Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informatiky a kvantitativních metod

Technologie NFC v systému Android

Bakalářská práce

Autor: Adam Lihm
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Pavel Kříž, Ph.D.

Hradec Králové duben 2015

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 23.4.2015 Adam Lihm

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Pavlu Křížovi, Ph.D. za metodické vedení práce, za pomoc, odborné konzultace a cenné rady při zpracovávání této práce.

Anotace

Cílem bakalářské práce je seznámení s problematikou Near Field Communication (NFC) v reálném světě, což zahrnuje seznámení se standardy, ale i s praktickým použitím a dále významem a použitím v operačním systému Android. NFC je velmi progresivní technologie s velkým potencionálem. V první části bakalářské práce je zmíněna historie, technické detaily, využití a stručný přehled NFC tagů. Ve druhé části práce je rozebráno jak technologie NFC funguje uvnitř operačního systému Android a jak systém Android zpracovává a pracuje s NFC tagy. Další část představuje reálné a praktické využití NFC, důvod, proč některé tagy nelze načíst, dále je zde naznačena budoucnost placení pomocí NFC v České republice a jsou zde porovnány přístupy dvou gigantů Apple a Googlu. V poslední části je představena emulace karet v systému Android.

Annotation

Title: NFC Technology in Android Operating System

The aim of this bachelor thesis is introduce with issue of Near Field Communication (NFC) in the real world, which includes familiarization with the standards, but also practical use and meaning and use in the operating system Android. NFC is very advanced technology with great potential. In the first part of bachelor thesis is mentioned history, technical detail, use and brief overview of the NFC tags. In the second part is discussed how NFC works within operating system Android and how the system handles and works with NFC tags. Another part introduces real and practical use of the NFC, reason why some tags cannot be loaded, next it is indicated future of payment by NFC in the Czech Republic and compares of approaches two giants Apple and Google. In the last part there is introduced card emulation in the system Android.

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

AAR	-	Android Application Record
AID	-	Application ID
APDU	-	Application Protocal Data Units
CPU	-	Cetral Processing Unit
HCE	-	Host Card Emulation
MIME	-	Multipurpouse Internet Mail Extensions
NDEF	-	NFC Data Exchange Format
NFC	-	Near Field Communication
OS	-	Operační Systém
PCD	-	Proximity Coupling Device
PICC	-	Proximity Integrated Circuit Card
QR	-	Quick Response Code
RFID	-	Radio-frequency Identification
RTD	-	Record Type Definition
SDK	-	Software Development Kit
SE	-	Secure Element
TNF	-	Type Name Format
UICC	-	Universal Integrated Circuit Card
UID	-	Unique ID
URI	-	Uniform Resource Identifier

1 Úvod

Near Field Communication (NFC) se v poslední době, hlavně díky velkému rozšíření do mobilních technologií, dostává stále více do podvědomí širokému spektru lidí. I přesto, že velké množství mobilních technologií obsahuje NFC, lidé stále netuší, jak tuto technologii vědomě a aktivně využívat v každodenním životě. Mnoho lidí však tuto technologii využívá nevědomky například jako součást přístupových systémů do objektů, či při bezkontaktním placení.

Kapitola Technologie NFC je věnována obecnému představení NFC, jak technologie funguje, je přiblížena historie a zformování NFC fóra. Kapitola dále představuje jednotlivé tři režimy, v kterých může NFC fungovat a ukazuje využití NFC v každodenním životě. Následuje představení ISO standardů definovaných dle NFC fóra a představení různých druhů NFC tagů, které lze na trhu koupit. Poslední podkapitola představuje průzkumy, které se týkají NFC a predikce toho, jak se toto odvětví bude vyvíjet.

Další kapitola NFC technologie a OS Android by měla poodhalit, jak systém Android pracuje s NFC tagy, co je to Secure Element, k čemu slouží a proč před tím, než přišla firma Simply Tapp se svým řešením, bylo tak obtížné v mobilním zařízení používat NFC. Dále je zde kapitola, kde je pečlivě rozebráno, jak je tag zpracováván a co se děje při jeho zpracovávání, této kapitole předchází kapitola o intentech, která slouží pro plné pochopení. V poslední kapitole je představeno Android Application Records, pomocí kterého se dá do tagu nastavit, která aplikace má být spuštěna.

Následuje kapitola Praktické využití, ve které je představen test, jak se chová mobilní zařízení při načítání karet, další je kapitola, kde je vysvětleno, proč některé mobilní zařízení dokáže načíst NFC tag a jiné ne, a proč se tak děje. Je zde naznačeno také to, kam směřuje placení přes mobilní zařízení v České republice. Společnost Apple vydala za velké slávy svůj nový mobilní telefon s NFC a službou Apple Pay, proto je v dalších kapitolách rozebrán přístup Applu k NFC a porovnání jejich řešení oproti řešení společnosti Google, která svůj první telefon s NFC představila již v roce 2010. V další kapitole je představen prototyp přístupového systému, který by fungoval s mobilními zařízeními s NFC zaměstnanců. V následující kapitole je popsáno, jak si člověk může sám naprogramovat svůj vlastní NFC tag a je zde také

doporučeno, který NFC tag vybrat. V poslední kapitole jsou představeni různí zástupci aplikací, které umějí pracovat s NFC a využívají ho.

V poslední kapitole je představena emulace karet v operačním systému Android. Je zde vysvětleno, jak se karty emulují, pokud se využívá Secure Element a také jak probíhá Host Card Emulation (HCE). Je popsáno, které karty lze emulovat a také je zde popsána komponenta Service, která je velmi užitečná. Další kapitola představí, jak funguje komunikace a co to je APDU, poté následuje kapitola, která přibližuje chování systému Android, pokud se v něm nachází jak emulovaná karta pomocí HCE, tak i další čip například SIM karta, která využívá Secure Element. Poté následuje kapitola, kde je na úryvcích kódu popsána základní aplikace, která umí HCE a následně jsou vybrané aplikace z hlediska kódu porovnány.

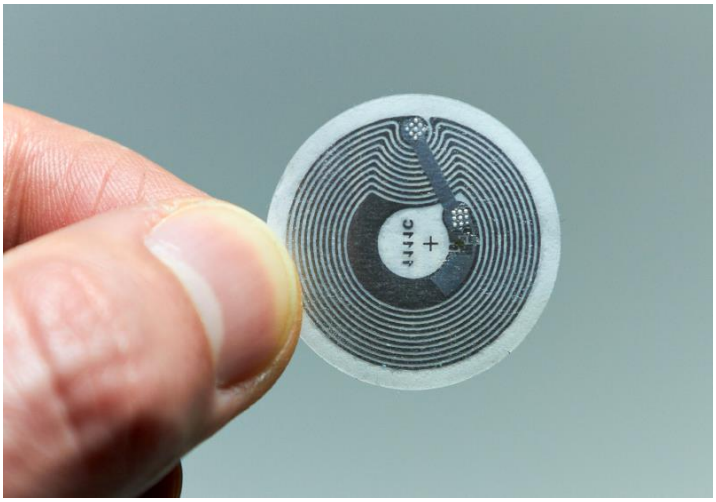
2 Technologie NFC

O tom, co NFC vlastně je, jak funguje, podle jakých standardů a jak se dá využít, budou pojednávat následující kapitoly.

2.1 Near Field Communication

NFC neboli Near Field Communication umožňuje jednoduchou a bezpečnou komunikaci mezi elektronickými zařízeními. Pomocí technologie NFC mohou zařízení uskutečňovat bezkontaktní transakce, přistupovat k digitálnímu obsahu a propojit elektronická zařízení jediným dotykem [1]. Technologie NFC pracuje na frekvenci 13,56 MHz s velmi omezeným dosahem, který se pohybuje v jednotkách centimetrů. Rychlost přenosu dat se pohybuje od 106 Kb/s do 424 Kb/s. Jde o malou rychlost, pro porovnání technologie Bluetooth disponuje rychlostí přenosu dat 24 Mbit/s. Technologie NFC je ale určena hlavně pro výměnu malých dat a pro snadnost tohoto přenosu [2]. Technologie NFC má také velmi malou energetickou náročnost a tak vždy pouze jedno zařízení musí být napájeno. Druhé zařízení může být pomocí elektromagnetické indukce napájeno tím prvním [3].

Technologie NFC spadá do standardů, které jsou zahrnuty pod technologií RFID (Radio-frequency identification). Hlavní rozdíl mezi těmito technologiemi je ta, že RFID pracuje na více frekvencích a slouží hlavně jako identifikační prostředek, za to technologie NFC je vytvořena pro přenos jakýkoliv dat [2].



Obr. 1 NFC tag
Zdroj: [4]

2.2 Historie

V roce 2003 bylo schváleno NFC jako ISO/EIC standard. O rok později společnosti Nokia, Sony a Philips založily neziskovou organizaci NFC Forum. NFC Forum je neziskové sdružení výrobců, vývojářů, finančních institucí a dalších [5]. Kromě zakládajících členů a většiny výrobců mobilních telefonů lze mezi členy fóra najít také například společnosti Blackboard Inc., Microsoft Corporation, Visa Inc., MasterCard Worldwide.

V roce 2006 vydává NFC Forum první specifikaci pro NFC tagy, k dnešnímu dni vzniklo celkem 16 specifikací. V roce 2006 se také objevil první mobilní telefon s podporou NFC – Nokia 6131 [6]. V letech 2007 a 2008 probíhá několik pokusů o uvedení technologie na trh, ovšem technologie nemá dostatečnou podporu, a tak tyto pokusy končí neúspěchem [5]. V roce 2009 vznikly standardy pro přenos kontaktů, URL, nebo iniciaci technologie Bluetooth. Postupem času začíná být technologie NFC stále častěji implementována do mobilních telefonů.

Průlomový byl rok 2011, kdy se NFC dostalo do platebních karet společnosti MasterCard [6]. Na téma NFC probíhá každý rok spousta konferencí, kde se výrobci snaží předvést co největší originalitu a inovaci v používání technologie NFC.

2.3 Režimy přenosu

Technologie NFC může fungovat v jednom ze tří režimů, a to Read/Write režim, Peer-to-Peer režim nebo režim emulace karty.

2.3.1 Read/Write režim

Read/Write režim neboli Čtení/Zápis umožňuje číst nebo zapisovat data do NFC objektů. Na základě získaných informací se potom dané objekty nějak zachovají. Tento režim je založen na standardech ISO/EIC 14443 a FeliCa [2]. Pokud je ve čtecím poli přítomno více karet dle anti-kolizního algoritmu, je vybrána ke čtení pouze jedna. Metoda, která je použita pro výběr správného anti-kolizního algoritmu, vybírá algoritmus dle typu načtené karty.

Při používání tohoto režimu se čtečka chová jako aktivní zařízení. Pokud je na tagu uložena informace, čtečka se zachová dle informace, bez nutné interakce

s uživatelem, tedy pokud je na tagu uloženo URL, potom se na mobilním zařízení s NFC technologií otevře webový prohlížeč. [7]

2.3.2 Peer-to-Peer režim

Peer-to-Peer režim dovoluje dvěma NFC zařízením spolu komunikovat, vyměňovat si informace a sdílet složky [8]. Komunikace probíhá v half-duplexním režimu, tedy v jednom momentu pouze jednosměrně [2]. Hlavní smysl tohoto režimu je umožnit uživatelům odeslat jejich data tak rychle, jak rychle je to jenom možné (v řádech milisekund) [7].

2.3.3 Emulace karty

Pomocí režimu emulace karty se do mobilního zařízení disponující technologií NFC emuluje NFC tag. Mobilní zařízení se potom chová jako pasivní NFC tag a čeká, dokud NFC čtečka nezačne iniciovat čtení [2]. Jedná se tedy o opak režimu Read/Write. Jelikož se emulují karty pomocí mobilního zařízení, je možné mít na zařízení více než pouze jednu emulovanou kartu. Karta je vybrána na základě požadavku čtečky, v případě, že pro danou situaci vyhovuje víc karet, vybírá se z karet dle preferencí, pokud ani to není možné, kartu vybere uživatel. Čtečka karet takovéto zařízení, které emuluje kartu, vidí pouze jako kartu a ne jako mobilní zařízení disponující technologií NFC. Tím pádem zařízení nemůže rozlišovat mezi NFC zařízením a kartou. [7]

2.4 Využitelnost NFC

Následuje rozdělení NFC tagů podle toho, jestli to jsou pouhé pasivní NFC tagy, které obsahují různorodý obsah, či aktivní NFC čipy, které s tagy pracují. Kapitola aktivní NFC představuje využití NFC, pokud jsou zabudovány v nějakém zařízení.

2.4.1 Pasivní NFC

Jedním z hlavních a v současnosti zřejmě nejdůležitějším představitelem v oblasti bankovnictví je společnost MasterCard. Společnost MasterCard se svým řešením využívající NFC přišla na trh mezi úplně prvními a dá se považovat za jakéhosi průkopníka technologie NFC v oblasti bankovnictví. MasterCard svůj

produkt nazývá PayPass a prezentuje ho jednoduchým, ale o to více výstižným „TAP & GO™“, což by se dalo volně přeložit, jako PŘILOŽ A JDI. Velké plus tohoto balíčku služeb je to, že není dostupný pouze v Americe, ale je dostupný také u nás v České republice. Technologie NFC může být zabudována buď přímo v kartě zákazníka, či zákazník může mít speciální nálepku, přívěšek na klíče, hodinky, nebo může mít platební kartu v telefonu [9]. Bezkontaktní platby nabízí také společnost Visa, ovšem ta pouze využívá technologii PayPass od společnosti MasterCard a nazývá jí payWave [10].

Mezi další využití technologie NFC patří NFC tagy. Jedná se o malé paměťové zařízení s anténou, které nepotřebuje napájení a umožňuje zasílat data bezdrátově. Jako napájení stačí NFC tagu pouze jev známý jako elektromagnetická indukce, jelikož spotřeba NFC tagu se počítá pouze v desítkách mikro wattů [11]. Do NFC tagu nelze uložit velké množství informací jedná se o velikost od 64B do 8kB [11]. Tato velikost vyhovuje různým ID číslům, URL adresám, kontaktům.

Může se sice zdát, že technologie NFC v tomto ohledu moc využitelná není, ovšem opak je pravdou. Tato pasivní zařízení se díky své velikosti mohou objevit například ve vizitkách, reklamních předmětech. Ovšem tím využití nekončí, tagy se mohou objevit na plakátech tzv. smarposters [12], v psích známkách, v prstýnkách [13], na lahvích od vína, kde díky NFC tagu zjistíme, jestli je víno originál [14], v kabelkách [14], na kufru, v podstatě kdekoliv. Využití v kartách totožnosti či jiných kartách denní potřeby je zřejmé. Karty na NFC tagu nesou své ID, které odesílají čtečkám a ty s ním dále pracují. Další využití NFC tagů je například v marketingu. Businessman vlastní vizitky s NFC tagem a osobě, která k vizitce přiloží své mobilní zařízení, se do přiloženého mobilního zařízení přenese kontakt a otevřou se webové stránky businessmanova podniku. Dále je k vidění využití třeba v restauracích, fastfoodech apod., kdy na veřejném místě visí reklama a člověk mající mobilní zařízení disponující technologií NFC může načíst NFC tag, který otevře na zařízení stránku s aktuálním jídelním lístkem [6].

Obr. 2 Ukázka Smartposteru
Zdroj: [15]

Firma Sony představila svou koncepci Xperia Smart Tags, která obsahuje čtyři různě zbarvené NFC tagy a software. Každý NFC tag slouží při jiné příležitosti, jeden pro situaci doma, další v práci, v autě a v posteli. Po přiložení mobilního zařízení k NFC tagu je možné, například po nastoupení do auta, aktivovat Bluetooth pro připojení zařízení k headsetu, aktivovat navigaci v zařízení a přepnout zařízení do módu auto [16].

2.4.2 Aktivní NFC

V předchozím textu se psalo o pasivním NFC tagu a aktivním čtecím zařízení disponující technologií NFC. Pokud se ale spojí dvě aktivní zařízení, je tu spousta dalšího využití. Například NFC umístěné ve fotoaparátu a v tiskárně. Fotograf vyfotí fotografii a chce-li ji okamžitě vytisknout, stačí mu pouze přiložit fotoaparát nad tiskárnu, která hned začne tisknout [17]. Jestliže chce obchodník předat zákazníkovi určitá data, a pokud mají oba dva mobilní zařízení s technologií NFC, tak stačí pouze k sobě obě dvě zařízení na pár vteřin přiblížit a přepošlou se všechny informace. Tento proces výměny dat slouží k elektronickému předání informací namísto fyzického předávání, například vizitky. Velmi jednoduché a praktické je sdílení souborů mezi dvěma mobilními telefony pomocí Android Beam. Stačí mít dva telefony disponující technologií NFC, mít na obrazovce vybraný soubor ke sdílení,

přiložit mobilní telefony zády k sobě a iniciovat přesun souborů. Dle velikosti souboru se potom zvolí, zda se použije NFC, Bluetooth či v určitých případech Wi-Fi.

Každý rok je pořádána spousta sportovních, kulturních či jiných akcí a vstupenky na tyto akce jsou často velké, špatně skladné a musí se tedy přehýbat, nebo se vstupenka může zmačkat, či může nastat to, že díky fyzické deformaci vstupenky je špatně čitelný kód EAN. Alternativou je uložit vstupenku do mobilního zařízení s technologií NFC a při vstupu na akci přiložit mobilní zařízení k čtecímu zařízení, které potvrdí pravost vstupenky.

Do mobilního zařízení disponujícího technologií NFC lze virtuálně uložit celý obsah peněženky. Do zařízení lze nahrát občanský průkaz, řidičský průkaz, cestovní pas, nejrůznější věrnostní karty, karty na MHD, ale také i platební karty a například také vstupní karty a klíče [18].

2.4.3 Shrnutí

NFC se používá každý den. Aktivně se může NFC používat například při spojení s NFC tagy, kdy v noci před spánkem se přiloží mobilní zařízení k tagu a v zařízení se zapne budík a ztlumí se zvuky. Další využití je přiložení mobilního zařízení k tagu jídelního lístku u restaurace, kdy se v zařízení načte celý jídelní lístek. Dále je možné technologii NFC využívat třeba při tisku dokumentů či fotografií. Do mobilního zařízení lze uložit identifikační doklady, věrnostní karty, klíče a spoustu dalších věcí.

2.5 Standardy

V této kapitole jsou představeny ISO standardy, dle kterých probíhá komunikace NFC a podle kterých jsou NFC čipy konstruovány.

2.5.1 ISO/EIC 7816-4:2013

Mezinárodní standard ISO/EIC 7816-4:2013 popisuje organizaci, ochranu a příkazy pro výměnu dat u karet. Konkrétně specifikuje:

- Obsah příkazů/odpovědí, které si dvojice vyměňuje
- Prostředky získávání datových elementů a datových objektů v kartě
- Struktura a obsah historických bajtů k popisu operačních vlastností karty

- Struktura pro aplikace a data v kartě, jak je vidět v interfacu během zpracovávání příkazů
- Přístupové metody k datům a složkám v kartě
- Bezpečnostní politiku řídící přístupová práva k datům a složkám v kartě
- Prostředky a mechanismus pro identifikaci a adresaci aplikace v kartě
- Metody pro bezpečnou výměnu informací
- Přístupové metody k algoritmům zpracovávaných kartou. Tyto algoritmy ovšem v tomto standardu popsány nejsou

Tento standard neobsahuje specifikace vnitřní implementace karty nebo okolního světa. Standard je nezávislý na fyzickém rozhraní technologie. Pokud má karta více než jedno fyzické rozhrání a je možné je používat najednou, tak vztah mezi těmito interfacy tento standard neřeší. Kapitola je zpracována dle oficiálních stránek ISO [19].

2.5.2 ISO/EIC 14443

Mezinárodní standard ISO/EIC 14443 má čtyři části pro bezkontaktní karty fungující na frekvenci 13,56 MHz v krátké blízkosti s čtecí anténou. Standard popisuje modulaci a přenosové protokoly mezi kartou a čtečkou k vytvoření provozuschopných bezkontaktních chytrých karet [20].

- 14443-1:2008
    - Standard 14443-1:2008 definuje fyzickou vrstvu PICC (proximity integrated circuit card – neboli karty s integrovaným obvodem) [21]
- 14443-2:2010
    - Standard 14443-2:2010 specifikuje charakteristiku polí, které mají být poskytnuté pro napájení a obousměrnou komunikaci mezi PCD (proximity coupling device – čtečka karet) a PICC [22]
- 14443-3:2011
    - Dotazování pro PICC, které vstoupilo do pole PCD
    - Formát bajtů, rámce a časování používané během iniciační fáze komunikace mezi PICC a PCD

- Obsah úvodních příkazů Request (požadavek) a Answer to Request (odpověď na požadavek)
- Metody k detekování a komunikaci mezi jedním PICC mezi několika PICCs
- Ostatní parametry nutné k inicializaci komunikace mezi PICC a PCD
- Optimální prostředky pro snadný a rychlý výběr jedno PICC mezi několika PICCs založené na kritériích aplikace [23]

- 14443-4:2008
  - Standard 14443-4:2008 specifikuje half-duplexní přenosový protokol představující speciální požadavky bezkontaktního prostředí a definuje aktivační a deaktivační sekvenci protokolu [24]

2.6 Druhy tagů

Kapitola byla zpracována dle článku Kryštofa Korba [11].

NFC tagy se od sebe mohou lišit použitým čipem. NFC fórum konkretizovalo celkem 4 druhy tagů. Tři druhy jsou postaveny na základě standardů 14443 a jeden je postaven podle japonského standardu JIS X 6319-4, který je pojmenován FeliCa. Tagy se od sebe liší způsobem použití, cenou, velikostí paměti, zabezpečením a přenosovou rychlostí.

- Typ 1 – je postaven na základě standardu 14443-A. Hlavní dominantou tohoto typu tagu je jeho nízká cena. Velikost paměti tohoto tagu je od 96 bajtů až po 2 kilobajty. Přenosová rychlost se pohybuje na úrovni 106 Kb/s. Tento typ tagu funguje v režimech čtení/zápis, ale lze ho i uzamknout pouze pro čtení.
- Typ 2 – tento typ tagu je naprosto stejný jako Typ 1, až na jeden malý rozdíl a tím je jeho minimální velikost paměti, která činí 48 bajtů.
- Typ 3 – jedná se o tag, který je postaven na japonském standardu FeliCa. Cena tohoto typu tagu je vyšší než u prvních dvou typů, ale nižší než u posledního typu tagů. Velikost paměti tohoto tagu je teoreticky až 1 MB. Režim pouze čtení nebo čtení/zápis se u tohoto tagu nastavuje již při výrobě. Přenosová rychlost tohoto tagu je 212 Kb/s nebo 424 Kb/s.

- Typ 4 – tento typ tagu podporuje standardy 14443-A i 14443-B. Velikost paměti tohoto typu tagu je 2, 4, 8, 16 nebo 32 kilobajtů. Přenosová rychlost u tohoto typu tagu se pohybuje na úrovni 106 Kb/s nebo 424 Kb/s. U tohoto typu tagu se stejně jako u typu 3 nastavuje režim čtení/zápis nebo pouze čtení již při výrobě.

2.6.1 Příklady NFC tagů

V následující tabulce jsou uvedeny příklady základních tagů první generace. Do dneška se nejvíce používají hlavně tagy Ultralight a tagy NTAG203.

NFC tag	Ultralight	Mifare Classic	Mifare DESfire	NTAG203
Použití	Všeobecné použití	Aplikace s většími nároky na paměť	Velkokapacitní makra, správa identit, vysoké požadavky na zabezpečení	Výborný výkon, všeobecné použití
Velikost paměti	64 B	1024 B	2 – 8 kB	192 B
Uživatelská paměť	46 B	716 B	2 – 8 kB	137 B
Standard NFC Fóra	Ano	Ne	Ne	Ano
Šifrování	Žádné	Crypto-1	DES	Žádné
Kompatibilita	Ano	Ne	Ne	Ano

Tabulka 1 Příklady NFC tagů
Zdroj: [25]

2.6.2 NFC tagy NTAG21X

Kapitola je zpracována dle článku představující tuto technologii na Rapid NFC [26].

V roce 2012 představila společnost NXP druhou generaci tagů, která by měla nahradit NFC tagy Ultralight, NTAG203 a plně nekompatibilní tagy Mifare. Nicméně

NFC tagy nové generace se spíše používají ve vývojářské sféře než v komerční. Je to díky tomu, že kromě větší paměti obsahují navíc následující vlastnosti, které budou popsány níže, UID ASCII mirror, známku pravosti, 24 bitové počítadlo, 32 bitové heslo, rychlé čtení a lepší čtecí vzdálenosti.

UID ASCII mirror dovoluje replikovat 7 bajtové ID do URL. Pokud se toto využije, může se do tagu zakódovat např.: www.mojeadresa.cz?data=xxxxxxx a tag dynamicky doplní místo „xxxxxxx“ 7 bajtové UID. Známka pravosti je snaha firmy NXP ochránit své dobré jméno, aby výrobci falešných NXP čipů nemohli vydávat své čipy jako pravé. 24 bitové počítadlo uchovává počet, kolikrát byl tag naskenovaný a může dynamicky zrcadlit tento počet do URL stejně jako v případě UID zrcadla. 24 bitové počítadlo může teoreticky načítat počty skenů až do hodnoty 16 777 215. Pomocí 32 bitového hesla lze obsah v NFC tagu zaheslovat. Heslo ovšem není zamýšleno jako náhrada za šifrování a už vůbec ne jako náhrada za uzamknutí. Heslo slouží pouze jako jednoduchá cesta k ochraně nedůležitých dat.

	NTAG210	NTAG212	NTAG213	NTAG215	NTAG216
Použitelná paměť	48 B	128 B	144 B	504 B	888 B
32 bitové heslo	ANO	ANO	ANO	ANO	ANO
24 bitové počítadlo	NE	NE	ANO	ANO	ANO
Rychlé čtení	ANO	ANO	ANO	ANO	ANO
UID ASCII zrcadlo	ANO	ANO	ANO	ANO	ANO
Známka pravosti	ANO	ANO	ANO	ANO	ANO

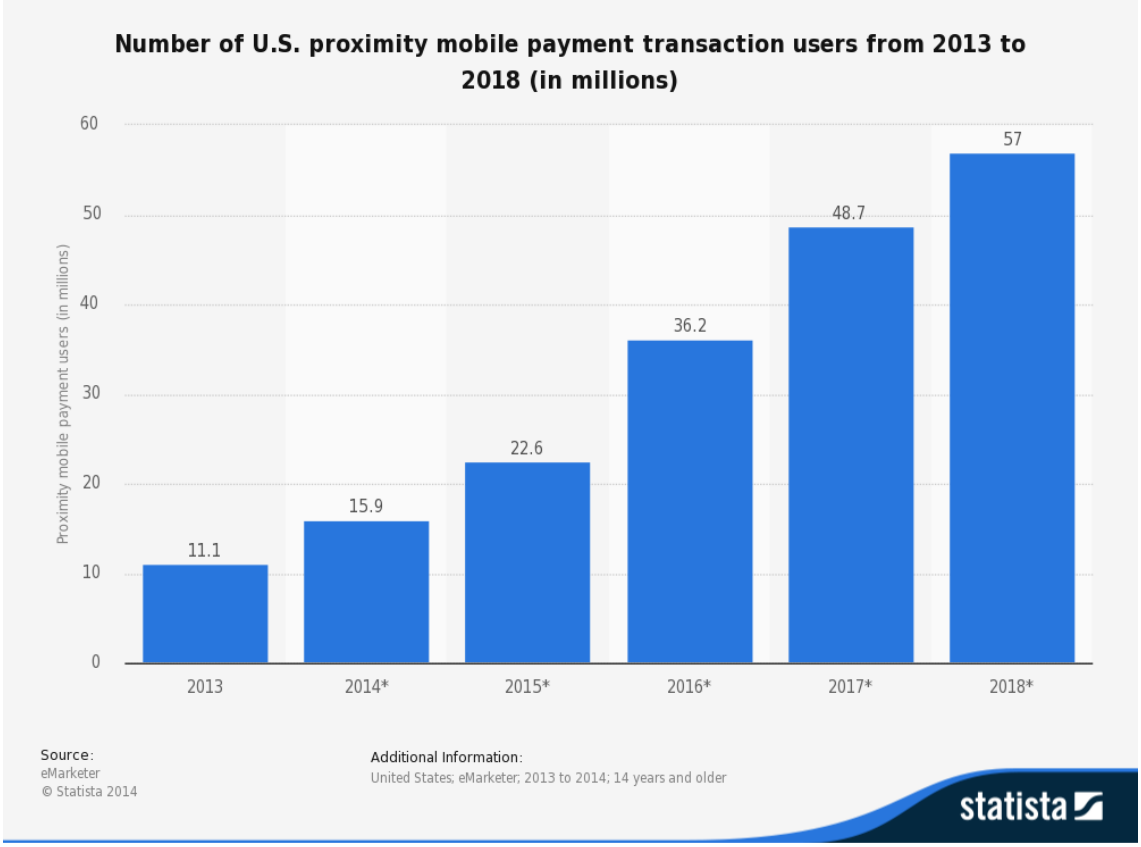
Tabulka 2 Druhy NFC tagů NTAG21X
Zdroj: [26]

2.7 NFC čip třetí generace

Společnost Samsung na svém blogu představila svůj nový NFC čip, který již byl certifikován spoustou společností jako je například Visa či MasterCard. Tyto nové čipy mají namísto ROM či EEPROM pamětí flash paměť. Nové čipy také mají velmi vysoký radiofrekvenční výkon, který Samsung nazývá „Smart Antenna“. To mimo jiné značí také to, že se anténa zmenšila o celých 30% při stejných parametrech. Jelikož je anténa menší, je menší také spotřeba a levnější jsou rovněž i čipy samotné. Nové, menší a bezpečnější čipy budou používány v mobilních zařízeních od Samsungu. [27]

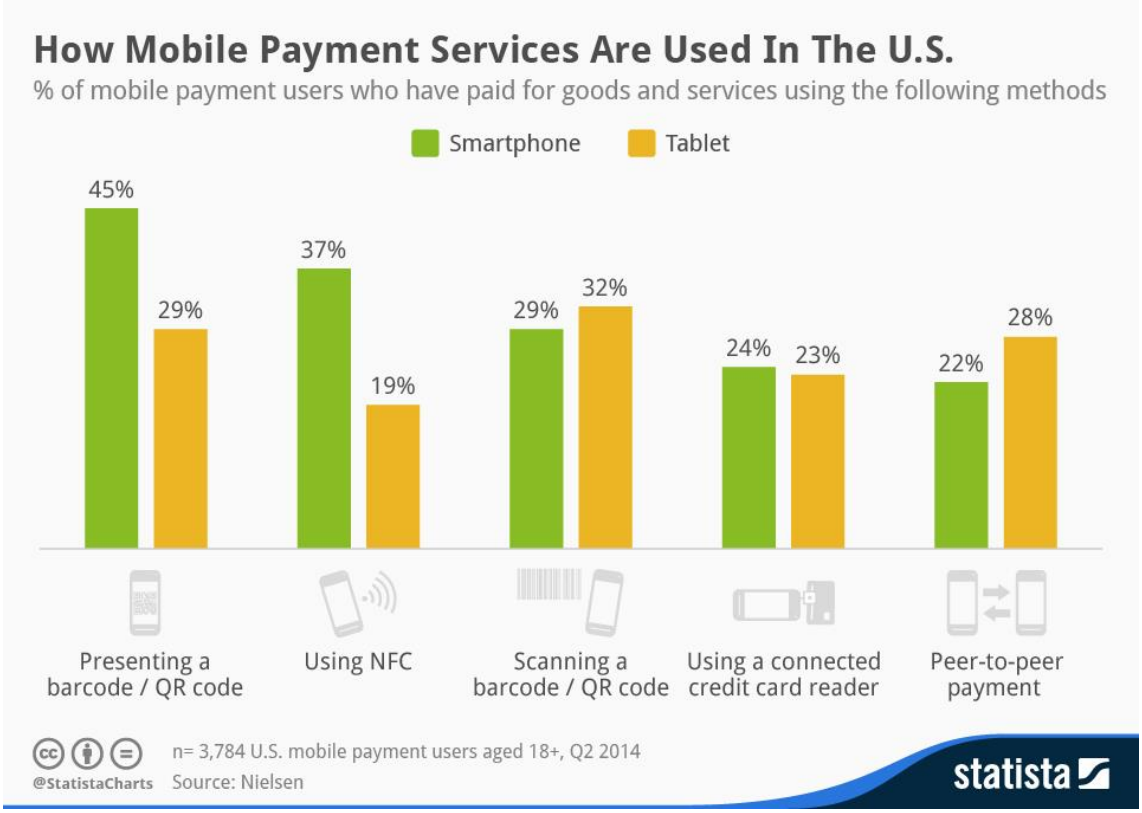
2.8 Využívání NFC

Pro představu, jak hodně se mobilní platby využívají, může sloužit následující graf počtu uživatelů. Na grafu níže je vidět prognóza, že počet uživatelů bude stoupat přibližně lineárně, a že v letošním roce by měl počet uživatelů v USA dosáhnout 22,6 milionů lidí.



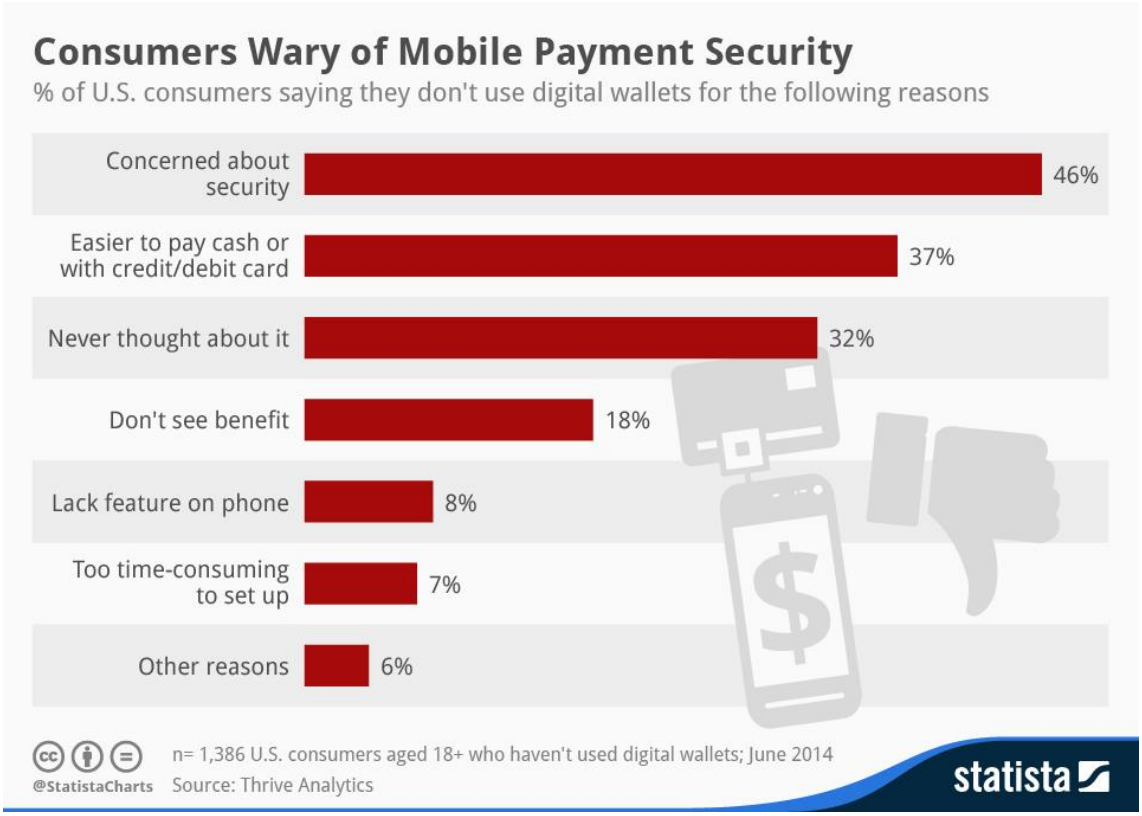
Obr. 3 Počet uživatelů bezkontaktních plateb v USA od roku 2013 do roku 2018 (v miliónech; prognóza)
Zdroj: [28]

Na následujícím grafu je vidět, jak je placení přes NFC u amerických obyvatel v oblibě. Je to druhý nejčastější způsob placení hned po předložení čárového či QR kódu. Měření probíhalo v druhém kvartálu roku 2014 u obyvatel starších 18 let. Zajímavé je také porovnání, jak se využívají k jednotlivým činnostem smartphony a tablety.



Obr. 4 Jak jsou jednotlivé služby mobilních plateb používané v USA
Zdroj: [29]

Poslední graf je zaměřen na to, proč lidé mobilní platby nevyužívají. Nejvíce lidí se bojí nedostatečné bezpečnosti mobilních plateb, pro některé je zase naopak snazší platit kreditní či debetní kartou. Dalších 32% nikdy na mobilní platby ani nepomyslelo, 18% lidí nevidí žádný přínos v mobilních platbách a zbytek lidí má buď zastaralé mobilní zařízení, nebo je pro ně moc náročné nastavit si mobilní platby v mobilním zařízení či mají jiný důvod.



Obr. 5 Nedůvěřivost k mobilním platbám

Zdroj: [30]

3 NFC technologie a OS Android

OS Android podporuje technologii NFC od verze 2.3 tedy Gingerbread. Úplně první mobilní zařízení, na kterém bylo NFC demonstrováno, byl referenční Google Nexus S v roce 2010 [31].

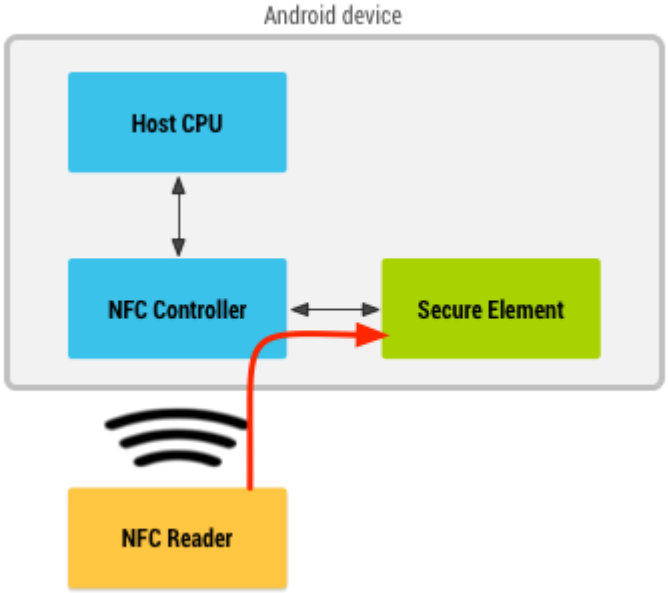
Následující kapitoly budou pojednávat o tom, jak OS Android pracuje s NFC, jak zpracovává informace předané přes NFC a jak je řešena bezpečnost.

3.1 Secure Element

Secure Element (dále jen SE) je nezávislý HW, který stojí mezi NFC a infrastrukturou telefonu, kam se ukládají veškerá zabezpečená data. Jde vlastně o takové zabezpečené úložiště dat, kam se ukládají data právě z emulovaných karet [32]. Než přišla firma Simply Tapp se svým řešením uložit SE do cloudu [33], objevovala se nejčastěji dvě řešení, a to SE přímo v kartě SIM nebo byl prvek integrován přímo do mobilního telefonu. Pokud se SE nachází přímo v SIM kartě, karta se potom nazývá UICC (Universal Integrated Circuit Card). Obsah SE na těchto kartách potom řídí mobilní operátor či jiná instituce, která kartu vystavila [32]. Takže pokud se mobilní operátor a banka dohodli, bylo možné uskutečňovat platby, případně se dalo s mobilním operátorem domluvit a operátor do SE nahrál potřebná data, aby se daly například otevírat dveře ve firmě. Toto řešení je z principu velmi nepraktické. Dalším řešením je SE v mobilním telefonu. SE v mobilním telefonu řídí výrobce telefonu. SE v telefonu využívala hlavně společnost Google se svou aplikací Google Wallet. Dokud nebyl SE v cloudu, nedalo se moc přemýšlet o rozumném využití z pohledu aplikací třetích stran.

SE v SIM kartách se v relativně velké míře využíval v bankovnictví a po absolvování náročného procesu mohl i běžný uživatel platit bezkontaktně na platebních terminálech. Velkým problémem těchto řešení je jednoznačně jeho složitost. V nejhorším případě bylo nutné založit si účet u nové banky, která vydala UICC. Poté bylo nutné čekat na dopis s kódy pro kartu. Následně musel jít člověk k novému mobilnímu operátorovi, aby mu do SIM karty nahrál telefonní číslo. Takto připravenou SIM kartu bylo potom nutné vložit jenom do hrstky mobilních telefonů, které byly podporované. Tato komplikovanost, finanční náročnost (pořízení

mobilního telefonu) vedlo k nízké užívanosti. V neposlední řadě šlo o řešení, která nebyla z dlouhodobého hlediska podporována. Příkladem za všechny budiž spolupráce mobilního operátora O2 Telefónica a banky GE Money Bank. Projekt skončil v březnu 2015, na aplikaci přestaly vycházet updaty, a proto jakmile se mobilní telefon aktualizoval na novější verzi operačního systému, než který aplikace podporovala, stalo se placení neproveditelné.



Obr. 6 Komunikace se Secure Elementem
Zdroj: [34]

3.2 NDEF zpráva a Android Beam™

Data z NFC tagů jsou přijímaná, ale i odesílaná, pomocí NFC Data Exchange Format (NDEF) zpráv. Data v NFC tagách nemusí být pouze NDEF formátů, ovšem systém Android preferuje NDEF zprávy. NDEF záznam musí mít správný formát, který je definován podle standardu NFC fóra. V systému Android jsou dva hlavní případy, kdy se pracuje s NDEF zprávami, při čtení NFC tagů a při výměně dat z jednoho zařízení do druhého pomocí Android Beam™. Čtení NDEF zpráv z NFC tagů je obsluhováno pomocí mechanismu zpracování tagu, který analyzuje tag a zachová se na základě zpracovaných dat z tagu. Pomocí Android Beam™ si začnou zařízení vyměňovat NDEF zprávy, když se dvě fyzická zařízení přiblíží na požadovanou vzdálenost. Tímto způsobem je lehčí si vyměnit data než například s technologií Bluetooth, kdy je nutné zařízení spárovat. Spojení je navázáno hned, jakmile se

zařízení dostanou do minimální požadované vzdálenosti. Takto se například mohou posílat z jednoho zařízení na druhé kontakty či webové stránky. [35]

3.3 Intent

Pro lepší pochopení následující kapitoly Mechanismus zpracování tagu je vhodné čtenáře seznámit s problematikou intentů a co v OS Android vykonávají.

Intenty jsou objekty, které se používají na spuštění akce z jiné komponenty v systému Android. Existují tři základní způsoby užití, které se používají ve spojení s intenty. Spustit aktivitu, kde aktivita představuje jedinou obrazovku v aplikaci. Intent tedy popisuje, kterou aktivitu je třeba spustit a nese v sobě data. Další způsoby použití jsou spuštění služby na pozadí a doručení broadcastové zprávy. Existují dva typy intentu: explicitní, kdy se musí přímo říci, jaká aktivita bude spuštěna nebo implicitní, kdy samotný systém buď vybere vhodnou aktivitu, nebo dá uživateli na výběr. [36]

3.4 Mechanismus zpracování tagu

Když mobilní zařízení s OS Android objeví NFC tag, metodika zpracování se nazývá The Tag Dispatch System neboli mechanismus zpracování tagu. Mobilní zařízení poháněné OS Android obvykle hledá NFC tag, pokud není zařízení uspané a obrazovka není zamknutá. Pokud zařízení objeví NFC tag, zařízení by se mělo zachovat tak, že spustí aplikaci, která souvisí s obsahem NFC tagu, bez optání uživatele. Je to z toho důvodu, jelikož NFC pracuje na velmi krátkou vzdálenost, takže při situaci, kdy by si musel uživatel vybrat aplikaci, kterou chce použít, mohlo by se stát, že s mobilním zařízením pohne do takové vzdálenosti, že čtení již nebude možné a přeruší celou operaci. Aby k tomu nedošlo, mechanismus zpracování tagu analyzuje naskenovaný NFC tag, zpracuje ho a pokusí se přiřadit na základě těchto informací aplikaci. Postup zpracování je následující:

1. Zpracování NFC tagu a zjištění MIME typu nebo URI, které identifikují obsah v tagu
2. Zapouzdření MIME typu nebo URI a jeho obsahu do intentu
3. Spuštění aktivity na základě intentu

NDEF data jsou zapouzdřena uvnitř NdefMessage, která obsahuje jeden nebo více NdefRecord. Když mobilní zařízení s OS Android naskenuje NFC tag, který obsahuje NDEF data, zpracuje zprávu a pokusí se zjistit MIME typ nebo URI. Aby se tak stalo, systém vezme první NdefRecord uvnitř NdefMessage, aby zjistil, jak správně zacházet s celou NDEF zprávou. Správně naformátovaný NdefRecord by měl obsahovat následující položky:

- 3-bitový TNF (Type Name Format)
    - Na základě TNF se určuje Variable length type (viz níže). Validní hodnoty jsou například TNF_EMPTY, TNF_UNKNOWN a TNF_UNCHANGED. Tyto hodnoty jsou mapovány ke spuštění intentu ACTION_TECH_DISCOVERED (popis níže). Dále jsou validní hodnoty, které obsahují URI či MIME typ.
- Variable length type
    - Variable length type popisuje typ záznamu. Pokud je hodnota TNF typu TNF_WELL_KNOWN, tak pomocí tohoto ukazatele se určuje RTD (Record Type Definition). Validní hodnoty RTD mohou být buď Smart Poster, Text, Uri a jiné. Některé hodnoty RTD mohou být namapovány ke spuštění intentu ACTION_TECH_DISCOVERED (popis níže).
- Proměnlivá délka ID (Variable length ID)
    - Jedinečné ID záznamu. Nemusí být vždy použito, slouží pouze pokud má být NFC tag jedinečně identifikován.
- Proměnlivá délka obsahu (Variable length payload)
    - Samotný obsah, který má být přečten nebo zapsán. Jelikož jedna zpráva může obsahovat více záznamů, nemusí být vždy celý obsah v jednom záznamu.

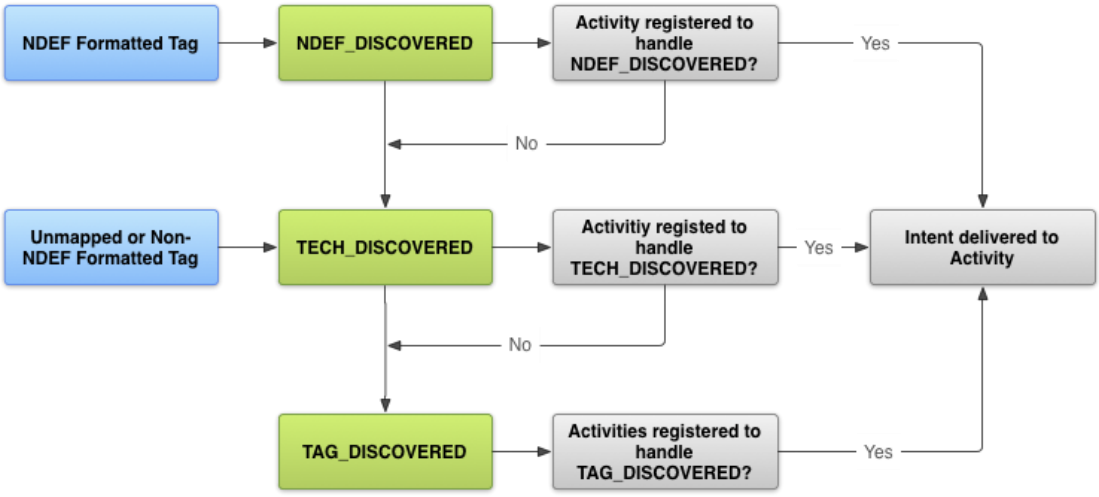
Mechanismus zpracování tagu používá k určení MIME typu nebo URI první dvě položky uvnitř záznamu NDEF zprávy, tedy TNF a typ. Pokud je vše úspěšné, systém zapouzdří informace do ACTION_NDEF_DISCOVERED intentu spolu s obsahem. Pokud systém nemůže určit MIME typ, nebo URI, nebo NFC tag

neobsahuje NDEF zprávu, potom je objekt Tag, který obsahuje obsah a technologie tagu zapouzdřen do ACTION_TECH_DISCOVERED intentu.

Jakmile mechanismus zpracování tagu zapouzdří NFC tag a jeho informace a vytvoří intent, pokusí se pomocí něho spustit správnou aplikaci. Pokud je aplikací víc, objeví se uživateli na výběr seznam těchto aplikací. Mechanismus zpracování tagu může vytvořit následující tři intenty:

- ACTION_NDEF_DISCOVERED
    - Intent ACTION_NDEF_DISCOVERED je používán k spuštění aplikace, pokud je NDEF obsah validní dle tabulek v TNF a typu. Systém se pokouší vždy vyvolat tento intent, kdykoliv je to možné, před následujícími intenty.
- ACTION_TECH_DISCOVERED
    - Pokud NFC tag obsahuje specifické technologie, které nejsou ve formátu NDEF, nebo obsahuje NDEF data, která neobsahují MIME typ nebo URI, je vyvolán intent ACTION_TECH_DISCOVERED.
- ACTION_TAG_DISOVERED
    - Pokud není vyvolán žádný z předešlých dvou intentů, potom je vyvolán intent ACTION_TAG_DISCOVERED.

Kapitola byla zpracována dle [35].



Obr. 7 Diagram mechanismu zpracování tagu
Zdroj: [35]

3.5 Android Application Records

V operačním systému Android 4.0 se objevilo AAR (Android Application Records), které dovoluje vývojáři to, aby po naskenování tagu byla spuštěna určitá aplikace. Uvnitř NDEF záznamu je AAR, který obsahuje jméno balíčku požadované aplikace. Pokud je při skenování NFC tagu objeven AAR záznam, tak se systém pokusí spustit specifikovanou aplikaci, pokud aplikace není na zařízení nainstalována, je spuštěn Google Play a aplikace je nabídnuta k stáhnutí. [35]

4 Praktické využití

V následujících kapitolách jsou vypsané praktické věci, na které bylo naraženo během výzkumu k bakalářské práci, dále je jedna kapitola věnována budoucnosti placení přes mobilní zařízení a jsou zpracovány rozdíly mezi společnostmi Google a Apple. Nakonec je kapitola věnována potenciálnímu využití NFC a jsou představeny různé aplikace, které využívají NFC.

4.1 Test – čtení karet

Na mobilním telefonu Samsung Galaxy S3 bylo testováno jak se NFC chová, pokud má ke čtení více než jeden zdroj. Ke zkoušení byly používány následující tři karty:

- InKartu od Českých drah
- ISIC kartu
- Bezkontaktní platební kartu VISA

Pokud byla přikládána jedna karta po druhé, pomocí náležitých aplikací bylo možné zjistit velké množství informací o kartách, ať už šlo o ID karet, jaká společnost kartu vyrobila, o jaký typ tagu jde nebo o jakou technologii se jedná. Platební karta a InKarta měli zašifrováno více informací než ISIC karta, a proto z nich nešlo vyčíst tolik informací. Přesto pomocí vhodné aplikace – EMV Paycard Reader – šlo z platební karty dostat číslo karty a datum exspirace (pro úspěšnou online platbu potom stačí znát pouze CVC2 kód).

Když se začaly přikládat ke čtečce dvě karty najednou, jedna karta se chovala vždy dominantněji a nezáleželo, jestli byla k telefonu blíže nebo dále. Načtená data ale nikdy nebyla kompletní, načetly se vždy pouze kusé informace. Jako nejdominantnější karta se ukázala ISIC karta, druhá byla platební karta a třetí InKarta. Pokud byla karta přiložena k telefonu předtím, než se v aplikaci zapnulo čtení nového tagu, karta se nenačetla. Když se přiložila další karta, načetly se pouze kusé informace.

Vždy, když se přikládalo více karet současně, čtení fungovalo velmi špatně, většinou to skončilo nezdarem, karty se nenačetly vůbec, nebo čtení vyžadovalo

velkou dávku trpělivosti při pohybování s kartou všemi směry, aby se načetly alespoň nějaké informace.

4.2 Různé NFC čipy v mobilních zařízeních

Při testování různých aplikací, které pracují s NFC, některé karty jedno mobilní zařízení přečetlo a druhé je vůbec nezaznamenalo. Jedná se o problém kompatibility, konkrétně s tagy Mifare Classic 1K. V podstatě všechny telefony s NFC čipem měly čip od firmy NXP, která byla největším výrobcem NFC HW na světě. NXP vyrobila tag Mifare Classic 1K, který byl plně kompatibilní s jejím HW, ovšem ne úplně se držel standardů definovaných NFC fórem. Dokud byly mobilní zařízení vybaveny čipem od NXP, nenastával problém. Problémy odstartovaly, jakmile výrobci mobilních telefonů začali obsazovat do svých telefonů čipy od jiných výrobců. Jedná se například o telefony Samsung Galaxy S4, Samsung Galaxy S5, HTC One M8, LG G2, Nexus 10 a další, které využívají čipy od společnosti Broadcom. Jelikož tag Mifare 1K není navržen přesně dle standardů, dokáže čip od Broadcomu přečíst pouze UID čipu, ale nemůže přečíst nic jiného, natož zapisovat na čip. [37]

4.3 Budoucnost placení přes telefon v České republice

Visa spouští v Evropě bezkontaktní platby. Začíná se na Slovensku, kde Visa umožňuje platby pro klienty VÚB banky. Během roku 2015 by se mělo začít s bezkontaktními platbami i u nás v ČR. Visa má být dle dostupných informací v jednání s několika bankami, které působí na domácím trhu. V ČR sice už jedno placení přes mobil funguje, ale takovým způsobem, že v mobilu je SE uložen na speciální SIM kartě, kterou vydává banka ve spolupráci s mobilním operátorem. Toto řešení provozoval telefonní operátor Telefónica O2 a banka GE Money Bank [38]. Avšak spolupráce již nadále netrvá, nicméně lidé, kteří využívali toto řešení, ho mohou i nadále využívat [39].

Jako první pilotní projekt s bezkontaktními kartami na principu NFC odstartovala Komerční banka v roce 2011 ve spolupráci s Citibank Europe, Globus ČR, Visa a Telefónica O2 Czech Republic. Jednalo se o půlroční pilotní projekt a pomocí UICC karty a podporovaných telefonů šlo platit na 50 pokladnách hypermarketů Globus [40]. Následně přišla v roce 2012 Česká spořitelna a posléze i

Komerční banka s dalším pilotním projektem pro bezkontaktní platby. Jednalo se o bezkontaktní platby pomocí iPhone 4 a iPhone 4S. Přestože tyto mobilní telefony v sobě žádný NFC čip neměli, byli i přesto vybrány pro tento projekt a NFC platby byli možné jen s použitím speciálního rámečku s NFC technologií, který obsahoval i Secure Element [41, 42]. V roce 2012 společnost Komerční banka společně s Telefónica O2 a Visa spustili bezkontaktní platby, které fungovali pomocí UICC karty a podporovaných mobilních telefonů. Nyní ovšem platby nebyly omezeny pouze na Globus, ale dalo se platit všude, kde bylo možné platit bezkontaktně [43]. V roce 2013 spustili pilotní projekt s NFC společnosti T-Mobile, Československá obchodní banka a MasterCard. Šlo o velmi uzavřený pilotní projekt pouze pro 500 lidí. Bezkontaktní platby fungovaly na principu UICC karty [44].

Visa by měla přijít s řešením, že během placení se bude identifikace ověřovat přes vzdálený server. Platební karta se do mobilního zařízení dostane pomocí emulace karet tzv. HCE. Ověřování bude probíhat pomocí speciální aplikace v mobilním telefonu [45]. Společnost MasterCard má již nějaký čas aplikaci MasterCard Mobile. Jedná se o aplikaci, kde se platí pomocí QR kódů. Pomocí této aplikace lze platit u přibližně 2 000 obchodníků v čele se společností Alza, České Dráhy, či například DámeJídlo.cz. V druhé polovině roku 2015 by měla být do aplikace přidána možnost s HCE. Dá se tedy očekávat, že na sklonku roku 2015 budou v České republice fungovat dvě konkurenční řešení, které umožní platit u obchodníků bezkontaktně pomocí mobilních zařízení, a to pomocí HCE [46].

4.4 Přístup firmy Apple k NFC

Šestá generace mobilních telefonů iPhone disponuje technologií NFC. Konkrétně to jsou produkty iPhone 6, iPhone 6 Plus a Apple Watch. I když mobilní přístroje nyní disponují technologií NFC, tak i přesto lze pomocí NFC pouze platit, žádné jiné možnosti Apple zatím nenabízí. Ani vývojáři nemají zatím přístup k NFC čipu, jelikož neexistuje žádné API. Ovšem s prvními hodinkami Apple Watch by mohla přijít změna, jelikož firma dává příklad s hodinkami, jak odemykají pomocí NFC dveře hotelového pokoje. Je tedy možné, že nakonec Apple dovolí vybraným vývojářům vytvářet aplikace s využitím NFC. Ovšem tyto hodinky půjdou na trh v prvním kvartálu roku 2015. [47]

Zatím hlavní a jediné využití NFC v mobilních zařízeních společnosti Apple je placení. Služba placení je nazývána Apple Pay. Pro uchovávání karet a jejich využívání se stará aplikace Passbook. Jelikož má každý uživatel účet na iTunes, kde jsou rovněž uloženy informace o jeho platební kartě, je tato karta v aplikaci Passbook jako výchozí karta pro platby. Platební karty lze do aplikace přidat buď ručním zadáváním, nebo také vyfocením. Výchozí kartu, kterou budou uskutečňovány platby, lze jednoduše v aplikaci změnit. [48]

Placení funguje nejjednodušší možnou cestou, telefon se přiloží k platebnímu terminálu podporující bezkontaktní platby s prstem přiloženým na Touch ID, platba se provede a vibrace a pípnutí dají zákazníkovi vědět, že vše proběhlo v pořádku. Pokud chce zákazník platit jinou kartou, než je výchozí, přiloží telefon k terminálu, bez přiloženého prstu na Touch ID, a aplikace dá uživateli na výběr všechny platební karty, které má k dispozici. Uživatel si poté jenom vybere, kterou kartu chce použít a přiloží prst na Touch ID a platba se provede s vybranou kartou. U Apple Watch bude vše fungovat stejně, jen místo držení prstu na Touch ID se dvakrát stiskne spodní mechanické tlačítko na boku hodinek. [49]

Apple Pay využívá hardwarový SE [48]. Situace je zde jiná než v případě mobilních telefonů, které mají operační systém Android. Apple jako výrobce HW i SW může zapisovat do SE. V telefonech s OS Android to není možné, proto se v OS Android přistoupilo k SE, který je v cloudu. Proto jakmile se přidá jakákoliv bankovní karta do aplikace Passbook, zároveň se vygeneruje unikátní zašifrované číslo, které se uloží právě do SE. Toto číslo je uloženo pouze v telefonu a na serverech společnosti Apple se nikdy neobjeví. Při platbě se používá vygenerované číslo spolu s dynamickým bezpečnostním kódem (pro každou transakci jedinečný), tudíž číslo karty, se kterou se platí, se nikde neobjeví. Záznamy plateb jsou uchovávány pouze pro uživatelovy potřeby v aplikaci Passbook. Apple Pay tuto skutečnost využívá k propagaci své služby tím, že obchodník nemá možnost dozvědět se ani číslo karty, ani PIN. [50]

Dva tablety iPad Air 2 a iPad Mini 3 také umožňují funkci Apple Pay, ovšem pouze pro nákup online či v aplikacích. Tablety obsahují pouze SE, kde jsou uloženy karty, pomocí nichž se platí, ovšem neobsahují NFC anténu. [51]

4.5 Srovnání přístupů firem Apple a Google

Obě dvě konkurenční firmy Apple a Google nyní poskytují placení pomocí mobilních zařízení, u společnosti Apple je to pomocí nových iPhone 6 a iPhone 6 Plus (omezeně lze také platit s Apple Watch – v obchodech a s iPad Air 2 a iPad Mini 3 – v aplikacích a na internetu) a jejich systému Apple Pay. U společnosti Google lze platit všemi mobilními zařízeními, které disponují technologií NFC a mají verzi Androidu minimálně 4.4. Rozdíl je také v tom, že Apple respektive Apple Pay používá HW SE, zato Google Wallet používá cloudový SE. Nyní lze zpozorovat první rozdíl a to ten, že mobilní platby od Google se týkají více uživatelů než ty od Applu. [52]

Služby od Applu fungují pomocí aplikace Passbook, která je předinstalovaná a doteď sloužila jako shromaždiště lístků, voucherů a podobně. Za to do mobilního zařízení s Androidem se musí stáhnout aplikace Google Wallet. Co se ale týká přidávání karet do aplikací, jedná se v podstatě o to samé. Ovšem ne všechny kreditní karty jdou přidat do Apple Pay, musí to být participující banka a karta samotná musí být kompatibilní se systémem Apple Pay. Google Wallet by měl fungovat se všemi kreditními a debetními kartami. [53]

Když se zeměpisně porovná, kde jednotlivé aplikace fungují, žádný vítěz z tohoto porovnání nevzejde. Obě dvě aplikace plně fungují pouze na území USA. Ovšem Google Wallet je na trhu už delší dobu a přitom to je Apple, kdo více mluví o rozšiřování služby do dalších zemí. [52]

Apple při představování svého platebního systému představil partnery, u kterých lze takto platit, byl to např. řetězec fast foodů McDonald's. Ovšem pokud je u těchto partnerů možnost platit pomocí NFC platebního terminálu, půjde tam zaplatit nejenom pomocí Apple Pay, ale i pomocí Google Wallet. [53]

Větší rozdíly nastávají v samotném placení. Zatímco iPhone s Apple Pay stačí přiložit k platebnímu terminálu a přiložit palec na Touch ID senzor a provede se platba, s Google Wallet je to o něco složitější. Je potřeba odemknout peněženku zadáním PIN po přiložení telefonu k terminálu, PIN ale nesmí být ten samý jako je PIN telefonu. Ovšem lze nastavit dobu platnosti PIN na nekonečno, takže lze tento krok se zadáváním PIN přeskočit, avšak tento způsob je nebezpečný např. pokud se mobil ztratí, či ho někdo ukradne. Následně je ještě potřeba potvrdit platbu – u

debetní karty je to PIN kód a u kreditní karty pouze tlačítko Enter a následně se platba provede. [53]

Pokud se vezmou v úvahu všechny klady a zápory, tak hlavně díky jednoduchosti placení v tomto souboji vyhrává Apple se svým Apple Pay. Google Wallet by mohl získat výhodu, pokud by se rozšířil do více zemí či zjednodušil placení. [52]

4.6 Návrh prototypu přístupového systému

Kapitola pojednává o možnosti, jak potenciálně využít přístupový systém do objektů a to tak, že by oprávněné osoby nemuseli přistupovat přes určitou identifikační kartu, ale mohli by přistupovat přes své mobilní zařízení, které podporuje NFC.

V současné době funguje systém otevírání dveří na přístupovou kartu v čím dál více objektech. Nemusí se ovšem jednat pouze o otevírání dveří, může se jednat i o další systémy, kde je potřeba identifikace, jako příklad lze uvést přístup do učitelských stolů v učebnách na UHK.

Čtečky karet fungují na principu RFID, kam se řadí také NFC. Smyslem této kapitoly je zamyslet se nad trochu odlišným přístupem a to pokud by se čtečky karet nahradily mobilním zařízením disponujícím NFC čipem a s OS Android ve verzi nejméně 4.4. Předpokladem je, že by mobilní zařízení byla neustále připojená k internetu a to kvůli tomu, aby vždy měli aktuální databázi oprávněných osob, či např. aby byli schopné odesílat každodenní reporty. Toto by neměl být zásadní problém, jelikož většina komplexů v dnešní době je pokrytá sítí WiFi. To jsou základní požadavky pro fungování systému, tedy mobilní zařízení s verzí OS Android minimálně 4.4 a připojení k internetu.

Následně je nutné mít nějakou aplikaci, která bude umožňovat vlastní přístup. Aplikace by měla umět rozšifrovat data, která čtečka přečte, porovnat s databází, zapsat do logu a následně na základě porovnání otevřít, či nechat zavřené dveře. To je uživatelská část aplikace, potom by musela být administrační část aplikace, pomocí které by se zadávali či mazali údaje z databáze. Aplikace by mohla být propojená například s účetním systémem firmy, kde jsou profily všech zaměstnanců. Při vytváření profilu by si potom aplikace rovnou vzala potřebné údaje a uložila do

databáze. Při přípravě tagů pro nové zaměstnance by se na tag kopírovaly v šifrované podobě jednotlivé řádky databáze. Po ukončení pracovního poměru by se nemuselo ručně rušit oprávnění, ale jméno, jelikož by již dále nebylo zavedené v účetním systému, aplikace by nenalezla záznam v databázi a tak by skončila platnost pro přístup do budovy. Samozřejmostí je i ruční zavedení do aplikace pro lidi, kteří mají přístup do objektů, nicméně nejsou zavedeni v účetním systému, s tím souvisí potom i ruční zrušení oprávnění. Tím, že by se data zaváděla na základě dat z účetního systému, by rovnou mohla být zavedena i různá oprávnění, tedy zaměstnanec vs. údržbář vs. manažer.

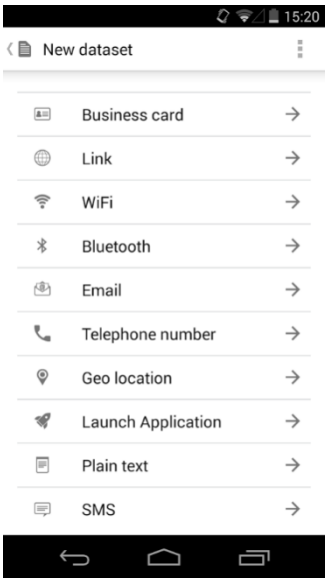
Pracovníkům by se následně rozdali příslušné tagy a celý systém přístupu by měl bez problémů fungovat. Určitě se ale najdou takoví uživatelé, kteří budou mít také mobilní zařízení s NFC a s OS Android ve verzi minimálně 4.0 (kvůli funkci Android Beam). Těmto uživatelům by bylo vhodné poskytnout aplikaci, pomocí které by se přihlásili, a na základě přihlášení by se jim do aplikace stáhly potřebné údaje. Kdyby tedy uživatelé měli zapnutou aplikaci a přiložili mobilní zařízení ke čtečce, pomocí Android Beam by se vyměnily potřebné údaje, na základě kterých by se přístup povolil či nikoliv.

4.7 Praktické využití

Kapitola představí, jak si může běžný uživatel naprogramovat svůj vlastní NFC tag pro jakékoliv vlastní praktické využití. V dnešní době, kdy je NFC relativně hodně rozšířené, je velmi snadné si objednat prázdný NFC tag. Problém nastává v tom, jaký NFC tag si pořídit. Kvůli plné kompatibilitě z nejlepších možností tagy od společnosti Mifare vypadávají. Jelikož všichni zástupci NTAG21x jsou si velmi podobní a liší se pouze v podpoře počítadla a velikosti paměti, pro další porovnávání se v kapitole bude používat pouze NTAG216. Tím pádem uživateli zbývá vybrat si mezi tagy Ultralight, NTAG216 a starším NTAG203. Další parametr, po kterém bude uživatel pátrat, bude samozřejmě cena. Tagy Ultralight a NTAG203 stojí přibližně stejně, proto z porovnávání lze vyřadit tag Ultralight, který je v porovnání parametrů oproti NTAG203 jasně horší. Obyčejný NTAG216 je o jednotky korun dražší. Pokud se vezme pro a proti obou tagů, NTAG203 nemá počítadlo skenů, nelze zaheslovat a vejde se na něj 137 bytů uživatelských informací. NTAG216 naopak počítadlo skenů

má, lze tag zaheslovat a nemusí se trvale uzamknout proti přepsání a lze na něj uložit 888 bytů informací. Proto velmi záleží na situaci, pokud uživatel vystaví NFC tag někde na veřejném místě a ví, že ho nebude přepisovat, nebo pokud bude mít NFC tag doma a bude naopak tag přepisovat často, není zřejmě nutné tag zaheslovat. Dražší NFC tag se tedy hodí pouze v případě, kdy uživatel potřebuje na NFC tag uložit velké množství informací, nebo pokud bude tag umístěn na veřejném prostranství a přesto uživatel bude chtít tag přepisovat.

Pokud má uživatel vybraný tag koupený a disponuje mobilním zařízením s NFC, může se pustit do programování tagu. Velmi dobrý nástroj na programování tagů poskytuje společnost NXP a to aplikaci NFC TagWriter by NXP.



Obr. 8 Ukázka aplikace TagWriter by NXP
Zdroj: [59]

Aplikace kromě čtení tagu umí také vymazání tagu, zabezpečení tagu (buď heslem, nebo uzamknutím tagu), a potom přehledné zapsání informací do tagu. Informace se do tagu dají zapsat buď zkopírováním jednoho tagu a přenesení obsahu do druhého tagu, nebo vytvořením vlastního datového souboru. Lze vytvořit kompletní vizitku, URL link, telefonní číslo, SMS, libovolný text, GPS polohu, email (obsahuje kompletní email – příjemce, předmět zprávy a text zprávy), připojení k WiFi (SSID WiFi, MAC adresa, heslo, typ autentifikace a typ šifrování), Bluetooth k párování, spuštění aplikace (pomocí jména balíčku). Pokud uživatel nepotřebuje

dlouhý libovolný text, e-mail, SMS nebo nemá spoustu informací na vizitce, postačí i starší NFC tag NTAG203.

4.8 Aplikace

Následuje přehled ukázkových aplikací a jejich stručné shrnutí pro ukázku fungování NFC v systému Android.

4.8.1 Google Wallet

V telefonech s operačním systémem Android nižší verze než 4.4, kde byl SE nevyhnutelnou součástí mobilního zařízení, měla přístup do SE pouze aplikace Google Wallet. Peněženka je založena na kooperaci vydavatele platební karty s firmou Google, kdy vydavatel platební karty poskytne Googlu applet, který je nainstalovaný na platební kartě a tento applet je zaveden do SE [54]. Další způsob je emulace virtuální karty, kdy se do aplikace uloží údaje potřebné pro platbu online, tzn. číslo karty, datum exspirace a CVC/CVV kód. Po provedení platby je částka stažena aplikací z účtu. Dalším způsobem, jak používat aplikaci, je virtuální účet, kdy se z účtu do aplikace převedou peníze [54]. Peněženka se neomezuje jen na platební karty, ale je možné do ní naemulovat i karty věrnostní [55]. Pomocí aplikace se potom v obchodě, který vlastní terminál pro bezkontaktní platby, může platit pomocí této aplikace.

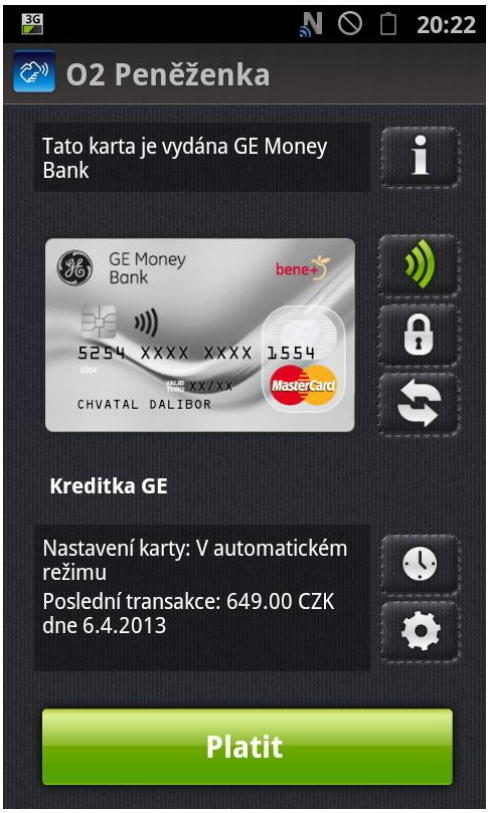
4.8.2 SwipeYours

Nástroj, který slouží pouze k emulování karet Visa a používá protokol Visa MSD. Protokol Visa MSD je protokol, který je používán při bezkontaktních platbách v USA a v Kanadě. K načtení dat je potřeba speciální čtečka, která si načte data z magnetického pásku karty. [56]

4.8.3 Bezkontaktní platby - peněženka

Bezkontaktní platby - peněženka je česká obdoba Google Wallet, tato aplikace vznikla spojením mobilního operátora Telefónica O2, banky GE Money Bank a vydavatele karet MasterCard. Pokud se má tato aplikace plnohodnotně používat, je nutné mít bankovní účet u banky GE Money Bank, pokud je tato podmínka splněna,

zákazník si může zažádat o SIM kartu se SE tedy UICC. Pokud tak udělá, do ruky se mu dostane UICC s nahranou bankovní kartou, tuto speciální SIM kartu potom stačí pouze vložit do mobilního zařízení disponující technologií NFC, aktivovat kartu a bude mít na svém mobilním zařízení zprovozněné bezkontaktní placení. Tato služba již bohužel skončila a nedostává se jí další podpory [38].



Obr. 9 Ukázka aplikace Bezkontaktní platby – peněženka
Zdroj: [57]

4.8.4 NFC Spy

Tato aplikace využívá dva mobilní telefony, z nichž jeden minimálně musí mít OS Android 4.4 a oba dva musí disponovat technologií NFC. Mobilní telefony se spojí pomocí WLAN direkt (WiFi – P2P). Jeden mobilní telefon se potom chová jako čtečka a NFC má ve čtecím režimu a druhý telefon (ten s OS Android 4.4) se chová jako emulovaná karta. Jeden mobilní telefon se poté přiblíží ke čtečce karet a posílá všechna APDU (paket zpracovávaný NFC čtečkou a HCE; více níže) druhému mobilnímu telefonu. Druhý mobilní telefon je u karty a pošle APDU z karty zpět do prvního mobilního telefonu, který data pošle do čtečky karet. Jak komunikace probíhá skrz dva mobilní telefony, tato aplikace zaznamenává všechna APDUs, která

projdou. Emulovány mohou být pouze ISO 14443-A a ISO 7816 karty a to ještě ne všechny, pouze s některými kartami je to možné. Dále aplikace funguje pouze s čtečkami, které jako první pošlou ISO 7816 SELECT NAME/AID příkaz. Je možné, že i když bude vše splněno, i přesto nebude aplikace fungovat, tvůrci navrhují řešení, které představuje nainstalování ROM od CyanogenModu. [58]

4.8.5 NFC TagWriter by NXP

Aplikace, která umí přečíst obsah NFC tagů, přepisovat je, pokud je to možné, importovat a exportovat data z datových souborů, párovat přístroje a další věci. Tato aplikace je vhodná pro každodenní práci s tagy na uživatelské úrovni [59]. Do tagu lze pomocí této aplikace uložit vizitku, URL adresu, ke které lze automaticky přiřadit počítadlo a mirror (princip vysvětlen v kapitole 2.6.2). V aplikaci jde dále nastavit, pro zapsání Bluetooth profil tedy když někdo přiloží své mobilní zařízení k NFC tagu, tak se spáruje Bluetooth. Lze na tag uložit i profil WiFi, to by mohlo být zajímavé například pro restaurace, kdy by jim u vchodu visel NFC tag a návštěvníci by při vchodu do restaurace pouze přiložili své mobilní zařízení k tagu a vytvořil by se jim profil sítě WiFi a následně by se automaticky připojili. V aplikaci jde k zapsání na tag připravit celý e-mail, včetně předpřipraveného předmětu a textu zprávy. Stejně lze vytvořit i SMS a telefonní číslo. Vytvořit lze i textový řetězec nebo GPS polohu. Na tag jde nahrát i to, že po přiložení se spustí určitá aplikace, nebo se odkáže na Google Play a tam jí půjde stáhnout, tuto funkcionalitu umožňuje AAR.

4.8.6 Otevírej Mobilem

Aplikace pochází z České Republiky. Po zakoupení bezkontaktní čtečky a nainstalování aplikace je možné otevírat dveře či garáž mobilním telefonem. U tohoto systém je možné identifikovat majitele mobilního zařízení, který dveře otevíral. Tím pádem tato aplikace neslouží pouze k tomu, aby se otevírali dveře, ale lze ji využít například i jako elektronickou docházku zaměstnanců. [60]

4.8.7 NFC-snadné připojení

Jedná se o aplikaci od firmy Sony a slouží pouze pro její výrobky, které jsou označeny písmenem N. S nainstalovanou aplikací a s mobilním zařízením

disponujícím technologií NFC stačí pouze přiložit zařízení k výrobku a započne proces párování technologie Bluetooth. Tato aplikace slouží k větší pohodlnosti a úspoře času. [61]

5 Emulace karet

Využití emulace karet je velmi zajímavý směr využití mobilního zařízení, neboť toto řešení umožňuje vytvářet řešení, které zahrnuje uživatele, jeho mobilní zařízení a čtečku karet, odpadává tedy velmi zdlouhavé hledání té pravé karty ke konkrétnímu přístupu.

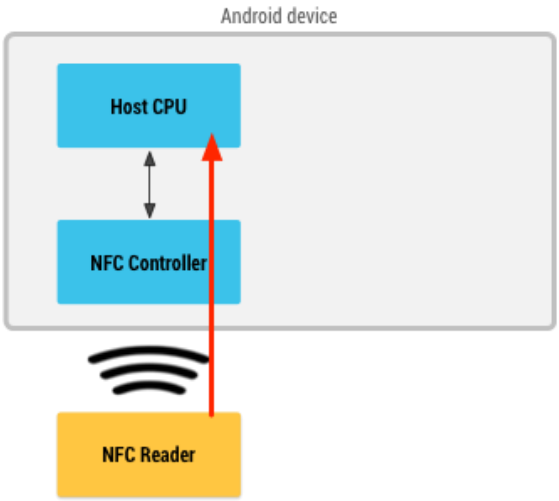
Kapitoly 5.1 až 5.6 jsou zpracovány dle dokumentace OS Android [34].

5.1 Host Card Emulation

Host Card Emulation (dále jen HCE) dovoluje aplikaci systému Android emulovat kartu a následně komunikovat se čtečkou. Tato funkce je v systému Android od verze KitKat tedy 4.4. Funkce HCE je umožněna díky tomu, že nezahrnuje SE.

5.2 Emulace karet

Pokud emulujeme NFC kartu pomocí SE, tak kartu nahrajeme do SE na zařízení pomocí aplikace pro Android. Jakmile uživatel přiloží mobilní zařízení ke čtečce, NFC kontrolér v mobilním zařízení rovnou směruje veškerou komunikaci do SE. Jelikož samotný SE vykonává komunikaci, tak do této operace není zahrnuta žádná aplikace. Aplikace může po skončení komunikace informovat uživatele o úspěchu či neúspěchu.



Obr. 10 Komunikace pomocí HCE
Zdroj: [34]

Pokud emulujeme NFC kartu pomocí HCE, data jsou směrována ne do SE, ale přímo do CPU konkrétního zařízení. Jelikož není komunikace směrována přímo do SE, vše zpracovává aplikace.

5.3 Podporované typy karet pro emulaci

Android 4.4 podporuje několik na trhu běžných protokolů. Tyto protokoly jsou využívány jak na trhu běžnými bezkontaktními kartami, tak i čtečkami těchto karet. Android 4.4 konkrétně podporuje karty, které jsou založené na standardu 14443-4 a zpracovávají APDUs (Application Protocol Data Units), jak je definováno ve standardu 7816/4.

ISO 7816-4: Organizace karet a struktura
ISO 14443-4: Přenosový protokol
ISO 14443-3 typ A: Aktivace a antikolize
ISO 14443-2: Signálové rozhraní rádiové frekvence
ISO 14443-1: Fyzická vrstva

Tabulka 3 Vrstvy protokolu HCE
Zdroj: [34]

5.4 HCE Service

Architektura HCE je postavena na komponentě Service. Jedna z hlavních výhod této komponenty je ta, že může běžet v pozadí bez jakéhokoliv uživatelského rozhraní. Tato funkce je velmi výhodná, pokud jde například o placení či činnosti podobného rázu, kdy uživatel nemusí spouštět žádnou aplikaci, stačí pouze přiložit mobilní zařízení ke čtečce a zařízení spustí správnou službu (nebo vybere již spuštěnou službu) a celá transakce proběhne v pozadí. Pokud je to potřebné, je samozřejmě možné uskutečnit toto i se spuštěnou aplikací.

Když uživatel přiblíží mobilní zařízení ke čtečce, je na systému Android, aby se rozhodl, kterou službu použije, se kterou chce čtečka komunikovat. Zde přichází ke slovu standard 7816-4, který mimo jiné definuje způsob, jak vybrat aplikaci podle Application ID(AID – ID aplikace). AID je složen z 16 bytů, a pokud se jedná o nějakou běžnou službu jako je placení apod., tak AID je známý a registrovaný (například AID

MasterCard A0000000049999). Pokud je potřeba spojit několik AID dohromady, vznikne tzv. AID group (AID skupina), která může být spojena s nějakou určitou kategorií. Všechna AID náleží do jedné HCE služby anebo žádné AID nepatří do jedné HCE služby, neexistuje žádný stav mezi tím.

Pokud je na mobilním zařízení více aplikací, které používají buď stejné AID skupiny, nebo stejné jednotlivé AID, operační systém Android musí vědět jakou aplikaci spustit. Pro co nejpohodlnější obsluhu bezkontaktních operací vykonávaných pomocí mobilního zařízení je nejlepší mít zvolenou defaultní aplikaci, nebo se systém Android začne dotazovat, kterou aplikaci použít a může kvůli manipulaci se zařízením dojít k přerušení celé operace.

5.5 Komunikace

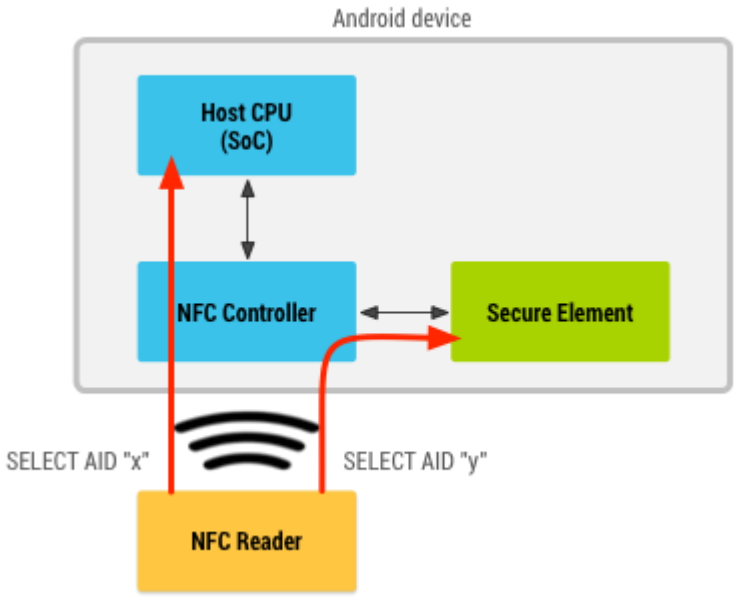
NFC čtečka a mobilní zařízení si mezi sebou vyměňují APDUs. APDUs jsou pakety na úrovni aplikace, které jsou vyměňovány mezi NFC čtečkou a HCE službou. APDUs protokol je pouze half-duplexní, tedy v daný moment pouze jednosměrný. V praxi to znamená, že čtečka pošle APDUs a čeká, než HCE služba odpoví a naopak. Specifikace 7816-4 sice definuje koncept paralelní výměny APDUs na několika oddělených kanálech, ale HCE systému Android podporuje pouze jeden jediný logický kanál. Typické první APDU od čtečky, které dorazí do HCE služby, je „SELECT AID“ APDU. Toto APDU obsahuje konkrétní AID, se kterým chce NFC čtečka komunikovat. Žádoucí chování je to, že po obdržení tohoto dotazu by se měla dostavit odpověď, a to z hlavního vlákna aplikace, které by nemělo být blokováno. Proto je nanejvýš vhodné, pokud nemůže HCE služba vrátit výsledek okamžitě, vracet NULL. Operační systém Android bude neustále předávat data ze čtečky do služby, dokud čtečka nepošle nové „SELECT AID“ APDU, nebo dokud spojení čtečky a mobilního zařízení není přerušeno.

5.6 Spolupráce se Secure Elementem

Může se stát, že mobilní zařízení, které využívá služeb HCE, obsahuje také SE ať už v podobě UICC nebo je SE implementován v mobilním zařízení. HCE operačního systému Android je navrhnut tak, aby dokázal paralelně spolupracovat i s jinými metodami implementace zahrnující použití SE. Této koexistence je

dosaženo díky tzv. AID routování. NFC kontrolér obsahuje routovací tabulku, která obsahuje konečný počet routovacích pravidel. Každé pravidlo obsahuje AID a cílovou destinaci, kde destinace může být buď CPU, nebo SE. Když čtečka karet pošle APDU „SELECT AID“, NFC kontrolér zprávu zpracuje a porovná získaný AID s AIDs z routovací tabulky. Pokud routovací tabulka najde AID, všechny další APDUs budou posílány do určeného místa, dokud není spojení přerušeno nebo nepřijde další „SELECT AID“. Pokud AID není v routovací tabulce nalezen, je použita defaultní routa, která je vždy nastavena do CPU zařízení. Díky tomuto jsou v routovací tabulce vypsány pouze AID, které komunikují se SE.

Routovací tabulku tvoří operační systém Android automaticky, jelikož ví, které AID jsou obsluhovány pomocí HCE, a které jsou obsluhovány pomocí SE.



Obr. 11 Spolupráce HCE se Secure Elementem
Zdroj: [34]

5.7 Potřebný kód pro HCE

Tato kapitola obsahuje fragmenty kódu popsané a převzaté z ukázky práce s HCE. Jedná se hlavně o základní popis toho, jak lze nejjednodušeji pracovat s HCE. Celá kapitola je vypracována na základě ukázky práce s HCE [62].

Při programování aplikace, která má využívat HCE, je potřeba zavést důležité informace do Manifestu. Nejdříve je důležité určit, pro jakou verzi OS Android je aplikace určená – jelikož se jedná o HCE, je potřeba minimální verze 4.4, což odpovídá verzi SDK 19.

```
<uses-sdk
      android:miniSdkVersion="19"
      android:targetSdkVersion="19"/>
```

Následně je nutné definovat, že aplikace bude používat NFC a HCE.

```
<uses-feature
      android:name="android.hardware.nfc.hce"
      android:required="true"/>
<uses-permission
      android:name="android.permission.NFC"/>
```

Dále je potřeba nadefinovat službu pro obsluhu komunikace NFC s terminálem.

```
<service
      android:name=".CardService"
      android:exported="true"
      android:permission=
            "android.permission.BIND_NFC_SERVICE">
```

Poté je potřeba definovat intent filtr pro podporu HCE.

```
<intent-filter>
      <action android:name=
            "android.nfc.cardemulation.action.
            HOST_APDU_SERVICE"/>
      <category android:name=
            "android.intent.category.DEFAULT"/>
</intent-filter>
```

Nakonec přidáme XML soubor, kde jsou uvedené AIDs, pro která karty emulujeme. Tímto definujeme, které protokoly služba emulace karet podporuje.

```
<meta-data
      android:name=
            "android.nfc.cardemulation.host_apdu_service"
      android:resource="@xml/aid_list"/>
```

XML soubor bude obsahovat následující řádky (použitý AID je používán pro věrnostní karty).

```
<aid-group
      android:description="@string/card_title"
      android:category="other">
      <aid-filter
            android:name="F222222222"/>
</aid-group>
```

Předchozími řádky se specifikoval manifest. Další části manifestu se budou odvíjet od toho, čeho se aplikace bude týkat, toto je minimum pro využití HCE v aplikaci. Při vytváření třídy, která bude HCE obsluhovat, se nesmí zapomenout importovat následující třída.

```
import android.nfc.cardemulation.HostApduService;
```

Po importování dalších potřebných tříd, které se budou využívat, je potřeba při definování třídy tuto třídu rozšířit o `HostApduService`. Následně se vytvoří potřebné proměnné.

```
private static final String TAG ="CardService";
```

Přidá se AID pro věrnostní karty.

```
private static final String SAMPLE_LOYALTY_CARD_AID=
      "F222222222";
```

Následuje ISO-DEP příkaz HEADER pro výběr AID.

```
private static final String SELECT_APDU_HEADER
="00A40400";
```

Pokud vše vyjde tak, jak má, tedy APDU sedí, odešle se OK.

```
private static final byte[] SELECT_OK_SW =
      HexStringToByteArray("9000");
```

Pokud APDU nesedí, odešle se UNKNOWN.

```
private static final byte[] UNKNOWN_CMD_SW=
      HexStringToByteArray("0000");
```

Ještě se musí nadefinovat proměnná, do které je vložen AID.

```
private static final byte[] SELECT_APDU=
      BuildSelectApdu(SAMPLE_LOYALTY_CARD_AID);
```

Pokud se nějakým způsobem přeruší spojení mezi čtečkou a kartou, či čtečkou byl vybrán jiný AID, je volána tato metoda, jelikož je potřeba zjistit příčinu přerušení komunikace.

```
@Override
public void onDeactivated(int reason){}
```

Tato metoda je volána, pokud ze čtecího zařízení byl poslán APDU příkaz. Hlavní v této metodě je posílat response APDUs co nejrychleji je to možné, pokud to není možné ihned, tak je lepší poslat null a response APDU později. V podmínce se ověřuje platnost APDU s definovaným AID, pokud vše sedí tak, jak má, odešle se číslo věrnostní karty s potvrzovacím OK. Pokud ne, tak se odešle UNKOWN.

```
public byte[] processCommandApdu(byte[] commandApdu,Bundle
 extras){
        Log.i(TAG,"Received APDU:
             "+ByteArrayToHexString(commandApdu));
        if(Arrays.equals(SELECT_APDU, commandApdu)){
            String account=
                    AccountStorage.GetAccount(this);
            byte[] accountBytes = account.getBytes();
            Log.i(TAG,"Sending account number: "+ account);
            return ConcatArrays(accountBytes,
                    SELECT_OK_SW);
        }else{
            return UNKNOWN_CMD_SW;
        }
    }
```

V této metodě se vytvoří APDU pro zvolené AID. Zde se určí, kterou službou chce čtečka komunikovat. Tuto problematiku řeší standard ISO 7816-4.

```
public static byte[]BuildSelectApdu(String aid){
        returnHexStringToByteArray(SELECT_APDU_HEADER
             +String.format("%02X", aid.length()/2)+ aid);
}
```

Pokud se doplní další vhodné metody, vznikne funkční kód, pomocí kterého mobilní zařízení komunikuje se čtečkou, při komunikaci vypíše např. zprávu apod.

5.8 Porovnání aplikací

V následující kapitole budou porovnány různé přístupy k HCE tří aplikací Bezkontaktní platby – peněženka (dále v textu pouze jako O2 peněženka), Google

Wallet a NFC Spy. Kódy aplikací O2 peněženka a Google Wallet byly získány pomocí webové služby, která umožňuje stáhnout soubor APK. Soubor APK byl dekompilován pomocí nástroje dex2jar do formátu JAR a tento soubor byl dále otevřen v java dekompileru JD-GUI. Bohužel pokud byla aplikace takto dekompilována, Manifest se ztratil, ovšem pokud se otevřel původní APK soubor pomocí dekomprimačního programu 7zip tak se podařilo Manifest dohledat. Nicméně tento Manifest obsahoval spoustu přebytečných znaků i tak byl, ale určitým způsobem čitelný. Kód aplikace NFC Spy je veřejně přístupný.

V případě O2 peněženky nelze mluvit o HCE, neboť je potřeba mít speciální SIM kartu (UICC) vydanou GE Money Bank, která obsahuje platební kartu, dále je potřeba mít jeden z osmi kompatibilních mobilních telefonů značky Samsung, které s aplikací správně spolupracují. Jelikož je zde zvolen tento konkrétní způsob, aplikace neobsahuje část emulace, ale kartu si načte přímo ze SIM karty. Nicméně to, že je karta uložena na SIM, znamená, že se musí řešit přístup přes SE. To znamená také jiný přístup k bezpečnosti, ta zde nehraje prim a ani nemusí vzhledem k tomu, že aplikace komunikuje skrz bezpečný Secure Element.

V aplikaci od Google Wallet lze vidět podobné části jako v aplikaci O2 peněženka. Samozřejmě zde chybí část ohledně Secure Elementu, tu nahradily třídy týkající se cloudu a přibylo velké množství tříd, které řeší kryptografii a třídy, které pracují v rámci HCE. Interface, který zaštiťuje platby, se jmenuje HcePaymentApplet a obsahuje abstraktní metody jako nastavení listeneru, nastavení expirace pinu, čtení záznamu, vypočtení kryptografického součtu a další. Třída WalletHceEventListener, se stará o to, když chce někdo platit a přiloží mobilní zařízení ke čtečce. Z této třídy se volají třídy pro APDU odpověď, pro kontrolní součty, pro šifrovaný přenos, pro zpracovávání odpovědí, pro zápis obchodní transakce apod. K nalezení jsou i třídy pro převod z 16 soustavy do dvojkové a obráceně (slouží k zpracování APDU), třídy obsahující různá AID jako pole bytů, další třídy pro obsluhu HCE atd.

U aplikace NFC Spy je lehce čitelný Manifest, který obsahuje části z předchozí kapitoly, kde je manifest popisován. Kromě XML souboru s AIDs obsahuje složka ještě jeden XML soubor apdu7816.xml, kde je vypsané co které APDU znamená, jakou má hodnotu a o jaký typ tagu se jedná. Ve třídě NfcManager jsou metody pro

práci s NFC, proto zde najdeme metodu, která obstarává objevení karty a poté následuje vytvoření nového intentu, ovšem pouze pokud má mobilní zařízení OS Android minimálně ve verzi 4.4, zjištění ID karty apod. Třída ApduParser zase za pomocí výše zmíněného XML souboru zpracovává informace.

Výše zmíněné aplikace je těžké porovnávat, nicméně každá slouží svému účelu dobře. O2 peněženka jako zkušební projekt v České republice částečně uspěl a v kódu aplikace je vidět, že se vývojáři snažili odvést svou práci dobře. Vývojáři měli ovšem práci lehce ulehčenou o to, že nemuseli řešit kryptografické funkce jako v případě druhé aplikace Google Wallet. Museli ovšem vyřešit komunikaci se Secure Elementem, kterému se věnovalo relativně velké množství tříd. Vývojáři měli mnohem méně práce s komunikací NFC s platebním terminálem. V aplikaci Google Wallet je vidět, že se vývojáři velmi poctivě zaměřili na bezpečnost. Aplikace je doslova plná tříd tvořících různorodé kryptografické služby. Přibyly třídy, které obstarávají cloudové služby. Práce listenerů, které obsluhují NFC čip jsou zvládnuty lépe než v případě O2 peněženky, ale dalo se zřejmě očekávat, že vývojáři Googlu budou mít tuto problematiku lépe zvládnutou. Poslední aplikace NFC Spy neřeší žádné bezpečnostní prvky, neimplementuje složité struktury navíc do listeneru apod. Tato aplikace slouží přesně svému účelu, ke kterému byla stvořena.

6 Shrnutí výsledků

Práce měla za cíl seznámit s problematikou Near Field Communication (NFC), podat základní informace o tom, jak tato technologie funguje, jak se používá v praxi, popsat jednotlivé standardy, naznačit, jak se staví OS Android ke zpracování tagu a seznámit s problematikou emulace karet.

Bylo vysvětleno, jak NFC funguje, vypsáno jeho využití a jaké standardy stanovilo NFC fórum. Byly představeny jednotlivé druhy tagů a byly nastíněny i tagy nové třetí generace. Bylo také představeno, že platby pomocí technologie NFC mají velkou budoucnost a je nutné s nimi počítat jako s důležitým hráčem.

Dále byl představen Secure Element a jeho úloha bezpečnostního prvku. Byl představen formát NDEF, tedy jak mají vypadat zprávy, které se vyměňují během komunikace. Velmi důkladně byl představen mechanismus zpracování tagu a více dopodrobna bylo ukázáno jak vypadá správně naformátovaný NDEF záznam. Bylo také uvedeno, jak lze pomocí AAR záznamu uloženého na tagu spouštět různé aplikace.

Následně bylo představeno, že pokud se ke čtečce přiblíží více jak jeden NFC tag, tak se vždy jeden zachová dominantně a čtečka přečte pouze jeden dominantní tag. Bylo vysvětleno, proč mají určité čipy od společnosti NXP potíže s kompatibilitou s NFC čipy od firmy Broadcom. Dále je predikováno, že v řádech měsíců budou spuštěny bezkontaktní platby pomocí mobilních zařízení s NFC v České republice a to ve spolupráci s Visou. Poté je představen nový bezkontaktní NFC platební systém u společnosti Apple a ten je následně porovnán s NFC platebním systémem od Google. Z tohoto souboje vyšel vítězně nováček na tomto poli a to společnost Apple, hlavně pro jednoduchost placení. Rovněž byl uveden návrh, jak využít NFC při přístupu do objektů, pokud by se nahradili klasické čtečky mobilními telefony. Následně je také popsáno vybrání tagu pro zápis dat, jako nejlepší tag z tohoto porovnávání vyšel NTAG203.

Nakonec byl představen koncept emulace karet a to, jak funguje v systému Android. Jsou vysvětleny problémy spojené s emulací a Secure Elementem. Následuje seznámení se s pojmem AID a s komponentou Service, díky které lze pohodlně například platit, protože je spuštěna stále na pozadí. Následně je

vysvětleno, jak komunikuje NFC čtečka s NFC čipem, a je doporučen vhodný návrh aplikace v tom smyslu, že odpověď na žádosti čtečky by měli putovat vždy z hlavního vlákna a pokud není odpověď k dispozici, tak lepší než čekání je posílání NULL. Také je ukázáno AID routování, díky kterému může v mobilním zařízení koexistovat HCE i SE. Nakonec je rámcově představen nejzákladnější kód pro aplikaci, ve které figuruje HCE a následuje porovnání kódů aplikací.

7 Závěry

NFC je velmi moderní technologie s velkým potencionálem, jsou si toho vědomi i výrobci, a proto lze najít NFC tag už i na prstenu nebo na lahvi od vína. Pro samotnou technologii je toto popularizování určitě velmi žádoucí, neboť čím víc bude technologie NFC nasazováno do běžného světa, tím více bude poptávka po tom, aby bylo NFC v mobilních technologiích. NFC je zřejmě takto úspěšné hlavně z důvodu pohodlnosti, kterou nabízí svým uživatelům. NFC jim dovoluje rychle a bezpečně spoustu operací, se kterými by jinak ztráceli čas. Pouhým dotykem spárují zařízení, připojí se k WiFi, vytisknou fotografii, uloží si kontakt, přenesou data a spoustu dalšího. Velkým přínosem je velká dostupnost NFC tagů, které lze zakoupit v řádech korun. NFC tagy dokáží být velkým přínosem jak v osobním životě (například systém různých profilů – doma, práce, auto…), tak i v komerční sféře (odkaz na jídelní lístek, rychlé připojení k WiFi na veřejném místě…). Největší výzvou, co se týká NFC tagů, je tedy vymyslet co nejoriginálnější způsob jejich použití.

Nejvíce atraktivní v oblasti NFC je v současné době hlavně placení pomocí mobilního zařízení. Je pouze politováníhodné, že největší hráči na trhu se stále drží pouze na území USA, nicméně Apple by toto mohl změnit. V Česku nicméně jeden projekt je ve spolupráci s O2 a GE Money Bank, ovšem projekt evidentně nemá prioritu ani u jedné společnosti, jelikož je ukončen. Ukončení projektu se dotkne všech uživatelů, kteří využívají placení, protože s ukončeným projektem se neaktualizuje ani aplikace, a tak nepodporuje nejnovější verze OS Android. I přesto, že lze platit přes mobilní zařízení, stále to není tak pohodlné řešení jako u Google Wallet nebo Apple Pay. Absenci bezkontaktních plateb v České republice snad vyřeší společnost Visa nebo MasterCard, která by měla přijít s lepším řešením než pomocí UICC a to s HCE.

Když bylo NFC představeno v mobilním telefonu poprvé v roce 2010, lze o NFC v mobilním zařízení mluvit ještě jako o relativně mladé technologii. Jelikož HCE bylo představeno o více než tři roky poté v OS Android 4.4 v září 2013, není zřejmě divu, že v této oblasti je stále minimum aplikací, které by HCE nabízeli. Pokud je řeč o čistém HCE, tedy pokud se přiloží nějaká karta, kterou lze pomocí NFC načíst,

k mobilnímu zařízení, které disponuje NFC, zařízení kartu přečte a následně zařízení vystupuje jako načtená karta, tak taková aplikace není k dispozici. V tomto oboru by šlo provádět další zkoumání a výsledek další práce by mohla být funkční aplikace, která by dokázala provádět výše zmíněnou činnost.

8 Seznam použité literatury

[1] "About the Technology," 2014. [Online]. Available: http://nfc-forum.org/what-is-nfc/about-the-technology/. [Accessed 10 05 2014].

[2] T. M. Martin Rosenberg, „Technologie NFC – popis, bezpečnost a využití," sv. 15, č. 2, 2013.

[3] „A different kind of wireless," [Online]. Available: http://www.nxp.com/techzones/nfc-zone/technology.html. [Přístup získán 19 11 2014].

[4] [Online]. Available: https://www.mojandroid.sk/wp-content/uploads/2013/12/NFC-tag.jpg. [Přístup získán 15 04 2015].

[5] „Co je NFC?," [Online]. Available: http://www.nfctech.cz/co-je-nfc/. [Přístup získán 11 05 2014].

[6] A. Trčálek, „Stačí přiložit: NFC a jeho využití v praxi," Mladá fronta a. s., 14 10 2013. [Online]. Available: http://www.mobilmania.cz/clanky/staci-prilozit-nfc-a-jeho-vyuziti-v-praxi/sc-3-a-1325034/default.aspx. [Přístup získán 11 05 2014].

[7] „NFC," 08 03 2011. [Online]. Available: http://www.nfc.cc/technology/nfc/. [Přístup získán 14 04 2015].

[8] K. T. F. D. Paula Hunter, „Peer-to-Peer Mode," 15 11 2013. [Online]. Available: http://nfc-forum.org/glossary/peer-to-peer-mode/. [Přístup získán 19 11 2014].

[9] „MASTERCARD PAYPASS," [Online]. Available: http://www.mastercard.com/cz/osobni-karty/paypass.html. [Přístup získán 11 05 2014].

[10] „Bezkontaktní platby," Internet Info, s.r.o., [Online]. Available: http://www.mesec.cz/bankovni-ucty/platebni-karty/bezkontaktni-platby/pruvodce/. [Přístup získán 11 05 2014].

[11] K. Korb, „NFC tagy: co jsou vlastně zač a jak fungují?,“ 24net s.r.o., 15 03 2012. [Online]. Available: http://nearfield.cz/clanky/nfc-tagy-co-jsou-vlastne-zac-a-jak-funguji-5. [Přístup získán 11 05 2014].

[12] „NFC in Smart Posters,“ 2014. [Online]. Available: http://www.smartposter.co.uk/what-is-nfc/nfc-in-smart-posters. [Přístup získán 11 05 2014].

[13] K. Korb, „NFC prsten bude: na Kickstarteru se vybralo 240 tisíc liber,“ 24net s.r.o., 27 08 2013. [Online]. Available: http://nearfield.cz/clanky/nfc-prsten-bude-na-kickstarteru-vybral-240-tisic-liber-123. [Přístup získán 11 05 2014].

[14] K. Korb, „Na láhvích vína z Château Le Pin hledejte NFC tagy,“ 24net s.r.o., 14 07 2013. [Online]. Available: http://nearfield.cz/clanky/na-lahvich-vina-z-chteau-le-pin-hledejte-nfc-tagy-113. [Přístup získán 11 05 2014].

[15] [Online]. Available: http://cdn.shopify.com/s/files/1/0112/5592/products/StoreHourse_v05_1024x1024.gif?v=1327476585. [Přístup získán 5 10 2014].

[16] M. P. Jan Pospíšil, „Xperia SmartTags od Sony: jak fungují? (video),“ 24net s.r.o., 12 03 2012. [Online]. Available: http://nearfield.cz/clanky/xperia-smarttags-od-sony-jak-funguji-video-8. [Přístup získán 11 05 2014].

[17] "NFC in Action," 2014. [Online]. Available: http://nfc-forum.org/what-is-nfc/nfc-in-action/. [Accessed 11 05 2014].

[18] „Co je to NFC a co umí?,“ 24net s.r.o., [Online]. Available: http://nearfield.cz/co-je-nfc. [Přístup získán 11 05 2014].

[19] „ISO/IEC 7816-4:2013,“ 4 4 2013. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54550. [Přístup získán 18 11 2014].

[20] „ISO14443,“ 16 12 2012. [Online]. Available: http://nfc-tools.org/index.php?title=ISO14443. [Přístup získán 18 11 2014].

[21] „ISO/IEC 14443-1:2008,“ 19 19 2013. [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39693. [Přístup získán 19 11 2014].

[22] „ISO/IEC 14443-2:2010,“ 10 3 2014. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50941. [Přístup získán 19 11 2014].

[23] „ISO/IEC 14443-3:2011,“ 12 04 2011. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50942. [Přístup získán 19 11 2014].

[24] „ISO/IEC 14443-4:2008,“ 27 10 2014. [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50648. [Přístup získán 19 11 2014].

[25] „Pomoc s výběrem čipu,“ [Online]. Available: http://www.nfcmall.com/cz/t/ChoosetagType. [Přístup získán 31 01 2015].

[26] „The NTAG21x Series Explained,“ [Online]. Available: https://rapidnfc.com/nxp_ntag21x. [Přístup získán 09 04 2015].

[27] M. Chroust, „Samsung informuje o svých nových NFC čipech třetí generace,“ Mladá fronta a. s., 01 12 2014. [Online]. Available: http://samsungmania.mobilmania.cz/bleskovky/samsung-informuje-o-svych-novych-nfc-cipech-treti-generace/sc-310-a-1329033/default.aspx. [Přístup získán 31 01 2015].

[28] „Number of U.S. proximity mobile payment transaction users from 2013 to 2018 (in millions),“ [Online]. Available: http://www.statista.com/statistics/244487/number-of-us-proximity-mobile-payment-transaction-users/. [Přístup získán 01 31 2015].

[29] F. Richter, „How People Use Mobile Payments,“ 02 09 2014. [Online]. Available: http://www.statista.com/chart/2650/mobile-payment-usage/. [Přístup získán 31 01 2015].

[30] F. Richter, „Consumers Wary of Mobile Payment Security,“ 10 09 2014. [Online]. Available: http://www.statista.com/chart/2691/reasons-not-to-use-mobile-payments/. [Přístup získán 31 01 2015].

[31] J. Raphael, „Android Gingerbread: The complete FAQ,“ 06 12 2010. [Online]. Available: http://www.computerworld.com/article/2469757/mobile-apps/android-gingerbread--the-complete-faq.html. [Přístup získán 16 03 2015].

[32] M. P. Kryštof Korb, „Secure element: klíč k mobilním platbám,“ 24net s.r.o., 06 04 2012. [Online]. Available: http://nearfield.cz/clanky/secure-element-klic-k-mobilnim-platbam-20. [Přístup získán 11 05 2014].

[33] S. Clark, "SimplyTapp proposes secure elements in the cloud," 19 09 2012. [Online]. Available: http://www.nfcworld.com/2012/09/19/317966/simplytapp-proposes-secure-elements-in-the-cloud/. [Accessed 11 05 2014].

[34] „Host-based Card Emulation,“ [Online]. Available: https://developer.android.com/guide/topics/connectivity/nfc/hce.html. [Přístup získán 19 11 2014].

[35] „NFC Basics,“ Android, [Online]. Available: https://developer.android.com/guide/topics/connectivity/nfc/nfc.html. [Přístup získán 11 18 2014].

[36] „Intents and Intent Filters,“ Android, [Online]. Available: http://developer.android.com/guide/components/intents-filters.html. [Přístup získán 18 11 2014].

[37] „What NFC Tags do & don't work with the some newer phones and why?,“ [Online]. Available: http://www.andytags.com/nfc-tags-compatibility-issues.html#.VM0WDUeG_TB. [Přístup získán 31 01 2015].

[38] K. Korb, „Platíme mobilem s O2 a GE Money Bank: jak na to?,“ 24net s.r.o., 14 02 2013. [Online]. Available: http://nearfield.cz/clanky/platime-

mobilem-s-o2-a-ge-money-bank-jak-na-to-94. [Přístup získán 11 05 2014].

[39] „Ukončení nabídky Karty v mobilu s GE Money Bank," Platťte bezkontaktně, 10 03 2015. [Online]. Available: http://www.kartavmobilu.cz/news_detail.php?id=25. [Přístup získán 14 04 2015].

[40] „Bezkontaktní mobilní platby v ČR: pilotní projekt odstartuje již v polovině letošního roku," KB, 24 03 2011. [Online]. Available: http://www.kb.cz/cs/o-bance/tiskove-centrum/tiskove-zpravy/bezkontaktni-mobilni-platby-v-cr-pilotni-projekt-odstartuje-jiz-v-polovine-letosniho-roku-1190.shtml. [Přístup získán 14 04 2015].

[41] K. Korb, „iKarta od Komerční banky: v hlavní roli opět iPhone," NearField, 14 08 2012. [Online]. Available: http://nearfield.cz/clanky/ikarta-od-komercni-banky-v-hlavni-roli-opet-iphone-51. [Přístup získán 14 04 2015].

[42] K. Korb, „Česká spořitelna startuje s platbami přes iPhone, zatím pilotně," NearField, 08 08 2014. [Online]. Available: http://nearfield.cz/clanky/ceska-sporitelna-startuje-s-platbami-pres-iphone-zatim-pilotne-50. [Přístup získán 14 04 2015].

[43] M. P. Kryštof Korb, „Je to tady: mobilní NFC platby v ČR pro všechny!," NearField, 23 08 2012. [Online]. Available: http://nearfield.cz/clanky/je-to-tady-mobilni-nfc-platby-pro-vsechny-56. [Přístup získán 14 04 2015].

[44] K. Korb, „Další NFC pilot: tentokrát T-Mobile, ČSOB a MasterCard," NearField, 22 10 2013. [Online]. Available: http://nearfield.cz/clanky/dalsi-nfc-pilot-tentokrat-t-mobile-csob-a-mastercard-127. [Přístup získán 14 04 2015].

[45] J. Láska, „Visa spouští NFC cloudové platby na Slovensku, ČR bude následovat," Mladá fronta a. s., 08 09 2014. [Online]. Available: http://www.mobilmania.cz/bleskovky/visa-spousti-mobilni-cloudove-

platby-na-slovensku-cr-bude-nasledovat/sc-4-a-1328147/default.aspx. [Přístup získán 01 31 2015].

[46] M. Fajmon, „MasterCard spustí NFC platby s aplikací MasterCard Mobile," NearField, 24 02 2015. [Online]. Available: http://nearfield.cz/clanky/mastercard-spusti-nfc-platby-s-aplikaci-mastercard-mobile-175. [Přístup získán 14 04 2015].

[47] C. Martin, „iPhone 6 NFC chip is restricted to ApplePay but may open to developers soon," IDG, 14 09 2014. [Online]. Available: http://www.pcadvisor.co.uk/news/apple/3572112/iphone-6-nfc-chip-is-restricted-applepay/. [Přístup získán 31 01 2015].

[48] K. Korb, „iPhone 6 má konečně NFC a bezkontaktní platby. Umí ale číst tagy?," 24net s.r.o., 09 09 2014. [Online]. Available: http://nearfield.cz/clanky/iphone-6-ma-konecne-nfc-a-bezkontaktni-platby-umi-ale-cist-tagy-155. [Přístup získán 31 01 2015].

[49] „Apple Pay," [Online]. Available: https://www.apple.com/apple-pay/. [Přístup získán 31 01 2015].

[50] „iPhone 6 Apple pay," [Online]. Available: https://www.apple.com/iphone-6/apple-pay/. [Přístup získán 31 01 2015].

[51] J. Kahn, „Source: NFC chip in new iPads just the Secure Element for Apple Pay," 24 10 2014. [Online]. Available: http://9to5mac.com/2014/10/24/nfc-ipad-air-2-secure-element/. [Přístup získán 31 01 2015].

[52] C. Hoffman, „Google Wallet vs. Apple Pay: What You Need to Know," 16 11 2014. [Online]. Available: http://www.howtogeek.com/201870/google-wallet-vs.-apple-pay-what-you-need-to-know/. [Přístup získán 31 01 2015].

[53] N. Lee, „Dabbling in the future of payment: A week of Apple Pay and Google Wallet," 29 10 2014. [Online]. Available:

http://www.engadget.com/2014/10/29/week-apple-pay-google-wallet/. [Přístup získán 31 01 2015].

[54] N. Elenkov, "Exploring Google Wallet using the secure element interface," 27 08 2012. [Online]. Available: http://nelenkov.blogspot.cz/2012/08/exploring-google-wallet-using-secure.html. [Accessed 11 05 2014].

[55] N. Chandler, "What is Google Wallet?," 26 02 2012. [Online]. Available: http://electronics.howstuffworks.com/google-wallet.htm. [Accessed 11 05 2014].

[56] D. Holodov, "SwipeYours," 09 01 2014. [Online]. Available: https://play.google.com/store/apps/details?id=to.noc.android.swipeyours. [Accessed 11 05 2014].

[57] [Online]. Available: http://i.iinfo.cz/images/259/o2-penezenka-ge-money-bank-2.png. [Přístup získán 12 04 2015].

[58] „NFC Spy," 09 09 2014. [Online]. Available: https://play.google.com/store/apps/details?id=com.sinpo.nfcspy. [Přístup získán 09 04 2015].

[59] N. Semiconductors, „NFC TagWriter by NXP," 21 12 2012. [Online]. Available: https://play.google.com/store/apps/details?id=com.nxp.nfc.tagwriter. [Přístup získán 11 05 2014].

[60] „Jak systém funguje a k čemu je připojitelný," 2013. [Online]. Available: http://www.otevirejmobilem.cz/. [Přístup získán 11 05 2014].

[61] S. Corporation, „NFC-snadné připojení," 30 09 2013. [Online]. Available: https://play.google.com/store/apps/details?id=com.sony.easyconnect. [Přístup získán 11 05 2014].

[62] „CardEmulation," 2013. [Online]. Available: https://developer.android.com/samples/CardEmulation/index.html. [Přístup získán 31 01 2015].

FIM UHK
UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Rokitanského 62, 500 03 Hradec Králové, tel: 493 331 111, fax: 493 332 235

Zadání k závěrečné práci

Jméno a příjmení studenta: **Adam Lihm**

Obor studia: Aplikovaná informatika
Jméno a příjmení vedoucího práce: **Pavel Kříž**

Název práce:
Technologie NFC v systému Android

Název práce v AJ:
NFC Technology in Android Operating System

Podtitul práce:

Podtitul práce v AJ:

Cíl práce: Analyzovat současnou využitelnost mobilních zařízení vybavených NFC. Prozkoumat možnosti emulace karet a představit současný stav tohoto problému. Celá problematika je zaměřena především na OS Android.

Osnova práce:
1.) Úvod
2.) Technologie NFC
3.) NFC technologie a OS Android
4.) Emulace karet
5.) Závěr
6.) Bibliografie

Projednáno dne: 14. 10. 14

Podpis studenta

Podpis vedoucího práce