Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra ekonomie

Moderní elektronické platební nástroje

Bakalářská práce

Autor: Petr Jaroš
Studijní obor: Informační management

Vedoucí práce: Ing. Ivan Soukal, Ph.D.

Hradec Králové duben 2015

Prohlášení:

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

V Hradci Králové dne 28.4.2015 Petr Jaroš

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Ivanu Soukalovi, Ph.D., za cenné rady, připomínky a metodické vedení práce.

Anotace

Tato bakalářská práce se zabývá moderními elektronickými platebními nástroji. V úvodu práce jsou představeny základní pojmy z oblasti elektronických plateb. Další část se věnuje popisu a rozdělení platebních karet. Z hlediska ochrany plateb se práce zaměřuje na prvky a protokoly, které se využívají v elektronických platebních systémech. V praktické části je zpracován přehled používaných platebních systémů na trhu včetně aktuálních trendů. Vybrané platební systémy jsou modelovány prostřednictvím BPMN jazyka a rozebrány podle funkčnosti a bezpečnosti. Při rozboru systémů je kladen důraz na procesy spojené s registrací, platbou a bezpečností. Závěr práce obsahuje zhodnocení daných systémů a naznačuje možná zlepšení v řešených procesech.

Annotation

Title: Modern electronic payment instruments

This bachelor thesis deals with modern electronic payment instruments. The introduction presents the basic concepts of electronic payments. Another part describes the distribution of payment cards. In terms of payments, the thesis focuses on the elements and protocols that are used in electronic payment systems. The practical part contains an overview of the payment systems on the market, including current trends. Selected payment systems are modelled through BPMN language and analysed by function and safety. When analysing systems, emphasis is placed on processes associated with registration, payment and security. Conclusion includes the assessment of the systems and suggests possible improvements to practical processes.

Obsah

Úvod

Cílem této bakalářské práce je zpracovat přehled a vývoj v oblasti elektronických plateb včetně aktuálně nabízených trendů s využitím modelování metodou Business Process Modeling (BPM). V dnešní době začíná být platba hotovostí na ústupu, protože jsou stále častěji upřednostňovány elektronické platební nástroje. Člověk denně tyto platební nástroje využívá, ale nemusí však tušit, jakým způsobem fungují. Práce by měla vymezit důležité pojmy v oblasti elektronického platebního styku a zhodnotit funkčnost a bezpečnost jednotlivých nástrojů na trhu.

V první kapitole jsou s využitím odborné literatury a webových zdrojů popsány základní pojmy z oblasti elektronického platebního styku, které se vyskytují v oblasti platebních systémů. V úvodu kapitoly je vymezeno rozdělení platebního styku podle jednotlivých hledisek a základních forem. Další podkapitola patří popisu platební karty, protože je významným prvkem v elektronických platbách. Platební karta je opět rozdělena podle různých technických hledisek. Závěr kapitoly je věnován bankovním systémům.

Druhá kapitola se zaměřuje s využitím odborné literatury a webových zdrojů na bezpečnostní protokoly a prvky, které zabezpečují platby v elektronických platebních systémech. Následně jsou uvedeny druhy autentizačních a autorizačních metod, které probíhají při platbě s aktuálními systémy. Velká část kapitoly se věnuje vývoji bezpečnostních protokolů. Druhou kapitolu uzavírá vysvětlení jazyka BPMN.

V třetí kapitole jsou s použitím odborné literatury, osobních zkušeností a dostupných webových zdrojů vysvětleny vybrané druhy elektronických platebních systémů, které jsou v dnešní době nejčastěji zastoupeny na trhu.

V poslední kapitole jsou s využitím dostupných webových zdrojů a osobních zkušeností prakticky zpracovány konkrétní druhy platebních systémů na trhu. U jednotlivých systémů je zmíněna historie a charakteristické vlastnosti, které

vybrané systémy od sebe odlišují. Při rozboru je kladen důraz na procesy spojené s registrací, bezpečností a platbou. V závěru kapitoly se nachází shrnutí zjištěných informací včetně návrhů zlepšení.

1 Platební systémy

V této kapitole je popsána teorie, která se vztahuje k základním pojmům v oblasti platebních systémů a elektronických plateb. Důležitou částí je popis platební karty, která je základem funkčnosti většiny elektronických platebních systémů.

1.1 Funkce peněz

V současnosti můžeme peníze definovat jako jakékoli aktivum, které je všeobecně uznáváno a přijímáno jako prostředek směny (tedy při platbě za zboží, služby, aj.). Z makroekonomického hlediska plní peníze 3 základní funkce (Pavelka, 2007):

- Prostředek směny – peníze slouží ke směně služeb a statků. Produkt se nemusí vyměnit za jiný (např. vejce za mléko), ale prodávající má možnost potřebný produkt směnit za peníze. Aby se staly peníze univerzálním platidlem, musely být přijímány všemi účastníky směny jako prostředek směny zboží a služeb.
- Zúčtovací jednotka – v penězích vyjadřujeme ceny statků a služeb, a to jak cen současných, tak i minulých a budoucích.
- Uchovatel hodnoty – peníze pomáhají lidem udržovat bohatství. Výhodou bohatství v této formě je to, že peníze jsou likvidní. Tedy mohou být téměř ihned použity k nákupu statků či služeb. Peníze umožňují určit hodnotu různých druhů statků a nastavit poměr směny mezi nimi (Juřík, 2003).

1.2 Platební styk

Platební styk je velice široký pojem, ale dá se definovat podle Schlossbergera, jako *peněžní vztah mezi plátcem a příjemcem, který je uskutečňován v určitých formách dohodnutými platebními instrumenty buď přímo mezi nimi, nebo prostřednictvím k tomu určených subjektů (např. bank nebo spořitelních a úvěrních družstev)* (2012, 11). Ve vztahu vystupuje na jedné straně jako zprostředkovatel především banka, spořitelní nebo uvěrová družstva a na druhé straně vystupují fyzické a právnické osoby v roli klientů těchto zprostředkovatelů. Mezi těmito subjekty poté probíhají operace platebního styku vybranými platebními nástroji. V České republice podléhá platební styk hlavní právní úpravě a tím je zákon č. 284/2009 Sb., o platebním styku (Schlossberger, 2012).

Základní rozdělení platebního styku realizovaným mezi jmenovanými subjekty můžeme dělit na hotovostní a bezhotovostní platební styk. Platební styk se dále dělí na další možná kritéria. Rozdělení platebního styku:

1) Podle typu platby:

- Hotovostní platební styk – mezi subjekty platebního styku dochází k přesunu množství peněz formou bankovek a mincí, např. restaurace.
- Bezhotovostní platební styk – prostřednictvím poskytovatelů platebních služeb dochází k přesunu peněz mezi bankovním účtem plátce a příjemce.
- Elektronický platební styk – peníze jsou uloženy v elektronické formě a peněžní přesun mezi plátcem a příjemcem probíhá odečtením peněz z elektronického nosiče odesílatele a připsáním těchto peněz příjemci.

2) Podle území:

- Vnitrostátní platební styk – poskytovatel platebních služeb plátce a příjemce se vyskytuje na stejném území.
- Přeshraniční platební styk – poskytovatel platebních služeb plátce a příjemce se vyskytuje na území Evropského hospodářského prostoru.
- Zahraniční platební styk – poskytovatel platebních služeb plátce a příjemce se vyskytuje v různých státech s výjimkou Evropského hospodářského prostoru.

3) Podle průvodních dokumentů:

- Dokumentární platební styk – mezi plátcem a příjemcem jsou při přesunu peněz potřebné dokumenty doprovázející transakci.
- Nedokumentární platební styk – tzv. hladké platby, mezi plátcem a příjemcem nejsou při přesunu peněz zapotřebí průvodní dokumenty.

4) Podle doby realizace:

- Expresní platební styk – poskytovatel bankovních služeb okamžitě odepíše peníze z bankovního účtu plátce a poskytovatel bankovních služeb příjemce peníze na účet připíše.
- Standartní platební styk – běžný přesun peněz mezi plátcem a příjemcem za předem stanovených podmínek.

5) Podle zapojení banky v transakci:

- Závazkový platební styk – dohoda mezi plátcem a příjemcem, že finanční instituce (banka) má možnost vstoupit do závazku, ale dostává povinnosti plátce.
- Bezzávazkový platební styk – poskytovatel platebních služeb vystupuje jako pouhý zprostředkovatel transakce (Schlossberger, 2012). V tomto vztahu nemá k transakci právní vztah.

6) V rámci bezhotovostního styku se dělí podle počtu zapojení bank:

- Vnitrobankovní platební styk – platební transakce je pouze mezi plátcem a příjemcem jedné banky.
- Mezibankovní platební styk – platební transakce mezi plátcem a příjemcem různých bank (Máče, 2006).

1.2.1 Hotovostní platby

Hotovostní platby jsou druhem platebního styku z hlediska způsobu placení. Platební styk se realizuje pomocí hotových peněz, respektive využitím mincí nebo bankovek. Bankovky jsou peníze papírového charakteru vydávané centrální bankou a naopak mince jsou kovového charakteru s obvykle nižší nominální hodnotou (Máče, 2006).

Využití hotovostních plateb se upřednostňuje při placení malého peněžního obnosu jako například trafiky, restaurace a další možnosti, kde probíhá platební styk bez poskytovatele platebních služeb mezi fyzickými osobami nebo také firmami. Do průběhu hotovostního platebního styku zasahuje různým postavením zákazník, obchodník, komerční banka a také centrální banka (Máče, 2006).

Jedním z účastníků je zákazník. Zákazník se nejčastěji dostane ke kontaktu s hotovostí, když vybírá peníze platební kartou prostřednictvím elektronického platebního prostředku, respektive bankomatu. Druhou možností, jak se dostat do kontaktu s hotovostí, je využitím klasického výběru u bankovních přepážek. Zákazníci, ale mohou své peníze také spořit, proto ukládají hotovosti na účty bankovních nebo jiných institucí. Zákazníci následně dávají vybrané peníze do oběhu platebními transakcemi za zboží nebo služby. Tyto peníze v platebním styku přijímá obchodník (Máče, 2006).

Dalším účastníkem s hotovostí jsou komerční banky, které dostávají peníze od občanů, podnikatelů nebo právnických osob. Komerční banka tyto získané peníze využívají pro další potřeby svých klientů. Příkladem může být poskytnutí úvěrů. Přebytečný finanční objem banky odvede centrální bance. Centrální banka dále přijaté peníze rozděluje a podle zákona neupotřebitelné peníze odstraní. Podobně probíhá posílání nových peněz do oběhu (Máče, 2006).

Bankovní instituce nabízejí klientům různé druhy hotovostních plateb. Jedna z možných forem je složení hotovosti ve prospěch účtu příjemce. Tato forma se realizuje pomocí pokladních složenek nebo na pokladnách bank. Další formou je šek, který slouží k vyplacení peněz. Forma výběrného lístku využívá při výběru peněz kontroly podpisu podle podpisového vzoru k účtu. Důležitou formu v oblasti platebních karet je výběr hotovosti z bankomatů (Máče, 2006).

1.2.2 Bezhotovostní platby

Bezhotovostní platební styk je další možnou variantou při výběru způsobu platby. Z názvu vyplívá, že se jedná o formu platebního styku, kde není vyžadována hotovost a to je také základní informace pro elektronické platební systémy. V úvodním rozdělení je již zmíněné, že bezhotovostní platební styk probíhá mezi plátcem a příjemcem pomocí poskytovatele platebních služeb, respektive zprostředkovatele (banky). Bezhotovostní platby se uskutečňují podle území vnitrostátně, tak také může být platba přeshraniční nebo zahraniční. Přesunutím požadovaných peněz mezi plátcem a příjemcem je podmíněno danými platebními příkazy a tento bezhotovostní platební styk není doprovázen průvodními dokumenty. Z hlediska zapojení banky do platební transakce se jedná o bezzávazkový styk, tzv. hladké platby. Varianta, která nepatří přímo do obou rozdělení, je spojení hotovostních a bezhotovostních plateb.

Mezi platební nástroje (příkazy) bezhotovostních plateb v dnešní době řadíme: Příkaz k úhradě, Příkaz k inkasu, Platební příkaz pro zahraniční platební styk, Platební příkaz pro přeshraniční styk, Šek a Platební kartu (Schlossberger, 2012).

- **Příkaz k úhradě** – jedná se o základní nástroj hladkých plateb, který je rychle vyhotovený, protože platba se uskutečňuje jednosměrně. Příkaz k úhradě je založený na tom, že plátce předá pokyn bance, aby požadovaný peněžní obnos převedla na bankovní účet příjemce. Tento druh nástroje se hojně využívá při bezhotovostním platebním styku (Černohorský, 2011).

  Při přesunu peněz se do procesu zapojuje plátce a příjemce a jejich bankovní účty u jednotlivých bank. Pokyn bance je možné podat přes standartní předepsané bankovní formuláře nebo v dnešní době přes často využívané elektronické bankovnictví. Příkaz k úhradě se dělí na další dva typy – trvalý příkaz k úhradě a hromadný příkaz k úhradě. Trvalý příkaz usnadňuje práci bance, protože slouží k zpracování opakujících se plateb. Využití má především, pokud se příjemce pravidelně opakuje. Hromadný příkaz k úhradě se využívá

při pokynu plátce převézt různé finanční obnosy na různé bankovní účty příjemců. (Máče, 2006).

- **Příkaz k inkasu** – jedná se o další nástroj hladkých plateb. Rozdíl mezi příkazem k úhradě a příkazem k inkasu je hlavně z hlediska podnětu k placení, protože při využití příkazu k úhradě předává pokyn plátce, ale naopak u inkasa dává podnět příjemce platby. Příkaz k inkasu je založený na tom, že příjemce předá pokyn bance (zprostředkovateli), aby provedla převod požadovaného finančního obnosu na účet zadavatele inkasního příkazu, zatížením tímto finančním obnosem bankovní účet plátce. Aby při inkasním příkazu nedocházelo k zneužití, vznikají mezi plátcem a příjemcem uzavřené dohody, které banka před zpracováním příkazu zkontroluje. To znamená, že plátce souhlasí s příkazem k inkasu (Černohorský, 2011).

  Při přesunu peněz se do procesu zapojuje plátce jako dlužník a příjemce jako zadavatel inkasního příkazu a jejich bankovní účty u jednotlivých bank. Pokyn k provedení tohoto příkazu je možné také předat pomocí standartního bankovního formuláře nebo elektronickým bankovnictvím. Příkaz k inkasu má podobně jako příkaz k úhradě další dva typy – hromadný příkaz k inkasu a trvalý příkaz k inkasu. Hlavním využitím inkasa je prostřednictvím tzv. SIPO (Sdruženém Inkasu Plateb Obyvatelstva). Jedná se o smlouvu plátce a příjemce o opakované platbě s danou pravidelností, například za elektřinu, plyn atd. (Máče, 2006).

- **Příkaz pro zahraniční platební styk** – tento platební příkaz se využívá právě tehdy, kdy nejde využít přeshraniční platební příkaz. Pokyn k přesunu peněžnímu obnosu probíhá mezi plátcem a příjemcem mimo území Evropského hospodářského prostoru (EHP). Výjimkou může být příkaz platebního styku provedený v EHP za použití jiné měny, než je stanovena zemím EHP (Schlossberger, 2012).

Platební příkaz je určen pro obchodní a také neobchodní platby. *Obchodní platby vyplívají z přímého uskutečňování obchodních transakcí, tj. z realizace obchodu, přepravy a zasílatelství. Neobchodní platby nevyplívají z přímé realizace obchodních operací. Například jde o úhrady darů, penzí, alimentů, výnosy z cenných papírů a nemovitostí atd. (Máče, 2006, 46).* Doba realizace převodu peněz do zahraničí trvá nejčastěji v rozmezí 3 až 5 dní. Uskutečnění platebního příkazu může realizovat plátce a příjemce po dohodě. Hladká platba proběhne po dodání zboží, ale je nutná důvěra všech účastníků nebo platba proběhne předem s následným odesláním zboží (Máče, 2006).

- **Příkaz pro přeshraniční platební styk** – Tento pokyn k přesunu peněžního obnosu využívá příjemce a plátce mezi státy Evropské unie (EU), tedy již zmiňovaný EHP v evropské měně (euro). V přeshraničním platebním příkazu není rozdíl mezi vnitrostátním příkazem k úhradě, či k inkasu. Podnět k příkazu k úhradě podává plátce a podnět k příkazu k inkasu podává příjemce. Proces zajišťují specializované platební systémy, které jsou detailněji popsaný v kapitole platebních systémů. Příkladem může být systém TARGET a SWIFT. Veškeré formuláře stejně jako předešlých příkazů provádět pomocí elektronického bankovnictví. (Jak funguje platební styk mezi státy Evropské unie?, Kalabis, 2012).

  U přeshraničního platebního styku je důležité zmínit pojem SEPA. Jedná se o projekt podnícený Evropskou komisí a Evropskou centrální bankou. Projekt SEPA (Single Euro Payments Area) se zaměřuje na vytvoření jednotné oblasti pro platby v eurech. Důvodem realizace projektu SEPA je sjednotit platební styk států EU, aby plátci a příjemci při platebních transakcích v eurech nemuseli rozlišovat vnitrostátní a přeshraniční platbu s různými podmínkami. Příjemce a plátce musí mít v SEPA zařízený bankovní účet a měna vedených účtů může být jiná, protože platební transakce probíhá ve zmiňovaných eurech. Cílem celého projektu je plně integrovat, zjednodušit, zrychlit bezhotovostní platby v eurech (Černohorský, 2011).

Obrázek 1 - logo SEPA

Zdroj: SEPA logos. In: [online]. [cit. 2015-01-20]. Dostupné na WWW: http://www.europeanpaymentscouncil.eu/index.cfm/about-sepa/sepa-logos/

- **Šek** – jedná se o cenný papír, který dává bezpodmínečný pokyn výstavcem šeku bance (šekovníkovi), aby přesunula určitý finanční obnos z bankovního účtu na účet držitele šeku (příjemce). Šek je dalším platebním nástrojem bezhotovostních plateb, který se realizuje jako platební příkaz. Tento druh se využívá k mezinárodním a vnitrostátním platebním transakcím, ale zejména v USA. Využívá se v platbách především v situacích, kdy nevíme bankovní spojení příjemce nebo není dostatečné bankovní spojení s plátcem a příjemcem. V dalším případě, pokud chceme využít platební styk diskrétně. Základním hlediskem rozdělení šeků je typ vystavitele. Šek bankovní vystavuje banka nebo jiný finanční institut a naopak šek soukromí vystavuje fyzická, či právnická osoba. Šeky mají samozřejmě další náležitosti a rozdělení, ale pro základní představu je popis dostatečný (Máče, 2006).

1.3 Platební karty

Platební karta patří mezi moderní nástroje pro bezhotovostní platební styk a je součástí elektronických plateb, proto jsou detailněji popsány její různé aspekty. Tento platební instrument souvisí s běžnými a úvěrovými bankovními účty, protože je jejich rozšířením, které se snaží zdokonalit proces šekových a hotovostních plateb. Vydavatelem platební karty jsou především banky, které dodržují pravidla mezinárodních asociací a vytvářejí podmínky vydaní. Držitelem karty je zpravidla klient dané banky.

Platební kartu můžeme charakterizovat jako platební instrument, jenž umožňuje vzdálený přístup majitele karty k peněžním prostředkům na účtu a kterým uživatel platebních služeb dává platební příkaz poskytovateli (Schlossberger, 2012). V dnešní době patří kreditní karty k mezinárodně nejvíce využívaným elektronickým platebním prostředkům a patří mezi nástroje platebních služeb (Polouček, 2013).

Platební karta se liší od jiných forem platebních prostředků, především danou normou ISO 3554. Norma platební karty tedy udává přesné instrukce, jak má tento platební prostředek vypadat. Důležité částí platební karty jsou popsány v tabulce, viz Tabulka 1. Jedná se zejména o danou velikost karty, vyznačení vydavatele karty, majitele platební karty, číslo platební karty a dobu platnosti. Dále se podle normy určuje použité medium elektronického záznamu, či bezpečnostní prvky, viz Obrázek 3 (Schlossberger, 2012).

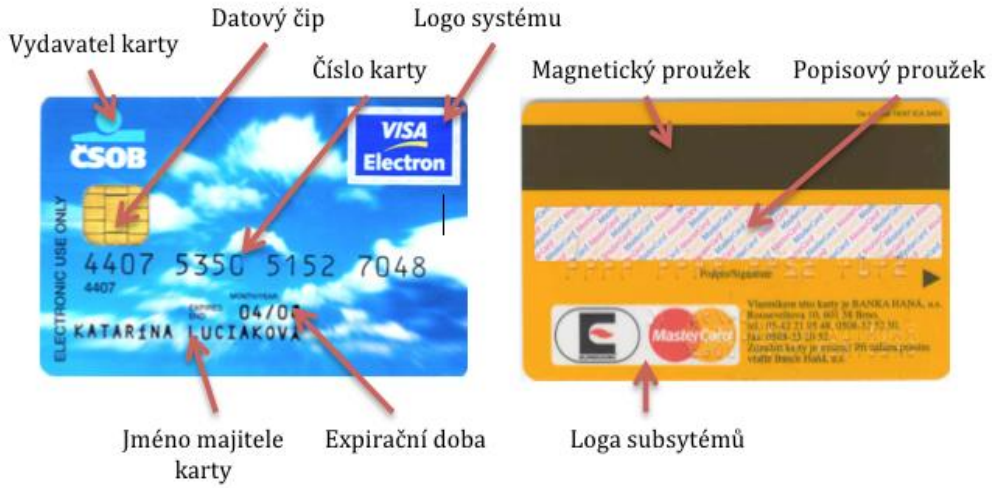
Tabulka 1 - Náležitosti platební karty

Důležité části platebních karet	
Označení vydavatele	Název a logo dané bankovní instituce
Číslo platební karty	Skládá se z 16 až 19 numerických znaků s příslušným významem (2 znaky – typ karty, 5 znaků – identifikátor vydavatele, zbytek – identifikátor držitele)
Část BIN čísla	Skládá se ze 4 znaků čísla BIN (Bank Indentification Number – číslo přidělené karetní asociace dané banky)
Expirační doba	Udává platnost platební karty – začátek a konec doby platnosti nebo jen její konec
Jméno majitele karty	Skládá se z max. 27 znaků a služebních karet, také název firmy
Elektronický záznam dat	Uložení elektronických dat danými technologiemi (magnetický proužek, …)
Podpisový proužek	Udává podpisový vzor majitele na zadní straně karty. Dále často obsahuje CVC – 3 znaky kontrolního prvku, který se využívá při internetových platbách

Zdroj: Vlastní zpracování dle (Máče, 2006)

Grafické znázornění náležitosti platebního instrumentu, se nachází, na následujícím obrázku viz Obrázek 2. Náležitosti jsou popsané v předešlé tabulce, viz Tabulka 1.

Obrázek 2 - popis platební karty



Zdroj: AUTOR NEUVEDEN [online]. [cit. 2015-01-22]. Dostupný na WWW: http://www.nenechsedojit.cz/sites/default/files/platebni_karta.png

1.3.1 Formy využití platební karty

Platební karta slouží ke spoustě platebním operacím a službám s ní spojených. Za standardně využívané formy pokládáme:

- **Výběr hotovosti z bankomatů** – forma sloužící majiteli platební karty přistupovat k hotovosti uložené na bankovním účtu, ke kterému byla karta vydána. Celý proces začíná u bankomatu identifikací držitele karty pomocí PIN (Personal Indentification Number) a následnému ověření práv provést danou platební operaci (Máče, 2006).

- **Výběr hotovosti na bankovních pobočkách** – forma sloužící majiteli platební karty přistupovat k hotovosti na pobočkách bank, směnáren nebo mezinárodních hotelích. Tato varianta je vysoce zpoplatněna a musí proběhnout ověření totožnosti. Držitelé karet volí výběr na bankovních pobočkách, pokud nelze použít bankomat nebo požadovaný finanční objem přesáhl maximální částku pro výběr z bankomatu (Máče, 2006).
- **Výběr hotovosti v obchodech** – forma sloužící majiteli platební karty přistupovat k hotovosti v obchodě, požádáním o vyplácení požadovaného finančního obnosu z účtu, společně s uhrazením zboží a služeb.

- **Bezhotovostní platby –** platba na internetu atd.

1.3.2 Průběh bezhotovostního placení

V první fázi je podmínkou, aby obchodník vlastnil elektronický platební terminál, kterým projede zákazník platební kartou přes čtečku nebo kartu zasune do zdířky terminálu. Pokud platební karta podporuje bezkontaktní platbu, zákazník kartu pouze přiloží. Obchodníkovi se na displeji zobrazí údaje potřebné pro uskutečnění platby. Příkladem může být číslo karty, doba platnosti, částka a jiné informace pro ověření. Pokud má držitel kartu elektronickou, je požádán o zadání PIN kódu. Dále jsou odeslány potřebné informace platebním terminálem do sítě platebního systému. Platební systém ze získaných informací zjistí vydavatele karty a vytvoří pro něho dotaz, jestli může být platební transakce provedena. Vydavatel karty zjistí zůstatek finančního obnosu na účtu pro zaplacení transakce, limity pro využití karty a zpětně odešle souhlas s transakcí platebnímu terminálu, použitím tzv. autorizačního kódu. Tímto krokem dostane platební terminál pokyn pro vytištění účtenky. Účtenku by měl zákazník ve většině případů podepsat a obchodník ověřit shodnost podpisu na účtence s podpisem na rubové straně platební karty, který je umístěn v podpisovém pruhu. Průběh celé transakce od zadání potřebných údajů až po potvrzení trvá v dnešní době zhruba okolo 30 sekund. (Jak probíhá platba kartou, Mastercard, 2014).

Platební terminál je programovaný na to, aby alespoň jednou denně předal informace o všech platebních transakcí, které se ten den provedli, do zúčtovací banky (Jak probíhá platba kartou, Mastercard, 2014). *Zúčtovací banka je banka, se kterou má obchodník uzavřenou smlouvu o přijímání platebních karet a která danému obchodníkovi na jeho podnikatelský účet posílá peníze za transakce na jeho prodejně uskutečněné* (Jak probíhá platba kartou, Mastercard, 2014). Provedení převodu peněz od zúčtovací banky k obchodníkovi trvá většinou do dvou pracovních dnů. Tato banka má také na starosti zabezpečení přenosu důvěrných informací o všech platebních transakcí k vydavateli karty. V poslední fázi je povinností vydavatele karty zaznamenat (započíst nebo odečíst) transakce z účtu držitele karty, kterým byla daná platební karta vydána. Klient banky se poté

všechny informace o činnostech na účtu dozvídá, pomocí měsíčních výpisů (Jak probíhá platba kartou, Mastercard, 2014).

1.3.3 Dělení platebních karet

Platební karty můžeme dělit do několika různých hledisek, viz Tabulka 2. Karty můžeme rozdělit například podle typu použité technologie, služeb nebo jakým způsobem jsou uložena elektronická data. V dalších kapitolách se detailněji zaměříme na druhy zúčtování a na typy nosičů elektronického záznamu.

Tabulka 2 - Třídění platebních karet

Kritérium rozdělení karet	Druh karty
Typ zpracování	• Debetní karta • Kreditní karta • Charge karty • Předplatní karty (elektronická peněženka)
Uživatel	• Osobní • Služební
Vydavatel	• Bankovní • Nebankovních organizací
Území použitelnosti	• Tuzemská • Mezinárodní • Lokální
Typ písma karty	• Reliéfní záznam • Hladký tisk
Typ elektronického záznamu	• Čip • Magnetický proužek • Laserový • Hybridní
Úroveň služeb karty	• Základní • Specializované • Prestižní • Výběrové

Zdroj: Vlastní zpracování

1.3.4 Rozdělení podle principu zúčtování

- **Debetní karty** – jsou to karty, které se váží na běžný účet. Pokud se debetní karta využije při platbě u obchodníka nebo pro výběr z bankomatu,

tak se peníze vydávají z účtu majitele dané karty. Úvěr u debetní karty lze sjednat pouze za situace, že je vytvořený kontokorent. Tedy zjednodušeně kontokorent znamená, že z karty jdou čerpat peníze i bez dostatku hotovosti. Limity kontokorentu se samozřejmě u každé banky liší. Debetní karta patří k nejpoužívanějším kartám v České republice (Matyáš, 2007). Jak je uvedeno v předešlé tabulce, debetní karty mají právo vydávat pouze banky s bankovní licencí.

- **Kreditní karty (úvěrové)** – jsou karty, u kterých probíhá vždy nákup na úvěr zprostředkovávaný vydavatelem kreditní karty, respektive bankou. Na rozdíl od debetní karty je tato karta spojena pouze s účtem úvěrovým. Ve výsledku to znamená, že veškeré platební transakce se čerpají z úvěru od banky. Podobně jako u kontokorentu, probíhá sjednání podmínek úvěru u každé banky odlišně (Matyáš, 2007). V České republice není tato karta oproti debetním kartám příliš v oblibě, jako tomu bylo v jiných státech EU a v Americe. Princip zúčtování vychází z podmínek vydavatele karty, kdy z celkové sumy platebních operací na úvěrovém účtu musí držitel uhradit minimální měsíční splátku, která se pohybuje kolem 5 až 10%. Zbývající část sumy bývá odložena na základě vlastního rozhodnutí držitele karty (Schlossberger, 2012).

- **Charge karty** – tato karta se velice podobá způsobu kreditní karty. Rozdíl je však v tom, že vydavatel karty (banka) na konci měsíce vytvoří seznam všech platebních transakcí k zaplacení provedených kartou. Držitel tedy nemusí za celé období využít žádné peněžní prostředky, protože je banka hradí. Celková dlužná částka se musí většinou do závěru dalšího měsíce, jednorázově zaplatit ve smluveném datu. Vydavatel karty nepřipočítává úrok, jestliže platbu klient uskutečnil ve smluveném období. Karta s odloženou splatností se v České republice nachází jen výjimečně. Ve světě je však tento typ karty běžný (Matyáš, 2007). Společně s kreditní kartou patřili k prvním v bankovnictví. Důvod byl jednoduchý, protože v začátcích platebních karet banky neměli k dispozici zúčtovací systémy v on-line režimu. Nejdříve byly platby klientů

u obchodníků zasílány vydavatelům v papírové podobě prostřednictvím pošty a až déle s využitím sítě způsobem off-line dávek (Schlossberger, 2012).

1.3.5 Rozdělení podle typu záznamu

- **Magnetický proužek** – proužek se nachází na rubu platební karty současně s podpisovým pruhem. Do podpisového pruhu se držitel karty podepisuje jako na všechny účtenky. V magnetickém proužku jsou zaznamenány elektronicky informace, potřebné zejména pro identifikaci a zároveň autentifikaci uživatele karty při výběru hotovosti v bankomatech, či při platbě pomocí elektronických terminálů (Schlossberger, 2012). Tento způsob je v dnešní době nejrozšířenější. Největší nevýhoda magnetického proužku je malá paměťová kapacita nebo větší náchylnost k poškození.

- **Čip** – pozice čipu na platební kartě se řídí podle mezinárodních standardizací. V současné době je čipová technologie povinná pro všechny země EHP, které vydávají platební karty pod hlavičkou VISA nebo Mastercard (Schlossberger, 2012). Manipulace s údaji čipové karty probíhá pomocí paměťového mikročipu umístěného v plastovém těle karty. Ten umožňuje režim čtení informací uložených na mikročipu nebo čtení kontrolou oprávnění uživatele, vyžádáním PIN kódu (osobní identifikační číslo). Protože banky nahrazují typ magnetického záznamu čipovým, řeší tento problém tzv. hybridními kartami, které využívají obě technologie. Výhodou oproti magnetickému záznamu je především větší úložná kapacita informací a vysoká bezpečnost proti zneužití. Posledním rozvojem v oblasti čipových karet jsou bezkontaktní platby. Bezkontaktní platby se provádějí pomocí NFC čipu umístěném na kartě. NFC platby jsou popsaný v nových trendech placení.

- **Laserová karta** – tento druh karty využívá pro elektronický záznam podobný způsob jako záznamy na kompaktních discích (CD). Bohužel druh tohoto záznamu se v oblasti elektronického záznamu platebních karet příliš neuchytil

(Schlossberger, 2012). Výhoda laserové karty je v možnosti uložení několika megabytů dat informací.

1.4 Bankovní platební systém

Převádění peněžních prostředků mezi účastníky tohoto platebního procesu zajišťují platební systémy. Aby se jednalo o platební systém, musí splňovat určité podmínky. Řídí se právem dané země (Česká republika) s minimálně třemi účastníky a provoz systému je podmíněn písemnou smlouvu. Provoz systému je dále povolen pouze s bankovní licencí České národní banky a veškeré operace s peněžními prostředky podléhají zákonu o platebním styku. Příkaz přijatý platebními systémy nelze odvolat. (Máče, 2006).

Platební systémy se dají rozdělit do třech základních hledisek. Prvním hlediskem je rozsah zajišťovaný systémem, podle toho se člení systémy na vnitrobankovní a mezibankovní. Vnitrobankovní systém zpracovává operace mezi účty klientů (plátcem a příjemcem) v rámci jedné banky a naopak mezibankovní systémy zpracovávají platební operace mezi účty klientů různých bank. Dalším hlediskem rozdělení systémů je podle typu jejich vnitřní organizace. S volně organizovanou strukturou se nazývají korespondentské systémy a s pevnou strukturou se nazývají clearingové systémy. Třetí hledisko vyplívá z typu systému a tím je princip zúčtování. Tyto dva typy jsou dále popsány (Polouček, 2013).

- **Korespondentský platební systém** – *Jedná se o vzájemnou dohodu dvou bank mezi sebou. Každá banka má u té druhé banky otevřený svůj účet. Banka A má účet u banky B a naopak banka B má účet u banky A (Platební styk mezibankovní a klientský, Vachtová, 2011).* Tyto účty, které jsou využity pro platební styk mezi bankami, se nazývají korespodentské účty a podle otevřenosti účtu se dělí na nostro nebo loro účet. Zúčtovací banka je centrální banka nebo komerční banka.

  Nostro účet je účet, který má banka otevřený u druhé banky a v rozvaze je umístěn v aktivech (pohledávka). Loro účet je účet, který vede banka pro jinou

banku, která má u ní otevřený účet a v rozvaze banky se nachází v pasivech (závazek). Typicky se systém používá v zahraničním platebním styku (Platební styk mezibankovní a klientský, Vachtová, 2011).

- **Clearingový platební systém** – *Banky v tomto systému nekomunikují přímo mezi sebou, ale přes zúčtovací banku. Banky zapojené v tomto systému mají otevřen nostro účet u zúčtovací banky. Přes tento účet provádějí platby mezi jednotlivými bankami (Platební styk mezibankovní a klientský, Vachtová, 2011).* Typicky se systém používá převážně vnitrostátním platebním styku. Clearingový systém se dělí podle zúčtování na netto a brutto princip nebo na kombinaci obou principů.

  Při netto principu se příchozí a odchozí platba současně zaúčtuje, proto má banka čistou zúčtovací pozici, která se započte, pokud je dostatek finančních prostředků. Při brutto principu se platební operace uskuteční bez vzájemné kompenzace. To znamená, že platba se neuskuteční, je-li nedostatek finančních prostředků (Platební styk mezibankovní a klientský, Vachtová, 2011).

1.4.1 Platební systém ČR

Mezibankovní platební clearingový systém používaný v České republice se označuje od roku 2001 názvem CERTIS (Czech Express Real Time Interbank Gross Settlement System). Provozovatelem je zúčtovací centrum ČNB a jedná se o jediný mezibankovní systém v České republice. Tento systém má zpracovat všechny mezibankovní procesy jako například příkazy dané plátcem a příjemcem bance, platební karty nebo šeky. Data platebních transakcí jsou několikrát denně posílána elektronicky přes komunikační síť (Jílek, 2013).

Hlavní podstata platebního systému CERTIS se zakládá na těchto principech:

- Brutto zaúčtování v reálném čase.
- Zpracování mezibankovních transakcí pouze v českých korunách.
- Přímá účast všech uživatelů platebního systému (banky, družstva).

- Zaúčtování se uskutečňuje na účtech mezibankovních transakcí vedených ČNB – účty povinných minimálních rezerv.
- Neodvolatelnost položek akceptovaných systémem.
- Zpracování různých platebních operací.
- Nezpracované nekryté platby se dostávají do fronty.
- Na účtech platebního styku není povoleno debetní saldo, respektive záporný zůstatek (Jílek, 2013).

1.4.2 Platební systém TARGET

Nadnárodní platební systém TARGET (Trans-European Automated Real-Time Gross-Settlement Express Transfer System) využívaný v Evropě je provozován prostřednictvím Evropské centrální banky (ECB). Jedná se o systém, který vzájemně propojuje clearingové systémy centrálních bank zemí Evropského hospodářského prostoru s platebním systémem ECB (Platební styk mezibankovní a klientský, Vachtová, 2011). V roce 2007 byla zprovozněna nová verze systému pod názvem TARGET2 (Jílek, 2013).

2 Bezpečnostní protokoly a prvky

S rozvojem technologii elektronických platebních systémů se musí rozvíjet i jejich bezpečnostní prvky. Maximální bezpečnost údajů a komunikace mezi uživateli, klienty, obchodníky je pro banku a jiné zprostředkovatele elektronických transakcí velmi důležité z hlediska důvěry jejich účastníků. Při komunikaci účastníků elektronických plateb se posílá mnoho informací, které podléhají bankovním a firemním tajemstvím, proto je jejich zneužití a odposlechnutí nepřípustné pro obě strany platebního procesu. Pro zachování bezpečné výměny informací slouží spousty metod, zásad, či protokolů. Komunikace mezi uživatelem elektronického platebního systému má určitá obecná bezpečností hlediska, viz Tabulka 3.

Tabulka 3 - Základní hlediska bezpečnosti elektronických transakcí

Hledisko	Pohled zákazníka	Pohled poskytovatele
Integrita – shoda dat před a po přenosu bez změny	Nebyla přijatá nebo odeslaná informace jakkoliv změněna?	Nebyla data na webové stránce změněna bez autorizace?
Nepopření – neodvolatelnost platební transakce	Může druhá strana popřít své jednání?	Může zákazník zamlčet platbu, či objednávku?
Důvěrnost- přístup k datům odpovědným osobám	Může někdo jiný nahlížet do mých informací?	Jsou data a informace přístupné pro někoho jiného než autorizovanou osobu?
Soukromí	Mohu kontrolovat používání a přenášení důvěrných informací?	Nedochází při ukládání dat k porušení zákona o ochraně osobních údajů?
Použitelnost – nemožnost provézt službu, ztráta dat, …	Je systém dostupný? Lze k němu přistupovat?	Je systém plně funkční a bezpečný?

Zdroj: Vlastní zpracování dle (ecom.ef.jcu.cz, Bezpečnost online systémů a platebních systémů)

Základní kategorie metod ochrany dat a informací, které využívají banky nebo nebankovní společnosti pro bezpečnost svých platebních systémů se dělí podle oblasti využití a typem použitých prvků:

- Autentizace klienta platebního systému
- Zabezpečení přenosu dat a informací transakce
- Autorizace platebních transakcí

2.1 Autentizace v platebním systému

Autentizace klienta probíhá, když se klient přihlašuje do určitého platebního systému nebo chce provést elektronickou operaci a poskytovatel musí zjistit, zda má klient pravomoci vstoupit do systému a manipulovat s ním. Základní termíny autentizace jsou:

- **Identifikace uživatele** – *proces určení identity (totožnosti) uživatele. Může se jednat buď o udání identity samotným uživatelem, nebo se identifikující systém snaží určit identitu uživatele hledáním v předem dané množině uživatelů. Systém prochází databázi buď obtížně podvrhnutelných záznamů všech uživatelů*

(např. otisk prstu nebo jiná biometrická informace), nebo tajných informací (např. identifikační kód) (Matyáš, 2007, 11).

- **Autentizace (verifikace) uživatele** – *proces ověřování identity uživatele. Uživatel obvykle udá svoji identitu (např. přihlašovací jméno) a bezprostředně také nějakým způsobem umožní její ověření* (Matyáš, 2007, 162).

2.1.1 Druhy autentizačních metod

Základním hlediskem rozdělení autentizace je její úspěšnost ochrany, respektive čas potřebný na prolomení této metody. Z toho vyplívá členění na silnou a slabou autentizační metodu. Příkladem slabé autentizační metody je PIN, či heslo a naopak silné autentizační metody používají čipové karty nebo kalkulátory (Matyáš, 2007). Konkrétní vybrané druhy metod jsou níže popsány.

2.1.1.1 Login a heslo

V dnešní době nejvyužívanější autentizací uživatele je přihlašovací jméno (login) a heslo, ale i přes tento fakt je tento druh autentizace slabý. Heslo se skládá obvykle z řetězce 6 – 10 znaků a nemělo by být triviální, aby nedošlo k slovníkovému nebo hrubému útoku. Systémy mají danou bezpečností politiku, kterou se při vytváření hesla uživatel drží (velká, malá písmena, čísla, atd.). Další součástí této autentizace, je spojení hesla uživatelským loginem. Systém následně ve své databázi ověří správnost autentizačních údajů s daty příslušného uživatele. Zvláštním typem hesla využívaným v platebních systémech se označují tzv. jednorázová hesla (Matyáš, 2007). Jedná se o krátkodobá generovaná hesla bez možnosti opětovného využití na rozdíl od standardních hesel.

- **PIN** – mezi autentizaci založené na znalosti lze pokládat osobní identifikační číslo (Personal Indentification Number). PIN se obvykle skládá z čtyřmístného řetězce číslic, který se používá u platebních karet a mobilních telefonů. Výhodou této formy je zvýšení bezpečnosti mechanismem omezeného počtu pokusů pro zadání správné hodnoty. PIN funguje na principu dvoufaktorové

autentizace, neboť bez fyzického vlastnění autentizačního tokenu nelze PIN využít (Matyáš, 2007).

2.1.1.2 Autentizační tokeny

Dalším druhem autentizace se využívají autentizační tokeny. Autentizační token je zařízení, které klienti mohou samostatně přenášet a jeho vlastnění je podmínkou pro autentizaci do platebního systému. Tokenu připadají určité fyzikální parametry (např. elektrický odpor, tvar, elektrická kapacita) nebo vlastní utajovaná data (např. heslo, kryptografický klíč), či dokáží zpracovávat některé výpočetní operace (Matyáš, 2007).

- **Karta** – V dnešní době jsou nejpoužívanějším autentizačním tokenem. Nejznámějšími zástupci jsou platební karty, které jsou popsané v předešlých kapitolách (magnetický proužek čipové karty) a čipové karty umístěné v mobilních telefonech ve formě SIM karet.
- **CVC2** – Tato obdoba PINu se používá u bezhotovostních plateb na internetu společně s číslem a platností karty. Jedná se o ochranné trojčíslí platební karty (Card Verification Code) umístěné na rubové straně. CVC2 se vyskytuje i pod jiným označením, které závisí na typu karetní asociace.
- **Autentizační kalkulátor** – Zařízení má nejrůznější podobu, ale obvykle obsahuje rozhraní vybavené displejem a také klávesnicí. Pokud obsahuje klávesnici, aktivování zařízení funguje na základě PINu. Principem autentizačního tokenu je časová synchronizace kalkulátoru s autentizačním serverem, který se nachází ve společnosti, do jejichž systému se autentizujeme. Rozhraní kalkulátoru poté zobrazí generovanou hodnotu (číslici), která má krátkou časovou dobu použitelnosti, proto se musí zadat do systému, než se opět změní. (Čermák, Autentizace: zasuň token, 2009).
- **Autentizační SMS** – Mobilní telefon se chová obdobně jako autentizační kalkulátor. Klient musí před vstupem do systému zadat mobilní číslo, na které mu obratem přijde autentizační SMS s generovaným jednorázovým heslem.

2.1.1.3 Biometrické údaje

Dalším druhem autentizace a identifikace klienta, který je v dnešní době na vzestupu, zpracovává fyziologické údaje člověka. Protože se člověk rodí s unikátními biometrickými charakteristikami, slouží tyto získané údaje k dobrému rozpoznání účastníka platebního systému. Biometrické techniky se tedy zakládají na rozpoznávání fyziologických vlastností člověka nebo jeho chování. Příkladem může být otisk prstu, geometrie ruky nebo vzorek hlasu. Systémy využívající biometrické údaje nemusí být vždy přesné, ale systémy zakládající se na fyziologických vlastnostech jsou spolehlivější, než systémy pracující s duševním stavem člověka (Matyáš, 2007).

Platební karta Zwipe MasterCard® je první bezkontaktní platební karta na světě, která se ověřuje pomocí otisků prstů. Obsahuje integrované biometrické čidlo a zabezpečenou biometrickou technologii autentizace Zwipe, jež uchovává biometrická data držitele karty. Biometrické ověření nahrazuje zadávání PIN kódu, díky čemuž mohou držitelé na rozdíl od ostatních bezkontaktních plateb na trhu platit jakékoli částky (Investujeme.cz, Bezkontaktní platební karty budoucnosti mají integrované čidlo na otisk prstu, 2014*).*

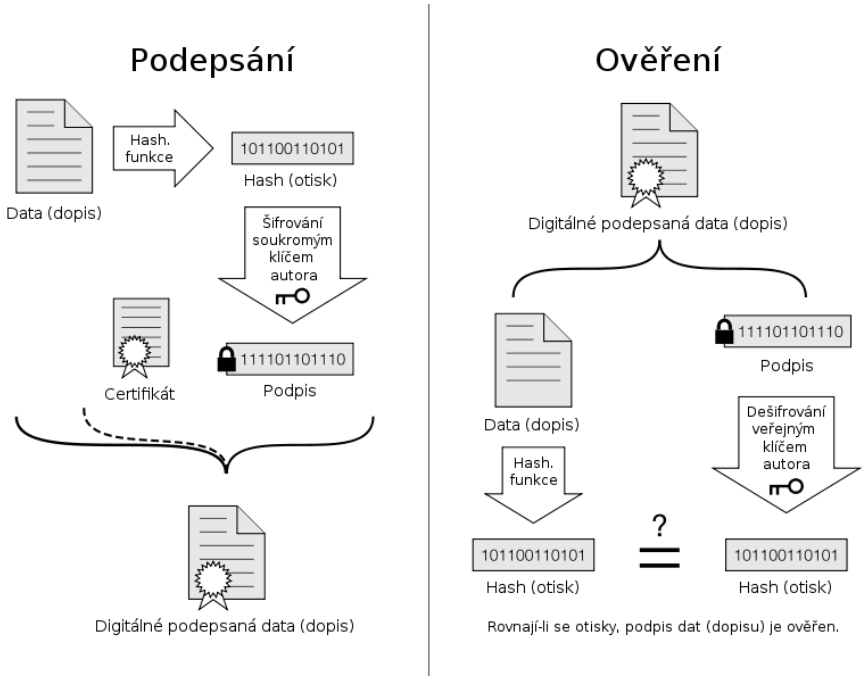
2.1.1.4 Digitální podpis

Digitální podpis je klientův tzv. osobní certifikát, který vzniká asymetrickou kryptografii. Asymetrická kryptografie spočívá v generování dvojice klíčů (veřejný a soukromí) na rozdíl od symetrické kryptografie, kde vzniká pouze jeden klíč. Digitální podpis je založen na tom, že šifrovaná data pomocí jednoho z dvojice klíčů je možné rozluštit (dešifrovat) v určitém časovém úseku pouze se znalostí toho druhého klíče nebo opačně. Jeden z klíčů se označuje jako soukromí klíč a bezpečně uložen například v čipové kartě. Druhý z klíčů se označuje jako veřejný klíč, protože je obecně známý všem. Výsledkem procesu je tedy zašifrování dat odesílatelem jedním z dvojice klíčů (soukromí, veřejný) a veřejným klíčem protistrany. Proběhne tedy identifikace a autentizace, viz Obrázek 3. Pro vytváření

klíčů se v dnešní době využívá RSA (Rivest, Shamir, Adleman) nebo DSA (Digital Signature Algorithm) asymetrický algoritmus. (Budiš, 2008).

- **Hash (otisk)** – Hashovací funkce je doplňkovým zabezpečením elektronického podpisu. Jedná se o funkci, která jednosměrné transformuje libovolná data na řetězec pevné délky (otisk). Mezi nejvýznamnější hashovací funkce patří MD-5 (Message digest) a SHA-1 (Secure hash Algortim) (Budiš, 2008). Příkladem může být soubor příkazů k úhradě, ke kterému se před odesláním vytvoří funkcí hash. Dokument s hashem se pomocí tajného klíče odesílatele a veřejného klíče příjemce zašifruje a pošle samotnému příjemci. Příjemce data rozšifruje svým klíčem a veřejným klíčem odesílatele a poté stejnou funkcí převede data na hash. Následně je nově vypočítaný hash porovnán s hashem odesílatele. Pokud jsou porovnané hodnoty shodné elektronický podpis je platný a důvěryhodný (Máče, 2006).
- **Certifikát a certifikační autorita (CA)** – CA je vydavatelem digitálních certifikátů, který vystupuje ve vzájemné komunikaci jako třetí autoritativní a nezávislý subjekt, který potvrzuje pravdivost informací, obsažené ve volně přístupném veřejném klíči. CA tedy svazuje prostřednictvím certifikátu fyzickou a elektronickou identitu. Digitálním certifikátem se označuje elektronicky podepsaný veřejný šifrovací klíč s údaji k identifikaci subjektu, pro který byl vydán (Budiš, 2008).

Obrázek 3 - princip digitálního podpisu



Zdroj: AUTOR NEUVEDEN [online]. [cit. 2015-01-24]. Dostupný na WWW: http://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis

2.2 Zabezpečení komunikace při transakci

V dnešní době, kdy se rozvíjejí bezhotovostní internetové platební systémy je nutností dodržovat zmiňovaná hlediska. Proces platební transakce musí dodržet integritu, protože při komunikaci nesmí dojít k odposlechu a získaní citlivých dat klienta nebo banky. Klient musí důvěřovat v použitý bezpečnostní prvky a technologie použité přesunu finančních prostředků, aby nedošlo například k přesměrování na cizí účet. Dále se musí brát v potaz hardwarové a softwarové možnosti obou účastníku komunikace při platební transakci. Samozřejmostí by mělo být na straně klienta, vlastnit kvalitní antivirový program a firewall. Jelikož jsou různorodá zařízení, kterým je možné realizovat platbu, využívají se pro komplexní bezpečnost komunikace protokoly elektronických platebních systémů. Následuje představení některých z nich.

2.2.1 SET

SET (Secure Electronic Transaction) je komplexní bezpečnostní protokol elektronických transakcí, který vyvinuli kreditní asociace MasterCard a Visa na začátku rozmachu elektronického obchodu. Tento protokol poskytuje komunikačním stranám důvěrnost, integritu a ověření platebních operací, které se provedené kartou. Slučuje skupinu bezpečnostních metod, které jsou v předešlé kapitole popsané (Protokoly pro elektronické platební systémy, 2009). Specifikace protokolu SET:

- Vytváří bezpečný komunikační kanál mezi účastníky transakce.
- Zajišťuje důvěryhodnost transakce pomocí digitálního podpisu a certifikátu veřejného klíče.
- Obsah zpráv je přístupný pouze autorizované straně (obchodník má přístup k objednávce, banka má přístup k platebnímu příkazu).
- Duální digitální podpis – spojení informace pro banku s informací pro obchodníka (Kunderová, Bezpečnost komunikačních přenosů, 2014).

2.2.2 3-D SET

Protože se SET kvůli své nákladné a složité implementaci neujal, začal se vyvíjet bezpečnostní protokol na bázi SETu s server-based implementací. Server-based SET byl výhodnější v tom, že digitální certifikát nebyl uložen u klienta nebo obchodníka, ale na serveru vydavatele karty, respektive zúčtovací banky. To umožnilo použít i mobilní zařízení při transakci, protože klient se spojil se serverem s využitím bezpečné komunikace (SSL) a stáhl program. Tento program se spojil se serverem s požadavkem na certifikát registrovaného klienta (Juřík, Jak platit bezpečně i na internetu, 2005).

2.2.3 SSL a TLS

Secure Sockets Layer (SSL) a jeho novější verze Transport Layer Security (TLS) je protokolem (vrstvou), který je vložený mezi transportní a aplikační vrstvu, který pomocí asymetrického šifrování a autentizace zabezpečuje komunikaci. Nejčastěji se využívá při komunikaci se servery prostřednictvím zabezpečeného protokolu

HTTPS, viz Obrázek 4. Protokol SSL a TLS fungují tedy na principu asymetrického šifrování, kdy oba účastníci mají dvojici klíčů (veřejný a soukromí) a certifikátů. Fungování asymetrického šifrování je v předešlé kapitole. Pro výměnu klíčů využívá RSA, Diffie-Hellman, DSA nebo Fortezza asymetrický algoritmus. Pro symetrické šifrování využívá RC2, RC4, IDEA, DES, 3DES nebo AES algoritmus a pro tvorbu hashe používá MD5 nebo SHA hashovací funkci (SSL-certifikáty.cz, SSl protokol, 2014). Tyto protokoly jsou obvykle využívaný bankami v elektronickém bankovnictví.

Obrázek 4 - ukázka využití TLS

Zdroj: vlastní úprava, www.ssl-certifikaty.cz

2.2.4 3D Secure

S rozvojem e-shopů a internetových plateb byl vyvinut mezinárodní bezpečnostní protokol 3D Secure, který si klade za cíl zvýšit bezpečnost plateb na internetu prostřednictvím platebních karet. Tento dodatečný bezpečnostní mechanismus, respektive soubor bezpečnostních požadavků online transakcí, byl vyvinut karetní asociací VISA. VISA označuje bezpečností standart pod názvem „Verified by Visa“. 3D Secure protokol byl přijat i dalšími karetními asociacemi jako například

MasterCard, který tento standart označuje pod názvem „MasterCard SecureCode“. (GPwebpay, bezpečnost, 2013). Pokud e-shop protokol podporuje, stránka při zadávání údajů o kartě obsahuje loga standartu obou karetních asociací, viz Obrázek 5.

Obrázek 5 - označení standartu na internetu

Zdroj: AUTOR NEUVEDEN [online]. [cit. 2015-01-23]. Dostupný na WWW: https://www.securepay.com.au/_uploads/images/_medium/combined.jpg

Vývoj 3D Secure protokolu vycházel ze získaných poznatků z vývoje a využívání předešlých nepříliš úspěšných systémů SET a 3-D SET, proto vzniklo bezpečnostní řešení, které nepotřebuje software a certifikát klienta. Do software není počítán klientův webový prohlížeč (Piják, Elektronické platební systémy, 2003). Základní architektura protokolu je založena na komunikaci tří domén (3D) během platební transakce. Komunikace mezi doménami probíhá pomocí komunikačního kanálu zabezpečeného prostřednictvím zmiňovaného protokolu SSL nebo TLS. Komunikujícími třemi doménami jsou:

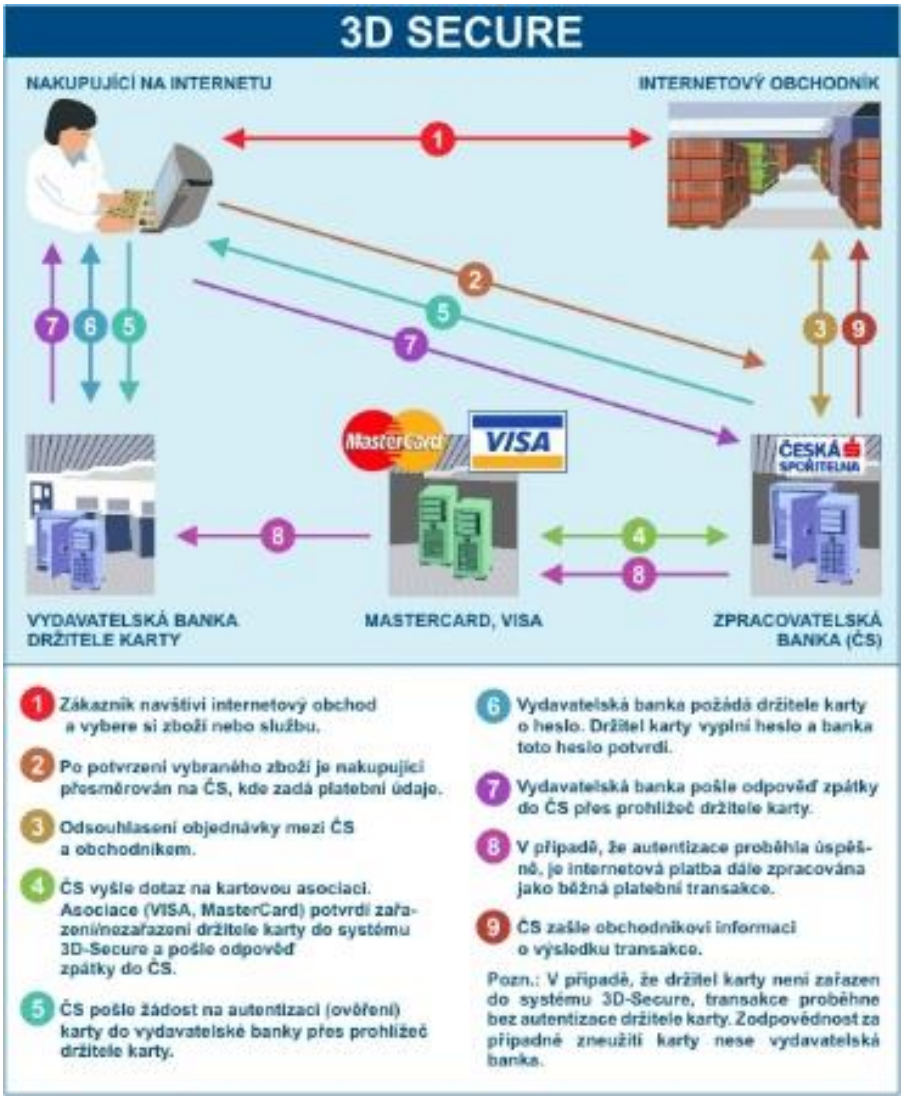
- Doména nabyvatele
- Doména vydavatele
- Doména komunikace

2.2.4.1 Platba uživatele přes 3D Secure

Tento standart je založen na tom, že uživatel při dokončení nákupu a výběru platby, je přesměrován na platební bránu (stránku) certifikovaného poskytovatele, kde zadá do formuláře požadované údaje o kartě (číslo, exspiraci a CVC2 platební karty). Poskytnuté údaje o kartě nezískává přímo obchodník, ale jsou přesměrovány do banky obchodníka. Toto spojení je šifrováno pomocí zmíněných protokolů, aby nedošlo k odposlechu citlivých dat. Banky při transakci komunikují

mezi sebou a výsledek transakce je předán obchodníkovi. Celý proces je detailně popsán viz Obrázek 6. Pro autorizaci platební transakce se využívá autorizační SMS s jednorázovým heslem (3D Secure kód), který platební transakci z hlediska klienta potvrdí (Raiffeisenbank, 3D Secure – Plaťte kartou na internetu bezpečně a bez obav, 2015).

Obrázek 6 - schéma fungování 3D Secure



Zdroj: AUTOR NEUVEDEN [online]. [cit. 2015-01-25]. Dostupný na WWW: http://www.eproton.cz/Images/Archive2/1/karty_3dsecure.jpg

2.3 Autorizace platební transakce

Autorizace platebních transakcí v oblasti nejen elektronického bankovnictví se shoduje s autentizačními metodami klienta v platebním systému. Jedná se většinou o poslední fázi elektronické platební transakce, před přesunem peněžního obnosu

na jiný účet. Dá se opět využít soukromý klíč a daný certifikát uložený v počítači nebo na čipové kartě. Velmi často se pro autorizaci plateb generují bankami jednorázové autorizační kódy s omezenou časovou platností, které jsou zaslané jiným zařízením pro komunikaci, například SMS zprávou přes mobilní telefon. Od banky může dostat soubor s omezeným počtem jednorázových autentizačních hesel TAN (Transaction Authentication Number) prostřednictvím pošty, pobočky, či SMS (Matyáš, 2007).

Další formou autorizace platby nabízející bankami spojené s platební kartou, může být uzamčení karty. Uzamčená karta nepovolí realizovat platební transakce a klient musí povolit její opětovné odemčení. Další možností pro elektronické platební transakce je nastavení časového limitu (obvykle denní limit), kdy klient nesmí přesáhnout určitou maximální částku (Matyáš, 2007). Relativně nový typ autorizace nastává při používání bezkontaktní platební karty, kdy klient u platební transakce nemusí zadat PIN, ale pouze při platbě do 500 Kč.

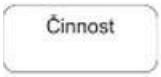
2.4 BPMN

Business Process Modeling Notation (BPMN) je jazyk sloužící pro modelování obchodních procesů, který vznikl ve spolupráci s organizací Business Process Management Initiative (BPMI). Do této organizace patří většina světových firem z oblasti zabývající se nástroji pro modelování podnikových procesů. V současné době je tato organizace součástí konsorcia Object Management Group (OMG) a BPMN se stalo jejím standardem (Kanisová, 2007).

*Business Process Modeling Notation je jazykem pro oblast procesů, a tudíž je procesně orientován. Lze tedy, říci že základními stavebními prvky tohoto jazyka jsou procesy. Jazykem můžeme kromě popisu celého procesního běhu a delegování zodpovědností též vyjádřit vzájemné předávání zpráv mezi procesy a tak umožnit jejich synchronizac*i (Kanisová, 2007, 31). Důležitou výhodou jazyka BPMN, která byla důvodem jeho vzniku, je zejména srozumitelná grafická notace pro znázornění modelů procesů. Pro jednoduché grafické znázornění slouží diagramy BPMN, které zobrazují a popisují jednotlivé kroky i celkový tok procesu

(Kanisová, 2007). Program pro tvorbu BPMN diagramů se používá například Enterprise Architect. V diagramech jsou využívány různé grafické elementy, které mají svůj účel.

Tabulka 4 - Základní elementy diagramu BPMN

Element	Notace v BPMN	Popis elementu
Proces		Proces v notaci BPMN znázorňuje dané pořadí vykonávaných činností pomocí sítě podprocesů nebo činností propojených řídícími prvky.
Činnost (aktivita)		Základní element v procesu reprezentující předepsanou činnost. Činnost se dělí na další typy: úkol a podprocesů.
Počáteční událost		Element zahajující řetězec aktivit v rámci procesu. Proces musí mít nejméně jednu počáteční událost.
Koncová událost		Element znázorňující konec procesu nebo řetězce činností. V procesu může být více koncových událostí.
Druhy událostí		Element definující důvod činnosti (události) a zároveň činnost může definovat, co je výsledkem zpracování dané sekvence zpracování. Existují různé druhy událostí, vyobrazena je časová událost a zpráva.
Sekvenční tok		Element vyjadřující následnost procesních prvků od počáteční ke koncové události.
Brána		Element zobrazující místa větvení nebo sdružování procesního toku. Rozhoduje o dalším postupu procesu.
XOR – typ brány		Synchronní brána, kde tok procesu pokračuje pouze jednou větví.
OR – typ brány		Paralelní brána, kde tok procesu pokračuje jednou nebo více vystupujícími větvemi najednou.
AND – typ brány		Paralelní brána, kde tok procesu pokračuje všemi vystupujícími větvemi najednou.

Zdroj: Vlastní zpracování dle informací (Kanisová, 2007)

3 Situace na trhu

V dnešní době rozmachu nakupování přes internet jsou elektronické platební systémy stále více využívány a tak se do pozadí dostává platba v hotovosti, respektive úhrada zboží, či služeb dobírkou. Kromě využití platební karty se dají využít další technologie pro elektronickou platební transakci jako například elektronické peněženky, mobilní platby nebo stále více využívané podpůrné elektronické bankovnictví, ale další možnosti dostávající se pomalu na trh. V úvodu je nutné představit elektronický platební prostředek a elektronický platební systém a dále jsou popsány vybrané druhy elektronických plateb.

3.1 Elektronický platební systém

Dle doposud dostupných definic by se daly elektronické platební systémy klasifikovat jako soubor instrukcí, pravidel, mechanismů a procedur, umožňující kupujícímu zaplatit prodávajícímu, a to vše je uskutečňováno elektronicky. Elektronické platební systémy (EPS) realizují bezhotovostní platby prostřednictvím internetu a jiných informačních technologií (Kysela, Mobilní komerce a elektronické platby, 2010).

Cena a rychlost převodu peněz od zákazníka k obchodníkovi se liší vždy podle toho, jaký platební systém je k danému převodu použit. Zpravidla jsou však tyto náklady velmi nízké a doba mezi odesláním platby a připsáním na účet příjemce se pohybuje řádově v hodinách a maximálně v několika dnech (Štěpánek, Online platební systémy v České republice a výběr vhodné varianty pro internetový obchod, 2012).

Základní rozdělení EPS podle typu realizace plateb (Kysela, Mobilní komerce a elektronické platby, 2010).:

- **Offline platby** – realizace platby proběhne se zpožděním v řádu několika dnů.
- **Online platby** – realizace platby proběhne okamžitě po zadání pokynu v řádu několika vteřin.

Základní rozdělení offline plateb používaných v tuzemsku (Kysela, Mobilní komerce a elektronické platby, 2010):

- Platební příkazy v elektronickém bankovnictví.
- Offline platby prostřednictvím kreditních a debetních karet.

Základní rozdělení online plateb používaných v tuzemsku (Kysela, Mobilní komerce a elektronické platby, 2010):

- Online platby prostřednictvím kreditních a debetních karet.
- Platby elektronickou peněženkou.
- Platby mobilním telefonem.

3.1.1 Elektronické peníze

Úzce s elektronickými platebními systémy souvisí elektronické peníze. Jedná se o peněžní hodnotu uchovávanou v elektronické podobě na elektronickém platebním prostředku (Máče, 2006).

Rozdělení podle způsobu uložení (Máče, 2006):

- Uložení na fyzickém nosiči (Card-based) – pro realizaci platby musí fyzicky být nosič přítomen (např. čipová karta)
- Uložení v paměti PC (Software-based) – přístup k peněžní hodnotě je pomocí informačních sítí pro přenos dat

Rozdělení podle povahy elektronických peněz (Máče, 2006):

- Token-based – elektronické peníze jsou virtuální kopií reálných peněz. Mají definovanou hodnotu zabraňující použít peněz vícekrát.
- Balance-based – elektronické peníze mají formu kladného nebo záporného zůstatku na elektronickém účtu.

3.2 Elektronická peněženka

Elektronická peněženka je velice využívaný platební systém na internetu zaměřující se na rychlé a bezpečné platby menších, ale také větších částek. Systém je podobný jako čipové karty na dopravu, parkování a další mikroplatby (Maytáš, 2007). Klient si musí nejdříve vytvořit uživatelský účet s přihlašovacími údaji u poskytovatele elektronické peněženky. Na elektronickou peněženku se finanční prostředky převádějí přesunem peněz z bankovního účtu nebo pomocí platební karty, či jiné elektronické peněženky. Některé systémy elektronických peněženek nabízejí propojení s bankovním účtem a strhávají částky přímo z něho (např. PayPal). Z virtuálního účtu peněženky se realizuje platba při přesměrování z eshopu na platební bránu, kde klient zadá své přihlašovací údaje. Správa účtu probíhá přes webové rozhraní služby, mobilním telefonem nebo emailem. Mezi nejvýznamnějšími zástupce patří mezinárodní PayPal, Skrill, GoPay nebo český systém Paysec. (Kysela, Mobilní komerce a elektronické platby, 2010).

Základní bezpečnostní prvky elektronické peněženky:

- V elektronické peněžence je pouze námi omezený finanční objem, který na ní přesuneme. V případě zneužití není ohrožen celý finanční objem jako na platební kartě.
- Při platební transakci není potřebné zadávat důležité údaje o platební kartě a jiná citlivá data, protože se využívá login a heslo.
- Některé platební systémy mají maximální částku, kterou nelze překročit s dodatečnou autorizací, například pomocí autorizačního hesla (ShopCentrik, Elektronická peněženka, 2015).
- Data jsou šifrována pomocí protokolů SSL a certifikáty.

3.3 Platební brána

Platební brány, či označení platební agregátory jsou poskytovatelé služeb, kteří sdružují několik metod bezhotovostních plateb do jednoho uživatelského rozhraní. Obchodníkovi, proto odpadá nutnost zavádět platební metody zvlášť. Platební agregátory zajišťují komunikaci s internetovým bankovnictvím různých bank,

ale také umožňují platby například elektronickými peněženkami, prémiovými SMS nebo také platebními kartami, čímž nabízejí obchodníkovi a zákazníkovi širokou škálu platebních služeb. Výhodou platebních bran je především rychlost plateb, protože obchodník obdrží požadovanou částku na svůj účet ihned nebo v řádu několika hodin. Další výhodou je jednoduchá implementace do internetového obchodu a bezpečnostní technologie plateb (EasyShop, Platební agregátory ulehčí a urychlí nákup, 2015).

3.4 Mobilní platby

Vývojem technologií mobilních zařízení, který rok od roku stoupá, se začínají využívat mobilní telefony nebo tablety pro elektronické platby. Některé jsou na trhu již delší dobu a některé se teprve snaží prosadit u klientů a obchodníků. Níže v textu se nachází výběr některých mobilních způsobů platby.

3.4.1 Premium SMS

Jedná se o službu, umožňující pomocí zaslaných prémiových SMS nakupovat služby nebo zboží. Službu nabízejí všichni mobilní operátoři a částka za tuto SMS se zúčtuje přímo z telefonního účtu klienta. Klientům s předplacenou kartou se částka hradí z kreditu a naopak klientům s tarifem se částka připočítá do měsíčního vyúčtování telekomunikačních služeb. Premium SMS fungují tak, že klient pošle požadované znění SMS zprávy určené obchodníkem na speciální číslo a obratem dojde k přijmutí potvrzovací SMS a zaúčtování. Speciální čísla většinou začínají předčíslím 90 a cena zpoplatněných SMS je v rozmezí 1 a 999 Kč podle výběru služby (Platmobilem, zpoplatněné SMS (Premium SMS), 2014). Nejčastěji se používá tato služba například na platby soutěží, jízdného, parkování nebo formou dárcovských SMS. Nevýhodou pro obchodníka jsou vysoké náklady za technické zprostředkování operátory a nutné zaplacení daně z přidané hodnoty.

3.4.2 NFC platby

Bezkontaktní placení nemusí zprostředkovávat pouze platební karta, ale také mobilní telefon. Tento způsob placení je založen na technologii NFC (Near Field Communication). Jedná se o elektromagnetickou bezdrátovou technologii

umožňující komunikovat mezi dvěma zařízeními na krátkou vzdálenost. Vzdálenost obou zařízení při komunikaci je v jednotkách centimetrů, nejčastěji do 5 centimetrů. Technologie NFC se stala v roce 2003 standardem ISO/IEC (NFCtech, Co je NFC?, 2011).

Komunikace pomocí této technologie se dá rozdělit podle koncových zařízení:

1) **Aktivní – Pasivní** – Za aktivní se pokládá zařízení vybavené NFC čipem umožňující čtení a zápis. Příkladem může být právě mobilní telefon. Pasivní zařízením je obvod, který není nijak napájen. Nejčastěji se jedná o NFC nálepky, které jsou označovány často jako tagy. Pokud se tyto dvě zařízení dostanou do vzájemné blízkosti, NFC čip vysílanými elektromagnetickými vlny nabije kondenzátor v obvodu a začnou mezi sebou odesílat potřebné informace - elektromagnetická indukce (NFCtech, Co je NFC?, 2011).

2) **Aktivní – Aktivní** – Komunikace probíhá podobně jako v prvním typu, ale s rozdílem, že pasivní zařízení má vlastní napájecí zdroj a nepotřebuje elektromagnetickou indukci. Příkladem mohou být dva mobilní telefony nebo mobilní telefon s platebním terminálem podporující NFC (NFCtech, Co je NFC?, 2011).

Aby bylo možné využít NFC platby platební kartou v mobilním telefonu, je nezbytné vlastnit mobilní telefon vybavený NFC technologii nebo NFC nálepkou. Druhou podmínkou pro uskutečnění platby je vlastnit NFC SIM kartu a aplikaci od operátora. Platba poté proběhne pouhým přiložením k platebnímu terminálu jako s bezkontaktní platební kartou a pokud částka k úhradě přesahuje 500 Kč, klient musí zadat autorizační PIN kód (Kartavmobilu, NFC platby obecně, 2015).

3.4.3 QR platby

Využívaní QR kódů v oblasti elektronických plateb patří mezi relativní novinku. Slouží především k usnadnění vytváření příkazů plateb k úhradě. Klient pomocí kamery nebo fotoaparátu mobilního telefonu naskenuje QR kód, který poté aplikace převede na údaje pro platbu (např. číslo účtu, částku atd.). Pokud

skenování QR kódů podporuje aplikace elektronického bankovnictví, údaje automaticky převede do formuláře příkazu k úhradě a platbu stačí pouze autorizovat. Uživatel použitím QR kódu předchází chybám, kterých bych se dopustil při ručním vystavování příkazu, a především zrychluje celý proces platby.

3.5 Elektronické bankovnictví

S platebními kartami je v dnešní době úzce spojeno elektronické bankovnictví a nejedná se pouze o platby přes internet, ale existují další správy vlastního bankovnictví. Trh nabízí různé druhy elektronického bankovnictví s využitím různých prostředků.

Pod elektronickým bankovnictvím si lze představit nabízení standardizovaných bankovních produktů a služeb elektronickými způsoby. Klienti a menší podniky využívají standardně poskytované služby, které umožňují vzdáleně přistupovat na účet v plném rozsahu. Naopak větší firmy používají typ elektronického bankovnictví banka – klient – banka pro předávání informací a platební styk. Obvyklá spolupráce banky a velké firmy (klienta) v elektronickém bankovnictví probíhá propojením informačních účetních systémů banky a klienta. Propojení probíhá s vysokou ochranou dat. Elektronické bankovnictví se stále dostává více do popředí, a proto byla v České republice vytvořena pravidla pro elektronické platební prostředky a peníze, které nabyly platnost v roce 2002 přijetím zákona o platebním styku (Polouček, 2013).

Banky slouží pro provoz systémů elektronického bankovnictví moderní technologie, které nejsou pro klienta nutné znát. Klient pracuje již s koncovým zařízením umožňující komunikaci s bankovním systémem. Nejčastěji mezi tyto koncové zařízení patří telefonní a výpočetní technika (PC, tablety, PDA apod.). Podle typu přenosu dat a využívaného koncového zařízení dělíme elektronické bankovnictví na mobilní, internetové, telefonické bankovnictví a homebanking (Polouček, 2013).

3.5.1 Telefonické bankovnictví

Bankovnictví po telefonu zprostředkovává komunikaci s bankou za použití klasického telekomunikačního zařízení. Klient se dorozumívá s call centrem banky, které ve většině případů pracuje 24 hodin denně. Komunikace probíhá s bezpečnostními prvky. Obě strany v komunikaci využívají systém hesel, přičemž tyto hesla zná jedině samotný klient a banka. Pro udržení bezpečnosti a snížení rizika odposlechu nejsou hesla používána celá. Banky nabízí také automatizované hlasové systémy pro předání základních informací klientovi. Tento typ bankovnictví umožňuje například zjistit aktuální stav účtu, o nabízených službách nebo zadávaní příkazů k úhradě (Polouček, 2013).

3.5.2 Mobilní bankovnictví

Mobilní bankovnictví se často označuje „smartbanking“. Mobilní bankovnictví se od telefonického liší hlavně z hlediska větších možností služeb a komfortu s příchodem „chytrých“ telefonů. Mobilní bankovnictví dává možnost klientovi vzdáleně spravovat bankovnictví využitím mobilního telefonu, či tabletu. Komunikace s bankou může probíhat různými způsoby. Jeden ze způsobů komunikace je odesílání šifrovaných SMS zpráv přímo bance. Klient tedy veškeré úkony a příkazy bance zadává pomocí klávesnice mobilu. Protože se v posledních letech dostávají do popředí moderní mobilní komunikační prostředky – tablety, „chytré“ telefony (*smartphony*), začaly banky vytvářet vlastní aplikace mobilního bankovnictví. Princip těchto bankovních aplikací a zároveň podmínkou fungování, je připojení mobilního telefonu k internetu s podporou dotykového ovládání. Proto se nejčastěji pojmenovává tato forma smartbanking. Smartbanking nabízí například sledování obratů na účtech, zjišťování kurzů měn nebo hledat nejbližší bankomaty v okolí (Polouček, 2013).

3.5.3 Internetové bankovnictví

Jak z názvu vypovídá, jedná se komunikaci a zpracování požadavků elektronického bankovnictví přes internet. Tento způsob zpracování nepožaduje žádné specifické zařízení, protože spojení s bankovní aplikací zprostředkovává počítač klienta. Aplikace banky mohou být spojené se soubory uloženými na určité pracovní

stanici nebo existují přenositelné aplikace, s kterými je možno pracovat po zadání přístupových údajů klienta (identifikační čísla, hesla, apod.). Internetové bankovnictví podobně jako smartbanking nabízí spoustu služeb jako například získávání informací o účtech, bance nebo opět vytváření platebních pokynů. V dnešní době se poskytované služby tohoto bankovnictví stále rozšiřují, proto se klientům otvírají nové oblasti správy účtů. Příkladem nových možností je například správa terminovaných vkladů (vytváření, rušení, atd.). K základním typům zabezpečení a zároveň nejvíce napadnutelných, určitě patří klasické použití přístupového klíče s heslem, tak využitím vyšší zabezpečovací úrovně pomocí kvalifikovaných certifikátů. Připojení je omezeno na dobu požadovanou na zpracování dané operace (Polouček, 2013).

3.5.4 Homebanking

Při využití homebankingu dochází ke spojení informačního systému klienta se systémem dané banky přes datové linky. Tento způsob bankovnictví omezuje papírovou komunikaci s bankou a má tedy podobu různých elektronických služeb. Pro vyšší bezpečnost při komunikaci se často využívá pevného propojení mezi bankou a klientem. Vyšší bezpečnost je zajištěna tím, že se veškeré úkony v systému dělají offline a po ukončení práce proběhne přenos dat s bankou přes internetovou síť. Před nasazení této formy elektronického bankovnictví bývá pro uživatele systému školení z důvodu větší složitosti použité technologie. Homebanking pro uživatele nabízí mnoho bankovních služeb jako například i zadávání zahraničních příkazů k úhradě, sledování akciových trhů aj. (Polouček, 2013).

4 Funkčnost a bezpečnost vybraných služeb

V této kapitole jsou prakticky popsány bezpečnostní a funkční hlediska vybraných platebních systémů na trhu. Každý platební systém se liší ve využité technologii při registraci, zpracovávání platby nebo bezpečnostními prvky a protokoly. Vybrané procesy platebních systém jsou modelovány standardem BPMN (viz kapitola 3.6 BPMN). V závěru této kapitoly jsou zpracovány výsledky a zhodnocení jednotlivých systémů včetně doporučení.

4.1 Model platby s 3D Secure

Tato podkapitola se zabývá bezpečnostním protokolem 3D Secure, který je teoreticky popsaný v kapitole 2.2.4 3D Secure. Použitý diagram BPMN zobrazuje platební proces, který začíná platbou kartou v elektronickém obchodě a končí provedením transakce. V procesu komunikují tři domény a jejich prvky s danými úkoly:

- **Doména nabyvatele** - doména nabyvatele je spojena s obchodníkem, zpracovatelskou bankou (bankou obchodníka) a VISA komponentou Merchant Server Plug-in (MPI). MPI je softwarová komponenta internetových stránek obchodníka pro komunikaci s ostatními prvky. Tato doména zodpovídá za definování procedur s cílem zajistit, že účastníci obchodu v internetových transakcích operují pod dohodou obchodníka s vydavatelem a poskytuje zpracování transakce po ověření pomocí MPI (Carbonell, 2009).
- **Doména vydavatele** - doména vydavatele je spojena s držitelem karty, vydavatelskou bankou (bankou držitele) a VISA složkou Acces Control Server (ACS). ACS je server kontroly přístupu, který obsahuje informace o držitelích karet a musí ho mít vydavatele karet. Tato doména má za úkol správu přihlášení držitele karty ke 3D Secure a autentizovat držitele karet během online nákupu pomocí ACS (Carbonell, 2009).
- **Doména komunikace** - doména je spojena s centrálním adresářem čísel platebních karet Visa Directory Server (DS) a serverem historie autentifikace Authentication History Server (AHS). Centrální adresář VISA řídí veškerou komunikaci mezi obchodníkem a příslušným ACS v procesu požadavku, jestli je autentifikace platby k dispozici. AHS ukládá zprávy z ACS pro každý pokus o autentifikaci platby (Carbonell, 2009).

4.1.1 Tok zpráv v 3D Secure

Mezi objekty domén probíhá výměna zpráv, která je názorně představena na modelu, viz Obrázek 7. Hlavní zprávy probíhající mezi objekty domén se označují:

- **VEReq** – zpráva od obchodníkova MPI do DS nebo z DS do příslušného ACS, která zjišťuje, jestli je autentizace pro dané číslo platební karty dostupná.
- **VERes**- zpráva od ACS pro DS, který následně předá informaci obchodníkovu MPI, jestli je autentifikace dostupná.
- **PAReq**- zpráva o požadavku autentizace poslaná od MPI do ACS (přes prohlížeč držitele karty) k vydavatelské bance s cílem ověřit držitele karty.
- **PARes** – zpráva formátována, digitálně podepsána a odeslána z ACS do MPI (přes prohlížeč držitele karty) poskytující výsledek o autentizaci držitele karty (Carbonell, 2009).

Tok zpráv v 3D Secure:

1) Nejdříve se držitel karty rozhodne k nákupu v elektronickém obchodě a odešle objednávku s platebními údaji. V tomto momentě je aktivován na straně obchodníka software MPI.

2) Obchodníkův MPI posílá zprávu (VEReq) k DS s cílem zjistit, jestli jsou pro držitele karty dostupné služby autentizace, respektive zda je účet přihlášen do systému 3D Secure.

3) Pokud držitel karty spadá do rozsahu zúčastněných karet a autentifikace je dostupná, přepošle DS zprávu s odpovědí (VERes) do MPI. Zpráva obsahuje údaje o držiteli karty a informace, jak kontaktovat příslušný ACS.

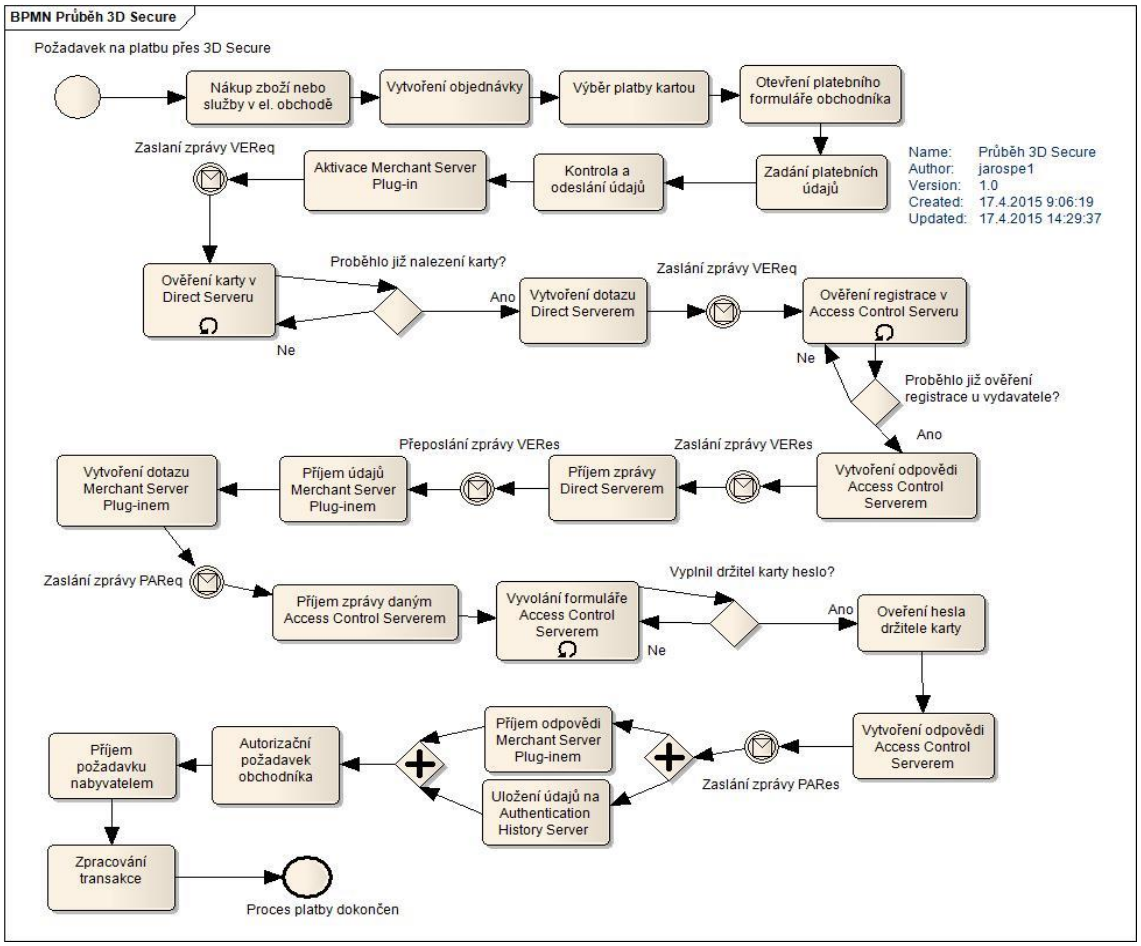
4) MPI posílá žádost autentizace (PAReq) do ACS pomocí prohlížeče držitele karty.

5) ACS ověří držitele karty vyvoláním autentizačního formuláře, který se zobrazí držiteli karty s žádostí o heslo či jinou metodu autentizace. Následně ACS zformátuje a digitálně podepíše autentizační odpověď (PARes). Autentizační odpověď poté vrací k MPI a některá data z odpovědi uloží na AHS.

6) Pokud MPI obdrží autentizační odpověď s úspěšným ověřením, obchodník odešle autorizační požadavek s potřebnými daty svému nabyvateli (bance obchodníka) k podání do autorizačního systému.

7) Nabyvatel (banka obchodníka) předá požadavek o platbě vydavateli (bance držitele karty) a provede se transakce (Carbonell, 2009).

Obrázek 7 - model platby 3D Secure



Zdroj: Vlastní zpracování v programu Enterprise Architect

4.2 PayPal

Celosvětově nejrozšířenější a nejznámější platebním systémem, který funguje jako elektronická peněženka (viz kapitola 3.2 Elektronická peněženka), se nazývá PayPal. V dnešní době zpracovává téměř 11,5 milionů platebních transakcí za den a má 162 000 000 aktivních účtů. Jeho dominanci potrhuje účast na 203 trzích a možnost platit ve více než 100 měnách (PayPal, Paypal Financial, 2015).

Společnost byla založena v roce 1998 a její vzestup zařídila masivní reklama, která byla kvůli organizovanému zločinu prodělečná. Podvodníci kradli identity, aby vytvářeli hromadné účty, protože každý nový uživatel dostal na účet 10 a poté 5 amerických dolarů. Dalším důležitým bodem pro společnost bylo odkoupení rozrůstající se a v dnešní době velice populární aukční síně eBay (Janů, Platební systém na internetu – 1.část, 2010).

Obrázek 8 - logo PayPal

Zdroj: AUTOR NEUVEDEN [online]. [cit. 2015-01-28]. Dostupný na WWW: http://www.underconsideration.com/brandnew/archives/paypal_2014_logo_detail.png

4.2.1 Registrace

Účet je možné vytvořit na oficiálních stránkách paypal.com, ale bohužel prozatím nemají českou jazykovou lokalizaci a českou podporu. Před registrací si uživatele vybere ze dvou základních virtuálních účtů:

- PayPal for you – obyčejný osobní účet
- PayPal for bussines – účet k firemním účelům

Následně je nutné vyplnit formulář s údaji (např. mobil, občanství, jméno, příjemní, atd.) a především emailovou adresu pro ověření a aktivaci účtu. Poté je možné přidat platební kartu s jejími náležitostmi. Pro ověření a proti zneužití platební

karty odečte PayPal z bankovního účtu částku 50 Kč (inkaso) a v přehledu transakcí vygeneruje čtyřmístný kód, který se zadá v rozhraní PayPalu (Kašpárek, PayPal pro začátečníky, 2011).

Pro přesun peněz na PayPal účet si uživatel může vybrat z 3 možností. Přidání platební karty do systému patří mezi způsoby nabití účtu. Uživatel zadá údaje platební karty do systému a následně se platby hradí přímo z ní. Základem druhého způsobu je převod peněz z běžného účtu. Při převodu peněz, nesmí uživatel zapomenout zadat své TransferID do poznámky platebního příkazu a bankovní účet musí být veden na jméno uživatele PayPal. Poslední možností pro uživatele, jak dobít účet, je využití tzv. prostředníka. Jedná se o službu, která umožňuje uživatelům okamžité dobití účtu z vlastního elektronického bankovnictví. Tento způsob podporuje například platební brána TrustPay.

4.2.2 Bezpečnostní prvky

Platební systém PayPal využívá bezpečné šifrování citlivých údajů uživatelů při komunikaci pomocí technologie SSL. PayPal podporuje bezpečnostní protokol 3D Secure pro bezpečnou manipulaci s údaji platební karty. Podobně jako u všech platebních systémů využívající k přihlášení hesla, je nutné dodržet bezpečnostní politiku hesel a pravidelně heslo obměňovat.

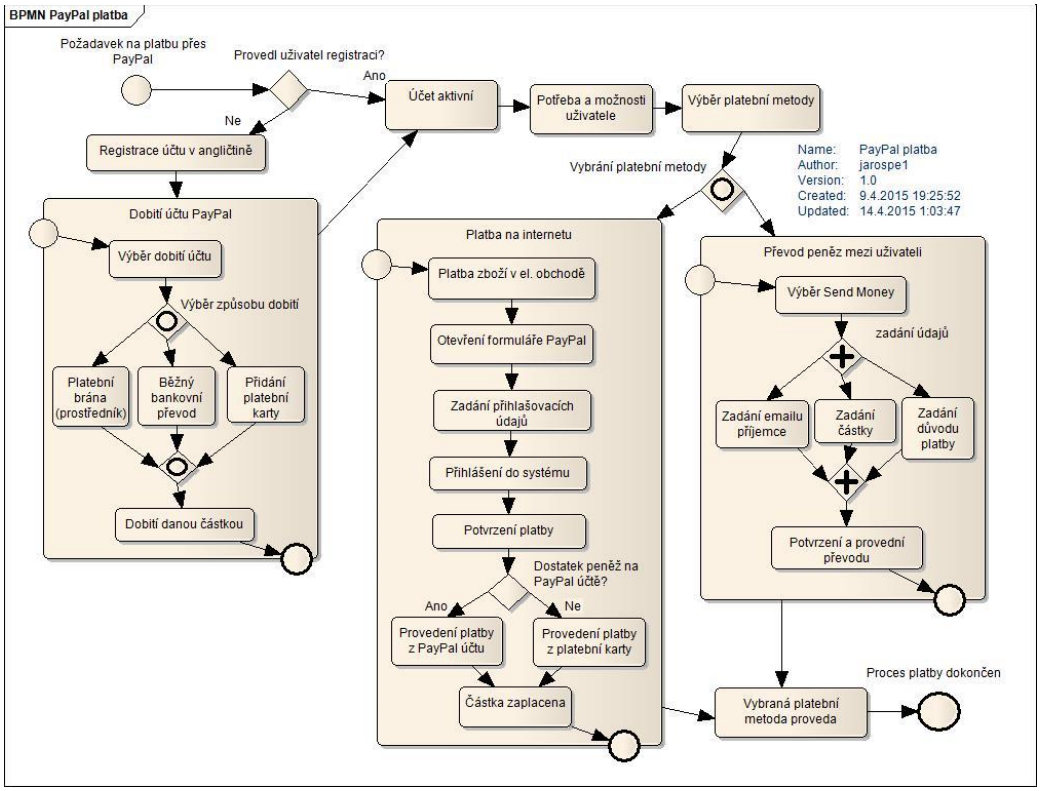
4.2.3 Platba

Výhodou platebního systému PayPal je možnost převádět české koruny na libovolnou podporovanou měnu a provádět tak platby v zahraničí. Vybrané platební metody:

- Platba na internetu - Při výběru platby v internetovém obchodě prostřednictvím PayPal, webová stránka přesměruje uživatele na formulář pro zadání uživatelských údajů. V konečné fázi uživatel odsouhlasí požadovanou částku a platba se provede z PayPal účtu nebo případně z platební karty. Odkud se provede platba požadované částky, závisí na zůstatku na PayPal účtu.

- Poslaní peněz uživateli – Při výběru záložky Send Money, která se nachází v menu systému, se zobrazí formulář pro zaslání peněz. Uživatel musí zadat emailovou adresu příjemce, částku, měnu a důvod uhrazení částky. V konečné fázi zadané údaje uživatel potvrdí a proběhne převod. Průběh je zachycen v následujícím modelu, viz Obrázek 9.

Obrázek 9 - procesy platebních metod PayPal



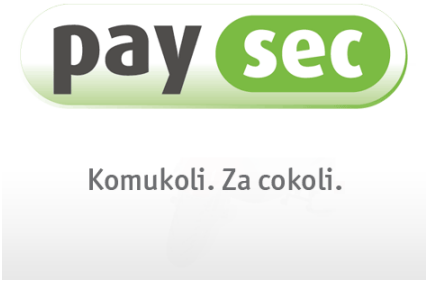
Zdroj: Vlastní zpracování v programu Enterprise Architect

4.3 PaySec

Český zástupce na trhu elektronických peněženek, který funguje na podobném principu jako PayPal, se nazývá PaySec. Platební brána s elektronickou peněženkou byla spuštěna v roce 2008 a jeho provoz zajišťuje Československá obchodní banka (ČSOB) ve spolupráci s Poštovní spořitelnou. Největší výhodou oproti popisovanému PayPalu je především česká lokalizace a česká legislativa. Podstatný rozdíl mezi těmito systémy, je v tom, že Paysec neumožňuje propojení s platební kartou, respektive úhradu částky přímo z bankovního účtu. Funguje tedy klasicky na předplaceném principu a úhrady se realizují pouze z finančních

prostředků na PaySec účtu uvnitř systému (Macich ml., PaySec aneb PayPal po česku, 2008).

Obrázek 10 - logo PaySec



Zdroj: AUTOR NEUVEDEN [online]. [cit. 2015-01-28]. Dostupný na WWW: https://www.erasvet.cz/pravnicke-osoby/platby-pro-obchodniky

4.3.1 Registrace

Založení probíhá na oficiálních stránkách vyplněním formuláře požadovanými údaji. Webové stránky jsou na dnešní poměry zastaralé. Mezi požadované údaje patří přihlašovací jméno, heslo, kontrolní otázka a ověřovací kód. Aktivace účtu se provádí pomocí emailového a SMS kódu. Účet pro obchodníky je nutné ověřit a podepsat osobně na pobočce spořitelny nebo provozovatele. Před registrací účtu si musí tedy uživatel vybrat typ, jestli si přeje osobní účet - Konto Paysec nebo obchodní účet - Konto pro obchodníky. Konto je možné dobít bez poplatku bankovním převodem nebo platební kartou s 2% poplatkem, který se odečítá přímo z nabité částky. (PaySec, PaySec – Nejčastější otázky, 2015).

4.3.2 Bezpečnostní prvky

Platební systém PaySec při nabití konta platební kartou využívá bezpečnostní protokol 3D Secure implementovaný v platební bráně PayMuzo a při nabití konta prostřednictvím bankovního převodu závisí na bezpečnostních podmínkách internetových bankovnictví konkrétní banky. Při komunikaci mezi účastníky využívá 128 bitové šifrování využitím technologie SSL.

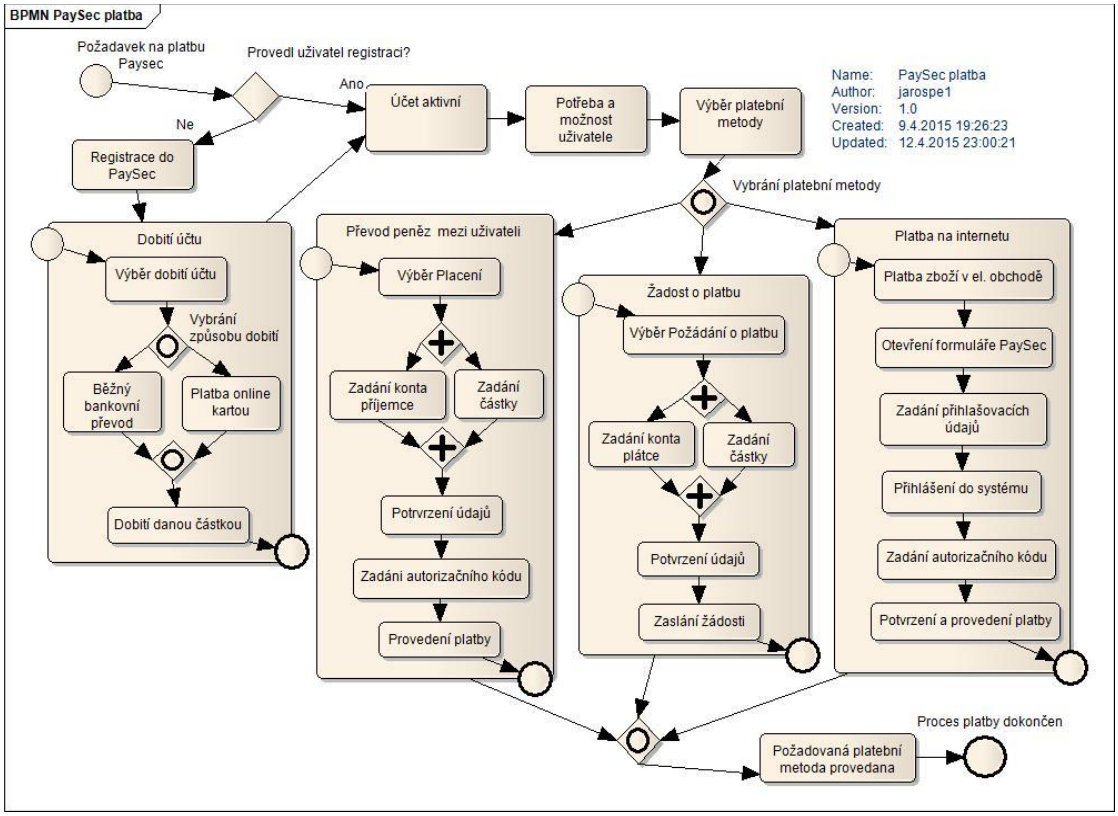
4.3.3 Platba

Platba je limitována úrovní ověření. Pokud uživatel nabije konto částkou větší než 58 000 Kč a vybije částkou větší než 23 000 Kč, musí provést ověření

v Poštovní spořitelně nebo na poště. Platební metody brány využívá pouze obchodní účet. Vybrané platební metody:

- Platba mezi uživateli – V platebním systému uživatel vybere v menu záložku „Placení“. Uživatel následně zadá konto příjemce a peněžní částku. V konečné fázi uživatel obdrží ověřovací SMS s kódem, který opíše a platbu po kontrole údajů potvrdí. Systém dovoluje provádět hromadné platby opakovaným přidáváním příjemce a částky.
- Žádost o platbu – V platebním systému uživatel vybere v menu záložku „Požádání o platbu“. Uživatel následně vybere účet plátce a požadovanou peněžení částku. V konečné fázi uživatel zadá znaky z ověřovacího obrázku a po kontrole údajů požadavek potvrdí. Systém opět dovoluje provádět hromadné žádosti o platbu.
- Platba na internetu – Při výběru způsobu platby v internetovém obchodě prostřednictvím elektronické peněženky PaySec, je uživatel přesměrován na platební formulář, kde vyplní své uživatelské jméno a heslo. V konečné fázi údaje o platbě zkontroluje a potvrdí autorizačním kódem, viz Obrázek 11.

Obrázek 11 – procesy vybraných platebních metod PaySec



Zdroj: Vlastní zpracování v programu Enterprise Architect

4.4 GoPay

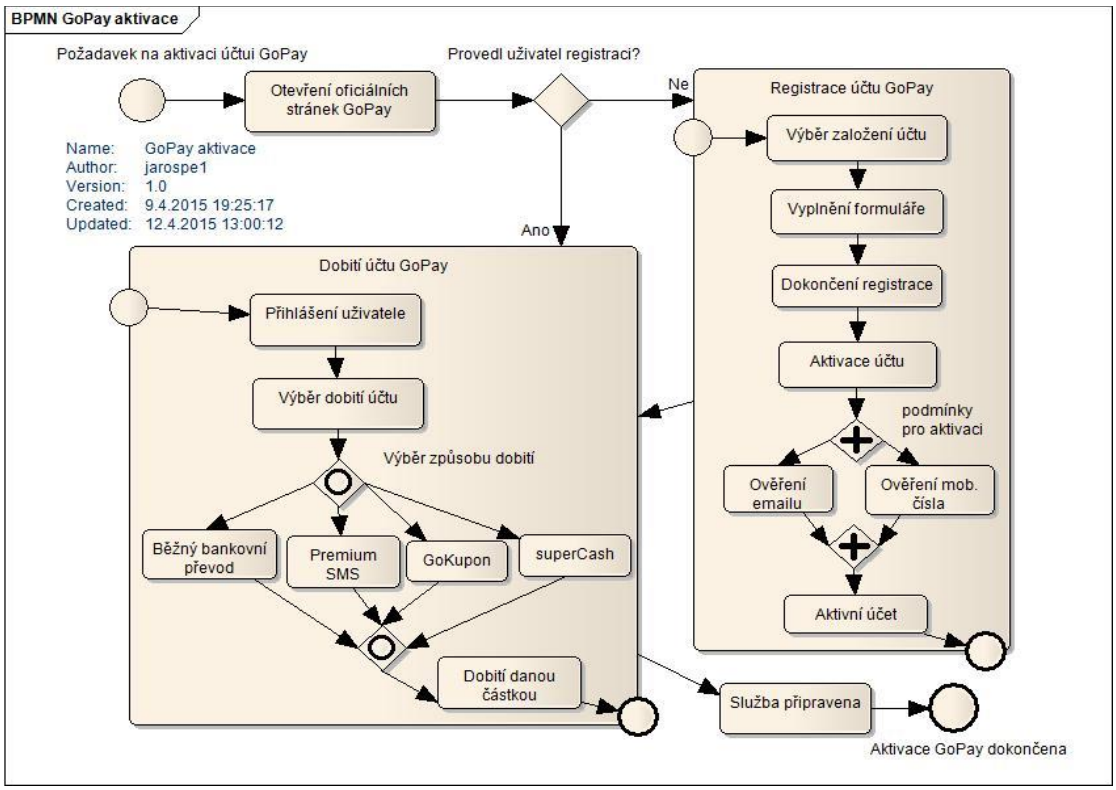
Mezi další české platební systémy patří GoPay. Společnost GoPay neprovozuje pouze elektronickou peněženku, ale také platební bránu, která centralizuje nejpoužívanější platební metody u nás a na slovenském trhu do jednotného uživatelského rozhraní. Platební brána má partnerství již s více než 3000 internetovými obchody. Platební systém je provozovaný od roku 2008 společností Gopay s.r.o. (GoPay, Naše historie, 2015).

4.4.1 Registrace

Založení uživatelského účtu a vedení účtu je zdarma jako ve většině platebních bran. GoPay účet lze vytvořit na oficiálních stránkách vyplněním jednoduchého formuláře. Mezi identifikátory GoPay účtu patří emailová adresa a GoID. Po registraci účtu může uživatel pouze přijímat platby, protože je účet neaktivní. Aktivace účtu se opět provádí pomocí emailového a SMS kódu. GoPay účet

zahrnuje různé druhy úrovně identifikace. Například pro částečně ověřenou úroveň, systém požaduje navýšit zůstatek GoPay účtu, zasláním malé částky z bankovního účtu. GoPay umožňuje založení obchodního účtu (GoPay, Jak založit GoPay účet?, 2015). GoPay účet je možné dobít například běžným bankovním převodem, Premium SMS, superCash nebo Gokuponem, viz Obrázek 12.

Obrázek 12 - aktivace účtu GoPay



Zdroj: Vlastní zpracování v programu Enterprise Architect

4.4.2 Bezpečnostní prvky

Při procesu platby jsou všechny informace komunikujících účastníků šifrované 128 bitovou technologii SSL/TSL. GoPay tedy využívá pro webové stránky síťový protokol HTTPS a digitální certifikát. Při platbě kartou využívá bezpečnostní protokol 3D Secure (GoPay, Bezpečnost platební brány, 2015).

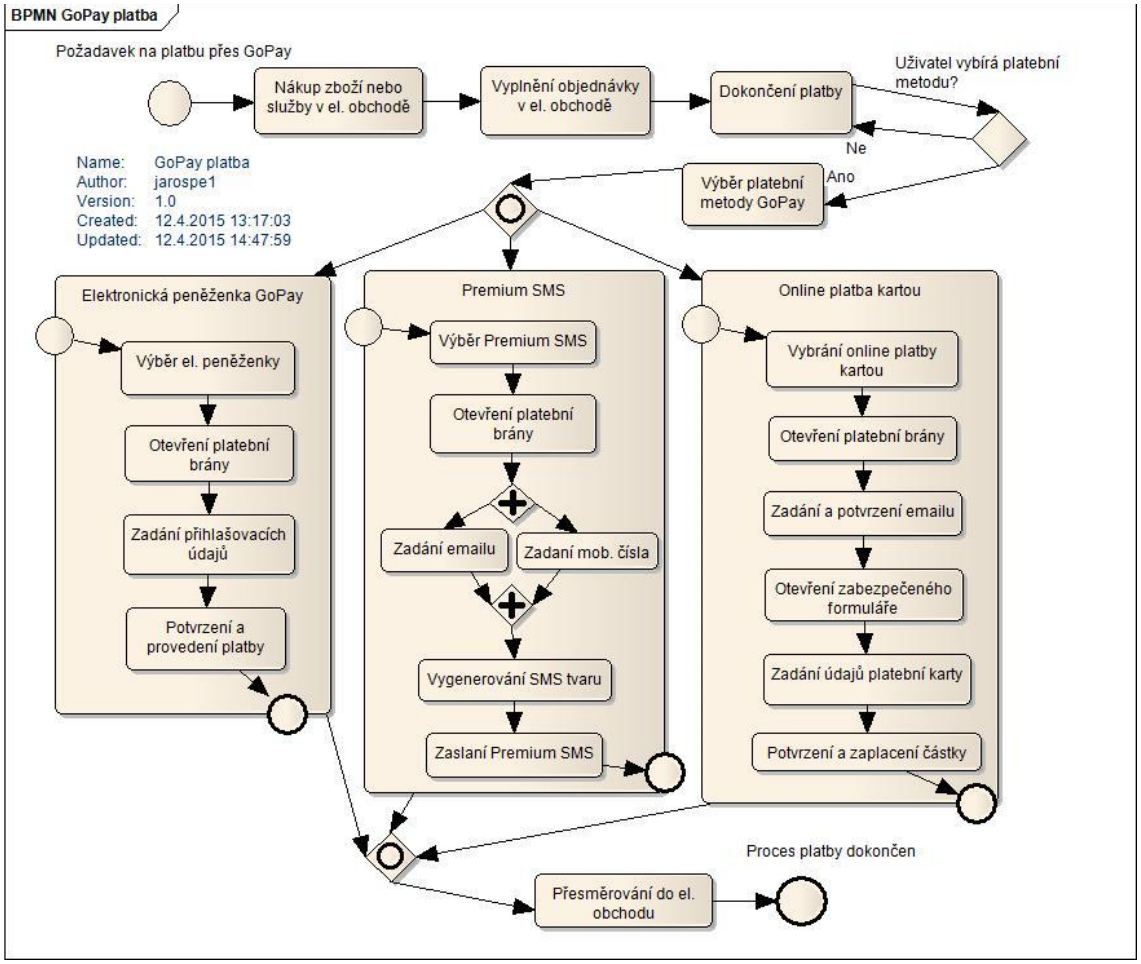
4.4.3 Platba

Klient po dokončení objednávky v internetovém obchodě vybere způsob úhrady částky výběrem platební brány GoPay. Protože se jedná o platební bránu,

tak nabízí různé druhy platebních metod, viz Obrázek 13. Vybrané podporované platební metody:

- Elektronická peněženka (účet) GoPay – Při výběru platby GoPay peněženkou je uživatel přesměrován na platební bránu, kde zadá emailovou adresu nebo GoID a potvrzením částku uhradí. Po dokončení platby je uživatel přesměrován zpět do internetového obchodu.
- Online platba kartou – Při výběru platby kartou proběhne opět přesměrování na platební bránu, kde uživatel zadá a odsouhlasí svoji emailovou adresu. V další fázi proběhne přesměrování na formulář konkrétní banky nebo GoPay. Do formuláře je nutné zadat číslo karty, expiraci karty, CVC2 a následně platbu potvrdit.
- Bankovní převod – Při výběru převodu na účet proběhne přesměrování na platební bránu, kde uživatel vybere a potvrdí banku, ze které chce provádět platbu. V další fázi procesu se zobrazí vygenerovaný platební příkaz, který je možné stáhnout ve formátu PDF, či provést převod ve svém internetovém bankovnictví.
- Premium SMS – Při výběru platby přes Premium SMS proběhne přesměrování na platební bránu, kde uživatel zadá a potvrdí emailovou adresu a telefonní číslo. V další fázi proběhne vygenerování tvaru SMS zprávy, kterou uživatel odešle na uvedené telefonní číslo. Pokud je částka vyšší než 100 Kč, musí uživatel zaslat ověřovací SMS.

Obrázek 13 - procesy vybraných platebních metod GoPay



Zdroj: Vlastní zpracování v programu Enterprise Architect

4.5 PayU

Platební brána PayU patří mezi nejrychleji rostoucí platební systémy v České republice. PayU začal fungovat v Evropě už v roce 2005 a nejdéle funguje v Polsku s více než 2000 internetovými obchody. V České republice byla společnost PayU Czech republic, s.r.o. založena vyspělou mezinárodní společností Naspers v roce 2011. PayU sdružuje nepoužívanější platební metody v České republice. Služeb PayU využívá například Heureka.cz nebo Aukro.cz (PayU, O PayU, 2015). S platební bránou spolupracují také finanční instituce jako například Česká spořitelna, Raiffeisenbank, Komerční banka, mBank, Sberbank, Fio banka, GE Money Bank a platební karty VISA a MasterCard.

Obrázek 14 - logo PayU

Zdroj: AUTOR NEUVEDEN [online]. [cit. 2015-01-29]. Dostupný na WWW: http://www.payu.cz/ke-stazeni

4.5.1 Registrace

Platební brána PayU se od ostatních systémů liší tím, že klient nepotřebuje a ani nevytváří žádný účet v systému. Pro využití platební brány je podmínkou, aby vybraný internetový obchod podporoval PayU při výběru způsobu platby zboží. Proto účet musí vytvářet pouze obchodník, který chce ve svém internetovém obchodě využít tuto platební bránu. Obchodník musí ověřit svoji totožnost osobně na pobočce.

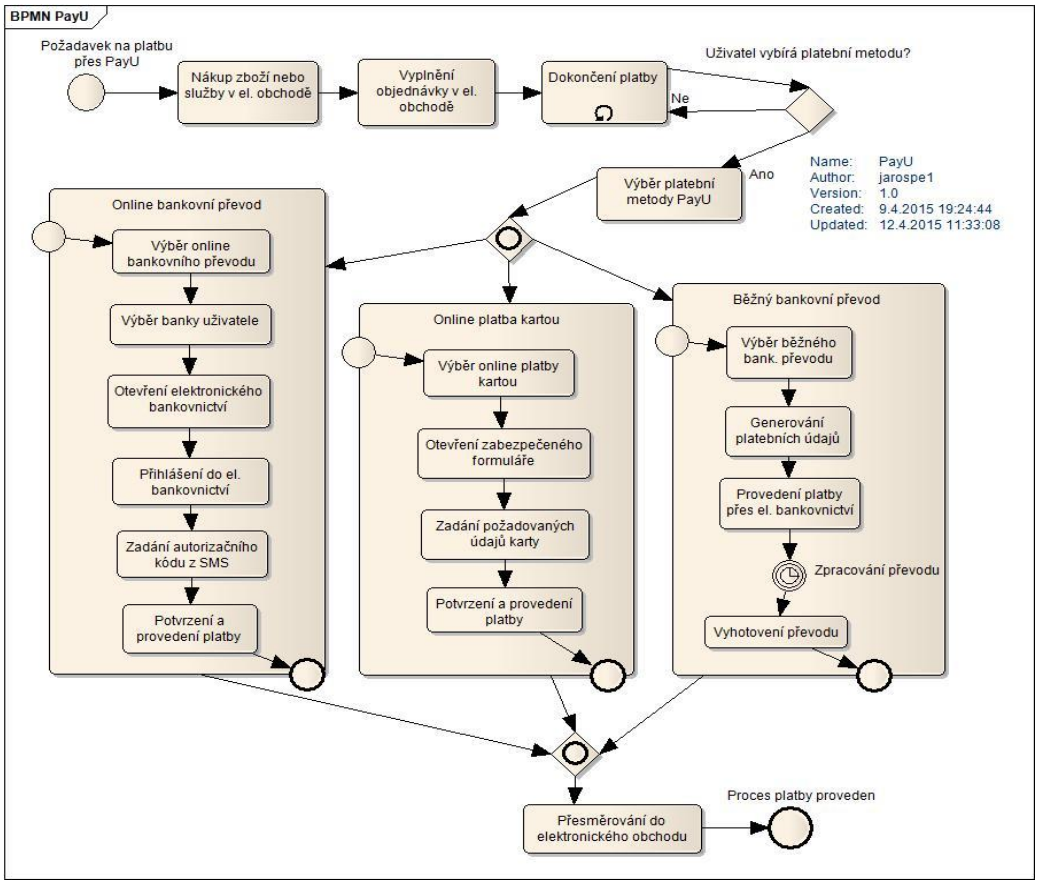
4.5.2 Bezpečnostní prvky

Systém PayU v komunikaci mezi účastníky využívá bezpečnostní protokol SSl (Secure Sockets Layer) a při platbě platební kartou zabezpečuje transakci pomocí 3D Secure protokolu. Veškeré platby jsou pod záštitou licence České národní banky (PayU, Bezpečnost přes PayU, 2015). Dále závisí na bezpečnostních protokolech jednotlivých internetových bankovnictví.

4.5.3 Platba

Klient po nákupu zboží a dokončení objednávky v internetovém obchodě podporující platební bránu PayU, vybere požadovanou platební metodu. Následně se provede vybraná platební metoda a zboží se uhradí. V konečné fázi je uživatel přesměrován zpět do elektronického obchodu. Platební brána podporuje online bankovní převod konkrétní banky, platbu kartou, běžný bankovní převod, platbu poštovní poukázkou nebo elektronické peněženky PaySec a MasterCard Mobile, viz Obrázek 15. Detailněji popsané vybrané platební metody podporované PayU:

Obrázek 15 - procesy vybraných platebních metod PayU



Zdroj: Vlastní zpracování v programu Enterprise Architect

- Online bankovní převod - Pokud vybere uživatel online převod, systém ho přesměruje do jeho elektronického bankovnictví, kde zadá přístupové údaje své banky. Po přihlášení do bankovnictví stačí uživateli potvrdit předvyplněný platební příkaz autorizačním PINem a platba se dokončí. Peníze se ihned převedou na bankovní účet prodejce, který má uvedený pro službu PayU (PayU, Fungování online plateb u PayU, 2015).
- Online platba kartou - Při platbě kartou systém přesměruje uživatele na formulář pro zadání údajů platební karty. Uživatel zadá číslo karty, datum expirace a CVC2. V konečné fázi tyto údaje uživatel potvrdí a proběhne okamžitá úhrada částky (PayU, Fungování online plateb u PayU, 2015).
- Běžný bankovní převod nebo poštovní poukázka – Tento způsob platby je určen pro ostatní nespolupracující bankovní ústavy. Při výběru platby běžným bankovním převodem nebo poštovní poukázkou proběhne

vygenerování údajů pro převod peněz elektronickým bankovnictvím, případně pro vyplnění poštovní poukázky.

4.6 Mobito

Mobilním platebním systémem, který je velice podobný elektronickým peněženkám, se nazývá Mobito. Mobito je také od českých tvůrců, který se dostal na náš trh v září 2012. Zakladatelem se stala společnost MOPET CZ s cílem vytvořit nový platební standart a zakládajícími členy se staly banky Česká spořitelna, GE Money Bank, Raiffeisenbank, UniCredit Bank a mobilní operátoři O2, T-Mobile a Vodafone. (Šefl, Mobito je placení telefonem, 2013).

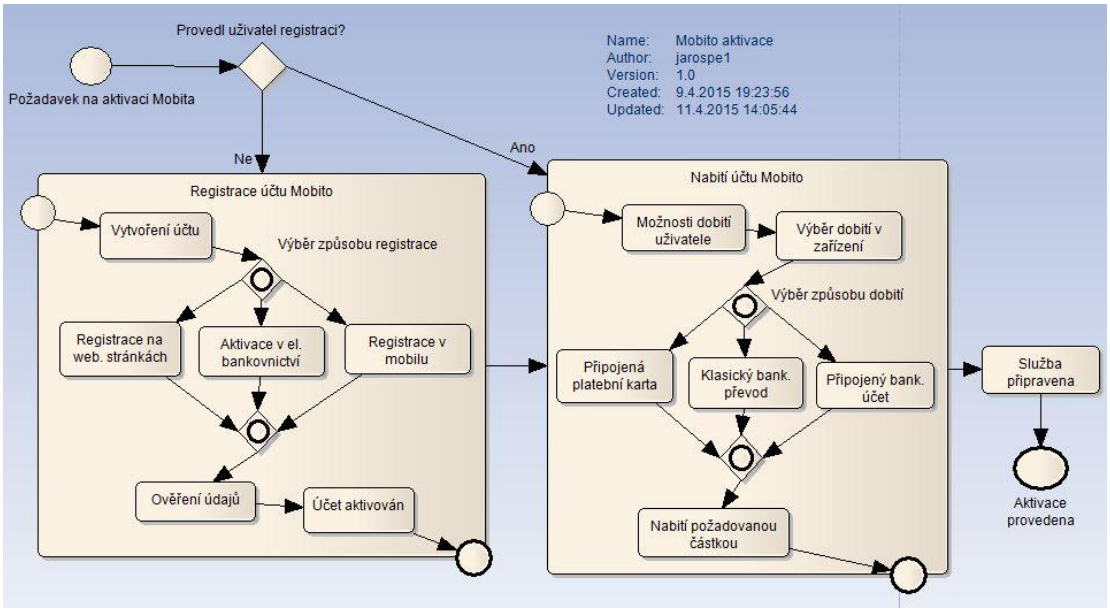
Obrázek 16 - logo Mobito

Zdroj: AUTOR NEUVEDEN [online]. [cit. 2015-01-30]. Dostupný na WWW: http://www.datart.cz/public/68/f9/27/50592_62581_mobito_logo.png

4.6.1 Registrace

Registrace účtu je opět velice snadné, stačí zadat do formuláře na stránkách mobito.cz telefonní číslo, email. Možnost aktivovat Mobito nabízejí klientům dále partnerské banky přímo v jejich elektronickém bankovnictví (Česká spořitelna, GE Money Bank, Raiffeisenbank, UniCredit Bank). Další možností je registrování služby v mobilních aplikacích Mobita, viz Obrázek 17. Mobilní aplikace se dají stáhnout pro systém iOS nebo Android. Ovládat službu umožňují i mobilní telefony podporující zprávy na displeji pomocí GSM signálu (Mobitoplatito, Jak si pořídit Mobito, 2015).

Obrázek 17 – aktivace účtu Mobita



Zdroj: Vlastní zpracování v programu Enterprise Architect

4.6.2 Bezpečnostní prvky

Bezpečnost platebního systému vychází z principu elektronických peněženek, neboli peníze v Mobitu nejsou fyzicky k dispozici, protože jsou uloženy na účtech partnerských bank. Pro vstup do prostředí Mobita i autorizaci platby se využívá PIN kód, který není přenosný mezi jiným mobilním zařízení. Veškerá komunikace v mobilní aplikaci a webovém rozhraní je šifrována síťovým protokolem HTTPS.

4.6.3 Platba

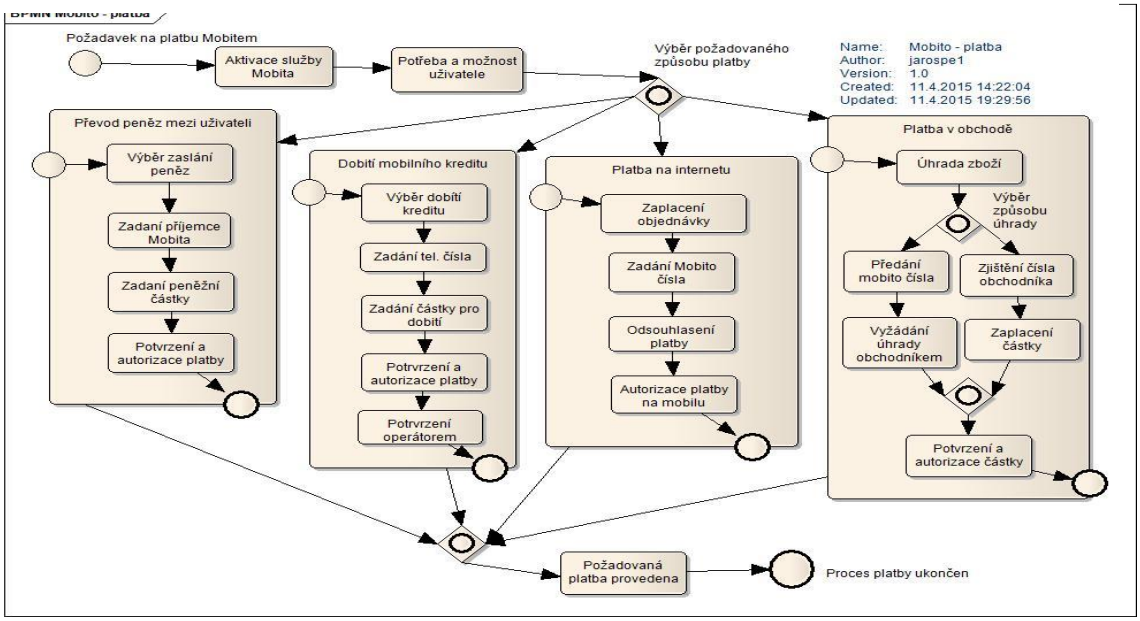
Před samotnou platbou je nutné nabít účet Mobita z mobilu pomocí bankovního účtu, připojenou platební kartou nebo klasickým bankovním převodem do 2 dnů (Příkaz k úhradě). Mobito tedy umožňuje podobně jako PayPal propojení přímo s bankovním účtem partnerských bank a provádět úhrady plateb z něho. Další způsob je stejný jako u klasické elektronické peněženky (Mobitoplatito, Peníze z banky, 2015). Mobito umožňuje různé druhy plateb primárně přes smartphone,

- Platba mezi uživateli Mobita – Proces začíná zadáním cílového telefonního čísla nebo Mobito čísla. Poté následuje zadání peněžní částky v rozmezí 1 a 10 000 Kč. V další fázi lze zvolit platbu přímo z připojeného bankovního účtu nebo platební kartou Raiffeisenbank. V konečné fázi se pomocí

autorizačního PIN kódu platba potvrdí a služba předá informace o výsledku platby.

- Dobití kreditu telefonu – Proces dobití kreditu začíná zadáním telefonního čísla pro dobití. V dalším kroku uživatel zadá požadovanou částku kreditu a autorizuje PINem. Operátor pošle potvrzující SMS o dobití kreditu.
- Platba na internetu – Proces platby na internetu začíná výběrem platebního systému Mobito při dokončení nákupu. Uživatel na webové stránce zadá pouze telefonní číslo, či Mobito číslo a následně obdrží zprávu s požadavkem na uhrazení částky. V konečné fázi platbu na mobilu opět autorizuje PINem. Informace o uhrazení částky uživatel obdrží na mobilu i webové stránce.
- Platba v obchodě – Proces platby v obchodě může být realizován podobně jako příkaz k úhradě nebo příkaz k inkasu. V prvním případě uživatel musí sdělit své telefonní nebo Mobito číslo obchodníkovi a následně obdrží požadavek na uhrazení částky, kterou autorizuje PINem. V druhém případě musí uživatel zvolit v aplikaci Zaplatit obchodníkovi a zadat jeho Mobito číslo, částku a variabilní symbol. V konečné fázi musí uživatel platbu autorizovat PINem.

Obrázek 18 - procesy platebních metod Mobita



Zdroj: Vlastní zpracování v programu Enterprise Architect

4.7 Apple Pay

Apple Pay je novým a inovativním platebním systémem americké společnosti Apple představený v září 2014, který se řadí mezi popisované mobilní platby využívající biometrické údaje (viz kapitola 3.4 Mobilní platby). Tento platební systém je podporovaný pouze výrobky Apple s NFC technologií, tedy s Apple iPhone 6, Apple iPhone 6 Plus, Watch, iPad Air 2 nebo iPad mini 3. Starší modely mohou platit prostřednictvím hodinek Watch (Apple, Apple Pay, 2015).

4.7.1 Registrace

Nastavení platebního systému probíhá v aplikaci Passbook, která již teď umožňuje ukládat palubní vstupenky, lístky a další. Představením Apple Pay dokáže aplikace načíst údaje o kreditní či debetní kartě přímo z používaného Apple účtu nebo klasickým ručním zadáním. Aplikace dále umožňuje načíst údaje zabudovaným fotoaparátem, oskenováním platební karty. V poslední fázi je nutné zadat bezpečnostní kód karty, respektive PIN a proběhne ověření správnosti zadaných údajů. Po načtení platební karty do zařízení Apple je služba připravena, viz Obrázek 19 (Apple, Apple Pay, 2015).

4.7.2 Bezpečnostní prvky

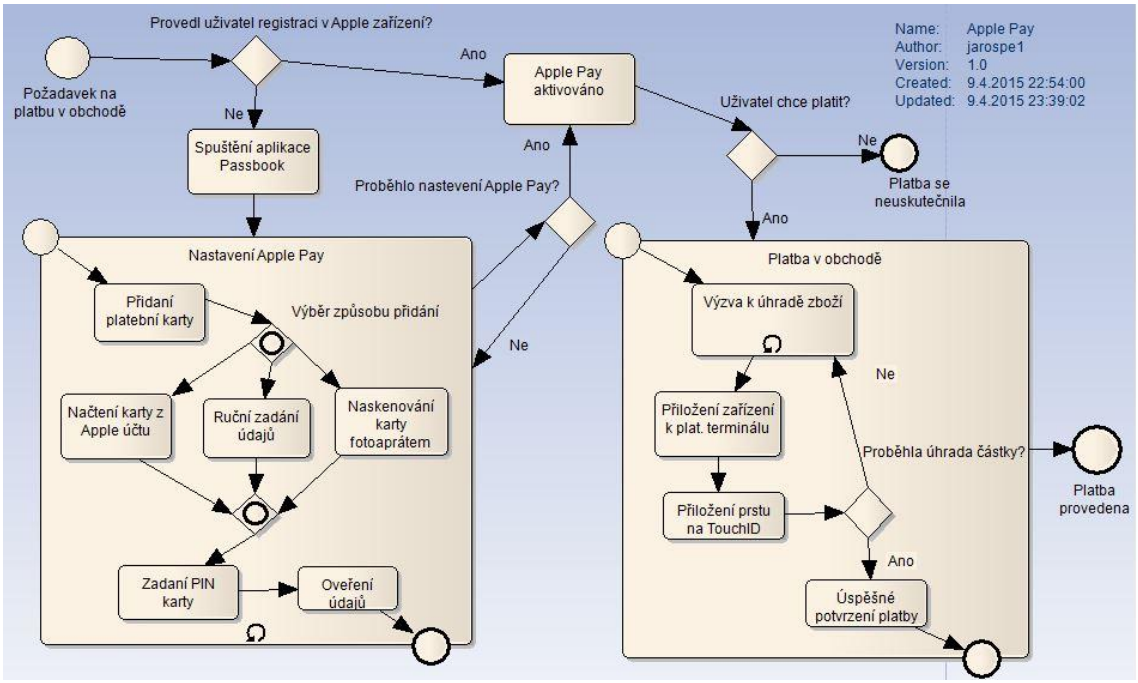
Bezpečnost plateb zaručuje především otisk prstu daného uživatele při každé platbě a přiřazení jedinečného čísla k zařízení, které je uloženo zašifrovaně ve vyhrazeném čipu tzv. Secure Elementu. Jedinečná sada čísel nahrazuje číslo účtu, datum platnosti a bezpečnostní kód. Toto jedinečné číslo se neukládá na servery Apple a není sdíleno s obchodníky nebo přenášeno v průběhu platby. Mezi výhody bezpečnostní technologie určitě tedy patří, že nevyužívá skutečné údaje kreditních nebo debetních karet a nevyžaduje žádný bezpečnostní kód (Apple, Apple Pay, 2015).

4.7.3 Platba

Platba v obchodech se uskuteční pouhým přiložením zařízení Apple s NFC čipem k platebnímu bezkontaktnímu terminálu. Uživatel mobilního zařízení je vyzván k přiložení prstu na domácí tlačítko tzv. Touch ID, které oskenuje prst a autentizuje

majitele platební karty. Platba se potvrdí a požadovaná částka se uhradí, viz Obrázek 19 (Apple, Apple Pay, 2015).

Obrázek 19 - proces platby a registrace Apple Pay



Zdroj: Vlastní zpracování v Enterprise Architect

4.8 Samsung Pay

Samsung Pay je nový platební systém jihokorejské společnosti Samsung, který byl představen v březnu 2015 a jednoznačně patří mezi přímé konkurenty platebního systému Apple Pay. Platební systém by měl být k dispozici v Evropě během léta 2015 a z počátku bude dostupný na mobilech Samsung Galaxy S6 a Samsung Galaxy Edge s operačním systémem Android a NFC technologii. Samsung Pay vznikl za spolupráce s odkoupenou společností LoopPay. Odkoupením společnosti získal Samsung její významný technologický patent, nazývaný MST (Magnetic Secure Transmission). Tento dále vysvětlený prvek výrazně odlišuje platební systém od konkurenčního Apple Pay. (Donohue, Samsung Pay Security, 2015).

4.8.1 Registrace

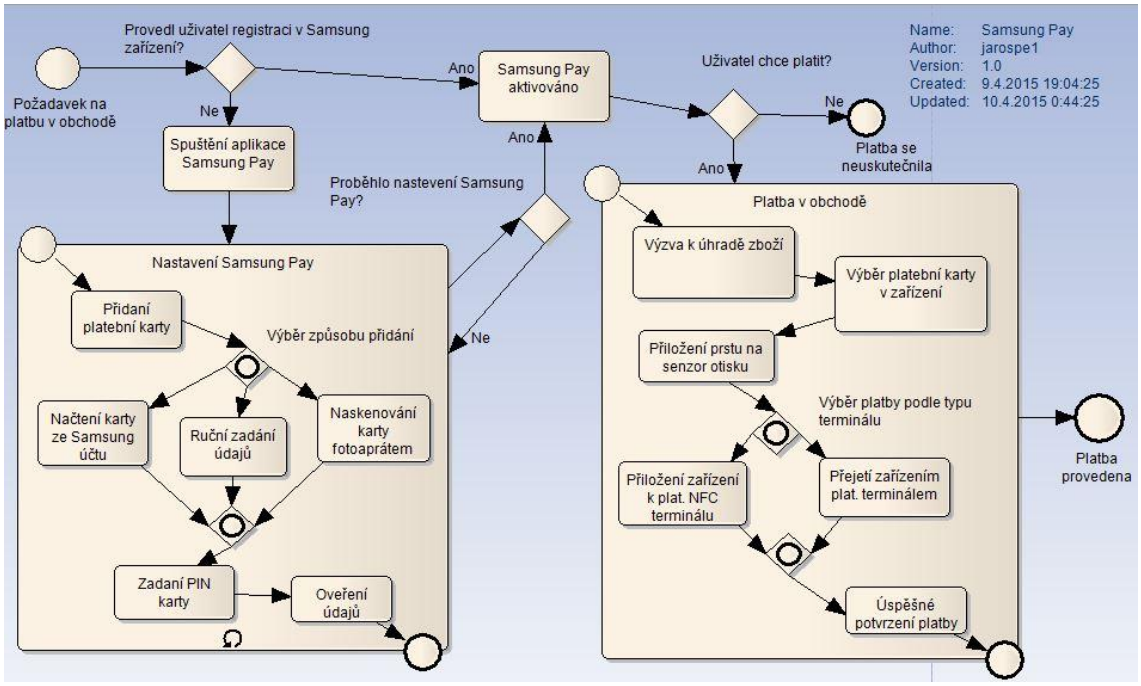
Nastavení platební služby opět probíhá prostřednictvím aplikace Samsung Pay, která načte údaje platební karty mobilní kamerou nebo tradičním ručním zadáním

požadovaných informací. V konečné fázi se musí opět zadat PIN platební karty a CVV2. Aplikace dovoluje uložit více platebních karet než pouze jednu. Po uložení platební karty a otisku prstu majitele do mobilu, se stává platební systém aktivní, viz Obrázek 20 (Samsung.uk, Samsung Announces Samsung Pay, 2015).

4.8.2 Bezpečnostní prvky

Bezpečnost plateb zajišťuje především otisk prst, provádějící se při každé platbě a stejně jako v případě Apple Pay, Samsung Pay je schopen používat technologii, která nahrazuje a šifruje 16místné číslo účtu, datum ukončení platnosti a bezpečnostní kód jedinečnou sadou čísel v průběhu platby. Dalším bezpečnostním prvkem je softwarové a hardwarové řešení nazývané Samsung Knox, které přidává Androidu bezpečností mód. Základ služby spočívá v kontrole bootovacích souborů Androidu a omezení práv spuštěných aplikací (Chroust, Samsung Knox: bezpečnost především, 2014).

Obrázek 20 - proces platby a registrace Samsung Pay



Zdroj: Vlastní zpracování v programu Enterprise Architect

4.8.3 Platba

Platba proběhne obdobným způsobem jako při použití konkurenčního systému Apple Pay. Uživatel si nejprve vybere v aplikaci Samsung Pay platební kartu, kterou potvrdí otiskem prstu a následně přiloží mobil k bezkontaktnímu platebnímu terminálu, viz Obrázek 20. Konkurenční výhodou Samsungu je patentovaná technologie nazývaná MST (Magnetic Secure Transmission), která dovoluje využívat starší platební terminály s čtečkami magnetického proužku, protože mobil dokáže emulovat (nahradit) signál magnetického proužku karty. Uživateli stačí přejet s mobilem přes čtecí hlavu terminálu a platba se potvrdí (LoopPay, Frequently Asked Questions, 2015). Některé detailnější informace o platbách Samsung prozatím nezveřejnil.

4.9 Shrnutí výsledků a doporučení

V úvodu byl modelován proces platby kartou na internetu s využitím bezpečnostního protokolu 3D Secure, který využívá většina dnešních platebních systémů pro ochranu plateb. K modelaci přispěli informace získané z článku, který se nachází v odborné databázi ScienceDirect. Únik dat ze systému obchodníka nastat nemůže, protože data nejsou u něho ukládána. Další výhodou je, že data jsou při přenosu zpráv šifrována SSL protokolem a k podvodnému zneužití zabraňují dodatečné autorizační metody. Systém však není absolutní ochranou, protože může nastat problém, pokud podvodník získá autentizační a autorizační informace. Pro případné řešení podvodů jsou autentizační pokusy při platbě ukládaný.

Prvním popisovaným platebním systémem byl PayPal, který jednoznačně patří mezi významné elektronické platební systémy současnosti. Tento platební systém spadá do oblasti elektronických peněženek. PayPal denně zpracovává miliony transakcí v 203 zemích na světě, proto z vybraných systémů nemá z hlediska počtu aktivních uživatelů konkurenci. Z mezinárodní působnosti systému vychází další výhoda a to možnost platby ve více než 100 měnách. Při registraci do systému musí uživatel zadat požadované osobní a autentizační údaje na oficiální webové stránce. Pro českého uživatele však může nastat problém, protože webové stránky nepodporují českou jazykovou lokalizaci, či českou podporu. Menší komplikaci

může způsobit při dobití účtu bankovním převodem nezadané uživatelské TransferID, protože se částka na účet nepřevede. PayPal se při platbě od klasických elektronických peněženek liší zejména v tom, že umožňuje provádět platbu přímo z připojené platební karty. Bezpečnou komunikaci se systémem standardně zajišťuje technologie SSL a využívá protokol 3D Secure. PayPal by měl zapracovat na zlepšení české jazykové podpory, protože není moc dostupných informací v rodném jazyce a chybí mu větší zastoupení v českých obchodech.

Druhým vybraným platebním systémem byl český zástupce PaySec, který se nabízenými službami opět řadí do elektronických peněženek. Největší výhodou oproti předchozímu PayPalu je především česká lokalizace. Registrace do systému probíhá na oficiálních internetových stránkách a uživatel zadává jen nutné autentizační údaje. Z vybraných platebních systému má nejhorší webovou prezentaci, protože webové stránky jsou na dnešní poměry zastaralé a nepřehledné. Podstatný rozdíl mezi PayPalem tímto systémem, je v tom, že Paysec neumožňuje propojení s platební kartou, respektive úhradu částky přímo z bankovního účtu. Platební kartou je možné účet pouze dobít s 2% poplatkem strhávající se přímo z nabité částky. Pro ochranu citlivých údajů využívá bezpečné šifrování technologii SSL. Protokol 3D Secure podporuje platební brána PayMuzu, přes kterou se může účet platební kartou dobít. Nabízené služby PaySecu se dají doporučit zejména pro platbu menších částek nebo jako první účet pro mladistvé. Bylo by vhodné zlepšit a zmodernizovat webového prostředí, protože většina důležitých informací pro uživatele je skryta v přiložených souborech. Dále by bylo vhodné přidat spárování s platební kartou.

Dalším popisovaným systémem byl český platební systém GoPay, který patří poskytovanými službami mezi platební brány. GoPay provozuje platební bránu, která centralizuje nejpoužívanější platební metody na českém a slovenském trhu do jednotného uživatelského rozhraní. Platební brána nabízí cca 22 platebních metod včetně vlastní elektronické peněženky, což je velká konkurenční výhoda. Registrace probíhá opět na oficiálních stránkách, které jsou velmi přehledně zpracované. Uživatel při registraci musí zadat jen nutné identifikační údaje, ale

vzniklý účet má další úrovně ověření. Na rozdíl od systému PaySec umožňuje nabít účet více způsoby a nabízí navíc možnost Premium SMS. Pro bezpečnost komunikujících účastníku využívá opět šifrování technologii SSL a systém podporuje protokol 3D Secure. GoPay by mohl zlepšit své služby vytvořením mobilní aplikace pro kontrolu stavu GoPay účtu, protože je uživatel odkázán na webové prostředí.

Třetím vybraným platebním nástrojem byl platební systém PayU, který patří poskytovanými službami mezi zástupce platebních bran. PayU se také zaměřuje na sdružení nejpoužívanějších platebních metod a jejich rozsah je obdobný jako v případě systému GoPay. Standardně systém podporuje online bankovní převod, platbu kartou, běžný bankovní převod, platbu poštovní poukázkou nebo elektronické peněženky. Platební brána PayU se od ostatních systémů liší tím, že klient nepotřebuje a ani nevytváří žádný účet v systému. Pro využití platební brány je nutné, aby vybraný internetový obchod podporoval PayU. Uživatel si při platbě zboží vybere pouze preferovanou platební metodu. Nevýhodou platební brány je, že nemá vlastní elektronickou peněženku. V seznamu platebních metod zahrnuje pouze elektronické peněženky PaySec a MasterCard Mobile. Systém opět využívá bezpečnostní technologii SSL a protokol 3D Secure. Systém PayU by mohl rozšířit své platební metody o vlastní elektronickou peněženku, která by nabízela propojení s platební kartou jako v případě PayPalu.

Čtvrtou vybranou platební službou byl platební systém Mobito. Mobito patří nabízenými službami mezi zástupce elektronických peněženek. Smyslem celého systému je však větší zapojení mobilního telefonu do platebního procesu, protože člověk má v dnešní době mobilní zařízení stále nadosah. Registrace účtu neprobíhá pouze na webových stránkách nebo v elektronickém bankovnictví, ale také v oficiálních mobilních aplikacích. Registrace je velmi snadná a rychlá, protože uživatel zadá pro identifikaci pouze emailovou adresu a mobilní číslo. Aby mohl uživatel použít účet k platbě, musí ho dobít preferovanou metodou. Systém nabízí výhodné propojení účtu s platební kartou podobně jako systém PayPal. Mobito například umožňuje platbu přímo v podporovaném kamenném obchodě

nebo na internetu. Podle dostupných informací chrání přenášená data protokolem HTTPS. Mobito by mohl rozšířit mobilní aplikaci na mobilní systém Windows 8, na kterém prozatím aplikace chybí. Dále systému chybí větší rozšířenost v kamenných, či internetových obchodech.

Dalším vybranou platební službou byl Apple Pay. Apple Pay patří mezi nově představené platební systémy, který kombinuje výhody spojené s mobilním telefonem a biometrickými údaji. Principem systému je načtení platební karty do telefonu a poté se veškeré platební operace provádějí s ním. Tento platební systém je podporovaný pouze výrobky Apple s NFC technologií. Starší zařízení bez podpory NFC technologie mohou platit prostřednictvím hodinek Watch. Nevýhoda pro případného zájemce o službu Apple Pay je tedy v tom, že musí vlastnit zařízení od Applu s operačním systémem iOS. Všechny důležité platební údaje jsou šifrovány a nahrazeny jedinečnou sadou čísel. Platba proběhne přiložením zařízení k bezkontaktnímu (NFC) terminálu a následným přiložením prstu na snímač otisku prstů. Nevýhodu je na rozdíl od konkurenčního systému Samsung Pay v tom, že nemůže využít i starší terminál s čtečkou magnetického proužku. Platba s využitím nových hodinek Watch přinese nový pohled na oblast plateb. Systém je prozatím k dispozici pouze v Americe, proto ho nejde otestovat v provozu v České republice.

Posledním popisovou platební službou byl systém Samsung Pay. Stejně jako přechozí systém Apple Pay byl představen minulý rok a patří tedy mezi nové trendy na trhu. Principem systému je opět načtení platební karty do mobilního telefonu, respektive vytvoření její virtuální kopie. Následně se mobilní telefon chová jako klasická platební karta. Protože se jedná o konkurenční produkt, potencionální uživatel může nabízenou službu využít pouze s mobily Samsung podporující NFC technologii. Platba probíhá obdobně jako v případě Apple Pay. Uživatel si nejprve vybere platební kartu, kterou potvrdí otiskem prstu a následně přiloží zařízení k platebnímu terminálu. Významná výhoda spočívá v patentované technologii MST, protože systém dokáže zpracovat platbu i přes

starší terminál bez NFC technologie. Systém má být spuštěn v létě 2015, proto ho nelze dostatečně prověřit.

Závěr

Cílem práce bylo zpracovat přehled a vývoj v oblasti elektronických plateb včetně aktuálně nabízených trendů s využitím nástroje pro modelování obchodních procesů. Cíl byl naplňován nejdříve popsáním teoretické části, která poté souvisela s rozborem platebních systémů v praktické části.

V úvodní kapitole byly vymezeny základní pojmy z oblasti platebního styku. Platební styk byl rozdělen podle daných hledisek a základních forem. Velký důraz byl kladen na popis formy bezhotovostního platebního styku. Velká část první kapitoly se zaměřovala na popis platební karty, protože je nástrojem pro hotovostní i bezhotovostní platební styk a je významným prvkem v elektronických platbách. Platební karta byla opět rozdělena podle různých technických hledisek a způsobů použití. Veškeré platební transakce jsou v případě bankovních služeb zpracovány danými platebními systémy, kterým byl věnován závěr kapitoly.

Další kapitola v teoretické části se zabývala popisem bezpečnostních protokolů a prvků, které zabezpečují platby v elektronických platebních systémech. Úvodem této kapitoly byly zmíněny požadavky na bezpečnost systému. Následně byly uvedeny druhy autentizačních a autorizačních metod platby. Důležitou část zahrnovalo vysvětlení bezpečnostních protokolů včetně protokolu 3D Secure, který se v dnešní době využívá pro platbu kartou na internetu. Druhou kapitolu uzavíralo představení jazyka BPMN, kterým jsou v praktické části tvořeny diagramy platebních systémů.

Ve třetí kapitole byly vysvětleny vybrané druhy elektronických platebních systémů z hlediska principu jejich fungování. Výběr systémů závisel na osobních zkušenostech a dostupných informací na internetu. Druhy systémů byly také vybírány podle nejčastějšího zastoupení na trhu. V kapitole byl definován samotný pojem elektronických platebních systémů a elektronických peněz. Poté následovali definice jednotlivých druhů systémů jako například elektronická peněženka, platební brána aj.

V poslední kapitole byly zpracovány konkrétní druhy platebních systémů na trhu. U jednotlivých systémů byly představeny obecné informace a charakteristické vlastnosti. Dostupné systémy byly prakticky vyzkoušeny nebo případně byla použita ukázková verze daného systému. Při rozboru byl kladen důraz na procesy spojené s registrací, bezpečností a platbou. Procesy se pro názornou ukázku modelovali prostřednictvím BPMN diagramů. Posledním bodem práce bylo shrnout vybrané platební systémy a případně doporučit zlepšení určité oblasti.

Nejprve byl modelován proces platby kartou na internetu s využitím bezpečnostního protokolu 3D Secure. Protokol však není absolutní ochranou, protože může nastat problém, pokud podvodník získá autentizační a autorizační informace. Mezi nevýhody patří, že musí být daným platebním systémem podporován. Prvním vybraným platebním systémem byla mezinárodní elektronická peněženka PayPal, která má výhodu v podpoře velkého množství měn a především nabízí propojení s platební kartou. Výraznou nevýhodou, která brání většímu rozšíření, je chybějící česká jazyková lokalizace a podpora. Další elektronickou peněženkou byl systém PaySec. Tento platební systém se svými službami hodí zejména pro mladistvé a pro platbu menších částek. Nevýhodou a zároveň případným zlepšením by bylo zmodernizování webového prostředí a nabídka propojení s platební kartou. Zástupcem platebních bran na trhu byl vybrán systém GoPay, který vyniká množstvím nabízených metod a vlastní elektronickou peněženkou v moderně zpracovaném prostředí. GoPay by mohl zlepšit své služby vytvořením mobilní aplikace pro kontrolu stavu GoPay účtu. Dalším zástupcem platebních bran byl vybrán systém PayU, který je velmi podobný se systémem GoPay. Platební brána PayU se od ostatních systémů liší tím, že klient nepotřebuje a ani nevytváří žádný účet v systému. Pro využití platební brány je nutné, aby ji internetový obchod podporoval. Brána by se mohla rozšířit o vlastní elektronickou peněženku. Dalším systém byl mobilní platební systém Mobito, který funguje na principu elektronické peněženky. Jako jediný ze systémů využívá k identifikaci mobilní číslo. Podobně jako Paypal nabízí výhodné propojení účtu s platební kartou. Systému chybí aplikace na mobilní operační systém

Windows. Posledními vybranými systémy byly Apple Pay a Samsung Pay. Oba dva systémy využívají NFC technologii a biometrické údaje k platbě prostřednictvím mobilního telefonu. Samsung Pay však umožňuje provádět transakce s platebními terminály bez NFC technologie. Nový trendem na trhu v oblasti plateb, je tedy přesun platebních systémů na mobilní zařízení, která člověk denně využívá.

Seznam použité literatury

Tištěné zdroje

BUDIŠ, Petr. *Elektronický podpis a jeho aplikace v praxi*. 1. vyd. Olomouc: ANAG, 2008. ISBN 978-80-7263-465-1.

ČERNOHORSKÝ, Jan a Petr TEPLÝ. *Základy financí*. 1. vyd. Praha: Grada, 2011, 304 s. ISBN 978-80-247-3669-3.

GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. *Podniková informatika. 2*., přeprac. a aktualiz. vyd. Praha: Grada, 2009, 496 s. ISBN 978-80-247-2615-1.

JÍLEK, Josef. Finance v globální ekonomice I: Peníze a platební styk. 1. vyd. Praha: Grada, 2013, 660 s. Finanční trhy a instituce. ISBN 978-80-247-3893-2.

JUŘÍK, Pavel. *Encyklopedie platebních karet: historie, současnost a budoucnost peněz a platebních karet*. 1. vyd. Praha: Grada, 2003, 312 s. ISBN 80-247-0685-7.

KANISOVÁ, Hana a Miroslav MÜLLER. *UML srozumitelně. 2.*, aktualiz. vyd. Brno: Computer Press, 2006, 176 s. ISBN 80-251-1083-4.

MÁČE, Miroslav. *Platební styk: klasický a elektronický.* 1. vyd. Praha: Grada, 2006, 220 s. ISBN 80-247-1725-5.

MATYÁŠ, Vašek a Jan KRHOVJÁK. *Autentizace uživatelů a autorizace elektronických transakcí: příručka managera*. Vyd. 1. Praha: Tate International, c2007, 318 s. Příručka manažera, 8. ISBN 978-808-6813-141.

PAVELKA, Tomáš. *Makroekonomie: základní kurz*. 2. vyd. Praha: Melandrium, 2007, 278 s. ISBN 978-808-6175-522.

POLOUČEK, Stanislav. *Bankovnictví*. 2. vyd. V Praze: C.H. Beck, 2013, xvi, 480 s. Beckovy ekonomické učebnice. ISBN 978-80-7400-491-9.

PŘÁDKA, Michal a Jan KALA. *Elektronické bankovnictví: rady a tipy : vše o používání karet, banka po telefonu a v počítači, je to opravdu bezpečné, pohledy do zákulisí - jak to dělá banka, co nás čeká zítra?, praktické informace pro všechny případy.* Vyd. 1. Praha: Computer Press, 2000, xii, 166 s. Praxe manažera. ISBN 80-722-6328-5.

SCHLOSSBERGER, Otakar. *Platební služby*. Vyd. 1. Praha: Management Press, 2012, 325 s. ISBN 978-80-7261-238-

Internetové zdroje

APPLE. *Apple pay* [online]. [cit. 2015-04-02]. Dostupné z: https://www.apple.com/apple-pay/.

BERÁNEK, LADISLAV. *Bezpečnost online systémů a platebních systémů*. Podnikání a obchodování na internetu [online]. [cit. 2015-01-22]. Dostupné z:http://ecom.ef.jcu.cz/web/download/teorie/p06-bezpecnost.pdf.

CARBONELL, Mildrey, José María SIERRA a Javier LOPEZ. *Secure multiparty payment with an intermediary entity* [online]. Elsevier, July 2009, roč. 28, č. 5 [cit. 2015-04-17]. ISSN 0167-4048. Dostupné z: http://www.sciencedirect.com/science/article/pii/S0167404808001351

ČERMÁK, Miroslav. Autentizace: zasuň token. Cleverandsmart.cz [online]. [cit. 2015-01-22]. Dostupné z:http://www.cleverandsmart.cz/autentizace-zasun-token/.

DONOHUE, Brian. Kaspersky.blog. *Samsung Pay Security* [online]. [cit. 2015-04-02]. Dostupné z: http://blog.kaspersky.com/samsung-pay-security/.

EASYSHOP. *Platební agregátory ulehčí a urychlí nákup* [online]. [cit. 2015-04-09]. Dostupné z: http://www.easy-shop.cz/platebni-agregatory-brany-ulehci-a-urychli-nakup/#.VSWZ9PmsXww.

GOPAY. *Bezpečnost platební brány* [online]. [cit. 2015-04-04]. Dostupné z: http://help.gopay.com/cs/tema/bezpecnost/bezpecnost-platebni-brany.

GOPAY. *Jak založit GoPay účet?* [online]. [cit. 2015-04-04]. Dostupné z: http://help.gopay.com/cs/tema/gopay-ucet/gopay-uzivatelsky-ucet/administrace-a-navody-uzivatelsky-ucet/jak-zalozit-gopay-ucet.

GPWEBPAY. *Bezpečnost* [online]. [cit. 2015-04-16]. Dostupné z: http://gpwebpay.cz/Security.

GOPAY. *Naše historie* [online]. [cit. 2015-04-04]. Dostupné z: http://www.gopay.com/cs/o-nas.

CHROUST, Martin. Mobilmania. *Samsung KNOX: bezpečnost především* [online]. [cit. 2015-04-02]. Dostupné z:http://samsungmania.mobilmania.cz/clanky/samsung-knox-bezpecnost-predevsim-recenze/uvod-bezpecnost-androidu-popis-knoxu/sc-309-a-1325928-ch-1061166#articleStart.

JANŮ, Stanislav. *Platební systém na internetu - 1. část*. Netzin.cz [online]. [cit. 2015-01-26]. Dostupné z: http://www.netzin.cz/platebni-systemy-na-internetu-1-cast.

JUŘÍK, Pavel. *Jak platit bezpečně i na internetu*. Finance.idnes.cz [online]. [cit. 2015-01-24]. Dostupné z: http://finance.idnes.cz/jak-platit-bezpecne-i-na-internetu-drx-/karty.aspx?c=A050727_140957_fi_osobni_zal.

KALABIS, Zbyněk. Jak funguje platební styk mezi státy Evropské unie?. [online]. [cit. 2015-01-20]. Dostupné z: http://www.mesec.cz/clanky/jak-funguje-platebni-styk-mezi-staty-evropske-unie/.

KARTAVMOBILU. *NFC platby obecně*. [online]. [cit. 2015-01-27]. Dostupné z: http://www.kartavmobilu.cz/info.php.

KAŠPÁREK, Michal. *PayPal pro začátečníky. Jak platit (a být placeni) nejoblíbenější virtuální peněženkou*. *Peníze.cz* [online]. [cit. 2015-01-26]. Dostupné z: http://www.penize.cz/nakupy/225341-paypal-pro-zacatecniky-jak-platit-a-byt-placeni-nejoblibenejsi-virtualni-penezenkou.

KUNDEROVÁ, Ludmila. *Bezpečnost komunikačních procesů*. [online]. [cit. 2015-01-23]. Dostupné z: https://akela.mendelu.cz/~lidak/bis/11prot.htm.

KYSELA, Jiří. *Mobilní komerce a elektronické platby* [online]. [cit. 2015-01-25]. Dostupné z:http://www.internetprovsechny.cz/mobilni-komerce-a-elektronicke-platby/

LOOPPAY. *Frequently Asked Questions* [online]. [cit. 2015-04-02]. Dostupné z: http://www.looppay.com/faqs/

MACICH ML., Jiří. *PaySec aneb PayPal po česku*. Lupa.cz [online]. [cit. 2015-01-26]. Dostupné z: http://www.lupa.cz/clanky/paysec-aneb-paypal-po-cesku/.

MASTERCARD. *Bezkontaktní platební karty budoucnosti mají integrované čidlo na otisk prstu*. Investujeme.cz [online]. [cit. 2015-01-22]. Dostupné z: http://www.investujeme.cz/bezkontaktni-platebni-karty-budoucnosti-maji-integrovane-cidlo-na-otisk-prstu/.

MASTERCARD. *Jak probíhá platba kartou*. [online]. [cit. 2014-07-01]. Dostupné z: https://www.mastercard.com/cz/jak-probiha-platba-kartou.html.

MOBITOPLATITO. *Jak si pořídit Mobito*. [online]. [cit. 2015-01-27]. Dostupné z: https://www.mobitoplatito.cz/vse-o-mobitu/ovladani-mobita/.

MOBITOPLATITO. *Peníze z banky*. [online]. [cit. 2015-01-27]. Dostupné z: https://www.mobitoplatito.cz/vse-o-mobitu/penize-z-banky/.

NFCTECH. *Co je NFC?.* [online]. [cit. 2015-01-27]. Dostupné z: http://www.nfctech.cz/co-je-nfc/.

PIJÁK, Michal. *Elektronické platební systémy*. [Online] [cit. 2015-01-24.] Dostupné z: http://www.fi.muni.cz/usr/staudek/vyuka/security/e_payment/.

PLATMOBILEM. *Zpoplatněné SMS (Premium SMS).* [online]. [cit. 2015-01-27]. Dostupné z: http://www.platmobilem.cz/pro-verejnost/premium-sms/co-to-jsou-premiove-sms.

PAYPAL. *Paypal Financials* [online]. [cit. 2015-01-26]. Dostupné z: https://www.paypal-media.com/about.

PAYSEC. *PaySec - Nejčastější otázky* [online]. [cit. 2015-04-04]. Dostupné z: https://www.paysec.cz/CmsPage.aspx?id=faq#payments.

PAYU. *Bezpečnost přes PayU*. [online]. [cit. 2015-01-26]. Dostupné z: http://www.payu.cz/zabezpeceni-line-plateb.

PAYU. *Fungování online plateb u PayU*. [online]. [cit. 2015-01-26]. Dostupné z: http://www.payu.cz/jak-funguji-line-platby.

PAYU. *O PayU*. [online]. [cit. 2015-01-26]. Dostupné z: http://www.payu.cz/o-payu.

RAIFFEISENBANK. *3D Secure – Plaťte kartou na internetu bezpečně a bez obav*. [online]. [cit. 2015-01-24]. Dostupné z: https://www.rb.cz/attachements/pdf/osobni-finance/kreditni-karty/3d-secure-factsheet.pdf.

SAMSUNG.UK. *Samsung Announces Samsung Pay, a Groundbreaking Mobile Payment Service* [online]. [cit. 2015-04-02]. Dostupné z:http://www.samsung.com/uk/news/local/samsung-announces-samsung-pay-a-groundbreaking-mobile-payment-service

SECURITY-PORTAL. *Protokoly pro elektronické platební systémy*. [online]. [cit. 2015-01-23]. Dostupné z: http://www.security-portal.cz/clanky/protokoly-pro-elektronick%C3%A9-platebn%C3%AD-syst%C3%A9my.

SHOPCENTRIK. *Elektronická peněženka*. [online]. [cit. 2015-01-25]. Dostupné z: http://www.shopcentrik.cz/slovnik/elektronicka-penezenka.aspx.

SSL-CERTIFÁTY. *SSL protokol*. [online]. [cit. 2015-01-24]. Dostupné z: https://www.ssl-certifikaty.cz/o-certifikatech/ssl-protokol/.

ŠEFL, Dominik. *Mobito je placení telefonem*. Jablíčkář [online]. [cit. 2015-01-27]. Dostupné z: http://jablickar.cz/mobito-je-placeni-telefonem/.

ŠTĚPÁNEK, Jiří. *Online platební systémy v České Republice a výběr vhodné varianty pro internetový obchod* [online]. Praha, 2012 [citováno 2015-01-25]. Bakalářská

práce. Vysoká škola ekonomická v Praze. Vedoucí práce Václav Šubrta. Dostupné z: http://info.sks.cz/www/zavprace/soubory/68440.pdf.

VACHTOVÁ, Jitka. Platební styk mezibankovní a klientský. [online]. [cit. 2015-01-21]. Dostupné z: http://vachtova.cz/article/show/215.

Seznam obrázků

Seznam tabulek

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

Zadání k závěrečné práci

Jméno a příjmení studenta: **Petr Jaroš**

Obor studia: Informační management (3)
Jméno a příjmení vedoucího práce: **Ivan Soukal**

Název práce:
Moderní elektronické platební nástroje

Název práce v AJ:
Modern electronic payment instruments

Podtitul práce:

Podtitul práce v AJ:

Cíl práce: Cílem práce je zpracovat přehled a vývoj v oblasti elektronických plateb včetně aktuálních trendů s využitím modelování metodou BPM.

Osnova práce:
1. Úvod
2. Platební systémy
3. Bezpečnostní protokoly a prvky
4. Situace na trhu
5. Funkčnost a bezpečnost vybraných služeb
6. Závěr

Projednáno dne: 15. 10. 2014

Podpis studenta Jaroš

Podpis vedoucího práce