Autonomní platební systém s využitím radiofrekvenční identifikace

Bc. David Šupa

Diplomová práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

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

Jméno a příjmení:	**Bc. David Šupa**
Osobní číslo:	**A17815**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**kombinovaná**
Téma práce:	**Vývoj autonomního platebního systému s využitím radiofrekvenční identifikace**
Téma anglicky:	**The Development of an Autonomous Payment System Based on RFID**

Zásady pro vypracování:

1. **Zpracujte teoretická východiska práce a stanovte cíle a metody jejího řešení.**
2. **Pojednejte o současném stavu řešené problematiky.**
3. **Navrhněte funkcionalitu platebního systému s využitím RFID karet.**
4. **Na základě teoretické části, realizujte navržený software.**
5. **Vypracujte závěr práce a stanovte možné směry jejího budoucího rozvoje.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **MCCONNELL, Steve. Software project survival guide. Redmond, Wash: Microsoft Press, c1998. ISBN 9781572316218.**
2. **KANISOVÁ, Hana a Miroslav MÜLLER. UML srozumitelně. Brno: Computer Press, 2004. ISBN 80-251-0231-9.**
3. **CLARKE, Nathan. Transparent user authentication: biometrics, RFID and behavioural profiling. New York: Springer, 2011. ISBN 978-0-85729-805-8.**
4. **WIEGERS, Karl Eugene. More about software requirements: thorny issues and practical advice. Redmond, WA: Microsoft Press, c2006. Best practices (Redmond, Wash.). ISBN 978-0-7356-2267-8.**
5. **SCHLOSSBERGER, Otakar. Platební služby. Praha: Management Press, 2012. ISBN 9788072612383.**

Vedoucí diplomové práce: **Ing. Bc. Pavel Vařacha, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **3. prosince 2018**

Termín odevzdání diplomové práce: **15. května 2019**

Ve Zlíně dne 7. prosince 2018

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
děkan

prof. Mgr. Roman Jašek, Ph.D.
garant oboru

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne

David Šupa, v. r.
podpis diplomanta

ABSTRAKT

V rámci této diplomové práce vznikl softwarový návrh autonomního platebního systému. Tento systém využívá identifikaci založenou na platebních kartách využívajících technologii rádio frekvenční identifikace. Hlavní oblast působení tohoto platebního systému představuje pohostinství. Převážně pak firemní kantýny či školní jídelny, systém tedy vznikl převážně pro použití v oblastech, kde se pohybují známý zákazníci (studenti či zaměstnanci). Systém lze ale i použít v rámci aquaparků, fitness center a dalších podobných oblastech. Součástí této diplomové práce je také praktická ukázka jak si lze tento platební systém představit. Praktická ukázka vznikla v programovacím jazyce C#.

Klíčová slova: Platební systém, RFID, Software, .NET Framework, UML

ABSTRACT

This thesis describes development of Autonomous Payment System Based on RFID technology. This payment system is meant to be used in company or school canteens, the system was created mainly for use in areas where well-known customers (students or employees) move. But the systém can also be used in aquaparks, fitness centers and other similar areas. Part of this thesis is also a practical example of how this payment system can be introduced. Practival example was created in C# programming language.

Keywords: Platební systém, RFID, Software, .NET Framework, UML

Tímto bych rád poděkoval svému vedoucímu Ing. Bc. Pavlovi Vařachovi, Ph.D. za profesionální přístup, cenné připomínky a odborné vedení, které vedlo ke zdárnému dokončení této práce. Nakonec patří velký dík mé rodině, bez které bych nemohl studovat a jejíž podpora pro mne mnoho znamená.

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

OBSAH

ÚVOD **10**

I TEORETICKÁ ČÁST **11**

1 RFID **12**

1.1 PRINCIP KOMUNIKACE 12

1.2 RFID TAGY 12

1.2.1 Konstrukce a operační frekvence 13

1.3 ČTEČKA 13

1.4 VYUŽITÍ 13

1.4.1 Sledování produktů 14

1.4.2 Identifikace 14

1.4.3 Zabezpečení přístupu 14

1.4.4 Použití ve zdravotnictví 15

1.4.5 Další způsoby využití 15

1.5 BEZPEČNOST A SOUKROMÍ 15

1.5.1 Odposlech 16

1.5.2 Analýza komunikace 16

1.5.3 Spoofing 16

1.5.4 Denial of Service Attack (DOS) 16

1.5.5 Integrita RFID čteček 17

1.5.6 Soukromí 17

1.6 PŘÍSTUP K PROBLÉMŮM BEZPEČNOSTI A SOUKROMÍ 17

1.6.1 Ochrana dat na RFID 17

1.6.1.1 Ochrana pomocí hesla 18

1.6.1.2 Fyzický zámek paměti 18

1.6.1.3 Ověření majitele 18

1.6.2 Zajištění integrity RFID čteček 18

1.6.2.1 Ochrana čtení 18

1.6.2.2 Detektory čtení 19

1.6.3 Ochrana soukromí 19

1.6.3.1 Příkaz zabij 19

1.6.3.2 Faradayova klec 19

1.6.3.3 Aktivní rušení 19

1.6.3.4 Logický Hash zámek 19

1.7 BEZPEČNOSTNÍ TRENDY 20

2 BEZKONTAKTNÍ PLATEBNÍ SYSTÉMY **21**

2.1 ÚČASTNÍCI TRANSAKCE 21

2.2 EMV PROTOKOL 22

2.2.1 Metody Autentizace Karet 23

2.2.2 Metody ověření držitele karty 23

2.2.3 Druhy transakce 24

3 LOKÁLNÍ PLATEBNÍ SYSTÉMY **25**

3.1 VYUŽITÍ LOKÁLNÍCH PLATEBNÍCH SYSTÉMŮ – PŘÍKLAD 25
3.2 ROZDÍL MEZI LOKÁLNÍM A NORMÁLNÍM PLATEBNÍM SYSTÉMEM 27
4 NÁVRH SOFTWARE 28
4.1 SOFTWAROVÉ POŽADAVKY 28
4.1.1 Druhy požadavků 28
4.2 PŘÍPADY UŽITÍ 28
4.3 DIAGRAMY 29
4.3.1 Sekvenční 29
4.3.2 Aktivitní 30
5 SROVNÁNÍ KONKURENČNÍCH SYSTÉMŮ 31
5.1 KASA FIK 31
5.2 FRAJT 32
5.3 IKOS 33
5.4 HASAM 33
6 SMĚRY BUDOUCÍHO ROZVOJE 35
6.1 PLATEBNÍ KARTY 35
6.2 MOBILNÍ PLATBY 36
6.2.1 NFC 36
6.2.1.1 Rozdíl mezi EMV a NFC 37
6.2.2 Bezkontaktní platební nálepky 37
6.2.3 MST 37
6.2.4 Sound Wave 37
6.2.5 Apple Pay 38
6.3 OTISKY PRSTŮ 38
6.4 ROZPOZNÁVÁNÍ OBLIČEJE 39
6.5 ROZPOZNÁNÍ SÍTNICE 41
6.6 HLASOVÉ ROZPOZNÁNÍ 41
II PRAKTICKÁ ČÁST 42
7 SOUČASNÉ ŘEŠENÍ PROJEKTU 43
7.1 MODUL INFOS CARDPAY 43
7.2 STRAVOVACÍ SYSTÉM CARDPAY 44
7.2.1 Objednávkové stravování 45
8 NOVÉ ŘEŠENÍ 46
8.1 MOTIVACE NÁVRHU NOVÉHO ŘEŠENÍ 46
8.2 POPIS NÁVRHU NOVÉHO ŘEŠENÍ 46
8.2.1 Základní funkcionality platebního systému 47
8.2.1.1 Správa interních uživatelských účtů 47
8.2.1.2 Definice limitů, položek prodeje a jídelníčků 48
8.2.2 Definice cenových hladin položek prodeje 49
8.2.2.1 Neomezený počet hladin 49
8.2.2.2 Časová závislost 50
8.2.2.3 Vazba na počet kusů 50
8.2.3 Provoz více organizačních a účetních jednotek na jednom systému 50
8.2.3.1 Zobrazení dat s ohledem na GDPR 51

8.2.3.2 Rozdělení jídelníčků na jednotlivé výdejny a časy výdeje 51
9 NÁVRH SOFTWAROVÝCH FUNKCIONALIT 52
9.1 POŽADAVKY 52
9.1.1 Nefunkční Požadavky 52
9.1.2 Funkční Požadavky 53
9.2 FUNKCIONALITY V PROSTŘEDÍ JÍDELNY 55
9.2.1 Model případů užití – jídelna 55
9.2.2 Scénáře k případům užití 55
9.2.2.1 Případ užití – Zaplacení 55
9.2.3 Sekvenční diagram případu užití – Zaplacení 56
9.2.4 Diagram aktivity - Zaplacení 58
9.3 FUNKCIONALITY WEBOVÉHO ROZHRANÍ 58
9.3.1 Model případů užití – webové rozhraní 58
9.3.2 Scénáře k případům užití 60
9.3.3 Sekvenční diagram případu užití – Vytvoření Objednávky 61
9.3.4 Diagram tříd pro webové rozhraní 61
9.3.5 Diagramy aktivit 62
9.3.6 Model případů užití – backoffice 64
9.3.7 Scénáře k případům užití 64
9.3.8 Sekvenční diagram případu užití – Vytvoření Jídelníčku 65
9.3.9 Diagram aktivit – Vytvoření výdejny 66
10 UKÁZKA NAVRŽENÉHO SOFTWARE 67
ZÁVĚR 70
SEZNAM POUŽITÉ LITERATURY 71
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 75
SEZNAM OBRÁZKŮ 76
SEZNAM TABULEK 78
SEZNAM PŘÍLOH 79

ÚVOD

Cílem této diplomové práce je uvedení do teoretické problematiky autonomních platebních systému s využitím technologie RFID a navrhnutí softwarových požadavků pro takovýto platební systém. Zásady pro vypracování diplomové práce vznikly na základě zadání smluvního výzkumu projektu INFOS. Body zadání tedy přímo vychází z požadavků zákazníka a to firmy COMINFO, a.s..

Vývoj software a jeho funkcionalit by měl za každou cenu jít s dobou a nestagnovat na místě. V případě, že by se vývoj zastavil a společnost by usnula na vavřínech, velice snadno by mohlo dojít k tomu, že by se řešení firmy stalo neatraktivním pro nové ale i stávající zákazníky a došlo by tedy ke ztrátě konkurence schopnosti.

V první kapitole této diplomové práce se nachází popis technologie RFID, spolu s potencionálním využitím. Také jsou zde uvedena možná bezpečnostní rizika, která použitím této technologie mohou vzniknout. Dále se zde nachází výpis bezpečnostních opatření proti potencionálním rizikům. Druhá a třetí kapitola uvádí do bližšího porozumění problematiky platebních systémů a rozdílů mezi nimi. Následující dvě kapitoly, pátá a šestá, pojednávají o současném stavu řešené problematiky a stanovují směry možného budoucího rozvoje.

První kapitola praktické části diplomové práce uvádí čtenáře do současného řešení problematiky projektu INFOS. Druhá a třetí kapitola v této části již představuje návrh nového řešení, tedy návrh funkcionalit platebního systému s využitím RFID karet. Poslední kapitola obsahuje ukázku realizovaného software, který vznikl na základě předchozích kapitol.

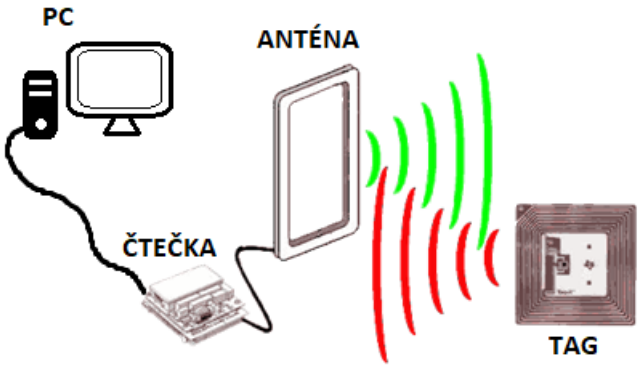
I. TEORETICKÁ ČÁST

1 RFID

RFID představuje zkratku pro Radio Frequency Identification. Jedná se o technologii využívající radiofrekvenční komunikace pro automatickou identifikaci objektů. Těmito objekty může být cokoliv, například knihy v knihovně, jakýkoliv produkt v obchodě, zboží ve skladu, platební anebo vstupní karty. Tato technologie se také používá při sledování zvířat, převážně pak ptáků. Tedy RFID technologii lze použít na vše k čemu lze přidělat RFID tag.

1.1 Princip komunikace

Identifikační systém se skládá z několika hlavních prvků, kterými jsou tagy (transpondéry), čtečky a další podpůrné systémy (počítače, databáze a další). Tagy obsahují informace o objektech, ke kterým jsou připojeny.



Obr. 1. Základní schéma komunikace

Princip komunikace se liší podle typů použitých tagů. Čtečka vysílá signály skrze anténu, když se RFID tag nachází v dosahu signálu, vyšle zpět signál s informacemi, které uchovává. Princip komunikace se podobá tomu, který se používá při čtení čárových kódů. Hlavní rozdíl představuje fakt, že při identifikaci pomocí radiofrekvenční komunikace není zapotřebí, aby byl tag ve viditelném dosahu, stačí být v dosahu signálu.

1.2 RFID tagy

Existuje více druhů tagů, aktivní, pasivní a polo-pasivní. Pasivní tagy nemají vlastní zdroj napájení a jsou závislé na energii ze signálu vyslaného čtečkou. Polo-aktivní tagy mají svůj vlastní zdroj energie, ale pro odeslání signálu zpět ke čtečce využívají stejně jako pasivní tagy energii získanou ze signálu vyslaného čtečkou. Aktivní tagy mají vlastní zdroj energie.

1.2.1 Konstrukce a operační frekvence

Složení RFID tagu:

- Transpondér – jedná jako přijímač a zároveň vysílač
- Kondenzátor – slouží pro uložení energie získané z přijatého signálu
- Mikroprocesor – ovládá vysílání tagu
- Paměť – ukládá informace o objektu, které jsou přenášeny po přijetí signálu

RFID tagy pracují na třech nejběžnějších frekvencích. Použití frekvencí se liší jak podle států, tak podle účelu s jakým je nasazení technologie RFID zamýšleno. Nejčastěji se používají tyto frekvence:

1. Nízké (125 kHz nebo 134 kHz) – Čtení na vzdálenosti do 10 cm, použití pro řízení přístupu a značení zvířat.
2. Vysoké (13,56 MHz) – Čtení na vzdálenosti mezi 10 cm až 1 m. Typické použití u lokálních platebních systémů.
3. Ultra vysoké (860 MHz až 960 MHz) – Operují ve vzdálenostech od 10 až do 15 m, a používají se pro označování objektů, typicky zboží v obchodech.

1.3 Čtečka

RFID čtečka představuje zařízení, které slouží ke sběru a zpracování dat získaných z RFID tagů a také komunikuje se serverem. [1]

V případě pasivních a polo-aktivních tagů slouží čtečka také jako zdroj energie potřebné pro aktivaci nebo nabití tagů, nacházejících se v dosahu elektromagnetického pole čtečky. Rozsah tohoto pole bývá obecně určen velikostí použitých antén na obou stranách (čtečka a tag). Velikost antény je definována podle oblasti použití a potřeb. Nicméně síla čtečky, která definuje intenzitu a dosah vytvořeného elektromagnetického pole, bývá limitována regulacemi. Každý stát má své vlastní standardy a regulace týkající se množství energie generované na různých frekvencích.

1.4 Využití

Technologie RFID se v současné společnosti stává tak všude přítomnou, že na ni průměrná osoba naráží denně a to bez toho aniž by si to uvědomila. Schopností levného, efektivního a spolehlivého způsobu shromažďování a ukládání dat, nabízí technologie RFID téměř neomezené možnosti použití a to jak v přítomnosti, tak v budoucnosti.

1.4.1 Sledování produktů

Využití RFID tagů neustále narůstá v oblasti sledování zboží či jako náhrada za běžně používané čárové kódy, právě díky nízké ceně. Tagy se například používají při odhalování, jakému zboží bude končit spotřební lhůta. V Číně se RFID tagy využívají při boji s padělky. [2]

1.4.2 Identifikace

RFID čipy mohou být implantovány do zvířat či lidí za účelem monitorování jejich pohybu, poskytnutí přístupu do zabezpečených oblastí anebo při hledání ztraceného mazlíčka.

Většina zemí prvního světa přidává RFID tagy do pasů. Tyto tagy obsahují informace, které slouží pro identifikování majitele pasu (například fotografie). Používají se také pro sledování pohybu na hranicích.

1.4.3 Zabezpečení přístupu

Jednou z nejběžnějších oblastí použití RFID představuje zabezpečení přístupu. Typickým příkladem jsou kancelářské prostory, kde je nežádoucí pohyb kohokoliv jiného než zaměstnanců. Můžeme tedy příslušným osobám, v našem případě zaměstnancům, poskytnout RFID čipy. Následně vchod do kancelářských prostor opatříme vstupními dveřmi ovládanými RFID čtečkou. Zaměstnanec se tedy do prostor dostane pomocí svého čipu. Jedná se o jednoduchou a inovativní metodu přístupu 21. století.

Obr. 2. Vzhled RFID čipu

Tento způsob kontroly přístupu přináší pár výhod i nevýhod. Jednou z výhod je, že zaměstnavatel resp. správce budovy má neustálý přehled o tom, kdo a kdy se dostal do budovy.

Nevýhodu pak představuje možnost odcizení čipu. Bezpečnost jednotlivých řešení probereme dále.

1.4.4 Použití ve zdravotnictví

Každý rok zemře v nemocnicích až 98,000 lidí kvůli chybám lékařů, kterým by se dalo předejít. [3]

Lékařským chybám by se dalo předejít vybudováním lepšího bezpečnějšího lékařského systému. RFID představuje levnou, snadnou a rychlou možnost pro použití ve zdravotnictví. Praktické využití, které může snížit chyby lékařů, představuje možnost rychle zjistit všechny potřebné informace o pacientovi. Tedy například alergie, kterými pacient trpí či léky, které právě užívá. Může pomoci sestřičkám rychle identifikovat pacienty a léčbu, kterou podstupují.

RFID má tedy vysoký potenciál pro snížení zdravotnických chyb a uvolnění pracovní zátěže zdravotních sester. Na druhou stranu vyvstávají otázky o bezpečnosti informací pacientů. Jednak má zdravotnický personál rychlý a snadný přístup k životně důležitým informací avšak na druhou stranu může dojít k úniku či krádeži těchto citlivých informací.

1.4.5 Další způsoby využití

Vybírání mýta na dálnicích bez nutnosti zastavení. Knihovny uchovávají pomocí RFID tagů informace o knihách (názvy, autoři atd..) a poskytují zabezpečení proti krádeži. Díky tomu, že RFID tagy mohou být čteny na vzdálenosti a bez nutnosti přímé viditelnosti, lze také snadno zjistit obsah nákladního vozu či lodního kontejneru.

1.5 Bezpečnost a soukromí

Bezpečnost a soukromí představují v dnešní době závažná témata. Tato témata musí řešit jak organizace zavádějící RFID technologii tak i samotní uživatelé.

Většina RFID čipů je označována za „hloupá“ zařízení v tom smyslu, že dokáží pouze poslouchat a odpovídat komukoliv kdo se zeptá. Tím vyvstává riziko neautorizovaného přístupu k datům a potencionální hrozba jejich úpravy. Jinými slovy nechráněné RFID čipy mohou být zranitelné na odposlech, analýzu komunikace, spoofing nebo útoky typu DOS.

1.5.1 Odposlech

Rádiové signály přenášeny z RFID čipu a čtečky mohou být detekovány na vzdálenost několika metrů i ostatními rádiovými přijímači. Je tedy možné aby neautorizovaná osoba získala přístup k datům, které se nachází na RFID čipech, za předpokladu nezabezpečené komunikace.

Výzkumníci v USA demonstrovali odposlech na kreditní kartě využívající technologii RFID. Dokázali, že se dají získat informace o držiteli karty, jako například jméno či informace o účtu v případě, že komunikace není dostatečně šifrována. [4]

1.5.2 Analýza komunikace

I když jsou data chráněna, je možné použít nástroje pro analýzu komunikace a tím po určité době předvídat odpovědi. Pokud se na získaných datech provede analýza a korelace, dá se získat přibližný obraz pohybu a finanční transakce. Zneužití těchto informaci představuje značné narušení soukromí.

1.5.3 Spoofing

Na základě dat získaných odposlechem či analýzou komunikace, je možné provést spoofing RFID značek. Například softwarový balíček známý jako „RFDump“ [5], který běží na notebooku, umožňuje uživateli provádět čtení či zápis na většinu běžných značek pokud nejsou dostatečně zabezpečená. Tento software dovoluje útočníkům podvrhnout existující data falešnými.

Podvržením dat může útočník obelstít RFID systém a tím získat výhody. Příkladem může být snaha o ušetření peněz tak, že útočník provede změnu dat takovým způsobem, aby se při čtení ukázala nižší cena, než jaká je ve skutečnosti.

1.5.4 Denial of Service Attack (DOS)

V případech, kdy dochází ke sdílení velkého množství dat mezi obchodními partnery či firmami obecně, vzniká spousta problémů týkajících se bezpečnosti a soukromí. DOS útok proti RFID infrastruktuře může nastat, pokud došlo k poškození většího množství RFID značek. Pro příklad lze uvést situaci, kdy útočník použije příkaz „kill“, který je implementován v RFID značkách k dočasnému zastavení RFID komunikace. [6] Takto lze „zasekat“ celý systém.

1.5.5 Integrita RFID čteček

Může nastat situace, kdy jsou RFID čtečky umístěny na špatném místě či nemají dostatečnou fyzickou ochranu kolem sebe. Díky tomu představují snadný cíl pro potencionálního útočníka, který může poblíž umístit svou vlastní čtečku. Tato čtečka poté dokáže přijímat stejné signály jako původní čtečka, ale také dokáže tyto signály rušit a vysílat jiné signály.

Následkem takového počínání mohou být data, která předává čtečka upravena či přímo ukradena. RFID čtečka může být také cílem útoku virů. Vědci demonstrovali v roce 2006, že RFID virus je reálný. Vytvořili koncept samo replikujícího viru, který dokázal napadnout systém pomocí SQL injection útoku. [7]

1.5.6 Soukromí

S narůstajícím používáním RFID v obchodním sektoru se začíná čím dál tím více produktů označovat pomocí RFID technologie. Tomuto napomáhá i cena RFID technologie, která není nijak vysoká a dá se očekávat, že bude v budoucnu klesat. RFID značení se rozšiřuje na oblečení, elektroniku atd. Důsledkem tohoto rozšiřování vyvstávají otázky ohledně soukromí. Veřejnost se ptá, jak se zachází s jejich daty. Jsou data použita pouze pro cílený marketing anebo může docházet přímo ke sledování. Pokud by se dal například typ oblečení propojit s jednotlivými uživateli, mohlo by docházet ke sledování bez vědomí či souhlasu.

Jako příklad se dá uvést RFID čip všitý do oblečení. Tyto čipy vydrží i roky praní aniž by došlo k jejich poškození. Je tedy možné, že vše co nakoupíme lze identifikovat a sledovat i po opuštění obchodu.

Největší novinku představuje použití v oblasti medicíny, kdy se po stránce ochrany soukromí jedná o velice závažnou věc. Za předpokladu, že by každá osoba měla u sebe RFID čip obsahující veškerá citlivá data, pak by únik těchto dat byl velikým zásahem do soukromí.

1.6 přístup k problémům bezpečnosti a soukromí

Způsob jakým lze přistupovat k problémům s bezpečností a soukromím se dá rozdělit do tří hlavních kategorií, které jsou uvedeny dále.

1.6.1 Ochrana dat na RFID

První kategorie se zabývá ochranou dat přímo uložených v paměti RFID čipu. [8]

1.6.1.1 Ochrana pomocí hesla

Přístup do paměti RFID čipu lze opatřit vstupním heslem, čímž dojde k ochraně před čtením dat bez vědomí majitele či hesla. Nicméně pokud je heslo pro mnoho RFID čipů stejné, pak dochází ke ztrátě jeho významu. Naopak při použití nového hesla pro každý RFID čip nastává problém opačný a to nepřeberné množství hesel. Tedy čtečka by potřebovala přístup do databáze, která by byla tak veliká, že by došlo k ovlivnění rychlosti čtení.

1.6.1.2 Fyzický zámek paměti

Při výrobě dochází k zápisu identifikační hodnoty do paměti RFID čipu a následně se zápis do paměti znemožní. Jedná se tedy o čipy read-only. Takto se dá zajistit, že RFID čip bude mít nestále stejnou hodnotu.

Samozřejmě tím vznikají zjevné nevýhody. Data na RFID čipu nelze aktualizovat. Aby to bylo možné, musela by se přidat přídavná paměť pro ukládání modifikovatelných informací. Bohužel toto řešení zvyšuje náklady.

1.6.1.3 Ověření majitele

Majitel RFID čipu zašifruje data pomocí svého vlastního privátního klíče a následně je uloží do paměti RFID čipu spolu se jménem autora, odkazem na veřejný klíč a použitý algoritmus v nezašifrované podobě. Následně pokud strana, která provádí čtení, chce ověřit pravost dat, musí získat jméno autora a další nešifrované informace aby mohlo dojít k ověření, zda data opravdu zapsal původní autor.

1.6.2 Zajištění integrity RFID čteček

1.6.2.1 Ochrana čtení

Při použití pasivních značek RFID, lze předejít pokusům o spoofing. Pokud čtečka zahodí všechny odpovědi, které mají anomálie buď v délce odpovědi anebo v síle signálu.

Čtečky mohou také vysílat s proměnlivou frekvencí. Tato forma zabezpečení chrání proti odposlouchávání. Lze použít pouze v případě, že RFID čipy jsou navrženy tak aby dokázali také měnit svou frekvenci.

1.6.2.2 Detektory čtení

Jedná se o speciální zařízení, která slouží k detekci neoprávněných pokusů o čtení či přenášení na frekvenci RFID čipů. Tyto detektory mohou být použity pouze spolu se speciálně navrženými RFID čipy, které vysílají na předem definované frekvenci každý pokus o čtení či úpravu dat.

1.6.3 Ochrana soukromí

1.6.3.1 Příkaz zabij

Vykonáním speciálního příkazu „zabij“ dojde ke zničení RFID čipu. Tento příkaz může odpojit anténu nebo přerušit obvod. Takto lze zajistit, že RFID čip již nebude nadále možné sledovat a tím dojde k ochraně soukromí osoby, která vlastní daný produkt. Nevýhodu představuje fakt, že po vykonání tohoto příkazu se stává RFID čip již nepoužitelným. [9]

1.6.3.2 Faradayova klec

RFID čip může být opatřen obalem z kovové síťky či fólie označovaným také jako „Faradayova klec“. Tento obal dokáže blokovat rádiové signály určitých frekvencí a tím se chrání proti odhalení. [10]

1.6.3.3 Aktivní rušení

Aktivní rušení rádiového signálu potřebuje další zařízení, které neustále vysílá rádiový signál. Tento signál ruší operace blízkých RFID čteček. Nicméně použití takového to zařízení může být nelegální. Záleží na síle signálu a omezeních daných státem. Vzniká zde ale vysoké riziko rušení okolních RFID čteček, pokud je síla rušivého signálu příliš silná.

1.6.3.4 Logický Hash zámek

Uzamčený RFID čip odmítne odhalit své identifikační číslo, dokud nedojde k jeho odemčení pomocí příslušného klíče či PINu.

Tento přístup má i své limity. Jednotlivci mohou spravovat až nepřeberně velké množství kolekcí RFID čipů. S tím vzniká nutnost pamatovat si spoustu identifikačních klíčů jednotlivých RFID čipů a jednotlivé PINy k nim.

1.7 Bezpečnostní trendy

Jelikož je RFID neustále se rozvíjející technologií tak dochází k vývoji nových bezpečnostních standardů a k vylepšování těch stávajících. Dále dochází k vývoji hardwaru za účelem podpory kryptografických funkcí, symetrického šifrování, ověřování zpráv a přidání generátorů náhodných čísel. Tato všechna vylepšení mohou pomoci se zabezpečením technologie RFID. V návaznosti na neustálé bezpečnostní vylepšování, dochází také k vylepšování návrhu samotného elektronického obvodu. Novější technologie ve výrobním sektoru snižují také náklady na výrobu.

Probíhají také pokusy se zabezpečením za pomoci veřejných klíčů. Takto se dá vylepšit zabezpečení, dají se ověřovat uživatelé a také se jedná o zlepšení ze strany soukromí. Další výzkum se provádí v oblasti RFID čteček a jejich zabezpečení. Navzdory všem výhodám se vývoj v oblasti veřejných klíčů zastavil, kvůli problémům s cenou či výkonem.

2 BEZKONTAKTNÍ PLATEBNÍ SYSTÉMY

Od vynálezu bezkontaktního způsobu platby odpadá nutnost nosit sebou veliké množství hotovosti, která je normálně potřebná při nákupu. Hotovost lze nahradit plastovou kartou anebo RFID tagem v jiné formě (čip), někdy stačí i pouze chytrý telefon.

Definice, která popisuje RFID a chytré karty se používá zaměnitelně, čímž vzniká zmatek v rozdílech mezi těmito technologiemi. Tento zmatek je pak převážně mezi bezkontaktními chytrými kartami a RFID. V obou případech, jak u chytrých karet tak u RFID, je využíváno radiofrekvenční komunikace mezi kartou a čtečkou. Použití těchto technologií se ovšem už vzájemně liší.

Užití RFID spadá převážně do oblasti sledování pohybu zboží. Bezkontaktní platební karty jsou na druhou stranu užívány převážně pro platby a bankovnictví. Nicméně ač jsou pro platby používány hlavně chytré karty, není to nezbytností a dá se využít také RFID. Bezkontaktní platební karty či chytré karty jsou pak běžně označovány názvem kreditní karty.

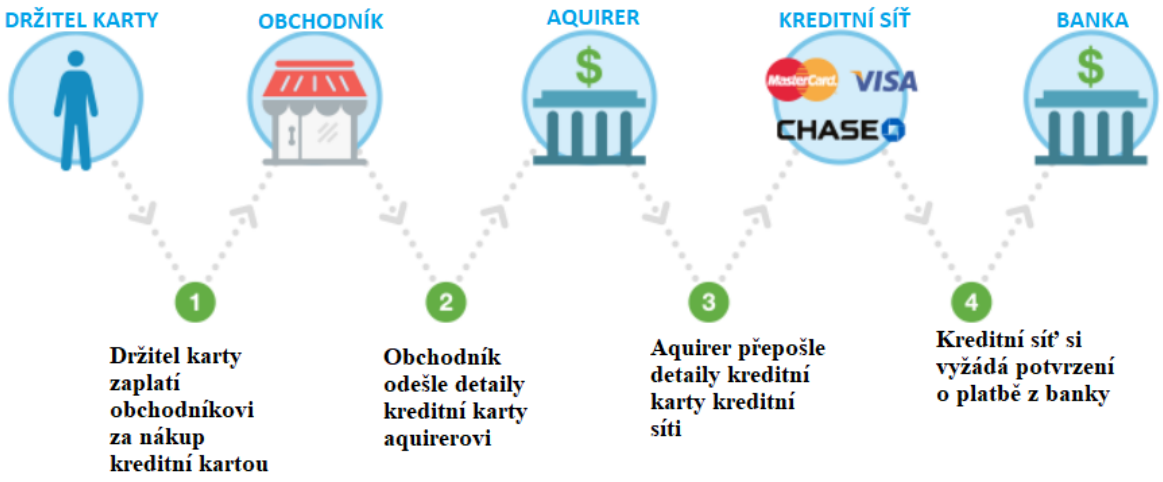
Obr. 3. Mezinárodní symbol pro bezkontaktní platby [11]

2.1 Účastníci transakce

Proces transakce kreditní kartou má několik hlavních účastníků, těmi jsou následující fyzické či právnické osoby [12]:

- **Držitel karty**: jak z názvu vyplývá, jedná se o fyzickou osobu, která pomocí karty platí zakoupené zboží.
- **Obchodník**: jedná se o obchod či obchodníka, který nabízí zboží anebo služby držiteli karty. Obchodník přijímá platby kreditní kartou a také odesílá a přijímá data o kreditní kartě bance, která karty vydala.

- **Aquirer**: představuje jednu ze třetích stran, která z procesu ověření platby vystupuje. Obchodník má většinou uzavřenu smlouvu s Aquirerem, který se stará o předání dat kreditní karty patřičné společnosti v kreditní síti.
- **Kreditní síť**: jsou to organizace, které spravují a kontrolují operace kreditních plateb. Kreditní síť zodpovídá za předání dat od aquirera patřičné bance, která kartu vydala a naopak.
- **Banka**: je právnickou osobou, skutečnou fyzickou bankou anebo finanční organizace, která poskytuje kreditní karty zákazníkům, tedy držiteli karty. Ke každé kartě náleží účet s finančními prostředky, kterými držitel karty disponuje.



Obr. 4. Cyklus platby kreditní kartou

2.2 EMV protokol

Kreditní karty pracují s mezinárodně uznávaným standardem pro platby EMV. EMV nepředstavuje jediný standard, ale jedná se o celou řadu protokolů, se spoustou variant a konfigurací. Typicky se používá v bankomatech, prodejních terminálech (POS), v internetovém bankovnictví a nyní již pár let i pro bezkontaktní platby a také platby za pomoci mobilů s využitím technologie NFC (popsána v dalším odstavci). [13]

Díky tomu, že EMV protokol představuje rodinu mnoha protokolů, jedná se o nástroj, který lze konfigurovat. EMV nabízí pro konfigurování platebních protokolů následující možnosti:

- *Tři metody autentizace karet:* SDA, DDA a CDA;
- *Pět metod verifikace držitele karty:* žádná, podpis, on-line PIN, off-line nekryptovaný PIN a off-line kryptovaný PIN;
- *Dva druhy transakcí:* on-line a off-line transakce.

2.2.1 Metody Autentizace Karet

EMV standard definuje tři druhy autentizačních metod karet: SDA, DDA a CDA. [14]

- **SDA (Static Data Authentication).** Karty SDA poskytují část digitálně podepsaných informací (číslo karty, datum platnosti) terminálu, který si vyžádá autentizaci. Jelikož terminál zná veřejný klíč vydavatele karty, může ověřit, zda jsou digitálně podepsaná data správná.
- **DDA (Dynamic Data Authentication).** DDA karty umožňují asymetrickou kryptografii, mají veřejný a soukromý klíč, a také podpis veřejného klíče pro ověření jeho autenticity. Terminál pak poskytne data, která karta podepíše svým soukromým asymetrickém klíčem a poté ověří jejich platnost. Bohužel po ověření karty již nedochází k ověřování, zda platba byla opravdu provedena ověřenou kartou.
- **CDA (Combined Data Authentication).** CDA metoda představuje vylepšenou metodu DDA. S CDA podepisuje karty všechna data a ne pouze v případě ověření její autenticity.

2.2.2 Metody ověření držitele karty

Metody s jakými se ověřuje platnost karty, jsou definovány výrobcem karty. Princip pak spočívá v tom, že karta předá terminálu seznam metod, které podporuje a na základě tohoto seznamu zvolí terminál metodu ověření. Základní metody ověření držitele jsou tři: pomocí PINu, ruční podpis anebo nemusí být provedeno žádné ověření. [15]

V případě ověřování pomocí PINu jsou tři možnosti:

1. **On-line PIN**, u nějž ověření provádí banka.
2. **Off-line PIN**, předáván v čistém textu. V tomto případě čip karty ověří, zda se jedná o správný PIN.
3. **Off-line šifrovaný PIN**, opět platnost PINu ověřuje čip karty, ale PIN se přenáší již zašifrován.

Jedním z důvodů proč upřednostňovat on-line PIN oproti off-line PINu, může být už pouhý fakt, že on-line PIN přinutí terminál připojit se k bance a tak lze i zjistit zda je karta případně nahlášena jako ztracená či kradená.

2.2.3 Druhy transakce

Po zvoleném ověření karty a ověření držitele karty, přichází na řadu samotná transakce. Transakce mohou být dvojího typu a to on-line a off-line. O tom, který druh transakce bude použit, rozhoduje terminál, ale i tak může karta odmítnout provedení off-line transakce a vynutit si on-line.

- **Off-line transakce**: při off-line transakci vystaví karta transakční certifikát, který poté terminál odešle vystavovateli karty, jako důkaz o proběhlé transakci.
- **On-line transakce**: oproti off-line transakci poskytne karta nejprve autorizační žádost, kterou terminál předá vydavateli karty. Vydavatel poté pošle kartě potvrzení přes terminál. Karta po obdržení potvrzení vystaví transakční certifikát.

3 LOKÁLNÍ PLATEBNÍ SYSTÉMY

S běžným platebním systémem se setkává většina lidí, každý den aniž by si to uvědomovala. Platební systémy jsou v dnešní době používány ve veliké škále oblastí, jakými jsou například obchody, restaurace, hotely a mnoho dalších.

Platební systém je jakýmkoliv systémem, který slouží k vyrovnání finančních transakcí skrze převod peněžní hodnoty a zahrnuje instituce, nástroje, osoby, pravidla, procedury, standardy a technologie, které umožňují takový to převod. [16]

Lokální platební systémy lze označit také za interní platební systémy, které fungují pouze v rámci jakéhosi objektu. Těmito objekty bývají často firmy a školy, které nabízejí doplňkové služby. Tyto doplňkové služby si lze představit například jako obchod v rámci firmy, který nabízí třeba sladkosti či cokoliv, co zde umístil majitel firmy za účelem zlepšení pracovního dne svým zaměstnancům.

Dalším typickým příkladem použití lokálního platebního systému může být firemní či školní jídelna. Tyto jídelny představují ideální příklad použití lokálního platebního systému a přímo se vztahují na zadání této práce, a proto se bude větší část definice lokálního platebního systému vztahovat na použití v jídelnách.

3.1 Využití lokálních platebních systémů – příklad

Jak již bylo zmíněno, typické použití lokálních platebních systémů představují firemní či školní jídelny. V rámci firmy obdrží zaměstnanci identifikační karty, které pracují na základě technologie RFID. Většinou tyto karty v sobě uchovávají pouze unikátní identifikační číslo zaměstnance a jsou tedy použitelné pouze v rámci firmy. Pokud by došlo ke ztrátě či krádeži karty nemusí mít zaměstnanec obavy, že by mohl přijít o své finance, jelikož karta nemá přístup k bankovnímu účtu zaměstnance. Vzniká pouze riziko zneužití karty v rámci firmy což, však nemusí mít pro zaměstnance fatální dopad, jaký by mohlo mít odcizení kreditní karty. Obavy však může mít majitel firmy za předpokladu, že karta slouží také pro vstup do firemních prostor, které jsou veřejnosti a neoprávněným osobám uzavřeny. Tohoto rizika se lze zbavit například zablokováním ztracené identifikační karty a vydáním nové karty.

Obr. 5. Průběh nákupu v rámci lokálního platebního systému

Obrázek (Obr. 5) popisuje běžný souhrn kroků, které nastanou například při nákupu ve firemní jídelně. Tyto kroky následně rozebereme podrobněji:

1. Zákazník (nadále označován jako zaměstnanec) vstoupí do jídelny a vybere si jeden z mnoha nabízených pokrmů.
2. Zaměstnance přistoupí k pokladně a přiloží svou identifikační kartu k terminálu. Ve stejné chvíli může začít pokladní markovat zakoupené zboží, nicméně k dokončení transakce nemůže dojít dříve, než po provedení úspěšného přihlášení zaměstnance.
3. Terminál ověří identitu zaměstnance oproti serveru, na kterém se nachází databáze, uchovávající všechny potřebné informace. Tento server může být jak v rámci firmy, tak se může jednat o třetí stranu, která poskytuje lokální platební systémy tak jako své služby pro jejich správu.
4. Po úspěšném ověření odešle server odpověď terminálu. Na základě odpovědi dojde k odemknutí dodatečných funkcionalit terminálu. Obsah těchto funkcionalit se liší podle požadavků firmy. Pokud firma umožňuje i nákup externím strávníkům za hotové peníze, bez nutnosti přihlášení pak tyto funkcionality mohou například zahrnovat lepší ceny pro zaměstnance či větší výběr pokrmů. V případě, kdy je firemní jídelna dostupná pouze interním strávníkům, tedy zaměstnancům pak do těchto funkcionalit spadá jedna hlavní funkcionalita a tou je možnost dokončení transakce. Dalšími doplňkovými funkcionality může být změna ceny pokrmu podle druhu zaměstnance, širší anebo naopak omezenější výběr atd.
5. Poslední fázi transakce představuje dokončení. Do tohoto bodu spadá ověření, zda zaměstnanec disponuje dostatečnými zůstatkem na svém účtu. Další možností pak je odečtení dané částky ze zaměstnancovi výplaty. V tomto případě nedochází ke kontrole zůstatku, ale zaměstnanec si může například sám definovat svůj měsíční limit, který nechce překročit, opět záleží na požadavcích firmy a na způsobu implementace.

3.2 Rozdíl mezi lokálním a normálním platebním systémem

U tomto druhu platebního systému vystupují vždy dvě hlavní role a to nakupující a prodejce. Do transakce lokálních platebních systémů nevstupují banky. Tento druh platebního systému se nejvíce podobá klasickému nákupu za hotovost. Místo kreditních karet vydaných bankovní či finanční společností se zde využívá obyčejných RFID karet či čipů, které obsahují většinou pouze své identifikační číslo, nicméně tyto identifikační karty nejsou vždy potřeba.

4 NÁVRH SOFTWARE

4.1 Softwarové požadavky

Požadavky představují specifikaci toho, co by mělo být implementováno. Jedná se o definice, toho jak se má systém chovat, definice jeho vlastností a atributů. Popisují to, co projekt dokáže, až bude jeho návrh u konce. Požadavky neurčují pouze to, co systém dokáže či co by měl dokázat, ale i to jak dobře dokáže systém tyto požadavky plnit. V případě vývoje software pro zákazníka, vznikají softwarové požadavky na základě požadavků zákazníka. [17]

4.1.1 Druhy požadavků

Požadavky se dají rozdělit do několika druhů, základní jsou dva a to funkční a ne-funkční požadavky. [18]

Funkční požadavky, jak z názvu vyplývá, definují funkce systému nebo jeho součástí, kde funkce je popsána jako specifikace chování mezi vstupy a výstupy. Funkční požadavky mohou zahrnovat výpočty, technické detaily, manipulaci s daty a jejich zpracování a další funkcionalitu, která popisuje, čeho má být systém schopen dosáhnout.

Ne-funkční požadavky specifikují jisté vlastnosti systému, případně podmínky omezující fungování systému. Definují, jaký má být systém, tedy jeho spolehlivost, rychlost, dostupnost, výkonost a další.

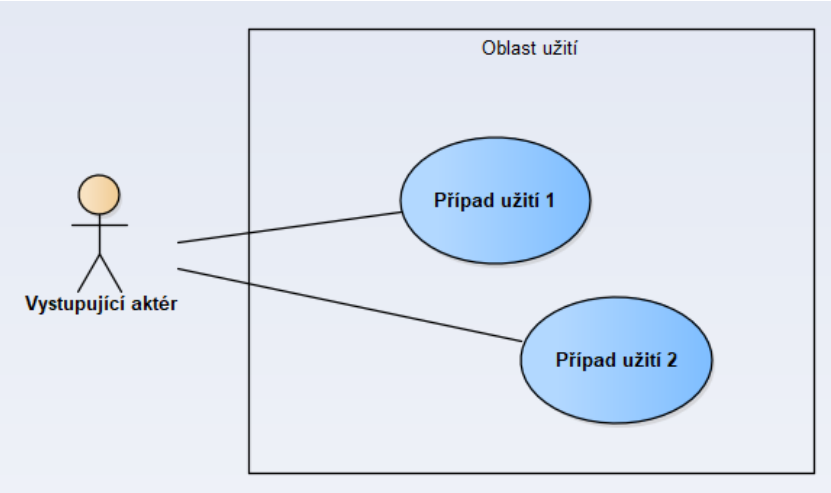
4.2 Případy užití

Známé v originálním názvu jako Use Case, představují modelování reálných situací, které zachycují interakci aktéra se systémem, slovo Aktér bude vysvětleno dále. Takto vytvořené modely slouží k bližšímu pochopení toho, jak se má systém v určitých situacích chovat a také k upřesnění požadavků budoucích uživatelů.

Případy užití zachycují přesně funkčnost, která bude budoucím informačním systémem pokryta a vymezují tak jednoznačně rozsah prací. Každý případ užití popisuje jeden ze způsobů použití systému, popisuje tedy jednu jeho požadovanou funkčnost. [19]

Aktér představuje osobu či proces, který komunikuje s daným informačním systémem. V rámci firmy může být hned několik aktérů, ovšem ne všichni přichází do styku s informačním systémem a proto je nutné zachytit pouze ty aktéry, s nimiž skutečně komunikuje informační systém. [20]

Aktéři vykonávají případy užití. V rámci systému může jeden aktér vystupovat hned v několika případech užití a naopak, jeden případ užití může být vykonáván vícero aktéry. Případy užití, které popisují funkčnost v rámci jedné oblasti, jsou sdružovány do celků spolu s aktéry, kteří v těchto případech užití vystupují tak jak je ukázáno na obrázku, tyto celky jsou označovány jako modely případů užití (Obr. 7).



Obr. 6. Ukázkový příklad modelu případů užití

4.3 Diagramy

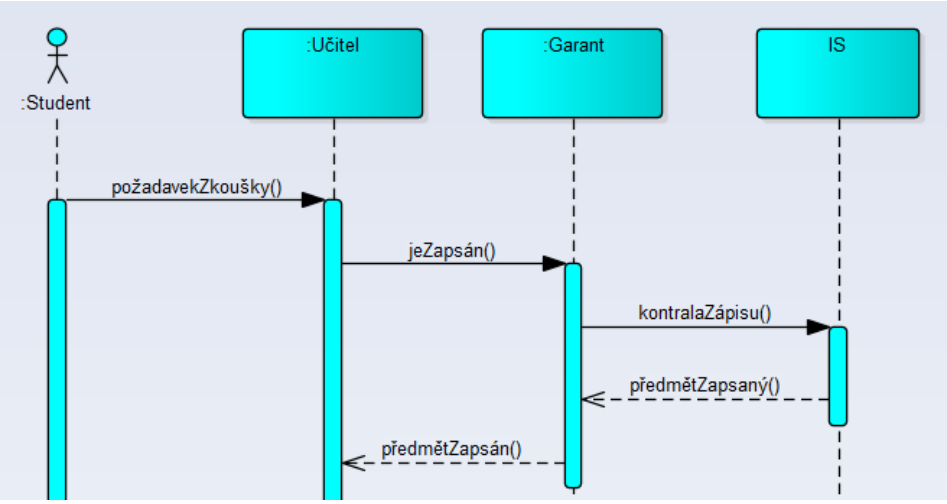
Pro modelování spolupráce objektů používáme zvláštní typy diagramů, které mají vyjadřovací schopnosti k tomu, aby znázornily, jak mezi sebou objekty spolupracují.

4.3.1 Sekvenční

Řadí se do skupiny takzvaných interakčních diagramů, které slouží pro modelování spolupráce objektů. Právě interakční diagramy pomáhají odhalit většinu operací spolupracujících tříd. Jedním ze základních diagramů, které patří do této skupiny, jsou sekvenční diagramy.

Sekvenční diagramy znázorňují objekty na horní straně diagramu. Z každého objektu vede svislá čára, takzvaná lifeline, která představuje život objektu v průběhu případu užití. Součástí objektů je i aktér, který ve většině případů zahajuje případ užití. Objekty si mezi sebou

předávají zprávy, tyto zprávy představují žádost jednoho objektu o vyvolání operace objektu druhého.



Obr. 7. Ukázkový příklad sekvenčního diagramu

4.3.2 Aktivitní

Další speciální případ diagramu popisujícího chování systému představuje diagram aktivit. Tento diagram zobrazuje sekvenci aktivit, které na sebe navazují a slouží k zobrazení logiky vnitřního algoritmu popisovaného systému. Popisují kroky prováděné v rámci případů užití a procesy nebo tok dat mezi uživateli systému.

Základní komponenty diagramu aktivit:

- Akce – jedná se o dále již nedělitelnou akci, takzvanou atomickou
- Aktivity – aktivita představuje stav dělání čehokoliv. Aktivity lze dále rozdělit a vyjádřit podrobněji
- Plavecké dráhy – tyto dráhy slouží pro definování toho, kdo vykonává dané aktivity (osoba, oddělení atd.)

Diagramy aktivit mají více komponent, ale pro pochopení diagramu stačí uvést tyto základní komponenty.

5 SROVNÁNÍ KONKURENČNÍCH SYSTÉMŮ

Následující výčet konkurenčních systémů byl získán průzkumem a zpracováním veřejně dostupných zdrojů na internetu, ovšem nepředstavuje kompletní průzkum trhu a všech jeho nabídek ale pouze malou část.

5.1 KASA FIK

Představuje bezhotovostní systém zahrnující platební terminály a nepřenosné zabezpečené platební štítky na bázi NFC/RFID. Společnost se pyšní navýšením obratů až o 20-30% při použití jejich aplikace, urychlením plateb a snížením front. Umožňují platby v online i offline režimu. [21]

Obr. 8. Logo společnosti KASA FIK

Hlavní funkce:

- EET evidence a napojení na Finanční úřad
- Hlášení tržeb v offline režimu
- Docházka
- Přihlašování zaměstnanců
- Evidence zákazníků
- Nasazení aplikace na terminálech POS
- Elektronická evidence tržeb
- Evidence pohybů na skladě

- Vzdálené naskladnění
- Vytváření mapy stolů (rozložení restaurace)
- Spousta dalších menších funkcí

Aplikace KASAFIK podporuje také mobilní telefony se systémem Android 4.4.x a vyšší. Další zajímavostí je také možnost provedení platby v elektronické měně Bitcoin.

5.2 Frajt

Tato Kroměřížská firma se specializuje na nadstandardní interiérové vybavení a od svého vzniku rozšířila své působení do vybavování center volného času, aquaparků, bazénů, rehabilitačních center, sportovních a kulturních zařízení, škol, administrativních budov, nákupních center, nemocnicí a laboratoří.

Obr. 9. Logo společnosti Frajt s.r.o.

Společnost nabízí jako jeden ze svých produktů autonomní platební systém **Pay-Pass**, který lze využít v následujících oblastech:

- Restaurace a občerstvení
- Nádražní areály
- Kempy a ubytovací zařízení
- Nákupní centra
- Veřejné toalety
- Letní aquaparky a koupaliště
- Čerpací stanice

Tento systém je součástí většího celku, který společnost prezentuje jako Elektronický platební a odbavovací systém EPOS10. Tento systém pracuje s identifikačními čipy, které pracují na frekvencích 125kHz, 13,56MHz nebo na duální technologii. [22]

5.3 IKOS

Společnost IKOS nabízí své služby v oblasti identifikačních technologií, čárových kódů a tiskáren plastových karet. Nejzajímavější oblast působení firmy představují identifikační systémy. Společnost nabízí vlastní hardware jako například snímače, terminály, komunikační zařízení, servery a podobné, ale také software, kterým lze provádět nastavení a zobrazování pořízených dat. Systémy bezkontaktní identifikace představují hlavní oblast činnosti.

Obr. 10. Logo společnosti Ikos s.r.o.

Součástí softwarového řešení společnosti je docházkový systém IKOS-D3, který slouží i mimo jiné pro evidenci docházky, řízení přístupu osob do uzavřených prostor, sledování výrobních operací nebo práce na zakázkách. Systém IKOS-D3 disponuje také funkcionalitami z oblasti objednávání a výdeje stravy [23]. Modul pro objednávání, evidenci a výdej stravy disponuje těmito hlavními funkcionalitami:

- Tvorba jídelníčků
- Pružné nastavování ceny jídel
- Rozlišení strávníků podle kategorií (externisté, zaměstnanci atd.)
- Nastavitelné limity objednaných jídel
- Neomezený počet druhů jídel

Z výše uvedeného vyplývá, že společnost Ikos nabízí téměř stejné služby jako COMINFO a tedy představuje přímého konkurenta na trhu.

5.4 HASAM

Společnost HASAM s.r.o. vznikla v roce 1993 a poskytuje své produkty jak z oblasti hardware tak i software. Nabízí komplexní řešení v segmentu systémů automatické identifikace a registrace a především využívající technologie RFID.

Obr. 11. Logo firmy HASAM s.r.o.

Softwarová aplikace, kterou společnost nabízí spolu se svými produkty, se nazývá EPOS. Aplikace umožňuje prodej vstupenek, na základě RFID čipu eviduje a řídí pohyb osob v rámci areálu, řídí provozy restaurací, eviduje pohyb skladových zásob. Nedílnou součástí softwarových funkcionalit je také možnost nastavení cenových hladin, slevových a marketingových akcí. [24]

Společnost již úspěšně nasadila svůj produkt v následujících oblastech:

- Objednávky a výdej stravy ve školních a závodních jídelnách
- Řízení parkovišť, ovládání závor, platební automaty
- Řešení pro aquaparky jako řízení vstupů, turnikety, platební a informační terminály, pokladní pracoviště a další.

Společnost HASAM s.r.o. tak poskytuje podobné služby a produkty jako COMINFO a opět tak představuje přímého konkurenta na trhu.

6 SMĚRY BUDOUCÍHO ROZVOJE

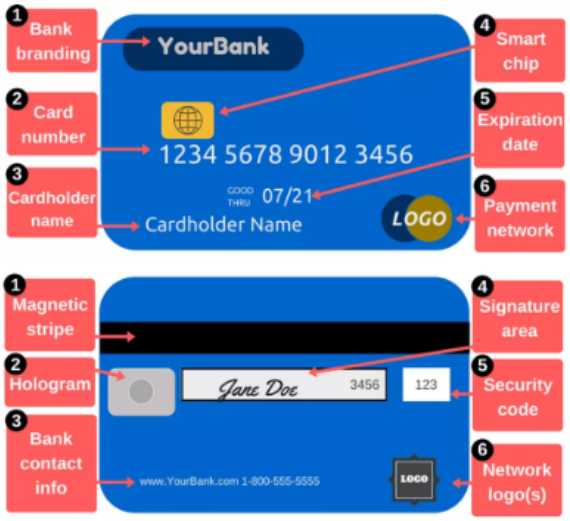
Bezkontaktní platby představují bezpečný způsob pro spotřebitele, jak zakoupit produkty či služby. V dnešní době se pro bezkontaktní platby používají debetní, kreditní či chytré karty, využívající technologie RFID či NFC.

Pro provedení takovéto bezkontaktní platby stačí, aby spotřebitel přiložil svou kartu do blízkosti platebního terminálu. Odtud pochází anglický termín „tap-and-go“. Jelikož bezkontaktní platby nepožadují žádné podepisování účtů či zadávání Pinu je ve většině případů velikost transakce limitována.

Aktuální řešení autonomního platebního systému je založeno pouze na použití identifikační technologie RFID. Software, na kterém je postaven tento autonomní platební systém by se měl do budoucna dále rozvíjet tak, aby následoval trendy v oblasti informačních technologií. V případě, že by k tomuto nedošlo, představoval by takovýto software bezpečnostní riziko a také by ztrácel konkurence schopnost.

6.1 Platební karty

V dnešní době jsou platby pomocí platebních karet již běžně dostupné. Téměř každý obchod či restaurace nabízí tuto možnost. S příchodem platebních karet začali spotřebitelé utrácet více. Jedna ze studií z roku 2001, která byla provedena výzkumníky z MIT, ukazuje, že spotřebitelé jsou ochotni utratit více peněz při platbě platební kartou než v hotovosti. V průměru spotřebitelé zaplatili až o 83% více při platbě platební kartou oproti platbě v hotovosti. [25]



Obr. 12. Schéma platební karty [26]

Z výše uvedené studie vyplývá, že investice do vývoje software pro podporu platebních karet se musí vyplatit. Nejenom, že spotřebitelé utrácejí průměrně více, ale s příchodem platebních karet lze i zvýšit počet potencionálních zákazníků. Z toho důvodu, je čistě logické aby další vývoj software a jeho funkcionalit směřoval k implementaci platby pomocí platebních karet a nahrazení, či doplnění stávajícího řešení využívajícího RFID karet.

6.2 Mobilní platby

Mobilní platby představují elektronickou formu provedení platby mezi spotřebitelem a prodejcem, přičemž alespoň jedna z obou stran musí platbu provést za pomoci mobilního zařízení, které není vázáno na místě a dokáže přijímat či odesílat data bezdrátově.

Provedení mobilních plateb umožňuje hned několik technologií, přičemž nejzajímavějšími a také nejrozšířenějšími jsou technologie NFC, MST a technologie Sound Wave.

Obr. 13. Mobilní platby [27]

6.2.1 NFC

NFC (Near Field Communication) je metoda bezdrátového přenosu dat, která detekuje blízká zařízení a umožňuje komunikaci mezi nimi.

Tato technologie se vyvinula z technologie RFID a je s ní tedy podobná. NFC čip se aktivuje, pokud obdrží signál od druhého čipu, který se musí nacházet ve vzdálenosti nanejvýše několika centimetrů a tak umožní přenos malého množství dat mezi oběma zařízeními.

Pro spojení není zapotřebí provádět párování mezi zařízeními, a jelikož technologie NFC využívá čipy, které spotřebovávají pouze velice malé množství energie, jedná se o jednu z nejúspornějších technologií bezdrátové komunikace.

6.2.1.1 Rozdíl mezi EMV a NFC

NFC komunikace je v dnešní době spojována převážně s mobilními bezkontaktními platbami. EMV představuje rodinu protokolů, které jsou vyvíjeny a spravovány společnostmi jako jsou například American Express, Discovery, Mastercard, Visa, určených pro platbu čipovými kartami.

6.2.2 Bezkontaktní platební nálepky

Ne všechny chytré mobilní telefony v dnešní době podporují technologii NFC. Pro umožnění mobilních plateb pomocí takovýchto telefonů, byly vyvinuty bezkontaktní platební nálepky. Tyto nálepky jsou kompatibilní s terminály podporujícími NFC technologii a nepotřebují samy, žádnou energii. Pracují téměř na stejném principu jako klasické pasivní RFID čipy. NFC nálepky jsou ovšem i zpětně kompatibilní s technologii RFID.

6.2.3 MST

Technologie MST neboli magnetic secure transmission, pracuje s magnetickými signály. Vytváří spojení mezi mobilním zařízením zákazníka a terminálem prodejce. Tyto magnetické signály představují magnetický pásek na standardní kreditní kartě.

MST lze použít úspěšně všude tam, kde lze využít i technologii NFC. Technologie MST představuje potencionální investici do budoucna a to z toho důvodu, že aktuálním majitelem této technologie se stala společnost Samsung. V budoucnu, lze tedy počítat s tím, že drtivá většina mobilních zařízení značky Samsung bude tuto technologii podporovat. Podle statistik bylo v roce 2018 aktivně používáno 893 milionů mobilních zařízení značky Samsung [28], což představuje pádný důvod pro vývoj software tímto směrem.

6.2.4 Sound Wave

Sound Wave využívá zvukových vln pro komunikaci mezi telefonem zákazníka a terminálem prodejce. Hlavní přednost této technologie představuje fakt, že pro její použití stačí, aby mobilní zařízení zvládalo přijímat a vysílat zvuk. Tuto vlastnost mají v dnešní době všechny telefony a ne jen ty chytré.

Podpora této technologie otevře trh pro použití mobilních plateb i v rozvojových zemích, kde ne všichni potencionální zákazníci jsou vlastníky chytrých telefonů, které podporují například technologii NFC. Veliký trh v této oblasti pak představuje Indie, která měla k roku 2017 přes 1.3 miliardy obyvatel [29]. Indie nepředstavuje ideální trh pouze kvůli velikosti její populace ale převážně díky faktu, že podpora technologie Sound Wave není tak cenově náročná pro obchodníky jako NFC [30].

6.2.5 Apple Pay

Další důvodem, proč rozšířit podporu software z RFID i na mobilní platby je technologie Apple Pay, která otevírá trh novým potencionálním zákazníkům. Společnost Apple spustila podporu technologie Apple Pay v České Republice teprve nedávno (19. 2. 2019).

6.3 Otisky prstů

Dalším potencionální rozšířením software do budoucna může být podpora identifikace, založené na rozpoznávání otisku prstů. Tuto technologie lze použít buď to v rámci uzavřených prostor, kam nemá široká veřejnost přístup a je tedy možné identifikovat veškeré potenciální zákazníky, tedy firemní obchody či kantýny atd.. Nebo také v rámci prostor dostupných široké veřejnosti, jako jsou supermarkety, aquaparky, fitness atd. a to v rámci ověření identity obsluhy pokladních systémů. [31]

Obr. 14. Vzorek otisku prstu [32]

V první variantě, tedy použití v uzavřených prostorech, by software pro svou implementaci potřeboval rozšířit databázi zaměstnanců o jejich otisky prstů. Nemohlo by tak dojít k odcizení RFID čipové karty a jak je všeobecně známým faktem, tak otisky prstů jedince jsou unikátní, tedy i možnost záměny by byla téměř nulová.

Druhá varianta, přináší také své výhody. Zaměstnanci, obsluhující pokladní terminály mají přiděleny své přihlašovací údaje. Nicméně tyto údaje mohou mezi sebou zaměstnanci sdílet, což je nežádoucí. Studie z roku 2009 [33], které byly provedeny v USA, ukazují, že zaměstnanci kradou více než zloději. Podle studií ukradne průměrně zloděj z obchodu zboží za $438. Naproti tomu, okrádají zaměstnanci své zaměstnavatele v průměru o $1890. Zavedením identifikace, založené na otiscích prstů, by vedlo k přesnější a jednoznačně dohledatelné historii operací provedených jednotlivými zaměstnanci.

6.4 Rozpoznávání obličeje

V ne tak vzdálené budoucnosti by mohlo být možné provádět nákupy velice jednoduchým způsobem. Zákazník by mohl přijít do obchodu a nakupovat rovnou do své vlastní nákupní tašky. Následně by pouze odešel z obchodu a nemusel by se zdržovat ve frontách, či na samoobslužných pokladnách. Také by ušetřil čas s nutností předělávat nákup z nákupního košíku do své tašky. [34]

Taková to forma nákupu, je v dnešní době pouze těžko představitelná, nicméně v nedaleké budoucnosti, by se mohlo jednat o zcela normální věc. Vše by mohlo být založeno a schopnosti rozpoznávání obličeje a na rozpoznávání zakoupeného zboží. V obchodě by se nacházelo nemalé množství kamer, které by pokrývaly celé prostory prodejny. Při vstupu zákazníka do obchodu, by došlo k naskenování jeho obličeje a rozpoznání o jakého zákazníka se jedná. Tedy získaná data by se prohnala databází, kde by se našla shoda.

Obr. 15. Obličejové rozpoznávání [35]

Pohyb zákazníka po prodejně by byl sledován a v případě, že by si zákazník vzal něco z police, došlo by k rozpoznání daného zboží. Opět by kamerový systém naskenoval zboží a v databází by našel jeho cenu. Také by zároveň snížil jeho stávající počet o množství, které by zákazník zakoupil. Takto by se i snadno udržoval přehled o dostupném množství zboží na prodejně. Poté co by zákazník opustil prodejnu, došlo by k finálnímu vyúčtování zboží zákazníka. Tedy částka, za kterou zakoupil zboží, by mu mohla být stržena z následující výplaty, či formou kreditu z jeho účtu.

Jak je již z výše uvedeného příkladu poznat, použití takovéto technologie v běžných prostorách, které jsou dostupné široké veřejnosti, nebude snadné a v dnešní době ani možné. Pro nasazení by byla potřeba databáze s identitou všech potencionálních zákazníků. Nicméně software autonomního platebního systému, je momentálně nasazen v prostorách, kde se široká veřejnost nepohybuje. Tedy nasazení takovéhoto software v prostorách firemní prodejny, kde se pohybují pouze zaměstnanci, by nemělo být žádným problémem.

V rámci nasazení takového software je možné zahrnout nové funkcionality, jako například identifikace dlužníků. Systém po načtení obličeje a rozpoznání osoby, provede kontrolu dostupných informací a zjistí o zákazníkovi dodatečné informace. Pokud bude zjištěno, že zákazník nemá finanční prostředky na provedení tak velkého nákupu o jaký se pokouší, bude mu tento nákup odepřen.

6.5 Rozpoznání sítnice

Vývoj software tímto směrem by umožnil zákazníkům platit za pomoci rozpoznání jejich oční sítnice. Tedy zákazník by neplatil pomocí kreditní karty, hotovosti či RFID čipem ale namísto toho, by zákazník pouze provedl ověření svého oka. Toto ověření si lze představit jako pohled do kamery, která provede načtení a rozpoznání oční sítnice.

Obr. 16. Rozpoznání sítnice [36]

Oční sítnice platí stejně jako otisk prstu za unikátní identifikační prvek každé osoby. Díky jejich složitosti a variabilitě se jedná o možná i lepší způsob identifikace než jaký představují otisky prstů. Bohužel se opět jedná o možnost rozšíření pouze v rámci uzavřených prostor, kde je možné předem znát identitu potencionálních zákazníků.

6.6 Hlasové rozpoznání

Další jinou formu identifikace zákazníka kromě RFID karty, může představovat také hlasové rozpoznávání. Opět se použití tohoto řešení hodí převážně do uzavřených prostor, kde se pohybují pouze předem známí jedinci. Rozpoznávání hlasu představuje jeden z několika bi-ofaktorů, které jsou pro každou osobu unikátní, a lze jich využít pro identifikace osoby.

V dnešní době technologie rozpoznání hlasu pokročila natolik, že ji již jen velice těžko dokáží ošálit profesionální imitátoři a mechanické nahrávky hlasu [37]. Implementace zařízení pro rozpoznání hlasu může být levnější než implementace jiných technologií, jako třeba rozpoznávání sítnice, otisků prstů a jednoznačně levnější oproti obličejovému rozpoznávání.

II. PRAKTICKÁ ČÁST

7 SOUČASNÉ ŘEŠENÍ PROJEKTU

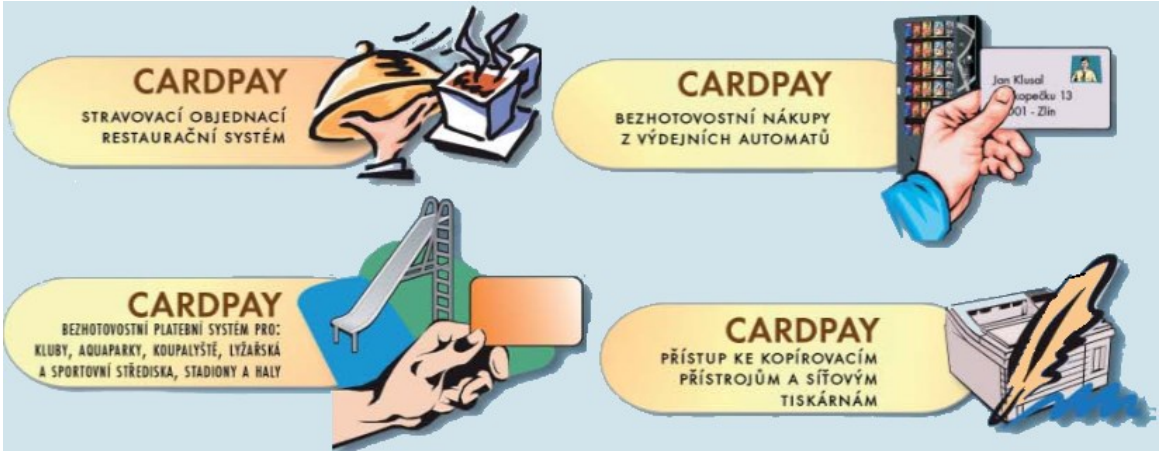
Systém INFOS představuje ucelený balík softwarových aplikací využívajících identifikačních prvků, zejména karet, v různých oblastech firemních, bezpečnostních i jiných činností. Od řízení a definování vstupů a vjezdů, přes zpracování docházky, evidenci návštěvníků, ovládání parkovišť, řízení výtahů až po řešení objednávkového i restauračního stravování, obsluhu automatů na výdej stravy a nápojů, vyhodnocení časové náročnosti zakázek, identifikace výrobků a dalších oblastí. [38]

Jednotlivé balíky mají své oficiální kódové označení, následuje krátký výčet modulů systému INFOS

- Access (přístupový systém)
- Passport (docházkový systém)
- Visit (návštěvnický evidenční systém)
- VLIT (monitorování zaměstnanců v dolech)
- Laundry (čipová identifikace prádla)
- WATT (Intranetová aplikace pro docházková data)
- SVZ (Sledování, vyhodnocení zakázek)
- Další speciální menší moduly, většinou dle požadavků zákazníka

7.1 Modul INFOS CARDPAY

Hlavní modul systému INFOS, jehož se týká tato část rešerše projektu je bezhotovostní platební systém CARDPAY. V době svého vzniku se jednalo o flexibilní moderní aplikaci. Tato aplikace se sama skládá z několika menších částí, které tvoří kompaktní celek.



Obr. 17. Možnosti použití modulu INFOS CARDPAY [39]

Tento celek představuje bezhotovostní platební systém, jehož hlavní předností je jeho vlastnost přizpůsobení se požadavkům uživatelů na základě zvoleného způsobu použití. Tento systém lze využívat různě a vysokou variabilitu poskytuje i možnost propojení modulu CARDPAY s dalšími moduly, například s ACCESS. Tato rešerše projektu se zabývá také propojením systému CARDPAY se snímači identifikačních karet, přičemž nejzajímavější techniku představuje identifikace založena na technologii RFID. Systém CARDPAY samozřejmě umožňuje i identifikaci založenou na použití jiných technologií (čárové kódy, magnetické karty atd..).

Základní možné oblasti nasazení systému CARDPAY jsou:

- Sportovní a zábavní střediska (např. fitness centra) formou klubového systému (identifikace a výhody pro členy)
- Vstupenkový a přístupový systém pro větší prostory (Aquaparky, koupaliště, bazény, stadióny, haly, lyžařská střediska a další)
- Parkovací systém
- Systém ovládání síťových tiskáren a kopírek (použití například ve školách)

7.2 Stravovací systém CARDPAY

Systémový modul CARDPAY se významně rozšířil také v oblasti stravovacích systémů. Lze jej uplatnit například ve firemních jídelnách, restauracích či školních menzách. Představuje řešení pro lokální bezhotovostní platební místa spojená do jednoho centra. V oblastech podnikového stravování představuje jednoduché a výhodné řešení plně nahrazující klasický „stravenkový“ systém.

Stravovací systém CARDPAY umožňuje správu uživatelských účtů, kdy každý účet má přidělenu unikátní identifikační kartu, pomocí které lze vykonávat bezhotovostní platby. Všechny uživatelské účty se spravují pomocí centralizovaného databázového systému, kde lze nastavit typ uživatelského účtu a spoustu dalších vlastností, kde jednou z těch zajímavějších představuje také možnost nastavení limitu, který nelze u karty přečerpat. Tento limit může například představovat vratnou zálohu, použitou při ztrátě karty.

U každého účtu se také uvádí stávající kredit, který představuje dostupné finanční prostředky. Při nákupu dochází k ověření množství aktuálního kreditu s cenou nákupu. V případě nízkého kreditu dojde k zamítnutí platby. Systém také umožňuje strhávat útratu přímo ze mzdy uživatele, či klasické nabíjení kreditu formou hotovosti.

7.2.1 Objednávkové stravování

Stravovací systém CARDPAY lze konfigurovat také do takzvaného módu objednávkového stravování. Tento způsob použití umožňuje objednávání jídel podle předem připravených jídelníčků. Tento mód stravování lze použít ve dvou variantách, přičemž první představuje předem definovaný jídelníček pro následující den a někdy i také číslo jídla. Druhou variantu tvoří dlouhodobé objednávky, kdy se vytváří fixní jídelníček na předem definovanou dobu (např. týden).

Systém CARDPAY použit v módu objednávkového stravování podporuje vytváření jídelníčků, nastavování výdejních míst spolu s možností nastavení omezení pro tyto výdejní místa. Současně poskytuje také intranetové rozhraní. Toto rozhraní poskytuje pohodlný způsob objednání jídla, přehled aktuálních jídelníčků, přehled objednávek či historii objednávek.

8 NOVÉ ŘEŠENÍ

8.1 Motivace návrhu nového řešení

Původní řešení platebního systému CARDPAY bylo začleněno do produktové platformy INFOS někdy kolem roku 2000. Na začátku běžela celá platforma INFOS v operačním systému MSDOS a byla napsána v jazyce C++. Vývoj platformy INFOS probíhal ve vývojovém prostředí Visual Basic 6, jehož oficiální podpora ovšem skončila již před více než 14 lety, tedy v roce 2005. Společnost Microsoft ještě ale poskytovala do roku 2008 prodlouženou podporu. [40]

V dnešní době se tedy jedná již o velice zastaralý systém, který byl původně vyvíjen pro dnes již nepoužitelný operační systém MSDOS. Je tedy jasné, že takovýto systém nelze již nadále udržovat a s novějšími verzemi operačního systému Windows jej nebude možné ani použít. Z tohoto důvodu se dá v budoucnu počítat s tím, že nový klienti nebudou mít o takovýto produkt zájem a také stávající klienti mohou zájem ztratit. Další problém může představovat bezpečnost takovýchto strojů. Starší stroje a vývojová prostředí mají známé chyby a slabiny, který lze využít při napadení systému. Toto je také pádným důvodem k přechodu na novější platformu.

Firma COMINFO a.s. se rozhodla přesunout stávající řešení na platformu .NET s jednotným jazykem C#. O tomto přesunu se začalo jednat již někdy kolem roku 2009, ovšem nové řešení je ve vývoji teprve od roku 2014 a dosud zahrnuje teprve malou část celé produktové platformy INFOS.

8.2 Popis návrhu nového řešení

Počítá se, že hlavní oblastí nasazení platebního systému budou představovat firemní jídelny, školní menzy či kantýny. Nicméně platební systém by mělo být možno používat také úspěšně v jiných oblastech (např. aquaparky). Samozřejmě, že se funkcionality platebního systému budou odvíjet od oblasti použití. Tyto funkcionality lze odemykat a uzamykat na základě použití licenčních klíčů.

V rámci řešení tohoto projektu vznikl návrh softwarových funkcionalit platebního systému, který mimo jiné splňuje následující základní funkcionality:

Tab. 1. Softwarové funkcionality lokálního platebního systému

Funkcionality	Detail
Základní funkcionality platebního systému	správa interních uživatelských účtů
	definice limitů, položek prodeje a jídelníčků
Definice cenových hladin položek prodeje	neomezený počet hladin
	časová závislost
	vazba na počet kusů
Provoz více organizačních a účetních jednotek na jednom systému	zobrazení dat s ohledem na GDPR
	rozdělení jídelníčků na jednotlivé výdejny a časy výdeje

8.2.1 Základní funkcionality platebního systému

8.2.1.1 Správa interních uživatelských účtů

Rozhraní pro správu uživatelských účtů je navrženo formou centrální webové aplikace, která má přístup do SQL databáze. Přístup do webové aplikace je umožněn pouze uživatelům s administrátorskými oprávněními. Počet těchto uživatelů by měl být omezen na nezbytné minimum, jelikož s větším množstvím roste riziko vzniku lidské chyby a mohlo by dojít k nežádoucím událostem.

Aplikace je navržena tak, aby pracovala se čtyřmi základními typy uživatelských účtů, přičemž je zde samozřejmě možnost vytvoření nového vlastního typu účtu. Tato funkcionalita je dostupná pouze z administrátorského účtu. Při návrhu aplikace se tedy vycházelo z těchto čtyř účtů:

- Administrátor
- Pokladní
- Dodavatel
- Uživatel

Administrátor jako jediný typ účtu má povoleny všechny funkcionality systému a představuje tedy nejvyšší právní roli v systému. Administrátor umí spravovat uživatelské účty, vytvářet jídelníčky, dodavatelské objednávky, výdejny a zvládá spoustu dalších funkcionalit.

Pokladní představuje druh uživatelského účtu, který má oprávnění pro přihlášení se k pokladnímu terminálu (POS). Dokáže zakládat nové objednávky, vybírat obsah objednávky, rušit objednávky a další funkcionality spojené s nákupem na POS.

Dodavatelský typ účtu není aktivní na výdejnách a nemá zde žádné oprávnění, nicméně má přístup do webového rozhraní. Ve webovém rozhraní vidí dodavatel všechny své aktivní objednávky, dokáže přijímat nové objednávky a upravovat je. Každý dodavatel vidí pouze ty výdejny, na které dodává zboží a přitom nevidí ostatní dodavatele.

Uživatelský účet představuje základní účet, tedy účet, který je přidělen klientovi výdejny. Má přístup do webového rozhraní, kde může sledovat historii objednávek, aktuální zůstatek na účtu, jednotlivé jídelníčky na jídelnách, ke kterým je registrován a další funkcionality. Uživatel si může i přes webové rozhraní rezervovat jídlo za předpokladu, že to výdejna dovoluje.

8.2.1.2 Definice limitů, položek prodeje a jídelníčků

Dalšími funkcionalitami, kterými systém oplývá, jsou funkcionality týkající se položek prodeje. Při nasazení v prostorách jídelen, lze definovat také dostupné jídelníčky a jednotlivá jídla pro tyto jídelníčky.

Lze si tedy představit, že platební systém bude nasazen v prostředí jídelny, kterou ovšem navštěvují zaměstnanci z mnoha různých firem a každá firma má jiné požadavky či dostupné služby pro své zaměstnance. Tedy poté co terminál ověří identitu zákazníka (Obr. 6) odešle server odpověď, která v sobě ponese právě zmiňované limity položek prodeje a jídelníčků.

Příklady:

1. Zaměstnanec A patří k firmě X a ta určila svým zaměstnancům následující limity: Zaměstnanci mají nárok na jeden oběd a jednu večeři. Obědy jsou vydávány pouze v časech od 11:00 do 13:00. Večeře jsou vydávány v časech od 17:00 do 18:00. Firma X neumožnila svým zaměstnancům další doplňkový prodej.
2. Zaměstnanec B patří k firmě Y a ta definovala tyto limity: Zaměstnanci si mohou vzít až dvě jídla současně, přičemž je pouze na nich zda si vyberou z nabídky obědů či večeří anebo z každé pouze jednu. Časy výdaje obědů i večeří platí stejně jako pro firmu X. Firma Y také ale omezila, z jakého výběru jídel si mohou zaměstnanci vybírat.

Z příkladů definice limitů lze odvodit následující omezení, která musí umožňovat platební systém:

- Limit počtu jídel, na která má zaměstnanec nárok. Tento limit lze definovat jako denní či měsíční anebo kombinace obojího.
- Limit času, ve kterém je možné si jídlo vyzvednout. Definice tohoto limitu se odvíjí spíše od nároků provozovatele jídelny. V případě, že se zde stravuje více firem, pak může být nežádoucí jejich vzájemné prolínání.
- Limit jídelníčků, představuje omezení nabídky nabízených jídel. Zaměstnavatel se může rozhodnout, že pouze výše postavení zaměstnanci mají nárok na dražší stravu. Také lze nabízet zaměstnanci jídla omezená na základě jeho alergií a tím usnadnění rozhodování zaměstnance a vyvarování se případným zdravotním potížím.

Při nasazení platebního systému v jiné oblasti, tedy třeba v oblasti aquaparků, lze samozřejmě počítat s definováním jiných limitů, které se budou odvíjet podle potřeb dané oblasti.

8.2.2 Definice cenových hladin položek prodeje

8.2.2.1 Neomezený počet hladin

Ke každé položce prodeje musí být možné přidělit neomezené množství cenových hladin. V reálné situaci se nejedná o neomezené množství, ale limitu by nemělo být dosaženo, tedy až desítky možných hladin pro jednotlivé položky prodeje.

Možnost nastavení různých cenových hladin položek prodeje slouží k nastavení jiných cen podle druhu strávníka, množství prodávaných položek anebo podle data spotřeby. Tedy například zaměstnanci mohou platit za stejné jídlo rozdílné částky. Rozdíl a důvod proč budou někteří zaměstnanci platit více či méně určuje zaměstnavatel. Také externí strávníci, kteří nejsou zaměstnanci žádné z firem a většinou tedy platí i hotovostí mají svou vlastní cenovou hladinu, mnohdy vyšší jelikož cena není dotována zaměstnavatelem. Jinou cenovou hladinu mohou představovat také akční položky, u kterých brzy vyprší doba trvanlivosti.

Příklad:

- Školní menza nabízí až tři rozdílné cenové hladiny položek prodeje. První cenová hladina patří pro studenty, kteří mají nejvýhodnější cenovou hladinu díky dotacím státu. Druhá cenová hladina v pořadí připadá zaměstnancům, jedná se tedy o učitele.

Třetí nejvyšší cenová hladina zahrnuje všechny externí strávníky, kteří nakupují za hotovost.

8.2.2.2 Časová závislost

Některé nebo dokonce i všechny položky prodeje jsou do míst prodeje dodávány externími dodavateli. Tito dodavatelé tedy určují základní pořizovací cenu, od které se odvíjí cenová hladina položek prodeje. Pořizovací cena je pevně dána smlouvou s dodavatelem a tato smlouva se uzavírá na pevnou dobu, může to být například celý rok. Jelikož dochází vlivem inflace či jiných faktorů k nárůstu pořizovací ceny, může dojít ke změně základní pořizovací ceny a tato změna se musí také promítnout dynamicky do cenových hladin položek prodeje. Tedy cenové hladiny položek prodeje musí mít časovou závislost a musí pružně reagovat na změny.

8.2.2.3 Vazba na počet kusů

Cenové hladiny položek prodeje se také odvíjí od velikosti objednávky. Platební systém by měl umožňovat, na základě nastavení filtrů, měnit cenovou hladinu položkám prodeje v návaznosti na velikosti objednávky.

Příklad:

- Ve smlouvě s dodavatelem je stanoveno, že při objednávce do 500 kusů zboží X, je cena za kus 0,6 Kč a při objednávce nad 500 kusů je cena již 0,5 Kč za kus. Platební systém musí na základě takto vytvořené objednávky automaticky promítnout změny do cenových hladin položek prodeje.

8.2.3 Provoz více organizačních a účetních jednotek na jednom systému

Základní ideologií lokálního platebního systému je nabídka jeho služeb například majitelům jídelen. Tito majitelé mohou mít více provozoven na více místech, přičemž je žádoucí aby mezi sebou mohli tyto výdejny komunikovat. Z tohoto předpokladu vyplývá následující:

- Jedna instance lokálního platebního systému se vztahuje na jednu jídelnu. Tyto instance se mohou shlukovat do celků v případě, že má zákazník více jídelen.
- Dodavatelé zákazníka disponují možností přístupu do webového rozhraní, které jim umožňuje správu objednávek pro jídelny, se kterými uzavřeli smlouvu.
- Zákazník musí mít možnost disponovat více organizačními jednotkami, které mají možnost současného přístupu do systému.

8.2.3.1 Zobrazení dat s ohledem na GDPR

Díky tomu, že zákazníkovi dodavatelé mají přístup do webového rozhraní, je nutné celý systém navrhnout na základě legislativy GDPR. To znamená, že dodavatelé vidí pouze údaje týkající se zákazníků, se kterými uzavřeli smlouvu a tyto údaje jsou viditelné pouze v omezené formě, která zabraňuje jakékoliv možné identifikaci zákazníka třetí osobou.

Tato stejná omezení platí v rámci platebního systému, pouze na úrovni výdejny. V případě ztráty identifikační karty nesmí být možné identifikovat zákazníky výdejny na základě identifikačního čísla této karty. Touto možností smí disponovat pouze navržený platební systém, který provádí kontrolu takzvaně nepřímo.

8.2.3.2 Rozdělení jídelníčků na jednotlivé výdejny a časy výdeje

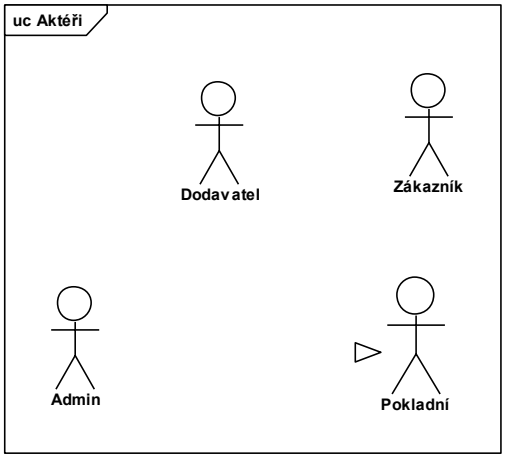
Jednou ze základních platebních funkcí systému je tvorba takzvaných jídelníčků. Tyto jídelníčky představují aktuální nabídku položek prodeje. Jsou vydávány na pevně stanovenou dobu, většinou se jedná o jeden celý týden. Jídelníčky se také mohou ohlašovat nějakou dobu před jejich platností kvůli možnému objednání jídel a tím zajištění lepší a přesné dodávky.

V případě, že zákazník disponuje více jídelnami, musí mít možnost vytvářet tyto jídelníčky nezávazně a přidělovat jim výdejny. Jídelníčky lze také aktivovat podle času výdeje to znamená, že v rámci jistého časového úseku je aktivní jídelníček C a s průběhem času může dojít k aktivaci jídelníčku B.

9 NÁVRH SOFTWAROVÝCH FUNKCIONALIT

Tato kapitola obsahuje pouze vybrané aktivitní diagramy, sekvenční diagramy, diagramy tříd, případy užití a scénáře k těmto případům užití. Popisují se zde tedy základní kořenové funkcionality navrhovaného programu.

Obr. 11. zobrazuje vystupující aktéry v rámci platebního systému. Tito aktéři jsou použiti dále pro prezentaci navržených softwarových funkcionalit autonomního platebního systému.



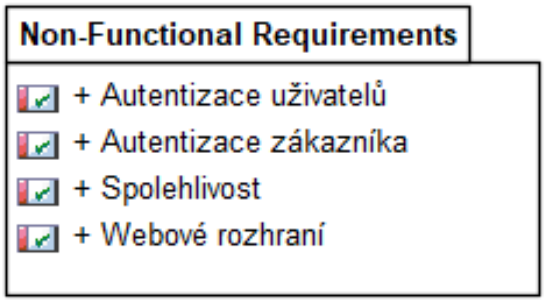
Obr. 18. Aktéři platebního systému

Aktéři a jejich role v systému jsou popsány v předchozí kapitole *8.2.1.1 Správa interních uživatelských účtů.*

9.1 Požadavky

Návrh softwarových funkcionalit autonomního platebního systému je založen na následujícím seznamu funkčních a nefunkčních požadavků.

9.1.1 Nefunkční Požadavky

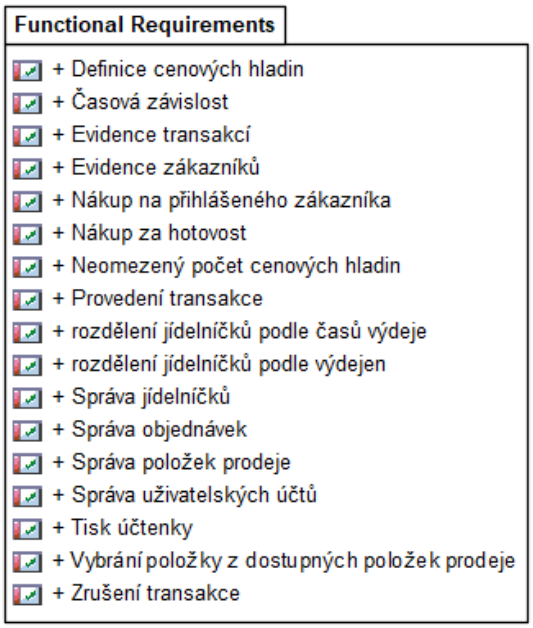


Obr. 19. Základní nefunkční požadavky

Seznam s detailním popisem nefunkčních požadavků:

- *Autentizace uživatelů* – Systém provádí ověření uživatelů, kteří se chtějí přihlásit do systému. Bez provedení autentizace je funkcionalita systému limitována či zcela zablokována.
- *Autentizace zákazníka* – Systém dokáže ověřit identitu zákazníka po přiložení identifikační karty k terminálu. Na základě této identifikace jsou zobrazeny položky prodeje, na které má zákazník nárok.
- *Spolehlivost* – Systém musí být v 100% případů spolehlivý. Tedy pokud se terminál nedokáže spojit se serverem, dochází k aktivaci bezpečnostních opatření, přechodu na prodej za hotové a omezení prodeje pouze na položky prodeje, které jsou dostupné všem zákazníkům.
- *Webové rozhraní* – Systém poskytuje i webové rozhraní uživatelům, převážně pak uživatelům ze skupiny dodavatelé. Toto webové rozhraní slouží dodavatelům ke správě svých objednávek.

9.1.2 Funkční Požadavky



Obr. 20. Základní funkční požadavky

Seznam s detailním popisem funkčních požadavků:

- *Evidence transakcí* – Všechny proběhlé transakce se skladují do databáze po určitou dobu. Tato data slouží k různým statistickým přehledům.

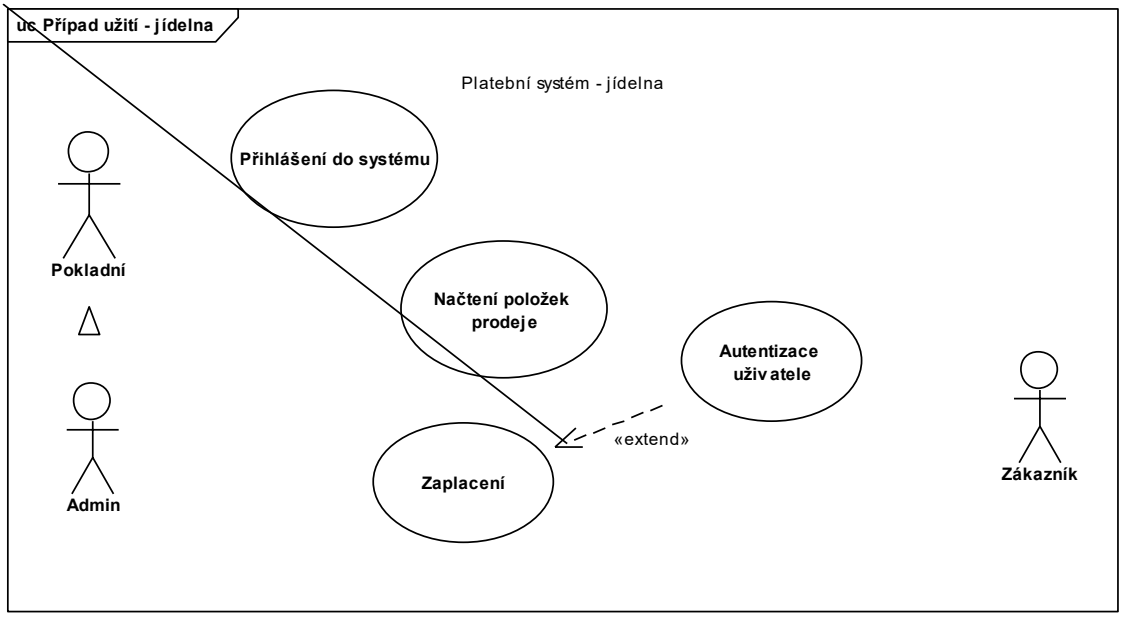
- *Evidence zákazníků* – Do této evidence spadají všichni zákazníci, kteří navštěvují jídelnu a mají svou identifikační kartu.
- *Nákup na přihlášeného zákazníka* – Pokud se zákazník přihlásí pomocí své identifikační karty při placení, proběhne platba formou strhnutí finanční částky z účtu zákazníka. Pokud má zákazník nedostatečný limit, transakce se nedokončí a přejde se na platbu hotovostí.
- *Nákup za hotovost* – Systém umožňuje provádět platbu formou hotovosti.
- *Provedení transakce* – Systém musí umožňovat provedení transakce, jedná se o jeden ze základních požadavků.
- *Rozdělení jídelníčků podle času výdeje* – Jídelníček lze nastavit jako aktivní pouze v konkrétním čase.
- *Rozdělení jídelníčků podle výdejen* – V případě aplikování jedné instance platebního systému na více různých jídelen, lze rozdělit jídelníčky na jednotlivé jídelny.
- *Správa jídelníčků* – Jídelníčky lze vytvářet, mazat, upravovat, nastavovat limity. Jídelníčky jsou skládány z položek prodeje.
- *Správa objednávek* – v rámci systému lze spravovat objednávky u dodavatelů, tedy lze je zadávat, upravovat, rušit.
- *Správa položek prodeje* – Položky prodeje lze vytvářet, upravovat a mazat. Lze nastavovat limity v případě omezení.
- *Správa uživatelských účtů* – Vytvoření, upravení, smazání uživatelů. Uživatelé mají nastavenu úroveň oprávnění.
- *Tisk účtenky* – Systém musí být schopen vytisknout po dokončení transakce účtenku, s podrobným seznamem zakoupených položek prodeje a jejich cenami.
- *Vybrání položky z dostupných položek prodeje* – Uživatelské rozhraní musí nabízet aktuálně dostupné jídelníčky a veškerý doplňkový sortiment, který je aktuálně prodáván.
- *Zrušení transakce* – Transakci lze zrušit před jejím finálním dokončením, spolu s odstraňováním již načtených položek prodeje.
- *Definice cenových hladin* – Každé položce prodeje lze nastavit vlastní cenovou hladinu. Výše této hladiny se odvíjí z ceny, která byla stanovena při objednávce. Tato cena se může měnit podle počtu objednaných kusů.
- *Časová závislost* – Cenové hladiny položek prodeje se mohou měnit automaticky podle časového období.

- *Neomezený počet cenových hladin* – Položky prodeje mají možnost vytvoření neomezeného počtu cenových hladin.

9.2 Funkcionality v prostředí jídelny

9.2.1 Model případů užití – jídelna

První základní model případů užití představuje chování systému v prostředí výdejny (Obr. 12).



Obr. 21. Model případů užití – jídelna

9.2.2 Scénáře k případům užití

9.2.2.1 Případ užití – Zaplacení

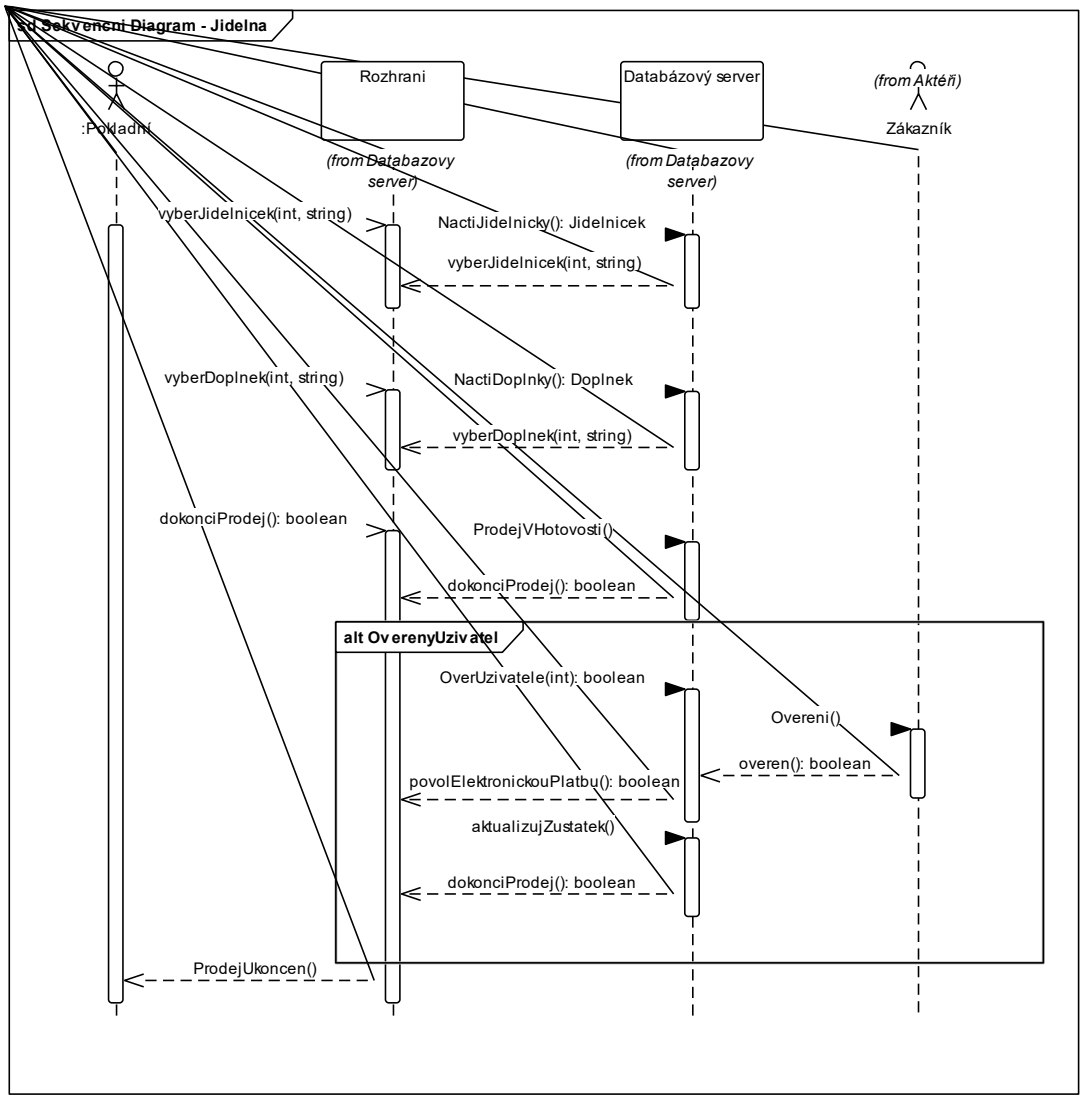
Tab. 2. Primární scénář případu užití – Zaplacení

Krok	Role	Akce
1.	Systém	zkontroluje autentizaci uživatele
2.	Systém	pro neautentizovaného uživatele povolí tlačítko platby v hotovosti (vyvolání alternativního scénáře)
3.	Aktér	stiskne tlačítko platby v hotovosti
4.	Systém	zobrazí formulář obsahující všechny vybrané položky a jejich ceny
5.	Aktér	Potvrdí formulář
6.	Systém	uzavře formulář a aktualizuje UI rozhraní

Tab. 3. Alternativní scénář případu užití – Zaplacení

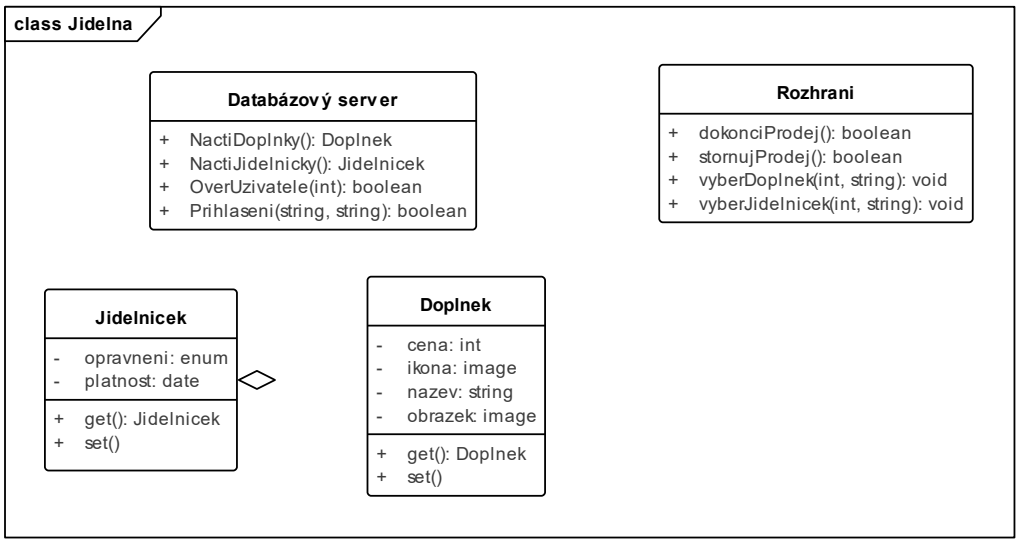
Krok	Role	Akce
2a1	Systém	provede kontrolu zůstatku na účtu uživatele
2a2	Systém	v případě dostatečného zůstatku na účtu povolí elektronické platby
2a3	Aktér	zvolí platbu elektronickou formou
2a4	Systém	zobrazí formulář s načtenými položkami, jejich ceny a zůstatek na účtu po odečtení načtených položek
2a5	Aktér	potvrdí formulář
2a6	Systém	aktualizuje zůstatek na účtu uživatele
2a7	Systém	odhlásí autentizovaného uživatele a pokračuje bodem 6 primárního scénáře

9.2.3 Sekvenční diagram případu užití – Zaplacení



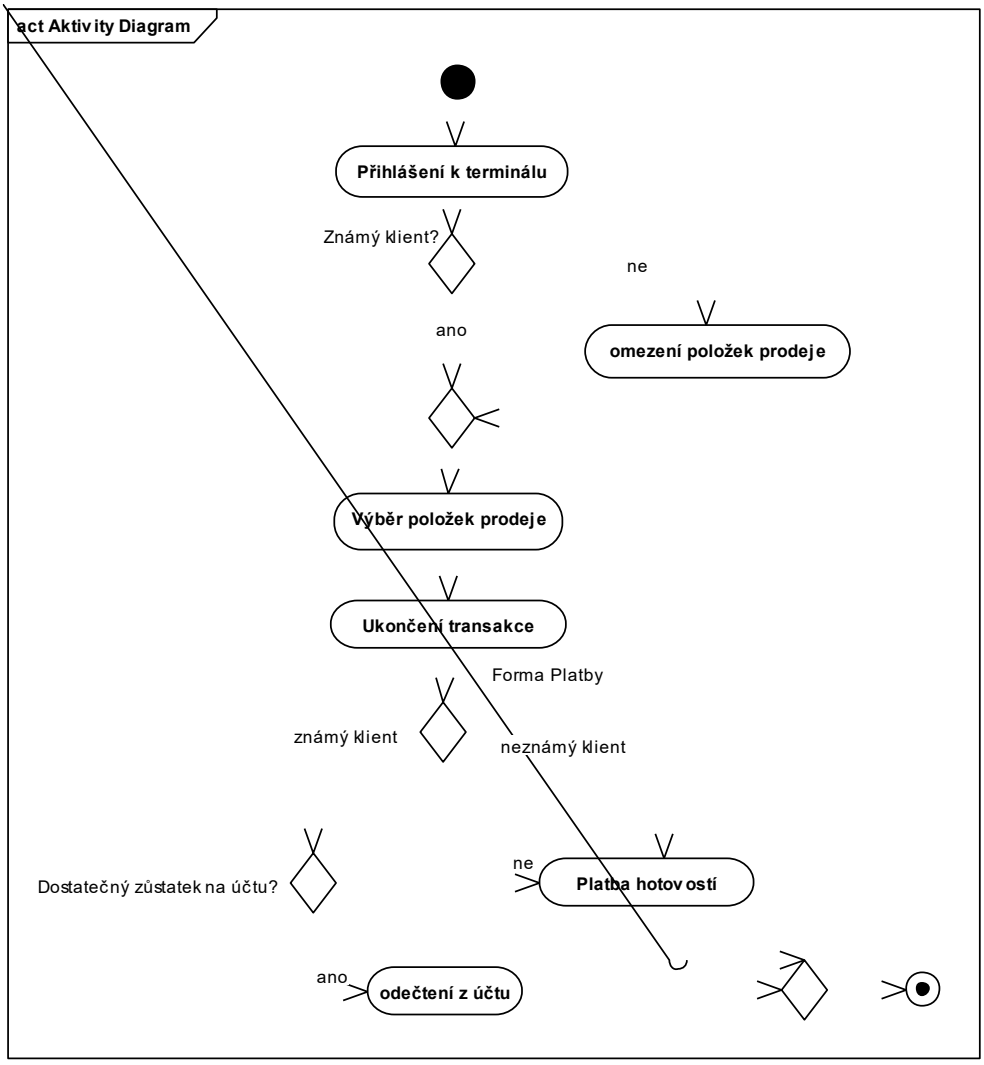
Obr. 22. Sekvenční diagram případu užití – Zaplacení

Sekvenční diagram interpretuje, jak spolu komunikují třídy vyobrazené na obrázku (Obr. 23).



Obr. 23. Diagram tříd – komunikace server - rozhraní

9.2.4 Diagram aktivity - Zaplacení



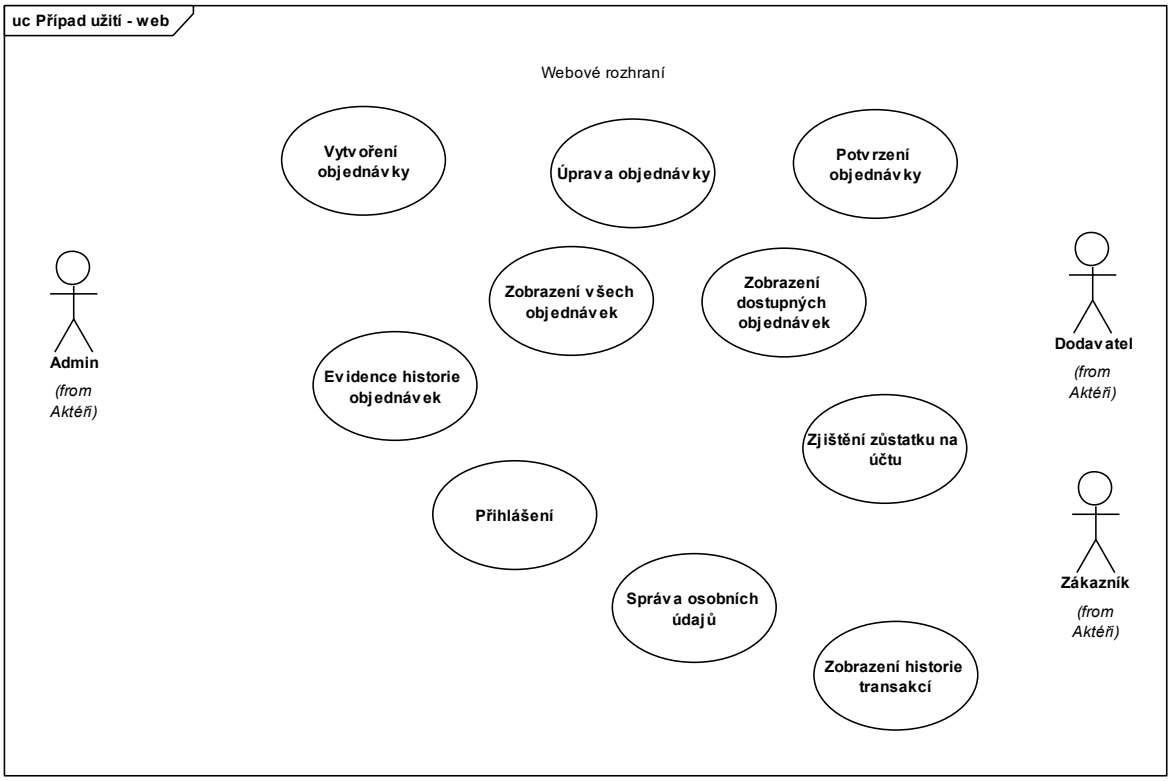
Obr. 24. Aktivitní diagram – zaplacení

9.3 Funkcionality webového rozhraní

Následující kapitola popisuje funkcionality autonomního platebního systému v rámci webového rozhraní. Toto rozhraní poskytuje převážnou většinu funkcionalit platebního systému.

9.3.1 Model případů užití – webové rozhraní

Dalším případem užití je webové rozhraní, které mimo jiné slouží dodavatelům a administrátorovi ke správě objednávek (Obr. 25). Do webového rozhraní mají také přístup uživatelé pro správu osobních údajů a kontrolu zůstatku na účtu.



Obr. 25. Model případů užití – webové rozhraní

9.3.2 Scénáře k případům užití

Tab. 4. Scénář případu užití - Přihlášení

Krok	Role	Akce
1	Systém	zobrazí přihlašovací formulář
2	Aktér	vloží přihlašovací údaje
3	Systém	ověří přihlašovací údaje
4	Systém	načte UI rozhraní podle Aktérovi role

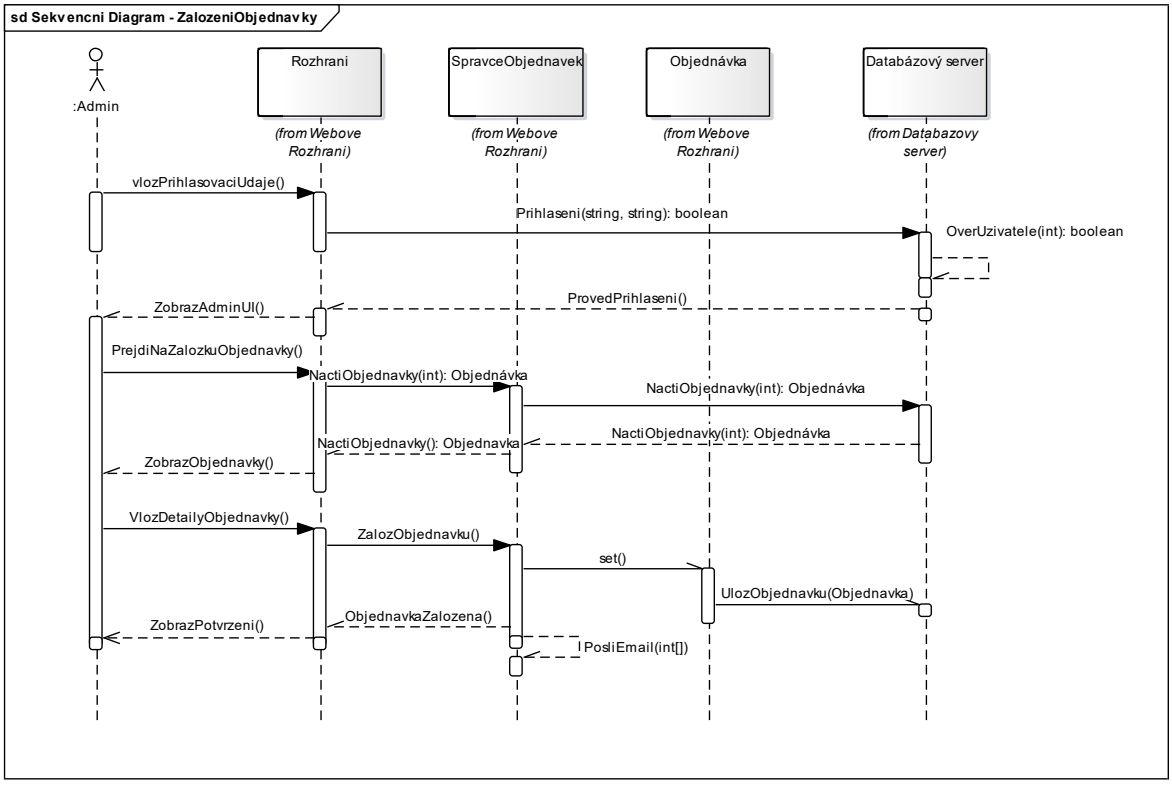
Tab. 5. Scénář případu užití – Vytvoření objednávky

Krok	Role	Akce
1	Aktér	zahájí případ užití stisknutím tlačítka Vytvořit objednávku.
2	Systém	zobrazí stránku pro nastavení detailů objednávky
3	Aktér	vyplní detaily objednávky a zvolí dodavatele
4	Systém	provede kontrolu zadaných údajů
5	Aktér	potvrdí objednávku
6	Systém	pošle emailové upozornění dodavateli a kopii administrátorovi
7	Systém	potvrdí úspěšné založení objednávky

Tab. 6. Scénář případu užití – Úprava objednávky

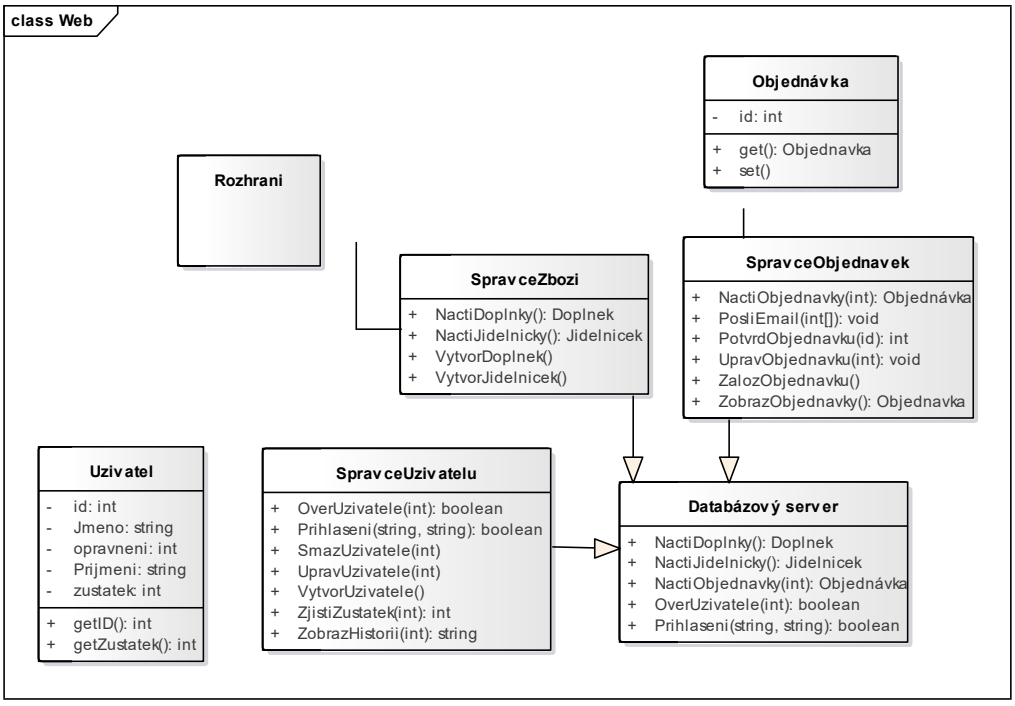
Krok	Role	Akce
1	Aktér	zvolí editaci existujících objednávek
2	Systém	zobrazí dostupné objednávky
3	Aktér	vybere objednávku pro editaci
4	Systém	zobrazí detaily objednávky
5	Systém	povolí editaci pouze pro vybrané detaily objednávky na základě oprávnění Aktéra
6	Aktér	upraví detaily objednávky
7	Systém	uloží úpravy do databáze
9	Aktér	ukončí editaci objednávky
8	Systém	odešle upozorňující email všem aktérům, kteří mají zapnuto sledování objednávky

9.3.3 Sekvenční diagram případu užití – Vytvoření Objednávky



Obr. 26. Sekvenční diagram případu užití – Vytvoření Objednávky

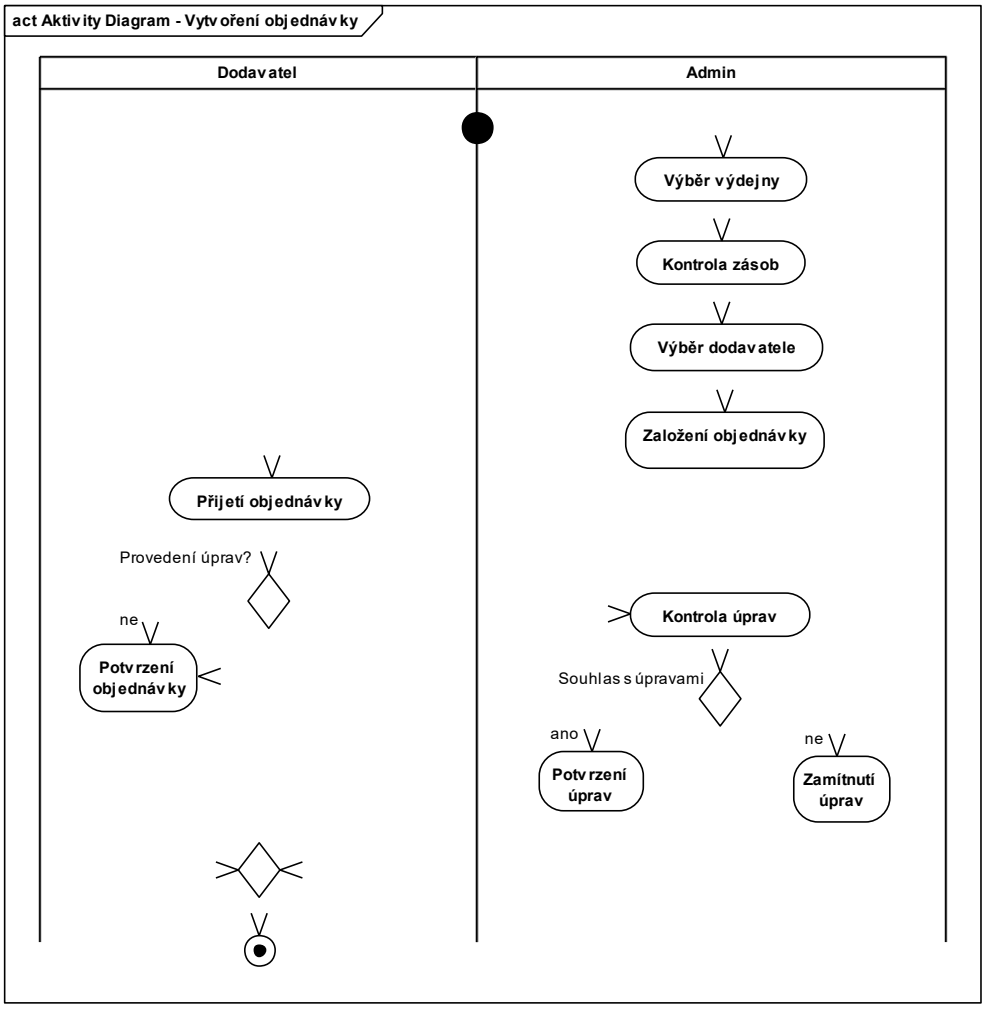
9.3.4 Diagram tříd pro webové rozhraní



Obr. 27. Diagram tříd – webové rozhraní

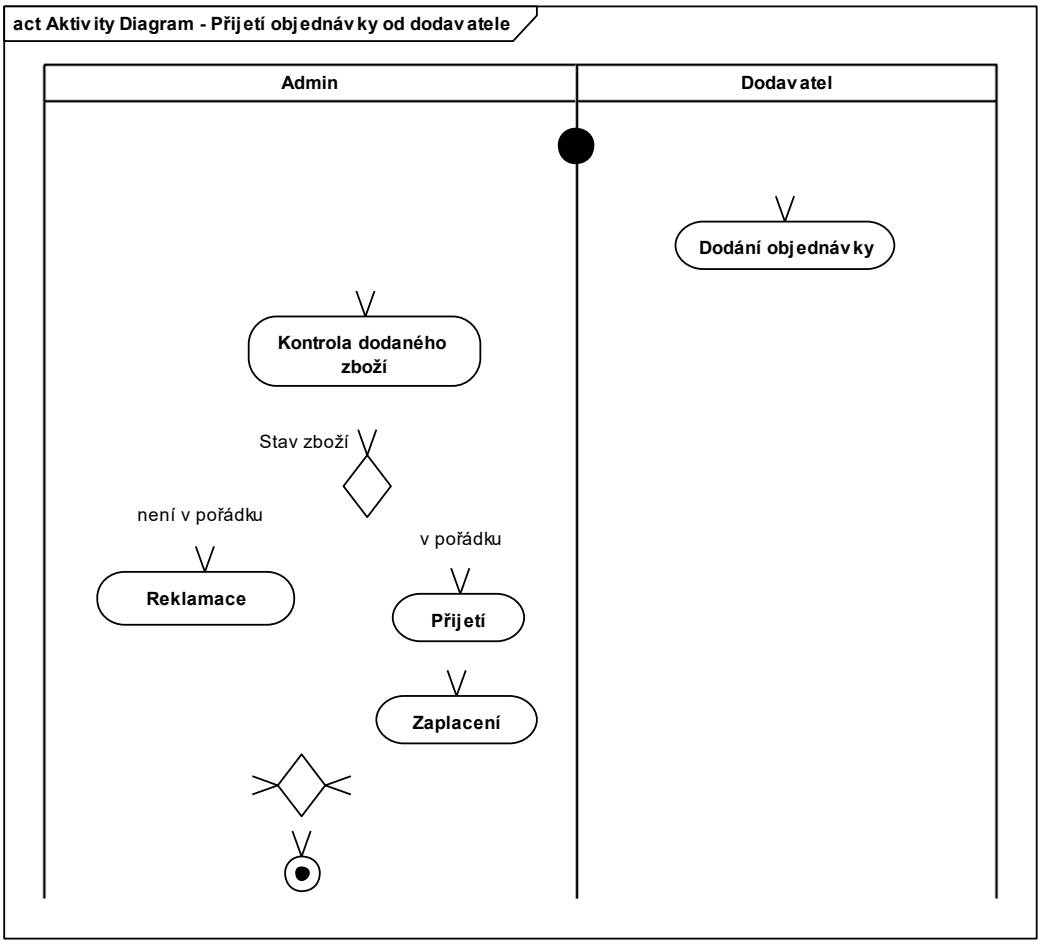
Diagram tříd zobrazuje základní návrh, jak by mohli vypadat třídy, které spolupracují v rámci webového rozhraní. Centrální třídy, které komunikují s uživatelských rozhraním jsou třídy SpravceZbozi, SpravceObjednavek a SpravceUzivatelu. Tyto třídy využívají třídu Databázový server, která slouží ke komunikaci s databází.

9.3.5 Diagramy aktivit



Obr. 28. Aktivitní diagram – Vytvoření objednávky

První diagram aktivit (Obr. 28) zachycuje chování systému při založení objednávky u dodavatele. Součástí diagramu je také případ, kdy dochází k úpravě zadané objednávky dodavatelem. Nejprve se musí administrátor přihlásit do webového rozhraní. Aktivita poté začíná ve chvíli, kdy administrátor přejde na záložku výdejen, provede kontrolu zásob a poté začne zakládat novou objednávku u dodavatele.

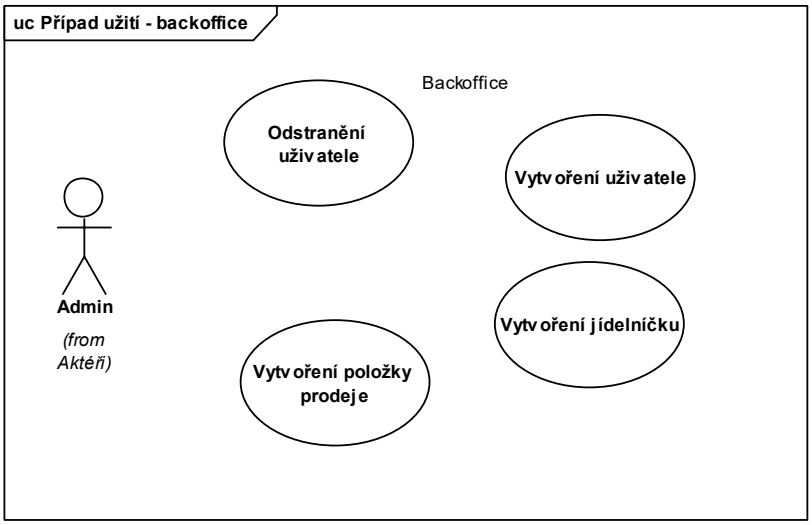


Obr. 29. Aktivitní diagram – Přijetí objednávky

Druhý aktivitní diagram (Obr. 29) popisuje chování systému při přijetí a potvrzení objednávky od dodavatele. Skrze systém lze zadávat případné reklamace, o kterých je dodavatel ihned informován emailem.

9.3.6 Model případů užití – backoffice

Tento případ užití popisuje kořenovou funkcionalitu platebního systému, která probíhá skrze webovou aplikaci (Obr. 30).



Obr. 30. Model případů užití – Backoffice

9.3.7 Scénáře k případům užití

Tab. 7. Scénář k případu užití – Vytvoření uživatele

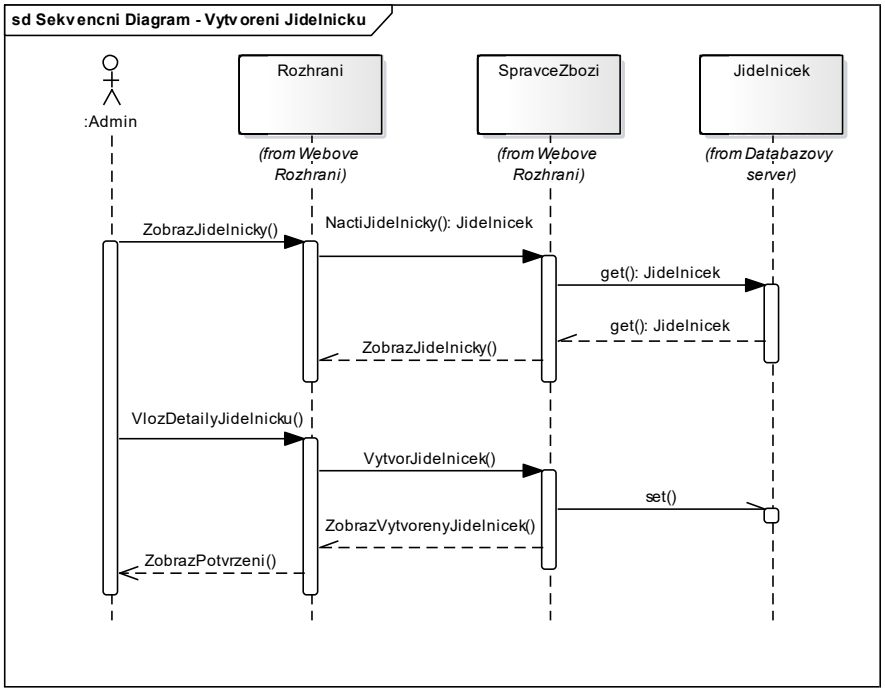
Krok	Role	Akce
1	Aktér	případ užití je zahájen stisknutím tlačítka pro přidání nového uživatele
2	Systém	zobrazí formulář pro vytvoření uživatele
3	Aktér	vloží detaily uživatele
4	Systém	ověří vložené údaje
6	Systém	zobrazí formulář pro nastavení úrovně oprávnění
7	Aktér	vybere oprávnění
8	Systém	zobrazí formulář pro nastavení omezení
9	Aktér	vybere oprávnění
10	Systém	vytvoří nového uživatele

Tab. 8. Scénář k případu užití – Vytvoření jídelníčku

Krok	Role	Akce
1	Aktér	zvolí záložku výdejen
2	Systém	zobrazí všechny vytvořené výdejny
3	Aktér	zvolí výdejnu
4	Systém	zobrazí detaily výdejny
5	Aktér	zvolí editaci jídelníčků výdejny
6	Systém	zobrazí jídelníčky spolu s formulářem pro vytvoření nového jídelníčku

Krok	Role	Akce
7	Aktér	vyplní detaily jídelníčku spolu s jeho omezeními a závislostmi
9	Systém	zkontroluje vložené údaje
10	Systém	zobrazí potvrzovací formulář
11	Aktér	potvrdí přidání jídelníčku

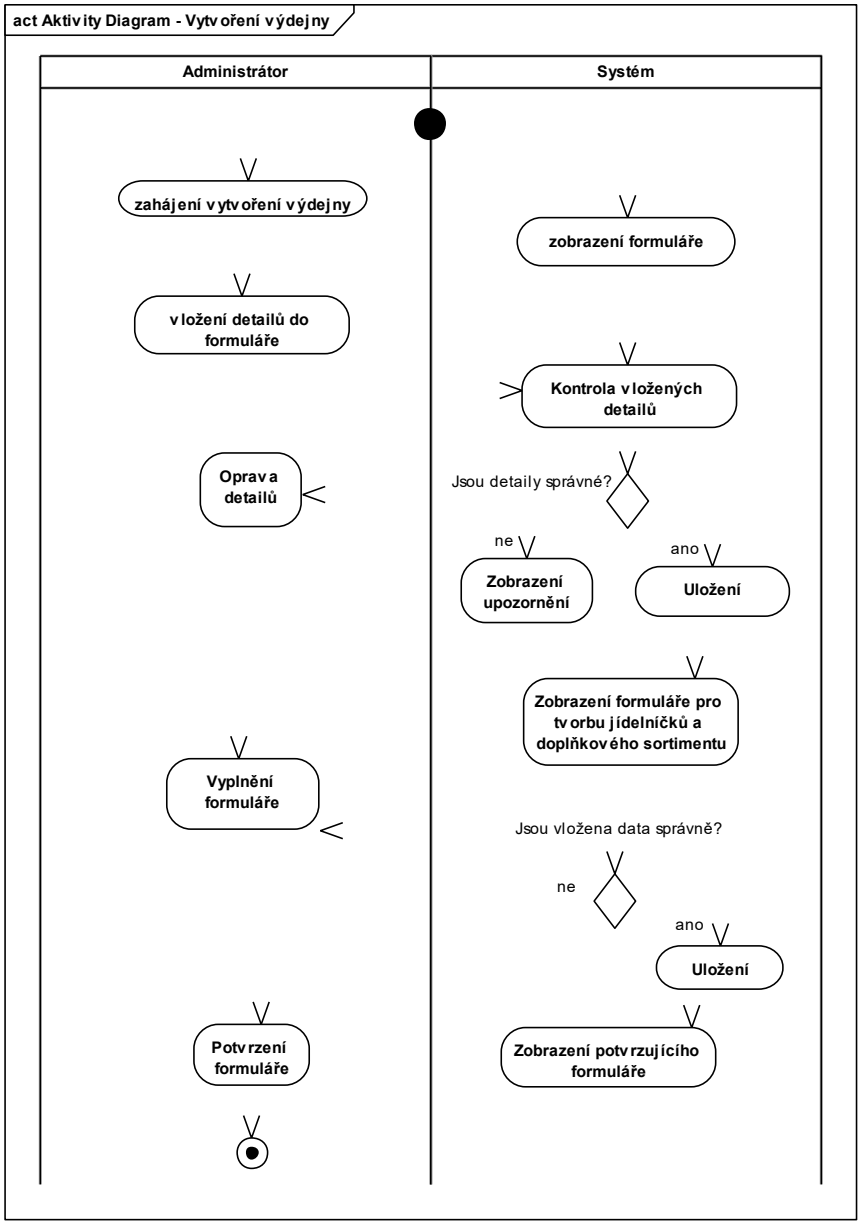
9.3.8 Sekvenční diagram případu užití – Vytvoření Jídelníčku



Obr. 31. Sekvenční diagram případu užití – Vytvoření Jídelníčku

Sekvenční diagram (Obr. 31) vychází z diagramu tříd webového rozhraní (Obr. 27). Aktér v tomto případě Administrátor zvolí v rozhraní systému záložku jídelníčky. Instance třídy SpravceZbozi obsahuje metodu NajdiJidelnicky, která vrací seznam dostupných jídelníčků. Rozhraní systému zobrazí tento seznam aktérovi spolu s formulářem pro vytvoření nového jídelníčku. Aktér vloží detaily jídelníčku do zobrazeného formuláře na rozhraní systému. Tyto detaily zpracuje třída SpravceZbozi.

9.3.9 Diagram aktivit – Vytvoření výdejny

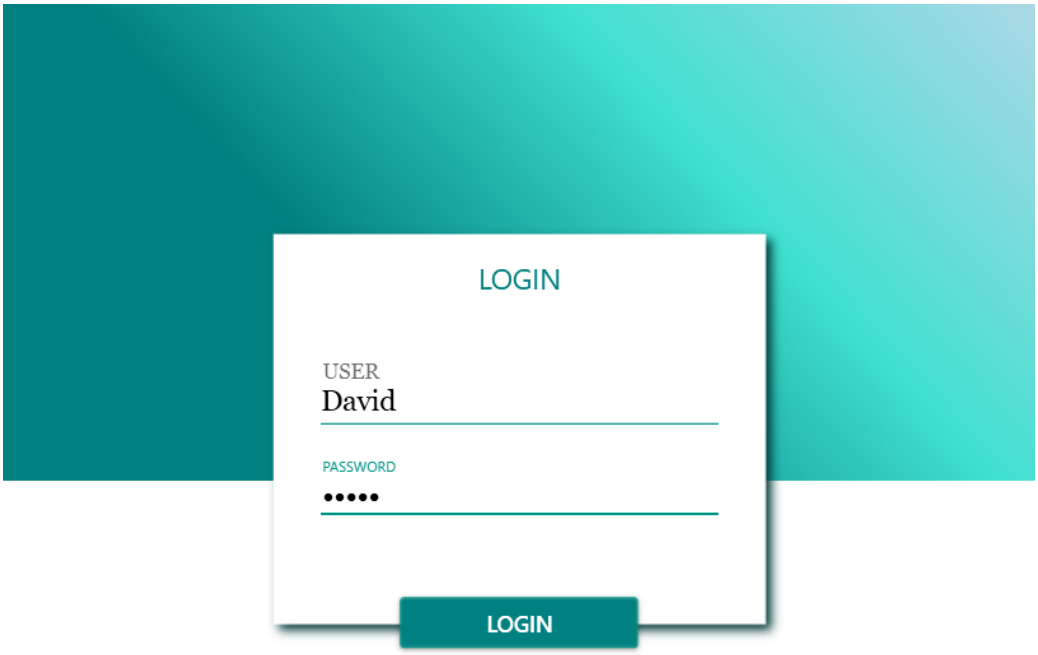


Obr. 32. Aktivitní diagram – Vytvoření nové výdejny

Diagram aktivit (Obr. 32) popisuje interakci systému s administrátorem během vytváření nové výdejny. Administrátor se musí nejprve přihlásit k webovému rozhraní platebního systému. Poté může teprve přejít do záložky výdejen a zde zahájit vytvoření výdejny kliknutím na patřičné tlačítko. V průběhu tvorby nové výdejny se nejprve vkládají detailní údaje o výdejně: název, umístění, možné počty a rozložení jídelních stolů a další. V dalším kroku dochází k nastavení jídelníčků a doplňkového sortimentu, který bude výdejna nabízet.

10 UKÁZKA NAVRŽENÉHO SOFTWARE

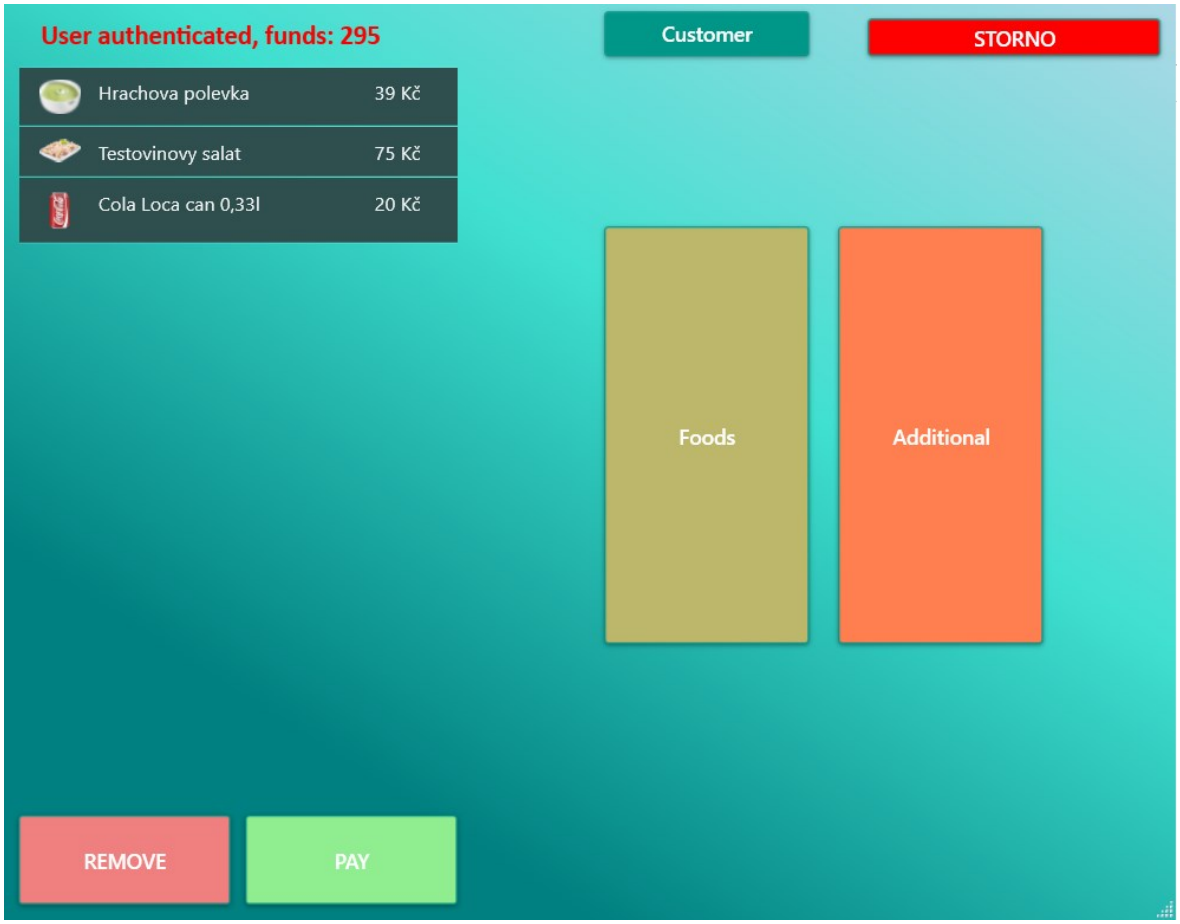
V rámci řešení diplomové práce vznikla praktická ukázka aplikace podle navržených softwarových funkcionalit. Při návrhu se vycházelo z funkcionalit pro prostředí jídelny, výsledkem je tedy desktopová aplikace platební pokladny.



Obr. 33. Praktická ukázka – Přihlašovací formulář

Přihlašovací formulář se skládá z komponenty textbox a slouží pro vložení uživatelského jména. Dále je zde komponenta PasswordBox, do které uživatel vloží své přihlašovací heslo, vložené údaje jsou cenzurovány a znaky jsou vizuálně nahrazeny za hvězdičky. Stisknutím přihlašovacího tlačítka login dojde k ověření vložených údajů vůči databázovému serveru.

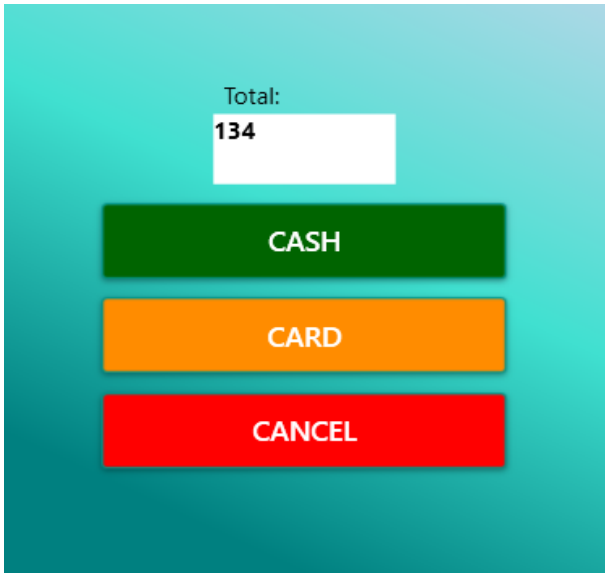
V případě úspěšného přihlášení dojde k otevření nového hlavního okna (Obr. 34). Hlavní okno poskytuje funkcionality pokladny. V levé části se nachází seznam zboží, které pokladní zvolil. V pravé části jsou dvě hlavní tlačítka, první zobrazí tabulku jídel, které jsou v databázi, druhé tlačítko zobrazí doplňkový sortiment.



Obr. 34. Praktická ukázka – Hlavní okno pokladny

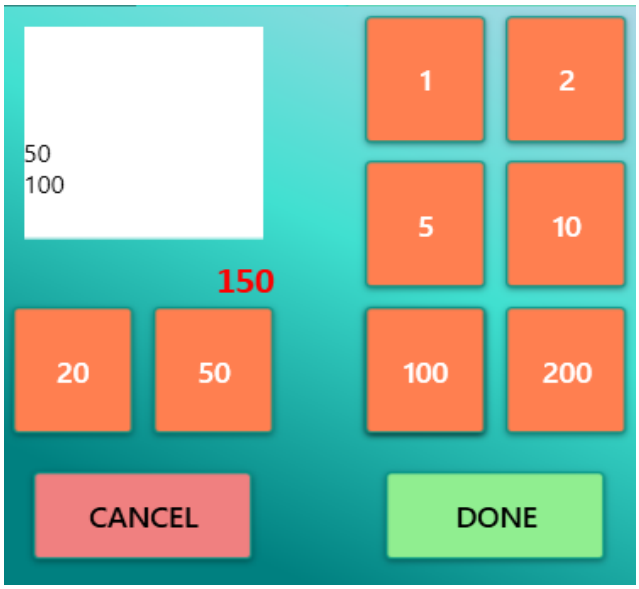
Seznam dalších komponent a jejich funkčnost:

- Tlačítko REMOVE – odstraní vybrané zboží ze seznamu
- Tlačítko PAY – zobrazí platební formulář (Obr. 35)
- Tlačítko CUSTOMER – zobrazí zákaznický formulář (Obr. 36)
- Tlačítko STORNO – zruší celou objednávku a smaže seznam zvoleného zboží
- Label – zobrazující se v případě, že zákazník provede ověření RFID kartou. Label také zobrazuje aktuální zůstatek na účtu uživatele.



Obr. 35. Praktická ukázka – Platební formulář

Platební formulář (Obr. 35) obsahuje komponentu textbox, která zobrazuje celkovou hodnotu nákupu. Tlačítko CASH je vždy aktivní a představuje platbu hotovostí. Tlačítko CARD, je aktivní v případě, že se jedná o ověřeného zákazníka a tento zákazník má dostatečný kredit. Tlačítko CANCEL ruší platbu.



Obr. 36. Praktická ukázka – Zákaznický formulář

Obrázek (Obr. 36) ukazuje formulář, který se zobrazí po stisknutí tlačítka CUSTOMER na hlavním okně aplikace. Tento formulář se skládá z několika komponent, kde převážnou většinu tvoří jednoduchá tlačítka pro nastavení zvolené částky. Další komponentou je textbox, který ukazuje historii navolených částek. Nabití kreditu autorizovanému uživateli probíhá až ve chvíli potvrzení tohoto dialogu.

ZÁVĚR

Tato diplomová práce se opírá o smluvní výzkum mezi školou a společností COMINFO, a.s. a nepřímo z něj vychází. Cíl této práce představuje návrh nového inovativního řešení software autonomního platebního systému využívajícího identifikaci založenou na technologii RFID. Tento návrh vychází ze základních funkčních požadavků, které byly zadány v rámci smluvního výzkumu a to přímo zákazníkem. Navržený software lze používat jak samostatně tak i také v kombinaci s dalšími moduly. Vzniklý návrh platebního systému si lze tedy představit jako kompaktní modul. Při kombinaci s dalšími moduly, lze tento platební systém používat v rozličném množství prostředí (restaurace, jídelny, fitness, aquaparky atd.).

Návrh vytvořený v rámci této práce zachycuje základní a důležitou kostru platebního systému obsahující nejdůležitější funkcionality systému, které jsou nadále rozšířeny doplňujícími funkcionalitami, na které je kladen důraz ze zadání smluvního výzkumu. Součástí řešení této diplomové práce je i praktická ukázka, jak by mohl vypadat software využívající navržených softwarových funkcionalit.

Současné řešení, které poskytuje společnost COMINFO nemusí v budoucnu dosahovat dostatečné úrovně konkurence schopnosti. Jelikož z průzkumu veřejně dostupných zdrojů vyplývá, že na našem trhu existuje hned několik dalších firem, které nabízí téměř stejné služby. Zároveň také tyto firmy nabízí jak softwarové tak i vlastní hardwarové řešení. Pokud společnost COMINFO začne používat nové řešení, zvýší tím svoji konkurence schopnost.

SEZNAM POUŽITÉ LITERATURY

[1] B. Manish, M. Shahram, RFID Field Guide: Deploying Radio Frequency Identification Systems, Prentice Hall PTR, 2005

[2] Smart label helping beat counterfeiters. The Star [online]. 27.9.2017 [cit. 2019-04-22]. Dostupné z: https://www.thestar.com.my/business/business-news/2017/11/27/smart-label-helping-beat-counterfeiters/

[3] Kohn LT, Corrigan J, Donaldson MS. Sumter, South Carolina: Natl Academy Pr; 2000. To err is human: Building a safer health system; p. 6.

[4] SCHWARTZ, John. Researchers See Privacy Pitfalls in No-Swipe Credit Cards. NYtimes [online]. 2006 [cit. 2018-11-29]. Dostupné z: http://www.nytimes.com/2006/10/23/business/23card.html?pagewanted=1&_r=1

[5] RFDump. Freshmeat [online]. [cit. 2018-11-29]. Dostupné z: http://freshmeat.sourceforge.net/projects/rfdump/?branch_id=61265&release_id=264928

[6] GRUNWALD, Lukas. DOS attack on RFID systems. Blackhat [online]. [cit. 2018-11-29]. Dostupné z: https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Grunwald.pdf

[7] RFID virus [online]. [cit. 2018-11-29]. Dostupné z: http://www.rfidvirus.org/

[8] *Transparent user authentication: biometrics, RFID and behavioural profiling*. New York: Springer, 2011. Best practices (Redmond, Wash.). ISBN 978-0-85729-805-8.

[9] *RFID SECURITY* [online]. In: . 2008, s. 37 [cit. 2019-05-11]. Dostupné z: https://www.infosec.gov.hk/english/technical/files/rfid.pdf

[10] YAN, Lu. *The Internet of things: from RFID to the next-generation pervasive networked systems*. New York: Auerbach Publications, c2008. Wireless networks and mobile communications series. ISBN 9781420052817.

[11] MasterCard Worldwide, Multinational financial corporation, http://www.mastercard.com, 2009

[12] *Platební služby: biometrics, RFID and behavioural profiling*. Praha: Management Press, 2012. Best practices (Redmond, Wash.). ISBN 9788072612383.

[13] VAN DEN BREEKEL, Jordi, Erik POLL a Joeri DE RUITER. *EMV in a nutshell* [online]. In: . 2016, s. 37 [cit. 2019-05-11]. Dostupné z: https://www.cs.ru.nl/E.Poll/papers/EMVtechreport.pdf

[14] Strengthening Card Authentication: a migration to DDA. *Smartpaymentassociation*. 2015, , 19.

[15] *EMV Cardholder Verification Methods* [online]. In: . 2010 [cit. 2019-05-11]. Dostupné z: https://www.level2kernel.com/blog/index.html%3Fp=47.html

[16] "What is a Payment System?" (PDF). Federal Reserve Bank of New York. October 13, 2000.

[17] *Software project survival guide*. Redmond, Wash: Microsoft Press, c1998, s. 114. ISBN 1-57231-621-7.

[18] *More about software requirements: thorny issues and practical advice*. Redmond, WA: Microsoft Press, c2006, s. 4. Best practices (Redmond, Wash.). ISBN 978-0-7356-2267-8.

[19] KANISOVÁ, Hana a Miroslav MÜLLER. *UML srozumitelně*. Brno: Computer Press, 2004. ISBN 80-251-0231-9.

[20] *More about software requirements: thorny issues and practical advice*. Redmond, WA: Microsoft Press, c2006, s. 85. Best practices (Redmond, Wash.). ISBN 978-0-7356-2267-8.

[21] *KASAFIK* [online]. [cit. 2019-04-20]. Dostupné z: https://www.kasafik.cz

[22] Pay-Pass [online]. Frajt s.r.o. [cit. 2019-04-20]. Dostupné z: http://www.frajt.cz/turnikety/pay-per-pass/

[23] KOS-D3 [online]. Ikos s.r.o. [cit. 2019-04-20]. Dostupné z: https://www.ikos.cz/category/6/software-ikos-d3-zakladni-informace

[24] EPOS [online]. HASAM [cit. 2019-04-20]. Dostupné z: http://www.hasam.cz/Produkty/EPOS

[25] HARTMAN, Annie. Paying With a Credit Card Makes You Spend More Money [online]. 27. 7. 2018 [cit. 2019-04-12]. Dostupné z: https://curiosity.com/topics/paying-with-a-credit-card-makes-you-spend-more-money-curiosity/

[26] PRITCHARD, JUSTIN. Get to Know the Parts of a Debit or Credit Card. In: Thebalance [online]. 20.1.2019 [cit. 2019-04-12]. Dostupné z: https://www.thebalance.com/parts-of-a-debit-or-credit-card-front-and-back-315489

[27] TENDER RETAIL TEAM, ACCEO. Mobile payment types available today. In: ACCEO Tender Retail [online]. 2017, 6.6.2017 [cit. 2019-04-14]. Dostupné z: https://tender-retail.acceo.com/blog/mobile-payment-types-available-today/

[28] MOURDOUKOUTAS, Panos. Samsung Beats Apple In The Global Smartphone Market As Chinese Brands Close In. Forbes[online]. 2018, 13.9.2018 [cit. 2019-04-13]. Dostupné z: https://www.forbes.com/sites/panosmourdoukoutas/2018/09/13/samsung-beats-apple-in-the-global-smartphone-market-as-chinese-brands-close-in/

[29] India. World Bank [online]. 2019 [cit. 2019-04-14]. Dostupné z: https://data.worldbank.org/country/india

[30] KAUL, Vidur. Sound Wave Technology: Revolutionizing payments and targeted marketing in retail. Happiest Minds [online]. 19.4.2017 [cit. 2019-04-14]. Dostupné z: https://www.happiestminds.com/blogs/how-sound-wave-technology-is-revolutionizing-payments-and-targeted-marketing-in-retail/

[31] THAKKAR, Danny. Biometric Payment is the Future of Retail Industry. *Bayometric* [online]. 2018 [cit. 2019-05-11]. Dostupné z: https://www.bayometric.com/biometric-payment-future-retail-industry/

[32] Fingerprinting. In: University of Colorado Boulder [online]. [cit. 2019-04-14]. Dostupné z: https://www.colorado.edu/police/records-reports/fingerprinting

[33] GREENHOUSE, Steven. Shoplifters? Studies Say Keep an Eye on Workers. The New York Times [online]. 2009, 29.9.2009, 2009[cit. 2019-04-14]. Dostupné z: https://www.nytimes.com/2009/12/30/business/30theft.html

[34] Creating Smarter Stores with Facial Recognition. *Viatech* [online]. 2018 [cit. 2019-05-11]. Dostupné z: https://www.viatech.com/en/2018/08/facial-recognition-smarter-stores/

[35] MAGRATH, MICHAEL. Biometric Facial Recognition Software: Massive Gains in Accuracy, But Challenges Remain. One Span[online]. 19.9.2018, 2019 [cit. 2019-04-14]. Dostupné z: https://www.onespan.com/blog/biometric-facial-recognition-software

[36] THAKKAR, DANNY. Retinal vs. Iris Recognition: Did You Know Your Eyes Can Get You Identified?. Bayometric [online]. [cit. 2019-04-14]. Dostupné z: https://www.bayometric.com/retinal-vs-iris-recognition/

[37] KASSNER, Michael. Vocal disguises and impersonations may fool voice recognition authentication. *Techrepublic* [online]. 2018 [cit. 2019-05-11]. Dostupné z: https://www.techrepublic.com/article/vocal-disguises-and-impersonations-may-fool-voice-recognition-authentication/

[38] Stravovací systém CARDPAY. DataExpert [online]. [cit. 2019-04-18]. Dostupné z: http://www.dataexpert.cz/cs/stravovaci-system-cardpay

[39] COMINFO a.s. CARDPAY. In: Docplayer [online]. [cit. 2019-04-18]. Dostupné z: https://docplayer.cz/3769591-I-nfos-www-cominfo-cz.html

[40] LINHART, Ondřej. 5 hlavních důvodů, proč nepoužívat visual basic 6.0. DotNET portal [online]. 2011, 28.4.2011 [cit. 2019-04-18]. Dostupné z: https://www.dotnet-portal.cz/blogy/9/Ondrej-Linhart/877/5-hlavnich-duvodu-proc-nepouzivat-Visual-Basic-6-0

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

RFID Radio Frequency Identification

DOS Denial of service

SQL Structured Query Language

PIN Personal identification number

EMV Europay, MasterCard, Visa

NFC Near Field Communication

GDPR General Data Protection Regulation

SEZNAM OBRÁZKŮ

Obr. 1. Základní schéma komunikace 12
Obr. 2. Vzhled RFID čipu 14
Obr. 3. Mezinárodní symbol pro bezkontaktní platby [11] 21
Obr. 4. Cyklus platby kreditní kartou 22
Obr. 5. Průběh nákupu v rámci lokálního platebního systému 26
Obr. 6. Ukázkový příklad modelu případů užití 29
Obr. 7. Ukázkový příklad sekvenčního diagramu 30
Obr. 8. Logo společnosti KASA FIK 31
Obr. 9. Logo společnosti Frajt s.r.o. 32
Obr. 10. Logo společnosti Ikos s.r.o. 33
Obr. 11. Logo firmy HASAM s.r.o. 34
Obr. 12. Schéma platební karty [26] 35
Obr. 13. Mobilní platby [27] 36
Obr. 14. Vzorek otisku prstu [32] 38
Obr. 15. Obličejové rozpoznávání [35] 40
Obr. 16. Rozpoznání sítnice [36] 41
Obr. 17. Možnosti použití modulu INFOS CARDPAY [39] 43
Obr. 18. Aktéři platebního systému 52
Obr. 19. Základní nefunkční požadavky 52
Obr. 20. Základní funkční požadavky 53
Obr. 21. Model případů užití – jídelna 55
Obr. 22. Sekvenční diagram případu užití – Zaplacení 56
Obr. 23. Diagram tříd – komunikace server - rozhraní 57
Obr. 24. Aktivitní diagram – zaplacení 58
Obr. 25. Model případů užití – webové rozhraní 59
Obr. 26. Sekvenční diagram případu užití – Vytvoření Objednávky 61
Obr. 27. Diagram tříd – webové rozhraní 61
Obr. 28. Aktivitní diagram – Vytvoření objednávky 62
Obr. 29. Aktivitní diagram – Přijetí objednávky 63
Obr. 30. Model případů užití – Backoffice 64
Obr. 31. Sekvenční diagram případu užití – Vytvoření Jídelníčku 65
Obr. 32. Aktivitní diagram – Vytvoření nové výdejny 66

Obr. 33. Praktická ukázka – Přihlašovací formulář 67
Obr. 34. Praktická ukázka – Hlavní okno pokladny 68
Obr. 35. Praktická ukázka – Platební formulář 69
Obr. 36. Praktická ukázka – Zákaznický formulář 69

SEZNAM TABULEK

Tab. 1. Softwarové funkcionality lokálního platebního systému 47
Tab. 2. Primární scénář případu užití – Zaplacení 55
Tab. 3. Alternativní scénář případu užití – Zaplacení 56
Tab. 4. Scénář případu užití - Přihlášení 60
Tab. 5. Scénář případu užití – Vytvoření objednávky 60
Tab. 6. Scénář případu užití – Úprava objednávky 60
Tab. 7. Scénář k případu užití – Vytvoření uživatele 64
Tab. 8. Scénář k případu užití – Vytvoření jídelníčku 64

SEZNAM PŘÍLOH

P I CD (Obsahující adresář se zdrojovými kódy a databází, ve které se nachází data potřebná pro testování.)