

Kanali e-bankarstva i hardverske komponente u bankarstvu

Hrehorović, Ivan

Undergraduate thesis / Završni rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Economics in Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Ekonomski fakultet u Osijeku**

Permanent link / Trajna poveznica: <https://urn.nsk.hr/urn:nbn:hr:145:545007>

Rights / Prava: [In copyright](#) / [Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-11-15**



Repository / Repozitorij:

[EFOS REPOSITORY - Repository of the Faculty of Economics in Osijek](#)



Sveučilište Josipa Jurja Strossmayera u Osijeku

Ekonomski fakultet u Osijeku

Sveučilišni prijediplomski studij Poslovna informatika

Ivan Hrehorović

Kanali e-bankarstva i hardverske komponente u bankarstvu

Završni rad

Osijek, 2023.

Sveučilište Josipa Jurja Strossmayera u Osijeku

Ekonomski fakultet u Osijeku

Sveučilišni prijediplomski studij Poslovna informatika

Ivan Hrehorović

Kanali e-bankarstva i hardverske komponente u bankarstvu

Završni rad

Kolegij: Informacijsko-komunikacijska tehnologija (ICT) u bankarstvu

JMBAG: 0010225861

e-mail: ihrehorovic@efos.hr

Mentor: prof. dr. sc. Šarlija Nataša

Komentor: dr. sc. Has Adela

Osijek, 2023.

Josip Juraj Strossmayer University of Osijek
Faculty of Economics and Business in Osijek
Unedrgraduate Study Business Informatics

Ivan Hrehorović


Channels of e-banking and hardware components in banking

Final paper

Osijek, 2023.

IZJAVA

O AKADEMSKOJ ČESTITOSTI, PRAVU PRIJENOSA INTELEKTUALNOG VLASNIŠTVA, SUGLASNOSTI ZA OBJAVU U INSTITUCIJSKIM REPOZITORIJIMA I ISTOVJETNOSTI DIGITALNE I TISKANE VERZIJE RADA

1. Kojom izjavljujem i svojim potpisom potvrđujem da je završni rad isključivo rezultat osobnoga rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu. Potvrđujem poštivanje nepovredivosti autorstva te točno citiranje radova drugih autora i referiranje na njih.
2. Kojom izjavljujem da je Ekonomski fakultet u Osijeku, bez naknade u vremenski i teritorijalno neograničenom opsegu, nositelj svih prava intelektualnoga vlasništva u odnosu na navedeni rad pod licencom *Creative Commons Imenovanje – Nekomercijalno – Dijeli pod istim uvjetima 3.0 Hrvatska*. 
3. Kojom izjavljujem da sam suglasan/suglasna da se trajno pohrani i objavi moj rad u institucijskom digitalnom repozitoriju Ekonomskoga fakulteta u Osijeku, repozitoriju Sveučilišta Josipa Jurja Strossmayera u Osijeku te javno dostupnom repozitoriju Nacionalne i sveučilišne knjižnice u Zagrebu (u skladu s odredbama Zakona o visokom obrazovanju i znanstvenoj djelatnosti, NN 119/2022).
4. izjavljujem da sam autor/autorica predanog rada i da je sadržaj predane elektroničke datoteke u potpunosti istovjetan sa dovršenom tiskanom verzijom rada predanom u svrhu obrane istog.

Ime i prezime studenta: Ivan Hrehorović

JMBAG: 0010225861

OIB: 05626055919

e-mail za kontakt: ivan.hrehorovic@gmail.com

Naziv studija: Sveučilišni prijediplomski studij Poslovna informatika

Naslov rada: Kanali e-bankarstva i hardverske komponente u bankarstvu

Mentor/mentorica rada: prof. dr. sc. Šarlija Nataša

U Osijeku, 13. rujna 2023. godine

Potpis

Ivan Hrehorović

Kanali e-bankarstva i hardverske komponente u bankarstvu

SAŽETAK

U ovom završnom radu istražuju se kanali e-bankarstva i njihova povezanost s hardverskim komponentama u bankarskom sektoru. Suvremeno bankarstvo sve više se oslanja na elektroničke kanale kako bi korisnicima pružilo brže i praktičnije usluge. Kroz analizu različitih kanala e-bankarstva, kao što su internetsko bankarstvo, mobilno bankarstvo, telefonsko bankarstvo, TV bankarstvo i bankomati, istražuje se njihova uloga u pružanju različitih bankarskih usluga. Nadalje, posebna važnost pridana je hardverskim komponentama koje podržavaju ove kanale. To uključuje POS uređaje, pametne telefone, kartice s mikročipom i biometrijske uređaje. Ovi hardverski elementi pružaju sigurnost i pouzdanost u bankarskim transakcijama te olakšavaju autentifikaciju korisnika. Detaljno su proučene njihove funkcionalnosti, prednosti i izazovi s kojima se suočavaju u kontekstu e-bankarstva. Kanali e-bankarstva pružaju korisnicima mogućnost brzog i praktičnog pristupa bankarskim uslugama, dok hardverske komponente osiguravaju sigurnost i autentičnost tijekom transakcija. Međutim, suočavamo se s izazovima poput sigurnosti podataka i potrebe za stalnim inovacijama u hardveru kako bi se unaprijedilo e-bankarstvo. U skladu s tim, ovaj rad pruža smjernice za daljnji razvoj e-bankarstva, uključujući integraciju naprednih tehnologija poput biometrije i unaprjeđenje sigurnosti podataka. Također naglašena je važnost obrazovanja korisnika kako bi se maksimalno iskoristile prednosti kanala e-bankarstva i hardverskih komponenti. Ukratko, ovaj rad pruža sveobuhvatan pregled kanala e-bankarstva i hardverskih komponenti u bankarstvu. Također pruža smjernice za bankarske institucije i korisnike kako bi uspješno iskoristili prednosti ovih tehnologija, uzimajući u obzir sigurnost, privatnost i prilagodbu novim tehnološkim inovacijama.

Ključne riječi: bankarstvo, funkcije e-bankarstva, kanali e-bankarstva, hardverske komponente, sigurnost

Channels of e-banking and hardware components in banking

ABSTRACT

This final paper examines e-banking channels and their relationship to hardware components in the banking industry. Modern banking increasingly relies on electronic channels to provide faster and more convenient services to users. By analyzing various e-banking channels such as Internet banking, mobile banking, telephone banking, TV banking, and ATMs, their role in providing various banking services is examined. In addition, special attention is given to the hardware components that support these channels. These include POS devices, smartphones, smart cards, and biometric devices. These hardware elements provide security and reliability for banking transactions and facilitate user authentication. Their functionalities, benefits, and challenges in the context of e-banking are examined in detail. E-banking channels provide users with the ability to access banking services quickly and conveniently, while hardware components ensure security and authenticity during transactions. However, we face challenges such as data security and the need for continuous hardware innovation to improve e-banking. This paper therefore presents guidelines for the further development of e-banking, including the integration of advanced technologies such as biometrics and the improvement of data security. It also highlights the importance of user education to take full advantage of e-banking channels and hardware components. In summary, this paper provides a comprehensive overview of e-banking channels and hardware components in banking. It also provides guidelines for banking institutions and users to successfully use these technologies, taking into account security, privacy, and adaptation to new technological innovations.

Key words: e-banking, functions of e-banking, e-banking channels, hardware components, security

Sadržaj

1. Uvod	1
2. Teorijska podloga i prethodna istraživanja	3
2.1. Ciljevi istraživanja	3
2.2. Metodologija rada	3
2.3. Transformacija bankarstva kroz povijest	4
2.4. Koncept e-bankarstva	6
2.5. Kanali e-bankarstva	6
2.5.1. Internetsko bankarstvo	7
2.5.2. Mobilno bankarstvo	8
2.5.3. Telefonsko bankarstvo	8
2.5.4. TV bankarstvo	9
2.5.5. Bankomati	10
2.5.4.1. Zaštita i sigurnost u bankomatu	11
2.5.5. Interaktivni kiosci	11
2.6. Hardverske komponente	12
2.6.1. Uređaji za autorizaciju korisnika	12
2.6.1.1. TAN tablica	13
2.6.1.2. Token	13
2.6.1.3. M-token	14
2.6.1.4. Display kartica	15
2.6.1.5. Čitač kartica	16
2.6.1.6. USB stick s certifikatom	16
2.6.1.7. Biometrijski uređaji za autorizaciju	17
2.7. Sigurnost u e-bankarstvu	18
2.8. Pregled prethodnih istraživanja	19

2.9. Prednosti i izazovi kanala e-bankarstva	20
4. Opis istraživanja i rezultati istraživanja	23
4.1. Primjeri bankomata i interaktivnih kioska	23
4.2. Telefonsko bankarstvo	25
4.3. Online (Internet) bankarstvo	26
4.4. Mobilno bankarstvo	27
4.5. TV bankarstvo	28
4.6. Usporedba online bankarstva PBZ i Erste banke	29
4.6. Anketno istraživanje	30
5. Rasprava	32
6. Zaključak	33
LITERATURA	34
Popis slika	38

1. Uvod

Ovaj rad istražuje kanale e-bankarstva i njihove hardverske komponente. E-bankarstvo je važan aspekt moderne financijske industrije, omogućavajući korisnicima da obavljaju bankovne transakcije i pristupaju bankarskim uslugama putem elektroničkih kanala. Ovaj rad fokusira se na pet kanala e-bankarstva i njihove povezane hardverske komponente. Prvi kanal koji se istražuje su bankomati i interaktivni kiosci. Ti uređaji omogućavaju korisnicima da obavljaju različite transakcije, kao što su podizanje gotovine, provjera stanja računa i prijenos sredstava. Hardverske komponente ovih kanala uključuju računalnu opremu, uključujući monitor, tipkovnicu i skener za čitanje kartica, kao i komunikacijsku opremu za povezivanje s bankovnim sustavom. Drugi kanal koji se istražuje je telefonsko bankarstvo. Telefonske linije omogućuju korisnicima pristup bankarskim uslugama putem telefonskog poziva. Hardverske komponente u ovom kanalu uključuju telefonsku opremu i komunikacijsku opremu koja omogućuje prijenos podataka između korisnika i banke. Treći kanal koji se istražuje je online bankarstvo, koje korisnicima omogućava pristup bankovnim uslugama putem interneta. Računala i računalna oprema, kao što su osobna računala, tableti i pametni telefoni, koriste se za pristupanje online bankarskim platformama. Osim toga, komunikacijska oprema kao što su mrežni uređaji i modemi, te sigurnosne komponente poput vatrozida (engl. firewall) i enkripcijskih sustava, također su važni dijelovi hardverske infrastrukture online bankarstva. Četvrti kanal koji se istražuje je mobilno bankarstvo. Mobilne aplikacije omogućavaju korisnicima pristup bankovnim uslugama putem njihovih mobilnih uređaja. Hardverske komponente ovog kanala uključuju mobilne telefone, tablete i druge prijenosne uređaje koji podržavaju mobilne aplikacije za bankarstvo. Posljednji kanal koji se istražuje je TV bankarstvo, koje omogućava korisnicima pristup bankovnim uslugama putem televizijskog sučelja. Hardverske komponente ovog kanala uključuju televizore, daljinske upravljače i set-top boxove koji omogućavaju interakciju korisnika s bankovnim sustavom putem TV ekrana. Uz kanale e-bankarstva, rad također istražuje hardverske komponente bankarstva koje podržavaju ove kanale. Računala i računalna oprema igraju ključnu ulogu u bankarskom sektoru, pružajući snagu procesiranja, skladištenje podataka i izvršavanje bankarskih aplikacija. Komunikacijska oprema, kao što su ruteri, mrežni uređaji i VPN (Virtual Private Network) sustavi, osigurava pouzdanu i sigurnu vezu između korisnika i bankarskih sustava. Mediji za pohranu podataka, poput tvrdih diskova i sigurnosnih kopija, koriste se za čuvanje osjetljivih informacija i podataka o transakcijama.

Ostala tehnička oprema, kao što su POS (Point of Sale) uređaji, skeneri, tiskalice i čitači kartica, također su važne hardverske komponente u bankarstvu. POS uređaji se koriste za obradu kartičnih transakcija, dok skeneri omogućavaju digitalizaciju dokumenata kao što su potpisi i identifikacijski dokumenti. Tiskalice se koriste za ispis potvrda i izvještaja, dok čitači kartica omogućuju čitanje i verifikaciju bankovnih kartica. Ukratko, ovaj seminarski rad proučava pet kanala e-bankarstva (bankomati i interaktivni kiosci, telefonsko bankarstvo, online bankarstvo, mobilno bankarstvo i TV bankarstvo) te pripadajuće hardverske komponente koje podržavaju ove kanale. Razumijevanje tih kanala i hardverskih komponenti ključno je za razvoj i upravljanje modernim bankarskim sustavima te pružanje sigurnih i učinkovitih e-bankarskih usluga korisnicima.

2. Teorijska podloga i prethodna istraživanja

2.1. Ciljevi istraživanja

U radu je postavljeno nekoliko ciljeva istraživanja:

Prvi cilj ovog istraživanja je provesti analizu različitih kanala e-bankarstva koji se koriste u bankarskom sektoru. To uključuje internetsko bankarstvo, mobilno bankarstvo, telefonsko bankarstvo, TV bankarstvo i bankomate. Cilj je istražiti njihove karakteristike, funkcionalnosti, prednosti i nedostatke te njihovu ulogu u pružanju različitih bankarskih usluga.

Drugi cilj istraživanja je istražiti kako različite hardverske komponente utječu na efikasnost i sigurnost kanala e-bankarstva. Fokus je na POS uređajima, pametnim telefonima, karticama s mikročipom i biometrijskim uređajima. Cilj je proučiti njihove funkcionalnosti, pouzdanost i doprinos sigurnosti bankarskih transakcija.

Treći cilj istraživanja usmjeren je na sigurnosne aspekte kanala e-bankarstva. Istražit će se sigurnosne mjere koje su implementirane kako bi se osigurala autentičnost korisnika, zaštitila privatnost podataka i spriječile prijevare. Posebna pažnja posvećena je ulozi hardverskih komponenti u osiguravanju sigurnosti tijekom bankarskih transakcija.

Identifikacija i analiza inovacija u području e-bankarstva i hardverskih komponenti je četvrti cilj istraživanja.. Istražit su se nove tehnologije koje se koriste u ovom području, poput biometrije, blockchain tehnologije ili umjetne inteligencije, te njihovu ulogu u poboljšanju efikasnosti, sigurnosti i korisničkog iskustva.

Konačno, cilj je ovog rada pružiti smjernice i preporuke za daljnji razvoj e-bankarstva. Uzimajući u obzir rezultate istraživanja, želja je identificirati ključne korake i strategije koje bankarske institucije i korisnici mogu poduzeti kako bi uspješno iskoristili prednosti kanala e-bankarstva i hardverskih komponenti.

2.2. Metodologija rada

Kroz metodologiju rada zaokružiti će se svi načini i oblici istraživanja korišteni u ovom radu. Točnije navest će se predmet istraživanja, korištene metode i izvori prikupljenih podataka. Nadalje, kroz ovaj će se dio iznijeti pretpostavke, ideje te neke ključne hipoteze vezane za kanale e-bankarstva i njihovu primjenu. Prilikom izrade ovoga rada korištene su sljedeće

metode: induktivna i deduktivna metoda, metoda analize i sinteze, metoda deskripcije (opisna metoda), anketiranje, te naposljetku metoda kompilacije kako bi se prikupljeni podaci spojili u smislenu cjelinu. Tema rada je aktualna i široko primjenjiva, sukladno tome dostupni su i mnogi izvori. Rad se temelji na sekundarnim izvorima podataka, odnosno knjige, radovi i znanstveni članci, a koje slijede relevantni internetski izvori. Predmet istraživanja ovog rada su kanali e-bankarstva i hardverske komponente u bankarstvu. Elementi istraživanja koje ovaj rad obuhvaća su: pet glavnih kanala e-bankarstva i hardverske komponente koje omogućavaju uspješno provođenje bankarskih zadataka i nesmetan promet kanala e-bankarstva. Također ovaj rad obuhvaća primjere dobre prakse u poslovanju i daje uvid u ono što se danas koristi, a isto tako daje smjernice i preporuke za budući razvoj e-bankarstva.

2.3. Transformacija bankarstva kroz povijest

Bankarstvo je doživjelo značajnu transformaciju kroz povijest, posebno s razvojem kanala e-bankarstva i integracijom hardverskih komponenti. Tradicionalno bankarstvo bilo je usmjereno na fizičke poslovnice i transakcije koje zahtijevaju prisutnost korisnika i bankovnih službenika. Međutim, s napretkom tehnologije, digitalizacija bankarskog sektora postala je neizbježna. Prema Cointelegraphu (2023) uvođenje kanala e-bankarstva započelo je s internetskim bankarstvom. Internetsko bankarstvo omogućilo je korisnicima pristup bankarskim uslugama putem interneta, omogućujući im pregled stanja računa, prijenose sredstava, plaćanja računa i druge financijske aktivnosti. Ovaj kanal je osigurao korisnicima praktičnost i fleksibilnost, smanjujući potrebu za posjetom fizičkoj poslovnici. Slijedila je transformacija bankarstva kroz integraciju mobilnih uređaja. Mobilno bankarstvo je postalo sve popularnije među korisnicima (Birovčec, 2021). Aplikacije mobilnog bankarstva omogućile su korisnicima pristup bankarskim uslugama putem pametnih telefona i tableta. Ovaj kanal je omogućio korisnicima obavljanje bankarskih transakcija u pokretu, uz dodatne značajke poput skeniranja čekova i upravljanja karticama. Nadalje, integracija hardverskih komponenti, kao što su POS uređaji, kartice s mikročipom i biometrijski uređaji, donijela je dodatnu sigurnost i autentičnost bankarskim transakcijama. Boban i Perišić (2015) istraživali su primjenu biometrije u bankarskom sektoru, uključujući autentifikaciju otiskom prsta i prepoznavanje lica. Autori zaključuju kako hardverski elementi pružaju sigurnost, pouzdanost i zaštitu podataka korisnika, osiguravajući povjerenje u kanale e-bankarstva. Digitalizacija bankarstva predstavlja ključni trend u bankarskoj industriji koji je značajno promijenio način na koji se

pružaju bankarske usluge i interakcija između banaka i korisnika. Uvođenje digitalnih kanala i tehnologija u bankarski sektor ima brojne pozitivne učinke i transformira način poslovanja. Jedan od najvećih utjecaja digitalizacije bankarstva je povećanje pristupačnosti i praktičnosti bankarskih usluga za korisnike. Korisnici više nisu ograničeni na fizičko posjećivanje poslovnica ili radno vrijeme banci. Umjesto toga, mogu pristupiti svojim računima i obavljati transakcije putem interneta ili mobilnih aplikacija u bilo koje vrijeme i s bilo kojeg mjesta. To pruža veću fleksibilnost i olakšava upravljanje financijama. Osim toga, digitalizacija bankarstva omogućuje brže i učinkovitije transakcije. Umjesto dugotrajnih postupaka u fizičkim poslovnicama, digitalni kanali omogućuju trenutačno prijenos sredstava, plaćanja računa i ostale bankarske aktivnosti. To rezultira većom efikasnošću i smanjenjem vremena potrebnog za obavljanje financijskih operacija. Prema Rončeviću (2006), digitalizacija također potiče inovaciju i razvoj novih bankarskih usluga i proizvoda. Bankarske institucije mogu implementirati nove tehnologije poput umjetne inteligencije, strojnog učenja i blockchaina kako bi poboljšale personalizaciju usluga, analitiku podataka, prevenciju prijevara i druge aspekte bankarskog poslovanja. To omogućuje stvaranje novih vrijednosti za korisnike i otvara put za razvoj novih poslovnih modela. Utjecaj digitalizacije bankarstva proteže se i na samu bankarsku industriju. Banke su suočene s potrebom prilagodbe na digitalnu transformaciju kako bi ostale konkurentne. To zahtijeva ulaganje u tehnologiju, obuku osoblja i usklađivanje sa zakonodavstvom i sigurnosnim standardima. Također se otvaraju nove mogućnosti suradnje s tehnološkim startupima i fintech tvrtkama koje pružaju inovativna rješenja za bankarske usluge. U konačnici, digitalizacija bankarstva ima pozitivan utjecaj na korisnike, banke i cjelokupnu ekonomiju (Dragičević, 2020). Pruža veću dostupnost, praktičnost i učinkovitost bankarskih usluga te potiče inovaciju i razvoj novih poslovnih modela u industriji. Bankarstvo se kontinuirano razvija i prilagođava novim trendovima i inovacijama kako bi zadovoljile promjenjive potrebe korisnika i iskoristile prednosti tehnologije. U nastavku su navedeni neki od glavnih trendova i inovacija koji oblikuju suvremeno bankarstvo kao što su Fintech tvrtke, Mobilno bankarstvo, Digitalni novčanici, Biometrija u bankarstvu i sl. Fintech tvrtke predstavljaju ključnu inovaciju u bankarskom sektoru. Koriste napredne tehnologije poput blockchaina, umjetne inteligencije, strojnog učenja i velikih podataka kako bi pružile inovativne bankarske usluge. Ove tvrtke često nude alternativne načine plaćanja, digitalne novčanike, kreditiranje temeljeno na podacima i druge financijske usluge koje pružaju brzinu, jednostavnost i pristupačnost Mobilno bankarstvo postala je neizostavan dio suvremenog

bankarstva. Korisnici mogu jednostavno pristupiti svojim računima, obavljati transakcije, provjeravati stanje i upravljati financijama putem svojih pametnih telefona. Mobilno bankarstvo omogućuje personalizirano iskustvo, brze transakcije i funkcionalnosti poput skeniranja čekova i plaćanja putem mobilnih uređaja. Digitalni novčanici ili e-novčanici postaju sve popularniji način plaćanja. Ovi elektronički novčanici omogućuju korisnicima pohranu, upravljanje i sigurno plaćanje putem mobilnih uređaja. Omogućuju brze i jednostavne transakcije bez potrebe za fizičkim novcem ili karticama. Korištenje biometrijskih podataka kao metode autentifikacije postaje sve raširenije u bankarstvu. Otisak prsta, prepoznavanje lica i skeniranje rožnice koriste se kao sigurnosne metode za autentifikaciju korisnika prilikom pristupa računima i obavljanja transakcija. Ova tehnologija osigurava visoku razinu sigurnosti i sprječava prijevare. Bankarske institucije sve više koriste chatbotove i umjetnu inteligenciju za pružanje korisničke podrške i poboljšanje korisničkog iskustva. Chatbotovi omogućuju korisnicima brzi pristup informacijama, odgovore na pitanja i rješavanje problema, dok umjetna inteligencija analizira podatke i pruža personalizirane preporuke korisnicima. Ovi trendovi i inovacije prema mijenjaju način na koji korisnici pristupaju bankarskim uslugama i kako banke pružaju te usluge (Money gate, 2022). Sve veća digitalizacija, automatizacija i personalizacija transformiraju bankarsko iskustvo i otvaraju nove mogućnosti za inovacije u industriji.

2.4. Koncept e-bankarstva

E-bankarstvo predstavlja suvremeni pristup pružanju bankarskih usluga putem elektroničkih kanala, što omogućuje korisnicima brz i praktičan pristup financijskim uslugama. Ova vrsta bankarstva integrira tehnološke inovacije kako bi se korisnicima omogućilo obavljanje bankarskih transakcija putem interneta, mobilnih uređaja, telefona i drugih elektroničkih sredstava. Kroz razvoj e-bankarstva, bankarski sektor kontinuirano transformira na globalnoj razini, nudeći širok spektar bankarskih usluga koje su prilagođene suvremenim zahtjevima i preferencijama korisnika.

2.5. Kanali e-bankarstva

Kanali e-bankarstva predstavljaju različite elektroničke platforme putem kojih se korisnicima pružaju bankarske usluge. Neki od najčešće korištenih kanala e-bankarstva uključuju internetsko bankarstvo, mobilno bankarstvo, telefonsko bankarstvo, TV bankarstvo i

bankomate. Internetsko bankarstvo omogućuje korisnicima pristup bankarskim uslugama putem web stranica ili aplikacija, dok mobilno bankarstvo omogućuje pristup putem mobilnih uređaja poput pametnih telefona i tableta. Telefonsko bankarstvo koristi interaktivne glasovne odgovore ili kontakt s agentima putem telefonskih poziva za pružanje bankarskih usluga. TV bankarstvo omogućuje korisnicima pristup bankarskim uslugama putem televizora i daljinskog upravljača, dok se bankomati koriste za obavljanje gotovinskih transakcija i drugih bankarskih usluga.

2.5.1. Internetsko bankarstvo

Internetsko bankarstvo, poznato i kao online bankarstvo, oblik je bankarstva koji upotpunjuje i obnavlja svoj tradicionalni koncept elektroničkim putem pristupa Internetu (Economy-pedia, 2021). Pretpostavlja mogućnost obavljanja višestrukih bankarskih operacija bez potrebe za fizičkom poslovnicom. To uključuje upravljanje računima, provjeru stanja, prijenos sredstava, plaćanje računa, postavljanje uplata i drugih financijskih transakcija. Korisnici mogu pristupiti internetskom bankarstvu putem web stranice banke ili mobilne aplikacije. Internetsko bankarstvo pruža korisnicima brojne mogućnosti i usluge, uključujući:

- Pregled stanja računa: Korisnici mogu provjeriti stanje svojih bankovnih računa, uključujući dostupni saldo, prikaz transakcija i detalje o izvratku računa. To omogućuje korisnicima praćenje i upravljanje svojim financijama.
- Prijenos sredstava: Korisnici mogu izvršiti prijenos sredstava između vlastitih računa ili na račune drugih korisnika unutar iste banke ili čak izvan nje. To uključuje prijenos novca na račune kreditora, plaćanje računa ili slanje novca obitelji i prijateljima.
- Plaćanje računa: Internetsko bankarstvo omogućuje korisnicima plaćanje raznih računa putem elektroničkih prijenosa. To može uključivati plaćanje računa za komunalije (struja, voda, plin), telefonske račune, internet usluge, kreditne kartice, kredite i druge obveze.
- Upravljanje financijama: Korisnici mogu pratiti i upravljati svojim financijama putem internetskog bankarstva. To uključuje postavljanje budžeta, praćenje troškova, pregledavanje statističkih podataka o financijskim transakcijama i generiranje izvještaja o financijskom statusu.

- Otvaranje računa i zahtjevi za uslugama: Putem internetskog bankarstva korisnici mogu otvoriti nove bankovne račune, aplicirati za kreditne proizvode ili usluge kao što su kreditne kartice, krediti ili štedni računi. Ovi zahtjevi mogu se podnijeti online, što olakšava proces i štedi vrijeme korisnicima.

Važno je napomenuti da internetsko bankarstvo obično zahtijeva sigurnosne mjere kako bi se osigurala privatnost i zaštita podataka korisnika. To uključuje upotrebu sigurnosnih protokola kao što su SSL (Secure Socket Layer) enkripcija, autentifikacija korisnika putem korisničkih imena i lozinki te često i dodatne sigurnosne metode poput tokena ili jednokratnih šifri.

2.5.2. Mobilno bankarstvo

Mobilno bankarstvo omogućuje korisnicima pristup bankarskim uslugama putem mobilnih uređaja poput pametnih telefona ili tableta (Investopedia, 2020). S razvojem pametnih telefona, razvijene su mobilne aplikacije koje omogućuju korisnicima pristup bankovnim računima i obavljanje bankarskih aktivnosti putem svojih mobilnih uređaja. Ove aplikacije često imaju intuitivno sučelje, a korisnici mogu obavljati transakcije, pregledavati račune, plaćati račune i pristupati drugim bankarskim uslugama putem mobilnih telefona. Putem mobilne bankarske aplikacije, korisnici mogu obavljati transakcije, provjeravati stanje računa, plaćati račune, preuzimati izvode i koristiti druge bankarske usluge. Mobilno bankarstvo često nudi dodatne funkcionalnosti kao što su skeniranje računa, prijenos sredstava putem mobilnog broja ili QR koda te personalizacija obavijesti o financijskim aktivnostima. Mobilno bankarstvo pruža korisnicima fleksibilnost, praktičnost i brzinu pristupa bankarskim uslugama, omogućujući im da obavljaju financijske transakcije bilo gdje i bilo kada. . Uza sve navedeno još je mnogo prostora u kojem bi se mobilno bankarstvo moglo razvijati. Neki od tih smjerova su bez kartični pristup bankomatima, planiranje budžeta i potrošnje, biometrija, glasovno plaćanje, tehnologija blockchain-a, financijska edukacija i umjetna inteligencija (Crowdbotics, 2023).

2.5.3. Telefonsko bankarstvo

Telefonsko bankarstvo se odnosi na korištenje telefona za pristup bankarskim uslugama i obavljanje bankarskih transakcija (Law Insider, 2023). Ovaj kanal e-bankarstva omogućuje korisnicima da koriste telefonske usluge kako bi pristupili svojim bankovnim računima i obavili razne bankarske aktivnosti. Telefonsko bankarstvo može se odvijati putem različitih telefonskih tehnologija i platformi, uključujući:

- Automatizirani glasovni odgovor (Interactive Voice Response - IVR): Korisnici mogu koristiti telefonski broj ili specifičnu bankarsku liniju kako bi pristupili sustavu IVR-a. Ovaj sustav omogućuje korisnicima da obavljaju određene bankarske aktivnosti, poput provjere stanja računa, prijenosa sredstava, plaćanja računa i slanja upita, koristeći glasovne naredbe i tipke na telefonu.
- Korisnički agenti i telefonska podrška: Telefonsko bankarstvo također uključuje usluge korisničkih agenata i telefonske podrške koje korisnicima pružaju informacije, pomažu u rješavanju pitanja i pružaju podršku u vezi s bankarskim uslugama. Korisnici mogu razgovarati s bankarskim stručnjacima i dobiti personaliziranu pomoć putem telefona.

Telefonsko bankarstvo pruža korisnicima jednostavan način za upravljanje njihovim bankovnim računima i obavljanje financijskih transakcija putem telefona. To je posebno korisno u situacijama kada korisnici nemaju pristup internetu ili nemaju pametni telefon.

2.5.4. TV bankarstvo

TV bankarstvo, poznato i kao televizijsko bankarstvo, odnosi se na pružanje bankarskih usluga putem televizijskog medija (ABC China, 2022). Ovaj kanal e-bankarstva omogućuje korisnicima da pristupe bankovnim uslugama i obavljaju transakcije putem televizora. TV bankarstvo obično uključuje korištenje posebnih televizijskih aplikacija, interaktivnih kanala ili set-top box uređaja koji se povezuju s televizorom i omogućuju korisnicima da pristupe svojim bankovnim računima. Neke od karakteristika TV bankarstva uključuju:

- Pregledavanje stanja računa: Korisnici mogu provjeriti saldo i transakcije na svojim bankovnim računima putem televizora.
- Plaćanje računa: TV bankarstvo omogućuje korisnicima da plaćaju račune putem televizora. To uključuje upisivanje podataka o računu i izvršavanje plaćanja.
- Prijenos sredstava: Korisnici mogu obavljati prijenose novca između svojih bankovnih računa, kao i na račune drugih korisnika, putem televizora.
- Financijske informacije: TV bankarstvo može pružiti korisnicima pristup financijskim informacijama poput tečajeva valuta, dionica i drugih relevantnih tržišnih podataka.
- Korisnička podrška: TV bankarstvo može pružati korisničku podršku putem telefona ili čet usluga koje se prikazuju na televizoru.

TV bankarstvo obično koristi tehnologiju poput interaktivne televizije, daljinskog upravljača i dodatnih uređaja za povezivanje s bankovnim sustavom. Ova vrsta bankarstva pruža korisnicima dodatnu mogućnost pristupa bankovnim uslugama i omogućuje im da obavljaju transakcije iz udobnosti svog doma koristeći svoj televizor.

2.5.5. Bankomati

Bankomati, također poznati kao bankovni automat ili ATM (Automated Teller Machine), su samostalni elektronički uređaji koji omogućuju korisnicima obavljanje određenih bankarskih transakcija bez potrebe za posjetom fizičkoj poslovnici banke. Oni su široko rasprostranjeni i dostupni na mnogim lokacijama, uključujući bankovne poslovnice, trgovine, benzinske postaje i druga javna mjesta. (Urban Money, 2023) Bankomati pružaju korisnicima mogućnost sljedećih usluga:

- Podizanje gotovine: Korisnici mogu podići gotovinu s bankovog računa pomoću bankomata. Unoseći svoju debitnu ili kreditnu karticu, zajedno s odgovarajućom PIN šifrom (Personal Identification Number), korisnik može odabrati željeni iznos gotovine koji želi podići.
- Provjera stanja računa: Bankomati omogućuju korisnicima provjeru stanja njihovih bankovnih računa. Nakon što unesu karticu i PIN, mogu dobiti informacije o preostalom stanju na računu, detalje o transakcijama ili ispis izvoda.
- Prijenos sredstava: Bankomati omogućuju korisnicima prijenos sredstava između različitih bankovnih računa. To može uključivati prijenos novca na vlastiti račun ili račun drugog korisnika unutar iste banke.
- Uplata gotovine: Neki bankomati omogućuju korisnicima da uplate gotovinu na svoje bankovne račune. To je posebno korisno kada korisnik želi uplatiti novac na račun izvan radnog vremena banke ili izvan poslovnice.
- Plaćanje računa: Određeni bankomati omogućuju korisnicima plaćanje računa, kao što su računi za komunalije (struja, voda, plin), telefonski računi ili računi za kreditne kartice. Korisnici mogu unijeti potrebne podatke i izvršiti plaćanje putem bankomata.

Bankomati su obično opremljeni zaslonom osjetljivim na dodir (touch screen) ili tipkovnicom, što omogućuje korisnicima interakciju s uređajem. Također, bankomati su opremljeni

sigurnosnim mjerama kao što su kamere za nadzor i enkripcija podataka, kako bi se osigurala sigurnost korisničkih transakcija.

2.5.4.1. Zaštita i sigurnost u bankomatu

Zaštita bankomata igra ključnu ulogu u osiguravanju sigurnosti korisnika i financijskih podataka. Postoje različite vrste i aspekti zaštite bankomata kao što su: (UCA EDU, 2023) :

Fizička sigurnost: Bankomati su čvrsto izgrađeni i opremljeni sigurnosnim mjerama kako bi se spriječilo fizičko oštećenje ili neovlašten pristup uređaju. To može uključivati jaku metalnu konstrukciju, sigurnosne brave, alarme protiv provale i video nadzor.

Zaštita protiv skimminga: Skimming je tehnika kojom se neovlašteno prikupljaju podaci s bankovnih kartica. Bankomati su opremljeni zaštitnim mjerama kako bi se otkrili i spriječili skimming uređaji. To uključuje upotrebu enkriptiranih kartičnih čitača, redovito provjeravanje bankomata radi otkrivanja nepravilnosti i postavljanje zaštitnih uređaja poput anti-skimming naprava (ATM Security, 2023).

Zaštita PIN-a: PIN (Personal Identification Number) koristi se za autentifikaciju korisnika prilikom uporabe bankomata. Važno je educirati korisnike o važnosti čuvanja PIN-a i osiguravanju da nitko ne promatra unos PIN-a prilikom transakcija.

Redovito održavanje: Bankomati se redovito održavaju kako bi se osigurala njihova pravilna funkcionalnost i sigurnost. To uključuje provjeru i čišćenje uređaja, ažuriranje sigurnosnog softvera i hardvera, te provjeru svih sigurnosnih mehanizama. **Praćenje aktivnosti:** Bankomati su često opremljeni sustavima za praćenje aktivnosti, uključujući video nadzor i praćenje promjena u okolini bankomata. Ovo pomaže u otkrivanju sumnjivih aktivnosti ili pokušaja neovlaštenog pristupa uređaju.

Suradnja s lokalnim vlastima: Banke često surađuju s lokalnim vlastima, sigurnosnim službama i financijskim institucijama kako bi razmijenile informacije o sigurnosnim prijetnjama, oblicima prijevara ili napada na bankomate te poduzimale potrebne mjere zaštite. Važno je da banke redovito nadgledaju sigurnosne standarde i provode kontinuirano ažuriranje sigurnosnih mjera kako bi osigurale sigurnost bankomata i zaštitile interese svojih korisnika

2.5.5. Interaktivni kiosci

Interaktivni kiosci u bankarstvu su posebni samoposlužni uređaji smješteni u bankovnim poslovnica ili drugim javnim prostorima, koji omogućuju korisnicima obavljanje različitih

bankarskih aktivnosti. Oni kombiniraju hardverske komponente poput zaslona osjetljivog na dodir, tipkovnice i skenera s bankarskim softverom radi pružanja intuitivnog korisničkog iskustva. (Info Kiosk, 2023). Kroz interaktivne kioske, korisnici mogu obavljati razne transakcije, kao što su provjera stanja računa, uplata i isplata gotovine, prijenos sredstava, plaćanje računa, ispis izvoda i drugo. Također mogu pristupiti informacijama o proizvodima i uslugama banke, poput kredita, štednih računa ili osiguranja, te dobiti korisne savjete i smjernice. Interaktivni kiosci pružaju korisnicima mogućnost brzog i jednostavnog pristupa bankarskim uslugama bez potrebe za odlaskom u banku i interakcijom s bankarskim osobljem. Ovi kiosci često podržavaju različite jezike i omogućuju personalizirane opcije za korisnike, prilagođene njihovim potrebama.

2.6. Hardverske komponente

Hardverske komponente igraju ključnu ulogu u održavanju kanala e-bankarstva. POS (Point of Sale) uređaji, pametni telefoni, kartice s mikročipom i biometrijski uređaji su neki od ključnih hardverskih elemenata koji pružaju sigurnost, autentičnost i pouzdanost u bankarskim transakcijama kaže (Law Insider, 2023). POS uređaji se koriste za obradu platnih kartica i omogućuju sigurne transakcije na prodajnim mjestima. Pametni telefoni pružaju mobilnost korisnicima i omogućuju pristup bankarskim uslugama putem aplikacija. Kartice s mikročipom koriste se za sigurnu pohranu i prijenos podataka tijekom bankarskih transakcija, dok se biometrijski uređaji koriste za autentifikaciju korisnika putem otiska prsta, prepoznavanja lica ili drugih biometrijskih karakteristika.

2.6.1. Uređaji za autorizaciju korisnika

U bankarstvu se koriste različiti uređaji za autorizaciju korisnika kako bi se osigurala sigurnost bankarskih transakcija i pristup korisničkim računima. Uređaji za autorizaciju korisnika u bankarstvu služe za osiguravanje identifikacije i autentifikacije korisnika kako bi se spriječili neovlašteni pristupi bankovnim računima i transakcijama. Glavna svrha ovih uređaja je pružiti sigurnost i zaštitu korisničkih podataka i financijskih sredstava. Prema (Stripe, 2022) neki od uobičajenih uređaja za autorizaciju korisnika koji se koriste u bankarstvu uključuju: Token, TAN tablice, display kartice, čitače kartica, USB stick s certifikatom, biometrijski uređaji i dr.

2.6.1.1. TAN tablica

TAN (*Transaction Authentication Number*) tablica je oblik autentifikacije koji se koristi u bankarstvu radi sigurnosti i autentifikacije prilikom obavljanja online transakcija (Investopedia, 2021). TAN tablica je popis jednokratnih autentifikacijskih brojeva koji se koriste kao dodatni sloj sigurnosti prilikom izvršavanja određenih transakcija putem internetskog bankarstva. Kada korisnik želi izvršiti transakciju putem internetskog bankarstva, sustav će tražiti unos odgovarajućeg TAN broja iz TAN tablice. TAN brojevi su unaprijed generirani i pohranjeni u TAN tablici koju je korisnik dobio od svoje banke. Svaki TAN broj može se koristiti samo jednom i vrijedi samo za određenu transakciju. Korisnik treba unijeti odgovarajući TAN broj koji se poklapa s transakcijom koju želi izvršiti. Upotreba TAN tablice osigurava dodatni sloj sigurnosti jer je svaki TAN broj jedinstven i može se koristiti samo jednom. To otežava zlonamjernim pojedincima da izvrše neovlaštene transakcije čak i ako imaju pristup korisničkim podacima. Važno je napomenuti da se s razvojem tehnologije i digitalnih sigurnosnih mjera, TAN tablica sve više zamjenjuje naprednijim metodama dvofaktorske autentifikacije, poput jednokratnih SMS kodova, mobilnih aplikacija ili sigurnosnih tokena. Ove metode pružaju veću sigurnost i praktičnost prilikom autentifikacije korisnika u internetskom bankarstvu.

2.6.1.2. Token

U kontekstu bankarstva i informacijske sigurnosti, token se odnosi na digitalni uređaj ili aplikaciju koji se koristi za generiranje jednokratnih ili dinamičkih autentifikacijskih kodova. Ti autentifikacijski kodovi se koriste kao dodatni sloj sigurnosti prilikom pristupa sustavima ili izvršavanja transakcija. Postoje različite vrste tokena koje se koriste u bankarstvu:

1. Hardverski token: To je fizički uređaj, poput USB uređaja ili pametne kartice, koji generira jednokratne autentifikacijske kodove. Korisnik pristupa tokenu putem odgovarajućeg sučelja (na primjer, USB priključak) i unosi generirani kod prilikom autentifikacije.
2. Softverski token: To je aplikacija koja se instalira na mobilnom uređaju (poput pametnog telefona) ili računalu korisnika. Softverski token generira jednokratne autentifikacijske kodove i prikazuje ih korisniku. Korisnik unosi generirani kod prilikom autentifikacije.

3. Mobilni token: Ovo je vrsta softverskog tokena koji je specifičan za mobilne uređaje. Mobilni token često koristi aplikaciju koja je instalirana na pametnom telefonu ili drugom mobilnom uređaju. Generirani autentifikacijski kodovi prikazuju se na mobilnom uređaju i korisnik ih unosi prilikom autentifikacije.

Tokeni se koriste za autentifikaciju korisnika kako bi se osiguralo da samo ovlaštena osoba može pristupiti bankovnom računu ili izvršiti transakcije (Thales group, 2021). Kada korisnik želi pristupiti svojem računu ili izvršiti transakciju, sustav generira jednokratni autentifikacijski token koji se šalje korisniku. Taj token može biti u obliku broja, slova ili kombinacije jedinstvenih znakova. Korisnik zatim unosi taj autentifikacijski token u odgovarajuće polje prilikom prijave na svoj račun ili prilikom potvrde transakcije. Sustav provjerava valjanost unesenog autentifikacijskog tokena i omogućuje pristup računu ili izvršavanje transakcije samo ako je token ispravan i jednokratan. Ova vrsta jednokratnih tokena pruža dodatni sloj sigurnosti jer su tokeni vrijedni samo za jednu transakciju ili prijavu te su obično važeći samo unutar određenog vremenskog perioda. To znači da čak i ako netko neovlašteno pristupi korisničkim podacima, neće moći koristiti već iskorišteni token za pristup računu ili izvršavanje transakcija. Tokeni pružaju dodatni sloj sigurnosti jer autentifikacijski kodovi koje generiraju vrijede samo za jednu transakciju ili jednu prijavu i često imaju vremensko ograničenje. To otežava neovlaštenim osobama da pristupe korisničkim računima ili izvrše transakcije čak i ako imaju pristup korisničkim podacima. Uz to, postoje i drugi oblici tokena u bankarstvu koji se odnose na digitalne valute ili digitalne identifikatore koji se koriste za pristup bankovnim uslugama i transakcijama putem aplikacija ili mobilnih uređaja. Ti tokeni često koriste kriptografske metode kako bi osigurali sigurnu razmjenu podataka i autentifikaciju korisnika.

2.6.1.3. M-token

M-token odnosno Mobilni token je vrsta softverskog tokena koji se koristi za autentifikaciju korisnika prilikom pristupa bankovnim računima ili izvršavanja transakcija putem mobilnih uređaja (HPB, 2023). M-token se temelji na mobilnoj aplikaciji koja se instalira na pametnom telefonu ili drugom mobilnom uređaju korisnika. Nakon instalacije, mobilni token generira jednokratne autentifikacijske kodove koji se prikazuju na zaslonu mobilnog uređaja. Korisnik unosi generirani autentifikacijski kod prilikom prijave na bankovni račun ili prilikom potvrde transakcije. Prema Ingwbu (2023) prednosti m-tokena su:

Mobilnost: Korisnici mogu koristiti mobilni token s bilo kojeg mjesta putem svog mobilnog uređaja, pružajući fleksibilnost i praktičnost pristupa bankovnim uslugama.

Sigurnost: Jednokratni autentifikacijski kodovi generirani od strane mobilnog tokena pružaju dodatni sloj sigurnosti. Budući da su ti kodovi vrijedni samo za jednu transakciju ili prijavu, otežava se neovlaštenim osobama da pristupe korisničkim računima.

Jednostavnost uporabe: Mobilni tokeni obično imaju korisničko sučelje koje je intuitivno i jednostavno za korištenje, olakšavajući korisnicima generiranje i unos autentifikacijskih kodova.

Važno je napomenuti da se konkretni mobilni tokeni mogu razlikovati ovisno o banci i sustavu elektroničkog bankarstva. Korisnici bi trebali slijediti upute banke za instalaciju, konfiguriranje i korištenje m-tokena kako bi ispravno koristili ovu metodu autentifikacije.

2.6.1.4. Display kartica

Display kartica služi kao sredstvo za prijavu i autorizaciju transakcija putem usluga elektronskog bankarstva (Erste Banka, 2023). Display kartica u kontekstu bankarstva je vrsta bankovne kartice koja ima ugrađeni digitalni zaslon. Taj zaslon omogućuje korisniku da vidi dinamičke informacije kao što su generirani jednokratni autentifikacijski kodovi ili informacije o transakciji. Display kartice često se koriste za dodatnu sigurnost prilikom autentifikacije korisnika ili potvrde transakcija. Kada korisnik želi pristupiti bankovnom računu ili izvršiti transakciju, kartica generira jednokratni autentifikacijski kod koji se prikazuje na zaslonu kartice. Korisnik taj kod zatim unosi prilikom prijave ili potvrde transakcije. Prednosti korištenja display kartica uključuju:

Sigurnost: Jednokratni autentifikacijski kodovi generirani na zaslonu kartice pružaju dodatni sloj sigurnosti. Budući da su ti kodovi vrijedni samo za jednu transakciju ili prijavu, otežava se neovlaštenim osobama da pristupe korisničkim računima.

Praktičnost: Zaslon na kartici omogućuje korisnicima da odmah vide generirane kodove ili druge relevantne informacije. Nema potrebe za posebnim uređajem ili aplikacijom za prikazivanje autentifikacijskih kodova.

Jednostavnost uporabe: Korisnici jednostavno pogledaju zaslon kartice kako bi vidjeli generirane kodove ili druge informacije. Nema potrebe za pisanjem ili unošenjem dodatnih kodova s drugih uređaja.

Važno je napomenuti da se konkretni mehanizmi i implementacija display kartica mogu razlikovati ovisno o banci i sustavu elektroničkog bankarstva. Korisnici bi trebali slijediti upute banke za korištenje display kartica kako bi ispravno koristili ovu metodu autentifikacije ili prikaza informacija.

2.6.1.5. Čitač kartica

Čitač kartica u sklopu bankarstva je uređaj koji se koristi za čitanje informacija s bankovnih kartica. To je obično vanjski uređaj koji se povezuje s računalom ili drugim terminalom putem USB ili drugog sučelja. Čitač kartica ima utor ili otvor u koji se umetne bankovna kartica. Kada se kartica umetne u čitač, uređaj čita podatke s magnetne trake ili mikročipa kartice. Nakon čitanja, informacije se prenose na povezani uređaj, kao što je računalo ili POS terminal, koji zatim obrađuje te podatke za potrebne transakcije ili autentifikaciju korisnika (NatWest, 2023). U bankarstvu, čitači kartica se često koriste za sljedeće svrhe:

- Autentifikacija korisnika: Korisnici umetnu svoju bankovnu karticu u čitač kako bi se autentificirali prilikom pristupa internetskom bankarstvu ili izvršavanju sigurnih transakcija.
- Izvršavanje transakcija: Čitači kartica se koriste u POS terminalima ili blagajnama kako bi se čitali podaci s bankovne kartice i izvršile financijske transakcije.
- Verifikacija kartica: U bankama i drugim financijskim institucijama, čitači kartica se koriste za verifikaciju kartica prilikom izdavanja novih ili zamjene postojećih kartica.

Važno je reći da se čitači kartica mogu razlikovati po vrsti i tehnologiji koju podržavaju. Primjeri uključuju čitače magnetnih traka, čitače mikročipova (EMV), čitače NFC tehnologije i drugo. Ovisno o bankovnom sustavu i propisima, specifičan tip čitača kartica može biti potreban za određene transakcije ili autentifikaciju.

2.6.1.6. USB stick s certifikatom

USB stick s certifikatom u sklopu bankarstva je uređaj koji sadrži digitalni certifikat koji se koristi za autentifikaciju i sigurnu razmjenu podataka u bankarskom okruženju. To je obično

USB uređaj male veličine koji se može povezati s računalom ili drugim terminalom putem USB priključka. Certifikat koji se nalazi na USB sticku je digitalni identifikacijski dokument koji potvrđuje identitet subjekta (npr. korisnika, banke) u elektroničkoj komunikaciji (Stack Exchange, 2016). Ovaj certifikat sadrži ključeve za kriptografske operacije, poput digitalnog potpisivanja i šifriranja, koji osiguravaju autentičnost, integritet i povjerljivost podataka. U bankarstvu, USB stick s certifikatom se često koristi za sljedeće svrhe:

- Digitalni potpis: Korisnici mogu koristiti USB stick s certifikatom za digitalno potpisivanje dokumenata, transakcija ili drugih elektroničkih poruka. Digitalni potpis pruža autentičnost i integritet potpisanog sadržaja, omogućujući primateljima da provjere identitet pošiljatelja i integritet poruke.
- Sigurna autentifikacija: USB stick s certifikatom se može koristiti za sigurnu autentifikaciju korisnika prilikom pristupa internetskom bankarstvu ili drugim sustavima koji zahtijevaju identifikaciju. Korisnik umetne USB stick u računalu i koristi certifikat za provjeru svojeg identiteta.
- Zaštita podataka: Certifikat na USB sticku se također može koristiti za šifriranje i dešifriranje podataka kako bi se osigurala povjerljivost prilikom razmjene osjetljivih informacija između banke i korisnika.

USB stickovi s certifikatima u bankarstvu osiguravaju sigurnost, pouzdanost i zaštitu privatnosti tijekom elektroničkih transakcija i komunikacije. Važno je da korisnici pravilno koriste i čuvaju USB stickove kako bi se spriječila zloupotreba i neovlašten pristup njihovim certifikatima.

2.6.1.7. Biometrijski uređaji za autorizaciju

Biometrijski uređaji za autorizaciju u sklopu bankarstva su tehnološki uređaji koji koriste biometrijske podatke za identifikaciju i autentifikaciju korisnika. Biometrija se odnosi na mjerenje i analizu fizičkih ili ponašajnih karakteristika pojedinca kako bi se potvrdio njegov identitet Boban i Perišić (2015). U bankarstvu, biometrijski uređaji se koriste za sljedeće svrhe:

- Identifikacija korisnika: Biometrijski uređaji koriste jedinstvene biološke karakteristike pojedinca, poput otiska prsta, prepoznavanja lica, skeniranja šarenice ili glasa, kako bi se identificirao korisnik prilikom pristupa bankovnom računu ili izvršavanja transakcija.

- Autorizacija korisnika: Nakon što je korisnik identificiran putem biometrijskih podataka, biometrijski uređaj se koristi za autentifikaciju korisnika i odobrenje pristupa bankarskim uslugama. To može uključivati dodatne korake, poput skeniranja otiska prsta za potvrdu identiteta prije izvršavanja financijskih transakcija.
- Poboljšanje sigurnosti: Biometrijski uređaji pružaju dodatni sloj sigurnosti u bankarstvu jer se biometrijski podaci teško krivotvore ili prenesu na neovlaštene osobe. To smanjuje rizik od neovlaštenog pristupa računima i potencijalne zloupotrebe bankarskih podataka.

Važno je istaknuti da se biometrijski uređaji mogu razlikovati u vrsti i tehnologiji koju podržavaju. Primjeri uključuju uređaje za skeniranje otiska prsta, kamere za prepoznavanje lica, uređaje za skeniranje šarenice, mikrofona za prepoznavanje glasa i drugo. Ovisno o bankovnom sustavu i sigurnosnim politikama, određeni tip biometrijskog uređaja može biti potreban za autentifikaciju korisnika i pristup bankarskim uslugama.

2.7. Sigurnost u e-bankarstvu

Sigurnost je ključni aspekt e-bankarstva, s obzirom na osjetljivost financijskih podataka i potrebu za pouzdanim autentifikacijskim mehanizmima. Implementacija sigurnosnih mjera i protokola od ključnog je značaja za zaštitu podataka korisnika, sprječavanje neovlaštenog pristupa i prijevara. Neki od sigurnosnih izazova s kojima se susreće e-bankarstvo uključuju zaštitu od krađe identiteta, sigurnu razmjenu podataka, prevenciju phishing napada i osiguranje privatnosti korisnika. Stalni napredak tehnologije i inovacije u sigurnosnim rješenjima ključni su faktori za održavanje sigurnog okruženja u e-bankarstvu. U sklopu bankarskog poslovanja primjenjuje se niz sigurnosnih mjera i tehnologija kako bi se zaštitili korisnici, financijski podaci i transakcije. Evo nekoliko ključnih vrsta sigurnosti koje se primjenjuju u bankarskom poslovanju (EM Bank, 2023):

- Sigurnost podataka: Bankarske institucije koriste napredne tehnike šifriranja podataka kako bi osigurale povjerljivost prilikom prijenosa i pohrane osjetljivih informacija. To uključuje šifriranje podataka prilikom prijenosa putem mreže i šifriranje podataka pohranjenih na serverima.
- Autentifikacija korisnika: Sigurnost se postiže kroz autentifikaciju korisnika prilikom pristupa bankovnom računu ili izvršavanja transakcija. Ovo može uključivati upotrebu

korisničkih identifikacija, lozinki, biometrijskih podataka (poput otiska prsta ili prepoznavanja lica) ili dodatnih sigurnosnih uređaja za autentifikaciju.

- Praćenje transakcija: Bankarske institucije imaju sustave za praćenje i analizu transakcija kako bi otkrile neobične ili sumnjive aktivnosti koje bi mogle ukazivati na prijevaru ili zloupotrebu računa. Ovi sustavi koriste algoritme i modele za otkrivanje nepravilnosti i prijevara.
- Fizička sigurnost: Bankarske institucije primjenjuju fizičke sigurnosne mjere kako bi zaštitile svoje prostorije i resurse. To uključuje upotrebu sigurnosnih sustava, video nadzora, pristupnih kontrola i zaštite od provale.
- Sigurnost mreže i IT infrastrukture: Bankarske institucije ulažu u sigurnost svoje mreže i IT infrastrukture kako bi se zaštitile od cyber napada i neovlaštenog pristupa. To uključuje korištenje vatrozida, antivirusnih programa, zaštite od zlonamjernog softvera, redovito ažuriranje softvera i praćenje najnovijih sigurnosnih smjernica i standarda.
- Sigurnost transakcija: Transakcije se osiguravaju kroz razne sigurnosne mehanizme, kao što su digitalni potpisi, jednokratne lozinke, SMS potvrde i tokeni. Ti mehanizmi osiguravaju autentičnost i integritet transakcija te sprječavaju neovlaštene promjene ili manipulacije podacima.
- Edukacija korisnika: Bankarske institucije pružaju edukaciju korisnicima o sigurnom korištenju kanala e-bankarstva. To uključuje upute o odgovornom rukovanju lozinkama, prepoznavanju phishing napada i sigurnom pristupu bankarskim računima putem javnih mreža.

Važno je da bankarske institucije redovito nadograđuju i prilagođavaju svoje sigurnosne mjere kako bi se nosile s rastućim prijetnjama i naprednim metodama napada. Također se kontinuirano educiraju korisnici kako bi bili svjesni sigurnosnih rizika i pridržavali se najboljih praksi zaštite svojih računa i financijskih podataka.

2.8. Pregled prethodnih istraživanja

U prethodnim istraživanjima, mnogi istraživači su se usredotočili na različite aspekte kanala e-bankarstva i hardverskih komponenti u bankarstvu. Navedeni radovi pružaju važan uvid u ove teme i doprinose razumijevanju njihove uloge, funkcionalnosti i izazova.

Birovčec (2021) proveo je istraživanje o preferencijama korisnika u pogledu kanala e-bankarstva. Njegova studija identificirala je ključne faktore koji utječu na izbor korisnika tehnologija poput internetskog bankarstva, mobilnog bankarstva i bankomata. Rezultati istraživanja ukazuju na važnost pružanja raznolikih i prilagođenih kanala kako bi se zadovoljile potrebe različitih korisnika. Boban i Perišić (2015) su istraživale implementaciju biometrijskih uređaja u bankarskom sektoru. Njihova studija je analizirala učinkovitost i prihvaćanje biometrijske autentifikacije korisnika putem otiska prsta i prepoznavanja lica. Rezultati ukazuju na visok stupanj sigurnosti i udobnosti koje biometrija može pružiti u bankarskim transakcijama. Parat (2015) u svom istraživanju usmjeren je na sigurnosne aspekte kanala e-bankarstva. Autor je identificirao glavne sigurnosne izazove poput zaštite od krađe identiteta, sigurne razmjene podataka i prevencije phishing napada. Rad je također analizirao primjenu sigurnosnih protokola i tehnologija koje se koriste u e-bankarstvu radi osiguranja pouzdanosti i sigurnosti transakcija. HPB je provela istraživanje pod nazivom: generacija Z o mobilnom bankarstvu u kojem su došli do zanimljivih predviđanja o tome kako će razvoj aplikacija mobilnog bankarstva napredovati u narednih tri do pet godina. Rezultati istraživanja govore o tome kako 38% ispitanika smatra da će mobilna plaćanja postati standard, 21% vjeruje da će glavni smjer biti digitalizacija valuta, 17% kaže da je to integracija mobilnog bankarstva s umjetnom inteligencijom, 11% studenata očekuje da će mobilno bankarstvo postati njihov osnovni financijski savjetnik, a 13% ispitanika kaže da će mBanking u potpunosti zamijeniti fizičke poslovnice.

2.9. Prednosti i izazovi kanala e-bankarstva

Kanali e-bankarstva imaju mnoge prednosti koje pružaju korisnicima i bankama. Kroz ove prednosti, kanali e-bankarstva omogućuju korisnicima brži, praktičniji i sigurniji pristup bankovnim uslugama te promiču digitalnu transformaciju bankarstva. U nastavku će biti navedeno nekoliko ključnih prednosti kanala e-bankarstva od strane (Banke & Biznis, 2018):

- **Praktičnost:** Kanali e-bankarstva omogućuju korisnicima da obavljaju bankovne transakcije i pristupaju svojim računima bilo kada i bilo gdje putem interneta ili mobilnih uređaja. Nema potrebe za odlaskom u banku ili čekanjem u redovima, što značajno štedi vrijeme i olakšava upravljanje financijama.

- Brzina: E-bankarstvo omogućuje brži prijenos sredstava i izvršavanje transakcija u usporedbi s tradicionalnim bankovnim metodama. Prijenos novca između računa, plaćanje računa ili slanje novca drugim korisnicima moguće je izvršiti u samo nekoliko trenutaka, čime se ubrzava proces financijskih transakcija.
- Dostupnost 24/7: Kanali e-bankarstva su dostupni 24 sata dnevno, 7 dana u tjednu. Korisnici imaju neprekidan pristup svojim financijskim informacijama i mogu obavljati transakcije u bilo koje vrijeme, što je posebno korisno za korisnike koji imaju različite vremenske zone ili imaju ograničeno radno vrijeme.
- Širok raspon usluga: Kanali e-bankarstva pružaju širok raspon bankovnih usluga. Korisnici mogu pregledavati stanje računa, provjeravati transakcijsku povijest, plaćati račune, upravljati kreditnim karticama, prijavljivati se za kredite i još mnogo toga, sve putem interneta ili mobilnih aplikacija.
- Niže transakcijske naknade: U mnogim slučajevima, transakcijske naknade za korištenje kanala e-bankarstva su niže u usporedbi s tradicionalnim bankovnim metodama. To može rezultirati uštedom korisnika i povećanjem njihove financijske efikasnosti.
- Sigurnost i privatnost: Kanali e-bankarstva pružaju visoku razinu sigurnosti i zaštite podataka. Kriptografija, višestupanjska autentifikacija, sigurnosni tokeni i drugi sigurnosni mehanizmi koriste se kako bi se osigurala sigurnost financijskih transakcija i zaštitila privatnost korisnika.
- Personalizacija i korisničko iskustvo: Kanali e-bankarstva omogućuju personalizirano korisničko iskustvo. Korisnici mogu prilagoditi postavke, preferencije i prioritetne funkcionalnosti sukladno svojim potrebama. Također, sustavi e-bankarstva koriste analitiku i podatkovne modele kako bi pružili personalizirane ponude i savjete korisnicima.

Unatoč mnogim prednostima, kanali e-bankarstva suočavaju se s nekim izazovima. Nadilaženje tih izazova zahtijeva kontinuirano ulaganje u tehnološki razvoj, sigurnosne mjere, obrazovanje korisnika i suradnju između banaka, regulatora i ostalih dionika u bankarskom sektoru. Glavni izazovi e-bankarstva su (HNB, 2019):

- Sigurnost podataka: Sigurnost podataka je ključna briga u e-bankarstvu. Napadi hakera, krađa identiteta i prijevare predstavljaju ozbiljnu prijetnju. Bankama je potrebno uložiti

značajne napore u implementaciju sigurnosnih mjera kako bi zaštitile povjerljivost i integritet podataka korisnika.

- Tehnički problemi: Tehnički problemi kao što su prekidi mreže, tehničke pogreške ili nedostupnost usluga mogu utjecati na funkcionalnost kanala e-bankarstva. To može frustrirati korisnike i smanjiti njihovo povjerenje u te kanale.
- Potreba za obrazovanjem korisnika: Mnogi korisnici možda nisu upoznati s mogućnostima i funkcionalnostima kanala e-bankarstva. Potrebno je educirati korisnike o tome kako ispravno koristiti te kanale, kako bi maksimalno iskoristili njihove prednosti i smanjili rizik od grešaka.
- Prilagodba korisničkim preferencijama: Svakom korisniku može biti potrebno vrijeme da se prilagodi korištenju kanala e-bankarstva, posebno ako su navikli na tradicionalne metode bankarstva. Bankama je važno pružiti korisničko iskustvo koje je intuitivno i jednostavno za korištenje kako bi potaknule korisnike na prihvaćanje i korištenje tih kanala.
- Sigurnost biometrijskih podataka: S razvojem biometrijskih tehnologija kao metode autentifikacije, bankama je potrebno osigurati visoku razinu sigurnosti biometrijskih podataka korisnika. Prikupljanje, pohrana i obrada biometrijskih podataka zahtijeva stroge sigurnosne mjere kako bi se spriječila zloupotreba ili neovlašteni pristup.
- Regulativni okvir: Kanali e-bankarstva podliježu brojnim regulatornim zahtjevima i propisima kako bi se osigurala zaštita korisnika i spriječila financijska zloupotreba. Bankama je potrebno pažljivo pratiti i pridržavati se tih regulacija kako bi osigurale usklađenost i zaštitile svoje korisnike.

4. Opis istraživanja i rezultati istraživanja

U ovom dijelu rada će se opisati primjena na konkretnim primjerima bankomata i interaktivnih kioska raznih banaka, primjeri telefonskog, online, Internet te mobilnog bankarstva kroz danas svima dostupne aplikacije te primjere TV bankarstva. Usporediti će se online bankarstvo na primjeru dvije hrvatske banke, a to su PBZ i Erste. Nakon toga pogledati ćemo rezultate anketnog istraživanja.

4.1. Primjeri bankomata i interaktivnih kioska

Bankomat kao važan dio svakodnevnice većine ljudi čini ga iznimno važnim kanalom bankarstva jer pomoću njega korisnici imaju direktan pristup svom novcu, odnosno onoj količini novca koja im se u tom trenutku nalazi na računu. Danas su bankomati iznimno geografsko rasprostranjeni kako bi bili što dostupniji svojim klijentima. Važno je napomenuti kako svaka banka ima svoj bankomat no u većini slučajeva to ne isključuje korisnike drugih banaka da ga koriste već se tada „naplati“ naknada za korištenje. Pojava te današnja široka dostupnost bankomata osigurava smanjenje gužvi te dugačkih redova u bankama.



Slika 1. - Primjer modernog bankomata banke "Barclays"

Izvor: Dreamstime (2023.)

Još jedan primjer olakšavanja te smanjivanja prometa fizičkim poslovnicama banaka je i interaktivni kiosk koji korisniku pruža razne informacije o stanju njegova računa te ostale važne informacije o njegovu računu. Danas se interaktivni kiosci vrlo često koriste i izvan banaka u raznu namjenu (primjerice u pošti, policiji). Razvoj tehnologije je omogućio širenje interaktivne kioske u razna poslovanja pa nije ni čudo što danas interaktivne kioske možemo naći u raznim poslovnicama te čak i ustanovama.



Slika 2. - primjer interaktivnog kioska

Izvor: Empire Digital Signs (2022.)

Iako nisu složeni kao bankomati, interaktivni kiosci olakšavaju ponajviše korisnicima jer im pruža bitne informacije te im služi kao brzi izvor informacija.

4.2. Telefonsko bankarstvo

Telefonsko bankarstvo kao kanal omogućuje direktnu komunikaciju klijenata te banke (zaposlenika banke), osnovno putem telefonskog poziva pomoću kojeg se održava kontakt te poslovi isto kao i u poslovnici banke fizičkim putem. Pojava telefonskog bankarstva je uvelike proširila te unaprijedila poslovanja brojnih banaka jer su ovime banke te njihove usluge postale više dostupnije nego inače. Mnogim klijentima odlazak u banku znači utrošiti dosta vremena u redu čekanja te se ovim putem ti redovi čekanja pokušavaju iskorijeniti te ubrzati proces komunikacije između klijenata i banke. Za primjer telefonskog bankarstva je uzeta usluge OTP banke.



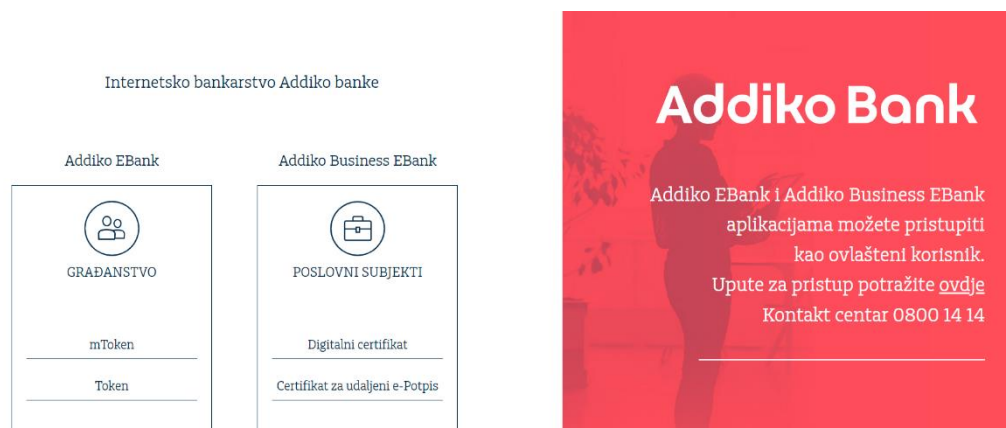
Slika 3. - primjer promidžbe telefonskog bankarstva OTP banke

Izvor: OTP banka (2022.)

OTP banka pružanjem usluge telefonskog bankarstva omogućuje svojim korisnicima pozivom na njihov broj razne mogućnosti, primjerice klijent OTP banke preko telefonskog bankarstva može izvršiti plaćanja u kunama, kupoprodaju deviza, uplatu rata aktivnih kredita, prijavu izgubljene ili oštećene kartice, ali i saznati informacije o stanju i prometu po računima, kreditima, punomoćima, jamstvima, oročenjima te ugovorenim trajnim nalogima. U sklopu telefonskog bankarstva, OTP banka nudi i usluge videorazgovora, chat-a ali i govornog automata čijim pozivom u bilo koje doba dana korisnik može provjeriti opće informacije o svome računu. Prioritet stalne dostupnosti usluga banke je na prvom mjestu kod telefonskog bankarstva te se i u mnogim drugim bankama razvija prema tom prioritetu.

4.3. Online (Internet) bankarstvo

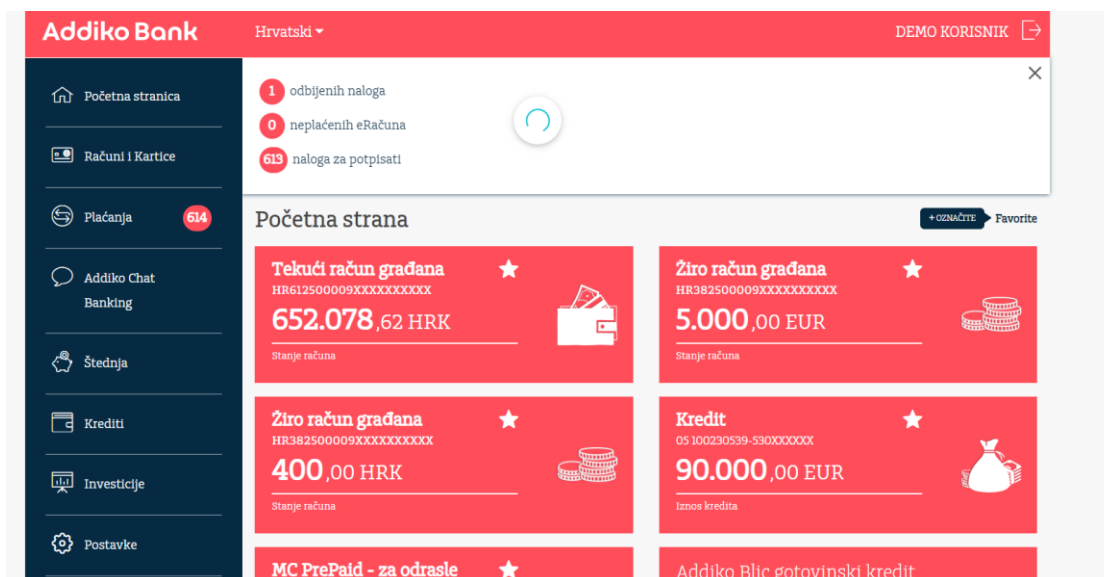
Danas jedan od najraširenijih kanala uz mobilno bankarstvo je i online odnosno Internet bankarstvo. Za objašnjenje primjera online bankarstva banaka je odabran primjer online bankarstva Addiko banke . Internet bankarstvo Addiko banke funkcioniра na način da klijent putem Internet aplikacije pristupi svome računu pomoću tokena koji mu banka daje pri izradi računa.



Slika 4. - primjer pristupa Internet bankarstvu putem tokena

Izvor: Addiko banka (2023.)

Pomoću tokena odnosno mTokena korisnik pristupljuje svome računu te mu se prikazuje sučelje u kojem mu se nude brojne mogućnosti vezane za njegov račun ali i bankarske radnje.



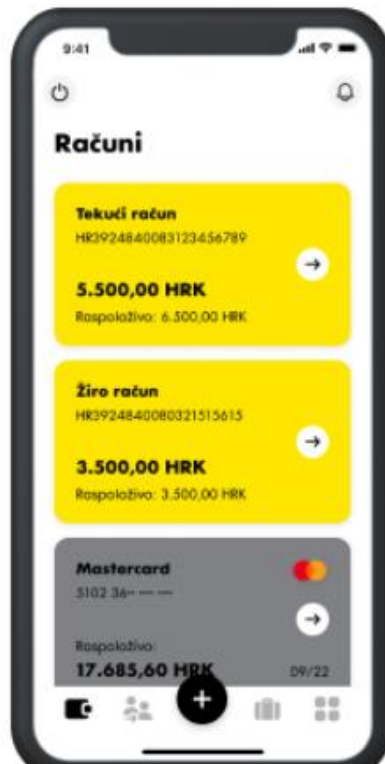
Slika 5. - primjer sučelja Internet bankarstva Addiko banke

Izvor: Addiko banka (2023.)

Pomoću sučelja korisnik izabire informacije ili čini razne uplate, provjerava stanje računa ili komunicira direktno sa bankom putem chata. Vrlo je važno da sučelje kvalitetno dizajnirano kako bi se klijent što lakše snalazio te da razvije pozitivno mišljenje kako o aplikaciji tako i o cijeloj banci.

4.4. Mobilno bankarstvo

Razvoj mobilnog bankarstva je ljudima dalo mogućnost pristupa informacija o svom računu te obavljanju raznih bankarskih poslova i to sve na svome mobitelu. Uvelike je doprinijelo razvoju ovog bankarstva i razvoj IT sektora koji svakim danom sve više i više unaprjeđuje ovo bankarstvo te je neupitno da će ovaj oblik bankarstva postati, ako već i nije, glavni oblik bankarstva 21. stoljeća. Kao i Internet bankarstvo, banke ovu uslugu naplaćuju korisniku na mjesečnoj bazi. Za primjer mobilnog bankarstva je uzeta „mojaRBA“ aplikacija Raiffeisen banke.



Slika 6. - primjer početnog zaslona "mojaRBA"

Izvor: RBA banka (2023.)

Aplikacije mobilnog bankarstva djeluju na skoro identičan način kao i kod Internet bankarstva. Kod mobilnog bankarstva su aplikacije posebno prilagođene za korištenje na mobitelu te čak

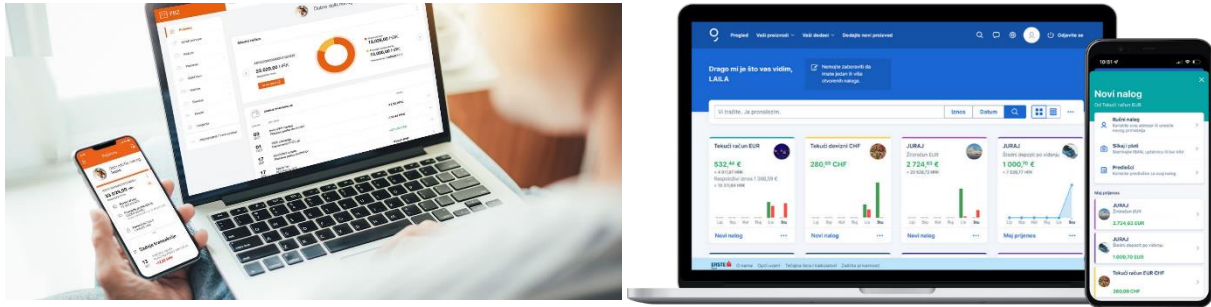
omogućavaju različite načine pristupa aplikaciji (recimo putem određenih biometrijskih metoda). Također aplikacija omogućava korisniku da promijeni redoslijed stavki kako bi sebi prilagodio cijelu aplikaciju. Visoka personalizacija je odlika ovakvog tipa aplikacije jer je važno da se korisnik neometano koristi aplikacijom kako bi što lakše ostvario bankarske radnje ili došao do njemu važnih informacija. Jedna od posebnih mogućnosti što ova aplikacija pruža je plaćanje putem foto naloga (odnosno plaćanje putem skeniranja QR koda). Korisna stvar kod aplikacija mobilnog bankarstva je što su sklonija češćim ažuriranjima što znači da su uvijek unaprjeđene najnovijom te najsigurnijom tehnologijom koja osigurava kako korisnikov račun, tako i njegove osobne informacije. Važno obilježje korištenja mobilnog bankarstva je da ono mora osiguravati sigurnost samog računa klijenta i da bi to uspjela banka mora učestalo ažurirati protokole te nove načine sigurnosti same aplikacije jer su mobilni uređaji vrlo često skloni većem riziku od povrede privatnosti podataka. S obzirom na važnost ove aplikacije, vrlo je bitno da klijent čuva svoj token odnosno pin koji mu je banka dala kojim pristupa aplikaciji jer je on direktni ulaz u njegov račun.

4.5. TV bankarstvo

Iako prema nekim istraživanjima na ovim prostorima TV bankarstvo nije u širokoj uporabi, u ostatku svijeta TV bankarstvo se smatra vrlo korisnim te važnim načinom pristupa svojim informacijama vezano uz banke, i to sve pomoću korištenja svoga televizora. U ovakav pristup se ponajviše investira u razvijenim zapadnim zemljama (SAD, Velika Britanija) te se smatra korisnom alternativom drugim vrstama kanala bankarstva jer klijent sve radnje čini pomoću svojeg televizora iz udobnosti svojeg doma. TV bankarstvo funkcionira na način da klijent pomoću aplikacije na svojem televizoru pristupi na isti način kao i kod mobilnog te Internet bankarstva. Funkcionira na istom principu te se zbog toga većina ljudi odluči za jednostavnije odnosno kompaktnije rješenje mobilnog bankarstva jer osjećaju da brže i jednostavnije mogu pristupiti putem svoga mobilnog uređaja ili osobnog računala. Trenutno u svijetu najveće napretke te ulaganja čine banke Barclays te HSBC koje vjeruju u razvoj TV bankarstva kao primarnog kanala e bankarstva.

4.6. Usporedba online bankarstva PBZ i Erste banke

Obje banke nude širok raspon bankarskih usluga, uključujući kredite, štednju, plaćanja, investicije i druge financijske proizvode. Uspoređivanjem njihovih ponuda možemo bolje razumjeti koje su usluge dostupne i koje najbolje odgovaraju vašim potrebama.



Slika 7. – slika prikazuje online sučelja PBZ i Erste banke

Izvor: PBZ i Erste banka (2023.)

Korisničko sučelje i funkcionalnost: U online bankarstvu, PBZ i Erste banka pružaju korisnicima pristup putem web preglednika. PBZ banka nudi jednostavno i pregledno sučelje koje omogućava korisnicima obavljanje raznih financijskih funkcija poput prijenosa i plaćanja. Erste banka također nudi korisničko sučelje prilagođeno različitim uređajima i omogućava pristup širokom rasponu bankarskih usluga.

Mobilna aplikacija: Objе banke imaju mobilne aplikacije koje omogućavaju korisnicima upravljanje financijama putem mobilnih uređaja. Mobilna aplikacija PBZ-a omogućava korisnicima da brzo izvršavaju transakcije, provjeravaju saldo i prate povijest transakcija. Erste banka pruža slične mogućnosti putem svoje mobilne aplikacije, s dodatkom značajki poput skeniranja računa i lakoće upravljanja karticama.

Funkcionalnosti i pristup uslugama: Online bankarstvo obje banke nudi širi raspon usluga u usporedbi s mobilnim bankarstvom. Putem online bankarstva, korisnici imaju pristup većem broju detaljnih izvješća, postavljanju trajnih naloga i drugim naprednim financijskim funkcijama. S druge strane, mobilno bankarstvo nudi veću praktičnost za brze transakcije i praćenje financija u pokretu.

Sigurnost i autentifikacija: Objе banke primjenjuju sigurnosne mjere kako bi zaštitile korisničke podatke i transakcije putem oba kanala. Kod mobilnog bankarstva PBZ, koriste se dodatne sigurnosne značajke kao što su biometrijska autentifikacija (otisak prsta ili prepoznavanje lica), no mora se voditi računa o tome da mobilni uređaj putem kojeg se pristupa

računu podržava takav oblik autentifikacije, kako bi se osiguralo da samo autorizirani korisnici mogu pristupiti aplikaciji.

4.6. Anketno istraživanje

Cilj ovog istraživanja je istražiti upotrebu kanala e-bankarstva i razumjeti važnost hardverskih komponenti u bankarskom sektoru. Prikupljanjem podataka o percepciji korisnika i njihovom iskustvu korištenja ovih kanala, te analizom uloge hardverskih komponenti u pružanju sigurne i praktične bankarske usluge, želi se dati uvid u trenutno stanje, prednosti i izazove povezane s e-bankarstvom. Ovo istraživanje ima potencijal pružiti korisne spoznaje bankama i donositeljima odluka u bankarskom sektoru kako bi unaprijedili svoje usluge i osigurali zadovoljstvo korisnika. Također može doprinijeti postojećem znanju o korištenju kanala e-bankarstva i ulozi hardverskih komponenti u pružanju sigurne i pouzdane bankarske usluge. U nastavku istraživanja koristit se anketni pristup kako bismo prikupili podatke od korisnika kanala e-bankarstva. Podaci su se analizirali s ciljem razumijevanja preferencija korisnika, njihovog zadovoljstva korištenjem e-bankarstva, percepcije sigurnosti i uloge hardverskih komponenti. Istraživanje je provedeno na uzorku od 40 ispitanika, ciljane skupne su studenti ekonomskog fakulteta u Osijeku. Pitanja koja su postavljena tokom istraživanja su sljedeća:

1. Koliko imate godina?
2. Koji kanal e-bankarstva najčešće koristite za obavljanje bankarskih transakcija?
3. Kako biste ocijenili svoje zadovoljstvo korištenjem internetskog bankarstva na skali od 1 do 5?
4. Koje vrste hardverskih komponenti koristite za dodatnu sigurnost prilikom korištenja e-bankarstva (npr. sigurnosni tokeni, biometrijski uređaji)?
5. Koliko se osjećate sigurno prilikom obavljanja bankarskih transakcija putem kanala e-bankarstva? – (skala od 1 do 5) u kojem 1 označava najmanji osjećaj sigurnosti dok 5 označava najveći osjećaj sigurnosti.
6. Koliko je važna sigurnost prilikom odabira kanala e-bankarstva?
7. Kako biste ocijenili svoje povjerenje u sigurnost hardverskih komponenti koje koristite prilikom korištenja e-bankarstva?
8. Kako biste ocijenili važnost dostupnosti kanala e-bankarstva 24 sata dnevno, 7 dana u tjednu?
9. Jeste li ikada iskusili bilo kakve poteškoće ili probleme prilikom korištenja nekog od kanala e-bankarstva? Ako jeste, navedite ih.

10. Koje biste kanale e-bankarstva preporučili drugima na temelju vašeg iskustva?
11. Kako biste ocijenili korisničko iskustvo korištenja e-bankarstva u usporedbi s tradicionalnim načinima bankarskih usluga (npr. posjeta bankovnim poslovnica)?

4.7. Rezultati ankete

Rezultati ankete ukazuju na visoku popularnost kanala e-bankarstva među korisnicima. Analiza anketnih podataka pokazala je da više od 80% ispitanika koristi internetsko bankarstvo i mobilno bankarstvo kao svoje preferirane kanale za obavljanje bankarskih transakcija. Također istraživala se uloga hardverskih komponenti u poboljšanju sigurnosti i pouzdanosti e-bankarskih usluga. Anketa je pokazala da njih 32,5% koristi sigurnosne tokene ili biometrijske uređaje. Ti dodatni slojevi autentifikacije pružaju dodatnu zaštitu od prijevара i neovlaštenog pristupa korisničkim računima. Kako su sve ocjene na pitanje o osjećaju sigurnosti bile 4 ili 5 nije primijećena značajna razlika u zadovoljstvu korisnika između različitih hardverskih komponenti koje su korištene. To sugerira da, iako su hardverske komponente važne za sigurnost, korisnicima je možda važnije da imaju opciju sigurnosnih mehanizama bez obzira na specifičan hardver koji se koristi. Na pitanje o tome da li su se susreli s nekim poteškoćama u okviru korištenja kanala e-bankarstva, najčešći odgovor je bio „ne“, dok su se ostali odnosili na to da su usluge ponekad nedostupne zbog rada na sustavu i sl. Kanal s najviše preporuka (njih 57,5%) odlazi mobilnom bankarstvu, 37,5% na internet bankarstvo, dok su ostali kanali prikupili samo 5% preporuka. Ovo istraživanje također ima nekoliko ograničenja. Prvi, uzorak ispitanika ograničen je na određenu populaciju i može se razlikovati od cjelokupne populacije korisnika e-bankarstva. Drugo, rezultati se temelje na samoprijavljenim podacima, što može podložno subjektivnom dojmu ili bilo kojim drugim pristranostima. Treće, anketa je usredotočena samo na trenutno stanje, ali budući razvoj tehnologije i promjene u industriji mogu utjecati na rezultate i zaključke.

5. Rasprava

U suvremenom bankarstvu, kanali e-bankarstva igraju ključnu ulogu u pružanju korisnicima brzog, praktičnog i sigurnog pristupa financijskim uslugama. Internet bankarstvo, mobilno bankarstvo, bankomati i POS uređaji sve su više postali nezaobilazni alati za klijente i banke. Internet bankarstvo omogućuje korisnicima da upravljaju svojim financijama putem internetskog preglednika, dok mobilno bankarstvo omogućuje pristup istim uslugama putem pametnih telefona i mobilnih uređaja. Osim virtualnih kanala, hardverske komponente igraju ključnu ulogu u pružanju sigurnih i praktičnih transakcija. Bankomati omogućuju korisnicima da podižu gotovinu, provjeravaju saldo i obavljaju depozite 24/7, pružajući veću dostupnost usluga. POS uređaji, koji su sve prisutniji u trgovinama, omogućuju brze i sigurne platne transakcije putem kartica ili mobilnih uređaja. Dodatno, sigurnosni tokeni ili fizičke komponente koje generiraju jednokratne autentifikacijske kodove osiguravaju sigurnost online transakcija. Međutim, izazovi poput sigurnosti i privatnosti ostaju važni aspekti. Potrebno je osigurati jake sigurnosne mjere kako bi se spriječile prijevare i zaštitili osjetljivi financijski podaci korisnika. Trendovi kao što su biometrija za autentifikaciju, korištenje blockchain tehnologije za transparentnost i Internet of Things (IoT) za unapređenje korisničkog iskustva ukazuju na buduće mogućnosti u ovom sektoru. Kombinacija e-bankarstva i hardverskih komponenti transformira način na koji banke pružaju usluge i kako korisnici upravljaju svojim financijama. Ova integracija osnažuje klijente i banke omogućujući im da iskoriste prednosti brzine, dostupnosti i sigurnosti koje digitalni kanali i hardverske komponente pružaju. U budućnosti, očekuje se daljnji rast i razvoj ovih tehnologija kako bi se zadovoljile potrebe sve zahtjevnijih korisnika i prilagodila se dinamika modernog bankarstva.

6. Zaključak

Ubrzani rast i razvoj tehnologije modernog doba primorao je banke na korištenje većeg broja kanala distribucije bankovnih usluga kako bi zadovoljile korisničke zahtjeve sve većeg broja klijenata koji koriste njihove usluge. Kako bi se smanjile gužve i čekanja u redovima, banke su sve usluge, koje se ne moraju obavljati posredstvom nekog od zaposlenika u banci, distribuirale u pet kanala. Najčešće se koriste bankomati, kiosci, online bankarstvo, mobilno bankarstvo, tele bankarstvo, te u ne toliko velikoj mjeri koristi se i TV bankarstvo. U današnje vrijeme, zahvaljujući razvoju tehnologije i Interneta najdominantniji kanali postali su mobilno i online bankarstvo. Zahvaljujući mobilnom bankarstvu, sve bankovne usluge dostupne su dvadeset i četiri sata dnevno bilo gdje da se klijent nalazi, jedini preduvjet za to su mobilni uređaj i pristup Internetu. Prednosti takvog bankarstva su višestruke: klijent ima mogućnost uvida u svoj račun u bilo kojem trenutku, može prebacivati novac s računa na račun, plaćati račune za režije i još mnogo toga bez odlaska u banku i čekanja u redovima. Da bi to sve bilo moguće, banke moraju stalno ulagati u razvoj novih tehnologija, razvijati vlastite aplikacije koje moraju biti pristupačne i jednostavne za korištenje svim klijentima, te ulagati u sigurnost kako bi zaštitili klijente i njihove podatke od upada i krađe. Kako smo mogli i iščitati iz rezultata dobivenih anketiranjem, sve više mladih prepoznaje prednosti i pogodnosti koje e-bankarstvo pruža. Također rezultati imaju važne implikacije za bankarski sektor. Banke bi trebale nastaviti ulagati u razvoj i unaprjeđenje kanala e-bankarstva kako bi zadovoljile potrebe svojih korisnika. Posebna pažnja trebala bi se posvetiti sigurnosnim aspektima, a integracija naprednih hardverskih komponenti, poput biometrije ili sigurnosnih tokena, može biti ključna za pružanje dodatnog povjerenja i osiguranje korisničkog iskustva.

LITERATURA

1. Birovčec, F. (2021.) *Osvrt na prethodna istraživanja* [Online] Raspoloživo na: <https://repositorij.efzg.unizg.hr/islandora/object/efzg%3A6845/datastream/PDF/view>. [Pristupljeno: 24. lipnja 2023.]
2. Boban, M. i Perišić, M. (2015.) *Biometrijski način zaštite u bankarstvu* [Online] Raspoloživo na: <https://hrcak.srce.hr/file/209925>. [Pristupljeno: 24. lipnja 2023.]
3. Boban, M. i Perišić, M. (2015.): *Biometrija u sustavu sigurnosti, zaštite i nadzora informacijskih sustava* [Online] Raspoloživo na: <https://hrcak.srce.hr/file/209925>. [Pristupljeno: 24. lipnja 2023.]
4. Dragičević, T. (2020.) *Utjecaj digitalizacije na bankarski sektor* [Online] Raspoloživo na: <https://repositorij.efzg.unizg.hr/islandora/object/efzg:5482/datastream/PDF/view> [Pristupljeno: 24. lipnja 2023.]
5. Parat, M. (2015.) *Osvrt na prethodna istraživanja u pogledu sigurnosnom aspektu.* [Online] Raspoloživo na: <https://zastita.info/UserFiles/file/zastita/SIGBANK%202015/PDF%20PREZENTACIJE/10.%20Milan%20Parat.pdf>. [Pristupljeno: 24. lipnja 2023.]
6. Rončević, A. (2006.) *Inovacija i razvoj novih bankarskih usluga* [Online] Raspoloživo na: <https://hrcak.srce.hr/file/12965> [Pristupljeno: 14. srpnja 2023.]

Internetski izvori:

1. ABC China (2022.) *Televizijsko Bankarstvo* [Online] Raspoloživo na: <https://www.abchina.com/en/personal/ebanking/tvb/tvbi/>. [Pristupljeno: 24. lipnja 2023.]
2. ATM Security (2023.) *Sigurnost i zaštita bankomata* [Online] Raspoloživo na: <https://www.aba.com/banking-topics/risk-management/physical-security/atm-security> [Pristupljeno: 14. srpnja 2023.]
3. Banke & Biznis (2018.) *Prednosti i izazovi e-bankarstva.* [Online] Raspoloživo na: <https://banke-biznis.com/izazovi-i-prednosti-elektronskog-bankarstva/>. [Pristupljeno: 24. lipnja 2023.]

4. Cointelegraph (2023.): *A brief history of digital banking* [Online] Raspoloživo na: <https://cointelegraph.com/news/a-brief-history-of-digital-banking>. [Pristupljeno: 24. lipnja 2023.]
5. Crowdbotics (2023.): *Razvoj mobilnog bankarstva u budućnosti* [Online] Raspoloživo na: <https://www.crowdbotics.com/blog/the-future-of-mobile-banking-applications> [Pristupljeno: 24. lipnja 2023.]
6. Economy-pedia (2021.): *Internetsko bankarstvo - što je to, definicija i koncept – 2021.* [Online] Raspoloživo na: <https://hr.economy-pedia.com/11031981-online-banking>. [Pristupljeno: 24. lipnja 2023.]
7. EM Bank (2023.) *Sigurnost u e-bankarstvu* [Online] Raspoloživo na: https://em.bank/accounts/safeguarding-accounts/?gclid=Cj0KCQjwxuCnBhDLARIsAB-cq1qHwptsNbK7O1Dmh7-fTSxnbhLzl-wTwiLaOp_GuvqvoaHIs_xoeggaAqtgEALw_wcB [Pristupljeno: 24. lipnja 2023.]
8. Erste Banka (2023.) *Što je display kartica?* [Online] Raspoloživo na: <https://www.erstebank.hr/hr/pomoc/help-center/poslovni-klijenti/on-line-bankarstvo/netbanking/sto-je-display-kartica>. [Pristupljeno: 24. lipnja 2023.]
9. HNB (2019.) *Trenutno stanje i izazovi za budućnost* [Online] Raspoloživo na: https://www.hnb.hr/documents/20182/2627205/hn13112019_Svaljek_prezentacija.pdf/3bcf30c8-c2a1-973c-ba44-64504bdcb17c?t=1573656092593 [Pristupljeno: 24. lipnja 2023.]
10. HPB (2021.) *Istraživanje: generacija Z o mobilnom bankarstvu* [Online] Raspoloživo na: <https://www.hpb.hr/hr/hpb-istrazivanje-generacija-z-o-mobilnom-bankarstvu/6763> [Pristupljeno: 14. srpnja 2023.]
11. HPB (2023.) *Što je mToken?* [Online] Raspoloživo na: <https://www.hpb.hr/hr/mtoken-6158/6158>. [Pristupljeno: 24. lipnja 2023.]
12. Info Kiosk (2023.) *Interaktivni kiosci* [Online] Raspoloživo na: <https://www.infokiosk.hr/hrvatski/proizvodi-i-usluge/mogu%C4%87nosti-kori%C5%A1tenja-info-kiosk/>. [Pristupljeno: 24. lipnja 2023.]
13. Ingwb (2023.) *Prednosti m-tokena* [Online] Raspoloživo na: <https://www.ingwb.com/en/service/insidebusiness-app/mtoken-easy-and-secure-access-to-insidebusiness-explained-in->

- [depth#:~:~:~:~:text=mToken%20is%20a%20feature%20of,Easy%20activation%20within%20minutes.](#) [Pristupljeno: 14. srpnja 2023.]
14. Investopedia (2021.) *TAN tablica* [Online] Raspoloživo na: <https://www.investopedia.com/terms/t/transaction-authentication-number-tan.asp#:~:~:~:~:text=A%20transaction%20authentication%20number%20is,account%20or%20conduct%20a%20transaction>. [Pristupljeno: 24. lipnja 2023.]
15. Investopedia (2020.): *Mobilno bankarstvo* [Online] Raspoloživo na: <https://www.investopedia.com/terms/m/mobile-banking.asp>. [Pristupljeno: 24. lipnja 2023.]
16. Law Insider (2023.) *Hardverske komponente u bankarstvu* [Online] Raspoloživo na: <https://www.lawinsider.com/dictionary/bank-hardware>. [Pristupljeno: 24. lipnja 2023.]
17. Law Insider (2023.) *Telefonsko bankarstvo, definicija i koncept* [Online] Raspoloživo na: <https://www.lawinsider.com/dictionary/telephone-banking>. [Pristupljeno: 24. lipnja 2023.]
18. Money gate (2022.) *New & recent Innovations in the Banking Sector 2023* [Online] Raspoloživo na: <https://money-gate.com/innovations-banking-sector-2020/>. [Pristupljeno: 24. lipnja 2023.]
19. NatWest (2023.) *Što je i čemu služi čitač kartica?* [Online] Raspoloživo na: <https://www.natwest.com/banking-with-natwest/how-to/card-reader.html>. [Pristupljeno: 24. lipnja 2023.]
20. Stack Exchange (2016.) *USB stick s certifikatom* [Online] Raspoloživo na: <https://security.stackexchange.com/questions/147463/how-can-usb-stick-online-identification-possibly-work>. [Pristupljeno: 24. lipnja 2023.]
21. Stripe (2023.) *Uređaji za autorizaciju u bankarstvu* [Online] Raspoloživo na: <https://stripe.com/en-hr/resources/more/card-authorization-explained#:~:~:~:~:text=Card%20authorization%20is%20approval%20from.using%20a%20card%20to%20complete>. [Pristupljeno: 24. lipnja 2023.]
22. Thales group (2021.) *Token u bankarstvu* [Online] Raspoloživo na: <https://www.aba.com/banking-topics/risk-management/physical-security/atm-security> [Pristupljeno: 14. srpnja 2023.]

23. UCA EDU (2023.) *The University of Central Arkansas Police Department – zaštita bankomata* [Online] Raspoloživo na: <https://uca.edu/police/crime-prevention/atm-safety-and-security-recommendations/>. [Pristupljeno: 24. lipnja 2023.]
24. Urban Money (2023.) *ATM Machine, Bankomati i gotovinske transakcije* [Online] Raspoloživo na: <https://www.urbanmoney.com/banking/atm-machine>. [Pristupljeno: 24. lipnja 2023.]

Popis slika

Slika 1. - Primjer modernog bankomata banke "Barclays"	23
Slika 2. - primjer interaktivnog kioska	24
Slika 3. - primjer promidžbe telefonskog bankarstva OTP banke	25
Slika 4. - primjer pristupa Internet bankarstvu putem tokena	26
Slika 5. - primjer sučelja Internet bankarstva Addiko banke	26
Slika 6. - primjer početnog zaslona "mojaRBA"	27
Slika 7.– slika prikazuje online sučelja PBZ i Erste banke.....	29