Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Diplomová práca

2017 **Bc. Matej Mazák**

Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Výber autentizačnej metódy pri prihlasovaní do elektronického bankovníctva v nadväznosti na zrušenie autentizácie GRID kartou

Vypracoval: Bc. Matej Mazák

Vedúci práce: prof. Ing. Petr Doucek, CSc.

Rok vypracovania: 2017

Čestné prehlásenie:

Prehlasujem, že som túto diplomovú prácu vypracoval samostatne. Všetky použité podklady, z ktorých som čerpal informácie, sú uvedené v zozname použitej literatúry a citované v texte podľa normy ČSN ISO 690.

V Prahe dňa Podpis: .....

Poďakovanie:

Na tomto mieste by som sa chcel poďakovať Prof. Ing. Petrovi Douckovi, CSc. za vedenie práce, poskytnutie návrhov a konštruktívnych rád počas celého priebehu písania tejto diplomovej práce. Osobitné poďakovanie patrí mojim rodičom, sestre a Veronike Trokanovej za ich podporu a pomoc počas celého štúdia.

Abstrakt

Cieľom diplomovej práce je výber vhodnej autentizačnej metódy pre prihlasovanie do elektronického bankovníctva. Vybrané riešenie bude slúžiť ako doplňujúci faktor pri autentizácii a autorizácii klienta a zároveň ako náhrada zastaraného bezpečnostného prvku GRID karty. V teoretickej časti je podrobne vysvetlený vývoj a smerovanie elektronického bankovníctva. Ďalej sú popísané výhody, ktoré tento kanál poskytuje klientom a zároveň banke. Z časti sú popísané niektoré trendy ovplyvňujúce každodenné smerovanie elektronického bankovníctva. Veľmi dôležitou časťou je bezpečnosť, ktorá je pri poskytovaní služieb elektronického bankovníctva nevyhnutná, a preto je spomenutá v každej časti diplomovej práce. Praktická časť obsahuje navrhovaný postup zrušenia autentizačnej metódy GRID karty, na ktorý nadväzuje návrh možných riešení, ktoré by tento prvok v budúcnosti nahradili. Praktická časť ďalej obsahuje výber a popis jednotlivých hodnotiacich kritérií a viackriteriálne hodnotenie vybraných riešení. Na určenie váh vybraných kritérií je použitá Saatyho metóda a pri viackriteriálnom rozhodovaní bodovacia metóda. Záver práce popisuje porovnanie dosiahnutých výsledkov jednotlivých autentizačných metód a prínosy práce.

Kľúčové slová:

autentizácia, autentifikácia, autorizácia, Internet banking, PSD2, digitalizácia, OTP kód, token, GRID karta, bankovníctvo

Abstract

The aim of this Master thesis is to choose appropriate authentication method for logging in to the electronic banking. The chosen solution will serve as an additional factor for authentication and authorization of client and at the same time as the replacement of the outdated security method – GRID card. Development and direction of the electronic banking is explained in the theoretical part of the thesis. Further on, the advantages of this channel that are provided to clients and bank, are described. Some of the trends which daily affect the direction of the electronic banking are also described. Security is very important part of the electronic banking and that is why it is mentioned in the each part of this thesis. The practical part contains proposed cancellation procedure of GRID cards and proposal of the new solutions that could replace them in the future. It also contains selection and description of evaluation criteria and multi-criteria evaluation of the selected solutions. Saaty method and scoring method were used to determine the weight of the particular criteria. Conclusion of the thesis compares achieved results of the individual authentication methods and assets of this Master thesis.

Key words:

authentication, authorization, Internet banking, PSD2, digitalization, OTP code, token, GRID card, banking

1 Úvod

Narastajúci počet dát, zvýšená regulácia a vyššia náročnosť nových technológií predstavujú pre organizácie zvýšené riziko výskytu informačno-bezpečnostnej hrozby, ktorá môže viesť až k narušeniu cieľov organizácie. Je preto nevyhnutné čo najrýchlejšie zabrániť vzniku možnej hrozby. Prípravou na situácie môže organizácia odolať nečakanému bezpečnostnému útoku a tým znížiť jeho dopad. Žijeme v dobe, kedy medzi najdôležitejšie aktíva spoločnosti patria informácie. Schopnosť organizácie chrániť svoje dáta sa stáva základom jej úspechu. Výnimkou nie je ani bankovníctvo, kde citlivé informácie patria medzi najväčšie aktíva banky.

S vývojom spoločnosti sa vyvíjali aj kanály elektronického bankovníctva. Dnes už môžeme povedať, že úspešne. Bankovníctvo v posledných desaťročiach uskutočnilo množstvo kvalitatívnych zmien. Trend čakania v dlhých radách na pobočke sa pomaly stáva minulosťou. Odráža sa to najmä na narastajúcej popularite elektronického bankovníctva. Bankové zvyky klientov sa menia každý deň spolu s vývojom nových zariadení. Internetové bankovníctvo sa transformuje zo statických webových stránok na samostatný kanál, schopný prinášať nezávislé príjmy. Úspešne dopĺňa ostatné kanály banky a efektívne podporuje riešenie online a off-line problémov. Banky postupne presviedčajú svojich klientov o množstve výhod, ktoré prináša elektronické bankovníctvo pre klienta. Dnes je už bežné, že si klient platí svoje účty cez mobilnú aplikáciu napr. skenovaním faktúry, prihlasuje sa do aplikácie odtlačkom svojho prsta, požičiava si peniaze z pohodlia svojho domova.

Preto je nevyhnutné, aby tieto služby boli dostatočne zabezpečené. Narastajúca popularita využívania služieb elektronického bankovníctva láka rôznych podvodníkov získať a zneužiť citlivé informácie. Bezpečnosť v banke je jedným z najdôležitejších kritérií, ktorých vývoj musí byť vždy na prvom mieste. To, že nedošlo k zneužitiu údajov dnes, ešte neznamená, že nedôjde zajtra. Ide najmä o udržanie si dobrej reputácie, čo je pri dnešnom trende switchingu[1] klientov medzi bankami nesmierne dôležité.

1.1 Cieľ práce

Cieľom diplomovej práce je analýza zrušenia bezpečnostného prvku GRID karta a výber novej autentizačnej metódy pre prihlasovanie do elektronického bankovníctva. Nová metóda v nadväznosti na zrušenie GRID karty rozšíri možnosti overenia totožnosti klienta pri prihlasovaní do elektronického bankovníctva. Analýza zrušenia GRID karty sa skladá z viacerých fáz, ktorých účinnosť je vyjadrená zmenou počtu vydaných GRID kariet pred začatím danej fázy a po jej skončení. Práca predovšetkým

[1] Presun účtu (spolu s ďalšími produktmi) z pôvodnej banky do novej banky bez potreby jej návštevy.

obsahuje viackriteriálne rozhodovanie medzi vybranými riešeniami pomocou bodovacej metódy. Pre odhad váh zvolených kritérií bola použitá Saatyho metóda.

1.2 Metódy práce

Na začiatku písania diplomovej práce je vhodné si stanoviť metódy práce, ktoré budú použité v teoretickej aj praktickej časti. Pri skúmaní problematiky v teoretickej časti boli použité metódy analýzy a syntézy informácií získaných predovšetkým štúdiom zahraničnej a slovenskej literatúry, príspevkov na Internete a rôznych článkov v odborných časopisoch. V teoretickej časti bola použitá aj metóda porovnávania. V praktickej časti sa autor opieral najmä o metódu analýzy, ktorú využil pri postupe zrušenia autentizačnej metódy GRID karta. Pri výbere nového bezpečnostného prvku, autor vychádzal z metódy porovnania. Na základe porovnania vybraných metód potom pomocou metódy riadeného rozhovoru s riaditeľom odboru elektronického bankovníctva, zvolil najlepšie riešenie. Autor tiež vychádzal zo svojich skúseností získaných z praxe pri riadení produktu elektronického bankovníctva a z podnetov získaných konzultáciami s vedúcim diplomovej práce.

1.3 Stanovenie hypotéz riešeného problému

Autor stanovuje hypotézy v súvislosti s porovnaním jednotlivých autentizačných metód, ktoré sú detailne popísané v podkapitole 6.2. Autor predpokladá, že autentizačná metóda off-line zdieľaný kľúč skončí v celkovom hodnotení na poslednom mieste. Dôvod tohto predpokladu je, že táto metóda patrí medzi najdrahšie spôsoby autentizácie z vybraných riešení. Druhá stanovená hypotéza hovorí o autentizácii Virtuálnou GRID kartou ako o najvhodnejšom z vybraných riešení, najmä z dôvodu ľahšej integrovateľnosti riešenia do existujúcich systémov a nižšej cene.

1.4 Štruktúra práce

Práca je rozdelená do dvoch hlavných častí. Prvá časť je teoretická, v ktorej autor detailne popisuje charakteristiku a vývoj elektronického bankovníctva, jeho výhody pre klienta a banku. Potom nasleduje popis vybraných trendov v oblasti elektronického bankovníctva. Veľmi dôležitou časťou je práve bezpečnosť elektronického bankovníctva, v ktorej sú popísané základné charakteristiky informačnej bezpečnosti, autentifikácie. V závere teoretickej časti sú popísané bezpečnostné hrozby, ktorým denno-denne čelia klienti elektronického bankovníctva a definícia požiadaviek na autentizačný prvok.

Druhá časť je praktická, v ktorej autor popisuje celý proces priebehu zrušenia GRID karty. V ďalšej časti je detailne popísaný výber autentizačného prvku pri prihlasovaní do Internet bankingu, ktorý pozostáva z definovania rozhodovacieho problému, výberu a popisu jednotlivých kritérií, podrobným opisom vybraných autentizačných metód a ich celkové zhodnotenie. Záverom tejto časti sú priradené

váhy ku každému z vybraných kritérií určené autorom práce a vedúcim pracovníkom odboru elektronického bankovníctva. Nakoniec je vybraná najlepšia autentizačná metóda na základe bodovacej metódy. Poslednou časťou praktickej časti ja záver, v ktorom sú zhodnotené prínosy nového riešenia.

Teoretická časť

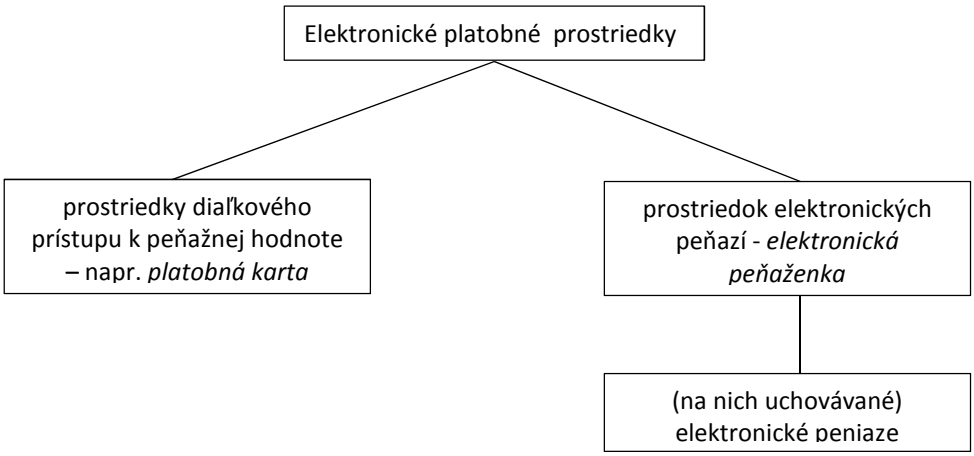
2 Charakteristika a rozvoj elektronického bankovníctva

Spoľahlivá, presná, bezpečná a rýchla realizácia platobných operácií je základným kameňom pre efektívne fungovanie banky. Priestor, v ktorom sa realizujú operácie platobného styku obsahuje dynamickú vrstvu, kde dochádza k tvarovaniu vzťahov banky s klientom. V tejto kapitole si popíšeme vývoj a formovanie kanálov elektronického bankovníctva a jeho zásadný vplyv na zmenu bankového správania klientov.

2.1 Elektronické platobné prostriedky

Zákon o platobnom styku č. 510/2002 Z. z. (1) obsahuje definíciu elektronických platobných prostriedkov. „Prostriedky, ktoré umožňujú prístup k elektronicky evidovaným alebo elektronicky uchovávaným peňažným hodnotám a ktoré umožňujú prostredníctvom elektronických alebo iných technických zariadení uskutočňovať vklady, výbery, prevody alebo iné operácie. Elektronický platobný prostriedok je:

- prostriedok, ktorý umožňuje oprávnenému držiteľovi prístup k peňažným prostriedkom prostredníctvom elektronických alebo iných technických zariadení cez platobnú aplikáciu elektronického bankovníctva.
- prostriedok uchovávajúci el. peniaze na el. zariadení umožňujúci oprávnenému držiteľovi prístup k uchovávaným elektronickým peniazom a je prijímaný ako platobný prostriedok na uskutočňovanie platobných operácií.“ (1)



Obrázok 1 Elektronické platobné prostriedky **(2)**

Do prvej skupiny elektronických platobných prostriedkov budú v súlade so spomínanou definíciou patriť platobné karty a aplikácie elektronického bankovníctva (Internet banking, Mobile banking). Do druhej skupiny zasa elektronické peňažné prostriedky. Platobným prostriedkom elektronických peňazí je:

- elektronická peňaženka, ktorá uchováva na čipovej karte peňažné prostriedky,
- softvérová peňaženka, uchovávajúca elektronické peňažné prostriedky na inom elektronickom zariadení ako na čipovej karte.

Elektronickými peniazmi (e-money) rozumieme peňažnú hodnotu v elektronickej forme, ktorá predstavuje peňažný záväzok vydavateľa a ktorá je uchovávaná na platobnom prostriedku elektronických peňazí. Iná osoba ako vydavateľ podľa odseku nemôže vydávať ani spravovať elektronické peniaze a platobné prostriedky elektronických peňazí (2).

Zároveň tento zákon vyhradzuje, aký subjekt môže vydávať elektronické platobné prostriedky:

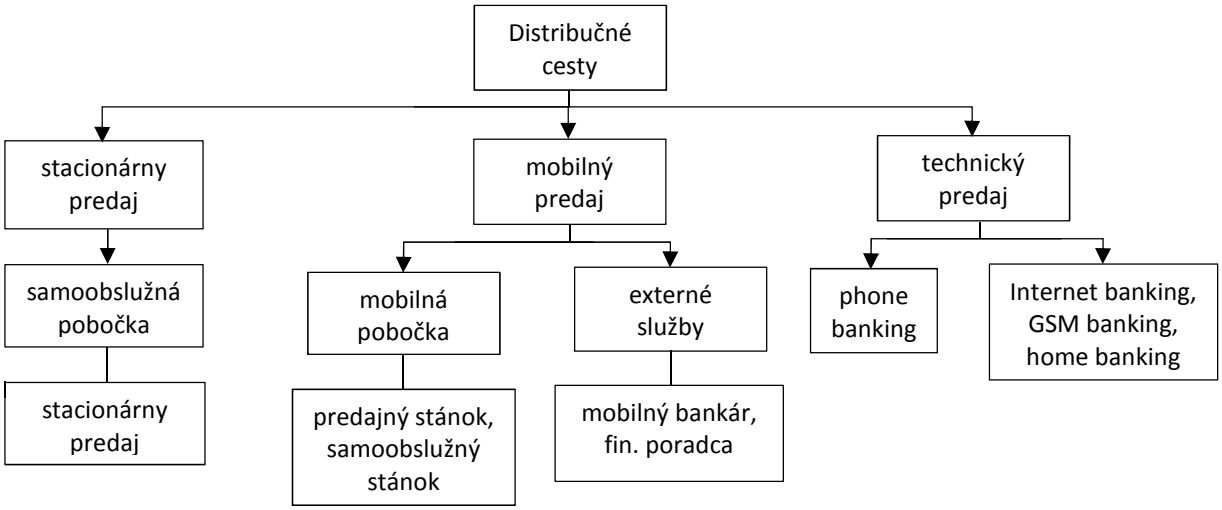
- Národná banka Slovenska,
- banky a pobočky zahraničných bánk, ktoré majú bankové povolenie na vydávanie elektronických bankových prostriedkov,
- iné osoby podľa osobitného zákona, ktoré môžu vydávať len platobné prostriedky diaľkového prístupu, ak sú na ich vydávanie oprávnené podľa osobitného zákona,
- inštitúcia elektronických peňazí, ktorou sa rozumie iná právnická osoba ako banka, zahraničná banka a Národná banka Slovenska, ak má podľa tohto zákona udelené povolenie na elektronickopeňažnú činnosť; elektronickopeňažnou činnosťou je vydávanie a správa elektronických peňazí a platobných prostriedkov elektronických peňazí,
- iné právnické osoby, ktoré na základe povolenia Národnej banky Slovenska môžu vydávať len platobné prostriedky elektronických peňazí.

Podľa Zákona o platobnom styku č. 510/2002 Z. z. je oprávneným držiteľom elektronického platobného prostriedku každá fyzická alebo právnická osoba, ktorej vydavateľ vydal na používanie elektronický platobný prostriedok na základe nimi uzavretej zmluvy o vydaní a používaní tohto elektronického platobného prostriedku. Oprávnený držiteľ platobnej aplikácie elektronického bankovníctva preukazuje svoju totožnosť osobným identifikačným číslom (prihlasovacím menom do elektronického bankovníctva) a zároveň autentizačným údajom, ktorý mu bol pridelený vydavateľom po dohode s oprávneným držiteľom. (1)

2.2 Rozvoj distribučných ciest v bankovníctve

Od obdobia rozvoja retailového bankovníctva, ktorý bol sprevádzaný poklesom výkonnosti bánk je dlhodobo sledovaný vzťah klient – produkt – banka. Podľa Václava Zemana dlhodobé sledovanie nákladovosti a výnosnosti jednotlivých klientskych skupín prinieslo výsledok, kde sa zistilo, že približne polovica klientskych kontaktov s bankou nevykazuje pre banku žiadny zisk a približne štvrtina prináša banke len nákladovosť na strane banky. Banky na základe týchto prínosov volia cestu k predaju svojich produktov jednotlivým tržným segmentom. V bankovníctve existuje niekoľko distribučných ciest, ktoré je možné rozdeliť do týchto skupín:

- stacionárne,
- mobilné,
- technické. (3)



Obrázok 2 Štruktúra distribučných ciest v bankovníctve podľa Václava Zemana (3)

2.2.1 Samoobslužný predaj

Banky sa snažili posilniť svoju ziskovosť a zefektívniť svoje činnosti rozvojom samoobslužných prístupov k bankovým službám. Pre dosiahnutie maximálneho využitia je potrebné, aby bol bankový produkt dostupný bez časového obmedzenia. Výhodou je časová nezávislosť predaja, tzn. 24 hodín a 7 dní v týždni. Pre dosiahnutie takéhoto stavu museli banky investovať nemalé finančné prostriedky do rozvoja nových technológií.

Samoobslužný predaj začal lobby bankingom, čo znamenalo umiestnenie bankomatov a samoobslužných terminálov do predajných priestorov pobočiek. Banky na zaistenie kontaktu klienta s personálom pobočky umiestňovali tieto zariadenia medzi predajné priehradky. Boli tam umiestnené, aby mohli bankoví poradcovia kontaktovať klientov a ponúkať im produkty na predaj. Ďalším spôsobom predaja bolo automatové bankovníctvo, ktoré bolo bez prítomnosti zamestnancov.

Banky tieto zariadenia umiestňovali mimo svoje pobočky a boli označované ako centra rýchleho servisu. Samoobslužný predaj produktov a služieb je spájaný so systémom kartového bankovníctva, kde platobná karta umožňuje vykonávať okrem hotovostných operácií (výbery a vklady hotovosti) aj bezhotovostné operácie (platby prostredníctvom POS terminálov u obchodníka a internetové platby). Bankomaty patria medzi najrozšírenejšie samoobslužné zariadenia bánk vo svete. (3)

2.2.2 Mobilný predaj

Spôsob predaja bankových produktov cez obchodného zástupcu bol dlhodobo považovaný za nevhodný. Táto forma predaja našla uplatnenie až v segmente firemných klientov. Spôsob predaja je vykonávaný firemným bankárom, ktorý vystupuje voči druhej strane ako zamestnanec banky. Jeho cieľom je predávať firemným klientom požadované služby, zodpovedať za všetky obchodné vzťahy s klientmi a ich ziskovosť, rozvíja obchodný vzťah a portfólio produktov. Banky začali využívať aj mobilných bankárov pre obchodovanie so skupinou bohatých privátnych klientov. Aj keď sa jedná o nákladný distribučný kanál, jeho využitie sa naopak rozvíja. Na klienta to pôsobí jedinečne, keď vidí osobitný prístup banky, ktorá sa snaží o vytvorenie intenzívneho vzťahu s klientom.

Ďalším spôsobom mobilného predaja je predajný stánok, ktorý banka prevádzkuje ako dočasné obchodné miesto, spojené vo väčšine prípadov s marketingovou kampaňou alebo prezentovaním nového produktu. Je prevádzkovaný ako nízko-nákladové pracovisko, ktoré ponúka nový typ produktu. Je zriaďovaný na základe prieskumu v miestach zvýšeného pohybu klientov (napr. obchodné domy, univerzity, podniky a pod.). (3)

2.2.3 Technický predaj

Do tejto kategórie môžeme zaradiť priamy marketing. Jedná sa o marketingový systém, ktorý využíva reklamné média na vytvorenie merateľnej odozvy.(4) Cieľom banky pri tejto forme komunikácie je osloviť nových potencionálnych klientov. Medzi klasické formy priameho marketingu využívaného bankou môžeme zaradiť rozhlasový a televízny spot, internetové reklamy. Banka môže spracúvať meno, priezvisko, adresu, telefón a e-mailovú adresu klienta na účely priameho marketingu produktov a služieb a tretích strán, s ktorými banka spolupracuje pri poskytovaní svojich služieb ak jej klient udelí súhlas so spracúvaním svojich osobných údajov na účely priameho marketingu v zmluve s bankou. Banky potom tieto údaje o klientoch využívajú najmä na cielenie konkrétnych reklám na klienta cez sociálne siete ako Facebook. Klient má právo tento súhlas kedykoľvek odvolať písomným oznámením na adresu banky. (5)

Ďalším distribučným kanálom je Phone banking. Kontaktné centrá neslúžia len na potreby priameho marketingu, ale najmä ako podpora pre klientov pri riešení problémov. Kontaktné centrum pohltilo ďalší distribučný kanál a to bankovníctvo cez telefón. Pred centralizáciou bankových informačných

systémov a distribúciou údajov z nich na ľubovoľné pracovisko banky bolo spojenie cez telefón najjednoduchším kontaktom klienta s pobočkou banky pre vyriadenie nejakej požiadavky. (3)

Napríklad Phone banking v Poštovej banke je určený pre klientov, ktorí radi telefonujú a chcú riešiť svoje požiadavky osobne s bankou, no zároveň sa nemôžu dostaviť na pobočku banky. V poštovej banke môžu klienti vybaviť cez telefón nasledovné požiadavky:

- zistenie aktuálneho stavu na účte,
- zrealizovanie prevodného príkazu,
- zistenie niektorých pohybov na účte,
- zadanie, zmenu alebo zrušenie trvalého príkazu alebo inkasa,
- zablokovanie platobnej karty. (6)

V súčasnosti je vďaka neustálemu rozvoju komunikačných technológií telefónne bankovníctvo sústredené do kontaktných centier. Systém fungovania je založený prioritne na komunikácií s informačným systémom a ak klient potrebuje riešiť zložitejší problém, tak komunikuje s telefónnym bankárom. Najväčšou výhodou pre klienta je možnosť komunikovať s bankou 24 hodín denne a 7 dní v týždni.

GSM bankovníctvo (SMS-bankovníctvo) vzniklo na základe obrovského nárastu počtu užívateľov mobilných telefónov. Poplatky za túto službu boli účtované len minimálne. Ku komunikácií klienta s bankou používa komunikačné technológie využívane v mobilných telefónoch prostredníctvom:

- SMS správ v zakódovanej podobe,
- technológie SIM Toolkit,
- technológie WAP.

Aby klient takúto službu mohol používať potrebuje mať podpísanú zmluvu s bankou, ktorá mu na seba poskytne telefonický kontakt a tiež mobilný telefón so sprístupnenou službou SMS. S bankou potom komunikuje formou krátkych SMS správ. Klient odošle do banky SMS a okamžite sa mu vráti odpoveď v rovnakej forme. Tento spôsob slúžil v minulosti najmä na získanie informácie o stave účtu alebo pre získanie aktuálnych kurzov zahraničných mien. (7)

Technológia SIM Toolkit zaisťuje šifrovanie SMS správ pri komunikácií klienta s bankou. Banková aplikácia na SIM karte v mobilnom telefóne vytvorí zašifrovanú správu, ktorú dokáže rozšifrovať len špeciálny software v banke. Následne je táto požiadavka zaslaná do bankového systému na spracovanie. O výsledku spracovania je klient informovaný automatickou generovanou SMS správou.

Najpokročilejšia služba v období tlačidlových telefónov bola služba WAP. Služba spočívala v komunikácií cez internet s protokolom Wireless Application Protocol, ktorá je kombináciou internetového a telefónneho bankovníctva. Klient sa prihlásil na webové stránky banky, kde mohol ovládať svoj účet a realizovať obmedzené množstvo akcií v porovnaní s dnešnými možnosťami. Vzhľadom k zvýšenej popularite používateľnosti smartfónov sa GSM bankovníctvo dostalo do úzadia a dnes ho poskytuje malé množstvo bánk. Je nahradzované mobilným bankovníctvom. (3)

2.3 Elektronické bankovníctvo

Rýchlo rozvíjajúce sa informačné technológie a počítačové siete ako Internet poskytujú ideálny priestor na rozvoj elektronického obchodu na globálnu úroveň. Rozvoj vytvára nový typ ekonomiky, ktorú mnohí volajú digitálna ekonomika. Táto rýchlo vznikajúca ekonomika prichádza s množstvom meniacich sa technológií a zvýšenou intenzitou vedomostí vo všetkých oblastiach biznisu. Vznikajú nové formy biznisu a kanálov na doručovanie služieb ako elektronické bankovníctvo (e-banking). (8)

Zákazníci stále vyžadujú vyššiu kvalitu služieb spĺňajúcu ich narastajúce požiadavky. Zároveň chcú mať danú službu poskytnutú v čo najkratšom čase za nižšie náklady. Na splnenie týchto požiadaviek potrebujú banky neustále vyvíjať čo najinovatívnejšie cesty vytvárania hodnôt, ktoré často požadujú rôznu IT infraštruktúru a rôzne spôsoby myslenia. Táto transformácia podnikania zo starých spoločností na nové agilné spoločnosti nie je jednoduchá a vyžaduje veľké investície najmä do inovatívnych riešení a plánovania.

2.3.1 Vývoj elektronického bankovníctva

Posledných 30 rokov evidujeme značný rozvoj elektronicko-finančných služieb. Začiatkom 70. rokov minulého storočia prevládalo ukladanie veľkého množstva regulačných opatrení. Jedným z hlavných dôsledkov týchto opatrení bola obmedzená konkurencieschopnosť jak doma, tak i v zahraničí. Výsledkom bolo spoliehanie sa na tradičné kamenné pobočky, založené na poskytovaní finančných služieb. Banky sa celý čas sústreďovali na osobný kontakt prostredníctvom pobočiek.

Bankovníctvo patrilo vždy do odvetví, ktoré sa snažili zavádzať rôzne inovácie a nové spôsoby riešenia problémov v podobe inovatívnych technologických riešení. Banky zo začiatku tieto technológie využívali len interne alebo na komunikáciu s ďalšími finančnými inštitúciami (centrálna banka). Trvalo dlhší čas, kým banky pochopili, že veľmi dôležitý je klient a vzájomná komunikácia. Dôvodom tohto zistenia bol nárast konkurencie v obore. Zmena prichádzala postupne spolu so spoločenskou zmenou počas 80. rokov minulého storočia, kedy vzrastala dôležitosť informačno-komunikačných technológií, prinášajúca súťaživosť a tlak na rýchlejšie tempo zmien.

Internet je pomerne stále novým kanálom na poskytovanie bankových služieb. Prvá forma on-line bankových služieb vznikla začiatkom 80. rokov minulého storočia. Na jej fungovanie bol potrebný počítač, modem a softvér, poskytovaný predajcom finančných služieb. Toto riešenie nebolo dostatočne akceptované a tak jeho ďalšie šírenie zlyhalo. S rapídnym nárastom iných typov elektronických služieb v polovici deväťdesiatych rokov banky zvýšili záujem o poskytovanie služieb prostredníctvom Internetu.

Rozvoj elektronického bankovníctva je priamo úmerné rozvoju vysoko-rýchlostného široko-pásmového pripojenia a narastajúcemu počtu používateľov, ktorí vedia pracovať s počítačom. Ďalším dôležitým faktorom v náraste používania elektronického bankovníctva je to, že banky objavili rôzne benefity, ktoré táto služba poskytuje. (9)

2.3.1.1 Vývoj internetového bankovníctva

Z tradičných kamenných pobočiek až po novú generáciu digitálneho bankovníctva prešla pomerne dlhá cesta. Bankové transakcie sa vyskytujú už od začiatku éry, kedy bol zavedený obchod a obchodné transakcie. Ale žiadna iná éra nemala taký revolučný dopad na bankovníctvo ako elektronický obchod so zavedením webu. Za posledné dve dekády od uvedenia webu pre obchodné operácie, prešiel Internet banking dlhým procesom vývoja.

V úplných začiatkoch banky používali nepriamy spôsob komunikácie, ako zverejňovanie ponúk a podnikateľských dát banky. V tomto štádiu bol Internet banking iba doplňujúci kanál, resp. zdroj informácií pre širokú verejnosť a klienta. Neskôr prišlo k poskytovaniu základných informácií na Internete v podobe funkcionalít, ako sledovanie si zostatkov na účte a platenie účtov on-line. Kým Internet banking podstupoval transformáciu jeho obsahu, paralelný rozvoj v telekomunikáciách, infraštruktúre a požadovanom softvéri pomohol zvýšiť možnosti rozšírenia tohto kanálu.

Zo stavu, kedy bol Internet banking len doplňujúcim kanálom na vykonávanie základných transakcií, prešiel dlhú cestu, a teraz je vnímaný ako seba riadiaci kanál umožňujúci vykonávať nezávisle všetky potrebné bankové operácie. Banky sa snažia Internet banking posunúť na kanál, ktorý je viac flexibilný a prispôsobený požiadavkám klienta vyplývajúcich z jeho potrieb. Tieto potreby sa banky snažia naplniť lepším dizajnom a kvalitou obsahu, ktorá značne zvyšuje klientsky zážitok. Internet banking je vyvíjaný nie len na to, aby splnil potreby klienta, ale musí naplniť najmä ciele a priority banky.

Každým vylepšením banky v širokom rozsahu zvyšujú zážitok klienta, pokiaľ ide o šírku technologických inovácií, prispôsobovania a vzájomnej integrácie front-officu a back-officu. S rozvojom nových technológií prichádzajú aj odstrašujúce bezpečnostné riziká, ktoré sú zakorenené v mysliach klientov aj bánk. Mnoho klientov považuje rôzne moderné trendy za málo bezpečné.

Banky sa snažia tieto predsudky odstrániť viacfaktorovou autentizáciou a neoblomným úsilím vytvoriť dostatočne bezpečné riešenia. Bezpečnosť bola vždy veľkou výzvou nie len pre banky, ale aj pre celú technologickú komunitu. Od obdobia jednosmerných statických webových stránok, Internet banking prijal novú tvár interaktívneho prostredia vo vzťahu ku klientovi, v ktorom sa banka snaží o:

- informovaní klienta o všetkom potrebnom,
- vzájomnú komunikáciu,
- vypočutie všetkých prianí klienta,
- neustálu podporu klienta.

Aktuálna generácia kanálov Internet bankingu má zadefinovaný ako kľúčový cieľ zvýšenie klientskeho zážitku, z dôvodu udržania tempa s novými viac kanálovými službami. Kanály ako pobočka, stánok, Internet a telefón sú náročné na prevádzku, ale netreba zabúdať, že vďaka ním banky získavajú nových klientov. Klient dnes už nie je len orientovaný na pobočku alebo Internet, ale využíva viacero kanálov, ktoré tvoria jeden celok bankovníctva. Vďaka týmto kanálom môže banka obsluhovať rozličných klientov naprieč rôznymi regiónmi, kanálmi a segmentami. (10)

2.3.2 Výhody elektronického bankovníctva

Veľa bánk a mnoho ďalších finančných inštitúcií už implementovalo elektronické bankovníctvo a zistilo, že prináša nespočetné množstvo výhod. Výhody prináša nie len pre banky, ale najmä pre klienta. Niektoré z týchto výhod si popíšeme v tejto podkapitole.

2.3.2.1 Výhody pre klienta

V období, kedy banky bojujú o každého klienta, je nevyhnuté na jeho udržanie poskytovať služby, z ktorých bude mať klient zážitok. Výnimkou nie je ani elektronické bankovníctvo. Prístup prvého dojmu je kritický pre dosiahnutie úspechu banky.

Avkiran, ktorý skúmal správanie bankových klientov hovorí, že klient chce od banky tradičný rozsah služieb, rozšírený o pohodlie on-line bankových služieb, spolu s rozvojom osobného vzťahu s bankou. Tiež zdôrazňuje dôležitosť osobného kontaktu v poskytovaní bankových služieb. Zdvorilosť a elegancia pri komunikácií, ochota poskytovať promptné služby, schopnosť sa ospravedlniť a vysvetliť znepokojujúce chyby sú všetko potreby vyžadované klientom. Je jasné, že väčšina týchto potrieb nemôže byť zautomatizovaná. Na lepšie pochopenie klienta a následné prispôsobenie produktu na mieru je potrebné analyzovať dáta. (11)

Medzí najväčšie výhody elektronického bankovníctva pre klienta patrí možnosť pracovať s jeho účtami kdekoľvek a kedykoľvek, všade tam, kde má klient prístup k Internetu. Klient môže vykonávať bankové operácie 24 hodín denne a 7 dní v týždni, dokonca aj v noci alebo cez prázdniny,

kedy sú banky zatvorené. Jediná vec, ktorú klient potrebuje, je aktívny prístup na Internet. Klient si cez kanály internetového bankovníctva môže zriadiť niektoré služby a produkty bez toho, aby musel osobne navštíviť pobočku. (12)

Používanie je rýchle a efektívne. Je možné riadenie viacerých účtov naraz a peňažné prostriedky sú posielané z jedného účtu na iný účet veľmi rýchlo. Cez Internet banking si klient môže sledovať všetky svoje financie na jednom mieste. Peňažné prostriedky klienta sú vo väčšom bezpečí v porovnaní s fyzickou držbou prostriedkov skrytých niekde v domácnosti. Zabezpečené je aj neustále monitorovanie účtu, klient je informovaný ak príde k nejakej podvodnej aktivite alebo útoku na jeho účet ešte pred vznikom možnej hrozby. V neposlednom rade je to šetrenie času, kedy klient nemusí stáť v rade na pobočke, aby zaplatil šek. Samozrejme, ďalšou výhodou je šetrenie finančných prostriedkov, kedy má klient nižšie alebo žiadne poplatky za realizáciu niektorých transakcií platobného styku.

2.3.2.2 Výhody pre banku

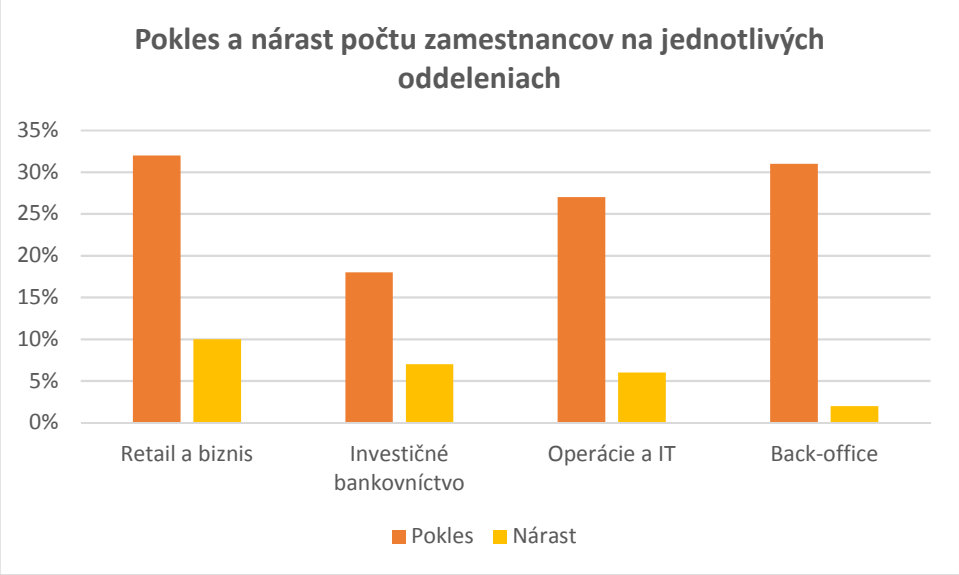
Jednou z hlavných výhod, ktoré môže elektronické bankovníctvo priniesť, sú zvýšené príjmy banky. Najmä kvôli možnému nárastu počtu klientov, zachovaniu si existujúcich klientov a príležitosti krížového predaja, ktorý tento kanál ponúka. Je ale otázne, či príjmy z týchto kanálov dostatočne pokryjú návratnosť vynaložených investícií (ROI – Return on investment). Ďalšou výhodou je, že kanály elektronického bankovníctva pomáhajú bankám zvyšovať ich celkový imidž. Banka sa navonok javí, že je zameraná na klienta a inovácie. Toto pravidlo platilo najmä v začiatkoch, keď len veľmi inovatívne banky mali vyvinutý kanál elektronického bankovníctva. Samozrejme, aj dnes, napriek väčšej dostupnosti, majú tieto riešenia veľký vplyv na rozhodovanie klienta. Atraktívna a prehľadná webová stránka, obsahujúca široké portfólio produktov, zvyšuje imidž banky. Tento imidž ma skrytý význam najmä pri získavaní mladých budúcich potencionálnych klientov, na ktorých to bude mať veľký vplyv. Rovnako veľký vplyv to bude mať aj pri rozhodovaní sa o banke po dovŕšení veku, kedy mladým klientom skončí vedenie študentských účtov zadarmo. Ak budú so svojou bankou spokojný, je veľká pravdepodobnosť, že v nej zotrvajú.

Ak sa v minulosti chceli banky geograficky rozširovať, museli otvoriť na týchto miestach nové pobočky. Tento spôsob znamenal pre banku veľké náklady na údržbu. Vývojom elektronických kanálov ako Internet sa tento spôsob pomerne zmenil. Dnes už banky s klientmi v jednej časti sveta môžu poskytovať svoje služby na iných miestach a získavať svojich klientov aj tam, kde nemajú svoje pobočky. Vďaka Internetu niektoré banky poskytujú službu zriadenia si účtu v banke on-line. Na tento spôsob nie je potrebná fyzická prítomnosť na pobočke. Vo veľa krajinách funguje medzi

bankami systém vzájomného zdieľania zdrojov ako bankomatov alebo pošty, ktorá je hlavným bodom pre styk s klientmi. (9)

Hlavným argumentom pre banku, prečo využívať služby elektronického bankovníctva, je redukcia nákladov. K znižovaniu nákladov dochádza najmä tým, že banky už nemusia vo veľkom rozširovať sieť svojich pobočiek, ktorých výstavba vyžaduje veľké počiatočné náklady. Nezanedbateľné sú určite aj náklady na chod pobočky, vyžadujúci potrebu fyzicky prítomných zamestnancov na pobočke. Výrazné zmeny v bankách, najmä kvôli technológiám, pozorujeme už dnes. Klienti stále menej navštevujú pobočky a stále viac komunikujú on-line. Technológie taktiež menia prostredie vo vnútri banky. Rýchly a efektívny software postupne nahrádza ľudský výkon. Od komunikácie cez investičné algoritmy, riadenie rizika až po bankový back-office.

Podľa štúdie Ernst and Young (EY) sa trend znižovania počtu zamestnancov najviac prejaví v oblasti komunikácie s klientom. Tretina bankových manažérov očakáva pokles počtu zamestnancov práve v tejto oblasti o 32% a v podporných procesoch centrály o 31%. Naopak nárast počtu zamestnancov by sa nemal nejako prudko zvýšiť. Banky budú svoje tímy rozširovať len o jednotlivcov s rôznou kombináciou schopností a osobnosti, ktorí povedú banku k celkovému rozvoju a zvyšovaniu príjmov. Banky sa budú musieť viac zamerať na kvalitu svojich pracovníkov. (13)



***Graf 1 Pokles a nárast počtu zamestnancov banky na jednotlivých oddeleniach podľa EY 2015* (13)**

Nové technológie menia jednotlivé role zamestnancov vo všetkých organizáciách. Súčasne s poklesom počtu zamestnancov bude potreba vytvoriť nové pracovné miesta, na ktorých budú noví pracovníci zabezpečovať rozmiestnenie a rozvoj nových technológií naprieč celou organizáciou a vykonávať dohľad nad správnym fungovaním. Banky preto neustále prehodnocujú svoje fungovanie a snažia sa dopadom nových technológií zjednodušovať procesy, ktoré majú samozrejme veľký dopad

na ich pracovnú silu. Technológie majú veľký potenciál nahradiť niektoré bankové pozície, najmä tie, ktoré sú založené na štandardizovanej práci a jednoduchosti ako bankári za priehradkou, predajcovia úverov alebo hypotekárni špecialisti. Dnes už roboti na základe algoritmov hodnotiacich emócie klienta dokážu predpovedať, aký typ bankovej služby klient potrebuje. Je však potreba si uvedomiť, že na niektorých pozíciách nebude automatizácia činností vhodná. Rôznorodosť na pracovisku bude vytvárať veľký tlak na nastavenie správnej firemnej kultúry, ktorá bude schopná prilákať a udržať aj tie najväčšie talenty banky. Vo veľkej výhode budú banky, ktoré vytvoria pracovné prostredie, vedúce k rozvoju banky a zvyšovaniu jej príjmov. Vytvorené tímy budú musieť ísť spoločne za jedným cieľom.

V prieskume, ktorý sa zaoberal transformáciou pobočiek v roku 2014, odpovedalo 26% respondentov skladajúcich sa z bánk, že mení model svojich pobočiek. V roku 2015 sa tento počet zdvojnásobil na 51%. Výsledky prieskumu ukazujú, že každá druhá finančná inštitúcia chce zmeniť model aspoň jednej pobočky. Až 64% opýtaných to robí s cieľom zlepšiť zážitok klienta. Na druhom mieste so 14% respondentov odpovedalo, že hlavným cieľom zmeny modelu pobočiek, je ziskovosť. Pre klienta je dobrou správou, že veľké množstvo bankových inštitúcií považuje za najdôležitejší práve jeho zážitok na pobočke. Zamestnanci na pobočke už dlhšie nebudú vykonávať len vklady hotovosti alebo presúvať peňažné prostriedky na iné účty, budú tam najmä preto, aby klientom pomohli, poradili a poskytli viac angažované služby pre banku (pôžičky a úvery). (14)

Ďalšou veľkou výhodou elektronického bankovníctva je to, že banka môže tento kanál využívať na marketingové účely. Elektronický marketing (iné názvy: i-marketing, e-marketing, internetový marketing) je postavený na schopnosti poskytovať detailné informácie o nákupnom správaní klientov a ich peňažných profiloch. Klient, ktorý je detailne preskúmaný, vytvára pre banku možnosť cielenia reklamy na konkrétneho klienta, ponúka mu produkty, o ktoré má klient záujem (napr. prostredníctvom push-notifikácií[2]) a v neposlednom rade si banka s takýmto klientom buduje dlhodobý vzťah cez rôzne aktivity ako cross-selling[3].

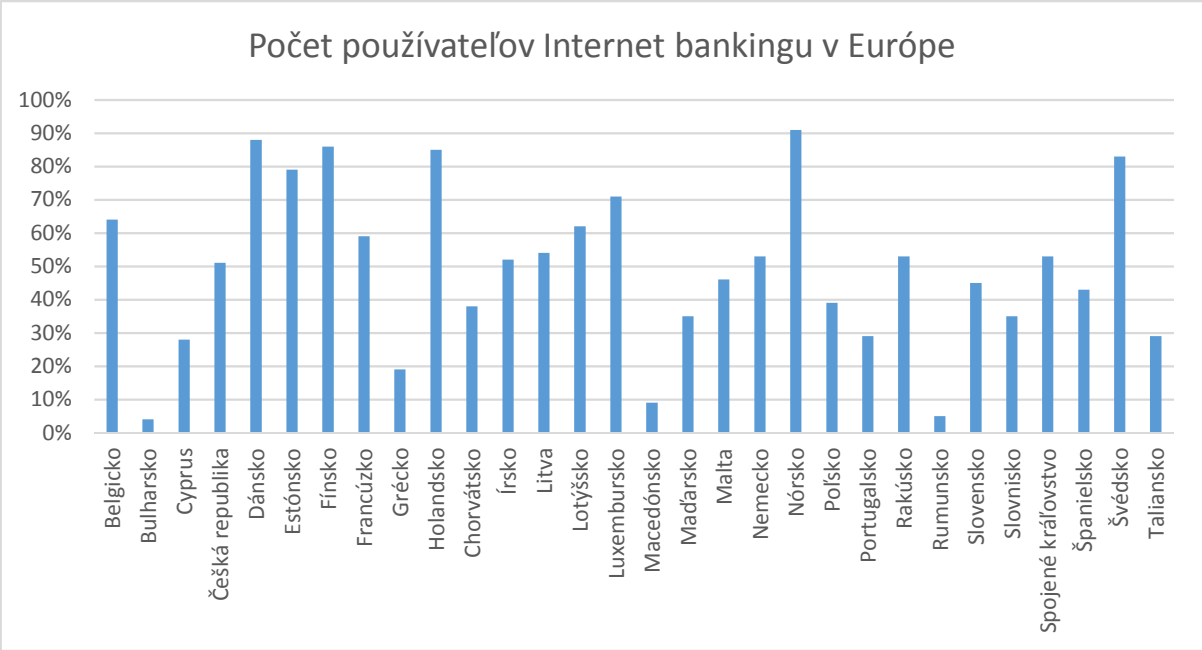
2.3.3 Internet Banking

Internetové bankovníctvo sa odvoláva na používanie Internetu ako vzdialeného kanála na doručovanie bankových služieb. Je to elektronický platobný systém, ktorý umožňuje klientom banky vykonávať finančné transakcie cez webové stránky banky. On-line bankový systém býva väčšinou pripojený na niektorú z častí core (jadra) bankového systému obsluhovaný bankou. Je to akési zrkadlo ku kamennej pobočke, ktorá bola tradičným spôsobom pristupovaniu klienta k bankovým

[2] Push-notifikácia: upozornenia z mobilných aplikácií, ktoré slúžia na oznámenie nejakej správy alebo poskytujú užívateľovi informácie o polohe, čase a dátume.
[3] Cross-selling: v preklade krížový predaj, je obchodná taktika ako využiť bázu klientov na zvýšenie objemu predaja.

službám. Internet banking ponúka svojim klientom rýchlu, bezpečnú a pohodlnú prácu s účtami z akéhokoľvek miesta na svete, kde má klient prístup na Internet. Z ekonomickej perspektívy zvýšili informačné technológie a počítačové siete automatizáciu, rýchlosť a štandardizáciu v komunikácií a vnútornej administratíve spolu s nárastom funkcionality a pohodlia klienta. Internetové bankovníctvo sa pomerne rýchlo rozšírilo a zažíva stále väčší úspech naberaním na popularite. Klienti bánk pochopili, že sa jedná o veľmi rýchlu, bezpečnú a pohodlnú formu spravovania svojich financií. (9)

Štatistika z portálu Statista.com zobrazuje využívanie internetového bankovníctva v európskych krajinách za rok 2016. Prieskum zistil, že najviac využívané služby internetového bankovníctva sú v Nórsku, kde až 91% nórskej populácie použilo v roku 2016 kanály internetového bankovníctva. Naopak, najmenší počet používateľov Internet bankingu je v Bulharsku (4%) a v Rumunsku (5%). Do internetového bankovníctva na Slovensku sa prihlásilo 45% populácie za rok 2016, čo je približne o 5% menej ako je priemer celej Európskej Únie. V Českej republike sa do Internet bankingu v roku 2016 prihlásilo 51% celkového počtu obyvateľstva, čo je 1% nad priemerom EÚ. (15)



Graf 2 Využitie Internet bankingu v európskych krajinách za rok 2016 podľa Statista.com (15)

2.3.3.1 Základné funkcionality Internet bankingu vo vybranej inštitúcií

V tejto podkapitole si popíšeme základné funkcionality Internet bankingu vybranej finančnej inštitúcie Prima banka Slovensko, a. s. Jedná sa o pomerne mladú banku, ktorej názov je na slovenskom trhu od 1. Januára 2012. Banka sa v rámci svojej stratégie orientuje najmä na retailovú klientelu, čoho výsledkom je jednoduché portfólio produktov a služieb. V dôsledku jej krátkeho pôsobenia na bankovom trhu sa neustále rozširuje najmä vďaka zväčšovaniu pokrytia svojej

pobočkovej a bankomatovej siete po celom Slovensku. (16) Klientovi Prima banky sú po prihlásení do Internet bankingu poskytnuté nasledovné funkcionality:

- Platby
    a. prehľad účtov, zostatky na účte, pohyby na účte,
    b. príkazy na úhradu v rámci krajín SEPA, cezhraničný príkaz, expresný príkaz a trvalý príkaz, importy príkazov,
    c. Inkaso – zadanie, zmena, zrušenie inkasa.
- Účty
    a. prehľad účtov – zostatky na účte, prehľad pohybov na účte, výpisy z účtov,
    b. možnosť požiadať o Termínovaný vklad, Sporenie.
- Karty
    a. prehľad platobných kariet, transakcie vykonané platobnou kartou,
    b. aktivácia platobnej karty, blokácia platobnej karty, zmena limitu na platobnej karte, povolenie alebo zakázanie platieb na Internete,
    c. klienti si môžu nastaviť alebo zmeniť PIN na platobnej karte cez Internet banking,
    d. znovuvydanie platobnej karty v prípade straty alebo krádeže.
- Úvery
    a. prehľad úverových produktov, zostatky úrokové sadzby, nahromadené úroky, atď.
    b. možnosť požiadať o pôžičku alebo povolené prečerpanie, ak má klient pred schválený limit.
- Správy
    a. správy – bežná komunikácia s klientom,
    b. dokumenty – zmluvná dokumentácia.

2.3.3.2 Ciele Internet Bankingu

V začiatkoch vývoja Internet Bankingu bol jeho hlavný cieľ zjednodušiť a uľahčiť bankovníctvo. Tieto ciele sa postupom času napĺňali a menili. Na ich zostavenie sa dnes kladú oveľa väčšie nároky, ako tomu bolo v minulosti. Na to, aby banky zostali konkurencieschopné, plnili požiadavky svojich klientov a dosahovali zisk, mali dodržiavať aspoň niektoré z nasledujúcich cieľov:

- služba prispôsobená na mieru,
- zvýšiť podiel na trhu,
- integrácia jednotlivých kanálov,
- poskytovať cross-sale,
- zvyšovanie počtu klientov,

- interaktívne funkcionality (zvýšiť klientsky zážitok).

Zmena vnímania Internet Bankingu sa postupne vyvíjala, až dospela do štádia, kedy je táto služba vnímaná ako nehnuteľnosť banky. Už to nie je len URL adresa, ktorej cieľom vytvorenia bolo ostať v súboji s konkurenciou. Filozofia bánk sa dávno zmenila a dnes sa požaduje doladenie každého detailu, ktorý s touto službou súvisí. Je potrebné správne rozhodnúť o kvalite, obsahu, mieste služby a posúdení, či pridaná funkcionalita poskytuje nejakú návratnosť investícií. Netreba tiež zabúdať na klientsky zážitok. Internet banking je pre banku kľúčovým kanálom, ktorý pomáha doručovať rôzne faktory a služby dôležité na nárast alebo udržanie predajných čísel. Akcionári sa musia na tento kanál pozerať z taktického a strategického hľadiska. (10)

Obrázok 3 Ciele elektronického bankovníctva (vlastné spracovanie) (10)

Predstava skúsenosti je vrodená od našej existencie. Vo všeobecnosti skúsenosť pokrýva všetko osobné s čím sme sa stretli, absolvovali alebo prežili. Slovo UX (user experience - klientsky zážitok) vyjadrujúce stretnutie klienta so systémom, ktoré má začiatok a koniec. Je to celkové určenie správania sa užívateľov počas práce so systémom, návštevy webovej stránky a pod. Tento pohľad zdôrazňuje spomienky a výstup zo skúsenosti vyplývajúcej z práce so systémom. Typickým príkladom je zameranie sa na klientsky zážitok pri špecifických aktivitách v istom období, napríklad pri hraní počítačových hier s nejakým príbehom (gradácia napätia so šťastným koncom) alebo výstup (skúsenosť) s používaním nejakého systému (učenie sa tancovať pomocou tanečnej hry). Existuje široké spektrum faktorov, ktoré môžu vyplývať na klientský zážitok pri práci so systémom. Tieto faktory môžeme klasifikovať do troch hlavných kategórií a to:

- obsah,
- užívateľ,
- systém.

Klientsky zážitok sa môže zmeniť aj vtedy, ak sa zmení obsah, ale systém zostane pôvodný. Obsah v kontexte UX pozná rôzne formy obsahov ako sociálny, kedy sa pracuje s inými ľuďmi alebo fyzický, kedy môžeme daný produkt použiť. Netreba však zabúdať aj na technický a informačný obsah. Klientsky zážitok je veľmi individuálny a zároveň dynamický počas toho, ako človek pracuje so systémom. Zážitok sa odráža najmä od motivácie užívateľa použiť daný produkt a zároveň od jeho súčasných mentálnych a fyzických zdrojov, očakávaní alebo nálady. Na vnímanie klientskeho zážitku užívateľa Internet bankingu budú vyplývať jeho vlastnosti. Dôležité pre klientsky zážitok sú požadované vlastnosti zahrnuté v systéme (funkcionalita, estetická stránka, navrhnuté interaktívne správanie, prispôsobovanie). Vlastnosti, ktoré používateľ pridal alebo zmenil v systéme vyplývajú z jeho používania, napríklad zmena obrázku. (17)

V praxi niektoré banky umožňujú klientovi navigáciu na základe pravdepodobných cieľov jednotlivca ako kúpa domu, vzdelanie, plán, alebo dôchodok oproti jednoduchému zobrazovaniu zoznamu kategórií pomenovaných ako osobné produkty, úverové produkty, sporiace produkty. Jednoduchšia forma zobrazovania produktov dostáva pozitívnu odpoveď od klientov. Banky by mali neustále vylepšovať klientsky zážitok nasledovnými aktivitami:

- počúvanie potrieb klienta,
- skúmanie jeho profilu a potrieb,
- podporiť zapojenie klienta do tohto procesu.

Navrhovanie webových stránok použitím rôznych scenárov bolo užitočné pre banky, kde vývojári webov mohli vizualizovať potreby a profily klienta, ktorý sa snažil vykonať napríklad transakciu alebo si otvoriť účet použitím Internet bankingu. Je preto dôležité sledovať správanie každého klienta a na jeho základe prispôsobovať či už obsah, alebo rozmiestnenie daných položiek na stránke.

V počiatočnej fáze, kedy potencionálny klient navštívi webovú stránku banky, je potrebné sa pokúsiť o možnosť priameho zobrazenia jeho preferovanej sekcie (mal by ju hneď nájsť). Je potrebné vytvoriť obojsmernú cestu s cieľom, že po jeho neskoršom návrate na stránku banky bude okamžite spojený s obsahom, ktorý predtým vyhľadával alebo bol úzko spätý. Marketingoví pracovníci sa snažia prekonvertovať príležitostného návštevníka stránky na klienta banky. Po jeho získaní sa banky snažia o vytvorenie automatických procesov prispôsobených klientovým potrebám.

Internet banking je indikátorom rastu každej banky. Avšak na to, aby rástol je nevyhnutné neustále zlepšovať jeho produkty a služby, ktoré budú úspešne čeliť konkurencii a plniť potreby klienta. Niektoré banky využili Internet na rozšírenie nových klientskych segmentov. Napríklad cezhraničné bezhotovostné transakcie ponúkli bankám možnosť rozvinúť nový špecifický segment klientov, pracujúcich v zahraničí, ktorí si často posielajú peňažné prostriedky naspäť do krajín, odkiaľ

pochádzajú. Ďalšou možnosťou, ktorú môžu banky využiť, je spolupráca so sociálnymi sieťami na získanie nového segmentu klientov, ktorým budú obchodníci predávať tovar pomocou kanálov elektronického bankovníctva.

Ďalšou významnou potrebou tohto kanála je neustále zvyšovanie jeho hodnoty. Internet banking bol prvotne plánovaný len na rozšírenie tradičného bankovníctva. Niektoré banky sa s týmto tvrdením nestotožnili a snažia sa poskytovať služby, ktoré povedú k zvýšeniu spokojnosti a pohodlia svojich klientov. Iné banky neponúkajú cez kanály internetového bankovníctva všetky služby súvisiace s transakciami, niektoré činnosti nechávajú stále na pobočky, prípadne kontaktné centrá. Naopak, snaha bánk, ktoré sú otvorené inováciám, vedie k dosiahnutiu každej jednej činnosti v reálnom čase, okamžite po vykonaní. Aby banky zvyšovali pohodlie klienta a jeho zážitok, musia neustále pracovať nie len na aplikáciách, ktoré klient vidí, ale najmä na systémoch a procesoch, ktoré nevidí no patria k hlavným zdrojom efektívnosti banky.

V počiatočných fázach, keď Internet bankingu slúžil len ako doplnok zobrazovania informácií o účte, sa návratnosť investícií (ROI) z tohto kanálu nepovažovala za dôležitú. Vývojom nových technológií sa tento kanál stal povinnou investíciou banky na jej prežitie, odhliadajúc od možnosti návratu finančných prostriedkov z tejto investície. Vnímaním dôležitosti internetového bankovníctva a získavaním veľkého množstva klientov, začali banky posudzovať kľúčové parametre úspechu tejto investície za isté časové obdobie. Náklady na Internet banking môžeme rozdeliť na dva kľúčové elementy:

- základné náklady (na údržbu tohto kanálu),
- špecifické náklady (vynaložené na rozvoj nových funkcionalít),
    a. bežné potreby,
    b. agresívne rozhodnutia (pomáhajúce sa udržať krok pred konkurenciou).

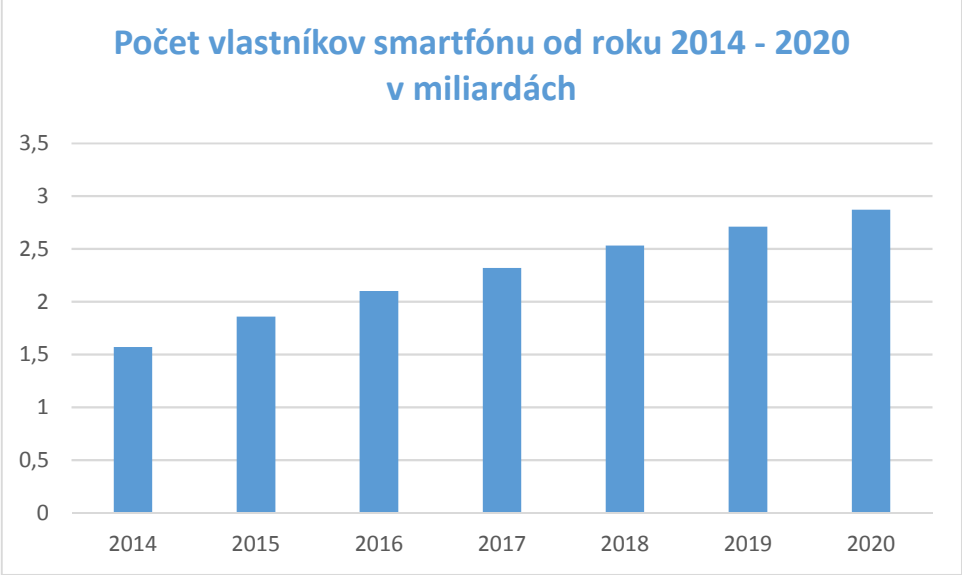
Návratnosť investícií zo služby internetového bankovníctva môžeme určiť na základe kombinácie:

- schopnosti kanálu priniesť nových klientov,
- redukcii nákladov na vykonávanie transakcií v porovnaní s inými kanálmi,
- schopnosti poskytnúť klientovi pohodlie,
- zvýšení celkovej hodnoty značky banky,
- generovaní toku príjmov z tohto kanálu.

Úspešnosť daných parametrov nemôžeme určovať len na základe získavania klientov, ale tiež zmenšovaním odporu klientov k tomuto kanálu. Nárastom dôvernosti klientov k banke, zlepšením indexu spokojnosti, transparentnosti a spoločenskej zodpovednosti. (10)

2.3.4 Mobilné bankovníctvo

Podľa celosvetových údajov z portálu Statista.com dnes vlastní 2.3 miliardy populácie smartfón. V roku 2020 má toto číslo narásť o celú miliardu. (18) Takýto prírastok smartfónov znamená pre bankové inštitúcie obrovskú príležitosť pripraviť pôdu pre zisk budúcich používateľov mobilných platobných služieb. Mobilné zariadenia sa stali neodmysliteľnou súčasťou životov ľudí a zároveň majú veľký vplyv na prebiehajúce zmeny správania zákazníkov.



***Graf 3 Vývoj počtu vlastníkov smartfónov vo svete podľa Statista.com* (18)**

Situácia na Slovensku je pomerne rovnaká. Podľa prieskumov agentúry Gfk z roku 2015, smartfón vlastní okolo 2 miliónov Slovákov. V roku 2012 bol počet smartfónov na Slovensku 4x menší ako v čase tohto prieskumu. Podľa informácií VÚB banky je typickým používateľom mobilného bankovníctva muž vo veku 31 rokov, ktorý vlastní smartfón s operačným systémom Android. (19)

Prima banka zasa uvádza, že sa počet aktívnych používateľov mobilnej aplikácie za rok 2016 zvýšil o 200% v porovnaní s rokom 2015. Bežný klient sa do aplikácie prihlási 11-krát za mesiac a aplikáciu využívajú najmä muži. (20)

Mobilné bankovníctvo môžeme definovať ako používanie mobilného telefónu na prístup do bankového účtu. Existuje niekoľko spôsobov ako pristupovať ku svojmu účtu v banke cez mobilný telefón:

- webový prehliadač na mobilnom zariadení,
- cez textovú správu,
- stiahnutím mobilnej aplikácie.

Každá banka sa snaží vyvinúť svoju vlastnú bankovú aplikáciu, v ktorej ponúkne klientovi pohodlnejší a rýchlejší prehľad jeho účtov v banke. Banky sa snažia svojich klientov motivovať, aby si osvojili tieto aplikácie. Mobilné bankovníctvo môžeme rozdeliť do troch kľúčových oblasti:

- informačná oblasť,
- transakčná oblasť,
- služby, marketing, akvizícia.

Prvá oblasť poskytuje klientovi tri základné funkcie, a to sledovanie zostatku na účte, históriu transakcií, zobrazenie úverov a pôžičiek, kreditné informácie, informácie o lokalite pobočiek a bankomatov, a taktiež funkcie personálneho finančného riadenia (PFM – Personal financial management). Do PFM patria funkcie ako sledovanie výdavkov, tvorba rozpočtov a pod.

Transakčné služby obsahujú rôzne transfery peňažných prostriedkov z účtov, platenie šekov, platenie iným osobám a vzdialené vklady. Do tejto kategórie už dnes môžeme zahrnúť aj funkciu platby mobilom, ktoré poskytujú niektoré banky, napríklad Tatra banka na Slovensku alebo ČSOB v Českej republike.

Posledná oblasť obsahuje funkcie, ktoré dopĺňajú celkový imidž aplikácie. Tieto funkcie zvyšujú klientsky zážitok z používania aplikácie zahŕňajúce kontaktné možnosti, pomocné informácie alebo výstrahy. Imidž aplikácie tvoria najmä pridané funkcie navyše obsahujúce e-mailové notifikácie, možnosť zriadiť si sporenie, kreditné ponuky, možnosti zriadenia rôznych produktov poistenia.

Podľa správy vykonanej ING. bankou so sídlom v Amsterdame, mobilné bankovníctvo si získava obľubu verejnosti so skoro viac ako polovicou vlastníkov smartfónov a tabletov, ktorí používajú ich zariadenia na riadenie svojich financií. V prieskume, do ktorého sa zapojilo približne 15000 respondentov z 15 krajín sa ukázalo, že počet užívateľov používajúcich svoj smartfón na mobilné bankovníctvo narástol na 47% v roku 2016, v porovnaní s rokom 2015, kedy bol počet takýchto zariadení len 16%. Pre banky je pozitívnym signálom, že ľudia začínajú viac dôverovať mobilnému bankovníctvu, čo pomôže ďalšiemu rozvoju tohto kanálu. (21)

Ďalšia správa z roku 2012 hovorí, že 90% používateľov mobilného bankovníctva používa bankovú aplikáciu v mobile na kontrolovanie zostatku na účte alebo na sledovanie histórie transakcií a 42% opýtaných zasa tvrdí, že aplikáciu využívajú na posielanie peňažných prostriedkov na iné účty. Len 12% majiteľov mobilných telefónov urobilo aspoň jednu mobilnú platbu za posledných 12 mesiacov. Hlavným dôvodom je nedostatočná dôvera bezpečnosti moderných technológií. Ďalším negatívnym dôvodom nedôvery bola príliš komplikovaná alebo komplexná mobilná aplikácia. Banky majú vysoké ciele a chcú sa líšiť od iných bánk najmä v poskytovaní svojich služieb, znižovaním klientskych obáv,

redukovaním nákladov pomocou automatizácie. Na dosiahnutie týchto služieb musia poskytovatelia platobných služieb najprv vyriešiť najdôležitejšiu kategóriu, a tou je bezpečnosť. (22)

2.3.4.1 Funkcionality mobilnej aplikácie vo vybranej inštitúcii

V tejto kapitole stručne popíšem základné funkcionality mobilnej aplikácie Prima Banky. Aplikácia má názov Peňaženka a je dostupná pre platformy Android a Apple (iOS). Aplikácia Peňaženka je určená ako jedna z mála bankových aplikácií, poskytujúcich mobilné bankovníctvo, aj pre klientov banky, aj pre iných používateľov. Pre užívateľov aplikácie, ktorí nie sú klientami banky, poskytuje funkcionality ako napríklad sledovanie výdavkov, možnosť vytvorenia pripomienky na vykonanie platby, vytvorenie rozpočtu na zvolené časové obdobie (možnosť exportu výdavkov do Excelu) a navigáciu k pobočkám a bankomatom. Takýto používatelia aplikácie si môžu ako prednastavenú sekciu nastaviť rozpočet, ktorá sa klientovi zobrazí hneď po spustení aplikácie.

Prístup do sekcie Internet banking je určený len pre klientov banky, ktorí majú zriadení prístup do elektronického bankovníctva. Prvé prihlasovanie do aplikácie je rovnaké ako do Internet bankingu, kedy nie je potrebná žiadna ďalšia aktivácia služby. Klient sa prihlasuje prihlasovacím menom, ktoré mu banka po podpísaní zmluvy odovzdala, heslom a SMS kódom. Po viacfaktorovej autentizácii si klient vytvorí 4-miestny PIN kód, ktorým sa bude pri ďalšom spustení aplikácie prihlasovať. Ak telefón klienta podporuje funkciu odtlačku prsta, tak si klient môže zvoliť aj túto možnosť pre prihlasovanie a to na oboch mobilných platformách. Po úspešnom prihlásení sú klientovi poskytnuté nasledovné možnosti:

- Platobné služby
    a. zadávanie tuzemských príkazov na úhradu,
    b. skener čiarového/QR kódu alebo poštovej poukážky,
    c. vytvorenie, zmena alebo zriadenie trvalého príkazu,
    d. vytvorenie šablóny príkazov,
    e. navýšenie kreditu na predplatenej karte,
    f. zriadenie sporenia,
    g. zriadenie, zmena alebo zrušenie povolenia na inkaso.
- Sledovanie zostatkov na účte
    a. prehľad všetkých transakcií.
- Manažment platobných kariet
    a. aktivácia alebo blokácia platobnej karty,
    b. zmena limitu na platobnej karte,
    c. nastavenie alebo zmena čísla PIN na karte.

3 Trendy v oblasti elektronického bankovníctva

Táto kapitola bude obsahovať aktuálne trendy v oblasti vývoja elektronického bankovníctva. V digitálnom svete sa hranice medzi jednotlivými odvetviami zmenšujú, zatiaľ čo potreby užívateľa neustále rastú. Banky a ďalšie odvetvia sa musia mať na pozore, pretože prichádzajú nové externé sily, ktoré menia spôsob, akými robia biznis. Môžeme hovoriť o dvoch aspektoch pri vývoji digitalizácie:

1. digitalizácia s cieľom optimalizácie existujúcich zdrojov a procesov,
2. digitalizácia s cieľom vytvárania nových služieb, ktoré budú mať hodnotu pre klientov (biznis príležitosť).

Mnoho bánk pracuje na prvom aspekte, tzn. vylepšujú už existujúce procesy alebo optimalizujú zdroje. Upravujú existujúce štandardy a snažia sa zvýšiť efektívnosť prevádzky vylepšovaním existujúcich procesov. Takéto postupy neprinášajú klientom žiadne nové inovácie. Treba však povedať, že stále majú príležitosť rozvíjať druhý aspekt digitalizácie, teda prinášať nové inovácie, ktoré prinášajú novú konkurenčnú výhodu pre banky. (23)

Obrázok 4 Zobrazenie rôznych aspektov digitalizácie podľa Soprabanking.com (23)

3.1 Video bankár

Jedným z nových trendov, ktoré pomaly nastupujú na trh, je využívanie video bankárov. Ich cieľom je do istej miery nahradiť pracovníkov sediacich na kamenných pobočkách. Podľa štúdie Video Banking: the next chapter in bank digital transformation spoločnosti Efma, ktorú vypracovala v spolupráci so spoločnosťou Vidyo sa zistilo, že sa táto služba stáva viac štandardom v bankovníctve. V roku 2016 túto službu využívalo len 10% opýtaných bánk. No podľa tejto štúdie, ho plánuje zaviesť do konca roka 2017 až 50% opýtaných bánk. Ide o spôsob, ako zvýšiť zážitok klienta v porovnaní s tradičným kanálom - pobočkou. Výhodou Video bankára sú pomerne nízke náklady v porovnaní s pobočkou, kde treba neustále školiť nových zamestnancov v dôsledku zvýšenej fluktuácie pracovníkov na pobočke. Ďalšou výhodou je pohodlnosť pre klienta.

Medzi úspešné projekty môžeme zaradiť projekt indickej banky IndusInd Bank, ktorá vykoná denne približne 1000 video hovorov a až približne 65% jej zákazníkov túto službu opakovane používa. Hlavné služby, ktoré banky plánujú v rámci projektu video bankár ponúkať je:

- možnosť spojenia sa cez web alebo mobilnú aplikáciu,
- naplánovanie hovoru,
- prechod z chatu do video hovoru,
- otvorenie bankového účtu.

Služba video bankára určite patrí do trendov budúcnosti bankovníctva. Pre banky je dôležité, aby nepodceňovali komunikáciu s klientom a robili všetko preto, aby mal klient zabezpečené čo najväčšie pohodlie pri výbere bankových služieb. (24)

3.2 Internetová banka

Internetová banka je banka, ktorá zriaďuje prístup svojim klientom k účtu bez povinnosti fyzickej návštevy pobočky. Banka nemá vlastnú sieť pobočiek, ale svoje aktivity realizuje prostredníctvom priamych komunikačných kanálov:

- Internet,
- mobilný telefón,
- bankomat.

Internetová ani virtuálna banka nemajú zvyčajne žiadne kamenné pobočky a v niektorých prípadoch dokonca ani sídlo spoločnosti. Banka profituje z toho, že má nižšie prevádzkové náklady a menší počet zamestnancov, vďaka čomu môže svojim klientom poskytnúť rôzne benefity. Benefity ako bezplatné vedenie účtu, alebo vyššie úročenie finančných prostriedkov, lákajú stále viac nových klientov, ktorí si v takýchto internetových bankách otvárajú svoje účty. Väčšina internetových bánk ponúka svojím klientom aj bezplatne debetnú alebo kreditnú kartu. (25)

3.3 Nárast konkurencie

Príchod nových účastníkov na bankový trh je podmienený vývojom rôznych regulácií. Ich cieľom je znižovať bariéry vstupu na bankový trh alebo umožniť prístup poskytovateľom platobných služieb k bankovým účtom na základe regulácie o platobných službách PSD2. Regulácia PSD2 je z pohľadu tejto práce veľmi dôležitá a budeme sa jej venovať v ďalšej podkapitole, pretože sa týka najmä bezpečnosti platieb. Kombinácia digitálnej evolúcie a takýchto nariadení v podobe regulácií sa vo veľkom rozsahu dotkne samotných bánk.

Square alebo Paypal poskytujú svojim klientom služby s ľahkosťou, vysokou bezpečnosťou, štandardizáciou platieb, alebo úverových produktov. Vplývajú na vedomie klientov najmä vytváraním novej hodnoty spolu s organizáciami z iných odvetví, ako napríklad Facebook, Amazon. Ich výsledkom je ponuka kombinácie finančných služieb s nefinančnými produktmi. Okrem týchto hráčov sa začínajú na trh tlačiť aj menšie rozvíjajúce sa firmy (Kickstarter, Zopa alebo Funding Circle), ktoré poskytujú pôžičky finančných prostriedkov (peer-2-peer lending) fyzickým osobám alebo podnikateľom cez on-line služby.

Tieto firmy okrem snahy uspieť na finančných trhoch, menia aj očakávania užívateľov. Prinášajú nové riešenia ako porovnávanie cien pôžičiek, či nové biznis modely. Keď tieto začínajúce firmy (start-upy) porovnáme s bankami, tak zistíme, že sú viac agilné. Vyplýva to najmä z nižšej záťaže legislatívnym systémom a rôznymi nariadeniami, ktoré musia naopak banky prísne dodržiavať. Banky majú jedinečnú výhodu v tom, že majú viac kompletný a celistvý pohľad na klientske dáta a tiež dlhodobé skúsenosti s riadením rizika. (23)

3.4 Regulácia platobných služieb (PSD2)

Druhá regulácia platobných služieb pod názvom PSD2 (Payment service directive) vstúpila do platnosti v Európskej únií 12. Januára 2016 a oficiálne by mala nadobudnúť platnosť 13. Januára 2018. Smernica sa zameriava najmä na zaistenie, že všetky elektronické platobné služby sú vykonávané bezpečným spôsobom, tzn. technológiami, ktoré garantujú bezpečnú autentifikáciu klienta a znižujú maximálny rozsah rizika. (26)

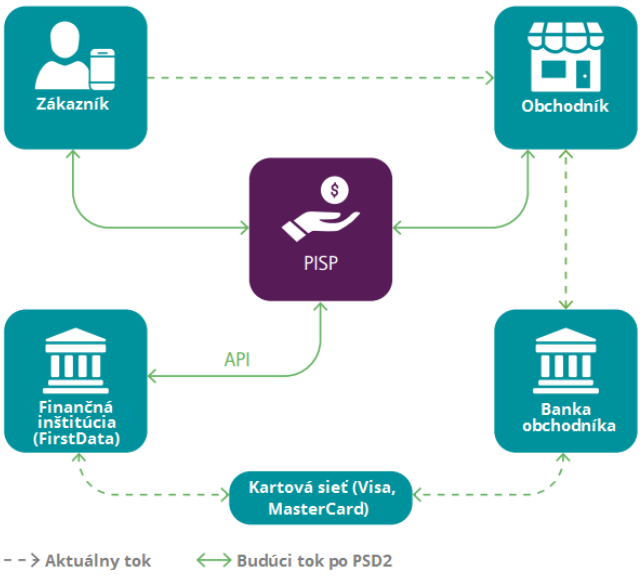
Európske banky sa nachádzajú v kritickom bode, kedy ich zmeny v bankovom sektore rezorte tlačia vykonať kľúčové strategické rozhodnutia. Majú možnosť si vybrať, či budú na užitočnej strane, tzn. podporovať ďalších poskytovateľov platobných služieb, alebo sa budú snažiť hrať kľúčovú rolu v dennom živote klientov. Hnacia sila za touto požiadavkou je známa ako Regulácia platobných služieb (PSD2), ktorá určuje rýchlosť konkurencie a digitálneho narušenia oblasti finančných služieb naprieč Európou. PSD2 bude stanovená ako právny rámec pre podnikateľov a zákazníkov, ktorí vytvárajú a prijímajú platby na území 28 členských štátov Európskej únie spolu s Nórskom, Islandom a Lichtenštajnskom. Táto smernica je dátovo a technologicky orientovaná a zameriava sa na nasledovné oblasti:

- prispieť k väčšej integrácií a výkonnosti európskeho platobného trhu.
- Podporovať konkurenciu pomocou regulačného rámca, ktorý podporuje vznik nových hráčov na bankovom trhu (napr. FinTechy) a rozvoj inovatívnych mobilných a internetových platobných služieb v Európe.

- Posilniť záujmy klienta a zvýšiť jeho ochranu pred rôznymi spôsobmi krádeže dát. Zabrániť zneužitiu a platobným incidentom pomocou zvýšených požiadaviek na bezpečnosť použitím silnej autentifikácie pre elektronické platby.
- Podporenie menších poplatkov za platby.

Jadrom smernice je požiadavka, aby bezpečným spôsobom poskytli banky tretím stranám on-line prístup k účtom klientov alebo platobným službám. V skratke ide o to, že banky musia otvoriť API svojho internetového bankovníctva. API je aplikačné programové rozhranie, ktoré môže byť definované ako zmes funkcii a procedúr, ktoré umožňujú pristupovať k dátam alebo službám, s cieľom poskytnúť väčšiu funkcionalitu používateľovi aplikácie. Toto pravidlo prístupu na účet poverí banku poskytnúť ďalšiemu poskytovateľovi platobných služieb (PSP) pomôcť bezpečne pristupovať cez API k účtom a údajom o klientovi, ktorý musí na poskytovanie svojich údajov udeliť súhlas. Na to, aby sa poskytol tento prístup k účtom, musia banky umožniť klientovi overenie identity a autentifikáciu prostredníctvom API. Prístup k účtom klientov cez API zabezpečí úplne nový spôsob poskytovania služieb, regulovaný smernicou PSD2.

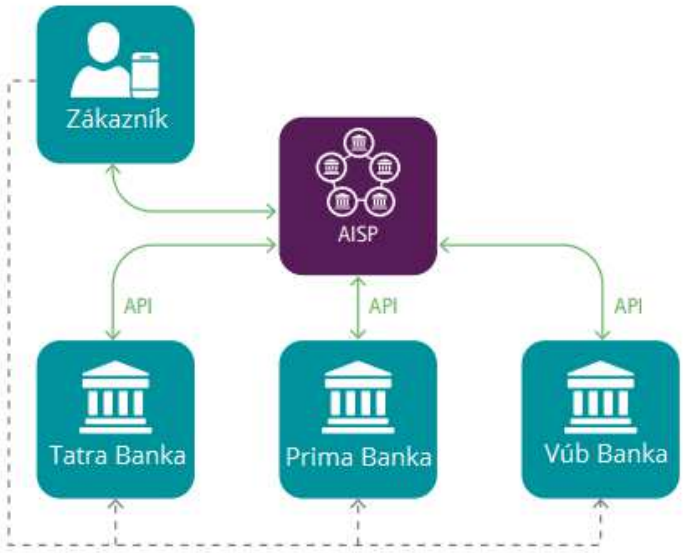
PISP (Payment Initiation Service Provider) je tretia strana, ktorá poskytuje a inicializuje platobné služby. Tretím stranám bude umožnené inicializovať on-line platby elektronickému obchodníkovi alebo ďalšiemu príjemcovi priamo z bankového účtu platiteľa prostredníctvom on-line portálu, ktorý bude umožňovať nové platobné riešenia. (27)



***Obrázok 5 Budúci platobný model nákupu tovaru cez tretiu stranu podľa PSD2* (27)**

AISP (Account Information Service Provider) je strana, ktorú PSD2 definuje ako poskytovateľ informácií o účte, schopný vyťažiť dáta o klientových účtoch, zahŕňajúc históriu transakcií a zostatky

na účte. Takýto poskytovatelia zbierajú finančné dáta z viacerých zdrojov, ktoré zlúčia do jedného zdroja, ako môžeme vidieť na príklade nižšie, kde klient bude vlastníkom účtov vo viacerých bankách. Do týchto účtov pristupuje oddelene, každá z týchto aplikácií má vlastné používateľské rozhranie – napr. Internet banking. Po implementácií požiadaviek PSD2 bude možné vidieť všetky tieto účty z jediného používateľského rozhrania – napr. mobilnej aplikácie, ktorú poskytne tretia strana AISP.



***Obrázok 6 Príklad modelu cez poskytovateľa informácií o účte (AISP) podľa PSD2* (27)**

PSD2 prinesie zásadné novinky ako:

- ovládanie účtov v iných bankách z jedného miesta,
- kompletný prehľad všetkých finančných produktov na jednom mieste,
- nástroje na finančné plánovanie vrátane auto-pilotov (ktorí budú posudzovať klientove prostriedky a presúvať ich napríklad medzi sporiacimi účtami, aby sa maximalizoval úrokový zisk klienta),
- zriaďovanie bankových produktov on-line – otváranie účtu on-line, zjednávanie úverov on-line, atď.

Ďalej je možné očakávať inovácie v oblasti platobných metód, napríklad okamžité platby, postupná náhrada platobných kariet. Platobné metódy budú vďaka Internetu vecí (Internet of Things) implementované do množstva pripojených zariadení ako auto, ktoré platí za mýto alebo parkovné. Ďalším príkladom môže byť práčka, ktorá si sama objedná prací prášok po jeho spotrebe, prípadne bude potreba len stlačiť tlačidlo na práčke. (28)

4 Bezpečnosť elektronického bankovníctva

Bankové prostredie je prostredie, ktoré prijalo nové technológie ako základ pre obchodné operácie, plány a stratégie na vytvorenie ešte silnejšieho, dostupnejšieho, konkurenčného a ekonomicky silného prostredia. Elektronické bankovníctvo je dôležité pre finančné inštitúcie. S nárastom počtu užívateľov elektronického bankovníctva rástol aj počet kriminálnych útokov. Bezpečnosť elektronického bankovníctva nie je závislá len na bezpečnostných opatreniach implementovaných bankou, ale je rovnako závislá na vedomí užívateľov týchto kanálov a na kvalite koncového zariadenia, ktorým užívateľ pristupuje do elektronického bankovníctva. Pre banku je povinnosťou chrániť dôvernosť a integritu bankových informácií.

4.1 Informačná bezpečnosť

Táto kapitola sa zaoberá informačnou bezpečnosťou. Účelom informačnej bezpečnosti je chrániť aktíva organizácie ako informácie, počítačový hardware a software. Hlavným cieľom bezpečnosti je pomôcť organizácií ochrániť fyzické a finančné zdroje, reputáciu organizácie, zamestnancov, právne postavenie a ďalšie hmotné a nehmotné aktíva. Správne zvolené bezpečnostné pravidlá a procedúry neexistujú len tak pre ich dobro, sú používané preto, aby chránili dôležité aktíva organizácie a boli podporou pre napĺňanie cieľov. Informačná bezpečnosť by mala byť založená na týchto základných prvkoch:

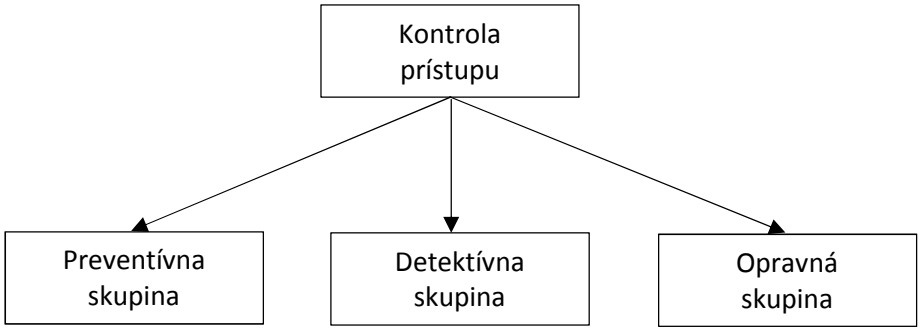
- podporovať ciele organizácie,
- rozhodovanie vrcholového manažmentu musí byť v súlade so záujmami organizácie,
- implementácia opatrení na základe nariadení je kontraproduktívna na klímu v organizácií. Predtým, než je nejaké opatrenie navrhnuté je potrebné posúdi existenciu daného rizika. Identifikáciou rizika a návrhom primeraného opatrenia budú ciele organizácie lepšie dosiahnuté. Z tohto vyplýva, že informačná bezpečnosť musí byť nákladovo efektívna,
- jedna z hlavných zodpovedností je monitorovať používanie, či je zaistené plnenie garantovanej úrovne autentifikácie užívateľovi.
- informačná bezpečnosť by mala byť pravidelne prehodnocovaná. Všeobecne platí, že čas mení potreby a ciele organizácie. Je to dynamický a meniaci sa proces a preto by mal byť prehodnocovaný najmenej raz za 18 mesiacov.

V biznise je zvyčajne až druhoradé mať efektívny bezpečnostný program, prvoradé je dosahovať zisk. Informačné systémy a informácie spracované v týchto systémoch sú často považované za kritické aktíva podporujúce ciele organizácie. Chrániť ich je preto rovnako dôležité ako chránenie iných zdrojov organizácie (finančné zdroje, fyzické aktíva a zamestnancov). Ak má systém externých používateľov, je potreba ich uistiť o dostatočnej bezpečnosti systému. (8)

4.2 Kontrola prístupu

Kontrola prístupu je vykonávaná prakticky na každom mieste a je základom informačnej bezpečnosti. Zamykáme dvere pri odchádzaní z našich domov, pri výbere hotovosti z bankomatu, kedy zadávame PIN kód na overenie majiteľa karty. Dôvodom, prečo tak robíme je, že sa snažíme chrániť hodnotu nejakého majetku (napr. peniaze na svojich účtoch v banke pri výbere z bankomatu). Je prirodzené, že každý si chce chrániť svoj majetok. Kontrola prístupu je spôsob ako riadiť prístup k dôležitým informáciám. Je to mechanizmus chrániaci tok informácií medzi subjektom a objektom, kde subjekt je vždy aktívna entita a objekt, naopak pasívna. V širšom význame je kontrola prístupu trojkrokový proces zahrnujúci identifikáciu, autentizáciu a autorizáciu. Význam autentifikácie je všeobecne používaný pojem, ktorý reprezentuje identifikáciu a autentizáciu. Kontrola prístupu je pojem používaný pre autorizáciu.

Kontrola prístupu podporuje jadro bezpečnostných zásad ako dôvernosť, integritu a dostupnosť tým, že vyžaduje od používateľa systému jeho jednoznačnú identifikáciu a overenie, že vlastní len také práva a disponuje takými informáciami, ku ktorým získal prístup v konkrétnom systéme. Po určení toho, čo chceme chrániť, je potrebné zvoliť vhodný spôsob kontroly prístupu, ktorá tieto informácie ochráni.



Obrázok 7 Tri vzájomne pôsobiace skupiny kontroly prístupu (vlastné spracovanie) **(8)**

Podľa Thomasa Peltiera môžeme rozdeliť kontrolu prístupu do troch skupín:

- preventívna,
- detektívna,
- opravná.

Každý efektívny informačno-bezpečnostný program by sa mal usilovať o dosiahnutie kombinácie týchto troch skupín, čo zabezpečí hlbokú obranu systému. Použitím opatrení, ktoré budú najviac efektívne pre danú situáciu poskytne najlepší spôsob ochrany. (8)

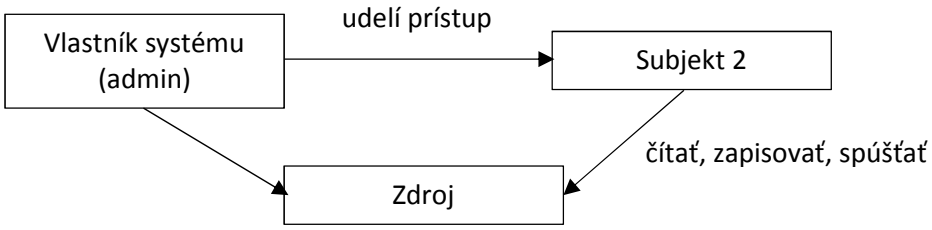
4.2.1 Modely kontroly prístupu

Model kontroly prístupu je rámec, ktorý formuje kontrolu prístupu použitím rozličných technológií. Každý model ma vlastné výhody a nevýhody a je prispôsobený špecifickým cieľom organizácie, ktoré závisia od jej potrieb, kultúry a prostredia, v ktorom pôsobí. Primárnym prístupovým kontrolnými modelmi sú:

- povinná kontrola prístupu (MAC – Mandatory Access Control),
- posudková kontrola prístupu (DAC – Discretionary Access Control),
- kontrola prístupu na základe jednotlivých rolí (RBAC – Role Based Access Control).

Povinná kontrola prístupu je založená na princípe, že vlastník dát má obmedzenú voľnosť pri určovaní kontroly prístupu. Informácie sú rozdelené do rôznych kategórií a každá kategória spadá pod určitú bezpečnostnú úroveň. Napríklad účty klientov sú veľmi dôverný zdroj, ktorému banka prideľuje úroveň veľmi dôverné. Ak sa užívateľ, ktorý patrí len do úrovne dôverné, snaží pristúpiť k účtom klientov, jeho prístup je zamietnutý, pretože sa tieto dve úrovne nezhodujú. Tento model je vhodný najmä v banke, kde je ochrana veľmi dôverných informácií kritická.

Posudková kontrola prístupu je založená na vlastníctve a delegovaní. V modeli je prístup riadený prístupovými právami udelenými používateľovi alebo skupine používateľov. Organizácia alebo administrátor môže nastaviť oprávnenia niektorému z objektov ako bude pristupovať k určitému zdroju dát.



Obrázok 8 DAC - Posudková kontrola prístupu (vlastné spracovanie) **(29)**

Kontrola na základe jednotlivých rolí je najviac používaná na trhu. Model umožňuje prístup k jednotlivému zdroju na základe role používateľa v jednotlivej organizácií. Je založený na princípe rozdelenia povinnosti. (29)

4.3 Autentifikácia

Autentifikácia alebo identifikácia sú prvým krokom pri riešení kontroly prístupu. Je to proces identifikácie klienta, či je to tá osoba, za ktorú sa vydáva. Identifikácia klienta je vykonaná pomocou známych informácií pre užívateľa (meno užívateľa alebo ID užívateľa) a informácií, ktoré pozná len

jediný subjekt (heslo užívateľa). Už dlhšiu dobu vo veľa prípadoch platí, že hlavným spôsobom overenia identity klienta pri vstupe do systému je heslo. Význam hesla spočíva v tom, že ho pri zadávaní do systému pozná len užívateľ, aby systém identifikoval, že práve táto osoba získala prístup k daným informáciám. Je zrejmé, že heslo v niektorých prípadoch nemôže stačiť. Užívatelia si heslo ťažko pamätajú a tak si ho zapisujú na rôzne ľahko dostupné miesta, alebo ho dokonca s niekým zdieľajú. Najmä banky sa stretávajú s hrozbou krádeže identity klienta. Skúsenosti ukazujú, že autentifikácia v podobe osobného identifikačného čísla (PID) a hesla poskytuje pomerne slabý spôsob overenia totožnosti, pretože môžu byť často ukradnuté alebo niekým uhádnuté. Na základe nárastu následkov spojených so zlyhaním bezpečnosti informácií, sa organizácie začali obzerať po silnejších formách overenia identity klienta. Autorizácia nasleduje až po úspešnej autentifikácií. Je to overenie k nejakému úkonu alebo k vykonaniu nejakej operácie. Jedná sa o zistenie, či daný subjekt môže danú operáciu vykonávať. Častokrát sa pojmy autorizácia a autentifikácia zamieňajú.

Dvojfaktorová autentifikácia je jednou z metodológií, ktoré využívajú najmä banky pre prístup do elektronického bankovníctva. Pri výbere hotovosti z bankomatu sa využíva dvojfaktorová autentifikácia, kedy musíme mať pri sebe platobnú kartu a poznať PIN kód karty. Požiadavky na silnú autentifikáciu sú vymedzené aj v smernici PSD2, ktorá vstúpi do platnosti začiatkom roka 2017. Viacnásobná autentifikácia poskytuje výhodu v tom, že sa skladá z viacerých autentizačných technológií poskytujúcich väčšiu bezpečnosť spoliehajúcu sa na dva alebo tri bezpečnostné faktory:

- niečo, čo užívateľ pozná (PIN),
- niečo, čo užívateľ vlastní (Smart karta),
- niečo, čo užívateľ je (odtlačok prsta).

Dobrá autentizačná technika obsahuje najmenej dva z vyššie uvedených faktorov. V prostredí klient-server je silnou autentifikačnou kombináciou autentizácia klienta a servera:

- serverová autentifikácia je autentizácia, pri ktorej server potvrdí identitu užívateľa,
- naopak klientska je, ak klient potvrdí jeho identitu serveru.

Existujú rôzne autentizačné metódy, ktoré môžu banky použiť pri zabezpečení prístupu do elektronického bankovníctva.

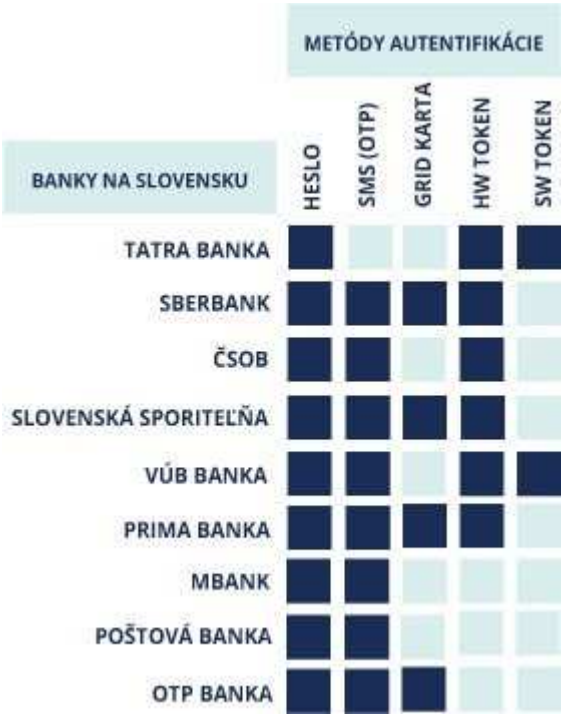
4.3.1 Autentizačné metódy používané slovenskými bankami

Dnes bankové inštitúcie poskytujú produkty a služby na Internete použitím rôznych autentifikačných techník na identifikáciu svojich klientov. Jednofaktorová autentizácia už nestačí a je potrebné hľadať nové riešenia, ako posilniť proces overenia identity klienta pri prihlasovaní do elektronického bankovníctva.

Každá autentifikácia začína identifikáciou klienta. Spôsob identifikácie klienta do elektronického bankovníctve spočíva v zadaní platného osobného identifikačného čísla (PID). PID je banka povinná odovzdať klientovi banky pri zriaďovaní prístupu do elektronického bankovníctva po podpise zmluvnej dokumentácie (podpisom dokumentu klient vysloví súhlas banke). Okrem PID je banka povinná odovzdať klientovi heslo (po zriadení prístupu je klientovi odoslané cez SMS s obmedzenou platnosťou) a aktivovať bezpečnostný prvok.

Zriadením prístupu do elektronického bankovníctva sa PID klienta stáva aktívny a klient sa môže okamžite prihlásiť. Po identifikácií klienta osobným identifikačným číslom prichádza na radu autentizácia klienta. Identifikácia a autentizácia nasledujú po sebe ako dva neoddeliteľné procesy. Heslo pozostávajúce z textového reťazca patrí stále medzi najviac používanú formu autentizácie. Heslo je zvyčajne v spojení s ďalšími autentizačnými metódami ako SMS autentizácia (One-time password), čo tvorí dvojfaktorovú autentizáciu. Porovnávacia tabuľka ukazuje rôzne spôsoby overenie identity klienta, ktoré používajú slovenské banky s cieľom ochrániť prístup do elektronického bankovníctva:

- heslo,
- SMS autentizácia (na základe overenia kódom, zaslaným na vopred zadané číslo),
- autentizácia GRID kartou (na základe overenia jednorazového prístupu hesla z GRID karty po výzve systému),
- Hardware token (na základe overenia jednorazového prístupu hesla z hardwarového zariadenia po výzve systému)
- Software token (na základe overenia jednorazového prístupu hesla zo softwarového zariadenia po výzve systému). (30)



Obrázok 9 Autentizačné metódy používané slovenskými bankami (vlastné spracovanie)

4.3.1.1 Používateľské heslo

Overenie totožnosti klienta heslom je v súčasnosti najviac používaná forma autentizácie (niečo, čo užívateľ pozná). Autentizácia heslom patrí medzi metódy, ktoré sú najmenej nákladné na implementáciu a zároveň pre klienta ľahko použiteľné v dôsledku častého používania. Jeho jednoduchá forma však môže užívateľom prinášať problémy. Najčastejšie problémy vznikajú, keď užívateľ zabudne heslo a musí kontaktovať bankovú inštitúciu na jeho resetovanie. Niektoré banky vykonávajú reset hesla cez kontaktné centrá pomocou bankových systémov. Pred resetom hesla musia najprv overiť totožnosť klienta. Nutnosť prevádzky kontaktných centier na tieto účely znamenajú pre banky zvýšené náklady.

Odkedy sa heslo stalo najpoužívanejšou formou elektronickej autentizácie je považované za jej najslabšiu formu. Mnoho užívateľov podceňuje vytvorenie si silného hesla, a tak sa heslá stávajú ľahko uhádnuteľné, alebo nezákonne získateľné. Podľa štúdie vykonanej spoločnosťou SplashData patrí heslo „123456“ medzi najviac používané a za ním nasleduje ďalšie slovo „password”. V prvej desiatke sa ešte umiestnili heslá ako „abc123“ alebo „111111“. (31) Podobná štúdia, ktorá skúmala 1800 dospelých ľudí zistila, že približne 25% používateľov používa heslá, ktoré sú ľahko uhádnuteľné, napr. dátumy narodenia alebo mená. Skoro viac ako polovica priznala, že rovnaké heslo používa na viacerých webových stránkach. (32)

Pokračujúce vzdelávanie svojich klientov o bezpečnosti hesiel je základom pre bankové inštitúcie a iné spoločnosti, ktoré vyžadujú heslo na overenie prístupu do ich aplikácií alebo webových stránok.

Bezpečnostní experti všeobecne odporúčajú nasledovné praktiky na poskytnutie bezpečného riadenia hesiel:

- výber silného hesla, ktoré obsahuje malé a veľké písmena, čísla a špeciálne znaky skladajúce sa minimálne z ôsmich znakov.
- Výmena písmen alebo číslic za znaky, namiesto S napíšem $ alebo namiesto L napíšem 1.
- Vyhnúť sa používaniu rovnakých hesiel pre viacero stránok ako aj použitím rovnakého základu slova, ktoré sa spojí napr. s menom stránky, kde sa klient registruje. Útočníci často používajú ako nástroj slovník pri automatizovaných útokoch na heslá.
- Pravidelnú zmenu hesla, najmenej jedenkrát ročne v aplikáciách ako Internet banking alebo iných citlivých webových stránkach obsahujúce osobné informácie užívateľa.
- Nezapisovať si heslo na miesta v blízkosti počítača alebo ho niekomu prezradiť.

Digitalizácia vyústila k viacerým digitálnym identitám a heslám, ktoré si nemôžeme pamätať. V jej dôsledku si heslo buď niekde zapíšeme, alebo si vytvoríme heslo jednoduchšie na zapamätanie. Existuje tendencia, že heslo, ktoré používame na jednom účte, použijeme na inom účte. Môže to znamenať vážne bezpečnostné rizika, napr. ak rovnaké heslo, ktoré používame na sociálnych sieťach použijeme pri prihlasovaní do Internet bankingu. Sociálne siete môžu byť napadnuté, čo vyústi do krádeže identity v dôsledku neadekvátnej ochrany databázy hesiel. Útočník sa bude potom pokúšať ukradnuté heslo použiť na inom účte osoby, ktorej identita bola ukradnutá. (33)

Pravidelná zmena hesla na základe požiadaviek na vytvorenie silného hesla môže na organizáciu negatívne vyplývať tým, že používateľ systému nevie pristúpiť do aplikácie, pretože zabudol heslo. Z dôvodu zníženia rizika pri realizácií väčšej sumy transakcie, mnoho spoločností implementovalo dodatočnú autentizačnú metódu.

4.3.1.2 Hardwarový Token

Bezpečnostné tokeny sú používané ako súčasť viacnásobnej autentizácie. Fyzický token patrí do skupiny bezpečnostných prvkov (niečo, čo užívateľ vlastní) v kombinácií s ďalšou bezpečnostnou metódou (niečo, čo užívateľ pozná). Token funguje na princípe OTP (One-time password) teda jednorazového kódu alebo hesla, ktoré zabraňuje opakovaným útokom. Mnoho bánk prijalo OTP autentizáciu použitím hardwarových tokenov, ktoré dodávajú svojim klientom ak jednu z častí viac faktorovej autentifikácie. Vreckové zariadenia sú vybavené malým displejom a prípadne klávesnicou, ktoré vo všeobecnosti nepotrebujú byť pripojené na užívateľov počítač. Zariadenie je nakonfigurované na autentizačný server ešte dávno pred vydaním zariadenia budúcemu užívateľovi, čo umožňuje serveru a tokenu zdieľať tajomstvo ako základ pre autentifikáciu. Typický scenár prihlasovania do Internet bankingu vyzerá tak, že cieľový systém bude vzájomne komunikovať

s autentizačným serverom a žiadosťou preukázať identitu užívateľa Internet bankingu. Užívateľ vstupuje do malého vreckového zariadenia tokenu zadaním PIN čísla a token následne zobrazuje autentizačnú informáciu, ktorú vyžaduje server. Táto informácia musí byť v stanovenom čase zadaná do zariadenia, na ktorom sa snaží užívateľ pristúpiť do Internet bankingu, čím umožní užívateľovi skompletizovať autentizačný proces. (34)

Ak je token stratený alebo ukradnutý, aspekt viacnásobnej autentizácie (zadanie hesla alebo PIN čísla) ho chráni pred možným rizikom. Ak klient zadá niekoľko krát nesprávne heslo pri vstupe do zariadenia, token sa zablokuje na serveri. Tokeny sú odolné aj voči reverznému inžinierstvu. Zariadenie obsahuje batériu, ktorá zabezpečuje fungovanie zariadenia. Vo všeobecnosti je životnosť takéhoto zariadenia približne 10 rokov. Okrem batérie požaduje aj systém riadenia s primeraným stupňom kontroly a administratívy. Niektoré banky pomaly upúšťajú od tohto riešenia. Hoci poskytuje vysokú bezpečnosť, náklady na prevádzku a riadenie procesov súvisiacich s tokenom odrádzajú banky od takéhoto riešenia.

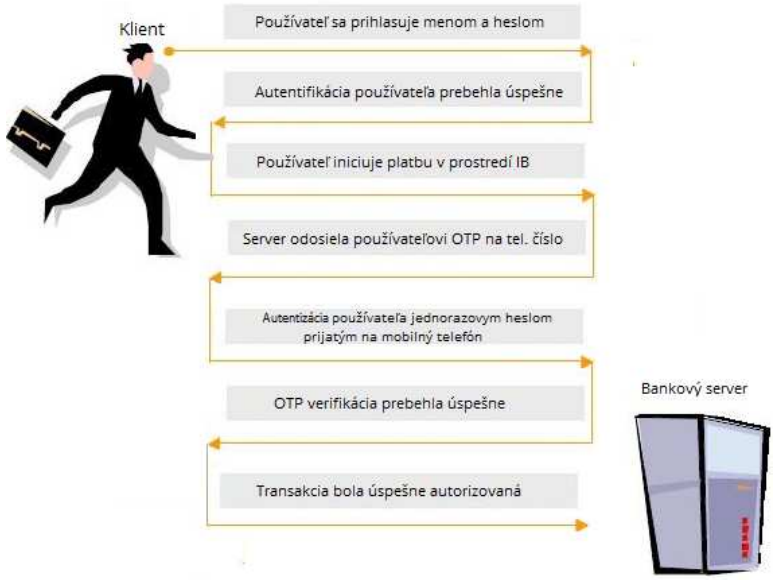
Obrázok 10 Jedno z riešení autentizácie tokenom spoločnosti Vasco **(35)**

4.3.1.3 SMS (OTP) autentizácia

Služba krátkych správ (SMS – Short Message Service) založená na OTP prišla s cieľom postaviť sa Phisingu a ďalším útokom proti autentifikácií a autorizácií internetových služieb. OTP je používané ako doplňujúci faktor pri viacfaktorovej autentifikácií alebo autorizácií. Táto metóda patrí medzi najviac používaný spôsob zabezpečenia internetového bankovníctva. Na jej používanie potrebuje užívateľ vlastniť mobilný telefón. Telefónne číslo užívateľa systému musí byť zaregistrované pre služby, ktoré poskytujú SMS OTP autentizáciu. Je to pohodlný spôsob, ako poskytnúť užívateľovi

heslo s určitou dobou platnosti, ktoré mu je následne poslané cez SMS správu. Celý proces autentizácie funguje tak, že užívateľ Internet bankingu musí zadať ďalšie jednorazové heslo (One-time password) na overenie identity hneď po zadaní osobného identifikačného čísla a hesla. Spôsob overenia identity jednorazovým heslom využívajú aj iné komerčné služby ako Google Mail, Viber a pod.

V Internet bankingu sa služba používa aj pri autorizácií platieb. V prvom kroku užívateľ vstupuje na webovú stránku banky, v ktorej má zriadený prístup do internetového bankovníctva. Na tejto stránke zadáva prihlasovacie meno a heslo. Po úspešnom overení totožnosti klienta vstupuje na jeho osobný účet. Užívateľ potom iniciuje transakciu a bankový server odpovedá späť formou jednorazového hesla, ktoré musí klient banky zadať do systému. Zadané jednorazové heslo je kontrolované na serveri, ak je správne, klient dostáva informáciu o úspešnej autorizácií transakcie. Transakcia je ihneď po autorizácií odoslaná do banky na spracovanie. Táto forma autorizácie transakcií známa pod skratkou TAN (Transaction Authorization Number) patrí do druhej úrovne autentifikácie a autorizácie s cieľom vyhnúť sa krádeži hesla.

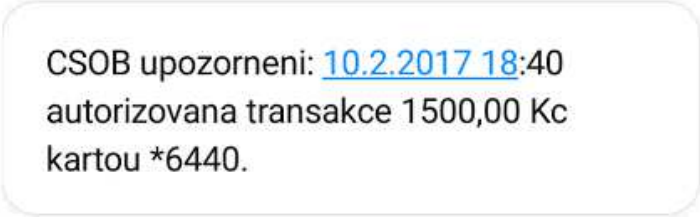


Obrázok 11 Autorizácia platby v prostredí internetového bankovníctva (vlastné spracovanie)

SMS autentizácia poskytuje neparalelnú kombináciu bezpečnosti a pohodlia, z ktorej vyplýva niekoľko výhod:

- zvyšuje bezpečnosť systému,
- znižuje náklady na celkovú bezpečnosť. V porovnaní s hardwarovými tokenmi, kde existujú náklady jak na nákup zariadenia, tak aj na jeho distribúciu spolu s nákladmi na administratívu pri strate zariadenia.

- Prináša dvojfaktorovú autorizáciu aj tam, kde to bolo v minulosti nepraktické.



Obrázok 12 Príklad SMS správy od ČSOB pri autorizovaní transakcie (snímka obrazovky)

4.3.1.4 GRID karta

GRID karta patrí do skupiny autentizačných prvkov (niečo, čo užívateľ vlastní), ktoré obsahujú náhodne vygenerované čísla a znaky usporiadané do riadkov a stĺpcov. Veľkosť karty je určená počtom buniek na mriežke. GRID karty sú lacné plastové karty, fungujúce na princípe jednorazového kódu (OTP). Sú klientami obľúbené najmä preto, že sú odolné a jednoducho prenášateľné. Tento typ autentizácie nevyžaduje žiadne zložité školenie. Ak je karta stratená, jej náhrada je relatívne jednoduchá a lacná. Proces autentizácie GRID kartou v Internet bankingu funguje tak, že užívateľ najskôr musí zadať jeho osobné identifikačné číslo PID a heslo stanoveným spôsobom. Ak sú informácie zadané korektne, užívateľ je systémom vyzývaný na zadanie vstupu obsahujúceho náhodne vybranú bunku z druhého autentizačného prvku (GRID karty). Užívateľ odpovedá zadaním údajov z danej bunky na karte, ktorá pre správne overenie totožnosti korešponduje s výzvou z Internet bankingu. Problém s GRID kartami je najmú kvôli limitujúcemu zoznamu buniek, ktorý môže byť ľahko použitý pre budúci prístup. Niektorí klienti takéto riešenie akceptujú v dôsledku ľahkej manipulácie, iní zasa tejto metóde nedôverujú z hľadiska bezpečnosti. Je to práve nízka bezpečnosť, čo vedie GRID kartu do záhuby. Ako môžeme vidieť aj na analýze autentizačných nástrojov jednotlivých bánk na Slovensku, takéto riešenie je na ústupe. Pomaly ho nahrádzajú iné, lepšie a bezpečnejšie autentizačné nástroje. Môže za to najmä neopatrné správanie klientov. Podrobnejšia analýza GRID kariet bude popísaná v praktickej časti.

	A	B	C	D	D	F	G	H
1	1234	1234	1234	1234	1234	1234	1234	1234
2	1000	1000	1000	1000	1000	1000	1000	1000
3	4321	4321	4321	4321	4321	4321	4321	4321
4	1234	1234	1234	1234	1234	1234	1234	1234
5	1000	1000	1000	1000	1000	1000	1000	1000
6	4321	4321	4321	4321	4321	4321	4321	4321
7	1234	1234	1234	1234	1234	1234	1234	1234

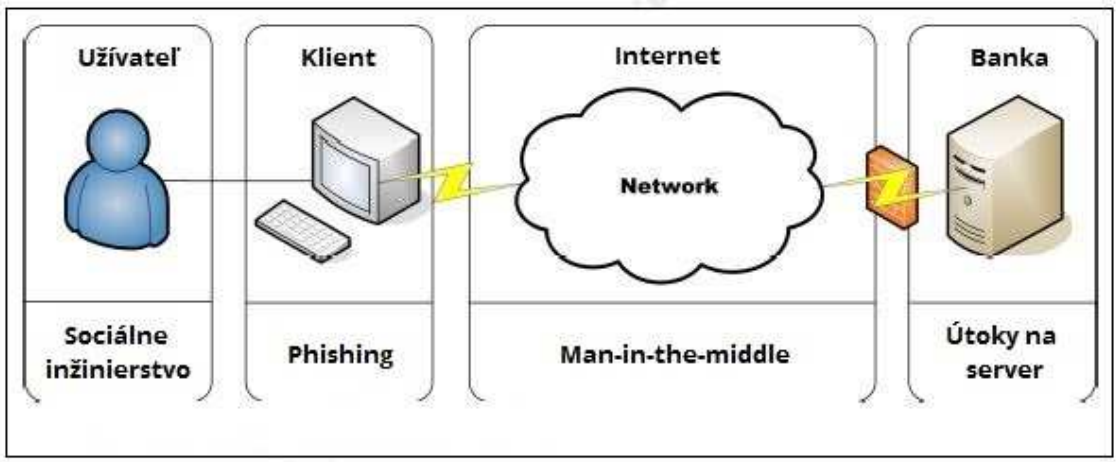
Obrázok 13 Zobrazenie GRID karty (vlastné spracovanie)

4.4 Bezpečnostné hrozby

Je to len pár rokov dozadu, čo finančné inštitúcie začali ponúkať svojim klientom služby elektronického bankovníctva, ktorého popularita rástla spolu s rozvojom Internetu. S popularitou sa tento kanál stal záujmom pre organizovaných útočníkov. Na rozdiel od prvých útokov, kedy útočníci svoje obete len obťažovali, sa tieto útoky vyvinuli do závažných zločinov, ktoré boli zamerané najmä na finančné služby. Podľa Hiltgena (36), môžeme autentizačné metódy klasifikovať podľa ich odolnosti voči útokom, ktoré potom rozdeľujeme na dva rôzne typy:

- útoky vykonávané off-line spôsobom, ktoré sa snažia nahromadiť všetky poverenia užívateľa. Takýto útok môže byť vykonávaný nejakým škodlivým softvérom ako vírus alebo trojský kôň, tým, že oklame užívateľa, ktorý dobrovoľne poodhalí jeho všetky poverenia cez phishingový útok.
- útoky vykonávané on-line spôsobom, ktoré dnes patria medzi najviac sofistikované útoky. Namiesto zachytenia užívateľových poverení, správy medzi klientskym počítačom a serverom sa nedajú pozorovane zachytiť. V takýchto prípadoch sa stáva, že útočník je zamaskovaný ako server voči klientovi a ako klient k serveru, v uvedenom poradí.

V minulosti sme mohli vidieť veľké množstvo útokov na strane serveru. Posledné útoky sa odkláňajú smerom na užívateľa, konkrétne na jeho počítač alebo sieť. Tento obrázok ukazuje možné miesta útokov.



Obrázok 14 Typy útokov vyplývajúce z miesta vykonania útoku **(37)**

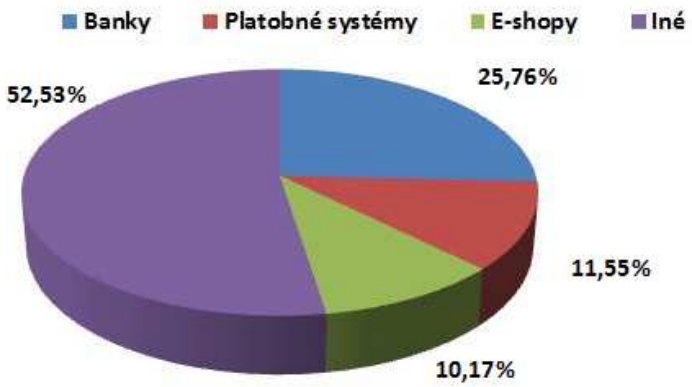
4.4.1.1 Phishing

Phishing je jednoduchá forma sociálneho inžinierstva, používajúca rôzne technické a netechnické metódy, s účelom získania osobných a dôverných informácií. Za dôverné informácie môžeme považovať osobné identifikačné číslo PID, číslo účtu, heslo alebo nejakú dôvernú informáciu, ktorá patrí určitému užívateľovi. Systematicky spôsob odoslania falošného e-mailu snažiaci sa naviesť klienta banky na falošné webové stránky, ktoré sa podobajú stránke banky. Cieľom je oklamanie klienta spôsobom, kedy klient svojou nevedomosťou netuší, že je na falošných stránkach banky, čím prezradí niektorý zo svojich dôverných údajov. Technická časť útoku pozostáva z e-mailu s falošnou adresou. Užívateľ klikne na odkaz nachádzajúci sa v podvodnom e-maile, ktorý ho presmeruje na falošnú webovú stránku útočníka, vyzývajúc užívateľa na zadanie jeho dôverných údajov do webového formulára. Miera úspechu phishingového e-mailu je udivujúco vysoká najmä preto, že užívateľ vo veľa prípadoch nevie s určitosťou identifikovať originálnu webovú stránku banky. Na vykonanie takéhoto útoku stačí rozposlať podvodný e-mail na veľký počet e-mailových adries. Ďalšia definícia hovorí, že phishing je forma sociálneho inžinierstva, v ktorej sa útočník pokúša podvodne získať dôverné a citlivé informácie užívateľa, napodobňovaním elektronickej komunikácie verejných organizácií. Techniky, ktoré zvyčajne používa, sú podvodné e-maily a webové stránky, ktoré sa podobajú legitímnym e-mailom a webovým stránkam. (38)

Obrázok 15 Proces phishingového útoku (vlastné spracovanie)

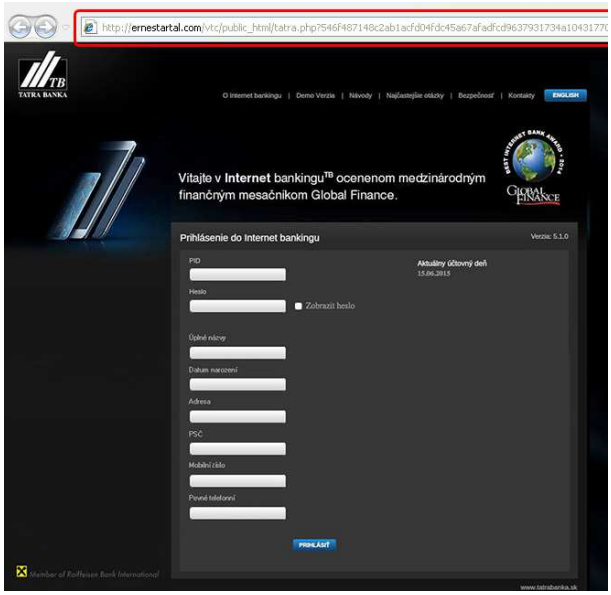
Útok na svoju obeť môže byť vykonávaný off-line spôsobom, s cieľom podvodne nahromadiť užívateľove údaje. Avšak phishingové útoky sa častokrát vyskytujú aj ako on-line útok, kedy útočník zbiera údaje užívateľa, ktoré okamžite využíva na prihlásenie sa do aplikácie a krádež finančných prostriedkov z účtu klienta. Autentizačné systémy založené na statických heslách sú viac zraniteľné voči phishingovým útokom. Naopak, pri dynamicky sa meniacich bezpečnostných kódoch je menšia pravdepodobnosť úspešnosti takéhoto útoku. (39)

Kaspersky Lab zaznamenal v roku 2016 takmer 155 miliónov pokusov užívateľov o otvorenie niektorej z falošných webových stránok, ktorej predmetom bola phishingová kampaň. Cieľom útokov bolo najmä pokus o zisk prístupu k citlivým osobným údajom ako prihlasovacie údaje, heslá a ďalšie informácie o bankových účtoch. Podľa správy Kaspersky Lab bol podiel finančných phishingových hrozieb doteraz najväčší. Až približne 25% zo všetkých phishingových útokov predstavujú útoky na klientov bankových inštitúcií.



Graf 4 Podiel zamerania phishingových útokov za rok 2016 podľa Kaspersky Lab (39)

S pokusmi o phishingový útok sa v poslednej dobe stretla aj Tatra banka, ktorá potvrdila zvýšený výskyt takejto aktivity. Princíp útoku spočíval v predpoklade, že človek je dôverčivý a keď zaznamená podobný e-mail, ktorý dostáva bežne od banky, nevšimne si to. V tele správy tohto e-mailu bol zakomponovaný odkaz na podvrhnutú webovú stránku.

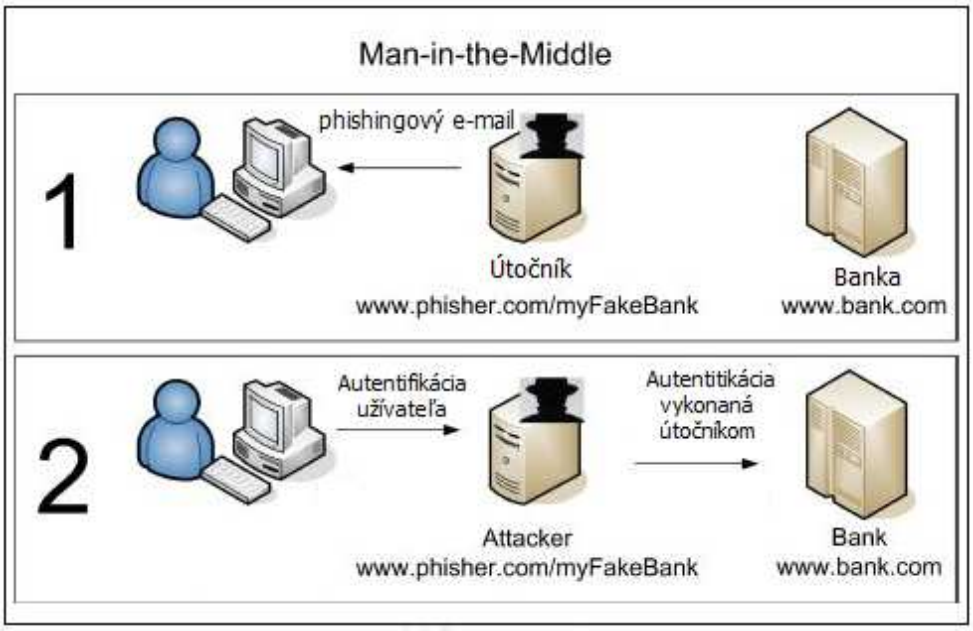


***Obrázok 16 Príklad phishingového útoku na Tatra banku* (40)**

Útoky podobného charakteru sú väčšinou mierené len na klientov banky a nie na banky samotné. Jediný spôsob, akým môžu banky bojovať proti týmto útokom, je prevencia a zverejňovanie informácií a rád, ako takýmto útokom predchádzať. (40)

4.4.1.2 Man in the Middle (MITM)

Jedná sa o typ útoku, kedy útočník zachytáva komunikáciu medzi bankou a klientom, ktorú následne zamieňa za jeho vlastnú formu komunikácie, aby celý proces vyzeral tak, že komunikujú medzi sebou. Cieľom je snaha útočníka odpočúvať komunikáciu medzi napr. bankou a klientom, tým že sa útočník stane prostredníkom medzi nimi. Existujú rôzne spôsoby, ako tieto útoky fungujú. Jedným zo spôsobov, je predložiť klientovi škodlivú stránku, ktorá vo všeobecnosti nahrádza originálnu stránku. Keď sa obeť prihlási so správnymi údajmi, útočník sa môže jednoducho pripojiť na vytvorenú on-line reláciu (session). Dokonca aj pri prípadoch, kedy sa pri prihlasovaní používa zariadenie čakajúce na výzvu (token) je útočník pasívne pozorujúci spojenie medzi serverom a obeťou. Útočník jednoducho sleduje celú premávku počas doby, kým je relácia spustená a potom posiela podvodnú transakciu.



***Obrázok 17 Spôsoby útokov pri Man-in-the-Middle podľa SANS Institute* (37)**

Obrázok zobrazuje dva typy útokov MITM (Man-in-the-Middle):

- útočník posiela falošný e-mail obeti, ktorý ju po kliknutí na odkaz v tele e-mailu presmeruje na falošnú webovú stránku,
- užívateľ zadáva autentifikačné údaje na falošnú webovú stránku. Útočník sa okamžite prihlasuje na skutočnú stránku banky s údajmi užívateľa, kde dochádza ku krádeži.

4.4.1.3 Iné typy útokov

Tradičné trojské kone a škodlivé vírusy patria do kategórie bežných útokov. Jedným z nich je aj škodlivý trojský kôň **keylogger**, ktorý sa vo všeobecnosti nepozorovane infiltruje do počítača, kde kradne údaje sledovaním úderov do klávesnice. Potom tieto údaje uloží ako textové záznamy do súboru a pošle ich vzdialenému útočníkovi. Niektoré formy keyloggerov dokážu zachytávať snímky obrazoviek počítača, ak by sa chcel užívateľ ubrániť útoku tým, že by použil myš pri prihlasovaní, tak by mu to v tomto prípade nemuselo pomôcť. Tento trojský kôň je najčastejšie posielaný ako príloha v e-mailoch alebo odkaz v správach na sociálnych sieťach. (41)

Ďalším typom útoku na kanály elektronického bankovníctva je **pharming**. Útok patrí do skupiny typu phishing a rovnako môže postihnúť viacero užívateľov naraz. Pharming je viac technologicky pokročilá forma phishingu, pri ktorej je v počítači tajne nainštalovaný vírus, alebo škodlivý program. Zadaním skutočnej webovej adresy počítač užívateľa presmeruje na imitáciu tejto stránky. Výsledkom je zadanie dôverných informácií na falošných webových stránkach. A to aj napriek tomu, že obrazovka počítača zobrazuje požadovanú webovú adresu stránky, DMS (doménový systém mien) presmeruje prevádzku na podvodné miesta. Aby bolo možné nadviazať spojenie, musí byť reťazec znakov tvoriacich internetovú adresu prevedení na IP adresu. Pharming patrí medzi zákernejšie formy útoku, pretože útočník neútočí priamo na užívateľa vytváraním podvodných stránok, ale snaží sa ovládnuť skutočné webové stránky určitej organizácie napr. banky. Po napísaní URL adresy požadovanej webovej stránky, prehliadač pristúpi na DNS server na načítanie číselnej IP adresy zodpovedajúcej zadanej URL adrese, aby zobrazila požadovanú webovú stránku. Pharming funguje tak, že mení zoznam adries na DNS serveri, čo znamená, že požadovaná URL adresa poukazuje na IP adresu podvodnej webovej stránky. Takýmto útokom môže zvýšiť počet užívateľov, ktorí nechcene navštívia podvodnú webovú stránku. Na ochranu pred týmto útokom môže pomôcť kvalitný antivírový program, ktorý rieši ochranu proti vírusom a škodlivým kódom. (42)

Phishingové e-maily nie sú jediná cesta, ktorou sa útočníci pokúšajú získať osobné informácie obete s cieľom ukradnúť mu jeho identitu alebo spáchať nejaký podvod. Útočníci pri tomto type útoku využívajú telefón. **Vishingu** sa hovorí aj ako telefónnej verzii phishingu. Jedná sa o podvodný postup vykonávaný prostredníctvom telefonického rozhovoru, ktorého cieľom je získanie citlivých údajov od obete útoku (napr. prístupové heslá do Internet bankingu, čísla platobných kariet alebo iné osobné údaje). Útočníci tento spôsob preferujú z dôvodu ťažšej identifikácie útočníka. Útočník zasiela obetiam textovú správu, telefónny odkaz alebo e-mail so stručnou informáciou, ktorá obsahuje informáciu o vzniknutom bezpečnostnom probléme. Útočník od svojej obete žiada, aby ho osoba priamo kontaktovala na telefónne číslo, ktoré sa nachádza v tele správy. Následne sa útočník predstaví ako banka klienta. Napr. Slovenská sporiteľňa na svojich webových stránkach uvádza

prípad, kedy si útočník na získanie dôvery pýta od klienta banky autorizačný kód práve doručenej SMS alebo pozície z GRID karty. Získané údaje klienta využíva buď okamžite, alebo neskôr v závislosti na bezpečnostnom prvku. Ak sa jedná o OTP kód napr. SMS správa, tak musí útočník reagovať okamžite. Banky svojim klientom odporúčajú, aby nikdy neposkytovali žiadne osobné, autorizačné alebo finančné informácie iným osobám, ktoré sa vydávajú za bankové inštitúcie či už elektronickou poštou alebo telefonicky. (43)

5 Definícia požiadaviek na autentizačný prvok

Bezpečnosť systému môže byť vo všeobecnosti kompromis medzi vysokou úrovňou bezpečnosti a jednoduchšou použiteľnosťou, alebo pohodlnosťou pre užívateľa. Čím viac bezpečnostných krokov je pridaných do procesu overovania totožnosti, tým menšia je miera akceptácie od užívateľov systému. Výnimkou nie je ani používanie internetového bankovníctva. Pre banky je preto veľkou výzvou nájdenie dostatočne bezpečných autentizačných systémov, ktoré budú akceptované klientmi. Klienti banky budú vždy požadovať nové aplikácie a funkcie s jednoduchým používateľským rozhraním, no zároveň budú žiadať, aby sa novými riešeniami zvyšovala aj bezpečnosť. Narastajúca mobilita klientov je ďalší veľmi dôležitý faktor. Klienti chcú pristupovať k svojim účtom nie len z počítačov v domácnosti, ale rovnako aj v práci, na dovolenke, na cestách, prostredníctvom mobilných zariadení. Tieto potreby sa stavajú pred dôležité požiadavky na bezpečnosť elektronického bankovníctva.

Pri definovaní požiadaviek na bezpečnosť systému je potrebné si jasne zadefinovať, aký problém riešime. Pri výbere bezpečnostného prvku treba mať na mysli nielen potreby klienta, ale aj záujmy organizácie. Nová metóda overovania identity pri prihlasovaní do internetového bankovníctva môže vyriešiť problémy súvisiace s bezpečnosťou. Môže ísť o problémy ako posilnenie slabého bezpečnostného protokolu, zvýšenie dôvery klienta a používania internetového bankovníctva, vyhovieť novým regulačným opatreniam alebo nahradenie starších autentizačných metód novými.

Problém, ktorý rieši táto diplomová práca je nahradenie jednej zo starších metód GRID karty výberom nového riešenia, ktoré by malo spĺňať nasledovné požiadavky:

- štandardy definované v smernici PSD2 na silnú autentifikáciu klienta,
- dostupnosť riešenia,
- spokojnosť používateľov a klientsky zážitok,
- životnosť riešenia,
- redukcia nákladov z dlhodobého hľadiska,

5.1.1 Silná autentifikácia podľa smernice PSD2

Európska banková asociácia (EBA) navrhuje regulačný technický štandard na silnú autentifikáciu klienta a bezpečnú komunikáciu známu pod menom PSD2 (Payment service directive). Jej cieľom je najmä zaistiť, že všetky elektronické platobné služby sa realizujú bezpečným spôsobom, teda technológiami, ktoré garantujú bezpečnú autentifikáciu užívateľa a znižujú maximálne možné riziko platobného podvodu. Je zaradená medzi hlavné požiadavky, ktoré by mal nový autentizačný prvok spĺňať. Bolo by maximálne neefektívne nedodržať požiadavky, ktoré táto smernica definuje z dôvodu,

že smernica vstúpi do platnosti 13. Januára 2018 pre všetkých poskytovateľov platobných služieb v Európskej únií. Od poskytovateľov platobných služieb bude vyžadovať použitie silnej autentifikácie, ak platiteľ:

- pristupuje k jeho platobnému účtu on-line,
- realizuje elektronickú platobnú transakciu,
- vykonáva akciu cez vzdialený kanál, ktorý môže implikovať riziko platobného podvodu alebo iného zneužitia.

Silnou autentifikáciou podľa článku 4 (30) smernice platobných služieb je autentifikácia:

- založená na použití dvoch alebo viacerých bezpečnostných metód, kategorizovaných ako:
    a. vedomosť (niečo, čo pozná len užívateľ t. j. statické heslo, osobné identifikačné číslo),
    b. vlastníctvo (niečo, čo užívateľ vlastní t. j. token, mobilný telefón),
    c. vrodenosť alebo inherencia (niečo, čo užívateľ je t. j. biometrický znak – odtlačok prsta),
- zaisťuje, že všetky prvky sú navzájom nezávislé jeden od druhého, tzn. niektorý z bezpečnostných prvkov nesmie ohroziť spoľahlivosť iného prvku. Ak napríklad OTP generátor je zachytený vo webovom prehliadači a druhým faktorom je PIN kód, ktorý používateľ napíše do webového prehliadaču, tak malware môže prevziať kontrolu nad OTP generátorom a keylogger môže zachytiť a následne uložiť používateľov PIN kód. Takéto riešenie nepatrí do kategórie nezávislé.
- Je navrhnutý spôsobom, ktorý chráni dôvernosť overovaných údajov. (26)

Ak napríklad obchodník alebo poskytovateľ platobných služieb zlyhal pri akceptovaní požiadavky na silnú autentifikáciu, potom tieto strany budú zodpovedné za každú neautorizovanú platbu. V prípade vykonávania platby cez vzdialený kanál bude poskytovateľ platobných služieb musieť vyžadovať:

- autentifikáciu, ktorá zahŕňa klientom špecifikovanú čiastku transakcie,
- autentifikáciu, ktorá zahŕňa špecifikovaného príjemcu transakcie. (27)

Ak banka používa ako autentizačný prvok jednorazové heslo OTP, mala by zaistiť, že doba platnosti takéhoto hesla je obmedzená na striktné nevyhnutné minimum. OTP heslo bez ďalšej doplňujúcej metódy autentifikácie je považované za nedostačujúce. Riešenia spoliehajúce sa na jediný bezpečnostný prvok, napr. token budú vylúčené. Ďalšou požiadavku tejto smernice je, že aspoň jeden z faktorov by nemal byť opakovane použiteľný alebo nejako sledovateľný. Príkladom je GRID karta, aj keď je výzva na zadanie pozície vždy rôzna, útočník je schopný zaznamenávať históriu transakcii

a tým sa naučiť všetky pozície na GRID karte. Obmedzené množstvo pozícií na GRID karte je jeden z dôvodov, prečo sú GRID karty nedostatočne bezpečné. (44)

5.1.2 Dostupnosť riešenia

Ďalšou dôležitou požiadavkou na návrh nového riešenia je práve dostupnosť. Istá skupina klientov môže žiť napríklad v zahraničí, no momentálne vlastní ako druhý faktor autentizácie len bezpečnostný prvok GRID kartu. Pri výbere nového bezpečnostného prvku, ktorý v budúcnosti nahradí GRID kartu bude veľmi dôležité zohľadniť, aby bolo toto riešenie pre klienta jednoduché na používanie. Je len ťažko predstaviteľné, že by skupina klientov žijúca v zahraničí musela osobne navštíviť pobočku pre zmenu bezpečnostného prvku. Ľahkou dostupnosťou nového riešenia sa zaistí, že ho klienti budú môcť používať aj v zahraničí.

Ďalšou dôležitou požiadavkou je dostupnosť riešenia 24 hodín denne a 7 dní v týždni bez akéhokoľvek obmedzenia. Kedykoľvek sa klient rozhodne pristúpiť do svojho internetového bankovníctva, musí byť zabezpečená neobmedzená dostupnosť a prevádzka tohto riešenia.

5.1.3 Spokojnosť klienta

Jedna z najdôležitejších častí implementácie viac-faktorovej autentizácie je hodnotenie dopadu na klientsky zážitok. V závislosti na zvolenom type metódy sa klientsky zážitok značne líši:

- niektoré riešenia môžu byť implementované bez vedomia klienta, že k nejakej zmene došlo,
- niektoré môžu požadovať klienta prejsť procesom registrácie,
- iné doplňujúce riešenia môžu od klienta vyžadovať mať daný prvok fyzicky v rukách pre prístup k jeho účtom.

Finančné inštitúcie z toho dôvodu musia nájsť také riešenie, ktoré bude mať pozitívny vplyv na pohodlie klienta. (45) Základnou požiadavkou je ponúknuť klientovi riešenie, ktoré bude zvyšovať jeho komfort a bude jednoduchú na používanie. GRID karty ponúkajú riešenie, ktoré je pre klienta vo veľa prípadoch obmedzujúce. Ak klient potrebuje pristúpiť ku svojim účtom do elektronického bankovníctva, tak musí mať fyzicky pri sebe GRID kartu. Ak si ju zabudol, resp. ju niekde stratil, alebo mu ju niekto ukradol, tak je jeho prístup do účtu v Internet bankingu nemožný. Na obnovenie resp. vydanie novej GRID karty potrebuje klient osobne navštíviť pobočku, kde mu vydajú novú kartu. Táto forma autentizácie nepredstavuje pre klienta veľké pohodlie a nezvyšuje jeho zážitok. Je preto potrebné nájsť riešenie, ktoré bude jednoduché na používanie zrýchli proces autentizácie a autorizácie.

5.1.4 Ostatné požiadavky

Medzi hlavné požiadavky určite patrí splnenie podmienok na prísnu autentifikáciu klienta. Prísna autentizácia klienta je postup založený na minimálne dvoch prvkov kategorizovaných ako poznatok, vlastníctvo a inherencia. (46) Z dôvodu celkových nákladov na nové riešenie je pre banku nevyhnutné, aby nový prvok spĺňal aspoň dve z týchto kritérií. V prípade, ak by sa jednalo o krátkodobé riešenie, banka by utratila veľké množstvo peňažných prostriedkov na implementáciu dočasného riešenie, ktoré by po pár rokoch musela nahradiť novým riešením. Implementácia nového autentizačného a autorizačného nástroja do systémov banky stojí tisíce eur. V závislosti na vybranom riešení by dodatočné náklady predstavovali distribúciu bezpečnostných predmetov na pobočky, ich úschovu a spôsob doručenia klientovi. Z tohto dôvodu je preto potrebné, aby sa pri výbere nového prvku bral veľký ohľad aj na jeho **životnosť**.

Ďalšou veľmi dôležitou požiadavkou je redukcia **nákladov** z dlhodobého hľadiska. Všeobecne platí, že fixné náklady služieb elektronického bankovníctva sú oveľa vyššie ako variabilné náklady. (9) Výnimkou nie je ani výber nového bezpečnostného prvku. Existujú dve kritické zložky celkových nákladov na vlastníctvo a to:

- obstarávacie náklady,
- prevádzkové náklady.

Pri rozhodovaní je potrebné posúdiť dva druhy nákladov. Obstarávacie náklady spolu s vynaloženými nákladmi počas celého životného cyklu riešenia, tzn. od nasadenia do prevádzky, obnovu zariadenia, riadiace náklady. Je nevyhnutné vybrať také riešenie, ktoré bude viesť k zníženiu nákladov na údržbu daného riešenia z dlhodobého hľadiska. (47)

Pri rozhodovaní o výbere vhodného bezpečnostného prvku je potrebné zobrať do úvahy aj **integráciu** riešenia do existujúcej architektúry Internet bankingu. Riešenie s kvalitnou integráciou môže ušetriť ľudské zdroje banky počas implementácie riešenia. Ušetrené zdroje potom môžu byť použité pri ďalších oblastiach rozvoja banky.

Praktická časť

6 Analýza zrušenia GRID karty

Táto kapitola sa zameriava na celkový proces zrušenia autentizačného prvku GRID karty. Na začiatok bude potrebné vysvetliť dôvody rušenia GRID kariet. S následným popisom aktuálneho stavu bezpečnostných prvkov, ktoré sú k dispozícii. Jadro analýzy bude predstavovať podrobný popis postupu smerujúci k úplnému zrušeniu tohto prvku. Postup sa bude skladať z viacerých fáz, ktorých č bude znížiť aktuálny stav GRID kariet.

6.1 Dôvod zrušenia GRID karty

Koncept silnej autentizačnej metódy nemal oficiálnu definíciu do Januára 2013, kedy bola publikovaná rozsiahla zbierka doporučení, určená na boj a ochranu proti útokom na poskytovateľov platobných služieb. Zároveň boli definované minimálne kritéria, ktoré by mál spĺňať proces silnej autentifikácie. Európska centrálna banka podčiarkla potrebu silnej autentifikácie na účely ochrany internetových platieb. Od obdobia, kedy GRID karty patrili k najrozšírenejším bezpečnostným prvkom, už prešla dlhá doba. Na základe porovnania v tabuľke nižšie môžeme prísť k záveru, že autentizačná metóda vo forme GRID kariet patrí medzi zastarané riešenia. (48)

	Aplikovaný autentizačný proces Prvá úroveň + 2. úroveň		
Minimálne kritéria	**GRID Karta**	**OTP (SMS)**	**OTP (HW TOKEN)**
Proces autentizácie prebieha použitím dvoch alebo viacerých prvkov na overenie totožnosti klienta	✓	✓	✓
Prvek bol posúdený alebo certifikovaný nezávislou treťou stranou s výsledkom, že úroveň bezpečnosti jednotlivých metód je robustná a odolná	✗	✓ Infraštruktúra ✗ Mobilné zariadenie	✓
Bezpečnostné mechanizmy nasledujú štandardy dostupné a uznané verejnosťou	✗	✓	✓
Platobný proces je inicializovaný prostredníctvom nezávislého kanála	✓	✓	✓
Prelomenie jedného z autentizačných prvkov nenaruší ochranu zvyšných prvkov	✓	✓	✓
Autentizačné kódy sa nedajú nijako napodobniť alebo odchytiť	✗	✓	✓
Nie je možné vytvoriť kópiu bezpečnostného prvku a bezpečne využiť túto kópiu	✗	✓	✓
Je zaručená dôvernosť od momentu inicializáie autentifikácie až po overenie serverom	✗	✗	✓

***Obrázok 18 Porovnanie jednotlivých bezpečnostných prvkov podľa bezpečnostných kritérií* (48)**

Na základe definovania minimálnych kritérií a porovnania, či jednotlivé prvky GRID karta, SMS autentizácia (OTP – jednorazovým heslom) a hardvérový token (OTP) spĺňajú tieto kritéria, môžeme dospieť k názoru, že GRID karty v tomto porovnaní so zvyšnými dvomi prvkami dopadli najhoršie. GRID karta nesplnila 5 z 8 definovaných minimálnych kritérií:

- bezpečnosť prvku bola posúdená alebo certifikovaná nezávislou treťou stranou,
- bezpečnostné mechanizmy nasledujú štandardy dostupné a uznávané verejnosťou,
- autentizačné kódy sa nedajú nijako napodobniť alebo odchytiť,
- nie je možné vytvoriť kópiu bezpečnostného prvku,
- je zaručená dôvernosť od momentu inicializácie autentifikácie až po overenie serverom.

Naopak GRID karty splnili len 3 kritéria, ktoré boli definované ako:

- proces autentifikácie prebieha použitím dvoch alebo viacerých prvkov overujúcich totožnosť klienta,
- platobný proces je inicializovaný prostredníctvom nezávislého kanála,
- prelomenie GRID karty nenaruší iné prvky – napr. statické heslo.

Podľa Mareka Michlíka sú GRID karty slabým článkom najmä v dôsledku neopatrného správania klientov. Viaceré banky sa mu vyhýbajú, alebo jeho použitie obmedzujú najmä preto, že neposkytuje dostatočnú ochranu pri používaní elektronického bankovníctva. (49)

Použitím špeciálnych nástrojov je možné odchytiť prístupové heslá a kódy klientov internetového bankovníctva. GRID karta má len obmedzený počet kódov, ktoré nie sú časovo nijako obmedzené, z toho dôvodu je riziko zneužitia vyššie ako pri iných prvkov. Posledným dôvodom, prečo prvok zrušiť, je redukcia prevádzkových nákladov, ktoré s jeho prevádzkou súvisia. Náklady vznikajú hneď pri tlačení tohto prvku, pri jeho distribuovaní, nevyhnutnej evidencii a skladovaní.

6.2 Aktuálny stav bezpečnostných prvkov

Pred určením presných krokov ako budeme postupovať pri rušení GRID karty, je potrebné popísať aktuálny stav jednotlivých bezpečnostných prvkov, ktoré máme k dispozícií. Bezpečnostné prvky sú pridelené klientovi banky. Identifikačným prvkom klienta pre prístup do elektronického bankovníctva je PID (náhodne vygenerovaný reťazec symbolov – prihlasovacie meno). Autentizačnou metódou na prvej úrovni je heslo. Klient si ho môže kedykoľvek zmeniť podľa svojich predstáv. Pre užívateľov internetového bankovníctva sú k dispozícií aktuálne tri bezpečnostné prvky dopĺňajúce prvú úroveň autentizácie (statické heslo):

- SMS kód (OTP) – zasielaný bankou klientovi na ním určené telefónne číslo.

- GRID karta – pridelená podľa sériového čísla, na prihlásenie klient potrebuje zadať kód vyžadovaného poľa numerickej matice.
- Hardvérový token – zariadenie založené na technológií, kedy na prihlásenie klient potrebuje zadať kód vygenerovaný týmto zariadením. (50)

6.2.1 Denné limity platobných príkazov

Klient môže odoslať zo svojich účtov platobné príkazy len v maximálnej výške limitu, ktorá je viazaná na bezpečnostný prvok, ktorým je klient prihlásený. Denné limity nie je možné meniť na žiadosť klienta, sú viazané na bezpečnostný prvok. Prevody medzi vlastnými účtami klienta sa nezapočítavajú do denného limitu viazaného na bezpečnostný prvok. Denné limity sú stanovené v závislosti na bezpečnostný prvok:

- SMS kód 50 000 Eur na prístup klienta,
- GRID karta 1 000 Eur na prístup klienta,
- HW token do výšky disponibilného zostatku na účte na prístup klienta.

Pri právnických osobách sú denné limity nastavené odlišne. Na každý bezpečnostný prvok je stanovený denný limit na 3 320 Eur na prístup klienta. Klient (právnická osoba) môže požiadať o zmenu limitu prostredníctvom osobnej žiadosti na pobočke banky. (51)

6.2.2 Stav podielu bezpečnostných prvkov

Aktuálny stav vydaných bezpečnostných prvkov v závislosti podľa podielu prístupov do elektronického bankovníctva je pred začatím procesu rušenia GRID kariet vyjadrený nižšie v tabuľke.

Bezpečnostný prvok	Počet klientov vyjadrený v percentách %
SMS kód (OTP)	76,60%
GRID karta	**7,18%**
HW token	0,13%
SMS kód (OTP) + GRID karta	**15,96%**
SMS + HW token	0,07%
SMS+GRID karta + HW token	**0,06%**
Súčet	100,00%

Tabuľka 1 Stav bezpečnostných prvkov pred procesom zrušenia GRID kariet **(52)**

Celkový percentuálny podiel klientov, ktorí majú vydanú len GRID kartu, je 7,18% z celkového počtu vydaných prístupov. Existujú aj klienti, ktorí majú vydaných aj viac autentizačných predmetov ako jeden. SMS autentizáciu a súčasne GRID kartu má vydaných približne 15,96% klientov. Najviac používaným bezpečnostným prvkom je SMS autentizácia v pomere 76,60% z celkového počtu vydaných bezpečnostných prvkov. Z vyššie zobrazených údajov v tabuľke vyplýva, že GRID kartu ako

bezpečnostný prvok (len GRID karta, GRID karta + SMS kód, GRID + SMS kód + HW token) má vydaných približne 23,20% prístupov.

Cieľom je vybrať stratégiu pre postupné rušenie bezpečnostného prvku GRID karta bez ohľadu na spôsob, či má klient vydaný aj iný bezpečnostný prvok, alebo nie. Tabuľka 2 popisuje podiel klientov s vydanou GRID kartou. Je rozdelená do dvoch skupín klientov.

Bezpečnostný prvok	Počet klientov s GRID kartou v percentách %
GRID karta	30,95%
GRID karta + iný bezpečnostný prvok	69,05%
Súčet	100,00%

***Tabuľka 2 Klienti, ktorí majú vydanú GRID* (52)**

Pre každú z týchto dvoch skupín sa postup rušenia GRID karty bude líšiť. V závislosti na bezpečnostnom prvku GRID karta budeme rozlišovať dve skupiny klientov banky:

- skupina klientov, ktorým bola vydaná len GRID karta na prístup do elektronického bankovníctva s približným počtom **30,95%** prístupov,
- skupina klientov, ktorí vlastnia kombináciu GRID karty a iného bezpečnostného prvku predstavuje približne **69,05%**.

6.3 Postup zrušenia GRID kariet

Postup rušenia bezpečnostného prvku nepatrí medzi jednoduché procesy. Podľa M. Gajcara zo spoločnosti Slovenská sporiteľňa je povinné rušenie GRID kariet kontraproduktívne, pretože môže viesť k narušeniu dôvery klientov, čo môže vyústiť k ich celkovej strate. (49) Z tohto dôvodu bude proces rušenia prvku opatrný a rozdelený na viaceré etapy. Každú z etáp si podrobne popíšeme a zhodnotíme, do akej miery prispeje a pomôže k požadovanému stavu.

6.3.1 Prvá fáza zrušenia GRID kariet

V prvej fáze zrušenia GRID kariet bude snaha banky motivovať klientov, aby prestali používať GRID kartu a prešli na SMS autentizáciu. Aktuálne je denný limit pri autorizácií platieb GRID kartou nastavený na 1000 Eur na deň. Prvým krokom na zvýšenie motivácie klienta prejsť na iný dostupný prvok bude zníženie denného limitu na 500 Eur na deň. Zmena sa bude týkať obidvoch skupín klientov, tzn. klienti s vydanou GRID kartou a klienti s vydanou kombináciu GRID karty a iného bezpečnostného prvku.

Pred rozhodnutím bolo potrebné zanalyzovať, koľko percent užívateľov elektronického bankovníctva obmedzí zníženie limitu o 500€. Tabuľka 3 vyjadruje počet užívateľov autorizujúcich platby v jednotlivých hladinách bezpečnostným prvkom GRID karta.

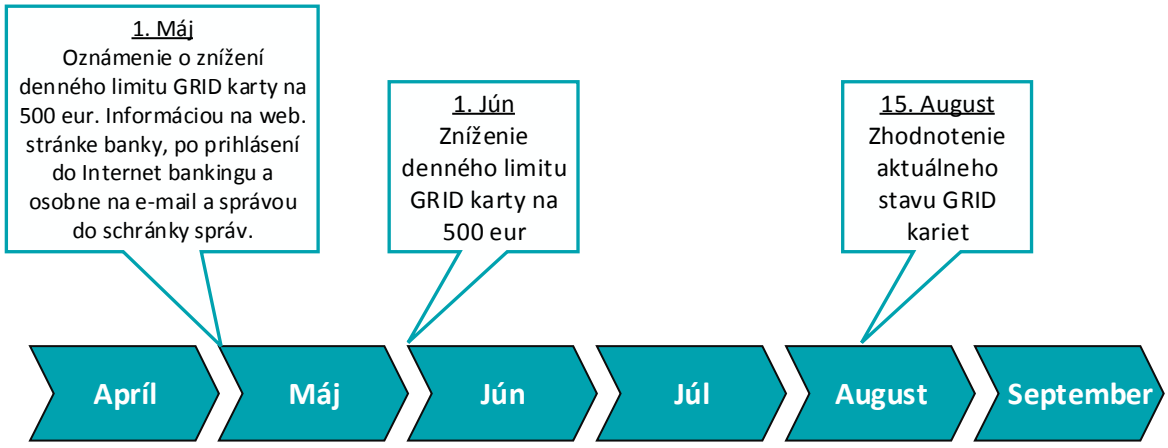
Suma v EUR	Počet klientov vyjadrený v percentách %
0-50 €	32,37%
50-100 €	21,14%
100-200 €	17,96%
200-300 €	6,63%
300-400 €	5,15%
400-500 €	4,93%
500-600 €	**2,63%**
600-700 €	**1,89%**
700-800 €	**1,62%**
800-900 €	**1,29%**
900-1000 €	**4,41%**
Súčet	100,00%

***Tabuľka 3 Počet užívateľov autorizujúcich platby v rôznych hladinách GRID kartou* (52)**

Z uvedenej tabuľky vyplýva, že zníženie limitu na 500 Eur môže mať dosah až na približne 11,83% klientov z celkového počtu užívateľov autorizujúcich platby GRID kartou. Predtým, než banka vykoná akúkoľvek zmenu týkajúcu sa elektronického bankovníctva, musí najskôr v zmysle všeobecných obchodných podmienok o tejto zmene informovať svojich klientov. Spôsoby, ktorými banka musí informovať klienta sú:

- zverejnením na svojich webových stránkach (aj z dôvodu, že niektorí klienti nemusia mať v systémoch banky vyplnenú e-mailovú adresu),
- osobná komunikácia na e-mailovú adresu klienta alebo do schránky v Internet bankingu.

Na obrázku môžeme vidieť postup zrušenia GRID karty v prvej fáze zobrazený z časového hľadiska ako k jednotlivým zmenám dochádzalo.



Obrázok 19 Prvá fáza zrušenia autentizačného prvku GRID karta (vlastné spracovanie)

Po znížení denného limitu na 500 Eur je nutné zhodnotiť, v akom rozsahu pomohla prvá fáza na znížení celkového podielu GRID kariet. Tabuľka 4 vyjadruje, ako sa zmenil počet GRID kariet po 2,5 mesiacoch od zníženia limitu na 500 Eur. Znížením limitu bola snaha motivovať klientov k zmene prvku na iný, bezpečnejší prvok a zároveň ho informovať o dostupných a bezpečnejších alternatívach autentizácie a autorizácie, ktoré sú k dispozícií.

Zníženie denného limitu prinieslo pokles GRID karty na 6,07% z celkového počtu vydaných prvkov, čo je približne 1,11% pokles oproti stavu pri dennom limitu 1000 Eur. Naopak pri SMS autentizácii bol spozorovaný nárast počtu klientov s týmto bezpečnostným prvkom na 77,49% z celkového počtu vydaných prístupov, čo je približne o 0,89% viac ako bolo pred znížením denného limitu. Čo znamená, že niektorí klienti s GRID kartou prešli na ďalší bezpečnostný prvok SMS autentizáciu.

Bezpečnostný prvok	Počet klientov vyjadrený v percentách %
SMS kód (OTP)	77,49%
GRID karta	**6,07%**
HW token	0,13%
SMS kód (OTP) + GRID karta	**16,18%**
SMS + HW token	0,07%
SMS+GRID karta + HW token	**0,06%**
Súčet	100,00%

***Tabuľka 4 Stav počtu prístupov po znížení limitu GRID kariet na 500 Eur* (52)**

6.3.2 Druhá fáza zrušenia GRID kariet

Po ukončení prvej fázy môžeme skonštatovať, že sa nepodarilo rapídne znížiť počet vydaných GRID kariet. V druhej fáze bude potrebné sa zamerať najmä na klientov, ktorí majú v systéme zadané mobilné telefónne číslo v správnom tvare a zároveň majú vydanú aj GRID kartu. Cieľom bude doplnenie možnosti zmeny bezpečnostného prvku GRID karta na SMS autentizáciu v Internet bankingu. Tabuľka 5 vyjadruje, ako sa zmenil podiel bezpečnostného prvku GRID karta. Po znížení denného limitu na tomto prvku sa počet klientov, ktorí majú len GRID kartu znížil približne o 3,75 %. Z uvedeného vyplýva, že si GRID kartu zrušili a dali si vydať iný bezpečnostný prvok. Hlavnou úlohou v druhej fáze bude znížiť počet klientov s len vydanou GRID kartou v oveľa väčšom rozsahu.

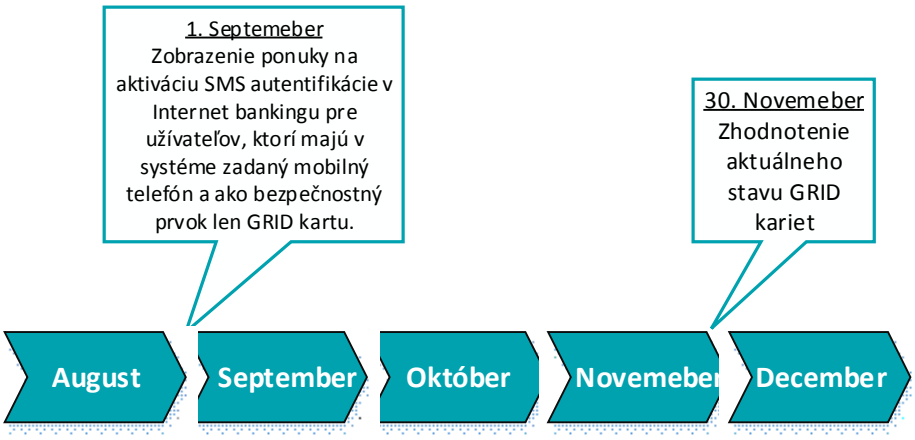
Bezpečnostný prvok	Počet klientov s GRID kartou v percentách %
GRID karta	27,20%
GRID karta + iný bezpečnostný prvok	72,80%
Súčet	100,00%

Tabuľka 5 Aktuálny stav klientov po znížení denného limitu, vlastniacich GRID kartu

Táto fáza popisuje riešenie pre klientov, ktorí sa prihlásia do Internet bankingu GRID kartou a zároveň majú v systéme banky nastavené mobilné telefónne číslo v správnom formáte (slovenský mobilný operátor). Takýmto klientom sa hneď po prihlásení do Internet bankingu zobrazí upozornenie, ktoré bude klienta vyzývať na nastavenie SMS autentizácie. Po kliknutí na upozornenie klienta okamžite presmeruje do sekcie SMS autentizácia, v ktorej budú zobrazené nasledovné informácie:

- informácie o procese zmeny prvku,
- telefónne číslo klienta, na ktoré bude kód SMS prichádzať. Toto číslo sa bude doťahovať zo systému banky. V prípade, ak klient požaduje zasielať SMS autentizáciu na iné mobilné telefónne číslo bude pridaná informácia o nutnosti osobne navštíviť pobočku z dôvodu aktualizácie osobných údajov klienta.
- odkaz na všeobecné obchodné podmienky, s ktorými musí byť pri zmene klient oboznámený a musí s nimi vyjadriť súhlas.

Po prečítaní uvedených informácií a všeobecných obchodných podmienok musí klient vyjadriť súhlas potvrdením zmeny prvku. Klientovi sa po potvrdení zobrazí požiadavka na zadanie niektorej z pozícií na GRID karte. Po úspešnom overení totožnosti príde klientovi ešte jedna požiadavka na overenie totožnosti vo forme SMS kódu, ktorý je klientovi zaslaný na pridané mobilné telefónne číslo pre zriadenú SMS autentizáciu. Po zadaní správneho SMS kódu sa od klienta pri každom ďalšom overovaní totožnosti pri prihlasovaní do Internet bankingu a autorizácií platieb bude automaticky vyžadovať len SMS kód (OTP). Klient bude o úspešnom vykonaní zmeny informovaný správou do schránky správ v Internet bankingu. Po zavedení možnosti zmeny bezpečnostného prvku v Internet bankingu je potrebné po určitom časovom období zhodnotiť, aký dopad mala ponuka zmeny bezpečnostného prvku na celkový podiel vydaných GRID kariet. Na obrázku 20 môžeme vidieť postup zrušenia GRID karty v druhej fáze zobrazený z časového hľadiska, ako k jednotlivým zmenám dochádzalo.



Obrázok 20 Druhá fáza zrušenia autentizačného prvku GRID karta (vlastné spracovanie)

Pred zobrazením ponuky na zmenu prvku bol podiel klientov, ktorí majú vydanú len GRID kartu, približne 6,07% z celkového podielu klientov (aj iné bezpečnostné prvky). Z uvedeného vyplýva, že sa mohla ponuka na zmenu bezpečnostného prvku zobraziť až 6,07% klientov s GRID kartou. Pri analýze však treba brať do úvahy aj to, že niektorí klienti nemusia mať vyplnené v systéme mobilné telefónne číslo, alebo sa nemuseli za zvolené obdobie od 1. Septembra do 30. Novembra prihlásiť do Internet bankingu. Podiel klientov, ktorí mali vydanú len GRID kartu a zároveň správne vyplnené mobilné telefónne číslo, bol 95% z celkového podielu klientov len s GRID kartou. Ponuka na zmenu autentizácie preto mohla byť zobrazená približne 5,76% klientov z celkového počtu všetkých prvkov. Z uvedeného podielu sa za zvolené obdobie 20% klientov vôbec neprihlásilo do Internet bankingu. Ponuka na zmenu autentizácie bola zobrazená až 4,61% klientov z celkového podielu klientov.

	Podiel klientov vyjadrený v percentách %
Zmena autentifikácie po zobrazení	**42%**
1. upozornenie	51%
2. upozornenie	19%
3. - 6. upozornenie	14%
7. - 10. upozornenie	9%
11 a viac upozornení	7%
Súčet	100%
Nezmenili autentifikáciu po zobrazení	**58%**
1. upozornenie	5%
2. upozornenie	3%
3. - 6. upozornenie	17%
7. - 10. upozornenie	22%
11 a viac upozornení	53%
Súčet	100,00%

***Tabuľka 6 Klienti, ktorí si zmenili prvok po zobrazení ponuky v Internet bankingu* (52)**

Z tabuľky vyplýva, že si GRID kartu za SMS autentizáciu prostredníctvom Internet bankingu zmenilo približne 42% klientov, ktorým sa ponuka zobrazila. Tabuľka detailne popisuje efektivitu zobrazovania upozornenia na zmenu autentizačného prvku, tzn. kedy a ako klient zareagoval po zobrazení upozornenia v Internet bankingu. Zo 42% klientov, ktorí si zmenili bezpečnostný prvok, súhlasilo najviac klientov so zmenou hneď po prvom zobrazení upozornenia. Až 51% užívateľov súhlasilo so zmenou hneď po prvom zobrazení upozornenia.

Naopak až 58% klientov, ktorým sa ponuka na zmenu prvku zobrazila nereagovalo vôbec. SMS autentizáciu si nezmenilo ani 53% klientov (z celkového počtu klientov, ktorí si prvok nezmenili), ktorým sa hláška zobrazila dokonca až 11-krát a viac. Z toho vyplýva, že najviac efektívne bolo práve prvé upozornenie a s každým ďalším upozornením sa efektivita zmeny znižovala. Možnosťou zmeny

prvku v prostredí elektronického bankovníctva bola snaha opäť motivovať klientov ku zmene prvku bez radikálnejšieho zásahu zo strany banky.

Bezpečnostný prvok	Počet klientov vyjadrený v percentách %
SMS kód (OTP)	79,60%
GRID karta	**4,13%**
HW token	0,13%
SMS kód (OTP) + GRID karta	**16,01%**
SMS + HW token	0,06%
SMS+GRID karta + HW token	**0,07%**
Súčet	100,00%

***Tabuľka 7 Stav prístupov po zobrazení ponuky na zmenu bezpečnostného prvku* (52)**

V tabuľke je zobrazený aktuálny stav po ukončení druhej fázy rušenia bezpečnostného prvku GRID karta. Zobrazenie ponuky na aktiváciu SMS autentizácie v Internet bankingu znížilo celkový podiel bezpečnostného prvku len GRID karta o približne 1,94%. Naopak nárast používania bezpečnostného prvku zaznamenala SMS autentizácia približne o 2,11%. Za rast podielu môže najmä zmena bezpečnostného prvku GRID karta na SMS a aj to, že novým klientom sa primárne vydáva ako nový prvok SMS autentizácia.

6.3.3 Tretia fáza zrušenia GRID karty

Po vyhodnotení druhej fázy zrušenia GRID karty môžeme konštatovať, že sa nám tento prvok podarilo zredukovať o skoro 42% oproti pôvodnému stavu pred začatím prvej fázy. Predchádzajúce fázy rušenia GRID karty sa snažili namotivovať klientov, aby si sami zmenili bezpečnostný prvok bez nejakých výrazných obmedzení. Druhá fáza sa týkala najmä klientov, ktorí vlastnili len GRID kartu. Tretia fáza sa bude zameriavať najmä na klientov, ktorí majú aj iný bezpečnostný predmet a bude rozdelená na dva postupy rušenia:

- obmedzenie prihlasovania do elektronického bankovníctva (exspirovaním GRID karty) klientom, ktorí sa neprihlásili dlhšie ako 12 mesiacov,
- exspirácia GRID kariet klientom, ktorí majú aj iný bezpečnostný prvok.

Prvá časť bude z pohľadu klienta pravdepodobne viac citlivá. Jej účinok pocítia najmä tí klienti, ktorým bola vydaná len GRID karta a svoje internetové bankovníctvo nepoužili dlhšie ako 12 mesiacov. Banka im automaticky po určenom dátume obmedzí prihlasovanie do elektronického bankovníctva. Počet klientov s vydanom GRID kartou, ktorí sa neprihlásili do Internet bankingu za posledných 12 mesiacov, tvorí približne 20,62% celkového počtu klientov s týmto prvkom. Takýmto postupom by sa počet klientov s vydanou GRID kartou mohol znížiť až na 3,27%. Ak sa klient bude chcieť prihlásiť do Internet bankingu, bude musieť navštíviť pobočku, ktorá mu na požiadanie vydá

nový bezpečnostný prvok. Podobným spôsobom postupovala aj Tatra banka, ktorá takýmto spôsobom menila spôsob prihlasovania. (52)

Druhým postupom zrušenia bude nastavenie exspirácie klientom, ktorí majú aj iný bezpečnostný prvok. Podiel klientov, ktorým bude v tejto fáze nastavená exspirácia je približne 16,08% z celkového počtu klientov. Čo znamená, že po uplynutí dátumu exspirácie sa zruší veľký podiel vydaných GRID kariet. O nastavení exspirácie bezpečnostného prvku musia byť klienti informovaní vopred. Povinná lehota zverejnenia všetkých zmien, týkajúcich sa bezpečnostných prvkov, musí byť uvedená vo všeobecných obchodných podmienkach. Informácie o exspirácií budú smerované len na tých klientov, ktorí vlastnia kombináciu GRID karty a iného bezpečnostného prvku. Existujú rôzne spôsoby, ako informovať klienta o exspirácií GRID kariet:

- zverejnením na svojich webových stránkach,
- osobná komunikácia na e-mailovú adresu klienta, alebo do schránky správ v Internet bankingu,
- oznam, ktorý informuje klienta o exspirácií GRID okamžite po prihlásení do Internet bankingu.

Po uplynutí určeného dátumu exspirácie by sa mal používateľov GRID kariet výrazne zredukovať. Ak vychádzame z posledného aktuálneho stavu po aplikovaní druhej fázy, exspiráciou GRID kariet by sa jej počet mal znížiť o približne 16,08% klientov, ktorí ju mali vydanú.

6.3.4 Štvrtá fáza zrušenia GRID karty

Štvrtá fáza by mala byť zároveň aj poslednou fázou rušenia bezpečnostného prvku. V tejto fáze by sa malo nastaviť úplné zrušenie GRID kariet. Tu bude potrebné rovnakým spôsobom ako v predchádzajúcej fáze informovať klienta o exspirácií GRID kariet:

- zverejnením na svojich webových stránkach,
- osobná komunikácia na e-mailovú adresu klienta alebo do schránky správ v Internet bankingu,
- oznam, ktorý informuje klienta o exspirácií GRID okamžite po prihlásení do Internet bankingu.

Toto riešenie bude patriť medzi agresívnejšie spôsoby rušenia bezpečnostného prvku, keďže klienti nebudú mať k dispozícií žiadny alternatívny prvok, ktorým by sa prihlásili do elektronického bankovníctva. Pre vydanie nového bezpečnostného prvku budú musieť požiadať osobne na pobočke banky. Zrušením sa však zredukuje zvyšný počet vydaných GRID kariet na celkový počet 0 aktívnych GRID kariet.

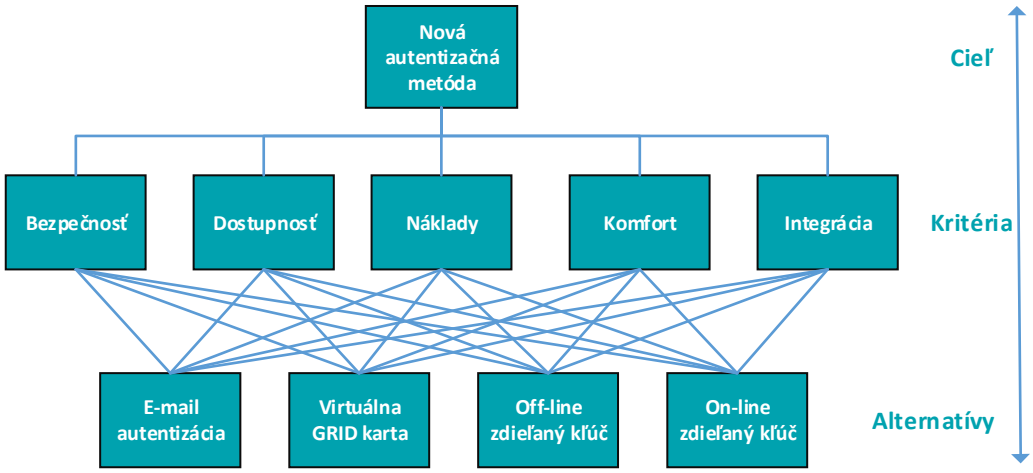
Existujú viaceré spôsoby ako môže banka pristúpiť k procesu rušenia bezpečnostného prvku, nesmie však zabudnúť na to, že bezpečnosť patrí medzi najcitlivejšie potreby klienta. Zvolením agresívnejšieho postupu rušenia GRID kariet by banka mohla prísť o viacero klientov. Je preto potrebné o každej zmene vopred informovať klienta a dať mu možnosť si vybrať z viacerých možností.

7 Výber autentizačného prvku

Rozhodovanie je proces identifikácie a výberu alternatív založený na hodnotách a preferenciách rozhodujúceho. Rozhodovanie je proces, pri ktorom dochádza k dostatočnému zníženiu neurčitosti a neistoty vzhľadom k dostupným alternatívam a rozumným výberom z nich. (53) Rozhodovací model zahŕňa rozhodovací proces vytvorením samostatného kritéria alebo kombináciou viacerých alternatív. Rozhodovacie modely sa rozdeľujú na dva typy rozhodovacích metód:

- jedno kriteriálne rozhodovanie,
- viac kriteriálne rozhodovanie.

V našom konkrétnom prípade si budeme vyberať z viacerých alternatív a celkový rozhodovací proces bude záležať na viacerých kritériách. Cieľom rozhodovania bude vybrať doplňujúcu autentizačnú metódu pre prihlasovanie do elektronického bankovníctva. Výstup rozhodovania nezávisí len od jedného kritéria, ale rovnako závisí od všetkých určených kritérií. Výber alternatív je navyše závislý od toho, ako dôležité je dané kritérium. V tejto práci sa bude proces rozhodovania spoliehať na metódu viac kriteriálneho rozhodovania pomocou bodovacej metódy. (54)



Obrázok 21 Proces rozhodovania (vlastné spracovanie)

Rozhodovanie je proces výberu jednej alternatívy z viacerých nastavených alternatív systematickým a logickým spôsobom. Proces rozhodovania pozostáva z nasledovných krokov:

- definovanie rozhodovacieho problému,
- výber a popis jednotlivých kritérií,
- identifikovanie jednotlivých alternatív,
- priradenie dôležitosti pomocou váh ku každému kritériu,
- ohodnotenie kritérií pre každú alternatívu,

- nastavenie rozhodovacích pravidiel,
- hodnotenie zvolených alternatív na základe stanovených kritérií,
- výber najlepšieho riešenia.

7.1 Definovanie rozhodovacieho problému

Pred vykonaním každého rozhodnutia je nevyhnutné sa dokonale oboznámiť s rozhodovacím problémom. Identifikácia a pochopenie problému sú základom pred vykonaním nejakého rozhodnutia. V tomto procese je potrebné správne identifikovať zdroje príčiny problému. (53)

Na základe postupného rušenia bezpečnostného prvku GRID karta je hlavným cieľom diplomovej práce výber autentizačného prvku pri prihlasovaní do elektronického bankovníctva na základe viac-kriteriálneho porovnania z vybraných autentizačných metód. Zhodnotenie dosiahnutého cieľa na základe porovnania a ďalšie závery budú uvedené na konci tejto kapitoly. Pred výberom nového riešenia viac-faktorovej autentizácie je potrebné sa oboznámiť s viacerými dostupnými metódami. Jasným pochopením a podrobnou analýzou rôznych typov dostupných riešení bude rozhodovanie o výbere doplňujúceho prvku oveľa jednoduchšie. Najmä kvôli pochopeniu hlavných znakov každej formy autentizácie. Rovnako dôležité je určenie správnych kritérií, na základe ktorých budeme posudzovať dané alternatívne riešenia. Jednotlivé kritéria budú popísané samostatne v ďalšej kapitole.

7.2 Výber a popis jednotlivých kritérií

Stanovené kritéria, na základe ktorých budeme rozhodovať medzi viacerými alternatívnymi riešeniami, musia byť založené na určenom cieli práce. Rozhodovací problém obsahujúci viacero hodnotiacich kritérií je obzvlášť nápomocný pri výbere najlepšej alternatívy. Ideálny stav je výber zmysluplných kritérií, ktoré nebudú zbytočné a nepotrebné. (53)

Autor diplomovej práce pracuje ako produktový manažér pre elektronického bankovníctvo približne štvrte roka. Na základe získaných skúseností má už určitý prehľad o možných kritériách, ktoré sa pri jednotlivých metódach dajú posudzovať. Kritéria a ich bodové ohodnotenie boli konzultované riaditeľom odboru elektronického bankovníctva. Pri výbere správnych kritérií je potrebné brať v úvahu, aby bolo čo najjednoduchšie porovnať rozličné vlastnosti a princípy zvolených autentizačných metód. Na záverečné hodnotenie a porovnanie rôznych parametrov jednotlivých metód budú použité nasledujúce kritéria:

- bezpečnosť,
- dostupnosť,
- náklady,

- komfort (jednoduchosť použitia),
- integrácia.

Prvým a najdôležitejším kritériom je **bezpečnosť**. Finančné inštitúcie musia viac chrániť seba a najmä svojich klientov pri pokračujúcich útokoch a krádeži dát. Pri používaní elektronického bankovníctva musí banka zaistiť svojim klientom pocit bezpečia. Autentizačná metóda by mala spĺňať kritéria na silný autentifikačný prvok definované smernicou platobných služieb PSD2, ktorá vstúpi do platnosti začiatkom roka 2017. Zároveň by mala spĺňať minimálne kritéria, ktoré boli spomenuté v kapitole 6.1:

- autentizácia prebieha použitím dvoch alebo viacerých metód na overenie totožnosti klienta,
- bezpečnostné mechanizmy spĺňajú štandardy dostupné a uznávané verejnosťou,
- autentizačné kódy sa nedajú nijako napodobniť alebo odchytiť,
- nie je možné vytvoriť kópiu bezpečnostného prvku,
- je zaručená dôvernosť od momentu inicializácie autentifikácie až po overenie serverom,
- platobný proces je inicializovaný prostredníctvom nezávislého kanála,
- prelomenie metódy nenaruší iné prvky.

Dostupnosť vybranej autentizačnej metódy pre každý segment klientov v banke. Je potrebné zabezpečiť, aby bol nový prvok ľahko dostupný pre všetkých klientov. Je ťažko predstaviteľné, že by z dôvodu potreby vydania novej metódy, museli tisícky klientov osobne navštíviť pobočku banky. Klient bude musieť pre vydanie novej metódy vyjadriť súhlas pôvodným bezpečnostným prvkom. Inak bude musieť pre zmenu prvku osobne navštíviť pobočku. Ďalšou podstatnou časťou kritéria, ktorú musí spĺňať nový bezpečnostný prvok, je nevyhnutnosť 24 hodinovej dostupnosti riešenia 7 dní v týždni.

Celkové náklady na používanie autentizačnej metódy a ďalšie potrebné investície. Pri rozhodovaní bude potrebné posúdiť obe formy **nákladov** jak obstarávacie, tak aj náklady na prevádzku a údržbu, riadiace náklady a náklady na obnovu.

Ďalším veľmi dôležitým kritériom zohľadneným pri výbere najlepšej varianty je **komfort** riešenia. Toto kritérium obsahuje súhrn niekoľkých vlastností, ovplyvňujúcich komfort pri používaní vybranej metódy. Jednou z týchto vlastností je jednoduchosť používania bezpečnostného prvku, tzn. z koľkých krokov pozostáva autentizačný proces. Užívateľ by mal pri prvom kontakte vedieť intuitívne pracovať s vybraným bezpečnostným prvkom. Pri posudzovaní bude dôležitá aj rýchlosť riešenia, za akú dobu systém správne vykoná požiadavku na autentifikáciu.

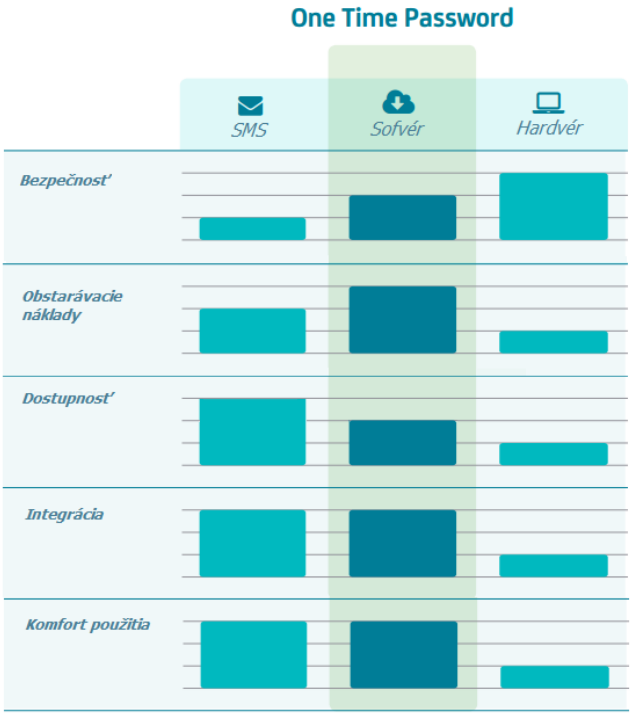
Pri **integrácií** sa bude posudzovať ako ľahko môže byť dané riešenie integrované do existujúcich systémov banky.

7.3 Identifikácia vybraných alternatív autentizácie

V tejto kapitole sa budeme zaoberať popisom vybraných autentizačných metód. Nebudeme posudzovať všetky existujúce alternatívy, ale len tie, ktoré sú z hľadiska banky najdostupnejšie a v súčasnosti patria medzi najpoužívanejšie metódy. Pred podrobnou analýzou každej varianty je potreba určiť účel, na ktorý bude slúžiť vybraný autentizačný predmet:

- prihlásenie do elektronického bankovníctva,
- autorizácia platobných príkazov (potvrdenie transakcií v Internet bankingu).

Narastajúci počet mobilných zariadení je nezastaviteľný v osobnom a profesijnom prostredí. Mobilné aplikácie menia spôsoby biznisu, pretože ponúkajú okamžitý prístup užívateľov k službám. S okamžitým prístupom rastie aj komfort pre klienta. V porovnaní s inými OTP riešeniami, token vo forme softvéru patrí medzi alternatívy s najlepším pomerom nákladov a výnosov. Z dlhodobého hľadiska nepredstavuje pre banku také náklady ako napr. SMS notifikácia, za ktorú banka platí poskytovateľovi telekomunikačných služieb dohodnutú sumu za jednu SMS. V porovnaní s hardvérovými riešeniami sú zasa zvýšené náklady na správu a údržbu týchto zariadení. Softvérové riešenia spĺňajú požiadavky definované Európskou centrálnou bankou. Proces implementácie je rýchly, v dôsledku eliminácie potreby distribuovať fyzické bezpečnostné prvky – tokeny. Obrázok nižšie zobrazuje porovnanie jednotlivých metód podľa stanovených kritérií založených na OTP riešení.

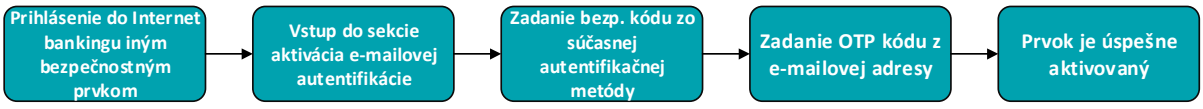


Obrázok 22 Porovnanie jednotlivých OTP metód podľa kritérií (vlastné spracovanie) **(48)**

7.3.1 E-mailová autentizácia

E-mailová autentizácia je metóda fungujúca na spôsobe overovania identity užívateľa a autorizácie transakcií zaslaným jednorazovým kódom OTP zaslaným na e-mailovú adresu klienta. Tento spôsob autentizácie bude fungovať na podobnom princípe ako funguje SMS autentizácia. Metóda by bola využívaná ako doplňujúca možnosť viac-úrovňovej autentizácie. Klient na vykonanie úspešnej autentifikácie alebo autorizácie potrebuje aktívny prístup na Internet, pomocou ktorého sa prihlási do e-mailovej adresy svojho poskytovateľa služieb elektronickej pošty. Na e-mailovú adresu zadanú v systéme banky mu príde e-mail, obsahujúci 6-miestny jednorazový OTP kód s obmedzenou dobou platnosti 5 minút.

Implementácia tohto spôsobu autentizácie je pre užívateľov pomerne jednoduchá. Na používanie je potrebné mať v systéme zadanú e-mailovú adresu. Existujú dve možnosti: buď má klient zadanú e-mailovú adresu v systémoch banky alebo nemá. Pre aktiváciu tejto formy autentizácie potrebuje klient zadať 6-miestny OTP kód, ktorý bude zaslaný klientovi na zadanú e-mailovú adresu, čím sa overí pravosť adresy a totožnosť klienta. Ak klient nemá zadanú e-mailovú adresu alebo ak nemá žiadnu inú formu autentizácie potrebuje pre aktiváciu e-mailovej autentizácie osobne navštíviť pobočku banky, kde mu bude priamo aktivovaný tento bezpečnostný prvok. Ak vlastní iný bezpečnostný prvok a zároveň má v systéme zadanú e-mailovú adresu, klientovi sa zobrazí ponuka na aktiváciu novej metódy v Internet bankingu. V internet bankingu sa ponuka zobrazí v sekcii Nastavenia/Aktivácia e-mailovej autentizácie. Aktivácia cez Internet bankingu bude dvoj kroková. V prvom kroku bude musieť klient zadať bezpečnostný kód z prvku, ktorý už vlastní. Zadanie bezpečnostného kódu nahradzuje klientov podpis pri aktivácií novej metódy. V druhom kroku overujúcom správnosť zadanej e-mailovej adresy bude musieť klient zadať OTP kód z e-mailovej adresy. Po úspešnom splnení týchto dvoch krokov (overení totožnosti klienta) sa e-mailová adresa zosynchronizuje so serverom banky a následne je e-mailová autentizácia aktívna. Postup aktivácie tohto prvku je popísaný na obrázku pod textom:

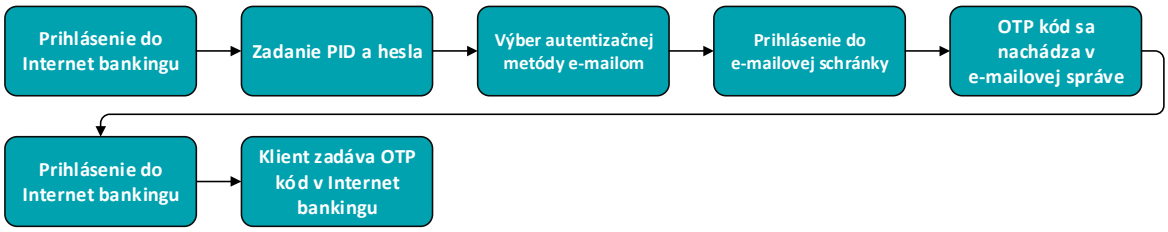


Obrázok 23 Aktivácia e-mailovej autentizácie, ak má klient aj iný bezpečnostný prvok

Po úspešnej aktivácii bude prihlasovanie do Internet bankingu týmto prvkom vyzerať nasledovne:

1. klient sa prihlasuje do Internet bankingu osobným identifikačným číslom a heslom,
2. vyberá si formu autentizácie e-mailom (OTP kód),
3. klient sa prihlasuje do svojej e-mailovej schránky,

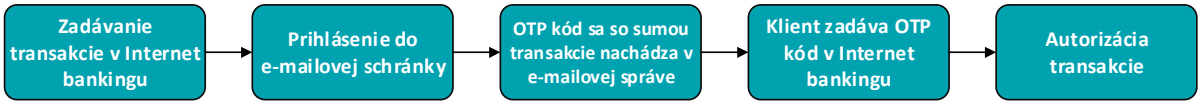
4. klientovi sa zobrazí e-mailová správa s vygenerovaným OTP kódom,
5. klient prepisuje vygenerovaný kód do Internet bankingu,
6. klient je prihlásený.



Obrázok 24 E-mailová autentizácia (OTP kódom)

Autorizácia transakcií funguje na podobnom princípe ako autentizácia a prebieha nasledovným spôsobom:

1. klient je prihlásený do Internet bankingu – autentizácia prebehla úspešne,
2. klient zadáva transakciu v prostredí Internet bankingu,
3. klient sa prihlasuje do svojej e-mailovej schránky,
4. klientovi sa zobrazí e-mailová správa so sumou transakcie a vygenerovaným OTP kódom,
5. klient prepisuje vygenerovaný kód do Internet bankingu,
6. príkaz bol úspešne autorizovaný.



Obrázok 25 Autorizácia transakcie e-mailom (OTP kódom)

7.3.2 Virtuálna GRID karta

Virtuálna GRID karta je metóda umožňujúca končenému užívateľovi generovať jednorazové heslo (OTP) prostredníctvom softvérovej aplikácie v mobilnom telefóne. Spôsob riešenia transformuje virtuálnu GRID kartu do mobilnej aplikácie. Virtuálna GRID karta obsahuje limitovaný počet šesť miestnych kódov v celkovom počte 999999, ktoré sú vyžadované pri autentizácii a autorizácií platieb. Limitovaný počet možných bezpečnostných kódov znamená, že náhodne vyžadovaná pozícia/bezpečnostný kód sa môže opakovať. Autentizácia virtuálnou GRID kartou ponúka nákladovo nezaťažujúci spôsob riešenia.

Pred prvým použitím mobilnej aplikácie (tokenu) je potrebné si ju najskôr nainštalovať a aktivovať. Po rýchlej inštalácií sa klientovi zobrazí ponuka na zadanie osobného identifikačného čísla PID, ktoré

slúži na prihlasovanie do Internet bankingu. Zároveň bude musieť klient zadať bezpečnostný kód, ktorý jednoznačne identifikuje virtuálnu GRID kartu. Klient získa bezpečnostný kód osobne na pobočke banky, alebo ak vlastní aj iný bezpečnostný prvok, tak sa mu ponuka na aktiváciu zobrazí v Internet bankingu, konkrétne v sekcii Nastavenia/Aktivácia mobilného tokenu. Bezpečnostný kód bude v tejto sekcii dostupný aj vo forme QR kódu a užívateľ ho môže skenovať priamo v aplikácií mobilného tokenu (Virtuálna GRID karta). Po úspešnom overení totožnosti klienta zadaním osobného identifikačného čísla PID a bezpečnostného kódu, si klient vytvorí vlastné PIN číslo, ktorým sa do aplikácie s virtuálnou GRID kartou bude v budúcnosti prihlasovať.

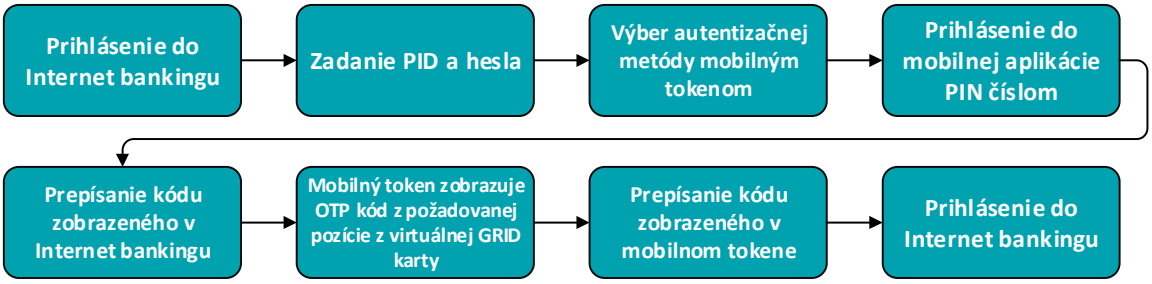
Po vytvorení čísla PIN sa zo servera banky stiahnu do aplikácie prostredníctvom Internetu (zabezpečeným protokolom SSL) kombinácie vygenerovaných pozícií a kódov, a budú uložené v šifrovanej podobe. Následne je mobilná aplikácia aktívna a pripravená na použite. Postup aktivácie virtuálnej GRID karty popíšeme v nasledovnom scenári:

1. inštalácia mobilnej aplikácie,
2. registrácia virtuálnej GRID karty prostredníctvom osobného identifikačného čísla a bezpečnostného kódu osobne získaného na pobočke banky alebo prostredníctvom Internet bankingu (numerickým kódom alebo QR kódom),
3. klient si vytvára PIN číslo pre ďalšie prihlasovanie do aplikácie,
4. klient je prihlásený do mobilnej aplikácie (tokenu),
5. aplikácia je úspešne aktivovaná.

Obrázok 26 Aktivácia mobilnej aplikácie virtuálnej GRID karty

Autentizácia klienta virtuálnou GRID kartou pri prihlasovaní do Internet bankingu prebieha nasledovne:

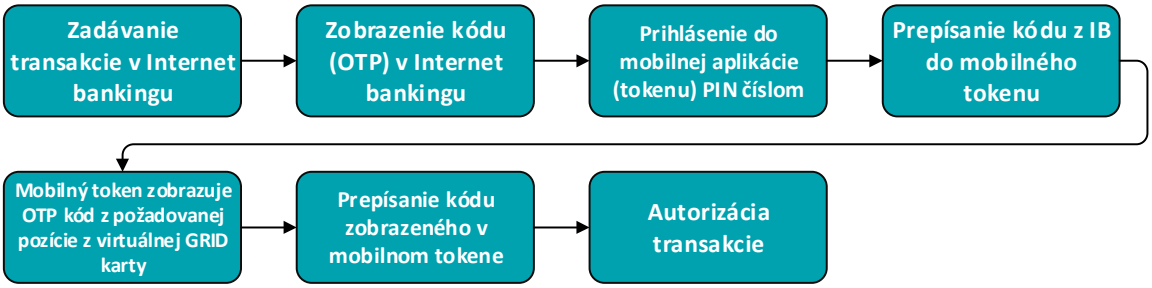
1. klient sa prihlasuje do Internet bankingu osobným identifikačným číslom a heslom,
2. vyberá si formu autentizácie mobilným tokenom (virtuálna GRID karta),
3. klient je vyzvaný na zadanie kódu (OTP) v numerickom tvare z mobilného tokenu,
4. klient sa prihlasuje do mobilného tokenu nastaveným PIN číslom,
5. prepisovanie pozície kódu (OTP) zobrazeného v Internet bankingu,
6. aplikácia zobrazuje vygenerovaný kód (OTP) z vyžadovanej pozície na virtuálnej GRID karte,
7. klient zadáva vygenerovaný kód do Internet bankingu,
8. klient je prihlásený.



Obrázok 27 Autentizácia virtuálnou GRID kartou (mobilným tokenom)

Autorizácia transakcie funguje na podobnom princípe, po úspešnom prihlásení z pohľadu klienta prebieha nasledovne:

1. klient je prihlásený do Internet bankingu – ak autentizácia prebehla úspešne,
2. klient zadáva transakciu v prostredí Internet bankingu,
3. Internet banking zobrazuje požadovanú pozíciu v numerickom tvare (OTP kód),
4. klient sa prihlasuje do mobilného tokenu nastaveným PIN číslom,
5. prepisovanie kódu (OTP) zobrazeného v Internet bankingu,
6. aplikácia zobrazuje vygenerovaný kód (OTP) z požadovanej pozície na virtuálnej GRID karte,
7. klient zadáva vygenerovaný kód do Internet bankingu,
8. príkaz bol úspešne autorizovaný.



Obrázok 28 Autorizácia transakcie virtuálnou GRID kartou (mobilným tokenom)

7.3.3 Zdieľaný kľúč (Off-line spôsob autentizácie)

Off-line zdieľaný kľúč je inovatívna metóda, založená na spôsobe overovania identity užívateľa a autorizácie transakcií QR kódom prostredníctvom mobilnej aplikácie v telefóne. Riešenie umožňuje efektívne čeliť zvýšenému množstvu sofistikovaných útokov ako Man in the Middle alebo Trojan. Aplikácia poskytuje optimálnu kombináciu riešení s pozitívnym vplyvom na správanie klienta s cieľom:

- zvýšiť komfort klienta pri autentizácii,
- zvýšiť bezpečnosť internetového bankovníctva,
- znížiť prevádzkové náklady.

Riešenie zvyšuje bezpečnosť najmä tým, že užívateľ musí potvrdiť (podpísať) vytvoreným PIN číslom výzvu na autentizáciu alebo autorizovanú transakciu. Off-line zdieľaný kľúč umožňuje klientovi autentizáciu a autorizáciu platieb kedykoľvek a z akéhokoľvek miesta.

Na používanie tejto metódy autentifikácie potrebuje mať klient nainštalovanú a aktivovanú mobilnú aplikáciu. Po rýchlej inštalácií sa klientovi zobrazí ponuka na zadanie osobného identifikačného čísla PID, ktoré slúži na prihlasovanie do Internet bankingu. Zároveň bude musieť klient zadať bezpečnostný kód, ktorý ho jednoznačne identifikuje na off-line zdieľaný kľúč. Tento bezpečnostný kód získa osobne na pobočke banky, alebo ak vlastní aj iný bezpečnostný prvok, tak sa mu zobrazí ponuka na aktiváciu nového bezpečnostného prvku v Internet bankingu. V internet bankingu sa ponuka zobrazí v sekcii Nastavenia/Aktivácia mobilného tokenu. Bezpečnostný kód bude v tejto sekcii dostupný aj vo forme QR kódu a užívateľ ho môže skenovať priamo v aplikácií mobilného tokenu (Off-line zdieľaný kľúč). Po úspešnom overení totožnosti klienta zadaním osobného identifikačného čísla PID a bezpečnostného kódu v mobilnej aplikácií si klient vytvorí PIN číslo, ktorým sa do aplikácie s mobilným tokenom v budúcnosti môže prihlasovať.

Po vytvorení PIN čísla sa aplikácia zosynchronizuje so serverom banky prostredníctvom internetu (zabezpečeným protokolom SSL), aby v budúcnosti vedela načítať vygenerované QR kódy Internet bankingom. Následne je mobilná aplikácia aktívna a pripravená na použite. Postup, ako si aktivovať mobilný token, je popísaný v nasledovnom scenári:

1. inštalácia mobilnej aplikácie,
2. aktivácia off-line zdieľaného kľúča prostredníctvom osobného identifikačného čísla a bezpečnostného kódu osobne získaného na pobočke banky alebo prostredníctvom Internet bankingu (numerickým kódom alebo QR kódom),
3. klient si vytvára PIN číslo pre ďalšie prihlasovanie,
4. Klient je prihlásený do mobilnej aplikácie (tokenu),
5. Aplikácia je úspešne aktivovaná.

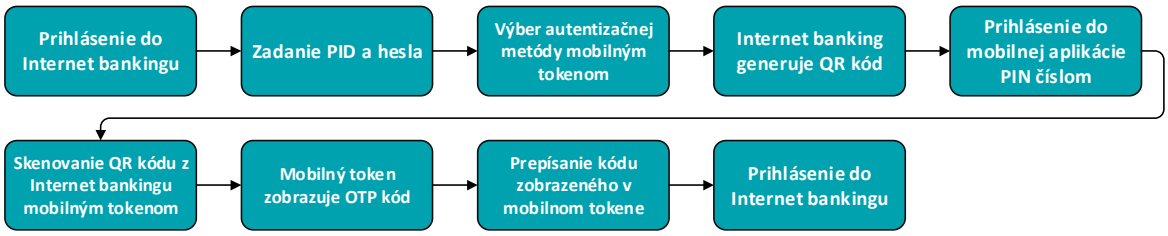
Obrázok 29 Aktivácia mobilnej aplikácie, riešenie off-line zdieľaný kľúč

Riešenie funguje na základe zobrazenia jedinečnej vizuálnej výzvy QR kódu, ktorý sa v meniteľnej forme zobrazí klientovi na obrazovke zariadenia, ktorým pristupuje do Internet bankingu. Klient musí použiť kameru na jeho mobilnom telefóne, ktorou zachytí tento QR kód (kryptogram) na obrazovke zariadenia, z ktorého pristupuje do Internet bankingu. Po zachytení QR kódu kamerou na mobilnom

telefóne dochádzka k okamžitému dekódovaniu zobrazeného QR kódu a mobilná aplikácia zobrazuje bezpečnostný kód s obmedzenou dobou platnosti, ktorý klient zadáva pri prihlasovaní do Internet bankingu.

Autentizácia klienta off-line zdieľaným kľúčom pri prihlasovaní do Internet bankingu prebieha nasledovne:

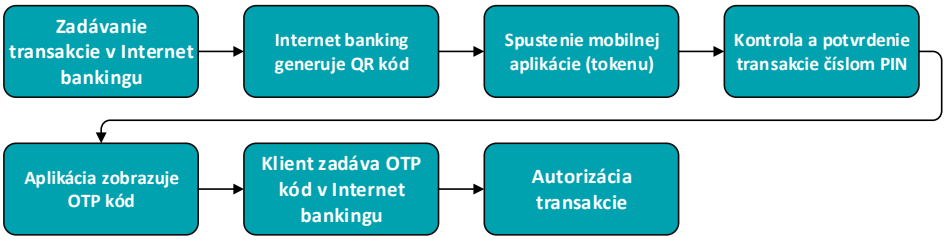
1. klient sa prihlasuje do Internet bankingu osobným identifikačným číslom a heslom,
2. vyberá si formu autentizácie mobilným tokenom (off-line zdieľaný kľúč),
3. Klientovi sa v Internet bankingu vygeneruje QR kód,
4. Klient sa prihlasuje do mobilného tokenu nastaveným PIN číslom,
5. Klient načíta QR kód z Internet bankingu do aplikácie (odfotí kamerou QR kód),
6. Aplikácia zobrazuje nový vygenerovaný kód (OTP),
7. Klient zadáva vygenerovaný kód do Internet bankingu,
8. Klient je prihlásený



Obrázok 30 Autentizácia off-line zdieľaným kľúčom (mobilným tokenom)

Autorizácia transakcie funguje na podobnom princípe ako prihlásenie do Internet bankingu. Pri tomto spôsobe mobilného tokenu prebieha nasledovným spôsobom:

1. klient je prihlásený do Internet bankingu – autentizácia prebehla úspešne,
2. klient zadáva transakciu v prostredí Internet bankingu,
3. Internet banking generuje QR kód,
4. klient sa prihlasuje do mobilného tokenu nastaveným PIN číslom,
5. klient načíta QR kód z Internet bankingu do aplikácie (odfotí kamerou QR kód),
6. aplikácia zobrazuje detaily zadanej transakcie,
7. klient podpisuje (potvrdzuje) transakciu v mobilnej aplikácií svojim PIN číslom,
8. aplikácia zobrazuje vygenerovaný kód (OTP),
9. klient zadáva vygenerovaný kód do Internet bankingu,
10. príkaz bol úspešne autorizovaný.



Obrázok 31 Autorizácia transakcie off-line zdieľaným kľúčom (mobilným tokenom)

7.3.4 Zdieľaný kľúč (on-line spôsob autentizácie)

Metóda je založená na on-line overovaní identity užívateľa a autorizácii transakcií prostredníctvom mobilnej aplikácie v telefóne. On-line zdieľaný kľúč je dvojfaktorová autentizačná aplikácia, umožňujúca klientom banky prihlasovať sa do Internet bankingu a autorizovať transakcie bezpečným spôsobom. Riešenie patrí medzi nejednoduchšie spôsoby autentifikácie a autorizácie pre klienta prostredníctvom mobilnej aplikácie.

Na používanie tejto formy autentifikácie potrebuje mať klient nainštalovanú a aktivovanú mobilnú aplikáciu. Rovnako potrebný počas procesu autentizácie alebo autorizácie transakcií je aj prístup na Internet. Po rýchlej inštalácií sa klientovi zobrazí ponuka na aktiváciu aplikácie, kde vyzýva klienta na zadanie osobného identifikačného čísla PID, ktoré slúži na prihlasovanie do Internet bankingu. Zároveň bude musieť klient zadať bezpečnostný kód, ktorý jednoznačne identifikuje on-line zdieľaný kľúč. Tento bezpečnostný kód získa osobne na pobočke banky, alebo ak vlastní aj iný bezpečnostný prvok, tak sa mu zobrazí ponuka na aktiváciu mobilného tokenu v Internet bankingu. V Internet bankingu sa ponuka zobrazí v sekcii Nastavenia/Aktivácia mobilného tokenu. Bezpečnostný kód bude v tejto sekcii dostupný aj vo forme QR kódu a užívateľ ho môže skenovať priamo v aplikácií mobilného tokenu (Off-line zdieľaný kľúč). Po úspešnom overení totožnosti si klient vytvorí PIN číslo, ktorým sa do aplikácie so mobilným tokenom bude v budúcnosti prihlasovať.

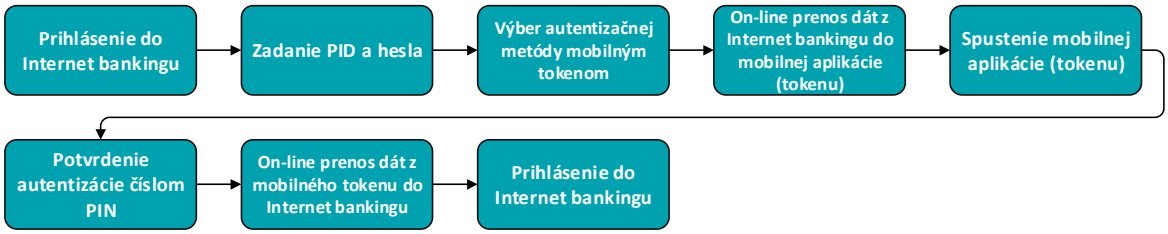
Po vytvorení PIN čísla sa aplikácia zosynchronizuje so serverom banky prostredníctvom Internetu (zabezpečeným protokolom SSL). Následne je mobilná aplikácia aktívna a pripravená na použite. Postup, ako si aktivovať mobilný token, je popísaný v nasledovnom scenári:

1. inštalácia mobilnej aplikácie.
2. aktivácia on-line zdieľaného kľúča prostredníctvom osobného identifikačného čísla a bezpečnostného kódu osobne získaného na pobočke banky alebo prostredníctvom Internet bankingu (numerickým kódom alebo QR kódom),
3. klient si vytvára PIN číslo pre ďalšie prihlasovanie do aplikácie,
4. klient je prihlásený do mobilnej aplikácie (tokenu),
5. aplikácia je úspešne aktivovaná.

Obrázok 32 Aktivácia mobilnej aplikácie, riešenie on-line zdieľaný kľúč

Riešenie podporuje silnú autentifikáciu najmä tým, že po aktivácií aplikácie sa od klienta vždy vyžaduje PIN číslo. Riešenie môže byť dostupné aj na viacerých zariadeniach klienta. Funguje na princípe on-line prenosu dát z Internet bankingu do mobilnej aplikácie (tokenu) a naopak prostredníctvom seba riadiaceho autentizačného servera. Čo znamená, že ak je od klienta v prostredí Internet bankingu vyžadovaná autentizácia alebo autorizácia touto metódou, požiadavka sa okamžite prenesie do aplikácie, kde musí klient pre overenie totožnosti zadať číslo PIN a aplikácia následne prenesie opačným smerom údaje o úspešnej autorizácií/autentizácii. Autentizácia klienta on-line zdieľaným kľúčom pri prihlasovaní do Internet bankingu prebieha nasledovným scenárom:

1. klient sa prihlasuje do Internet bankingu osobným identifikačným číslom a heslom,
2. klient si zvolí formu autentizácie mobilným tokenom (on-line zdieľaný kľúč),
3. on-line prenesenie autentizačných dát z Internet bankingu do mobilnej aplikácie,
4. automatické spustenie mobilnej aplikácie (tokenu),
5. klient pre potvrdenie autentizácie zadáva svoje číslo PIN,
6. on-line prenesenie autentizačných dát z mobilnej aplikácie do Internet bankingu
7. klient je prihlásený.

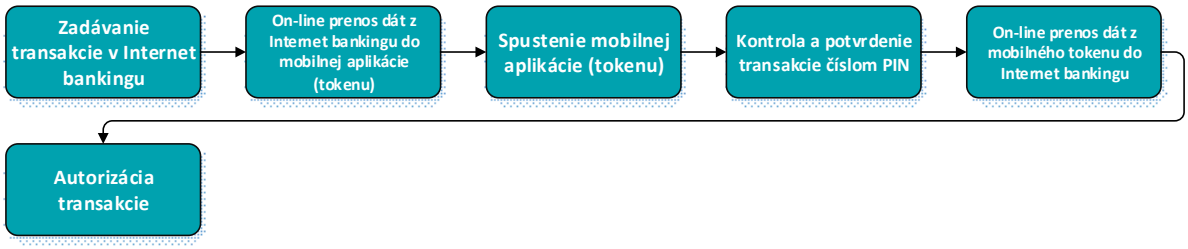


Obrázok 33 Autentizácia on-line zdieľaným kľúčom (mobilným tokenom)

Autorizácia transakcie prebieha nasledovným spôsobom:

1. klient je prihlásený do Internet bankingu – autentizácia prebehla úspešne,
2. klient zadáva transakciu v prostredí Internet bankingu,
3. on-line prenesenie dát o transakcii z Internet bankingu do mobilnej aplikácie,
4. automatické spustenie mobilnej aplikácie (tokenu),
5. aplikácia zobrazuje detaily transakcie,
6. klient po kontrole detailu transakcie, potvrdzuje transakciu svojim číslom PIN,
7. on-line prenesenie dát z mobilnej aplikácie do Internet bankingu,

8. príkaz bol úspešne autorizovaný.



Obrázok 34 Autorizácia transakcie on-line zdieľaným kľúčom (mobilným tokenom)

7.4 Priradenie váh ku každému kritériu

V tejto kapitole budú pridelené k zvoleným kritériám určité váhy. Väčšina metód viac-kriteriálneho rozhodovania požaduje rozlíšenie jednotlivých kritérií z hľadiska ich významnosti pomocou tzv. váh (číselná hodnota vyjadrujúca významnosť zvoleného kritéria). Existuje viacero metód hodnotiacich kritéria rozhodovacieho problému. Pre podrobnejšie hodnotenie kritérií, bola pre tento rozhodovací problém zvolená Saatyho metóda. Jedná sa o kvantitatívnu metódu párového porovnávania kritérií. Pre hodnotenie párových porovnaní zvolených kritérií bude použitá 9-bodová stupnica skladajúca sa z hodnôt 1, 3, 5, 7, 9 porovnávajúca kritéria:

- 1 – znamená, že kritéria i a j sú rovnocenné (rovnako významné),
- 3 – znamená, že prvé kritérium i je slabo preferované pred druhým kritériom j,
- 5 – silno preferované kritérium i pred j,
- 7 – veľmi silne preferované kritérium i pred j,
- 9 – absolútne preferované kritérium i pred j.

Pri používaní Saatyho metódy je potrebné porovnať každú dvojicu kritérií súčasne s veľkosťou preferencií jedného kritéria vzhľadom k druhému kritériu. Veľkosť preferencie i-teho kritéria vzhľadom k j-temu kritériu sa zapíše do Saatyho matice S = (s_{ij}). Ak je j-te kritérium preferované pred i-tym, tak sa do matice zapisuje hodnota v obrátenom tvare. To znamená, že ak je kritérium uvedené v riadku významnejšie, ako kritérium v stĺpci, tak zapíšeme do príslušného riadku počet bodov vyjadrujúci preferenciu kritéria v riadku vzhľadom ku kritériu k stĺpci. Pokiaľ je, naopak, kritérium v stĺpci významnejšie, tak sa zapíše do príslušného riadku prevrátená hodnota zvoleného počtu bodov napr. 1/3.

$$s_{ii} = 1 \; pre \; všetky \; i, \qquad s_{ji} = \frac{1}{s_{ij}} \; pre \; všetky \; i \; a \; j.$$

$$S = \begin{pmatrix} 1 & s_{12} & s_{13} \\ 1/s_{12} & 1 & s_{22} \\ 1/s_{13} & s_{23} & 1 \end{pmatrix}$$

Určenie váh viackriteriálneho rozhodovania prebiehalo pomocou konzultácií (rozhovoru) autora s riaditeľom odboru elektronického bankovníctva Marekom Beňom (konzultant). Na základe tohto rozhovoru bola zostavená tabuľka 8, ktorá vyjadruje porovnanie jednotlivých kritérií pomocou Saatyho metódy. Jedná sa o subjektívne zhodnotenie vyplývajúce z logiky veci a zo skúsenosti autora a najmä konzultujúceho v danom obore. Ako môžeme vidieť z tabuľky 8, na základe konzultácie autora a konzultanta boli zaradené medzi najviac preferované kritériá bezpečnosť a náklady.

Po ohodnotení preferencií jednotlivých kritérií číselnými hodnotami sú tieto čísla autorom zaokrúhlené na dve desatinné miesta, pokiaľ to vyžaduje situácia. Po ohodnotení preferencií jednotlivých kritérií bolo potrebné určiť váhy kritérií. Hodnoty váh kritérií autor vypočítal pomocou geometrického priemeru jednotlivých riadkov Saatyho matice. Hodnoty geometrického priemeru pre jednotlivé kritéria sú vyjadrené v stĺpci Geometrický priemer b_i. Vzorec pre výpočet geometrického priemeru Saatyho matice je (55):

$$b_i = \sqrt[n]{\prod_{j=1}^{n} s_{ij}}$$

Normalizáciou geomterického priemeru potom autor vypočítal váhy ako:

$$v_i = \frac{b_i}{\sum_{i=1}^{n} b_i}$$

Kritéria	Bezpečnosť	Dostupnosť	Náklady	Komfort	Integrácia	Geometrický priemer bi	Váhy
Bezpečnosť	1	7	3	9	7	4,21	0,52
Dostupnosť	0.1	1	0,14	3	3	0,71	0,09
Náklady	0,33	7	1	7	5	2,41	0,30
Komfort	0,11	0,33	0,14	1	3	0,44	0,05
Integrácia	0,14	0,33	0,20	0,33	1	0,32	0,04
	Suma					8,09	1

Tabuľka 8 Hodnotenie kritérií pomocou Saatyho metódy (vlastné spracovanie)

7.5 Hodnotenie kritérií vybraných autentizačných metód

V tejto kapitole si porovnáme výhody a nevýhody vybraných autentizačných metód a na základe tohto porovnania pomocou bodovacej metódy vyberieme novú metódu. Hodnotenie vybraných metód pomocou jednotlivých kritérií bude realizované na základe konzultácií s riaditeľom odboru elektronického bankovníctva, ktorý za túto oblasť zodpovedá a rovnako aj pomocou poznatkov autora získaných pri spracovávaní tejto práce a z praxe. Výber ideálnej metódy zo štyroch zvolených spôsobov autentizácie nie je vôbec ľahká úloha. Existujú rôzne faktory, ktoré od seba vybrané

metódy odlišujú, a na ktorých sú tieto metódy závislé. Pre zjednodušenie procesu porovnávania si uvedieme hlavné výhody a nevýhody zvolených prístupov riešení. Na ich základe sa bude ľahšie vykonávať finálne rozhodnutie. Potom zostavíme tabuľku, vyjadrujúcu pomocou bodovacej metódy úspešnosť plnenia zvolených rozhodovacích kritérií. Na základe výsledku hodnotenia sa pre daný rozhodovací problém zvolí najprijateľnejšia forma autentizácie.

7.5.1 Ohodnotenie e-mailovej autentizácie

Medzi výhody e-mailovej autentizácie môžeme zaradiť:

- jednoduchá integrácia,
- cenovo prístupné riešenie,
- proces autentizácie prebieha použitím dvoch alebo viacerých prvkov na overenie totožnosti klienta,
- pohodlnosť riešenia pre klienta, predpokladá sa, že klient pristupuje do Internet bankingu zo svojho počítača a tým pádom nemusí mať pri sebe nejaký hmotný bezpečnostný predmet. Stačí ak sa prihlási do svojej e-mailovej schránky.
- jednoduchší proces aktivácie bezpečnostného prvku,
- Šetrenie nákladov a odstránenie potreby nakupovať, distribuovať a robiť údržbu tomuto bezpečnostnému prvku.

Medzi nevýhody patrí:

- klient mohol uviesť e-mailovú adresu, ktorej poskytovateľ e-mailovej služby je z hľadiska bezpečností nedôveryhodný,
- neexistencia platnej legislatívy vedúca k vynúteniu dodržiavania bezpečnostných štandardov od poskytovateľov e-mailových služieb - možnosť odchytenia e-mailu na strane poskytovateľa e-mailových služieb,
- rôzna úroveň bezpečnosti poskytovateľov e-mailových služieb, ktoré sú voľne dostupné,
- možnosť prijatia podvrhnutého phishingového e-mailu, ktorý by obsahoval podobnú automaticky generovanú e-mailovú správu obsahujúcu výzvu k zadaniu autentifikačných údajov,
- prvky nie sú zabezpečené pred utajeným odcudzením prostredníctvom Internetu,
- pri ovládnutí počítača klienta je jednoduchšie získať kód e-mailu klienta ako z SMS správy,
- nie je zaručená dôvernosť od momentu inicializácie autentifikácie až po overenie serverom.

7.5.2 Ohodnotenie virtuálnej GRID karty (mobilného tokenu)

Medzi hlavné výhody tohto riešenia patrí:

- drobné požiadavky na integráciu z dôvodu využitia aktuálneho systému banky,
- z vybraných mobilných tokenov najjednoduchšia metóda na implementáciu,
- cenovo prístupné riešenie,
- dáta na báze GRID karty sú zašifrované v mobilnej aplikácií,
- bezpečný proces aktivácie virtuálnej GRID karty z pohľadu banky,
- odpadáva potreba prvok nakupovať, distribuovať stačí, ak si klient stiahne mobilnú aplikáciu (token) z dôverného zdroja (Apple store, Google play),
- na používanie tejto metódy nie je potrebný prístup na Internet.

Hlavné nedostatky, ktoré boli zistené pri hodnotení Virtuálnej GRID karty, sú:

- užívateľsky najmenej prívetivé riešenie,
- obmedzený počet bezpečnostných kódov na Virtuálnej GRID karte,
- pri autentifikácií je potrebné mať pri sebe mobilný telefón (slabšia dostupnosť),
- potreba inštalácie aplikácie, niektorí klienti nemusia mať smartfón,
- zložitejší proces aktivácie aplikácie pre klienta,
- dlhší proces autentifikácie a autorizácie,
- nutný vývoj aplikácie pre dve platformy (IOS a Android),
- nespĺňa smernicu PSD 2.

7.5.3 Ohodnotenie zdieľaného kľúča (off-line spôsob autentizácie)

Medzi hlavné výhody tohto riešenia patria najmä:

- silná ochrana proti phsihingovým útokom a tiež Trojanom ako Man-in-the-Middle a pod.
- znižuje prevdzkové náklady z dlhodobého hľadiska,
- riešenie spĺňa požiadavky definované v smernici PSD 2 a zároveň EBA/GL/2014/ týkajúce sa bezpečnosti internetových platieb. Do autentifikácie sú zahrnuté prvky spájajúce autentifikáciu s konkrétnou sumou a príjemcom, čím sa zvýši istota klienta pri povoľovaní platieb,
- dáta na báze QR kódov nie sú uložené v zašifrovanej podobe v aplikácií, ale sú uložené na autentizačnom serveri,
- bezpečný proces aktivácie mobilného tokenu z pohľadu banky,
- možnosť obrovského množstva kombinácií jednotlivých QR kódov,

- užívateľsky prívetivé riešenie,
- možnosť budúceho rozšírenia na verziu s on-line autorizáciou,
- viackroková autentizácia klienta v aplikácií,
- nie je potrebný prístup na Internet.

Nevýhody tohto riešenia sú:

- náročnejšie na integráciu riešenie,
- vyššie náklady na obstaranie (vývoj aplikácie pre dve platformy, licencie pre autorizačný server),
- potreba inštalácie aplikácie, niektorí klienti nemusia mať smartfón, alebo im nemusí fungovať kamera na zachytenie QR kódu,
- možné problémy s načítaním QR kódov,
- pri autentifikácií je potrebné mať pri sebe mobilný telefón (slabšia dostupnosť).

7.5.4 Ohodnotenie zdieľaného kľúča (on-line spôsob autentizácie)

Medzi výhody tohto riešenia patrí:

- užívateľsky maximálne prívetivé riešenie,
- riešenie spĺňa požiadavky definované v smernici PSD 2 a zároveň EBA/GL/2014/ týkajúce sa bezpečnosti internetových platieb. Do autentifikácie sú zahrnuté prvky spájajúce autentifikáciu s konkrétnou sumou a príjemcom, čím sa zvýši istota klienta pri povoľovaní platieb,
- moderný spôsob autentifikácie môže zlepšiť imidž banky,
- dáta nie sú uložené v zašifrovanej podobe v mobilnej aplikácií, ale sú generované on-line autorizačným serverom,
- veľmi rýchly proces autentifikácie a autorizácie,
- bezpečný proces aktivácie mobilného tokenu z pohľadu banky,
- vysoká bezpečnosť riešenia,
- prináša bezpečnosť a jednoduchosť,

Medzi nevýhody patrí:

- najnáročnejšie na implementáciu z dostupných riešení,
- vysoké obstarávacie náklady (vývoj pre dve platformy, autorizačný server, atď.),
- pri autentifikácii je potrebné mať pri sebe mobilný telefón (slabšia dostupnosť),
- pre používanie je potrebný prístup na Internet.

Pred porovnaním a výberom najlepšieho riešenia na základe stanovených kritérií autora zaujímajú stanovené hypotézy:

- H1: Autentizačná metóda Off-line zdieľaný kľúč skončí v celkovom hodnotení na poslednom mieste, z dôvodu vyššej ceny riešenia.
- H2: Autentizácia Virtuálnou GRID kartou sa umiestni na prvom mieste z vybraných alternatív, z dôvodu nižšej ceny a ľahšej integrovateľnosti do existujúcich systémov banky.

7.6 Výber najlepšieho riešenia

Na celkové zhrnutie dostupných autentizačných metód a následný výber novej metódy využijeme bodovaciu metódu vychádzajúcu z porovnania významnosti jednotlivých kritérií. Na základe konzultácii s riaditeľom elektronického bankovníctva, budú tieto metódy ohodnotené v nasledujúcej tabuľke 9 podľa určených kritérií. Každá autentizačná metóda bude ohodnotená na základe konzultácií autora a konzultanta podľa daného kritéria na číselnej stupnici od 1 – najhoršie ohodnotenie až po 10 – najlepšie ohodnotenie. Čím je kritérium dôležitejšie, tým väčší počet bodov získa. Pred použitím bodovacej metódy bolo potrebné najskôr porovnať jednotlivé kritéria podľa poradia preferencií. Postup výberu najlepšej z dostupných metód sa rozšíril aj o váhy kritérií, ktoré autor vypočítal na základe preferencií pomocou Saatyho metódy. (55)

Autor práce poskytol pre lepší prehľad pomocnému konzultantovi (riaditeľ odboru elektronického bankovníctva) vytlačenú tabuľku 9. Po konzultácií autor na základe hodnotenia pomocou bodovacej stupnice pridelil každej metóde podľa kritéria príslušný počet bodov v hladine 1 až 10. Získaný počet bodov autor prenásobil váhami a dostal celkový počet bodov určujúci poradie vybraných autentizačných metód.

Autentizačné metódy	Bezpečnosť	Dostupnosť	Náklady	Komfort	Integrácia	Celkový počet bodov	Poradie
E-mail autentifikácia	2	5	9	4	9	4,75	4.
Virtuálna GRID karta	5	6	7	6	6	5,78	3.
Off-line zdieľaný kľúč	8	7	5	7	5	6,84	**1.**
On-line zdieľaný kľúč	9	4	3	9	3	6,51	2.
Váhy	0,52	0,09	0,30	0,05	0,04		

Tabuľka 9 Záverečná porovnávacia tabuľka na základe bodovacej metódy (vlastné spracovanie)

Pred záverečným zhodnotením autentizačných metód je potrebné upozorniť na to, že hodnotenie váh vybraných kritérií bolo konzultované s riaditeľom odboru elektronického bankovníctva. Pri porovnaní vybraných riešení najhoršie dopadla e-mailová autentizácia najmä kvôli nesplneniu základných bezpečnostných požiadaviek. Aj keď patrí medzi riešenia s najľahšou integráciou a najnižšími nákladmi. Požiadavky na silnú autentifikáciu definované v smernici platobných služieb vstúpia do platnosti začiatkom roka 2017 a tak by bolo nezmyselné implementovať túto metódu.

Naopak najlepším riešením podľa stanovených kritérií sa stal mobilný token založený na off-line zdieľanom kľúči. Je potrebné skonštatovať, že rozdiely v celkovom počte bodov medzi jednotlivými formami autentizácie nie sú príliš veľké, čo môže vyplývať aj z menšieho rozsahu hodnotiacej stupnice, ktorá bola stanovená na 1 až 10 bodov. Off-line zdieľaný kľúč sa umiestnil v celkovom poradí vybraných autentizačných metód na prvom mieste najmä preto, že z hľadiska bezpečnosti patrí medzi riešenia, ktoré najviac spĺňajú bezpečnostné kritéria. Bezpečnosť metódy patrila pri rozhodovaní medzi najviac preferované kritéria. Výhodou víťaznej metódy oproti druhej v poradí (on-line zdieľaný kľúč) boli celkové náklady, ktoré neboli až tak vysoké ako pri on-line spôsobe autentizácie. Pri rozhodovaní o najlepšej z vybraných metód rozhodla aj dostupnosť riešenia, kedy pri používaní off-line spôsobu autentizácie nie je potrebný prístup na Internet.

8 Záver

Cieľom práce bolo vybrať vhodnú autentizačnú metódu pre prihlasovanie do elektronického bankovníctva. Navrhnuté riešenie by sa dalo aplikovať vo viacerých finančných inštitúciách, v ktorých kladú veľký dôraz na bezpečnosť a inovácie riešení. Pre lepšie pochopenie jednotlivých riešení bolo potrebné najskôr v kapitole 2 podrobne vysvetliť vývoj a charakteristiku elektronického bankovníctva. V tejto časti boli podrobne popísané hlavné dôvody a príčiny vzniku elektronického bankovníctva, ktorého používanie prináša mnohé výhody. V dnešnej dobe skoro každá banka poskytuje služby elektronického bankovníctva z dôvodu veľkého množstva výhod pre banku aj pre klienta. Táto práca môže slúžiť ako podklad pri rozhodovaní a implementácii takéhoto riešenia bankou, alebo pri začatí používania klientom. V kapitole 3 sú spomenuté trendy, ktoré každodenne ovplyvňujú rozhodovanie manažérov o budúcnosti smerovania kanálov elektronického bankovníctva.

Predposledná kapitola teoretickej časti popisuje bezpečnosť, ktorá patrí medzi najdôležitejšie kritéria pri poskytovaní služieb elektronického bankovníctva. V tejto kapitole je popísaná dôležitosť ochrany aktív v každej organizácii pomocou informačnej bezpečnosti. Ďalej sú to popísané pojmy ako autentifikácia, autorizácia alebo autentizácia, ktoré sa najviac vyskytujú v tejto práci a z toho dôvodu je potrebné si význam týchto pojmov ujasniť. Pri výbere novej autentizačnej metódy je potrebné poznať aktuálne riešenia, dostupné na slovenskom trhu, ktoré sú podrobne rozpísané v podkapitole autentifikácia. Rovnako dôležité je aj poznať možné bezpečnostné hrozby, ktorým kanály elektronického bankovníctva vzdorujú každý deň.

Posledná kapitola teoretickej časti obsahuje popis základných požiadaviek na výber autentizačnej metódy. V tejto časti netreba zabúdať najmä na smernicu o platobných službách PSD2, ktorá jasne definuje požiadavky na silnú autentifikáciu.

Praktická časť začína popisom skutočností, ktoré treba pred výberom nového bezpečnostného prvku zohľadniť. Banka sa v dôsledku nedostatočnej bezpečnosti GRID kariet rozhodla tento prvok postupne zrušiť. Zmeny, týkajúce sa zrušenia bezpečnostných prvkov, sú pre klientov pre klientov citlivými témami. Popísaná analýza zrušenia tohto prvku prišla s riešením, ktoré bolo rozdelené do viacerých fáz, s cieľom nestratiť existujúcich klientov a zároveň ich namotivovať na zmenu prvku. Bolo zaujímavé sledovať, ako klienti pristupovali k jednotlivým fázam pri zmene prvku.

Významnú časť práce tvorí návrh a výber možných autentizačných metód a popis vybraných hodnotiacich kritérií, ku ktorým boli priradené váhy na základe konzultácie s riaditeľom odboru elektronického bankovníctva. Výber jednotlivých autentizačných metód bol postavený najmä na výbere riešenia, ktoré by bolo dostupné na mobilných platformách (IOS, Android). Táto časť sa predovšetkým zaoberá viackriteriálnym rozhodovaním medzi navrhnutými riešeniami. Pri určení váh

vybraných kritérií bola použitá Saatyho metóda, po ktorej nasledovalo viackriteriálne hodnotenie autentizačných metód za pomoci bodovacej metódy. Na základe pridelenia bodov jednotlivým riešeniam sme dospeli k výsledku, ktorý nám slúžil ako základ pre porovnanie autentizačných metód, čím sa naplnil cieľ práce.

Na základe porovnania vybraných riešení môžeme dospieť k názoru, že hypotézy, ktoré určil autor práce, sa nepotvrdili. Autorova hypotéza H1, ktorá hovorila o poslednom mieste autentizačnej metódy Off-line zdieľaný kľúč sa nepotvrdila, a nakoniec toto riešenie dostalo najlepšie hodnotenie spomedzi všetkých dostupných riešení, najmä kvôli vysokej bezpečnosti, komforte riešenia a dostupnosti aj bez internetového pripojenia. Naopak, riešenie Virtuálnou GRID kartou bolo pri viackriteriálnom rozhodovaní umiestnené až na treťom zo štyroch miest. Preto môžeme dospieť k záveru, že ani hypotéza H2 sa nepotvrdila.

Očakávaným prínosom tejto diplomovej práce bolo vybrať vhodné riešenie, ktoré by nahradilo zastaranú autentizačnú metódu a zároveň by rozšírilo možnosti autentizácie pri prihlasovaní do Internet bankingu. Pri rozhodovaní sme brali za najdôležitejšie kritérium bezpečnosť, netreba však zabúdať, že s rastúcou bezpečnosťou rastie aj cena výsledného riešenia. Preto by sa pri rozhodovaní nemalo zohľadňovať len jediné kritérium, ale mali by sme ich posudzovať viac.

Táto diplomová práca mala veľký prínos aj pre samotného autora, ktorému pomohla rozšíriť obzory najmä v oblasti trendov autentizačných metód a spôsobov zabezpečenia elektronického bankovníctva, ktoré môže využiť pri svojom aktuálnom zamestnaní.

Zoznam použitej literatúry

1. www.nbs.sk. *Zákon o platobnom styku č. 510/2002 Z. z.* [Online] 19. August 2002. [Dátum: 1. Február 2017.] http://www.nbs.sk/_img/Documents/_Legislativa/_UplneZneniaZakonov/Z510-2002_567-08.PDF.

2. **Půlpánová, Stanislava.** *Komerční bankovnictví v České republice.* Praha : Oeconomica, 2007. ISBN: 978-80-245-1180-1.

3. **Zeman, Václav.** *Bankovnictví.* Brno : Vysoké učení technické v Brně, 2008. ISBN 978-80-214-3581-0.

4. **EuroEkonóm.sk.** Priamy marketing - direct marketing. *www.euroekonom.sk.* [Online] 20. Január 2017. [Dátum: 18. Február 2017.] http://www.euroekonom.sk/marketing/priamy-direct-marketing/priamy-marketing/.

5. **Prima banka Slovensko, a.s.** Ochrana osobných údajov. *www.primabanka.sk.* [Online] 2017. [Dátum: 4. Marec 2017.] https://www.primabanka.sk/preview-file/ochrana_osobnych_udajov_prima_banka_slovensko_final_web-1203.pdf.

6. **Poštová banka.** Poštová banka. *www.postovabanka.sk.* [Online] 2017. [Dátum: 1. Marec 2017.] https://www.postovabanka.sk/korporatni-klienti/podnikatelske-ucty-a-baliky/phone-banking/.

7. **Kováč, Jaroslav.** GSM-banking (SMS-banking) a mailbanking. *www.zive.sk.* [Online] 13. Február 2001. [Dátum: 5. Február 2017.] http://www.zive.sk/clanok/7210/gsm-banking-sms-banking-a-mailbanking.

8. **PELTIER, THOMAS R.** *Information Security Fundamentals, Second Edition. 2nd ed.* Hoboken : Taylor and Francis, 2013. ISBN: 978-1439810620.

9. **Mahmood Steve, Shah Clarke.** *E-banking management.* Hershey, PA : Information Science Reference, 2009. ISBN1605662534.

10. **Tata Consultancy services.** tcs.com. *www.tcs.com.* [Online] [Dátum: 3. Marec 2017.] http://www.tcs.com.

11. **Kemal, Avkiran Necmi.** *International Journal of Bank Marketing.* UK : MCB Uni. Press, 1999. ISSN 0265-2323.

12. **Zimková, Emília.** *Bankovníctvo.* Banská Bystrica : Univerzita Mateja Bela, 2009. ISBN 978-80-8083-801-0.

13. *Technologie mění bankovnictví.Jsou na ně připraveny banky i jejich zaměstnanci?* **Bankovnictví.** 8, Praha : 4H production s.r.o, 2016. ISSN 1212 - 4273.

14. **Deaton, Matt.** Survey on Branch Transformation. *www.ababankmarketing.com.* [Online] ABA Bank Marketing, 22. Október 2015. [Dátum: 25. Február 2017.] http://ababankmarketing.com/insights/survey-on-branch-transformation/.

15. **Statista.** Online banking penetration in selected European markets in 2016. *www.statista.com.* [Online] 4. Február 2017. [Dátum: 3. Marec 2017.] https://www.statista.com/statistics/222286/online-banking-penetration-in-leading-european-countries/.

16. **Prima banka Slovensko, a.s.** O banke. *www.primabanka.sk.* [Online] 4. Február 2017. [Dátum: 3. Marec 2017.] https://www.primabanka.sk/o-banke##top.

17. **Allaboutux.** Bringing clarity to the concept of user experience. *www.allaboutux.org.* [Online] 11. Február 2011. [Dátum: 07. Február 2017.] http://www.allaboutux.org/files/UX-WhitePaper.pdf.

18. **Statista.** Number of smartphone users worldwide: Statista. *www.statista.com.* [Online] 3. Február 2016. [Dátum: 2. Marec 2017.] https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

19. **Bestro, Robert.** Popularita mobilného bankovníctva stúpa. *www.banky.sk.* [Online] 8. August 2015. [Dátum: 14. Február 2017.] http://banky.sk/popularita-mobilneho-bankovnictva-stupa/.

20. **GAVENDOVÁ, ALŽBETA HARRY.** Prima banka Penaženka videoblog. *www.mojandroid.sk.* [Online] 13. Február 2017. [Dátum: 21. Február 2017.] https://www.mojandroid.sk/prima-banka-penazenka-videoblog/.

21. **Mobile World Live.** European mobile banking penetration to surpass 50% next year. *www.mobileworldlive.com.* [Online] 7. Júl 2016. [Dátum: 24. Február 2017.] https://www.mobileworldlive.com/money/european-mobile-banking-set-to-soar/.

22. **Symantec.** Safe Mobile Apps for Financial Services. *www.symantec.com.* [Online] Júl 2012. [Dátum: 8. Marec 2017.] https://www.symantec.com/content/en/us/enterprise/white_papers/b-safe-mobile-apps-financial-svcs-WP-21261440.en-us.pdf.

23. **Andrieux, David.** Banking in the digital age. *Soprabanking.com.* [Online] Sopra - banking software, 2016. [Dátum: 5. Február 2017.] https://www.soprabanking.com/docs/librariesprovider17/sopra-banking-software/white-paper---banking-in-the-digital-age.pdf?sfvrsn=0.

24. *Videobankéř - standard, který klienti buduou vyžadovat.* **Sobková, Martina.** 8, Praha : 4H Production s.r.o., 2016. ISSN 1212-4273 MK ČR E 8022.

25. **Finance.cz.** Přímé bankovnictví. *www.finance.cz.* [Online] 2017. [Dátum: 24. Február 2017.] http://www.finance.cz/ucty-a-sporeni/bezne-ucty/abeceda-beznych-uctu/prime-bankovnictvi/.

26. **European Banking Authority.** CONSULTATION PAPER ON DRAFT RTS ON AUTHENTICATION AND COMMUNICATION UNDER PSD2. *www.eba.europa.eu.* [Online] 12. August 2016. [Dátum: 5. Marec 2017.] https://www.eba.europa.eu/documents/10180/1548183/Consultation+Paper+on+draft+RTS+on+SCA+and+CSC+(EBA-CP-2016-11).pdf.

27. **Jeremy Light, Andrew McFarlane, Killian Barry, Ilkka Ruostila.** Unlocked by the EU´s Revised Payment Services Directive. *www.accenture.com.* [Online] 8. Október 2015. [Dátum: 8. Marec 2017.] https://www.accenture.com/t20160518T092811__w__/us-en/_acnmedia/PDF-19/Accenture-Banking-Opportunities-EU-PSD2-v2.pdf.

28. *Už není čas být konzervativní! Technológie mění svět rychleji než kdy dřív.* **Bankovnictví.** 8, Praha : 4H Production, 2016. ISSN 1212 - 4273 MK ČR E 8022.

29. **Purohit, Vinay.** Tutorialspoint.com. *Authentication and Access Control - The Cornerstone of Information Security.* [Online] September 2007. [Dátum: 26. Február 2017.] http://www.tutorialspoint.com/assets/white-papers/40.pdf.

30. **Prima banka Slovensko, a. s.** Informačná bezpečnosť na strane banky. *www.primabanka.sk.* [Online] 2017. [Dátum: 15. Február 2017.] https://www.primabanka.sk/dolezite-informacie/informacna-bezpecnost/banka.

31. **Kinder, Lucy.** Worst password of 2013 was ´123456´ according to new research. *www.telegraph.co.uk.* [Online] Telegrapgh, 21. Január 2014. [Dátum: 4. Marec 2017.] http://www.telegraph.co.uk/technology/news/10587694/Worst-password-of-2013-was-123456-according-to-new-research.html.

32. **Action Fraud.** Ofcom reveals online password security risk. *www.actionfraud.police.uk.* [Online] Actionfraud, 25. April 2013. [Dátum: 5. Marec 2017.] http://www.actionfraud.police.uk/contact-us.

33. **Thigpen, Seth.** Authentication Methods Used for Banking. *Infosecwriters.com.* [Online] [Dátum: 2. Marec 2017.] http://www.infosecwriters.com/text_resources/pdf/Authentication_Methods_For_Banking.pdf.

34. **Purser, Steve.** *A practical guide to managing Information Security.* Norwood : Artech House, INC., 2004. ISBN 1-58053-702-2.

35. **Vasco.** Vasco Digipass Family of Authentication Devices. *www.vasco.com.* [Online] [Dátum: 10. Marec 2017.] https://www.konicaminolta.de/fileadmin/content/de/IT_Solutions/Produkte/IT-Security/Identity_und_Access_Management/PDF/Vasco_Whitepaper_Digipass_Family_of_Authentication_Devices_EN.pdf.

36. **Hiltgen A., Kramp T., Weigold T.** *Secure Internet banking authentication.* s.l. : IEEE Security and Privacy, 2006. ISSN 1540-7993.

37. **Meyer, Roger.** Secure Authentication on the Internet. *www.sans.org.* [Online] 4. Apríl 2007. [Dátum: 26. Február 2017.] https://www.sans.org/reading-room/whitepapers/securecode/secure-authentication-internet-2084.

38. **Siska, Juraj.** Choosing the Right Authentication. *www.proviti.com.* [Online] 2006. [Dátum: 15. Február 2017.] https://www.protiviti.com/sites/default/files/united_states/insights/authentication_whitepaper.pdf.

39. **C., Wüest.** Phishing in The Middle of The Stream Today´s Threats To Online Banking. *www.symantec.com.* [Online] 2005. [Dátum: 26. Február 2017.] https://www.symantec.com/avcenter/reference/phishing.in.the.middle.of.the.stream.pdf.

40. **Hodás, Martin.** Phishingové útoky na klientov slovenských bánk: Ako sa chrániť? *www.zive.sk.* [Online] 24. Jún 2015. [Dátum: 4. Marec 2017.] http://www.zive.sk/clanok/105906/phishingove-utoky-na-klientov-slovenskych-bank-ako-sa-chranit.

41. **Landesman, Mary.** What is a Keylogger Trojan? *www.lifewire.com.* [Online] 3. Septembter 2016. [Dátum: 1. Marec 2017.] https://www.lifewire.com/what-is-a-keylogger-trojan-153623.

42. *PHISHING, PHARMING AND IDENTITY THEFT.* **Brody Richard G., Mulig Elizabeth, Kimball Valerie.** 3, s.l. : Academy of Accounting and Financial Studies Journal, 2007, Zv. 11. ISSN: 1096-3685.

43. **Slovenská sporiteľňa.** Čo je vishing? *www.slsp.sk.* [Online] 2017. [Dátum: 23. Február 2017.] https://www.slsp.sk/sk/otazky-a-odpovede/co-je-vishing.

44. **European banking association.** Final Guidelines on the Security of Internet Payments. *www.eba.europa.eu.* [Online] 19. December 2014. [Dátum: 1. Marec 2017.] https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+(Guidelines+on+the+security+of+internet+payments)_Rev1.

45. **Gregory, D., Williamson.** Enhanced Authentication in Online Banking. *www.utica.edu.* [Online] 2006. [Dátum: 25. Február 2017.] https://www.utica.edu/academic/institutes/ecii/publications/articles/51D6D996-90F2-F468-AC09C4E8071575AE.pdf.

46. **European banking authority.** *Záverečné usmernenia týkajúce sa bezpečnosti internetových platieb.* Bratislava : EBA, 2014.

47. **Entrust.** A Practical Approach to Authentication in an Evolving Enterprise Enviroment. *www.entrust.com.* [Online] Marec 2011. [Dátum: 27. Február 2017.] https://dsimg.ubm-us.net/envelope/129292/323052/1302014527947_wp_enterprise_auth_web.pdf.

48. **Latch.** The alternative to GRID card. *www.latch.elevenpaths.com.* [Online] [Dátum: 15. Marec 2017.] https://latch.elevenpaths.com/www/public/documents/brochuresLatch/Brochure_Latch_Coordenadas_web_en.pdf.

49. **Jarošová, Gabriela.** Grid karty len na vlastné riziko. *www.etrend.sk.* [Online] 11. Marec 2009. [Dátum: 4. Marec 2017.] https://www.etrend.sk/technologie/grid-karty-len-na-vlastne-riziko.html.

50. **Prima banka Slovensko, a. s.** Všeobecné obchodné podmienky. *www.primabanka.sk.* [Online] 2017. [Dátum: 5. Marec 2017.] https://www.primabanka.sk/vop/preview-file/vop-160_75_0116_final-1913.pdf.

51. —. Limity pre platobné služby prostredníctvom internet bankingu. *www.primabanka.sk.* [Online] 1. Jún 2016. [Dátum: 12. Marec 2017.] https://www.primabanka.sk/pre-samospravy/ucty/elektronicke-bankovnictvo/limity-pre-platobne-sluzby-prostrednictvom-internet-bankingu.

52. **Prima banka Slovensko, a.s.** Interný dokument spoločnosti Prima banka Slovensko, a.s. Bratislava : s.n., 2017.

53. **Csernák, Peter.** Tatra banka ruší GRID karty. *www.etrend.sk.* [Online] News and Media Holding, 9. Júl 2008. [Dátum: 1. Marec 2017.] https://www.etrend.sk/financie/tatra-banka-rusi-grid-karty.html.

54. **Fulop, János.** Introduction to Decision Making Methods. *www.academic.evergreen.edu.* [Online] [Dátum: 20. Marec 2017.] http://academic.evergreen.edu/projects/bdei/documents/decisionmakingmethods.pdf.

55. **Gade, Praveen Kumar a Osuri, Manjit.** Evaluation of Multi Criteria Decision Making. *www.diva-portal.org.* [Online] [Dátum: 25. Marec 2017.] https://www.diva-portal.org/smash/get/diva2:831025/FULLTEXT01.pdf.

56. **Brožová, H, Houška, M a Šubrt, T.** *Modely pro vícekriteriální rozhodování.* Praha : ČZU, 2003. ISBN: 978-80-213-1019-3.

57. **M., Jakobsson.** *Phising and Countermeasures: Understanding the In-creasing Problem of Electronic Identity Theft.* s.l. : Wiley, 2007. ISBN: 978-0-471-78245-2.

58. Financial Threats in 2016: Half of All Phishing Attacks Aimed to Steal Money. *www.usa.kaspersky.com.* [Online] 22. Február 2017. [Dátum: 27. Február 2017.] http://usa.kaspersky.com/about-us/press-center/press-releases/2017/financial-threats-in-2016-half-of-all-phishing-attacks-aimed-to-steal-money.

59. **Prima banka Slovensko, a. s.** Limity pre operácie prostredníctvom služieb EB. *www.primabanka.sk.* [Online] 1. Jún 2016. [Dátum: 10. Marec 2017.] https://www.primabanka.sk/elektronicke-bankovnictvo-pre-biznis/preview-file/limity-pre-operacie-elektronickeho-bankovnictva_ucinne_1-6-2016-2285.pdf.

60. **Wikipédia.** Internetová akciová bublina. *www.wikipedia.org.* [Online] 9. Marec 2013. [Dátum: 7. Február 2017.] https://sk.wikipedia.org/wiki/Internetov%C3%A1_akciov%C3%A1_bublina.

Zoznam obrázkov

Zoznam tabuliek

Zoznam grafov