

# **Identifikace firemních objektů s využitím technologie NFC v mobilních zařízeních**

Identification of Company Sites using NFC Technology in Mobile  
Devices

Bc. Jiří Grigar

---

Diplomová práce  
2015

 Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2014/2015

## ZADÁNÍ DIPLOMOVÉ PRÁCE (PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Jiří Grigar**  
Osobní číslo: **A13417**  
Studijní program: **N3902 Inženýrská informatika**  
Studijní obor: **Informační technologie**  
Forma studia: **prezenční**

Téma práce: **Identifikace firemních objektů s využitím technologie NFC v mobilních zařízeních**

Téma anglicky: **The Identification of Company Sites Using NFC Technology in Mobile Devices**

Zásady pro vypracování:

1. Vypracujte literární řešení na dané téma.
2. Popište aktuální trendy v oblasti bezdrátové komunikace NFC.
3. Zhodnoťte zabezpečení NFC čipů a datových přenosů, diskutujte možné útoky na tyto čipy.
4. Zvolte vhodné šifrování pro komunikaci s NFC čipy.
5. Vytvořte mobilní aplikaci v jazyce Delphi, pomocí které bude možné identifikovat firemní objekty s využitím technologie NFC.

Rozsah diplomové práce: 67s.

Rozsah příloh: 2

Forma zpracování diplomové práce: tištěná/elektronická

Seznam odborné literatury:

1. IGOE, Tom, Don COLEMAN a Brian JEPSON. Beginning NFC: near field communication with Arduino, Android, and Phoneygap. Vyd. 1, 2014. ISBN 14-493-7206-6.
2. PAAR, Christof. Understanding cryptography: a textbook for students and practitioners. Heidelberg: Springer, 2010. ISBN 978-3-642-04100-6.
3. TEIXEIRA, Steve. Mistrovství v Delphi 6. Vyd. 1. Praha: Computer Press, 2002. ISBN 80-722-6627-6.
4. COSKUN, Vedat, Kerem OK a Busra OZDENIZCI. Professional NFC application development for Android. Chichester, Wiley, 2013. ISBN 978-111-8380-093.
5. PERIS LOPEZ, Pedro, Julio C HERNANDEZ-CASTRO a Tieyan LI. Security and trends in wireless identification and sensing platform tags: advancements in RFID. 2013. ISBN 978-146-6619-920.
6. HOWARD, Michael a David LEBLANC. Bezpečný kód. Vyd. 1. Brno: Computer Press, 2008. ISBN 978-80-251-2050-7.

Vedoucí diplomové práce:

Ing. Radek Vala

Ústav informatiky a umělé inteligence

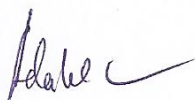
Datum zadání diplomové práce:

6. února 2015

Termín odevzdání diplomové práce:

15. května 2015

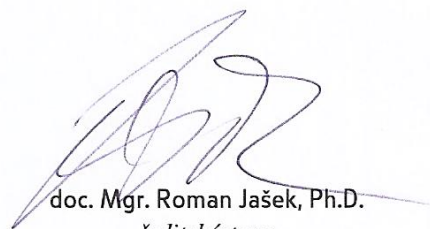
Ve Zlíně dne 6. února 2015



doc. Mgr. Milan Adámek, Ph.D.  
děkan



L.S.



doc. Mgr. Roman Jašek, Ph.D.  
ředitel ústavu

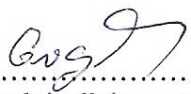
### **Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí. Že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejména § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen přibouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vvrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, podř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

### **Prohlašuji,**

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné

Ve Zlíně 13.5.2015

  
.....  
podpis diplomanta

## **ABSTRAKT**

Diplomová práce se zabývá technologií NFC, pomocí které bude možné identifikovat firemní objekty. V rámci teoretické části bude provedena rešerše dané technologie, kde bude kladen důraz především na bezpečnost čipů a datových přenosů. Praktická část bude založena na vytvoření aplikace v jazyce Delphi. Pomocí ní bude možno číst NFC čipy jednotlivých objektů s využitím mobilních zařízení. Dále bude provedena komunikace typu klient-server se vzdáleným ukládáním dat do databáze.

Klíčová slova: NFC, RFID, čipové karty, Mifare, AES šifrování, Delphi, Android, SQL

## **ABSTRACT**

Diploma thesis deals with NFC technology, through which it will be possible to identify company sites with using mobile devices. Research of the technology will performed, which will focus especially on chip security and data transfer. The practical part will be based on creating mobile application in Delphi language. Application will allow read NFC chips of individual objects using mobile devices. Next part will be communication client-server with remote data storage in a database.

Keywords: NFC, RFID, smart cards, Mifare, AES cryptography, Delphi, Android, SQL

Rád bych poděkoval Ing. Radku Valovi, PhD. za odborné vedení diplomové práce a velmi cenné rady při tvorbě teoretické i praktické části. Dále bych chtěl poděkovat mé rodině a přítelkyni za podporu, poskytnutí zázemí a trpělivosti během mého studia.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

# OBSAH

<b>ÚVOD</b> .....	<b>9</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>10</b>
<b>1 ZÁKLADY NFC A RFID</b> .....	<b>11</b>
1.1 CO JE RFID .....	11
1.2 CO JE NFC .....	12
1.3 ČIPOVÉ KARTY .....	13
1.3.1 SCOS.....	13
1.3.2 Kontaktní.....	14
1.3.3 Bezkontaktní .....	15
1.3.4 Hybridní .....	16
1.4 HISTORICKÝ VÝVOJ .....	16
<b>2 VLASTNOSTI A PRINCIPY</b> .....	<b>19</b>
2.1 STRUKTURA ČIPU .....	19
2.2 POUŽÍVANÉ ZAŘÍZENÍ .....	20
2.3 REŽIMY PŘENOSU .....	21
2.3.1 Čtení/Zápis .....	21
2.3.2 Peer-to-Peer.....	23
2.3.3 Emulace karty.....	24
2.4 NDEF FORMÁT .....	26
2.5 ARCHITEKTURA NFC .....	27
2.6 TYPY NFC ČIPŮ.....	28
2.7 SROVNÁNÍ S OSTATNÍMI TECHNOLOGIEMI .....	29
<b>3 KRYPTOLOGIE A ŠIFROVÁNÍ</b> .....	<b>31</b>
3.1 ZÁKLADNÍ ROZDĚLENÍ .....	31
3.2 SYMETRICKÉ ŠIFRY .....	32
<b>4 BEZPEČNOST NFC</b> .....	<b>34</b>
4.1 PŘEHLED POPULÁRNÍCH KARET .....	34
4.1.1 Výrobci čipů.....	34
4.1.2 Karty Mifare.....	35
4.2 ZÁKLADNÍ TYPY ÚTOKŮ .....	36
4.2.1 Odposlech.....	36
4.2.2 Přepojování .....	36
4.2.3 Postranní kanál .....	36
4.2.4 Klonování obsahu.....	36
4.2.5 Kryptoanalytický.....	37
4.2.6 Přerušené spojení .....	37
4.3 ÚSPĚŠNÉ ÚTOKY.....	37
4.3.1 Útok na Mifare Classic.....	37
4.3.2 Útok na Mifare DESFire .....	38
4.3.3 Útok na Mifare Ultralight.....	39
4.4 PROTIPATŘENÍ.....	39
4.4.1 Serverové ověřování.....	39

4.4.2	Blacklist.....	39
4.4.3	Dynamická změna hesla.....	40
4.4.4	Izolace karty .....	40
4.4.5	Vhodné šifrování .....	40
4.4.6	Využití hashovacích funkcí.....	40
<b>II</b>	<b>PRAKTICKÁ ČÁST .....</b>	<b>41</b>
<b>5</b>	<b>DOKUMENTACE POD NDA .....</b>	<b>42</b>
5.1	INFORMACE V NDA .....	42
5.2	DOKUMENTACE KARET MIFARE DESFIRE EV1 .....	42
5.2.1	Získání dokumentů.....	43
5.2.2	Zabezpečení dokumentů.....	43
5.2.3	Data sheet .....	43
5.2.4	Dokumentace vybraných příkladů .....	44
<b>6</b>	<b>POUŽITÉ TECHNOLOGIE A NÁSTROJE .....</b>	<b>45</b>
6.1	EMBARCADERO RAD STUDIO XE7 .....	45
6.1.1	Rozhraní vývojového prostředí .....	45
6.1.2	Programovací jazyky.....	46
6.2	SQLITE .....	46
6.3	SAMSUNG GALAXY S3 .....	47
6.3.1	Konfigurace mobilního telefonu .....	47
6.3.2	Android SDK .....	48
6.4	VOLBA ČIPOVÝCH KARET .....	48
<b>7</b>	<b>VYTVOŘENÉ APLIKACE .....</b>	<b>49</b>
7.1	ENTERPRISE ARCHITECT .....	49
7.1.1	Diagram užití.....	49
7.1.2	Diagram tříd .....	51
7.2	KOMUNIKACE SE SERVEREM .....	51
7.3	KLIENSKÉ APLIKACE .....	52
7.3.1	Uživatelská.....	52
7.3.2	Administrátorská .....	53
7.4	OŠETŘENÍ VSTUPNÍCH PARAMETRŮ .....	54
<b>8</b>	<b>ZABEZPEČENÍ ČIPOVÝCH KARET .....</b>	<b>56</b>
8.1	ŠIFROVÁNÍ AES .....	56
8.2	KONTROLNÍ SOUČTY CRC.....	57
8.3	CBC REŽIM .....	57
8.3.1	Režim šifrování .....	57
8.3.2	Režim dešifrování .....	58
	<b>ZÁVĚR .....</b>	<b>59</b>
	<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>60</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>63</b>
	<b>SEZNAM OBRÁZKŮ .....</b>	<b>65</b>
	<b>SEZNAM TABULEK.....</b>	<b>66</b>
	<b>SEZNAM PŘÍLOH.....</b>	<b>67</b>

## ÚVOD

Diplomová práce se zabývá technologií NFC a jejím využitím v mobilních zařízeních. První kapitola popisuje základní termíny jako NFC a RFID, dále pak souhrnnou historii a jednoduché principy. Následující kapitola rozebírá již NFC z technologického hlediska, kde byl kladen důraz především na jednoduchý a názorný popis. Kapitola se věnuje také podrobnému rozboru jednotlivých datových přenosů. Třetí kapitola slouží jako jednoduchý úvod do kryptologie a popis souvisejících základních pojmů, které lze v diplomové práci najít. Poslední kapitola teoretické části se zabývá bezpečností technologie NFC a datových přenosů. Popisuje základní možné útoky, se kterými se můžeme při použití technologie setkat. Následně jsou uvedeny známé útoky spolu s různými protiopatřeními.

Praktická část se zabývá vytvořenými aplikacemi, které jsou napsané všechny v jazyce Delphi. Základní zadání bylo pro mne vytvořit mobilní aplikaci umožňující číst NFC čipy. Tyto čipy by měly být umístěny na různých místech firemních objektů. Poté členové bezpečností ostrahy firmy budou vždy při své obchůzce čipy číst a tímto bude zaznamenána jejich trasa obchůzky. Čip tedy bude pomyslným spouštěčem dalších úkonů, jako jsou např. zaznamenání času, data, jména ostrahy do databáze apod. Hlavním úkolem není vytvořit pouze mobilní aplikaci, ale zaměřit se také na bezpečnost NFC. Musí být zajištěno především to, aby dané karty nešly zkopírovat či emulovat.

Diplomovou práci jsem vypracovával ve spolupráci firmy Cathedral Software s.r.o., ve které jsem dříve vykonával povinnou praxi v rámci školy. Firma mi poskytla pro tvorbu především svůj vlastní čas, velmi cenné rady a pracovní nástroje nutné k vytvoření aplikací. Výsledek diplomové práce bude sloužit především jako technologické demo znázorňující základní principy a použití jednotlivých komponent a technologií. Tyto principy budou později využity k nasazení do reálného projektu a bude je možné využít pro další účely.

## **I. TEORETICKÁ ČÁST**

## 1 ZÁKLADY NFC A RFID

Identifikace na základě rádiové frekvence (RFID) se stává běžným jevem v každodenním životě. S technologií se setkáváme u bezkontaktních platebních karet, MHD, přístupových systémů, plateb mytného apod. Nejvíce je nám však známé použití v obchodech jako zabezpečující prvek proti krádeži a také k identifikaci zboží. V posledních několika letech se začal objevovat v souvislosti s RFID také termín NFC. Pokud se ve svém okolí zeptáte co to je, nebo jaký je rozdíl mezi RFID a NFC, mnoho lidí Vám nedokáže odpovědět. Pro začátek stačí uvést, že technologie NFC se postupně vyvinula z RFID a nabízí širší možnosti použití oproti starší technologii. Tato kapitola si klade za cíl seznámení s technologií NFC a jeho využití v běžném životě.

### 1.1 Co je RFID

RFID je zkratkou anglických slov Radio Frequency Identification, což znamená identifikace na rádiové frekvenci. Jednoduché příklady RFID čipů můžeme vidět na Obr. 1. První patent na tuto technologii získal Charles Walton již v roce 1983.



*Obr. 1. RFID čipy (tagy) [8], [9]*

Princip komunikace se pokusím vysvětlit na následujících jednoduchých příkladech. Představte si, že sedíte v noci na verandě a rozsvítíte světlo. Poté můžete vidět osoby, které se blíží k Vašemu domu, jelikož se světlo odráží zpět k Vám. Na základě odraženého světla můžete např. poznat, že jde o souseda. Tomuto popisu odpovídá pasivní komunikace. Tedy RFID čtečka vysílá rádiový signál, který následně nabíjí čip a ten „odráží“ zpět svou identitu. [1]

Nyní si představte podobnou situaci, že sedíte na verandě, rozsvítíte světlo a soused také. Pokud na souseda zamáváte a on to uvidí, může také „odpovědět“ a zamávat. Tomuto popisu pak odpovídá aktivní komunikace. Tedy obě RFID zařízení vytváří svůj rádiový

signál, pomocí kterého mohou komunikovat. To může vést k většímu dosahu komunikace obou zařízení. Obecně technologie RFID není brána jako komunikační, ale zejména jako identifikační. Je to z důvodu malého dosahu signálu a přenosových rychlostí. Proto se velikost paměti čipů pohybuje v řádech tisíce bajtů. [1]

## 1.2 Co je NFC

NFC je zkratkou anglických slov Near Field Communication, což znamená komunikace v blízkém poli. Jinak řečeno, jedná se o bezdrátovou technologii, která slouží ke komunikaci mezi dvěma elektronickými zařízeními. Komunikace probíhá na velmi krátkou vzdálenost, obvykle několik milimetrů až jednotek centimetrů. [6]



*Obr. 2. InKarta s NFC čipem [10]*

NFC technologie vychází přímo z principů RFID, přičemž umožňuje složitější operace mezi zařízeními. Stále můžete číst pasivní RFID čipy s čtečkou NFC nebo také zapisovat data do jejich omezené paměti. NFC umožňuje zápis dat do určitých druhů RFID čipů pomocí standardního formátu nezávisle na typu značky a výrobce. Dále je možná komunikace s ostatními zařízeními v duplexním nebo poloduplexním módu. NFC zařízení si mohou mezi sebou vyměňovat informace o svých schopnostech, uložené záznamy nebo zahájit dlouhodobou vzájemnou komunikaci. [1]

Dnes se setkáváme i s kombinací různých technologií, typicky NFC spolu s WiFi či Bluetooth. Příkladem může být párování mobilního telefonu s chytrými reproduktory. Povolením NFC na mobilním telefonu a následným dotykem s reproduktory dojde ke spárování. Samotný přenos hudby z mobilního telefonu do reproduktorů probíhá skrze Bluetooth či WiFi. Proč se data neposílají rovnou skrze NFC technologii? Prvním důvodem je především krátký dosah, obvykle do 10 cm nebo méně. To umožňuje nízkou spotřebu energie vysílače a také nedochází k rušení s dalšími rádiovými zařízeními.

Druhým důvodem je relativně nízká přenosová rychlost v porovnání s WiFi, Bluetooth nebo dalšími komunikačními protokoly. NFC není určena pro vysokorychlostní přenos dat, ale pro výměnu krátkých zpráv, výměnu ověřovacích údajů nebo k zahájení komunikace.

Nejzajímavější na technologii NFC je to, že umožňuje pro sofistikované činnosti jednoduché použití, např. zvládne bez potíží změnu hesla, párování zařízení a všechny ostatní složitější kroky, které přicházejí s tímto protokolem. To znamená, že pokud si budete chtít s přáteli vyměňovat telefonní kontakty nebo platit pomocí telefonu bezkontaktně, není nic jednoduššího než prostý dotyk obou zařízení. Obecně je platná bezpečnost přenosu informací, kdy si sami určujete, co se poslat může a co nikoliv. Přijímací zařízení nemá nikdy přístup k celé paměti vysílacího zařízení. [1]

### 1.3 Čipové karty

Čipová karta obsahuje zabudovaný integrovaný obvod s paměťovou jednotkou a také často zabezpečeným mikrořadičem. Tato struktura je vhodná pro efektivní uchování, zpracování a přenos dat v bezpečném multiaplikačním prostředí. Typický systém se skládá z čtecího zařízení, samotných čipových karet a obslužného systému. Takovýto systém může komunikovat pomocí fyzického kontaktu (kontaktní čipové karty) nebo vzdáleně (bezkontaktní čipové karty). Čtečka je připojena k obslužnému systému, který uchovává, zpracovává a řídí veškerá data.

Čipové karty můžeme rozdělit dle zpracování dat na: paměťové a mikroprocesorové. Paměťové čipové karty mohou ukládat data, ale potřebují k tomu externí jednotku. Mikroprocesorové čipové karty mohou ukládat větší množství dat a provádět vlastní operace, jako je např. vzájemná autentizace čtečky a karty. Tyto karty mají svůj vlastní operační systém, který se označuje zkratkou SCOS (Smart Card Operating System). V dnešní době se setkáváme častěji s rozdělením na základě provozních mechanismů na čipové karty: kontaktní, bezkontaktní a hybridní. [4]

#### 1.3.1 SCOS

Až do konce roku 1990 bylo vzhledem k omezení struktury paměti velmi obtížné, aby na čipové kartě běželo více aplikací než pouze jedna. S rozvojem SCOS přichází trend použití několika aplikací na jedné čipové kartě. To nám umožňuje dynamičtější využití multiaplikačních platforem, kdy se snažíme mít např. jízdenky, identifikaci a vstupenky v podobě jedné karty. V dnešní době každá chytrá čipová karta obsahuje svůj vlastní

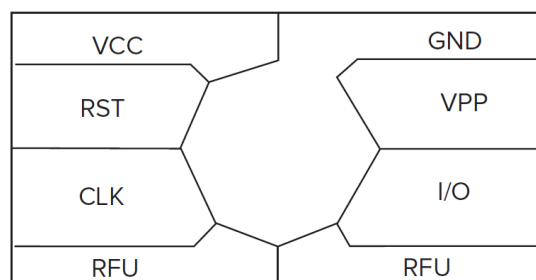
SCOS, který může být definován jako soubor instrukcí uložených v paměti ROM. Mezi základní prvky tohoto systému řadíme:

- správa přenosů mezi čipovou kartou a externím zařízením (př. pokladní terminál)
- správa uložených dat v paměti karty
- řízení přístupů k informacím
- správa zabezpečení čipových karet, zejména v oblasti integrity dat
- správa životního cyklu využití karty

Dříve byly aplikace nebo služby na čipové kartě psány pouze pro specifické OS (operační systémy). To znamenalo, že se museli dohodnout dodavatelé karet, vývojáři aplikací a poskytovatelé systému. Zákazníci tak potřebovali pro každou službu zvláštní čipovou kartu, což bylo nákladné a neefektivní. [4]

### 1.3.2 Kontaktní

Jako kontaktní čipové karty označujeme ty karty, které obsahují modul s pamětí a mikroprocesorem. Tento modul je vodivá kontaktní deska na povrchu čipové karty a ve většině případů je pozlacena. Externí zařízení poskytuje přímý elektrický kontakt k vodivému modulu. Přenos příkazů, dat a informací o stavu karty probíhá přes tyto fyzické kontaktní místa. Karty neobsahují žádný zdroj elektrické energie, proto jsou považovány za pasivní. Jako externí zařízení mohou sloužit počítače, pokladní terminály, tablety nebo mobilní telefony. Čipové karty s platebními terminály jsou typickým příkladem platebního styku. Ve skutečnosti mají čipové karty pro platební operace stejnou hardwarovou strukturu jako SIM karty v mobilních telefonech. Hlavním rozdílem je odlišné naprogramování. Související normy s čipovými kartami jsou ISO/IEC 7810 a ISO/IEC 7816. Ty definují fyzický tvar, elektrické pozice konektorů, elektrické vlastnosti a komunikační protokoly. Na Obr. 3 můžeme vidět fyzickou strukturu kontaktů. Popis jednotlivých kontaktů je uveden v následující tabulce (Tab. 1). [4]



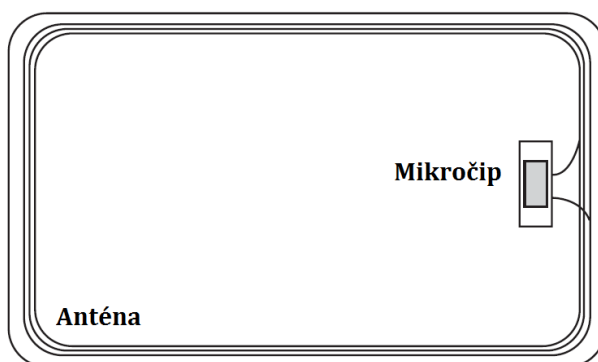
Obr. 3. Fyzická struktura kontaktů [4]

Tab. 1 Popis kontaktů čipových karet

Kontakt	Funkce
VCC	napájení
RST	reset mikroprocesoru
CLK	hodinový signál
RFU	vyhrazeno pro budoucí použití
GND	zem
VPP	programovací nebo zapisovací napětí
I/O	sériový vstup/výstup

### 1.3.3 Bezkontaktní

Bezkontaktní čipová karta je druh karty, kde jsou data přenášena pomocí fyzického kontaktu s externím zařízením. Jedná se o kombinaci mikročipu a antény, která umožňuje datové přenosy, viz Obr. 4.



Obr. 4. Struktura bezkontaktní čipové karty [4]

Anténa je obvykle tvořena několika dráty. Data jsou uložena v mikročipu, který se skládá z mikroprocesoru a interní paměti. Na rozdíl od kontaktních čipových karet je zde energie dodávaná skrze anténu bezdrátově z externího zařízení. Výměna dat mezi kartou a čtečkou probíhá pomocí antény a elektromagnetického pole, které poskytne dostatečnou energii k přenosu dat. Bezkontaktní karty mají schopnost bezpečně spravovat a ukládat data. Obvyklá je také funkce vzájemné autentizace karty a čtečky. [4]

Bezkontaktní technologie se používá v aplikacích, kde je kladen důraz na zabezpečení informací jako je zdraví, údaje totožnosti, peněžní transakce, elektronické pasy apod. Karty jsou dostupné v několika provedeních, např. plastové karty, přívěšky na klíče nebo

doklady. V současné době existují tři hlavní standardy pro bezkontaktní čipové karty: ISO/IEC 10536, ISO/IEC 14443 a ISO/IEC 15693.

#### 1.3.4 Hybridní

Hybridní čipové karty jsou kombinací kontaktních a bezkontaktních karet. Obvykle karta obsahuje dva mikročipy, kdy je jeden použit pro kontaktní a druhý pro bezkontaktní rozhraní. Oba tyto mikročipy jsou vzájemně nezávislé. Příkladem mohou být dnešní platební karty MasterCard s technologií NFC.

### 1.4 Historický vývoj

Historie moderních počítačů zahrnuje práci, která byla provedena v průběhu posledních 200 let. Osobní počítače (PC) byly důležitým krokem od počátků prvních počítačů. Změnily způsob, jakým uživatelé s počítači komunikují, a to od dřevných štítků a kabelů, po dnešní podobu klávesnice, myši a monitoru. Uživatelé si postupem času zvykli na používání myši, kdy pohybem ruky a prstu mění polohu kurzoru na displeji. [4]

Dotykové obrazovky posunuly formu interakce ještě dále. Odstranily potřebu předchozích vstupních zařízení a dotyk s obrazovkou pomocí prstu se stal novým trendem. Tohoto vývoje se drží především nejrychleji se rozvíjející trh s mobilními telefony, resp. smartphony. Pro mnohé uživatele je používání dotykového displeje mnohem intuitivnější, navíc se dotyková plocha stává jak vstupním, tak výstupním zařízením. Konzervativnější uživatelé stále preferují mobilní telefony s tlačítky, tzv. feature phone, které stále vydrží nabitě i celý pracovní týden.

Všudypřítomná výpočetní technika je v dnešní době v nejvyšší interakci mezi lidmi a počítači. Výpočetní zařízení jsou plně integrovány do každodenního života. Asi málo z nás si již dokáže představit pracovní den bez počítače, notebooku, mobilního telefonu apod. Technika se nám snaží přizpůsobovat, což vede ve většině případů k větší mobilitě a produktivitě.

Stejně jako oblast moderních počítačů, tak oblast mobilní komunikace je také důležitým krokem v rozvoji výpočetní techniky. Mobilní telefony měly ještě před zavedením NFC mnoho možností, jak komunikovat s vnějším prostředím. Při představení původních telefonů byl cíl jasný, umožnit hlasovou komunikaci. GSM komunikace postupně umožnila několik služeb:

- hlasová komunikace
- krátké textové zprávy (SMS)
- multimediální zprávy (MMS)
- video telefonie
- přístup k Internetu

Dále se o rozvoj bezdrátových technologií zasloužilo zavedení GPS, WiFi, či IrDA. Nové technologie změnily způsob, jakým mobilní telefony dnes používáme. Později byla představena technologie Bluetooth, která pomocí PAN sítě spojuje periferní zařízení s počítači. Tato technologie se stala velmi populární a používá se dodnes. V jeden okamžik téměř nahradila starší technologii IrDA, která se v posledních letech stala opět oblíbenou, především díky možnosti využití mobilního telefonu jako ovladače k televizím. [4]

Aktuálním trendem v mobilních telefonech je nasazení technologie NFC, která nám postupně vstupuje do každodenního života. Za počátek objevení technologie NFC se považuje rok 2004. Pokud však půjdeme dále do historie, musíme si uvědomit, že prvotní myšlenkou jednoduché bezdrátové komunikace byly čárové kódy (rok 1949). Z jednoduchých čárových kódů se později odvozovaly další kódy, např. pro nás dnes běžně známé na obalech zboží (EAN), nebo také Data Matrix, QR kódy apod. Jako konkurent pro čárové kódy byly poprvé patentovány v roce 1983 RFID čipy. Následníkem RFID čipů jsou pak samotné NFC čipy, které jsou postaveny na standardech organizace NFC Forum. Dále zde uvedu některá důležitá data týkající se především technologie NFC čerpaná data z literatury [11].

**2002:** firmy Sony a Philips se dohodly na nové technologii komunikace prostřednictvím NFC a stanovili technický přehled.

**2004:** firmy Nokia, Sony a Philips zakládají neziskovou organizaci NFC Forum.

**2006:** první specifikace pro technologii NFC tagů.

**2006:** první mobilní telefon Nokia 6131 s technologií NFC.

**2009:** vytvoření standardů pro přenos kontaktů, URL, inicializaci Bluetooth apod.

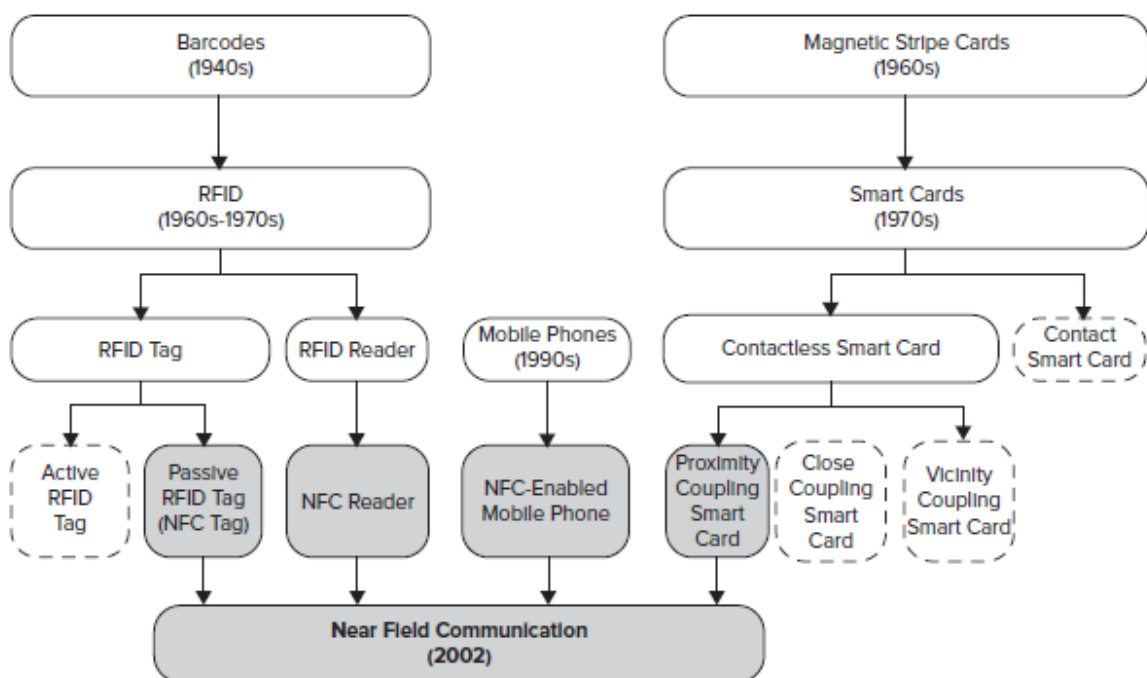
**2010:** první telefon s Androidem využívající NFC, Samsung Nexus S.

**2011:** RIM je první firmou, jejíž zařízení jsou firmou MasterCard Worldwide certifikovány pro funkci MasterCard PayPass.

**2012:** firma Sony představuje chytré čipy (Smart Tags), které umožňují změnu režimů a profilů na svých mobilních telefonech.

**2014:** firma Apple oznamuje produkt Apple Pay (mobilní platby a digitální peněženka), který je dostupný pro zařízení iPhone 6, iPhone 6 Plus a hodinky Apple Watch.

Na následujícím obrázku je uveden kompletní historický vývoj a oblasti spojené s technologií NFC. Šedé buňky zachycují oblasti technologií, které přímo ovlivnily NFC.



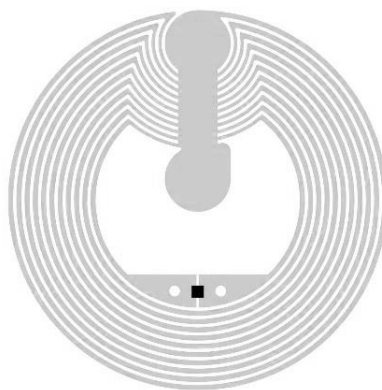
Obr. 5. Vývoj technologie NFC [4]

## 2 VLASTNOSTI A PRINCIPY

NFC je bezdrátová technologie komunikující až do vzdálenosti 10 cm. V dnešní době se většinou setkáváme se vzdáleností kratší, řádově v jednotkách milimetrů, kdy je zapotřebí čip přiložit (dotknout se) ke čtecímu zařízení. NFC má pro komunikaci vyhrazené frekvenční pásmo 13.56 MHz, které bylo voleno tak, aby žádná z jejích harmonických nezasáhla do jiných vysokofrekvenčních zařízení. Maximální přenosová rychlost je 424 kb/s, tedy technologie není vhodná pro přenos objemných dat. Základem jsou standardy ISO/IEC 14443, JIS X 6319 (FeliCa) a ISO/IEC 18092, jenž jsou rozšiřovány o další technické specifikace, které definují komunikaci mezi dvěma NFC zařízeními. [12]

### 2.1 Struktura čipu

Čipy NFC, označovány také jako štítky či tagy, jsou pasivní součástky, tedy neobsahují přímé napájení (baterii). Napájeny jsou samotnou čtečkou prostřednictvím elektromagnetické indukce. Ke své funkci vyžadují velmi malou energii (řádově desítky mikrowattů). Každý tag se skládá se dvou základních částí – malého čipu a relativně rozměrné antény.



Obr. 6. Struktura NFC čipu [14]

Jak si můžeme všimnout z Obr. 6, tak samotný čip (černý čtvereček) je poměrně malý oproti velmi rozměrné anténě. Skrze anténu probíhá přenos energie i dat, a platí, že anténa musí být dostatečně velká na to, aby byla komunikace možná. S velikostí antény pak úzce souvisí citlivost příjmu. Samotný čip obsahuje kromě paměti, kde jsou uložena data, i řídicí jednotku a kondenzátor, který akumuluje energii naindukovanou na anténě. [14]

Tvary NFC tagů mohou být téměř libovolné, obvykle se setkáváme s hranatými či kulatými samolepkami, v podobě přívěšků, klíčenek či fólií, náramků apod. Omezení tvaru nesouvisí pouze s velikostí čipu a antény, ale také s umístěním na kov. Ten může signál tagu tlumit, nicméně se dnes můžeme setkat i se speciálními odstíněnými samolepkami, které na kov umístit lze.

## 2.2 Používané zařízení

**Mobilní telefony** s podporou NFC jsou nejvýznamnějšími zařízeními. Integrace NFC do mobilních telefonů je velkou příležitostí pro snadné použití, rozšíření a přijetí technologie NFC. V dnešních době se NFC vyskytuje u mobilních telefonů, které přesahují hranici asi 5 000 Kč, nejedná se tedy o samozřejmost.

**NFC čtečky** jsou zařízení, které jsou schopné přenášet a číst data z jiných zařízení nebo čipů. Nejběžnějším příkladem jsou bezkontaktní platební terminály podporující NFC platby.

**NFC tag (štítek)** je čip, který nemá integrovaný zdroj napájení. Běžně použití je v platebních kartách, chytrých vizitkách, přístupových systémech apod.

NFC technologie pracuje intuitivním způsobem, kdy přiložením dvou zařízení vyvoláme spuštění události. Typicky mezi sebou obě zařízení zahájí komunikaci a začnou vyměňovat data. Dnešní aplikace jsou navrženy tak, že když se s mobilním telefonem dotknete jiného zařízení, obvykle nastane automaticky určitá akce, např. otevření webové stránky prohlížeče.

Pro každou komunikaci rozlišujeme 2 základní označení zařízení. Stranu, která zahájila komunikaci, označujeme jako *zdrojové zařízení* (iniciátor). Zařízení, jenž reaguje na požadavky od zdroje, nazýváme *cílové zařízení*. V následující tabulce můžeme vidět různé druhy zařízení, které spolu mohou komunikovat.

Tab. 2 Možné druhy komunikace mezi dvěma zařízeními

<b>Zdrojové zařízení</b>	<b>Cílové zařízení</b>
Mobilní telefon	NFC tag
Mobilní telefon	Mobilní telefon
NFC čtečka	NFC tag
NFC čtečka	Mobilní telefon

Zdrojové zařízení musí být vždy aktivním zařízením, jelikož vyžaduje zdroj napájení pro zahájení komunikace. Cílové zařízení může být aktivní nebo pasivní. Pokud je cílové zařízení aktivní, využívá svůj vlastní zdroj energie na reakce od cílového zařízení. Naopak pokud je cílové zařízení pasivní, využívá energie generované ze zdroje. NFC tag je nízkonákladové zařízení, proto je vždy pasivním prvkem. Neobsahuje žádný zdroj energie a potřebuje pro svou činnost energii ze zdrojového zařízení. Obvykle ukládá data, která může zdrojové zařízení číst. [4]

### 2.3 Režimy přenosu

Režimy přenosu technologie NFC rozlišujeme na 2 základní typy – aktivní a pasivní. Každý typ se liší v napájení zařízení.

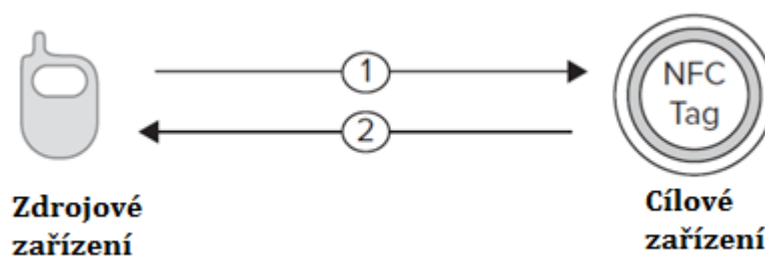
- Aktivní – 2 aktivní (napájené) zařízení
- Pasivní – 1 aktivní a 1 pasivní zařízení

Častěji se dnes setkáváme s rozdělením podle způsobu využití: čtení/zápis, peer-to-peer a emulace karty. Služby používané v každém NFC zařízení se liší v závislosti na používaných NFC objektech. Každý režim přenosu má své vlastnosti, proto je možné definovat modely využití pro každý režim. V následujících podkapitolách jsou popsány základní charakteristiky obecných režimů přenosů. [4]

#### 2.3.1 Čtení/Zápis

Režim čtení/zápis se používá pro standardní čtení a zápis z čipu, resp. do čipu. V obou případech je tag napájen ze zdroje elektromagnetického záření a čip sám o sobě je pasivní součástí. Tento režim definuje dva různé způsoby použití, a to režim čtečky a režim zapisovače. [7]

V režimu čtení čte zdrojové zařízení data z NFC čipu, který obsahuje požadované údaje. Specifikace těchto čipů upravuje organizace NFC Forum. Kromě požadovaných dat obsahuje čip také obvod, který tyto data poskytuje. V režimu zápisu zdrojové zařízení zapisuje požadované data do NFC čipu. Pokud je paměť čipu zaplněna, data budou přepsána. Nicméně algoritmus může být navržen tak, aby se místo přepisu pouze aktualizovaly požadované informace. Pro oba možné režimy lze bez problému využít dnešní telefony s podporou technologie NFC. Obecně patří tento režim přenosu k nejpoužívanějším. Schématické znázornění je uvedeno na následujícím obrázku. [4]



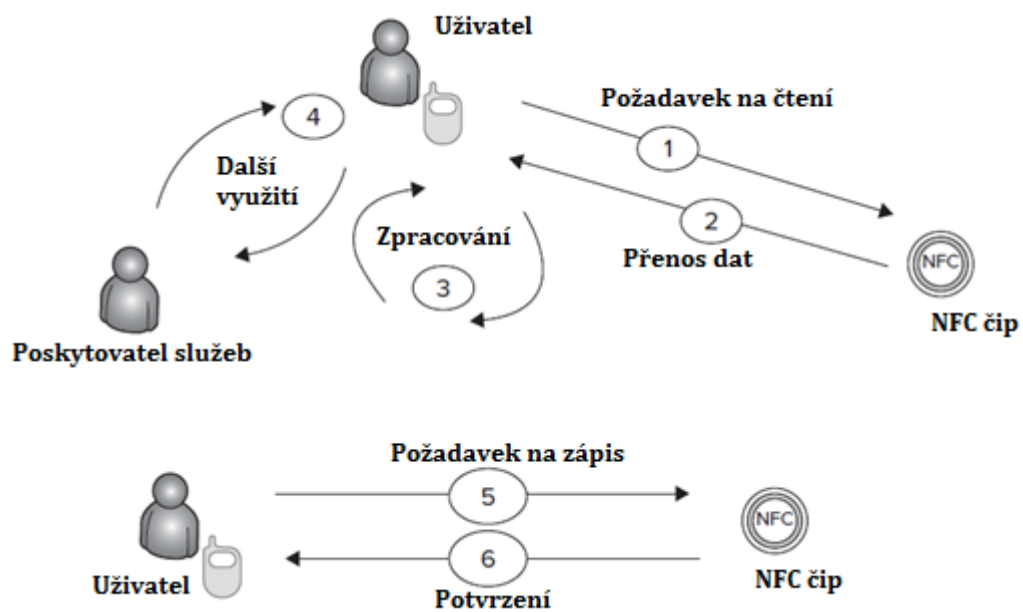
Obr. 7. Režim přenosu čtení/zápis [4]

Mobilní telefon může provést několik akcí po tom, jakmile přečte data z čipu. Pokud čip obsahuje URL adresu, může telefon spustit webový prohlížeč a zobrazit načtenou stránku. Mezi výhody mobilního telefonu řadíme výpočetní výkon, audio/video schopnosti a přístup k Internetu, který poskytuje mnoho možností s využitím tohoto režimu. V oblasti mobilního telefonu jako čtecího/zapisovacího zařízení je více možností, jenž mohou být velmi inovativní se spojením stávajících systémů.

### Praktické využití režimu čtení/zápis

Využití režimu se pokusím objasnit v následujících krocích. Tyto kroky jsou také zobrazeny na Obr. 8.

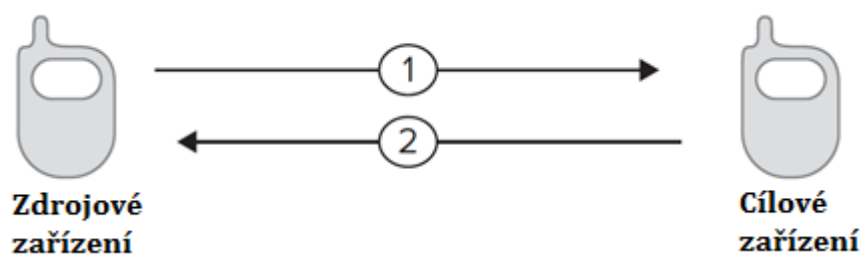
- 1) Požadavek na čtení: uživatel požaduje data, kdy se dotkne mobilním telefonem NFC čipu. Čip může být v podobě různých typů a tvarů, typicky jako inteligentní plakáty, vizitky, klíčenky apod.
- 2) Přenos dat: Data uložená v čipu se přenesou do mobilního telefonu.
- 3) Zpracování: Jakmile jsou data odeslána do mobilního zařízení, mohou být použity pro různé účely, jako je spuštění aplikace, zobrazení dat uživateli, nebo sloužit k pozdějšímu zpracování.
- 4) Další využití: Tento volitelný krok využívá pokročilých vlastností, především připojení mobilního telefonu k Internetu. Když jsou data zpracována mobilním telefonem, mohou být skrze Internet dále použita např. ve webové službě pro další aplikace.
- 5) Požadavek na zápis: Uživatel požaduje zapsat data dotykem mobilního telefonu s NFC čipem.
- 6) Potvrzení: Mobilní telefon odešle požadovaná data a čip „odpoví“ o úspěšném potvrzení operace.



Obr. 8. Praktické použití režimu čtení/zápis [4]

### 2.3.2 Peer-to-Peer

Naopak v režimu Peer-to-Peer probíhá komunikace mezi dvěma aktivními zařízeními. Tohoto způsobu se využívá pro vzájemnou výměnu informací, kontaktů, textových zpráv apod. Komunikace probíhá v poloduplexním módu, tedy pouze jedním směrem, kdy obě strany mohou přijímat i vysílat, ale nikoliv současně. Schématické znázornění je uvedeno na Obr. 9. [7]



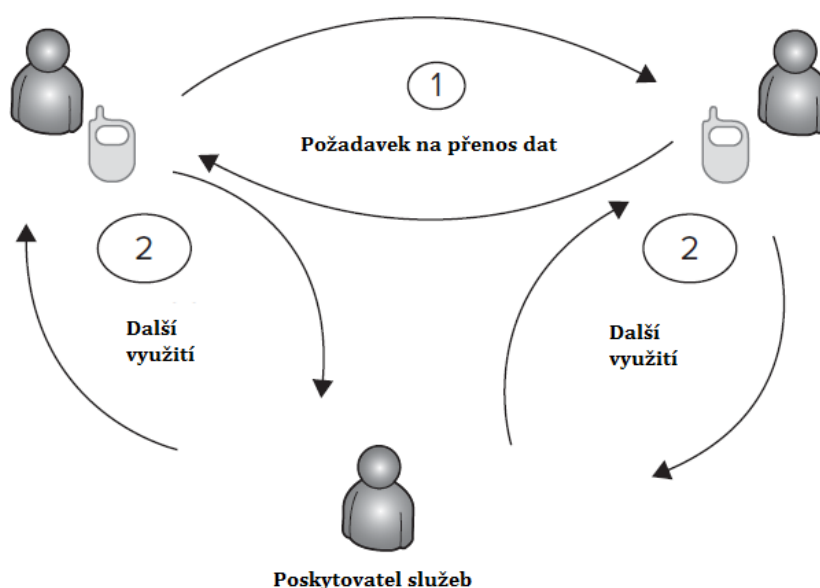
Obr. 9. Režim přenosu peer-to-peer [4]

#### Praktické využití režimu peer-to-peer

V režimu peer-to-peer mezi sebou uživatelé komunikují pomocí dvou aktivních (napájených) zařízení – mobilních telefonů. Při základním typu komunikace se u tohoto režimu nevyužívá poskytovatel služeb. Pokud uživatelé chtějí využívat některých služeb

Internetu, bývá dodatečně zahrnut do procesu také poskytovatel služeb. Praktické použití režimu rozdělím do následujících kroků. Tyto kroky jsou také znázorněny na Obr. 10.

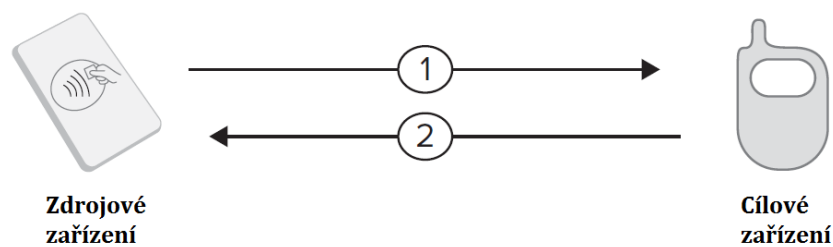
- 1) Požadavek na přenos dat: dva uživatelé mezi sebou požadují výměnu dat skrze mobilní telefony.
- 2) Další využití: Jakmile jsou data mezi mobilními telefony úspěšně vyměněna, mohou být dále použity pro další účely, jako je ukládání přijaté vizitky do databáze skrze Internet. Po dokončení nahrání může také dojít k navázání přátelství skrze sociální síť.



Obr. 10. Praktické použití režimu peer-to-peer [4]

### 2.3.3 Emulace karty

Režim emulace karty umožňuje to, aby se aktivní NFC zařízení chovalo jako pasivní čip. Komunikace probíhá podobně jako v režimu čtení/zápis. Tento způsob můžeme použít typicky při platbě mobilním telefonem. Zajímavé na tomto režimu je to, že mobilní telefon může v sobě uchovat několik typů emulovaných karet. Schématické znázornění je uvedeno na Obr. 11. [7]



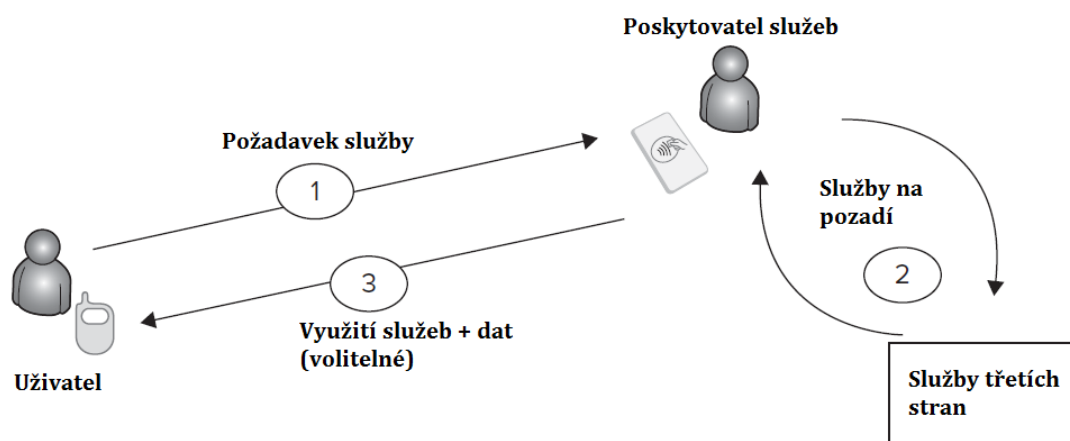
Obr. 11. Režim přenosu emulace karty[4]

Při tomto režimu nevytváří mobilní telefon (cílové zařízení) své vlastní rádiové pole, ale pouze tento signál přijímá ze zdrojového zařízení. Toto chování je zajímavé, protože mobilní telefon je aktivní zařízení a klidně by mohl využívat své vlastní energie. V současné době jsou podporovány následující komunikační protokoly: ISO/IES 14443 Typ A, Typ B a Felicia. Tento režim přenosu je důležitý především díky možnosti bezkontaktních plateb či prodeji vstupenek. To je praktické řešení, jelikož je vše kompatibilní se stávající infrastrukturou. [4]

### Praktické využití režimu emulace karty

V režimu emulace karty mezi sebou obvykle komunikují čtečka a také mobilní telefon, který zastupuje NFC čip. Čtečka je typicky připojena přes poskytovatele služeb do Internetu. Praktické použití režimu rozdělím do několika kroků. Tyto kroky jsou také znázorněny na Obr. 12.

- 1) Požadavek služby: uživatel vytvoří požadavek na poskytovatele služeb tím, že se dotkne mobilním telefonem čtecího zařízení. Požadované údaje se přenáší skrze čtecí zařízení k poskytovateli služeb.
- 2) Služby na pozadí: zprostředkovatelská služba běží na pozadí pro získání dat od uživatele. Příkladem může být ověření kreditní karty nebo ověření vstupenek.
- 3) Využití služeb + dat (volitelné): poskytovatel služeb vrací informace zpět uživateli, jako jsou úspěšné zaplacení zboží, vystavení jízdenky nebo povolení platby.



Obr. 12. Praktické použití režimu emulace karty [4]

## 2.4 NDEF formát

Údaje přenášené mezi dvěma zařízeními je možné formátovat pomocí NDEF (NFC Data Exchange Format). O tomto termínu pravděpodobně v budoucnu uslyšíte více, jelikož se jedná o klíčové vylepšení technologie RFID. Jedná se o univerzální datový formát, který pracuje se všemi NFC zařízeními bez ohledu na výrobce čipu nebo zařízení. Každá zpráva NDEF obsahuje jeden nebo více NDEF záznamů. Každý takový záznam má svůj vlastní typ, jedinečný identifikátor, délku a data, která nese. Existuje několik běžných typů záznamů, na které může mobilní telefon nebo jiné zařízení reagovat. [1]

### Textové záznamy

Textové záznamy obsahují jakýkoliv řetězec, který chcete poslat. Tyto záznamy obvykle neobsahují pokyny pro cílové zařízení. Do této skupiny řadíme i metadata indikující jazyk a kódové schéma (například UTF-8). Tento typ záznamu jsem zkusil poslat na NFC kartu přes mobilní telefon a karta neměla problém s uložením českých znaků s diakritikou.

### URI

URI (Uniform Resource Identifier) obsahují webové adresy. Zdrojové zařízení, které tento typ záznamu přijímá, očekává, že přečtený záznam přímo otevře aplikaci, jež dokáže záznam zobrazit, typicky webový prohlížeč.

### Intelligentní plakáty

Intelligentní plakáty obsahují data, která přímo poskytují více informací o zobrazovaném objektu – filmu, výstavě nebo koncertu. Mohou také obsahovat dohromady URL adresy nebo textové zprávy, se kterými lze dále pracovat. Zdrojové zařízení tyto informace přijímá a může po přečtení záznamu otevřít webový prohlížeč, SMS nebo emailovou aplikaci v závislosti na obsahu zprávy.

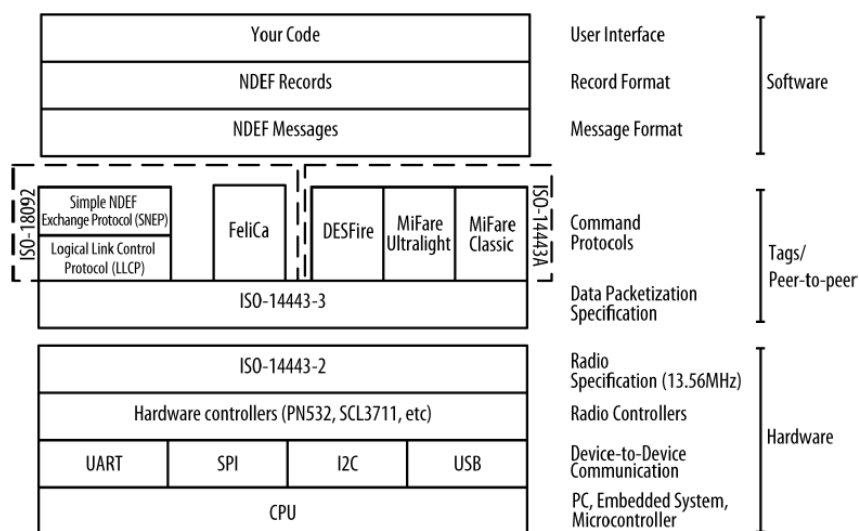
### Podpisy

Podpisy poskytují způsob, jak poskytnout důvěryhodné informace o původu údajů obsažených v záznamu NDEF.

Obecně lze záznamy ve zprávě NDEF kombinovat nebo je možné poslat jeden záznam v jedné NDEF zprávě. NDEF je jedním z důležitých technických rozdílů mezi NFC a RFID. NFC i mnoho RFID protokolů komunikuje na frekvenci 13.56 MHz, ale RFID nemohou formátovat svá data do formátu NDEF. RFID protokoly nemají žádný společný protokol pro formát dat, tak jako je tomu u NFC.

## 2.5 Architektura NFC

Abychom správně pochopily NFC technologii, je vhodné zavést referenční model architektury. Tento model si rozdělíme na několik základních částí. Nejnižší vrstvu tvoří fyzický model obsahující procesor (CPU) a rádiová zařízení, která zajišťují komunikaci. Uprostřed jsou údaje (pakety) transportní vrstvy, následuje vrstva dat a nakonec zdrojový kód aplikace. Jednotlivé vrstvy jsou zobrazeny na Obr. 13.



Obr. 13. Jednotlivé vrstvy architektury NFC [1]

NFC pracuje na fyzické vrstvě 13.56 MHz na základě principů RFID, které popisuje ISO 14443-2. Další vrstva popisuje rozdělení dat do rámců před odesláním a je upravena na základě standardu ISO 14443-3. Pro jakékoliv rádiové zařízení můžeme použít oddělené hardwarové komponenty a to buď v telefonu, tabletu, mikropočítači nebo osobním počítači. Tyto komponenty komunikují s procesorem zařízení pomocí jednoho nebo více standardních protokolů: univerzální asynchronní sériové rozhraní UART (Universal Asynchronous Receive Transmit), sériové periferní rozhraní SPI (Serial Peripheral Interface), multimasterová sběrnice I<sup>2</sup>C (Interintegrated Circuit Communication) nebo univerzální sériové sběrnice USB (Universal Serial Bus). Hardwarovým nadšencům jsou známě pravděpodobně první 3 rozhraní, softwarovým pak jen USB. [1]

Nad fyzickou vrstvou se nachází několik protokolů založených na příkazech. Základní čtení a zápis do NFC čipu je založen na původním ISO 14443A. Čipy Mifare od firmy NXP Semiconductors (divize Philips) jsou s ISO 14443A kompatibilní. Režim přenosu peer-to-peer je založen na protokolu ISO 18092. Čipy FeliCa od firmy Sony, známé především v Japonsku, jsou založeny také na této normě. [1]

Jedním z dalších rozdílů mezi RFID a NFC je podpora režimu přenosu peer-to-peer. K dispozici jsou dva protokoly, které řídí komunikaci mezi zařízeními v tomto režimu: LLCP (Logical Link Control Protocol) a SNEP (Simple NDEF Exchange Protocol). Dalším rozdílem mezi RFID a NFC je výměna dat na základě zpráv NDEF probírané v předcházející kapitole.

## 2.6 Typy NFC čipů

V zásadě existují 4 typy NFC čipů definované organizací NFC Forum, které jsou všechny založeny na komunikačních protokolech popsanych v předchozí kapitole. Dle literatury [1] jsou čipy typu 1, 2 a 4 upraveny normou ISO 14443A a typ 3 je definován normou ISO 18092. Vlastnosti následujících typů jsou přebrány z literatury [1].

### Typ 1

- založen na specifikaci ISO 14443A
- nejjednodušší a nejlevnější typ
- může být pouze pro čtení nebo pro čtení a zápis
- velikost paměti od 96 B po 2 kB
- přenosová rychlost 106 kb/s

- bez ochrany kolize dat
- příklad: Innovision Topaz, Broadcom

### Typ 2

- stejné vlastnosti jako Typ 1
- bez zabezpečení
- podpora anti-kolize dat
- příklad: NXP - Mifare Ultralight

### Typ 3

- čipy založené na Sony FeliCa (ISO 18092, JIS-X-6319-4)
- bez šifrování a autentizace
- může být pouze pro čtení nebo pro čtení a zápis
- velikost paměti až 1 MB
- přenosová rychlost 212 nebo 424 kb/s
- podpora anti-kolize dat
- příklad: Sony FeliCa

### Typ 4

- stejně jako typ 1 a 2 založeny na specifikaci ISO 14443A
- může být pouze pro čtení nebo pro čtení a zápis
- velikost paměti až 64 kB
- přenosová rychlost 106, 212 nebo 424 kb/s
- podpora anti-kolize dat
- příklad: NXP – Mifare DESFire, SmartMX-JCOP

## 2.7 Srovnání s ostatními technologiemi

Největší výhodou bezdrátové komunikace je především mobilita, která má velký dopad na každodenní život okolo nás. Mobilní komunikace podporují nejen produktivitu, ale také společenský život, jelikož mohou lidé zůstat trvale spojeni skrze sociální sítě. Mezi nejpoužívanější technologie sem můžeme zařadit GSM, 3G, LTE, WiFi a WiMAX. [1]

V následující tabulce je uveden stručný přehled celosvětově používaných bezdrátových technologií. Tabulka zobrazuje porovnání dle parametrů pracovního dosahu, frekvence

a přenosové rychlosti. Uvedené parametry jsou pouze teoretické, v praxi se setkáváme obvykle s nižšími hodnotami.

*Tab. 3 Srovnání bezdrátových technologií*

<b>Technologie</b>	<b>Frekvence</b>	<b>Přenosová</b>	<b>Dosah</b>
<b>UMTS</b>	900, 1800, 1900 MHz	300 Mb/s	široký rozsah
<b>GPRS, EDGE</b>	900, 1800, 1900 MHz	160 Kb/s	široký rozsah
<b>802.16 WiMAX</b>	10 – 66 GHz	134 Mb/s	1 - 4,8 km
<b>802.11b/g WiFi</b>	2,4 GHz	54 Mb/s	100 m
<b>802.11 a WiFi</b>	5 GHz	54 Mb/s	100 m
<b>802.15 Bluetooth 2.1</b>	2,4 GHz	3 Mb/s	10 m
<b>802.15 Bluetooth 4.0</b>	2,4 GHz	200 kb/s	100 m
<b>NFC</b>	13,56 MHz	106 - 424	4 cm
<b>RFID</b>	125 – 134 kHz (LF) 13,56 MHz (HF) 400 – 930 MHz (UHF) 2,5 GHz, 5 GHz (SHF)	1 – 200 kb/s	20 cm pasivní 400 cm aktivní

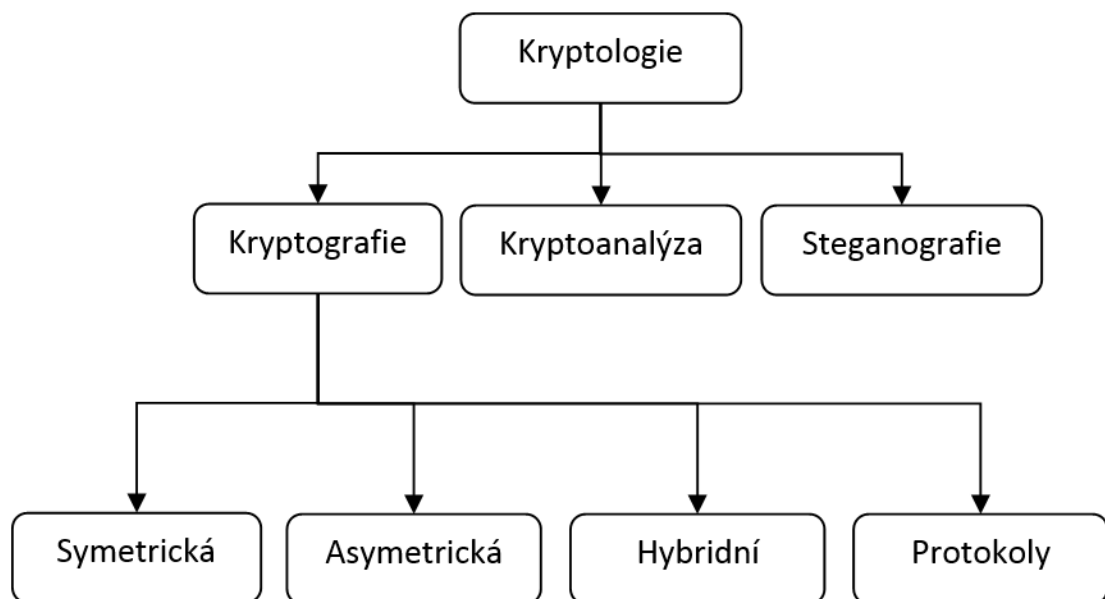
Přenosová rychlost není u NFC příliš vysoká, ale stačí k základním přenosům jednoduchých informací. K tomuto účelu je také NFC technologie stavěna a nikdo neočekává, že by se zvýšil dosah nebo rapidně přenosová rychlost. Dnes se setkáváme i s kombinací různých technologií, typicky NFC spolu s Wifi či Bluetooth.

### 3 KRYPTOLOGIE A ŠIFROVÁNÍ

Pojem kryptologie nám připadá, že úzce souvisí s moderní elektronickou komunikací a rozvojem počítačů, nicméně opak je pravdou. S kryptologií a potažmo šifrováním jsme se setkali již okolo let 2000 př. n. l. Z této doby ze starověkého Egypta se dochovaly první utajované a nestandardní hieroglyfy. Jako nejznámější šifru můžeme uvést Caesarovu, která pouze prováděla posun znaků v abecedě. Za největší rozmach kryptologie je považováno 20. století, kdy se začínají rozvíjet stroje a první počítače. Tato kapitola by měla osvětlit základy kryptologie a také umožnit nahlédnout do moderních šifer a principů, kterých je využito při komunikaci s NFC čipy. [2]

#### 3.1 Základní rozdělení

Kryptologii můžeme rozdělit na 3 základní části: kryptografii, kryptoanalýzu a steganografii. Kryptografii rozlišujeme na symetrickou, asymetrickou a kryptografické protokoly. Základní rozdělení je uvedeno na Obr. 14, popis jednotlivých bloků pak dále v textu.



Obr. 14. Základní rozdělení kryptologie

#### Kryptografie

Kryptografie je věda, která se zabývá matematickou tvorbou a odvozním šifer. Smyslem kryptografie je utajení významu zprávy (vstupního textu) do nečitelné podoby.

## **Kryptoanalýza**

Kryptoanalýza je věda, jenž se snaží dostat k tajným informacím bez znalosti potřebných informací, např. šifrovacího klíče.

## **Steganografie**

Steganografie je vědní disciplína, která ukrývá informace do běžné zprávy, ale obsah nemění. Tajnou zprávu maskuje, aby pozorovatel vůbec nezjistil, že komunikace probíhá. Typickým příkladem je ukrytí informace do obrázku v podobě změn nejméně významných bitů (LSB).

## **Symetrická kryptografie**

V případě symetrické kryptografie mají dvě strany šifrovací i dešifrovací metodu, pro kterou si mezi sebou sdílí tajný klíč. Zprávu je možné tedy šifrovat i dešifrovat jedním neveřejným klíčem. Symetrické šifry jsou stále ve velké míře využívány především k šifrování a kontrole integrity dat. [2]

## **Asymetrická kryptografie**

Asymetrická kryptografie je zcela odlišná od symetrické. U těchto metod je využito pro šifrování a dešifrování dvou odlišných klíčů – veřejného a soukromého. Šifrování probíhá pomocí veřejného klíče, dešifrování pak pomocí soukromého. Nejrozšířenější použití asymetrické kryptografie je digitální podpis. [2]

## **Hybridní kryptografie**

Pod pojmem hybridní kryptografií se rozumí kombinace asymetrické a symetrické kryptografie. Prakticky je využito rychlosti symetrických šifer a použitelnosti asymetrických šifer.

## **Kryptografické protokoly**

Kryptografické protokoly úzce souvisí s aplikací kryptografických algoritmů. Algoritmy tvoří pouze stavební bloky, protokoly pak tyto bloky používají. V dnešní době se řadí mezi nejznámější TLS nebo HTTPS komunikace na Internetu. [2]

### **3.2 Symetrické šifry**

Hlavním důvodem, proč se zabývám pouze symetrickým šifrováním, je ten, že právě toto šifrování se využívá u bezkontaktních NFC čipů a také je předmětem praktické části

díplomové práce. Symetrické šifry se využívají především díky své rychlosti a jednoduchosti. Obě komunikující strany používají stejný klíč k šifrování i dešifrování. To může být slabinou symetrických šifer, proto je nutné používat silné šifry s dostatečně dlouhým klíčem. Tyto šifry rozdělujeme do dvou základních kategorií: blokové a proudové.

### **Proudové**

Proudové šifry zpracovávají vstupní text po jednotlivých bitech. Od blokových šifer se odlišují především v generování klíče. Výhodou těchto šifer je jejich rychlost a pro implementaci jim stačí jednodušší hardware. Mezi nejznámější řadíme: RC4, Fish. [2]

### **Blokové**

Blokové šifry zpracovávají vstupní text po blocích určité délky. Text si tedy musí rozdělit na jednotlivé části a šifrovat nezávisle na ostatních blocích. Poslední blok bývá zpravidla doplněn o zarovnávací bity. Mezi nejznámější řadíme: DES, 3DES, AES. [2]

## 4 BEZPEČNOST NFC

Technologie NFC je v základu považována za bezpečnou díky krátkým vzdálenostem mezi čtečkou a samotným čipem. Tímto způsobem je částečně zamezeno tzv. odposlechu dat. V následujících podkapitolách se podíváme na populární typy karet, základní typy útoků a také úspěšné útoky na vybrané karty. Poslední podkapitola je věnována protiopatřením.

### 4.1 Přehled populárních karet

V této podkapitole jsou uvedeni výrobci s nejvýznamnějším postavením na trhu. Pokud vezmu v potaz společný prodej NFC karet, tak počet prodaných kusů se celkově pohybuje v řádu miliard. Při takto vysoké prodejnosti je důležité brát ohled na použitelnost a bezpečnost jednotlivých karet. Uživatel si tak může prakticky zvolit dle svých preferencí, ke kterému výrobcu se přiklonit.

#### 4.1.1 Výrobci čipů

Výrobci NFC čipů se specializují vždy na určité odvětví. Zpravidla každý výrobce nabízí k určitým úkonům odlišné typy karet. Trendem poslední doby se však stává mít jednu univerzální bezkontaktní kartu, pomocí které bude možné např. platit v obchodech, autorizovat přístupy do budovy, identifikovat osoby, vyměňovat si vizitky apod. V následující tabulce jsou uvedeny vybrané typy karet společně s výrobcu a také jednotlivé standardy, které daná karta využívá.

*Tab. 4 Populární typy NFC čipů*

Typ čipu	Standard
<b>Mifare (NXP)</b>	ISO 14443A
<b>CryptoRF</b>	ISO 14443B
<b>Felica (Sony)</b>	ISO 14443C
<b>OTI</b>	ISO 14443D
<b>Cubic</b>	ISO 14443E
<b>Legic (KABA)</b>	ISO 14443F
<b>Tab-IT</b>	ISO 15693

### 4.1.2 Karty Mifare

Mezi nejvyužívanější karty pro veřejnou dopravu, chytré vizitky, přístupové karty se používají karty Mifare od firmy NXP (divize Philips). Počet prodaných karet firmou NXP se pohybuje okolo 10 miliard, čtecích zařízení pak 150 miliónů. Zajímavostí je, že v bankovním sektoru se čipy od firmy NXP příliš nevyžívají. Firma se specializuje na výrobu karet založených na standardu ISO/IEC 14443 A. Do hlavního portfolia řadíme tyto karty: [17]

- Mifare Classic
- Mifare Ultralight
- Mifare DESFire
- Mifare Plus

#### **Mifare Classic**

Mifare Classic karta se v dnešní době používá prakticky pouze k ukládání dat do paměti přístroje (1 nebo 4 kB). Typickým příkladem mohou být vizitky nebo informační kartičky. Karta je nejlevnějším a nejjednodušším typem, které firma NXP nabízí. Proto jich bylo prodáno nejvíce v historii a stále se používají. Za největší nevýhodu považují to, že šifrování Crypto1 i čipové karty byly v roce 2007 prolomeny. V dnešní době jsou prakticky nepoužitelné v platebních nebo přístupových systémech. [17]

#### **Mifare Ultralight**

Mifare Ultralight karty mají velikost paměti pouze 64 B. Obvykle se používají jako jednorázové vstupenky na různé akce, příkladem může být mistrovství světa ve fotbale v roce 2006. V roce 2012 firma NXP nabídla novou revizi karet s novými vlastnostmi a především pamětí o velikosti až 1 kB. Zabezpečení karet je provedeno v podobě OTP (one time programmable) aby bylo zabezpečeno, že čipy nepůjdou dále přepisovat. [17]

#### **Mifare DESFire**

Mifare Desfire karty obsahují vlastní operační systém, který nabízí jednoduchou adresářovou a souborovou strukturu. Karty jsou založeny na procesoru 8051 s HW podporou šifrování DES, 3DES a AES. Firma nabízí tyto paměťové varianty: 2, 4 a 8 kB k zápisu libovolných dat. Kartu lze díky své univerzálnosti použít ve veřejné dopravě, k řízení přístupů, mikropláťbám apod. V dnešní době NXP nabízí nové revize karet Ev1 a Ev2, které jsou zpětně kompatibilní se stávajícími systémy. [17]

## Mifare Plus

Mifare Plus karty se snaží postupně nahradit Mifare Classic. Karty poskytují jednoduchý přechod stávajících infrastruktur na tyto karty. Zabezpečení se již zlepšilo na šifrování pomocí AES, nicméně kvůli kompatibilitě mohou být karty náchylné ke stejným útokům jako v případě Mifare Classic. [17]

## 4.2 Základní typy útoků

Obecně lze útoky rozdělit na: útoky v reálném čase a pasivní útoky. Ve většině případů se setkáváme s útoky v reálném čase, mezi které patří téměř všechny dále probírané. Mezi pasivní útoky můžeme zařadit v určitých případech např. klonování obsahu či kryptoanalytický útok.

### 4.2.1 Odposlech

Při tomto útoku se snažíme zachytit komunikaci mezi zařízeními a to pomocí výkonných antén. Můžeme tak odposlouchávat radiofrekvenční signál vysílaný zařízením. Vzdálenost, ze které je možné provést odposlech, závisí na mnoha parametrech, především na použitém režimu přenosu. U pasivních zařízení je odposlech mnohem náročnější, téměř nemožný. U aktivních zařízení je možný odposlech ve vzdálenosti jednotek metrů. [11]

### 4.2.2 Přepojování

Při přepojovaném útoku se snaží útočník tvářit jako bezkontaktní čip. Musí tedy přijímat požadavky od čtečky a v reálném čase vracet odpovědi zpět. Jedná se o podobný útok jako Man-in-the-Middle (MIM). K přepojovaným útokům může docházet díky technologii a standardu ISO/IEC 14443, který je na tento typ útoků náchylný. [15]

### 4.2.3 Postranní kanál

Útok pomocí postranního kanálu je založen na zneužití informací, které unikají přímo z fyzické implementace systému během kryptografického algoritmu. Neútočí se pouze na získání hesla, ale také na informace: jaké je použito šifrování, délka vykonání algoritmu apod. Určitým způsobem lze tento útok považovat za odposlech. [15]

### 4.2.4 Klonování obsahu

Jak již z názvu vyplývá, při tomto útoku se snažíme zkopírovat/klonovat obsah karty na reálný hardware nebo přímo vykopírovat na prázdnou kartu. Tento útok se stal velmi

populární, proto existují firmy, které se specializují na vývoj HW s podporou klonování čipových karet. Tyto přístroje dokáží klonovat nebo emulovat vybrané druhy karet. Zaměřují se především na populární karty firmy NXP.

#### 4.2.5 Kryptoanalytický

Při tomto útoku se nesnažíme získat přímo data, ale útočíme na samotné zabezpečení. Útok může například vycházet z útoku hrubou silou na heslo šifry, kdy testujeme všechny možné kombinace hesla. Při krátkém hesle ztrácí v některých případech šifrování smysl. Karty by měly být zabezpečeny tak, že pokud by útočník chtěl vyzkoušet všechny možné kombinace hesla, bylo by nutné heslo hledat stovky let. [11]

#### 4.2.6 Přerušené spojení

Při komunikaci čtečky s čipem dochází k tzv. otevření spojení. Toto spojení se automaticky uzavírá, pokud není zaznamenána žádná aktivita. Pokud opouští zařízení komunikační kanál a neuzavře toto spojení, může dojít k opětovnému navázání spojení. Interval uzavření spojení se může měnit, je tedy nutné, aby interval nebyl příliš dlouhý. Úspěšnost útoku závisí na navrženém programu, který obsluhuje NFC čipy. [15]

### 4.3 Úspěšné útoky

Proč útočit na karty pouze firmy NXP? Odpověď je jednoduchá, protože patří mezi nejvyužívanější a nejlevnější. Níže jsou uvedeny vybrané případy, kdy byl proveden úspěšný útok na tyto karty.

#### 4.3.1 Útok na Mifare Classic

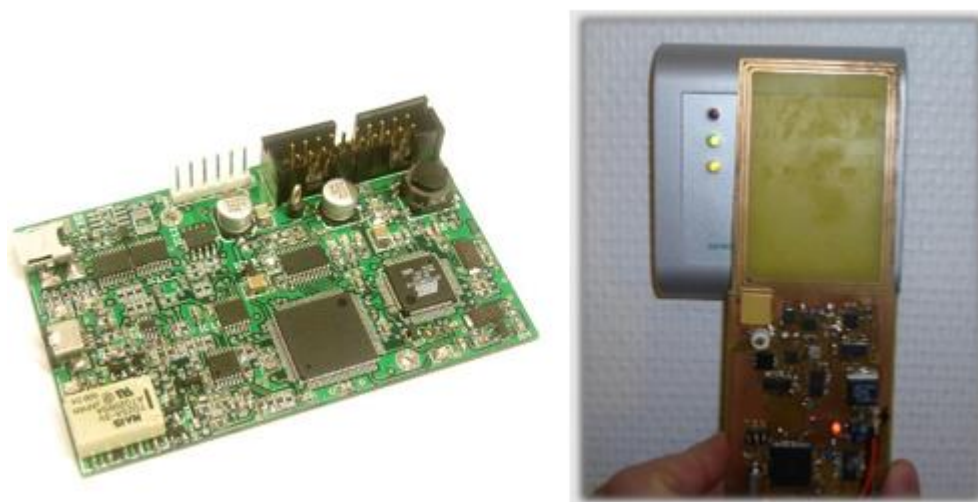
Karet typu Mifare Classic bylo prodáno okolo 1 miliardy, přičemž stále v oběhu je asi 100 milionů karet. V ČR se tento typ stále také využívá např. v knihovnách, přístupových systémech, hotelích apod.



Obr. 15. Mifare Classic karty

Poprvé byly v roce 2007 zveřejněny zmínky o tom, že nepoužívanější karty Mifare Classic byly prolomeny. Prolomení spočívalo v reverzním inženýrstvím, kdy bylo provedeno několik řezů čipem a zkoumala se pod mikroskopem jejich struktura. Tímto způsobem se poté odvodilo schéma zapojení i výsledný algoritmus. Karsten Nohl, v té době studentem doktorského studia, objevil, že karty jsou zabezpečeny proudovou šifrou Crypto1. Její problém je především krátká délka klíče - 48 bitů. [15]

Po roce 2008 se začínají objevovat první hardwarové zařízení (Obr. 16), které umožňují nejprve emulaci karty, později pak provedení kompletní kopie na prázdnou kartu. Cena těchto zařízení byla zpočátku velmi vysoká, nicméně dnes je lze pořídit přibližně do 200 dolarů. [18]



Obr. 16. Proxmark (vlevo) a Project Chameleon (vpravo)

Další výzkum ukázal, že také mnoho karet Mifare Classic mají v sobě některé sektory šifrované výchozím klíčem výrobce. Na základě toho je možné získat odvozením až 99% obsahu karty v tzv. pasivním (offline) útoku. [19]

#### 4.3.2 Útok na Mifare DESFire

Z roku 2011 jsou také známé útoky na kartu typu Mifare DESFire (MF3ICD40), která podporuje šifrování DES a 3DES. Prolomení bylo založeno na útoku postranním kanálem a trvalo asi 7 hodin. Tyto karty se také dříve používaly u nás, konkrétně v projektu Open Card a také jako In Karty od Českých drah. Výrobce NXP v dnešní době tuto verzi již nevyrábí a nahradil je novějšími revizemi Mifare DESFire Ev1, resp. Ev2, které dosud prolomeny nejsou. [15]

### 4.3.3 Útok na Mifare Ultralight

V roce 2012 na prezentaci o bezpečnosti v Amsterdamu byl prezentován útok na karty Mifare Ultraligh. Tyto karty se využívají v New Jersey a San Franciscu v přepravních systémech. Pomocí mobilního telefonu s Androidem je možné upravovat data těchto karet, tj. obnovovat výši kreditu a cestovat tak zcela zdarma. NXP v dnešní době nabízí poslední revizi karet Ev1, u kterých je podporováno šifrování 3DES a také automatický čítač, který omezuje počet změn dat. [17]

## 4.4 Protiopatření

V této kapitole je uveden přehled základních opatření, jak se zachovat, co použít nebo jakým způsobem reagovat na hrozbu útočníka. Obecně při vytváření nového projektu je nutné udělat průzkum o aktuálních používaných kartách s dostatečným zabezpečením. Pokud jde o peněžní služby, důležité kontroly vstupů nebo utajované informace, vždy je nutné dodatečné opatření a nespoléhat se pouze na šifrování a bezpečnost NFC čipů. V zásadě je také důležité sledovat aktuální trendy v oblasti útoků na tyto čipy. V případě hrozby je nutné vždy karty nahradit novými bezpečnějšími a staré zablokovat. Následující doporučení jsem čerpal ze svých znalostí a především z jiných odvětví, ve kterých takovéto protiopatření fungují.

### 4.4.1 Serverové ověřování

V drtivé většině případů čtecí zařízení obsahuje připojení k Internetu. Pomocí tohoto připojení je možné dodatečně ověřit správnost čipu nebo přímo autorizovat NFC čip. Na základě komunikace typu klient–server by bylo z ověření patrné, zda autorizace proběhla úspěšně či nikoliv.

### 4.4.2 Blacklist

Každý projekt či firma využívající principů NFC by si měla udržovat v databázi seznam používaných čipů. Tento seznam je vhodné si rozdělit do několika podskupin v závislosti na množství používaných čipů. Pokud by došlo k úspěšnému útoku v určité podskupině, je účelné vytvořit tzv. „blacklist“, který bude obsahovat vyřazené (napadené) čipy. Tento blacklist může také sloužit k tomu, že při načtení infikované karty se změní status určitého bitu na kartě. [5]

#### 4.4.3 Dynamická změna hesla

NFC čipy lze ochránit také způsobem dynamické změny hesla. Princip může spočívat v tom, že při každém načtení nebo jednou za určitý časový úsek dojde k automatické změně hesla na kartě. V tomto případě je nutné udržovat nejen seznam používaných čipů, ale také seznam používaných a změněných hesel.

#### 4.4.4 Izolace karty

Při manipulaci s NFC čipy může docházet k tomu, že si naši kartu bude chtít přečíst někdo jiný. Principem ochrany je vytvoření kovového pouzdra z kovové fólie k vytvoření tzv. Faradayovi klece. Karta v takovémto obalu je chráněna proti jakémukoliv rádiovému signálu. [5]

#### 4.4.5 Vhodné šifrování

Při koupi nových čipů je nutné si ověřit, jaké druhy šifrování karta podporuje. Obvykle je vhodné využití šifrování AES s dostatečně dlouhým klíčem. Aby čipy nebyly pomalé při šifrování, jsou standardně doplněny o HW podporu šifrování.

#### 4.4.6 Využití hashovacích funkcí

NFC čipy lze ochránit také využitím hashovacích funkcí. Data uložené na kartě budou dodatečně zahashovány z důvodu toho, aby byl obsah pro čtenáře i po prolomení karty stále nečitelný. [5]

## **II. PRAKTICKÁ ČÁST**

## 5 DOKUMENTACE POD NDA

Tato kapitola se zaměřuje na informace související k získání kompletní dokumentace karet Mifare DESFire Ev1. Když jsem si po vhodném průzkumu bezpečnosti karet NFC vybral nejlepší variantu, nepočítal jsem se s tím, že pouhé získání dokumentace mi zabere 2 měsíce. Předpokládal jsem, že s koupí karet dostanu i dokumentaci, abych si mohl karty programovat dle své libosti. Bohužel takto to u firmy NXP nefunguje, proto je nutné veškeré informace získat na základě podepsané smlouvy o mlčenlivosti. Toto řešení nabízí většina firem, které poskytují bezkontaktní NFC karty. Je to především z toho důvodu, že každá firma používá svá proprietární řešení ke komunikaci s kartami. Univerzálnost bezpečného komunikačního protokolu by byla velkým ulehčením, nicméně variabilita karet je vysoká, proto by musely na trh přijít nové karty se stejnou nebo podobnou strukturou. Příchod takovýchto karet by však znamenal vysoké finanční náklady spojené s výrobou čipů a novou implementací stávajících systémů.

### 5.1 Informace v NDA

Smlouva o mlčenlivosti (NDA, Nondisclosure Agreement) byla podepsána firmou BowCloud s.r.o. (divize Cathedral Software s.r.o.) a obsahuje standardní informace, které jsou rozepsané na 2 stránkách formátu A4. Veškeré údaje získané na základě podepsané smlouvy jsou důvěrnými informacemi firmy NXP B.V. sídlící v Nizozemí. Tyto informace nemohou být dále šířeny třetím stranám. V případě porušení podepsané smlouvy bude zahájeno soudní řízení, přičemž veškeré náklady spojené se soudem bude hradit firma, která smlouvu o mlčenlivosti podepsala. Dále je v NDA uvedeno, že všechna soudní řízení budou probíhat v zemi, kde sídlí firma NXP. Soudní řízení bude probíhat tak, že se firma k veškerým porušením práv přizná a nebude klást odpor při prokazování porušení smlouvy o mlčenlivosti. Smlouva mezi oběma stranami je platná po dobu 3 let, poté je nutné smlouvu obnovit.

### 5.2 Dokumentace karet Mifare DESFire Ev1

Následující podkapitola popisuje způsob získání dokumentů a jejich zabezpečení od firmy NXP. V poslední části jsou uvedeny dokumenty, které byly využity při tvorbě diplomové práce.

### 5.2.1 Získání dokumentů

Komunikace s firmou NXP před podepsáním jakékoliv smlouvy je poněkud složitá. Když jsem oslovil technickou podporu pod vlastním jménem s tím, že pracuji na diplomové práci a chtěl bych dokumentaci k čipovým kartám Mifare DESFire Ev1, podpora mi ani na jednu ze dvou žádostí dodnes neodpověděla.

Na základě negativního dojmu z firmy NXP jsem se pokusil využít všechny dostupné prostředky k tomu, abych dokumentaci získal: psal jsem na několik diskuzních fór, emaily přímo lidem pracujícími s kartami Mifare DESFire, ale co mi nejvíce pomohlo, bylo kontaktovat české distributory pro firmu NXP. Kontakty na 5 těchto firem jsem dohledal na stránkách firmy NXP. Všechny firmy jsem kontaktoval telefonicky se svou situací, nicméně všechny požadovaly ještě sepsání podrobných informací do emailu s tím, že se mi budou snažit pomoci. Z těchto 5 kontaktů se mi později ozvala pouze firma Future Electronics Prague ([www.futureelectronics.com](http://www.futureelectronics.com)).

S touto firmou jsem komunikoval necelé dva týdny, po kterých jsem oficiální dokumentaci získal. Velmi důležitým krokem počínání bylo, že výše uvedená firma měla ve firmě NXP kontaktní osobu, která celý proces velice urychlila.

### 5.2.2 Zabezpečení dokumentů

Na základě podepsané smlouvy o mlčenlivosti firma zasílá certifikát, který je nutné nainstalovat do počítače. Certifikát je zabezpečen heslem a šifrováním 128 bit AES, přičemž platnost instalace certifikátu je pouze jeden týden. Po uplynutí jednoho týdne je možné si tento certifikát na zvláštní vyžádání nechat zaslat znovu. Dokumenty tedy nelze otevírat na jiných počítačích, než na ověřených certifikátem. Tisk nebo převod dokumentů do jiných formátů není povolen, samotný tisk na papír možný je. Dále je na každé straně dokumentu vodoznak s kontaktní osobou a názvem firmy, která NDA podepsala.

### 5.2.3 Data sheet

Hlavička dokumentace, se kterou jsem pracoval, je zobrazena na Obr. 17. V hlavičce je uveden úplný název, revize a verze dokumentu. Dále obsahuje informace o tom, že se jedná o kompletní data sheet (product data sheet) a obsahuje citlivé firemní údaje. Z důvodu podepsání smlouvy o mlčenlivosti nemohu žádné informace z tohoto dokumentu dále prezentovat.



Obr. 17. Hlavička úplné dokumentace karet Mifare DESFire Ev1

Dokument je rozdělen do 17 kapitol, které jsou při orientaci v textu vhodně rozvrženy. Celkový počet stran přesahuje 110 ve formátu A4.

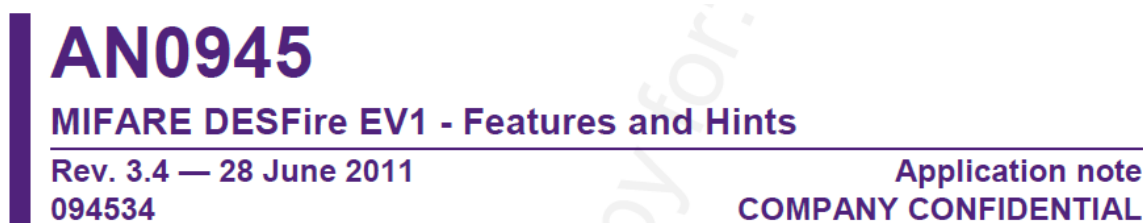
Veškeré informace, které jsou veřejně dostupné, jsou ve zkrácené verzi dokumentace (product short data sheet). Tento dokument je velice omezený a je sepsán jen do 18 stran. V seznamu literatury diplomové práce jde o položku [20]. Hlavička dokumentu je zobrazena na Obr. 18. a obsahuje stejnou strukturu jako kompletní data sheet.



Obr. 18. Hlavička zkrácené dokumentace karet Mifare DESFire Ev1

#### 5.2.4 Dokumentace vybraných příkladů

Důležitým pomocníkem při implementaci je dokument s vybranými příklady a doporučeními. Hlavička dokumentu je zobrazena na Obr. 19. a obsahuje stejnou strukturu jako kompletní data sheet.



Obr. 19. Hlavička dokumentace příkladů a doporučení

## 6 POUŽITÉ TECHNOLOGIE A NÁSTROJE

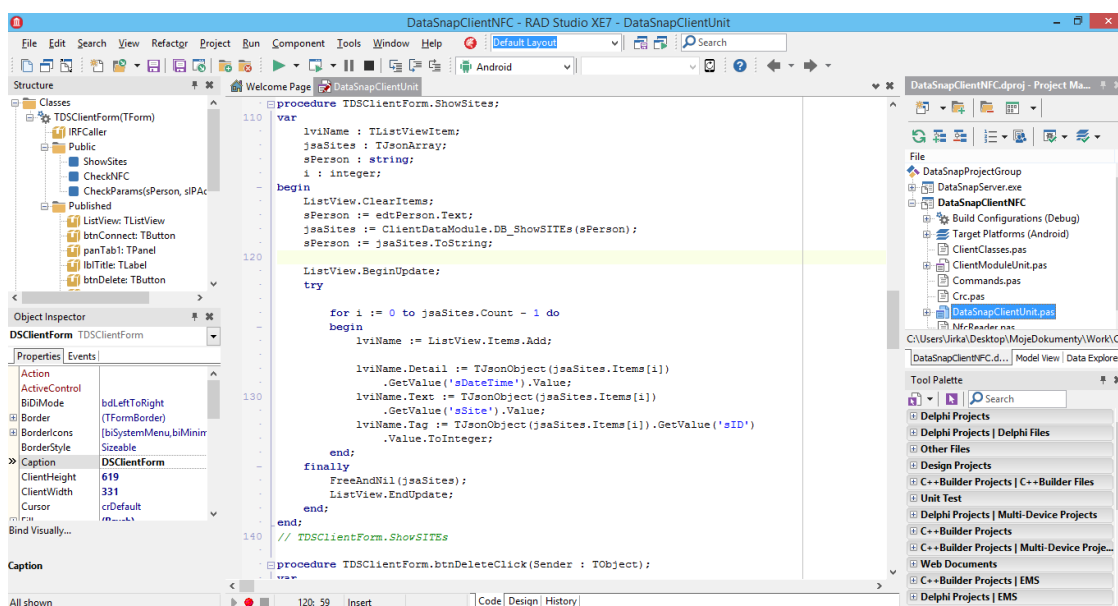
Kapitola použité technologie a nástroje popisuje, jaké jsem využil vývojové prostředí, databázový stroj nebo mobilní telefon. Ve vybraných částech je uveden jednoduchý postup, co je nutné nastavit pro správnou detekci zařízení s vývojovým prostředím.

### 6.1 Embarcadero RAD Studio XE7

Embarcadero RAD Studio XE7 je vývojové prostředí od společnosti Embarcadero Technologies, která se také stará o vývoj programovacího jazyka. Vývojové prostředí nabízí kompletní řešení v oblasti vývoje softwaru od návrhu až po samotné programování. Důležitým prvkem je multiplatformní vývoj softwaru, kdy prostředí nabízí vývoj aplikací pro Windows, Mac, iOS, Android a chytrého hardwaru. Poskytuje kompletní řešení pro vývoj multiplatformních nativních aplikací s podporou mobilních zařízení, chytrých hodinek nebo cloudových služeb. [21]

Vývojové prostředí lze ke studijním účelům využít pouze omezenou dobu (trial verze) s platností pouze 30 dní. V mém případě mi firma, se níž spolupracuji, poskytla pracovní notebook, který Embarcadero RAD Studio XE7 již obsahoval. Cena standardní verze vývojového prostředí se pohybuje v řádu desítek tisíc Kč. V době psaní diplomové práce byla vydána již nová verze vývojového prostředí s označením XE8. Náhled uživatelského rozhraní je zobrazen na Obr. 20.

#### 6.1.1 Rozhraní vývojového prostředí



Obr. 20. Vývojové prostředí Embarcadero RAD Studio XE7

Design vývojového prostředí se přizpůsobuje aktuálním trendům v oblasti vývoje softwaru. Dle mého názoru se nejvíce podobá vývojovému prostředí Visual Studio od firmy Microsoft. Rozhraní aplikace je rozděleno do několika sekcí. V horní části okna můžeme vidět funkční lištu, ve které je možné otevírat soubory, procházet nastavení či provádět build aplikace. V levé části vidíme přehled procedur a funkcí zdrojového kódu, pod ním pak Object Inspector, pomocí kterého lze nastavovat vlastnosti komponent. Uprostřed aplikace se nachází textové okno pro psaní zdrojového kódu. V pravé části je prohlížeč souborů projektu a také lišta s komponentami. Celé rozhraní je možné si upravit dle uživatelských preferencí s možností uložení rozložení nastavení.

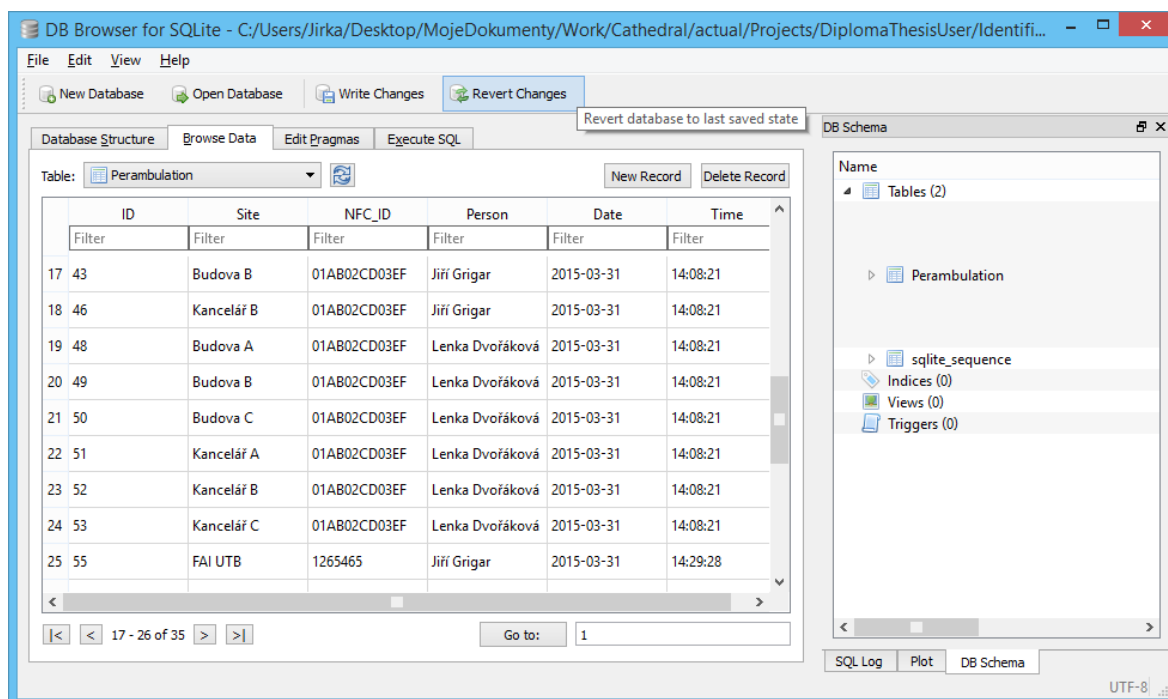
### 6.1.2 Programovací jazyky

Vývojové prostředí nabízí psaní i kompletní build aplikace pro dva programovací jazyky: C++ a Object Pascal (Delphi). Co se týče C++, nenašel jsem žádný problém při testování. Moje práce je kompletně napsaná v jazyce Object Pascal, dnes známý spíše pod názvem Delphi. Jedná se o rozšíření jazyka Pascal o objekty, tedy objektově založené programování spolu s přidáním komponentami. Komponenty si lze představit jako stavební bloky formuláře podobné např. tlačítkům. Všechny komponenty obsahují své vlastnosti, které lze nastavit v Object Inspectoru. Každá komponenta je vlastně třídou (objektem), tedy nemusíme ji přidávat do okna aplikace ručně, ale můžeme všechny komponenty vytvářet a nastavovat programově. Programová úprava komponent je výhodná především při nastavování přihlašovacích údajů, přidávání cest k databázím, nastavení portů, IP adres apod.

## 6.2 SQLite

SQLite je volně dostupný software, který implementuje soběstačný databázový stroj. Není třeba žádných konfigurací nebo vytváření serveru, databázi může tvořit jediný soubor. Ten je možné libovolně kopírovat mezi různými zařízeními. Databáze je postavena na relačním modelu, dotazy jsou intuitivní a jednoduché. [22]

Databázi SQLite jsem si vybral z toho důvodu, že je možné ji použít téměř v každém zařízení a operačním systému. Databáze si obecně poradí jak s desktopovými aplikacemi, tak mobilními zařízeními. Jako největší výhodu vidím jednoduchost a použitelnost pro základní operace či prezentace projektů. Databáze je vhodná také pro testovací a vývojářské účely. Uživatelské rozhraní je zobrazeno na Obr. 21.



Obr. 21. Rozhraní DB Browser pro SQLite

## 6.3 Samsung Galaxy S3

K vývoji jsem použil vlastní mobilní telefon Samsung Galaxy S3, který v roce uvedení 2012 tvořil vlajkovou loď mobilních telefonů firmy Samsung. Dnes jde spíše o střední třídu, nicméně k vývoji aplikací je plně dostačující. Mezi hlavní parametry telefonu se řadí čtyř-jádrový procesor, 1 GB operační paměti RAM a 16 GB vnitřní paměti pro ukládání uživatelských dat. Aktuálně běží v telefonu Android ve verzi 4.3 a nejdůležitějším prvkem v mém případě je podpora technologie NFC.

### 6.3.1 Konfigurace mobilního telefonu

Před samotným vývojem je nutné každé mobilní zařízení správně nakonfigurovat, jelikož bez správně připojeného zařízení jej vývojové prostředí nedetekuje. Prvním krokem je mít nainstalovaný ovladač k mobilnímu telefonu. Ve Windows 7 či 8 je tento problém odstraněn při připojení zařízení skrze USB, kdy dojde k automatickému stažení všech ovladačů. Dalším krokem je nastavit u mobilního zařízení režim přenosu, ten je nutné volit jako PTP (režim fotoaparátu). Posledním krokem je povolení režimu ladění skrze USB. Tento krok se provádí v nastavení telefonu a standardně je tato volba neviditelná. Zviditelnění volby se skrývá v nastavení v informacích o telefonu, kdy je nutné několikrát kliknout na verzi sestavení. Poté se nám objeví v nastavení volba vývojářské možnosti, kde

můžeme režim ladění povolit. Po těchto krocích je vše správně nakonfigurováno a vývojové prostředí detekuje mobilní telefon ve výběru platformy. [23]

### 6.3.2 Android SDK

Pro vývoj aplikací je obecně nutné mít vždy stažené knihovny SDK (Software Development Kit). Tyto knihovny obsahují základní API rozhraní potřebné k vývoji aplikací. V mém případě jsem pracoval s Android SDK ve verzi 19 (4.4 KitKat). Byť mám v mobilním zařízení starší verzi Androidu 4.3, s vývojem jsem neměl sebemenší problémy. Je to především z toho důvodu, že jsem využíval základní stavební prvky API, které jsou zpětně kompatibilní se starší verzí SDK.

## 6.4 Volba čipových karet

Po průzkumu trhu a komunikaci s bezpečnostními analytiky čipových karet jsem pro diplomovou práci vybral čipy Mifare DESFire Ev1. Pro můj účel jsou plně dostačující, umožňují několik typů uložených dat a šifrování pomocí AES. Cena karet zejména záleží na počtu odebíraných kusů, v mém případě při koupi 4 karet se cena pohybovala okolo 85 Kč bez DPH. Při odběru 100 a více kusů se lze dostat na částky podstatně nižší.

Struktura čipu je rozdělena do několika tzv. aplikací, těch může být na kartě až 28. Aplikaci si můžeme představit jako rozhraní mezi daty a typem použití. Aktuálním trendem je mít jednu čipovou kartu pro mnoho využití, tedy každá aplikace na kartě bude odpovídat jednomu typu využití. V každé aplikaci můžeme mít až 32 souborů, což jsou pouze alokovaná data na kartě.

Důležitým prvkem těchto čipových karet je diverzifikace klíčů. Karta poskytuje pro každou aplikaci použití odlišného klíče s odlišným šifrováním. K základní komunikaci je vždy vyžadováno master heslo, které je nezávislé na aplikacích. Tímto způsobem máme zaručeno, že při prolomení jednoho z klíčů se nelze dostat ke všem datům na kartě.

## 7 VYTVOŘENÉ APLIKACE

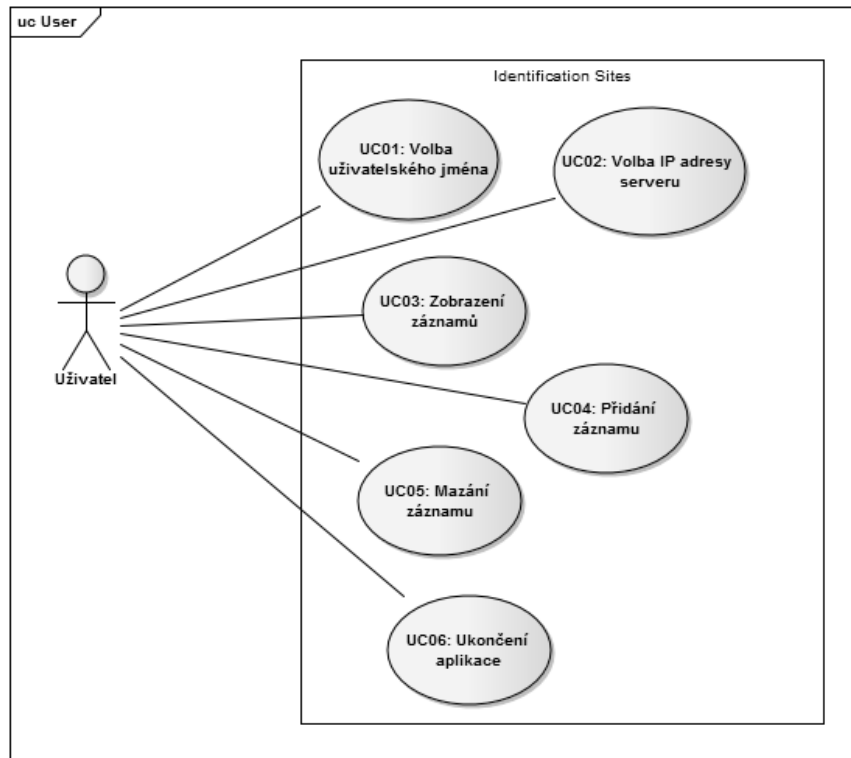
V této kapitole je uveden popis výsledných aplikací diplomové práce. První část se zabývá softwarovými návrhy v programu Enterprise Architect. K popisu jsem využil diagramy užití a také zjednodušený diagram tříd, který je pro svou velikost uveden v příloze P I. Dále je uveden popis uživatelského rozhraní jednotlivých aplikací. V poslední části je nastíněn způsob komunikace klient-server, kterou jsem musel také vyřešit. Vytvořené aplikace jsou pouze jakési technologické demo, jenž slouží k prezentaci způsobu komunikace mobilního telefonu s technologií NFC. Data z mobilního telefonu jsou dále spravována pomocí vzdáleného databázového serveru. V mém případě jsem se zaměřil především na tvorbu komunikace s NFC čipy na mobilních zařízeních a následnou komunikaci se vzdálenou databází. Obecně práce pouze demonstruje možnosti využití jednotlivých komponent. V reálném nasazení by bylo nutné vyřešit některé procesy, které jsem pro prezentační účely zjednodušil. V kapitole záměrně neuvádím popis zdrojového kódu, jelikož bych zveřejněním porušil smlouvu o mlčenlivosti s firmou NXP.

### 7.1 Enterprise Architect

Enterprise Architect je nástroj s bohatou sadou funkcí v oblasti analýzy softwaru. Tyto funkce nám pomáhají spravovat informace a provádět inovace v dnešním složitém a náročném prostředí. Nástroj je vhodný především k modelování a návrhu softwarových procesů. V oblasti vývoje SW jde o jeden z nejlepších nástrojů, který běžně firmy využívají. Pro diplomovou práci jsem využil verzi programu 10. [26]

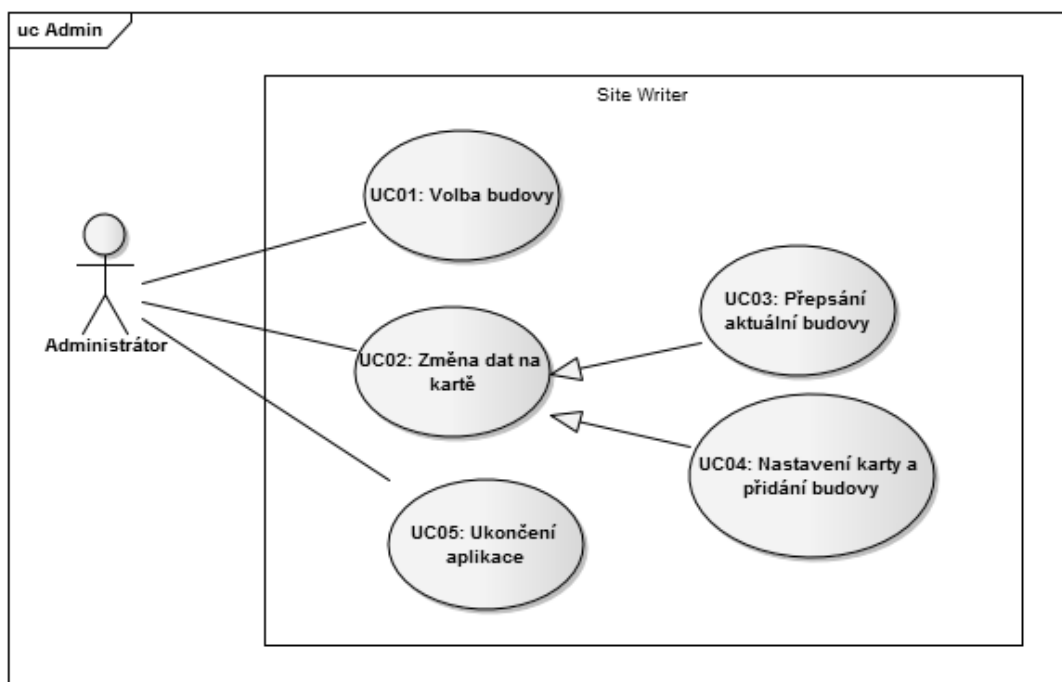
#### 7.1.1 Diagram užití

Diagram užití (Use Case) je vhodným zobrazením funkcionality navrženého systému. Na Obr. 22 je uveden diagram užití pro uživatelskou aplikaci se jménem „Identification Sites“. Hlavním smyslem aplikace je přihlášení uživatele do systému a při načtení NFC čipu provést automatické vložení záznamu do databáze. Z diagramu je patrné, že jsem volil pro uživatele co nejméně funkcí, co se týče správy nebo nastavení. Je to především z toho důvodu, že ne všichni uživatelé jsou schopni bez problému používat dotykové zařízení. Do diagramu jsem zařadil také volbu IP adresy serveru s databází (UC02), nicméně tento případ je pouze v rámci diplomové práce. V reálném nasazení by si veškeré konfigurační údaje držela aplikace v sobě, popř. četla z externího zdroje, jako jsou konfigurační soubory nebo databáze.



Obr. 22. Diagram užití pro uživatelskou aplikaci

Na Obr. 23 je zobrazen diagram užití pro administrátorskou aplikaci „Site Writer“. I v tomto případě jsem dbal především na jednoduchost použití aplikace. Ta má sloužit především k zápisu a úpravě dat na kartě.



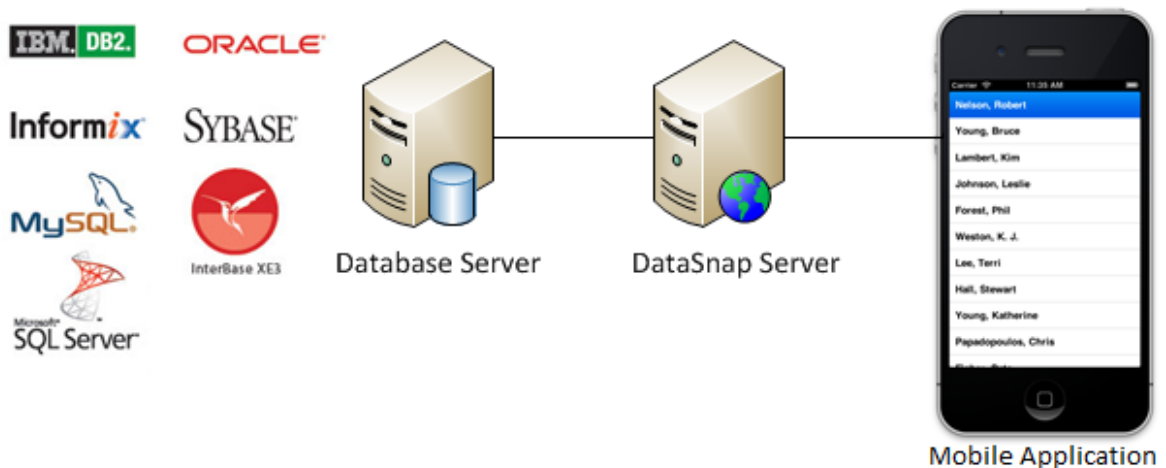
Obr. 23. Diagram užití pro administrátorskou aplikaci

### 7.1.2 Diagram tříd

Diagram tříd (Class Diagram) znázorňuje statickou strukturu programu. Popisuje také datové struktury a operace nad objekty. Jako velkou výhodou oceňuji v Enterprise Architectu možnost volby programovacího jazyka, kdy SW nabízí podporu i pro jazyk Delphi, který není příliš rozšířený. Obecný diagram tříd shodný pro obě vytvořené aplikace je uveden z důvodu velikosti v příloze P I. Diagram obsahuje vybrané části programu důležité pro pochopení struktury. Hlavní část tvoří třída NfcReader, která obsahuje všechny funkční bloky pro komunikaci s technologií NFC. Třidu je nutné vložit do používaného formuláře či třídy. Důležitým blokem je rozhraní (interface) IRF\_Caller, který je nutné podědit do hlavního okna aplikace. Interface obsahuje pouze jednu proceduru vracující ve svém vstupním parametru unikátní označení čipové karty.

## 7.2 Komunikace se serverem

Uživatelská aplikace Identification Sites ukládá načtená data z čipových karet do vzdálené databáze s typem komunikace klient-server. V Delphi se tento typ komunikace označuje obecně jako DataSnap. Principem je mít oddělený databázový server (Database Server) od aplikačního serveru systému (DataSnap Server). Schéma komunikace je znázorněno na Obr. 24.



Obr. 24. Princip komunikace klient-server [27]

### DataSnap Server

DataSnap Server slouží jako rozhraní mezi databázovým serverem a mobilním klientem. V tomto serveru je nutné implementovat všechny funkce, které je jsou nutné pro komunikaci s databází. Důležité je především poskytnutí vhodných dotazů

do databáze, které lze ověřit ve vývojovém prostředí bez nutnosti implementace klientské části aplikace. Jako výhodou tohoto řešení vidím univerzálnost použití v oblasti změny databázového serveru. Přejít na jiný databázový server není příliš složité, jelikož všechny komponenty zůstávají stejné a mění se pouze drivery a vlastnosti jednotlivých komponent. Typické použití DataSnap Serveru je v podobě běžící služby na pozadí. V mém případě jsem ale zvolil Win32 aplikaci, která zobrazuje pouze okno, nicméně na pozadí obsluhuje kompletní databázový server.

### **JSON objekty**

V případě DataSnap serveru je nutné zajištění správné komunikace klient-server. K tomuto účelu se využívá protokolu TCP/IP, kde je potřeba znát cílovou IP adresu serveru a také port, na kterém bude komunikace probíhat. DataSnap server poskytuje pouze primitivní návratové datové typy, proto nelze využít seznamů, polí, kolekcí apod. V mém případě byl požadavek na využití právě neprimitivních datových typů. Proto se musela všechna data kódovat do podoby JSON objektů a JSON polí, které je nutné následně převádět do podoby stringu a posílat ke klientské aplikaci. Klientská aplikace musí tento JSON zpět převést do podoby správných datových typů a následně může data využívat.

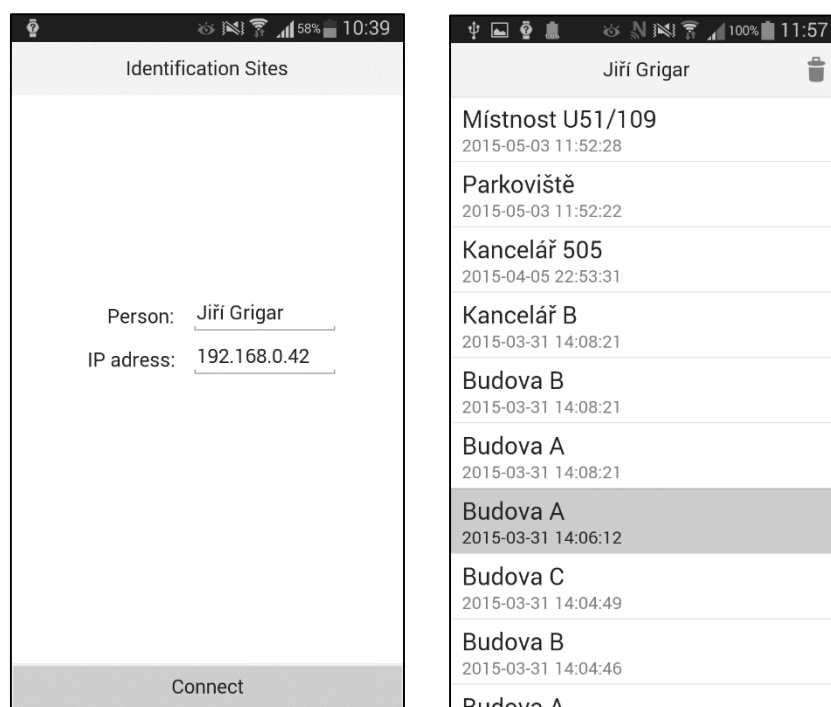
## **7.3 Klientské aplikace**

Kapitola 7.3 uvádí základní popis uživatelské a administrátorské aplikace. Dále je proveden rozbor uživatelského rozhraní aplikací spolu s postupem použití.

### **7.3.1 Uživatelská**

Uživatelská aplikace Identification Sites slouží k samotné identifikaci firemních objektů pomocí technologie NFC. První okno aplikace znázorňuje přihlašovací formulář, kde uživatel zadá své jméno a také IP adresu k databázovému serveru. Volba IP adresy slouží pouze pro vývojářské účely, jelikož aplikace neběží na žádném veřejném serveru. Po vyplnění údajů uživatel klikne na tlačítko connect, pomocí kterého se připojí k databázovému serveru. Po správném připojení se uživateli zobrazí hlavní okno aplikace (Obr. 26 vpravo). V něm lze vidět v hlavičce jméno přihlášené osoby a také list načtených budov. Ve výpisu se vždy zobrazuje také datum společně s časem přečtení budovy. Uživatel má možnost pouze mazat vybrané záznamy. Pokud mobilní telefon s aplikací přiloží uživatel k čipové kartě, provede se autentizace a v případě úspěchu se přečtou data

zapsaná v paměti čipu. Po přečtení se data zapíší do vzdálené databáze a také do výpisu přečtených budov. Přihlašovací formulář a hlavní okno aplikace je zobrazeno na Obr. 26.

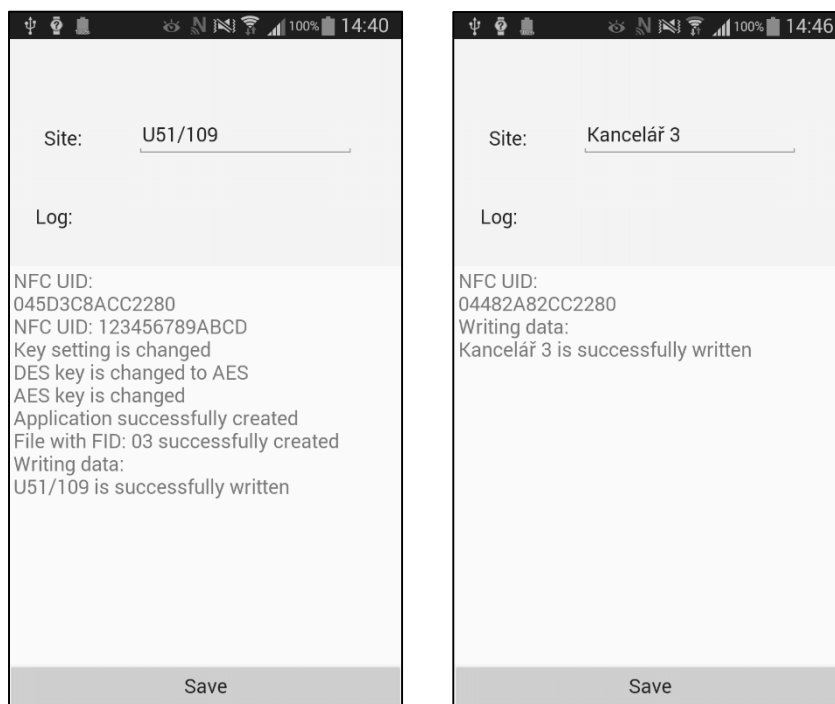


Obr. 25. Rozhraní uživatelské aplikace: přihlášení a hlavní okno

### 7.3.2 Administrátorská

Administrátorská aplikace Site Writer slouží k zápisu dat (budov) do paměti čipových karet. Hlavní okno se skládá z jednoduchého formuláře, který zobrazuje jedno editační okno pro uživatele a také výpis logu do textového pole, které nelze editovat. Důležitým bodem je mít přiloženou čipovou kartu u mobilního telefonu při zápisu dat. Aby uživatel věděl, že může zapisovat data na kartu, je při přiložení čipové karty do logu zapsán unikátní identifikátor čipové karty bez ohledu na to, zda chce uživatel zapisovat či nikoliv. Pokud bude uživatel zapisovat na úplně prázdnou čipovou kartu, zobrazí se mu po stisku tlačítka Save v logu informace, které jsou uvedené na Obr. 27 vlevo. Na pozadí aplikace se spouští procesy, jenž nastavují čipovou kartu do vhodné podoby. Prvním krokem je změna nastavení hesla neboli změna administrátorských práv na takové nastavení, aby pro každou činnost bylo vyžadováno ověření pomocí master hesla. Dalším krokem je změna typu šifrování z DES na AES a také změna nastaveného výchozího hesla. To je u čipových karet od firmy NXP obvykle nastaveno na nulové bajty. Následně je na kartě vytvořena aplikace s unikátním identifikátorem a příslušnými právy. Dále se vybere aktuálně vytvořená aplikace a do ní se vytvoří soubor, respektive se přidělí paměť

zadanému identifikátoru souboru. Poté dojde k samotnému zápisu zadané budovy do čipové karty. Opačnou situaci tvoří karta s již zapsanou budovou, příklad můžeme vidět na Obr. 27 vpravo. V tomto případě dojde pouze k přepsání stávajících dat uložených na čipové kartě. V obou případech je název budovy omezen na 15 znaků.



Obr. 26. Rozhraní administrátorské aplikace

## 7.4 Ošetření vstupních parametrů

Všechny formuláře aplikací bylo nutné ošetřit z pohledu zadávaných dat od uživatele. V případě volby IP adresy byl vytvořen regulární výraz, pomocí kterého je ošetřeno správné zadání IP adresy. Pokud není IP adresa zadána korektně, je vyvolána výjimka s chybovou hláškou. Volba jména osoby je pouze ošetřena proti zadání prázdných znaků. V reálné aplikaci by spíše uživatel vybíral z již dostupných osob z roletového menu. Dalším prvkem je zadání jména budovy v aplikaci Site Writer. V tomto případě je také ošetření provedeno na základě testování prázdnoty zadaného textu. Vstupní text jsem také omezil na velikost 15 znaků. Data, která jsou uložena v paměti čipové karty, mají bajtovou podobu. Proto jsem musel provádět kódování dat ze vstupního textu do bajtové podoby a opačně. K tomu jsem využil kódování textu do UTF-8, tedy aplikace si poradí běžně s českou diakritikou.

Dalším ošetřením parametrů bylo nutné na databázovém stroji. Pokud neošetříme správně vstupní parametry od uživatele, může dojít k tzv. útoku SQL Injection. V této situaci uživatel místo vstupních dat zkouší zadávat přímo SQL dotazy do databáze. Při nesprávném ošetření může v nejhorším případě klidně smazat celou databázi nebo pouze upravovat údaje. V programovacím jazyku Delphi je možné tento útok eliminovat s využitím třídy Params, pomocí které si přímo definujeme datové typy, které chceme využívat. V případě útoku dojde k výjimce či v některých případech vložení infikovaného dotazu přímo do sloupce, který uchovává textová údaje.

## 8 ZABEZPEČENÍ ČIPOVÝCH KARET

Tato kapitola se věnuje zabezpečení čipových karet Mifare DESFire Ev1, které jsou využívány v rámci praktické části diplomové práce. V případě koupě nových karet jsou čipové karty prázdné a nastaveny na výchozí šifrování DES, které je v dnešní době kvůli prolomení nepoužitelné. Mým úkolem bylo nastudovat všechny dále probírané principy a aplikovat je v programovacím jazyku Delphi. V praxi se před odesláním dat do čipové karty postupuje dle těchto bodů:

- sloučí se jednotlivé parametry do podoby bloku vstupních dat
- ze vstupních dat se vypočte kontrolní součet CRC
- poslední blok dat se zarovná (doplní) nulami na velikost 16 B
- zašifruje/dešifruje se každý blok dat na základě módu CBC
- jednotlivé bloky se sloučí a odešlou čipové kartě
- karta na přijímaná data vhodně zareaguje

### 8.1 Šifrování AES

AES (Advanced Encryption Standard) šifra patří dnes k nejrozšířenějším symetrickým šifrám. Vstupní text je šifrován i dešifrován po blocích stejné délky. Délka bloku je vždy 128 bitů, délka klíče může být 128, 192 nebo 256 bitů. Šifra se v dnešní době používá k šifrování dokumentů, zabezpečení WiFi sítí nebo pro různé bezpečnostní protokoly. Dodnes nebyly publikovány žádné dokumenty o prolomení šifry AES s délkou klíče 128 bitů a více. Znamé jsou pouze útoky hrubou silou na neúplnou šifru, proto můžeme považovat šifru za stále bezpečnou. Obecně zde platí pravidlo, čím delší klíč šifry AES použijeme, tím bude útok hrubou silou náročnější. [2]

V mém případě karty Mifare DESFire Ev1 umožňují šifrování dat pomocí 128 bit (16 B) dlouhého klíče. Šifrování i dešifrování probíhá po blocích o velikosti 16 bajtů. Pokud jsou data odesílána na kartu kratší než 16 B nebo je délka posledního bloku kratší než 16 B, je nutné tento blok zarovnat do velikosti 16 B. U karet Mifare jsou data doplněna o nulové bajty. K šifrování i dešifrování jsem využil volně dostupnou knihovnu LockBox 3 pro Delphi (<http://sourceforge.net/projects/tplockbox/>). Tato knihovna obsahuje šifry DES, 3DES, AES, hashovací funkce apod.

## 8.2 Kontrolní součty CRC

CRC neboli cyklický redundantní součet (Cyclic redundancy check) je speciální druh hashovací funkce, která se používá k detekci chyb během přenosu či ukládání dat. Kontrolní součet se obvykle přidává k odesílaným datům a čtecí zařízení je schopno data přijmout a nad nimi vypočítat nový CRC součet. Poté čtecí zařízení porovná, zda jsou oba kontrolní součty stejné a vhodně na toto porovnání zareaguje. [24]

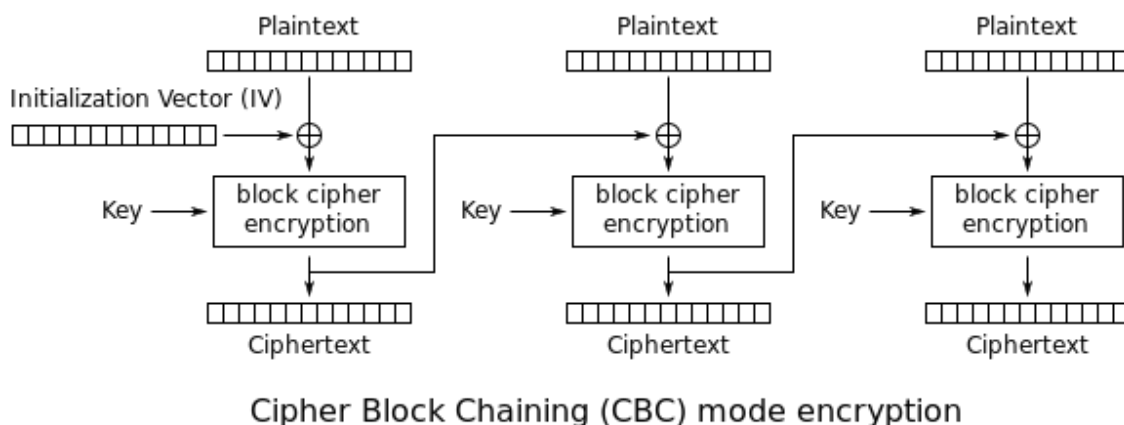
Při manipulaci s daty uloženými v paměti čipové karty může docházet vlivem rádiového spojení k určitému zkreslení těchto dat. Proto se i v NFC čípech principu detekce chyb hojně využívá. Karty Mifare DESFire Ev1 obsahují dva typy kontrolních součtů: CRC16 bit a CRC32 bit. Obecně počet bitů značí velikost výsledného kontrolního součtu, v mém případě 2 a 4 bajty. Pro oba kontrolní součty jsem musel vytvořit algoritmy a také zvolit vhodné vstupní parametry, jelikož karty od firmy NXP používají poupravené verze těchto kontrolních součtů. Principem kontrolního součtu je pro libovolně velký vstup vypočítat výstup (CRC) pevné délky. Pro implementaci jsem využil vlastní třídy TCrc, která obsahuje 2 funkce pro výše uvedené kontrolní součty. Funkce jsem volil jako třídni, tedy lze je volat bez vytvořených instancí.

## 8.3 CBC režim

Šifrovací režim CBC (Cipher Block Chaining) je metoda šifrování/dešifrování, kdy je mezi každým blokem provedena operace XOR před průchodem do šifrovacího procesu. Pomocí režimu jsme schopni docílit toho, že každý šifrovaný blok je závislý na celém vstupním textu a ne pouze na jeho částech. Režim se liší dle šifrování a dešifrování. [2]

### 8.3.1 Režim šifrování

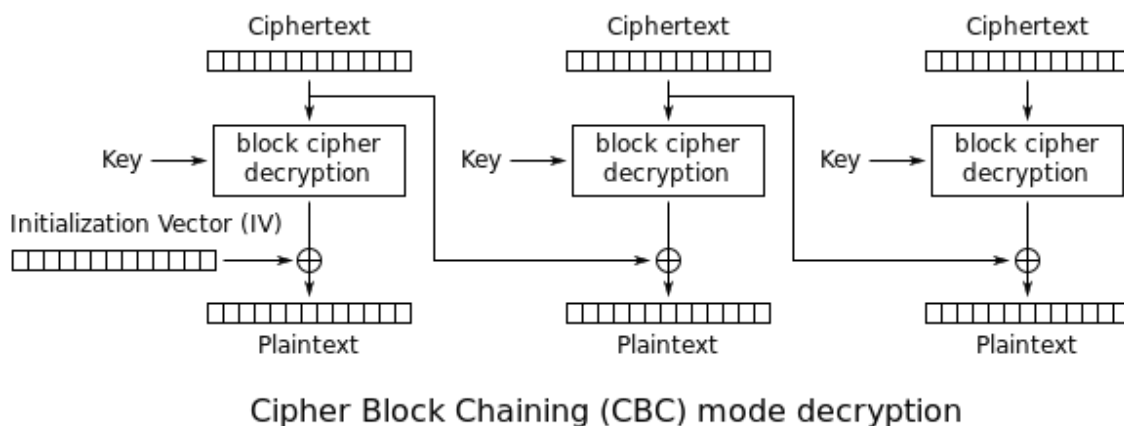
Při šifrovacím režimu potřebujeme vždy inicializační vektor (IV). U čipových karet Mifare DESFire Ev1 je tento vektor v počátku nulový, tj. obsahuje 16 nulových bajtů. Před každým procesem šifrování se provede operace XOR mezi blokem vstupního textu a inicializačním vektorem. Inicializační vektor je pro následující proces šifrování výstupem z šifrovacího procesu předcházejícího bloku. Pro lepší názornost uvádím blokové schéma, které je zobrazeno na Obr. 28.



*Obr. 27. Blokové schéma šifrování v módu CBC [25]*

### 8.3.2 Režim dešifrování

Dešifrování je postaveno na podobném principu jako šifrování. Rozdíl tvoří operace XOR, která se provádí až po samotném dešifrování. Pro tuto operaci je také vyžadován inicializační vektor, který je v prvním bloku nastaven staticky. V dalších dešifrovacích procesech se mění na základě vstupního textu. Blokové schéma dešifrovacího procesu je znázorněno na Obr. 29.



*Obr. 28. Blokové schéma dešifrování v módu CBC [25]*

## ZÁVĚR

V dnešní době se setkáváme s technologií NFC stále častěji, téměř každý den. V ČR mohou uvést např. bezkontaktní platební karty, registrace jízdenek (InKarta, OpenCard), studentské karty apod. Hlavním důvodem nasazení této technologie je především jednoduchost a také rychlost použití. Jako největší výhodu technologie vidím podporu v mobilních zařízeních, kde se v poslední době stává téměř standardem.

S rychlostí rozmachu čipových karet se zvyšují také útoky na NFC karty. Nejvíce prodaných karet registruje firma NXP, která jich prodala celkem okolo 10 miliard kusů. Z toho je asi 100 milionů karet Mifare Classic stále v oběhu. Ty se používají jako platební karty hromadné dopravy (Charlie Card, USA), přístupové karty hotelů, studentské karty, univerzální vizitky apod. Důvod proč tato čísla uvádím, je ten, že všichni kdo tyto karty využívají, jsou ohroženi. Uvedený typ karet lze emulovat a také celý obsah zkopírovat na prázdnou kartu. Výše částky, kterou musí útočník vynaložit na pořízení doporučeného hardwaru, se pohybuje v jednotkách tisíc Kč. Za tuto cenu ale může útočník získat informace, jež výrazně převyšují pořizovací náklady. Použití karet Mifare Classic tedy nelze doporučit. Jednoduché ověření typu karty lze provést pomocí mobilní aplikace (např. NFC TagInfo pro Android).

V rámci praktické části byly vytvořeny celkem 3 aplikace. První tvoří Win32 aplikace, která slouží jako mezičlánek mezi databázovým serverem a mobilním klientem. Aplikace obhospodařuje kompletní komunikaci a SQL dotazy do databáze. Další aplikace je již pro mobilní zařízení s Androidem a slouží k zápisu názvů budov do paměti čipových karet. Poslední aplikace je také pro mobilní zařízení a slouží jako záznamové médium pro načtené čipy z budov a také jako komunikátor se vzdáleným serverem.

Při řešení tématu diplomové práce vyvstalo několik problematických oblastí, které se však podařilo vyřešit. První nevýhodou tvoří psaní aplikací v jazyce Delphi. Ten přímo nepodporuje technologii NFC, která je standardem pro jazyk Java. Pro využití NFC v Delphi je nutné třídy Javy dodatečně překládat. Za největší problém lze považovat komunikaci s čipovými kartami. Obecně je NFC technologie univerzální, nicméně každá čipová karta kromě NDEF formátu využívá ke komunikaci svá proprietární řešení. Získání dokumentace čipových karet trvá delší dobu, jelikož důkladným ověřením žadatele si firmy zvyšují zabezpečení přístupu k jednotlivým dokumentům.

**SEZNAM POUŽITÉ LITERATURY**

- [1] IGOE, Tom, Don COLEMAN a Brian JEPSON. *Beginning NFC: near field communication with Arduino, Android, and Phonegap*. First edition. viii, 233 pages. ISBN 14-493-7206-6
- [2] PAAR, Christof, Don COLEMAN a Brian JEPSON. *Understanding cryptography: a textbook for students and practitioners*. First edition. Heidelberg: Springer, c2010, xviii, 372 s. ISBN 978-3-642-04100-6.
- [3] TEIXEIRA, Steve, Don COLEMAN a Brian JEPSON. *Mistrovství v Delphi 6: a textbook for students and practitioners*. Vyd. 1. Praha: Computer Press, 2002, xxv, 822 s.;. ISBN 80-722-6627-6.
- [4] COSKUN, Vedat, Kerem OK a Busra OZDENIZCI. *Professional NFC application development for Android*. Chichester [England]: Wiley, 2013, xxiv, 283 p. Programmer to programmer.
- [5] PERIS LOPEZ, Pedro, Julio C HERNANDEZ-CASTRO a Tieyan LI. *Security and trends in wireless identification and sensing platform tags: advancements in RFID*. Hershey, Pa.: Information Science Reference, c2013, xii, 298 p. ISBN 978-146-6619-920.
- [6] HOWARD, Michael, David LEBLANC a Tieyan LI. *Bezpečný kód: [techniky a strategie tvorby bezpečných webových aplikací]*. Vyd. 1. Brno: Computer Press, 2008, 895 s. ISBN 978-80-251-2050-7.
- [7] *NFC Forum*. [online]. [cit. 2015-04-15]. Dostupné z: <http://nfc-forum.org/what-is-nfc/>
- [8] *RFID chipexample*. [online]. [cit. 2015-04-15]. Dostupné z: [http://www.ideen2020.de/wp-content/uploads/RFID\\_Chip\\_004.jpg](http://www.ideen2020.de/wp-content/uploads/RFID_Chip_004.jpg)
- [9] *Mifare RFID chipexample*. [online]. [cit. 2015-04-15]. Dostupné z: <http://gatekits.ie/WebRoot/Register365/Shops/950003867/5181/95E1/276F/CF69/A46A/C0A8/190B/92D8/EM-ID-125khz-MIFARE-13-56mhz-RFID-Tag.jpg>
- [10] *In-Karta*. In: [online]. [cit. 2015-04-09]. Dostupné z: <http://www.rodicum.com/wp-content/uploads/in-karta.jpg>
- [11] *Near Field Communication*. In: *Wikipedia* [online]. [cit. 2015-03-22]. Dostupné z: [http://en.wikipedia.org/wiki/Near\\_field\\_communication](http://en.wikipedia.org/wiki/Near_field_communication)

- [12] *NFC technologie – odborný pohled na funkčnost a využití v praxi*. In: *Mobilizujeme.cz* [online]. [cit. 2015-04-21]. Dostupné z: <http://mobilizujeme.cz/clanky/nfc-technologie-odborny-pohled-na-funkcnost-a-vyuziti-v-praxi/>
- [13] CANTU, Marco, David LEBLANC a Tieyan LI. *Mistrovství v DELPHI 2 - pro Windows 95/NT: [techniky a strategie tvorby bezpečných webových aplikací]*. Vyd. 1. Praha: Computer Press, 1996, 975 s. ISBN 80-858-9675-3.
- [14] TRČÁLEK, Antonín. *Stačí přiložit: NFC a jeho využití v praxi*. In: *Mobilmania.cz* [online]. [cit. 2015-04-21]. Dostupné z: <http://www.mobilmania.cz/clanky/staci-prilozit-nfc-a-jeho-vyuziti-v-praxi/sc-3-a-1325034/>
- [15] KASPER, Timo, David OSWALD a Christof PAAR. *Cloning Cryptographic RFID Cards*. In: *Slideshare.net* [online]. [cit. 2015-04-26]. Dostupné z: <http://www.slideshare.net/lockeracid/opencard-hack-projekt-chameleon>
- [16] PETER VAN ROSSUM. *Mifare Classic Troubles*. In: *Ict-forward.eu* [online]. [cit. 2015-04-26]. Dostupné z: <http://www.ict-forward.eu/media/workshop2/presentations/rossum-mifare.pdf>
- [17] *Mifare*. In: *Wikipedia* [online]. [cit. 2015-04-26]. Dostupné z: <http://en.wikipedia.org/wiki/MIFARE>
- [18] GAUDIN, Sharon. *RFID hack could crack open 2 billion smart cards*. In: *Computerworld.com* [online]. [cit. 2014-11-22]. Dostupné z: <http://www.computerworld.com/article/2537619/mobile-apps/rfid-hack-could-crack-open-2-billion-smart-cards.html>
- [19] LUPTÁK, Pavol. *Mifare Classic analysis in Czech Republic / Slovakia*. In: *Nethemba.com* [online]. [cit. 2014-11-22]. Dostupné z: <http://www.nethemba.com/mifare-classic-slides.pdf>
- [20] NXP B.V. *MIFARE DESFire EV1 contactless multi-application IC: MF3ICDX21\_41\_81\_SDS*. Nizozemsko, 21. prosince 2010. Dostupné z: [http://www.nxp.com/documents/short\\_data\\_sheet/MF3ICDX21\\_41\\_81\\_SDS.pdf](http://www.nxp.com/documents/short_data_sheet/MF3ICDX21_41_81_SDS.pdf)
- [21] EMBARCADERO TECHNOLOGIES. *RAD Studio* [online]. [cit. 2015-04-29]. Dostupné z: <http://www.embarcadero.com/products/rad-studio>

- [22] About SQLite. *Sqlite.org* [online]. [cit. 2015-04-29]. Dostupné z: <http://www.sqlite.org/about.html>
- [23] Mobile Tutorial: Set Up Your Development Environment on Windows PC (Android). *Docwiki.embarcadero.com* [online]. [cit. 2015-04-29]. Dostupné z: [www.docwiki.embarcadero.com/RADStudio/XE8/en/Mobile\\_Tutorial:\\_Set\\_Up\\_Your\\_Development\\_Environment\\_on\\_Windows\\_PC\\_\(Android\)](http://www.docwiki.embarcadero.com/RADStudio/XE8/en/Mobile_Tutorial:_Set_Up_Your_Development_Environment_on_Windows_PC_(Android))
- [24] Cyclic redundancy check. In: *Wikipedia* [online]. [cit. 2015-05-01]. Dostupné z: [http://en.wikipedia.org/wiki/Cyclic\\_redundancy\\_check](http://en.wikipedia.org/wiki/Cyclic_redundancy_check)
- [25] Block cipher mode of operation. In: *Wikipedia* [online]. [cit. 2015-05-01]. Dostupné z: [http://en.wikipedia.org/wiki/Block\\_cipher\\_mode\\_of\\_operation](http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation)
- [26] Exceptional High-End Modeling Power. SPARX SYSTEMS. [online]. [cit. 2015-05-03]. Dostupné z: <http://www.sparxsystems.com/products/ea/>
- [27] Mobile Tutorial: Connecting to an Enterprise Database from a Mobile Client (iOS and Android). *Docwiki.embarcadero.com* [online]. [cit. 2015-05-04]. Dostupné z: [http://docwiki.embarcadero.com/RADStudio/XE8/en/Mobile\\_Tutorial:\\_Connecting\\_to\\_an\\_Enterprise\\_Database\\_from\\_a\\_Mobile\\_Client\\_\(iOS\\_and\\_Android\)](http://docwiki.embarcadero.com/RADStudio/XE8/en/Mobile_Tutorial:_Connecting_to_an_Enterprise_Database_from_a_Mobile_Client_(iOS_and_Android))

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

<i>3DES</i>	Triple Data Encryption Standard
<i>AES</i>	Advanced Encryption Standard
<i>API</i>	Application Programming Interface
<i>CBC</i>	Cipher Block Chaining
<i>CPU</i>	Central Processing Unit
<i>CRC</i>	Cyclic redundancy check
<i>DES</i>	Data Encryption Standard
<i>EPC</i>	Electronic Product Code
<i>GPS</i>	Global Positioning System
<i>GSM</i>	Global System for Mobile Communications
<i>HF</i>	Vysoká frekvence
<i>HTTPS</i>	Hypertext Transfer Protocol Secure
<i>I<sup>2</sup>C</i>	Interintegrated Circuit Communication
<i>IEC</i>	International Electrotechnical Commission
<i>IrDa</i>	Infrared Data Association
<i>ISO</i>	International Organization for Standardization
<i>LF</i>	Nízká frekvence
<i>LLCP</i>	Logical Link Control Protocol
<i>LSB</i>	Nejméně významný bit (least significant bit)
<i>MIM</i>	Man in the middle
<i>MMS</i>	Multimedia Message Service
<i>NDA</i>	Nondisclosure agreement
<i>NDEF</i>	NFC Data Exchange Format
<i>NFC</i>	Near Field Communication

---

<i>OS</i>	Operační systém
<i>PAN</i>	Personal Area Network
<i>PC</i>	Osobní počítač
<i>QR</i>	Quick Response
<i>RAM</i>	Random access memory
<i>RC4</i>	Rivest Cipher 4
<i>RFID</i>	Radio Frequency Identification
<i>RIM</i>	Research In Motion Limited
<i>ROM</i>	Read only memory
<i>SPI</i>	Serial Peripheral Interface
<i>SCOS</i>	Smart Card Operating System
<i>SDK</i>	Software development kit
<i>SHF</i>	Super vysoká frekvence
<i>SIM</i>	Subscriber Identity Module
<i>SMS</i>	Short Message Service
<i>SNEP</i>	Simple NDEF Exchange Protocol
<i>TAG</i>	Čip, štítek, kata NFC
<i>TLS</i>	Transport Layer Security
<i>UART</i>	Universal Asynchronous Receive Transmit
<i>UHF</i>	Ultra vysoká frekvence
<i>URI</i>	Uniform Resource Identifier
<i>USB</i>	Universal Serial Bus
<i>WiFi</i>	Wireless Fidelity

**SEZNAM OBRÁZKŮ**

<i>Obr. 1. RFID čipy (tagy) [8], [9]</i> .....	11
<i>Obr. 2. InKarta s NFC čipem [10]</i> .....	12
<i>Obr. 3. Fyzická struktura kontaktů [4]</i> .....	14
<i>Obr. 4. Struktura bezkontaktní čipové karty [4]</i> .....	15
<i>Obr. 5. Vývoj technologie NFC [4]</i> .....	18
<i>Obr. 6. Struktura NFC čipu [14]</i> .....	19
<i>Obr. 7. Režim přenosu čtení/zápis [4]</i> .....	22
<i>Obr. 8. Praktické použití režimu čtení/zápis [4]</i> .....	23
<i>Obr. 9. Režim přenosu peer-to-peer [4]</i> .....	23
<i>Obr. 10. Praktické použití režimu peer-to-peer [4]</i> .....	24
<i>Obr. 11. Režim přenosu emulace karty[4]</i> .....	25
<i>Obr. 12. Praktické použití režimu emulace karty [4]</i> .....	26
<i>Obr. 13. Jednotlivé vrstvy architektury NFC [1]</i> .....	27
<i>Obr. 14. Základní rozdělení kryptologie</i> .....	31
<i>Obr. 15. Mifare Classic karty</i> .....	37
<i>Obr. 16. Proxmark (vlevo) a Project Chameleon (vpravo)</i> .....	38
<i>Obr. 17. Hlavička úplné dokumentace karet Mifare DESFire Ev1</i> .....	44
<i>Obr. 18. Hlavička zkrácené dokumentace karet Mifare DESFire Ev1</i> .....	44
<i>Obr. 19. Hlavička dokumentace příkladů a doporučení</i> .....	44
<i>Obr. 20. Vývojové prostředí Embarcadero RAD Studio XE7</i> .....	45
<i>Obr. 21. Rozhraní DB Browser pro pro SQLite</i> .....	47
<i>Obr. 22. Diagram užití pro uživatelskou aplikaci</i> .....	50
<i>Obr. 23. Diagram užití pro administrátorskou aplikaci</i> .....	50
<i>Obr. 24. Princip komunikace klient-server [27]</i> .....	51
<i>Obr. 25. Rozhraní uživatelské aplikace: přihlášení a hlavní okno</i> .....	53
<i>Obr. 26. Rozhraní administrátorské aplikace</i> .....	54
<i>Obr. 27. Blokové schéma šifrování v módu CBC [25]</i> .....	58
<i>Obr. 28. Blokové schéma dešifrování v módu CBC [25]</i> .....	58

**SEZNAM TABULEK**

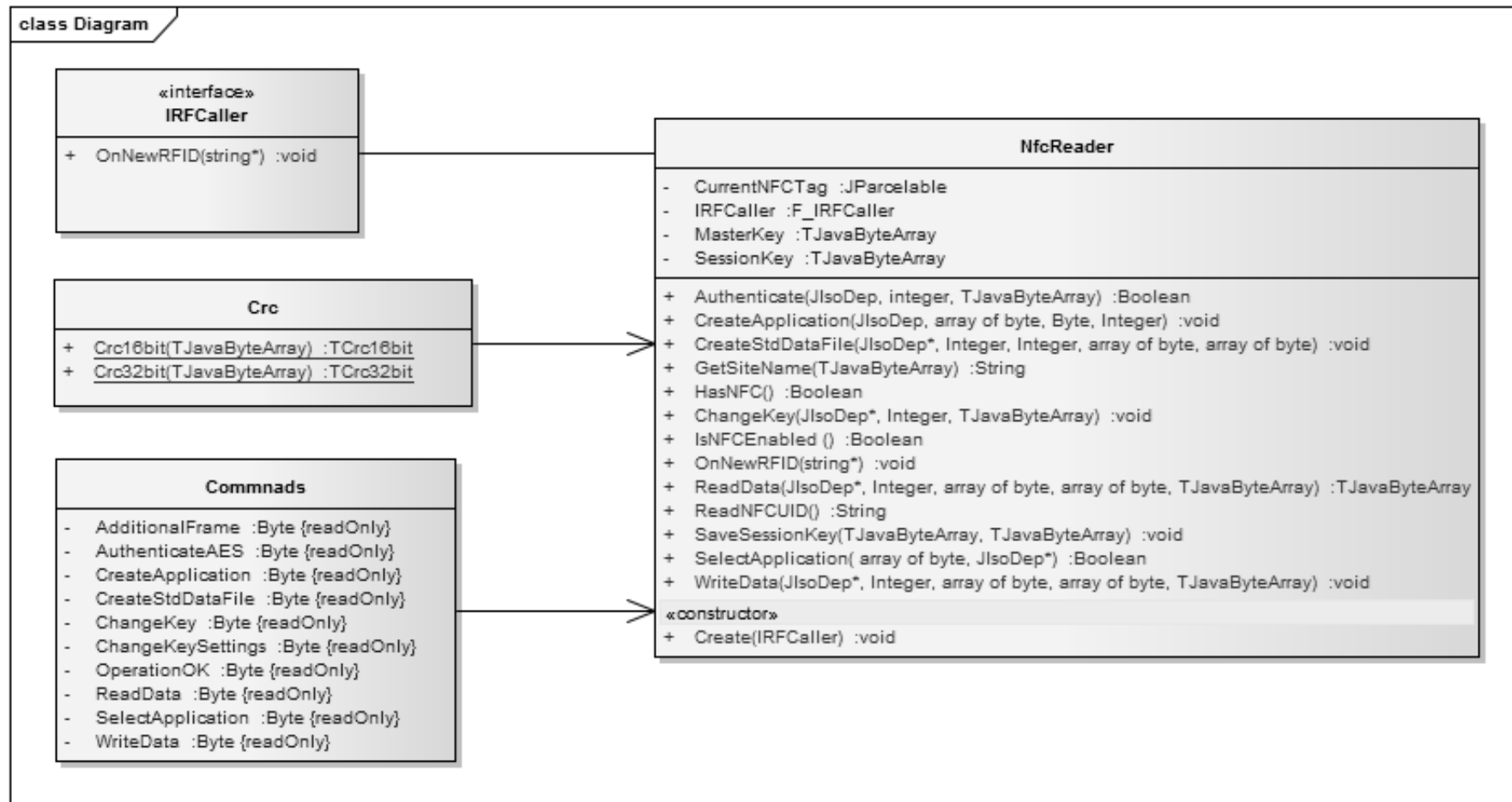
<i>Tab. 1 Popis kontaktů čipových karet .....</i>	15
<i>Tab. 2 Možné druhy komunikace mezi dvěma zařízeními .....</i>	20
<i>Tab. 3 Srovnání bezdrátových technologií .....</i>	30
<i>Tab. 4 Populární typy NFC čipů .....</i>	34

## **SEZNAM PŘÍLOH**

PŘÍLOHA P I: DIAGRAM TŘÍD – PRINCIP STRUKTURY

PŘÍLOHA P II: PŘEHLED SOUBORŮ NA CD

## PŘÍLOHA P I: DIAGRAM TŘÍD – PRINCIP STRUKTURY



## PŘÍLOHA P II: PŘEHLED SOUBORŮ NA CD

Struktura souborů:

- **bin**
  - DataSnapServer.exe
  - IdentificationSites.apk
  - IdentificationSites.s3db
  - SiteWriter.apk
- **doc**
  - fulltext.pdf
- **src**
  - AdminMainFormUnit.pas
  - AndroidManifest.template.xml
  - ClientClasses.pas
  - ClientModuleUnit.pas
  - Crc.pas
  - DataSnapClientUnit.pas
  - DataSnapServerUnit.pas
  - DeveloperExperts.Android.nfc.pas
  - DeveloperExperts.Android.nfc.Helper.pas
  - nfc\_tech\_filter.xml
  - ServerContainerUnit.pas
  - ServerModuleUnit.pas