Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Diplomová práce

Vývoj softwaru pro bezkontaktní placení s využitím NFC čipů

Dominik Klodner

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Dominik Klodner

Systémové inženýrství a informatika
Informatika

Název práce

Vývoj softwaru pro bezkontaktní placení s využitím NFC čipů

Název anglicky

Development of software for contactless payment using NFC chips

---

Cíle práce

Cílem diplomové práce je vyhotovení funkčního návrhu a implementace desktopové aplikace pro bezkontaktní platby pomocí NFC čipů určenou primárně pro stánkový prodej. Aplikace by měla eliminovat práci s hotovostí a umožnit tak podnikatelům lepší přehled nad tržbami z prodejů. Dílčím cílem je seznámení čtenáře s problematikou NFC čipů a jejich využití v praxi.

Metodika

Diplomová práce je složena z teoretické a praktické části. Metodika pro zpracování teoretické části zahrnuje studium odborných informačních zdrojů na jejichž základě budou formulována teoretická východiska práce. Teoretická část bude věnována vývoji aplikací a problematice NFC čipů, jejich využití v praxi a při vývoji aplikací.

Praktická část bude spočívat v návrhu a implementaci desktopové aplikace pokladního systému využívajícího NFC čipy na základě poznatků získaných z teoretické části. Při vývoji aplikace bude využito standardních postupů softwarového inženýrství. Desktopová aplikace bude vyvíjena v jazyce C# v prostředí .Net společně s databázovým systémem PostgreSQL. Součástí pokladního systému bude i online přehled v podobě webové aplikace. V závěru práce bude aplikace otestována a budou navrženy případné možnosti jejího dalšího vývoje.

Doporučený rozsah práce

60-80 stran

Klíčová slova

C#, .Net, NFC, bezkontaktní platba, čip, pokladní systém, pokladna, Node.js, RFID

Doporučené zdroje informací

Coskun, V., Ok, K., & Ozdenizci, B. (2012). Near Field Communication From Theory to Practice.

Čápka, David (2020). Největší český C# .NET portál a kompletní on-line kurzy. [online] Itnetwork.cz. Available at: https://www.itnetwork.cz/

Docs.microsoft.com. (2020). Technical documentation, API, and code examples. [online] Available at: https://docs.microsoft.com

Finkenzeller, K., & Müller, D. (2010). RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identificatio and Near-Field Communication.

Mardan, A. (2014). Practical Node.js.

Msdn.microsoft.com. (2020). Learn to Develop with Microsoft Developer Network | MSDN. [online] Available at: https://msdn.microsoft.com/en-us/dn308572.aspx

Troelsen, A., & Japikse, P. (2017). Pro C# 7: With .NET and .NET Core.

Předběžný termín obhajoby

2021/22 ZS – PEF

Vedoucí práce

Ing. Jiří Brožek, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 23. 2. 2021

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 23. 2. 2021

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 31. 03. 2022

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Vývoj softwaru pro bezkontaktní placení s využitím NFC čipů" jsem vypracoval(a) samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor(ka) uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31.3.2022 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Jiřímu Brožkovi, Ph.D. za odborné vedení, dohled a cenné konzultace při psaní této práce.

Vývoj softwaru pro bezkontaktní placení s využitím NFC čipů

Abstrakt

Tato diplomová práce se zaměřuje na možnosti praktického využití NFC technologií a jejich obecnou problematiku v oblasti vývoje softwaru. Jejich nasazení a přínos je demonstrován na aplikaci bezkontaktního cashless NFC pokladního systému, včetně kompletního návrhu určeného výhradně pro festivaly a hromadné akce se stánkovým prodejem. Systém je vyvíjen v programovacím jazyce C# ve spolupráci s .Net a Entity Frameworkem.

Paralelně je vyvíjen multiplatformní systém pro správu pokladního systému a NFC čipů pro webové rozhraní v jazyce Javascript, který je přístupný jak obsluze, tak zákazníkům a poskytuje další rozšíření funkcí pokladního systému.

Veškeré použité technologie a postupy budou podrobně vysvětleny v teoretické části práce a následně použity při vývoji samotné aplikace. Část vlastní práce poté nabídne praktické zkušenosti z oblasti moderního vývoje softwaru a implementací NFC čtecích zařízení pro vlastní programovatelná řešení a automatizaci.

Závěr provází zhodnocení finálního výsledku práce, splnění stanovených cílů a diskuse možných úprav a zlepšení obou systémů z pohledu dalšího vývoje.

Klíčová slova: C#, .Net, NFC, bezkontaktní platba, čip, pokladní systém, pokladna, Node.js, RFID

Development of software for contactless payment using NFC chips

Abstract

This diploma thesis focuses on the practical applications of NFC technologies and their general issues in software development. Their deployment and benefits are demonstrated through the application of a contactless NFC cash register system, including a complete design exclusively for festivals and mass events with stall sales. The system is developed in C# programming language in collaboration with .Net and Entity Framework.

In parallel, a multi-platform system for managing the POS system and NFC chips is being developed for a web interface in Javascript, which is accessible to both operators and customers and provides further extensions to the POS system functionality.

All the technologies and procedures used will be explained in detail in the theoretical part of the thesis and then used in the development of the application itself. The actual work part will then offer practical experience of modern software development and implementation of NFC reader devices for custom programmable solutions and automation.

The conclusion is accompanied by an evaluation of the final result of the thesis, the achievement of the set objectives and a discussion of possible modifications and improvements of both systems in terms of further development.

Keywords: C#, .Net, NFC, contactless payment, chip, POS system, cash register, Node.js, RFID

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

NFC – Near Filed Communication

UID – Unique Identification Number

ISO / IEC – Mezinárodní organizace pro normalizaci a Mezinárodní elektrotechnická komise

HTTP – Hypertext Transfer Protocol

REST – Representational state transfer

CRUD – Create, Read, Update, Delete

NPM – správce balíčků Javasriptu

1 Úvod

Neustále jsme svědky toho, že moderní technologie jsou stále rostoucím trendem napříč různými směry a odvětvími. Pracujeme s nimi v podstatě na denní bázi. Jejich nasazení a implementace dokáže v případě dobře navrženého softwaru přinést mnohá vylepšení z pohledu efektivity práce a automatizace procesů.

To samozřejmě doprovází rostoucí nároky z řad zákazníků na poskytované služby. S vyššími požadavky zákazníků roste úměrně tlak na majitele podniků, kteří musí své služby neustále zlepšovat. Vzhledem k velkému množství dnešní konkurence a celkově poměrně tvrdého konkurenčního prostředí je pro firmu udržení zákazníka stále těžší. Mimo to je podmínka kvality důležitá i z důvodu udržení smluvených kontraktů mezi dodavateli služeb a jejich zadavateli, resp. objednavateli.

To platí i pro dodavatelské firmy poskytující cateringové služby, na které jsou kladeny striktní podmínky přístupu k zákazníkovi. Tato práce se zaměřuje na zdokonalení některých zaběhnutých principů použitím alternativních řešení stávajících postupů a implementací moderních technologií do prostředí festivalů a hromadných akcí pohledem dodavatelů cateringových služeb a stánkového prodeje a nabídnout jim konkrétní řešení na míru v podobě plnohodnotného cashless systému.

Cashless systémy jako takové nejsou úplnou novinkou, ovšem jejich nabídka a reálné nasazení je v praxi velmi omezené. Cashless systém funguje na principu klasických platebních karet, kdy je ovšem možné pro majitele podniku analyzovat prodeje a sbírat statistická data o chování zákazníků, což přináší lepší možnosti plánování a logistiky v průběhu akce. Cashless pokladní systémy mimo jiné omezují práci obsluhy s hotovostí, kdy tak nehrozí její ztráta a odpadá potřeba jejího vracení v případě přeplatku a tvorba manka v pokladně.

Nasazení takového systému přináší také zvýšení kvality nabízené služby dobou nutnou k odbavení zákazníka. Celý proces je v případě kvalitně navrženého systému mnohonásobně rychlejší a efektivnější jak z pohledu obsluhy, tak i zákazníka.

U zákazníků je proti tomu dokázáno, že placení virtuální měnou přináší provozovatelům služeb dlouhodobě vyšší tržby. To je založeno na psychologickém jevu virtuálnosti měny, kdy zákazník své peníze fyzicky nevidí a jsou pro něho snadněji postradatelné, tak také na jednoduchosti uskutečnění transakce a finálního technologického požitku z uskutečněné platby.

2 Cíl práce a metodika

2.1 Cíl práce

Práce zkoumá paradigma bezkontaktních NFC čipů a karet a jejich možnosti užití v praxi ve smyslu automatizace a zefektivnění některých rutinních procesů. Primárně se práce zabývá oblastí elektronických bezkontaktních plateb a cashless systémů.

Cíl práce spočívá v navržení a realizaci pokladního cashless systému, který plnohodnotně nahradí hotovostní platby a implementuje bezkontaktní platební metody za účelem omezení práce obsluhy s hotovostí z důvodu její možné ztráty nebo případného manka v pokladně. Zároveň má systém sloužit jako nástroj pro zvýšení rychlosti odbavení potencionálního zákazníka a sběr důležitých statistických dat pro tvorbu reportů. Systém bude fungovat na principu přednabitého platebního NFC čipu nebo karty a bude koncipován výhradně pro použití na festivalech, veřejných hromadných akcích a místech stánkového prodeje.

2.2 Metodika

Diplomová práce bude rozvržena do dvou částí, a to teoretické části a praktické části. Metodiky pro zpracování teoretické části vychází ze studia odborné literatury a důvěryhodných informačních kanálů. Syntézou zdrojů, na základě získaných poznatků, budou stanovena teoretická východiska z oblasti bezdrátových technologií a bezkontaktních NFC čipů.

Praktická část práce bude vycházet ze získaných poznatků v teoretické části. K dosažení stanovených cílů bude vypracována analýza, zaměřující se na odhalení případných chyb před samotným vývojem obou aplikací, a návrh kompletní struktury s ohledem na vzájemnou kompatibilitu a škálovatelnost aplikací. Při vývoji aplikací budou použity standardní nástroje a metodiky moderního programování a systémového inženýrství. Desktopová aplikace pokladny bude vyvíjena v programovacím jazyce C# s frameworky .Net a Entity Framework. Pro webovou aplikaci bude zvolen programovací jazyk Javasript na straně frontendu i backendu aplikace se serverem Node.js.

Výsledné zhodnocení zváží případná vylepšení a rozšíření aplikace.

3 Teoretická východiska

3.1 Technologie pro bezdrátovou komunikaci

Bezdrátové komunikační technologie měly a stále mají obrovský dopad po celém světě napříč odvětvími. Od průmyslu přes obchod, až po zábavu se stále se rozšiřující základnou zařízení, které ji využívají ke svému provozu nebo jako jakýsi komunikační kanál, kterým mezi sebou jednotlivá zařízení komunikují. Vzhledem k tomu, že se dnes nacházíme v době informací, kterou jinak také můžeme nazývat jako informační věk (popř. věk informací), v níž bezdrátové technologie, společně s informacemi, hrají významnou roli (tj. s přesahem do ekonomie a sociálních vztahů), tak stejně tak tyto technologie hrají dnes významnou roli v běžném každodenním životě a ovlivňují v zásadě téměř vše, co děláme. Od používání našich všudypřítomných smartphonů k hlasovým hovorům, přístupu informací na internetu, nakupování, poslouchání hudby a spousty dalších sofistikovaných užití zejména v oblasti obchodních záměrů a cílů za účelem automatizace a zefektivnění některých rutinních, ale i zdánlivě složitějších procesů, jako například počítání inventur pomocí ručních bezdrátových skenerů nebo používání čteček debetních karet, které komunikují přes mobilní telefonní síť a také mohou číst karty jednoduše tak, že jsou umístěny poblíž zařízení.

Vezmeme-li z kybernetiky model černé skřínky (angl. Black box), kdy není podstatné, jak jednotlivá zařízení detailně fungují na úrovni jednotlivých elektrických obvodů, tak typický komunikační systém se po stránce technického zpracování skládá z vysílačů a přijímačů vzájemně komunikujících pomocí fyzických kanálů. Tímto fyzickým kanálem je myšleno médium spojující vysílač s přijímačem, nejčastěji reprezentováno optickým vláknem, kabelem nebo kroucenou dvoulinkou.

U bezdrátových technologií se v zásadě jedná o přenos, případně výměnu digitálních dat mezi zařízeními či jinými periferiemi, které spolu navzájem komunikují skrze datovou síť bez fyzického spojení těchto periferií tímto fyzickým kanálem (tj. kabelem), tedy bezdrátově. Přenosovým médiem se tak stává vzduch. Při takovéto komunikaci je pro zavedení spolehlivého přenosu důležité plně využít tři základní zdroje bezdrátové komunikace – frekvence, zdroj energie a prostorový zdroj.

Frekvence neboli šířka frekvenčního pásma, je pásmo frekvencí s vymezenou horní a dolní mezí. Je tak třeba zajistit, aby subjekty dosahovaly vzájemné kompatibility v rámci

frekvencí, na kterých komunikují. Zdroj energie udává vysílací výkon a prostorový zdroj má formu náhodných polí vytvořených během toho, kdy se bezdrátový signál šíří prostorovým kanálem s množstvím rozptylovačů v náhodném pohybu směrem k transceiveru. „Používá se několik různých termínů, když se odkazuje na přenosovou rychlost rádiových vln. Samotné elektromagnetické vlny vždy cestují rychlostí světla, 300 000 kilometrů za sekundu. Když se digitální informace přenášejí pomocí rádiových vln, rychlost přenosu se obvykle zobrazuje v bitech za sekundu (b/s), protože primárním problémem je, jak efektivně lze data přesouvat z jednoho místa na druhé.“ (Olenewa, 2016). V České republice je přidělování jednotlivých frekvenčních pásem řízeno Českým telekomunikačním úřadem, který zároveň stanovuje jejich maximální vyzářený výkon.

Pojem bezdrátová komunikace je obecným pojmem sdružující nespočet technologií, které mohou být pro takovýto přenos dat použity. Cílem komunikace, stejně jako u systémů s fyzickým kanálem, je spolehlivý přenos dat z vysílače do cíle.

3.1.1 Historie bezdrátové komunikace

Vývoj bezdrátových technologií není otázkou posledních let. „Bezdrátové sítě tak, jak byly vyvíjeny původně, byly zaměřovány především na oblast komerčního použití pro běžné spotřebitelské aplikace. Využití komerčně běžně dostupných bezdrátových komunikací v průmyslovém prostředí, které klade zvýšené nároky na spolehlivost i na práci v reálném čase, není úplně bezproblémové.“ (Bradáč, a další, 2003).

Obecně se uvádí, že historie bezdrátových technologií se váže až do 60. let 19. století, konkrétně do roku 1865, kdy skotský fyzik James C. Maxwell objevil a matematicky definoval existenci elektromagnetických vln, které se šíří rychlostí světla.

Tato skutečnost Maxwellovy hypotézy o existenci elektromagnetických vln byla experimentálně demonstrována německým fyzikem Henrichem R. Hertzem v roce 1888. S reálným využitím této technologie přišel až Guglielmo Marconi, kterému se podařilo přijímat Morseovu abecedu na rádiové vlně vysílané do přijímače vzdáleného 2,4 km. Tento experiment umožnil vytvořit základní koncept pro bezdrátovou komunikaci v současnosti.

Později byl tento koncept rozvíjen především pro vojenské použití, kdy byly vyvíjeny a vylepšeny různé bezdrátové technologie.

3.1.2 Využití

Vzhledem k dynamickému požadavku na bezdrátový přenos byly po celém světě vyvinuty různé metody a standardy bezdrátové komunikace založené na různých komerčně řízených požadavcích, jako je konkrétní aplikace a dosah přenosu. Tyto technologie lze zhruba rozdělit do čtyř jednotlivých kategorií. Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), Wireless Metropolitan Area Network (WMAN), Wireless Wide Area Network (WWAN). Jak vyplývá z jejich názvů, vlastnosti těchto řešení, pokud jde o rozsah a rychlost přenosu dat, jsou optimalizovány pro osobní, místní, metropolitní nebo celosvětové pokrytí a použití. „Na spodním konci spektra datové rychlosti jsou technologie jako NFC, Bluetooth, Zigbee, radiofrekvenční identifikace (RFID), které nabízejí datové rychlosti v rozmezí několika stovek Kbps nebo méně. Na horním konci jsou technologie, jako je bezdrátové USB, WiFi a ultrawideband (UWB), které mohou nabízet datové rychlosti v rozmezí několika stovek Mbps až několika Gbps.“ (Gupta, 2016).

3.1.3 Používaná pásma pro bezdrátový rádiový přenos

Bezdrátové sítě využívající radiové frekvenční pásma lze rozdělit do několika kategorií podle velikosti a rozsáhlosti sítě. Český telekomunikační úřad vyhraňuje pro radiový přenos kmitočty elektromagnetického vlnění od 9 kHz do 3000 GHz (dle ITU se jedná o 4 – 12 skupinu). „Vlnová délka je nepřímo úměrná frekvenci, což znamená, že když je frekvence vysoká, vlnová délka je krátká a vrcholy jsou blíže k sobě, a když je frekvence nízká, vlnová délka je dlouhá a vrcholy jsou dále od sebe.“ (Olenewa, 2016). Jsou definovány i spektra pro nižší frekvence s větší vlnovou délkou v řádech desetitisíců kilometrů. Sestrojení takové antény by však bylo finančně i konstrukčně velmi náročné.

- **Personal Area Network (PAN / WPAN):**
  Svou rozsáhlostí se jedná o nejmenší typ sítě do několika metrů s relativně malými přenosovými rychlostmi**.** Klasickým zástupcem je například technologie Bluetooth či NFC.

- **Local Area Network (LAN / WLAN)**

  Nejčastější typ sítě, která propojuje zařízení v rámci desítek metrů s vysokými přenosovými rychlostmi, které se pohybují v řádech Mbitů/s až Gbitů/s. U bezdrátových sítí používán výraz WLAN (Wireless Local Area Network). Využívá se nejčastěji pro sítě uvnitř budov. V případě bezdrátových sítí je klasickým zástupcem sítě typu LAN síť Wi-Fi.

- **Metropolitan Area Network (MAN / WMAN)**

  Typ rozsáhlejší sítě, která spojuje zařízení v okruhu několika kilometrů. Koncepcí se v rámci technického provedení podobá LAN sítím. Obdobně jako u sítí LAN může být ke komunikaci mezi zařízeními využita technologie Wi-Fi, případně technologie WiMax.

- **Wide Area Network (WAN / WWAN)**

  Pro bezdrátový typ sítě WAN je vyhraněn výraz WWAN neboli Wireless Wide Area Network. Svou rozlohou jde o nejrozsáhlejší typ bezdrátové sítě. Umožňuje komunikaci v rámci desítek až stovek kilometrů. Je využívána výhradně pro infrastrukturu mobilních sítí.

Rozdělení bezdrátových radiofrekvenčních pásem je základně založeno na typu komercializace. Správu užívaných pásem v České republice řeší Český telekomunikační úřad (ČTÚ), který zároveň pronajímá a vymezuje jejich užívání. Dále také vydává standardy týkající se užívání jednotlivých pásem na území České republiky. Radiofrekvenční spektrum je tak z pohledu komerčního využití rozděleno na licencovaná a bezlicenční pásma.

- **Licencovaná pásma:**

  „Využívání rádiových kmitočtů vymezených všeobecným oprávněním je stanoveno v jednotlivých všeobecných oprávněních. V těchto všeobecných oprávněních jsou stanoveny podmínky, za nichž lze příslušné kmitočty a kmitočtová pásma využívat.“ (Český telekomunikační úřad, 2019). Licencované pásmo je Českým telekomunikačním úřadem nabízeno formou nájmu. Cena za pronájem je individuální a

odvíjí se od jednotlivých vlastností konkrétního pásma. Obecně však platí, že se nejedná o levnou záležitost. Mnohdy je přidělování oprávnění k pronájmu realizováno na základě výběrového řízení formou aukce. Nájemci je v případě udělení oprávnění poskytnuto výhradní právo provozovat a užívat licenční pásmo a garantována čistota komunikačního kanálu bez rušivých elementů způsobující nestabilitu frekvenčního spektra.

- **Bezlicenční pásma:**
  Do bezlicenčních pásem jsou zahrnuta všechna frekvenční spektra, jejichž užívání není podmíněno vlastnictvím licence. Není tak zde ovšem garance výhradního užití a čistoty komunikačního kanálu. Vzhledem k tomu, že jsou volně dostupná, jsou tato pásma naopak mnohem více vytížena a může zde docházet k vzájemné kolizi signálů.

Dle Mezinárodní komunikační unie (ITU) pro rozvoj komunikačních technologií jsou bezdrátová pásma rozdělena do několika skupin a kategorií.

ITU skupina	Kategorie	Frekvenční pásmo	Vlnová délka
4	VLF	3 – 30 kHz	10 – 100 km
5	LF	30 – 300 kHz	1 – 10 km
6	MF	300 – 3000 kHz	100 – 1000 m
7	HF	3 – 30 MHz	10 – 100 m
8	VHF	30 – 300 MHz	1 – 10 m
9	UHF	300 – 3000 MHz	10 – 100 cm
10	SHF	3 – 30 GHz	1 – 10 cm
11	EHF	30 – 300 GHz	1 – 10 mm
12	THF	300 – 3000 GHz	0,1 – 1 mm

Tabulka 1 - Bezdrátová pásma dle ITU

3.1.4 Přehled bezdrátových technologií a standardů

- **NFC (WPAN – Near Field Communication):** Nabízí nízkorychlostní připojení s jednoduchým nastavením a nízkou spotřebou energie, které lze použít k zavedení chytřejších bezdrátových připojení. Zařízení NFC se používají v bezkontaktních

platebních systémech, sociálních sítích, jako je sdílení kontaktů, fotografií, videí nebo souborů.

- **RFID (WPAN – IEEE 802.15):** Radio Frequency Identification (RFID) je bezkontaktní technologie využívající rádiové vlny ke čtení a snímání informací digitálně uložených na značce připojené k objektu. Jedná se o vyhrazenou komunikaci na krátkou vzdálenost.
- **Bluetooth (WPAN – IEEE 802.15.1):** Bluetooth používá technologii WPAN pro bezdrátovou výměnu dat na krátké vzdálenosti. Používá se pro mobilní telefony, sluchátka, osobní počítače, počítačové periferie a spoustu dalších elektronických zařízení.
- **Zigbee (WPAN – IEEE 802.15.4):** Jedná se o bezdrátovou ad-hoc síť s nízkou spotřebou, nízkou rychlostí přenosu dat a těsnou blízkostí. Implementuje komunikační protokoly k vytváření sítí nízkého dosahu s malými digitálními rádii s nízkým výkonem, například pro domácí automatizaci, senzory, sběr dat zdravotnických zařízení a další potřeby s nízkou šířkou pásma a nízkou spotřebou.
- **Z-Wave (WPAN – vlastní standard):** Z-Wave je bezdrátová vysokofrekvenční technologie, která umožňuje inteligentním zařízením vzájemně komunikovat. Z-Wave jsou určeny pro zařízení v domácnosti, jako jsou chytrá světla, dveřní zámky a termostaty atd. Používá se především v aplikacích pro automatizaci domů nebo budov.
- **WiFi (WLAN – IEEE 802.11):** Wi-Fi umožňuje uživateli získat přístup k internetu kdekoli v daném místě, jako jsou hotely, knihovny, vysoké školy, univerzity, kampusy, soukromé instituty, kavárny, a dokonce i na veřejném místě. Wi-Fi umožňuje připojení více zařízení, například počítačů, telefonů, tiskáren atd.
- **LoRa (LPWAN):** LoRa je protokol LoRaWAN, otevřený standard pro zabezpečené připojení. Jedná se o standard s dlouhým dosahem, nízkou spotřebou a nízkou přenosovou rychlostí, určený pro bateriová zařízení pro sítě M2M a IoT. Jedná se o nejvíce převládající technologickou volbu pro budování sítí IoT na celém světě.
- **Sigfox (LPWAN):** Podobný LoRa, ale neotevřený. Bezdrátová síť určená k připojení nízkoenergetických zařízení v ultra úzkém pásmu, zejména pro aplikace IoT napájené z baterie.
- **Mobilní (WWAN – IEEE 802.16):** Bezdrátová technologie používaná pro mobilními telefony, využívá vysokofrekvenční pásma, aby umožnila komplexní obousměrnou

komunikaci. Využívá několik malých bodů umístěných na široké zeměpisné ploše, které jsou vzájemně propojeny prostřednictvím centrální ústředny a tvoří WWAN.

3.2 NFC

Historicky byly systémy založené na kartách s magnetickým pruhem. Tyto karty vyžadovaly, aby uživatel pro vykonání akce přejel kartou přes magnetickou čtečku. Tato technologie měla řadu nevýhod, včetně faktoru nepohodlí, vysoké míry opotřebení a velmi nízké bezpečnosti. Právě tyto nevýhody vedly k vývoji bezkontaktní bezdotykové technologie umožňující čtení karet bez fyzického kontaktu se čtečkou.

„Koncept NFC je navržen na základě synergie několika technologií, včetně bezdrátové komunikace, mobilních zařízení, mobilních aplikací a čipových karet.“ (Coskun, a další, 2012). NFC je kombinace bezkontaktních komunikačních technologií, resp. protokolů umožňujících přenos a výměnu dat mezi dvěma subjekty na krátké vzdálenosti s teoretickým dosahem až 20 cm. Reálná vzdálenost pro úspěšný přenos dat se pak pohybuje někde okolo 5 cm. U NFC je v přijímači i vysílači aplikována smyčková indukční cívka, která využívá pouze malou část vlny, jejíž vlnová délka je 22 m.

Technologie NFC umožňuje komunikaci buď mezi dvěma aktivními prvky (např. komunikace mezi dvěma mobilními telefony s podporou NFC) nebo mezi jedním aktivním a pasivním prvkem (např. NFC čtečka a NFC tag). Svým obecným principem je velice podobný čárovým kódům nebo QR kódům. Z technologického pohledu se ovšem jedná o zcela jiné řešení. Komunikace je realizována pomocí elektromagnetických vln, kdy mezi anténami zařízení vzniká elektromagnetické pole. K přenosu a výměně dat mezi zařízeními s podporou NFC technologie je využíváno nelicencovaného pásma 13,56 MHz. Vzhledem k tomu, že v případě NFC se jedná o bezpečnější verzi starší technologie RFID, která je dnes již ve velké míře zastoupena právě NFC technologií, je NFC díky použité frekvenci a standardům s RFID technologií zpětně kompatibilní.

3.2.1 Přenos dat

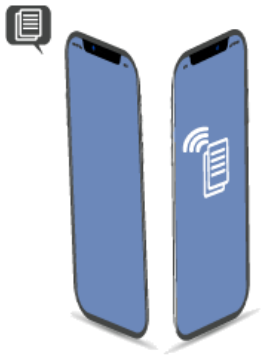
„Komunikace probíhá v oboustranném poloduplexním režimu, což znamená, že komunikující zařízení mohou odesílat a přijímat kdykoli, ale ne obojí současně. Aby se zabránilo kolizím, musí každé zařízení předtím, než začne vysílat, nejprve ověřit, že žádné jiné zařízení již nevysílá na nosné frekvenci.“ (Rankl, a další, 2010). Vždy je k dispozici

pouze jediný kanál na frekvenci 13,56 MHz a jedno ze zařízení musí fungovat jako iniciátor který naslouchá na příslušném přenosovém kanálu a druhé zařízení jako cíl, který na základě standardů zpětně odpovídá na požadavky iniciátora.

Přenos dat skrze technologii NFC má základně 3 pracovní režimy, které definují hlavní případy použití NFC. Tyto režimy výrazně odlišují NFC od jiných typů bezdrátových technologií.

1. Peer to peer

Režim peer to peer (P2P) je jedním ze tří režimů přenosu dat, který podporuje místní obousměrnou komunikaci mezi dvěma aktivními zařízeními s podporou NFC technologie. Je vytvořen bezdrátový komunikační kanál krátké vzdálenosti, který primárně slouží k přenosu malých dat (např. kontaktů, webových URL atd.). „Peer-to-peer přenosy se opírají o NFC protokol Simple NDEF Exchange Protocol (SNEP). SNEP je protokol požadavku a odpovědi: iniciátor pošle požadavek na druh dat, který by si chtěl vyměnit, a cíl odpoví požadovanými daty. SNEP se zakládá na protokolu NFC Forum Logical Link Control Protocol (LLCP).“ (Igoe, a další, 2014).

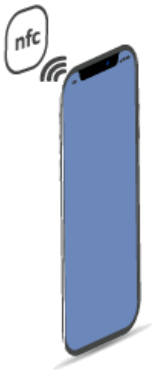


Obrázek 1 - NFC komunikace Peer to peer

2. Reader / Writer

Tento provozní režim umožňuje aplikacím přenášet nebo zapisovat digitální data nezabezpečeným způsobem a interagovat s různými informačními zdroji přiblížením aktivní jednotky k pasivní. Zařízení s podporou NFC pracuje jako aktivní zařízení (např. mobilní telefon nebo NFC čtečka). Jedná se o zařízení, která mají možnost napájení a dokáží vytvářet elektromagnetické pole a napájet pasivní tagy. Tyto tagy neobsahují vlastní zdroj energie a musí být napájeny aktivním médiem. Zpravidla obsahují uložené datové údaje například pro identifikaci jména, URL adresu, elektronickou vizitku atd. Přiblížením

aktivního čtecího nebo zapisovacího média se vytvoří elektromagnetické pole, které vyvine dostatek energie pro aktivaci pasivního prvku a navázání komunikace. Následně probíhá samotný přenos dat skrze radiové vlny na frekvenci 13,56 MHz.



Obrázek 2 - NFC komunikace Reader / Writer

3. Card Emulation

V tomto provozním režimu může mobilní telefon s NFC emulovat bezkontaktní kartu, například pro nákup zboží, služeb, pro přístup ke službám na veřejných místech, například veřejné dopravě. Mobilní telefony s NFC tak mohou komunikovat s prodejními pokladními místy, automaty na lístky nebo jakýmkoli jiným objektem s NFC. Aktuálně se jedná o nejrozšířenější režim, kdy lze využít stávající zařízení založených na technologii RFID.

Tento režim, ačkoli se chová jako tradiční bezkontaktní čip nebo karta, může jít v případě identifikace, autorizace nebo ukládání dat nad rámec funkcí tradičních bezkontaktních karet. Toho lze dosáhnout především pomocí mobilních telefonů s podporou NFC. Například načtené informace lze zobrazit na obrazovce mobilního telefonu a lze požadovat ověření uživatele.

Obrázek 3 - NFC komunikace Card Emulation

3.2.2 Normy

„Není v podstatě možné vytvořit technologii, kterou může používat každý, aniž by se vytvořili standardy, které tuto technologii řídí. Standardy jsou pravidla, která se každý výrobce zavazuje dodržovat, aby byla zajištěna vzájemná kompatibilita zařízení různých výrobců. Standard obsahuje přesnou sadu pravidel a omezení pro implementaci výrobku. V případě bezdrátových technologií by například mohl definovat jaká frekvence bude použita pro komunikaci, kolik energie by zařízení mělo generovat, aby byl signál dostatečně silný atd.“ (Sabella, a další, 2016).

Standardy navíc podléhají organizacím, které je vytváří a skupinám, které je certifikují. V případě NFC je hlavní skupinou norem NFC Forum. NFC Forum postavilo svou specifikaci pro NFC technologii na standardech organizací ISO / IEC, které spolu často vytvářejí, propagují, certifikují a spravují standardy. Je důležité si uvědomit, že standardy řídí pouze problémy týkající se technologie, nikoli prvků, které by prodejce mohl využít pro individualizaci konkrétního produktu. NFC standardy tak například neuvádí přesnou velikost paměti nebo konkrétní barvu produktu. Soustředí se pouze na důležité části technologie v rámci inovací a funkcionality.

Někteří prodejci vyrábějí a nasazují do provozu nestandardní a proprietární NFC, která nejsou v technickém souladu s žádným standardem NFC Forum. Tyto produkty většinou fungují a vypadají jako klasické NFC, ale ve skutečnosti používají jako základní technologii vysokofrekvenční RFID technologii (HF RFID). Jedním z důvodů je také fakt, že v době, kdy na trh přišli první NFC technologie, tak standardy, které se dnes běžně používají ještě nebyly připraveny. Dobrým příkladem proprietární použití jsou např. přístupové karty do budov od společnosti HID Global, které nejsou standardizovány v rámci norem NFC. To mimo jiné společnosti umožňuje vlastní správu zabezpečení svých produktů.

Klasicky jsou pro NFC technologii využívány základní standardy ISO / IEC (ISO / IEC 14443 a ISO / IEC 18000-3) pro identifikační a bezpečnostní karty komunikující na frekvenci 13,56 MHz. „Řada norem ISO / IEC 14443 má umožnit provoz bezdotykových karet za přítomnosti jiných bezkontaktních karet nebo předmětů vyhovujících řadě norem ISO / IEC 10536 a řadě norem ISO / IEC 15693 a komunikaci v blízkém poli (NFC) zařízení vyhovující ISO / IEC 18092 a ISO / IEC 21481.“ (ISO / IEC, 2018). Standard ISO / IEC 14443 je následně ještě rozšířen o standard ISO / IEC 18092 pro peer-to-peer

komunikaci dvou zařízení. Japonský standard JIS 6319-4 je dalším standardem užívaným pro bezdrátové NFC technologie, který ovšem nebyl přijat jako přípustná varianta ISO / IEC 14443. NFC Forum slučuje normy ISO / IEC 14443, JIS 6319-4 a ISO / IEC 18092 do jediného interoperabilního digitálního protokolu, který ke komunikaci využívá jednotné rozhraní.

Norma ISO / IEC 14443 se celkově skládá ze čtyř částí, které definují jednotlivé části pravidel standardu a jeho funkční vlastnosti NFC technologie.

- **ISO / IEC 14443-1: 2008 Část 1: Fyzikální vlastnosti:**
  Určuje, jak jsou karty fyzicky sestaveny. Standard pojednává o dvou typech karet: identifikační karty vyhovující ISO / IEC 7810 a tenké, flexibilní karty vyhovující ISO / IEC 15457-1. Norma však také počítá s tím, že se technologie může objevit v jiných formách.

- **ISO / IEC 14443-2: 2010 Část 2: Vysokofrekvenční výkonové a signální rozhraní:**
  Určuje vlastnosti elektromagnetických polí používaných k zajištění energetické a obousměrné komunikace mezi bezdotykovými spojovacími zařízeními (PCD) a bezdotykovými kartami nebo objekty (PICC). Tato specifikace neurčuje prostředky použité ke generování pole. Karty typu A, B a FeliCa používají různé modulační metody a kódovací schémata.

- **ISO / IEC 14443-3: 2011 Část 3: Inicializace a ochrana proti kolizi:**
  Definuje, jak komunikační proces začíná, pokračuje a končí. Například tato část standardu popisuje, jak zařízení dotazuje a hledá potenciální připojení a poté iniciuje příkaz k zahájení komunikace. Karty typu A, B a FeliCa používají různé postupy inicializace protokolu.

- **ISO / IEC 14443-4: 2008 Část 4: Přenosový protokol:**
  Definuje protokol zpráv, který se má použít pro komunikaci s bezdotykovými kartami. Například tato část popisuje formát zprávy, který by se použil ke čtení dat z karty nebo k zápisu dat na kartu. Stejný protokol pro zasílání zpráv platí pro karty typu A i B. FeliCa používá jiný protokol definovaný ve standardu JIS 6319-4.

Norma ISO / IEC 18000-3 pro bezdrátový přenos NFC definuje požadavky radiofrekvenční identifikace (RFID) na frekvenci 13,56 MHz. Tato norma definuje tři provozní režimy. Režimy vzájemně nespolupracují, ani se vzájemně neovlivňují. Každý režim definuje různé rychlostní charakteristiky pro přenos dat mezi zařízeními pomocí různých technik kódování signálu.

Norma JIS 6319-4 byla původně navržena jako doplněk ISO / IEC 14443 (typ C), ale byla zamítnuta asociací pro vydávání standardů ISO / IEC. Jedná se o standard společnosti Sony, který reguluje japonská rada JICSAP. Je užívána u karet a tagů typu FeliCa.

Aby bylo možné vytvořit kompletní řešení, musí výrobce zařízení NFC podporovat všechny typy značek (označovány také jako tagy): ISO / IEC 14443 typ A, ISO / IEC 14443 typ B a FeliCa.

- **ISO / IEC 14443 typu A**

  Norma ISO / IEC 14443 definuje značky typu A, které se používají ve třech různých typech značek NFC. Z pohledu norem ISO / IEC 14443 má značka typu A následující vlastnosti:

  Rychlost komunikace: 106 kb/s, 212 kb/s a 424 kb/s

  Kódování: 100 % ASK, Manchester Encoding

- **ISO / IEC 14443 typu B**

  Značky ISO / IEC 14443 typu B fungují podobně jako značky typu A. Rozdíl mezi značkou typu A a značkou typu B sestává z modulace a použitého kódování. Značka typu B používá kódování 10 % ASK, Non-Return to Zero.

- **FeliCa (JIS 6319-4)**

  Typ značky FeliCa je japonský standard, který se ve velké míře používá v Japonsku a dalších asijských zemích. Tato značka je často označována jako značka NFC typu 3. Standard JIS 6319-4 definuje tyto vlastnosti pro značku FeliCa:

  Rychlost komunikace: 212 kb/s a 424 kb/s

  Kódování: 8-30 % ASK, Manchester Encoding

3.2.3 Typy čipů

Současné standardy NFC zároveň popisují základní vlastnosti pasivních tagů pro komunikaci se čtecími zařízeními. Každý typ tagu má svou speciální funkci, která umožňuje tagy využívat pro různé účely. „Tagy NFC Forum jsou bezkontaktní čipové karty hostující takzvanou zprávu NDEF definovanou specifikací NFC Forum. Fórum NFC aktuálně definovalo pět různých typů tagů, které umožňují použití mnoha různých existujících implementací čipových karet jako značky NFC Forum. Tyto různé typy tagů se liší podle základního komunikačního protokolu a datové struktury pro ukládání zpráv NDEF, ale výsledné celkové chování tagů NFC Forum je stejné.“ (NFC Forum, 2019). Těchto pět typů podléhá používaným standardům NFC a je tak zaručena kompatibilita s čtecími zařízeními NFC.

- **Tag typu 1**

  NFC tag typu 1 je základní a nejjednodušší z aktuálně dostupných NFC tagů. Podléhá standardu ISO / IEC 14443. Zároveň se jedná o nejpomalejší typ čipu. Pro svou jednoduchost a funkční vlastnosti je cena tagu tohoto typu velmi nízká. Z pohledu funkčních vlastností má tag typu 1 následující specifikace:

  Standard: ISO-14443A

  Velikost paměti: 96 bajtů

  Rychlost: 106 kb/s

  Přístup k datům: Čtení / zápis nebo pouze ke čtení

  Kolizní mechanismus: Ne

  Obvykle je tento typ tagů využíván pro jednorázové užití, aplikace pro čtení, vizitky, párování zařízení s Bluetooth atd.

- **Tag typu 2**

  Tagy typu 2 bývají nejoblíbenější variantou pro běžné užívání díky svému nejlepšímu poměru ceny a výkonu. Z pohledu funkčních vlastností má tag typu 2 následující specifikace:

  Standard: ISO-14443A

  Velikost paměti: 48 bajtů / 144 bajtů

  Rychlost: 106 kb/s

Přístup k datům: Čtení / zápis nebo pouze ke čtení

Kolizní mechanismus: Ano

Obvykle je tento typ tagů využíván pro nízko-nákladové transakce, vstupenky na akce, URL přesměrování, přechodné průkazy atd.

- **Tag typu 3**

  Jako jediný typ tagu nepodléhá klasickému standardu ISO 14443, nýbrž se spoléhá na japonský standard JIS 6319-4 pro tagy FeliCa. Jedná se o tagy, které poskytují širokou škálu funkcí, ale využívány jsou především pro japonský trh i vzhledem k ceně, která je oproti ostatním typům tagů vyšší.

  Standard: ISO-18092, JIS 6319-4

  Velikost paměti: 1 / 4 / 9 kb

  Rychlost: 212 nebo 424 kb/s

  Přístup k datům: Čtení / zápis nebo pouze ke čtení

  Kolizní mechanismus: Ano

  Obvykle je tento typ tagů využíván pro elektronické průkazy totožnosti, členské a věrnostní karty, platební karty atd.

- **Tag typu 4**

  Tagy typu 4 nabízí největší paměť a největší flexibilitu ze všech typů tagů. Jsou koncipovány v rámci standardů ISO-14443A i ISO-14443B. Disponují vysokou mírou zabezpečení splňující normu ISO / IEC 7816. Tagy jsou konfigurovány již při výrobě a dovolují vlastní přizpůsobení obsahu NDEF.

  Standard: ISO-14443A a ISO-14443B

  Velikost paměti: 4 / 32 kb

  Rychlost: 106 / 212 / 424 kb/s

  Přístup k datům: Čtení / zápis nebo pouze ke čtení

  Kolizní mechanismus: Ano

  Obvykle je tento typ tagů využíván pro platby a zabezpečení.

- **Tag typu 5**

  Tento typ tagu je nejmladší z celého souboru používaných tagů. Jeho specifikace vznikla v roce 2015 a odpovídá specifikaci protokolu pro RFID čipy ISO-15693, primárně z důvodu podpory aktivní komunikace a vyšší čtecí vzdálenosti.

  Standard: ISO-14443A, MF1 IC S50

  Velikost paměti: 192 / 768 / 3584 bajtů

  Rychlost: 106 kb/s

  Přístup k datům: Čtení / zápis nebo pouze ke čtení

  Kolizní mechanismus: Ano

3.2.4 NDEF

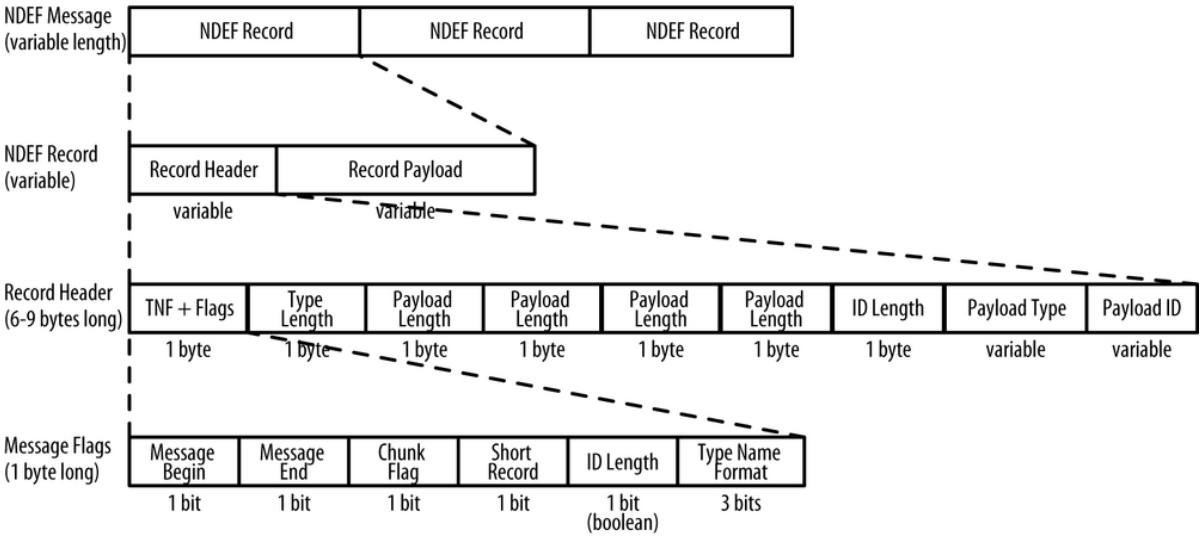
Aby bylo možné číst data mezi jednotlivými platformami, byl zároveň se standardy pro komunikaci skrze NFC představen nový datový formát NDEF (NFC Data Exchange Format). NDEF formát dat představuje předpis pro normalizovanou strukturu přenášených dat. NDEF formát podporují všechny standardizované tagy. U proprietárních tagů není podpora garantována.

„Dříve zavedené standardy pro přenos dat pomocí RFID podporovaly pouze přenos identifikačních dat (URI – Uniform Resource Identifier nebo znaky z ASCII tabulky). Proto byl zaveden rozšiřující standard pro přenos jakýchkoliv dat pomocí technologie NFC. S tím přišla organizace NFC fórum, která specifikovala datový formát NDEF (NFC Data Exchange Format). NDEF tedy definuje formát zapouzdření zpráv pro výměnu dat mezi NFC zařízeními.“ (Rosenberg, a další, 2013). Zpráva (message) poskytuje standardizovanou metodu pro NFC čtecí zařízení. Každá zpráva může být následně rozdělena do několika záznamů (record). Každý z těchto záznamů se dále skládá z hlavičky (header), která obsahuje metadata záznamu jako ID záznamů, délku, typ atd. a datového obsahu (payload), který obsahuje uložená odesílaná data. Kompletní soubor těchto záznamů tvoří výslednou zprávu.

Prvních osm bitů hlavičky obsahuje příznaky, které definují, jakým způsobem bude interpretován zbytek záznamu.

Příznak	Název příznaku	Popis	Délka
MB	**Message Begin**	Určuje, zda záznam odpovídá začátku zprávy. Pokud ano, je nastaven na logickou 1 (true). V opačném případě je nastavena hodnota 0 (false)	1 bit
MF	**Message End**	Určuje, zda záznam odpovídá konci zprávy. Pokud ano, je nastaven na logickou 1 (true). V opačném případě je nastavena hodnota 0 (false)	1 bit
CF	**Chunk Flag**	Určuje, zda se jedná o data rozptýlena do více záznamů Pokud ano, je nastaven na logickou 1 (true). V opačném případě je nastavena hodnota 0 a záznam obsahuje celou zprávu.	1 bit
SR	**Short Record**	Určuje délku datového obsahu. V případě, že délka datového obsahu je 1 byte, je nastaven na logickou 1 (true). V opačném případě je nastaven na hodnotu 0 a délka je 4 byty.	1 bit
IL	**ID Length**	Určuje, zda bude použita délka ID. V případě, že je nastavena hodnota 1, je příznak aktivní. V opačném případě je nastavena hodnota 0 a délka ID je v záznamu vynechána.	1 bit
TNF	**Type Name Format**	3-bitové pole, které určuje typ datového obsahu	3 bity

Tabulka 2 - Příznaky NDEF formátu



Obrázek 4 - Struktura NDEF formátu

3.2.5 Využití

Dnešní možnosti využití technologie NFC jsou obrovské. Většinou se jedná o usnadnění každodenních úkonů a sdílení dat. Od jednoduchých operací typu sdílení vizitek, odkazů přes ovládání produktů chytré domácnosti, autorizaci přístupových systémů, prodej jízdenek až po bezkontaktní platby.

- **Veřejná doprava**

  Již běžně se lze v prostředcích městské hromadné dopravy setkat s automaty pro nákup krátkodobých jízdních kupónů vybavených NFC validátory. Jízdní kupón je tak možné zaplatit běžnou bezkontaktní platební kartou nebo mobilním telefonem s NFC. Tento způsob úhrady cestovného je velmi populární v zahraničí, zejména pak v Číně, kde je vstup do hromadné dopravy podmíněn turnikety. Ovšem v posledních letech se tento trend platby jízdného rozšiřuje i České republice, primárně v příměstské hromadné dopravě, kdy se cestující prokazuje platným jízdním dokladem při vstupu do vozidla nebo jej hradí přímo na místě.

  V České republice je NFC využíváno i pro předplacené kupóny typu starší Opencard nebo novější Lítačky pro Pražskou integrovanou dopravu a u karet dalších dopravců. Pro tyto karty jsou použity čipy společnosti NXP Semiconductors s vysokou mírou zabezpečení z kategorie produktů Mifare Desfire. Kupón je přiřazen konkrétní kartě, informace o platnosti jsou ovšem ukládány na servery dopravce. Při ověřování platnosti kupónu je tak potřeba aby kontrolor ve svém validátoru měl stažena aktuální data nebo měl aktivní datová připojení.

  Dalším způsobem prokazování se platným jízdním dokladem je využití mobilní aplikace některého z dopravců, kdy je kupón uložen v aplikaci. Aplikace nabízí doložit platný jízdní doklad buď naskenováním příslušného QR kódu přímo z obrazovky mobilního telefonu s příslušnou aplikací nebo jako alternativu využít ověření přiložením mobilního telefonu s NFC k validátoru dopravce.

  Podobně jako u služeb pro bezkontaktní placení mobilním telefonem se i u předplacených karet pro cestování v hromadné dopravě při vkládání nové karty do aplikace registruje vždy konkrétní zařízení, resp. mobilní telefon.

  V Pražské integrované dopravě platí, že „každý cestující si sice může zaregistrovat vyšší množství identifikátorů – zelenou kartu Lítačku, In-kartu Českých

drah, bankovní kartu společností Master Card nebo Visa a nově také mobil s aplikací PID Lítačka, jenomže jako nosič kuponu si může vybrat pouze jeden z nich. Jako nosič předplatní jízdenky se registruje konkrétní mobilní telefon, přenést kupon je tedy třeba například i při koupi nového.“ (Sojka, 2019). Dopravní podnik tak chce čelit podvodům způsobených v případě více nosičů platného průkazu. České dráhy se naopak dovolují současně prokazovat klasickou kartou i jejím otiskem v aplikaci.

- **Chytrá domácnost**

  NFC tagy jsou jednoduchým řešením pro automatizaci za pomoci mobilního telefonu. Automatizace domácností umožňuje snížit spotřebu energie, což vede k efektivnímu snižování nákladů na účty za energii. NFC tagy lze naprogramovat na množinu jednoduchých akcí, které se provedou vždy po načtení tagu pomocí tzv. maker.

  Klasickým zástupcem jednoduché automatizace v domácnosti za použití NFC tagu je například vytvoření značky pro automatické připojení k domácí Wi-Fi síti. Potencionální návštěvník tak nemusí žádat o přístupové údaje pro připojení a následně ztrácet čas zdlouhavým nastavováním, ale pouhým přiložením mobilního telefonu k takto naprogramovanému tagu se automaticky k síti připojí.

  Aplikaci s vytvořenými makry je možné dále spojit s dalšími aplikacemi, například pro obsluhu bran chytré domácnosti. To opět rozšiřuje možnosti užití při řízení chytrých domácností. Aplikace s makry funguje jako jakýsi spouštěč akcí a úkolů, které se aktivují po přiložení mobilního telefonu k NFC tagu. Je tak možné vytvořit makra, která obsluhují celou řadu akcí.

  Aplikace nabízí možnost konfigurace množství tagů pro jednotlivé specifické události. Je tak možné vytvořit například značku definující sadu událostí (například vypnutí spotřebičů) při odchodu z domácnosti nebo naopak vytvořit jiný tag se sledem událostí, které se provedou při příchodu do domácnosti pouze přiložením mobilního telefonu s NFC k naprogramovanému tagu.

- **Bezkontaktní platby**

  Původní nasazení bezkontaktních platebních karet mělo zjednodušit a urychlit průběh plateb a nahradit stávající druh karet, které se pro uskutečnění platby musely

nejdříve vložit do platebního terminálu. Bezkontaktní platební karty jsou navíc mnohem méně náchylné na poškození, právě protože je není nutné vkládat do terminálů.

Mimo klasické placení pomocí bezkontaktních platebních karet se čím dál častěji lze setkat s bezkontaktním placením pomocí mobilního telefonu nebo chytrých hodinek či náramku. Největší zásluhu na rozšíření tohoto trendu má společnost Apple, která v roce 2019 zavedla svou službu Apple Pay i pro Českou republiku. Již dříve byla v České republice možnost využít pro platby některou z konkurenčních služeb, které ovšem začaly nabývat na popularitě až s příchodem zmiňovaného Apple Pay.

Z bezpečnostního hlediska se placení mobilním telefonem považuje jako bezpečnější varianta oproti klasickým platebním kartám. Z pohledu NFC technologií se jedná o spojení typu Card Emulation. To znamená, že platební terminál je během placení v roli aktivního zařízení a mobilní telefon v podstatě vystupuje v roli pasivního média a emuluje platební kartu. Mobilní telefon ovšem neemuluje kartu jako takovou, ale jen její otisk neboli token, což je právě důvodem vyšší bezpečnosti před běžnými platebními kartami.

„Jméno a úplné údaje o kartě se v aplikaci nikdy nezobrazují a nikdy se s prodejcem nesdílejí. Token je vždy nastaven pouze pro určitou mobilní aplikaci, takže jej není možné zachytit a zneužít k nákupu po internetu či někde jinde, vysvětlil Marcel Gajdoš, šéf společnosti Visa pro Českou republiku a Slovensko.“ (Klička, 2017).

Token je speciální ověřovací číslo generované přímo pro konkrétní zařízení, na kterém je karta simulována. Pro platby tak není použito skutečné číslo karty, ale jen její otisk v podobě tokenu. Při nahrávání nové karty do zařízení je potřeba vyplnit údaje o své kartě, ty se však do zařízení ani do žádného cloudu neukládají. Rovněž jelikož je token vázán přímo ke konkrétnímu zařízení, v případě zneužití či odcizení token nebude s jiným mobilním zařízením fungovat.

Telefon se ve skutečnosti propojí s bankou přímo jen jednou, při vložení karty. Následně je vytvořen zmiňovaný token. Jelikož je token uložen přímo v zařízení, pro které byl vytvořen, pro platby není potřeba aktivní datové připojení mobilního telefonu. Pomocí tohoto tokenu a automaticky generovaného přístupového kódu, který je

generován speciálně pro každou platbu probíhá samotné placení. Skutečné číslo karty a další údaje tak nemá obchodník šanci získat.

Nejrozšířenějšími službami pro bezkontaktní platby mobilem jsou aktuálně Apple Pay a Google Pay, které jsou podporovány většinou českých bank. Dále je u některých bank možnost využít služby jako Garmin Pay nebo Fitbit Pay.

		Možnosti platby				
		Google Pay	Apple Pay	Garmin Pay	Fitbit Pay	Vlastní řešení
Název banky	Air Bank	✓	✓	✓	✓	✓
	CREDITAS	✓	✓	✓	✗	✗
	Česká Spořitelna	✓	✓	✓	✓	✗
	ČSOB	✓	✓	✓	✗	✓
	Equa Bank	✓	✓	✗	✗	✗
	Fio Banka	✓	✓	✓	✓	✗
	Komerční Banka	✓	✓	✓	✓	✗
	mBank	✓	✓	✓	✓	✗
	MONETA Money Bank	✓	✓	✓	✓	✗
	Raiffeisenbank	✓	✓	✓	✓	✓
	Sberbank	✗	✗	✗	✗	✗
	UniCredit Bank	✓	✓	✗	✗	✗

Tabulka 3 - Podpora služeb bezkontaktních plateb v ČR

- **Další případy využití**

Technologie NFC je často spojována v souvislosti s přístupovými a autentizačními systémy. Tyto systémy běžně slouží pro přístup do fyzických objektů, tak ale i pro autentizaci na úrovni zabezpečení softwaru nebo v docházkových systémech atd. Hojně využívána je NFC technologie také v průmyslu a skladovém hospodářství pro identifikaci produktů jako alternativa čárových kódů.

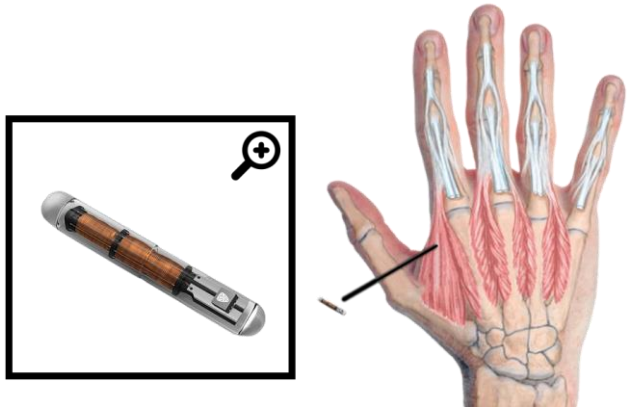
Pro softwarové programy vyžadující vyšší stupeň zabezpečení vícefaktorovým ověřením, je autentizace pomocí NFC jedním z užívaných řešení. V tomto případě je NFC tag využit jako jeden z ověřovacích prvků pro přístup do systému. Obdobně lze

NFC tagy udělovat přístupy do fyzických objektů, zvláště budov. Skrze přístupové čtečky může správce objektu vytvářet oprávnění konkrétním osobám nebo skupinám. V případě ztráty či odcizení přístupové karty nebo čipu lze jednoduše odebrat příslušná oprávnění z databáze. Přístupové systémy častokrát bývají propojeny s dalšími systémy na bázi docházkových systémů, kdy se zaměstnanci prokazují přidělenou identifikační kartou nebo čipem. Majitel podniku má poté přehled na příchody a odchody svých zaměstnanců.

Mimo přístupu do budov, jsou v posledních letech vyvíjeny i vozy s implementovanými NFC čtečkami. Takto navržené vozy nabízí uživatelovi větší komfort při ovládání svého vozidla. Pouhým přiložením NFC tagu či mobilního telefonu lze vozidlo automaticky odemknout nebo nastartovat. Pro mobilní zařízení byl vytvořen standard digitálního klíče organizací Car Connectivity Consortium s označením Digital Key, aktuálně ve verzi 2.0. Mezi hlavní výhody digitálního klíče patří možnost sdílení klíčů mezi uživateli v podstatě odkudkoliv. Na podobném principu funguje strategie řady společností provozující carsharing či další služby sdílených dopravních prostředků.

Dnes již dokonce existují technologie, které umožňují aplikaci NFC čipu přímo do těla. Tělní NFC čipy jsou distribuovány v podobě kapslí, které se zavádí pod kůži uživatele. Obecně se používá termín biohacking a takto modifikovaní lidé jsou poté označováni za transhumanoidní. „Implementace čipů do lidského těla a další formy propojování s chytrou technikou samozřejmě budou vyvolávat otázky všeho druhu, od zdravotních, přes etické až po možnosti sledování a ochrany soukromí.“ (Sedlák, 2016). Z praktického hlediska je čip totožný s klasickým NFC tagem, je však speciálně upraven, aby mohl být zaveden do těla uživatele. Podporuje tak všechny funkce klasických NFC značek. Aplikace je prováděna pomocí sterilní jehly, nejčastěji do oblasti mezi palec a ukazováček ruky. Zavedení je možné svépomocí, doporučuje se však využít praktických klinik, které zavádění čipů umožňují. V České republice aplikaci čipu umožňuje pouze salon HELL. Čipové implantáty nabízí například společnosti VivoKey Technologies, Digiwell, Dangerous Things a další. Implantát je možné využít například jako vizitku, úložiště hesel, klíč nebo pro platby Bitcoinem atd. Čip je dále možné naprogramovat pro případ zranění nebo nehody, kdy záchranná služba naskenuje implantovaný čip pro potřebné informace o pacientovi. VivoKey

Spark navíc slibuje podporu klasických bezkontaktních plateb nebo průkazů veřejné dopravy.



Obrázek 5 - NFC implantát VivoKey Spark

3.2.6 NFC čtečky

NFC čtečka je čtecí, případně zapisovací zařízení, které funguje na principu radiových vln a elektromagnetické indukce. Umožňuje přenos dat na krátké vzdálenosti. NFC čtečky jsou aktivní zařízení a pro svou funkčnost potřebují vlastní napájení.

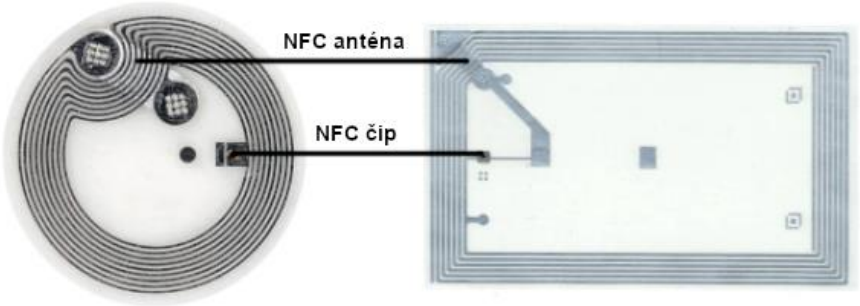
Aktivní čtecí zařízení NFC obsahují smyčkovou cívku, kterou prochází malý elektrický proud a tím vytváří elektromagnetické pole, které slouží pro vytvoření bezdrátového komunikačního kanálu a aktivování pasivního tagu. V zásadě se přiblížením obou zařízení vytvoří transformátor se vzduchovou mezerou. Komunikace mezi NFC zařízeními probíhá v radiofrekvenčním spektru 13,56 MHz, zpravidla za použití malých proudů, zhruba do 15 mA.

3.2.7 NFC tagy

NFC tag je nízkoenergeticky náročný pasivní prvek uchovávající datový obsah. Konstrukční zpracování či design tagu není striktně definován, avšak nejčastěji bývá konstruován v podobě čipové karty nebo klíčenkového tokenu. Neobsahuje vlastní zdroj energie, ale díky své malé energetické náročnosti stačí je-li napájen elektromagnetickým polem některého aktivního NFC zařízení. Celková energetická náročnost je v řádech mikroWattů.

NFC tagy po konstrukční stránce obsahují dvě základní části. První část je cívka, resp. smyčková indukční anténa pro navázání komunikace. Druhá část je tvořena samotným NFC čipem, který uchovává data. NFC čip často zaujímá jen malou část

celkové velikosti celého tagu. Zbytek je ve většině případů použit pro anténu, která musí být dostatečně velká, aby mohlo proběhnout navázání komunikace a následný přenos. Největším výrobcem NFC čipů je společnost NXP Semiconductors, která vyrábí čipy do většiny NFC tagů. Pro správnou funkčnost by NFC tag neměl mít kovovou konstrukci a neměl by být v průběhu přenosu v přímém kontaktu s kovovými předměty, které by snižovaly výkon antény.



Obrázek 6 - konstrukce NFC tagu / karty

3.3 Mifare

Rodina bezdrátových tagů, resp. čipů používaných v bezkontaktních NFC kartách společnosti NXP Semiconductors je na trh uváděna pod označením Mifare. Čipy Mifare splňují mezinárodní standard ISO / IEC 14443A, který je běžně používán pro bezkontaktní čipové karty. Společnost NXP Semiconductors nabízí Mifare karty v několika dostupných variantách v závislosti na potřebách zákazníka. Mimo jiné je v případě potřeb integrace Mifare karet do starších systému možnost pořízení Mifare karet s magnetickým proužkem.

Technologie Mifare je založena především na bezpečném přenosu dat mezi čipem a čtecím médiem. Rádiový přenos mezi oběma zařízeními je proto symetricky šifrován. Zabezpečené šifrování rovněž zabraňuje neoprávněnému přístupu k datům uloženým na kartě nebo čipu. Díky tomu je proces duplikace Mifare čipů velice náročný.

Dalšími výhodami je, že každá karta má své unikátní sériové číslo a možnost provozovat na jedné kartě tohoto typu více aplikací od různých výrobců současně. „Karty Mifare obsahují v prvním sektoru továrně nastavené UID karty. Toto UID je neměnné a vždy náhodně generované. Množina těchto hodnot se sestává z 2^{32} = 4294967296 kombinací. To je poměrně dobrá množina možných hodnot. V případě využití těchto karet podnikem nebo organizací o 1000 přístupových kartách je pravděpodobnost kolize karty se stejným UID z jiného karetního systému přibližně 1 : 4294967, což je hodnota, kterou

můžeme označit za bezpečnou.“ (Lieskovan, 2019). Každý sektor obsahuje vlastní 48bitový klíč pro přístup ke čtení a zápisu dat.

3.3.1 Typy Mifare čipů

Mifare přichází s celou rodinou čipů pro různé případy použití a různou úrovní zabezpečení. Většina čipů je rovněž nabízena v různých paměťových variantách.

- **Mifare Classic**

  Nejstarší typ Mifare karet, které se využívaly např. při bezkontaktním prodeji jízdenek. Hlavním důvodem, proč jsou tyto karty široce používány, je jejich snadné použití a jejich nízké náklady. Vzhledem k používané šifrovací metodě jej výrobce již nedoporučuje používat pro aplikace vyžadující vysokou bezpečnost. To vedlo k vývoji vysoce zabezpečených řad Mifare Plus a Mifare DesFire.

Název čipu	Šifrovací algoritmus	Velikost paměti
Mifare Classic EV1	**CRYPTO1**	**1 kB / 4 kB**
Mifare Classic Mini	**CRYPTO1**	**224 B**

Tabulka 4 - Produkty Mifare Classic

- **Mifare Plus**

  Řada Mifare Plus je navržena jako bezpečnější alternativa starších karet. Nabízí plynulý přechod stávajících instalací založených na produktech řady Mifare Classic. Lze tak pro stávající systémy vydávat karty, které jsou zpětně kompatibilní s Mifare Classic a využívají šifrovací metodu AES.

Název čipu	Šifrovací algoritmus	Velikost paměti
Mifare Plus S	**CRYPTO1, AES**	**2 kB / 4 kB**
Mifare Plus X	**CRYPTO1, AES**	**2 kB / 4 kB**
Mifare Plus SE	**CRYPTO1, AES**	**1 kB**
Mifare Plus EV1	**AES**	**2 kB / 4 kB**
Mifare Plus EV2	**CRYPTO1, AES**	**2 kB / 4 kB**

Tabulka 5 - Produkty Mifare Plus

- **Mifare Ultralight**

  Karty Mifare Ultralight jsou ideální pro levné a velkoobjemové aplikace (např. veřejná doprava, věrnostní karty atd.). Slouží jako bezkontaktní náhrada za karty s magnetickým proužkem nebo čárových kódů.

Název čipu	Šifrovací algoritmus	Velikost paměti
Mifare Ultralight C	**3DES**	**144 B**
Mifare Ultralight EV1	**32bit heslo**	**48 B / 128 B**
Mifare Ultralight Nano		**40 B**

Tabulka 6 - Produkty Mifare Ultralight

- **Mifare DesFire**

  Produkty řady Mifare DesFire splňují požadavky na rychlý a vysoce bezpečný přenos dat. Je vhodná pro provozovatele systémů vytvářející spolehlivá, interoperabilní a škálovatelná bezkontaktní řešení. Zaměřují se na víceaplikační řešení čipových karet. V České republice je typ karet Mifare Desfire využíván například pro karty Opencard a Lítačka.

Název čipu	Šifrovací algoritmus	Velikost paměti
Mifare DesFire EV1	**3DES, AES**	**2 kB / 4 kB / 8 kB**
Mifare DesFire EV2	**3DES, AES**	**2 kB / 4 kB / 8 kB / 16 kB / 32 kB**
Mifare DesFire EV3	**3DES, AES**	**2 kB / 4 kB / 8 kB**
Mifare DesFire Light	**AES**	**640 B**

Tabulka 7 - Produkty Mifare DesFire

3.3.2 Šifrovací algoritmy

- **CRYPTO1**

  Šifrovací algoritmus CRYPTO1 zajišťuje šifrovaný přenos dat produktů Mifare. Jedná se o vlastní bezpečnostní kryptovací algoritmus společnosti NXP Semiconductors vytvořený speciálně pro čipy Mifare Classic. Jak se následně ukázalo, myšlenka vydat se cestou tvorby vlastního šifrovacího algoritmu se společnosti neověřila. Společnost NXP Semiconductors nikdy nezveřejnila princip šifrovacího algoritmu, ovšem díky technikám reverzního inženýrství, jehož cílem bylo odkrýt princip fungování šifrovacího algoritmu, bylo možné bezpečnostní kód dešifrovat. Karty Mifare Classic byly i samotným výrobcem označeny jako produkty s nízkou úrovní zabezpečení a pro aplikace vyžadující vysokou míru zabezpečení je doporučeno využít některou z vyšších řad karet Mifare.

- **DES / 3DES**

  Původní šifrovací algoritmus DES byl v roce 1977 na základě veřejné soutěže USA uznán za standard. Jde o symetrickou blokovou šifru na principu Feistelovy šifry, kdy bloky mají velikost 64 bitů a šifrování i dešifrování se provádí pomocí stejného klíče. Ovšem už ve stejném roce bylo poukazováno na bezpečnost šifrovacího klíče, který měl délku pouhých 56 bitů. Na základě relativně snadného prolomení klíče hrubou silou byla podpora standardu ukončena. Následně byla přijata bezpečnější varianta této šifry s označením Triple-DES (3DES), která třikrát aplikuje původní algoritmus DES, čímž se délka kryptografického klíče prodloužila na 168 bitů. „3DES poskytuje metodu pro virtuální zvětšení velikosti klíče bez návrhu nového algoritmu. Proto se předpokládá, že algoritmus DES je relativně bezpečný pouze ve formě 3DES.“ (Coskun, a další, 2012). Využívá se například u vyšších řad karet Mifare, které vyžadují vyšší míru zabezpečení. Triple-DES standard byl v roce 2002 nahrazen novějším standardem AES.

- **AES**

  Aktuálně je algoritmus AES nejpoužívanější metodou pro symetrické šifrování, který nahrazuje méně bezpečnou metodu šifrování DES / 3DES a zároveň je zhruba 6x rychlejší. Od roku 2002 je uznávaným standardem jako bezpečná metoda ochrany dat. Podobně jako u standardu DES se šifrování dat provádí v blocích. Vzhledem k tomu, že jde o symetrickou metodu, tak i zde se k šifrování i dešifrování používá stejný klíč. „AES je varianta šifry Rijndael, která používá velikost pevného bloku 128 bitů a klíč proměnné velikosti 128, 192 nebo 256 bitů. AES je založen na konstrukčním principu, který je známý jako substituční-permutační síť. jedná se o kombinaci substituce i permutace, která je rychlá jak v softwaru, tak v hardwaru.“ (Haunts, 2019). Je podporována vyššími řadami karet Mifare. Mimo jiné je využívána například pro zabezpečení VPN, hesel Wi-Fi sítí a většiny dnešních aplikací.

3.4 Další bezdrátové technologie

Bezdrátová technologie NFC je často spojována s dalšími bezdrátovými technologiemi, ač každá technologie ve výsledku funguje trochu na jiných principech. Nejčastěji je NFC spojováno s technologiemi jako Wi-Fi, Bluetooth nebo například RFID

s kterou si je NFC nejblíže, nýbrž z ní vychází. „Hlavním omezením RFID je ovšem pouze jednocestná komunikace. NFC již umožňuje komunikaci oboucestnou mezi koncovými zařízeními. Jelikož mohou být nenapájené NFC tagy čteny aktivními NFC zařízeními, jsou schopné starší RFID systémy plně nahradit.“ (Trčálek, 2013) Je tak důležité si uvědomit, že každá technologie má svůj specifický smysl pro různá využití.

3.4.1 Bluetooth

V případě vzniku této technologie bylo hlavní myšlenkou sjednotit dříve používané standardy bezdrátové komunikace jednotlivých výrobců, aby spolu přístroje mohly vzájemně komunikovat. Jelikož se již jedná o standard, lze jej dnes najít v téměř každém chytřejším zařízení, které vyžaduje komunikaci s dalšími periferiemi, jako notebooky, smartphony, reproduktory, herní zařízení atd. Vývojáři této technologie se zároveň snaží držet původní myšlenky, a proto jsou novější verze protokolů Bluetooth zpětně kompatibilní.

Technologie Bluetooth, stejně jako NFC umožňuje bezdrátově přenášet data na krátké vzdálenosti. Řadíme jej tedy do sítí typu PAN (Personal Area Network). „Obecně platí, že PAN překlenuje mnohem kratší vzdálenost než bezdrátová LAN a přenáší data mnohem pomaleji.“ (Comer, 2019). Jedná se o typ sítě, kdy spolu jednotlivá zařízení komunikují na malém území, zvláště v řádech jednotek až desítek metrů. Ačkoliv se nejedná o řešení na dlouhé vzdálenosti, je stále vzdálenost komunikujících zařízení mnohonásobně větší než v případě NFC. Podstatným rozdílem je také to, že Bluetooth neumožňuje připojení pouze mezi dvěma přístroji, nýbrž dokáže fungovat i v režimu ad-hoc sítě.

NFC je novější technologie než Bluetooth, ačkoli použitá technologie je starší. Základní rozdíl mezi těmito technologiemi je použité frekvenční pásmo, přenosová rychlost a způsob navazování komunikace. Zatímco NFC pro komunikaci využívá frekvenční pásmo 13,56 MHz, Bluetooth pracuje v pásmu 2,4 GHz. V obou případech se tak jedná o nelicencovaná pásma. Jelikož je pásmo 2,4 GHz značně vytíženo dalšími přístroji pracujících na této frekvenci, je požadovaný výkon Bluetooth přibližně od 1 do 10 mW, dle výkonové úrovně. Takto nízká spotřeba energie, společně s metodou FHSS, pak brání v rušení jiných bezdrátových zařízení ve stejné oblasti.

Rychlost přenosu je neúměrně závislá na vzdálenosti komunikujících stran a na čistotě prostorového kanálu. Verze Bluetooth protokolu ve verzi 5.0 dosahuje teoretické rychlosti až 2 Mbit/s na vzdálenost až 200 m. Na zvyšování rychlosti má také vliv stále se rozvíjející odvětví internetu věcí. NFC technologie data přenáší o poznání pomaleji, kdy se přenosová rychlost pohybuje od 106 do 424 kbit/s.

Ve srovnání s Bluetooth technologií se ovšem NFC dokáže v podstatě okamžitě spojit s protistranou a navázat spojení. Takovéto úzké a rychlé připojení je ideální např. pro zpracování plateb a jejich zabezpečení. Pro bezpečné navázání komunikace skrze Bluetooth je zapotřebí obě zařízení nejdříve autorizovat a následně spárovat.

3.4.2 Wi-Fi

Jako v případě technologie NFC či Bluetooth funguje Wi-Fi na principu radiových vln. Opět se jedná o soubor protokolů umožňující bezdrátovou komunikaci. Wi-Fi však primárně pracuje v režimu síťové infrastruktury, kdy jsou zařízení připojována k některému z přístupových bodů. Zařízení tak nekomunikují přímo mezi sebou, ale připojují se centrálnímu bodu (nejčastěji se jedná o nějaký typ Wi-Fi routeru), který jejich komunikaci řídí.

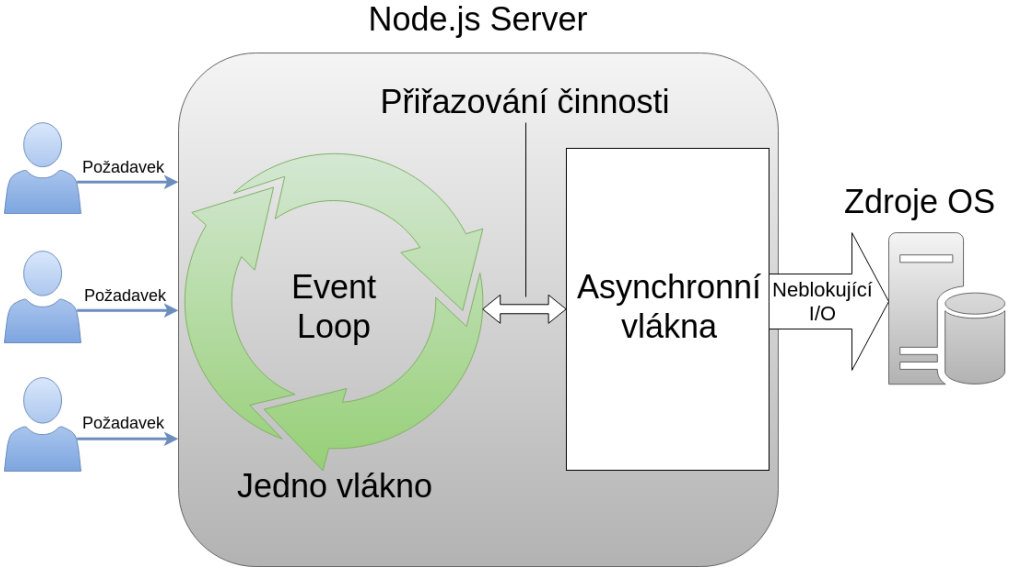
Tak jako Bluetooth umožňuje pracovat v režimu ad-hoc, i Wi-Fi naopak umožňuje práci v režimu P2P. Nejčastěji je tento režim označován jako Wi-Fi Direct. Princip je obdobný klasické Bluetooth technologii, kdy zařízení komunikují přímo mezi sebou. Oproti Bluetooth jsou u Wi-Fi Direct vyšší nároky na energii, kterou ovšem kompenzuje o poznání vyššími přenosovými rychlostmi, které dosahují teoretických hodnot až 250 Mbit/s, a stabilitou. Opět zde samozřejmě platí úměra vzdálenosti obou zařízení a čistota komunikačního kanálu. S častým využitím technologie Wi-Fi Direct se lze setkat například u bezdrátových tiskáren.

3.5 Node.js

Node.js je multiplatformní open-source běhové prostředí, které je primárně navrženo pro psaní backendových serverových částí aplikace. „Node.js poskytuje událostně řízenou a asynchronní platformu pro JavaScript na straně serveru. JavaScript nikdy neměl standardní I / O knihovny, které jsou společné pro jazyky na straně serveru. Byl však od základu postaven, aby měl událostně řízený a asynchronní model. Přináší JavaScript na

server stejným způsobem, jakým jej prohlížeč přináší klientovi.“ (CANTELON, a další, 2014). Zdrojový kód napsaný v Node.js je do strojového kódu překládán jádrem V8 JavaScript Engine vyvinutý společností Google pro prohlížeče Google Chrome společně s dalšími knihovnami. Aplikace v Node.js jsou psány v Javascriptu a je tak možné je spustit na většině operačních systémů.

Architektura Node.js je postavena na principu smyčky událostí neblokujících vstupy a výstupy API, které je navrženo tak, aby optimalizovalo propustnost a škálovatelnost webové aplikace v reálném čase. Zjednodušeně je vytvořena smyčka, jejímž úkolem je přijímat uživatelovi požadavky a předávat jej příslušným controllerům. Přednostně mohou být prováděny další požadavky s menší náročností, aby nedocházelo k blokaci vlákna složitějšími procesy. Po zpracování požadavku je vrácen výsledek Používáním smyčky událostí a asynchronní komunikace je tak možné obsloužit velké množství uživatelských požadavků. „Asynchronní programování je možná současně jednou z nejlepších a nejasnějších funkcí Node.js. Asynchronní programování znamená, že pro každou asynchronní funkci, která je spuštěna, nelze očekávat, že vrátí výsledky, než bude pokračovat v toku programu. Místo toho je třeba zadat blokování / funkci zpětného volání, které se spustí, jakmile asynchronní kód skončí.“ (Doglio, 2018).



Obrázek 7: Smyčka událostí v Node.js

Dlouhou dobu byly dostupné frameworky pro vývoj webových aplikací založené na bezstavovém modelu. V bezstavovém modelu jsou data generována v jedné relaci a neudržují se pro použití v další relaci s uživatelem (např. informace o uživatelských nastaveních a událostech, ke kterým došlo). Pro udržení informací o relaci mezi požadavky

uživatele byla potřeba spousta práce. Node.js nabízí způsob, jak mohou mít webové aplikace obousměrná připojení v reálném čase, kde klient a server zahájí komunikaci a umožní jim volnou výměnu dat.

Node.js se nehodí využívat, vyžaduje-li aplikace příliš dlouhé doby pro zpracování požadavků. Událostní smyčka je totiž strukturována do jednoho vlákna. Jeli tedy dlouhodobě vyžadováno provádění náročných výpočtů na pozadí, není server schopen zpracovávat další požadavky. Node.js se proto nejlépe hodí pro zpracovaní požadavků s nízkou potřebou vyhraněného procesorového času.

3.5.1 REST API

Architektura REST byla poprvé popsána Royem Fieldingem (americký počítačový vědec), který je zároveň jeden z hlavních autorů protokolu HTTP1 a jedním ze spoluautorů webového serveru Apache2. Svou myšlenku nové architektury navrhl a vysvětlil ve své disertační práci v roce 2000. V ní definoval termín REST, architektonický styl pro distribuované systémy. V zásadě se jedná o systémy, kdy spolu jednotlivé části programu (např. webová aplikace) dokáží komunikovat skrze síť (protokol HTTP), ačkoli se tyto části nachází na různých periferiích. Oproti dřívějším používaným stylům byl REST navržen datově, nikoliv procedurálně. Webové služby jsou účelové webové servery, které podporují potřeby webu nebo jakékoli jiné aplikace. „Klientské programy používají ke komunikaci s webovými službami aplikační programovací rozhraní (API). Obecně řečeno, API zpřístupňuje sadu dat a funkcí, které usnadňují interakce mezi počítačovými programy a umožňují jim vyměňovat si informace.“ (Massé, 2012).

Architektura REST bývá často označována za návrhový vzor, případně o standard, který ovšem přesně nedefinuje princip této architektury a ani nedefinuje pravidla, která by měla být použití REST architektury splněna. Jedná se tedy skutečně o architekturu (způsob přístupu) při tvorbě webových aplikací.

Hlavní myšlenkou REST architektury je, že se distribuovaný systém zlepší v následujících oblastech:

Výkon – Komunikační styl REST architektury je navržený tak, aby byl jednoduchý, efektivní a umožnil zvýšení výkonu v systémech které jej používají.

Škálovatelnost – Škálovatelnost by měla být v distribuovaných systémem jednou z předních priorit. Vzhledem k bezzstavovosti REST architektury a rozdělení na server-

side a client-side část, jsou aplikace využívající REST architekturu velmi dobře škálovatelné.

Jednoduchost rozhraní – Jednoduché rozhraní poskytuje jednodušší interakce mezi systémy, což má za následek lepší výkon a škálovatelnost.

Modifikatelnost komponent – Distribuovaná povaha systému a oddělení jednotlivých částí programu umožňuje úpravy komponent nezávisle na sobě s minimálními náklady a rizikem.

Přenositelnost – Architektura REST je technologicky v zásadě jazykově nezávislá, že je možné ji implementovat a používat jakýmkoli typem technologie.

Spolehlivost – Vzhledem k bezzstavovosti REST architektury se server v případě selhání dokáže snadněji obnovit.

REST API pro komunikaci se zdroji jako výchozí bod využívá protokol HTTP. „Protokol HTTP neboli Hypertext Transfer Protocol byl původně navržen pro přenos hypertextových dokumentů napsaných ve formátu/jazyku HTML. Dnes se ovšem používá i pro mnohé další účely; například ho využívají REST API služby atd. Protokol HTTP pracuje způsobem dotaz-odpověď neboli request-response.“ (Tišnovský, 2020). To zahrnuje znalost sady slov, která lze použít k odkazu na typ prováděné akce nad prostředkem. Tato sada slov obsahuje metody pro získání přístupu k prostředku, odeslání nového zdroje dat na server, aktualizaci daného zdroje nebo k odstranění zdroje. Obecně se tyto metody nazývají jako CRUD metody (create, retrieve, update, delete).

Název metody	Popis metody
GET	Získání přístupu k prostředku v režimu pro čtení
POST	Odeslání nového zdroje dat na server – vytváření akce
PUT	Aktualizace celého daného zdroje
DELETE	Mazání daného zdroje

Tabulka 8 - HTTP REST CRUD metody

3.5.2 REST API – pravidla a omezení

Client-server

Jedná se o jedno z nejběžnějších omezení v síťových client-server architekturách. Server je zodpovědný za zpracování sady služeb a naslouchá požadavkům týkajících se

těchto služeb. Požadavky jsou oproti tomu vytvářeny prostřednictvím komunikačních kanálů klientským systémem, který jednu z těchto služeb potřebuje.

Hlavním principem tohoto omezení je rozdělení různých funkcionalit systému. Je tak možné oddělit část front-endového kódu, reprezentující možné zpracování informací související s uživatelským rozhraním, od kódu serverové části, který by se měl postarat o ukládání a zpracování dat na straně serveru. Toto omezení umožňuje nezávislý vývoj obou komponent a nabízí velkou flexibilitu v oblasti klientských aplikací bez vzájemného ovlivnění kódu serveru a naopak.

Bezstavovovst

Jedním z omezení REST architektury je bezstavovost. Komunikace mezi serverem a klientem by tak měla být bezstavová. To znamená, že každý požadavek přicházející od klienta musí mít všechny potřené informace k tomu, aby mu server porozuměl, aniž by využíval výhod jakýchkoli uložených dat. Opět toto omezení přináší do základní architektury některé výhody a vylepšení.

- **Viditelnost** – Jsou-li všechny požadované informace obsaženy v požadavku, je monitorování systému značně jednodušší.
- **Škálovatelnost** – Díky tomu, že odpadá potřeba ukládaní dat mezi požadavky, může server mnohem rychleji uvolňovat zdroje
- **Spolehlivost** – Systém, který je založen na bezstavovosti, se v případě selhání dokáže mnohem rychleji obnovit, protože jedinou věcí, kterou je třeba obnovit, je samotná aplikace.
- **Snadnější implementace** – Protože se neukládají jednotlivé stavy komunikace, je kód na straně serveru jednodušší a snadněji implementovatelný.

Nevýhodou v tomto případě může být potencionální selhání síťového provozu při každém požadavku odesílání opakovaných informací o stavu. Záleží proto na typu a konkrétních potřebách implementovaného systému.

Cache

Toto omezení je zaváděno z důvodu zvýšení efektivity sítě a přenosu dat. Navrhuje, že každá odpověď na požadavek by měla být implicitně nebo explicitně nastavena jako casheable nebo non-casheable.

Ukládání odpovědí do mezipaměti má některé nesporné výhody, které jsou do architektury přidány. Na straně serveru existují některé interakce, které jsou klientem často opakovaně požadovány (například požadavek na databázi). Obsah takových požadavků je uložen do mezipaměti a při opakovaném volání je opětovně použit. Na straně klienta je následně vnímáno zjevné zvýšení výkonu. Nevýhodou tohoto omezení je možnost zastaralých dat v mezipaměti kvůli špatně nastaveným pravidlům jejich ukládání.

3.5.3 Balíčkovací systém

„Balíček v Node.js obsahuje všechny soubory, které jsou potřebné pro modul. Moduly jsou knihovny JavaScriptu, které lze zahrnout do vytvářeného projektu.“ (Refsnes Data, 2011). Moduly v Node.js jsou způsobem zapouzdření kódu do samostatné logické jednotky. Tvorba modulů je programovacím postupem, který oddělí kód takovým způsobem, aby byl lépe ovladatelný a udržovatelný pro budoucí účely. Každý modul je nezávislá entita s vlastní zapouzdřenou funkčností, kterou lze spravovat jako samostatnou pracovní jednotku. Aby bylo možné moduly v Node.js aplikaci použít, je třeba každý modul nejprve nainstalovat pomocí správce balíčků.

4 Vlastní práce

4.1 Koncept vlastní práce

Praktická část této práce vychází z teoretických předpokladů popsaných v předchozí části této práce, které budou aplikovány a prakticky demonstrovány během vývoje aplikace vlastního řešení bezkontaktních plateb.

Prezentační část desktopové aplikace je založena na moderních technologiích Windows Presentation Foundation (dále jen WPF), jakožto architektura tvorby uživatelských rozhraní postavená na rozšířeném značkovacím jazyce XAML. Logická vrstva je dále postavena na jazyce C#, s rozšířením systémové služby Microsoft Smart Card API, resp. knihovny WINSCARD.DLL určené pro navázání a následnou komunikaci s bezkontaktními NFC čtečkami a čipovými kartami. Aplikace je vyvíjena ve vývojovém prostředí Microsoft Visual Studio 2019. Pro demonstraci funkčnosti aplikace je využita bezkontaktní NFC vývojová čipová sada ACR122 SDK.

Pro webovou aplikace byla z důvodu rostoucího zájmu vývojářů a budoucího potenciálu v oblasti rozšiřování aplikace zvolena technologie Node.js založena na jazyce Jacascript v prezenční i backendové části aplikace, vyvíjena ve vývojovém prostředí Microsoft Visual Studio Code.

Datová část využívá výkonný objektově relační model databáze s přístupem DatabaseFirst a klientem PostgresSQL ve verzi 9.6, který zároveň vytváří sdílený prostor ukládání dat pro obě vyvíjené aplikace, vzhledem k zachování konzistence a aktuality dat.

4.1.1 Požadavky na aplikaci

Aktuální nabídka na trhu pokladních systémů a systémů umožňujících bezdrátové a jiné platby, včetně komplexních platebních bran, je relativně uspokojující. Nicméně, spousta z těchto systémů přistupuje k platbě čistě za účelem vykonání transakce a pro samotného provozovatele služeb nevytváří dostatečnou informaci o prodeji jako takovém, na jehož základě by bylo možné přistupovat k zákazníkovi individuálně dle jeho preferencí vzhledem k historickým dat. To je převážně z důvodu, že během prodeje nelze zákazníka nijak identifikovat.

Vezmeme-li v úvahu například systémy používané pro e-shopy, je zákazník ve většině případů před prodejem přes internet nucen vytvořit registraci svého účtu pro

úspěšné vyřízení objednávky. Pomocí tohoto účtu je již možné zákazníka identifikovat při dalším nákupu a nabídnout mu případnou slevu na nově vytvořenou objednávku či jinou individuální nabídku. Zároveň je pro poskytovatele mnohem snadnější vytvářet různé reporty pro svůj podnikatelský záměr.

Vyvíjená aplikace je určena primárně pro stánkový prodej v rámci pořádané akce, kdy si zákazník před příchodem na konkrétní akci objedná identifikační kartu nebo čip, na který si následně dobije libovolnou částku v podobě jakéhosi kreditu. Tento identifikační čip může po dohodě s pořadatelem akce sloužit jako vstupenka na danou akci.

Základně se tímto čipem zákazník prokazuje během nákupu např. občerstvení a čip v zásadě funguje jako lokální platební karta, kterou je však možné uplatnit na jakékoli akci konkrétního poskytovatele, která je v systému registrována a která pro stánkový prodej využívá tento systém.

Výhoda tohoto modelu plateb je na straně zákazníka i provozovatele. Vzhledem k tomu, že si zákazník dobije svůj čip před příchodem na akci, je následně rovnocenná cena za produkt pro každého zákazníka a nemůže se stát, že by si měnový kurz a jakoukoli měnovou politiku, v případě plateb v cizí měně nastavoval sám provozovatel. Zákazník objednáním čipu získává přístup do klientské části aplikace webového rozhraní, kde nalezne přehled svých uskutečněných nákupů na konkrétních akcích. Pro provozovatele je výhodou, že odbavení zákazníka je rychlejší, protože odpadá vracení hotovosti, pokud zákazník platí větší částkou, než je cena vydávané objednávky. Zároveň odpadá manipulace s hotovostí jako takovou, nehrozí tak možná manka v pokladně, okradení zákazníka nebo provozovatele ve výsledné tržbě, ani případná ztráta hotovosti. Provozovatel má také aktuální přehled o svých tržbách ihned k dispozici, společně s důležitými reporty ve webové aplikaci.

Pro bezproblémový běh jednotlivých systémů a jejich správnou funkčnost a kompatibilitu s použitým hardwarem jsou dále uvedeny doporučené minimální specifikace na systém a hardwarové komponenty každé aplikace. Obě aplikace fungují nezávisle na sobě, ovšem vzhledem k funkcím, které jednotlivé systémy zastávají je doporučené použití obou systémů současně, není však podmínkou. V případě, že budou používány oba systémy, tvoří společnou komponentu pouze databáze, resp. databázový server.

4.1.2 Požadavky na desktopovou aplikaci

Systémové požadavky

- Operační systém Windows 7 SP1 (x86 a x64) a vyšší
- Microsoft .Net Framework 4.5
- Sdílený databázový server s databázovým klientem PostgresSQL 9.6 a vyšší

Hardwarové požadavky

- 2 GB operační paměti RAM a vyšší
- 500 MB volného místa na disku
- Čtečka NFC čipů ACR122U NFC

4.1.3 Požadavky na webovou aplikaci

Systémové požadavky

- Operační systém Windows Server 2019
- Aktuální verzi Node.js
- Aktuální verze webového prohlížeče (klient)
- Sdílený databázový server s databázovým klientem PostgresSQL 9.6 a vyšší

Hardwarové požadavky

- Node.js server
- 8 GB operační paměti a vyšší
- 1 GB volného místa na disku

Veškeré požadavky se mohou lišit v závislosti na rozsahu provozovaných klientských zařízení a velikosti konané hromadné akce a jejího reálného vytížení. Zmíněná konfigurace je určena pro středně velké akce do maximálního počtu 100 pokladen a 1000 zákazníků.

4.2 Návrh struktury aplikace

Pro lepší pochopení paradigmatu rozvržení a propojení jednotlivých komponent byl před vypracováním podrobnější specifikace projektu vyvíjené aplikace sestaven funkční koncept schématu rozdělený na modul desktopové aplikace a modul webové aplikace z hlediska popsání komunikace mezi jednotlivými periferiemi, který zároveň popisuje

jednotlivé bloky datové, logické a prezentační vrstvy na obecné úrovni zpracování a prezentace získaných dat. Pro vytvoření schématu byl použit online nástroj pro tvorbu a vizualizaci schémat a diagramů, Draw.io.

Databáze je společným prvkem obou vytvářených aplikací z důvodu udržení konzistence, integrity a také aktuality dat v reálném čase. Vytváří tak jednotnou datovou strukturu obou systémů. Databázový klient proto představuje samostatnou funkční jednotku v podobě vzdáleného serveru, který skrze internetový protokol TCP/IP komunikuje s controllery příslušných částí aplikace. Server by měl splňovat podmínku veřejné IP adresy pro identifikaci v rámci veřejné sítě.

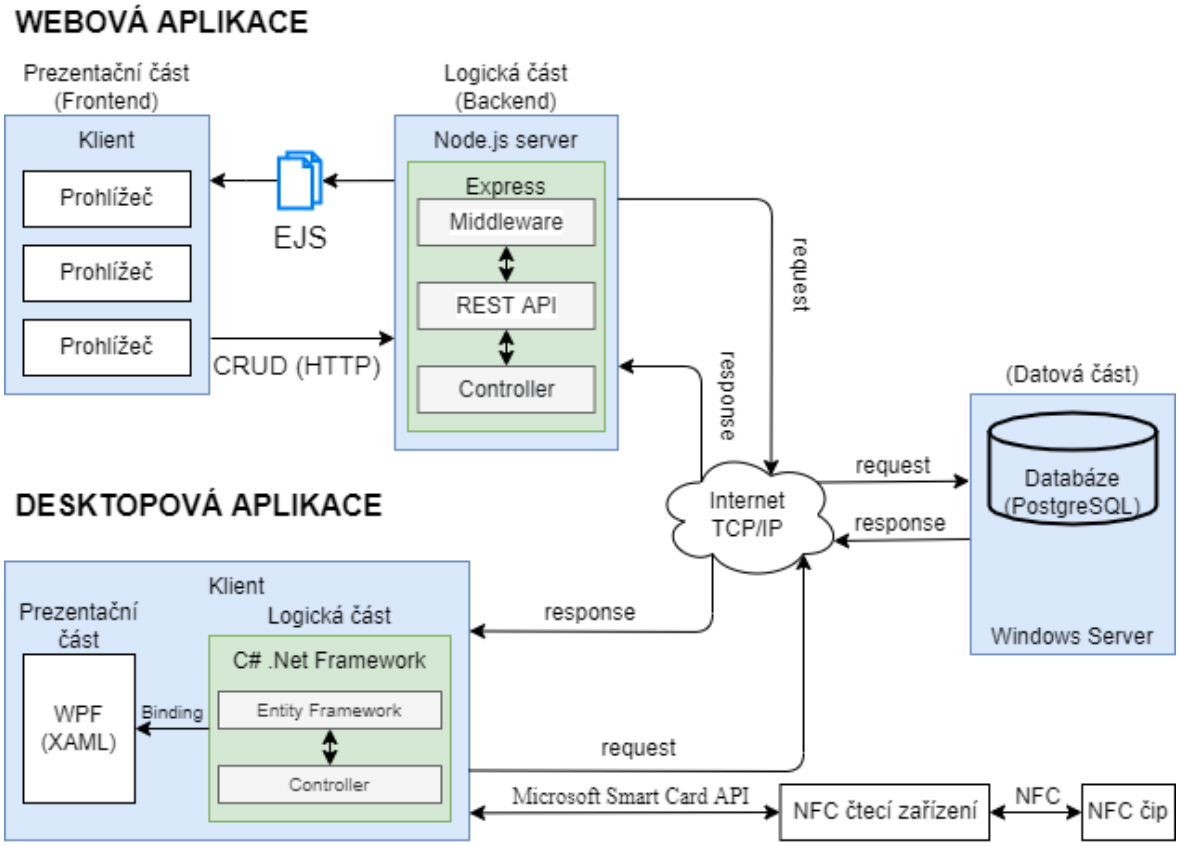
V desktopové části aplikace je komunikace s datovou vrstvou realizována přímo klientem skrze jeho logickou část a jím příslušným controllerem ve spolupráci s objektově relačním mapováním (ORM) pomocí Entity Frameworku. Zároveň jsou na úrovni logické vrstvy přijímána a zpracovávána data externího NFC čtecího zařízení. Získaná data jsou následně uživateli prezentována metodou databindingu.

Webová aplikace je standardně rozdělena na dvě části. Backendovou část, tvořící logickou vrstvu aplikace a Frontendovou část, která funguje jako prezentační vrstva klienta. Backendová část komunikuje skrze vlastní controller protokolem TCP/IP se vzdálenou databází. Komunikace s klientem je realizována skrze webovou architekturu REST API založenou na HTTP protokolu a tzv. endpoints společně s CRUD operacemi. Takto získaná data jsou následně pomocí šablonovacího systému EJS (ang. Embedded Javascript Templating) přenesena ke klientovi, kde se v podobě dynamické webové stránky klientovi prezentují skrze jakýkoliv moderní webový prohlížeč.

V porovnání s jinými programovacími systémy využívaných pro psaní backendu webových aplikací je Node.js s rostoucím počtem iterací z pohledu výkonu o 93% rychlejší než architektury založené na programovacím jazyce PHP. Pro aplikace, které předpokládají vyšší zátěž klientských požadavků se jedná o vhodnější řešení a vylepšení výkonu aplikace. V případě backendové části vyvíjené aplikace je proto zvolen Node.js.

Počet iterací	Node.js (milisekundy)	PHP (milisekundy)
100	2.00	0.14
10 000	3.00	10.53
1 000 000	15.00	1 119.24
10 000 000	143.00	10 621.46
1 000 000 000	11 118.00	1 036 272.19

Tabulka 9 - Porovnání výkonu Node.js a PHP



Obrázek 8 - Návrh struktury aplikace

4.3 Použité technologie

Před začátkem vývoje jsou na základě navržené struktury aplikace definovány jednotlivé nástroje a technologie, které usnadní práci během vývoje a zároveň budou vést k dosažení stanovených cílů konečné realizace.

4.3.1 Desktopová aplikace

- **C# (.Net Framework)** – Programovací jazyk doplněný o .Net Framework 4.5 pro vývoj logické části desktopové aplikace
- **WPF** – Architektura pro tvorbu grafického rozhraní desktopové aplikace založené na jazyce XAML s podporou databindingu
- **Entity Framework 6** – Framework pro objektově relační mapování databáze a práce s daty v jazyce LINQ
- **NPGSQL** – Poskytovatel pro komunikaci se vzdálenou relační databází PostgreSQL v rámci knihovny ADO.Net jako součást .Net Frameworku, kompatibilní s Entity Frameworkem

- **WINSCARD.DLL** – Microsoft Windows systémová knihovna (Microsoft Smart Card API) pro správu a komunikaci s čipovými kartami a čtečkami čipových karet

4.3.2 Webová aplikace

- **Javascript** – Multiplatformí scriptovací jazyk pro tvorbu komplexních a škálovatelných webových aplikací
- **Node.js** – Software pro vývoj multiplatformních aplikací založený na jazyce Javascript v backendové části aplikace na straně serveru, konkrétně její logické vrstvy
- **Express** – Modul, resp. framework pro tvorbu webových serverů Node.js
- **EJS** – Jednoduchý šablonovací systém pro tvorbu dynamických webových stránek založených na Javascriptu
- **PG (NPM)** – Kolekce modulů vytvořených pro Node.js a jeho komunikaci a práci se vzdálenou databází PostgreSQL
- **REST API** – Architektura pro komunikaci backendové části s klientskou částí aplikace a podporou CRUD operací na úrovní HTTP protokolu

4.3.3 Databáze

a) **PostgreSQL** – Objektově relační databázový systém pro uložení a uchování dat.

4.4 Využití vlastní aplikace

Pro zpřesnění požadovaných realizačních cílů je stanovena motivace tvorby vlastního řešení v případě vývoje pokladního systému na bázi čipových karet a konečná definice požadovaného cíle.

4.4.1 Motivace

Motivací k tvorbě vlastního řešení pokladního systému je hlavní myšlenka inovací v oblasti dosavadních pokladních systémů a spojení dostupných technologií při běžných rutinních úkolech reálného světa a jejich automatizaci. Vzhledem k rozšiřující se tendenci „spojování těchto světů“ na všech úrovních lidských činností vyplívá, že trend bezdrátových technologií bude i nadále významnou oblastí při realizaci tohoto

propojování, včetně metod bezhotovostních plateb, které již nyní mají ve světě podstatné zastoupení.

4.4.2 Definice cíle

Hlavním cílem je vytvoření komplexního, ovšem uživatelsky přívětivého a intuitivního řešení pokladního systému, který se primárně zaměřuje na stánkový prodej v rámci festivalových a venkovních akcí. Vyvíjený systém má poskytnout optimalizaci během platebního procesu v podobě rychlosti odbavení objednávky zákazníka a uchování dat pro tvorbu statistických reportů za účelem navýšení prodejů pomocí identifikačních a platebních čipových karet, resp. tokenů.

Vzhledem k vysokému počtu platebních operací na takovýchto akcích je důležitým faktorem kvalitní navržení síťové infrastruktury pro udržení stability systému a také integrity a aktuálnosti dat.

4.4.3 Konkurenční systémy bezhotovostních plateb na hromadných akcích v Čr

Obecně se jedná o tzv. cashless systémy, které z pohledu pořadatelů hromadných akcí nabývají na popularitě. Z hlediska tržeb se jedná o systémy, které řeší problémy spojené s manipulací hotovosti a ve výsledku přináší jejich použití vyšší zisk.

V České republice zastoupení takových systému tvoří zatím velmi malou část trhu a ve většině případů je použití takového systému stále spíše experimentální záležitostí, která si klade za cíl přiblížit veřejnosti tento typ transakcí pro budoucí plnohodnotné nahrazení klasických hotovostních plateb na hromadných akcích.

Aktuálně systémy založené na cashless technologii v České republice nabízí společnosti

- NFCtron – největší a nejpopulárnější cashless systém v Čr
- Phestio

4.5 UI a UX specifikace

UI specifikace projektu je realizována za účelem rozvržení prvků aplikace a jejich komponent tak, aby bylo možné jejich efektivní využití z pohledu uživatelské přívětivosti a celkové intuitivnosti systému, kdy práce se systémem poskytne uživateli příjemný zážitek z používání. Dále je při samotném návrhu uživatelského rozhraní třeba předpokládat, že

z hlediska použití bude vzhledem ke svým kompaktním rozměrům nejčastější a zároveň nejpraktičtější platformu pro běh aplikace pokladny představovat dotykový tablet s operačním systémem Microsoft Windows. Uživatelské rozhraní by proto mělo splňovat podmínky a specifika pro snadné ovládání pomocí dotykové obrazovky.

Současně je v rámci tvorby UX specifik kladen důraz na efektivitu některých procesů a celkové rychlosti odbavení zákazníka, jakožto jedna z hlavních priorit návrhu. Vzhledem k tomu, že jedním z hlavních cílů tvorby vlastního řešení pokladního systému je zefektivnění dosavadního procesu hotovostních plateb na festivalech, nahrazením zcela jiným modelem, tak celý proces odbavení musí být navržen tak, aby na výdejních místech nedocházelo k vytváření front z důvodu nedostatečně rychlého nebo neefektivního pokladního systému.

Případná potřebná optimalizace z pohledu kódu aplikace bude následně reverzním inženýrstvím, konkrétně metodou refaktoringu provedena za účelem čistějšího, přehlednějšího, a především efektivnějšího kódu.

4.5.1 Cílové skupiny

Cílovou skupinu uživatelů systému tvoří primárně osoby neznalé v oblasti IT a vývoje softwaru. Jedná se většinou o skupinu uživatelů z oblasti pohostinství a služeb, případně studentů v rámci brigády. Jsou tak pouze koncovými uživateli, kteří k systému přistupují jako k hotovému a funkčnímu řešení, který má za úkol usnadnit práci na pokladně a automatizovat proces obsluhy. Systém používají čistě k tomu, k čemu je primárně určen – tj. k uskutečnění transakcí a odbavení zákazníka, případně sledování prodejních statistik.

Pokladní systém je vyhrazen

- Osobám ve věku 15 – 60 let
- Osobám, které budou se systémem pracovat příležitostně v rámci pořádané akce
- Osobám neznalým v oblasti IT (obsluha primárně znalá v jiné oblasti)
- Osobám poučeným s prací se systémem (osoby proškolené)
- Majiteli a obsluze firmy
- Zákazníkům

4.5.2 Vzorové persony

Primární persona

Jméno: Anežka Hromková

Pohlaví: žena

Věk: 19

Povolání: Student, brigáda – obsluha ve stánku s občerstvením, práce na pokladně

Zájmy: kosmetika, setkávání s přáteli, sledování filmů a seriálů, sociální sítě

Charakteristika: Anežka je studentka prvního ročníku vysoké školy ekonomické. Ráda si užívá studentský život se svými přáteli, na který si přivydělává v podobě různých brigád. Brigádně pracuje jako hosteska na kulturních akcích, jejíž primární náplní práce je obsluha stánkového prodeje s přesahem práce na pokladně. Je společenská, komunikativní a ráda pracuje s lidmi. Naopak není technický typ s rozšířenými znalostmi v oblasti informačních technologií.

Řešení: Intuitivní pokladní systém založený na minimalistických prvcích uživatelského rozhraní, které výrazně zvyšují přehlednost a produktivitu celého systému a zároveň snižují riziko chyb během jeho obsluhy.

Sekundární persona

Jméno: Petr Zbořil

Pohlaví: muž

Věk: 52

Povolání: Majitel cateringové společnosti

Zájmy: cestování**,** moderní technologie, sport

Charakteristika: Petr je majitelem cateringové společnosti a vlastníkem několika hospod v centru města. Ve své firmě zaměstnává velké množství zaměstnanců, z nichž vysoké procento pracuje na dohodu o provedení práce jako brigádník a často tak dochází k obměně zaměstnanců. Nerad ztrácí čas, protože čas jsou pro něho peníze. Z pohledu podnikatele má rád ve svých aktivitách pořádek. Svému byznysu věnuje množství času a vyžaduje kontrolu nad činností zaměstnanců. V soukromí se amatérsky věnuje obchodování s kryptoměnami.

Řešení: Festivalový režim pokladního systému, který poskytne praktický přehled nad průběhem pořádané akce s minimální potřebou zaškolení zaměstnanců. Online

přehled se statistickými reporty v reálném čase i v průběhu akce a vzdálené nastavení některých důležitých funkcí systému.

Negativní persona

Jméno: Zdeněk Babka

Pohlaví: muž

Věk: 72

Povolání: Údržbář, momentálně v důchodu

Zájmy: četba, rybaření

Charakteristika: Zdeněk je osoba s jasně vyhrazenými názory a postoji, které jsou dle něho pověřeny věkem, a které jen zřídka mění. Je majitel chytrého telefonu, jehož používání se nejdříve bránil a který ovšem nyní využívá pouze pro základní funkce související s klasickou telefonní komunikací (telefonní hovor, SMS). Užívá si zaslouženého důchodu s vnoučaty.

Řešení: Jedná se o uživatele, u kterého se předpokládá, že systém nebude využívat, či s ním, jakkoliv pracovat.

4.5.3 Návrh struktury desktopové aplikace

1. **Přihlašovací formulář**

   Umožní obsluze přihlášení do pokladního systému pomocí přihlašovacích údajů nebo PINu.

2. **Hlavní menu**

   Nabídne rychlý přístup k dalším úrovním systému v podobě přehledných dlaždic.

3. **Nastavení**

   Nabídne možnosti nastavení v rámci pokladního systému. Tj. volba konané akce, výběr prodejní lokace a konkrétních klapek ze seznamu dostupných možností.

4. **Tvorba prodejních položek**

   Poskytne možnost vytvoření nové prodejní položky, editaci již stávajících položek, či jejich mazání. Současně poskytne přehled nad všemi dosud vytvořenými položkami.

5. **Tvorba klapek**

   Návrhář pokladních klapek. Umožní vytvořit seznam s libovolným množstvím provozovaných skupin, mezi kterými lze přepínat dle aktuální potřeby. Každá skupina klapek nabídne čtvercovitou maticovou síť velikosti 8x8, která bude sloužit jako základ pro ukotvení navrhovaných klapek na principu bitmapy. Návrhář u klapek umožní definovat pozici, velikost, barvu pozadí, barvu písma a prodejní položku.

6. **Pokladna**

   Hlavní část aplikace. Pracovní plocha pokladny poskytne funkci markování prodejních položek a uskutečnění plateb. Matice použitelných položek se vykreslí na základě nastavení pokladny výběrem dostupných klapek z vytvořeného seznamu. Potvrzení platby vyvolá spojení s NFC čtečkou pro dokončení aktuálně prováděné transakce. Po úspěšně provedené transakci bude vygenerován email s detailem účtenky a zaslán na email zákazníka uvedeného při registraci čipu.

7. **Uzavřené účty**

   Zobrazí všechny doposud uzavřené účty se seznamem položek účtu s možností zpětného uživatelského storna v případě vytvoření chyby při odbavování zákazníka.

8. **Uživatelé**

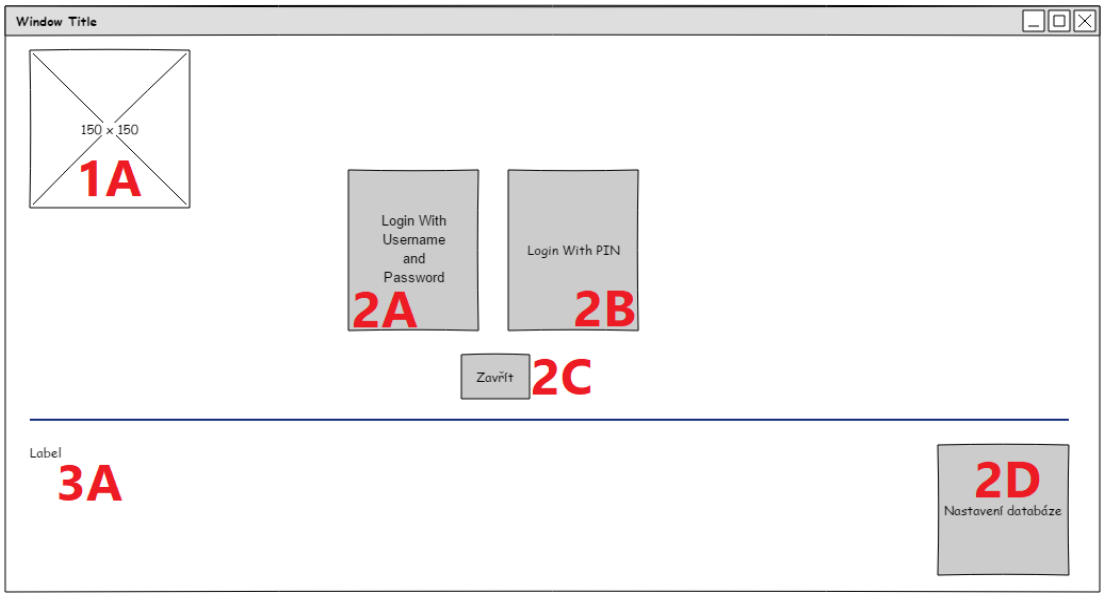
   Poskytne možnost vytvoření nového uživatele obsluhy, editaci již stávajících uživatelů, či jejich mazání. Současně poskytne přehled nad všemi dosud vytvořenými uživateli obsluhy.

9. **Manažer připojení databáze**

   Konfigurační utilita pokladního systému. Umožní přímé připojení k jakémukoliv dostupnému databázovému serveru.

4.5.4 Rozvržení rozhraní desktopové aplikace

4.5.4.1 Logický design přihlašování



Obrázek 9 - Wireframe přihlašování

1. **Obrázek**
    a) Logo systému
2. **Tlačítko**
    a) Přihlášení přihlašovacími údaji
    b) Přihlášení PINem
    c) Zavření systému
    d) Nastavení databáze
3. **Label**
    a) Informace o systému

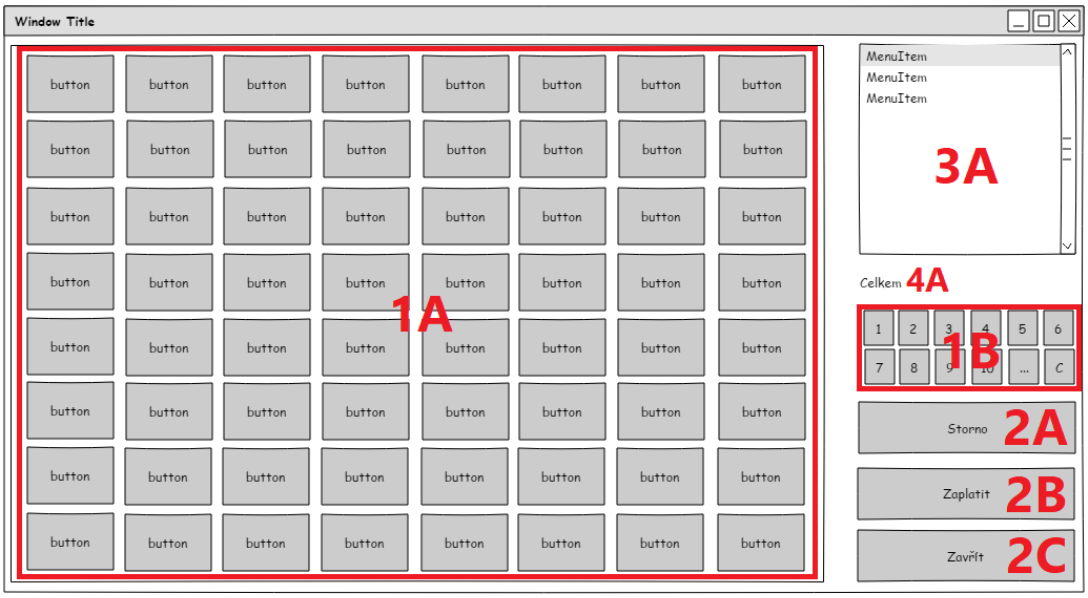
4.5.4.2 Use Case – Přihlašovací formulář

1. Uživatel očekává:
    b) Možnost nastavení připojení databáze
    c) Vyplnění přihlašovacích údajů nebo PINu
        - Uživatelské jméno
        - Hesla
        - PINu
    d) Po vyplnění validních údajů
        - Zobrazení hlavního menu
    e) Upozornění v případě nevalidních údajů

4.5.4.3 Scénář – Přihlašovací formulář

1. Systém zobrazí:
    a) Logo systému
    b) Tlačítko přihlášení uživatelským jménem a heslem
        - Po kliknutí systém zobrazí dotykovou klávesnici k zadání údajů
    c) Tlačítko přihlášení PINem
        - Po kliknutí systém zobrazí dotykovou klávesnici k zadání PINu
    d) Tlačítko nastavení databáze
        - Po kliknutí systém zobrazí formulář pro nastavení databáze

4.5.4.4 Logický design pokladny



Obrázek 10 - Wireframe pokladny

1. **Pole tlačítek**
    a) Klapky prodejních položek
    b) Množství
2. **Tlačítko**
    a) Storno
    b) Zaplatit
    c) Návrat do menu systému
3. **ListMenu**
    a) Seznam namarkovaných položek
4. **Label**
    a) Celková částka transakce

4.5.4.5 Use Case – Pokladna

1. Uživatel očekává:
    a) Možnost namarkování položek
    b) Zobrazení namarkovaných položek v seznamu
    c) Storno položky v seznamu
    d) Platbu objednávky
    e) Možnost návratu do hlavního menu

4.5.4.6 Scénář – Pokladna

1. Systém zobrazí:
    a) Pole klapek pokladny
        - Vyčkává na interakci uživatele
        - Po kliknutí se položka zobrazí v seznamu namarkovaných položek
    b) Pole rychlé volby množství
        - Po kliknutí lze namarkovat zvolené množství konkrétní položky
        - Po kliknutí „…“ systém umožní zadat libovolné množství
        - Po kliknutí „C“ systém vynuluje zvolené množství
    c) Seznam namarkovaných položek
        - Zobrazí aktuální seznam namarkovaných položek
        - Po kliknutí na položku seznamu lze položku stornovat
    d) Tlačítko storno
        - Po označení položky seznamu umožní storno označené položky
    e) Tlačítko zaplatit
        - Po kliknutí zobrazí rozhraní pro platbu bezkontaktním NFC čipem
            - Je-li čip přijat – přechází do stavu transakce úspěšná
            - Je-li čip zamítnut – přechází do stavu transakce neúspěšná
    f) Tlačítko zavřít
        - Po kliknutí zobrazí hlavní menu

4.5.5 Návrh struktury webové aplikace

Webová aplikace rozděluje zobrazovaný obsah na základě rolí, které uživatel v systému představuje. Z pohledu návrhu uživatelského rozhraní je kladen důraz na

responzivitu celé aplikace, kdy se předpokládá, že většina přístupů do webové aplikace bude tvořena mobilní platformou oproti verzi desktopové.

Administrátorské rozhraní

1. **Přihlašovací formulář**

   Umožní obsluze přihlášení do administrátorské zóny webového rozhraní pomocí přihlašovacích údajů.

2. **Dashboard**

   Úvodní obrazovka rozhraní po přihlášení do systému. Nabídne rychlý základní přehled nad systémem v podobě nástěnky s informacemi určenými pro roli administrátora systému.

3. **Prodejní položky**

   Poskytne možnost vytvoření nové prodejní položky, editaci již stávajících položek, či jejich mazání. Současně poskytne přehled nad všemi dosud vytvořenými položkami.

4. **Uzavřené účty**

   Zobrazí všechny doposud uzavřené účty se seznamem položek účtu s možností zobrazení detailu účtenky, která se bude shodovat s účtenkou v emailu zákazníka.

5. **Statistiky**

   Nabídne přehledné statistické reporty z oblasti tržeb, prodejů a storna na základě vybraných kritérií lokace a datumu.

6. **Lokace**

   Poskytne možnost vytvoření nové prodejní lokace, editaci již stávajících lokací, či jejich mazání. Současně poskytne přehled nad všemi dosud vytvořenými lokacemi.

7. **Objednávky**

   Vypíše seznam přijatých objednávek bezkontaktních platebních NFC čipů.

8. **Zákazníci**

   Zobrazí přehled nad registrovanými zákazníky systému a majiteli bezkontaktních NFC čipů, včetně kompletních profilů a seznamu vlastněných platebních tokenů a jejich správy a autorizace z pohledu platnosti jednotlivých tokenů a možnosti dobití kreditu. Zároveň umožní zobrazit seznam validních objednávek nových čipů konkrétních uživatelů.

9. **Nastavení**

   Nabídne možnosti nastavení v rámci pokladního systému. Tj. založení nového eventu, volba konané akce ze seznamu dostupných možností, nastavení uživatelů a správa měrných jednotek produktů.

Klientské rozhraní

1. **Dashboard**

   Úvodní obrazovka rozhraní po přihlášení do systému. Nabídne rychlý základní přehled nad systémem v podobě nástěnky s informacemi určenými pro roli zákazníka.

2. **Účty**

   Zobrazí všechny zákazníkovi doposud uzavřené účty se seznamem položek účtu s možností zobrazení detailu účtenky, která se bude shodovat s účtenkou v emailu zákazníka.

3. **Statistiky**

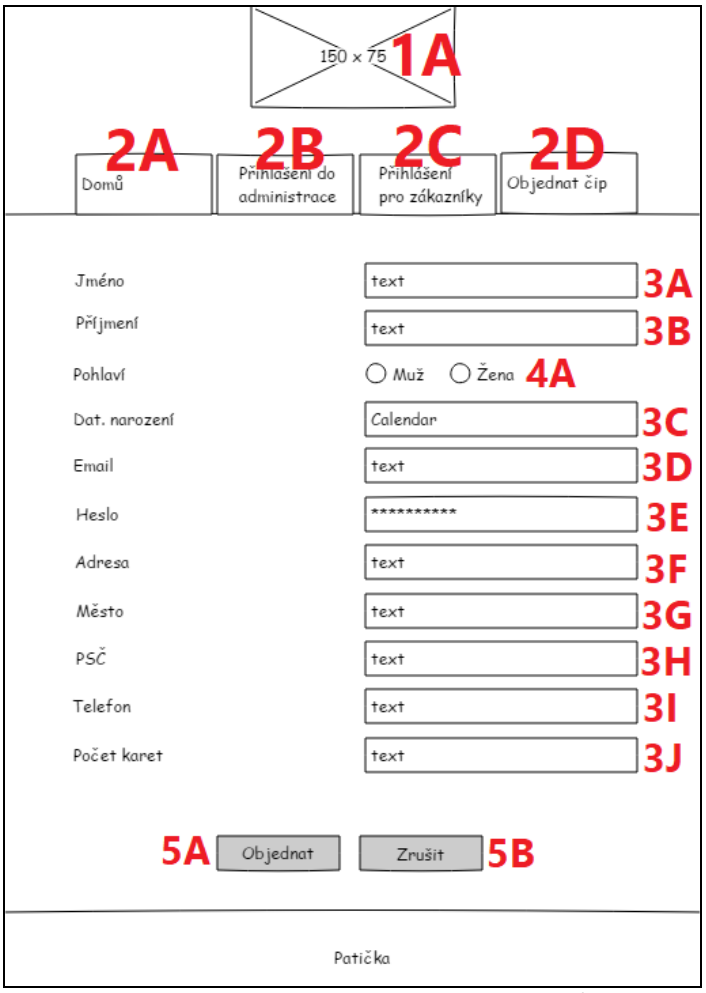
   Nabídne přehledné statistické reporty z oblasti nákupů na základě vybraných kritérií lokace a datumu.

4. **Správa čipů**

   Poskytne přehled nad všemi zákazníkovými platebními čipy s informací o jeho platnosti a výši zůstatku kreditu na jednotlivých čipech.

4.5.6 Rozvržení rozhraní webové aplikace

4.5.6.1 Logický design objednávky čipů



Obrázek 11 - Wireframe objednávek čipů

2. **Obrázek**
    a) Logo systému
3. **Menu záložek**
    a) Domů
    b) Přihlášení do administrace
    c) Přihlášení pro zákazníky“
    d) Objednat čip
4. **InputBox**
    a) Jméno
    b) Příjmení
    c) Datum narození
    d) Email
    e) Heslo
    f) Adresa
    g) Město
    h) PSČ
    i) Telefon
    j) Počet karet

5. **RadioButton**
    a) Pohlaví
6. **Tlačítko**
    a) Objednat b) Zrušit

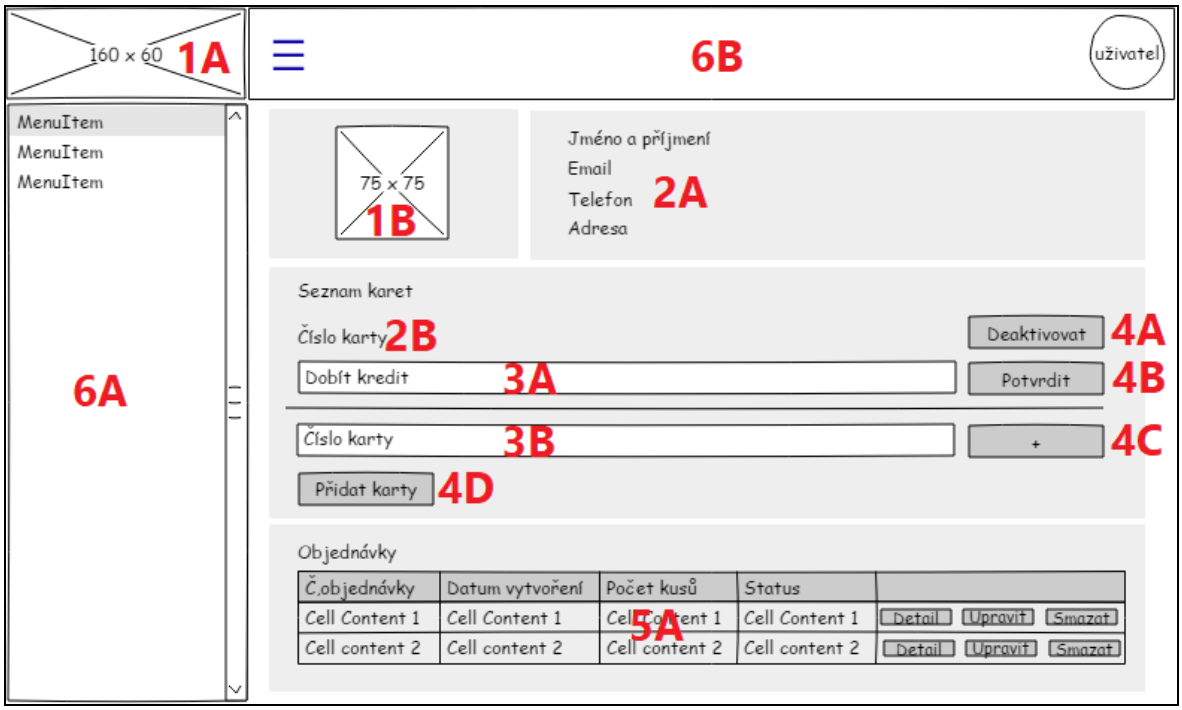
4.5.6.2 Use Case – Objednávka čipů

1. Uživatel očekává:
    a) Vyplnění údajů
    b) Možnost vytvoření objednávky čipů

4.5.6.3 Scénář – Objednávka čipů

1. Systém zobrazí:
    a) Objednávkový formulář
        - Vyčkává na interakci uživatele
    b) Tlačítko Objednat
        - Po vyplnění validních informací vytvoří novou objednávku
        - Po vyplnění nevalidních informací vypíše chybně zadané hodnoty
    c) Tlačítko Zrušit
        - Po kliknutí přesměruje na úvodní obrazovku

4.5.6.4 Logický design profilů



Obrázek 12 - Wireframe profilu zákazníka

1. **Obrázek**
   a) Logo systému
   b) Avatar uživatele
2. **Label**
   a) Informace o zákazníkovi
   b) Číslo čipu
3. **InputBox**
   a) Dobíjená částka
   b) Číslo nového čipu
4. **Tlačítko**
   a) Aktivace / deaktivace čipu
   b) Potvrzení dobití částky
   c) Přidat více čipů
   d) Přidat zvolené čipy
5. **Tabulka**
   a) Seznam objednávek zákazníka
6. **Menu**
   a) Menu aplikace – template
   b) Hlavička aplikace – template

4.5.6.5 Use Case – Profil zákazníka

1. Uživatel očekává:
   a) Zobrazení základních informací zákazníka

b) Zobrazení seznamu čipů zákazníka
c) Vytvoření nového čipu
d) Možnost dobití kreditu jednotlivých NFC čipů zákazníka
e) Možnost aktivovat / deaktivovat konkrétní NFC čip zákazníka
f) Zobrazení seznamu všech vytvořených objednávek zákazníka

4.5.6.6 Scénář – Profil zákazníka

1. Systém zobrazí:
    a) Základní informace o zákazníkovi
        - Muž – vykreslí siluetu muže
        - Žena – vykreslí siluetu ženy
    b) Seznam aktivních a neaktivních NFC čipů
        - Pro vytvoření nového čipu (možnost hromadného přidávání čipů) systém vyžaduje zadání reálného UID bezkontaktního NFC čipu a následné potvrzení tlačítkem „Přidat karty“.
            - Systém vygeneruje 16-ti místný identifikační token
        - Pro dobití kreditu systém vyžaduje vyplnění validní hodnoty a potvrzení tlačítkem „Potvrdit“
            - Čip je aktivní – systém vyžaduje deaktivaci čipu
            - Čip je neaktivní – systém vyžaduje aktivaci čipu
    c) Seznam objednávek
        - Vyřízeno – systém označí zeleně
        - Nevyřízeno – systém označí červeně

4.6 Databáze

Jako systém řízení báze dat (zkr. DBMS) byl zvolen objektově relační databázový klient PostgreSQL. Společně s bází dat byl vytvořen databázový systém, který dodržuje obecně přijímané standardy normalizace relačního modelu databáze a jejich forem. Databázový systém tvoří podstatnou část obou vyvíjených aplikací, je proto také dodržena integrita dat na základě platných integritních omezení. Jednotlivé entity jsou v rámci těchto omezení navrženy a navzájem provázány tak, aby bylo možné skrze složený SQL dotaz dosáhnout kterékoliv entity v systému.

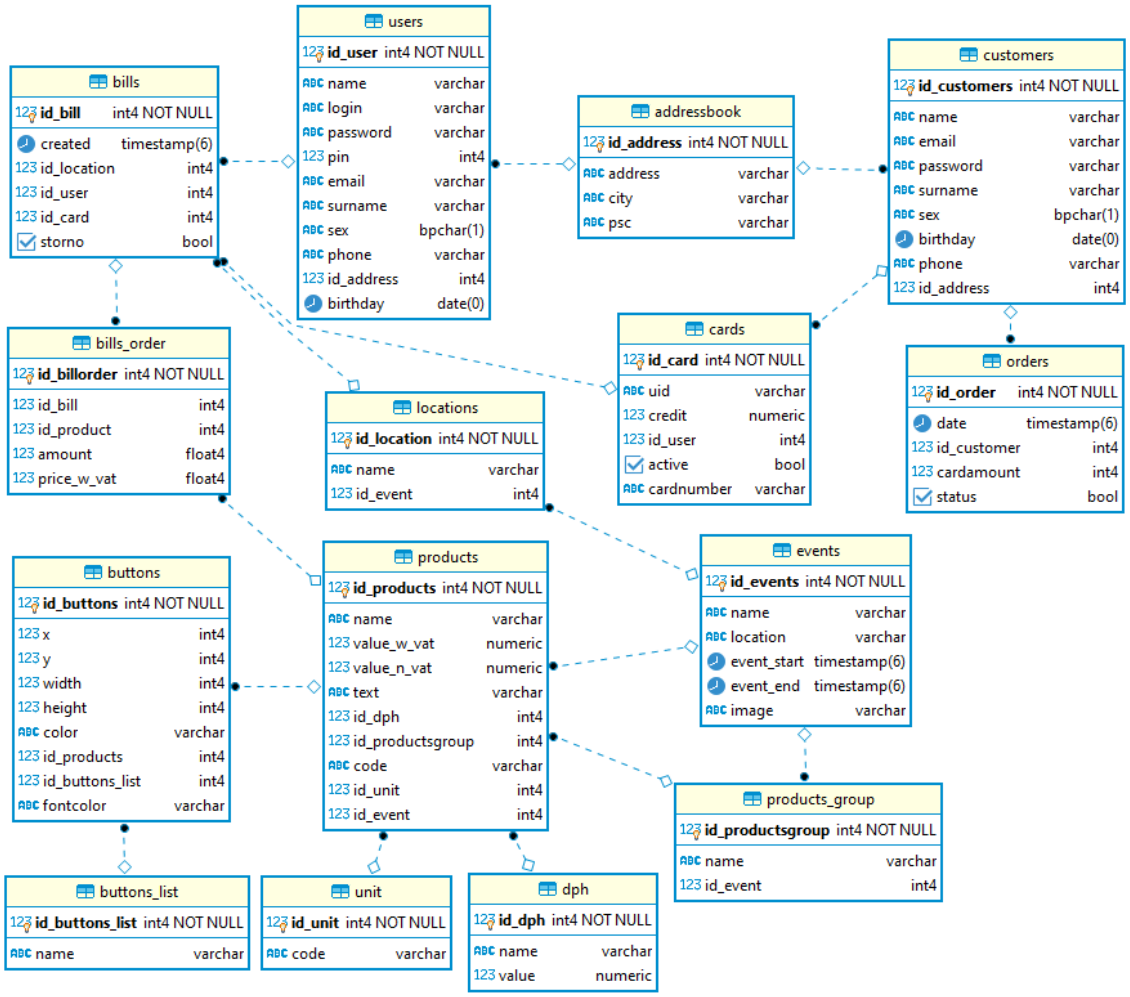
Připojení k databázovému systému je v desktopové i webové aplikaci realizováno pomocí připojovacích řetězců (angl. connectionString)

Připojení desktopové aplikaci k DB – realizováno poskytovatelem NPGSQL

```
string connectionstring = String.Format("Server={0};Port={1};Database={2};User
Id={3};Password={4}", HostTXT.Text, PortTXT.Text, DatabaseTXT.Text, UserTXT.Text,
PassTXT.Password);
```

Připojení webové aplikaci k DB – realizováno poskytovatelem PG

```
const connectionString =
`postgresql://${process.env.DB_USER}:${process.env.DB_PASSWORD}@${process.env.DB_HOST}:$
{process.env.DB_PORT}/${process.env.DB_DATABASE}`;
```



Obrázek 13 - Návrh struktury databáze

4.6.1 Popis entit systému

Databázový model se skládá z celkem 15 tabulek a je navržen tak, aby kopíroval skutečný model reality. Celá databázová struktura je vytvořena tak, aby se její dílčí části odvíjely na základě konkrétně pořádané akce. To znamená, aby požadovaný zobrazovaný obsah byl vázán vždy ke konkrétní akci a nemohlo dojít k záměně, redundanci nebo duplicitě dat mezi eventy.

Název tabulky	Popis
Users **(Uživatel administrator)**	Entita představující uživatele v roli administrátora (tj. osoby pověřené vedením společnosti prací se systémem. Např. management společnosti, obsluha atd).
Customers **(Uživatel zákazník)**	Entita představující uživatele v roli hosta, resp. zákazníka**.** Vstupuje do systému jako osoba s vlastním přístupem a pravomocemi při užívání systému. Zákazník nemá přístup do administrátorské části systému.
Addressbook **(Seznam adres)**	Tabulka pro uložení adres jednotlivých uživatelů a zákazníků. Ve vztahu addressbook a users, rovněž jako ve vztahu addressbook a customers se vždy jedná o kardinalitu typu 1:1 (tj. každému zákazníkovi nebo uživateli je přiřazena právě jedna adresa ze seznamu).
Orders **(Objednávky karet zákazníků)**	Tabulka představující entitu objednávky identifikačního čipu či bezkontaktní karty zákazníka. Na základě vytvoření objednávky zákazníkem a jejího následného zpracování administrátorem je zákazníkovi zaslán nový bezkontaktní čip dle množství kusů zadaného v objednávce. Tabulka je vázána na zákazníka kardinalitou 1:N (tj. každá objednávka patří právě jednomu zákazníkovi a každý zákazník má možnost vytvořit N objednávek)
Cards **(Bezkontaktní platební karty, čipy)**	Tabulka obsahující seznam všech vytvořených karet systému reprezentující entitu bezkontaktního platebního čipu nebo karty. Na základě atributu active je definováno, zda je čip platný a lze s ním provádět operace spojené s placením, či bylo administrátorem systému zakázáno jeho používání a čip byl vyřazen z oběhu. Zároveň entita uchovává informaci o stavu konta konkrétního čipu v podobě částky přednabitého kreditu. Karta je vázána na zákazníka vazbou 1:N (tj. každá jedna karta připadá konkrétnímu zákazníkovi, ale každý zákazník může vlastnit N karet).

Název tabulky	Popis
Bills **(Seznam provedených transakcí)**	Tabulka zaznamenávající každou úspěšně provedenou transakci bezkontaktním čipem. Tabulka uchovává informaci o tom, kdy byla transakce vytvořena, kdo transakci vytvořil a kým byla zaplacena, kdy informace, kým byla transakce zaplacena odkazuje na bezkontaktní kartu nebo čip, kterým byla transakce uhrazena. Zároveň je každá transakce přiřazena lokaci, na které byla uskutečněna, případně, zda byla transakce následně stornována.
bills_order **(Seznam položek tranksakce)**	Jedná se o vazební tabulku mezi tabulkami bills a products rozšířenou o atributy amount a price_w_vat. Tabulka uchovává informace o objednaných produktech vztahující se ke konkrétnímu účtu a jejich množství a ceně.
products_group **(Kategorie produktů)**	Tabulka s názvy kategorií nabízených produktů. Tvoří vazbu s tabulkou produktů, které obsahuje.
Products **(Seznam produktů)**	Tabulka Products je seznamem prodávaných produktů. Shromažďuje atributy o produktu jako je název, kód nebo cena produktu s odkazem na její měrnou jednotku, dph a skupinu produktů do které patří.
Unit **(Měrné jednotky produktů)**	Tabulka se seznamem použitelných měrných jednotek pro daný produkt. Je provázána kardinalitou s tabulkou produktů vazbou 1:N.
Dph **(Sazby DPH produktů)**	Tabulka reálných sazeb DPH použitelných u jednotlivých produktů. Je provázána kardinalitou s tabulkou produktů vazbou 1:N.
Events **(Seznam pořádaných akcí)**	Tabulka pořádaných eventů. Důležitá tabulka z pohledu plateb a rozvržení lokací na pořádané akci. Je provázána s množstvím tabulek, které na základě zvolené akce reagují při zobrazování obsahu a manipulaci s daty. Rovněž obsahuje informace spojené s konáním akce, místem a názvem, případně úvodním obrázkem. Jedná se o Entitu nejvyšší úrovně celé struktury.
Locations **(Lokace prodejních míst)**	Tabulka lokací představující jakousi podskupinu eventů. Eviduje lokace o reálných prodejních místech na konané akci. Lokace je vždy vytvořena na základě příslušné akce a měla by obsahovat výstižný název pro následnou identifikaci prodejního místa, např. Pivo sektor1, Bar podium atd.

Název tabulky	Popis
buttons_list **(Seznam klapek)**	Tabulka kompletního seznamu klapek. Obsahuje pouze atributy id_buttons_list a name. Pro lepší správu a práci se systémem je v ideálním případě vhodné pojmenovat položku seznamu dle příslušné lokace prodejního místa, ke kterému budou klapky využity. Klapky je možné opakovaně použít na více pořádaných akcí, resp. eventech.
Buttons **(Klapky)**	Tabulka jednotlivých klapek je spojena vazbou 1:N s tabulkou buttons_list a vázána na konkrétní produkt, který představuje. Každá klapka tak patří právě do jednoho seznamu klapek a seznam klapek obsahuje N klapek.

Tabulka 10 - Popis tabulek databáze

4.7 Bezkontaktní NFC čtečka čipových karet

Bezkontaktní NFC čtečka ACS ACR122U byla pro vývoj pokladního systému primárně zvolena pro své univerzální použití, interoperabilitu a rozhraní podporující většinu typů bezkontaktních čipů a karet.

Mimo to, že NFC čtečka umožňuje čtení dat z bezkontaktních čipů a karet, podporuje též zápis dat na bezkontaktní médium. Čtečka ACS ACR122U má provozní frekvenci 13,56 MHz a podporu rozhraní PC/SC a Smart Card ISO 14443 Typ A a B, včetně všech čtyř typů značek NFC MIFARE nebo jakékoli bezkontaktní karty založené na protokolu FeliCa.

Standardně je tato bezkontaktní čtečka využívána při aplikacích ověřování identity, elektronických plateb, řízení přístupu atd.

Obrázek 14 - Bezkontaktní NFC čtečka ACS ACR122U

4.7.1 Implementace bezdrátové NFC čtečky ASC ACR122U

Bezkontaktní čtečka ACS ACR122U je do systému implementována v podobě dvou tříd Card.cs a NFCReader.cs, které společně fungují jako interface pro komunikaci s hardwarem čtečky a jeho možnosti ovládání. Implementace se zakládá na standardu interoperability PC/SC, čímž splňuje teoretický předpoklad integrace libovolné čtečky s podporou standardu PC/SC.

Třída Card.cs definuje možné stavy, které vychází z teoreticky předpokládaných stavů, ve kterých se NFC čtečka během zapnutého stavu může nacházet a jež jsou popsány v dokumentaci dodávané k zařízení. Dále třída pokrývá seznam potencionálních chybových kódů, resp. návratových hodnot čtecího zařízení a komunikuje se systémovou knihovnou winscard.dll, která do programu importuje důležité funkce poskytující jejich použití na úrovni aplikačního rozhraní.

Knihovna winscard.dll po interakci NFC čtečky s bezkontaktním čipem třídě předá stavový kód návratové hodnoty a třída následně vrátí příslušnou zprávu o aktuálním stavu. Nejsou-li během transakce nalezeny žádné chyby, knihovna vrátí stavový kód `0 (0x0)`, který se následně uloží do proměnné `SCARD_S_SUCCESS`.

Druhá třída NFCReader.cs vychází z třídy Card.cs a aplikuje funkce pro ovládání čtečky, které jsou následně volány v dalších úrovních programu. Primárně jsou v třídě zastoupeny funkce pro navázání a ukončení spojení programu se čtečkou a funkce umožňující čtení a zápis na bezkontaktní NFC médium skrze funkce importované knihovny winscard.dll v třídě Card.cs.

Aby bylo možné předcházet zamrzání celého systému během navázání spojení se čtecím zařízením, je třeba využít možnosti multithreadingu a operace spojené s komunikací mezi hardwarem čtečky a programem spouštět paralelně v novém vlákně (angl. Thread) kořenového procesu.

```
public bool Connect()
{
    string readerName = GetReadersList()[0];
    connActive = true;
    retCode = Card.SCardConnect(hContext, readerName, Card.SCARD_SHARE_SHARED,
                        Card.SCARD_PROTOCOL_T0 | Card.SCARD_PROTOCOL_T1, ref hCard, ref Protocol);
    if (retCode != Card.SCARD_S_SUCCESS)
    {
        connActive = false;
        return false;
    }
    else
        return true;
}
public void Disconnect()
{
    if (connActive)
    {
        retCode = Card.SCardDisconnect(hCard, Card.SCARD_UNPOWER_CARD);
    }
}
```

Obrázek 15 - Navázání komunikace s bezkontaktní NFC čtečkou

4.8 Platební bezkontaktní karty a čipy

Prodej položek na obslužných lokacích je realizován pomocí bezkontaktních čipů a karet. V současnosti jsou systémem podporovány 3 typy bezkontaktních NFC identifikátorů. Jedná se o NFC identifikátory, které jsou v rámci systému otestovány a jsou se systémem plně kompatibilní. Konečný počet funkčních NFC čipů muže být reálně několikanásobně vyšší.

4.8.1 Bezkontaktní NFC karty

Bezkontaktní NFC karty jsou díky svým rozměrům, odpovídající klasickým platebním kartám, nejčastější volbou identifikačních čipů pro běžné pokladní systémy. Vzhledem k jejich popularitě na poli bezkontaktních identifikátorů jsou implementovány i do vyvíjeného pokladního systému, nejsou však nejvhodnějším kandidátem kvůli nepraktickému použití na konaných akcích, zejména festivalech, kde hrozí jejich snadné odcizení nebo ztráta.

Vzhledem k použité čtečce bezkontaktních čipů ACS ACR122U lze použít jakoukoli bezdrátovou kartu MIFARE ISO 14443 A a B, včetně všech čtyř typů značek NFC MIFARE, ale i jakoukoli bezkontaktní kartu založenou na protokolu FeliCa. Vzhledem k bezpečnosti přenosu dat je doporučeno využívat bezkontaktní NFC karty MIFARE DesFire.

Obrázek 16 - Bezkontaktní NFC karty

4.8.2 Bezkontaktní NFC čipy

Bezkontaktní NFC čipy pro použití v průběhu festivalových akcí lepší volbou než NFC karty. Je to především z důvodu lepšího uložení a manipulaci během placení.

Analogicky jako u bezkontaktních NFC karet je možné využít jakýkoli bezkontaktní čip MIFARE ISO 14443 A a B nebo FeliCa.

Obrázek 17 - Bezkontaktní NFC čipy

4.8.3 Bezkontaktní NFC náramky

Použití bezkontaktního NFC náramku je v podmínkách jakýchkoli festivalových akcí ideálním řešením. Jedná se o silikonový voděodolný náramek s NFC čipem, který může mít účastník akce neustále u sebe, aniž by mu jakkoliv překážel. Náramek má ovšem majitel neustále na očích, proto není tak snadné jej ztratit nebo odcizit jako v případě ostatních řešení.

Obrázek 18 - Bezkontaktní NFC náramky

4.9 Model platebního systému

Před vývojem samotného platebního mechanismu je potřeba zvolit optimální možnost uložení potřebných údajů. Z technického hlediska se nabízejí dva různé přístupy uložení dat. Každý model samozřejmě vykazuje reálné výhody i nevýhody, které je třeba nejdříve důkladně zvážit, vzhledem k účelu, ke kterému má být použit.

4.9.1 Fyzické uložení dat

Prakticky se jedná o uložení dat fyzicky přímo na NFC čipu. Tento přístup se v komplexnějších systémech využívá zřídka a slouží spíše pro uložení méně citlivých údajů, např. vizitky. Platí zde pravilo, že na NFC čipu by nikdy neměli být uloženy důležité informace, kvůli případnému zneužití.

Výhody

1. Přístup k datům i v případě výpadku online režimu

Nevýhody

1. Složitá správa NFC tokenů
2. Bezpečnostní riziko v podobě duplikace NFC čipu
3. Neaktuálnost dat

4.9.2 Virtuální uložení dat

Z praktického hlediska je tento model častějším a bezpečnějším řešením u rozsáhlejších systémů se specifickým zaměřením. Data o NFC tokenu jsou virtuálně

uložena v rámci databáze na vzdáleném serveru. Takto uložená data jsou chráněna před fyzickým zneužitím a jsou lépe škálovatelná. Nevýhodou je nedostupnost dat v případě výpadku spojení s databázovým serverem. Při implementaci tohoto modelu je důležité mít kvalitní a stabilní síťovou infrastrukturu.

Výhody

1. Jednoduchá správa NFC tokenů
2. Bezpečnost
3. Data vždy aktuální
4. Škálovatelnost
5. Implementace do dalších systémů
6. Online stav konta

Nevýhody

1. Nepřístupnost dat v offline režimu

Spuštění produkční verze systému reálně předpokládá nasazení většího množství čipů, které budou fungovat jako platební tokenizační médium s citlivými údaji. Jeho zneužití nebo padělání by mohlo být potencionálně značné riziko, které je třeba brát v úvahu a snažit mu předejít již během vývoje.

Za účelem snížení rizika padělaní platebního tokenu, včetně všech uložených dat a převažujícího množství výhod přístupu virtuálního uložení dat je i z hlediska bezpečnosti a konkrétního zaměření vyvíjeného systému zvolen model, kdy veškerá data bezkontaktního čipu jsou uložena jako záznam v databázi na vzdáleném serveru.

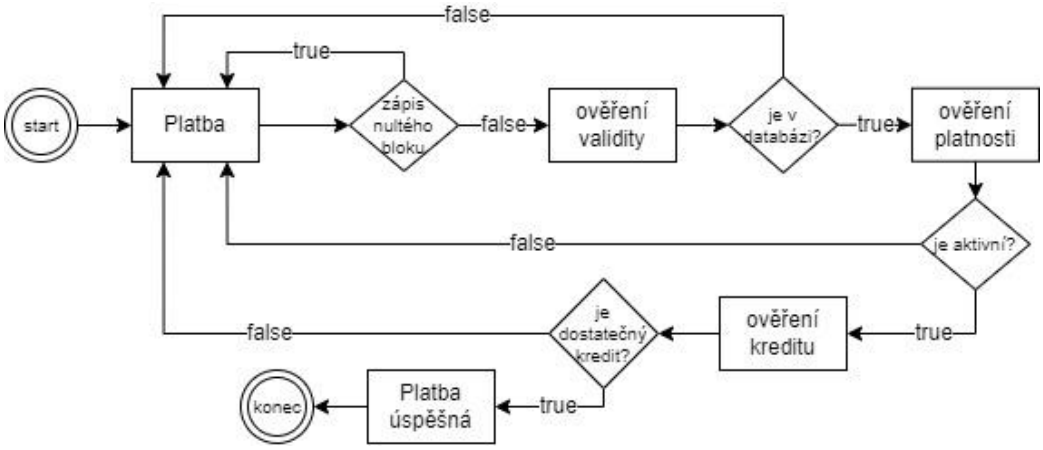
Volba uložení dat na vzdáleném databázovém serveru také klade vyšší nároky na vybudování kvalitní síťové infrastruktury s kvalitním, rychlým a bezpečným přenosem dat, která minimalizuje pravděpodobnost výpadku a ochromení celého systému, což by přineslo značné obchodní ztráty.

Model platebního systému	Použito
Virtuální uložení dat	✓
Fyzické uložení dat	✗

Tabulka 11 - Model platebního systému

Celý model je založen na unikátním 4 byte dlouhém identifikačním čísle (UID) každého bezkontaktního čipu, které jednoznačně identifikuje každý čip. Toto identifikační číslo je uloženo v nultém bloku karty, je definováno výrobcem a nelze jej přepsat. Protože jsou v současnosti distribuovány i bezkontaktní čipové karty s přepisovatelným nultým blokem (NFC MagicCard), budou systémem uznávány pouze karty, které mají pevně definovaný a nepřepisovatelný blok vyhrazený pro identifikační číslo UID.

Tento způsob ověření je realizován pokusem o zápis do nultého bloku identifikačního čipu, určeného pro UID bezkontaktní karty nebo čipu, během procesu ověřování platby. V případě, že systém vyhodnotí pokus o zápis jako úspěšný (tj. vrátí hodnotu true), bezkontaktní karta nebo čip není systémem uznána pro nesplnění podmínky jedinečnosti UID a vydání karty příslušnou autoritou s pevně definovaným identifikačním číslem čipu. V opačném případě (tj. vrátí hodnotu false) je po splnění podmínek aktivace čipu a dostatečného kreditu platba systémem úspěšně přijata.



Obrázek 19 - Ověření platby

4.10 Uživatelské role

Na základě stanovených požadavků na systém, jsou jeho dílčí části řízeny a rozděleny na úrovni uživatelských rolí. Autorizace přístupu dle přidělených uživatelských rolí je běžně uznávanou praxí většiny specializovaných a komplexnějších aplikací. Každý jeden uživatel má tak v rámci systému přístup k obsahu podle role, kterou v systému představuje. V konkrétním případě řešení autorizace jsou role v systému přidělovány za účelem zvýšení bezpečnosti, použitelnosti a přístupnosti celého systému.

Současně se předpokládá, že veškerý personál bude před prací s pokladním systémem a jeho obsluhou zaškolen na konkrétní prodejní lokaci a pracovní pozici, kterou bude vykovávat a k níž bude pokladní systém využívat. Jedině tak může být využit plný potenciál automatizace prodejních procesů a osvojení práce se systémem.

4.10.1 Role administrátora

Role administrátora je zásadní z důvodu obsluhy a práce se systémem. Administrátor má zvýšená oprávnění z pohledu autorizace uživatele pro účel správy celého systému a přístupu do obsluhy pokladního systému.

Uživatel v roli administrátora získává přístup do aplikace pokladního systému, jakožto kvalifikovaný a pověřený uživatel obsluhy, kterému je na základě přidělené lokace umožněno provádět obchodní a platební transakce.

Mimo přístupu do desktopového klienta pokladního systému je uživateli přidělen přístup do rozšířeného režimu webového rozhraní s možností správy a obsluhy systému, včetně vydávání nových platebních tokenů.

4.10.2 Role zákazníka

Role zákazníka je značně omezena na přístup k obsahu určeného primárně pro osoby vstupující do systému v roli zákazníka (tj. majitele bezkontaktního platebního čipu). Každý takový uživatel má přístup do klientské zóny webového rozhraní, kde má přehled o svých transakcích a vlastněných bezkontaktních čipech, včetně elektronických kopií účtenek a výše zůstatku kreditu na svých platebních NFC čipech.

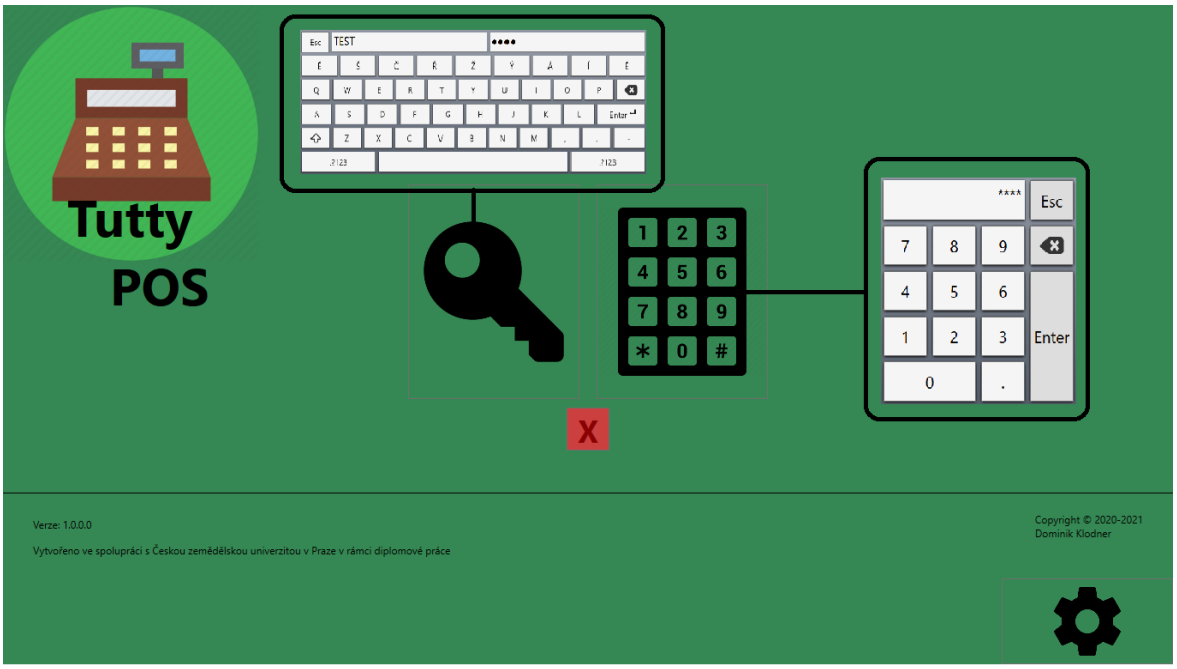
Jakožto majitel bezkontaktního platebního tokenu je uživatel v roli zákazníka pokladním systémem považován za entitu stojící za potvrzením vyvolané transakce, jsou-li splněny veškeré podmínky pro její řádné uzavření.

4.11 Grafický design desktopové aplikace

Grafické rozhraní desktopové aplikace využívá moderních metod tvorby vzhledu aplikace, ke které využívá framework WPF, který je součástí .Net frameworku. Díky databindingu je aplikace více interaktivní a vzhledově atraktivnější.

4.11.1 Přihlašovací obrazovka

Desktopová aplikace, kterou představuje modul pokladny slouží pouze pro interní účely podniku. Přístupy jsou tak omezeny pro administrátory systému, kteří jsou základně tvořeny zaměstnanci podniku jako obsluha prodejního místa. Autentizaci uživatele lze pohodlně provést skrze plnohodnotné přihlašovací údaje uživatele tvořené jménem a heslem nebo příslušným PINem pomocí dotykové klávesnice. Před samotným přihlášením je ještě potřeba nakonfigurovat připojení k databázi s kterou bude pokladní systém následně pracovat.



Obrázek 20 - Grafický design přihlašovací obrazovky

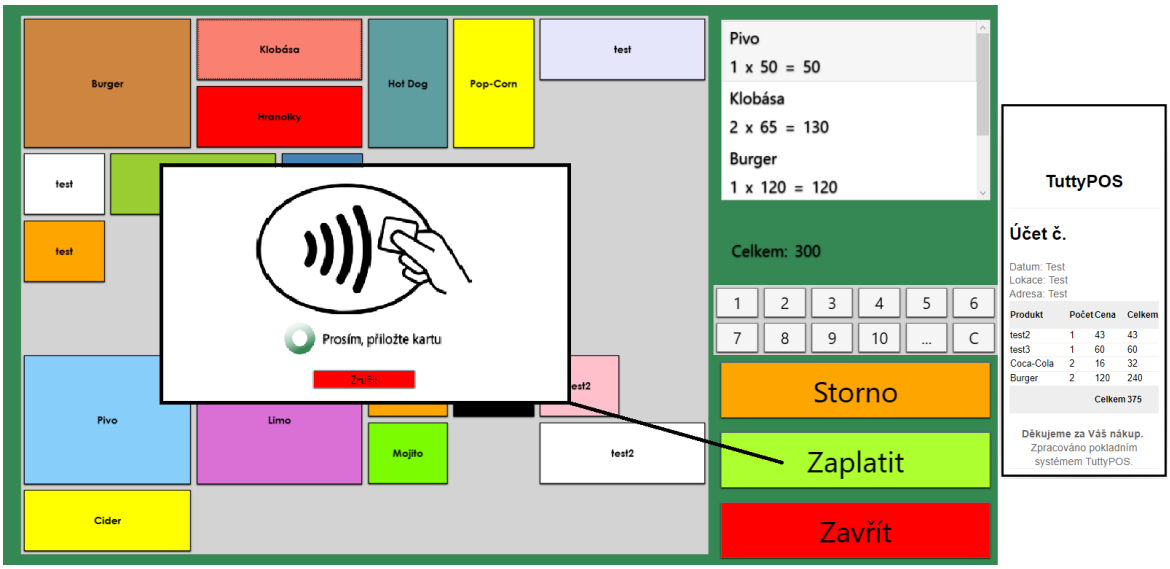
4.11.2 Obrazovka pokladny

Obrazovka pokladny je navržena dle kritérií UI specifikace tak, aby nevytvářela zbytečné nároky na hardware pokladny použitím vektorové grafiky a poskytla plynulý chod aplikace s ohledem na jednodušší práci obsluhy se systémem a rychlou orientaci na panelu prodejních položek.

Obrazovka je tak rozdělena na dvě části, z níž jedna je tvořena pracovní plochou prodejních položek a druhá funkčním panelem pro práci s položkami. Díky rozsáhlým možnostem nastavení panelu klapek (barva pozadí, barva písma, velikost, pozice) je z hlediska kognitivního vnímání softwaru pro uživatele jednodušší orientace v matici

klapek s prodejními položkami a lze tak výsledně dosáhnout rychlejšího odbavení zákazníka.

Panel je co nejvíce intuitivní bez zbytečných matoucích prvků. Během procesu platby je uživatel obsluhy informován o tom, že vyžaduje vyžadována interakce zákazníka přiložením platebního čipu k bezkontaktní NFC čtečce. Následně je tímto dialogem informován i o stavu úspěšnosti uskutečněné transakce. V případě úspěchu je zákazníkovi emailem zaslána kopie účtenky.



Obrázek 21 - Grafický design obrazovky pokladny a kopie účtenky z emailu zákazníka

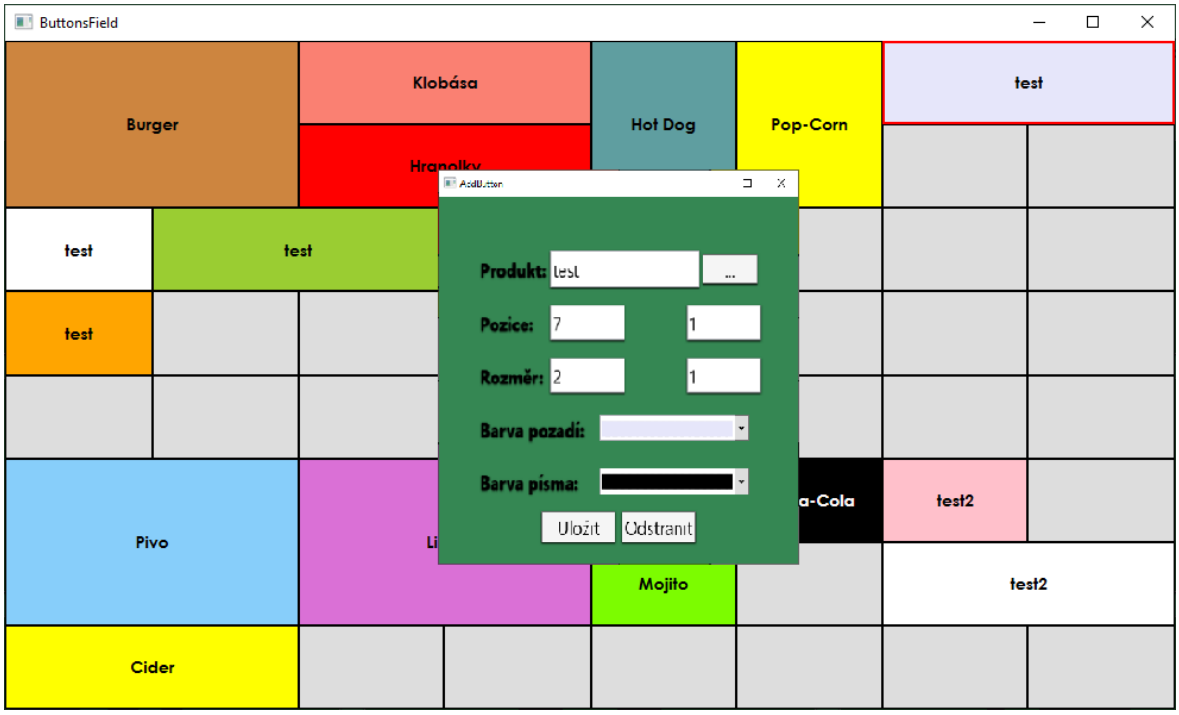
4.11.3 Obrazovka tvorby klapek

Rozhraní tvorby klapek co nejvíce simuluje finální vizuální podobu panelu klapek v pokladně už při samotném návrhu. Prostředí je plně interaktivní a reaguje na požadavky uživatele se změnou parametrů. Veškeré změny je možné provádět pomocí standardního externího příslušenství osobního počítače nebo dotykové obrazovky přímo na pokladně.

Novou klapku je možné vytvořit kliknutím na libovolnou prázdnou dlaždici v matici klapek. Následný dialog umožní klapce přiřadit prodejní položku z nabídky dostupných produktů a nastavit vybrané parametry designu klapky.

Úpravu klapky lze následně provést kliknutím na příslušnou klapku, kdy je zobrazen totožný dialog jako v případě tvorby klapky s již předvyplněnými daty, které má uživatel možnost libovolně editovat.

Pomocí klasické myši je možné u klapky v matici vyvolat rychlou změnu pozice označením požadované klapky pravým tlačítkem myši (okraj klapky bude červený) a následným výběrem libovolné pozice v matici klapek.



Obrázek 22 - Grafický design obrazovky tvorby klapek

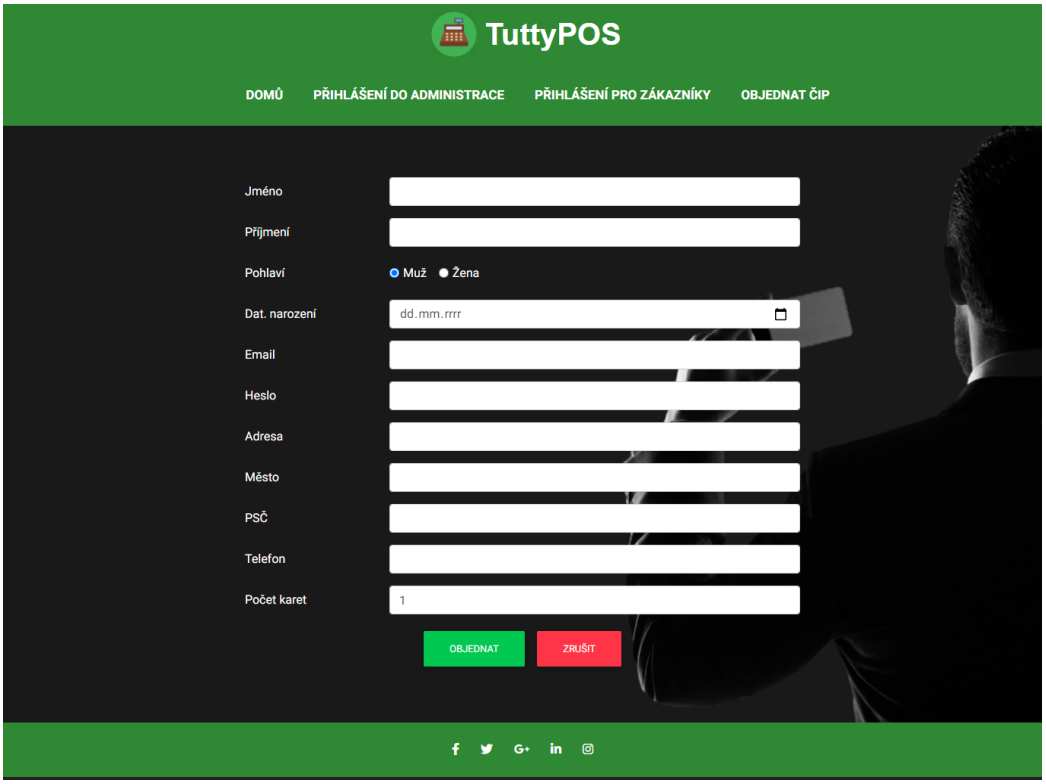
4.12 Grafický design webové aplikace

Grafický design webové aplikace je přizpůsoben responzivnímu designu pro použití na zařízeních různé velikosti a typu.

4.12.1 Obrazovka objednávkového formuláře

Objednávkový formulář slouží zákazníkům při objednávání nového bezkontaktního NFC čipu, či jejich většího množství. Množství objednávaných čipů se uvádí přímo v objednávacím formuláři. Po vytvoření nové objednávky zákazník získává přístup do klientské sekce webové aplikace, kde může své čipy spravovat.

Administrátorská sekce webového rozhraní obsahuje modul správy vytvořených objednávek a vydávání nových čipů. Za poskytované čipy si následně zodpovídá firma, jakožto pořadatel akce. Vydávané čipy nesmí být typu MagicCard – v opačném případě nebudou čipy systémem uznávány.

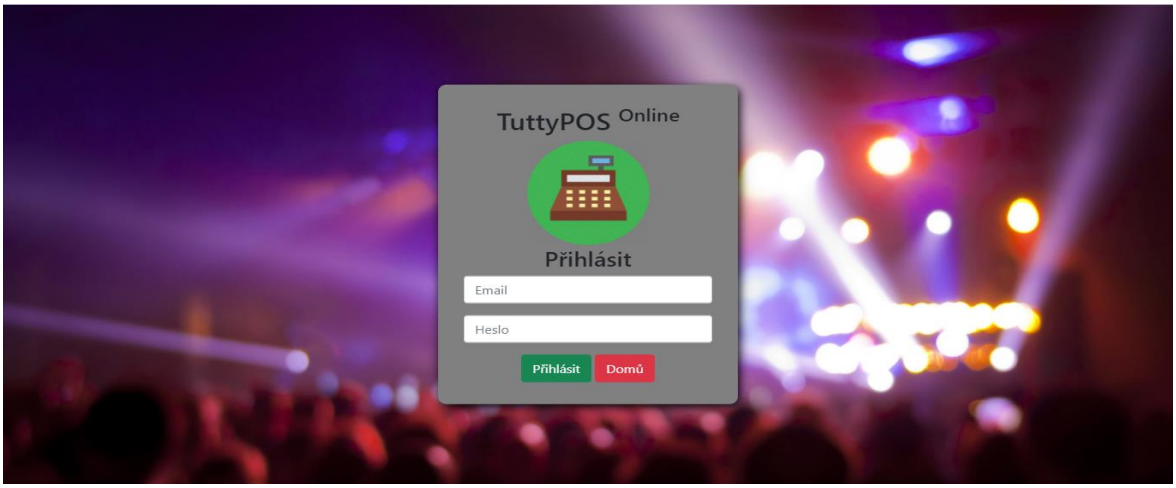


Obrázek 23 - Grafický design obrazovky objednávkového formuláře

4.12.2 Obrazovka přihlašovacího formuláře

Webová aplikace poskytuje dva režimy autentizace uživatele dle systémové role. Před přihlášením si proto uživatel musí zvolit, do které sekce se bude přihlašovat.

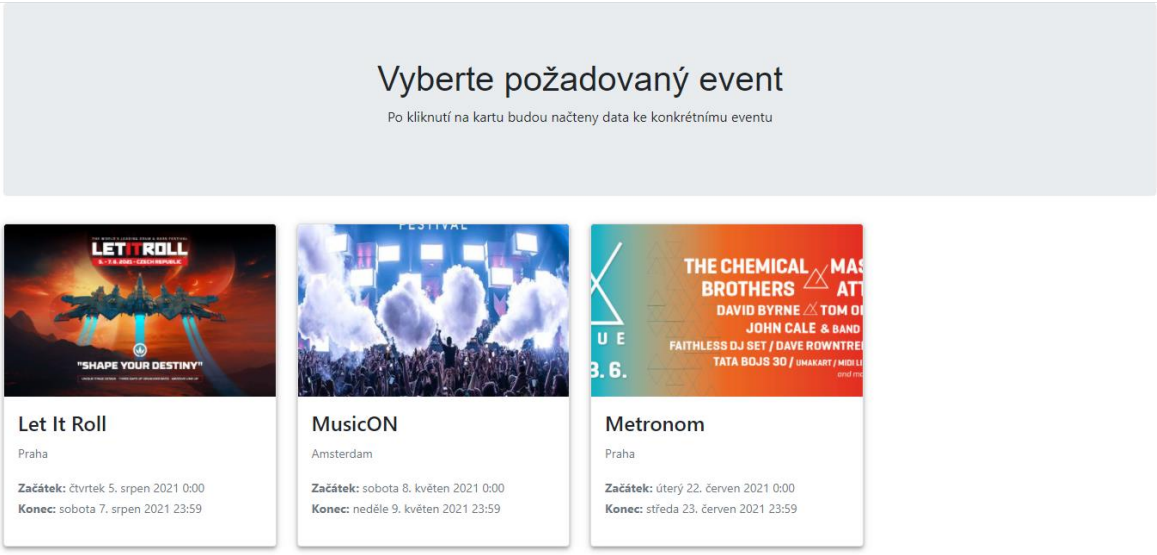
Aplikace nabízí režim pro zákazníky, kam je možné se přihlásit na základě vytvoření objednávky NFC čipu zvoleným e-mailem a heslem. Dále aplikace nabízí režim pro administrátory systému, kteří jsou zpravidla tvořeny zaměstnanci dané firmy a jejichž účet musí být vytvořen správcem systému v rámci dané společnosti.



Obrázek 24 - Grafický design obrazovky přihlašovacího formuláře

4.12.3 Obrazovka výběru eventu

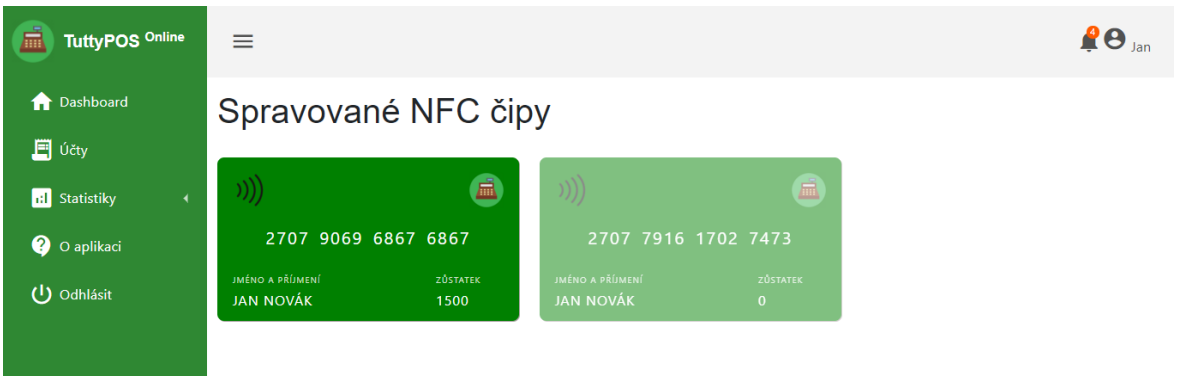
Zobrazovaný obsah webové aplikace je vykreslován v závislosti na volbě uskutečněného eventu, resp. pořádané akce. Po přihlášení je systémem od uživatele vyžadována volba příslušné akce a následně udělen přístup k validním datům. Volbu je následně možné kdykoli změnit přímo v nastavení aplikace.



Obrázek 25 - Grafický design výběru eventu

4.12.4 Obrazovka správy NFC čipů

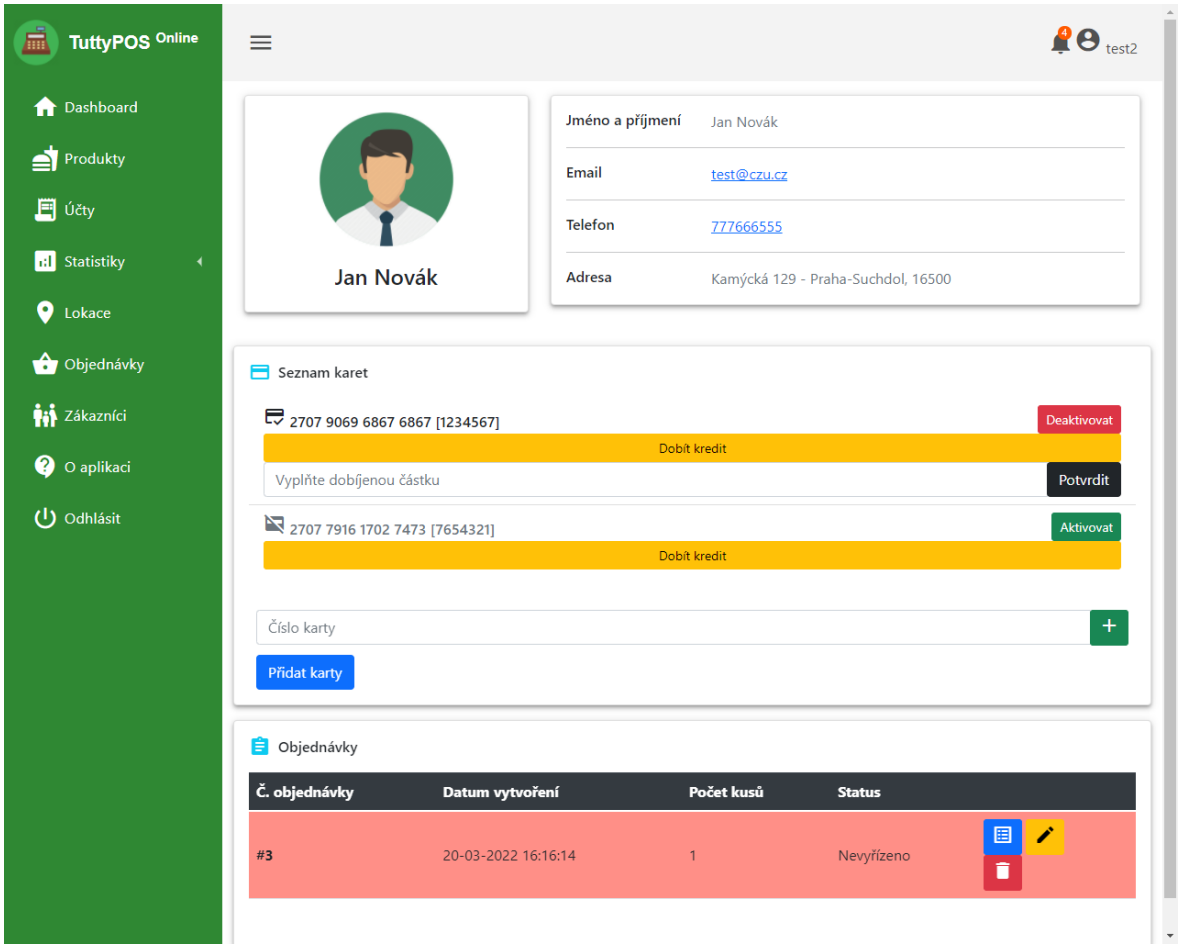
Zákazník má se svým přístupem povolený přístup k přehledu svých NFC čipů. Čipy jsou systémem graficky prezentovány v podobě karet. Karta vždy obsahuje informace o 16-ti místném identifikačním čísle, majiteli karty a zůstatku kreditu. Pomocí grafického rozhraní zákazník také pozná stav platnosti jednotlivých karet nebo čipů. V případě, že je karta vykreslena s efektem průhlednosti, znamená to, že karta není aktivní a nelze ji využít pro uskutečnění jakékoli transakce. V opačném případě je čip validní a připravený pro placení na obslužných místech.



Obrázek 26 – Grafický design obrazovky NFC čipů

4.12.5 Obrazovka profilu zákazníka

Administrátor systému má přístup do profilu zákazníka za účelem správy jeho virtuálně přiřazených tokenů, vytvořených objednávek a dobíjení kreditu bezkontaktních NFC čipů a karet. V profilu má administrátor systému možnost libovolně aktivovat nebo deaktivovat zákazníkovi platební tokeny na základě platného reálného stavu. V případě deaktivace platebního tokenu nebude příslušný NFC čip přijat pokladním systémem pro uskutečnění transakce.



Obrázek 27 - Grafický design obrazovky profilu zákazníka

4.12.6 Obrazovka účtů

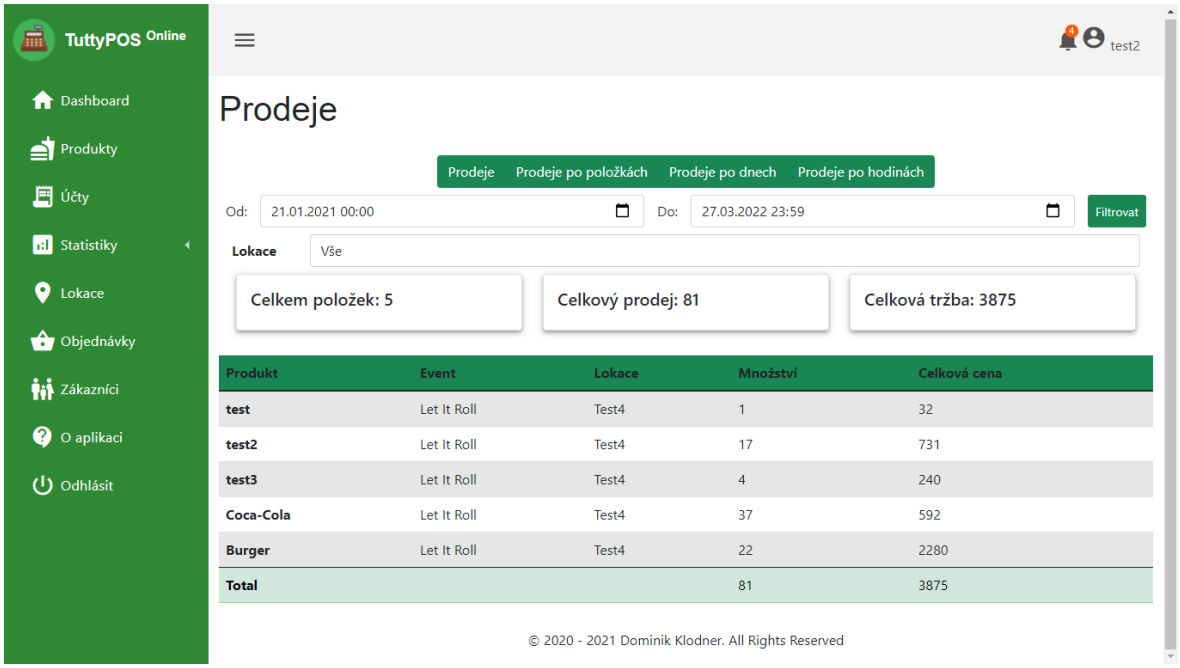
Administrátor systému má přístup ke všem uzavřeným účtům s identifikačními údaji transakce. Účty jsou graficky odlišeny dle aktuálního stavu účtu. Zelenou barvou jsou označeny zpracované účty, červeně jsou označeny účty, které byly obsluhou stornovány.

Po rozkliknutí karty konkrétního účtu má obsluha přehled o detailech účtu, včetně prodaných položek účtu a kopií účtenky.

Obrázek 28 - Grafický design obrazovky účtů a detailu kopie účtenky

4.12.7 Obrazovka statistik

Webová aplikace obsahuje několik typů statistických ukazatelů, které vytváří soubor pokladních reportů. Reporty je možné generovat na základě filtrů datumu a času a lokace prodejního místa. Administrátoři systému tak mají přehled o svých tržbách, prodejích apod. Zákazníci oproti tomu mají přehled např. o svých nákupech.



Obrázek 29 - Grafický design obrazovky statistik

5 Výsledky a diskuse

5.1 Zhodnocení a výsledky

Splnění cílů odpovídá požadavkům stanovených před začátkem vývoje. Vlastní práce realizuje zhotovení dvou fungujících aplikací pro bezkontaktní NFC platby v podobě desktopové verze cashless pokladního systému, který implementuje možnosti bezhotovostních NFC plateb a webového rozhraní pro správu pokladního systému a platebních tokenů s řízením přístupu založeného na rolích, tedy administrátorského a zákaznického přístupu k validnímu obsahu konkrétní role a uživatele, včetně statistických reportů.

Část systému obsahující platební modul pokladního systému se podrobně zaměřuje na bezpečnost transakcí a minimalizuje možnosti padělání NFC čipů vydávaných důvěrnou autoritou a jejich dopady při pokusu o duplikování čipu s použitím MagicCard.

Dále zpracovává detailní dokumentaci a postup vývoje obou systémů, kde je popsána kompletní struktura aplikací, včetně použitých technologií a metodik moderního programování.

5.2 Testování aplikace

Vzhledem k nepříznivé pandemické situaci nebylo možné systémy otestovat v ostrém provozu. Byla proto zvolena testovací skupina uživatelů, pro kterou byly vytvořeny konkrétní testovací scénáře, na jejichž základě proběhlo samotné testování aplikací. Scénáře se zaměřovaly na použitelnost systému, uživatelskou přívětivost, intuitivnost během práce a celkovou funkčnost konkrétních jednotlivých částí systémů.

Většina testovaných subjektů neprokázala výraznější potíže při práci na pokladně a požadované úkoly byly splněny, bez nutnosti školení, pouze na základě intuitivního chápání systému. Uživatelsky složitější se jevilo samotné nastavení systému, u kterého bylo potřeba testované uživatele proškolit. Odhalené chyby při testování funkčnosti dílčích částí systému byly následně analyzovány a opraveny.

Aplikace rovněž podstoupila testování kompatibility různých verzí operačních systémů a platforem. Cílem této fáze testování bylo ověřit kompatibilitu operačních systémů Microsoft Windows pro desktopovou aplikaci a různé platformy klientů pro desktopovou aplikaci. Z testování vyplývá, že desktopová aplikace pokladního systému je

kompatibilní s operačními systémy Microsoft Windows 7 a vyšší. Starší verze nejsou systémem podporovány z důvodu zastaralé verze .Net frameworku. Multiplatformní testování webové aplikace proběhlo úspěšně na všech testovaných zařízeních s operačním systémem Microsoft Windows s nejnovější verzí webového prohlížeče, OS Android a iOS.

U testování náročnosti aplikace bylo zkoumáno využití zdrojů procesoru a operační paměti testovaného hardwaru. Při testování bylo odhaleno značné využití operační paměti RAM během procesu vytváření klapek. Chyba byla způsobena špatně navrženou provázaností logické a grafické částí systému při vykreslování jednotlivých klapek. Tato část systému byla po odhalení chyby optimalizována.

5.3 Diskuse

Oficiálně se jedná o první veřejně dostupný build obou aplikací. Lze tak předpokládat, že systémy v této verzi nebudou ještě zcela odladěny a zbaveny veškerých softwarových chyb, které by přineslo ostré nasazení aplikací do provozu. Je tak potřeba brát v úvahu skutečnost, že v budoucnu bude třeba na základě zkušeností se systémy, jak z pohledu obsluhy, tak i zákazníků, vydávat funkční systémové aktualizace a bezpečnostní záplaty.

Z perspektivy budoucího vývoje softwaru by bylo vhodné zvážit, jakou cestou se bude ubírat vývoj aplikací v následujících letech a rozšířit celý soubor systémů o další moduly nebo celé aplikace.

Vedle základní desktopové aplikace pokladny by proto paralelně mohla vzniknout samostatná a kompaktnější verze aplikace pokladny pro operační systém Android, která by přinesla nové možnosti rozšíření celé aplikace, menší hardwarovou náročnost, nižší pořizovací náklady a jednodušší implementaci. Mimo jiné by konkurovala dnešním moderním systémům založeným na této platformě.

Při dalším vývoji webové aplikace by mohlo dojít k nahrazení doposud využívaného šablonovacího enginu EJS pro frontend aplikace a zcela rozdělit backendovou a frontendovou část aplikace za přítomnosti některého komplexnějšího frameworku pro tvorbu uživatelských rozhraní např. React.js, který nabízí širší možnosti vývoje webových aplikací.

Další fáze vývoje by mohla přinést vylepšení v oblasti fyzických platebních čipů, které by bylo možné rozšířit o virtuální platební tokeny, jež by sloužily jako alternativa

fyzických bezkontaktních karet nebo čipů. Pro platbu by tak bylo možné využívat mobilní telefon nebo např. chytré hodinky.

6 Závěr

Diplomová práce shrnuje získané poznatky z oblasti NFC technologií se speciálním zaměřením na bezpečnost těchto technologií a snaží se čtenáře seznámit s jejich praktickým využitím v oblasti vývoje a návrhu softwaru. Okrajově popisuje moderní programovací techniky a obecně platné a uznávané postupy při tvorbě desktopových a webových aplikací.

Teoretická část obecně informuje o bezdrátových technologiích a jejich technických hledisek. Detailně poté představuje bezkontaktní technologii Near Field Communication, její využití v průmyslu a obchodu v podnikových informačních systémech, tak i veřejností. Práce poukazuje na jednotlivé typy přístupu a vysvětluje paradigma spojené s nakládáním dat uložených na komunikačním médiu. Jsou zde vysvětleny rozdíly mezi jednotlivými druhy veřejně dostupných NFC čipů, případných bezpečnostních rizik spojené s duplikováním čipů, a kompatibility se čtecími zařízeními.

Vlastní práce vychází ze znalostí získaných v teoretické části a doplňuje kapitolu o praktické zkušenosti s vývojem softwaru s přesahem do oblasti psychologie uživatelského chování a prostředí obchodu a služeb. Demonstrace znalostí je realizována na prototypu dvou částí aplikace pokladního cashless NFC systému desktopové verze programu a doplňující aplikací webového rozhraní.

V rámci praktické části byly před zahájením vývoje stanoveny konkrétní požadavky a cíle, které by měla aplikace splňovat a kterých by mělo být dosaženo. Dále byl vypracován seznam relevantních a dostupných technologií, které by umožnily naplnit stanovené cíle s možností implementace NFC čtecího zařízení. V samotném návrhu byla vypracována podrobná UI/UX specifikace logické, datové a grafické vrstvy s analýzou možných scénářů s následnou realizací.

Na závěr bylo provedeno testování aplikací se skupinou testovacích subjektů a v rámci refaktoringu programu, na základě výsledků testovacích scénářů, opraveny zjištěné chyby aplikací. Také byly navrženy změny a případné možnosti vylepšení obou aplikací v případě jejího budoucího vývoje.

7 Seznam použitých zdrojů

Bradáč, Zdenek, Fiedler, Petr a Kačmář, Milan. 2003. Bezdrátové komunikace v automatizační praxi I: historie a současnost. *Automa.* [Online] květen 2003. https://automa.cz/cz/casopis-clanky/bezdratove-komunikace-v-automatizacni-praxi-i-historie-a-soucasnost-2003_05_28818_2096/.

CANTELON, MIKE, a další. 2014. *Node.js in Action.* Shelter Island : Manning Publications Co., 2014. 9781617290572.

Comer, Douglas E. 2019. *The Internet Book - Everything You Need to Know about Computer Networking and How the Internet Works.* Boca Raton : Taylor & Francis Ltd, 2019. 978-1-138-33133-4.

Coskun, Vedat, Ok, Kerem a Ozdenizci, Busra. 2012. *NEAR FIELD COMMUNICATION FROM THEORY TO PRACTICE.* Hoboken : John Wiley & Sons Ltd, 2012. 9781119971092.

Český telekomunikační úřad. 2019. Využívání vymezených rádiových kmitočtů. *Český telekomunikační úřad.* [Online] 2019. https://www.ctu.cz/vyuzivani-vymezenych-radiovych-kmitoctu.

Doglio, Fernando. 2018. *REST API Development with Node.js.* Berkely : Apress, 2018. 978-1-4842-3714-4.

Gupta, Naresh. 2016. *Inside Bluetooth Low Energy.* Boston : Artech House, 2016. 978-1-63081-089-4.

Haunts, Stephen. 2019. *Applied Cryptography in .NET and Azure Key Vault.* Belper : Apress, 2019. 978-1-4842-4374-9.

Igoe, Tom, Coleman, Dom a Jepson, Brian. 2014. *Beginning NFC Near Field Communication with Arduino, Android, and PhoneGap.* Sebastopol : O'Reilly Media, Inc., 2014. 978-1-449-37206-4.

ISO / IEC. 2018. ISO/IEC 14443-4:2018(en). *ISO - International Organization for Standardization.* [Online] 2018. https://www.iso.org/obp/ui/#iso:std:iso-iec:14443:-4:ed-4:v1:en.

Klička, Jan. 2017. Deník. *Kartu netřeba. U kasy můžete odteď zaplatit i mobilem.* [Online] 15. listopad 2017. https://www.denik.cz/ekonomika/u-kasy-muzete-odted-zaplatit-i-mobilem-20171115.html.

Lieskovan, Tomáš. 2019. Bezpečnost autentizačních systémů založených na kartách. *Elektrorevue.* [Online] 28. Únor 2019. http://www.elektrorevue.cz/cz/download/bezpecnost-autentizacnich-systemu-zalozenych-na-kartach-mifare-classic-a-overovani-pomoci-uid--security-of-authentication-systems-based-on-mifare-classic-and-uid-verification-/. 1213-1539.

Massé, Mark. 2012. *REST API Design Rulebook.* Sebastopol : O'Reilly Media, Inc., 2012. 978-1-449-31050-9.

NFC Forum. 2019. ABOUT THE TECHNOLOGY. *NFC Forum.* [Online] 23. říjen 2019. https://nfc-forum.org/what-is-nfc/about-the-technology/.

Olenewa, Jorge L. 2016. *Guide to Wireless Communications.* Boston : Cengage Learning, 2016. 978-1-305-95853-1.

Rankl, Wolfgang a Effing, Wolfgang. 2010. *Smart Card Handbook.* Chichester : John Wiley & Sons Ltd, 2010. 978-0-470-74367-6.

Refsnes Data. 2011. Node.js NPM. *w3schools.* [Online] 2011. https://www.w3schools.com/nodejs/nodejs_npm.asp.

Rosenberg, Martin a Mertlík, Tomáš. 2013. Aplikace na přenos dat pomocí NFC. *Elektrorevue.* [Online] 20. prosinec 2013. http://www.elektrorevue.cz/cz/download/aplikace-na-prenos-dat-pomoci-nfc--application-for-nfc-data-transmission-/.

Sabella, Robert P. a Mueller, John Paul. 2016. *NFC For Dummies.* Hoboken : John Wiley & Sons, Inc., 2016. 978-1-119-18292-4.

Sedlák, Jan. 2016. První lidé v Česku mají v těle čip. Platí s ním za kafe a otevírají dveře. *Lupa.* [Online] 2. květen 2016. https://www.lupa.cz/clanky/prvni-lide-v-cesku-maji-v-tele-cip-plati-s-nim-za-kafe-a-oteviraji-dvere/.

Sojka, Libor. 2019. Pražští revizoři vyfasovali power banky. Kupony MHD lze nově nahrát do mobilu, pak ale nefunguje plastová karta. *Česká televize.* [Online] 2. prosinec 2019. https://ct24.ceskatelevize.cz/regiony/2993234-kupony-prazske-mhd-miri-do-mobilu-cestujici-si-ale-musi-vybrat-jestli-bude-vyuzivat.

Tišnovský, Pavel. 2020. Testování webových aplikací s REST API z Pythonu. *Root.* [Online] 7. červenec 2020. https://www.root.cz/clanky/testovani-webovych-aplikaci-s-rest-api-z-pythonu/.

Trčálek, Antonín. 2013. Stačí přiložit: NFC a jeho využití v praxi. *Mobilmania.* [Online] 14. říjen 2013. https://mobilmania.zive.cz/clanky/staci-prilozit-nfc-a-jeho-vyuziti-v-praxi/sc-3-a-1325034/default.aspx.

8 Přílohy

Příloha 1 Přiložené CD, které obsahuje:

- Zdrojové kódy desktopové pokladní aplikace
- Zdrojové kódy webové aplikace
- Exportovanou zálohu databáze PostgreSQL
- Diplomovou práci ve formátu PDF