Ekonomická fakulta
Faculty of Economics

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích
Ekonomická fakulta
Katedra aplikované matematiky a informatiky

Bakalářská práce

NFC platby mobilním telefonem

Vypracovala: Tereza Čapková
Vedoucí práce: doc. Ing. Ladislav Beránek, CSc.

České Budějovice 2021

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

Ekonomická fakulta

Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Tereza ČAPKOVÁ**
Osobní číslo:	**E18300**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Ekonomická informatika**
Téma práce:	**NFC platby mobilním telefonem**
Zadávající katedra:	**Katedra aplikované matematiky a informatiky**

Zásady pro vypracování

Cílem bakalářská práce je zmapovat potřebné technologie související s NFC, analyzovat současné aplikace, tedy konkrétní možnosti uživatele bezkontaktních plateb dle předem stanovených kritérií. Součástí práce bude vytvoření aplikace ve frameworku Xamarin.Android a jeho otestování. Práce bude také analyzovat možnosti užití NFC v nositelné elektronice a možný budoucí vývoj v této oblasti.

Metodický postup:

1. Teoretický popis konkrétních dostupných NFC technologií a aplikací na základě literární rešerše.
2. Návrh, popis vývoje a implementace aplikace ve frameworku Xamarin a jeho otestování.
3. Zhodnocení, vypracování doporučení a závěrů.

Rozsah pracovní zprávy:	**40 – 50 stran**
Rozsah grafických prací:	
Forma zpracování bakalářské práce:	**tištěná**

Seznam doporučené literatury:

1. Igoe, T., Coleman, D., & Jepson, B. (2014). *Beginning NFC: near field communication with Arduino, Android. and Phonegap*. Beijing: O'Reilly. NFC and Contactless Technologies [online]. Dostupné z: <http://nfc-forum.org/what-is-nfc/about-the-technology/>.
2. Programování NFC štítků. In: *NFCmall*. [online]. Dostupné z: <http://www.nfcmall.com/cz/t/NFCTagsEncoding>.
3. Další odborná literatura vztahující se k tématu práce.

Vedoucí bakalářské práce: **doc. Ing. Ladislav Beránek, CSc.**
Katedra aplikované matematiky a informatiky

Datum zadání bakalářské práce: **17. ledna 2020**
Termín odevzdání bakalářské práce: **16. dubna 2021**

JIHOČESKÁ UNIVERZITA
V ČESKÝCH BUDĚJOVICÍCH
EKONOMICKÁ FAKULTA
Studentská 13 (26)
370 05 České Budějovice

doc. Dr. Ing. Dagmar Škodová Parmová
děkanka

doc. RNDr. Tomáš Mrkvička, Ph.D.
vedoucí katedry

V Českých Budějovicích dne 26. března 2020

Prohlášení

Prohlašuji, že svou bakalářskou práci „NFC platby mobilním telefonem“ jsem vypracovala samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to – v nezkrácené podobě/v úpravě vzniklé vypuštěním vyznačených částí archivovaných Ekonomickou fakultou – elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

Datum	Podpis

Poděkování

Ráda bych poděkovala vedoucímu bakalářské práce doc. Ing. Ladislavovi Beránkovi, CSc. za jeho cenné rady, připomínky a vstřícnost při vypracování bakalářské práce.

Obsah práce

1 Úvod a cíl bakalářské práce

NFC neboli Near Field Communication je technologie bezdrátového připojení krátkého dosahu, která využívá interagující elektromagnetická rádiová pole. Funguje na standardizované frekvenci 13,56 MHz (dle standardy ISO/IEC 1892) a přenáší data rychlostí až 424 Kbit/s. Používá se tak pro usnadnění komunikace a sdílení dat na velmi krátkou vzdálenost (4 cm). Velkou výhodou je, že ke svému fungování nepoužívá internetové připojení.

V dnešní době je tato technologie velmi rozšířená díky chytrým telefonům, které mají již v základu implementovaný tento čip. Tuto technologii můžeme nalézt téměř v každém odvětví. Od dopravního sektoru až po zdravotní péči. Nejrozšířenější je však možnost platby, kterou každým dnem objevuje celá řada nových uživatelů.

Cílem bakalářské práce je zmapovat potřebné technologie související s NFC a analyzovat současné mobilní aplikace, tedy možnosti uživatele v tomto odvětví. Dalším cílem je vytvoření aplikace pomocí frameworku Xamarin, která bude sloužit jako demonstrace propojení kódu a technologie NFC.

V úvodu je popsána samotná technologie a její historie. Část práce je věnována implementaci NFC do mobilního zařízení a její bezpečnosti v rámci mobilních plateb. Zanalyzovány jsou také hrozby ohrožující přenos pomocí NFC. Součástí je i srovnání českého a světového trhu mobilních plateb. Hlavní částí je analýza všech dostupných mobilních aplikací v ČR, které jsou rozděleny na bankovní a nebankovní aplikace. V závěru teoretické části se uceleně popisuje současný stav technologie a její budoucnost.

Praktická část se zabývá vývojem mobilní aplikace pomocí frameworku Xamarin. Výsledná aplikace demonstruje propojení kódu a NFC technologie. Aplikace disponuje několika základními funkcemi jako je čtení a zápis. Součástí praktické části je také testování aplikace vývojářem a uživateli.

2 Technologie NFC

2.1 NFC vs. RFID

Technologie NFC vznikla rozšířením technologie RFID (Radio Frequency Identification). RFID není komunikační technologií jako je NFC, ale slouží pouze pro identifikaci. RFID tag dokáže udržet pouze malé množství dat, konkrétně hovoříme o 1000 bytech a méně. NFC bylo vytvořeno na základě RFID umožněním více komplexní výměny mezi zařízeními. Je tedy pořád možné přečíst RFID tag pomocí NFC. (Igoe et al., 2014)

RFID výměna obsahuje dva hráče – iniciátora a cíl. Iniciátorem může být čtečka tagů nebo čtecí/zapisovací zařízení. Iniciátor začíná výměnu generací rádiového pole a čeká na odezvu od jakéhokoliv cíle v poli. Cíl odpovídá pomocí UID (unique indetifier number) podle kterého se navzájem dokážou identifikovat. (Igoe et al., 2014)

Tato výměna může být buď pasivní nebo aktivní. Pasivní výměna probíhá mezi čtečkou či zapisovatelem a tagem, který nemá žádný zdroj energie. Tag získává potřebnou energii z rádiového pole. Tato energie je zpravidla velmi malá a dostačí pouze pro odeslání signálu zpět iniciátorovi. Aktivní výměnou rozumíme cíl, kterým je nezávisle napájené zařízení. Díky tomu, že je cíl napájen je výměna zprostředkována i na větší vzdálenosti.

NFC je sadou bezdrátových technologií krátkého dosahu. Technologie NFC pracuje na 13,56 MHz na vzduchovém rozhraní ISO/IEC 18000-3 a rychlostí od 106 kbit/s do 424 kbit/s. (Drhlík, 2017)

O NFC můžeme přemýšlet jako o rozšíření RFID technologie. Výměna probíhá také mezi dvěma zařízeními a obsahuje iniciátora a cíl. NFC toho však dokáže mnohem více než si pouze vyměnit UID a přečíst data cíle. Největším rozdílem mezi těmito dvěma technologiemi je, že NFC jsou ve většině případů programovatelná zařízení – mobilní telefony. To nabízí široké využití. NFC tedy nedoručuje pouze statická data z paměti, ale cíl může pokaždé generovat unikátní odpověď například podle UID. (Igoe et al., 2014)

2.2 Historie NFC

Technologie Near Field Communication byla původně vyvinuta koncem 19. století, kdy Thomas Edison experimentoval s rádiem. Nikdo však neměl ponětí, jak široké využití bude v budoucnu mít.

První opravdový pokus o vytvoření technologie podobnou NFC měl Charles Walton, který 17.května 1983 získal patent spojený s technologií RFID. V praxi se Waltonova technologie nevyužívala až do roku 1997, kdy byla využita společností Hasbro v jejich Star Wars hračkách, které mezi sebou uměly komunikovat na krátkou vzdálenost. (Sabella, 2019)

Přesouváme se do roku 2002, kdy se Sony spojilo se společností Phillips, aby vytvořili jakýsi nástin technologie NFC. Phillips požádalo konkrétně o 6 patentů na NFC. Tyto patenty byly vyvíjeny australskými a francouzskými inženýry – konkrétně Franz Amtmann a Philippe Maugars.

V roce 2004 vzniklo NFC Forum pod záštitou firem Nokia, Phillips a Sony. Tato nezisková organizace se zaměřuje na vytváření standardů NFC, podporu rozvoje produktů využívajících tuto technologii, jejich kontrolu a rozšiřování povědomí o NFC mezi zákazníky a firmami. Součástí tohoto fóra je i značka N-mark, díky které jde snadno identifikovat místa na kterých lze využít technologii NFC. (NFC forum, n.d.)

Byl to však rok 2006, kdy společnosti začaly vyrábět první NFC štítky. Byly to malé objekty, téměř jako samolepky, které umožňovaly přenosy velmi malých souborů, pokud byly dva telefony (v té době konkrétně Nokia 6131) přiloženy k sobě. V začátcích neexistovaly žádné pokročilé aplikace, a tak využití bylo téměř nulové. (Sabella, 2019)

První telefon vyroben s plně funkční technologií tohoto typu byl vyroben až v roce 2010 s operačním systémem Android. Konkrétně to byl model Nexus S od společnosti Samsung.

O několik let později se začalo projevovat široké využití této technologie. V roce 2014 společnost Apple představila aplikaci Apple pay, která fungovala na iOS. O rok později, listopad 2015, společnost Google následovala a vydala aplikaci Android pay. Od té doby se však technologie plateb rapidně změnila – je v neustálém vývoji, a to hlavně v oblasti bezpečnosti.

2.3 Módy přenosu dat NFC

Na rozdíl od technologie RFID dokáže NFC operovat ve třech módech přenosu dat: reader/writer mód, režim emulace karty a peer-to-peer mód. To otevírá další možnosti využití a větší způsob zabezpečení.

2.3.1 Reader/Writer mód

V režimu zapisovače funguje mobilní telefon jako iniciátor a zapíše data do tagu. Pokud značka již obsahuje některá data před procesem zapisování, jsou data přepsána. V režimu čtečky iniciátor čte data, která jsou již v paměti cíle. Zařízení NFC musí rozpoznat o jaký typ tagu se jedná a podle toho s ním nakládat. Data se vrací zpátky ve formátu NDEF a dle typu dat jsou zobrazena uživateli. (Igoe et al., 2014)

Pokud iniciátor zaznamená více než jeden cíl ve svém rádiovém poli, spoléhá se na anti kolizní algoritmus pro výběr právě jednoho cíle. (Sabella, R., 2019)

2.3.2 Režim emulace karty

Režim emulace karty umožňuje NFC zařízení fungovat jako bezkontaktní čipová karta. Hlavním příkladem jsou kreditní či debetní karty, identifikační karty nebo přístupové karty. NFC zařízení umožňuje uložení více než jedné karty. U tohoto režimu je důležité si uvědomit, že zabezpečení NFC (prostřednictvím SE nebo HCE) chrání pouze tokeny používané k identifikaci jednotlivce. Je tedy nutné mít další aplikaci, která poskytuje zabezpečení dat. V tomto režimu si mobilní telefon nevytváří své rádiové pole, ale funguje zde jako cíl. O rádiové pole se stará NFC čtečka. (Igoe et al., 2014)

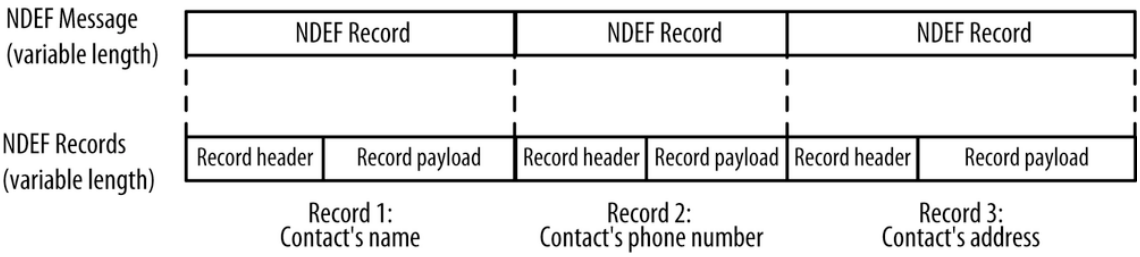
2.3.3 Peer-to-peer

Tento režim je specifický právě pro NFC technologii. Jedná se o režim, kdy si dvě NFC zařízení dokážou vyměnit data oběma směry. Využití nalezne především ve výměně dat, posílání zpráv, či výměně kontaktů. Podmínkou je, že obě zařízení jsou napájena. (Igoe et al., 2014)

2.4 Datový formát NDEF

Data vyměňované mezi NFC zařízeními a tagy se formátují pomocí NDEF (NFC Data Exchange Format). NDEF je společný datový formát, který funguje napříč všemi NFC zařízeními. Každá NDEF zpráva obsahuje jeden nebo více NDEF záznamů (Obr.1).

Každý záznam obsahuje hlavičku a payload. Hlavička se skládá z typu obsahu, unikátního ID a informaci o délce payloadu. Za payloadem se skrývají samotná přenášená data. Každý NDEF záznam nese jeden set dat (Obr.1). Konkrétní příklad je při odesílání kontaktních informací, kdy jeden NDEF záznam nese jméno kontaktu další telefonní číslo a poslední adresu kontaktu.



Obrázek 1: Datový formát NDEF

Zdroj: Igoe et al., 2014

Těchto záznamů existuje hned několik druhů a NFC zařízení musí vědět, co s každým typem dělat. Nejpoužívanější typy jsou vyjmenovány níže.

2.4.1 Jednoduché textové záznamy

Tento typ obsahuje jakýkoliv text ve formátu string, který chce uživatel poslat. U tohoto typu záznamu existují dva hlavní případy užití: zobrazení prostého textu na zařízení nebo uložení jedinečného ID na NFC tag, které může být používáno v dalších aplikacích. Tento typ vždy obsahuje metadata ukazující jazyk a kódování (např. UTF-8). (Igoe et al., 2014)

2.4.2 URI

Typ URI obsahuje síťovou adresu. Cíl, který přijme URI NDEF záznam je očekáván předat záznam aplikaci, která ho dokáže zobrazit. Předává tedy tuto informaci ve většině případů webovému prohlížeči.

2.4.3 Smart Poster

Využití tento typ získává, pokud chce uživatel přidat více informací ke svému plakátu. To může obsahovat URI, ale také může obsahovat další data jako je textová zpráva nebo kontaktní informace. V cíli je typ zpracován dle obsahu zprávy. V zařízení se tedy zobrazuje dle daného typu NDEF.

2.4.4 Podpis

Podpisový NDEF poskytuje cestu, jak předat důvěryhodné informace o původu dat obsažených v NDEF záznamu.

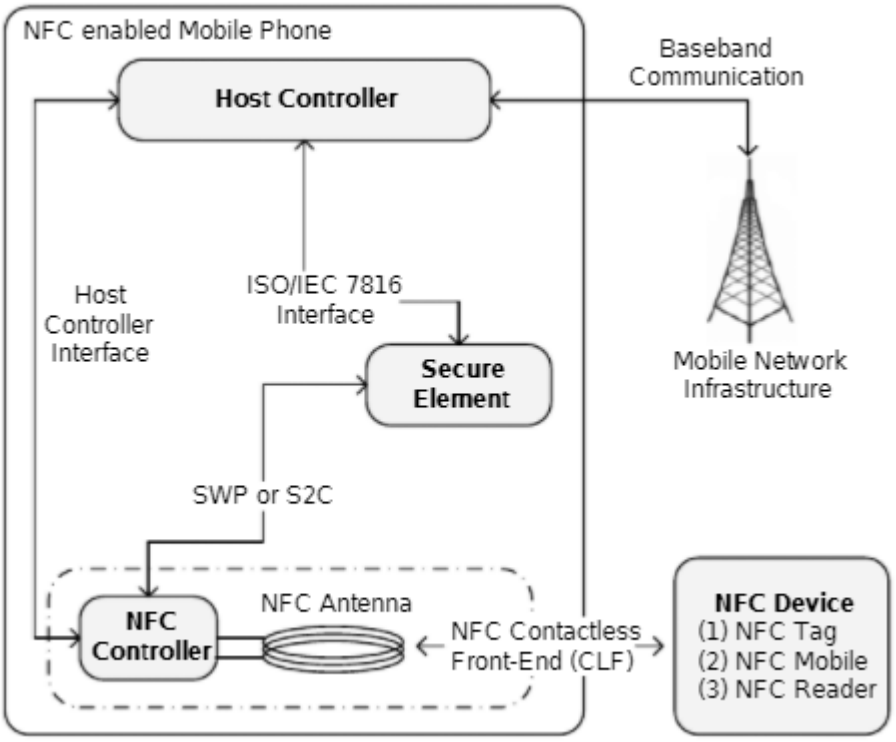
2.4.5 Kontakt

NDEF typu kontakt se používá pro rychlé a efektivní předávání kontaktů. Může být naprogramován i tak, že se kontakt rovnou uloží do zařízení nebo se pouze zobrazí v textové formě.

3 NFC v mobilních telefonech

3.1 Architektura NFC v mobilních telefonech

Technologie NFC se v mobilních zařízeních skládá ze dvou prvků. První z nich je zabezpečená část neboli Secure Element (SE) a druhým je samotné rozhraní pro komunikaci NFC. Toto rozhraní se skládá z NFC antény, integrovaného obvodu NFC ovladače a NFC bezdrátového front-endu. Propojení SE s NFC a jejich komunikační cesty zobrazuje obr.2.



Obrázek 2: Obecná architektura mobilních telefonů s NFC

Zdroj: Coskun et al., 2013

NFC ovladač umožňuje NFC spojení. Slouží jako modul mezi analogovým radiofrekvenčním signálem a NFC anténou. Bezdrátový NFC front-end je definicí protokolu na vrchu datového spojení linkové vrstvy. Zprávy jsou tak přenášeny mezi zabezpečenou částí (SE) a tímto NFC front-endem. Nejdůležitějším prvkem pro NFC platby je právě zabezpečený prvek. Toto místo v telefonu slouží jako úložiště pro citlivá data uživatele, kterými mohou být například informace o platební kartě. Všechna tato citlivá data jsou na SE šifrována a zabezpečena heslem. SE je jakousi kombinací mezi

hardwarem, softwarem, rozhraním a protokolem. Tímto SE může být čip již implementovaný od výrobce, speciální typ SIM karty nebo externí čip v mikro SD kartě. Nejčastějším z nich je implementovaný čip od výrobce. Novou technologií, která se používá místo SE je HCE, kde se pro ukládání dat používá virtuální cloud, ve kterém jsou data zabezpečena. (Coskun et al., 2013)

3.2 Zabezpečení NFC

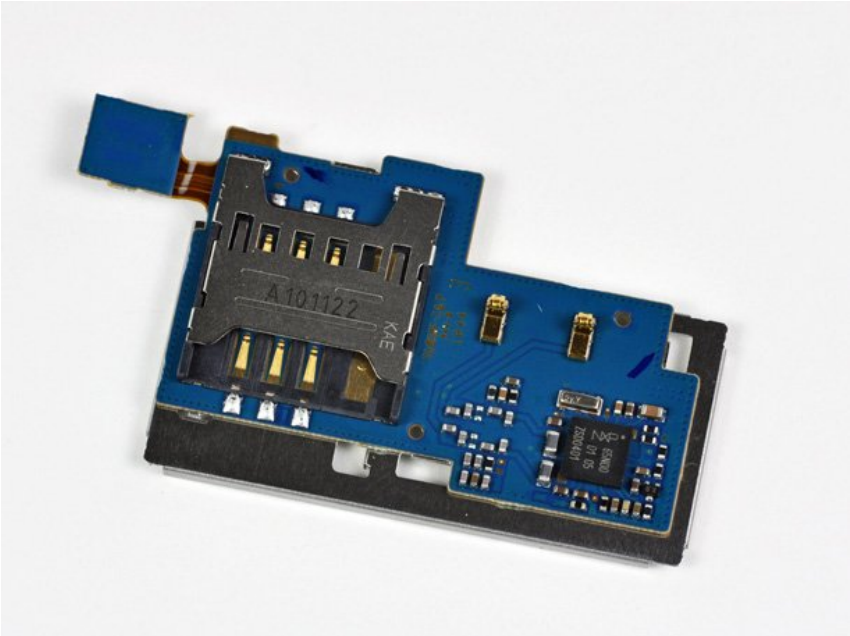
3.2.1 Secure-element (SE)

Jde o zabezpečené úložiště dat, které je chráněno heslem. Tento čip je v podstatě stejný čip jako ten, který se používá na kreditních kartách. Má samostatný operační systém. Všechny informace jsou uloženy právě na tomto čipu a nelze je číst nebo kopírovat ani v operačním systému telefonu. Secure element funguje pouze se speciálními důvěryhodnými aplikacemi, jako jsou vybrané virtuální peněženky.

Čip komunikuje přímo s platebními terminály, takže i když je smartphone napaden malwarem, hackeři tyto informace nemohou zachytit, protože data se nepřenášejí do hlavního operačního systému, ale vždy zůstávají ve specializovaném systému Secure Elementu.

Secure Element ve skutečnosti nemusí být zabudován do smartphonu. Může být odnímatelný – například ve formátu paměťové karty. Někteří mobilní operátoři dokonce vyrábějí SIM karty, které mohou ukládat informace o kreditních kartách nebo průkazech veřejné dopravy.

Konkrétně existují tři formy SE v mobilních zařízeních. První z nich je UICC (Universal Integrated Circuit Card). Jedná se o novou generaci klasické SIM karty, na kterou se pak ukládají samotná data. Tento typ SE má nevýhodu v tom, že tyto SIM karty vydává mobilní operátor, který si sám řídí přístup do SE. Druhá forma je integrace SE přímo do telefonu (Obr.3). Zabezpečený čip se nachází přímo v telefonu a nejde nijak vyjmout. Poslední formou je externí SE například ve formě speciální microSD karty. Tato forma se již téměř nevyužívá.

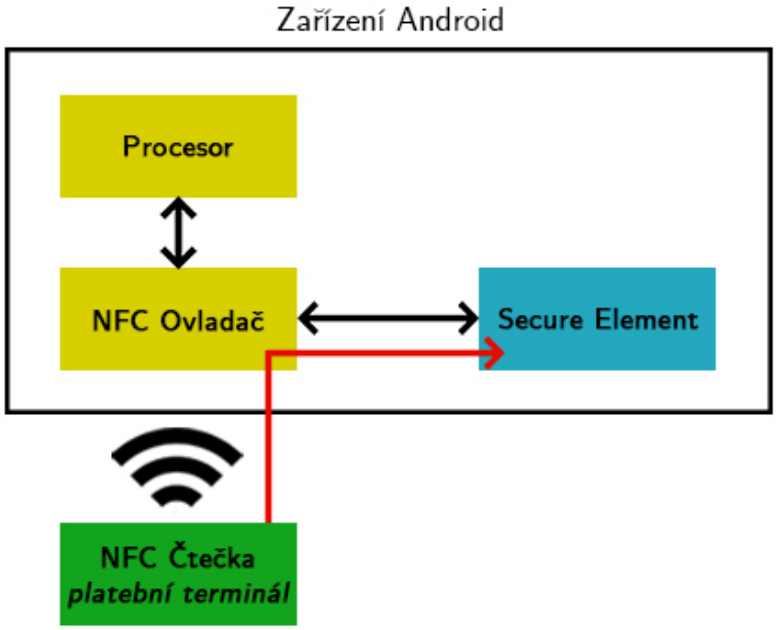


Obrázek 3: Integrovaný obvod z Google Nexusu S s čipem NXP PN65N

Zdroj: Korb & Pultzner, 2012

Komunikace pomocí SE (Obr.4) probíhá mezi několika komponenty. Pro zjednodušení hovoříme o komunikaci na operačním systému Android. Platební terminál představuje samotný NFC reader, který čeká na iniciátora. V zařízení se nachází NFC ovladač a SE.

Platební karta musí být předem nahrána do SE pomocí speciálních důvěryhodných aplikací. Tyto citlivá data se nacházejí pouze v SE, kde jsou zabezpečena heslem. Při přiložení mobilního telefonu k terminálu naváže NFC čtečka (platební terminál) komunikaci s NFC ovladačem. Tento ovladač provede nastavení správného režimu pro komunikaci. V tomto případě tedy režim emulace karty. Přes NFC ovladač probíhá oboustranná komunikace mezi čtečkou a SE. Tato komunikace není nikam přeposílána. Samotný Secure Element neprovádí bezkontaktní platby. O to se stará aplikace, která posílá všechny požadavky i odpovědi. Jiné aplikace k těmto datům přístup nemají.



Obrázek 4: Komunikace pomocí SE

Zdroj: Autor práce

3.2.2 Host Card Emulation (HCE)

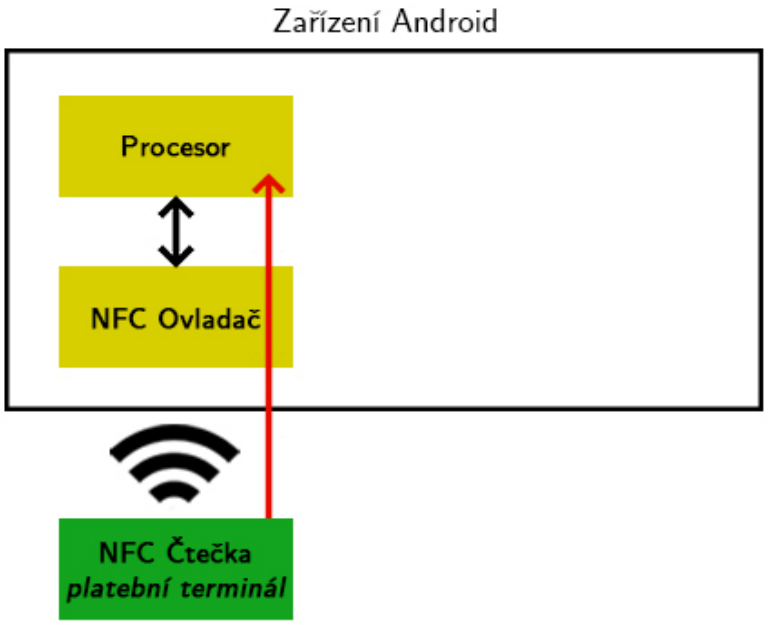
Emulace hostitelské karty (HCE) je softwarová architektura, která poskytuje přesnou virtuální reprezentaci různých elektronických identifikačních (přístupových, tranzitních a bankovních) karet pouze pomocí softwaru. Na rozdíl od SE tedy nepotřebuje přítomnost fyzického čipu v mobilním zařízení, což je tou největší výhodou.

S touto technologií přišla na trh společnost Google. Jedná se o zabezpečený virtuální cloud, kam jsou ukládána citlivá data. Ke správné funkčnosti tak stačí pouze připojení k internetu i když novější aplikace už nepotřebují ani to (platba je uložena do zařízení a proběhne až v momentě připojení na internet). Pro zvýšení zabezpečení se využívají tokeny, hesla či otisky prstů k samotné autorizaci platby. Platby jsou zde také chráněny pomocí umělé inteligence díky analýze zkoumající chování majitele. Tato analýza zkoumá každou platbu, aby nedocházelo k podezřelým transakcím. V případě podezřelé transakce (např. neobvyklá částka) je platba zablokována.

HCE umožňuje mobilním aplikacím běžícím na podporovaných operačních systémech nabízet řešení platebních karet a přístupových karet nezávisle na třetích stranách, přičemž využívá kryptografické procesy, které tradičně používají hardwarové zabezpečené prvky bez nutnosti fyzického zabezpečeného prvku. Tato technologie umožňuje obchodníkům

snadněji nabízet řešení platebních karet prostřednictvím mobilních bezkontaktních platebních řešení s uzavřenou smyčkou, nabízí distribuci platebních karet v reálném čase a umožňuje scénář snadného nasazení, který nevyžaduje změny softwaru uvnitř platebních terminálů.

Komunikace pomocí HCE (Obr.5) probíhá pouze pomocí NFC čtečky (platebního terminálu) a procesoru mobilního zařízení. Samozřejmě je zde přítomný i NFC ovladač, který zajišťuje přepnutí NFC do správného módu tedy režim emulace karty. Opět je nutné předem nahrát platební kartu do speciální důvěryhodné aplikace. Při přiložení mobilního telefonu k terminálu dochází k inicializaci komunikace s NFC ovladačem, který přepíná NFC mód. Mobilní aplikace, která posílá požadavky a odpovědi platebnímu terminálu, běží na procesoru. Proto je komunikace přímá a není potřeba přítomnost Secure Elementu.



Obrázek 5: Komunikace pomocí HCE

Zdroj: Autor práce

3.3 Podpora NFC jednotlivými OS

Pro správnou funkčnost NFC v mobilních zařízeních není dostatečná pouze přítomnost NFC rozhraní, ale musí být vybaveno i operačním systémem, který technologii NFC umožňuje. V současné době všechny velké mobilní operační systémy tuto technologii podporují.

Trh s operačními systémy v roce 2020 ovládají pouze dva velikáni. První místo zaujímá Android (84,8 %) a druhým je iOS (15,2 %). Jiné operační systémy jako je například Windows Phone již na trhu téměř zanikly resp. je ukončena podpora tohoto OS. Novým hráčem na tomto trhu je KaiOS jehož rozvoj se předpokládá v následujících letech. (Smartphone Market Share, 2020)

Vzhledem k tomu, že se později v práci zabývám analýzou jednotlivých mobilních aplikací, které umožňují platby pomocí NFC, je důležité si tyto mobilní operační systémy představit.

3.3.1 Android

Android je mobilní operační systém založený na upravené verzi jádra Linuxu a dalšího softwaru s otevřeným zdrojovým kódem, který je primárně určen pro mobilní zařízení s dotykovou obrazovkou, jako jsou smartphony a tablety. Android je vyvíjen konsorciem vývojářů známým jako Open Handset Alliance a komerčně sponzorovaný společností Google. Byl představen v listopadu 2007 a první komerční zařízení Android bylo spuštěno v září 2008.

Nad jádrem Linuxu je middleware, knihovny a API napsané v jazyce C a aplikační software běžící na aplikačním rámci, který zahrnuje knihovny kompatibilní s Javou. Vývoj linuxového jádra pokračuje nezávisle na dalších projektech zdrojového kódu systému Android.

Je to bezplatný a otevřený software. Jeho zdrojový kód je známý jako Android Open Source Project (AOSP), který je primárně licencován pod licencí Apache. Většina zařízení Android se však dodává s předinstalovaným dalším vlastním softwarem, zejména s Google Mobile Services (GMS), který zahrnuje základní aplikace, jako je Google Chrome, digitální distribuční platforma Google Play a související vývojová platforma Google Play Services.

Android je celosvětově nejprodávanějším operačním systémem na smartphonech od roku 2011 a na tabletech od roku 2013. V květnu 2017 má více než dvě miliardy aktivních uživatelů měsíčně, největší nainstalovanou základnu jakéhokoli operačního systému a od srpna 2020 Google Play Store obsahuje více než 3 miliony aplikací. Aktuální stabilní verze je Android 11 vydaný 8.září 2020.

3.3.2 iOS

Operační systém iOS je mobilní OS vytvořený a vyvinutý společnosti Apple Inc. a to výhradně pro jejich hardware. Tento operační systém momentálně běží na mobilních zařízeních iPhone a je základem pro další tři operační systémy od společnosti Apple: iPadOS, tvOS a watchOS. Na rozdíl od Androidu se jedná o proprietární software i když jsou některé jeho části open source na základě licence Apple Public Source License.

Systém iOS, který byl představen v roce 2007 pro iPhone první generace a od té doby byl rozšířen o podporu dalších zařízení Apple, jako je iPod Touch (září 2007) a iPad (leden 2010). V březnu 2018 obsahuje Apple App Store více než 2,1 milionu aplikací pro iOS, z nichž 1 milion je nativní pro iPady. Tyto mobilní aplikace byly kolektivně staženy více než 130 miliardkrát.

Hlavní verze iOS jsou vydávány každoročně. Aktuální stabilní verze iOS 14 byla pro veřejnost vydána 16. září 2020. Přinesla mnoho změn uživatelského rozhraní, včetně možnosti umístit widgety na domovskou obrazovku, kompaktního uživatelského rozhraní pro Siri i telefonní hovory a možnosti změnit výchozí webový prohlížeč i e-mailové aplikace.

4 Mobilní platby

Mobilní platby mohou probíhat i jinak než využitím technologie NFC. Je důležité zmínit široké rozšíření mobilních plateb probíhajících přes QR kódy, které technologii NFC konkuruje obzvlášť v USA, kde obchodníci nabízejí tuto platbu i v běžných obchodech či restauracích.

Platba NFC je speciální typ mobilní platby. V odborné literatuře byly mobilní platby definovány jako typ bezhotovostní platby, kterou lze provést pomocí mobilních zařízení, jako jsou mobilní telefony, tablety nebo notebooky. (Chen, & Zhang, 2017)

Klíčovým rozdílem mezi platbou pomocí bezkontaktní karty a NFC je využití komunikačních postupů a použitých kanálů. Tradiční bezkontaktní platby zasílají informace prostřednictvím vyhrazených kanálů, a to obzvlášť pro všemi známé systémy jako je MasterCard nebo Visa. Při platbě pomocí NFC probíhá výměna informací pouze mezi zařízením a terminálem. Po odeslání dat ze zařízení NFC je komunikace v platebním systému prováděna pouze terminálem.

Kombinace mobilních plateb a bezkontaktních plateb činí tuto technologii atraktivní z hlediska jednotlivých uživatelů. Uživatel u sebe nepotřebuje mít fyzickou kartu. Díky technologii NFC probíhá platba jednoduchým způsobem, nevyžaduje totiž před provedením platby inicializaci – stačí klepnout nebo umístit telefon s NFC modulem poblíž terminálu. Další výhodou je rychlý přístup k informacím jako je historie nákupu nebo zůstatek na účtu.

4.1 Bezpečnost

Bezpečnost mobilních plateb je otazníkem pro mnohé uživatele. Někteří uživatelé stále nevěří, že telefon je naprosto bezpečné zařízení v rámci využívání NFC. Technologie NFC je velmi nová, a tak vyvolává mnoho otázek. Uživatelé se bojí o svá citlivá data a mají strach, že jim je někdo velmi jednoduše může ukrást například pomocí odcizení telefonu či pomocí načtení přes speciální čtečky. Na následujících stránkách proto uvádím jednotlivé zabezpečovací prvky.

4.1.1 Tokenizace NFC plateb

Tokenizace probíhá z důvodu zabezpečení pro bezkontaktních platbách. Tokenizace snižuje riziko úniku citlivých informací a je standardem pro jakékoliv bezkontaktní platby (nejen NFC).

Základním prvkem tokenizace NFC je nahrazení čísla primárního účtu (PAN) tokenem. Token je náhodně vygenerované 16místné číslo, které nahrazuje PAN. Při odposlechu mimo probíhající konverzaci je získání tohoto čísla zcela zbytečné, protože token je náhodné číslo určené právě pro jednu transakci.

Kromě tokenizovaného PAN generuje software pro mobilní platby dynamickou hodnotu ověření karty neboli dCVV. Tento dCVV je kryptografická hodnota, která je jedinečná pro jednu transakci a lze ji použít pouze jednou. Životnost dCVV je velmi krátká a tento token je vázán na konkrétní telefon. Nelze jej tedy použít k výrobě padělané platební karty ani nákupu na webu. Jakékoliv transakce, které obsahují tento unikátní token, nepocházející z registrované telefonní peněženky jsou zablokovány.

4.1.2 Zamčená obrazovka

Každá aplikace pro platby vyžaduje, aby byl telefon uzamčen alespoň pomocí gesta či číselného kódu. Pokud má uživatel pouze jednoduché odemykání bez žádného zabezpečení aplikace ho nenechá vložit ani informace o jeho kreditní kartě.

4.1.3 Biometrie

Trendem v bezpečnosti mobilních telefonů je přítomnost čtečky prstů v každém chytrém telefonu. Tento prvek může sloužit i jako forma autorizace platby. Díky tomuto zabezpečení má uživatel jistotu, že všechny platby může provádět pouze on. Modernější, ale méně využívané řešení, je rozpoznání obličeje. Některé aplikace tak při platbě nad určité částky požádají uživatele, aby se vyfotil. Mezi lidmi však tato metoda ověřování nemá příliš velkou oblibu, protože odstraňuje jednu z výhod NFC, a to je rychlost.

4.1.4 Displej

Aby mohla transakce proběhnou musí být při platbě rozsvícený displej s odemčeným telefonem. Bez odemčeného a rozsvíceného telefonu se NFC nepokouší o spojení.

4.1.5 Vzdálenost

Jak již bylo zmíněno, NFC přenáší data na velmi malé vzdálenosti. Při platbě uživatel přiloží mobilní telefon k terminálu. Zloděj by se se svým čtecím zařízením musel přiblížit

přibližně na 5 cm, aby mohl něco odposlechnout, a to je v prostředí obchodů velmi složité a každý by si toho jistě všiml.

4.1.6 Heslo k aplikaci

V případě, že uživatel si chce být zabezpečením jistý, může přidat extra vrstvu ochrany pomocí přidání hesla k aplikaci. Tento typ zabezpečení lze použít u jakékoliv aplikace, ovšem u platebních aplikací je to vhodné. Pokaždé při otevírání aplikace se tak systém zeptá na heslo, bez kterého se do aplikace nelze dostat.

4.2 Hrozby

Jako každá finanční transakce i NFC má své slabiny a mezery. Komunikace pomocí této technologie je standardně nezabezpečené a o samotné zabezpečení se starají až komunikující strany na vyšších vrstvách. V některých případech se používají i přídavné algoritmy pro větší zabezpečení. Následující text se zabývá jednotlivými hrozbami a jejich řešeními.

4.2.1 Odposlech

Odposlech je pravděpodobně největší hrozbou pro všechny bezkontaktní platby pomocí NFC, ale jak bylo zmíněno díky tokenizaci je již hrozba minimální. Odposlouchávání je metoda útoku, která se nutně nezaměřuje na krádež informací nebo osobní či finanční škody pro oběť. Tento útok může sloužit k narušení a blokování komunikace mezi dvěma zařízeními NFC nebo k poškození dat, která mají být přenášena. (Korhonen, 2017)

Pomocí antény, zesilovače a dekódovacího zařízení lze realizovat odposlech radiofrekvenčního signálu komunikujících zařízení. Úspěšnost odposlechu je závislá na mnoha proměnných. Samotný odposlech se dělí do dvou kategorií, kde záleží hlavně na typu komunikace. (Rosenberg & Mertlík, 2013)

Při pasivní komunikaci mezi dvěma zařízeními je odposlech velmi složitý. NFC totiž generuje svou odpověď pouze při přítomnosti čtecího zařízení. Zároveň tato komunikace nedosahuje velkých vzdáleností. Tento odposlech je teoreticky možný na maximální vzdálenost jednoho metru, a to v případě využití opravdu dobré antény. (Rosenberg & Mertlík, 2013)

Pokud jde o aktivní komunikaci je odposlech pro útočníka mnohem jednodušší. NFC totiž nepotřebuje čtečku k napájení, a tak vysílá data s větším ziskem. Vzdálenost možnosti odposlechu se tak zvětšuje až na 10 metrů.

Odposlechu mohou zabránit dvě metody. Nejprve je tu funkce samotného NFC. Vzhledem k tomu, že zařízení musí být k odesílání signálů poměrně blízko, má zločinec omezený rozsah, aby mohl pracovat na zachycování signálů. Druhou metodou jsou zabezpečené kanály. Když je vytvořen zabezpečený kanál, jsou informace šifrovány a dekódovat je může pouze autorizované zařízení. Důvod existence těchto zabezpečených kanálů je, že NFC technologie sama neobsahuje žádný mechanismus pro šifrování.

4.2.2 Korupce a modifikace dat

K poškození a manipulaci s daty dochází, když zločinec manipuluje s daty odesílanými čtenáři nebo zasahuje do odesílaných dat. Přijímaná data jsou poté poškozená nebo zbytečná. Vyměňovaná data se v průběhu upraví takovým způsobem, aby z toho měl útočník nějaký prospěch. Funguje to tak, že útočník může použít rušičku RFID ke krátké výměně dat a ke změně binárního kódování původní výměny.

K narušení komunikace stačí, aby zařízení s větším výkonem rušilo přenášenou posloupnost bitů na rádiové frekvenci 13,56 MHz. Tím je průběh NFC komunikace náhodně modifikován a dochází ke špatnému vyhodnocování dat na straně příjemce. V případě modifikace dat se útočník snaží poslat modifikovaná data příjemci tak, aby se mu data jevila jako validní. Pokud chce útočník změnit přenášená data, tak musí modifikovat jednotlivé bity radiofrekvenčního signálu v přesně daném okamžiku. (Rosenberg & Mertlík, 2013)

Tomuto rušení může zabraňovat to, že NFC zařízení kontrolují elektromagnetické pole ve svém okolí. Energie nutná k přerušení komunikace je totiž mnohem větší než energie, kterou je třeba využít na detekci NFC zařízení. Útok tak můžeme snadno detekovat, ale nemůžeme mu zabránit. Zařízení tedy průběžně kontrolují radiofrekvenční pole kolem nich a pokud zjistí narušení automaticky zastavují přenos dat a uzavírají komunikaci. (Rosenberg & Mertlík, 2013)

4.2.3 Vkládání dat

V případě, že NFC zařízení potřebuje dlouhou dobu na odpověď ke čtecímu zařízení, má útočník možnost vložit svoji zprávu do komunikace mezi těmito zařízeními. Funguje to tak, že útočník odešle svou odpověď dříve než dotazované zařízení. V případě, že by se tyto zprávy překrývali, data se vyhodnotí jako chybná.

Tomuto útoku se zabraňuje zkracováním doby nutné pro odpověď. Při zkrácení této doby totiž útočník nestačí vložit svá data do komunikace a budou přijata pouze data od

správného zařízení. Standardem je monitorování elektromagnetických vln v okolí a v případě detekce zrušení komunikace. Nejzákladnějším řešením je však použití zabezpečeného kanálu pro komunikaci.

4.2.4 Man in the Middle – Útok ze středu

Úkol útočníka je se stát aktivním prostředníkem v komunikaci díky odposlechu. V případě, že je úspěšný může odposlouchávat i modifikovat data. Prakticky je tento útok opravdu složitý a nebyl zaznamenán žádný takový útok.

4.2.5 Přepojovaný útok

Přepojovaný útok probíhá tak, že útočící zařízení přijímá požadavky od čtecího zařízení a následně je přeposílá k oběti útoku. Oběť začne odesílat odpověď, kterou opět zachytí útočící zařízení a přepošle je zpět ke čtecímu zařízení. Útočník může tyto data nejen odposlouchávat, ale i modifikovat. Vše musí probíhat v reálném čase, aby komunikující strany nezjistili narušení komunikace. (Rosenberg & Mertlík, 2013)

Tohoto útoků známe hned několik typů podle toho, v jakém režimu je zařízení a čtečka. Například pokud jsou obě strany v aktivním režimu musí útočník zachytit data a patřičným rušením zabránit jejímu doručení. V tomto případě musí útočník rychle střídat směry na odposlech a při tom musí provádět i rušení, aby zabránil přímé komunikaci. (Rosenberg & Mertlík, 2013)

V praxi jsou přepojované útoky v radiofrekvenčním pásmu zcela nemožné. Pro útočníka je totiž složité vysílat jedním směrem rušení a z druhé strany odposlouchávat.

4.2.6 Ztráta zařízení nebo krádež

Hlavním strachem uživatelů je i ztráta či krádež samotného telefonu. K ochraně před krádeží či ztrátou je heslo či PIN kód, taky aby se cizí osoba do telefonu nemohla dostat a používat tak uživatelovu kartu k placení. Také se doporučuje mít NFC funkci u svého telefonu vypnutou a zapínat jen ve chvílích nutných pro použití.

Pokud má uživatel kartu uloženou na svém telefonu a ten ztratí nebo je mu odcizen banky doporučují okamžité blokace karty, tak aby žádné informace nemohly být zneužity.

4.3 České banky a NFC

Téměř všechny banky v ČR již podporují Google Pay či Apple Pay. Jedinou výjimkou je Sberbank, která platby pomocí NFC nepodporuje vůbec. V následující tabulce vidíme přehledně, které české banky podporují, jaké aplikace.

Banka	Google Pay	Apple Pay	Garmin Pay	Fitbit Pay
Air Bank	✓	✓	✓	✓
CREDITAS	✓	✓	✓	✗
Česká Spořitelna	✓	✓	✓	✓
ČSOB	✓	✓	✓	✗
Equa Bank	✓	✓	✗	✗
Fio Banka	✓	✓	✗	✗
Komerční Banka	✓	✓	✓	✓
mBank	✓	✓	✓	✓
MONETA Money Bank	✓	✓	✓	✓
Raiffeisenbank	✓	✓	✓	✓
Sberbank	✗	✗	✗	✗
Unicredit Bank	✓	✓	✗	✗

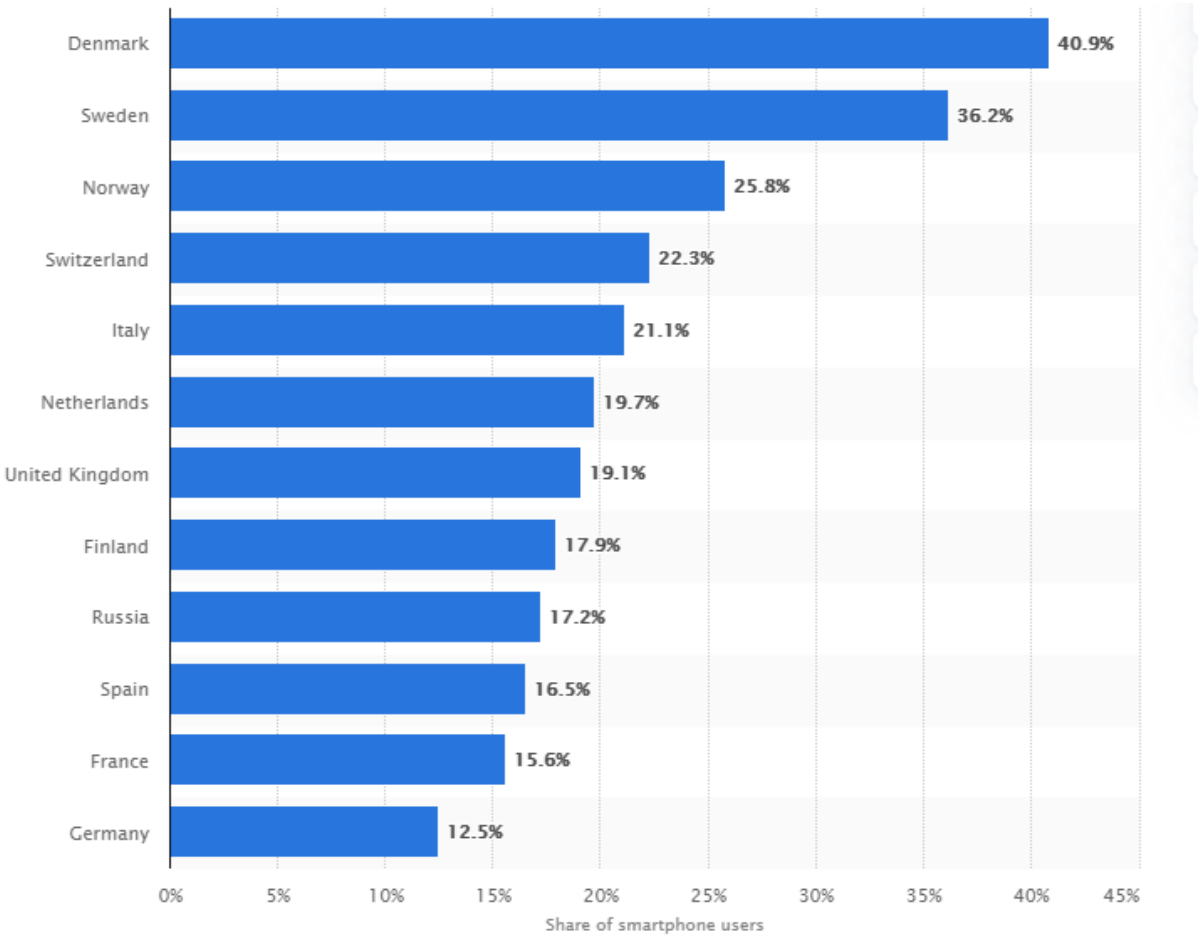
Tabulka 1: Podpora aplikací českými bankami

Zdroj: NFC platby mobilem (NÁVOD) (2020)

U uživatelů i v ČR popularita těchto plateb stále roste a je jen otázkou času, kdy pro každého Čecha bude NFC platba absolutním normálem. Dle tiskové zprávy z roku 2019 platilo pomocí mobilního zařízení více než 120 tisíc klientů České spořitelny. Obecně české banky uvádějí, že počet karet aktivovaných pro bezkontaktní placení chytrým telefonem či hodinkami je v současné době zhruba okolo 10-15 %. (Hrubý, 2019)

4.4 Využití mobilních plateb ve světě

V Číně je tento způsob platby již naprosto adaptován mezi uživateli a využívá ho téměř každý. V Evropě je používání smartphonů pro bezkontaktní platby nejvyšší v Dánsku a Švédsku, přičemž čtyři z deseti majitelů smartphonů provedli jednu takovou platbu za posledních šest měsíců (2019). Jaké je procentuální využití v jiných evropských zemích můžeme vidět na obr.7. (Statistica Research Department, 2021)



Obrázek 6: Graf využití mobilních plateb v Evropě

Zdroj: Statistica Research Department, 2021

5 Aplikace pro mobilní platby

Díky velkému potenciálu tohoto způsobu plateb je trh s mobilními aplikacemi určenými pro NFC platby opravdu široký a stále se rozrůstající. Tyto aplikace v základu dělíme na nebankovní a bankovní aplikace. V případě bankovních aplikacích se bavíme o aplikacích vydaných přímo konkrétní bankou. Nebankovní aplikace jsou vydané nezávislou třetí stranou.

Některé české banky vyžadují využívání jejich vlastní aplikace. Postupem času však tyto požadavky na vlastní aplikace upadají a banky se snaží přecházet na univerzální platformy. Nabízejí tak uživateli možnost volby. Některé banky mají své vlastní aplikace, které samy o sobě NFC platby nepodporují, ale v rámci balíčku funkcí integrují nebankovní aplikace.

Největší výhodou nebankovních aplikací je uložení více kreditních či debetních karet nezávisle na sobě, a to od jakékoliv banky. Při placení tak uživatel jednoduše vybere, kterou kartou chce zaplatit a aplikace se postará o zbytek.

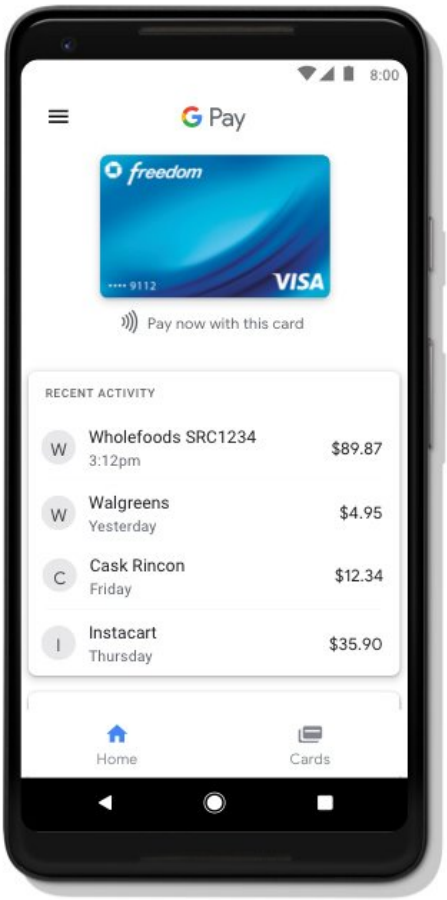
Dříve bylo nebankovních aplikací opravdu mnoho, ale trh se vyčistil a nyní jsou k dispozici dvě hlavní aplikace pro mobilní telefony, konkrétně Google Pay a Apple Pay. Ostatní aplikace, které se tváří jako mobilní peněženky již nemají vlastní podporu plateb, ale využívají tyto dvě aplikace. Uživatel se vždy musí překliknout do jedné z těchto aplikací, aby mohl provést NFC platbu. Výjimkou je Samsung Pay, který je exluzivně dostupný pouze pro uživatele mobilních telefonů značky Samsung, zároveň však zatím nemá podporu v ČR. Pokud jde o aplikace pro nositelnou elektroniku tak v České republice banky podporují pouze dvě – Garmin Pay a Fitbit Pay.

5.1 Nebankovní aplikace

5.1.1 Google Pay

Google Pay je mobilní peněženka a online platební systém vyvinutý společností Google, který umožňuje placení pomocí mobilních telefonů a tabletů se systémem Android (verze 5.0 a novější) nebo chytrých hodinek se systémem Wear OS pomocí bezkontaktního

NFC. Uživatelé ve Spojených státech a Indii mohou také používat zařízení s iOS, ale funkčnost je omezená. Kromě toho služba podporuje také jiné karty, jako jsou kupóny, palubní vstupenky, studentské průkazy, lístky na akce, lístky do kina, lístky na veřejnou dopravu, karty do obchodů a věrnostní karty. Uživatel má zároveň vše na jednom místě. Jak můžeme vidět z obrázku (Obr.7) uživatel má přehled o všech svých kreditních či debetních kartách a jejich historii.



Obrázek 7: Interface Google Pay

Zdroj: Google Play

Hlavní výhodou této aplikace je, že spojuje všechny druhy plateb do jedné. Uživatelé mohou platit pomocí NFC v obchodech, snadno platit v aplikacích pomocí dedikovaného tlačítka, na jakémkoliv webu a také v obchodě Google. Tato aplikace totiž vznikla spojením dvou separátních aplikací Android Pay (NFC platby) a Google Wallet (platby na internetu) na začátku roku 2018. Rebrandovaná služba poskytla nové API, které obchodníkům umožňuje přidat platební službu na weby, aplikace, Stripe, Braintree a Google Assistant.

Uživatelé mohou do služby přidávat platební karty některým ze čtyř způsobů: prostřednictvím platební karty uvedené na jejich účtech Google, pořízením fotografie karty, poskytnutím z aplikace vydavatele karty nebo ručním zadáním údajů o kartě.

Pokud jde o zabezpečení jedná se o aplikaci založenou na HCE technologii. Data proudí přímo do operačního systému a verifikace je prováděna až vzdáleně na serverech. Tato technologie je používána i samotnými bankami v jejich aplikacích. Pro banky je tato aplikace přitažlivější, protože využívá známou technologii a z principu nechává větší kontrolu nad platbou bankám.

Google Pay používá specifikaci tokenizace plateb EMV. Tato tokenizace udržuje informace o platbách zákazníka v soukromí, díky nahrazení čísla kreditní nebo debetní karty pomocí DPAN (Device Primary Account Number) a zároveň s tím vytváří

dynamický bezpečnostní kód pro každou transakci zvlášť. (EMV® Payment Tokenisation, n.d.)

Google myslí i na ztrátu telefonu a svým uživatelům doporučuje aplikaci Najdi moje zařízení. Díky této aplikaci může uživatel na dálku najít, uzamknout nebo vymazat celý telefon. Tyto funkce budou nejspíše implementovány do samotného Google Pay v následujících letech.

Aby mohli uživatelé platit v obchodech, podrží své zařízení Android na čtečce NFC neboli platebním terminálu. Uživatelé Androidu ověřují platbu odemknutím telefonu pomocí biometrie, vzoru nebo přístupového kódu, zatímco uživatelé systému Wear OS se ověřují otevřením aplikace před zaplacením.

Aplikace podporuje všechny hlavní výrobce karet například tedy Mastercard, Visa, American Express nebo Discover. V Německu je možné prostřednictvím Google Pay využívat i PayPal.

Do České republiky se tato aplikace dostala rok po jejím vydání, a to díky Air Bank (5.1.2019). Od této doby je tato aplikace na špičce žebříčku mobilních platebních aplikací v ČR.

5.1.2 Apple Pay

Apple Pay (Obr.8) je služba mobilních plateb a digitálních peněženek společnosti Apple Inc., která umožňuje uživatelům provádět platby osobně, v aplikacích pro iOS a na webu pomocí prohlížeče Safari. Je podporován na zařízeních iPhone, Apple Watch, iPad a Mac. Funguje u každého obchodníka, který přijímá bezkontaktní platby – nevyžaduje specifické platební terminály pro Apple Pay.

Na rozdíl od největšího konkurenta této aplikace, tedy Google Pay, Apple Pay využívá pro zabezpečení secure element. Výhodou tohoto řešení je teoreticky větší bezpečnost, neboť jsou citlivá data uložena na speciálním hardwarovém prvku. Problémem však je, že jde o uzavřený systém a jednotlivé banky tak musí s Applem úzce spolupracovat. Pro banky je tak složitější tuto službu zpřístupnit. Zároveň se kontrola nad celým procesem

transakce přesouvá spíše do rukou Applu. Ačkoli uživatelé dostávají okamžité oznámení o transakci, systém Apple Pay není nástrojem okamžité platby, protože převod prostředků mezi protistranami není okamžitý.

Stejně jako Google Pay používá i Apple Pay specifikaci tokenizace plateb EMV. (EMV® Payment Tokenisation, n.d.)

Uživatelé telefonů se ověřují pomocí Touch ID, Face ID nebo hesla, zatímco uživatelé Apple Watch se ověřují poklepáním na tlačítko na zařízení.

Novinkou této aplikace je funkce Apple Cash, která umožňuje převod peněz z jednoho uživatele na druhého prostřednictvím služby iMessage. Ve chvíli, kdy uživatel obdrží platbu, prostředky se mu automaticky uloží na jeho kartu a může je rovnou používat. Tato funkce je zatím dostupná pouze v USA.

Obrázek 8: Interface Apple Pay

Zdroj: Google Play

Do České republiky se Apple Pay dostalo o měsíc později než její největší konkurent (19.2.2019), ale za to rovnou s podporou 8 českých bank.

5.1.3 Samsung Pay

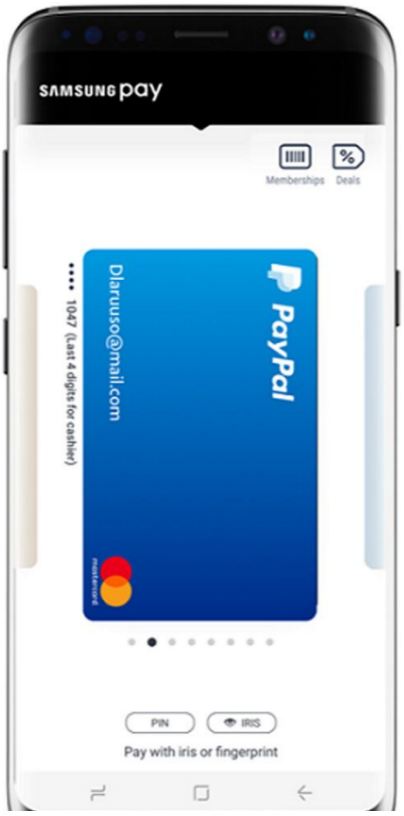
Samsung Pay (Obr.9) je služba mobilních plateb a digitálních peněženek od společnosti Samsung Electronics, která uživatelům umožňuje provádět platby pomocí kompatibilních telefonů a jiných zařízení vyrobených společností Samsung.

Tato služba podporuje jak mobilní platební systémy založené na NFC (které mají při detekci podpory přednost), tak i ty, které podporují pouze magnetické pruhy. Toho je dosaženo pomocí technologie známé jako magnetický zabezpečený přenos (MST), který emuluje pohyb permanentního magnetického pásu kolem čtečky přímým generováním magnetického průběhu blízkého pole. Tato aplikace je jedinou, která tento způsob platby

podporuje. V praxi je to však téměř irelevantní, protože téměř každý obchodník již vlastní platební terminál podporující NFC čipy.

V rámci zabezpečení Samsung spojil obě technologie dohromady. Respektive nabízí možnost pro banky si vybrat, kterou z technologií chtějí používat. Díky této kombinaci SE i HCE je tato aplikace velmi univerzální. Nevýhodou je, že je vázané na konkrétní přístroje značky Samsung, zatímco Google Pay funguje kdekoliv.

V České republice tato aplikace zatím nemá podporu.



Obrázek 9: Interface Samsung Pay

Zdroj: Google Play

5.1.4 Garmin Pay

Garmin Pay je systém bezkontaktních plateb, který je k dispozici ve vybraných hodinkách značky Garmin (Obr.10). Myšlenkou bylo zjednodušení plateb pro sportovce. Uživatel u sebe nemusí mít ani mobilní telefon.

Pokud jde o zabezpečení, tento systém funguje na technologii SE. Bylo by totiž obtížné mít hodinky připojené na internet.

Obrázek 10: Garmin Pay v hodinkách

Zdroj: https://explore.garmin.com/cs-CZ/garmin-pay/

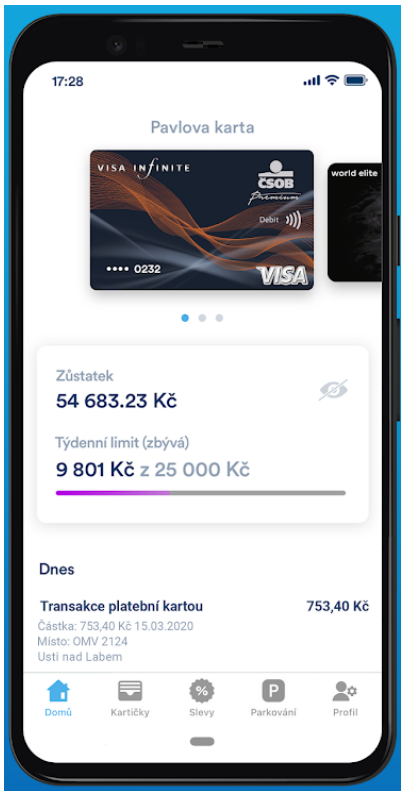
5.1.5 Fitbit Pay

Fitbit Pay funguje na stejném principu jako Garmin Pay ovšem podporuje zatím jen velmi malé množství zařízení. Konkrétně tři: Fitbit Charge 3, Versa a Ionic. Rozdílem je zabezpečení platby. Při nižších částkách stačí hodinky pouze přiložit a žádné další ověření není vyžadováno. Při platbách s vyššími částkami nebo platbami vyhodnocenými jako neobvyklé, je třeba potvrdit platbu na terminálu pomocí PIN kódu. Fitbit také vyžaduje zadávání PIN kódu do hodinek každých 24 hodin pro ověření, že s nimi chce platit oprávněný majitel.

5.2 Bankovní aplikace v ČR

5.2.1 DoKapsy – ČSOB

DoKapsy je mobilní aplikace banky ČSOB (Obr.11). Tato aplikace je na trhu nově od září roku 2020. Aplikace tak nahradila původní NaNákupy, která byla první bankovní aplikací v ČR. Tato aplikace mimo umožnění transakcí pomocí NFC také slučuje věrnostní karty a exkluzivní slevy do jedné aplikace. Myšlenkou za touto aplikací je možnost pro klienty vyrazit na nákupy pouze s telefonem v kapse.



Obrázek 11: Interface DoKapsy

Zdroj: Google Play

Aplikace využívá NFC s technologií HCE. Aplikace vyžaduje autorizaci při platbách nad 500 Kč pomocí hesla aplikace nebo otisku prstu. ČSOB na této aplikaci stále pracuje a slibuje mnohá rozšiřování. Například možnost placení parkování ve velkých městech nebo kupování lístků na MHD, a to vše v rámci jedné aplikace.

Uživatelé si mohou snadno zobrazit zůstatek na účtu i vyčerpání limitu. Velmi jednoduše mohou přidat i další karty a zobrazit si jejich historii plateb. V případě, že uživatelé nechtějí využívat tuto aplikaci pro placení pomocí NFC mohou svou kartu pomocí dedikovaného tlačítka přidat do Google Pay. Tyto dvě aplikace se pak propojí a zobrazují přehledy samostatně.

Aplikaci DoKapsy mohou využívat všichni uživatelé bez ohledu na to, u které banky mají účet. Zároveň je to jediná bankovní aplikace v ČR, která podporuje i systém iOS konkrétně 11 a vyšší.

5.2.2 RaiPay

RaiPay je bankovní aplikace banky Raiffeisenbank, která umožňuje platbu pomocí debetních a kreditních karet Mastercard vydané touto bankou (Obr.12). Tato aplikace byla vydaná v září roku 2019 a mohou ji využívat uživatelé mobilních telefonů s operačním systémem Android 6.0 a vyšší.

Uživatel této aplikace může vkládat více svých kreditních či debetních karet o každé z nich si zobrazovat jednotlivé přehledy.

Aplikace funguje pomocí technologie HCE, tudíž má nad všemi transakcemi banka plnou kontrolu. Při aktivaci aplikace, přidávání karet a přihlášení do aplikace je nutné datové nebo Wi-Fi připojení k internetu. Při placení nebo výběrech zařízení online být nemusí.

Uživatel si může nastavit různé úrovně zabezpečení. V každé úrovni je však nutné při platbě mít odemknutý telefon. Výchozí nastavení aplikace nevyžaduje žádné další ověření při platbě do 5 000 Kč. Při zvolení vyšší úrovně aplikace vyžaduje ověřování všech plateb nad 500 Kč heslem nebo otiskem prstu. Nejvyšší úrovní zabezpečení je ověřování každé platby nezávisle na tom, jak velká je, pomocí biometrie.

Obrázek 12: Interface RaiPay

Zdroj: Google Play

Prostřednictvím této aplikace mohou uživatelé vybírat z bankomatu. Místo vkládání fyzické karty do bankomatu, uživatel přiloží telefon zadní stranou ke čtečce bankomatu. Tento výběr hotovosti je možný pouze na bankomatech s bezkontaktními čtečkami. Všechny bankomaty Raiffeisenbank touto technologií disponují. Vklady zatím provádět nelze.

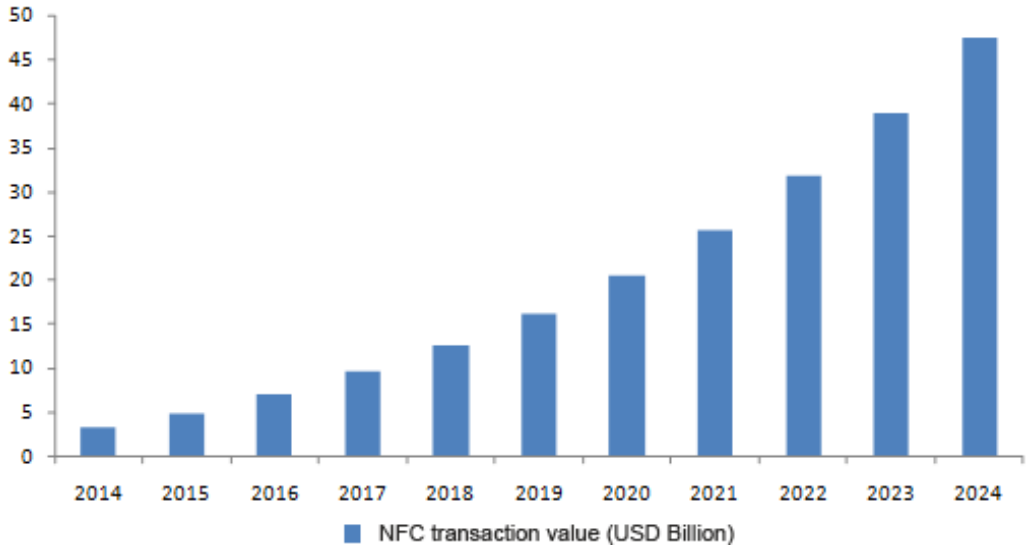
5.2.3 Poketka

Poketka je bankovní aplikace od České spořitelny, která se na venek tváří jako aplikace umožňující NFC platby, ale ve skutečnosti to tak není. Aplikace pouze propojuje Google Pay se zákaznickým servisem České spořitelny.

Dříve tato aplikace sloužila úplně stejně jako Google Pay, ale Česká spořitelna se rozhodla pro přechod na Google Pay a zaměření se spíše na výhody aplikace. Pokud klienti České spořitelny využívají tuto aplikaci získávají odměny. Jednou z nich je například CashBack. Poketka také nabízí uložení slevových karet a přehled o historii plateb.

6 NFC v současnosti

Technologie NFC má opravdu bohaté využití. Jako důkaz předkládám graf (Obr.13), kde je jasně vidět exponenciální růst celosvětového trhu s NFC technologiemi. Tento graf ukazuje minulost, současnost i předpověď tohoto trhu. Tento graf byl součástí studie z roku 2016, kdy byla hodnota tohoto trhu vyčíslena na 4,8 miliardy USD. Za pět let, tedy roku 2020, vystoupala tato hodnota na 18 miliard USD. Předpokládá se, že v roce 2025 bude hodnota tohoto trhu 34,9 miliardy USD. (NFC Market worth $34.9 billion by 2025, n.d.)



Obrázek 13: Graf velikost trhu NFC

Zdroj: Chang, H., 2017

Díky stále rostoucí popularitě mobilních zařízení a stále rostoucímu počtu zákazníků byl rozvoj technologie NFC rychlý. Počátek datujeme právě do roku 2014, kdy byla uvedena první možnost platby pomocí NFC, a to díky společnosti Apple. To mělo za následek rozšíření NFC do dalších technologií jako například IoT. Pro větší představu uvádím několik příkladů využití NFC v běžném životě.

6.1 Internet věcí

Internet věcí slibuje svět, ve kterém jsou fyzické předměty všeho druhu – od domácích systémů až po monitory zdraví – schopné shromažďovat a vyměňovat si data. Jedná se o atraktivní vyhlídku, která umožňuje pozoruhodnou efektivitu a produktivitu, menší návratnost dat, snazší kontrolu a mnoho výhod spojených s analytikou dat.

Díky přímému mechanismu klepnutí a spuštění umožňuje NFC snadné a intuitivní připojení dvou různých zařízení IoT. Vzhledem k tomu, že čipy NFC musí být k zahájení transakce v těsné blízkosti, je NFC jasným znamením, že uživatel má v úmyslu provést určitou akci. Krátký dosah NFC také chrání před neoprávněným přístupem hackerů.

Konkrétní příkladem může být použití NFC jako náhradu za hotelové karty. Uživatel si stáhne rezervaci do mobilní aplikace a čip NFC v telefonu se stane klíčem, který mu odemkne dveře. Technologii NFC lze navíc integrovat naprosto všude, kde je potřeba levných elektronických štítků bez baterií – vstupenky na akce, štítky pro divokou zvěř atd.

6.2 Průmysl 4.0

Průmysl 4.0 začalo v roce 2016 německou vládou. Hlavním účelem je optimalizovat zdroje a současně zlepšit výkon továrny, což vede ke snížení výrobních nákladů. Průmysl 4.0 byl umožněn zejména díky technickému pokroku v oblastech souvisejících s umělou inteligencí, počítačovými a komunikačními technologiemi.

Schopnost značek NFC pojmout až 1 MB rekonfigurovatelných dat slouží průmyslu 4.0 tím, že umožní ukládání informací, jako je stav zpracování a pokyny k dalším krokům ve výrobním procesu. Dále také umožňuje zaměstnancům vybavených NFC enabled tablety zobrazovat stav konkrétních objektů v reálném čase. Blízkost, která je vyžadovaná pro komunikaci, zvyšuje zabezpečení systému a snižuje pravděpodobnost odposlechu.

NFC tagy jsou používány nejen pro identifikaci jedince při vstupu do továrny, ale také pro identifikaci jednotlivých komponentů. To zajišťuje, že roboti používají vždy správný komponent pro jejich zadaný úkol.

6.3 Mobilní peněženka

NFC tagy nalézají v odvětví financí největší budoucnost. Uživateli totiž přináší možnost platby telefonem velké pohodlí.

6.4 Nositelná technologie

Jak již název napovídá, nositelnou technologií nazveme cokoliv, co můžeme nosit na sobě. Ať už to jsou hodinky, náramky, prsteny nebo implantované čipy, které jsou trendem poslední doby. Díky implementaci NFC tagů můžou být tyto doplňky využívané

místo kreditní karty nebo vizitky. Nositelná technologie ve spojení s IoT otevírá uživateli úplně nový svět. Uživatel může například odemykat svůj byt pouze přiložením ruky.

6.4.1 Chytré hodinky

Chytré hodinky se staly součástí životů mnohých uživatelů a s nimi přišla i možnost NFC plateb pomocí nich. Uživatel jednoduše nahraje kartu do svých hodinek a pak ji může libovolně používat. Ověřování u některých hodinek probíhá pomocí otisku prstu, u jiných je pak nastaven pevný limit.

6.4.2 Náramky

V oblasti náramků si uživatelé mohou vybírat mezi chytrými fitness náramky a jednoduchými náramky pouze s NFC. V případě fitness náramků se nabízí možnost platby stejně jako u chytrých hodinek. V druhém případě jednoduchých náramků se pak NFC využívá například k otevření zámku od bytu.

6.4.3 Prsteny

Prsteny s NFC se využívají podobně jako jednoduché náramky s NFC. Velké využití mají například při předávání osobních informací, které může uživatel jednoduše poklepnutím odeslat na zařízení druhého uživatele. Může sloužit také jako klíč k chytrým zámkům. Vyrábí se ve všech možných variantách a velikostech, takže si vybere každý.

6.4.4 Implantovaný čip

Novinkou, ale také dle předpokladů budoucností technologie NFC, je implantovaný čip s NFC přímo pod kůži uživatele, a to konkrétně do ruky (Obr. 14). Tento čip toho zatím tolik neumí a našel využití jen u opravdových technologických nadšenců, ale v budoucnosti si dokážeme představit takový čip v ruce každého uživatele. Tento čip si každý může pořídit za 69 USD. Přijde v balíčku i s nástroji pro implantaci. Tu si může uživatel provést sám v pohodlí domova. Zatím čip umí jen základní funkce jako je ukládání informací a odemykání zámků.

Obrázek 14: Implantovaný čip v ruce

Zdroj: Maxwell, 2014

6.5 Zdravotnictví

NFC tagy jsou velmi užitečné v nemocničních zařízeních ke sledování materiálů a zdrojů. Posilují tak bezpečnost celého zařízení, které je velmi zranitelné vůči mnohým bezpečnostním hrozbám (například krádeže léků). NFC tagy slouží také ke kontrole přístupu zaměstnanců a pacientů.

Technologie NFC může pomáhat pečovatelům a ošetřovatelům spojit se navzájem pomocí bezdrátových pásem pro sledování dat, která monitorují životní funkce pacienta a odesílají všechna relevantní data lékaři. Domácí zdravotní péče je oblastí, kde NFC může hrát důležitou podpůrnou roli u řady řešení a produktů zdravotní péče.

Žhavou novinkou je využívání NFC tagů přímo na balení léků. Pacient či doktor snadno získá data o daném léku, zejména se jedná o datum spotřeby nebo správné dávkování léku.

7 Budoucnost NFC

Technologie NFC je stále na svém počátku a do budoucna můžeme očekávat opravdu velký rozvoj. Se zvyšujícím se povědomím o technologii a rostoucí základnou telefonů schopných ji nativně číst, tyto možnosti rostou každým dnem. Vzhledem k širokému používání plateb NFC jsou nyní zákazníci obecně spokojeni s používáním NFC a chtějí ho používat.

Pokud jde o Českou republiku a bezkontaktní platby pomocí NFC tak i u nás popularita každým rokem roste. To, co se však dá očekávat, je kompletní vymizení bankovních aplikací. Pro banky je totiž mnohem jednodušší propojit svou aplikaci, která nabízí různé výhody a přehledy, s bezpečným a stále aktualizovaným Google Pay. Konkrétním příkladem je Poketka od České Spořitelny. Zároveň se rozšíří infrastruktura bezkontaktních bankomatů. Již polovina bankomatů v České republice vydá klientovi hotovost pouze po přiložení telefonu či karty k NFC čtečce.

Vzhledem k tomu, jak je jednoduché tuto technologii používat, očekává se růst využívání ve všech oblastech. Za několik let nás čeká svět, kde bude NFC normální součástí našeho života. Uživatelé budou seznámeni s myšlenkou přikládání telefonu k tagům pro získání více informací a vyměňování dat. V budoucnu bude naprosto normální platit účty prostřednictvím této technologie. (Chang, 2017)

Velmi zajímavá je také budoucnost NFC v oblasti marketingu. Ve světě je standardem využívání NFC plakátů, kdy uživatel přiloží svůj telefon pro získání více informací. V budoucnu by mohly firmy umístit NFC tagy do vchodů svých obchodů tak, aby se uživatelé mohli automaticky ohlásit na sociálních sítích. Hlavní myšlenkou je dostat více informací o firmě ke svým zákazníkům.

Potenciál ve vývoji je možné vidět i v oblasti přístupu do budov. Ať už jde o zaměstnance či studenty v některých firmách či školách je využívání aplikace místo fyzické karty již standardem. Příkladem může být univerzita v San Franciscu, která využívá systém One Card. Pomocí tohoto systému se student dostane do školy, na koleje, a dokonce je schopen i zaplatit v menze. V ČR se bohužel s tímto způsobem využití zatím nemůžeme setkat. (Sacco, 2012)

Do této technologie je vkládána velká víra a je očekáváno, že jednoho dne člověk vyjde ven z domu bez své peněženky a vše za něj bude spravovat jeho telefon. Otázkou pro

mnohé uživatele však stále zůstává bezpečnost. Bezpečnost mobilních telefonů bude stále růst a s ní i tato skvělá technologie. Jde jen o to probudit v uživatelích důvěru. Technologie NFC totiž opravdu usnadňuje životy vzhledem k dnešní době, kdy telefon má u sebe každý téměř vždy, ale například peněženku lze zapomenout snadno.

8 Vývoj mobilní aplikace

Cílem této části bakalářské práce je vyvinout mobilní aplikaci pomocí frameworku Xamarin pro mobilní operační systém Android. Tato aplikace bude demonstrovat propojení fyzického adaptéru NFC a kódu. Aplikace bude velmi jednoduchá pouze s jednou hlavní stránkou, kde budou tlačítka pro jednotlivé funkce aplikace. Původní funkce aplikace mělo být přeposílání zpráv mezi dvěma zařízeními, ale tato funkčnost NFC v mobilních telefonech byla v předchozím Androidu 10 odstraněna. Jako důvod Google uvedl, že je mnohem jednodušší posílat jednoduché zprávy pomocí Bluetooth nebo Wi-Fi. Bylo tedy nutné vymyslet alternativu. Po dohodě s vedoucím této práce bude konečná aplikace sloužit pro čtení a zápis na NFC tagy. Aplikace bude umět přečíst jakýkoliv štítek a zapsat na něj jednoduchý text nebo URL. Při přečtení URL by měla aplikace otevřít prohlížeč s danou URL stránkou.

8.1 Výběr programovacího jazyka

Celá aplikace bude napsána pomocí frameworku Xamarin. Xamarin je open-source platforma od společnosti Microsoft pro vytváření aplikací pro iOS a Android pomocí C# a .NET. Tento framework nabízí dvě možnosti, jak aplikace psát. Programátor si může vybrat mezi verzí pouze pro jeden operační systém (Xamarin.Native) nebo pro oba (Xamarin.Forms).

Xamarin.Native (v našem případě Xamarin.Android) je původní forma frameworku Xamarin. Tento způsob lze použít pouze v případě vývoje aplikace pouze na jeden operační systém. Vzhledem k tomu, že je aplikace vyvíjena přímo pro konkrétní OS, nabízí více funkcionalit spojených s daným OS. Pro zápis uživatelského rozhraní používá formát XML.

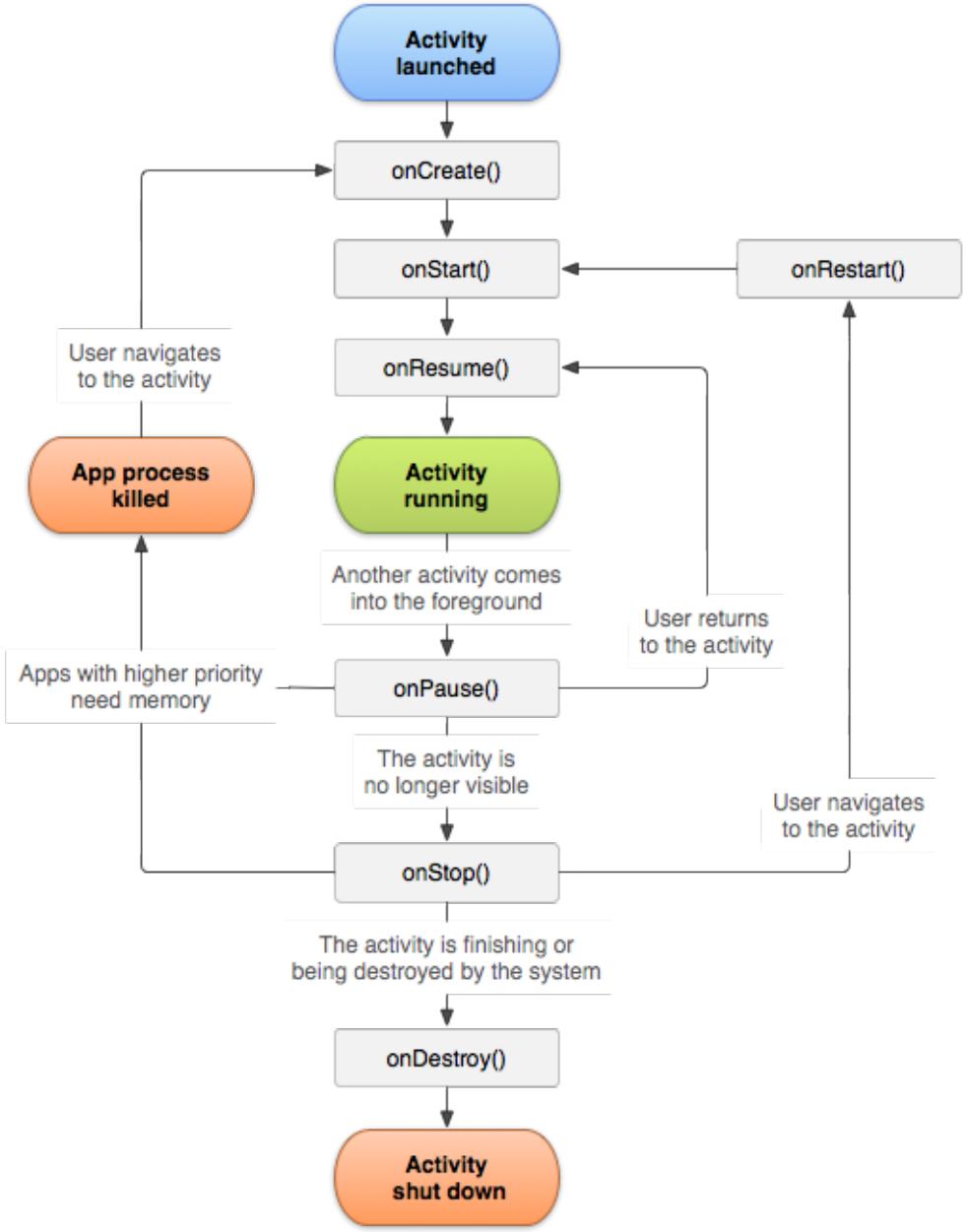
Xamarin.Forms je pokročilá verze Xamarin Native, která umožňuje zápis jednoho XAML pro cílení na více systémů najednou. Celý kód je napsán v C# a uživatelské rozhraní se definuje buď přímo v kódu nebo pomocí XAML, takže jej lze sdílet mezi všemi platformami. Zdrojový soubor Xamarin.Forms vždy obsahuje jednotlivé kódy Xamarin.Native, které jsou zpravidla prázdné a je v nich jen jedna funkce pro inicializaci C# kódu.

Vzhledem k tomu, že má aplikace má být vyvíjena pouze pro Android, zvolila jsem Xamarin.Android ze dvou důvodů. V první řadě je mi otevřeno mnohem více

funkcionalit, pomocí kterých mohu přistupovat k NFC. Každý OS má totiž odlišný přístup k NFC adaptéru. Další výhodou je jednodušší sestavování samotného kódu. V případě Xamarin.Forms musí být sestaveny dva separátní kódy. Časově je to tedy dvakrát náročnější a vzhledem k tomu, že po každém sestavení musí být aplikace nainstalována na mobilní zařízení pro kontrolu chyb (emulátor nepodporuje NFC), byla volba jasná.

8.2 Životní cyklus mobilní aplikace

Ještě předtím, než začnu popisovat samotný vývoj mé aplikace, je nutné si představit životní cyklus mobilní aplikace pro Android. Aplikace se skládá z jednotlivých aktivit, pro zjednodušení si můžeme představit, že jedna aktivita je rovna jedné straně v aplikaci. Každá aktivita se skládá ze sedmi metod, které jsou postupně volány (Obr.15). Tyto metody mohou být přepsány vývojářem.



Obrázek 15: Životní cyklus aplikace

Zdroj: Android Developers, n.d.

Nejdůležitější z těchto metod je onCreate(). Tato metoda je volána pokaždé, když je aktivita poprvé vytvořena. V této metodě se tedy iniciuje uživatelské rozhraní a přiřazují se jednotlivé proměnné.

Metoda onStart() je volána ve chvíli, kdy se aktivita zapne a je zobrazena uživateli. V této metodě se obvykle nachází různé kontroly. V našem případě budeme tuto metodu používat pro kontrolu, zda je NFC přítomné v telefonu.

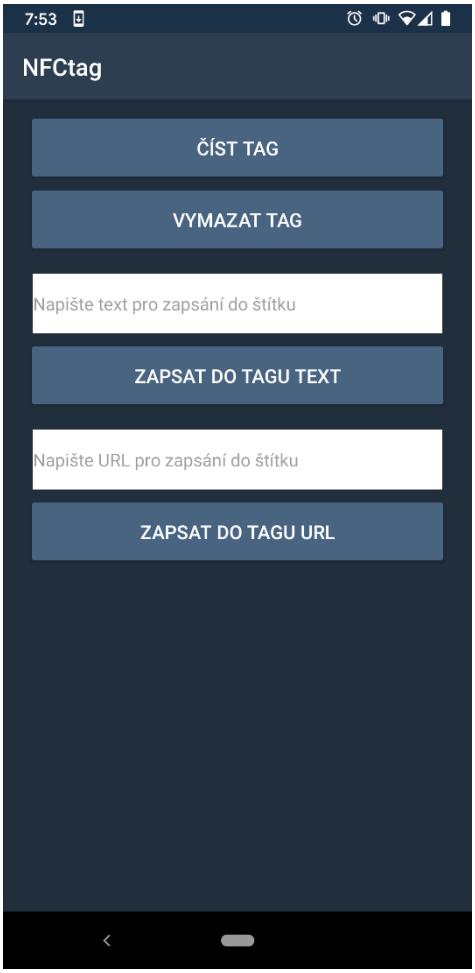
Ve chvíli, kdy uživatel začne komunikovat s aplikací, je volána metoda onResume(). Tato metoda se stará o veškerý vstup od uživatele a může být použita i pro nastavení priorit. V mém případě tuto metodu využiji pro definici záměrů a jejich filtrů. Záměr je abstraktní popis operace, která má být provedena a označujeme jí jako intent. (Android Developers, n.d.)

Další tři metody už nejsou pro naši aplikaci tak důležité. Metoda onPause() je volána, když aktivita běží na pozadí a ještě nebyla ukončena. Ve chvíli, kdy je aktivita ukončena, je volána metoda onStop(). Pokud se uživatel vrátí zpět k přechozí aktivitě je volána metoda onRestart(). Poslední metoda je onDestroy(), která je volána jako poslední předtím než je aplikace zcela ukončena.

Do tohoto životního cyklu patří i další metody, které budeme ve vývoji využívat. Tyto metody budou vysvětleny a popsány na konkrétních případech.

8.3 Uživatelské rozhraní

V první fázi vývoje je nutné definovat všechny funkce aplikace a přizpůsobit jim uživatelské rozhraní, tedy to, co uživatel uvidí při spuštění aplikace. V tomto případě je to několik tlačítek s jednotlivými funkcemi a dvě okénka pro zadání textu. Uživatelské rozhraní se kóduje pomocí XML. Výsledné rozhraní aplikace je zobrazeno na obrázku č.16. Skládá se tedy ze čtyřech tlačítek s funkcemi a dvěma okny pro zadání textu pro zapsání. Všechna tyto tlačítka jsou stejná, a tak není nutné popisovat každé zvlášť.



Obrázek 16: Uživatelské rozhraní aplikace

Zdroj: Autor práce

```
<LinearLayout
    xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:app="http://schemas.android.com/apk/res-auto"
    xmlns:tools="http://schemas.android.com/tools"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    android:orientation="vertical"
    android:paddingRight="20dp"
    android:paddingLeft="20dp"
    android:paddingTop="10dp"
    android:background="#212e3b">
```

Zdrojový kód 1: Základní uživatelské rozhraní

Na začátku kódu XML je nutné vybrat, který z předem definovaných layoutů chceme pro aplikaci použít. V případě této aplikace byla volba jasná pro LinearLayout. Tento layout slouží pro zobrazování jednotlivých prvků v lineárním směru. Níže v kódu je naprogramován lineární směr vertikální. Také je zde zakódováno ohraničení neboli padding. Všechna xmlns jsou v kódu automaticky a nebylo do nich zasahováno.

```
    <Button
        android:text="Číst tag"
        android:layout_width="match_parent"
        android:layout_height="wrap_content"
        android:minHeight="60dp"
        android:id="@+id/ReadTagButton"
        android:backgroundTint="#486480"
        android:textColor="#ffffffff"
        android:textSize="16dp"
        tools:ignore="HardcodedText" />
```

Zdrojový kód 2: Tlačítko

Ve zdrojovém kódu 2 výše je kódování prvního tlačítka s nápisem Číst tag. Nejdůležitější součástí je přiřazení id, díky kterému může být tlačítko programováno. Toto ID je při kompilaci automaticky vytvořeno v Resource.designer.cs, kde jsou uložena všechna ID v rámci aplikace. Resource.designer.cs obsahuje přiřazené jedinečné ID každému prostředku aplikace a stará se i o jejich udržování. Každému prostředku je tedy automaticky přiřazen 32bitový jedinečný integer, díky kterému aplikace pozná, o jaký prostředek se jedná.

Ostatní části kódu se starají pouze o vzhled tlačítka. Pro zjednodušení struktury kódu jsem zvolila pevně zakódované popisy na každém z tlačítek. Proto přes tools je toto upozornění ignorováno. Pro správné umístění tlačítka slouží layout_width a layout_height. Pomocí match_parent zajišťuji, aby bylo tlačítko stejně velké jako okno aplikace. Wrap_content

se stará, aby tlačítko bylo jen tak veliké, jak je potřeba. Bylo nutné nastavit i nejmenší výšku minHeight na 60 dp. Android dává přednost udávání jednotek výšky právě v dp místo pixelů. Virtuální jednotka měření dp slouží jako pixel nezávislý na hustotě. Pomocí této jednotky vypadá aplikace na každém zařízení správně, protože se automaticky převádí na dané pixely pomocí dpi zařízení. Pokud bychom pevně kódovali v pixelech mohla by aplikace na menších rozlišení vypadat jinak. Součástí tohoto kódu je i určení velikosti a barvy písma.

```
<EditText
    android:id="@+id/editText"
    android:layout_width="match_parent"
    android:layout_height="50dp"
    android:textSize="15dp"
    android:layout_marginTop="10dp"
    android:layout_margin="5dp"
    android:hint="Napište text pro zapsání do štítku"
    android:inputType="text"
    android:background="@android:color/white"
    tools:ignore="HardcodedText" />
```

Zdrojový kód 3: EditText

Kromě tlačítek je v rozhraní aplikace i okénko pro psaní textu. K tomu se používá prostředek EditText. Stejně jako u tlačítka je zde vytvoření id, aby text z něj mohl být předáván aplikaci v kódu. Vždy je nutné mít definované jaký typ vstupu bude vkládán. V našem případě máme tyto okna dvě. V prvním případě, jak můžeme vidět ve zdrojovém kódu 3, je prvním z nich inputType text. V druhém případě však uživatel vkládá vždy URL, a proto je také definován inputType textURI. Tato definice vstupu zajišťuje správnou manipulaci s daty uvnitř aplikace. Uvnitř tohoto okna je pevně zakódován text přes hint, aby uživatel poznal, co do příslušného okna napsat. Ostatní části jsou stejné jako u tlačítka a již byly popsány výše.

```
private Button readTagButton;
readTagButton = FindViewById<Button>(Resource.Id.ReadTagButton);
readTagButton.Click += ReadTagButton_Click;
```

Zdrojový kód 4: Inicializace uživatelského rozhraní v kódu

Uživatelské rozhraní je pak v kódu voláno pomocí již zmiňovaných id. Jak inicializace vypadá je ukázáno ve zdrojovém kódu 4. Pomocí FindViewById se spojí tlačítko v kódu a fyzické tlačítko v rozhraní uživatele. Po spojení těchto prostředků je možné přiřadit na stisk tlačítka metodu, tak jak je napsáno na řádku tři. Stejně to funguje u všech

komponentů z uživatelského rozhraní. Každé z nich je inicializováno na začátku kódu aplikace a je s ním pak pracováno samostatně.

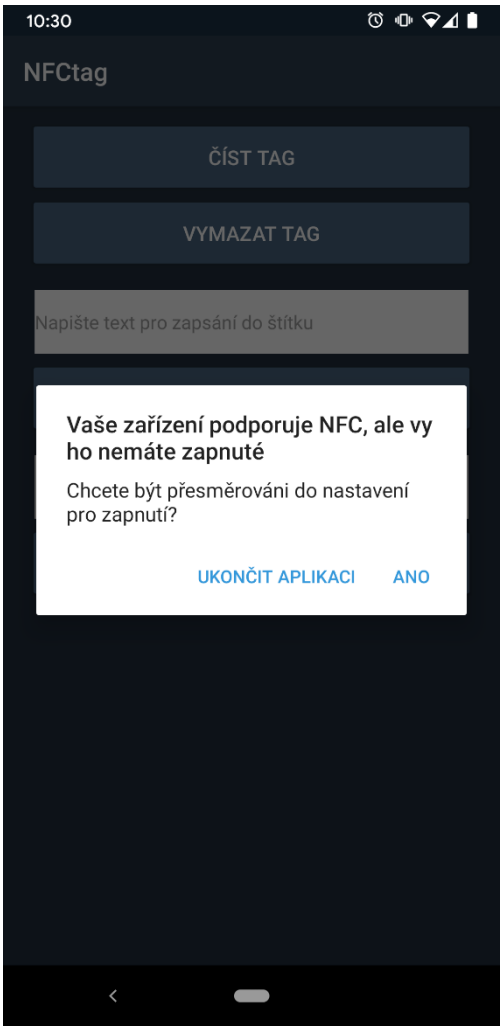
8.4 Funkce aplikace

Tato aplikace je vyřešená pomocí metod životního cyklu a podmínek v nich. V následujících řádkách popisuji, jak celá aplikace funguje obecně, později zacházím více do hloubky i s ukázkami zdrojového kódu.

Při spuštění aplikace na pozadí aplikace zjistí, zda je v telefonu NFC čip. Nastávají tak tři možnosti výstupu:

- NFC čip v telefonu není
- NFC čip v telefonu je, ale není zapnut
- NFC čip v telefonu je a je zapnut

Dle těchto výstupů aplikace buď zobrazí alert box nebo v případě, že je vše v pořádku neprovádí pro uživatele nic. V druhém případě, kdy NFC čip v telefonu je, ale není zapnut se zobrazí alertbox s výběrem možností (Obr.17). Tento alertbox dává uživateli dvě možnosti – aplikaci ukončit nebo se nechat přesměrovat přímo do nastavení telefonu a čip zapnout.



Obrázek 17: Alert box

Zdroj: Autor práce

Ve chvíli, kdy je NFC zapnuto aplikace je připravena pro další pokyny od uživatele. Uživatel může využít čtyři funkcionality této aplikace:

- Přečíst tag
- Vymazat tag
- Zapsat text do štítku
- Zapsat URL do štítku

Ve všech funkcionalitách je v rámci kódu určitá podobnost, ale pro uživatele aplikace dělá velmi odlišné věci. Při kliknutí na jakékoliv tlačítko se zobrazí alertbox s dalšími pokyny. Zpravidla jsou tyto alertboxy dva. Jeden udává pokyn k přiložení k NFC tagu a druhý upozorňuje na to, že okno pro vkládání nebylo vyplněno. Po úspěšném

provedení jakékoliv operace je uživateli zobrazen informační alertbox s popisem provedené akce.

Při zápisu na tag mohou nastat určité problémy například v rámci špatného formátování štítku nebo nedostatečného místa pro zapsaní. Aplikace tyto případy před zápisem kontroluje a pokud některý z nich nastane informuje uživatele pomocí alertboxu.

8.5 Kódování aplikace

Uživatelské rozhraní je v této fázi již vytvořeno a můžeme s ním pracovat. Druhá fáze vývoje je samotné programování celé aplikace. Aby tato aplikace mohla spolupracovat s NFC čipem uvnitř telefonu je nutné povolit aplikaci oprávnění. To se provádí v manifestu pro Android. Tento soubor manifestu popisuje základní informace o aplikace pro nástroje Android Build, operační systém Android a v neposlední řadě také Google Play. Pokud nejsou oprávnění správně nastavena, Android přístup k NFC zablokuje – v našem případě se aplikace není schopná na zařízení ani spustit.

K NFC se dostaneme pomocí Androidem předem definovaného jmenného prostoru Android.Nfc. Díky tomu je nám poskytnut přístup ke všem funkcím NFC, včetně čtení NDEF zpráv ve značkách NFC.

Na začátku je nutné definovat proměnné, které budeme využívat v průběhu celého kódu. Jedná se zejména o jednotlivá tlačítka, alerboxy, ale také NFC (Zdrojový kód 5). Proměnná NfcAdapter bude sloužit pro získání informací o fyzickém čipu v telefonu. Ostatní proměnné v tomto kódu slouží pro vytvoření NDEF zpráv ve správném formátu. Slouží jako identifikátory NDEF zpráv, aby příjemce věděl, z jaké aplikace bylo na štítek zapsáno.

```
private NfcAdapter nfcadapter;
public const string DataMimeType = "application/xamarin.nfctag";
public static readonly string NfcAppRecord = "xamarin.nfctag";
public static readonly string Tag = "nfcreaderwriter";
```

Zdrojový kód 5: Proměnné NFC

8.5.1 OnCreate

První metodou, která je třeba upravit je metoda OnCreate, která se volá vždy při vytvoření aktivity. V této metodě se inicializuje uživatelské rozhraní (Zdrojový kód 4). Zároveň také definuje, co se stane, když je na jednotlivá tlačítka kliknuto. Pro příklad vezmeme

tlačítko pro čtení štítku. Po kliknutí na tlačítko se spustí metoda. V našem případě metoda ReadTagButton_Click (Zdrojový kód 6). Pomocí této metody je uživateli zobrazen alertbox s pokyny.

```
private void ReadTagButton_Click(object sender, EventArgs e)
    {
        DisplayAlert("Přiložte telefon ke štítku");
        WriteMode = false;
        EraseMode = false;
        WriteUrlMode = false;
    }
```

Zdrojový kód 6: Kliknutí tlačítka

V této metodě jsou definované jednotlivé případy. Vzhledem k tomu, že je aplikace řešená pomocí intentů přiřazujeme v těchto metodách pouze jednotlivým proměnným boolean. Jak můžeme vidět v případě čtení štítku všem módům nastavujeme false. S těmito informacemi si aplikace dále poradí v metodě OnNewIntent.

8.5.2 OnStart

Tato metoda se volá vždy, když se aplikace zapne. Využíváme ji proto pro kontrolu NFC čipu. Tato kontrola funguje na základě podmínek. Na začátku je nutné přiřadit proměnné NfcAdapter fyzický adaptér z telefonu. To se dělá pomocí metody GetDefaultAdapter, která nám je zpřístupněna díky Android.Nfc.

Po přiřazení adaptéru již řešíme jen podmínky. Pokud je přiřazená hodnota nulová aplikace zobrazí uživateli informaci o absenci NFC čipu v jeho telefonu a nabídne uživateli ukončení aplikace. V druhém případě, kdy je přiřazen adaptér, kontrolujeme, zda je zapnut. V tomto případě se zobrazuje alertbox z obr.17. V posledním případě je vše v pořádku, a tak se nezobrazuje ani neprovádí nic.

8.5.3 OnResume

Dostáváme se k jádru celé aplikace. V této metodě nastavujeme jednotlivé události a filtry pro spuštění nejdůležitější metody OnNewIntent.

```
var tagDetected = new IntentFilter(NfcAdapter.ActionTagDiscovered);
var ndefDetected = new IntentFilter(NfcAdapter.ActionNdefDiscovered);
var techDetected = new IntentFilter(NfcAdapter.ActionTechDiscovered);
var filters = new[] { ndefDetected, tagDetected, techDetected };

var intent = new Intent(this,
            GetType()).AddFlags(ActivityFlags.SingleTop);
var pendingIntent = PendingIntent.GetActivity(this, 0, intent, 0);

nfcadapter.EnableForegroundDispatch(this, pendingIntent, filters, null);
```

Zdrojový kód 7: Metoda OnResume

Celý tento proces zobrazuje zdrojový kód 7. Na začátku nastavujeme všechny události, které mohou začít jednotlivé akce. Konkrétně tedy detekování štítku, detekování NDEF zprávy a pro jistotu i pokud je detekován tag s různými technologiemi. Tyto události pak vkládám do pole filtrů, aby nemusely být vkládány po jednom.

Jako poslední krok je nutné nastavit prioritu NFC nad všemi ostatními aktivitami. O to se stará poslední řádek.

8.5.4 OnNewIntent

V tuto chvíli je aplikace připravena na všechny pokyny. Přesouváme se proto do metody OnNewIntent, která je volána pomocí předchozího kódu. To znamená v případě, že je detekován NFC štítek nebo NDEF zpráva.

V kódu máme tři proměnné, které se starají o správný chod této metody. V těchto proměnných je uložený bool předávající informaci o tom, který z módů má být zapnut – zapisovací nebo mazací. Tyto proměnné jsou WriteMode, EraseMode, WriteUrlMode. Jejich hodnota je měněna po stisknutí tlačítka (Zdrojový kód 6).

Aplikace pomocí podmínek zjistí, který z módu je zapnut a dle toho se zachová. Pokud není zapnut ani jeden z módů spustí se mód čtecí (vzhledem k tomu, že je posledním není nutné pro něj udržovat proměnnou). Jak aplikace s podmínkami pracuje ukazuje diagram 1.

```
string inputText = GetText();
if (inputText.Length == 0)
    return;
var payload = Encoding.UTF8.GetBytes(inputText);
var mimeBytes = Encoding.UTF8.GetBytes(DataMimeType);
var ndefRecord = new NdefRecord(NdefRecord.TnfMimeMedia, mimeBytes,
                 new byte[0], payload);
var ndefMessage = new NdefMessage(new[] { ndefRecord });
```

Zdrojový kód 8: Tvorba payloadu zapisovacího módu

Nejdůležitější částí tohoto kódu je vytvoření samotného payloadu, který je poté odesílán na tag. Pomocí metody GetText() jsou přenesena data z okna pro vkládání textu od uživatele. Všechna data musí být zakódován pomocí UTF-8. Takto zakódujeme samotný payload obsahující text, ale také hlavičku. Poté vytváříme jeden NDEF záznam, který obsahuje typ záznamu, označení aplikace a payload. Tento záznam je poté uložen do NDEF zprávy, která je připravena k odeslání na tag.

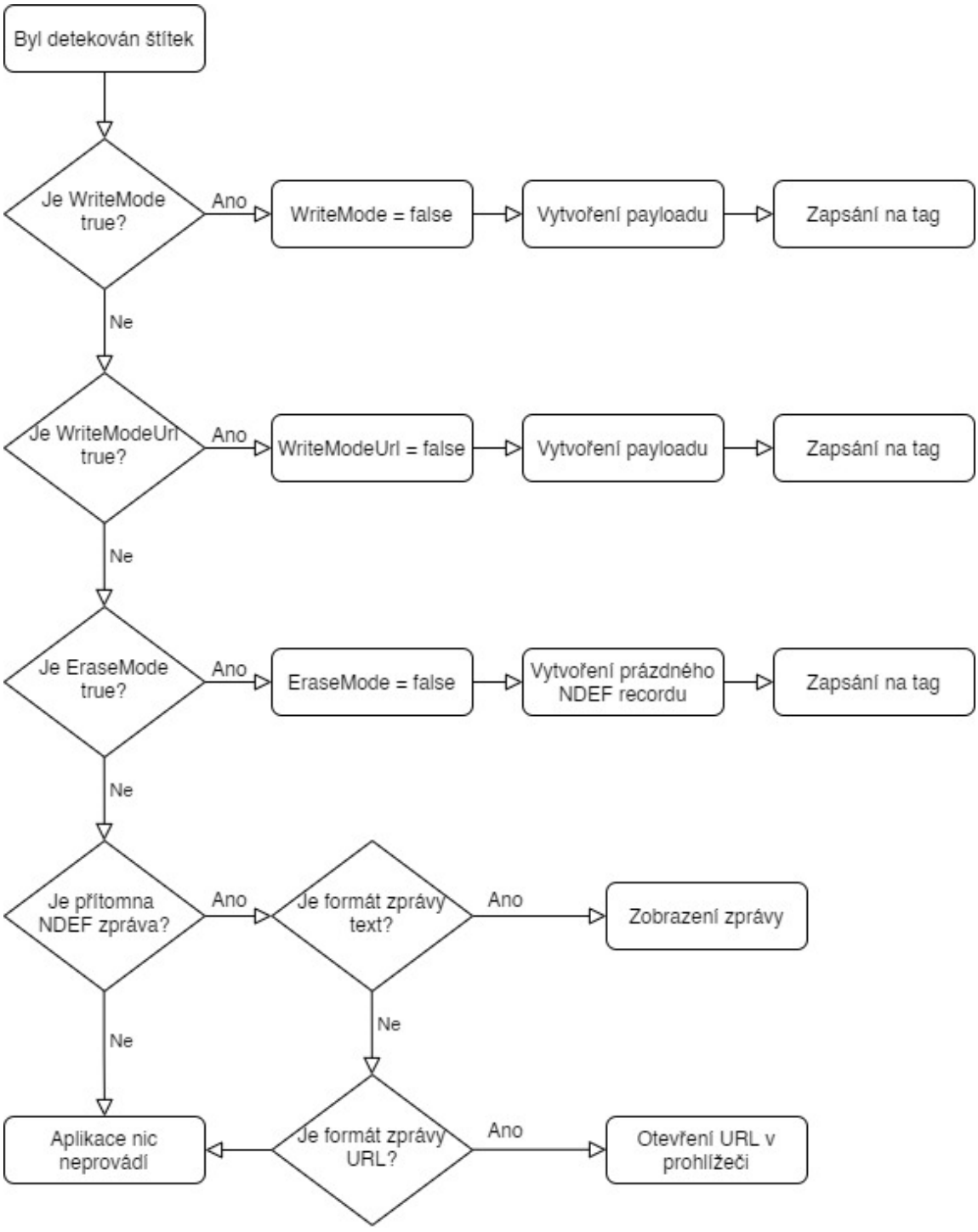


Diagram 1: OnNewIntent

Zdroj: Autor práce

Po takto připravené NDEF zprávě je nutno ji odeslat. K tomu slouží metoda WriteToTag(). V této metodě nejprve získáváme informace o tagu. Je nutné znovu zkontrolovat, zda je štítek přítomný. Pokud přítomný je může se zařízení na tento tag připojit. A přichází série kontrol, aby vše proběhlo hladce. Nejprve aplikace kontroluje, jestli není štítek pouze ve čtecím módu, v takovém to případě nemůže na tag zapisovat a

zobrazí uživateli chybovou hlášku. Dále kontroluje velikost zprávy. Dle typu tagu je také jeho kapacita, a tedy z ní vyplývá i maximální velikost zprávy. V případě, že je zpráva moc velká, vyhodí chybovou hlášku. Pokud všechny tyto kontroly projdou, aplikace zapíše NDEF zprávu na tag a zobrazí uživateli, že byla zpráva úspěšně zapsána.

Při zapisování URL se postupuje téměř identicky. Jen je nutné NDEF záznamu zapsat jiný typ. Konkrétně předáme do NDEF záznamu typ AbsoluteUri. V případě mazání obsahu z tagu vytváří aplikace NDEF záznam plný hodnoty null. Tento NDEF záznam pak předá úplně stejně jako při předávání textového záznamu.

Poslední možností je čtení z tagu. Postup je velmi podobný, jen zde nevytvářím žádný payload. Nejprve je nutné znovu zkontrolovat, zda je přítomný tag a poté zda je přítomna NDEF zpráva. Z této NDEF zprávy pomocí metody GetRecords() vezmeme první záznam. Můžeme si dovolit brát pouze první NDEF záznam, protože víme, že se jedná o čtení ze štítku. Posledním krokem je identifikace typu záznamu. V případě textu ho uživateli aplikace jednoduše zobrazí (Zdrojový kód 9). Pokud se jedná o URL je třeba nejprve zkontrolovat formát URL. Pokud není správný je uživateli zobrazena chybová hláška. V případě, že je správný je uživateli automaticky otevřen prohlížeč s danou URL adresou.

```
if (record.Tnf == NdefRecord.TnfMimeMedia)
{
    var data = Encoding.UTF8.GetString(record.GetPayload());
    DisplayAlert("Obsah štítku: " + data);
}
```

Zdrojový kód 9: Zobrazení obsahu štítku uživateli

8.6 Testování

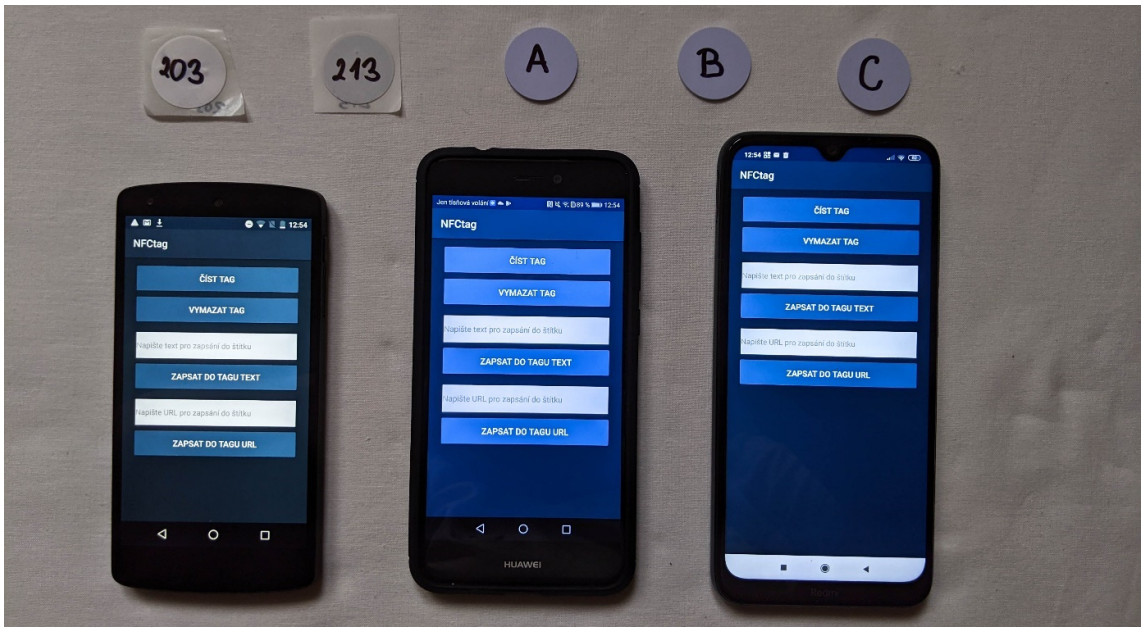
8.6.1 Testování vývojářem

Posledním krokem při vývoji aplikace je její testování. Pro testování byly zvoleny čtyři telefony s různými verzemi Androidů:

- Nexus 5 – Android 6
- Huawei P9 Lite 2017 – Android 8
- Redmi Note 8T – Android 9

Na všech třech telefonech byly prováděny stejné testy a byly očekávány i stejné výsledky. Pro testování byly využito pět odlišných NFC tagů. Konkrétně Ntag203, Ntag213 a 3x

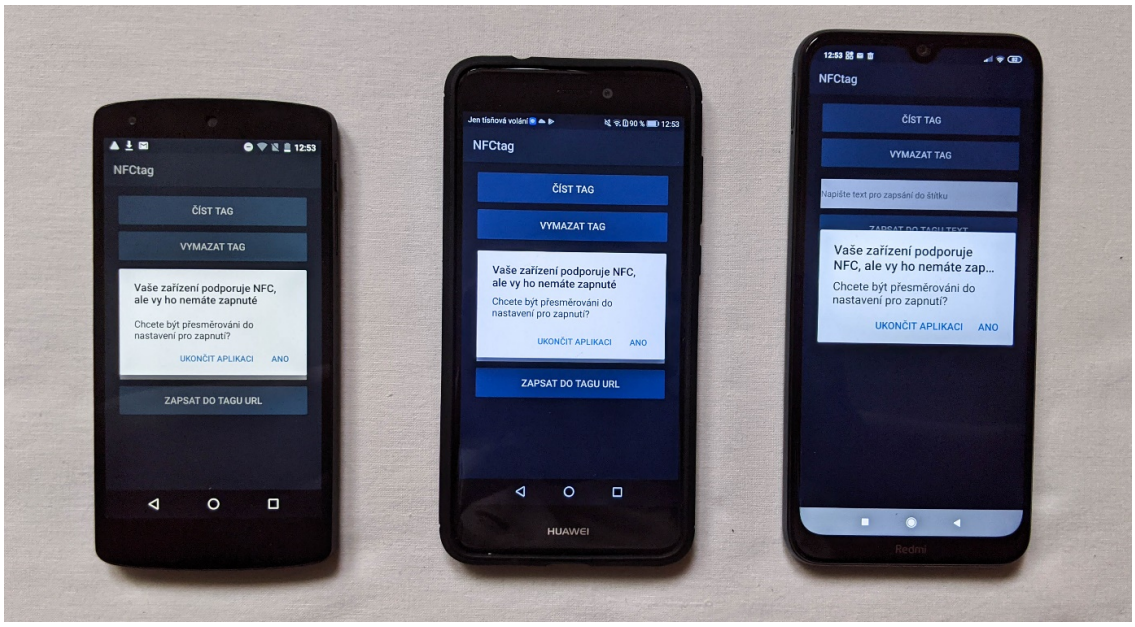
Ntag215. Tyto tagy se liší zejména ve velikosti úložiště, ale také například možností počítání skenů. Na obr. 18 můžeme vidět tři telefony a jednotlivé NFC tagy. Zleva: Nexus 5, Huawei P9 Lite, Redmi Note 8T. Štítky jsou součástí příloh této práce, aby si mohl kdokoliv tuto aplikaci vyzkoušet.



Obrázek 18: Testování spuštěné aplikace

Zdroj: Autor práce

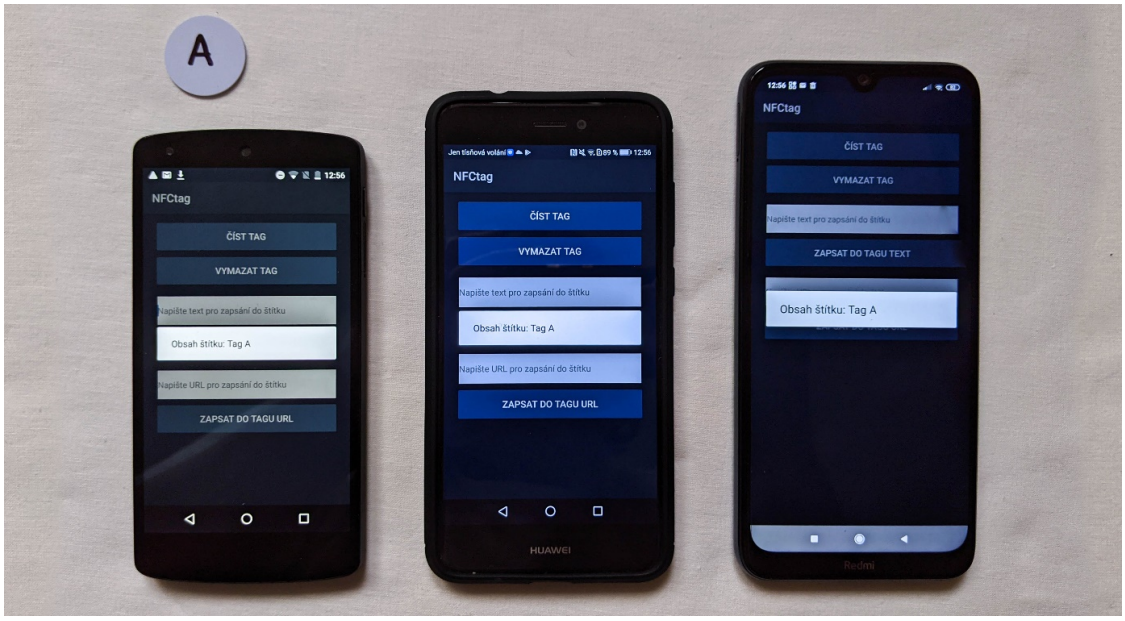
Test číslo jedna spočívá v tom, že na všech zařízeních vypneme NFC a očekáváme, že aplikace zkontroluje přítomnost NFC a uživateli nabídne možnost tuto funkci zapnout. Jak můžeme vidět na obr.19 aplikace u všech třech zařízení prošla, protože zobrazila uživateli správné okno s nabídkou pro zapnutí nebo ukončení aplikace. Po vrácení se zpět z nastavení do aplikace je z uživatelského pohledu vše v pořádku a může pokračovat k používání aplikace.



Obrázek 19: První test aplikace – kontrola NFC

Zdroj: Autor práce

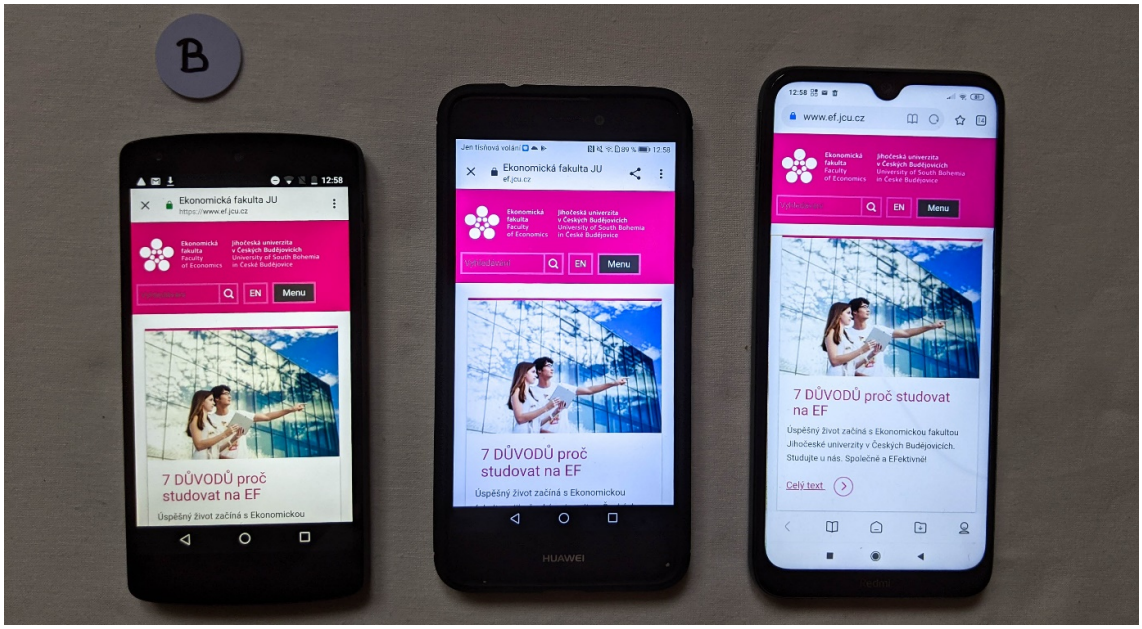
Druhým testem aplikace je zjistit, zda umí správně zapsat text na štítek a tento štítek posléze přečíst. K tomu slouží štítek A, na který bylo postupně ze všech tří aplikací zapsán text: „Tag A“. Díky tomuto testu jsme ověřili i funkci vymazat tag, která také dělala, co měla. Jak můžeme vidět na obr.20 aplikace na všech zařízeních zobrazila vše správně.



Obrázek 20: Druhý test aplikace – zápis a smazání štítku

Zdroj: Autor práce

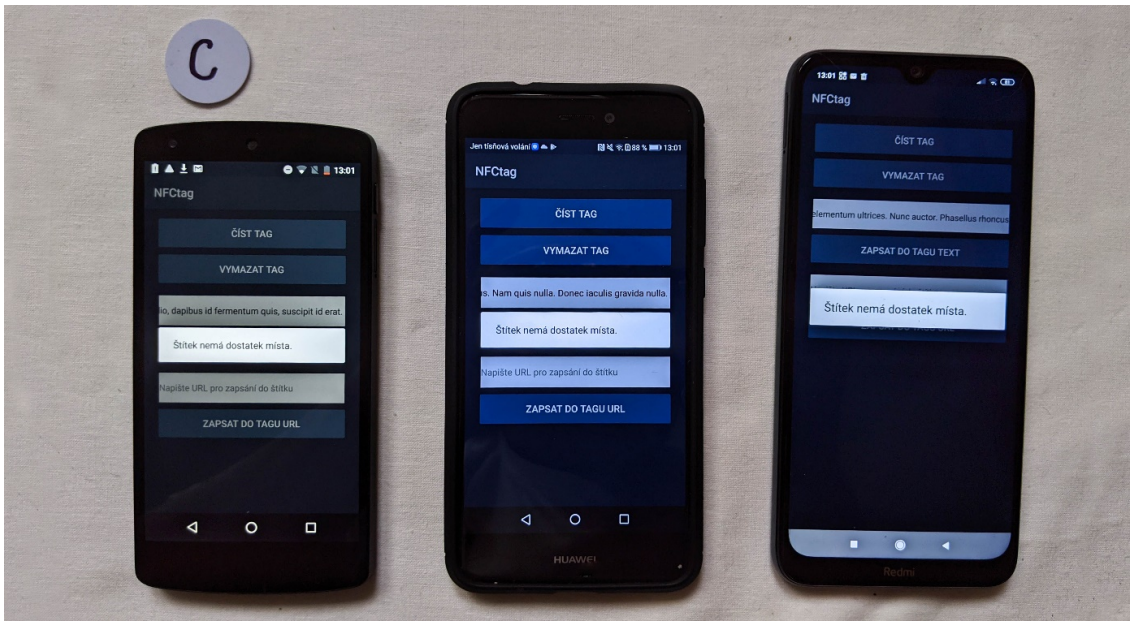
Třetí test sloužil pro kontrolu správné funkcionality zápisu a čtení URL. Aplikace umí správně zapsat URL na jakýkoliv štítek a ten pak v případě přečtení zobrazí přímo uživateli. Na štítek B bylo tedy postupně ze všech telefonů zapsána URL Ekonomické fakulty Jihočeské univerzity. Na obr.21 můžeme vidět výstup po přečtení URL ze štítku. Aplikace téměř instantně otevře prohlížeč dostupný na zařízení s danou URL. V této části testování byl proveden i test při zapsání špatně formátovaného URL. Aplikace při špatném formátování ukázala na obrazovce chybovou hlášku, a tak i v tomto případě bylo vše v pořádku.



Obrázek 21: Třetí test aplikace – zápis a čtení URL

Zdroj: Autor práce

Posledním prováděným testem bylo testování jednotlivých chybových hlášek. K tomu byly použity zbývající štítky. Při zápisu štítek kontroluje dvě věci: zda je na štítku dost místa a zda není štítek pouze v módu pro čtení. Štítek 203 byl nastaven do módu pouze pro čtení a aplikace si s ním poradila na výbornou. Zobrazila chybovou hlášku tak jak měla. V případě kontroly dostupného místa na štítku se aplikace sama ukončovala. Bylo tedy nutné přejít zpět do kódu a podívat se, kde nastala chyba. Po několika minutách debugování byla chyba nalezena a opravena. Problém byl v jedné z podmínek, kdy se aplikace i v případě, že na štítku nebylo dost místa snažila na štítek zapsat, a proto se ukončovala. Na obr.22 vidíme, že aplikace po úpravě funguje i v případě nedostatku místa a zobrazuje správnou chybovou hlášku.



Obrázek 22: Čtvrtý test – chybová hláška

Zdroj: Autor práce

8.6.2 Testování uživateli

Poslední fází bylo testování pomocí uživatelů. Aplikace byla předána třem dobrovolníkům společně se třemi identickými štítky (konkrétně Ntag215). Tito uživatelé měli týden na to, aby aplikaci ve všech směrech otestovali a vrátili se s poznatky o aplikaci. Jejich telefony byly následující:

- Google Pixel 3a – Android 11
- Realme X2 Pro – Android 10
- Honor 10 – Android 10

Po týdnu jsem se s uživateli setkala pomocí video hovoru a o aplikaci s nimi pohovořila. Všichni uživatelé se shodli na tom, že aplikace funguje bez žádných problémů. Nenašli tedy žádnou chybu a tvrdili, že aplikace dělá přesně to, co má. Jednoho z uživatelů velmi zaujala funkcionalita zápisu a čtení URL. NFC předtím vůbec neznal a byl rád, že mu tato technologie byla představena.

9 Závěr

Cílem bakalářské práce bylo zmapovat potřebné technologie související s NFC a analyzovat současné mobilní aplikace, tedy možnosti uživatele v tomto odvětví. dalším cílem bylo i vytvoření mobilní aplikace spojující kód a NFC.

V teoretické části jsem nejprve představila samotnou technologii NFC a její stručnou historii. Poté jsem vysvětlila všechny tři módy přenosu společně s typy zpráv, které lze pomocí této technologie poslat. V dalším kroku jsem se přesunula k implementaci NFC do mobilních zařízení, kde jsem nastínila architekturu a dva způsoby zabezpečení. Dále jsem zpracovala téma mobilních plateb pomocí NFC, kde jsem vylíčila nejen zabezpečovací prvky, ale také hrozby ohrožující přenos. Z této části vyplývá, že technologie NFC je velmi bezpečnou. Následovala krátká analýza světové a českého trhu v rámci využívání mobilních plateb. V Evropě se tento způsobem plateb již stává běžnou součástí lidského života. Skvělým příkladem je Dánsko, kde mobilní platby využívá většina obyvatelstva. Velkou částí práce je výpis všech dostupných aplikací v ČR nabízejících platby pomocí NFC. Největšími zástupci těchto aplikací jsou Google Pay a Apple Pay. Jedním z rozdílů mezi nimi je podpora jiných OS v mobilních zařízeních nebo také způsob zabezpečení. Teoretická část je ukončena uceleným pohledem na NFC v současnosti a její možný vývoj v budoucnosti.

V praktické části jsem se zabývala vývojem aplikace pomocí frameworku Xamarin. Zpočátku jsem se potýkala s problémy v rámci funkcionality aplikace, ale nakonec jsme vše vyřešili s vedoucím této práce. Na začátku jsem popsala životní cyklus aplikace, pomocí kterého byla pak celá aplikace zkonstruována. Prvním krokem bylo uživatelské rozhraní, kde byly zaimplementovány všechny požadavky na aplikaci. Kód jsem popsala pomocí jednotlivých funkcí, které jsem doplňovala o samotný kód. Závěrem praktické části bylo otestování vývojářem, tedy mnou, které jsem doplnila o fotografie z testů. V průběhu těchto testů byla zjištěna jedna chyba v oblasti chybových hlášek, která byla opravena. V přílohách práce jsou i NFC štítky z tohoto testování. Poté jsem aplikaci předala třem uživatelům, kteří tuto aplikaci týden testovali. Po týdnu testování proběhl videohovor s každým z nich, kde proběhla krátká diskuse. Všem uživatelům splnila aplikace očekávání a hodnotily ji velmi kladně.

Summary and keywords

This bachelor's thesis explores the technology behind payments by NFC chips. The first part of this thesis is theoretical and maps all the needed technologies connected to NFC. It shows the history of NFC, how it was developed and how it looks today. Including all the current applications and specific options for the user of contactless payments. The main part is dedicated to the safety and encryption of payments by NFC technology.

The second part of this thesis shows developing mobile application for Android using the Xamarin framework. It shows the whole process of developing an application using encryption and the NFC technology, and testing the application in the field. At the end it includes analysis of possibilities with usage of NFC in wearable electronics and possible future developments in this area.

Keywords: NFC technology, mobile application, development, encryption, contactless payments

Seznam literatury

Chang, H. (2017). *Everyday NFC: Near field Communication Explained* (3rd ed.).

Hermes, D. (2015). *Xamarin mobile application development: cross-platform C# and Xamarin.forms fundamentals. Apress.*

Igoe, T., Coleman, D., & Jepson, B. (2014). *Beginning NFC: near field communication with Arduino, Android, and Phonegap.* O'Reilly.

Rosenberg, M., & Mertlík, T. M. (2013). Technologie NFC – popis, bezpečnost a využití (NFC technology – description, security and usablity). Elektrorevue, 2013(2), 9.

Coskun, V., Ozdenizci, B., & Ok, K. (2013). A Survey on Near Field Communication (NFC) Technology. Wireless personal communications, 71(3), 2259-2294.

Elektronické zdroje

Android Developers. Intent [Online]. Načteno z: https://developer.android.com/reference/android/content/Intent+

Android Developers. Activity [Online]. Načteno z:

https://developer.android.com/reference/android/app/Activity.html#ActivityLifecycle

Carvalho, J. (2019). Fresh SmartPhone Statistics And What They Mean For You, NFC And The World [Online]. Načteno z: https://nfc-forum.org/fresh-smartphone-statistics-and-what-they-mean-for-you-nfc-and-the-world/

Drhlík, K. (2017). Bezdrátové technologie: Co je NFC a jak ho využít? [Online]. Načteno z: https://www.svetandroida.cz/bezdratove-technologie-nfc/

EMV® Payment Tokenisation [Online]. Načteno z: https://www.emvco.com/emv-technologies/payment-tokenisation/

Hrubý, F. (2019). Česká spořitelna spouští bezkontaktní placení pomocí chytrých hodinek s Garmin Pay a Fitbit Pay [Online]. Načteno z: https://www.csas.cz/cs/o-nas/pro-media/tiskove-zpravy/2019/09/24/ceska-sporitelna-spousti-bezkontaktni-placeni-pomoci-chytrych-hodinek-s-garmin-pay-a-fitbit-pay#

Chau, M., & Reith, R. (2020). Smartphone Market Share [Online]. Načteno z: https://www.idc.com/promo/smartphone-market-share/os

Korb K., Pultzner M. (2012). Secure element: klíč k mobilním platbám [Online]. Načteno z: https://nearfield.cz/clanky/secure-element-klic-k-mobilnim-platbam-20

Korhonen, N. (2017). NFC Payment & Security Threats [Bakalářská práce, Haaga-Helia University of Applied Sciences]. Načteno z: https://www.theseus.fi/bitstream/handle/10024/125290/Korhonen_Niko.pdf?sequence=1&isAllowed=y

Maxwell R. (2014). Taking "being connected" to the next level: Man implants NFC chip into his hand [Online]. Načteno z: https://www.phonearena.com/news/Taking-being-connected-to-the-next-level-Man-implants-NFC-chip-into-his-hand_id62057

NFC forum [Online]. Načteno z https://nfc-forum.org/

NFC Market worth $34.9 billion by 2025 (n.d.). Načteno z: https://www.marketsandmarkets.com/PressReleases/near-field-communication.asp

NFC platby mobilem (NÁVOD) (2020). Načteno z: https://www.alza.cz/nfc-platby-mobilem

Sabella, R. R. (2019). A Quick History of Near Field Communication (NFC) [Online]. Načteno z: https://www.dummies.com/consumer-electronics/quick-history-near-field-communication-nfc/

Sabella, R. R. (2019). NFC Operating modes [Online]. Načteno z: https://www.dummies.com/consumer-electronics/nfc-operating-modes/

Sacco, A. (2012). NFC Not Just for Mobile Payments: Six Future Uses. Načteno z: https://www.cio.com/article/2393217/nfc-not-just-for-mobile-payments--six-future-uses.html

Smartphone Market Share (2020). Smartphone Market Share [Online]. Načteno z: https://www.idc.com/promo/smartphone-market-share/os

Statistica Research Department (2021). Penetration of proximity mobile payment apps in selected countries in Europe in 2019 [Online]. Načteno z https://www.statista.com/statistics/1113874/mobile-payment-app-use-in-selected-countries-in-europe/

Seznam obrázků, zdrojových kódů, diagramů, tabulek a zkratek

Seznam obrázků

Seznam zdrojových kódů

Seznam diagramů

Seznam tabulek

Seznam zkratek

API – rozhraní pro programování aplikací

dCVV – dynamická hodnota pro ověřování karty

ID – identifikační číslo/karta

IoT – internet věcí

MST – magnetický zabezpečení přenos

NDEF – formát zapouzdření zpráv pro výměnu informací mezi zařízeními

NFC – technologie rádiové bezdrátové komunikace

OS – operační systém

PAN – skupina osobních sítí

SE – jedna z možností zabezpečení NFC komunikace

RFID – identifikace na rádiové frekvenci

HCE – jedna z možností zabezpečení NFC komunikace

TAG – štítek nebo značka

UICC – univerzální karta integrovaných obvodů neboli SIM karta

UID – unikátní identifikační číslo

URI – textový řetězec s definovanou strukturou

Přílohy

Příloha 1: CD se zdrojovým kódem aplikace, samotnou aplikací a plným textem bakalářské práce

Příloha 2: NFC štítky použité při testování aplikace vývojářem