VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

BEZPEČNOST ELEKTRONICKÉHO BANKOVNICTVÍ
ELECTRONIC BANKING SECURITY

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR
Tomáš Tomko

VEDOUCÍ PRÁCE
SUPERVISOR
doc. Ing. Václav Zeman, Ph.D.

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Tomáš Tomko ***ID:*** 203177

Ročník: 3 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Bezpečnost elektronického bankovnictví

POKYNY PRO VYPRACOVÁNÍ:

Práce je zaměřena na rozbor a popis technik, které se využívají v elektronickém bankovnictví. Prostudujte a stručně popište technologie využívané pro elektronický převod transakcí a infrastrukturu, která je k převodu využívána. Proveďte srovnání z hlediska uživatele, bezpečnosti a použitých kryptografických prostředků. Na základě uvedeného rozboru navrhněte a realizujte aplikaci, která bude demonstrovat funkci elektronického bankovnictví.

DOPORUČENÁ LITERATURA:

[1] MATYÁŠ , V. a J. KRHOVJÁK. Autorizace elektronických transakcí a autentizace dat i uživatelů . Brno: Masarykova univerzita, 2008. ISBN 978-80-210-4556-9.

[2] MÁČE, M.: Platební styk: klasický a elektronický. Grada Publishing, a.s., Praha 2006. Vydání 1., 220 stran. ISBN 80-247-1725-5.

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 8.6.2020

Vedoucí práce: doc. Ing. Václav Zeman, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Cieľom bakalárskej práce „Bezpečnosť elektronického bankovníctva“ je charakterizovať platobné elektronické služby a možnosti ich realizácie a tiež komparácia ponúk bankových platobných služieb s cieľom poukázať a upozorniť na ich bezpečnosť a riziká spojené s tým. Táto práca sa najskôr venuje vysvetleniu základných pojmov súvisiacich s danou problematikou, potom je spísaná aktuálna dostupná právna úprava tohoto odvetvia predovšetkým v Českej republike. Ďalej sa zaoberá jednotlivými formami elektronického bankovníctva a ich podrobnejším popisom. Jedna celá kapitola je venovaná aj jednej z najnovších technológií, NFC. V poslednej kapitole teoretickej časti je zhrnutý elektronický platobný styk. Praktická časť opisuje čo je výstupom tejto bakalárskej práce.

KĽÚČOVÉ SLOVÁ

Apple pay, bezpečnosť, elektornické bankovníctvo, Google pay, GSM, homebanking, internetbanking NFC, phonebanking, platobná karta, zákon

ABSTRACT

The main goal of this bachelor thesis „Security of electronic banking“ is to characterize payment electronic services and possibilities of their realization and also comparison of offers of bank payment services in order to point out and draw attention to their security and risks involved. This thesis at first deals with the explanation of the basic concepts related to the issue, then the current available legislation of this sector is written, especially in the Czech Republic. It also deals with individual forms of electronic banking and their detailed description. One whole chapter is devoted also to one of the latest technology, the NFC. In the last chapter of the theoretical part is summarized electronic payment system. The practical part describes what is the output of this bachelor thesis.

KEYWORDS

Apple play, electronic banking, Google pay, GSM, homebanking, internetbanking NFC, payment card, phonebanking, safety , law

TOMKO, Tomáš. *Bezpečnosť elektronického bankovníctva*. Brno, 2020, 70 s. Bakalárska práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedúci práce: doc. Ing. Václav Zeman, Ph.D.

VYHLÁSENIE

Vyhlasujem, že svoju bakalársku prácu na tému „Bezpečnosť elektronického bankovníctva“ som vypracoval samostatne pod vedením vedúceho bakalárskej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora

POĎAKOVANIE

Rád by som poďakoval vedúcemu bakalárskej práce pánovi doc. Ing. Václavovi Zemanovi, Ph.D. za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k mojej práci.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Klienti, ktorí v minulosti navštevovali banky, prichádzajú na to, že využívanie elektronických služieb bankovníctva z počítača je oveľa pohodlnejšie a lacnejšie. Elektronické bankovníctvo v poslednej dekáde zažilo nevídaný rozmach a nie je sa čomu čudovať, že stále napreduje a rozširuje sa po celom svete. Čoraz viac ľudí rozumie a prišlo k tomuto modernému spôsobu komunikácie s bankou a finančné operácie už takmer všetci robia z pohodlia svojho domova. Elektronické bankovníctvo je rozšírené medzi všetkými vekovými kategóriami aj keď niektorí starší ľudia stále radšej uprednostnia osobný styk a to či už z toho dôvodu, že s počítačom nie sú tak zžití ale môže to byť aj z dôvodu toho, že sú príliš konzervatívni. Banky robia všetko pre získanie a udržanie si klienta, a tak ponúkajú rôzne formy elektronického bankovníctva a neustále zdokonaľujú svoje služby, ktoré sú buď zadarmo alebo za minimálne poplatky. Každá moderná banka už ponúka svoje služby aj cez internet.

Vplyvom rozvoja informačných a telekomunikačných technológií sa informácie stali viac dostupné. Banky sa odkláňajú od klasických foriem bankových služieb vykonávaných prostredníctvom ich pobočiek a nahrádzajú ich novými formami elektronického bankovníctva. Zatiaľ čo v minulosti boli dominantné pobočky bánk, kde prebiehala väčšina platobných operácií, dnes je to všetko inak. S príchodom mobilnej komunikácie a internetu význam elektronického bankovníctva dynamicky vzrástol. Na raste a význame elektronického bankovníctva sa nepodieľajú len samotné banky a ich klienti, ale aj tretie strany, ktoré klientom umožňujú nakupovať tovar prostredníctvom internetu. V súvislosti s rozvojom nových technológií však netreba zabúdať na bezpečnosť bankovníctva. Zákazníci sú zraniteľnejší a náchylní na rôzne formy bankových podvodov. A práve problém bezpečnosti elektronického bankovníctva predstavuje pre banky obrovskú výzvu.

Preto som sa rozhodol pre túto tému kde som sa rozhodol viac popísať jednotlivé bezpečnostné riziká, ktoré internetové bankovníctvo a jeho služby predstavujú. Chcel by som najskôr predstaviť základné pojmy, ktoré sú v práci dôležité a neskôr sa postupne prepracovať od právnej úpravy až ku jednotlivým technikám. Mojím cieľom je spraviť komplexný súhrn informácií, ku ktorým je možnosť sa dostať a spísať ich do jedného celistvého diela. Ďalej si za cieľ dávam urobiť praktický výstup práce aby boli informácie pre ľudí dostupnejšie.

1 ZÁKLADNÉ POJMY

Elektronické bankovníctvo - je to forma bankovníctva, pri ktorej nedochádza k priamemu kontaktu medzi bankou a klientom a pri ktorej sa zároveň na komunikáciu využívajú moderné telekomunikačné technológie. Prostredníctvom elektronického bankovníctva je možné realizovať pasívne operácie, poskytujúce všeobecné informácie napr. o zostatku na účte [1].

Elektronické platobné prostriedky - sú elektronické prostriedky, ktoré umožňujú prístup k elektronicky evidovaným alebo elektronicky uchovávaným peniazom a ktoré umožňujú prostredníctvom elektronických alebo iných technických zariadení uskutočňovať vklady, výbery, prevody alebo iné operácie. Vydavateľom elektronického platobného prostriedku môže byť centrálna banka, banka, iné osoby a inštitúcie oprávnené zákonom, resp. s príslušným povolením od centrálnej banky [2].

Služby elektronického bankovníctva - sú služby, ktoré poskytuje banka, a ktoré umožňujú diaľkovú komunikáciu klienta banky s bankou samotnou prostredníctvom rôznych technických prostriedkov od počítačov až k mobilným telefónom, ktoré umožňujú aktívne alebo pasívne operácie.

Pasívne operácie - umožňujú klientovi získať informácie všeobecného charakteru, napr. základné informácie o banke, aktuálny kurzový lístok, stav účtu. Nemôže však realizovať žiadne operácie na svojom účte [3].

Aktívne operácie - ponúkajú možnosť disponovania s účtom. Klient môže realizovať tuzemský aj cezhraničný platobný styk, inkasá z účtu, presuny peňažných prostriedkov z bežného účtu na termínovaný a podobne [3].

Autorizácia - znamená povolenie k nejakému úkonu alebo operácie. Pojem sa používa ako aj pre samotné povolenie tak aj pre proces zistenia, či daný subjekt môže danú činnosť či operáciu vykonať (má k tomu právomoc, povolenia alebo súhlas). V procese kontroly oprávnení zvyčajne nadväzuje na overenie identity, teda autentizáciu.

Autentizácia - je mechanizmus identifikácie a overenia identity, ktorý sa snaží dosiahnuť a zabezpečiť integritu, dôvernosť a nepopierateľnosť. Pozostáva z dvoch zložiek:

- *Identifikácia* - login, meno používateľa, prihlasovacie ID, predstavenie sa.
- *Autentizácia* - overenie identity jedinečným príznakom, osobné heslo, osobný certifikát vystavený na konkrétnu osobu, odtlačok prsta.

Autentizačný nástroj - je nástroj, ktorý banka vydá majiteľovi účtu a prostredníctvom ktorého sa užívateľ prihlasuje (autentizuje) pre služby elektronického bankovníctva. Autentizačnými nástrojmi môžu byť napríklad heslo (pre pasívnych uží-

vateľov), PIN, GRID karta, elektronický osobný kľúč - token (zariadenie, ktoré slúži na generovanie jedinečného bezpečnostného kódu), SMS správa obsahujúca bezpečnostný kód alebo elektronický podpis uložený na komunikačnom médiu ale aj ďalšie nástroje, ktorých je mnoho.

Elektronický osobný kľúč - je zariadenie na zaistenie vysokej ochrany prístupu k elektronickému bankovníctvu. Toto zariadenie generuje jednorázové heslá na prihlásenie, overuje spojenie s bankou a môže generovať aj jednorázové kódy na potvrdenie transakcií.
Transakcia - je to dohoda(zmluva), komunikácia, presun(prevod) zrealizovaný medzi separátnymi entitami alebo objektami, často sprevádzaný výmenou položiek s určitou hodnotou ako sú informácie, tovar, služby a peniaze.

Platobná karta - je moderný, relatívne bezpečný a stále viac používaný prostriedok bezhotovostného platobného styku využívaný hlavne k úhrade spotrebných výdavkov a výberu hotovosti. Najčastejšie využívaným druhom platobných kariet je debetná karta, ktorá je viazaná na bežný účet a majiteľ karty používa vlastné finančné prostriedky z vlastného účtu. Menej rozšírenou je kreditná karta, v prípade ktorej klient čerpá úver za banky. Platobná karta obsahuje povinné náležitosti [4].

Internetbanking - spôsob komunikácie klienta s bankou, ktorý umožňuje klientovi nadviazať spojenie s bankou prostredníctvom internetu. Nevyžaduje sa počítač vybavený špeciálnym softwarom (aplikáciou) banky.

Homebanking - služba, ktorá umožňuje komunikáciu medzi klientom a bankou prostredníctvom prepojenia osobného počítača klienta, ktorý je vybavený špeciálnym softwarom (aplikáciou) banky, ktorý však musí byť vybavený špeciálnym softwarom od banky.

Phonebanking - služba umožňujúca klientovi komunikovať s bankou prostredníctvom telefónu s tónovou voľbou, možnosťou spojenia s hlasovým informačným systémom alebo s operátom.

GSM banking - GSM banking je banková služba, ktorá umožňuje ovládať bežný účet prostredníctvom mobilných technológií siete GSM. Medzi najpoužívanejšie služby patrí SIM Toolkit, ktorá formou inštalované aplikácie na SIM karte umožňuje zabezpečenú komunikáciu s bankou pomocou šifrovaných textových správ. Komunikácia s bankou je potom založená na princípe odosielania a prijímania klasických krátkych textových správ, pričom bezpečnosť je postavená buď len na zadaní PIN kódu ku konkrétnej SIM karte alebo využití tzv. autentizačných kalkulátorov.

WAP banking - využitie mobilného telefónu s možnosťou pripojenia na internet prostredníctvom aplikácie WAP s následným realizovaním aktívnych alebo pasívnych operácií cez WAP [1].

NFC - je technológia umožňujúca rýchlu a zabezpečenú výmenu dát na vzdialenosť do 4 cm. Podporuje ju rada chytrých zariadení. NFC funguje na báze krátkych rádiových vĺn a má veľmi nízku spotrebu [5].

Google Pay - je platforma digitálnej peňaženky a online platobný systém vyvinutý spoločnosťou Google (tiež označované G Pay), ktorý umožňuje nákupy v aplikáciách a platby len jedným kliknutím na mobilných zariadeniach a umožňuje používateľom uskutočňovať platby pomocou telefónov, tabletov alebo hodiniek s Androidom [6].

Apple Pay - je platobná služba, ktorá umožňuje používateľom vykonávať platby v aplikáciách iOS alebo na webe. Digitalizuje a môže nahradiť čip z kreditnej alebo debetnej karty na termináli bezkontaktného predaja. Veľmi podobné bezkontaktným platbám ale s pridaním dvoj-faktorovej autentizácie pomocou Touch ID, Face ID, PINu alebo hesla. Služba umožňuje zariadeniam Apple bezdrôtovo komunikovať s predajnými systémami pomocou technológie NFC [7].

Garmin Pay - je systém bezkontaktných platieb, ktorý vo vybraných modeloch chytrých, športových GPS hodinkách ponúka značka Garmin. K aktivácii Garmin Pay sú potrebné kompatibilné hodinky a platobnú kartu od banky, ktorá platby Garmin Pay podporuje [8].

1.1 Elektronický platobný styk

S tým ako sa posúvala a vyvíjala doba rýchlo dopredu prichádzali aj požiadavky na prenos informácií. Hľadali sa možné spôsoby a začali sa využívať už dostupné prostriedky pre vzdialenú komunikáciu. Prvú veľkú zmenu predstavoval telefón. Telefón ale nebol pre bankovníctvo najspoľahlivejší komunikačný prostriedok, pretože klient sa autentizoval iba menom a známym heslom alebo dohodnutým kódom. Neskôr sa začal používať fax, kde sa začalo používať identifikácia na základe mena a čísla klienta, čísla jeho účtu sa autentizovalo s pomocou kódovej tabuľky.

Revolúciu priniesli počítače, ktoré umožňovali spracovávanie takmer všetkých dát. V počiatkoch boli dáta predávané v textových súboroch formou tzv. kontrolných viet. Kontrolné vety boli reťazce znakov s presne stanovenou štruktúrou so zabezpečovacím kódom pre daný deň. Prvé súbory sa prenášali na disketách. Pre banky to znamenalo prvý veľký krok pretože na prenesenie veľkého objemu dát priamo do systému k zaúčtovaniu vynechali ľudský faktor priamo na pobočke v banke. Po disketách už prišli na rad prenosy dát z počítača do počítača prostredníctvom BBS (Bulletin Board Service) stanice. Táto stanica umožňovala prenášať zabezpečené príkazy domáceho platobného styku a informácie o spracovaných položkách priamo do banky.

Elektronický podpis odštartoval vznik zložitejších programov, pomocou ktorých banky môžu ponúkať svojím klientom väčšiu a pohodlnejšiu obsluhu svojich účtov. Táto inovácia mala za následok, že elektronická komunikácia s bankou sa rozšírila na 24 hodín denne a 7 dní v týždni a spektrum ponúkaných služieb sa výrazne rozšírilo, napríklad možnosť objednávať a platiť služby a tovar prostredníctvom internetu. Rovnako odpadli zdĺhavé návštevy pobočiek bánk za účelom jednoduchých a bežných bankových operácií ako sú platby alebo len prevody na iný účet. K tomu aby komunikácia bola funkčná, musia byť užívateľské aplikácie prepojené s bankovými systémom. V banke sa nachádzajú komunikačné servery, pomocou ktorých prebieha komunikácia. Z bankového systému sa do nich prenášajú dáta a tie si následne môžu klienti stiahnuť. Programy pre elektronickú komunikáciu znamenajú pre klienta aj určitú ochranu pred chybami a znižujú riziko chybovosti.

Rozvoj elektronického bankovníctva a elektronických peňazí môže rapídne zvýšiť efektivitu platobného systému a bankovníctva a znížiť nám náklady na drobné operácie ako v národnom, tak aj medzinárodnom meradle. Tieto kroky by následne mohli viesť k zvýšeniu produktivity a ekonomickej prosperite [9].

1.2 Vymedzenie pojmu platobných produktov

Obecne je možné za platobné produkty elektronického bankovníctva považovať všetky produkty banky, pri ktorých je kontakt klienta s bankou alebo využívanie daného produktu, ktorý je prevádzaný elektronickou formou.

Pre praktické účely je pri vymedzení platobného produktu elektronického bankovníctva možné vyjsť zo zákona o platobnom styku, ktorý vymedzuje dve varianty elektronických platobných prostriedkov:

- prostriedok vzdialeného prístupu k peňažným prostriedkom (Pri jeho používaní sa spravidla vyžaduje identifikácia držiteľa osobným identifikačným číslom, ktoré bolo pridelené vydavateľom.)
- elektronický peňažný prostriedok (Jedná sa o platobný prostriedok, ktorý uchováva peňažnú hodnotu v elektronickej podobe, a ktorý je aj ako platobný prostriedok inými osobami prijímaný. Peňažná hodnota uchovávaná na týchto prostriedkoch sa tak označuje za elektronické peniaze.)

Toto rozlíšenie nesie v sebe veľký význam. V prvom prípade sa píše len o nových možnostiach využívania „klasických platobných prostriedkov“, v druhom prípade sa hovorí o vzniku novej formy peňazí – elektronické peniaze [9].

1.3 Ochrana dát v elektronickom platobnom styku

Maximálna bezpečnosť údajov vo vzdialenej komunikácii je pre banku aj pre klientov v dnešnej informačnej dobe najväčšia priorita. A to najmä z hľadiska dôvery ich klientov, partnerov, konkurencie, verejnosti a udržania si dobrého mena. Pri elektronickom kontakte sa posiela mnoho informácií, ktoré sú predmetom bankového a firemného tajomstva, a ktoré sa nesmú cestou od klienta až po ich spracovanie žiadnym spôsobom zmeniť, a ani nesmie byť umožnené prečítanie obsahu pri prípadnom pasívnom odpočúvaní alebo kopírovaní.

Princíp komunikačnej výmeny bezpečným spôsobom, nie len v elektronickom bankovníctve, spočíva v zašifrovaní dát odosielateľom a v odšifrovaní dát len príjemcom. Za týmto účelom sa používa mnoho kryptografických techník a metód. Od najjednoduchších, používaných pri komunikácii telefónom, až po technicky najnáročnejšie prostredníctvom špeciálnych komunikačných programov.

V rámci tých najjednoduchších techník sa používa meno a heslo. Ako ďalší bezpečnostný prvok býva napríklad volený limit platby a ak si klient takú možnosť zvolí tak väčšina bánk ponúka aj odosielanie SMS správy na klientov mobilný telefón pri každom prihlásení alebo uskutočnení platby. Klient tak môže veľmi rýchlo reagovať na prípadné nežiadúce manipulovanie s účtom a môže účet nechať zablokovať. Než však prebehne blokácia účtu, môže falošný majiteľ vykonať niekoľko platieb pokiaľ bude dostatočne šikovný a rýchly. Nízka je aj pravdepodobnosť návratu zmiznutého množstva nadobudnutých peňazí, pretože banka neručí za transakcie vykonané v rámci bezpečnostných prvkov, za tie si ručí a plnú zodpovednosť nesie klient.

Vyššie zabezpečenie pri telefonickej komunikácii je možné dosiahnuť využitím niektorých z nasledujúcich troch prvkov. PIN (osobné identifikačné číslo) päťciferné číslo, ktoré si klient môže ľubovoľne meniť, identifikačného čísla IPPID (jedinečné osemmiestne číslo v rámci banky), a heslo - šesť až desaťmiestny alfanumerický reťazec s rozlíšením veľkých a malých písmen, ktoré si pri aktivácii služby môže klient sám zvoliť a meniť.

Ešte vyšším zabezpečením pri telefonickej komunikácii je zabezpečenie pomocou mobilného telefónu, prostredníctvom ktorého sa generuje PIN alebo dochádza k prenášaniu kódových správ priamo z aplikácie nahranej na SIM Toolkitovej karte zabezpečenej pomocou BPIN. Viac bude rozpísané v podkapitole GSM Banking.

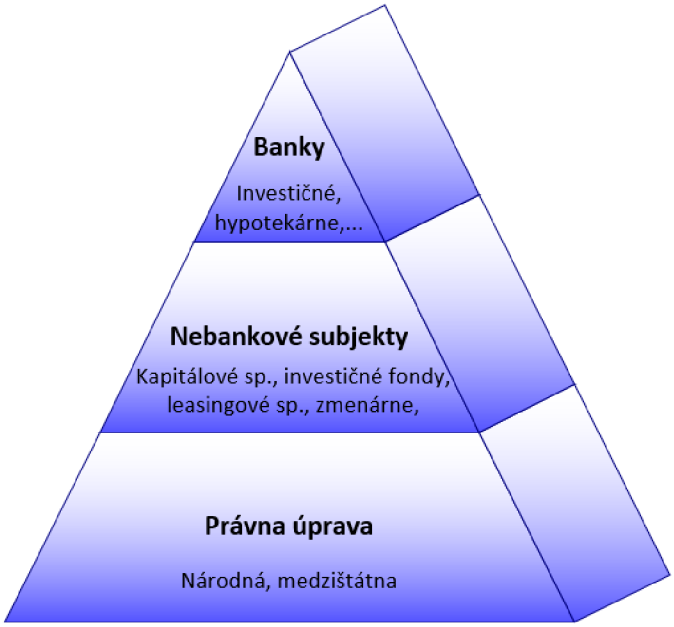
Najlepšie ale technicky najnáročnejšie zabezpečenia telefonického bankovníctvo je ponúkané prostredníctvom PIN kalkulátora (elektronického kľúča), ktorý musí mať klient pri sebe, ak chce túto službu používať.

Pri komunikácii špeciálnymi programami sa najčastejšie využíva tzv. digitálny podpis, algoritmus, ktorý je postavený na báze dvoch kľúčov. Pracuje na princípe

asymetrického šifrovania. Verejný kľúč musí byt pre danú komunikáciu certifikovaný. Každá z komunikujúcich strán má vytvorené dva kľúče. Proces zabezpečenia a komunikácie spočíva v tom, že odosielateľ dáta zašifruje pomocou svojho tajného (súkromného, privátneho) kľúča a pomocou verejného kľúča protistrany. Protistrana súbor pomocou svojho tajného a verejného kľúča odosielateľa dáta rozšifruje, a tým je zaistená identifikácia aj autentizácia. Elektronický podpis je údaj v elektronickej podobe, ktorý je pripojený alebo logický spojený s inými elektronickými dátami a ktorý slúži ako dôkaz, že uvedené dáta boli vytvorené konkrétnou osobou alebo konkrétnym elektronickým systémom, teda slúži ako metóda overenia ich pravosti. Využíva sa na jednoznačnú identifikáciu osôb [9].

2 KLASICKÝ PLATOBNÝ STYK

Medzi základné služby, ktoré banky poskytujú svojím klientom patrí realizácia platobného styku. Patria sem bezhotovostné a hotovostné presuny peňažných prostriedkov medzi subjektami teda fyzické a právnické osoby doma aj v zahraničí. Platobný styk predstavuje trojvrstvovú architektúru produktov platobného styku (obr. č. 2.1), operácií bánk a nebankových inštitúcií, kde služba v každej z vyššej vrstvy predpokladá využitie služby z vrstvy nižšej. Platobný styk sa tak stáva nekončiacou inováciou služieb bánk a nebankových inštitúcii, preto trojvrstvový model nie je konečným modelom komunikácie bánk a jej klientov.



Obr. 2.1: Trojvrstvová architektúra platobného styku

2.1 Právna úprava platobného styku

Často sa stáva, že platobný styk je chápaný len ako prosté platenie prostredníctvom bánk bez hlbšej znalosti jeho jednotlivých foriem. A tie sa od seba niekedy podstatne líšia a vychádzajú z rôznych prameňov práva. Preto je táto práca tiež zameraná na výklad základných právnych noriem, ktoré upravujú platobný styk priamo alebo len okrajovo.

2.2 Zákon o platobnom styku

Základným prameňom pre úpravu oblasti platobného styku bol zákon č. 284/2009 Zb. z., ktorý bol zrušený a je nahradený novým zákonom č. 370/2017 Zb. z. Tento zákon spracováva príslušné predpisy Európskej únie, zároveň nadväzuje na priamo použiteľné predpisy Európskej únie a upravuje:

1. činnosť niektorých osôb oprávnených poskytovať platobné služby a vydávať elektronické peniaze, vrátane činnosti týchto osôb v zahraničí,
2. účasť v platobných systémoch a vznik a prevádzkovanie platobných systémov,
3. práva a povinnosti podnikateľov, ktorí poskytujú platobné služby,
4. práva a povinnosti podnikateľov, ktorí vydávajú elektronické peniaze,
5. práva a povinnosti podnikateľov, ktorí prostredníctvom internetových stránok porovnávajú odplaty za služby spojené s platobným účtom,
6. používanie jednotného označenia služieb spojených s platobným účtom,
7. postup pri zmene platobného účtu,
8. prístup k platobnému účtu [10].

2.2.1 Zákon o bankách

Ďalším významným právnym predpisom, ktorého ustanovenia sa týkajú oblastí platobného styku je zákon č. 21/1992 Zb. z., O bankách, v znení neskorších predpisov. Platobného styku a zúčtovaní sa však dotýka najmä § 20c, ktorý stanovuje podmienky tzv. Opravného zúčtovania. Za povšimnutie potom ďalej stojí ustanovenia týkajúce sa bankového tajomstva vo väzbe na platobný styk (§ 38) a otázky poistenia pohľadávok (§ 41). Tento zákon spracováva príslušné predpisy Európskej únie, zároveň nadväzuje na priamo použiteľný predpis Európskej únie a upravuje niektoré vzťahy súvisiace so vznikom, podnikaním a zánikom bánk so sídlom na území Českej republiky, vrátane ich pôsobenie mimo územia Českej republiky, a ďalej niektoré vzťahy súvisiace s pôsobením zahraničných bánk na území Českej republiky [9].

2.2.2 Obchodný zákonník

Medzi ďalšie zákony, ktoré upravujú platobný styk v ČR, patrí aj zákon č. 513/1991 Zb. z., Obchodný zákonník, v znení neskorších predpisov. Tento predpis upravuje problematiku vedenia bežného účtu a obsahové náležitosti zmluvy o bežnom účte a zmluvy o vkladovom účte. Vzhľadom k nutnosti vykonania veľa zmien a vytvorenie nového občianskeho zákonníka, bolo rozhodnuté o zrušení obchodného zákonníka a k následnej úprave mnoho oblastí už v rámci občianskeho zákonníka. Ten sa tak teraz (s účinnosťou od 1.1.2014) stáva najvýznamnejším právnym predpisom súkromného práva. Nový občiansky zákonník, ako zákon č. 89/2012 Zb. z., tak zavádza

iný typ zmluvy o účte, ktorý sa na rozdiel od úpravy v predchádzajúcom obchodnom zákonníku, vzťahuje ako na zmluvu o účte bežnom, tak aj o účte vkladovom. Samotná úprava platobného styku však nebola významne upravená, predovšetkým kvôli tomu, že v platnosti aj naďalej zostáva vyššie spomínaný zákon o platobnom styku [9].

2.2.3 Ďalšie predpisy upravujúce platobný styk v ČR

- **Všeobecné obchodné podmienky Českej národnej banky:** táto norma, ktorá nie je normou právnou, a teda nemá právnu záväznosť, slúži pre potreby obchodných bánk ako odrazový mostík pre vytváranie vlastných obchodných podmienok pri zriaďovaní a vedení účtov.
- **Zákon č. 6/1993 Zb. z. o Českej národnej banke, v znení neskorších predpisov:** na základe tohto zákona bola ČNB ustanovená jedinou inštitúciu, ktorá je oprávnená na vydávanie bankoviek a mincí a riadi peňažný obeh, platobný styk a zúčtovanie bánk.
- **Zákon č. 87/1995 Zb. z. o sporiteľných a úverových družstvách a niektorých opatreniach s tým súvisiacich a o doplnení zákona Českej národnej rady č. 586/1992 Zb. z. O daniach z príjmov v znení neskorších predpisov:** upravuje poskytovanie platobného styku sporiteľnými a úverovými družstvami.
- **Nariadenie Európskeho parlamentu a Rady (ES) č. 924/2009 zo 16. septembra 2009 o cezhraničných platbách v Spoločenstve a zrušenie nariadenia (ES) č. 2560/2001:** toto nariadenie patrí medzi hlavné predpisy európskeho práva, upravuje prevody realizované v eurách či iných menách, a upravuje postup pri vykonávaní priameho inkasa členskými krajinami EÚ.
- **Nariadenie Európskeho parlamentu a Rady (ES) č. 1781/2006 z 15. novembra 2006 o údajoch o príkazcovi sprevádzajú prevody finančných prostriedkov:** toto nariadenie si kladie za cieľ zabrániť využívania finančného systému na zhromažďovanie finančných prostriedkov na podporu terorizmu, a za týmto účelom bola vytvorená povinnosť pre všetky inštitúcie vykonávajúce platobný styk uvádzať údaje o príkazcovi, ktoré umožní jasne určiť skutočného platca [9].

2.3 Judikatúra elektronického bankovníctva ČR a SR

Oblasť elektronického bankovníctva je predmetom úpravy na úrovni EÚ. Za základnú normu v tomto smere sa považuje smernica č. 2000/46/ES, o prístupe k činnosti inštitúcií k elektronickým peniazom, ich výkone a dohlaď nad touto činnosťou.

Cieľom tejto smernice je zamedziť emitovaniu elektronických peňazí do obehu, zvýšiť právnu istotu klienta a zvýšiť dôveru verejnosti k elektronickej forme peňazí. Pre účely tejto smernice môžu byť elektronické peniaze považované za elektronickú náhradu za mince a bankovky, ktorá je uložená na elektronickom nosiči ako čipová karta alebo pamäť počítača, a ktorá je vo všeobecnosti určená na účel uskutočňovania elektronických platieb obmedzených množstiev [11]. Vydávanie elektronických peňazí môže ovplyvniť stabilitu finančného systému a hladkú činnosť platobných systémov. Vyžaduje sa úzka spolupráca pri odhadovaní celistvosti schém elektronických peňazí.

Ďalej to je smernica č. 2002/65/ES, o uvedení finančných služieb pre spotrebiteľov na trh na diaľku a smernica č. 97/7/ES, o ochrane spotrebiteľa v prípade zmlúv uzatvorených na diaľku, v ktorých je upravený postup pri zneužití platobnej karty. Komisia ES takisto vydala odporučenie č. 97/489/ES, o operáciách prevádzaných platobnými prostriedkami a najmä o vzťahu medzi vydavateľom a držiteľom, ktoré je zamerané na predovšetkým jasnú úpravu vzťahov medzi vydavateľom a držiteľom s akceptom na ochranu práv držiteľa.

Základná právna úprava v oblasti elektronického platobného styku je v Českej republike upravená v zákone č 124/2002 Zb., o prevodoch peňažných prostriedkov, elektronických platobných prostriedkov a platobných systémov (zákon o platobnom styku), ktorý implementuje do právneho rádu vyššie uvedené smernice a do určitej miery reflektuje aj spomenuté odporučenia. Zákon stanovuje práva a povinnosti subjektom, ktoré sa zúčastňujú na prevádzaní peňažných prostriedkov.

Pre porovnanie právne normy, týkajúce sa elektronického bankovníctve v Slovenskej republike, sú obsiahnuté predovšetkým v zákone č. 483/2001 Zb. zákona o bankách v znení neskorších právnych predpisov, zatiaľ čo normy elektronického podnikania v zákone č. 22/2004 Zb. zákona o elektronickom obchode v znení neskorších právnych predpisov a v zákone č. 510/2002 Zb. zákona o platobnom styku v znení neskorších právnych predpisov.

Slovenská republika sa svojím členstvom v Európskej únii zaväzuje implementovať smernice Európskeho parlamentu a Rady, v tomto prípade ide o:

- Smernica Európskeho parlamentu a Rady 2009/110/ES zo 16. septembra 2009 o začatí a vykonávaní činností a dohľade nad obozretným podnikaním inštitúcií elektronického peňažníctva, ktorá ustanovuje pravidlá pre vykonávanie činností vydávania elektronických peňazí.
- Smernica 2002/21/ES o spoločnom regulačnom rámci elektronických komunikačných sietí a služieb, smernica č. 2002/58/ES o súkromných a elektronických komunikáciách a ďalšie transponované do zákona č. 610/2003 Zb. zákona o elektronických komunikáciách.

Ustanovenia slovenského právneho poriadku boli v priebehu času novelizované a nahradené tak, aby vyhovovali najnovším požiadavkám Európskej únie, rovnako ako aj technologickému vývoju v oblasti [12].

K podávaniu žiadostí o udelenie povolenia na vydávanie elektronických peňazí NBS vydala opatrenie č. 14/2011, ktoré slúži na doplnenie podrobností týkajúcich sa výkonu činnosti a podnikania platobných inštitúcií a inštitúcií elektronických peňazí. Podrobnejšie vysvetlenie k splneniu podmienok na udelenie povolenia k vykonávaniu činností inštitúcií elektronických peňazí na území SR sa nachádza v Metodickom usmernení Útvaru dohľadu nad finančných trhom NBS č. 4/2012 k podávaniu žiadosti o udelenie povolenia na vydávanie elektronických peňazí podľa § 82 zákona o platobných službách [13].

2.4 Zhrnutie judikatúry pre el. bankovníctvo

Oblasť bankovníctva v SR aj ČR je upravená nie len vnútroštátnymi predpismi a zákonmi ale bankovníctvo je podmienené aj tým, že obe krajiny sú členskými štátmi EÚ a teda sa zaviazali aj prijatím regulácií od EÚ. Základný prameň pre úpravu platobného styku v ČR je zákon č. 370/2017 Zb. zákona. Je to zákon o platobnom styku a tento zákon zapracováva príslušné predpisy Európskej únie [14] a pre SR to je 510/2002 Zb. zákona, ktorý je rovnako ako v ČR zákonom o platobnom styku a o zmene a doplnení niektorých zákonov [2]. Úlohy bánk definuje v ČR 21/1992 Zákon o bankách, Zb. zákona, ktorý popisuje to o čo sa banky v štáte starajú a aké sú oblasti ich pôsobenia [15]. V SR toto zastáva zákon 483/2001 Zákon o bankách, Zb. zákona [16]. Tieto zákony sú špecifikované hlavne pre komerčné banky. Centrálne banky majú vlastnú judikatúru a tou je pre ČR zákon 6/1993 Zákon Českej národnej rady o Českej národnej banke, Zb. zákona [17] a pre SR zákon 566/1992 Zákon Národnej rady Slovenskej republiky o Národnej banke Slovenska, Zb. zákona [18]. Centrálne banky v oboch štátoch spĺňajú štandardné funkcie ako je napríklad to, že majú emisný monopol na hotovostné peniaze, alebo aj to, že uskutočňujú menovú politiku štátu a regulujú bankový systém. Okrem týchto funkcií sa však od seba ČNB a NBS aj odlišujú s prístupom k určitým veciam. Napríklad v ČR je ČNB zverený dohľad nad celým finančným trhom a zároveň ČNB netradične ponúka aj ochranu spotrebiteľa. NBS na druhú stranu nevedie účty štátu a štátnych organizácií a ani nevydáva pokladničné poukážky a štátne dlhopisy. Ďalší rozdiel je, že NBS narozdiel od ČNB nie je národným rezolučným orgánom. Kľúčový rozdiel medzi NBS a ČNB je, že ČNB nie je členom Eurosystému a preto aj napriek úzkej spolupráci s Európskou radou vykonáva všetky svoje funkcie a povinnosti samostatne. Celé zhrnutie je v stručnosti uvedené v tabuľke č. 2.1.

Tab. 2.1: Zhrnutie judikatúry pre elektronické bankovníctvo

Slovenská republika	**Česká republika**	
510/2002 Zb. z.	370/2017 Zb. z.	základný prameň práva
483/2001 Zb. z.	21/1992 Zb. z.	judikatúra úlohy bánk
(NBS) 566/1992 Zb. z.	(ČNB) 6/1993 Zb. z.	zákon o centrálnej banke
394/2019 Zb. z.	89/2012 Zb. z.	občiansky zákonník
156/2019 Zb. z.	89/2012 Zb. z.	obchodný zákonník
2018/389 Zb. z.	2018/389 Zb. z.	bezpečnostné štandardy komunikácie
nie	áno	samostatné rozhodnutie o menovej politike
áno	nie	súčasť Eurosystému
áno (od r. 2004)	áno (od r. 2004)	regulácie od EÚ
áno	nie	vedenie štátnych účtov

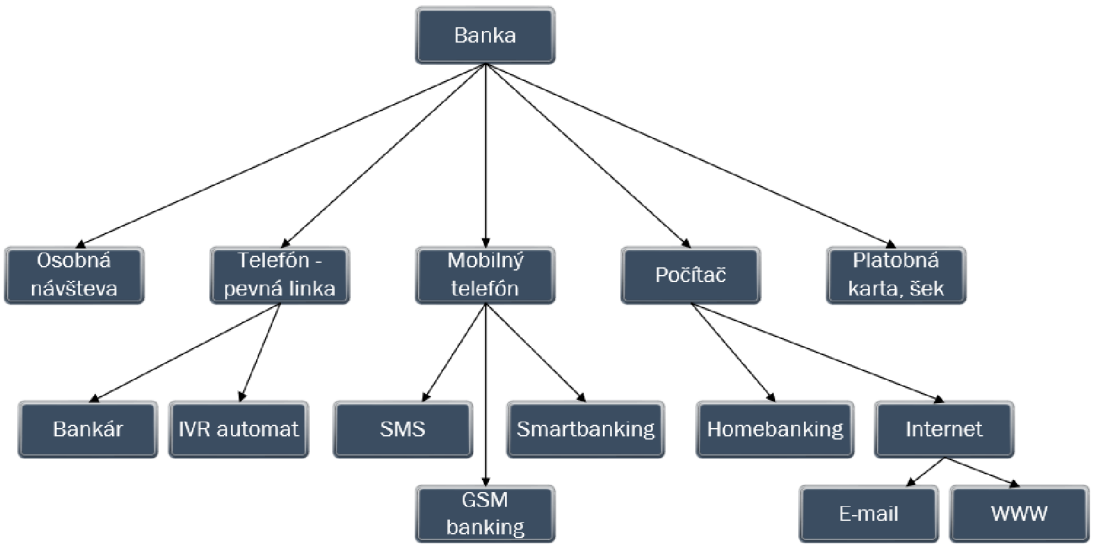
Oblasť elektronického bankovníctva je upravená v oboch štátoch na úrovni EÚ a to smernicou č. 2000/46/ES, ktorá hovorí o začatí a vykonávaní činností a dohľade nad obozretným podnikaním inštitúcií elektronického peňažníctva [19]. Táto smernica hovorí o regulačných technických predpisoch pre silnú autentizáciu zákazníka a spoločné a pomenúva bezpečné otvorené komunikačné normy. Platobné služby ponúkané elektronicky by mali byť vykonávané bezpečným spôsobom, za použitia technológií, ktoré sú schopné zaručiť bezpečné overenie používateľa a v maximálnej možnej miere znížiť riziko podvodu. Postup overenia by mal všeobecne zahŕňať mechanizmy sledovanie transakcií a mechanizmy k odhaleniu pokusov o použití osobných bezpečnostných údajov používateľa.

Ďalej je potreba zabezpečiť, aby bol používateľ platobných služieb oprávneným užívateľom, ktorý teda udelil súhlas s prevodom peňažných prostriedkov. Okrem toho je potrebné stanoviť požiadavky na silné overenie klienta, ktoré by sa mali uplatniť zakaždým, keď platca využíva on-line prístupu k svojmu platobnému účtu, iniciuje elektronickú platobnú transakciu alebo prostredníctvom prostriedkov komunikácie na diaľku vykoná akýkoľvek úkon, ktorý by mohol viesť k riziku platobného podvodu či iného zneužitia, teda je potrebné požadovať vytvorenie overovacieho kódu, ktorý by mal byť odolný voči riziku sfalšovania v celom rozsahu.

Keďže sa spôsoby podvodov neustále vyvíjajú, mali by požiadavky na silné overenie klienta umožniť inovácie technických riešení, ktoré sa zaoberajú vznikom nových hrozieb pre bezpečnosť elektronických platieb [20].

3 FORMY EL. BANKOVNÍCTVA

Na základe rozličných typov elektronických zariadení sa postupne vyvinuli viaceré formy elektronického bankovníctva. Niektoré z nich sú už považované za zastaralé ale v tejto práci budú tiež spomenuté. Dôvodom prečo sa prestali používať niektoré formy je ich technológia, na ktorej bolo založené ich fungovanie. Staršia technológia (napr. PDA, GSM, WAP banking) sa prestáva používať a bola nahradená novou, rýchlejšou a bezpečnejšou. Za hlavné formy súčasného elektronického bankovníctva sú považované internetbanking, smartbanking, platobné karty a NFC. Vhodným doplnkom k nim sú notifikačné služby informujúce klienta o stave účtu a transakciách v mobilných telefónoch. V oblasti elektronického bankovníctva vládne momentálne veľká konkurencia a tak sú služby vo väčšine prípadov dostupné zadarmo. Zhrnutie dostupných služieb bánk pre ich klientov viz obr. 3.1 [9].



Obr. 3.1: Možnosti komunikácie medzi bankami a klientom

3.1 Platobné karty

Platobné karty sú významným, moderným a stále sa rozvíjajúcim nástrojom platobného styku. Slúžia predovšetkým k úhrade spotrebných výdajov a výberu hotovosti. Prvé platobné karty sa začali používať v dvadsiatych rokoch 20. storočia. Neboli to karty v dnešnom slova zmysle.

V súčasnej dobe je najrozšírenejším a bezkonkurenčným produktom elektronického bankovníctva, ktorý umožňuje vzdialený prístup k účtu elektronickou cestou a to prostredníctvom terminálov a prostredníctvom internetu. Momentálne už niektoré banky využívajú platobné karty aj ako autentizačný nástroj pre prihlásenie sa do služby internetbanking. Mnoho ľudí však platobnú kartu používa iba na výbery z bankomatov, čo sa pochopiteľne banky snažia odbúrať zvýšenou propagáciou bezhotovostného platenia, prípadne znevýhodnenie takejto služby, keďže cieľom bánk je, aby ich klienti kartami robili obraty, a nie aby ich používali iba ako prostriedok na vybratie hotovosti, čo je pre banky nevýhodné.

Je to platobný prostriedok, ktorý banky klientom vydávajú ako základnú súčasť k bežnému účtu. Po technickej stránke môžeme povedať, že platobná karta je plastiková karta, odpovedajúca (z hľadiska materiálu, rozmerov 85,6 x 54,0 x 0,76 mm, konštrukcie) medzinárodným normám, ktorou oprávnený držiteľ môže prevádzať peňažné transakcie, ktoré boli dohodnuté medzi držiteľom karty a ich emitentom [21]. Forma tohto platobného prostriedku je daná medzinárodnou normou ISO 3554. Platobná karta by teda mala obsahovať tieto prvky:

- označenie vydavateľa karty, meno držiteľa karty,
- prípadne určitú formu identifikácie,
- číslo platobnej karty a tzv. BIN,
- platnosť platobnej karty,
- nosič elektronického záznamu,
- ochranné prvky,
- typ karty [9].

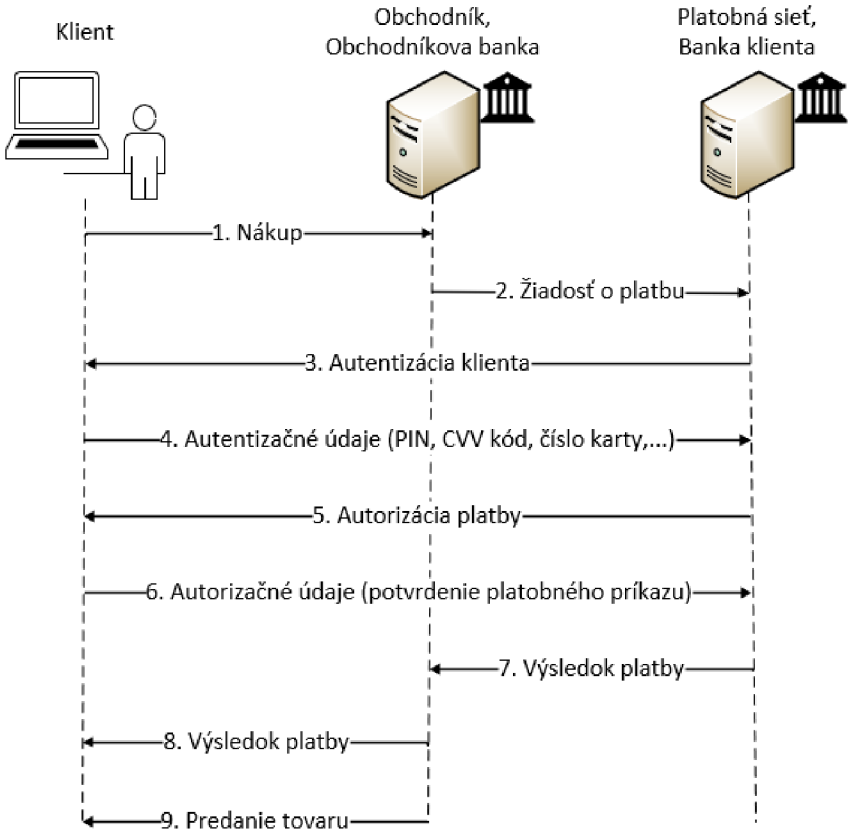
3.1.1 Využitie platobných kariet

Platobné karty nám ponúkajú mnoho možností využitia a taktiež s nimi môžu byť spojené aj niektoré doplnkové služby. Základné formy použitia platobnej karty sú:

1. výber hotovosti v bankomatoch,
2. výber hotovosti na pobočkách bánk,
3. bezhotovostná platba, ku ktorej patrí aj platba na internete. Jej autentizácia je zobrazená na obrázku 3.2.
4. výber hotovosti v obchodoch.

1. výber hotovosti v bankomatoch

Bankomatová karta nespĺňa len funkciu bezhotovostnej platby ale slúži aj pre jej držiteľa k prístupu k jeho finančným prostriedkom uložených na účte. Jedná sa o hotovostnú operáciu.



Obr. 3.2: Autentizácia platobnej karty pri platbe na internete

Na rozdiel od platenia v obchode tak výber hotovosti v automatoch prebieha výhradne v elektronickej podobe. Autentizácia klienta je vykonávaná prostredníctvom zadania PIN (Personal Identification Number). Bankomaty pracujú výhradne v online režime, a preto nám umožňujú autorizáciu každej realizovanej transakcie v reálnom čase.

2. výber hotovosti na pobočkách

Tento spôsob pre klienta nie je príliš výhodný, pretože je zaťažený príliš veľkými poplatkami. Využíva sa len v krajných prípadoch keď nie je k dispozícii bankomat alebo čiastka, ktorú je potreba vybrať presahuje zadaný limit pre výber v bankomate. Každá transakcie je autorizovaná a okrem platobnej karty sa klient musí autentizovať aj dokladom totožnosti.

3. bezhotovostná platba

Autorizácia transakcie spočíva v kontrole údajov na karte (Kontrola ochranných prvkov slúži na kontrolu karty, či nie je sfalšovaná. Kontrola čísla karty slúži na overenie karty, či nie je zapísaná na zozname zakázaných kariet a kontrola platnosti karty.),

ale aj pokiaľ zadaná transakcia presahuje limit musí byť autorizovaná. To znamená overenie finančného krytia transakcie (telefónom alebo na internete u autorizačného strediska). Autorizačné stredisko je po sieti prepojené s jednotlivými vydavateľmi platobným karát a tým pádom môže danú transakciu overiť až u vydavateľa.

4. výber hotovosti v obchodoch
Ak je tovar platený v obchode klient môže požiadať o vyplatenie určitej čiastky v hotovosti. Avšak v takom prípade je účet klienta zaťažený nie len platbou za nákup, ale aj výberom hotovosti. Táto transakcia si vyžaduje zadanie PIN kódu.

3.1.2 Účastníci platby platobnou kartou

Účastníci bezhotovostného platenia platobnou kartou sú:

- klient (držiteľ karty, odberateľ, platca),
- banka (vydavateľ karty, emitujúca inštitúcia),
- banka (obchodníka),
- obchodník (dodávateľ, príjemca platby),
- autorizačné stredisko [9].

3.1.3 Výhody a nevýhody používania platobných kariet

Výhody pre klienta:

- neobmedzený prístup k finančným prostriedkom – výber hotovosti z bankomatu možno využívať 24 hodín denne, 7 dní v týždni a každý deň v roku
- vyššia ako bezpečnosť používania hotovosti
- možnosť použitia karty v zahraničí – nie je potrebné zamieňať si hotovosť
- doplnkové služby poskytované ku karte – napr. cestovné poistenie

Nevýhody pre klienta:

- poplatky súvisiace s používaním karty a v prípade straty
- v prípade straty hrozí aj riziko zneužitia

Výhody pre obchodníka:

- bezpečnosť prijímania kariet je väčšia ako bezpečnosť prijímania hotovosti
- väčší obrat – platí tu psychologický aspekt predaja
- zaručená platba – pri splnení určitých podmienok

Nevýhody pre obchodníka:

- poplatok za prenájom POS terminálu (point of sale, elektronické zariadenia umožňujúce realizovať bezhotovostné platby platobnými kartami). Platí hlavne pre malých obchodníkov.

3.1.4 Delenie platobných kariet

Platobné karty sa dá členiť podľa rôznych hľadísk. Základné delenie je zobrazené na v tabuľke č. 3.1.

Tab. 3.1: Delenie platobných kariet

Charakter triedenia	Druh platobných kariet
podľa spôsobu zúčtovania transakcií	debetná karta
	kreditná karta
	charge karta
podľa záznamu dát	embosovaná karta
	karta s magnetickým záznamom
	čipová karta
	karta s laserovým záznamom
teritoriálne členenie	domáce, národné, tuzemské karty
	medzinárodné karty

Debetná karta – Je vydaná k bežnému účtu. Držiteľ s ňou platí za zbožie, služby alebo si vyberá hotovosť z bankomatu. Banka neposkytuje užívateľovi úver.

Kreditná (úverová) karta – Banka poskytuje klientovi možnosť čerpať spotrebiteľský úver. Držiteľ s ňou platí tiež za zbožie, služby alebo si vyberá hotovosť z bankomatu.

Charge karta – Historicky najstarší typ, pri ktorom držiteľ karty uhrádza platby za určité obdobie, z pravidla to je 30 dní, a za týchto 30 dní mu potom vydavateľ karty vydá výzvu k úhrade svojho úväzku.

Embosovaná karta – Autentizačné údaje sú na tejto karte vyrazené (embosované) reliéfovým písmom. Dôvodom je možnosť snímania údajov v mechanickom snímači obchodníkov (v imprintoch).

Karta s magnetickým záznamom – Autentizačné údaje a dáta o prevedených transakciách sú zaznamenávané na magnetický prúžok, čo nám umožňuje prevádzanie elektronických transakcií platobnou kartou.

Čipová karta – Dáta sú umiestnené v mikročipe, ktorý je umiestnený na prednej strane karty. Čipové karty prinášajú ako aj klientom tak aj banke mnoho výhod:

- problematická výroba kópie čipu, t.j. získanie rovnakého čipu a operačného systému vrátane získania dát, ktoré sú šifrované,
- kapacita pamäte čipu poskytuje priestor pre ďalší softvér, s možnosťou doplniť ďalšie softvérové bezpečnostné prvky a nové aplikácie,

- vylepšenie procesu rozhodovania čítačky kariet - podpora online a offline overenia pravosti karty a možnosť použitia náročnejších šifier, čo prináša lepšiu ochranu pri platobných termináloch,
- možnosť reakcie na novo vzniknuté požiadavky – možnosť konfigurácie a aktualizácie aplikácií.

Karta s laserovým záznamom – Dáta sú zaznamenávané a uchovávané do podkladovej vrstvy laserovou technológiou ako u CD diskov. Výhodou je vysoká kapacita záznamu, nevýhodou zas jednoduché kopírovanie.

V poslednej dobe sa stali trendom bezkontaktné platobné karty zjednodušujúce menšie platby v obchodoch, pri ktorých nie je potrebné zadanie PIN kódu [9].

3.1.5 Údaje zobrazené na platobnej karte

Ich fyzikálne vlastnosti a vzhľad a aj obsahové prvky sú v medzinárodnom meradle štandardizované. Na prednej strane platobnej karty (obr. č. 3.3) sú zobrazené nasledovné údaje:

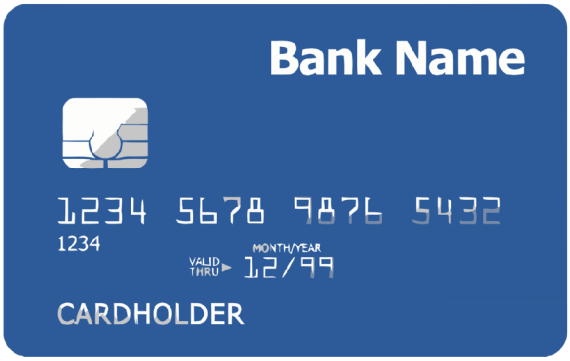
- **označenie vydavateľa** – názov a logo príslušnej banky
- **číslo platobnej karty** – 16 až 19 miestne číslo, kde prvé dve číslice identifikujú druh karty, ďalších 5 čísel identifikuje vydávajúcu banku karty a posledných 9 číslic identifikuje konkrétneho držiteľa karty
- **časť čísla BIN** – 4 znaky, číslo BIN (Bank Identification Number) je číslo pridelené kartovej asociácii konkrétnej banky
- **platnosť platobnej karty** – udáva obdobie, počas ktorého je karta použiteľná, obdobie je uvedené v tvare MM/RR
- **meno držiteľa platobnej karty** – maximálne 27 znakov, pri služobných kartách sa píše aj názov podniku
- **v niektorých prípadoch čip**

Na zadnej strane platobnej karty sú zobrazené nasledovné údaje:

- **podpisový prúžok** – slúži ako podpisový vzor držiteľa karty
- **magnetický prúžok** – obsahuje dve alebo tri stopy pre elektronický záznam identifikačných údajov, je na ňom zaznamenané číslo karty, platnosť karty, informácie o druhu karty, informácie o možnosti použitia a bezpečnostné údaje
- **logo vydávajúcej banky, kartovej spoločnosti, resp. združenia bankových kariet**

3.1.6 Bezpečnosť platobných kariet

Bezpečnosť využitia platobných kariet prostredníctvo internetu má na starosti služba 3-D secure. 3-D Secure je protokol založený na XML, ktorý je navrhnutý ako do-



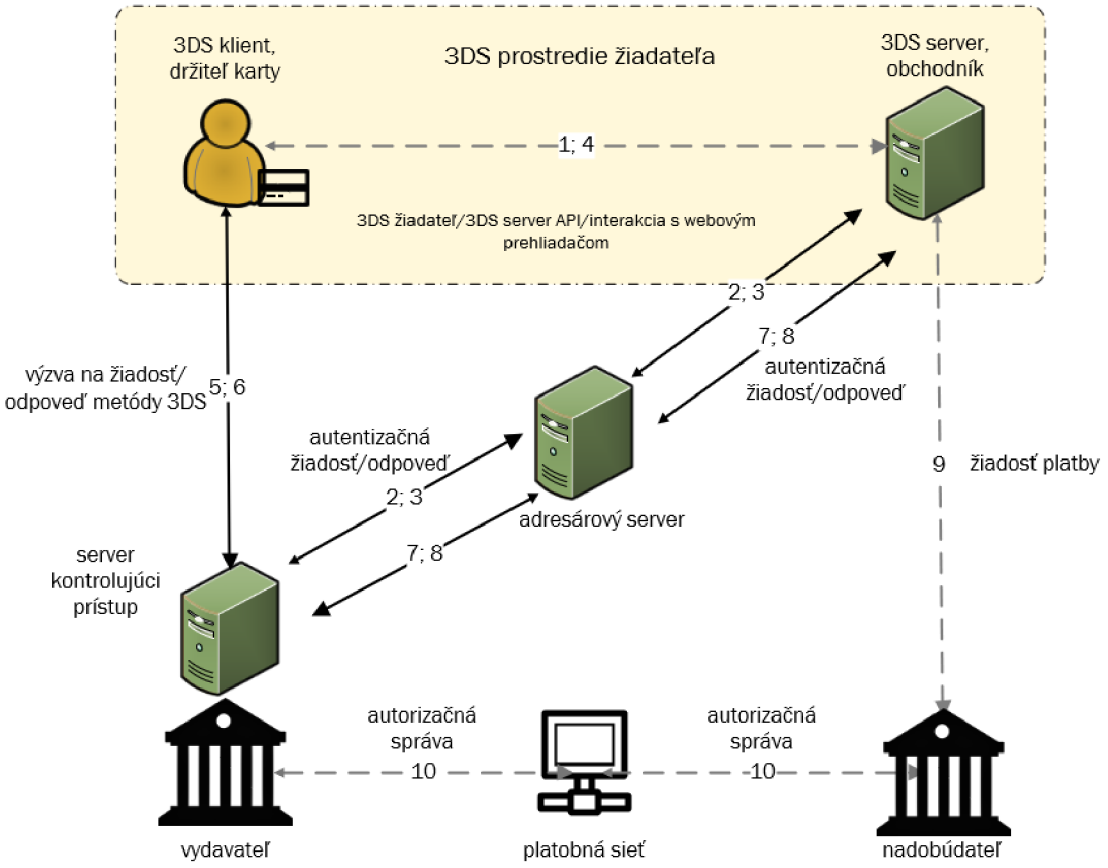
Obr. 3.3: Platobná karta a jej ochranné prvky (Zdroj:<shorturl.at/ezGL5>)

datočná bezpečnostná vrstva pre transakcie kreditných a debetných kariet online. Pôvodne bola vyvinutá spoločnosťou Arcot Systems (teraz CA Technologies) a prvýkrát nasadená spoločnosťou Visa, ktorej cieľom bolo zlepšiť bezpečnosť internetových platieb. Táto služba bola ponúkaná pod označením Verified by Visa alebo aj Visa Secure. Neskôr boli všetky funkcie boli prevzaté aj spoločnosťou Mastercard ako SecureCode.

3-D secure (3DS) je protokol správ, ktorý umožňuje klientom sa autentizovať u vydavateľa karty pri uskutočňovaní transakcií, pri ktorých nie je klient prítomný, CNP, teda Card Not Present. Dodatočná bezpečnostná vrstva pomáha zabrániť neoprávneným transakciám CNP a chráni obchodníka pred podvodom prostredníctvom CNP. Tri zabezpečené domény, ktoré poskytuje 3DS pozostávajú z domény obchodníka/nadobúdateľa, domény vydavateľa a domény interoperability (infraštruktúra poskytovaná schémou kariet, kreditnými, debetnými, predplatenými alebo inými typmi platobných kariet).

Tento protokol používa správy XML odosielané prostredníctvom pripojenia SSL s overením totožnosti klienta (to zabezpečuje pomocou digitálnych certifikátov). Transakcia, ktorá bola overená prostredníctvom Visa alebo SecureCode iniciuje presmerovanie na webovú stránku banky, ktorá kartu vydala, na autorizáciu transakcie. Každý vydavateľ by mohol použiť akýkoľvek druh autentizačnej metódy, ale zvyčajne sa pri online nákupoch zadáva heslo spojené s kartou. Protokol Verified-by-Visa odporúča stránku banky, ktorá slúži na overenie pravosti, načítať v rámci tzv. inline frame session. Týmto spôsobom môžu byť systémy banky zodpovedné za väčšiu časť prienikov cez ich bezpečnosť. Dnes už je totiž jednoduché poslať jednorazové heslo ako súčasť textovej správy SMS na mobil alebo na e-mail klientov na autentizáciu. Alebo aspoň počas registrácie a na zabudnuté heslá tiež e-mail klientov poslúži veľmi dobre [22]. Tento proces je naznačený na obrázku č. 3.4.

Klient najprv naviaže komunikáciu so serverom pomocou webového prehliadača alebo cez aplikačné prostredie daného serveru (1. krok). Tam vyplní potrebné údaje k platbe a platobnej karte. Toto prostredie sa nazýva 3DS prostredie žiadateľa. Ďalej prebieha komunikácia od obchodníka (jeho serveru) cez adresárový server k banke aby si overil, že karta ja zalistovaná v systéme 3-D secure a overí ju server, ktorý kontroluje prístup (2. krok). Adresárový server odpovie správou, ktorá indikuje či je alebo nie je karta registrovaná (3. krok). Obchodník použije túto správu na presmerovanie klienta na stránku služby 3-D secure (4. krok). Následne prebieha komunikácia priamo medzi bankou vydavateľa, tým že klient požiada o autentizáciu a server odpovie (5. krok). Klient sa autentizuje, tým že vloží do stránky jednorázový PIN, ktorý je zaslaný väčšinou prostredníctvom SMS (6. krok). Výsledok autentizácie je preposlaný cez adresárový server až ku obchodníkovi (7., 8. krok). Obchodník posunie informácie o karte vo formáte výsledku z 3-D secure autentizácie banke nadobúdateľa (9. krok). Banka, ktorá prijíma platbu autentizuje platbu cez platobnú sieť u banky vydavateľa (10. krok).



Obr. 3.4: Princíp 3-D secure

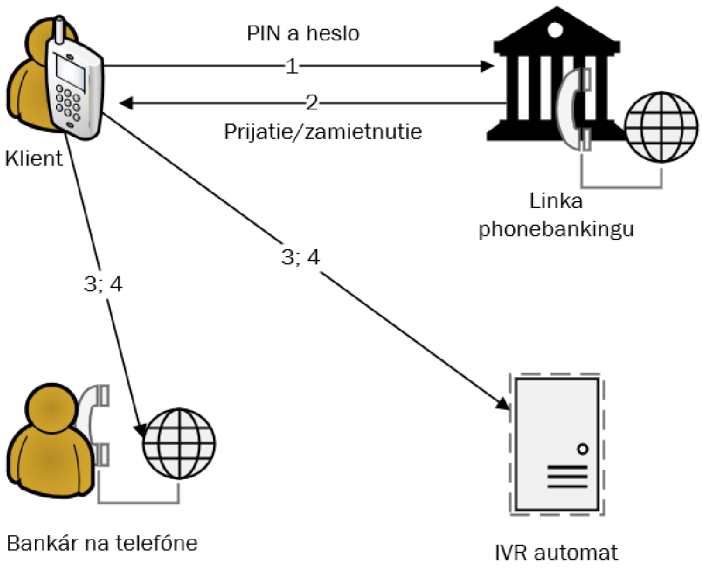
Ďalším bezpečnostným prvkom pri platobných kartách, ktorý stojí za zmienku je čip. Prevažnú časť procesorov v dnešných čipových kartách tvoria 8-bitové CISC procesory (Complex Instruction Set Computing) so 16-bitovou pamäťovou zbernicou a s inštrukčnými sadami založenými na architektúrach Motorola 6805 alebo Intel 8051 spolu s rôznymi rozšíreniami. Bezpečnosť čipovej karty vychádza z medzinárodných štandardov ISO 7816-4, EMV a ISO 10202. Bezpečnosť čipovej karty je založená na rozdelení a ochrane prístupu k jednotlivým oblastiam čipu oprávnenými subjektmi pomocou sústavy prístupových hesiel alebo kľúčov. Táto problematika je medzinárodne zjednotená normou ISO 10202. Z hľadiska bezpečnosti je dôležitá tretia časť normy, ktorá špecifikuje minimálne požiadavky na vzťahy medzi kryptografickými kľúčmi používaných na čipových kartách. V priebehu výroby karty a vytvárania jednotlivých pamäťových oblastí je prístup výrobcu zaistený pomocou produkčných kľúčov. Produkčné kľúče sú len dočasné kľúče, ktoré nesmú byť použiteľné po dokončení personifikácie karty. V priebehu personifikácie karty produkčný kľúč zaisťuje kryptografickú kontrolu zavedenia tajných parametrov na integrovaný obvod. Pokiaľ nie sú produkčné kľúče použité, zavádzanie týchto parametrov musí byť fyzicky chránené spôsobom odsúhlaseným vydavateľom karty a personifikátorom karty.

Personálne kľúče sú používané v personalizovaných procesoch, ktoré sú riadené vydavateľom platobných kariet. Tieto kľúče sú závislé na požiadavkách kariet na aplikácie a načítanie dát. Aplikačné kľúče sú vyžadované jednotlivými aplikáciami, významnými časťami systémových transakcií a personalizovaným systémom pre generovanie unikátnych kľúčov. Kryptografické prostriedky, ktoré využíva čipová karta je napríklad symetrické DES a asymetrické RSA. Vydavateľský privátny kľúč sa používa buď k overeniu statických dát uložených na karte (tzv. metóda SDA) alebo sa prostredníctvom dynamickej autentizácie dát (tzv. DDA) overuje pravosť dát uložených na karte a dát prijatých z terminálu. Súčasťou normy ISO 10202 je časť, ktorá špecifikuje metódy overenia držiteľa karty v spolupráci s čipovou kartou, spravidla pomocou PIN [23].

3.2 Phonebanking

Tiež nazývaný telebanking je aplikácia založená na komunikácii s bankou. Princíp tejto služby je jednoduchý. Schéma phonebankingu je načrtnutá na obr. č. 3.5. Klient si len zavolá na linku telefónneho bankovníctva. U väčšiny bánk je toto číslo bezplatné a možno naň volať aj z mobilného telefónu. Táto služba sa vyskytuje v dvoch verziách. V prvej verzii klient komunikuje s automatickým informačným hlasovým systémom (Interactive Voice Response - IVR). Tu je možné získavať informácie o produktoch, o aktuálnom zostatku, ale aj tu je možné zadávať príkazy na úhradu

alebo inkaso, trvalé príkazy, vykonávať konverziu mien. Niekedy je však prevádzanie transakcií obmedzené limitom a nadlimitné transakcie musia byť autorizované. Pri tejto služby je dôležité mať telefón s tónovou voľbou.



Obr. 3.5: Schéma phonebankingu

Komunikácia je zahájená tým, že klient zavolá na číslo banky, ktoré je určené na služby pre phonebanking a identifikuje sa banke na základe PINu a hesla. Banka tieto údaje overí a následne klienta príjme alebo odmietne a presmeruje hovor na službu, ktorú si klient vyberie a to môže byť buď bankár na telefóne alebo IVR automat. Obe možnosti poskytujú rovnaké služby a teda na základe žiadosti poskytnú klientovi odpoveď.

V druhej verzii klient komunikuje s telefónnym bankárom, ktorý poskytuje rovnaké služby ako pracovník na pobočke od zadávania príkazov po zakladaní termínovaných vkladov. Nevýhodou je, že mimo pracovnú dobu budete komunikovať len s hlasovým systémom.

Medzi hlavné výhody phonebankingu určite patrí rýchlosť a úspora času a skutočnosť, že táto služba nevyžaduje žiadne špeciálne technické vybavenie, je postačujúci mobilný telefón. Na druhú stranu medzi nevýhody patrí obmedzená ponuka služieb a obava klientov z možnosti zneužitia ich účtu prostredníctvom manipulácie s ich mobilným telefónom.

3.2.1 Bezpečnosť phonebankingu

Bezpečnosť je založená na identifikácii klienta a overeniu jeho totožnosti na základe jeho jedinečného identifikačného čísla (PIN) a bezpečnostného prístupového hesla. Aby bolo možné využívať služby phonebankingu vo svojej banke, musí sa zákazník najprv zaregistrovať v inštitúcii pre túto službu. Tu je zákazníkovi osobne pridelené jeho číslo (nie je rovnaké ako jeho číslom účtu) a ako druhé mu môže byť pridelené alebo si môže nastaviť vlastné heslo na jeho overenie.

Na používanie služby by klienti volali na špeciálne telefónne číslo zriadené bankou a autentizujú svoju totožnosť prostredníctvom spomínaného zákazníckeho čísla a hesla, ktoré môže pozostávať či už z čísel alebo slov, alebo prostredníctvom bezpečnostných otázok položených živým zástupcom banky. [9] Celá komunikácia, či už s bankárom alebo IVR automatom je už od začiatku šifrovaná aby sa predišlo man-in-the-middle útoku. Šifrovanie v drvivej väčšine prípadov zabezpečuje asymetrický algoritmus AES-256. Samotný systém sa po viacnásobnom neúspešnom zadávaní hesla spravidla automaticky zablokuje. Na požiadanie klientov sa môže zvýšiť stupeň ochrany autentizovaním platobných príkazov užívateľským menom a heslom. Kontrolný záznam pritom obsahuje všetky údaje o klientovi, počet položiek v súbore, dátum splatnosti atď. Ďalší prvok bezpečnosti sa využíva v prípadoch, keď banka umožňuje priame typovanie alebo importovanie údajov z a do účtovníctva svojho ekonomického informačného systému. V tomto prípade sa totiž uskutočňuje aj formálna kontrola správnosti každého platobného príkazu, to predstavuje kontrolu čísla účtu, banka a konštantný symbol.

3.3 GSM banking

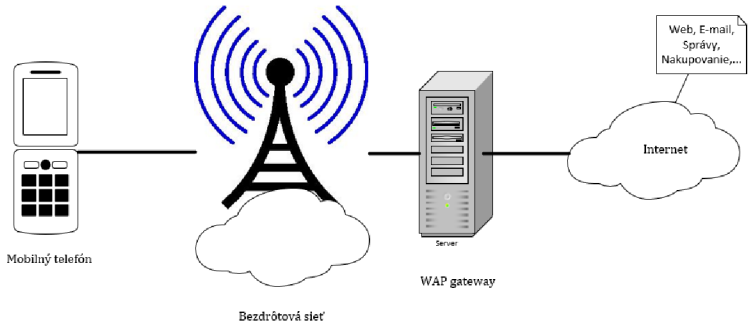
Platobný styk GSM je založený na komunikácii s bankou prostredníctvom mobilného telefónu, ktorá môže byť založená:

- prostredníctvom SMS správ,
- prostredníctvom technológie SIM Toolkit, táto možnosť je šifrovaná,
- s využitím technológie WAP.

Prvý spôsob je GSM banking prostredníctvom SMS správ, ktorého výhodou je možnosť použitia z akéhokoľvek telefónu, bez ohľadu na operátora. Komunikácia medzi bankou a klientom prebieha pomocou SMS správ. Nevýhodou je nutnosť odoslať SMS správu v presnom zadefinovanom formáte, čo vyžaduje zvýšenú pozornosť klientov.

Druhý spôsob komunikácie s bankou, SIM Toolkit, vyžaduje od klientov mať mobilný telefón s aplikáciou od banky. Pozostáva zo súboru príkazov naprogramovaných na karte SIM, ktoré definujú, ako má karta SIM komunikovať priamo s vonkajším

svetom. To umožňuje karte SIM vybudovať interaktívnu výmenu medzi sieťovou aplikáciou a koncovým používateľom a prístupom alebo riadením prístupu do siete. Karta SIM tiež vydáva príkazy pre telefón, to čo sa má zobraziť, tu patrí napríklad zobrazenie ponúk alebo vyžiadanie vstupu od klienta.



Obr. 3.6: Schéma fungovania služby WAP

Posledná služba, služba WAP, spočíva v komunikácii na internete pomocou protokolu WAP (Wireless Application Protocol). Je to v podstate kombinácia telefónneho a internetového bankovníctva. Umožňuje spojenie s bankovým účtom prostredníctvom mobilného telefónu vybaveného technológiou WAP. WAP banking ale nie je obmedzený na vlastnú SIM Toolkitovú aplikáciu. Služba WAP je založená na trojvrstvovej architektúre. Prvou časťou je tzv. mikrobrowser prítomný v mobilnom telefóne predstavujúci interface aplikácie pre užívateľov (ako WWW prehliadač). Druhú časť teda prostrednú vrstvu, predstavuje WAP gateway (vlastný server s IP adresou, umiestnenou u operátora GSM), umožňujúci preklad WAP požiadavky do ďalších externých sietí, predovšetkým internetu. Najčastejšie sa jedná o prevod WAP požiadavky na HTTP požiadavku, ktorý je poslaný na príslušný HTTP/WAP server. Treťou časťou je teda HTTP/WAP server, umiestnený v internete, spracúvajúci požiadavky a odosielajúc odpovedi užívateľovi vo formáte WML. Funkciu protokolu HTTP a formátovacieho jazyka HTML pri webe nahrádza pri WAPe protokol WAP a jazyk WML.

Použitie WAPu je jednoduché. Potom čo užívateľ otvorí mikrobrowser, je poslaná požiadavka na WAP gateway, ten požiadavku spracuje a vyžiada si odpoveď od WAP servera, po jej prijatí ju odošle späť užívateľovi na mobilný telefón. V dnešnej dobe ale už WAP nahradili moderné internetové prehliadače v mobilných telefónoch, poprípade rovno chytré telefóny s bankovými aplikáciami [9].

3.3.1 Bezpečnosť GSM bankingu

Pre bezpečnosť GSM SMS správ je použitý tzv. autentizačný kalkulátor, s pomocou ktorého si klient vygeneruje unikátny kód, ktorý následne vloží do SMS správy a banka mu späť odošle odpoveď SMS správou obsahujúcou požadovanú informáciu.

SIM Toolkit zabezpečuje šifrovanie SMS správ. Šifrovanie správ prebieha algoritmom RSA s 2048 bitovým kľúčom. Po spustení aplikácie je vyžiadané zadanie BPINu. Po zadaní všetkých požadovaných údajov v menu GSM bankovníctva je spustený prenos dát, ktorý je zabezpečený šifrovaním (algoritmus Triple DES) – správa odoslaná z mobilného telefónu je prijatá bankou iba vtedy, keď je zašifrovaná správnym šifrovacím kľúčom. Správy zaslané na mobilný telefón klienta sú šifrované a ukladajú sa do zvláštnej schránky nedostupnej bez BPINu. Následne je táto šifrovaná správa automaticky odoslaná na určené telefónne číslo do banky. Tu je správa prenesená do systému a klientovi pošle potvrdenie o prijatí k ďalšiemu spracovaniu.

Triple DES je definovaný štandardom FIPS 46-3. FIPS (Federal Information Processing Standards) je súbor štandardov, ktoré popisujú spracovanie dokumentov, šifrovacie algoritmy a ďalšie štandardy informačných technológií, ktoré sa používajú v nevojenských vládnych agentúrach a vládnymi dodávateľmi a predajcami, ktorí spolupracujú s agentúrami. Jedná sa o symetrický šifrovací algoritmus s dĺžkou kľúča 128 alebo 192 bitov (112 alebo 168 bitov pri 56 bitovej dĺžke kľúča pre DES) a šifrovaným blokom dĺžky 64 bitov založeným na algoritme DES.

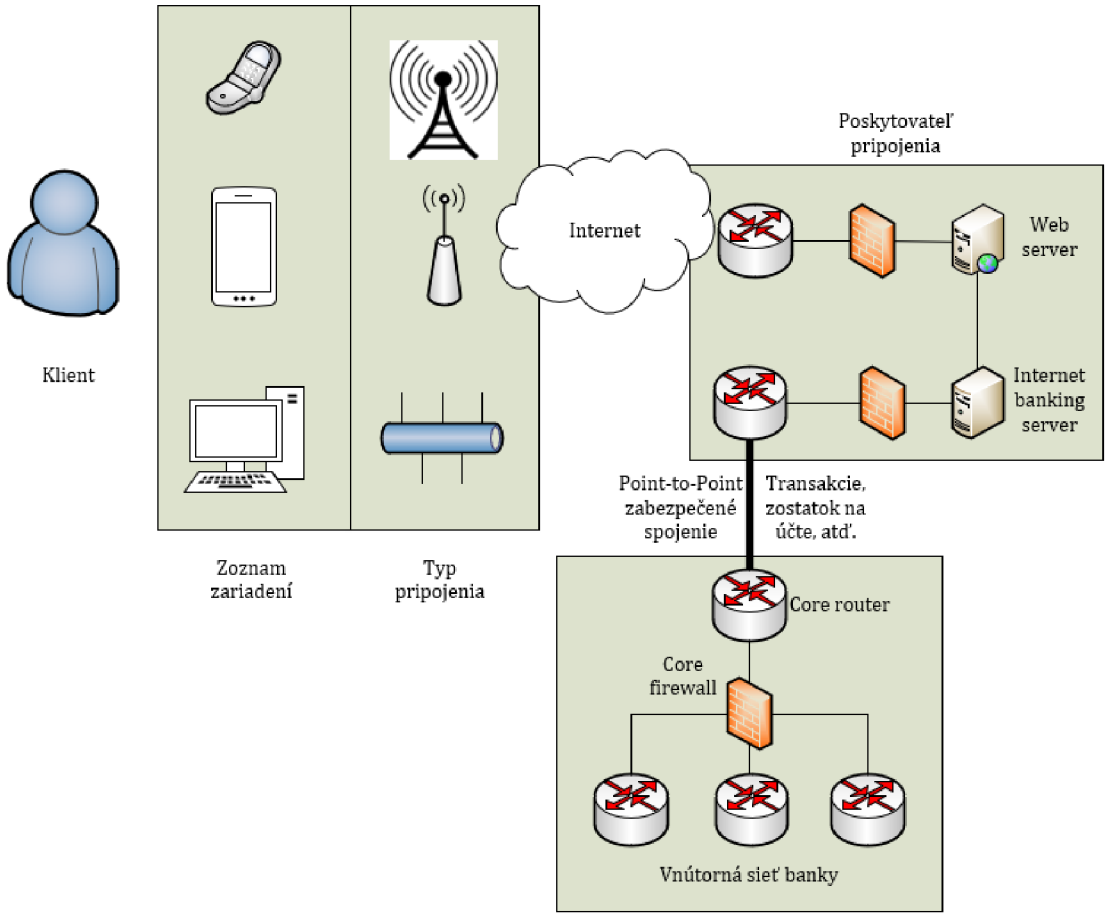
Prenos informácií medzi mikrobrowserom a WAP gateway môže byt realizovaný niekoľkými dátovými službami. Pomocou mobilného telefónu a autorizačného kľúča je možné zadávať napr. príkazy na úhradu, zisťovať zostatok na účte aj informácie o jeho histórii, zriaďovať termínované vklady alebo zistiť aktuálne kurzy [9].

Medzi hlavné potencionálne hrozby v systéme GSM patrí napríklad Man in the Middle Attack, nedostatočná viditeľnosť pre používateľov, zraniteľnosť voči útoku Denial of service (Dos) a zraniteľnosť pri opakovaných útokoch. Ako riešenia sa navrhli napríklad použitie bezpečných algoritmov pre implementácie A3/A8, ktoré môžu chrániť kartu SIM pred akýmkoľvek útokom klonovania [24].

3.4 Internetbanking

Najznámejšou formou elektronického bankovníctva je internet banking. Ide vlastne o domáce bankovníctvo, ktoré je výhodné aj pre klienta ale aj banku samotnú. Pomocou internetbankingu je možné sledovať svoje pohyby na účtoch, prezerať si zostatky na účtoch a zadávať príkazy na inkaso či trvalé príkazy ale aj rôzne iné operácie. To ako vyzerá v dnešnej podobe internetbanking môžeme vidieť na obr. č. 3.7.

Internetbanking, ktorý poznáme dnes, využíva internetovú sieť a bežný webový prehliadač spolu s bezpečnostnou nadstavbou SSL. Klient sa prihlasuje do systému banky a po overení prostredníctvom elektronického osobného kľúča (EOK) alebo cez elektronické podpisy a digitálne certifikáty, či je daný klient oprávnený vykonávať dané úkony sa klient prihlási na webové stránky svojej banky kde priamo môže zadávať príkazy. Najväčšou výhodou je bezpochyby to, že všetky úkony môže klient vykonávať z pohodlia domova a má k ním neustále prístup [9].



Obr. 3.7: Architektúra internetbankingu

3.4.1 Bezpečnosť internetbankingu

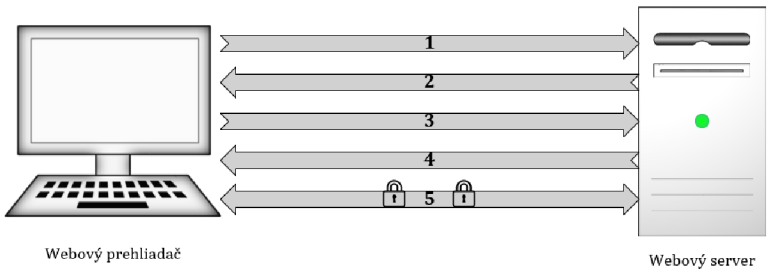
Secure Sockets Layer (SSL) je štandardizovaná bezpečnostná technológia na vytvorenie šifrovaného spojenia medzi serverom a klientom - zvyčajne webovým serverom a prehliadačom. SSL umožňuje bezpečný prenos citlivých informácií, ako sú čísla

kreditných kariet a prihlasovacie údaje. Údaje odosielané medzi prehliadačmi a webovými servermi sú zvyčajne odosielané vo forme plain textu, čo predstavuje veľké riziko.

Naviazanie SSL spojenia sa skladá z niekoľko častí:

1. Prehliadač sa pripojí na webový server (web) zabezpečený pomocou SSL (https). Aby prehliadač mohol fungovať požaduje sa od serveru aby sa sám identifikoval.
2. Server odošle kópiu svojho certifikátu SSL spolu s verejným kľúčom serveru.
3. Prehliadač skontroluje root certifikát zo zoznamu dôveryhodných CA, ktorých databázu má uloženú, a zisťuje či je certifikát platný, nevypršala mu platnosť, či mu verí a kontroluje aj jeho bežný názov či je platný pre webovú stránku, ku ktorej sa pripája. Ak prehliadač dôveruje certifikátu, tak vytvorí, zašifruje a odošle späť symetrický kľúč relácie pomocou verejného kľúča servera.
4. Server dešifruje symetrický kľúč relácie pomocou svojho súkromného kľúča a pošle späť potvrdenie (ACK) zašifrované pomocou kľúča relácie na spustenie šifrovanej relácie.
5. Server a prehliadač teraz šifrujú všetky prenášané údaje pomocou kľúča relácie.

Názornosť krokov je zobrazená na obrázku č. 3.8.



Obr. 3.8: Vytvorenie SSL spojenia

Všetky prehliadače sú schopné interagovať so zabezpečenými webovými servermi pomocou protokolu SSL. Prehliadač a server však potrebujú to, čo sa nazýva SSL certifikát, aby bolo možné vytvoriť zabezpečené pripojenie. SSL zabezpečuje každý deň milióny údajov o ľuďoch na internete, najmä pri online transakciách. To, že je daná internetová stránka zabezpečená dokážeme poznať podľa zeleného zámku, ktorý sa zobrazí pri rámčeku, kde zadávame internetovú adresu webovej stránky. Webové stránky zabezpečené pomocou SSL tiež začínajú https a nie http.

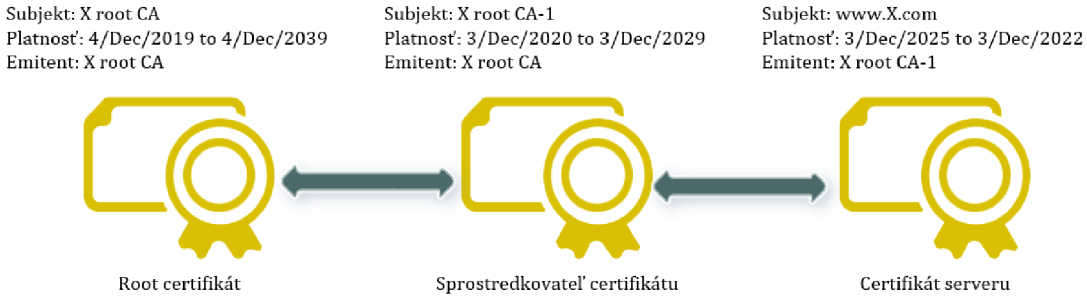
Počas prvej fázy ustanovenia bezpečného spojenia si klient a server dohodnú kryptografické algoritmy, ktoré budú použité. V dnešnej implementácií to môžu byť tieto:

1. pre výmenu kľúčov: RSA, Diffie-Hellman;
2. pre symetrickú šifru: RC2, RC4, IDEA, DES, 3DES alebo AES;
3. pre jednocestné hashovacie funkcie: rodina hashovacích funkcií SHA [25].

Public Key Infrastructure (PKI) je sada hardvéru, softvéru, ľudí, politík a postupov, ktoré sú potrebné na vytváranie, distribúciu, používanie, ukladanie a rušenie digitálnych certifikátov. PKI je tiež to, čo viaže kľúče s totožnosťou užívateľa prostredníctvom certifikačnej autority (CA). PKI používa hybridný kryptosystém a ťaží z používania oboch typov šifrovania. Kľúč relácie, ktorý server a prehliadač vytvárajú počas SSL handshake, je symetrický.

Na zisk certifikátu, je potrebné na svojom serveri vytvoriť Certificate Signing Request (CSR). Tento proces vytvorí serveri súkromný kľúč a verejný kľúč. Dátový súbor CSR, ktorý odošlete vydavateľovi certifikátu SSL (nazývaný certifikačná autorita alebo CA), obsahuje verejný kľúč. CA používa dátový súbor CSR na vytvorenie štruktúry údajov, ktorý sa zhoduje so súkromným kľúčom bez toho, aby sa ohrozil samotný kľúč. CA nikdy nevidí súkromný kľúč. Po prijatí certifikátu SSL ho nainštalujete na svoj server. Nainštalujete tiež prechodný certifikát, ktorý preukáže dôveryhodnosť vášho certifikátu SSL jeho prepojením s koreňovým certifikátom vašej CA. Pokyny na inštaláciu a testovanie certifikátu sa odlišujú v závislosti od typu servera.

Na obrázku č. 3.9 je zobrazený reťazec certifikátov, ktorý prepojí serverový certifikát s koreňovým certifikátom CA prostredníctvom sprostredkovateľa certifikátu.



Obr. 3.9: Reťazec certifikátov

Najdôležitejšou súčasťou certifikátu SSL je to, že je digitálne podpísaný dôveryhodnou CA. Certifikát môže vytvoriť ktokoľvek, ale prehliadače dôverujú iba certifikátom, ktoré pochádzajú od organizácie na zozname dôveryhodných CA. Keď si inštalujeme prehliadače tak už v sebe majú predinštalovaný zoznamom dôveryhodných CA, známych ako Trusted Root CA store. Na to aby sa spoločnosť mohla pridať

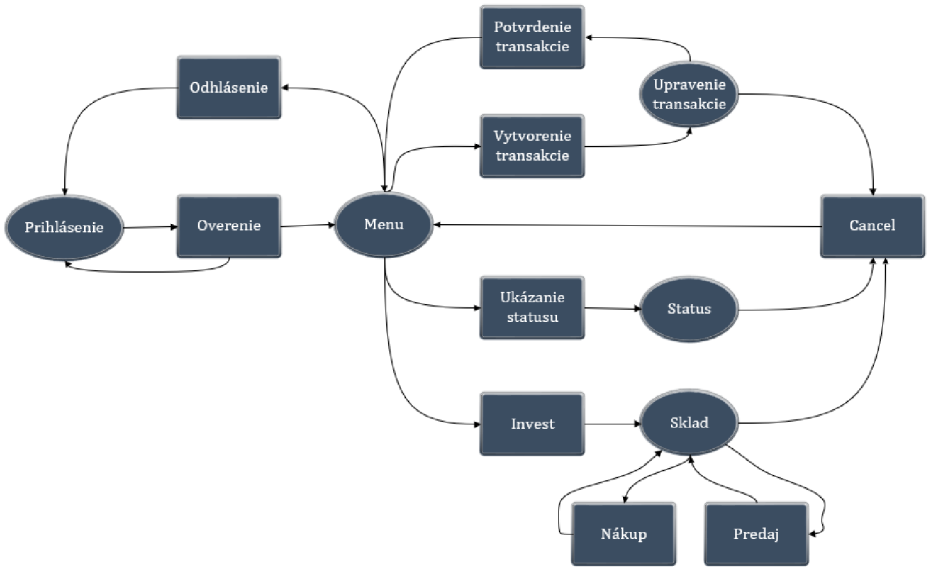
do zoznamu dôveryhodných root CA a stať sa tak certifikačnou autoritou, musí dodržiavať štandardy zabezpečenia a autentizácie stanovené prehliadačmi. Certifikát SSL vydaný organizáciou CA a jej doménou/webovou stránkou overuje, či dôveryhodná tretia strana overila totožnosť tejto organizácie [25].

3.5 Homebanking

Služba homebanking patrí medzi najstaršiu a najpoužívanejšiu službu elektronického bankovníctva, určenou najmä pre inštitucionálnych klientov, malých a stredných podnikateľov a firmy, ktoré majú záujem o rýchlejšiu formu komunikácie s bankou. Homebanking má v celosvetovom meradle začiatky v 80 rokoch minulého storočia.

Prostredníctvom služby homebanking môže klient komunikovať priamo s pobočkou banky, ktorá vedie jeho účet a to 24 hodín denne, 7 dni v týždni. Klient môže uskutočňovať tuzemské a zahraničné platby, zadávať inkasa, alebo trvalé príkazy. Výhodou pre firmy a podnikateľov je možnosť prepojenia platobného styku s účtovníctvom klienta.

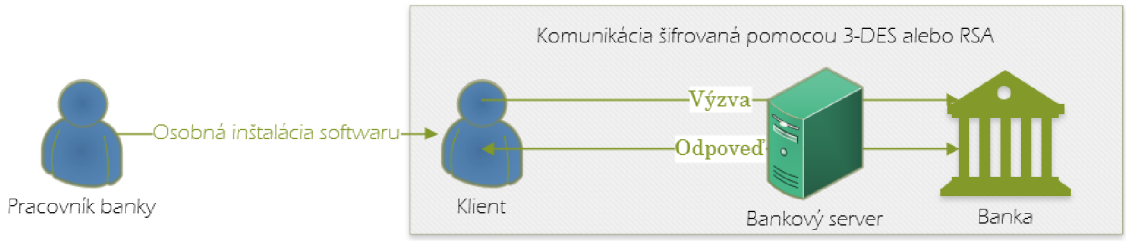
Nevýhodou tejto služby je to, že je viazaná na konkrétny počítač a je inštalácia aplikácie alebo prípadné zmeny alebo opätovná inštalácia u klienta je pomerne nákladná. Ďalšou nevýhodou môže byť neaktuálnosť informácií, ktorá vyplýva z off-line režimu, ktorý je vyžadovaný pre zvýšenie bezpečnosti. Príklad ako služba homebanking môže fungovať a čo môže ponúkať môžeme vidieť na obrázku č. 3.10.



Obr. 3.10: Ponuka služieb homebankingu

3.5.1 Bezpečnosť homebankingu

Identifikácia klienta je realizovaná užívateľským menom a prístupovým heslom. Prenášané údaje sú kódované symetrickou šifrou DES. resp. 3-DES, každú správu z finančnej transakcie klient potvrdzuje elektronickým podpisom, založenom na asymetrickom šifrovaní RSA (s voliteľnou dĺžkou kľúča 512-2048 bitov). V prípade záujmu klienta je možné zvýšiť bezpečnosť uložením RSA kľúčov na čipovú kartu. V tomto prípade je potrebné pripojenie čítačky čipových kariet na paralelný alebo sériový port osobného počítača klienta. Inou modifikáciou zvyšovania bezpečnosti je podpisovanie každej finančnej úhrady, ktoré sa podpisujú jednotlivo a samostatne, samostatne sa overuje aj autentičnosť. Banka a klient vlastní dvojicu kľúčov (verejný a privátny), pričom komunikácia medzi bankou a klientom je uskutočniteľná len po vzájomnej výmene verejných kľúčov. Rozšíreným systémom pre službu homebanking je systém MultiCash. Systém MultiCash je založený na komunikácii klient-banka prostredníctvom bankového serveru. Údaje prenášané cez túto službu majú len jeden stupeň ochrany a tou je elektronický podpis. Systém MultiCash je určený pre klientov, ktorý odovzdávajú na spracovanie väčšie množstvo príkazov [9]. Priebeh komunikácie v službe homebanking viz obrázok č. 3.11.



Obr. 3.11: Priebeh komunikácie homebankingu

4 BEZKONTAKTNÉ PLATBY S NFC

Jedná sa o platobnú funkcionalitu, ktorá zrýchľuje a zjednodušuje platenie za tovar a za služby nízkej ceny. Bezkontaktná platba je spravidla rýchlejšia varianta platenia. Limit takejto platby je väčšinou do 20 eur čo odpovedá momentálne približne 500 Kč. Namiesto vloženia karty do POS terminálu stačí chytré zariadenie jednoducho priložiť. Ak však zákazník platí viac ako je stanovený limit pre platbu bez overenia, musí sa autentizovať. A to buď zadaním čísla PIN alebo biometriou či už odtlačkom prstu alebo nasnímaním tváre. To ako sa užívateľ overí je na ňom a na možnostiach chytrého telefónu aké technológie podporuje.

4.1 Platby NFC

Skratkou NFC – Near Field Communication sa označuje bezdrôtová komunikácia medzi zariadeniami ako sú chytré telefóny, tablety alebo chytré hodinky, chytré telefóny a ďalšie. NFC poskytuje rýchlu a bezpečnú výmenu dát do vzdialenosti 4 cm. NFC stačí menej ako 100 ms.

Zo začiatku platby NFC podporovala hŕstka bánk, postupne ho ale zaviedli aj ďalšie. Nasledovali systémy Apple Pay, Garmin Pay a Fitbit Pay. [5] Mobilné telefóny, ktoré túto technológiu využívajú, môžu NFC využiť pre prenos dát u rôznych užívateľských systémov ako sú prístupové systémy, mikroplatby, dátové transakcie a podobné. NFC vzniklo z RFID technológie (Radio Frequency Identification). Veľký prelom nastal po roku 2004 keď sa táto technológia postupne začala implementovať do mobilných zariadení. Platforma Android uvoľnila poprvýkrát aplikačné rozhranie NFC vo verzii 2.3. Od verzie Androidu 4.4 KitKat sa pridala aj podpora pasívneho NFC, čo umožnilo emulácie čipovej karty. NFC disponuje prenosovou rýchlosťou 106, 212 alebo 426 kb/s pri frekvencii 13,56 MHz s kódovaním Manchester.

Technológia NFC na platforme Android podporuje tieto štandardy:

- NFC-A (ISO 14443-3A),
- NFC-B (ISO 14443-3B),
- NFC-F (JIS 6319-4),
- NFC-V (ISO 15693),
- ISO-DEP (ISO 14443-4),
- NDEF.

Komunikácia cez NFC je v aplikácii realizovaná pomocou špeciálnych správ, tzv. intent. Napríklad pri prečítaní NFC tagu dochádza k intentu, ktorý je ďalej spracovávaný aplikáciou. Je tiež možné nakonfigurovať reakcie na určité typy tagov [28].

4.1.1 Ako funguje NFC

Pri dotyku alebo priblížení dvoch zariadení s NFC sa automaticky spustí ich komunikácia. NFC funguje na báze krátkych rádiových vĺn, má veľmi nízku spotrebu a na rozdiel od technológie Bluetooth umožňuje aj vytvorenie pasívnych bodov, tzv. „tagov“. Tie sa jednoducho nalepia na potrebné miesto a slúžia k tomu k čomu budú naprogramované. Medzi bežné situácie kde sa dá využiť NFC patria mikrotransakcie ale NFC nám ponúka aj napríklad rýchly prenos kontaktov.

NFC v mobile možno využiť hneď s pomocou niekoľkých aplikácií, či už sa jedná o NFC iOS alebo NFC Android aplikácie. Pre platobné úkony sú všeobecne považované najlepšie už spomínané Apple Pay a Google Pay. Väčšina spoločností vyvinuli vlastnú verziu a teda o výbere aplikácie sa môže rozhodnúť značka telefónu. Medzi najznámejšie patrí NFC Reader, ktorý ponúka možnosť prečítať ľubovoľné tagy a zobraziť ich správu. Alebo pomocou NFC Tools (Android) a NFC Actions (iOS) je možné si naprogramovať vlastný NFC tag. Stačí naskenovať NFC tag a zvoliť inštrukcie [5]. Základným princípom technológie NFC je magnetická indukcia kde zdroj signálu, tag, generuje okolo seba elektromagnetické pole. Cieľové zariadenie, prijímač, ktoré je v dosahu tohto poľa, vytvorí magnetickú väzbu so zdrojom prostredníctvom magnetickej indukcie.

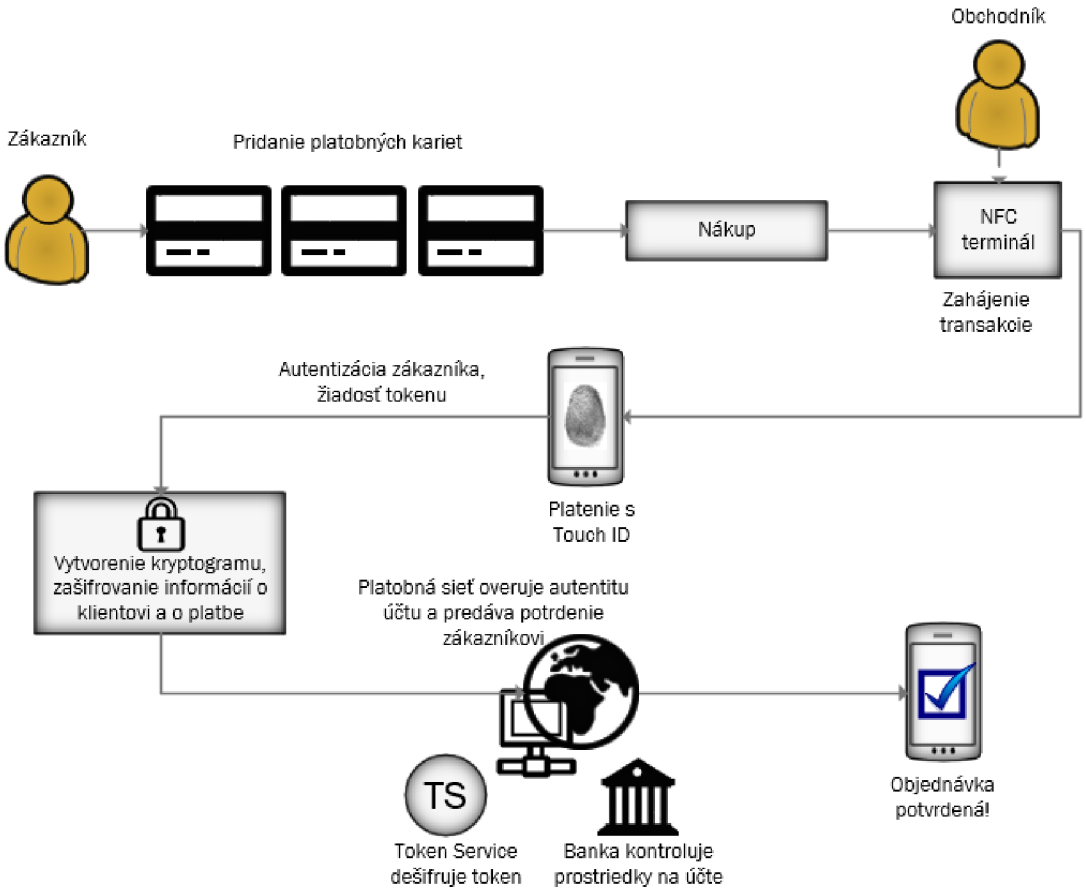
Obr. 4.1: Režimy komunikácie NFC

U NFC rozlišujeme tri režimy komunikácie, viz obr. č. 4.1:

- peer-to-peer režim - P2P komunikácia (napr. funkcia Android Beam),
- read/write režim - komunikácia medzi aktívnym zariadením a NFC tagom. Cieľom tejto komunikácie je čítanie alebo zapisovanie dát z / do pamäte NFC tagu pomocou správ NDEF (NFC Data Exchange Format),
- card Emulation režim - v tomto režime sa aktívne NFC zariadenie správa ako pasívny NFC tag. Je to režim, ktorý napodobňuje používanie bezkontaktných platieb. Od verzie Android 4.4 možno telefón použiť ako čipovú kartu kompatibilnú s normou ISO / IEC 14443 [28].

4.1.2 Priebeh platby

NFC platby sú jednoduché. V ideálnom prípade banka podporuje Google Pay alebo Apple Pay. V tom prípade sa s danou aplikáciou spáruje platobná karta a všetko je pripravené. V obchode je potom nutné len telefón odomknúť napríklad pomocou odtlačku prsta a priložením mobilu k terminálu. Platba prebieha rovnako ako v prípade platobnej karty. Niekedy sa stáva, že banka vyžaduje kvôli NFC platbám vlastnú aplikáciu a tam je potrebné pridať platobnú kartu a teda nestačí len aplikácia banky. Vlastné aplikácie ponúkajú napríklad ČSOB, Raiffeisenbank a Air bank. Koncom roku 2019 už všetky banky podporujú platby pomocou NFC. Celý priebeh platby môžeme vidieť na obrázku č. 4.2.



Obr. 4.2: Priebeh NFC platby

Platenie mobilom je oproti platbe bežnou bezkontaktnou platobnou kartou a bezpečnejšie. NFC platby nevyžadujú aktívne dáta alebo pripojenie na WiFi, teda všade, kde majú platobný terminál je možné zaplatiť. Ďalšie výhody NFC plynú

zo škálovateľnosti platobných aplikácií. Aplikácie podporujú mať uložených viac kariet, či už kreditné, debetné. A medzi nimi je možnosť ľubovoľne prepínať podľa toho, ktorú kartu chceme práve použiť. Jednou z výhod môže byť aj to, že pri platbe akoukoľvek kartou je zadávaný PIN, ktorý bol zvolený pri aktivácii aplikácie. Poslednou výhodou je považovaná prípadná strata mobilného telefónu. Prípadná strata mobilu s uloženými kartami nie je tak kritická pretože môžeme na diaľku zablokovať aplikáciu a vymazať z nej všetky údaje.

Jedným z problémov platenia NFC môže byť jeho kompatibilita s operačným systémom telefónu. Problém rovnako nastáva, keď obchodník nedisponuje s terminálom, ktorý je schopný ľahko načítať NFC kartu v mobile. Tento prípad sa však nedeje často.

4.1.3 Bezpečnosť platby

Metóda NFC neposiela číslo platobnej karty pri platbe ani ho neukladá do telefónu. Pri platbe sa vytvorí virtuálny kód, ktorý sa priradí k jednotlivej transakcii. Pri nízkych sumách stačí telefón „prebudiť“, a pri platbe nad 20 eur treba zadať PIN alebo odomknúť obrazovku. Veľkou výhodou je, že pri strate mobilného zariadenia je možné ho uzamknúť na diaľku novým heslom alebo vymazať celý obsah. Nie je teda potreba podstupovať blokáciu karty a vystavenie novej, ako je tomu pri jej strate [29]. Pri platbe mobilom prostredníctvom NFC sa pri výmene kľúčov využíva niekoľko algoritmov, ktoré rovnako slúžia aj pri autentizácii, zaistení integrity a dôvernosti. Medzi najrozšírenejšie patrí TripleDES, DSA, RSA, AES, alebo kryptografia založená na eliptických krivkách. Týmito algoritmami sa predchádza možnému man-in-the-middle útoku, ku ktorému dochádza často prostredníctvom prepojovacieho útoku.

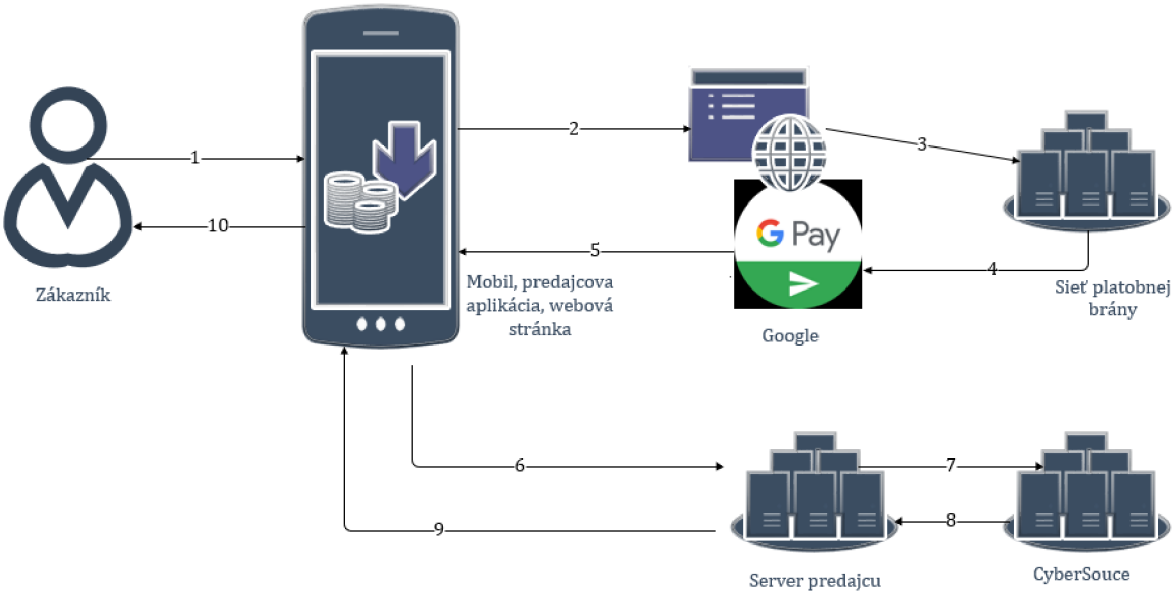
4.2 Google Pay

Je to rýchly jednoduchý spôsob platenia prostredníctvom Googlu. Logo, ktoré sa je potreba hľadať ak chceme zistiť či je možné platiť prostredníctvom tejto služby je na obrázku č. 4.3. Google Pay dorazil do Českej republiky v roku 2017, na Slovensku to bolo o niečo neskôr a to presnejšie vo februári roku 2018.

V tejto časti je ukázané ako podľa obrázku č. 4.4 prebieha platba na službe Google Pay a ako sa vymieňajú informácie medzi jednotlivými entitami.

1. Zákazník zvolí platbu cez Google. Použitím rozhrania Google API systém iniciuje žiadosť, ktorá je šifrovaná (napr. AES), o platbu prostredníctvom Google

Obr. 4.3: Logo Google Pay (Zdroj:<shorturl.at/fTX38>)



Obr. 4.4: Priebeh platby v Google Pay

Pay, ktorá ako platobnú bránu identifikuje kybernetický zdroj, pričom ako obchodného partnera brány použije ID obchodníka.

2. Zákazník potvrdí šifrovanú žiadosť o platbu. Rozhranie Google API kontaktuje služby Google Pay a zisťuje parametre platby zákazníka.
3. Ak údaje o platbe od zákazníka sú už tokenizované alebo sa práve tokenizuje nová platba, služba Google Pay kontaktuje príslušnú platobnú sieť a načíta vhodný kryptogram.
4. Platobná sieť vráti príslušný token a kryptogram službe Google Pay.
5. Google vytvára šifrované údaje o platbe pomocou kľúča špecifického pre bránu, ktorý je dodávaný v žiadosti o peňaženku, a je zahrnutý do odpovede rozhrania Google API.
6. Spätné volanie Google Pay vráti šifrované platobné údaje.
7. Systém nachystá informácie s odpoveďou Google Pay na predloženie pre službu CyberSource.

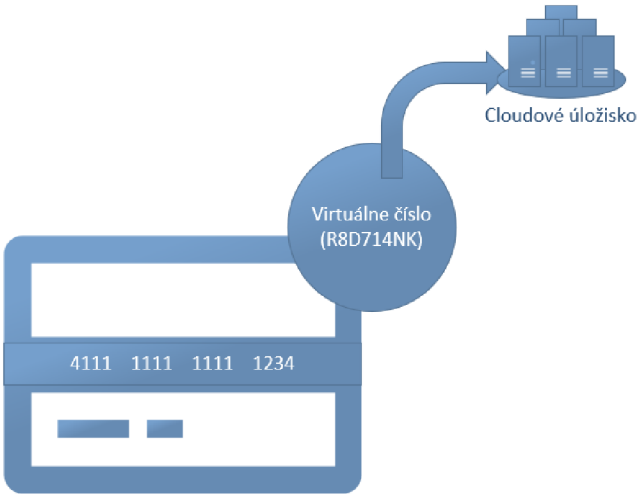
(a) CyberSource odošle požiadavku na autorizáciu pre nadobúdateľa.
(b) Nadobúdateľ spracuje požiadavku z CyberSource a vytvorí žiadosť o autorizáciu platobnej siete.
(c) Platba sieť spracováva žiadosť nadobúdateľa a vytvorí žiadosť o povolenie vydavateľa.
(d) Emitent spracováva žiadosť o platbu siete. Emitent vyhľadá informácie o platbe a vracia schválenú alebo zamietnutú autorizačnú správu do platobnej siete.
(e) Platobná sieť vráti autorizačnú odpoveď nadobúdateľovi.
(f) Nadobúdateľ vráti autorizačnú odpoveď službe CyberSource.

8. CyberSource vráti autorizačnú odpoveď do systému.
9. Systém vracia autorizačnú odpoveď na platobnú aplikáciu.
10. Aplikácia platby zobrazí zákazníkovi správu s potvrdením alebo odmietnutím.
    (a) Nadobúdateľ predloží žiadosť o vyrovnanie emitentovi za prostriedky.
    (b) Emitent dodáva prostriedky nadobúdateľovi na autorizované transakcie [6].

Na využívanie služby Google Pay je potrebné splňovať niekoľko podmienok. Základnou podmienkou je mať v telefóne aplikáciu Google Pay. Okrem debetných a kreditných kariet je možné do aplikácie nahrať aj vernostné karty obchodníkov. Je nutné ale vlastniť telefón či tablet s operačným systémom Android 4.4 a novším. A poslednou dôležitou podmienkou je, že banka, ktorú klient používa musí podporovať Google Pay.

4.2.1 Bezpečnosť Google Pay

Technika zabezpečenia pre Google Pay je tzv. tokenizácia, ktorá namiesto skutočného čísla karty využíva špeciálne vytvorený šifrovaný kód. Bezpečnosť Google Pay zabezpečuje technológia HCE (Host Card Emulation). Táto služba využívajúca emulované platobné karty, ktoré sú nahrané priamo v aplikácii v telefóne. A každá táto karta má priradené virtuálne číslo účtu, ktorý sa používa pri platbách namiesto pravého čísla karty a toto číslo je uložené na cloudovom úložisku čo je hlavný rozdiel oproti Apple Pay, kde je číslo uložené priamo na telefóne (obr. č. 4.5). Číslo vašej karty nie je vo vašom mobile nikde uložené a ani obchodník, u ktorého nákup vykonávate, sa ho nikdy nedozvie. Platbu je z bezpečnostných dôvodov obmedzená na 30 sekúnd a ak sa do tej doby neprevedie je automaticky zrušená. Na to aby karta mohla byť úspešne pridaná do aplikácie tak musí byť overená. Overenie prebieha v dvoch krokoch. Buď môže byť z účtu strhnutá veľmi malá čiastka napríklad v halieroch, ktorá bude následne v priebehu 24 hodín vrátená späť na účet alebo banka môže požiadať o zadanie kódu, ktorý nám príde v podobe SMS alebo e-mailu [30].



Obr. 4.5: Ukladanie čísla karty na cloud

4.3 Apple Pay

Apple Pay je jednoduché platenie iPhonom alebo pomocou smart hodiniek Apple Watch na všetkých bezkontaktných platobných termináloch. Jeho logo, ktoré sa dá nájsť v obchodoch, ktoré prijímajú platbu prostredníctvom neho je na obrázku č. 4.6. Všetko funguje na princípe NFC. Pri každej platbe je potreba sa jednoznačne autentizovať a to buď zadaním PIN kódu alebo biometriou, Face ID alebo Touch ID. Apple Pay do Českej republiky dorazil 19.2. 2019 a na Slovensko so štvrťročným oneskorením 26.6. 2019. Atypická vec na ktorú treba myslieť je to, že Apple Watch pre platby vystupujú ako samostatné zariadenie a aj preto treba do hodiniek pridať platobnú kartu zvlášť. V prípade hodiniek už ani nie je potreba autorizácia pri platení pretože hodinky autorizujú užívateľa hneď pri nasadení na ruku.

Pay

Obr. 4.6: Logo Apple Pay (Zdroj:<shorturl.at/nAJN8>)

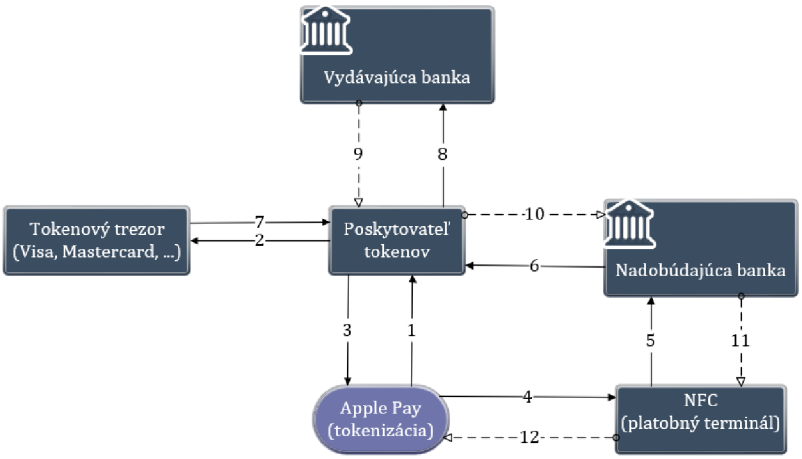
Platobná služba Apple Pay je pochopiteľne zviazaná s produktami od Apple a je podporovaná a dostupná na týchto zariadeniach: iPhone SE, iPhone 6 a vyššie rady, všetky Apple Watch Series, iPad mini 3 a 4, iPad Air 2, iPad 5. a 6. generácia a Macbooky uvedené na trh od roku 2012 v kombinácii s Iphonom alebo Apple

Watch. Apple Pay funguje v spolupráci s kartovými asociáciami (Visa, MasterCard) a jednotlivými bankami. Je teda nutné, aby banka službu podporovala. Momentálne Apple Pay v Česku a na Slovensku podporujú už takmer všetky banky [7].

4.3.1 Bezpečnosť Apple Pay

Bezpečnosť Apple Pay ťaží z úplne uzavretého systému, ktorý má Apple pod kontrolou. Aj tu sa používa tzv. tokenizácia a detaily platobnej karty nepozná Apple a samozrejme sa ich nedozvie ani obchodník. Tokenizácia tu funguje tak, že zadáme číslo svojej platobnej karty do aplikácie, potom sa toto číslo zašifruje a odošle na servery Apple. Servery dešifrujú číslo účtu, pridajú platobnú sieť platobnej karty k informáciám o čísle účtu a potom ju zašifrujú pomocou kľúča, ktorý je možné odomknúť iba prostredníctvom platobnej karty. Spoločnosť vydávajúca platobné karty od spoločnosti Apple prijme tieto zašifrované informácie, dešifruje ich, autorizuje použitie karty v službe Apple Pay a potom vytvorí číslo DAN (Device Account Number). Toto číslo DAN je iné ako číslo kreditnej karty (ktoré je stále pripojené k existujúcemu účtu platobnej karty), ktoré používa iba konkrétny telefón. Spoločnosť vydávajúca platobné karty šifruje toto číslo DAN, odošle ho spoločnosti Apple (ktorá NEMÁ kľúč na jeho opätovné dešifrovanie) a spoločnosť Apple potom pridá šifrované číslo DAN do zabezpečeného prvku (secure element). Spoločnosť Apple nemá číslo účtu potrebné na uskutočnenie platby a tak iba telefón môže dešifrovať číslo účtu potrebné na vykonanie platby. Platobnému terminálu je počas transakcie odovzdané iba špeciálne ID, vďaka ktorému banka platbu potvrdí. Platobná karta tak nie je umiestnená v službe iCloud a je nutné ju na každé zariadenie pridať samostatne. IPhone (prípadne Apple Watch) má všetky potrebné údaje priamo uložené v zariadení a s terminálom komunikuje na krátku vzdialenosť pomocou NFC [7]. Spôsob výmeny informácii v službe Apple pay je zobrazený na obr. č. 4.7.

1. Predanie informácií o karte (4111 1111 1111 1234)
2. Vydanie tokenu
3. Zašifrovaný token (4123 **** **** 9876)
4. Prijatie tokenu na platobnom termináli (4123 **** **** 9876)
5. Token s údajmi o transakcii poslaný nadobúdajúcej banky (4123 **** **** 9876, 50€)
6. Overenie tokenu s údajmi o transakcii u jeho poskytovateľa(4123 **** **** 9876, 50€)
7. Dešifrovanie tokenu (4111 1111 1111 1234)
8. Overenie informácii o karte a autorizácia platby (platnosť, identita,. . .)
9. Schválenie a zaslanie výsledku
10. 11. 12. Preposlanie výsledku



Obr. 4.7: Výmena informácií v Apple pay

4.4 Garmin Pay

Garmin Pay je podobne ako Google Pay alebo Apple Pay efektívnym riešením pre bezkontaktné platby. Rovnako taktiež funguje na princípe NFC. Na rozdiel od Google Pay a Apple však u seba nemusíme mať ani mobil pretože všetko prebieha len s vybranými hodinkami Garmin. Aktivácia tzv. peňaženky na hodinkách Garmin prebieha v prostredí Garmin Connect. Do hodiniek sa zadávajú potrebné údaje – číslo karty, platnosť, CVV kód, ale aj osobne vytvorený štvormiestny PIN kód slúžiaci na zabezpečenie informácií a platieb. Tento PIN kód nemusí byť rovnaký ako PIN na platobnej karte. Aktivácia peňaženky sa ukončí autorizáciou v banke, zvyčajne pomocou SMS správy alebo zákazníckej podpory, ktorej kontakt sa zobrazí v poslednom kroku aktivácie na mobile.

Hodinkami Garmin sa dá platiť všade tam kde majú bezkontaktné platobné terminály a to bez ohľadu na krajinu kde sa nachádzame. Platba sa vykoná tak, že v hodinkách treba aktivovať virtuálnu peňaženku. Po jej zapnutí hodinky Garmin požiadajú o zadanie štvormiestneho PIN kódu, čím sa služba aktivuje a začne prebiehať približne jedna minúta slúžiaca na priloženie inteligentného zariadenia k bezkontaktnému platobnému terminálu. V prípade, že čas vyprší o niečo skôr, stačí len znovu virtuálnu peňaženku otvoriť. Výhodou je, že pri druhej alebo aj ďalšej platbe už PIN zadávať netreba, v priebehu 24 hodín alebo kým hodinky nezložíme z ruky, tak si ho hodinky pamätajú. Zneužite je značne obmedzené pretože akonáhle sa hodinky zložia zo zápästie znovu sa vyžaduje prístupový kód [8].

4.4.1 Bezpečnosť Garmin pay

Aj pri platbe cez Garmin Pay je bezpečnosť riešená pomocou jedinečného tokenu, ktorý je šifrovaný. Citlivé údaje sa dokonca neukladajú ani na server spoločnosti Garmin. Pri strate hodiniek službu Garmin Pay možno tiež zablokovať prostredníctvom zákazníckeho centra banky. Veľkým rozdielom oproti predošlým službám je, že ani platbu nad 20 € na pokladni nie je potreba autentizovať opakovaným zadávaním PIN kódu na termináli ale stačí zadanie PIN kódu na hodinkách.

Hodinky sú kompatibilné so systémami Android aj iOS. Platbu pomocou Garmin Pay podporujú tieto modely: D2 Delta (S, PX), Fenix 5 Plus, 5S Plus, 5X Plus, Forerunner 645, Vivoactive 3. V zahraničí je mnoho bánk, ktoré už službu Garmin Pay podporujú. Do Českej a Slovenskej republiky sa dostal Garmin Pay o niečo neskôr. V oboch krajinách sa však predpokladá a očakáva plná podpora od všetkých bánk [8].

5 WEBOVÁ APLIKÁCIA

Práca je zameraná na rozbor a opis techník, ktoré sa využívajú v elektronickom bankovníctve. Na základe uvedenej analýzy je navrhnutá a realizovaná aplikácia, ktorá demonštruje prehľad elektronického bankovníctva a jeho bezpečnosť. V rámci semestrálneho projektu bol vykonaný koncepčný návrh aplikácie, ktorý v nadväzujúcej bakalárskej práci bol realizovaný.

5.1 Realizácia

Webová aplikácia je naprogramovaná v jazyku Python a ďalej je využívané aj HTML a CSS. Python je vysoko úrovňový skriptovací programovací jazyk. Všeobecne povedané, CSS je nejaký zápis, ktorý určuje vzhľad (farby, dekoračné obrázky, rozmiestnenie prvkov) HTML dokumentu. HTML tvorí obsahovú kostru webovej stránky a vzájomne prepojuje texty.

Na jednoduchšiu prácu s webovými aplikáciami slúži pre jazyk Python webový framework Flask, ktorý je použitý aj v tejto práci. Na použitie tohoto frameworku bolo potrebné ho najskôr nainštalovať na počítač. Pre písanie kódu bol používaný editor Sublime text 3. Tento popis je platný len pre užívateľov operačného systému Windows pretože pri iných operačných systémoch je postup mierne odlišný. Na inštaláciu je potrebné si otvoriť príkazový riadok a nainštalovať si balíček Flask. Na to slúži príkaz `pip install flask`. Následne je potreba overiť, že inštalácia prebehla úspešne tým, že si otvoríme nové okno s príkazovým riadkom a zadáme text `python` a následne `import flask`.

Aby sme mohli webovú aplikáciu spustiť je potrebné sa nachádzať v priečinku kde máme uložený náš projekt cez príkazovú riadku pomocou príkazu `cd`. Predtým než spustíme aplikáciu musíme nastaviť premennú prostredia na súbor, v ktorom chceme mať našu aplikáciu a to sa nastavuje príkazom `set FLASK_APP=názov_súboru.py`. Spustenie aplikácie prebehne napísaním `flask run` do príkazového riadku. Po spustení sa v príkazovom riadku vypíše ip adresa a port na ktorej aplikácia beží. V tomto prípade `127.0.0.1:5000`. Do webového prehliadača je teda nutné napísať túto adresu aj s portom alebo len alias ip adresy `localhost:5000`.

Pre prehliadanie stránky musíme nechať tento server bežať lebo inak ju nebudeme schopný vidieť. Pri vývoji aplikácie aby sa zmeny urobené v kóde previedli aj na stránku bolo nutné server vypnúť cez klávesovú skratku CTRL+C a znovu ho zapnúť aby boli zmeny badateľné. Aby sa tomu predišlo stačí keď je nastavená aplikácia v móde debug. To sa dá urobiť nastavením novej premennej prostredia na

`set FLASK_DEBUG=1`. Teraz však na spustenie aplikácie treba napísať do príkazového riadku `python názov_súboru.py`. Po tomto už pre zobrazenie zmeny stačí len znovu načítať webovú stránku. Pre prehliadanie aplikácie je vytvorených niekoľko ciest k rôznym záložkám a stránkam aplikácie pomocou funkcie `@app.route`.

5.2 Obsah tretích strán

Na to aby nebolo nutné písať HTML kód priamo do súboru s príponou .py je použitá funkcia `render_template`, ktorá je importovaná a použitá pre vygenerovanie HTML kódu z templatu, ktorý je možné si buď vytvoriť alebo stiahnuť. V tejto práci je použitý template s názvom „Hyperspace“ zo stránky `www.HTML5up.net`, ktorý je voľne dostupný pod Creative Comons BY a je teda šíriteľný aj pre opätovné komerčné aj nekomerčné použitie a je možné si ho akokoľvek meniť. Stačí ak sa zmienime o autorovi, teda stránke so zoznamom daných templatov. Template je upravený tak aby fungoval na webovom serveri cez framework Flask. To predovšetkým zahŕňa upravenie odkazovania sa na obrázky a na ďalšie stránky pomocou importovania funkcie `url_for`. Template, ktorý bol stiahnutý obsahoval nie len súbory HTML ale aj súbory s CSS kódom a JavaScript súbory, ktorú sú tu tiež použité.

Všetky obrázky, ktoré sú použité na vytvorenie tejto aplikácie sú zo stránky `www.pixabay.com`. Pixabay je medzinárodná stránka pre publikovanie fotiek, vektorov, ilustrácií a videí pod licenciou Creative Comons 0. Táto licencia znamená, že osoba, ktorá k dielu priložila toto vyhlásenie, súhlasila s vystavením tohoto diela ako diela voľného a celosvetovo sa vzdala všetkých svojich autorských práv k dielu, vrátane všetkých práv súvisiacich a práv príbuzných v rozsahu, ktorý je povolený zákonom. Toto dielo je možné kopírovať, upravovať, distribuovať a spracovávať, a to aj pre komerčné účely, bez potreby získavania ďalšieho súhlasu. Tieto diela (v tomto prípade obrázky) vďaka tejto licencii je možné sťahovať, používať a upravovať akokoľvek chceme a to dokonca bez uvedenia autorstva.

Ako druhú možnosť, tentokrát pre verejné publikovanie aplikácie navrhnutej pomocou frameworku Flask napísanom v programovacom jazyku Python som si vybral online integrované vývojové prostredie a webhostingovú službu PythonAnywhere. Je to služba, ktorá funguje už od roku 2012 a poskytuje prístup prostredníctvom webového prehliadača k rozhraniam príkazového riadka Python a Bash. Programové súbory je možné prenášať do alebo zo služby pomocou prehliadača. Webové aplikácie hostované touto službou sa dajú písať pomocou akéhokoľvek aplikačného rámca založeného na WSGI (Web Server Gateway Interface). Webová aplikácia je teda verejná pre všetkých a je dostupná na adrese `http://xtomko04.pythonanywhere.com/`.

Záver

Bakalárska práca predstavuje popis základných pojmov v elektronickom bankovníctve a ich využitie a bezpečnostné prvky, ktoré používajú. Ďalším okruhom ktorý má táto práca pokryť bola právna úprava elektronického bankovníctva a jej pôsobenie. Práca by mala čitateľovi ponúknuť dostatočný prehľad a predstavu o formách elektronického bankovníctva. Niektoré informácie, ktoré možno na prvý pohľad chýbajú v tejto bakalárskej práci chýbajú pretože je veľmi ťažko sa k ním dopátrať a veľa inštitúcií si nepraje aby boli tieto informácie zverejňované a mali by byť predmetom obchodného tajomstva. Dokonca aj zamestnanci, ktorí pracujú na bezpečnosti nemôžu poskytovať tieto informácie pretože všetci podpisujú zmluvu o mlčanlivosti.

Medzi hlavné výhody priameho bankovníctva môžeme zahrnúť časovo neobmedzený prístup klienta k svojmu účtu. Platobnú transakciu je možné uskutočniť kedykoľvek a kdekoľvek za veľmi krátky čas. Klasické transakcie hotovostného platobného styku v pobočkách bánk nahradili chytré zariadenia ako mobilné telefóny alebo tablety a internetbanking. S elektronickým bankovníctvom sa spájajú aj nižšie poplatky za bankové operácie. Elektronický distribučný kanál je pre banky podstatne lacnejší ako klasická forma, ktorá prebieha osobne na pobočke banky. Aj cieľom samotných bánk je motivovať ľudí aby využívali služby elektronického bankovníctva pre ich jednoduchosť. Ľudia, ktorí preferujú realizáciu bankových operácií priamo v pobočke banky dnes už v porovnaní s ostatnými zaplatia viac. Štatisticky však už v dnešnej dobe navštevuje banky osobne podstatne menej ľudí.

V dnešnej dobe predstavuje elektronické bankovníctvo najmodernejšiu formu poskytovania bankových služieb a je považované za štandardný distribučný kanál. Oblasť elektronického bankovníctva prechádza veľkými reformami a vývojom aby bola schopná naplniť požiadavky klientov. Elektronické bankovníctvo so sebou však prináša aj určité riziká. Riziko zneužitia osobných údajov z dôvodu rozmachu informačných technológií rastie rovnako ako aj veľké nebezpečenstvo hroziacich podvodov. Chrániť citlivé údaje už nie je povinnosťou len banky, ale aj samotného klienta samotného, a to je práve najväčšie riziko pretože klienti sú často nezodpovední a nedbanliví. Neuvážené správanie klienta môže viesť až k odcudzeniu prístupových údajov klienta a získania prístupu k jeho účtu. Ak klient komunikuje s bankou prostredníctvom internetu, je nutné aby dodržiaval aj všeobecné pravidlá bezpečnosti internetového bankovníctva. Dôsledné dodržiavanie týchto bezpečnostných pravidiel eliminuje riziko zneužitia bankových účtov.

V záverečnej časti, ktorá je venovaná praktickej časti je spísané aké aplikácie tretích strán boli použité a akým spôsobom je vo vypracovávaní postupované. Webová aplikácia, ktorá bola vytvorená bola vytvorená predovšetkým za účelom podpory výuky na našej škole pretože sám považujem túto tému za dôležitú. Informácie sú aj obecné a tam kde bolo nájdených dostatok informácii tam sú popísané aj jednotlivé techniky zabezpečenia s podrobným popisom. Na základe daného rozboru sa teda podarilo naplniť zadanie a ciele práce a vytvoriť webovú aplikáciu.

Literatúra

[1] *Elektronické bankovníctvo.* TotalMoney.sk [online]. [cit. 2019-12-12]. Dostupné z: <https://totalmoney.sk/slovnik/E/elektronicke-bankovnictvo/>

[2] *Zákon o platobnom styku a o zmene a doplnení niektorých zákonov.* Zákony pre ľudí [online]. Bratislava, 2002 [cit. 2020-02-24]. Dostupné z: <https://www.zakonypreludi.sk/zz/2002-510>

[3] *Aktivní, pasivní a neutrální bankovní operace.* Vysokeskoly.cz/ [online]. [cit. 2019-12-18]. Dostupné z: <https://www.vysokeskoly.cz/maturitniotazky/ekonomika/aktivni-pasivni-a-neutralni-bankovni-operace>

[4] *Platobná karta.* Poštová banka [online]. [cit. 2019-12-12]. Dostupné z: <https://www.postovabanka.sk/slovnik-pojmov/p/platobna-karta/>

[5] *Co je NFC?* Alza [online]. 2019 [cit. 2019-12-01]. Dostupné z: <https://www.alza.cz/co-je-nfc>

[6] *Google Pay.* CyberSource [online]. [cit. 2019-12-02]. Dostupné z: <https://developer.cybersource.com/api/developer-guides/dita-payments/CreatingOnlineAuth/CreatingAuthReqGooglePay.html>

[7] *Apple Pay v Česku: Jak a kde platit pomocí iPhone a Apple Watch?* Alza [online]. 2019 [cit. 2019-12-01]. Dostupné z: <https://www.alza.cz/apple-pay#slovensko>

[8] *Garmin Pay: Peněženku nechte doma a platte hodinkami.* Alza [online]. 2019 [cit. 2019-12-01]. Dostupné z: <https://www.alza.cz/garmin-pay>

[9] MÁČE, Miroslav. *Platební styk: klasický a elektronický.* Praha: Grada, 2006. Osobní a rodinné finance. ISBN 80-247-1725-5.

[10] *Zákony pro lidi.*[online]. 2019 [cit. 2019-11-30]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2017-370/zneni-20180113#p279-1-1>

[11] *Európska smernica 2000/46/ES.* EUR-Lex: Acces to European Union law. EUR-Lex [online]. [cit. 2019-11-30]. Dostupné z: <https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A32000L0046>

[12] BARVIRČÁK, Matej. *MOŽNOSTI PREPOJENIA E-BANKOVNÍCTVA A ELEKTRONICKÉHO PODNIKANIA V SR.* [online]. Brno, 2015 [cit. 2019-12-19]. Dostupné z: <https://is.muni.cz/th/udl09/BP_Barvircak.pdf> Bakalářská práce. Masarykova univerzita Ekonomicko-správní fakulta, Studijní obor: Finance. Vedoucí práce Prof. Ing. Jiří Dvořák, DrSc.

[13] *Vydávanie elektronických peňazí.* NÁRODNÁ BANKA SLOVENSKA [online]. Slovensko, 2009 [cit. 2019-11-30]. Dostupné z: <https://www.nbs.sk/sk/dohlad-nad-financnym-trhom/dohlad/vydavanie-elektronickych-penazi>

[14] *Zákon o platebním styku.* Zákony pro lidi [online]. Praha, 2017 [cit. 2020-02-24]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2017-370>

[15] *Zákon o bankách.* Zákony pro lidi [online]. Praha, 1992 [cit. 2020-02-24]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1992-21>

[16] *Zákon o bankách.* Epi [online]. Bratislava, 2001 [cit. 2020-02-24]. Dostupné z: <https://www.epi.sk/zz/2001-483>

[17] *Zákon České národní rady o České národní bance.* Zákony pro lidi [online]. Praha, 1993 [cit. 2020-02-24]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1993-6>

[18] *Zákon Národnej rady Slovenskej republiky o Národnej banke Slovenska.* Zákony pre ľudí [online]. Bratislava, 1992 [cit. 2020-02-24]. Dostupné z: <https://www.zakonypreludi.sk/zz/1992-566>

[19] *Smernica Európskeho parlamentu a Rady o začatí a vykonávaní činností a dohľade nad obozretným podnikaním inštitúcií elektronického peňažníctva.* EUR-Lex [online]. 2000 [cit. 2020-02-24]. Dostupné z: <https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A32000L0046>

[20] *Európska smernica 2000/46/ES* EUR-Lex: Acces to European Union law. EUR-Lex [online]. 2017 [cit. 2020-02-15]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1520948030732&uri=CELEX:32018R0389>

[21] DVOŘÁK, Petr. *Bankovnictví pro bankéře a klienty.* Praha: Linde, 2005. Vysokoškolská učebnice (Linde). ISBN 807201515x.

[22] *3-D Secure.* Wikipedia [online]. [cit. 2019-12-09]. Dostupné z: <https://en.wikipedia.org/wiki/3-D_Secure#3-D_Secure_2.0>

[23] KUČKA, Roman. *Bezpečnosť platobných kariet.* [online]. Banská Bystrica, 2009 [cit. 2019-12-19]. Dostupné z: <https://is.ambis.cz/th/hnisj/Bezpecnost_platobnych_kariet.pdf.> Diplomová práca. Zahraničná vysoká škola Banská Bystrica. Vedoucí práce Ing. Radoslav Forgáč, PhD.

[24] [online]. Anchor Academic Publishing, 2013, s. 10-12 [cit. 2019-12-20]. ISBN 978-3954890774. Dostupné z: *An Investigation into Authentication Security*

of GSM algorithm for Mobile Banking. <https://books.google.cz/books?id=g_ymAgAAQBAJ&pg=PA2&lpg=PA2&dq=gsm+banking+security&source=bl&ots=hueLNRtNXN&sig=ACfU3U0nhcNPGk3tQZcjLawKI7FJX7nJVg&hl=sk&sa=X&ved=2ahUKEwjt1vO7lcLmAhViTBUIHbdPAoYQ6AEwA3oECAkQAQ#v=onepage&q&f=false>

[25] *What is an SSL certificate?* Digicert [online]. [cit. 2019-11-30]. Dostupné z: <https://www.digicert.com/ssl/>

[26] *Behind the Scenes of SSL Cryptography.* Digicert [online]. [cit. 2019-11-30]. Dostupné z: <https://www.digicert.com/ssl-cryptography.htm>

[27] *Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014.* EUR-Lex [online]. 2014 [cit. 2019-11-30]. Dostupné z: <https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A32014R0910>

[28] MALINA, Lukáš. *Kryptografie v informatice.* Technická 12, 616 00 Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2014. ISBN 978-80-214-5024-0.

[29] *Platby mobilem probíhají jednoduše a usnadní nakupování.* Alza [online]. 2019 [cit. 2019-12-01]. Dostupné z: <https://www.alza.cz/nfc-platby-mobilem>

[30] *Google Pay v Česku: jak funguje a které banky službu podporují?* Alza [online]. 2019 [cit. 2019-12-01]. Dostupné z: <https://www.alza.cz/android-pay>

Zoznam symbolov, veličín a skratiek

3DES	Triple DES
3DS	3-D secure
ACK	Príznak Acknowledgement
AES	Advanced Encryption Standard
API	Application Program Interface
BBS	Bulletin Board Service
BIN	Bank Identification Number
BPIN	Bezpečnostný Personal Identification Number
CA	Certifikačná Autorita
CD	Compact disc
CISC	Complex Instruction Set Computer
CNP	Card Not Present
CSR	Certificate Signing Request
CSS	Cascading Style Sheets
CVV kód	Card Verification Value
ČR	Česká republika
ČSOB	Československá obchodná banka
ČNB	Česká Národní Banka
DAN	Device Account Number
DDA	Dynamic Data Authentication
DES	Data Encryption Standard
Dos	Denial of service
EB	elektronické bankovníctvo
eIDAS	Electronic IDentification, Authentication and trust Services
EMV	Europay, Mastercard, Visa
EOK	Elektronický Osobný Kľúč
ES	Európske spoločenstvo
EÚ	Európska únia
FIPS	Federal Information Processing Standards
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HCE	Host Card Emulation
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IB	internetbanking
IBM	Firma International Business Machines

ID	Identifikátor
iOS	Mobilný operačný systém pre iPhone
IPPID	Jedinečné osemmiestne číslo v rámci banky
ISO	International Organization for Standardization
IVR	Interactive Voice Response
Kč	Korún českých
kb/s	Kilobit za sekundu, prenosová rýchlosť
MD5	Message-Digest Algorithm 5
MM	Značka pre uvedenie mesiacu platnosti
MHz	MegaHertz, jednotka frekvencie
NBS	Národná Banka Slovenska
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NSA	National Security Agency
P2P	Point-to-Point, Peer-to-Peer
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POS	Point-Of-Sale
RFC	Requests for Change
RFID	Radio Frequency Identification
RR	Značka pre uvedenie roku platnosti
RSA	Rivest–Shamir–Adleman
SDA	Static Data Authentication
SHA	Secure Hash Algorithm
SR	Slovenská republika
SMS	Short Message Service
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TS	Token Service
USA	United States of America - Spojené štáty americké
WAP	Wireless Application Protocol
WiFi	Wireless Fidelity
WML	Wireless Markup Language
WSGI	Web Server Gateway Interface
WWW	World Wide Web
XML	eXtendible Markup Language
Zb.	zbierky (v zákone)