáze komunikace mezi PICC a PCD. Úpravu úvodních příkazů jako je Request (požadavek) a Answer to Request (odpověď na požadavek). Dále obsahuje metodologii pro detekování a komunikaci mezi jedním konkrétním PICC, pokud jich je v dosahu k dispozici několik. Upravuje i další nutné parametry k inicializaci komunikace.

- ISO / IEC 14443-1: 2008 Část 4:
    - Tato část upravuje half-duplexní přenos a jeho protokol. Ten představuje speciální požadavky na bezkontaktní prostředí. Dále zde jsou definovány aktivační a deaktivační sekvence protokolu. Protokoly v rámci této části standardu jsou volitelné. [6]

Standard ISO/IEC 14443 také obsahuje definici pro dva typy komunikačního rozhraní mezi čtecím zařízením a transpondérem (NFC Tagem).

- **Rozhraní typu A** – Pro komunikaci od čtecího zařízení transpondéru je použito ASK (Amplitude Shift Keying) se 100% hloubkou modulace. Binární informace je zde přenášena pomocí změn amplitudy modulového signálu. Ke kódování dat je použito modifikované Millerovo kódování. Komunikace opačným směrem probíhá prostřednictvím OOK (On-Off Keying). Jedná se o modulaci, která označuje základní dvoustavovou ASK modulaci. Použité je kódování Manchester, kde přechod z vysoké úrovně na nízkou znamená 1. Naopak přechod z nízké do vysoké úrovně znamená 0.

- **Rozhraní typu B** – Pro komunikaci od čtecího zařízení k transpondéru je využito stejně jako u předešlého typu ASK avšak s 10% hloubkou modulace. Použité kódování je NRZ-L (Non Return to Zero Level). U tohoto kódování 1 znamená vyšší úroveň a 0 nižší, ne však nulovou. [5]

3.3.4.3 NFCIP

Jedná se o rozšíření standardu ISO/IEC 14443 a přizpůsobení pro NFC. NFCIP-1 je ekvivalentem protokolu pro komunikaci ze skupiny TCP/IP. Obsahuje rozšíření pro transportní protokoly, komunikační režimy a protokoly pro přenos dat. Ve standardu dále nalezneme normy pro modulační schémata, přenosové rychlosti a další důležité parametry pro přenos. Standard obsahuje také LLCP (Logical Link Control Protocol), který pracuje na spojové vrstvě NFC pro peer-to-peer komunikační režim. LLCP je odvozené od staršího standardu IEEE 802.2. Specifikace uvádí dva typy služeb spojově a nespojově orientovanou. První z nich navazuje komunikaci ještě před samotnou výměnou dat, zabezpečuje spolehlivé doručení a řízení toku dat. Služba nespojově orientovaná naopak nepodporuje spolehlivé doručení dat a řízení toku. Zařízení pracující na standardu NFCIP-1 nesmí operovat na jiných přenosových rychlostech než 106, 212 a 421 kb/s. V případě potřeby je možné mezi rychlostmi přepínat. K tomu dochází za pomoci změny parametrů procedury. Nelze ale měnit režim komunikace. To znamená, že nelze změnit režim komunikace z pasivního na aktivní a naopak. [6]

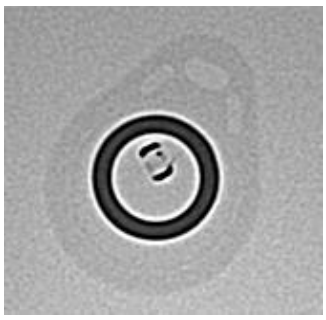
3.3.5 Zařízení využívající NFC

Mezi nejčastěji zmiňované zařízení poslední doby patří chytré mobilní telefony, smartphony. Jejich výkon je dnes již srovnatelný se stolními počítači před několika lety. To umožňuje tyto přístroje osadit moderními komunikačními prostředky jako je i NFC. V posledních letech se častěji objevuje spotřební elektronika obsahující tuto technologii. Je použita především tam, kde je nutné spárování a ověření. Samotný přenos dat pak probíhá za použití starších technologií jako je WiFi a Bluetooth. NFC nalezneme například i v kuchyňských zařízeních jako je pečicí trouba. Společnost LG tuto troubu představila na veletrhu CES už v roce 2013. Troubu spárujete za použití chytrého telefonu s NFC a poté například navolíte recept, který plánujete vařit. Pak opět prostřednictvím NFC přenesete tuto informaci do trouby, ta automaticky nastaví délku a teplotu pečení. Již dlouhou dobu je možné na trhu vidět bezdrátové reproduktory jako doplňkové příslušenství k mobilnímu telefonu. Často jsou doplněny právě o tuto technologii. Samotný přenos dat opět probíhá prostřednictvím Bluetooth, ale ke spárování tedy ověření přístroje dochází právě za použití NFC. Mnohdy jsou k vidění i držáky mobilních telefonů do auta, které obsahují pasivní NFC čip. Pak stačí telefon do držáku vložit a dle uživatelem nastaveného pasivního čipu dojde okamžitě k zapnutí navigace apod. Další zajímavostí je pasivní NFC čip umístěn v dálkovém ovladači k televizi. S tímto řešením jako první přišla společnost Sony. Po přiložení chytrého mobilního telefonu s nahranou kompatibilní aplikací okamžitě dojde k zrcadlení obrazu v mobilním zařízení. NFC technologie pomalu proniká do našich každodenních životů a snaží se nám ulehčovat práci s jednotlivými elektronickými zařízeními. Mimo spotřební elektroniku nalezneme technologii v bezkontaktních platebních kartách, ale také jako prostředek k ověření identity. Většina firem stále dává přednost staršímu RFID, ale v nově zřizovaných podnicích se začíná NFC objevovat stále častěji. Technologie se v poslední době objevuje také v kartách dopravců, kde slouží jako elektronická peněženka jízdného. Nesmíme také opomenout NFC Tagy - malé přívěšky, které lze využít jako uložiště dat.

3.3.6 NFC Tag

Jednou ze schopností technologie NFC je práce s NFC Tagy. NFC Tag si můžeme představit jako malou bezdrátovou paměťovou kartu, ale s výrazně menší kapacitou paměti. Největší prodávané Tagy mají co do kapacity stále jen několik kilobajtů. Proto na tyto zařízení není možné ukládat obrázky, videa a jiné velké soubory a data. Umožňuje uložení vizitky s kontaktem, odkaz na webovou stránku nebo krátkou zprávu. Další zajímavou funkcí je naprogramování vlastního Tagu. Stačí pak telefon položit na NFC Tag na nočním stolku a telefon se automaticky ztlumí a budík se nastaví na předem nastavenou hodinu. Jedná se o pasivní součástky, to znamená, že nevyžadují žádné vlastní napájení. Jak již bylo zmíněno v předchozích kapitolách, energie do NFC Tagu je předávána prostřednictvím elektromagnetické indukce. Jsou konstruovány tak, aby jejich spotřeba energie byla minimální. Reálná spotřeba se pohybuje řádově v desítkách mikro wattů. Každý NFC Tag se skládá z antény a čipu. To vidíme na obrázku č. 3. Miniaturní čip je napojen na kruhovou anténu, kterou je napájen po vložení do elektromagnetického pole. Krátké rentgenové záření nemůže NFC Tag nebo kartu poškodit a ke ztrátě dat také nedojde.

Obrázek č. 3. X-Ray snímek NFC Tagu.



Zdroj: Vlastní.

Velikost antény oproti čipu je několikanásobná. Především proto, aby byla schopná přenést potřebnou energii k čipu. Velikost Tagů je proto limitována velikostí antény. Mohou být desetiny milimetrů tenké, ale plocha antény musí být dostatečně velká. Na obrázku č. 3 vidíme kulatý tvar Tagu. Na trhu je nepřeberné množství tvarů a designových možností. Jediným problémem pak zůstává čtení Tagu z kovového povrchu. Pokud již musíme Tag umístit na kovovou základnu, je nutné vybrat speciálně určený Tag, který je upraven a obsahuje odstínění pro okolní prostředí. Vlastní Tag se liší především tím, který čip je uvnitř

použit. Na dnešním trhu je obrovské množství výrobců Tagů, ale čipy mnoho firem nevyrábí. Největším výrobcem je nizozemská firma NXP. Tato firma dodává čipy všem ostatním výrobcům. Zde je důležitým faktorem také to, že NFC je zpětně kompatibilní s RFID Tagy, které spadají pod normu ISO/IEC 14443. NFC také pracuje se standardem FeliCa společnosti Sony, ten normou ISO/IEC 14443 přijat nebyl. Úpravu tohoto standardu nalezneme v JIS X 6319. NFC Forum definovalo čtyři formáty Tagů určených primárně pro NFC. Jejich cena je oproti RFID větší, ale nabízejí větší možnosti využití. Tři z těchto Tagů jsou založeny na normě ISO/IEC 14443 a jeden na standardu společnosti Sony FeliCa.

- **Typ 1** – postaven na standardu ISO/IEC 14443. Podporuje režim Read/Write a lze ho uzamknout pouze pro režim Read. Kapacita je od 96 bajtů do 2 kilobajtů. Rychlost přenosu pak 106 kb/s. Mezi hlavní výhody patří nízké pořizovací náklady.
- **Typ 2** – srovnatelný s čipem typu 1, ale minimální kapacita je 48 bajtů.
- **Typ 3** – tento čip je postaven na japonském standardu FeliCa. Pro tento čip je režim Read/Write a Read nastavován přímo během výroby. Při pořízení je nutné dát si pozor a vybrat čip dle způsobu použití. Kapacity čipů jsou variabilní teoreticky až 1 Mb. Rychlost přenosu zde dosahuje 212 nebo až 424 Kb/s. Nevýhodou zde můžou být vyšší pořizovací náklady na čip.
- **Typ 4** – kompatibilní se standardem ISO/IEC 14443. Stejně jako u předešlého čipu je jeho režim přenosu nastaven už při samotné výrobě. Maximální velikost paměti je 32 kilobajtů a rychlost zápisu je 106 a 424 Kb/s.

- **Mifare Classic –** velmi oblíbený a v minulosti velice často využívaný Tag. Je zde několik možností kapacity 192, 768 a 3,584 bytů. Komunikační rychlost je 106 Kb/s. Nalezneme zde podporu předcházení kolizím. Nejčastěji se můžeme na trhu setkat s NXP Mifare Classic 1K, Mifare Classic 4K, Mifare Classic Mini. Je zde ale riziko problému kompatibility, protože není standardním typem Tagu, podle NFC Forum. Některá zařízení tento Tag nedokáží přečíst a hlásí chybu. [6]

3.3.7 Využití NFC

Tato relativně mladá technologie postupně nalézá mnohem širší možnosti využití. Objevuje se stále častěji v kartách městské hromadné dopravy a v docházkových systémech firem. I přes krátký dosah nalezneme místa, kde lze využít potenciál NFC. DogNTag je projektem firmy CALL, spol. s.r.o. Firma uvedla na trh chytrou psí známku. Na rozdíl od klasických gravírovaných psích známek umožňuje DogNTag uložit daleko více informací než pouze registrační číslo. Známka je cenově dostupná a stále roste počet uživatelů, kteří mají o tuto technologii zájem. Zejména proto, že po načtení známky je automaticky odeslán e-mail majiteli a pokud to zařízení dovoluje i s mapou, kde k načtení známky došlo. Vzhledem k možnostem naprogramování ulehčují nastavení mobilního telefonu pro danou situaci apod. NFC také slouží pro spárování zařízení jejich autentizaci a následný přenos dat zabezpečený prostřednictvím Bluetooth nebo WiFi.

3.3.8 Bezpečnost NFC

Z důvodu komunikace na krátkou vzdálenost je tato technologie relativně bezpečná. Nicméně i během přenosu na krátkou vzdálenost nalezneme určitá bezpečnostní rizika spojená s přenosem dat. NFC nemá zabezpečenou komunikaci, proto je nutné přidat bezpečnostní algoritmy pro zabezpečení přenosu. Oblíbenost této technologie roste zejména pro její jednoduchost. Nemá žádnou ochranu proti odposlechu komunikace, a proto se může stát v této oblasti zranitelná a data mohou být odposlouchávána nebo modifikována během procesu komunikace.

3.3.8.1 Odposlech

Odposlech neboli Eavesdropping přináší možnost komunikaci NFC odposlechnout a to z důvodu toho, že technologie využívá bezdrátové komunikační rozhraní pro přenos dat. Pomocí zařízení, které obsahuje anténu, zesilovač a dekodér je možné provést odposlouchávání radiofrekvenčního signálu dvou komunikujících zařízení. Proti tomuto odposlechu není NFC nijak zabezpečeno. Stále je zde několik faktorů, které možnost odposlechu ovlivňují, jako radiofrekvenční charakteristika odesílatele dat a útočníka, dále kvalita útočníkova přijímače a dekodéru. Velkou roli hraje i místo, kde je odposlech realizován, množství překážek, stěny a ostatní šum. Posledním důležitým aspektem je výkon NFC zařízení, mezi kterými komunikace probíhá. Samotný odposlech lze rozdělit do dvou kategorií podle charakteristiky transpondéru, který má být napaden, odposloucháván.

Odposlech pasivních transpondérů bývá složitější hlavně z důvodu, že jejich odpověď je generována až po vložení do elektromagnetického pole čtecího zařízení, které zajišťuje jeho napájení. Odpověď je odesílána s velmi malým ziskem na krátkou vzdálenost. Díky tomu je možnost odposlechu možná do vzdálenosti jednoho metru. Pokud budeme odposlouchávat aktivní zařízení, lze odposlech realizovat až na vzdálenost deseti metrů. Aktivní zařízení je schopné vysílat data i bez přítomnosti čtecího zařízení a také s větším ziskem díky vlastnímu napájení.

3.3.8.2 Přepojovaný útok

Přepojovaný útok jinak známý také jako Relay Attack je založen na přeposlání požadavků. Útočící zařízení přijme požadavek od čtecího a následně ho přeposílá k oběti útoku. Zařízení oběti po obdržení požadavku odesílá odpověď přes útočníkovo zařízení zpět do čtecího zařízení. Útočník může data odposlouchávat, ale také modifikovat. Vše musí probíhat v reálném čase, aby komunikující zařízení neidentifikovaly narušení komunikace. V praxi to u pasivního transpondéru znamená, že pasivní transpondér po vložení do elektromagnetického pole získá napětí pro odpověď. Pokud je útočník v dostatečné blízkosti, může komunikaci odposlechnout. Dochází ke generaci rušivého elektromagnetického vlnění směrem k čtecímu zařízení, tím znemožňuje komunikaci směrem od transpondéru. Může nastat situace, že čtecí zařízení detekuje tyto rušivé elektromagnetické vlny a odstoupí od komunikace. Jedná se o teoretický popis útoku, protože v praxi by byla realizace mnohem složitější. Jak již bylo zmíněno, komunikující strany by detekovaly rušivé vlny a přerušily svoji komunikaci.

3.3.8.3 Modifikace dat

Narušení komunikace je jednoduché. Se zařízením pracujícím na frekvenci 13,56 MHz s dostatečným výkonem lze narušit přenášenou posloupnost bitů. Tím dochází k modifikaci přenosu a špatnému vyhodnocování přijatých dat u příjemce. V současné době není známa ochrana před touto modifikací dat. Z tohoto důvodu je možné realizovat cílenou modifikaci dat, kdy se útočník snaží poslat modifikovaná data příjemci, tak aby je považoval za validní. Jde o složitý proces a hlavním faktorem je zde použité kódování a použitá hloubka modulace. Aby bylo možné data modifikovat, musí být jednotlivé přenášené bity radiofrekvenčního signálu modifikovány v přesně daném okamžiku. Musí být použito zařízení se silnějším vysílacím výkonem než má vysílací zařízení. Modifikace bitů je závislá především na hloubce amplitudové modulace.

3.3.8.4 Vkládání dat

Tento útok je založen na vložení dat do komunikace mezi zařízeními. Pro úspěšné vložení zprávy do komunikace je nutná dlouhá odezva odpovědi ke čtecímu zařízení. Díky tomu lze realizovat odeslání odpovědi dříve, než to udělá dotazovaný transpondér. Pokud dojde k odeslání odpovědi současně, budou datové toky překryty a tím poškozena data. Čtecí zařízení je poté vyhodnotí jako chybné.

3.3.8.5 Přerušení spojení

Citlivá data mohou být chráněna časovačem. Po vypršení dané doby je zamezen přístup k datům a je požadována opětovná autentizace. Časovač je aktivován v případě, že není detekována aktivita již autentizovaného zařízení. V případě, že komunikace není správně ukončena a nedojde k uzavření komunikačního kanálu lze navázat komunikaci tam, kde odstupující zařízení svoji komunikaci ukončilo bez nutnosti autentizace.

3.3.8.6 Opakované přenášení dat

Tato bezpečnostní hrozba je založena na opakujícím se přenosu originálních dat. Útočník je schopen odposlechnout počáteční komunikaci mezi zařízeními. Komunikaci nemusí rozumět, ani ji žádným způsobem měnit. Dojde pouze k uložení této komunikace pro pozdější využití. Útočník je pak schopen po vyslání takto získaných dat vytvořit originální transpondér. Tento způsob byl využit u MHD karet. Po zachycení prvotní komunikace bylo možné vytvořit kopii originálního transpondéru a využívat tak účet a finanční prostředky napadené osoby. Stejným způsobem je možné odposlechnout ověřovací sekvenci uživatele bezkontaktní platební karty. Po přehrání takto získaných informací je možné získat přístup k bankovnímu účtu. V praxi se s tím ovšem často nesetkáme, protože platební karty mají vysokou úroveň zabezpečení.

4 Vlastní práce

V první části vlastní práce bude ověřena možnost kopírování RFID čipů. Vytvořené kopie budou ověřeny v praxi a bude shrnuto riziko, plynoucí ze zneužití takto vytvořené kopie. Pro kopírování byla autorem práce vybrána čtyři dostupná zařízení. Dvě zařízení přenosná s jednoduchým ovládáním a dvě zařízení potřebující ke své funkci počítač opatřený softwarem. Druhá část práce je věnována návrhu realizace bezpečnostního systému pro fiktivní firmu. Autorem budou navrhnuta různá řešení a srovnána s ohledem na jejich nákladovost a úroveň zabezpečení.

4.1 Kopírování RFID čipů

Jak již bylo zmíněno v teoretické části nejpoužívanější RFID čipy pro identifikaci pracují na frekvenci 125 kHz a 13,56 MHz. S ohledem na to byla vybrána zařízení, za jejíž pomoci by měla být identická kopie čipu vytvořena. Následující podkapitoly představí jednotlivá zařízení, jejich funkci a výsledky dosažené jejich použitím.

4.1.1 Jednofrekvenční kopírovací zařízení 125 kHz

Zařízení pracuje na frekvenci 125 kHz. Jedná se o nejjednodušší zařízení, které lze na trhu zakoupit. Pracovně bude nazváno zařízení A. Nízké ceně odpovídá i kvalita zpracování, která je na nízké úrovni, to vyvažuje jednoduché použití. Napájení je realizováno prostřednictvím dvou baterií typu AAA. Jde o přenosné zařízení s rozměry 115x70x30 milimetrů. Reálný pracovní dosah za použití standardní antény je 7 centimetrů. Po úpravě antény lze teoreticky dosah zvětšit. Zařízení ke své obsluze využívá pouze dvě tlačítka. Příkaz READ a WRITE. Zařízení je primárně určeno pro karty typu EM 4100 a karty kompatibilní. Systémy, které využívají pro identifikaci právě tento typ, jsou založeny na porovnávání ID čipu s databází. Pokud je ID obsaženo v databázi, je uživatel ověřen. Po stisknutí tlačítka READ dojde k demodulaci vzorků a dekódování samotného ID. Příkaz WRITE zapíše ID originálního čipu do připraveného přepisovatelného čipu. Pro tuto práci byly autorem vybrány čipy s označením TK5577. Obsluha je tedy velmi jednoduchá a kopii čipu lze vytvořit během 5 vteřin.

Obrázek č. 4. Jednofrekvenční kopírovací zařízení 125 kHz.

Zdroj: Vlastní.

4.1.2 Multifrekvenční kopírovací zařízení

V tomto případě se jedná o přenosné zařízení určené pro širší spektrum pracovních frekvencí. Pracovně bude nazváno zařízení B. Napájeno je dvěma bateriemi typu AAA, stejně jako zařízení A. Velikost je 105x45x25 milimetrů. Multifrekvenční kopírovací zařízení je schopné vytvářet kopie UID i pro karty typu MiFare Classic. Dojde ovšem pouze ke zkopírování UID nikoliv obsahu karty. Takto vytvořené kopie lze použít v případě, že systém ověřuje pouze shodu UID s databází. Hlavní předností zařízení je rozpoznání pracovní frekvence karty. Pokud pracujete s kartou, u které není známa její pracovní frekvence, čtečka ji sama rozpozná. Zařízení je doplněno o audio výstup v anglickém jazyce. Po načtení karty je sdělena její pracovní frekvence a její UID. Frekvenci lze manuálně měnit příkazem SWITCH. Po nastavení pracovní frekvence je příkazem READ načteno UID do paměti. Stejně jako u zařízení A použitím příkazu WRITE dojde k zapsání UID do připravené prázdné karty. Pokud známe UID a chceme ho zapsat do prázdné karty, použijeme příkaz INPUT. UID na kartě je uloženo v hexadecimálním formátu, po vložení UID v decimálním formátu je převedeno do hexadecimálního a uloženo. Stejně jako u předchozího zařízení je kopie vytvořena v krátké době v řádu několika vteřin.

Obrázek č. 5. Multifrekvenční kopírovací zařízení a podporované frekvence.

1	125 kHz
2	250 kHz
3	375 kHz
4	500 kHz
5	625 kHz
6	750 kHz
7	875 kHz
8	1 MHz
9	13,56 MHz

Zdroj: Vlastní.

4.1.3 Zařízení pro kopírování UID 125 kHz

Nyní bude představeno první zařízení, které využívá pro svůj provoz počítač a software pro kopírování karet. Pracovně bude nazváno zařízení C. Zařízení je určeno pro pracovní frekvenci 125 kHz. Napájeno je prostřednictvím USB portu z počítače. Rozměry zařízení jsou 108x78x15 milimetrů a bylo zakoupeno za 700 Kč. Software, který slouží ke čtení a zapisovaní UID čipu pracuje obdobně jako u zařízení B. Výhodou je okamžitě viditelné UID v hexadecimálním i decimálním formátu. Pokud chceme do čipu karty vložit nám známé UID, lze ho zapsat na čip v obou formátech. Samozřejmě pokud ho zapisujeme do softwaru v decimálním formátu je opět převedeno do hexadecimálního. Zařízení je schopné pracovat i jako standardní čtečka. Pokud tedy máme k dispozici software s databází UID můžeme toto zařízení použít pro identifikaci. Čtečka přečte UID karty, porovná jej s databází a pokud nalezne shodu, nastane přednastavená činnost. Podobná zařízení jsou využívána například pro objednávání jídel v závodních stravovacích zařízeních. Pro konkrétní UID je zřízen účet na který jsou ukládány platební prostředky. Po přiložení karty jsou poté z účtu odčerpávány.

Obrázek č. 6. Zařízení pro kopírování UID 125 kHz.

Zdroj: Vlastní.

4.1.4 Zařízení ACR 122U

Zařízení ACR 122U je určeno pro pracovní frekvenci 13,56 MHz. Pracovně bude nazváno zařízení D. Na frekvenci 13,56 MHz pracuje poměrně rozšířená karta MiFare Classic. Stejně jako zařízení C využívá pro své napájení USB port počítače. Bezpečná pracovní vzdálenost je 5 centimetrů s ohledem na použitý čtený čip. Čtečka disponuje antikolizní funkcí. Pokud je v dosahu čtečky více čipů, detekuje pouze jednu kartu. Rychlost komunikace je až 424 Kbps. Rozměry 98x65x13 milimetrů, jsou velmi podobné jako u předchozího zařízení C. Mimo MiFare Classic podporuje karty dle standardu ISO/IEC 14443 Typ A / B, FeliCa, 4 standardy NFC dle ISO/IEC 18092, Mifare Plus. MiFare Classic je často používána jako karta dopravců nebo jako permanentní karta. Pokud by se podařilo dešifrovat kartu, lze například opakovaně dobíjet kredit. Primárně je zařízení určeno pro e-banking, e-platby a přístupové systémy. Obsahuje dvoubarevnou signalizaci stavu prostřednictvím LED, které lze uživatelem nastavit. LED signalizace je doplněna akustickým potvrzením načtení karty, které je také uživatelem nastavitelné. Cena zařízení je přibližně 2500 Kč.

Obrázek č. 7. Zařízení ACR 122U.

Zdroj: Vlastní.

4.1.4.1 Vytvoření kopie karty MiFare Classic

Autorem byla vybrána karta MiFare Classic, která sloužila jako dobíjecí karta pro přístup do Fit Centra a byly z ní odčerpávány finanční prostředky. Využívá šifrování CRYPTO-1. Jedná se o pasivní útok na čipovou kartu. Pokud se podaří prolomit šifrování, bude možné přečíst kompletní obsah paměti. Díky tomu můžeme data zálohovat, přehrát na jinou kartu nebo s daty libovolně manipulovat nebo je modifikovat. Pro realizaci přístupu do paměti je nutná znalost všech klíčů jednotlivých sektorů, které budeme číst nebo do nich zapisovat data. Pro dešifrování karet MiFare Classic je autorem vybrána Open Source knihovna Libnfc. Knihovna je vyvíjena pod GNU licencí. Pracuje na základě technologie NFC. Tato knihovna je psána v jazyce C++. Z těchto důvodů byl autorem vybrán operační systém Linux, konkrétně BackTrack 5 R3. Po nainstalování ovladačů čtečky máme zařízení připraveno. Aby bylo možné offline útok realizovat je nutné mít k dispozici kód. Pro NFC komunikaci byl zvolen kód nfc-utils.c, crapto1.c a crypto1.c. Pro identifikaci čipové karty MiFare Classic je využito kódu mifare.c. Pro výpočet šifrovacích klíčů je použit mfoc.c. Všechny tyto kódy jsou volně k dispozici na internetu. Jedinou podmínkou pro použití mfoc.c je, aby minimálně jeden ze sektorů čipu obsahoval defaultní klíč, který je právě známý. Pokud by nastala situace, že ani jeden z klíčů nebude defaultní, lze tento klíč získat odposlechem komunikace mezi čipem a autorizovanou čtečkou. Bohužel to už v praxi opět stěžuje prolomení bezpečnosti karty. Pro odposlech je nutné další zařízení, u kterého je již vyšší pořizovací cena. Pro odposlech lze využít například Promax 3, cena tohoto zařízení je v současné době přibližně 5200 Kč. Koupit lze na zahraničních e-shopech. Karty využívané pouze pro identifikaci dle UID mají všechny sektory defaultní ve tvaru FF FF FF FF FF FF. Tento typ karty není nutné žádným způsobem dešifrovat, ale lze použít výše zmíněného zařízení B v kapitole 4.1.2. Pokud je na kartě jeden klíč defaultní a ostatní jiné, započne dešifrování karty. Použitá karta obsahovala 15 sektorů s klíči A a B. Výpočet klíčů je realizován ověřením příslušného sektoru defaultním klíčem. Poté je přečtena odpověď karty. Toto je opakováno znovu. Během druhého ověření je již proces ověření šifrován. V tuto chvíli dojde k výpočtu času posunu LFSR zásobníku. Poté je odhadnuta hodnota a ověřen jiný paměťový sektor. Systém musí projít 2^{36} hodnot. Z toho důvodu může dešifrování karty s ohledem na použitý výkon hardwaru trvat od pěti do třiceti hodin. Po dešifrování jsou označeny sektory obsahující data. Ostatní prázdné sektory nejsou nijak zajímavé pro další použití. Pokud jsou úspěšně dešifrovány všechny klíče A a B je obsah karty uložen do souboru tzv. dump file. Takto vytvořený soubor můžeme v budoucnu použít pro dešifrování stejné karty, ale od jiného

majitele. Poslouží jako zdroj přístupových kódů a značně urychlí proces dešifrování. Pokud modifikujeme anténu zařízení a bude mít dostatečný výkon, postačí pak být v přítomnosti karty na několik metrů a dešifrování proběhne v řádu vteřin. U karet obsahující například kredit pro vstup do zpoplatněných zařízení je možné upravovat zůstatek na kartě. Po dobití karty si její obsah zálohujeme. Když bude nutné kartu opět dobít, využijeme zálohu, kterou do karty přehrajeme a tím tak obnovíme původní zůstatek na kartě. Další možností je za použití softwaru příslušný sektor, ve kterém je informace o zůstatku obsažena, editovat. Pro toto konkrétní řešení byly vynaloženy náklady 2500 Kč. Pokud budeme kartu využívat opravdu často, tato investice se rychle vrátí. Z tohoto důvodu by měli provozovatelé těchto systémů s rizikem počítat a raději investovat do dražších karet jako například DESFire EV1. Pořizovací náklady jsou samozřejmě větší, ale v současné době se stále ještě jedná o bezpečné řešení. Bohužel nikdo nedokáže s jistotou říci, jak dlouho bude trvat prolomení zabezpečení této technologie a kdy dojde k jejímu zneužití, podobně jako se tomu stalo u MiFare Classic. Často je proto vyžadována vratná záloha za kartu, která provozovateli částečně kompenzuje náklady spojené se ztrátou nebo odcizením karty. V mnoha případech postačí pouze výměna softwaru, který je pro evidenci použit a čtecí zařízení je možné zachovat. Samozřejmě musí předchozí nahrazovaná technologie pracovat na stejné frekvenci. Provozovatelé těchto systémů musí zvážit rizika a investice do nových bezpečnějších systémů. Pro zavádění nových systémů autor doporučuje využití karet DESFire EV1. Jak již bylo řečeno výše, jsou v současnosti stále bezpečné.

4.1.5 Možnosti zvýšení ochrany

V úvodu této kapitoly jsme se přesvědčili, že kopírování karet EM4xxx je opravdu snadné a dostupné pro každého. Autorem bylo vyzkoušeno odečtení karty z peněženky, která mimo platební karty obsahovala i mince. I přes přítomnost kovu byla informace z karty načtena a poté bezproblémově vytvořena její kopie. Potenciální ohrožení spočívá tedy i v přečtení karty pokud například stojíte v autobusu, ve frontě na oběd apod. Jistou možností je využití speciálního obalu karty, který kolem karty vytvoří tzv. Faradayovu klec. Na obrázku č. 8. můžeme vidět obal karty, který byl autorem úspěšně otestován.

Obrázek č. 8. Speciální obal karty.

Zdroj: Vlastní.

Pokud jde o systém samotný, je vhodné doplnit ho dalším bezpečnostním prvkem. Může se jednat o zadání pinu po přiložení karty. V poslední době bývají tyto starší systémy doplněny o biometrickou čtečku, čímž se zvyšují náklady, které například zaměstnavatelé menších firem nechtějí investovat. Další možností je zřízení kamerového systému, který by v případě zneužití karty byl schopen pachatele identifikovat. Obecně tyto tzv. starší technologie identifikace nelze doporučit. Nicméně v praxi jsou právě kombinovány s jiným doplňkovým systémem a není investováno do modernějších a bezpečných technologií. Ve srovnání s kamerovým systémem ke stávajícímu zastaralému identifikačnímu systému a pořízení úplně nového bezpečného systému jsou náklady znatelně rozdílné v řádu desetitisíců Kč.

4.2 Návrh projektu realizace přístupového systému

V této kapitole byla autorem navrhnuta vybraná možnost realizace projektu přístupového systému. Realizace projektu byla hodnocena z pohledu bezpečnosti a nákladů pro konkrétní řešení. Realizace byla připravena pro středně velký podnik s počtem sto osmdesáti zaměstnanců. Ve firmě je zaveden třísměnný provoz. Realizace spočívala v návrhu přístupového systému do areálu firmy. Dále byl zřízen terminál pro evidenci docházky s použitím vybraného softwaru. V poslední podkapitole byly zhodnoceny náklady realizace projektu s ohledem na jeho stupeň bezpečnosti.

4.2.1 Základní charakteristika projektu

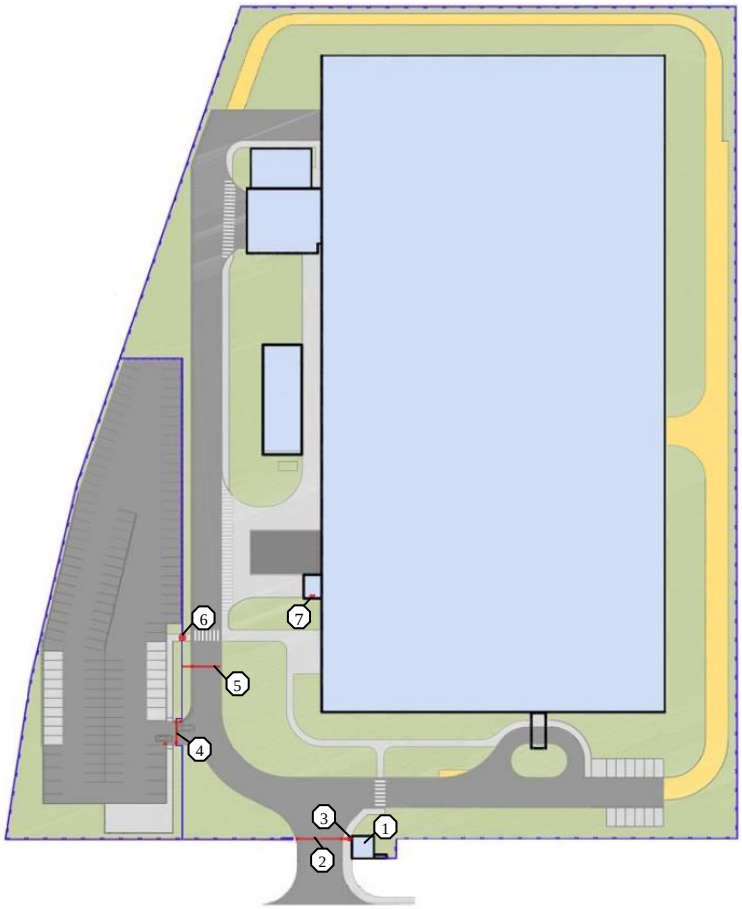
V první řadě musí být definovány požadavky pro systém. Dle zadaných požadavků je zvolen postup realizace a vybráno vhodné řešení.
Požadavky na realizaci projektu:

- řízení přístupu do areálu firmy,
- monitoring pohybu zaměstnanců včetně záznamu,
- evidence pracovní docházky zaměstnanců,
- kompatibilita pro možnost rozšíření o stravovací systém,
- vysoká bezpečnost,
- nízké pořizovací a provozní náklady.

Součástí charakteristiky projektu je i stanovení míst, kde bude k identifikaci docházet. Na obrázku č. 9 je mapa objektu s vyznačenými místy klíčových bodů. Před realizací je nutné zohlednit zaměstnance, kteří budou využívat pěší vstup do objektu vedle vrátnice ale také ty, kteří dojíždějí do zaměstnání automobilem, případně na kole. Tomu bude nutné přizpůsobit sestavení přístupového systému a místa, kde bude identifikace realizována. V současné době disponuje areál čtyřmi závorami. Jedna je přímo na vrátnici a druhá u vjezdu do logistické části areálu. Další dvě jsou připraveny pro přístupový systém ve vjezdu a výjezdu na parkoviště firmy. Během výstavby bylo již počítáno s přípravou pro podobný systém a spojovací materiál byl položen během výstavby. To značně sníží finální náklady realizace projektu. Mezi další požadavek patří řízení přístupu na parkoviště a zpět pro pěší. Tento požadavek bude dále řešen v jednotlivých návrzích přístupových systémů. Podnik trvá na zachování zaměstnance na vrátnici, který obstarává pouze automobilový provoz v areálu a návštěvy. Z vrátnice je možné ovládat hlavní závoru do areálu a druhou závoru v logistické části. Takto byl areál rozdělen zejména proto, aby zaměstnanci nemohli zajíždět s vozidlem do částí závodu, kam nemají přístup. Další otázkou byla kontrola vozidel zaměstnanců přímo na vrátnici. S ohledem na nízké náklady byla pro majitele firmy nejlevnější dostupnou variantou příprava registračních karet, kde je typ vozidla, barva, SPZ a jméno držitele karty. Karta o velikosti A5 musí být umístěna viditelně, tak aby zaměstnanec vrátnice mohl údaje identifikovat a po kontrole vozidlo vpustit dále od areálu. Registrační karty jsou spravovány ve vlastní režii podniku. Samotná identifikace zaměstnance tak proběhne, až ve chvíli kdy

vjíždí na parkoviště a podruhé když parkoviště opouští jako pěší a míří do firmy. Ve vstupní hale bude umístěn docházkový terminál a dveře opatřené elektromagnetickým zámkem.

Obrázek č. 9. Mapa areálu firmy s legendou.



1	Vrátnice
2	Závora - vrátnice
3	Turniket - vrátnice
4	Závory - parkoviště
5	Závora – logistická oblast
6	Turniket - parkoviště
7	Docházkový systém

Zdroj: Vlastní.

4.2.2 Přístupový systém EMmarin 125 kHz

Autorem vybraný přístupový systém je založen na technologii EMmarin popsané v kapitole 3.2.6.2. Pro řízení přístupu do areálu firmy autor vybral jako nevhodnější řešení turniket. První bude umístěn na vrátnici firmy a bude umožňovat přístup oprávněným osobám do areálu. S ohledem na náklady byl vybrán jednosměrný turniket. Ve firmě je zaveden třísměnný provoz, a proto nehrozí, že by v jeden okamžik byl turniket využíván v obou směrech. Druhý jednosměrný turnike bude umístěn ve vchodu/východu na parkoviště. Pro autorizaci musí být doplněny o čtecí jednotky v obou směrech a příslušným softwarem. Další dvě jednotky je nutné umístit ke každé závoře ve vjezdu/výjezdu na parkoviště v areálu firmy. Autorem byly vybrány čtecí jednotky od společnosti Sebury pro jejich relativně nízkou

cenu a dobrou kvalitu zpracování. Pro realizaci projektu je nutná podpora zapojení více jednotek do systému. Čtecí jednotky Sebury PC BC 2008NT tuto možnost podporují. Mimo jiné bude zařízení vystaveno povětrnostním vlivům, a proto musí splňovat minimální krytí IP52. Systém podporuje možnost módu karta + kód, prostřednictvím toho je možné bezpečnost systému zvýšit. Připojení je realizováno rozhraním RS 485. Připojeny musí být přes datový převodník, který je součástí realizace sestavy. Pro projekt je nutné zajistit i sledování pohybu zaměstnanců. Zejména proto, aby nebyla docházka označena někým jiným, kdo se v daný čas ve firmě nevyskytuje. Lze pak jednoduše porovnat čas vstupu do areálu firmy a čas načtení karty na docházkovém terminálu. Díky použitému softwaru lze každé čtecí zařízení pojmenovat. V této konkrétní realizaci to bude Vrátnice IN a Vrátnice OUT a stejně tak budou označeny čtecí jednotky závor parkoviště a turniketu na parkovišti. Pokud je karta přiložena, její UID je do systému zaznamenáno, včetně názvu konkrétního čtecího zařízení a času. Po vstupu do areálu je zaznamenáno jméno držitele karty spárované s UID a čas načtení karty na konkrétní čtecí jednotce. Dalším krokem je realizace docházkového systému. Pro středně velký podnik bylo vybráno čtecí zařízení od společnosti Estelar s.r.o., model RT300-B. Čtečka disponuje krytím IP 41 a je tedy pro použití v hlavním vchodu do budovy dostatečné. Obsahuje vlastní paměť, pokud dojde k výpadku spojení mezi terminálem a počítačem, data nebudou ztracena. Vzhledem k možnosti připojení až dvou zámků dveří je pro tuto realizaci ideální. S ohledem na bezpečnost je vhodné využít doplňkovou funkci zadání PINu a tím je bezpečnost zvýšena. Po načtení karty a zadání PINu je uživatel ověřen a přístupové dveře do budovy lze otevřít. V případě, že půjde více zaměstnanců současně, toto bezpečnostní opatření ztrácí smysl. Dveře nebudou při každém načtení karty v krátkém časovém horizontu zavřeny. Z tohoto důvodu je dalším vhodným prvkem realizace cenově dostupného kamerového systému. Pro tento projekt bude využit systém pracující s pěti kamerami současně. Budou umístěny na vrátnici, u hlavního vchodu do budovy a na příjmovém skladu pro monitoring pohybu dodavatelů a odběratelů. Kamerový systém obsahuje vlastní záznamové medium, které umožňuje dohledání záznamu v případě potřeby. S ohledem na cenové omezení byly vybrány dostatečné komponenty, které zaručí v případě problému identifikaci osob. Systém zůstává otevřený a do budoucna je možné ho dle potřeby rozšířit o větší paměťové medium nebo o přidání dalších kamer. Systém s technologií EMmarin je připraven pro rozšíření o stravovací systém. Systém stravování musí být založen na účtech spojených s UID karet jednotlivých majitelů. S použitím těchto karet nelze kredit pro stravování uchovávat přímo na kartě, ale eviduje a spravuje ho software na základě jednotlivých UID karet a jejich majitelů.

4.2.2.1 Rozpočet realizace projektu

Dle požadavku na systém byly vybrány funkční a cenově dostupné komponenty. Návrh cenové realizace níže je sestaven z aktuálních cen k 1. 11. 2016 ve spolupráci s firmou Estelar s.r.o. Ceny jsou uváděny bez DPH. Do realizace projektu jsou samozřejmě zahrnuty i ceny instalace a s tím spojené pracovní úkony. Jednotlivé položky nebudou z důvodu obsáhlosti uváděny a rozpočtová kalkulace bude rozdělena do skupin.

Tabulka č. 1. Rozpočet turniketového systému pro vrátnici a parkoviště.

P.č.	Název položky	MJ	Množství	Cena / MJ	Celkem (Kč)
Díl:	**Proražení otvorů**				
1	Vysekání kapes cihly duté	kus	22,00	47,00	1 034,00
2	Vysekání kapes cihly duté	kus	15,00	29,00	435,00
	Celkem za proražení otvorů				**1 469,00**
Díl:	**Montážní práce**				
3	Turniket Entry	kus	2	64 103,00	128 206,00
4	Montáž turniketu	kus	2	12 820,00	25 640,00
	Celkem za montáž turniketu				**153 846,00**
Díl:	**Elektromontáže**				
5	Čtecí jednotka Sebury	kus	6	1 256,00	7 536,00
6	Deska síťového kontroleru	kus	1	7 169,00	7 169,00
7	PC sestava HP Pro 280 G1	kus	1	7 430,00	7 430,00
8	Software	kus	1	13 025,00	13 025,00
9	Zálohovaný zdroj	kus	1	5 100,00	5 100,00
10	DU485 datový převodník USB	kus	1	1 450,00	1 450,00
11	Spojovací materiál	m	10	25,20	252,00
12	Montáž	kus	1	7 136,00	7 136,00
	Celkem za elektromontáže				**49 098,00**
Celkové náklady:					**204 413,00**

Zdroj: Vlastní.

Tabulka č. 2. Rozpočet docházkového systému EMmarin.

P.č.	Název položky	MJ	Množství	Cena / MJ	Celkem (Kč)
Díl:	**Proražení otvorů**				
1	Vysekání kapes cihly duté	kus	24,00	47,00	1 128,00
2	Vysekání kapes cihly duté	kus	10,00	29,00	290,00
	Celkem za proražení otvorů				**1 418,00**
Díl:	**Elektromontáže**				
3	Karta bezkontaktní EMmarin	kus	200	59,00	11 800,00
4	RT-300B docházkový terminál	kus	1	11 900,00	11 900,00
5	DU485 datový převodník USB	kus	1	1 450,00	1 450,00
6	Zálohovaný zdroj	kus	1	5 100,00	5 100,00
7	PC sestava HP Pro 280 G1	kus	1	7 430,00	7 430,00
8	Software – SQL NET2/100	kus	1	17 800,00	17 800,00
9	Kamerový systém	kus	1	9 093,00	9 093,00
10	Elektromagnetický zám. SH 200	kus	1	11 568,00	11 568,00
11	Spojovací materiál	m	20	25,20	504,00
12	Montáž	kus	1	12 969,00	12 969,00
	Celkem za elektromontáže				**89 614,00**
Celkové náklady:					**91 032,00**

Zdroj: Vlastní.

4.2.2.2 Bezpečnost a náklady systému EMmarin

Přístupový systém byl sestaven dle požadavků na realizaci projektu. S ohledem na požadavek nízkých nákladů byl sestaven bezpečný systém pro kontrolu vstupu do areálu firmy a evidenci docházky. Celková cena realizace projektu činí 295 445 Kč. Systém je založen na kontrole UID karet s databází softwaru. V kapitole 4.1 byly popsány způsoby kopírování UID karet a tedy bezpečnostní rizika s tímto spojená musí být akceptována. Jako bezpečnostní doplněk byl proto zvolen kamerový systém. V případě potřeby lze dohledat kamerový záznam zpětně a tak identifikovat případného pachatele. Pokud by byl systém realizován prostřednictvím karet MiFare Classic na pracovní frekvenci 13,56 MHz, nebylo by dosaženo vyšší bezpečnosti, právě z důvodu kopírování UID. Náklady by byly zvýšeny o pořízení karet, které jsou oproti EMmarin vyšší, ne však výrazně. V následující kapitole bude sestaven bezpečnostní systém na základě biometrického ověření.

4.2.3 Biometrický přístupový systém

Pro realizaci biometrického přístupového systému využijeme požadavky z předešlé kapitoly. Dojde tedy pouze k výměně čtecích zařízení a použitého software pro kontrolu přístupu na vrátnici. Jako čtecí biometrické jednotky pro turniket byly autorem vybrány čtecí zařízení Sebury F007 EM-II a byly autorem otestovány v praxi. Jednotky jsou schopné načítat i znečištěné nebo mastné prsty. Čtečka se zaměřuje především na jednotlivé papilární linie otisku než na jejich pokrytí. Problém nastal ve chvíli, kdy byl testován mokrý prst. Čtečka vůbec nereagovala a bylo nutné, prst osušit. Po osušení prstu bylo načtení opakovaně korektní. Výrobce garantuje provoz až do -20°C, což je pro naše účely dostačující. Výhodou je software dodávaný přímo se čtečkou. Tím dojde ke snížení nákladů. Pro docházkový systém byl autorem vybrán biometrický terminál společnosti Estelar s.r.o., konkrétně model FT500FM. Systém je schopen pracovat i s kartami typu MiFare na frekvenci 13,56 MHz. Možnost použít kartu namísto otisku prstu nebude povolena z bezpečnostních důvodů popsaných v kapitole 4.1.

Tabulka č. 3. Rozpočet turniketového biometrického systému pro vrátnici.

P.č.	Název položky	MJ	Množství	Cena / MJ	Celkem (Kč)
Díl:	**Proražení otvorů**				
1	Vysekání kapes cihly duté	kus	22,00	47,00	1 034,00
2	Vysekání kapes cihly duté	kus	15,00	29,00	435,00
	Celkem za proražení otvorů				**1 469,00**
Díl:	**Montážní práce**				
3	Turniket Entry	kus	2	64 103,00	128 206,00
4	Montáž turniketu	kus	2	12 820,00	25 640,00
	Celkem za montáž turniketu				**153 846,00**
Díl:	**Elektromontáže**				
5	Čtecí jednotka Sebury F007	kus	6	2 899,00	17 394,00
6	Řídící jednotka Sebury IC 104	kus	1	3 399,00	3 399,00
7	PC sestava HP Pro 280 G1	kus	1	7 430,00	7 430,00
8	Zálohovaný zdroj	kus	1	5 100,00	5 100,00
9	Spojovací materiál	m	10	25,20	252,00
10	Montáž	kus	1	4 395,00	4 395,00
	Celkem za elektromontáže				**37 970,00**
Celkové náklady:					**193 285,00**

Zdroj: Vlastní.

Tabulka č. 4. Rozpočet biometrického docházkového systému.

P.č.	Název položky	MJ	Množství	Cena / MJ	Celkem (Kč)
Díl:	**Proražení otvorů**				
1	Vysekání kapes cihly duté	kus	24,00	47,00	1 128,00
2	Vysekání kapes cihly duté	kus	10,00	29,00	290,00
	Celkem za proražení otvorů				**1 418,00**
Díl:	**Elektromontáže**				
3	FT500FM docházkový terminál	kus	1	24 900,00	24 900,00
4	Zálohovaný zdroj	kus	1	5 100,00	5 100,00
5	PC sestava HP Pro 280 G1	kus	1	7 430,00	7 430,00
6	Software – SQL NET2/100	kus	1	17 800,00	17 800,00
7	Softwarový modul FINGER	kus	1	3 000,00	3 000,00
8	Elektromagnetický zám. SH 200	kus	1	11 568,00	11 568,00
9	Spojovací materiál	m	20	25,20	504,00
10	Montáž		1	14 060,00	14 060,00
	Celkem za elektromontáže				**84 362,00**
Celkové náklady:					**85 780,00**

Zdroj: Vlastní.

4.2.3.1 Bezpečnost a náklady biometrického systému

Podobně jako při realizaci přístupového systému EMmarin byl kladen důraz na bezpečnost a nízké pořizovací náklady. V této realizaci byl vynechán kamerový systém, protože zde nehrozí riziko v podobě kopírování UID. Celková cena realizace biometrického přístupového systému činí 279 065 Kč. To je o 16 380 Kč méně než v případě bezkontaktního přístupového systému s použitím karet. V rozpočtu si můžeme povšimnout absence USB datového převodníku, který je již součástí docházkového terminálu. Vyšší cenu čtecích zařízení kompenzuje absence přístupových karet, které byly v rozpočtu za 11 800 Kč. Jedním z požadavků byla příprava pro stravovací systém. Pokud karty budeme chtít eliminovat úplně, lze i stravovací systém realizovat prostřednictvím biometrické čtečky. Software přiřadí určitému otisku prstu profil, ve kterém bude uložen zůstatek peněžních prostředků a podobně. Vzhledem k možnosti prolomení systémů EMmarin autor doporučuje realizovat systém založený právě na biometrickém ověření.

4.3 Využívání a vývoj RFID

V této kapitole bude autorem zhodnoceno do jaké míry je technologie RFID využívána ve vybraných odvětvích. Bude hodnocen vývoj této technologie z dostupných dat, a dále bude provedeno porovnání s jinými vybranými technologiemi.

Od roku 2009 do roku 2014 došlo v České republice téměř k dvojnásobnému nárůstu v oblasti využívání RFID technologie pro účely identifikace osob. K velkému nárůstu došlo mezi roky 2011 a 2014. Jak lze vidět v tabulce č. 2 využití této technologie pro tento účel má stoupající trend. Jedním z důvodů je i klesající cena technologie, která se tím stává dostupnější.

Tabulka č. 5. Využití RFID pro identifikaci osob v letech.

Rok	**Využití RFID pro identifikaci osob v %**
2009	2,5 %
2011	3,8 %
2014	6 %

Zdroj: Český statistický úřad, 2014.

Další významný rozdíl lze pozorovat ve využívání RFID v závislosti na velikosti podniku. Kde mezi velkými podniky byla technologie použita téměř v 27 % a mezi malými podniky pouze v přibližně 3 % případů jak můžeme vidět v tabulce č. 3. V tomto případě se nejedná pouze o využití pro účely identifikace nebo řízeného přístupu do objektů, jsou zde zahrnuty oblasti poprodejní identifikace produktů a využití pro účely logistiky, výroby a služeb.

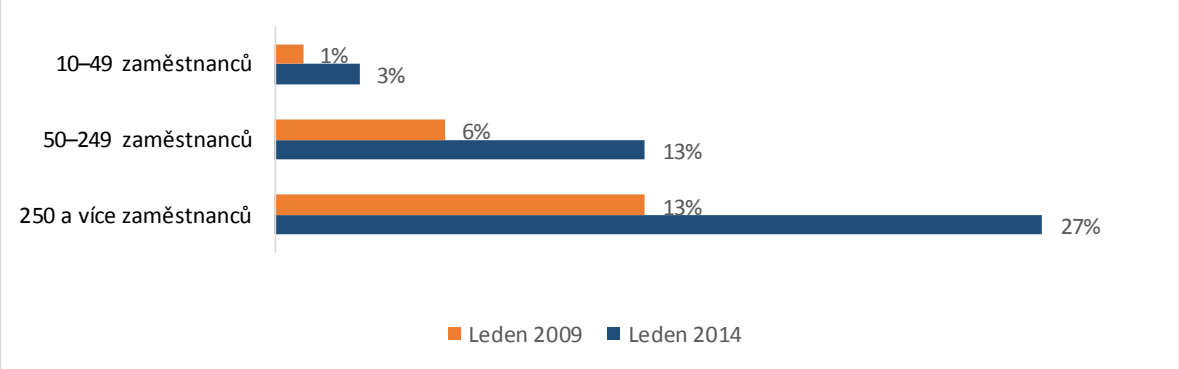
Tabulka č. 6. Využití RFID v závislosti na velikosti podniku.

Velikost podniku	**Využití RFID celkem v %**
10–49 zaměstnanců	3,3 %
50–249 zaměstnanců	13,4 %
250 a více zaměstnanců	26,6 %

Zdroj: Český statistický úřad, 2014.

V tabulce č. 2 bylo interpretováno využití technologie RFID v letech. V tabulce č. 3 vidíme velké rozdíly mezi využitím technologie v závislosti na velikosti podniku. K vývoji tedy nedocházelo pravděpodobně lineárně bez ohledu na velikost podniku. Následující graf ukazuje využití technologie pro identifikaci osob s ohledem na velikost podniku mezi roky 2009 a 2014.

Graf č. 1. Využití RFID pro identifikaci osob dle velikosti podniku.



Zdroj: Český statistický úřad, 2014.

Stejně jako je nutné zohlednit velikost podniku, tak i v různých odvětvích je tato technologie využívána rozdílně. V tabulce č. 4 je rozdělení dle účelu použití pro vybraná průmyslová odvětví.

Tabulka č. 7. Využití RFID dle účelu s ohledem na odvětví v %.

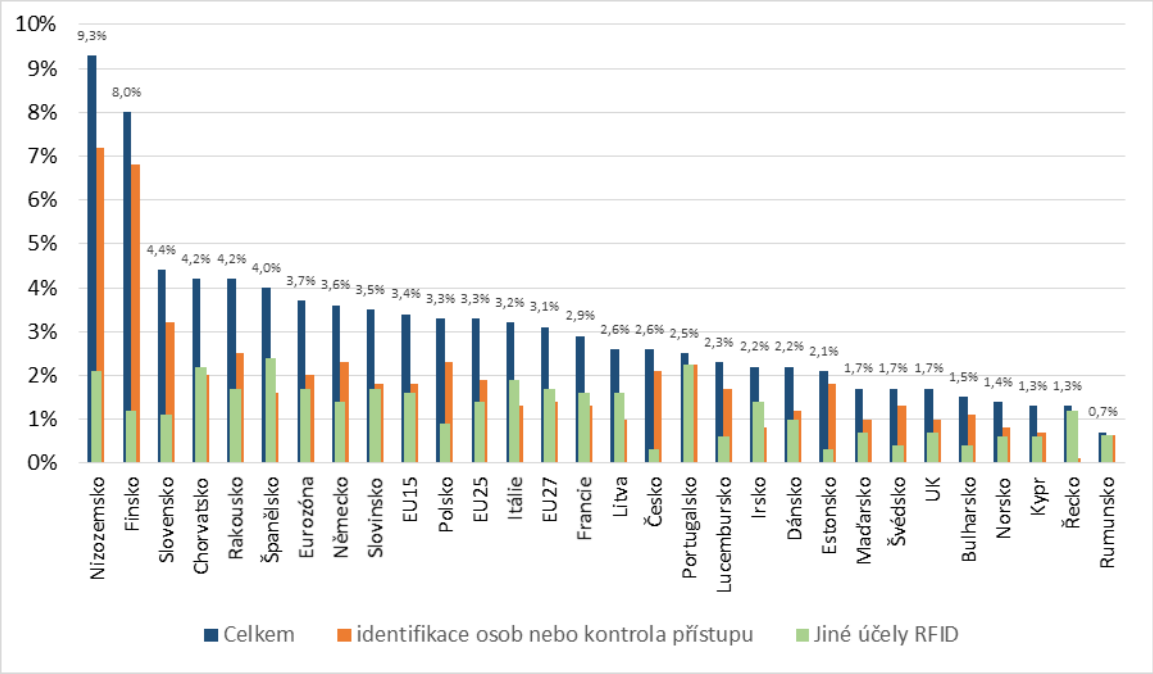
	Účel použití RFID v %.		
Odvětví	Identifikace osob / kontrola přístupu	Poprodejní identifikace produktu	Výroba, služby a logistika.
Zpracovatelský průmysl	7,6 %	0,2 %	1,9 %
Výroba a rozvod energie, plynu, tepla	7,4 %	0,4 %	1,5 %
Stavebnictví	0,7 %	0,6 %	-
Obchod; opravy motorových vozidel	4,7 %	0,9 %	0,5 %
Doprava a skladování	4,1 %	-	1,1 %
Ubytování, stravování a pohostinství	1,7 %	-	0,2 %
Informační a komunikační činnosti	13,1 %	0,9 %	1,7 %
Peněžnictví a pojišťovnictví	9,7 %	-	-
Činnosti v oblasti nemovitostí	3,3 %	-	0,2 %
Profesní, vědecké a technické činnosti	4,9 %	-	0,5 %
Administrativní a podpůrné činnosti	5,7 %	-	1,3 %

Zdroj: Český statistický úřad, 2014.

Z tabulky č. 4 vyplývá, že nejvíce byla v lednu roku 2014 využívána technologie RFID pro účely identifikace osob nebo kontrole přístupu v odvětví informačních a komunikačních činností. Naopak nejméně byla technologie zastoupena pro účely poprodejní identifikaci produktu. Další zajímavou oblastí je zemědělství, kde je tato technologie využívána pro identifikaci produktů i zvířat. Bohužel tato data nejsou sbírána.

V zemích EU je RFID technologie nejvíce využívána v Nizozemsku a Finsku přičemž průměr EU27 činil 3,1 %. V grafu č. 5 jsou uvedeny vybrané země EU a způsob využití této technologie.

Graf č. 2. RFID a způsoby jeho použití v jednotlivých zemích EU.



Zdroj: Český statistický úřad, 2009.

V roce 2009 byla tato technologie ještě minimálně využívána. V lednu roku 2009 ji využívalo přibližně jen 2,5 % podniků. Samozřejmě i v ostatních státech EU bylo zastoupení rozdílné dle velikosti podniku.

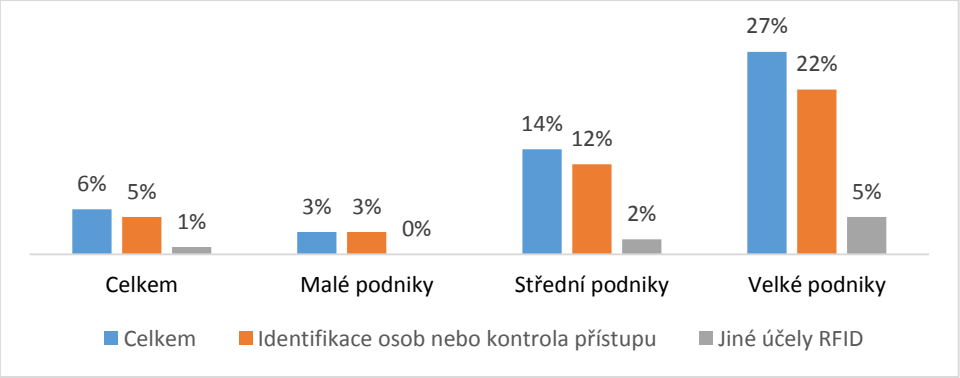
Tabulka č. 8. Využití RFID v EU v závislosti na velikosti podniku

Velikost podniku	**Využití RFID v EU celkem v %**
10–49 zaměstnanců	1,4 %
50–249 zaměstnanců	5,5 %
250 a více zaměstnanců	13 %

Zdroj: Český statistický úřad, 2009.

Hlavní využití nalezla tato technologie v identifikaci osob nebo kontrole přístupu. V České republice tomu bylo u 2,1 % podniků a k ostatním účelům ji využívalo pouze 0,5 % podniků. Autor se domnívá, že vzhledem ke stoupajícímu trendu využití technologie budou nyní tato čísla nejméně dvojnásobně větší. To potvrzují data z ledna roku 2014 v grafu č. 6. Opět můžeme pozorovat, že převládají velké podniky. Pro malé podniky zůstává tato technologie i v současné době příliš nákladná nebo nenacházejí její využití. Z dostupných dat vyplývá, že Česká republika stále zaostává za evropským průměrem.

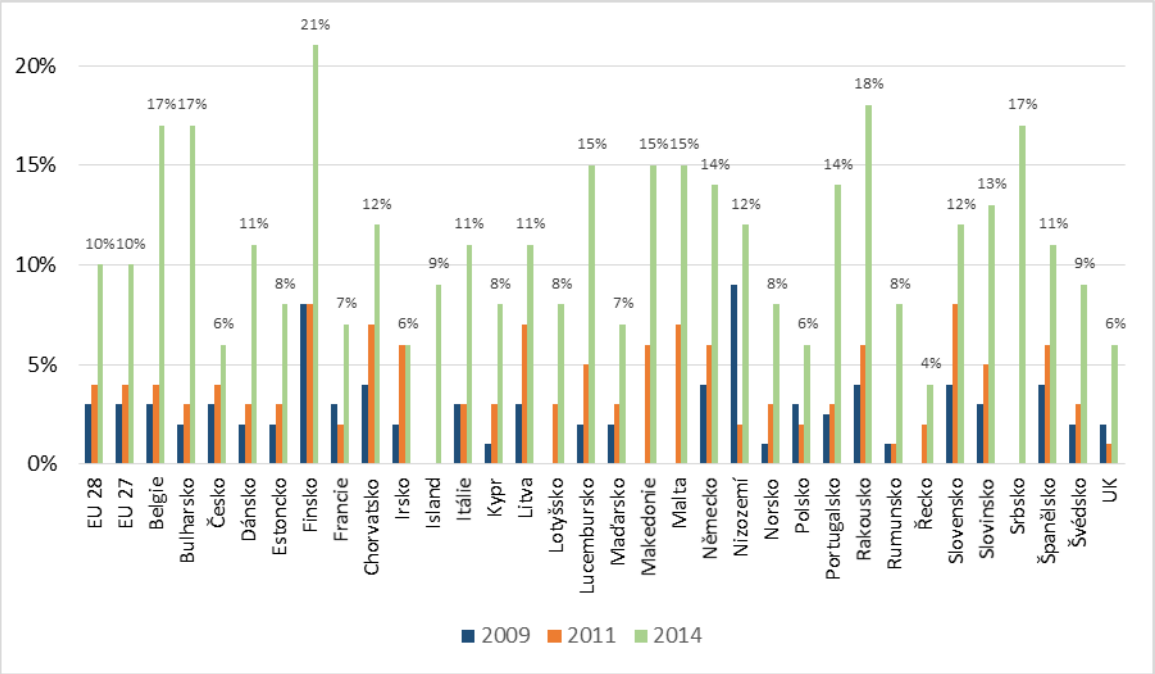
Graf č. 3. Podniky využívající RFID v České republice.



Zdroj: Český statistický úřad, 2014.

Vývoj v ostatních státech vykazuje stoupající trend stejně jako je tomu v České republice. Data v grafu č. 4 byla zaokrouhlena na celá procenta. V Německu došlo mezi roky 2011 a 2014 k trojnásobnému nárůstu používání této technologie. Ve Finsku dokonce z 8 % na 21 %. Další významný skok můžeme pozorovat v Portugalsku, kde v roce 2011 byla tato technologie využita pouze v 3 % podniků. V roce 2014 to bylo již 14 %. Lze se domnívat, že stoupající trend využití bude pokračovat i v následujících letech.

Graf č. 4. Podniky využívající RFID v rámci EU.



Zdroj: Eurostat, 2014.

Z uvedených dat je patrné, že RFID technologie má stále silný potenciál a nalézá svoje využití v nových oblastech trhu. Největší zastoupení nacházíme v identifikaci osob nebo kontrole přístupu. V současné době je často využívána v logistice pro označování zboží a tím jednodušší sledovatelnosti během logistického procesu. Lze očekávat, že publikovaná data v roce 2017 budou opět vykazovat silně rostoucí trend. Zejména proto, že technologie proniká do oblastí, kde doposud byla zastoupena pouze okrajově.

4.4 Zabezpečení bezkontaktních karet

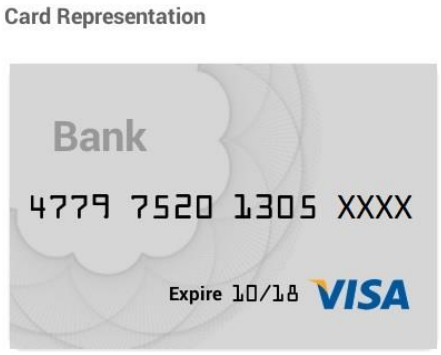
Technologie NFC je v současné době nejvíce využívána pro bezkontaktní platbu. Bezpečnost během platby je na vysoké úrovni. Zejména proto, že karta je během realizace platby zcela pod kontrolou držitele. Během transakce je aktivována čtečka platebního terminálu a na ní je karta přiložena. Přitom je nutné kartu přiložit do dvou centimetrů, aby transakce proběhla. Transakce je zabezpečena dynamickými kódy, které jsou v kartě dopočítávány. Toto opět znemožňuje načtení informací z karty jiným zařízením, ale přesto existují možnosti, jak lze kartu zneužít. Dynamické kódy by bylo teoreticky možné přečíst během komunikace karty s terminálem, kdy dochází k realizaci bezkontaktní platby. Kartu má držitel po celou dobu pod kontrolou a jedinou možností by tedy bylo, umístění upravené čtečky do těsné blízkosti platebního terminálu. Tento způsob je v praxi velmi složitý. Další možnosti útoků na NFC byly popsány v kapitole 3.3.8. Přesto existuje možnost jak získat určité informace o kartě a jejím držiteli. Tato možnost bude nyní ověřena a autor posoudí rizika plynoucí z takto získaných dat.

Pro testování byl vybrán starší model telefonu Samsung S2 Plus, který obsahuje NFC čtecí zařízení. Telefon disponuje operačním systémem Android. Upravená aplikace pro čtení karet je dostupná na internetu. Nejedná se ovšem o aplikace, kterou lze oficiálně stáhnout prostřednictvím Obchodu play, který je pro zařízení Android určen ke stahování aplikací. Na následujících obrázcích budou některé informace upraveny tak, aby nehrozilo jejich zneužití. Pro ověření byly autorem vybrány dvě platební karty. První z nich MasterCard od společnosti MONETA Money Bank, a.s. Druhou vybranou kartou byla karta VISA od společnosti Komerční banka, a.s.

4.4.1 Čtení informací z karty VISA a MasterCard

Po přiložení kreditní karty ke čtečce v telefonu dojde k nahrání informací. Potřebný čas je do dvou vteřin. Na obrázku č. 10 vidíme číslo kreditní karty a datum její platnosti po načtení informací. Číslo karty je z bezpečnostních důvodů nekompletní.

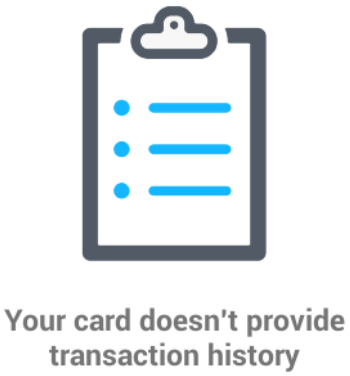
Obrázek č. 10. Číslo VISA karty po načtení informací.



Zdroj: Vlastní.

Pokud přejdeme ke čtení historie transakcí u karty VISA, historie transakcí se nezobrazí. Přestože transakce byly kartou provedeny, nelze je načíst, jak je vidět na obrázku č. 11.

Obrázek č. 11. Historie transakcí karty VISA.



Zdroj: Vlastní.

Další dostupné informace vybrané autorem vidíme na obrázku č. 12. Kde je mimo jiné opět číslo karty, ale také přesné datum platnosti, typ karty, kód země a další údaje o kartě.

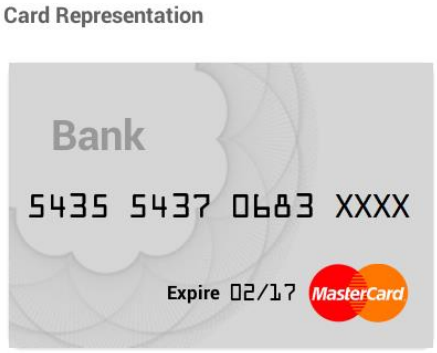
Obrázek č. 12. Informace o kartě VISA.

```
      Application
        AID: a0 00 00 00 03 10 10 (VISA Debit/Credit
(Classic))
          RID: a0 00 00 00 03
          PIX: 10 10
        Label: Visa Debit
        Preferred Name:
        Application Expiration Date: Wed Oct 31
00:00:00 CET 2018
        Issuer Country Code (ISO 3166-1): 203 (Czech
Republic)
        Application Transaction Counter (ATC): 133
        Last Online ATC Register: 122
        Primary Account Number (PAN) -
477975201305XXXX
          Major Industry Identifier = 4 (Banking and
financial)
          Issuer Identifier Number: 477XXX
          Account Number: 20130XXXX
```

Zdroj: Vlastní.

Pro kartu MasterCard bude ověřena možnost čtení stejným způsobem. Úvodní identifikace karty po načtení je na obrázku č. 13.

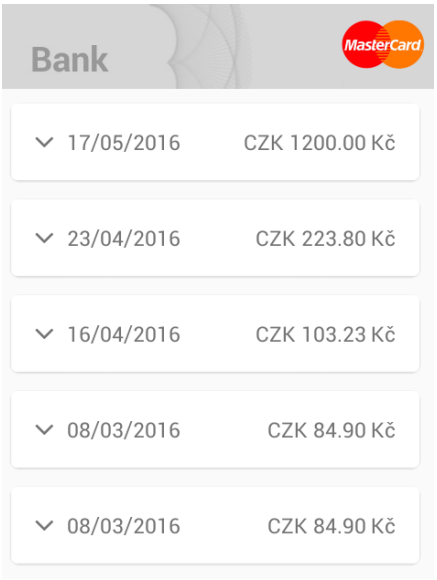
Obrázek č. 13. Číslo MasterCard karty po načtení informací.



Zdroj: Vlastní.

U karty MasterCard se podařily načíst i informace o posledních realizovaných transakcích. Výpis transakcí můžeme vidět na následujícím obrázku s číslem 14. Načteny byly poslední provedené transakce za rok 2016. Jiné informace, jako například, kde byla transakce provedena nebo přesný čas nejsou k dispozici.

Obrázek č. 14. Historie transakcí karty MasterCard.

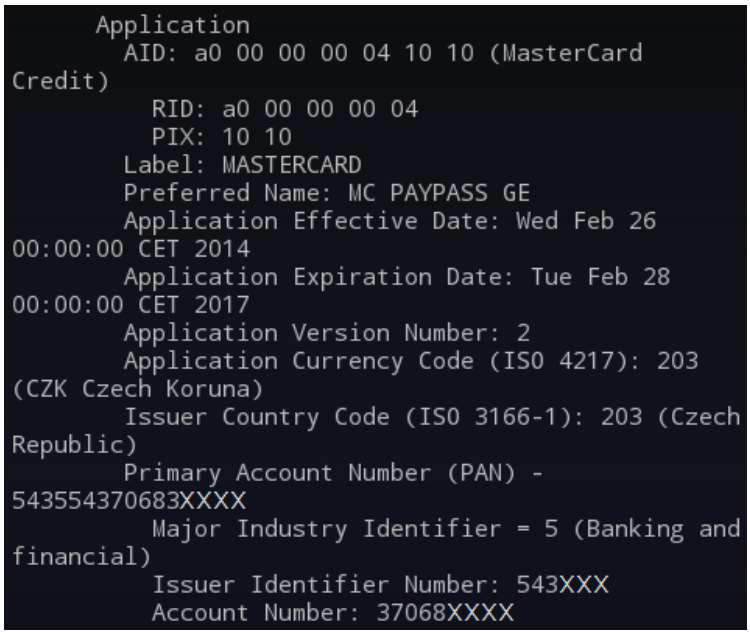


Zdroj: Vlastní.

Pokud obě karty porovnáme, hlavním rozdílem je načtení historie transakcí pro kartu MasterCard. Karta VISA pravděpodobně nedovolila načtení těchto informací. Pro ověření byla autorem použita další karta typu VISA. I po načtení jiné karty stejného typu nelze číst v historii transakcí. Z tohoto pohledu se lze domnívat, že karta VISA je proti neoprávněnému čtení lépe zabezpečená. Nicméně informace o historii transakcí není přímo zneužitelná. Na jejich základě lze, ale odhadnout, jak často je karta používána a jak velké částky jsou z účtu majitele karty odčerpávány. To může napovědět potencionálním pachatelům k určení finanční situace majitele karty.

Stejně jako v předchozím případě byly i pro kartu typu MasterCard nahrány doplňkové informace. Ty můžeme vidět na obrázku č. 15. Informace nejsou kompletní z důvodu bezpečnosti.

Obrázek č. 15. Informace o kartě MasterCard.



Zdroj: Vlastní.

Pokud data porovnáme, z karty MasterCard bylo načteno více informací. To může být i důvod, proč u karty VISA není viditelná historie transakcí. V následující kapitole budou zhodnocena rizika plynoucí z takto získaných dat. Možnosti jejich zneužití a způsoby jak se bránit nebo riziko odcizení těchto informací snížit, případně eliminovat úplně.

4.4.2 Rizika zneužití získaných dat

Na začátku této kapitoly budou shrnuta získaná data prostřednictvím upravené aplikace pro čtení platebních karet používající technologii NFC. V předchozí kategorii se autorovi podařilo získat ve velmi krátkém čase, informace o kartě, konkrétně číslo kreditní karty, typ karty a datum její platnosti. Pokud budeme hodnotit možnosti zneužití těchto informací, jako hlavní riziko autor bere v úvahu nákup přes internet - online platbu. Pro úspěšnou realizaci takové platby je nutné znát následující údaje:

- jméno majitele karty,
- číslo kreditní karty,
- datum platnosti karty,
- typ kreditní karty,
- CVV/CVC kód.

Ze získaných údajů tedy chybí jméno majitele karty a CVV/CVC kód. Jde o kód, který je uveden na zadní straně karty. Teoreticky je kód možné zahlédnout například během realizace platby jejím majitelem. Autorem použitý přístroj a software nedokázal informaci o jméně majitele karty načíst. Teoreticky je možné použít tablet na platformě Windows a za použití externí čtečky a lepšího softwaru přečíst i tuto informaci. Ovšem tím se opět zhoršuje manipulativnost a potenciální pachatel se stává nápadnějším. Pokud tedy budeme znát jméno majitele karty, stále ještě existují internetové obchody nevyžadující CVV/CVC kód k autorizaci platby. V tom případě lze takto získané informace zneužít a realizovat platbu přes internet. Těchto případů, ale není zaznamenáno velké množství. Zvýšit ochranu platební karty můžeme stejně jako u ID karet speciálním pouzdrem nebo peněženkou, která nedovolí průchod elektromagnetického pole a tak nedojde k přečtení informací z karty.

5 Výsledky a diskuse

5.1 Kopírování RFID čipů

Kopírování UID karet je v dnešní době již běžně dostupné pro širokou veřejnost. Pro technologie EMmarin pracující na frekvenci 125 kHz a technologie MiFare s frekvencí 13,56 MHz je k dispozici několik možností. Autorem vybrané zařízení může obsluhovat každý bez znalosti technologie, čipů nebo sektorů, které karta obsahuje. Bezpečnost je tedy na minimální úrovni. Ovšem již z principu kopírování vyplývá nutnost přítomnosti originální karty. Pokud dojde včas k nahlášení ztráty, případně odcizení karty, je UID karty se systému odstraněno a karta se stane nepoužitelnou pro přístup do objektu. Při použití silné antény je možné karty kopírovat i na vzdálenost několika metrů, aniž by majitel měl tušení, že jeho karta byla zkopírována. Vytvořené kopie karet byly v praxi otestovány ve dvou na sobě nezávislých firmách, používající jiné zařízení i software. V obou firmách byla kopie karty bez problému použita a přístup do objektu povolen. Teoreticky by bylo možné vyrobit generátor náhodných UID. Zařízení by po přiložení na čtečku každou vteřinu vyslalo náhodně vygenerované UID. Vzhledem k desetimístnému číslu by trvalo vygenerování známého UID pro systém v extrému i 30 let. Pro dešifrování karet MiFare Classic, kde je použito šifrování CRYPTO-1, je již nutná znalost problematiky a technologie. Pro tuto práci byla použita stará karta Fit-Centra, která dnes již není používána. Provozovatel byl obeznámen dodavatelem o možných rizicích a systém upravil pro karty typu MiFare DESFire EV1, které dnes stále patří mezi bezpečné.

5.2 Přístupové systémy

Tato práce představila možnosti realizace přístupových systémů s ohledem na jejich bezpečnost. Součástí práce jsou i rozpočty pro jednotlivé typy přístupových systémů. Na základě získaných informací a provedených pokusů je systém postaven na biometrickém ověřování otisku prstu bezpečnější, je zde eliminována hrozba vyplývající z možnosti kopírovaní UID karet. Nicméně i tato technologie přináší jisté úskalí. Zejména v podobě s problémem detekce mokrých prstů, se kterou se autor setkal během testování biometrické čtecí jednotky Sebury. Pro konkrétní firmu musí být připraven systém, který vyhovuje požadavkům zadání projektu a charakteristice projektu.

5.3 Zabezpečení bezkontaktních karet

Bezkontaktní karty jsou v dnešní době velice dobře zabezpečeny. Riziko zneužití informací z karty je minimální. Jsou ovšem možnosti, kdy lze informace z karty přečíst a následně zneužít. V poslední době se objevovaly upravené bankomaty, které obsahovaly čtecí zařízení přímo vedle pravé čtečky bankomatu. Toto technické řešení je ovšem náročné na instalaci. V této práci byly otestovány dvě platební karty prakticky dostupnými metodami široké veřejnosti. Některé informace z karty byly přečteny, ale možnost jejich zneužití nebyla prokázána. Teoreticky lze za bezpečnější považovat kartu VISA, u které se za použití vybraného softwaru, nepodařilo přečíst historii realizovaných transakcí. Další zabezpečení, pozorované autorem, spočívalo v nemožnosti použití bezkontaktní platby. Po přečtení informací, prostřednictvím mobilního telefonu s NFC čtečkou, nebylo možné kartu bezkontaktně použít k platbě. Bylo nutné kartu použít v terminálu, včetně zadání kódu PIN. Následující bezkontaktní transakce, již proběhla v pořádku. Autor se domnívá, že zabezpečení karet je v současné době na vysoké úrovni a nehrozí vážnější rizika. V každém systému, ať již v platebním nebo jiném, existují možnosti jak ochranu zvýšit. Ve většině případů, ale dochází ke snížení komfortu během používání a toto je důvod, proč pro platbu do 500 Kč není vyžadován PIN. Pokud Vám bude karta odcizena a budou provedeny bezkontaktní platby, většina bankovních institucí po prokázání krádeže, tyto platby vrací. Stále je nutné přemýšlet nad zabezpečením, protože v budoucnosti, by dnes bezpečné platební karty mohly o svoji bezpečnost přijít.

6 Závěr

Cílem diplomové práce bylo ověření kopírování UID čipů technologie RFID a prolomení šifrování CRYPTO-1 použité ve značně rozšířených kartách MiFare Classic. Tato práce neslouží jako návod na prolomení ochrany, a proto také nezveřejňuje žádné detaily použitých karet pro kopírování, jako jejich klíče, informace obsažené v čipu nebo jednotlivá UID použitých karet. Teoretická část formou literární rešerše popisuje historie technologií RFID a NFC, princip jejich komunikace a využití. Práce zahrnuje problematiku standardizace a legislativní aspekty jednotlivých technologií. Popsány jsou i zařízení využívající tyto bezdrátové komunikace v praxi. Představeny jsou nejčastěji využívané RFID Tagy a jejich rozdělení. Bezpečnosti technologií je věnována velká pozornost a v práci jsou popsány známé i teoretické možnosti útoků. První část vlastní práce se věnuje přímo kopírování RFID čipů a technologii MiFare Classic, kde je použito šifrování CRYPTO-1. V obou případech byly dokázány možnosti kopírování karet a následné použití vytvořených kopií v praxi. Z tohoto důvodu je v současné době vhodnější použití technologie MiFare DESFire EV1. Není ovšem zaručeno, jak dlouho bude tato technologie bezpečná a časem se dá předpokládat i prolomení zabezpečení použité u této karty.

Využití identifikačních systémů a technologií se postupně stává běžnou součástí našich životů. Velké množství firem využívá pro realizaci kontroly přístupu do objektů právě technologii RFID, které je věnována druhá část vlastní práce. Ve druhé části vlastní práce jsou navrhnuty přístupové systémy, včetně systému docházkového pro fiktivní firmu o sto osmdesáti zaměstnancích. Autorem byly zvoleny dva způsoby identifikace. Prvním byla bezdotyková identifikace pomocí karet využívajících technologie EMmarin a jejich bezpečnost s ohledem na možnosti kopírování UID, která není na vysoké úrovni. Z tohoto důvodu byl navrhnut druhý identifikační systém, založený na biometrickém ověření otisku prstu. Celková realizace tohoto systému byla o 11 128 Kč levnější, než systém založený na čtení UID z karet. Autor s ohledem na bezpečnost a cenovou náročnost upřednostňuje biometrický systém. Pokud pomineme náklady, odpadá i problematika manipulace s kartou, případně její zapomenutí nebo ztráta. RFID a NFC jsou dynamicky se rozvíjející technologie a v budoucnosti se jejich využití rozšíří. Můžeme očekávat implementaci například v automobilovém průmyslu, kde bude prostřednictvím RFID nebo NFC čipů zajištěn větší komfort majitelům vozů.

Technologie NFC nalézá v současné době největší využití v bezkontaktních platbách. V této práci bylo dokázáno, že lze z bezkontaktní platební karty v krátkém čase vyčíst určité informace. Autorem bylo posouzeno, že jejich zneužití, není vždy možné. Nepodařilo se zjistit jméno majitele karty a také CVV/CVC kód, který se nalézá na zadní straně karty. Bez těchto údajů není možné realizovat platbu přes internet ani jiné úkony vedoucí ke zneužití originální karty. Samotná platba je zabezpečena dynamickými kódy, které jsou v kartě dopočítávány. Teoreticky lze během tohoto přenosu informace odposlechnout, ale nutností je speciální zařízení. Autor doporučuje jakým způsobem ochranu zvýšit. Prvním doporučením je speciální obal, který vytváří kolem karty tzv. Faradayovu klec. Druhou možností je speciální peněženka, která pracuje na stejném principu, jako obal karty. Levnější investicí může být neprůhledný obal karty, který dovoluje realizaci bezkontaktní platby, ale znemožňuje přečtení CVV/CVC kódu z karty. V budoucnosti bude muset i stávající systém pokročit ve svém zabezpečení.

7 Seznam použitých zdrojů

[1] SARKAR Tapan K. and col. History of Wireless. Vydavatel: J. Wiley, 2006. ISBN: 978-0471783015.

[2] MENKEN Ivanka. Near Field Communication Complete Certification Kit - Core Series for IT. Vydavatel: Emereo Publishing, 2013. ISBN: 978-1486458219.

[3] NÁPRSTEK Miloslav. Co je near field communication. Dostupné na WWW: <http://www.nfctech.cz/co-je-near-field-communication>

[4] AHSON Syed A., ILYAS Mohammad. Near Field Communications Handbook. Vydavatel: CRC Press, 2011. ISBN: 978-1420088144.

[5] RANKL Wolfgang, EFFING Wolfgang. Smart Card Handbook. Vydavatel: Wiley-Blackwell, čtvrtá edice, 2010. ISBN: 978-0470743676.

[6] COSKUN Vedat, OK Kerem, OZDENIZCI Busra. Near Field Communication (NFC): From Theory to Practice. Vydavatel: Wiley – Blackwell, 2011. ISBN: 978-1119966906.

[7] ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. Všeobecné oprávnění č. VO-R/10/05.2014-3. Dostupné na WWW: <http://www.ctu.cz/vseobecne-opravneni-c-vo-r10052014-3>

[8] SHEPARD Steven. RFID: Radio Frequency Identification. Vydavatel: McGraw-Hill Professional, 2004. ISBN: 978-0071442992.

[9] POSLANECKÁ SNIMOVNA PARLAMENTU ČESKÉ REPUBLIKY. Předpis 17/2003 Sb. Dostupné na WWW: <http://www.psp.cz/sqw/sbirka.sqw?cz=17&r=2003>

[10] POSLANECKÁ SNIMOVNA PARLAMENTU ČESKÉ REPUBLIKY. Předpis 88/2010 Sb. Dostupné na WWW: <http://www.psp.cz/sqw/sbirka.sqw?cz=88&r=2010>

[11] POSLANECKÁ SNIMOVNA PARLAMENTU ČESKÉ REPUBLIKY. Předpis 490/2009 Sb. Dostupné na WWW: <http://www.psp.cz/sqw/sbirka.sqw?cz=490&r=2009>

[12] POSLANECKÁ SNIMOVNA PARLAMENTU ČESKÉ REPUBLIKY. Předpis 616/2006 Sb. Dostupné na WWW: <http://www.psp.cz/sqw/sbirka.sqw?cz=616&r=2006>

[13] SBÍRKA ZÁKONŮ: Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1. ledna 2015.
Dostupné z WWW: < https://www.uoou.cz/zakon-c-101-2000-sb-o-ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu-ve-zneni-ucinnem-od-1-ledna-2015/ds-3109/archiv=0&p1=1261>

[14] NORMA ISO/IEC 7816. Dostupné z WWW:
< http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx>

[15] NORMA ISO/IEC 7810. Dostupné z WWW:
< http://everything.explained.today/ISO%2FIEC_7810/>

[16] NXP SEMICONDUCTORS. Smart Label and Tag ICs. Dostupné z WWW:
<http://www.nxp.com/products/identification-and-security/smart-label-and-tag-ics:MC_71109>

[17] NXP SEMICONDUCTORS. HITAG. Dostupné z WWW:
<http://www.nxp.com/products/identification-and-security/smart-label-and-tag-ics/hitag:MC_42027>

[18] NXP SEMICONDUCTORS. SmartMX Controllers. Dostupné z WWW:
<http://www.nxp.com/products/identification-and-security/security-controller-ics/smartmx-controllers:MC_53567>

[19] NXP SEMICONDUCTORS. MIFARE® ICs. Dostupné z WWW:
<http://www.nxp.com/products/identification-and-security/mifare-ics:MC_53422>

[20] EM Microelectronic-Marin SA. Overview and Positioning. Dostupné z WWW:
<http://www.emmicroelectronic.com/node/20>

[21] COLE Peter H., RANASINGHE Damith C. Networked RFID Systems and Lightweight Cryptography: Raising Barriers to Product Counterfeiting. Vydavatel: Springer Science & Business Media, 2007. ISBN: 978-3540716419.