Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Analýza způsobů a míry využití Bankovní identity a jejích alternativ v České republice

Stanislav Konopásek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Stanislav Konopásek

Systémové inženýrství a informatika
Informatika

Název práce

Analýza způsobů a míry využití Bankovní identity a jejích alternativ v České republice

Název anglicky

Analysis of the methods and rate of use of Banking Identity and its alternatives in the Czech Republic

---

Cíle práce

Hlavním cílem práce bude analýza zavádění bankovní identity v České republice. Dílčím cílem v takto definovaném hlavním cíli, bude analyzovat část bankovní identity s názvem NIA, která slouží pro ověřování identity v základních registrech (egovernment) a kompletace základních pojmů z oblasti bankovnictví se zaměřením na internetové bankovnictví a digitalizaci.
V praktické části bude zjištěn aktuální stav bankovní identity v rámci jednotlivých českých bank. Dílčím cílem bude také průzkum názoru občanů na bankovní identitu.

Metodika

Metodika praktické části:

• analýza bankovního trhu – tzn. představení nejznámějších českých bank,

• průzkum a analýza stavu bankovní identity v již představených bankách,

• interpretace získaných výsledků – tj. připravenost jednotlivých bank,

• vytvoření dotazníku pro občany České republiky a interpretace výsledků z dotazníku,

• interpretace jednotlivých výsledků a stavu jednotlivých bank, míra užitečnosti a použitelnosti bankovní identity v ČR.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

bankovnictví, bankovní identita, egovernment, SONIA, digitalizace, trh, ověřování, kryptografie

---

Doporučené zdroje informací

BURDA, Karel. Kryptografie okolo nás. Praha: CZ.NIC, z.s. p.o., 2019. CZ.NIC. ISBN 978-80-88168-49-2.

KUMAR, Puneet, JAIN, Vinod Kumar and PAREEK, Kumar Sambhav. The stances of e-government: policies, processes and technologies. Boca Raton, FL : CRC Press, Taylor & Francis Group, 2018. ISBN 9781138304901.

TAAFFE, Ouida and TAAFFE, Ouida Mary. Banking on change: the development and future of financial services. Chichester, West Sussex, England : Wiley, 2019. ISBN 9781119609988.

VEBER, Jaromír. Digitalizace ekonomiky a společnosti: výhody, rizika, příležitosti. Praha: Management Press, 2018. ISBN 978-807-2615-544.

Předběžný termín obhajoby

2022/23 ZS – PEF

Vedoucí práce

Ing. Mgr. Vladimír Očenášek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 10. 8. 2021

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2021

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 15. 10. 2022

Čestné prohlášení

Prohlašuji, že svou diplomovou práci „Analýza způsobů a míry využití Bankovní identity a jejích alternativ v České republice“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 22. listopadu 2022 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Mgr. Vladimíru Očenáškovi, Ph.D., za jeho odborné vedení, pomoc a praktické rady, které mi předal prostřednictvím vzájemné komunikace při zpracovávání diplomové práce.

Analýza způsobů a míry využití Bankovní identity a jejích alternativ v České republice

Abstrakt

Diplomová práce se zabývá analýzou zavádění bankovní identity v České republice. Teoretická část popisuje základní pojmy bankovní identity, její výhody a nevýhody. Dále definuje principy a pojmy spojené s e-governmentem, pojetí kryptografie a na závěr digitalizaci, a to jak ve společnosti a ekonomice, tak v samotném bankovnictví. Navazující praktická část v úvodu objasňuje aktuální stav bankovního trhu s ohledem na bankovní identitu v České republice. Po představení následuje analýza stavu bankovní identity ve třech největších bankách a interpretace získaných výsledků. Dalším tématem praktické části je představení možností využití bankovní identity ve státní a soukromé sféře. Na základě informací a zkušeností získaných z analýzy jsou v další kapitole vytvořeny procesní diagramy popisující princip jejího využití v obou sférách. V praktické části je též popsán způsob založení a využití dvou nejznámějších alternativ bankovní identity. Představeny jsou i jejich rozdíly v porovnání s bankovní identitou. Závěr praktické části se věnuje dotazníkovému šetření, jež má za cíl na základě odpovědí představit informace týkající se názoru na bankovní identitu, její alternativy, bezpečnost, budoucnost, míru využití a vůbec povědomí o ní. Kapitola zahrnující výsledky a diskuse definuje souhrn získaných závěrů a popisuje přínosy, doporučení a možné rozšíření celé diplomové práce.

Klíčová slova: bankovnictví, bankovní identita, e-government, SONIA, digitalizace, trh, ověřování, kryptografie, využití, alternativy

Analysis of the methods and rate of use of Banking Identity and its alternatives in the Czech Republic

Abstract

The diploma thesis deals with the analysis of the introduction of Banking Identity in the Czech Republic. The theoretical part describes essential concepts of Banking Identity, its advantages and disadvantages. Furthermore, it defines principles and concepts connected with e-government, cryptography meaning and finally digitalisation both within the society and economy and in banking itself. The following practical part clarifies in its introduction the current situation of banking market with respect to Banking Identity in the Czech Republic. After the introduction, an analysis of the state of Banking Identity in the three largest banks an interpretation of obtained results follows. Another topic of the practical part is the presentation of the possibilities of using Banking Identity in the state and private sphere. Based on information and experience obtained from this analysis, there are diagrams created in the following chapter, that describe the principle of its utilisation in both sectors. The practical part also describes the method of establishment and utilisation of the two best-known alternatives of Banking Identity. Also, their differences in comparison with Banking Identity are introduced. The conclusion of the practical part is devoted to a questionnaire construction that is aimed at the introduction of information concerning an opinion on Banking Identity, its alternatives, security, future, utilisation rate and awareness of it on the basis of obtained answers. The chapter containing results and discussions defines a summary of obtained conclusions and describes assets, recommendations and possible enlargement of the whole diploma thesis.

Keywords: Banking, banking identity, e-government, SONIA, digitalisation, market, verification, cryptography, utilisation, alternatives

Obsah

1 Úvod **11**

2 Cíl práce a metodika **13**

2.1 Cíl práce 13

2.2 Metodika 13

3 Teoretická východiska **15**

3.1 Bankovní identita 15

3.1.1 NIA 16

3.1.2 SONIA 17

3.1.3 Potenciál bankovní identity 18

3.1.4 Výhody 18

3.1.5 Nevýhody 18

3.1.6 Alternativy 19

3.2 E-government 21

3.2.1 Typy e-governmentu 21

3.2.2 IoT a e-government 22

3.2.3 E-government v České republice 22

3.2.4 E-government ve vzdělání 27

3.2.5 Přínosy e-governmentu 27

3.3 Kryptografie 28

3.3.1 Přístupové systémy 28

3.3.2 Autentizace versus autorizace 30

3.3.3 Autentizační protokoly 32

3.3.4 Autorizační protokoly 33

3.3.5 Přístupové protokoly 34

3.3.6 Phishing a bankovní identita 34

3.3.7 Internetové bankovnictví 34

3.4 Digitalizace a změny v bankovnictví 35

3.4.1 Pojem digitalizace 35

3.4.2 Bankovní produkty 36

3.4.3 Bankovní technologie 36

3.4.4 Budoucnost plateb 38

3.4.5 Jak banky vydělávají peníze 39

3.4.6 Otevřené bankovnictví 40

3.4.7 České banky a digitalizace 40

3.5 Digitalizace v ekonomice a společnosti 41

3.5.1 Ekonomické přínosy digitalizace 41

3.5.2 Rizika ... 42
3.5.3 Obchodování na internetu ... 44
3.5.4 Incidenty spojené s digitalizací ... 45

4 Praktická část ... 46
4.1 Současná situace v ČR ... 46
4.1.1 Největší banky v ČR ... 46
4.1.2 Banky s bankovní identitou ... 47
4.1.3 Společnost BankID ... 48
4.2 Bankovní identita v českých bankách ... 48
4.2.1 Komerční banka ... 49
4.2.2 ČSOB ... 50
4.2.3 Česká spořitelna ... 53
4.2.4 Připravenost bank ... 54
4.3 Možnosti využití bankovní identity ... 55
4.3.1 Soukromá sféra ... 56
4.3.2 Státní sféra ... 60
4.4 Analýza principu fungování bankovní identity ... 66
4.4.1 Proces ověřování v soukromé sféře ... 67
4.4.2 Proces ověřování ve státní sféře ... 68
4.5 Alternativy bankovní identity ... 69
4.5.1 MojeID ... 69
4.5.2 Mobilní klíč eGov ... 71
4.6 Dotazníkové šetření ... 73
4.6.1 Analýza odpovědí využívajících respondentů ... 76
4.6.2 Analýza odpovědí nevyužívajících respondentů ... 82
4.6.3 Názor na budoucnost a bezpečnost ... 85

5 Výsledky a diskuse ... 87
5.1 Zhodnocení připravenosti jednotlivých bank ... 87
5.2 Zhodnocení možností využití bankovní identity ... 88
5.2.1 Analýza v soukromé sféře ... 88
5.2.2 Analýza ve státní sféře ... 89
5.3 Bankovní identita v porovnání s alternativami ... 91
5.4 Zhodnocení výsledků dotazníkového šetření ... 91
5.5 Přínosy a doporučení ... 94
5.6 Možná rozšíření práce ... 96

6 Závěr ... 97

7 Seznam použitých zdrojů ... 100

Seznam obrázků ... 107

Přílohy **108**
Příloha A BPMN diagram – soukromá sféra 108
Příloha B BPMN diagram – státní sféra 109

1 Úvod

Společnost se v mnoha směrech neustále rozvíjí a mění. Přicházející krize pak tuto skutečnost jenom urychlují. Největší rozvoj představuje v poslední letech digitalizace, jež reagovala a reaguje na pandemii covid-19 a hrozící energetickou krizi. Digitalizace probíhá nepřetržitě v mnoha odvětvích od strojírenství přes státní služby až po banky a další. Na řadu firem je vyvíjen neustálý konkurenční tlak, aby zdokonalovaly své informační systémy a technologie, které mají za cíl usnadňovat jejich klientům řadu činností. Samotní zákazníci se pak musí s těmito technologiemi seznamovat a učit se je používat.

Jednou z nejrychleji se rozrůstajících služeb, jež úzce souvisí s digitalizací, je bankovní identita. Ta se nejprve začala využívat ve státní sféře a postupně se dostává i do sféry soukromé. Bankovní identita umožňuje lidem ověřit si svou identitu na různých portálech, e-shopech a dalších stránkách. Její uživatelé se nemusí registrovat, vymýšlet přihlašovací jméno a heslo nebo se ověřovat pomocí dalších metod, ale stačí jim přihlásit se stejně jako do svého internetového bankovnictví. Podmínkou však je, že tuto službu musí jejich banka nabízet, což se postupem času stává standardem.

Jak již bylo nastíněno, zavádění bankovní identity roste rychlým tempem, lze jí využít u mnoha bank a na stále více místech, a to jak na jednotlivých portálech státních sféry, tak v e-shopech, energetických či investičních portálech a jiných oblastech. To může být pro klienty někdy nepřehledné, jelikož ani neví, kde všude mohou službu využít, k čemu vůbec slouží a jak funguje. Nastala tak potřeba tyto oblasti stručně a přehledně představit a vysvětlit princip jejich fungování. Ještě před příchodem bankovní identity byly pro ověřování zavedeny jiné prostředky, o nichž se práce zmiňuje jako o jejích alternativách. Je proto nutné je objasnit a uvést rozdíly v porovnání s bankovní identitou, jelikož mohou ovlivňovat míru jejího využití. Celkově nabízí bankovní identita řadu otázek, týkajících se její bezpečnosti, budoucnosti a jejího aktuálního využití ve společnosti a zvýšení povědomí o ní. Diplomová práce se tedy bude zabývat naplněním těchto požadavků, a to uceleným způsobem tak, aby na sebe části logicky navazovaly a propojily jednotlivé oblasti, které byly zmíněny.

Teoretická část bude mít za úkol popsat základní pojmy spojené s bankovní identitou a celkově digitalizací, jež pak budou tvořit stavební kameny praktické části, která bude mít za úkol splnění hlavního cíle práce založeného na zmíněných potřebách. Úvod teoretické části se za účelem objasnění bankovní identity a dalších souvisejících pojmů bude zabývat právě touto problematikou. Dále budou zmíněny její výhody, nevýhody, potenciál a

alternativy. Protože možnosti jejího využití byly prvotně v oblasti státní správy, dojde též k vysvětlení e-governmentu, jeho typů, situace v České republice v tomto kontextu, možností jeho využití ve vzdělávání a jeho celkových přínosech. Bankovní identita je jedním z prostředků ověřování a s tím souvisí i pojem kryptografie. Dojde tedy k představení a objasnění náležitostí z této oblasti, jako jsou například autentizace, autorizace, přístupové systémy nebo autentizační či autorizační protokoly. Závěr kapitoly se pak bude zabývat bezpečnostní hrozbou, tzv. phishingem. Digitalizace postupuje rychlým tempem a zahrnuje v sobě i samotnou bankovní identitu, proto se závěrečné části práce budou zabývat právě tímto tématem. Dojde k objasnění dvou oblastí této problematiky, a to digitalizace v bankovnictví a v ekonomice a společnosti. V rámci digitalizace v bankovnictví pak budou představeny jednotlivé bankovní produkty, technologie, platby a otevřené bankovnictví. Naopak digitalizace v ekonomice a společnosti se bude zabývat jejími ekonomickými přínosy, riziky a incidenty, jež jsou s ní spojené.

Po stanovení teoretických základů dojde ke zpracování praktické části. Ta se v úvodu bude zabývat představením současné situace v České republice z hlediska bankovního sektoru a bankovní identity. Budou představeny největší banky, ty, které bankovní identitu zprostředkovávají, a společnost BankID. Zároveň dojde k analýze stavu bankovní identity ve třech největších bankách v České republice. Na základě analýzy bude definována připravenost bank. To znamená, jak si aktuálně stojí a jak vypadá jejich aktuální řešení bankovní identity. Následně bude provedena analýza možností využití v soukromé i ve státní sféře. Budou popsány praktické ukázky užití na předem vybraných portálech, stránkách a e-shopech. Na základě získaných zkušeností z provedených analýz bude zobrazeno a popsáno fungování bankovní identity k vytvoření procesních diagramů. Další část se pak bude věnovat alternativám bankovní identity, představena bude praktická ukázka jejich založení, využití a rozdílů v porovnání s bankovní identitou. Závěr praktické části se pak bude věnovat výzkumu mínění veřejnosti, v jehož rámci bude vytvořen dotazník, ze získaných odpovědí pak budou vyvozeny závěry. Otázky dotazníku budou strukturované stejně jako osnova praktické části práce.

Závěr práce pak představí ucelený souhrn získaných výsledků z jednotlivých analýz, z praktických ukázek z jednotlivých oblastí a z interpretovaných odpovědí nabytých v rámci dotazníkového šetření. Budou též sděleny přínosy, doporučení a možné rozšíření diplomové práce.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem práce je analýza zavádění bankovní identity v České republice. Dílčími cíli v takto definovaném hlavním cíli bude objasnění teoretických principů bankovní identity, samotných ověřovacích metod a kompletace základních pojmů z oblasti bankovnictví se zaměřením na internetové bankovnictví a celkově na digitalizaci.

V praktické části by mělo dojít k představení nejznámějších bank a stavu bankovní identity v České republice. Měl by být proveden průzkum jejího aktuálního stavu v rámci vybraných bank a interpretovány možnosti jejího využití v jednotlivých sférách, čímž je myšlena analýza ve státní sféře (NIA) a v soukromé sféře (SONIA). Na základě jednotlivých analýz by mělo dojít k popisu jejího fungování a porovnání rozdílů s alternativami. Dalším cílem bude též průzkum názoru občanů na bankovní identitu, do jaké míry je využívána, jak je zabezpečena, jaké jsou její alternativy a budoucnost.

2.2 Metodika

Použitá metodika diplomové práce se zakládá na studiu teoretických zdrojů a řešení dané problematiky. Analýzy a výzkumy, jež se uskuteční, budou brát v úvahu jednotlivé cíle a potřeby práce. Na základě analýz a získaných zkušeností dojde k vytvoření procesních diagramů, kde bude využit nástroj Camunda BPMN/DMN Process Modeler. Pro vytvoření dotazníku a získání odpovědí bude v závěru praktické části zvoleno řešení od společnosti Survio.

Diplomová práce bude postupovat v následujících krocích:

1. Vymezení teoretických poznatků: Na základě různých zdrojů budou uvedeny teoretické principy, na nichž bude založeno následné řešení praktické části. Budou popsány základní pojmy spojené s bankovní identitou, e-governmentem, kryptografií a jednotlivými tématy týkajícími se digitalizace.
2. Analýza českého bankovního trhu: Bude představena aktuální situace v České republice, uvedeny budou největší a nejznámější banky, které umožňují bankovní identitu, a společnost BankID.
3. Průzkum a analýza stavu bankovní identity v představených bankách: Dojde k analýze stavu bankovní identity ve třech nejznámějších bankách, budou

uvedeny zásadní události spojené s bankovní identitou a konkrétní bankou a zároveň dojde k představení řešení bankovní identity u jednotlivých bank.

4. Interpretace výsledků analýzy představených bank: Bude definována připravenost jednotlivých bank, to znamená, jaký je jejich aktuální stav, zda se vyskytl v průběhu zavádění bankovní identity nějaký závažnější problém a jaký je rozdíl mezi jednotlivými řešeními.
5. Průzkum možností využití bankovní identity ve státní a soukromé sféře: Bude proveden popis oblastí a principů v soukromé a státní sféře za účelem představení použitelnosti bankovní identity v České republice.
6. Vytvoření procesních diagramů popisujících princip využití: Na základě zkušeností získaných z předchozích analýz budou vytvořeny a popsány procesní diagramy, jež ukáží jednotlivé kroky ověření prostřednictvím bankovní identity.
7. Praktické představení alternativ: Budou přiblíženy alternativy spolu s popisem jejich využití. Na základě toho budou definovány rozdíly v porovnání s bankovní identitou.
8. Dotazníkové šetření a interpretace výsledků: Bude provedeno dotazníkové šetření pro občany České republiky, které má zjistit informace ohledně míry a oblastí využití bankovní identity, jejích alternativ, budoucnosti a bezpečnosti.
9. Diskuse o přínosech a rozšířeních: Na základě interpretovaných výsledků budou definovány přínosy, doporučení a možné rozšíření práce.
10. Závěr diplomové práce: V posledním bude shrnuta daná problematika a na základě syntézy teoretických poznatků, získaných zkušeností a výsledků budou interpretovány závěry diplomové práce.

3 Teoretická východiska

V teoretické části práce budou vymezeny pojmy a oblasti, které jsou nějakým způsobem spojeny s bankovní identitou. V úvodu bude definována samotná bankovní identita. Tato kapitola se bude zabývat pojmy, jako jsou NIA, SONIA, jaký má bankovní identita potenciál a jaké jsou její výhody či nevýhody. Dále dojde k vysvětlení pojmu e-government, v němž se bankovní identita začíná stále více využívat. Zde budou uvedeny typy e-governmentu a jeho stav v České republice, ve vzdělávání a jeho celkové přínosy. Dalším tématem, které je též úzce spojeno s bankovní identitou, bude kryptografie. Ta se využívá při samotném ověřování klientů. Vysvětleny budou přístupové systémy, autentizace, autorizace, protokoly a další. Poslední dvě kapitoly se budou zabývat digitalizací, jež ve skutečnosti stojí za zrodem celé bankovní identity. Dojde tedy k vymezení toho, co to digitalizace je a jaké má dopady na bankovnictví. Budou zde též vymezeny bankovní produkty, technologie, pojem otevřeného bankovnictví a další. Závěr teoretické části se bude zabývat digitalizací v ekonomice a v samotné společnosti. Hlavní náplní kapitoly budou přínosy a rizika digitalizace, které ve výsledku mají vliv na celou ekonomiku a na společnost. Dalším bodem bude vysvětlení, jak probíhá a jak se vyvíjí obchodování na internetu, kde by vlastně měla být v budoucnu bankovní identita využívána jako prostředek pro ověřování identity. Na závěr kapitoly budou uvedeny příklady incidentů, k němž v minulosti ve spojitosti s digitalizací došlo.

3.1 Bankovní identita

Bankovní identita je jednoduchý nástroj, jenž umožňuje digitálně ověřit totožnost prostřednictvím přihlašovacích údajů do internetového bankovnictví. Umožňuje například jednoduše podat daňové přiznání nebo podepsat smlouvy s dodavateli energií či telefonními operátory, a to vše online. Měla by rovněž umožnit online si zažádat o sociální dávky či opatřit e-recept nebo potvrzení od lékaře (Mertová, 2021). Pro využívání všech těchto činností klientovi stačí ověření prostřednictvím jednoho hesla, nebo za pomoci jiné přihlašovací metody do internetového bankovnictví. Bankovní identita je zákazníkům bank dána automaticky, nebo po jejím vytvoření v rámci internetového bankovnictví. V zásadě jde o jakousi „digitální občanku“. Možnost přidat se k projektu bankovní identity je dostupná všem bankám na českém trhu (HEX, 2021).

Bankovní identitu má šanci využít až 5,5 milionu obyvatel České republiky, kteří disponují internetovým bankovnictvím. Začít využívat ji mohou i soukromé firmy, a to nikoli jen pro identifikaci vlastních klientů, nýbrž i pro digitální podepisování smluv. Česko se při jejím zavádění inspirovalo především u severských zemí. Například ve Švédsku a Norsku je bankovní identita v provozu již od počátku tohoto tisíciletí a je využívána drtivou většinou populace. Pro Českou republiku to může představovat hlavní krok na cestě k digitalizaci, v níž až dosud stále pokulhávala (Mertová, 2021).

3.1.1 NIA

NIA ID je identifikační prostředek, jenž poskytuje zaručené dokazování totožnosti při přihlašování k online službám, které požadují přinejmenším velkou úroveň důvěry prostředků identifikace. Jde o tzv. dvoufaktorový styl ověření (Správa základních registrů, 2020).

Konkrétně slouží pro přihlašování k službám veřejnoprávním. NIA (Národní bod pro identifikaci a autentizaci) hraje roli prostředníka během každého přihlašování ke službám e-governmentu. Využívá se tedy při veřejnoprávním použití bankovní identity k online jednání s orgány veřejné moci. Dále sjednocuje poskytovatele elektronických identit, tím pádem i banky nabízející bankovní identitu s poskytovateli služeb e-governmentu.

V rámci kteréhokoli přihlášení ke službám e-governmentu pomocí bankovní identity tudíž nedochází k bezprostřednímu přihlášení, avšak k přihlášení skrze NIA, jenž spojí „obě strany řetězce“. Argumentem je zejména co možná nejvyšší míra ochrany údajů o uživatelích zmíněných služeb, což je umocněno i realitou, že ani banky nedokážou určit, k jaké určité službě e-governmentu se klient bankovní identitou přihlašuje (BusinessInfo.cz, 2021).

Přihlášení skrze NIA

Tato část diplomové práce se bude zabývat tím, jak přihlášení přes NIA probíhá prakticky z pohledu uživatele. Celý proces začíná skutečností, že se klient chce přihlásit k nějakému poskytovateli služeb, k němuž se lze přihlásit skrze NIA. V dalším kroku může předpokládat přesměrování na stránky NIA. V rámci, něhož vznáší poskytovatel služby uzlu požadavek, jenž v sobě zahrnuje úroveň záruky, s kterou se má konkrétní uživatel přihlásit. Zmíněná úroveň může být buď „nízká“, „značná“ či „vysoká“. Na základě požadavku je nabídnut výčet současně dostupných možností přihlášení, jež mají totožnou, nebo vyšší úroveň.

Jestliže poskytovatel služby žádá přihlášení s úrovní „vysoká“, NIA poskytne aktuálně pouze dvě možnosti, jež takovou úrovní disponují, a to eObčanku a kartu Starcos od

1. certifikační autority. Avšak banky se zaměřují hlavně na úroveň „značná“, přestože v rámci vlastní akreditace mají možnost mít i prostředky úrovně „nízká“. V případě, že poskytovatel služby vyžaduje přinejmenším úroveň „značná“, příkladem může být přihlašování k datovým schránkám, je spektrum nabízených možností přihlášení o poznání větší a obsahuje i možnosti přihlášení skrze vybrané banky, respektive bankovní identity. Jestliže si uživatel vybere v určité nabídce některou z možností přihlášení skrze banku, je opět přesměrován, a to na stránky náležité banky. Tam se musí přihlásit způsobem, jenž si předtím zvolil v rámci nabídky NIA. Uživatel se bude přihlašovat k identitě, pod kterou ho zná jeho banka. Avšak způsob, kterým k tomuto přihlašování přistupují jednotlivé banky, se někdy poněkud liší (Peterka, 2021).

3.1.2 SONIA

Pod pojetím SONIA si lze představit soukromoprávní NIA. To znamená, že se jedná o výše popsanou NIA pod správou soukromoprávních společností. Jde o projekt soukromých subjektů, kde u projektu NIA existuje alternativa, jejíž užití je nepovinné (HEX, 2021).

SONIA by měla občanům zprostředkovávat zjednodušené vyřizování svých záležitostí s úřady i se soukromými společnostmi, a to elektronicky. K tomu je nezbytné prokázat elektronicky vlastní identitu. V rámci České republiky ale tento všestranný „digitální“ doklad totožnosti, s jehož pomocí lze komunikovat se státními úřady nebo soukromými společnostmi, chyběl (Česká bankovní asociace, 2019).

Soukromoprávní bankovní identita je závislá především na společném řešení od bank. Toto řešení pracuje jako ona soukromoprávní NIA, přesněji řečeno jako agregátor služeb ověření identity dílčích bank, jež budou poskytovány soukromoprávním dodavatelům služeb, to znamená např. e-shopům a operátorům. Jednotné řešení bank by vlastně mohlo být pouze jedno, a to od společnosti Bankovní identita (BankID). Právě na jeho rozhraní by se připojovaly systémy soukromoprávních dodavatelů služeb, jež mají v úmyslu využívat soukromoprávní bankovní identitu pro přihlašování klientů k jejich službám.

Mezi služby bankovní identity patří například AML, KYC, CONNECT nebo SIGN. AML je služba, v jejímž rámci získáte kompletní sadu údajů o zákazníkovi. Tato sada zprostředkovává provedení vzdálené identifikace klienta dle AML zákona či dalších nařízení, jež musí daná firma dodržovat. Pomocí služby KYC basic lze získat sadu informací za účelem ověření zákazníka, a to například při přihlášení do klientské zóny nebo při dohodnutí nové smlouvy. CONNECT dává možnost užít bankovní identitu pro přihlašování,

kde se ke službám poskytovatele zákazník hlásí se stejnými údaji jako do svého internetového bankovnictví. Službu SIGN lze využít na úrovni zabezpečeného podpisu pro podpis dokumentů ve formátu PDF (Peterka, 2021).

3.1.3 Potenciál bankovní identity

Jak již bylo zmíněno v úvodu kapitoly Bankovní identity, severské státy či například Estonsko využívají bankovní identitu pro identifikaci při čerpání online služeb již několik let, a to úspěšně. Pro rozmach elektronizace české správy to představuje důležitou příležitost. V Česku používá internetové bankovnictví 97 % Čechů s přístupem k internetu. Zároveň Češi také značně důvěřují bankám a jejich řešením, týkajících se uživatelské přívětivosti a bezpečnosti. Stát tudíž zásluhou bankovní identity dosáhne dá se říct přes noc 5,5 milionu uživatelů, kteří budou moci užívat jeho online služby a zároveň s ním komunikovat. Tato skutečnost bude současně i velkým impulzem pro to, aby stát koncept služeb eGovernmentu nepřetržitě zdokonaloval a rozšiřoval (Česká bankovní asociace, 2021).

3.1.4 Výhody

Bankovní identita má řadu výhod, jež usnadňují klientům bank řadu činností. Mezi takové výhody se řadí například to, že má klient pouze jedno heslo či otisk prstu pro přihlášení do mnoha institucí (státních i soukromých), může si tak spoustu věcí vyřešit elektronicky. Další výhodou je, že pokud nastane situace, kdy se budou předávat osobní údaje prostřednictvím BankID, u řady formulářů budou tyto údaje předvyplněny. Výhodou je též to, že pokud se budou měnit některé údaje v klientově občanském průkazu, samy se aktualizují. BankID kromě toho také poskytuje elektronické podepisování smluv, takže v několika případech nemusí klient vážit cestu na pobočku (Bureš, 2021). Za pozitivum lze také považovat to, že identifikace má prostřednictvím bankovní identity stejný stupeň zabezpečení jako přihlášení do internetového bankovnictví. Banky ji zprostředkovávají zdarma a osoba, která ji využívá, má možnost získávat státní i firemní elektronické služby online a s její pomocí elektronicky podepisovat řadu dokumentů (HEX, 2021).

3.1.5 Nevýhody

Hlavní důvod, proč nechtít bankovní identitu, může představovat například bezpečnost. V případě, že by nastal jeden z nejhorších scénářů a útočník by se dostal do internetového bankovnictví klienta, tak by měl jednoduchou možnost využít elektronické služby státu pod

jeho identitou. Někdy by se tedy stát a banka měly považovat za dvě základní věci, které je nutno oddělit, aby se v situaci průniku minimalizovaly následky (Zmeškal, 2021). Z hlediska bezpečnosti je nevýhodou také elementárnost přihlášení skrze jednu aplikaci, což může vzbuzovat zájem útočníků. Pokud se potom klientovu BankID podaří prolomit, může to vést k nebezpečnému úniku informací (Bureš, 2021).

S příchodem bankovní identity se může též významně rozšířit tzv. phishing, který bude lépe vysvětlen v kapitole s názvem Kryptografie. Příčinou může být skutečnost, že se zkomplikuje ověření uživatelem, jestliže je stránka nebo služba, k níž má touhu se přihlásit, reálná služba eGovernmentu. Klient tak nemá žádnou možnost si validovat, že stránka, jež vyžaduje přihlášení, je skutečně službou zaznamenanou v NIA jako kvalifikovaný poskytovatel (Zmeškal, 2021).

Nevýhodou je též fakt, že díky bankovní identitě má každá banka o klientech mnoho informací. Tato data se budou dále předávat i třetím stranám, avšak pokaždé se souhlasem klienta (Bureš, 2021).

Banky se prezentují jako kvalifikovaný správce podobně jako v případě mojeID. Diferencí je, že mojeID si klient zřizuje úmyslně s cílem elektronické identifikace. Bankovní účet se většinou zakládá za docela odlišným účelem. Stát tedy dal možnost (teď se hovoří o NIA) zrodu bankovní identity, avšak je na místě otázka, jestli zabezpečil občanům dostatečnou ochranu vůči chování samotných bank (Zmeškal, 2021).

3.1.6 Alternativy

Jak již bylo zmíněno v odstavci výše, bankovní identita nemusí být a není jedinou možností pro prokazování identity například u veřejné správy. Další možností může být buď eOP, mojeID, karta Starcos, Mobilní klíč eGov a další. A právě ty se pokusí popsat a vysvětlit tato podkapitola.

eOP

Jedná se o občanský průkaz s aktivovaným čipem. Ten dává možnost jistého prokazování identity při využívání online služeb veřejné správy. Každý občanský průkaz vystavený po datu 1. července 2018 má čip. K použití elektronického občanského průkazu jako identifikačního nástroje pro přihlášení k online službám je třeba provést aktivaci. Znamená to vložení přístupových kódů na působišti osobních dokladů na kterémkoliv úřadu obce s rozšířenou působností, a to buď při vyzvednutí občanského průkazu, či později, když chce občan začít využívat občanský průkaz jako nástroj pro identifikaci. Pokud se držitel po

aktivaci rozhodne, že aktivované elektronické funkce již nadále nemá chuť používat, je možné je prostřednictvím jednoduchého telefonátu deaktivovat. Jestliže uživatel nemá zařízení s integrovanou čtečkou, jako jsou například vybrané klávesnice či notebooky, které čtečku zahrnují, musí si pořídit čtečku externí. Tu lze připojit prostřednictvím konektoru či bezdrátově (například pomocí Bluetooth). Další funkcí eObčanky je mimo jiné i vytváření kvalifikovaných elektronických podpisů, kde si držitel do čipu může vložit kvalifikované certifikáty pro tvoření elektronických podpisů (Správa základních registrů, 2020).

MojeID

Služba mojeID je více než 10 let zprostředkovávaná sdružením CZ.NIC. Eviduje tisíce uživatelských účtů, z nichž je část již připojena k Národnímu bodu pro identifikaci (NIA). Přes zmíněný bod si mohou uživatelé zjednodušit řadu činností, jako je například bezpečná komunikace se zdravotní pojišťovnou či daňovým úřadem, jak již bylo zmíněno v kapitole NIA. Získání účtu mojeID a jeho používání je zcela zdarma, přičemž cena bezpečnostního klíče činí přibližně 600 korun českých. MojeID dostala od Ministerstva vnitra akreditaci na úroveň záruky „vysoká“. Předpokladem je užití specifického hardwarového klíče. Takovou akreditaci měla doposud pouze společnost První certifikační autorita, vyjma toho ji poskytuje státní eOP s čipem (Kučera, 2021).

Karta Starcos

Čipová karta Starcos byla uznána Ministerstvem vnitra za nástroj k elektronické identifikaci s vysokou úrovní záruky. Zásluhou této skutečnosti funguje pro každou službu veřejné správy, ke které je možno se přihlásit prostřednictvím nástrojů pro elektronickou identifikaci pomocí NIA. Tento způsob elektronické identifikace od První certifikační autority má podobné využití jako již dříve zprovozněné východisko pomocí aktivovaného elektronického občanského průkazu (eOP) (Ministerstvo vnitra České republiky, 2020).

Z praktického hlediska se nenachází mezi těmito možnostmi příliš velká diference. Elektronické občanky představují ve skutečnosti také čipové karty podobně jako karta Starcos. Pouze neobsahují komerční certifikát, ale mají na čipu identitní applet. Diference se nenachází ani v základní myšlence fungování. Karta Starcos a eOP nepředstavují ve skutečnosti zdroj elektronické identity, i když jsou nazývány jako nástroje pro elektronickou identifikaci. V jejich případě se totiž nejedná o „poskytování identity“ přinejmenším v tom významu, že by zmíněné nástroje zprostředkovávaly protistraně skutečné údaje o identitě osoby, jež se aktuálně přihlašuje. Skutečnost je tedy taková, že nová eOP i karta Starcos

s certifikátem představují pouze určité „průkazy“, jenž proti prostředníkovi dokazují, že uživatel, který se snaží přihlásit, je doopravdy ten, za koho se vydává. Avšak údaje, jež charakterizují, o koho se jedná, jako jsou například jméno nebo datum narození, protistraně říká až daný prostředník, tedy NIA (Peterka, 2020).

Mobilní klíč eGov

Mobilní klíč eGovernmentu je identifikačním prostředkem, jenž poskytuje sám stát, a to zcela bezplatně. Reprezentuje přihlašování, aniž by muselo dojít k zadání jiných ověřovacích kódů. Po instalaci a následné aktivaci klíče eGovernmentu je uživateli zprostředkováno přihlašování k službám, které používají elektronickou identifikaci pomocí NIA. Pro zajištění fungování tohoto nástroje je nezbytné mít nainstalovanou na mobilu aplikaci mobilního klíče (Ministerstvo vnitra České republiky, 2021).

3.2 E-government

Jedná se o online administraci dotyčné vlády, jež využívá informační a komunikační technologie (IKT) pro posílení otevřené administrativní komunikace za účelem posílení korespondenčních kanálů a obecně celé společnosti. Správný gouvernement je zásadní pro dobrý život každého občana. Ten se udrží v případě, že vláda, politické strany, parlament, soudnictví a média budou pracovat komplexně a systematicky. Použití slova e-government tedy znamená správu elektronických systémů pro lepší služby a dostupnost (Kumar, 2018). Jedná se o proces, jenž by měl vést k převedení pracovní náplně související s výkonem veřejné správy do elektronické podoby. Klíčovými dopady, které se zabývají zavedením e-governmentu, by mělo být zlepšení výměny informací a zjednodušení komunikace mezi úřady, firmami a občany (EZDRAV.cz, 2019).

3.2.1 Typy e-governmentu

Jednotlivými typy eGovernmentu jsou (Kumar, 2018):

- G2G (Government to Government): jde o elektronickou správu, která probíhá pouze mezi vládními subjekty. Může jít například o interakci mezi různými vládními agenturami nebo národními, provinčními a místními vládními agenturami. Může jít také o komunikaci mezi odlišnými úrovněmi v organizaci.
- G2C (Government to Citizen): zahrnuje interakci mezi vládou a občany. Hlavním cílem a zaměřením je poskytnout přístup ke schématům gouvernementu a službám

pro každého občana. Příkladem G2C může být online registrace daně z příjmu nebo vyhledávání narození/ úmrtí a jiných dokumentů.

- G2B (Government to Business): představuje interakci mezi vládou a obchodem za účelem vytvoření transparentnějšího a efektivnějšího obchodního prostředí. Zahrnuje služby, jako jsou online registrace, zajištění povolení, licence, platby daní a další.
- G2E (Government to Employees): tento způsob elektronické správy zajišťuje komunikaci mezi vládou a jejími zaměstnanci. Příkladem G2E můžou být online konference nebo školení pro zaměstnance.

3.2.2 IoT a e-government

Jedním z největších a nejdůležitějších problémů, s nimiž se setkávají odborníci v oblasti IT, je predikce negativních, nebo pozitivních účinků, které způsobují každodenní aktivity ve společnosti. Zabezpečení a správa představují nejobtížnější problematiky v IoT. Myšlenky pro e-government založený na IoT nejsou zcela zformulovány a průmyslové nebo výzkumné asociace navrhují různé definice a nápady. Podle Evropské unie naráží administrativa na principy, postupy a chování, jež ovlivňují způsob, jakým jsou pravomoci zpracovány, zejména pokud jde o transparentnost, spolupráci, odpovědnost a srozumitelnost. V poslední době mohou fúze distribuovaných výpočtů a IoT společně s cloudovými výpočty díky svým neomezeným kapacitám přinést daným zúčastněným stranám zisk.

IoT využívá internet k míchání odlišných heterogenních věcí a dává těmto věcem jednoduchý význam. Každá zmíněná „věc“ musí být připojena k internetu. Senzorové systémy, které jsou založené na IoT, lze využít k monitorování nadměrného využívání energie, jako jsou například správa světla nebo ventilačního systému. K dosažení tohoto bodu mohou být senzory umístěny v různých oblastech, aby shromažďovaly a šířily informace, které by vedly ke změně využití (zefektivnění). IoT má také obrovské výhody v oblasti zdravotní péče, kde existuje možnost sledovat stav pacientů s nějakým konečným cílem, a to za účelem poskytnutí co nejlepších a nejrychlejších výsledků lékaři (Kumar, 2018).

3.2.3 E-government v České republice

Původní idea, na jejímž základě mělo dojít k použití informačních technologií v české státní správě, se zrodila už na počátku devadesátých let dvacátého století. K realizaci této idey došlo v roce 1999, kde prvotní elektronickou funkcí pro občany České republiky

představovala šance předložit žádost o informace podle zákona o svobodném přístupu k informacím pomocí elektronické pošty (Vodička, 2014).

Mezi základní současné prvky eGovernmentu v České republice patří například: Czech POINT, datové schránky nebo základní registry. Všechny tři vybrané prvky budou rozebrány v odstavcích níže.

Czech POINT

Zkratku Czech POINT lze definovat, jako Český Podací Ověřovací Informační Národní Terminál. Ten byl vytvořen jako projekt, jenž měl za cíl sjednotit komunikaci se státem do jednoho všestranného místa, na němž je možno opatřit si data z informačních systémů, přepracovat psané dokumenty do elektronické podoby, a opačně dostat informace ze správních řízení nebo přednést znění k započetí řízení správních orgánů. Má tak simplifikovat komunikace mezi státem a občanem. Primárním cílem Czech POINT je řešení všech problémů občana vzhledem k veřejné správě z pohodlí domova (Vaníček, 2011).

Souhrnně ho lze vystihnout jako místo ve státní správě, kde dochází ke řešení požadavků zákazníků, a to jak na počkání, tak v delších zákonných lhůtách. Hlavní skutečností je, že výsledky z provozu kontaktních míst již nepředstavují jenom papírovou formu, ačkoli pořád dominuje, avšak může dojít k jejich doručení v elektronické podobě rovnou daným příjemcům (Felix, 2015).

Služby, jež Czech POINT na kontaktních místech zprostředkovává veřejnosti, je možné rozdělit do několika kategorií. Těmi jsou: výpisy ze systémů veřejné správy (např. z trestního rejstříku), předložení žádostí ke státní správě, datové schránky (např. požadavek o deaktivaci přihlašovacích údajů), základní registry, různé změny na žádost (např. Centrální uložiště ověřovacích doložek) a umožněná identifikace osoby. Jako kontaktní místa si lze představit zejména Českou poštu, obecní či krajské úřady, notáře, nebo banky, jimž Ministerstvo vnitra dalo příslušnou autorizaci. Pro úspěšné získání výpisu či učinění podání je potřeba s sebou na kontaktní místo donést některé podklady. Může se například jednat o doklad totožnosti, plnou moc, peníze a další (Mašínová, 2019).

Datové schránky

Datové schránky pracují na obdobném principu jako e-mailová schránka, avšak zprostředkovávají to největší ověření identity odesílatele. Probíhá skrze ně spojení jak mezi úřady, tak s podnikateli a za peněžní poplatek mohou podnikatelé komunikovat i vzájemně. Jedná se tedy o státem zaručený prostředek elektronické komunikace, jenž má vystřídat

papírové dopisy. Využívají se z velké části pro komunikaci s orgány veřejné moci (Solitea a.s., 2020). K jejich vzniku došlo podle zákona o elektronických úkonech a autorizované konverzi dokumentů, aby zajistily přesvědčivé a garantované spojení s veřejnou správou. Její předchůdce už na počátku digitalizace veřejné správy představovaly tzv. elektronické podatelny, jež vznikly na základě zákona o elektronickém podpisu. Podobně byl v dalších obdobích vytvořen transakční sektor Portálu veřejné správy, s jehož pomocí docházelo k vypořádávání podání odlišných životních situací. U obou zmíněných platforem byl ale požadován elektronický podpis, jehož využívání bylo docela komplexní a nákladné. Další nevýhodou byla skutečnost, že žádná z nich nebyla schopna splnit požadavky bezpečného, efektivního a důvěryhodného spojení občanů, společností nebo podnikatelů s veřejnou správou (Felix, 2015). Datové schránky byly tedy zřízeny z toho důvodu, aby (Solitea a.s., 2020):

- snížily režie týkající se papírové komunikace.
- zjednodušily a zefektivnily vzájemnou komunikaci podnikatelů a úřadů.
- vzrostla vyhlídka na správné doručení zpráv (datové schránky se pyšní i 99 % možností doručení na rozdíl od 45 % u doporučených dopisů).
- poskytly příležitost získání důkazné informace o doručení dokumentu (dokumenty v elektronické podobě disponují totožnou právní účinností jako papírový dopis s patřičným potvrzením, a pokud dojde k uložení zprávy, nachází se možnost její obsah kdykoli dokázat).

Jsou tři způsoby, jak datovou schránku založit, a to buď osobně na pobočce Czech POINT, online nebo poštou. V dnešní době je nejspíše nejjednodušší cestou její zřízení na stránce mojedatovaschranka.cz. Schránku lze založit též skrze portál eIDENTITA.cz. Na serveru se vyskytuje mnoho možností, jak se skrze zmíněný portál přihlásit. Jedná se například o Mobilní klíč eGovernmentu, eOP, mojeID nebo též o bankovní identitu. Jestliže ji banka nabízí, s její pomocí se klient může dostat do portálu eIDENTITA a je schopen si datovou schránku zřídit z domova. Přihlášení do schránky pak probíhá prostřednictvím totožných údajů, jež klient použil při jejím zakládání (Vokřál, 2021). Jestliže jde o subjekt, jenž má ze zákona uvedenou povinnost vlastnit datovou schránku, bude mu schránka založena automaticky, až daný subjekt realizuje zápis do evidence, jenž stanovuje zákon. Jde například o obchodní rejstřík nebo seznam insolvenčních správců (Vodička, 2014).

Použití datových schránek lze tedy rozdělit na povinné a nepovinné. Povinné je zejména při oboustranné komunikaci orgánů veřejné moci, spojení s vybranými právnickými osobami, či komunikaci s fyzickými nebo právnickými osobami, jež si datovou schránku založily sami od sebe. Povinné použití je nařízeno s cílem minimalizace ekonomických nákladů. Nepovinné použití datových schránek je při spojení fyzických osob s orgány veřejné moci nebo při oboustranné komunikaci osob, jež podnikají (Vaníček, 2011). Od okamžiku, kdy si daná osoba vytvoří datovou schránku, probíhá veškerá komunikace s úřady jenom skrze ni. Zprávy uvnitř schránky jsou uloženy po čas 90 dnů a pokládají se za doručené ve chvíli, kdy se osoba, jenž má kompetence zprávu číst, k datové schránce přihlásí. Jestliže se uživatel nepřihlásí, je pokládána za doručenou již desátým dnem po jejím předání do datové schránky (Vokřál, 2021).

Základní registry

Základní registry veřejné správy jsou složkou jejího moderního provozu a představují jádro celého eGovernmentu. Byly vytvořeny za účelem efektivního využívání soudobých informačních technologií, zesílení výkonnosti státní správy, zefektivnění zpracování žádostí ze stran jedinců či firem a snížení byrokracie. Systém základních registrů byl stvořen v reakci na stav, kdy předcházející způsoby a systémy shromažďování a uchovávání údajů už nebyly vhodné, jelikož docházelo k duplicitnímu vedení údajů. Údaje byly také v odlišné kvalitě v nejrůznějších rejstřících, evidencích nebo registrech. Dané osoby pak byly zatíženy skutečností, že musely stále dokola poskytovat totožné údaje a dokládat jejich korektnost. Zákon týkající se základních registrů tedy stmelil rozdrobenost právní úpravy informačních systémů veřejné správy (BusinessInfo.cz, 2020).

Základní registry se skládají ze čtyř hlavních registrů. Těmi jsou: registr osob, registr obyvatel, registr územní identifikace, nemovitostí či adres a registr práv a povinností. Vesměs jde o systém, jenž dává dohromady data dílčích úřadů. Předávání a přístup k těmto datům je umožněn přes Informační systém základních registrů. Základní registry zachází s tzv. referenčními údaji (Felix, 2015). Ty ztělesňují unikátní a důvěryhodné údaje, jež jsou vedené v daném základním registru veřejné správy, který je sdílený každým významným informačním systémem veřejné správy podle jednoznačně stanovených pravidel. Díky tomu je zabezpečen soulad obsahu všech informačních systémů veřejné správy z hlediska flexibilní a bezpečné aktualizace (BusinessInfo.cz, 2020).

Jestliže tedy nastane změna u některého z údajů, jsou samočinně přepsány do aktuálního stavu v každém registru a společnosti, občané, podnikatelé či ostatní už nemají povinnost změny hlásit na všech dílčích úřadech zvlášť. O registr obyvatel se stará Ministerstvo vnitra ČR, přičemž je v rámci něho možné nalézt referenční informace o fyzických osobách, jako jsou například datum narození, příjmení, jméno, adresy dočasných nebo trvalých pobytů a jiné. Registr osob je řízen Českým statistickým úřadem a posluhuje zejména k evidenci právnických či podnikajících fyzických osob. Dává tedy přístup k referenčním údajům týkajících se názvů obchodních společností, dat jejich vzniku, ID datové schránky nebo právní formy. Registr územní identifikace, nemovitostí a adres vede Český úřad zeměměřický a katastrální. Zahrnuje informace týkající se katastrálních ulicí, územích, stavbách nebo pozemcích atd. Zprostředkovává tak evidenci územní segmentace. Registr práv a povinností je řízen Ministerstvem vnitra ČR a dává kompetence dílčím editorům a uživatelům základních registrů pro vstup k referenčním údajům ve zbylých registrech (Felix, 2015).

Hlavním problémem, jenž v poslední době trápí „páteřní" systém českého eGovernmentu, jsou kapacitní možnosti základních registrů. Tento problém je způsobený také nedostatkem finančních prostředků pro případné rozšíření kapacit a celkovou modernizaci registrů. Registry jsou přitom klíčovým nástrojem pro implementaci novely zákona o bankách, voleb do Poslanecké sněmovny, sčítání lidu, jež proběhlo v roce 2021, nebo pro samotný nouzový stav, během něhož docházelo k tvorbě mnoha požadavků na velké množství dat ze základních registrů ve velmi krátkém čase. S postupem času stárne a odchází i hardware. Problémem však není jenom stáří HW infrastruktury, ale také ukončení softwarové podpory jako například u licencí Oracle, jelikož je není možné použít na aktuální technologie (Slížek, 2021).

Budoucnost veřejné správy v ČR

V příštích několika letech by měly čekat úřady značné výzvy, a to včetně elektronizace. Změny by měly nastat například v oblasti poskytování digitálních služeb, kde orgány veřejné moci mají povinnost poskytovat digitální služby, avšak v první řadě musí dát možnost klientům využívat digitální služby orgánů ostatních. Typickou ukázkou je obměna paradigmatu v ověřování údajů, kde je možné, aby uživatel prokázal realitu odkazováním na zprostředkovanou digitální službu. Další oblastí, která se dočká změny, je používání informací z agendových systémů. Novou skutečností v této oblasti je obměna vzoru

používání informací vzhledem k činnostem veřejné správy. Do nedávna musela veřejná správa používat jako povinné jenom referenční údaje ze základních registrů, avšak aktuálně se nastoluje celková nutnost používat předané údaje z agendových informačních systémů přes jednotlivé pracovní činnosti veřejné správy. Poslední oblastí, jež byla vybrána jako příklad v rámci diplomové práce, je potencionální ukončení rodných čísel a založení klientských či stykových identifikátorů. Přičemž rodné číslo by se nemělo od roku 2023 vyskytovat na dokladech totožnosti. Následně by se mělo od roku 2029 ukončit jeho zakládání čerstvě narozeným osobám. Veřejná správa se díky této skutečnosti nachází před klíčovou povinností, a to nebrat rodné číslo jako jediný, jasný a rozhodující identifikátor určité fyzické osoby (Rada, 2021).

3.2.4 E-government ve vzdělání

E-government lze tedy chápat jako rychlý a efektivní nástroj, který poskytuje služby veřejnosti za pomoci informačních technologií, a to účelným způsobem bez jakéhokoli byrokratického zdržení. V oblasti zdravotnictví je díky eGovernmentu například možné, aby vláda podala svým občanům základní informace o veřejné hygieně a dalších preventivních opatřeních v boji proti smrtelným chorobám. Podobně je možné pomocí elektronické správy rozšířit a zlepšit kvalitu vzdělávacího systému a reformovat ho tak, aby odpovídal budoucím výzvám a požadavkům. Příkladem může být zemědělský sektor, kde je možné vzdělávat zemědělce ohledně metod, jež mají být přijaty za účelem zvýšení růstu zemědělství, příjmů a podobně (Kumar, 2018).

3.2.5 Přínosy e-governmentu

Elektronická správa má oproti tradičním vládním metodám řadu výhod. Těmi mohou být například (Kumar, 2018):

- Všechny zásady a služby jsou od lidí vzdáleny pouze na „jedno kliknutí“. Díky tomu jsou transparentnější a důvěryhodnější.
- E-government je pro uživatele plynulejší a rychlejší, jelikož provedení dané činnosti zabere méně času.
- Šetří tedy lidem čas i peníze, protože nemusí cestovat po různých kancelářích, a omezuje korupci, což vede ke snížení nákladů a lepšímu růstu příjmů.
- Elektronicky přístupné služby vyžadují méně papíru, a proto jsou šetrnější k životnímu prostředí.

Jak již bylo nastíněno výše, eGovernment přináší větší uživatelský komfort. Elektronizace tak zefektivňuje a zjednodušuje komunikaci a podporuje demokratizaci veřejné správy coby služby. Tyto výhody by tedy neměly směřovat pouze k adresátům, ale i k úředníkům, kteří díky eGovernmentu nemusí věnovat tolik času nutnému papírování. Výsledkem by tak mělo být zefektivnění úkonů veřejné moci, kde by úřady fungovaly 7 dní v týdnu 24 hodin denně (EZDRAV.cz, 2019).

3.3 Kryptografie

V rámci kapitoly Kryptografie bude vysvětleno, co to vlastně kryptografie je a čím se zabývá. Dále se bude zabývat tématy, jež určitým způsobem souvisí přímo s bankovní identitou.

Kryptografie je věda, která se zabývá výzkumem matematických metod skrývání obsahu i prokazování zdroje přenášených zpráv. Zprávou se v tomto případě rozumí číselná posloupnost, v níž je otevřeně známým kódem zakódována informace. Autorem zprávy je tzv. původce. Ten svou zprávu zasílá žádoucím přenosovým systémem (typicky přes počítačovou síť) konkrétnímu příjemci, tzv. adresátovi. Kryptografické techniky poskytují původci a adresátovi možnost zaručit ochranu přenášených zpráv před různými hrozbami. Co se týče skrývání obsahu zpráv, útočníci nejsou schopni odhalit, jaké zprávy jsou v přenosovém kanálu. Tomu se říká tzv. důvěrnost zpráv.

Zabezpečenou komunikaci mezi původcem a adresátem formuluje tzv. kryptografický protokol, jehož základem jsou datové jednotky. Jedná se o bloky bitů, jež si mezi sebou střídají původce a adresáta. Všechny typy datových jednotek mají vlastní určenou strukturu a svůj význam. Vyjma odlišných typů datových jednotek je součástí protokolu i sada pravidel, která výměna datových jednotek mezi původcem a adresátem dodržuje (Burda, 2019).

3.3.1 Přístupové systémy

Pod pojmem přístupové systémy si lze představit takové systémy, jež řídí přístup k aktivům, přičemž tento pojem představuje cokoliv, co má nějakou hodnotu. V praxi jde většinou o data, počítačové nebo komunikační služby, tajné skutečnosti či movitý majetek. Ke zmíněným aktivům se snaží přistupovat tzv. entity, což jsou obvykle osoby, avšak mohou to být i zařízení, jako jsou robotická vozidla, servery apod. (Burda, 2019).

Přístupové systémy neboli systémy kontroly přístupu provádějí ověřování totožnosti a autorizaci uživatelů a subjektů vyhodnocením požadovaných přihlašovacích údajů, jež mohou představovat hesla, biometrické kontroly, osobní identifikační čísla (PIN), biometrické kontroly, tokeny zabezpečení nebo jiné ověřovací faktory. Často důležitou a využívanou součástí vrstvené obrany sloužící k ochraně systémů řízení přístupu je multifaktorové ověřování, které vyžaduje dva nebo více ověřovacích faktorů (Lutkevich, 2020).

Architektura přístupových systémů

Na přístupové systémy lze pohlížet jako na téměř výběrově fungující překážku mezi entitami a aktivy. Entita, která má zájem o přístup k aktivům, musí v první řadě zkontaktovat náležitou autoritu (většinou jde o správce nebo majitele aktiv) a požádat ji o přístupová práva. Jestliže entita vyhovuje stanoveným požadavkům, tak jí autorita náležitá práva udělí. V obvyklých přístupových systémech jsou práva napojena na identitu entity, a tak se z hlediska autorizace také sjednává:

- Identita: představuje v přístupovém systému jednoznačný identifikátor příslušné entity.
- Dokazovací faktor – je něco, pomocí čeho entita systému dokazuje svou identitu, a tedy i svá práva.
- Ověřovací faktor – data, jimiž sytém ověřuje identitu dané entity.

Postup je takový, že pro autorizovanou entitu poté autorita zadá do systému kontroly přístupu její identitu, určená práva a ověřovací faktor. Od následujícího okamžiku má příslušná entita povoleno přistupovat k aktivům. Vyjma samotného řízení přístupu je přístupový systém rovněž schopen evidovat, jaké činnosti entity v přístupovém systému provádějí a informace poté autoritě poskytovat. Tomu se říká tzv. účtování neboli „accounting“) (Burda, 2019).

Typy přístupových systémů

Mezi hlavní modely řídící přístup patří například povinné řízení přístupu (v angličtině Mandatory acces control). Jde o bezpečnostní model, v němž jsou přístupová práva regulována ústředním orgánem na základě více úrovní zabezpečení. Tento model se často využívá ve vládních a vojenských prostředích. Jako další bude zmíněn model volitelného řízení přístupu (v angličtině Discretionary access control). V rámci tohoto modelu mohou

vlastníci a správci chráněného systému, dat nebo prostředků nastavovat zásady, které určují, kdo či co je oprávněno přistupovat ke zdroji. Běžnou kritikou systémů volitelného řízení je nedostatečná míra centralizovaného řízení. Následujícím modelem je řízení přístupu na základě rolí (Role-based acces control). Jedná se o široce využívaný mechanismus, jenž omezuje přístup k počítačovým prostředkům na základě jednotlivců nebo skupin s jasně definovanými byznysovými funkcemi, jako je například výkonná či inženýrská úroveň. Je to bezpečnostní model, jenž se opírá o složitou strukturu přiřazování, autorizace a oprávnění rolí za účelem dirigování přístupu zaměstnanců k systémům. Jako předposlední bude zmíněn model řízení přístupu na základě pravidel (Rule-based access control). V tom správce systému definuje pravidla, kterými se reguluje přístup k daným objektům. Pravidla obvykle vycházejí z podmínek, jako jsou denní doba nebo místo. Posledním modelem je řízení přístupu na základě atributů (Attribute-based access control). Jedná se o metodiku, jež spravuje přístupová práva prostřednictvím vyhodnocení sady pravidel, zásad a vztahů pomocí atributů uživatelů, systémů a podmínek daného prostředí (Lutkevich, 2020).

3.3.2 Autentizace versus autorizace

Ačkoli oba termíny zní téměř stejně, odkazují na zcela odlišné bezpečnostní procesy. V rámci oblasti správy identit se autentizace zabývá ověřením identity uživatele, kdežto autorizace ověřuje, zda má daný uživatel přístup k provádění konkrétní funkce. Důkladněji budou tyto dva pojmy a jejich metody popsány níže.

Autentizace

Autentizace je zjednodušeně řečeno proces identifikace uživatelů a ověřování, za koho se prohlašují. Jedním z nejběžnějších faktorů ověřování identity je heslo (Irshivangini, 2020). Pro zajištění jednoznačné diferenciace se entity označují jedinečnými identifikátory (například u osob jde o příjmení nebo křestní jména). Pojem identifikace poté znamená proces zjištění identifikátoru určité entity. Identifikace může být buď průkazná, nebo neprůkazná. Jestliže se mluví o průkazné identifikaci (tzv. autentizaci), je identita určité entity posouzena s požadovanou mírou záruk. V případě neprůkazné identifikace není možné posouzený identifikátor entity považovat za dostatečně důvěryhodný. Klasicky jde o situaci, kde se například daná osoba jednoduše představí (tzn. sdělí svůj identifikátor), aniž by vlastní tvrzení nějakým způsobem prokázala (Burda, 2019). Autentizace může být tedy například skutečnost, že se uživatel pomocí svých přihlašovacích údajů (jméno/heslo) do

internetového bankovnictví nebo zodpovězením bezpečnostních otázek identifikuje a ověří se tak, že je tím, za koho se vydává (Sullivan, 2018).

Autorizace

Autorizace oproti autentizaci určuje, jaká oprávnění má uživatel v dané aplikaci. Jinými slovy vymezuje, jaké akce mohou uživatelé provádět, co mohou dělat, například zda mohou požadovat či upravovat data. Autorizační proces také uděluje povolení třetím stranám ohledně přístupu k údajům, a to jménem uživatelů. Tím se myslí například skutečnost, že se uživatel může přihlásit do aplikace třetí strany prostřednictvím Facebooku nebo Googlu (Sullivan, 2018). Autorizace tedy nastává až po úspěšném ověření identity uživatele. V praxi to funguje tak, že jakmile je zaměstnanec autentizován pomocí ID a hesla, je dalším krokem definování, ke kterým zdrojům by měl mít přístup. Může se například jednat o částečná, nebo úplná práva k databázi, fondům a dalším důležitým informacím (Irshivangini, 2020). Autorizace je též obzvláště důležitá u aplikací, jejichž cílem je zkvalitnit život uživatelů v oblasti bankovnictví. Dává uživatelům možnost přistupovat ke svým bankovním údajům v jakékoli aplikaci, s níž se je rozhodnou sdílet. Tato skutečnost jim zprostředkovává přístup k finančním nástrojům, jež mohou napomoci zejména s investováním, rozpočtováním svých financí nebo s vytvořením plánu, jak se zbavit dluhů (Sullivan, 2018).

Autentizační metody

Autentizace se obvykle provádí zadáním uživatelského jména a hesla. Jedná se o základní kámen online zabezpečení, jelikož zajišťuje, že k požadovaným a často i citlivým informacím přistupuje správný uživatel. Mezi prostředky autentizace tak patří například skenery na ověřování otisků prstů, bezpečnostní otázky či přihlašovací údaje k bankovnímu účtu. Jako metodu autentizace lze uvést autentizaci dvoufaktorovou (2FA). Při jejím využívání zadá nejprve uživatel své uživatelské jméno a heslo a poté potvrdí přijetí jednorázového hesla, jež mu bylo zasláno na jeho e-mailovou adresu nebo prostřednictvím SMS (Sullivan, 2018). Vyžaduje tak více než jednu úroveň zabezpečení. Jako další metoda bude uvedena tzv. autentizace bez hesla. Zde se uživatel ověřuje pomocí jednorázového hesla (OTP), nebo magického odkazu, jenž mu je doručen na registrovaný e-mail nebo telefonní číslo. Jinou metodou je například tzv. jediné přihlášení (single sign-on). To umožňuje uživatelům přístup k více aplikacím s jedinou sadou přihlašovacích údajů. Jako poslední možnost autentizace, která bude v práci zmíněna, je ověření uživatele prostřednictvím přihlašovacích údajů z platforem sociálních sítí, kde se uživatel k dané

aplikaci může přihlásit nebo zaregistrovat pomocí stejných přihlašovacích údajů, jako má například při přihlašování na Facebook (Irshivangini, 2020).

3.3.3 Autentizační protokoly

Protokoly, jež se nacházejí v přístupových systémech, lze rozdělit na autentizační, autorizační a přístupové. Autentizační protokoly mají jediný účel, a to autentizaci žadatele (Burda, 2019). Ověřování uživatelů v rámci aplikací je jednou z největších výzev současnosti, se kterými se informační technologie potýkají. Existuje velké množství systémů, k nimž uživatel potřebuje přístup, a proto je převážná většina autentizačních protokolů představována otevřenými standardy (Mehl, 2018). Mezi autentizační protokoly lze řadit zejména HTTP autentizaci BAA a DAA, síťový protokol Kerberos, obecný protokol EAP nebo webový protokol OpenID Connect. Vysvětleny budou pouze některé z nich.

Autentizace BAA a DAA se používá k autentizaci stran, jež komunikují pomocí protokolu HTTP. Ten tvoří základ („World Wide Web“) webového systému, což je globální systém sloužící k práci s elektronickými dokumenty, které jsou psané v jazyce HTML. Pro ověření uživatelů webových serverů se využívá autentizace hesla. Na základě normy jsou standardizovány dvě metody, jež lze pojmenovat zkratkami BAA („Basic access authentication“) a DAA („Digest access authentication“). Metoda BAA se například vyznačuje tím, že se heslo uživatele prostě přenáší protokolem HTTP v otevřené formě, a tudíž je nutné spojení mezi uživatelem a serverem nejdříve zabezpečit – často se využívá protokol TLS. Naopak metoda DAA používá kryptografii přímo (Burda, 2019).

Jako druhý a zároveň poslední z autentizačních protokolů bude stručně popsán protokol Kerberos. Jedná se o síťový ověřovací protokol, který je navržen tak, aby poskytoval silnou autentizaci pro aplikace klient/server. Dává uživatelům sítě velkých organizací možnost tzv. jednorázového přihlášení, kde se uživatel během příchodu do práce autentizuje oproti svému počítači a zmíněný počítač se poté po celý zbytek pracovní doby autentizuje vůči serverům určité organizace jménem svého uživatele. Bezplatná implementace tohoto protokolu je k dispozici od Massachusetts Institute of Technology a je samozřejmě k sehnání také v mnoha komerčních produktech. Nejzákladnějšími kroky k ověření jsou (Mehl, 2018) (Bouška, 2014):

1. Klient požaduje autentizační tiket (TGT – „Ticket – Granting Ticket“) z klíčového distribučního centra („Key Distribution Center“).

2. Distribuční centrum ověří přihlašovací údaje a zašle zpět zašifrovaný autentizační tiket a klíč dané relace (ten je šifrovaný hashem klientova hesla).
3. Klient žádá o přístup k aplikaci na serveru. Posílá tedy žádost o tiket pro aplikační server („Service Ticket“) do distribučního centra.
4. Distribuční centrum vrací uživateli „Service Ticket“ a klíč dané relace.
5. „Service Ticket“ je odeslán na aplikační server. Jakmile je tiket a autentizátor přijat, server může klienta ověřit.
6. Server odpovídá a zasílá klientovi potvrzení. Po obdržení potvrzení od serveru může klient ověřit server. Ověřil se tedy nejen klient na serveru, ale i server proti klientovi.

3.3.4 Autorizační protokoly

Autorizace byla již výše definována jako akt, kdy autorita uděluje žadatelovi přístupová práva. V kontextu s ukládáním dat velkého množství uživatelů na sociální sítě ale nastal problém, jak tito uživatelé budou ovládat přístup ostatních uživatelů ke svým datům, která jsou ale uložena na cizích serverech. Reakcí je autorizační protokol OAuth (Burda, 2019).

OAuth je autorizační protokol nebo také framework, jenž popisuje, jak nesouvisející servery a služby mohou bezpečně povolit ověřený přístup ke svým aktivům, aniž by ve skutečnosti došlo ke sdílení počátečních přihlašovacích údajů. Typickým příkladem je, když se uživatel dostane na webovou stránku a ta mu nabízí možnost přihlášení pomocí přihlášení či nějaké služby jiného webu. Poté uživatel klasicky klikne na tlačítko, jež je propojené s jinou webovou stránkou. Druhá stránka ho autentizuje a webová stránka, na niž se původně připojoval, ho sama přihlásí pomocí povolení získaného z druhé webové stránky (Grimes, 2019). V souhrnu se tedy jedná o autorizační framework, který umožňuje aplikacím získat omezený přístup k uživatelským účtům v HTTP službě, jako je například Facebook, GitHub či DigitalOcean (Mehl, 2018).

OAuth versus OpenID Connect

OpenID Connect je oproti OAuth protokol autentizační. Jedná se o standard, jenž rozšiřuje protokol OAuth o jednoduchou vrstvu identity. Tato vrstva staví na OAuth, avšak nikoli na jeho úpravách, ale dává možnost, aby protokoly spolupracovaly a zároveň poskytovaly jednotné přihlašování a autorizaci pro přístup k API jménem uživatele. Samotné OpenID Connect toho dosahuje například prostřednictvím tokenů. Dokáže tedy „proměnit“

OAuth autorizační server na poskytovatele identity (či poskytovatele OpenID) (Brady, 2015).

3.3.5 Přístupové protokoly

Přístupové protokoly zabezpečují ovládání přístupu v tzv. distribuovaných systémech, to znamená v přístupových systémech, jež se skládají z geograficky rozptýlených zařízení. Typicky se jedná o systémy s centralizovanou konfigurací. Příkladem může být protokol RADIUS. Ten se často využívá ke správě přístupu stanic uživatelů do počítačových sítí LAN (Burda, 2019).

Protokol RADIUS je AAA protokolem. AAA, jinak řečeno autentizace, autorizace a účtování, je protokol, jenž dává možnost monitorovat, zda a k čemu má daný uživatel přístup. Dále také umožňuje sledovat aktivity uživatele uvnitř systému. Model AAA je sestaven tak, aby fungoval v prostředích s odlišnými požadavky uživatelů a odlišnými návrhy sítě. Autentizace a autorizace byly vysvětleny v odstavcích výše. Zbylé účtování slouží k monitorování toho, jaké zdroje využívá připojený uživatel. Jedná se například o spotřebované množství dat či souhrnnou dobu připojení. Protokol RADIUS byl vytvořen společností Livingston Enterprises, jež zareagovala na poptávku společnosti Merit Networks. Ta vyžadovala autentizační, autorizační a účtovací služby pro uživatele, již potřebovali přístup ke komplexním datům (Hassell, 2003).

3.3.6 Phishing a bankovní identita

S příchodem bankovní identity se může rozšířit tzv. phishing. Jedná se o podvodnou techniku používanou na internetu, při níž se útočník snaží získat osobní a velmi citlivé údaje klienta. Těmito údaji může být například heslo, číslo kreditní karty či osobní údaje v elektronické komunikaci. Základní myšlenou phishingu je rozesílání na první pohled důvěrných e-mailových zpráv nebo SMS, jež adresáta vyzývají k potřebnému zadání osobních údajů. Stránka uvedená v takové zprávě může být velice podobná bance adresáta, tudíž je podstatné si zprávu předem ověřit u banky, a to nejlépe telefonicky a ihned (Duofinance, 2021).

3.3.7 Internetové bankovnictví

Jedná se o elektronický systém, jenž bankovním klientům zprostředkovává možnost vzdáleně spravovat peníze na jejich účtu. Pomocí zmíněného systému si klienti mohou

průběžně kontrolovat stav vlastního účtu a zadávat platební příkazy, jejichž prostřednictvím se převádějí peníze z jejich účtu na jiný. Internetové bankovnictví je postaveno na komunikaci mezi webovým prohlížečem klienta a webovým serverem banky. Uvedená komunikace probíhá prostřednictvím protokolu HTTP, jenž je kryptograficky zabezpečen protokolem TLS. Bankovní server se autentizuje prostřednictvím svého certifikátu, přičemž klient se autentizuje ve vytvořeném TLS spojení zpravidla pomocí hesla (Burda, 2019).

3.4 Digitalizace a změny v bankovnictví

Aby mohly finanční služby efektivně sloužit dnešní velké a rozmanité společnosti, musí mít dostatečný rozsah. Tomu má právě napomáhat se svými funkcemi v oblasti sběru, analýzy dat a řízení rizik, jež byly před 10 lety stále ještě snem, digitalizace průmyslu. Pro zaměstnance bank to může znamenat, že v blízké budoucnosti bude docházet k automatizaci všech rutinních prací. Další velkou změnou je uzavírání poboček bank a převádění podpory do digitální podoby (například návody nebo zřízení si účtu online). Vzhledem k tomu, že do finančních služeb vstupují velké technologické společnosti, bude docházet k rozlišování bank pomocí služeb, které nabízejí, nebo podle toho, zda zahrnují hluboké znalosti odvětví, profesionalitu, soukromí a důvěru. To vše závisí na tom, zda banky a společnosti zaměstnávají odborný personál (Taaffe, 2019).

Vše se začíná převádět do online podoby, jak veřejná správa, školství, tak i bankovnictví. Celý tento proces ještě více urychlila nedávná pandemie. Digitalizace bankovnictví je úzce spojena právě s bankovní identitou, proto dojde k vymezení pojmů, které s touto problematikou souvisí.

3.4.1 Pojem digitalizace

Pojetí digitalizace je v překladu z angličtiny interpretováno jako složený z číslic. Základní vymezení pojmu říká, že jí lze vylíčit jako převod analogového signálu na digitální. Digitalizaci je též možné chápat jako používání elektronických metod místo papírových dokumentů, formulářů nebo dopisů. Dříve bylo toto pojetí pojeno hlavně s textovou digitalizací, čímž je myšlen například převod knih nebo dokumentů do digitální podoby. V současné době je možné vidět proces digitalizace na všech místech okolo nás, a to přes dílčí obory, ať už jde o výrobní společnost, trh práce či školství (PortálDigi | DigiStrategie, 2020).

3.4.2 Bankovní produkty

Jelikož v poslední době dochází k rychlé digitalizaci celého bankovnictví, jsou s tím spojeny i bankovní produkty. Ty se dělí na pasivní a aktivní.

Pasivní bankovní produkty lze klasifikovat podle doby trvání, typu subjektu či formy. Z hlediska formy se člení na netermínované vklady, což zahrnuje například spořicí a běžné účty, termínované vklady, vkladové listy, bankovní dluhopisy, pojištění vkladů apod. (Kantnerová, 2016). Jednou ze základních služeb, kterou banka poskytuje svým klientům, je běžný účet. Lidé si obvykle tento účet vytvářejí pro základní správu financí. Za pomoci běžných účtů lze hospodařit s penězi bezhotovostně skrze některý z bankovních domů. Je též nezbytný pro elementární finanční operace a je vyžadován naprostou většinou zaměstnavatelů k tomu, aby na něj byla odesílána výplata (Vokřál, 2021).

Součást aktivních produktů bank představují úvěrové operace, jež realizují banky s cílem dosažení zisku z úroků. Mezi ně se řadí například provozní nebo investiční úvěry a ty se dále dělí na kontokorentní úvěr, revolvingový úvěr atd. Poskytování úvěrů je hlavní, nejdůležitější a zároveň nejziskovější činností každé obchodní (komerční) banky. Touto problematikou se ale bude podrobněji zabývat podkapitola Jak banky vydělávají peníze (Kantnerová, 2016).

3.4.3 Bankovní technologie

Technologie je pro bankovní sektor zásadní již několik let. Zatímco v historii bylo těžké si představit, že by bankovnictví bylo její součástí, nyní se jedná o odvětví, jež je schopno třídit, převádět, ukládat, načítat, transformovat a prohlížet data. Díky této skutečnosti je bankovnictví úzce propojeno se změnami v oblasti informačních technologií. Technologie mění celé bankovnictví nepřetržitě, jelikož nezahrnuje pouze vývoj v oblasti hardwaru, softwaru a sítí, ale stále více i vývoj obchodního modelu (Taaffe, 2019).

Technologie se řadí mezi faktory, jež ve 20. a 21. století mají významný vliv na vývoj takřka každého odvětví. Zásluhou vývoje informačních technologií se během posledního století hluboce přeměnila i oblast bankovnictví. Informační technologie přišly na svět společně se zrodem původního počítače, jenž zahájil další technologickou revoluci. Od vzniku počítače, napříč počátkem internetu se svět přesouvá do období digitalizace, kde je hlavním cílem zautomatizovat jeho významnou část. Oblast bankovnictví díky digitalizaci a informačním technologiím prošla mnoha změnami, které měly kladný důsledek na její další rozmach. Došlo tak k použití technologií například u digitalizace platebního styku či

bankovních služeb, což dalo možnost ke zvyšování pružnosti, produktivity a zesílení informovanosti každého subjektu. Tato skutečnost též napomáhá k minimalizaci správních, zaměstnaneckých a transakčních nákladů (Polouček, 2013).

Pro zprostředkovatele bankovních služeb jsou zpracování transakcí, vedení záznamů o transakcích a poskytování přístupu k nim jádrem celého podnikání. Z hlediska technologií bude vyzdvižen moment, kdy americká banka s názvem Bank of America začala využívat počítače ERMA (neboli „Electronic Recording Machine, Accounting"). V době, kdy byly počítače doménou vědců a inženýrů, kteří modelovali jaderné zbraně a aerodynamiku, si Bank of America nechala objednat 32 strojů ERMA. Tyto počítače se zakládaly na 5letém výzkumu, jenž provedl Stanfordský výzkumný institut. Na základě výzkumu došlo k pokroku v rozpoznávání znaků magnetickým inkoustem, což umožňovalo strojům pracovat při shromažďování dat zcela samostatně. ERMA toho mohla využít při zakládání zákaznických účtů. Používání počítačů v bankách tak zahájilo éru centralizace dat, automatizovaného zpracování a zvyšování úspor (Taaffe, 2019).

Banky se dlouhou dobu zdráhaly aktualizovat své systémy, a to z dobrého důvodu. Soudobé systémy používané bankami jsou produktem a výsledkem neustálých inovací, které se snaží splňovat okamžité požadavky svých zákazníků. Banky a ostatní finanční služby musely reagovat řadou digitalizačních a inovačních iniciativ. Zmíněné iniciativy využívají nejlepší technologie, které zajišťují perspektivu zaměřenou spíše na zákazníka než tradiční zaměření na produkty, jako tomu bylo v minulosti. Je mnoho technologií, jež by mohly ovlivnit budoucnost bankovnictví. Patří mezi ně například: rozšířená realita, hybridní cloud, blockchain, inteligentní stroje, okamžité platby, API platformy, preskriptivní zabezpečení a další (Bharadwaj, 2018).

Jednou ze zmíněných technologií je rozšířená realita. Její používání v bankovnictví má šanci nejen zvýšit efektivitu určitých operací, ale také zlepšit celkový uživatelský komfort. Prostřednictvím rozšířené reality může například dojít k vytvoření virtuální pobočky, kde se zákazníci mohou více zapojit, může jim tak být poskytnuta větší míra informací a pozornosti. Zákazníkům banky lze též zprostředkovat 360stupňový pohled na různé stavy jejich požadavků, nové nabídky a mnoho dalšího. Klíčovou funkcí, kde virtuální realita bude mít také dopad, je dokumentace, například vyplňování různých formulářů. Dopad by mohla mít též u plateb, pojištění, obchodování s daty či mobilitou (Sahu, 2020).

3.4.4 Budoucnost plateb

Jednou z nejdůležitějších a nejvyužívanějších oblastí v bankovnictví jsou platby. Právě proto byla tato oblast vybrána, aby došlo k vysvětlení digitalizace a možné budoucnosti samotných plateb.

Svět kolem se mění neuvěřitelným tempem a někteří jedinci jsou v očekávání, že nás digitalizace, automatizace a umělá inteligence dovedou k nějaké „singularitě" – tedy inteligenci založené na počítači, která ji ale bude daleko převyšovat a významně změní každý aspekt společnosti. Pro někoho to může znít až příliš revolučně, než aby to bylo věrohodné, ale mnoho malých revolucí již existuje, a to nejen ve finančních službách, případně platbách. Provádění plateb se nemusí zdát jako nejatraktivnější bankovní činnost, a to i z pohledu platící osoby, ale to, co bylo poněkud zastaralým nástrojem, se ukázalo jako oblast, kde se spojuje pohodlí spotřebitelů a technologické inovace za účelem vytvoření transformativních řešení (Taaffe, 2019).

S budoucností plateb obecně souvisí i termín bezhotovostní společnost. Jejímu dosažení jsou relativně blízko například Čína, Švédsko či Velká Británie. Stačí zběžný průzkum globálních statistik, aby bylo možné lehce odhadnout, že mnoho zemí bude v blízkém horizontu v podstatě bezhotovostních. V takové společnosti hotovost samozřejmě pořád bude, avšak vymizí z každodenních životů většiny obyvatel. Dojde k převodu od společnosti debetních karet ke společnosti chytrých telefonů a od nich ke společnosti biometrické. Hotovost tedy nepřestane zcela existovat, ale všem, již bude lhostejná. Vzniká tak otázka, jak by měla vypadat opatření pro novou bezhotovostní infrastrukturu (Birch, 2020). Pandemie covidu-19 ale urychlila změnu, jež měla trvat řadu let. Zavedená omezení a opatření s cílem zabránit šíření nemoci spolu s obavami o zdraví a bezpečnost, jež jsou spojené s platbou v hotovosti či dotykovými povrchy, jako jsou zejména platební terminály, donutily spotřebitele upravit své každodenní chování a vedly k nárůstu a rozvoji digitálních a bezkontaktních plateb (Wickes, 2021).

K pokrokům v oblasti plateb přispěla nejen pandemie, ale také několik architektonických změn. Zásadní novinkou na systémové úrovní byla samozřejmě SEPA („Single Euro Payments Area"). Ta jako první umožnila lidem provádět přes hranice bezhotovostní platby v eurech, a to z pohodlí jejich domovů. Zajímavé je, že v téže době přišel na trh Bitcoin jako vůbec první soukromá kryptoměna na světě (Taaffe, 2019). Jednou z pokrokových funkcí, která slouží konkrétně při autentizaci platícího klienta, je biometrie. Ta se již používá k ověřování plateb v mobilních zařízeních, tím pádem si kupující nemusí pamatovat svůj

PIN nebo hesla. Průmysl tak usiluje o větší využívání biometrie k ověřování plateb, jelikož se při něm spotřebitelé cítí bezpečně, protože jejich otisk nikdy neopouští jejich zařízení. V poslední době se po celém světě široce diskutovalo o pojmu digitálních měn centrálních bank a o roli, kterou by mohly hrát v ekosystému finančních služeb. Jedná se v zásadě o peníze v digitální podobě, které by fungovaly jako náhrada bankovek, poskytovaly by lepší zabezpečení, omezovaly podvody a snižovaly náklady (Wickes, 2021).

3.4.5 Jak banky vydělávají peníze

Banky v zásadě nedosahují zisku, dokud nemají peníze svých klientů. Lákání a udržení zákazníků jsou tedy pro bankovní instituce klíčovými činnostmi. To je argument toho, proč banky nabízejí dárky za registraci a doporučení, zříkají se poplatků za přímé vklady a poskytují všemožné výhody pro klienty. Jako každá firma mají i banky zdroje nákladů a příjmů, jež strategicky využívají k svému růstu (Sang, 2021). Mezi obecné, ale také klíčové vlastnosti bank patří přijímání vkladů a poskytování úvěrů. Nelze však opomenout, že současný ekonomický růst a výdělky bank jsou do značné míry závislé na aplikování informačních technologií. Je tedy potřeba, aby banky využívaly a rozvíjely své IT aplikace či systémy, které jsou svou povahou spíše duševním vlastnictvím než fyzickým majetkem (Taaffe, 2019).

Je jasné, že banky vydělávají peníze tím, že majitelům účtů strhávají opakované poplatky. Avšak dalším způsobem získávání peněz jsou půjčky. Banky vydělávají z úroků z dluhů, a to tak, že když klient vloží své prostředky na bankovní účet, banka je poté využije k poskytování půjček jiným lidem a podnikům, kterým účtuje úrok. Banka pak klientovi výměnou za ponechání daného vkladu zaplatí určitý úrok. Banky však inkasují více úroků z půjček, jenž poskytují jiným, než je výše úroků, které platí majitelům účtů. To jim opět přináší zisk (Sang, 2021).

V rámci České republiky získávají banky peníze stále na elementárních produktech, a to ne na jejich zpoplatnění, nýbrž na úrocích. Dále vydělávají peníze například na tom, že se firmy zajišťují proti pohybům měny či že komerční banky mají možnost předat volné peníze České národní bance, jež jim vyplácí dvouprocentní úrok. Okolo 70 procent výnosů banky dosahují prostřednictvím čistého úrokového výnosu, kde se jedná o diferenci mezi získanými úroky z klientských půjček, dluhopisů a úložek u České národní banky a vyplacenými úroky za vklady klientů. Klíčový výdělek pro české banky tedy pochází z elementárních produktů, jako jsou úvěry, spořicí nebo běžné účty (Moniová, 2019).

3.4.6 Otevřené bankovnictví

Systém otevřeného bankovnictví je založen na skutečnosti, že uživatel má možnost sám si zvolit, ve kterém rozhraní bude své finance spravovat. Kromě toho bude v budoucnu možné na webovém rozhraní či mobilní aplikaci uvnitř API („Application Programming Interface“) připojovat specializované služby třetích stran, které umožní zejména kontrolu nad osobními nebo firemními financemi či vedením firemního účetnictví (Koutný, 2019). Otevřené bankovnictví tedy popisuje procesy bank a jiných finančních institucí, které klientům a třetím stranám poskytují jednoduchý digitální přístup k jejich finančním datům. To kupříkladu zahrnuje možnost stahovat a sdílet informace o zůstatcích na účtech, transakcích, platbách či investicích (Kelly, 2021).

Jednou z překážek přijetí otevřeného bankovnictví a PSD2 může být principiální důvěra. Kladem ale je, že mohou například zrychlit a zlevnit zpracování hypoték a dalších půjček (Taaffe, 2019). Zastánci otevřeného bankovnictví tvrdí, že by zákazníci měli mít přístup ke svým datům, aby mohli získávat výhodnější služby. Otevřené bankovnictví by také podpořilo větší růst konkurence a zákazníci, nikoli banky, by měli rozhodovat o tom, kdo uvidí jejich informace. Kritici naopak tvrdí, že bankovní odvětví je již konkurenceschopné a že obavy o soukromí a kybernetickou bezpečnost by měly být nadřazeny ostatním úvahám. Vzhledem k tomu, že údržba a ochrana zákaznických dat je nákladná, banky se též bránily poskytování informací zdarma (Kelly, 2021). Nástupu tohoto trendu zřetelně napomáhá i implementace evropské směrnice PSD2 (Koutný, 2019).

3.4.7 České banky a digitalizace

Digitalizace služeb, informačních kanálů či procesů představuje běžné směřování velkého množství firem, a to bez ohledu na jejich pole působnosti. Mimořádně zásadní je ale digitalizace v odvětví bankovnictví, kde nepředstavuje pouze původ konkurenční výhody, ale i podmínku samotného chodu a fungování finančních institucí, což potvrdila nedávná pandemie. Banky v České republice potřebu digitalizace vlastních služeb velmi dobře chápou a v porovnání s celosvětovou konkurencí si nevedou vůbec špatně (Bartůňková, 2020). Technologie mění bankovní sektor v České republice již dvacet let, ačkoli ve výsledku byla pokaždé víceméně stejná. Až poslední dobou jsou k dispozici takové technologie, které dávají možnost tyto změny provádět daleko pohotověji a v mnoho větším rozsahu. Jako i v jiných zemích k tomu přispěla doba pandemie, kdy lidé neměli možnost se volně pohybovat venku a zároveň vyžadovali možnost spravovat si stále vlastní finance.

Digitalizace se tak úplně rozběhla, změny měly vliv na celý sektor a posunuly bankovnictví na vyšší úroveň (Iannaccone, 2021). Majoritní část bankovních vnitrostátních zástupců lze označit jako poskytovatele s nadprůměrnou kvalitou digitálních služeb. Diference lze například vidět v efektivitě adaptace dílčích zprostředkovávaných služeb, jako jsou zejména založení účtu online nebo příležitost si přes internet nakoupit různé produkty. Každý poskytovatel má pak stejnou dlouhodobou strategii, a to zprostředkovávání online služeb a celkovou digitalizaci komunikace. Strategie poté bere zmíněné náležitosti jako klíčové prostředky v boji vůči krizi a klíč ke klientské spokojenosti (Bartůňková, 2020).

3.5 Digitalizace v ekonomice a společnosti

Pojem digitální ekonomika poukazuje na prorůstání informačních a komunikačních technologií především do produkčních sfér a respektive do celé společnosti. Záměr zavádění digitalizace do ekonomické sféry zajisté není samoúčelný, avšak má napomáhat posílení konkurenceschopnosti dané ekonomiky, ať už z pohledu mikro, tj. konkurenceschopnosti příslušné firmy, jejíž prvky digitalizace implementuje, nebo z makropohledu národní konkurenceschopnosti. Charakteristickým odvětvím, jež v digitalizaci vidí další prosperitu, je průmysl. Různé projekty se uskutečňují v dopravě, stavebnictví, zdravotnictví, ale i v provozu měst, regionů či v oblasti veřejné správy.

Jediným předpokladem pro vývoj digitalizace není pouze to, zda v konkrétní oblasti či sektoru bude mít digitalizace úspěch, či nebude, ale může hrozit určité digitální zaostávání, jež může mít za následek tzv. propast (digital cap), což je stav, kdy konkrétní oblast nebo určitý sektor začnou mít potíže s přístupem k informacím, nebudou způsobilí komunikace či nebudou moci vyhovět některým legislativním požadavkům (Veber, 2018).

3.5.1 Ekonomické přínosy digitalizace

Digitalizace přináší do ekonomiky obecně řadu výhod a přínosů. Jedním z nejrelevantnějších a nejaktuálnějších přínosů digitalizace je skutečnost, že by měla přispět k oživení ekonomiky po pandemii covidu-19. Koronavirus ukázal zcela klíčovou potřebu digitalizace a online spolehlivého pracovního prostředí. Na tuto potřebu reagoval i český Google, jenž přišel s pomocnou rukou a pod záštitou Ministerstva průmyslu a obchodu připravil pro české podniky zdarma vzdělávací program (Langerová, 2021).

Z nejobecnějšího hlediska však ekonomické přínosy posuzují, zda se vyplatí investice do digitalizace na těchto úrovních (Veber, 2018):

- Na makroekonomické úrovni se vyskytují odlišné odhady, kolik celoplošná implementace jednotlivých digitálních aplikací přinese ročně. Obvykle se toto měří absolutními nebo relativními přínosy HDP.
- Na podnikové úrovni se prosazují klasické propočty efektivnosti, které jsou ve vztahu k zaváděným digitalizačním programům. Jedná se například o aparát propočtů ekonomické efektivnosti investic. Ten zprostředkovává mnoho metod, a to od statických přes dynamické až po metody, jež se opírají o analýzu kapitálových trhů. Dále lze pro elementární rozhodování a orientaci kupříkladu využít i rentabilitu či dobu návratnosti investice.
- Na úrovni spotřebitelské hraje zajisté zásadní roli ekonomické hledisko, a to především při volbě digitální služby nebo zboží od více poskytovatelů. U některých služeb se dokonce klient spokojí i s nižší mírou užitku, pakliže je služba poskytována levněji. Příkladem této skutečnosti může být sdílené ubytování (Airbnb) či osobní doprava (Uber). Na druhou stranu ekonomické hledisko nemusí být jedinou složkou, jež hraje při rozhodování o službách nebo zboží roli.

Poslední bod této podkapitoly se bude zabývat vlivem digitální ekonomiky na konkurenceschopnost daných zemí. Mezinárodní konkurenceschopnost dané země je klíčová pro prosperitu jejích obyvatel. Jestliže je ekonomika země konkurenceschopná, mohou tuzemské společnosti prodávat své produkty jak doma, tak v zahraničí. To zajišťuje pracovní místa a vytváří příjem pro zaměstnance. Se zvýšenou konkurenceschopností může země produkovat více zboží a služeb a tím zvýšit HDP. Digitální transformace vlastní ekonomiky se tak stává předpokladem pro zajištění a zefektivnění prosperity země (Petersen, 2019).

3.5.2 Rizika

Příchod digitalizace zahrnuje vyjma nepopíratelných pozitiv i další, méně sympatickou stránku. Jedná se o výskyt rizik, jež vycházejí z aktivity tzv. hackerů, kteří se bez jakýchkoliv práv snaží dostat do počítačových systémů. Jejich záměry jsou většinou odlišné, obvykle jsou však spojeny s nabytím finančního obnosu. Pro napadeného to poté znamená buď odcizení dat, případně jejich zneužití, nebo je výsledkem úspěšného útoku jejich nedostupnost, jež ohrožuje nebo omezuje správný chod firmy či instituce (Vodička, 2021).

Kromě bezpečnostních útoků se vyskytují ještě další rizika, která mohou zapříčinit ztrátu či nedostupnost dat. V případě rizikových faktorů nelze nic prohlásit s jistotou, nicméně nejpravděpodobnějším faktorem, jenž způsobuje řadu krizových situací v obyčejných firmách, je interní lidský faktor, tzn. vlastní zaměstnanci společnosti. Samotné selhání zaměstnance může mít tři příčiny, jimiž jsou: vědomá chyba, chyba z nedostatku soustředění, chyba z nedostatku znalostí. Na druhou stranu i technika se někdy může mýlit. Technické chyby mohou být například zapříčiněny nevhodným naprogramováním či nastavením. To by však mělo být postupně odstraňováno patřičnými ladicími a verifikačními postupy. Nelze však vyloučit řadu poruch, jež souvisejí se spolehlivostí komunikačního a informačního hardwaru. Obecnějším rizikem mohou být také přírodní faktory, kde se jako nejnebezpečnější vnitřní faktor jeví požár. Jako prevence před ním by mělo docházet k ochraně úložišť dat a zároveň programátorských i počítačových pracovišť (Veber, 2018).

Jak již bylo zmíněno výše, ztráta, zneužití a nedostupnost dat se řadí mezi největší možná rizika. Konkrétně u ztráty a zneužití dat jde o momenty, kdy se zneužitelné údaje dostanou k nekompetentní osobě a kvůli tomu mohou být použita jako nástroj k vydírání či obohacení. Obvyklým cílem jsou údaje, jež se týkají platebních prostředků. Příčinami zneužití a ztráty dat může být zejména prolomení zabezpečení, ztráta zařízení, riziko komunikace nebo prolomení ochrany datového úložiště. Rizikem komunikace se myslí skutečnost, že se útočníkovi podaří odcizit přihlašovací údaje ve formě e-mailové adresy nebo hesla, které byly uloženy například v e-shopu, na některé ze sociálních sítí apod. Hlavním účelem útoků ale není nezbytně zpronevěření či zneužití údajů, může jít i o pokus zapříčinit jejich nedostupnost. Zmíněná rizika jsou velice aktuální, a to kvůli vlivu rostoucího množství DDoS útoků či ransomwarů. Ransomware lze definovat jako nepříznivý program, jenž znemožní dostat se k datům či k počítačovému systému (Vodička, 2021).

Digitalizace může mít negativní dopad na různé oblasti. Je velmi pravděpodobné, že digitalizace bude mít velký vliv i na trh práce, a to konkrétně na zaměstnanost. Například v průmyslové výrobě dojde k většímu nasazení robotizace a automatizace. To může mít za následek uvolnění pracovníků, kteří zabezpečují méně kvalifikované rutinní práce. Podobně jsou v ohrožení skupiny administrativních pracovníků, jelikož se bude zavádět automatizace administrativních prací. Digitalizace může mít též negativní dopad na intelektuální vývoj jedince. Příkladem může být skutečnost, že u zaměstnání, kde je podmínkou trávit převážnou část pracovní doby sezením u počítače, se zvyšuje riziko zánětů šlach u ruky, nemocí páteře a zároveň dlouhodobý pohled na monitor kvalitě zraku též nepřidá (Veber, 2018).

Konkrétnější oblastí, kde se nachází řada rizik spojených s digitalizací, je internetové bankovnictví a digitalizace bank celkově. Přechod bank do digitální podoby otevřel dveře novému a rostoucímu souboru rizik, jako jsou zejména narušení soukromí, počítačová kriminalita a potřeba držet krok s novými technologiemi a platformami. Poslední oblastí, jež bude zmíněna, je fakt, že většina společností převádí stále více produktů do digitální podoby a dodává je online. Organizace si tak musí vytvořit správnou strategii pro budoucnost, musí zaujmout promyšlený a zodpovědný přístup k moderním technologiím či trendům a nesmí se aktivně vyhýbat změnám (Jogani, 2019).

3.5.3 Obchodování na internetu

Téma obchodování na internetu je úzce spojeno s bankovní identitou, jelikož právě ona by v budoucnu měla nakupování online zjednodušit. Digitalizace, a to především ve formě pohotové mobilní a internetové komunikace či rozměrných datových úložišť, je podmínkou rozvoje e-shopů. V roce 2018 se počet e-shopů, jenž působí v České republice, odhadoval na cca 37 tisíc. V porovnání s okolními státy je rozmach e-shopů v České republice nebývalý. Není pochyb, že popularita nákupů prostřednictvím e-shopů roste, avšak nelze též přehlédnout velkou četnost subjektů, jež zprostředkovávají služby obchodování na internetu. Tato a další skutečnosti vedou k tomu, že majitelé e-shopů musí v nelehkém tržním prostředí pátrat po nových možnostech, jak zlepšovat podnikání v této oblasti (Veber, 2018).

Mezi aktuální trendy v této oblasti patří například donášková služba, a to všechny její způsoby. Především tento trend platí pro potraviny a restaurace, kde vzniká velké množství spoluprací se společnostmi, jež se orientují na poslední míli. Dochází rovněž k zapojování lokálních prodejen, odkud se poté produkty rozvážejí klientům po okolí. Dalším z trendů je fakt, že se kamenné prodejny postupně mění ve výdejní místa. Zejména jestliže má prodejce obchodů víc, má klient možnost vybrat si ten nejbližší a během vyzvednutí objednávky si ještě něco přikoupit. Trendem, který je jak dlouhodobý, tak aktuální, je realita, že spotřebitelé požadují udržitelnost a zodpovědné chování. To znamená, že velkým lákadlem pro zákazníky je, pokud jsou produkty „zelené“ či udržitelné, nebo pokud například e-shopy darují určité procento peněz z každého nákupu na dobrou věc. Posledním trendem je alternativní finanční řešení. To lze vysvětlit tak, že lidé už nemají povinnost platit ihned, ale objevují se i jiné možnosti placení, a to buď předplatné či opožděná platba (MediaGuru, 2021).

3.5.4 Incidenty spojené s digitalizací

Jak již bylo zmíněno v předchozích kapitolách, aplikace digitálních technologií není bez rizika. Její nešikovné použití či nepostačující zabezpečení může mít za následek různé incidenty. Nejprve budou zmíněny ty z českého prostředí, a to konkrétně z roku 2017. Prvním incidentem je hackerský útok na data e-shopu, jenž se uskutečnil v srpnu roku 2017. Hackeři se během něj dostali do databáze klientů společnosti Mall.cz a pronikli ke jménům, heslům, e-mailovým adresám a objednávkám, které patřily cca 750 tisícům zákazníků společnost. Příčinou byla skutečnost, že firma před rokem 2015 používala k ochraně dat kódovací systém MD_5, jenž je už zaostalý. Cílem útoku se stala jenom tato data. Dalším incidentem z tohoto roku jsou falešné slevové kupóny, které se často objevovaly v e-mailové korespondenci. Obsahem e-mailu byla informace, že renomovaný řetězec daruje slevové kupóny, s upozorněním, že akce bude již zanedlouho ukončena. Odkazovaná stránka zahrnovala informaci o aplikaci, kterou si žadatel o kupón musel stáhnout do svého počítače. Tím však zprostředkoval útočníkovi přístup ke svému počítači a zároveň i uloženým datům, kde poté útočník mohl manipulovat s daty, různá data stahovat a vše mohl využít k vydírání oběti útoku (Veber, 2018).

4 Praktická část

V souvislosti se zaváděním bankovní identity se praktická část bude zabývat mírou a možnostmi jejího využití v České republice. Zprvu dojde k představení aktuální situace. Budou představeny nejznámější české banky, které jí zprostředkovávají a společně s tím firma BankID. V následné části dojde k průzkumu a analýze stavu bankovní identity ve třech největších bankách v České republice. Na základě provedeného průzkumu bude definována připravenost jednotlivých bank. Tím je myšlena skutečnost, jaký je aktuální stav, zda nedošlo v průběhu času k nějakým závažným incidentům a jak řešení bankovní identity u dílčích bank vypadá. V praktické části bude též provedena analýza možností a způsobů využití bankovní identity v soukromé (SONIA) a státní sféře (NIA). Na jejím základě pak budou vytvořeny procesní diagramy, které budou popisovat proces ověření v jednotlivých oblastech. Předposlední část práce bude popisovat založení a využití dvou vybraných alternativ bankovní identity. Závěr se pak bude věnovat dotazníkovému šetření, během něhož dojde k získání názorů na bankovní identitu, její bezpečnost, využití, alternativy a názor na její budoucnost v České republice.

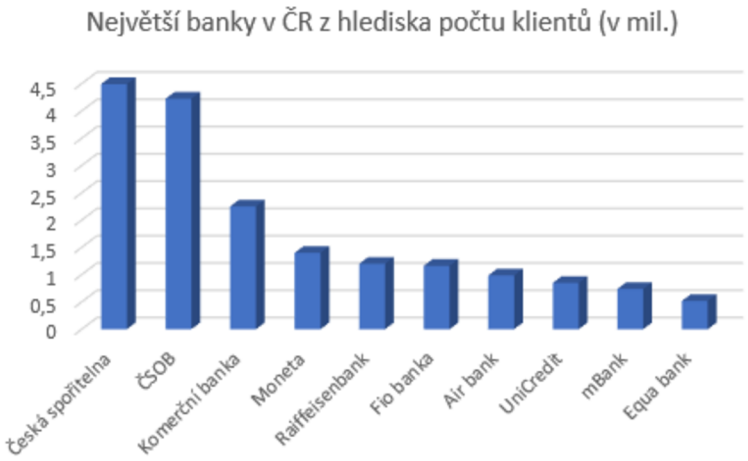
4.1 Současná situace v ČR

Bankovní identita se v České republice rozšiřuje rychlým tempem. Řada bank tak postupně přechází ke zprostředkování bankovní identity svým klientům. Kapitola se bude zabývat analýzou současné situace v ČR z hlediska bank na trhu, kde na závěr bude uvedeno, která z nich bankovní identitu zprostředkovává. Zároveň bude představena i společnost, která je se zaváděním bankovní identity úzce spojená.

4.1.1 Největší banky v ČR

Na českém bankovním trhu figuruje řada bank, které se předhánějí v počtech svých klientů. Pro budoucí výzkum je potřeba uvést, o které banky se jedná a jaké je aktuální pořadí podle počtu jejich klientů. Data byla získána z (Skalková, 2022) a na jejich základě pak byl vytvořen graf, viz obrázek níže.

Obrázek 1: Největší banky v ČR



Zdroj: Skalková (2022)

Jak je patrné z grafu výše, bankou s nejvyšším počtem klientů je Česká spořitelna s cca 4,5 mil. klientů. Na druhé pozici je ČSOB se 4 mil. klientů. Celkově se mezi 5 největších bank v České republice řadí Česká spořitelna, ČSOB, Komerční banka, Moneta a Raiffeisenbank. Zmíněné banky jsou na českém trhu již řadu let a úspěšně si udržují své postavení.

4.1.2 Banky s bankovní identitou

Za poslední dva roky roste velmi rychlým tempem počet bank, které umožňují svým klientům využívat bankovní identitu. Podle stránek BankID (BankID.cz, 2022) ji v České republice poskytuje celkem 7 bank. Jedná se o:

- Komerční banku,
- Monetu,
- ČSOB,
- Fio banku,
- Raiffeisenbank,
- Českou spořitelnu a
- Air Bank.

V porovnání s výše zobrazeným grafem je patrné, že bankovní identitu poskytuje 7 největších bank, které na bankovním trhu v České republice působí.

4.1.3 Společnost BankID

V rámci diplomové práce byla oslovena prostřednictvím e-mailu společnost BankID za účelem získání základních informací týkajících se bankovní identity. Jedná se o jednoho z největších zprostředkovatelů bankovní identity v České republice, přičemž hlavní akcionáře společnosti tvoří 9 českých bank. Firma odkázala na několik zdrojů, které budou využity a zpracovány v průběhu praktické časti.

Podle zdrojů společnosti je bankovní identita využívána v několika oblastech, jako jsou například (BankID.cz, 2022):

- Obchod a služby – mezi nejznámější společnosti, které umožňují ověření pomocí bankovní identity, patří v oblasti obchodu a služeb například Seznam.cz, Hlídačky.cz nebo Centrální depozitář cenných papírů.
- Daně – prostřednictvím bankovní identity se lze přihlásit do portálu Mojedane.cz a podat daňové přiznání.
- Získání rodičovského příspěvku – proces funguje tak, že se uživatel přihlásí pomocí BankID do portálu úřadu práce, vyplní formulář a žádost rovnou odešle.
- Výpočet důchodu – pomocí BankID je možné si nechat vypočítat důchod, a to na ePortálu ČSSZ.
- Řidičský průkaz a trestné body – BankID lze využít i ke zjištění trestných bodů na Portálu občana.
- Nahlížení do katastru – prostřednictvím BankID lze nahlížet do katastru nemovitostí.

4.2 Bankovní identita v českých bankách

Jedním z dílčích cílů práce je provést analýzu stavu bankovní identity v rámci českých bank. Pro zhodnocení připravenosti a aktuální situace byly zvoleny tři největší banky, které byly zmíněny v odstavcích výše. Jedná se o Komerční banku, Českou spořitelnu a ČSOB. V následujících odstavcích dojde tedy k popisu aktuálního stavu bankovní identity a k praktické ukázce ověření u vybrané banky. Na závěr bude zhodnocena připravenost popsaných bank.

4.2.1 Komerční banka

Komerční banka figuruje na českém bankovním trhu již řadu let. Jako jedna z nejvíce využívaných bank v České republice poskytuje svým klientům též ověření prostřednictvím bankovní identity.

Pilotní provoz služby banka spustila 26. ledna v roce 2021, přičemž vzápětí došlo k jejímu testování za pomoci desítek zaměstnanců banky. Cílem banky bylo nabídnout využití bankovní identity ve státní správě a digitálních službách komerčních subjektů. Pilotní provoz byl proveden za účelem odhalení a odstranění slabých míst. Proto se nejprve řešil pouze interně (Komerční banka, 2021).

Možnost využití bankovní identity ze stran klientů banky bylo zahájeno 24. března 2021. Ověření funguje stejně, jako do internetového bankovnictví MojeBanka. Zajímavostí je, že provoz bankovní identity byl spuštěn těsně před Sčítáním lidu v roce 2021. Přesněji řečeno šlo o tři dny před započetí sčítání. To probíhalo od 27. března do 9. dubna 2021 (Komerční banka, 2021).

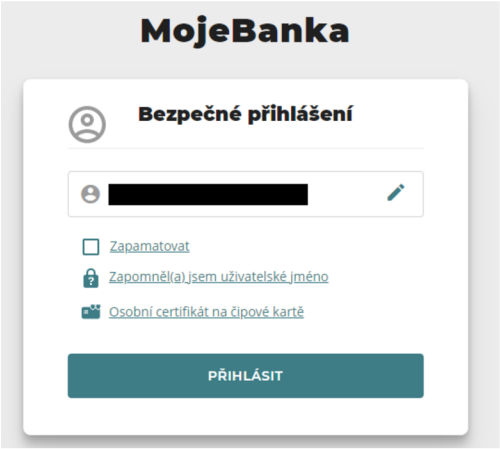
Aktuálně banka zprostředkovává službu pro všechny své klienty. Zároveň též na stránkách propaguje nabídku BankID firmám, které by měly zájem ověřovat a získávat informace o svých klientech pomocí zmíněné služby. Banka nabízí tři základní formy BankID pro firmy, a to (Komerční banka, 2022):

- Connect – obecně se jedná o online přihlašování zákazníků firmy, které je vhodné především pro e-shopy, klientské zóny a aplikace.
- Identify – jde o online ověření totožnosti bez nutnosti návštěvy provozovny. Hodí se pro online vyplnění a ověřování údajů do smlouvy s klientem.
- Sign – využívá se pro online podpis smlouvy.

Ověření pomocí bankovní identity u KB

Pro představení využití bankovní identity u KB byl vybrán způsob ověření pomocí KB klíče. Jedná se o aplikaci, kde dochází k ověření identity klienta jak už pomocí PIN, nebo biometriky. Všechny banky, které bankovní identitu poskytují, ji zakládají klientům automaticky. Klient si nemusí nic dalšího nastavovat, zakládat či registrovat. Celý proces začíná tím, že klient zadá uživatelské jméno, viz obrázek 2 níže.

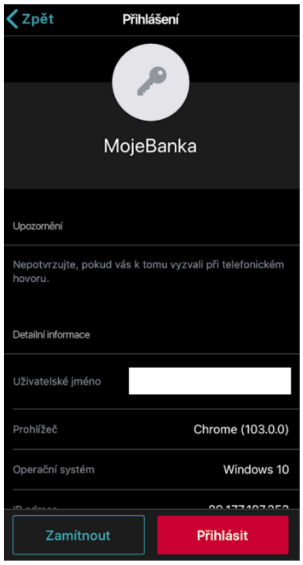
Obrázek 2: Přihlášení do KB



Zdroj: login.kb.cz (2022)

Následně dostane uživatel na chytrý telefon notifikaci do KB klíče, kde vidí všechny informace o pokusu o přihlášení, viz obrázek 3 níže. Klient má možnost pokus zamítnout, nebo potvrdit. Pokud zvolí přihlásit, dojde k ověření prostřednictvím PIN, nebo biometriky. Po úspěšném dokončení je klient přihlášen do internetového bankovnictví, nebo přesměrován na stránku, jež vyžadovala jeho ověření.

Obrázek 3: Potvrzení v aplikaci KB klíč



Zdroj: Aplikace KB klíč (2022)

4.2.2 ČSOB

Druhou bankou, jež byla vybrána pro představení a popis aktuálního stavu bankovní identity, je Československá obchodní banka. Ta jako první získala v říjnu v roce 2020 akreditaci pro spravování kvalifikovaného systému elektronické identifikace v ČR.

Akreditaci udělilo Ministerstvo vnitra, přičemž hlavním záměrem bylo zpřístupnění ověření klientů banky na dílčích portálech provozovaných státem. Nejvíce zmiňovaným pak byl Portál občana a jeho možnosti využití. Skrze portál si může klient například opatřit výpis z trestního rejstříku, z bodového registru řidičů a další. Banka se zároveň řadí k zakládajícím akcionářům společnosti Bankovní identita a.s., jež v České republice zprostředkovává elektronickou identifikaci založenou na digitální identitě klientů bank (ČSOB, 2020).

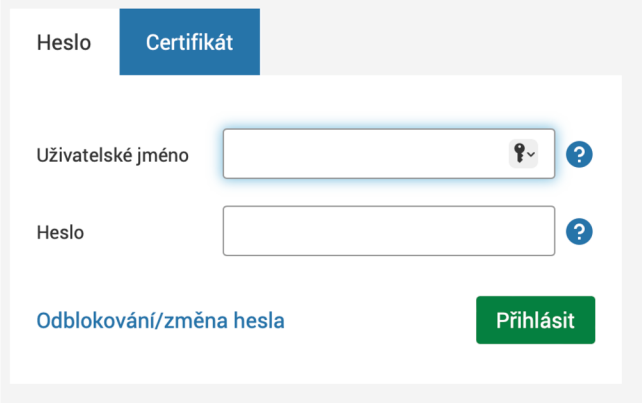
Dalším krokem ČSOB v oblasti implementace bankovní identity bylo její zpřístupnění pro ověření u služeb soukromých poskytovatelů (tzv. SONIA). Stalo se tak 1. června v roce 2021. Banka zároveň přesvědčovala své klienty o bezpečnosti služby tím, že se provozovatel BankID ani společnosti nedostanou k přihlašovacím údajům klientů. Přihlášení ke službám dílčích společností je umožněno pomocí dvoufaktorového ověření, a to buď prostřednictvím SMS kódu či v mobilní aplikaci Smart klíč. Využít ověření pomocí ČSOB identity bylo stejně jako u KB možné u Sčítání lidu 2021 (ČSOB, 2021).

Jednou z posledních inovací týkající se ČSOB identity je digitální podpis dokumentů. Konkrétně se jedná o možnost klienta digitálně podepsat smlouvu či dokument u soukromé společnosti, která je začleněná do řešení BankID. Další výhodou je též možnost založit si běžný účet prostřednictvím bankovní identity jiné banky. Založení běžného účtu je rychlé a efektivní, přičemž došlo i k vyzkoušení a potvrzení této skutečnosti v rámci diplomové práce. Uživatel nemusí skenovat žádné dokumenty, ale pouze se přihlásí pomocí bankovní identity jiné banky a provede patřičné souhlasy. Poté dojde k vytvoření účtu a uživatel může ihned provádět libovolné operace (ČSOB, 2021).

Ověření pomocí bankovní identity u ČSOB

Ověření prostřednictvím bankovní identity u ČSOB probíhá podobně, jako tomu bylo u Komerční banky. Uživatel se ověřuje stejným způsobem, jako při přihlášení do internetového bankovnictví. Nejprve musí zadat uživatelské jméno a heslo, viz obrázek 4 níže. Po zadání patřičných údajů existují dva možné způsoby, jak ověřit svou identitu. První možností je pomocí SMS kódu a druhou je pomocí tzv. Smart klíče, kde se jedná o obdobné řešení aplikace, jako u KB klíče Komerční banky.

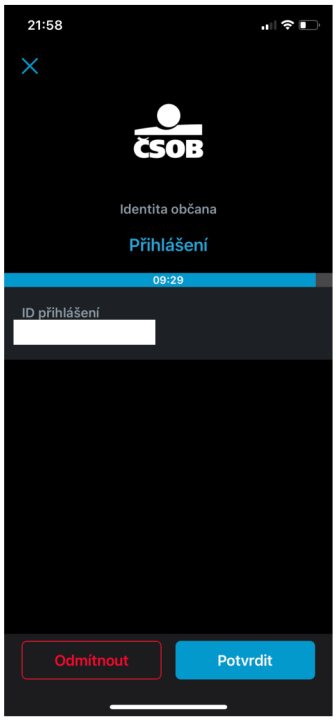
Obrázek 4: Přihlášení do ČSOB



Zdroj: identita.csob.cz (2022)

V rámci ukázky byla vybrána možnost ověření pomocí Smart klíče, a to z důvodu jednoduššího využití a možnosti ověření pomocí biometriky. Proces postupuje tak, že po zadání uživatelského jména a hesla přijde na mobilní telefon do aplikace Smart klíče notifikace s žádostí o ověření. Uživatel má možnost jí potvrdit, nebo odmítnout, viz obrázek 5 níže. Po potvrzení dojde k ověření identity, a to dvěma možnými způsoby. Prvním je pomocí předem nastaveného PIN kódu a druhý způsob je prostřednictvím biometriky. Pokud ověření projde v pořádku, tak je uživatel přesměrován na stránku, kde bylo vyžadováno jeho ověření.

Obrázek 5:Potvrzení v aplikaci Smart klíč



Zdroj: Aplikace Smart klíč (2022)

4.2.3 Česká spořitelna

Česká spořitelna je jednou ze tří bank, která jako první v České republice začala zprostředkovávat svým klientům bankovní identitu a jako druhá získala akreditaci od Ministerstva vnitra pro ověřování klientů u služeb veřejné správy. Tím se zvýšil potencionální počet uživatelů bankovní identity o 1,7 milionu. První bankou s akreditací, jak již bylo zmíněno výše, byla ČSOB (Ministerstvo vnitra České republiky, 2020).

Banka v září 2021 rozšířila své portfolio míst, kde lze bankovní identitu využít, například o energetickou společnost ČEZ či o Generali Českou pojišťovnu. Zároveň již v té době bylo možno využít ověřování prostřednictvím České spořitelny pro online získání produktů a služeb u 35 komerčních společností. V září 2021 bankovní identitu využilo přes 200 tisíc klientů, kteří provedli 1,3 milionu přihlášení, přičemž více než polovinu tvořili klienti České spořitelny (Česká spořitelna, a.s., 2021).

V říjnu 2021 Spořitelna jako první banka v České republice spustila digitální podpis dokumentů prostřednictvím BankID SIGN. Jedná se o službu, prostřednictvím níž může klient digitálně podepsat smlouvu u různých komerčních subjektů. S implementací řešení pomáhala společnost Signi, která České spořitelně pomáhá s digitalizací, a to nikoli jen uvnitř banky, ale i u klientů (Česká spořitelna, a.s., 2021).

Jelikož mají Komerční banka, ČSOB a Česká spořitelna velmi podobné řešení bankovní identity, což je asi tím, že se všechny banky podílejí na stejném projektu, tak dojde pouze ke stručnému popisu ověření. Na základě hledání možností u České spořitelny, se však našla zajímavá funkčnost, která umožňuje sledovat, kdy byla historicky bankovní identita u klienta využívána, více viz popis níže.

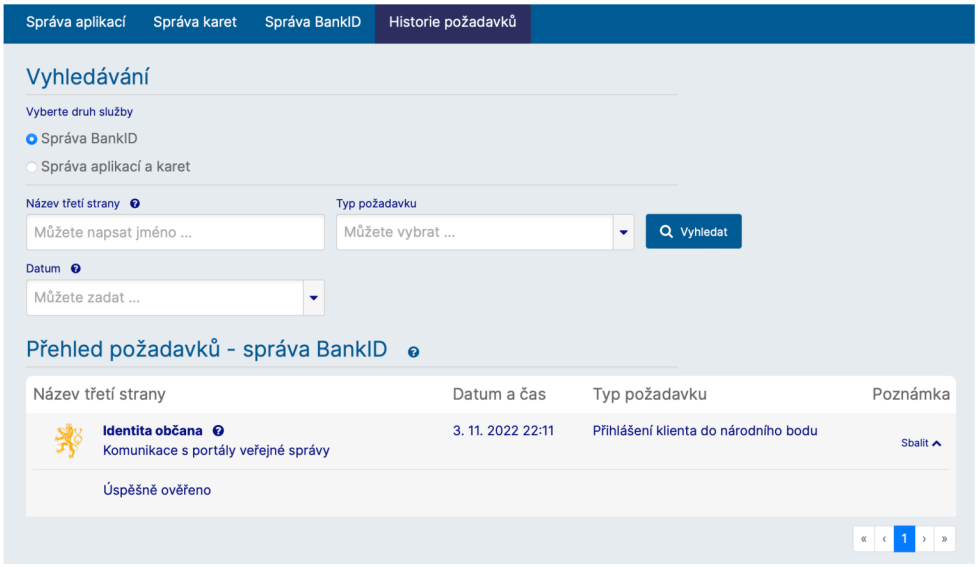
Možnosti bankovní identity u České spořitelny

Pokud se klient chce přihlásit či registrovat na zvolenou stránku pomocí bankovní identity Spořitelny, tak mu stačí zadat pouze uživatelské jméno, stejně jako tomu bylo u Komerční banky. Následně ho vyzve aplikace George klíč pro potvrzení žádosti o ověření. Pokud uživatel žádost potvrdí, tak musí zadat předem nastavený PIN. Po úspěšném zadání PIN je přesměrován s tím, že došlo k ověření a předání patřičných informací mezi bankou a danou stránkou.

Zajímavostí u České spořitelny je, že umožňuje svým klientům sledovat, kdy byla jejich bankovní identita využívána. Uživatel tak může svoje ověření u třetích stran stále kontrolovat a kdykoli ho odvolat v aplikaci Správa třetích stran (Česká spořitelna, a.s.,

2022). Dále má možnost v aplikaci vidět souhrn požadavků, které byly prostřednictvím BankID provedeny. Zobrazované informace o konkrétním požadavku představují například název třetí strany, datum a čas ověření, typ požadavku nebo poznámku. Všechny informace lze vidět na obrázku 6 níže. Zároveň si v aplikaci uživatel může odebrat souhlas s využíváním bankovní identity. Lze tak po odebrání souhlasu bankovní identitu uživatele znepřístupnit. Popsaná možnost správy bankovní identity byla nalezena pouze u řešení České spořitelny.

Obrázek 6: Aplikace Správa třetích stran



Zdroj: cdn.csas.cz (2022)

4.2.4 Připravenost bank

Pojmem připravenosti bank je myšleno shrnutí jejich aktuálního stavu a stanovení závěrů plynoucích z výše popsané analýzy. Obecně stanovit připravenost bank je velmi subjektivní a nejsou pro to dána žádná pevně stanovená kritéria. Jedním z podnětů, podle kterého lze nějaký závěr stanovit, je to, že za dobu fungování a zavádění bankovní identity v České republice nenastal žádný zásadní bezpečností problém, jež by s ní byl spojen. Zároveň nebyly nalezeny žádné další větší komplikace při jejím zavádění a rozšiřování.

Důvodem je nejspíše skutečnost, že banky musí získat od státu potřebnou akreditaci, aby mohly poskytovat ověření svých klientů ke službám veřejného státu. Zároveň banky musí splňovat tzv. Zákon o bankovní identitě, jenž vznikl pro širší začlenění bank ke zprostředkovávání elektronické identifikace. Platným se stal 1. ledna 2021, přičemž se jedná spíše o novelizaci již existujících zákonů. Dalším cílem zákona je též napravení limitujícího

přístupu pojišťoven a bank do základních registrů či zvolených agendových informačních systémů státu. Hlavní myšlenky zákona o bankovní identitě jsou (Korbel, 2021):

- příležitost bank zprostředkovávat elektronickou identifikaci a s ní spojené služby v rámci vlastní podnikatelské činnosti,
- limitované bezplatné využití služeb bank jako akreditovaných správců v NIA jenom pro orgány státu či územních samosprávných celků,
- limitovaný přístup pojišťoven a bank k základním registrům se záměrem účinějšího vykonávání jejich zákonných povinností,
- příležitost uplatnit bankovní identitu ke splnění zákonných povinností v souvislosti s identifikací zákazníka podle AML zákona.

Pro potřeby analýzy aktuálního stavu došlo k popisu řešení bankovní identity u Komerční banky, ČSOB a České spořitelny, jako u tří největších bank z hlediska počtu klientů v České republice. Ověření u všech zmíněných bank probíhá téměř totožně. Jedná se prakticky o ověření ve dvou krocích, které klientovi přináší rychlý způsob přístupu do různých služeb jak už ve státní, tak soukromé sféře. Zajímavou odlišností byla popsaná možnost správy bankovní identity klienta u České spořitelny. Jelikož ale banky na celkovém řešení bankovní identity spolupracují, tak jsou prostředky a způsoby ověření klienta téměř totožné. Každá banka má svou aplikaci zvanou klíč, pomocí níž se klient ověřuje. Závěrem lze říct, že se bankovní identita velmi dynamicky rozvijí, což potvrzují jednotlivé fakty, které byly zmíněny v popisu u jednotlivých bank a též skutečnost, že jí využívá stále více klientů. Připravenost a možnosti využití bankovní identity lze popsat i prostřednictvím analýzy v soukromé či státní sféře a dotazníkovým šetřením, které má za cíl zjistit stav bankovní identity z hlediska vybraných respondentů. Tím vším se budou zabývat kapitoly níže.

4.3 Možnosti využití bankovní identity

V souvislosti s analýzou zavádění bankovní identity v České republice dojde k popisu možností jejího využití v soukromé a státní sféře. Jelikož výše došlo k analýze řešení bankovní identity u jednotlivých bank, tak se zdá být přínosné popsat, kde všude a jakým způsobem jí lze využít. První část se bude zaměřovat na využití tzv. Soukromoprávní NIA, jež se věnuje ověřování pomocí banky v soukromé sféře. Druhá část pak bude analyzovat využití tzv. NIA, která se používá pro ověřování ve státní sféře. V rámci druhé části dojde též k oslovení Týmu portálu občana, kde je hlavním cílem získání odpovědí na otázky

týkajících se bankovní identity. Na základě analýzy způsobů využití dojde v následující kapitole k popisu procesu ověření ve státní a soukromé sféře, aby byl získán podrobnější popis aktuálního stavu bankovní identity v České republice.

4.3.1 Soukromá sféra

Začátek působení bankovní identity v České republice se váže spíše na státní sféru. S jejím rozvojem a rostoucím počtem klientů se ale začíná více využívat v neméně důležité oblasti, a to v soukromé sféře. K největším společnostem umožňujícím ověření pomocí BankID se řadí například Alza, Seznam, Pražská plynárenská nebo Sazka. Počet takových společností konstantně roste. Z toho důvodu dojde k představení a praktickým ukázkám využití BankID u vybraných tří firem.

Alza

Alza je jedním z největších e-shopů v ČR. Právě ona využívá k ověření svých klientů také bankovní identitu. Jednou z nejnovějších služeb společnosti Alza, ve které se využívá BankID, je tzv. „třetinka“. Ta, jak je patrné z názvu, dává zákazníkům možnost zaplatit pouze třetinu ceny. Zbytek doplatí buď najednou, nebo po částech do tří měsíců. Díky BankID nemusejí klienti chodit do kamenných provozoven a nemusejí ztrácet čas jejich osobní návštěvou.

Díky plnohodnotné digitalizaci služby se jejím zákazníkům otevírá celá škála možností dopravy, jež je dostupná při klasickém nákupu na Alza.cz. Společnost využívá ověření identity prostřednictvím BankID od začátku července 2022. V prvních 14 dnech se pomocí této metody uzavřelo 10 % smluv, i přestože e-shop tuto možnost aktivně nenabízel.

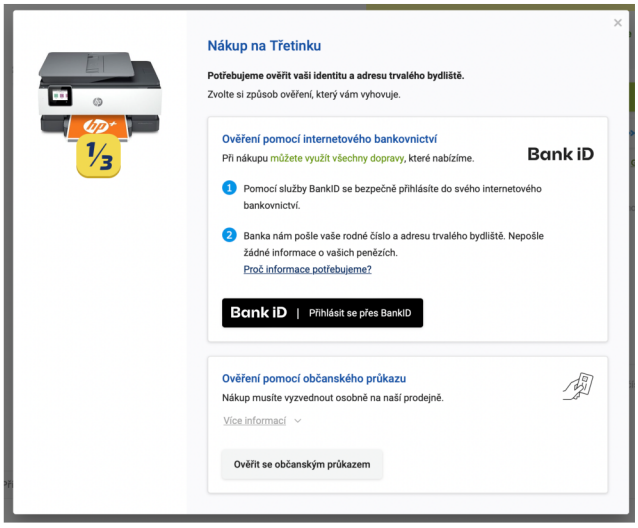
Princip služby spočívá v tom, že klient zaplatí jenom třetinu ceny a její zbytek, aniž by došlo k nějakému navýšení, musí uhradit do 3 měsíců. Nakupující si může platby rozvrhnout, jak sám uzná za vhodné. Než dojde ke schválení objednávky, e-shop zkontroluje bonitu zákazníka a využívá k tomu různé zdroje hodnocení. Praktický příklad bude detailněji popsán níže (Alza.cz, 2022).

Praktická ukázka využití

Jak již bylo zmíněno výše, služba umožňuje zaplatit zákazníkovi pouze třetinu ceny, přičemž zbytek musí doplatit do tří měsíců. Pokud si tedy uživatel vybere produkt na e-shopu Alza.cz, má při koupi možnost vybrat „Zaplať pouze třetinku“, přičemž koupi potvrdí prostřednictvím zeleného tlačítka „Koupit“. Pokud uživatel na tlačítko klikne, je vyzván

k přihlášení. Po přihlášení do jeho účtu mu jsou nabídnuty dvě možnosti, jak lze ověřit svou identitu. První možností je BankID a druhou je ověření pomocí občanského portálu. Na základě praktické ukázky byla vybrána první možnost, jejíž umístění lze na stránce Alzy vidět na obrázku 7, viz níže.

Obrázek 7: Využití BankID na stránce Alza.cz



Zdroj: Alza.cz (2022)

Po vybrání možnosti ověření prostřednictvím bankovní identity je uživatel přesměrován na stránku, kde musí zvolit banku, s jejíž pomocí se chce ověřit. Na výběr má uživatel všechny banky, které BankID v České republice poskytují, kromě jedné, a to Fio banky. Pod výběrem je možné ještě zvolit „Nenašli jste svou banku?“. V rámci práce byla vybrána Komerční banka.

V dalším kroku je uživatel přesměrován na stránky banky, kde musí zadat svoje ID. Po úspěšném zadání mu do KB klíče přijde potvrzovací notifikace, kde se musí ověřit buď pomocí PIN, nebo biometriky. Jestliže ověření proběhlo úspěšně, je přesměrován zpět na stránky Alzy. Ta si na pozadí na základě získaných údajů z banky ověřuje bonitu uživatele. Pokud projde, je přesměrován k posledním krokům, a to k dokončení objednávky. To znamená zadání fakturačních údajů, dodací adresy a volbu způsobu platby.

Investiční společnost Avant

Společnost Avant se pohybuje na investičním trhu od roku 2007. Zabývá se hlavně rozvojem fondů a zajímavými investičními příležitostmi. Poskytuje investiční poradenství a zaměřuje se na zakládání, administraci a správu fondů způsobilých investorů. Nabízí svým

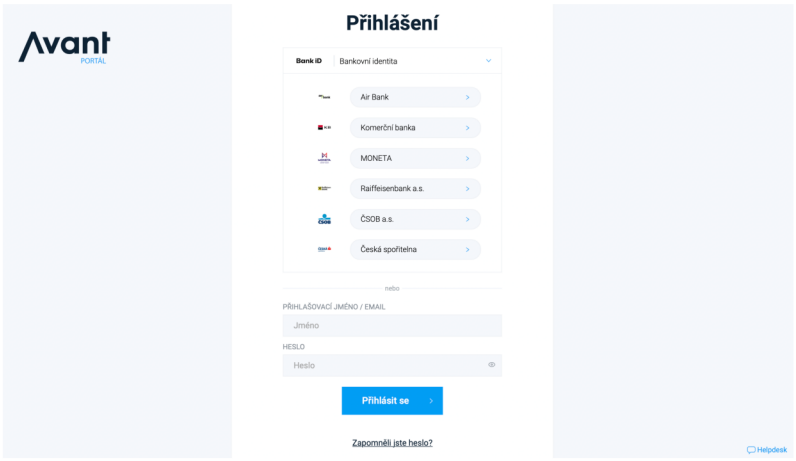
potenciálním zákazníkům založit si vlastní fond, nebo do některého již existujícího investovat (Avantfunds.cz, 2022).

V rámci diplomové práce je firma zmíněna, jelikož též využívá na svém portálu ověřování pomocí bankovní identity. Dalším důvodem je, že společnosti ve finančním sektoru tvoří dominantní část využívajících bankovní identitu v soukromém sektoru. Jedná se například o: WOOD & Company Financial Services, Zonky, Modrá pyramida a další.

Praktická ukázka využití

Firma Avant využívá ověřování pomocí bankovní identity ke vstupu do investičního portálu pro své zákazníky. Zmíněná služba se nabízí hned jako první možnost přihlášení/registrace do investičního portálu, viz obrázek 8. Pokud si uživatel BankID nezvolí, je ověřován klasickým způsobem pomocí jména a hesla. Na rozdíl od jiných webových stránek, které využívají bankovní identitu, je odlišnost v nabídce bank, kde uživatel vybírá konkrétní banku. Rozdílem je, že uživatel má rozbalovací seznam s bankami hned na přihlašovací stránce. Přičemž u jiných stránek byla volba až na další stránce po kliknutí na tlačítko „Ověřit účet pomocí bankovní identity“.

Obrázek 8: Využití BankID u společnosti Avant

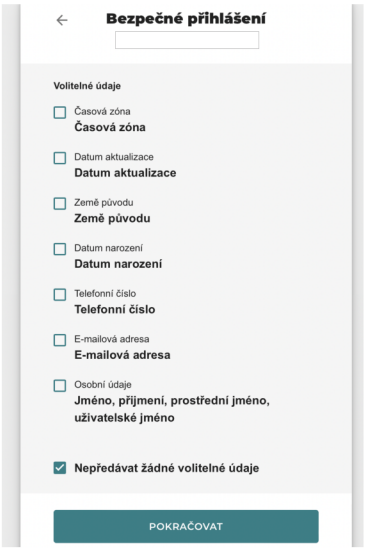


Zdroj: avantfunds.cz (2022)

Celý proces pak funguje tak, že si uživatel vybere banku a je přesměrován na přihlašovací stránku. Pro účely práce byla vybrána Komerční banka. Pokud má uživatel zavedený KB klíč, s jeho pomocí pak probíhá ověření. Od předešlých příkladů ověřování se toto liší v tom, že uživatel dostává možnost si vybrat volitelné údaje, jež je ochoten firmě sdílet, viz obrázek 9 níže, hned na přihlašovací stránce banky. Mezi volitelnými údaji je časová zóna, země původu, telefonní číslo a další osobní údaje. Uživatel též dostává možnost žádné volitelné

údaje nepředávat. Předávání volitelných údajů je nabízeno podle toho, komu bude banka údaje následně posílat. Další stránkou, u které tato akce probíhá, je například Sazka.cz. Následně je uživatel v mobilní aplikaci vyzván k autorizaci pomocí biometriky, nebo PIN stejně jako v předešlých případech. Po ověření identity je přesměrován zpět na stránky společnosti.

Obrázek 9: Nastavení volitelných údajů při ověřování



Zdroj: login.kb.cz (2022)

Pražská plynárenská

Další oblastí, která využívá ověřování prostřednictvím BankID, je energetika. Jednou z největších energetických společností, která BankID umožňuje, je právě společnost Pražská plynárenská. Na základě toho dojde k představení možností, které BankID v této oblasti nabízí, a popisu praktického využití přímo na webu Pražské plynárenské.

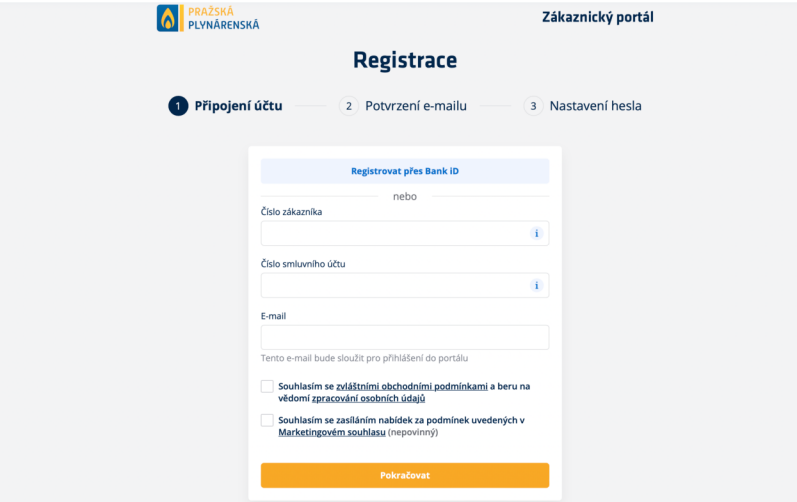
Hlavním přínosem pro zákazníky Pražské plynárenské je, že se mohou při registraci do zákaznického portálu ověřit stejně jako při vstupu do svého internetového bankovnictví. Dalším potenciálním benefitem je uzavírání smluv pomocí BankID na nekomoditní produkty, což znamená výměnu spotřebičů za nové, jejich servis či budování energetických zdrojů ve formě tepelných čerpadel a fotovoltaiky (Mašek, 2021).

Praktická ukázka využití

Pražská plynárenská využívá BankID pro registraci uživatele do zákaznického portálu. Jak k registraci, tak k přihlášení ale potřebuje být uživatel zákazníkem společnosti. Pokud není, do portálu se nedostane ani prostřednictvím bankovní identity. Pokud je uživatelem,

stačí mu na stránce registrace kliknout na tlačítko „Registrovat přes BankID“, které je vidět hned na úvodní obrazovce, viz obrázek 10 níže. Následně je uživatel klasicky přesměrován na výběr banky, kterou chce využít pro ověření své identity. Pro potřeby práce byla vybrána Komerční banka. Uživatel se ověří prostřednictvím KB klíče, a to pomocí PIN, nebo biometriky. Po ukončení procesu si Pražská plynárenská prověří za pomoci údajů z banky, zda je uživatel opravdu zákazníkem společnosti. Pokud ano, tak si uživatel nastaví heslo do portálu a registrace je úspěšně ukončena.

Obrázek 10: Registrace na zákaznickém portálu Pražské plynárenské



Zdroj: moje.ppas.cz (2022)

Z praktické ukázky je patrné, že pro registraci do portálu musí být uživatel zákazníkem společnosti. Stejně si tedy musí osobně zařídit a podepsat smlouvu. To se jeví jako částečná nevýhoda. Naopak výhoda spočívá v tom, že pokud uživatel zákazníkem je, nemusí pracně hledat zákaznické číslo či číslo smluvního účtu, ale stačí se identifikovat pomocí BankID. Jako potenciální výhoda se též jeví uzavírání smluv prostřednictvím BankID, například u fotovoltaiky s ohledem na energetickou krizi a rostoucí zájem o tuto službu.

4.3.2 Státní sféra

Státní sféra byla jednou z prvních oblastí, jež umožňovala ověření prostřednictvím bankovní identity. Stát zároveň neustále rozšiřuje počet míst a portálů, kde lze BankID uplatnit. Na základě toho je zřejmé, že jde o významnou část působnosti bankovní identity, která bude v rámci diplomové práce z hlediska možností využití popsána, a to na různých místech ve státní sféře. Mezi nejznámější portály, kde lze BankID využít, se řadí například: Portál občana nebo Moje daně. Mimo jiné se bankovní identita uplatnila i při Sčítání lidu

v roce 2021. Nejaktuálnějším portálem využívajícím BankID ve státní správě je klientský portál MPSV. Ten kvůli krizi umožňuje občanům zažádat o příspěvek na dítě 5000 Kč. Níže dojde k popsání vybraných portálů společně s možnostmi využití bankovní identity.

Portál občana

Portál občana představuje službu, jež zprostředkovává elektronické služby státu. Na portálu má každý občan vlastní účet, k němuž má přístup pouze on. Může si na něm spravovat vlastní doklady, petice, registrovaná vozidla a další údaje ze státních registrů a databází. Skrze portál si lze zřídit i datovou schránku, pomocí níž lze elektronicky komunikovat s úřady. Z portálu má občan i jednoduchý přístup do portálu ostatních úřadů, jako jsou například: finanční správa, ČSSZ, úřad práce či portál jeho obce. K přihlášení do Portálu občana existují dva způsoby, a to prostřednictvím Identity občana nebo datové schránky. Identita občana mimo jiné dává možnost se přihlásit i pomocí bankovní identity. Tento způsob bude popsán níže (Ministerstvo vnitra, 2022).

V rámci zpracovávání diplomové práce došlo v srpnu 2022 k přímému oslovení Portálu občana prostřednictvím e-mailové komunikace. Cílem bylo získání odpovědí na otázky týkající se základních skutečností, názorů a zajímavostí ohledně bankovní identity ve státní správě. Tým Portálu občana je poskytl.

Otázky

- Kolik přihlášených občanů České republiky již využilo bankovní identitu pro přihlášení do Portálu občana?

„Portál občana z důvodu ochrany osobních údajů neeviduje přesné počty užitých identifikačních prostředků u svých registrovaných uživatelů. Avšak dle našich odhadů tvoří identifikační prostředky bankovní identity více než polovinu přihlášení pomocí ID prostředků s úrovní záruky značná (bankID, mobilní klíč, NIA ID, mojeID...) do Portálu občana. Díky identifikačním prostředkům bankovní identity spuštěným v roce 2021 tvořily identifikační prostředky LoA značná hlavní způsob přihlašování do Portálu občana v roce 2021, a to podílem 74,5 %. Zbytek uživatelů se přihlašovalo datovými schránkami (ISDS) – 20,7 %, anebo identifikačními prostředky s LoA vysoká – 4,8 % (eObčanka, karta Starcos). V roce 2020 hlavní způsob v přihlašování do Portálu občana tvořily datové schránky, a to podílem 56,2 %, LoA značná 24,2 % a LoA vysoká – 19,7 %. Aktuální počet registrovaných uživatelů Portálu občana k začátku června 2022 byl 443 tisíc, z toho 278

tisíc, tedy 60 %, začalo portál využívat od června 2021. Za tu dobu také zásadně vzrostl počet přihlášení do portálu z necelých 800 tisíc před 1. červnem 2021 na více než 2,4 milionu přihlášení k začátku června 2022.“

- Pro přihlášení do Portálu občana lze využít i jisté alternativy bankovní identity jako mojeID, NIA ID apod. V porovnání s uvedenými alternativami je využívána více, či méně?

„Aktuálně nejoblíbenější elektronický identifikační prostředek (eID) pro přihlašování k online službám veřejné správy (nejen do Portálu občana) je NIA ID, který uživatelé už použili více než 5,1milionkrát. Následuje BankID České spořitelny s 2,8 miliony použití.“ Následně došlo k odkázání na další tiskové zprávy.

- Existuje nějaký hlavní důvod, proč by banky a jejich klienti měli využívat bankovní identitu?

„Bankovní identita je jedním z autentizačních prostředků k bezpečnému přihlášení k online službám veřejné správy. Klienti bank díky tomu mohou jednoduše pomocí přihlašovacích údajů svého internetového bankovnictví kromě využití služeb své banky komunikovat i se státní správou nebo svou obcí.“

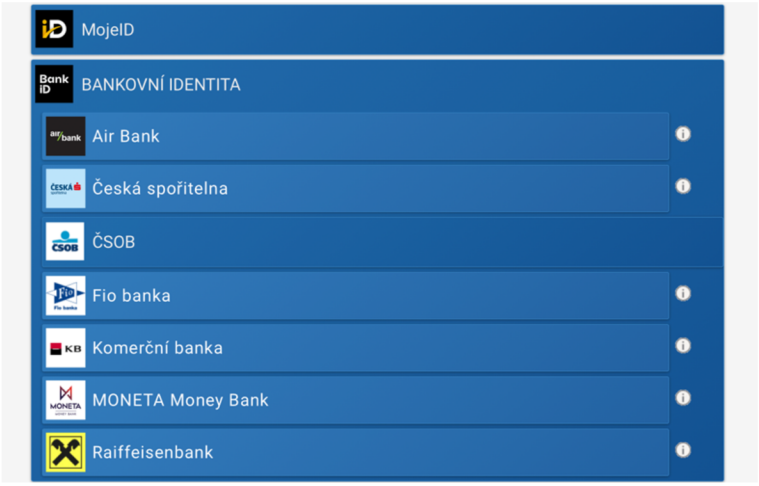
- Čím myslíte, že je způsobeno, že se bankovní identita v poslední době tak rychle rozšiřuje?

„Přihlášení pomocí bankovní identity je pro uživatele oblíbeným prostředkem z důvodu jednoduchého přístupu k online službám státu, který již uživatelé akreditovaných bank mají zřízený v rámci přihlašování do svého internetového bankovnictví.“

Praktická ukázka využití

Jak již bylo zmíněno výše, do Portálu občana se lze přihlásit dvěma způsoby. V rámci práce dojde k analýze využití tzv. Identity občana, která umožňuje i bankovní identitu. Pokud se tedy občan dostane na přihlašovací stránku Portálu občana, je mu nabídnuto, aby si vybral způsob, kterým se chce přihlásit. V tomto případě uživatel zvolí Identita občana. Po přesměrování na další stránku se mu zobrazí seznam identit, pomocí kterých se může přihlásit. Mezi nimi je i volba s názvem „BANKOVNÍ IDENTITA“. Po volbě této možnosti se uživateli zobrazí rozbalovací seznam s nabídkou jednotlivých bank, viz obrázek 11 níže. V souvislosti s prací byla vybrána Komerční banka.

Obrázek 11: Volba ověření identity na Portálu občana



Zdroj: nia.identitaobcana.cz (2022)

Následně je uživatel přesměrován na přihlašovací stránku banky, kde musí zadat své přihlašovací údaje. Konkrétně se jedná o ID uživatele. Pokud má zřízený KB klíč, probíhá ověření ve stejném duchu jako v kapitolách výše. To znamená, že uživatel dostane notifikaci na svém mobilním telefonu, aby se ověřil pomocí PIN, nebo biometriky. Po ověření je uživatel na svém prohlížeči přesměrován zpátky na stránky Portálu občana. Tam musí udělit souhlas pro výdej údajů pro Ministerstvo vnitra, viz obrázek 12. Jednotlivé údaje si lze rozkliknout a zobrazit. Zároveň si lze vybrat, jaký údaj uživatel chce/nechce poskytnout. Nabízí se zde i možnost udělit trvalý, nebo jednorázový souhlas s poskytnutím údajů. Po výběru jedné z těchto možností je uživatel přihlášen a přesměrován přímo na Portál občana, kde může vykonávat všechny činnosti, jež byly popsány v úvodu kapitoly.

Obrázek 12: Udělení souhlasu pro výdej údajů na Portálu občana

Zdroj: nia.identitaobcana.cz (2022)

Moje daně

V předešlých kapitolách byly popsány portály, které spadají pod jednotlivá ministerstva. Konkrétně se jednalo o Ministerstvo vnitra a Ministerstvo zdravotnictví. Další portál, na němž bude představeno využití bankovní identity, se nazývá Moje daně. Jedná se o portál, jenž spadá pod Ministerstvo financí. Moje daně nabízí služby jako: online finanční úřad, elektronické podání pro finanční správu, registr DPH a jiné.

V rámci práce dojde k popisu ověření u služby Online finanční úřad. Ta zprostředkovává zjednodušenou, komfortnější a zrychlenou elektronickou komunikaci s finanční správou. Daňový subjekt pak má možnost pomocí daňové informační schránky dostávat informace uložené ve spisu či na osobním daňovém účtu (GENERÁLNÍ FINANČNÍ ŘEDITELSTVÍ, 2020).

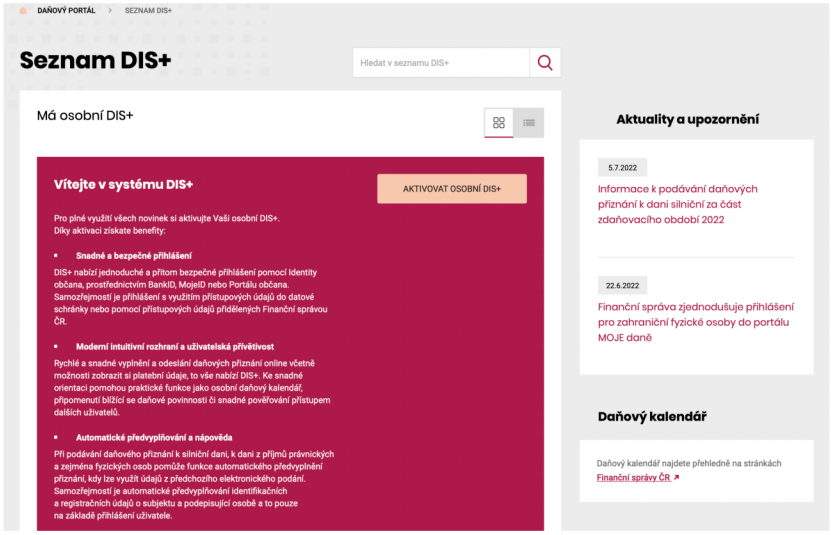
Praktická ukázka využití

Jelikož se jedná o portál, jenž je spravován ministerstvem, ověření pomocí BankID probíhá stejně jako v předchozích kapitolách, a to prostřednictvím Identity občana. Po ověření občana a udělení souhlasu k výdeji údajů je uživatel přesměrován na daňový portál. Zajímavostí a zároveň odlišností od ostatních portálů je služba s názvem DIS+ (Daňová informační schránka), jejíž využití lze vidět na obrázku 13.

Tu v roce 2021 zpřístupnila Finanční správa ČR. Je určená daňovým subjektům pro získání informací, jež se zaobírají daňovými povinnostmi. Díky zmíněné službě může subjekt odesílat finanční správě daňová přiznání, dívat se na osobní daňové účty nebo nastavovat notifikace událostí. Jde o elektronickou samoobsluhu, kterou mohou využívat daňové subjekty. Služba DIS+ představuje tzv. „Online finanční úřad“ (Finanční správa ČR, 2022).

Aby mohl uživatel službu využívat, musí si ji nejprve aktivovat. Aktivuje si ji tím, že zvolí po přihlášení do portálu volbu „Aktivovat osobní DIS+“. Po aktivaci proběhne zpracování a přenos dat z finančního úřadu. Do té doby může uživatel schránku používat pouze v omezeném režimu. Schránku by měl mít uživatel plně přístupnou do 48 hodin od aktivace.

Obrázek 13: Využití Daňové informační schránky



Zdroj: adisspr.mcfr.cz (2022)

Klientský portál MPSV

Protože se v roce 2022 dostala řada rodin do svízelné finanční situace, vláda se rozhodla dát jednorázový příspěvek na dítě ve výši 5 000 Kč. Na základě usnadnění vyplácení příspěvku došlo k vytvoření klientského portálu, jenž bude sloužit této činnosti. Jelikož je nutným krokem pro bezpečné ověření žadatele přihlášení pomocí elektronické identity, bude se touto problematikou diplomová práce také zabývat.

Aplikace s názvem „Jenda“ byla vytvořena za účelem jednoduchého podání žádosti o příspěvek. V prvních 2 dnech podalo skrze aplikaci žádost více než 22 tisíc občanů. Druhou možnost, jak žádost o příspěvek podat, představují Czech POINTy, které jsou rozmístěné po celé České republice. Na základě zprávy od Ministerstva práce a sociálních věcí ale většina žadatelů využila právě klientský portál (Ministerstvo práce a sociálních věcí, 2022).

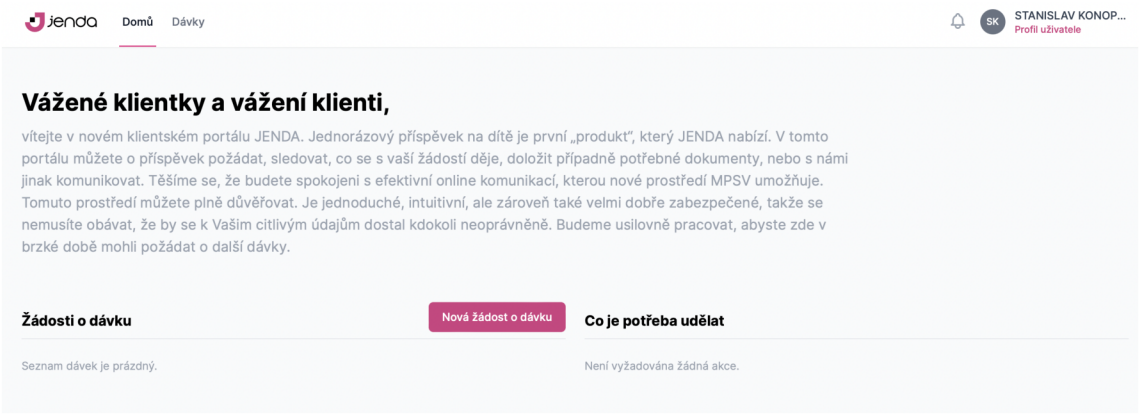
Praktická ukázka využití

Pokud se potenciální žadatel rozhodne podat žádost o příspěvek na dítě prostřednictvím aplikace, dostane se do ní pomocí oficiálních stránek Ministerstva práce a sociálních věcí. Odtud je přesměrován rovnou do aplikace Jenda. Pokud zvolí „Vstoupit do aplikace“, zobrazí se mu stránka Identita občana. Tam si zvolí způsob, kterým má být jeho identita ověřena. V souvislosti s prací byla vybrána bankovní identita. Dále postupuje jako ve výše popsaných portálech. Po ověření a udělení souhlasu pro výdej údajů se dostane na úvodní stránku aplikace, kde stiskne „Nová žádost o dávku“ a postupuje v dalších krocích. Aplikace

následně vyžaduje další akce, jako jsou: vyplnit údaje žadatele, způsob platby, děti, na které není pobírán přídavek na dítě, údaje o partnerovi a čestné prohlášení. Jelikož autor nemá na přídavek nárok, nebyla žádost dovedena do konce. Úvodní stránka aplikace s tlačítkem pro podání nové žádosti je vidět na obrázku 14.

Pro občany České republiky přináší toto řešení řadu výhod. Mezi ně se dá zařadit i to, že rodiče nemusí řešit přepravu do nejbližšího Czech POINTu, ale stačí jim ověřit se prostřednictvím jakékoli identity. Pokud mají účet u některé banky, jež zprostředkovává BankID, ani si ji nemusí zakládat a stačí se jim do portálu přihlásit stejným způsobem jako do svého internetového bankovnictví.

Obrázek 14: Aplikace Jenda



Zdroj: jenda.mpsv.cz

4.4 Analýza principu fungování bankovní identity

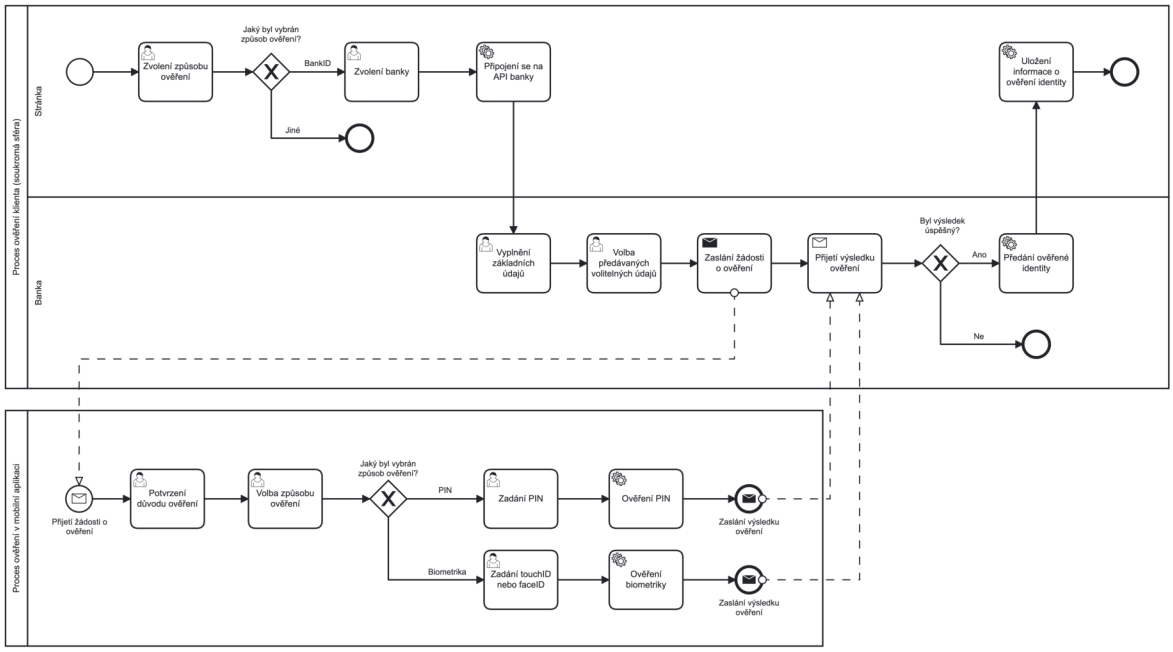
V kapitolách a odstavcích výše došlo k popisu možností využití bankovní identity na jednotlivých portálech, a to jak v soukromé, tak státní sféře. V rámci analýzy zavádění bankovní identity v České republice se zdálo být příhodné popsat, jak proces ověřování v aktuálním stavu funguje. Jelikož mají všechny banky řešení bankovní identity velmi podobné, tak lze celý proces popsat souhrnně s rozdělením na státní a soukromou sféru.

Na základě získaných poznatků tedy dojde k vytvoření procesního modelu, jenž bude souhrnně vysvětlovat, jak bankovní identita obecně funguje. Popis nejde až do úplného detailu, jako jsou například využitá API apod., protože jsou tyto informace těžko dostupné. Celý procesní model bude zkonstruován pomocí BPMN diagramu a měl by dát jasnější pohled na to, jak BankID vlastně v praxi funguje. Jelikož je přístup v ověření identity v soukromé a státní sféře trochu rozdílný, budou popsány a vytvořeny dva diagramy.

4.4.1 Proces ověřování v soukromé sféře

Proces ověřování v soukromé sféře byl představen na jednotlivých ukázkách, viz výše. Konkrétně se jednalo o ukázky na webu společnosti Alza, investiční společnosti Avant a Pražské plynárenské. Ve výsledku proces probíhal tak, jak je znázorněno na obrázku 15. Pro lepší přehlednost byl přidán i jako Příloha A na konci práce. Celému procesu předchází skutečnost, že uživatel chce ověřit svou totožnost na konkrétní stránce. Proces začíná tím, že si uživatel vybere způsob ověření. Pokud by si vybral jiný, než je bankovní identita, ověřuje se klasickým (jméno a heslo), nebo jiným způsobem. V případě této práce si uživatel vybírá BankID a proces pokračuje. V dalším kroku si uživatel musí vybrat banku, u níž chce ověření vykonat. Po dokončení volby ze stran uživatele se stránka připojí přes API do vybrané banky se žádostí o ověření klienta. Uživatel je následně přesměrován na stránku banky, jež vypadá stejně jako přihlašovací stránka do internetového bankovnictví. Zde musí vyplnit základní údaje pro identifikaci klienta. Ve většině případů se jedná o ID uživatele. Dalším krokem je volba předávaných volitelných údajů, kde si uživatel vybere údaje, které je ochoten příslušné stránce sdílet. Jelikož byl ve všech ukázkových případech vybrán pro ověření KB klíč, došlo k přidání dalšího procesu, jenž se zabývá ověřením na mobilním zařízení. Po volbě předávaných volitelných údajů je tedy zaslána do KB klíče (na mobilní telefon) žádost o ověření klienta a začíná proces ověření na mobilním zařízení. Klientovi se objeví obrazovka s informacemi o důvodu ověření, kterou musí potvrdit. Následně je mu zobrazena nabídka způsobu ověření. KB klíč umožňuje ověření pomocí PIN, nebo biometrikou. Pokud si klient vybere biometriku, v dalším kroku zadá faceID nebo touchID a dojde k ověření jeho identity. Na konci procesu ověření v mobilní aplikaci se zasílá výsledek ověření zpět do procesu ověření klienta u konkrétní banky. Pokud ověření proběhlo v pořádku, banka předává ověřenou identitu stránce, jež o tuto akci žádala skrze API. Stránka identitu přijme, uloží informaci o úspěšném ověření a proces končí.

Obrázek 15: BPMN diagram procesu ověření v soukromé sféře

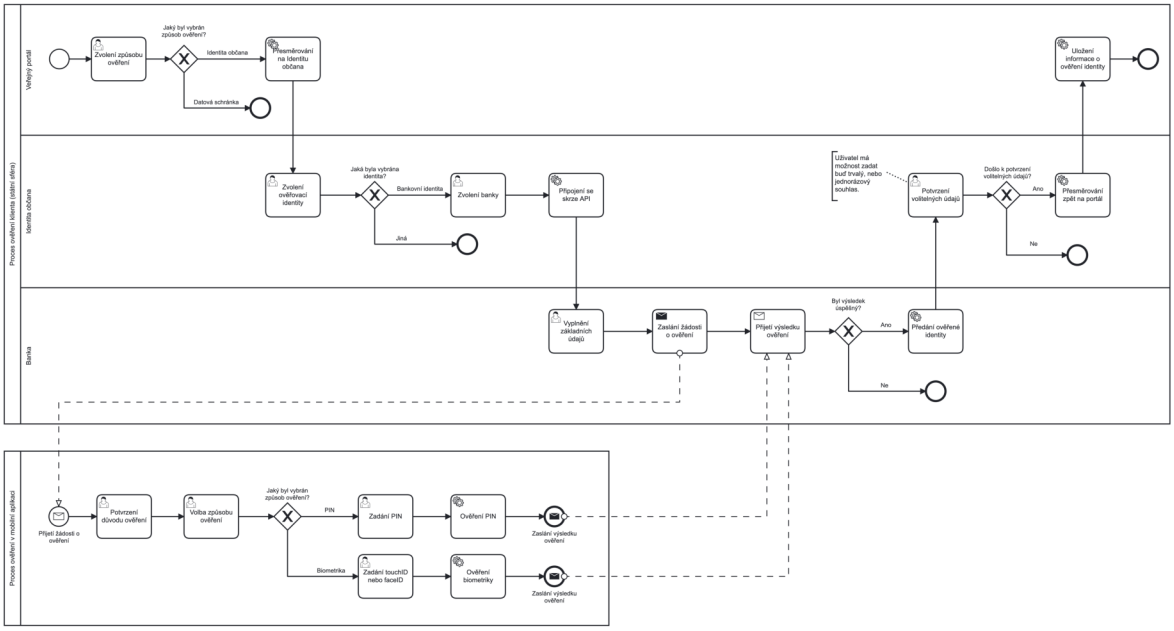


Zdroj: Vlastní (2022)

4.4.2 Proces ověřování ve státní sféře

Proces ověřování ve státní sféře funguje na portálech jednotlivých ministerstev téměř totožně. V rámci práce byl vytvořen procesní diagram, jenž lze vidět na obrázku 16 níže. Pro lepší přehlednost byl přidán i jako Příloha B na konci práce. Vytvořen byl na základě poznatků získaných z praktických ukázek dílčích portálů, přičemž hlavním zdrojem byl Portál občana. Proces začíná tím, že si uživatel vybere způsob ověření do portálu. V případě popisovaného procesu si vybírá „Identitu občana“, jako alternativa se mu nabízí datová schránka. V dalším kroku portál uživatele přesměruje na stránku pro zvolení identity, kterou chce použít. Kromě bankovní identity je též na výběr mobilní klíč eGovernmentu, mojeID a další. Uživatel si vybere bankovní identitu, kde v rozbalovacím seznamu musí zvolit, jakou banku k ověření využije. Po volbě jedné z bank dochází ke spojení Identity občana s vybranou bankou skrze API. Pro tuto práci byla vybrána Komerční banka. Ověření ze strany banky probíhá stejně jako u soukromoprávní identity, tudíž již nebude popisováno. Po úspěšném ověření klienta bankou dojde k přesměrování zpět do Identity občana. Tam se uživateli zobrazí stránka s předávanými údaji. Má na výběr ze tří možností, a to zadat trvalý, či jednorázový souhlas se zpracováním údajů, nebo předávání údajů zamítnout. Jestliže uživatel svůj souhlas potvrdí, je přesměrován zpět na portál s ověřenými údaji a proces končí. Pokud ne, ukáže se uživateli obrazovka, aby zkusil přihlášení později, a proces je též u konce.

Obrázek 16: BPMN diagram procesu ověření ve státní sféře



Zdroj: Vlastní (2022)

4.5 Alternativy bankovní identity

V souvislosti s postupným zaváděním bankovní identity v České republice dojde k definování a popisu jejích dvou nejznámějších alternativ. Zároveň se jedná o alternativy, které jsou v úzkém spojení s pojmem NIA, která též představuje jeden z dílčích cílů práce. Dalším důvodem, proč bylo vybráno téma alternativ k bankovní identitě, je jejich zařazení do otázek ohledně zjištění veřejného mínění, jehož výsledky budou popsány v kapitolách níže. Dojde tedy k popisu a praktické ukázce jejich využití, přičemž na závěr budou definovány rozdíly v porovnání s bankovní identitou. Pro představení byly vybrány alternativy mojeID a Mobilní klíč eGov. Obě byly obecně popsány v teoretické části práce.

4.5.1 MojeID

Jelikož k obecnému definování služby došlo již v teoretické části, budou rovnou popsány praktické možnosti využití.

Praktická ukázka využití

Založení identity mojeID probíhá na stránce mojeid.cz, kde uživatel zvolí „Založit mojeID“. Následně je vyzván k vyplnění základních údajů, jako jsou uživatelské jméno, příjmení, mobil, adresa trvalého bydliště a další. Stránka též dává uživateli na výběr předvyplnit formulář přes Google či Facebook. Po vyplnění povinných formulářových polí

a odsouhlasení podmínek má uživatel možnost založit účet. V dalším kroku musí zadat dva PIN kódy, přičemž jeden mu byl zaslán na zadané telefonní číslo a druhý na e-mail. Jestliže oba kódy zadal správně, je přesměrován na stránku pro nastavení nového hesla. Po vytvoření hesla je uživateli založen nový účet. V něm si může zadat další osobní údaje, jež může sdílet při ověřování své identity. Pokud však chce službu využívat pro přihlášení do veřejné správy, musí svůj účet zabezpečit. To se dělá pomocí tzv. mojeID klíče, jenž si musí stáhnout a nastavit prostřednictvím QR kódu. Po načtení QR kódu má uživatel možnost nastavit v aplikaci biometrické ověřování. Následně zadá na stránce heslo a proces nastavení mojeID klíče je u konce. Pro úplné dokončení přístupu do státní správy je ještě potřeba ověřit svoji totožnost. To lze třemi způsoby. Jedná se o:

- Použití existujícího prostředku – jedná se o způsob, kdy uživatel ověří svou identitu například pomocí NIA ID, eObčanka apod. V nabídce ovšem není BankID.
- Osobně navštívit pracoviště Czech POINT.
- Použit k ověření datovou schránku.

V rámci práce byla vybrána datová schránka. Proces vypadá tak, že je uživatel přesměrován do datové schránky, kde se přihlásí a udělí souhlas ověření totožnosti pro mojeID. Následně odešle žádost pro ověření totožnosti datovou schránkou. Po úspěšném ověření, jenž trvá pár minut, si uživatel v nastavení svého účtu zkontroluje své údaje a klikne na dokončit. Po všech těchto krocích má mojeID pro vstup do veřejné správy aktivní pro úroveň „značná“.

Další částí praktické ukázky je testování využití identity pro přihlášení do Portálu občana. Proces probíhá velice podobně jako u bankovní identity. Uživatel je po volbě možnosti přihlášení přesměrován do „Identity občana“, kde si vybere mojeID. Tam má v rozbalovacím seznamu na výběr dvě možnosti, a to úroveň „značná“, nebo „vysoká“. Jelikož bylo mojeID v rámci práce založeno pouze pro úroveň „značná“, byla vybrána tato volba. Následně je uživatel přesměrován na stránku, jež vypadá stejně jako přihlašovací stránka do portálu mojeID. Zde musí zadat jméno a heslo. Po úspěšném zadání přihlašovacích údajů přijde uživateli do aplikace klíč mojeID žádost o ověření. Proces ověření v aplikaci funguje stejně jako u KB klíče. Uživatel tedy potvrdí žádost a je ověřen pomocí biometriky. Následně potvrdí na stránce dokončení ověření a dostává se na stránku Portálu občana jako přihlášený uživatel.

Porovnání s BankID

V praktickém využití identity mojeID pro přihlášení na Portál občana se zdá být proces ověření stejný jako u bankovní identity. Jako velké mínus identity mojeID lze chápat způsob, jakým se zakládá. Ten je sice asi bezpečný, ale pro uživatele poněkud zdlouhavý, protože musí zadat osobní údaje, pracovat s PIN kódy, zabezpečit a ověřit svůj účet, aby vůbec mohl mojeID využívat. V porovnání s BankID, kde má uživatel vše zařízeno a nemusí se o nic starat, pouze se přihlásí stejně jako do svého internetového bankovnictví, se tento přístup zdá být pro uživatele velmi nevýhodný.

Hlavním rozdílem mezi službou mojeID a bankovní identitou jsou možnosti úrovní záruky. Bankovní identita umožňuje pouze úroveň záruky „značná“, přičemž mojeID podporuje i nejvyšší úroveň záruky „vysoká“. Certifikaci CZ.NIC získalo 8. března 2021 a využívá pro to token FIDO2 s certifikací na úrovni L2. Přístup k tokenu musí být vázán na zadání správného PIN. (Peterka, 2021)

4.5.2 Mobilní klíč eGov

Stejně jako u služby mojeID došlo k obecnému popisu již v teoretické části práce. Bude tedy rovnou popsáno praktické užití služby Mobilní klíč eGov.

Praktická ukázka využití

Služba Mobilní klíč eGov je v porovnání s výše popisovanými identitami poněkud rozdílná. Nezakládá se prostřednictvím webové stránky, ale pro jeho zavedení a zprovoznění musí mít uživatel staženou příslušnou mobilní aplikaci. Tu si může stáhnout ať už v Google Play, nebo App Store. Po jejím stažení dostává uživatel na výběr metody, s jejichž pomocí se může přihlásit. Mezi volbami je PIN, obrázkové či normální heslo. Jelikož se obrázkové heslo v přihlašovacích portálech moc nevidí, byla vybrána právě tato volba. Obrazovku s nastavením obrázkového hesla lze vidět na obrázku 17. Zde si uživatel vybere minimálně 4 obrázky pro nastavení svého hesla. V principu nastavení funguje stejně, jako když se nastavuje PIN, pouze místo čísel jsou obrázky. Po nastavení hesla je nabídnuta možnost biometrického ověření. V následujícím kroku si uživatel vybírá, k čemu chce klíč využívat. Na výběr má aktivaci klíče pro Identitu občana, připojení klíče do datové schránky nebo obnovení dat mobilního klíče ze zálohy. V rámci zpracování praktické ukázky byla vybrána aktiva klíče k Identitě občana. Aby se k ní uživatel mohl připojit, musí již mít u této služby založený účet (to znamená má účet u NIA ID, eObčanky nebo bankovní identitu). Dalším z nabízených způsobů je připojení pomocí datové schránky či zřízení účtu Identita občana

návštěvou kontaktního místa Czech POINT. Vybrána byla první možnost, a to přihlášení za předpokladu, že uživatel má již účet u služby Identita občana. Pro tuto volbu musí být uživatel přihlášen do Portálu národního bodu (Identita občana). Tam se lze přihlásit pomocí bankovní identity stejně jako do ostatních portálů státní správy. V portálu zvolí možnost s názvem „Připojení Mobilního klíče eGovernmentu“. Na stránce má uživatel zobrazený QR kód, který načte pomocí mobilní aplikace klíče eGovernmentu. V posledním kroku se mu zobrazí kód, který si porovná jak na mobilním zařízení, tak na webové stránce. Pokud kódy souhlasí, klikne na potvrdit a dojde k úspěšné aktivaci mobilního klíče.

Obrázek 17: Možnost nastavení obrázkového hesla

Zdroj: Aplikace Mobilní klíč eGovernment

Další částí praktické ukázky využití je otestování přihlášení do Portálu občana prostřednictvím Mobilního klíče eGovernmentu. To začíná tím, že si uživatel na portálu vybere možnost přihlášení pomocí Identity občana. Po přesměrování zvolí jako ověřovací způsob identity Mobilní klíč eGovernmentu. Na následující stránce se mu zobrazí QR kód, jenž načte pomocí mobilní aplikace. Aplikace se ho vzápětí zeptá, zda souhlasí s ověřením pomocí NIA. Po odsouhlasení je uživatel přesměrován z Identity občana do Portálu občana, to znamená úspěšně přihlášen.

Porovnání s BankID

Z praktické ukázky vyplývá, že Mobilní klíč eGovernmentu zprostředkovává o něco jednodušší způsob ověření než bankovní identita. Konkrétně se jedná o to, že uživatel nemusí zadávat žádné ID nebo telefonní číslo, ale stačí pouze oskenovat QR kód v mobilní aplikaci. Naopak stejně jako u porovnávání s mojeID se jeví jako velká nevýhoda oproti bankovní

identitě nutnost zakládání a aktivace identity v aplikaci Mobilního klíče. Proces sice není tak složitý, avšak BankID tento krok úplně vynechává. Další výhodou bankovní identity oproti Mobilnímu klíči eGovernmentu je možnost využití v soukromé sféře.

4.6 Dotazníkové šetření

Poslední oblastí praktické části je sběr a analýza dat týkajících se bankovní identity a jejích alternativ. Dotazníkové šetření se bude zabývat využitím, bezpečností a povědomím o bankovní identitě v České republice. Jedním ze zkoumaných bodů je též využití jejích alternativ.

Otázky, jež budou respondentům pokládány, lze rozdělit do tří částí. Cílovou skupinou jsou občané, kteří mají povědomí o bankovní identitě. Kapitolu Dotazníkové šetření lze pak rozdělit do tří částí, jež kopírují zpracování celé praktické části. Otázky se proto týkají hlavních bank v České republice, které banky zprostředkovávají BankID, u kterých je bankovní identita využívána nejvíce, kde se dá využít v soukromé, či státní sféře a jak jsou využívány její alternativy. První část se zaměřuje na povědomí občanů o bankovní identitě. Ti, kteří bankovní identitu znají, tak pokračují v dotazníku dále. Naopak pro ty, kteří o ní nikdy neslyšeli, dotazník končí. Druhou skupinou respondentů jsou občané, kteří aktivně bankovní identitu využívají. Těm jsou postupně kladeny otázky jako například: jak často bankovní identitu používají, zda využívají i jiný způsob ověřování, jejich názor na bezpečnost apod., více viz analýza níže. Třetí a zároveň poslední skupinou respondentů jsou občané, kteří bankovní identitu nevyužívají, ale ví, co to je.

Dohromady bylo získáno 460 respondentů a sběr odpovědí probíhal od 17. července do 28. srpna 2022. Respondenty lze rozdělit do tří hlavních skupin, jak bylo popsáno výše. Pro získání odpovědí byly využity sociální sítě jako Facebook, Instagram a LinkedIn. Dále došlo k vyvěšení letáku s QR kódem na vybraná místa. Dotazník měl 772 návštěv, přičemž byl vyplněn 460 respondenty. Jedná se tedy o 59,6% úspěšnost vyplnění dotazníku. Kromě otázek k tématu bankovní identity došlo v úvodu i k položení několika demografických dotazů, které měly za cíl zjistit věkové skupiny respondentů, jejich vzdělání a banky, které aktivně využívají. Tyto otázky budou rozebrány níže.

Vyberte prosím Vaše pohlaví

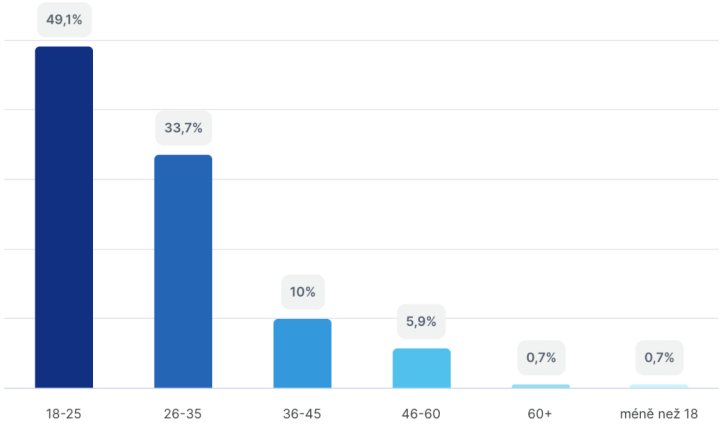
Jedna z prvních otázek dotazníku se týkala pohlaví respondentů. Jejím účelem bylo získat základní demografický přehled o poměru mužů a žen mezi dotazovanými respondenty. Na

základě odpovědí bylo zjištěno, že větší podíl tvořily ženy, a to 52,2 % z celkového počtu. Naopak muži představovali 47,8 % dotazovaných. Ve výsledku se ale nejedná o markantní rozdíl, jelikož představuje pouze 20 respondentů. Dotazník nebyl cílen na konkrétní pohlaví, tudíž šlo spíše o obecnou otázku, jež měla za cíl zjistit genderové rozložení respondentů.

Vyberte prosím Váš věk

Další z demografických dotazů se týkal věku. Jeho cílem bylo zjistit věkové rozložení respondentů. V rámci práce došlo k dohledávání informace týkající se dostupnosti bankovní identity osobám, které jsou mladší 15 let. Nikde nebylo nalezeno, že je bankovní identita přístupná až od 18 let, avšak tato informace není stoprocentní. Vznikl tedy rozpor, zda respondenty neroztřídit podle věku. Nakonec byl vyřešen tak, že tři dotazovaní mladší 18 let odpověděli na následující otázku, že neví, co to bankovní identita je, tudíž v dotazníku dále nepokračovali. Celkové věkové rozložení je znázorněno na grafu níže. Nejpočetnější věkovou skupinu tvořili respondenti ve věku 18–25 let, což je 49,1 % ze všech dotazovaných. Druhou skupinu představuje 33,7 % z celkového počtu ve věku 26–35 let. Graf, jenž detailně ukazuje věkové kategorie respondentů a jejich procentuální rozložení, lze vidět na obrázku 18.

Obrázek 18: Graf – věkové kategorie respondentů



Zdroj: Vlastní (2022)

Jaké je Vaše nejvyšší dosažené vzdělání?

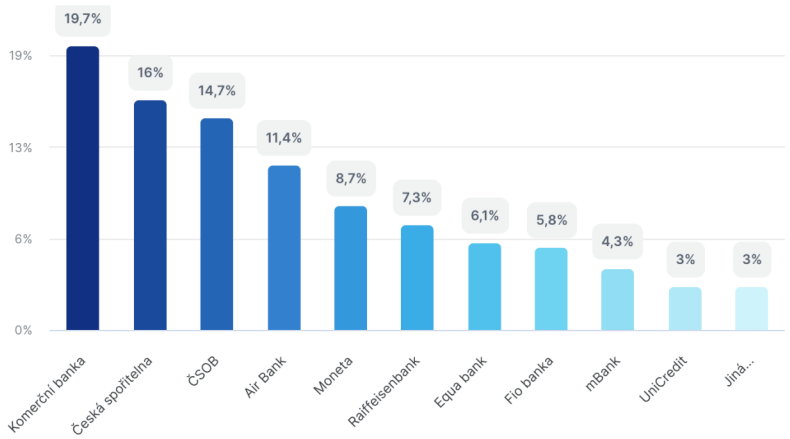
Mezi spíše informativní dotazy lze řadit i následující otázku, jež se týká vzdělání jednotlivých respondentů. Ta měla za cíl zjistit, jaká úroveň vzdělání dominuje mezi dotazovanými. Dotazník vyplnili převážně vysokoškolsky vzdělaní lidé. Ti tvořili

nadpoloviční většinu, a to 57,6 % z celkového počtu respondentů. Zbytek dotazovaných má převážně středoškolské vzdělání s maturitou. Jedná se o 34,3 %.

U které banky máte vedený účet?

V úvodu praktické části byly na základě popisu aktuálního stavu v České republice uvedeny největší banky a jejich řešení bankovní identity. Díky tomu byla položena otázka, která má za cíl zjistit, které banky respondenti nejvíce využívají. Při vyplňování otázky byla možnost volby jedné či více odpovědí. Podle výsledků je nejvíce využívána Komerční banka, která představuje 19,7 %, viz obrázek 19. Tato skutečnost napomáhá předchozím kapitolám, jelikož pro analýzu možností využití u všech portálů a stránek bylo vybráno právě ověřování prostřednictvím Komerční banky. Mezi tři nejvyužívanější banky, které uvedli respondenti, se tedy řadí: Komerční banka, Česká spořitelna a ČSOB. Výsledky otázky tak souhlasí s grafem, jenž je zobrazen na obrázku 1 v úvodu praktické části, to znamená, že tři nejvíce využívané banky jsou totožné v obou grafech.

Obrázek 19: Graf – nejvíce využívané banky



Zdroj: Vlastní (2022)

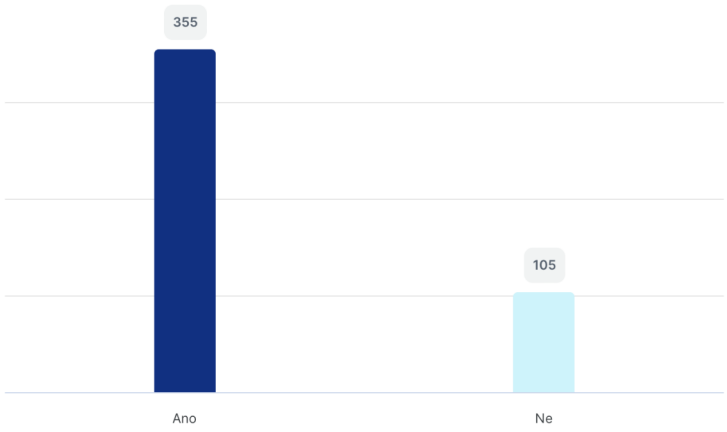
Povědomí o bankovní identitě

Jedním z cílů dotazníkového šetření bylo roztřídit respondenty do dvou kategorií. První kategorie zahrnuje občany, kteří neví, co bankovní identita znamená a čeho se týká. Druhá se naopak skládá z lidí, kteří o ní mají povědomí. Touto problematikou se zabývá následující otázka, již zodpovědělo celkem 460 respondentů. Pokud respondent odpověděl, že o bankovní identitě nic neví, byl ihned přesměrován na konec dotazníku, jelikož by následující otázky byly v tomto ohledu bezpředmětné. Konkrétní znění otázky: „*Máte povědomí o tom, co je to bankovní identita a k čemu se využívá*?“

Z celkového počtu respondentů odpovědělo 355, že má povědomí o bankovní identitě, zbývajících 105 o ní nic neví, viz obrázek 20. Poměr mezi oběma skupinami dotazovaných je 77,2 : 22,8. Většina o bankovní identitě ví. To naznačuje, že se s tímto tématem setkává stále více lidí. Na druhou stranu se zde nachází významný prostor se zlepšovat směrem ke klientům bank, co se týká komunikace a podávání informací o této službě. S ohledem na věkové skupiny měla většina z nich celkový poměr respondentů, kteří o bankovní identitě něco ví, téměř totožný. Jak již bylo uvedeno výše, všichni mladší než 18 let odpověděli, že o bankovní identitě nic neví. Jedná se ale pouze o 3 respondenty, takže z toho nelze dělat žádné významné závěry. Naopak největší podíl těch, kteří povědomí mají, měla věková skupina 26–35 let, a to v poměru 87 : 13.

Dále dojde k analýze poměrů u klientů tří největších a zároveň nejvíce využívaných bank. Respondentů, kteří využívají Komerční banku, je celkově 143. Z nich 72 % odpovědělo, že mají povědomí o bankovní identitě. Naopak 28 % o ní nic neví. U klientů ČSOB je rozdíl mezi zmíněnými dvěma skupinami výraznější. Tam je poměr znajících a neznajících bankovní identitu 91,6 : 8,4. Co se týká České spořitelny, tak 82,8 % ví, čeho se BankID týká, a 17,2 % nemá o ní tušení. Ze získaných dat lze tvrdit, že nejlépe si vede ČSOB. Důvodů může být více, například lepší způsob využití, implementace nebo komunikace směrem ke klientům.

Obrázek 20: Graf – povědomí o bankovní identitě



Zdroj: Vlastní (2022)

4.6.1 Analýza odpovědí využívajících respondentů

Jestliže respondent v předchozí otázce uvedl, že má povědomí o bankovní identitě, byl mu položen dotaz, zda ji též využívá. Podle jeho odpovědi se mu následně generovaly další otázky. Cílem otázky bylo zjistit, kolik z celkového množství respondentů využívá, či

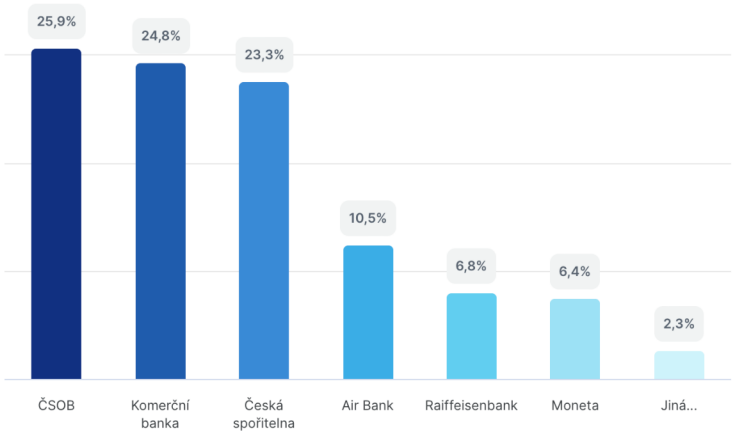
nevyužívá bankovní identitu. Jelikož v předchozím dotazu došlo k vyfiltrování respondentů, je celkové množství odpovědí o něco menší. Na otázku, zda je respondent uživatelem bankovní identity, odpovědělo celkem 355 respondentů, z toho 225 BankID využívá a 130 nevyužívá. Tato kapitola se bude zabývat odpověďmi 225 využívajících respondentů. Zbytek bude popisovat kapitola Analýza odpovědí nevyužívajících respondentů, jež bude uvedena níže.

Celkově tedy 63,4 % uvedlo, že bankovní identitu využívá. Jedná se sice o vyšší číslo než u nevyužívajících respondentů, avšak rozdíl není tak velký. Důvodem může být například skutečnost, že občané využívají jiné alternativy, nebo jsou zvyklí na klasické ověřování prostřednictvím jména a hesla či bankovní identitě nedůvěřují. Všemi těmito otázkami se bude zabývat tato kapitola.

Prostřednictvím které banky aktivně bankovní identitu využíváte?

První otázka, jež byla položena respondentům využívajícím bankovní identitu, se týkala bank, které jim tuto možnost nabízejí. Cílem bylo zjistit, které banky jsou z hlediska BankID nejvyužívanější. Na výběr byly banky uvedené v úvodu praktické části. Mezi jiná se řadí Fio banka. Odpovědi respondentů byly jednoznačné, a sice že k ověřování využívají převážně největší banky v České republice. Všechny tři banky měly zhruba stejné výsledky. Nejvíce měla ČSOB 25,9 %, za ní Komerční banka 24,8 % a jako třetí byla Česká spořitelna s 23,3 %. Další hodnoty lze vidět na obrázku 21 níže. Hlavní příčinou výše popsaných výsledků je nejspíše to, že banky mají velký počet klientů. Dalším důvodem může být například lepší rozpočet na marketingové kampaně či propagace nových služeb.

Obrázek 21: Graf – banky, u kterých je bankovní identita nejvíce využívána

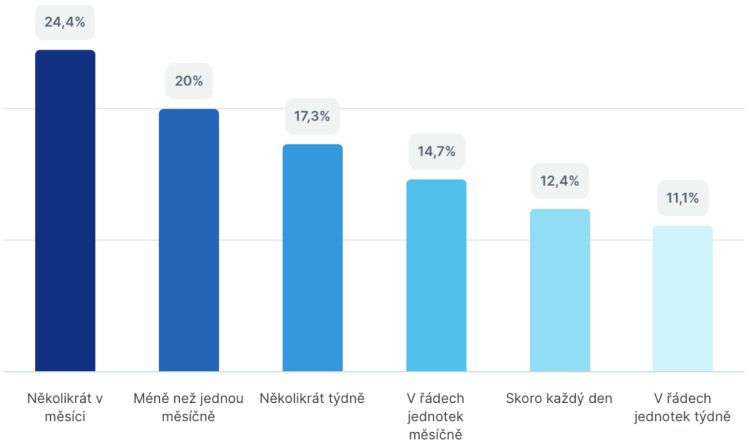


Zdroj: Vlastní (2022)

Jak často využíváte bankovní identitu?

Cílem dotazu bylo zjistit, s jakou mírou je bankovní identita u respondentů používána. Na výběr bylo 6 odpovědí, přičemž nejvíce dotazovaných uvedlo, že ji využívá několikrát v měsíci. Jednalo se o 24,4 % z celkového počtu 225 respondentů. Méně než jednou měsíčně používá bankovní identitu 20 %, několikrát týdně 17,3 %, v řádech jednotek měsíčně 14,7 %, skoro každý den 12,4 % a v řádech jednotek týdně 11,1 % respondentů. Z výsledků je patrné, že větší část respondentů využívá bankovní identitu spíše v řádech jednotek měsíčně. Nejedná se tedy o službu, jež by pro ně byla k využití na denní bázi. V současné době se dá bankovní identita využívat převážně u státních portálů, pojišťoven či energetických společností. Jedná se o místa, kam běžný uživatel nevstupuje každý den. Tato skutečnost může být důvodem ne tak intenzivního využívání. Avšak postupně BankID proniká do dalších soukromých a státních služeb. To by mohlo napomoci jejímu rozsáhlejšímu používání. Detailnější výsledky pak popisuje graf na obrázku 22 níže.

Obrázek 22: Graf – jak často respondenti využívají bankovní identitu



Zdroj: Vlastní (2022)

Zdá se Vám využití bankovní identity praktičtější než ověřování klasickým způsobem (registrace, zadání jména a hesla)?

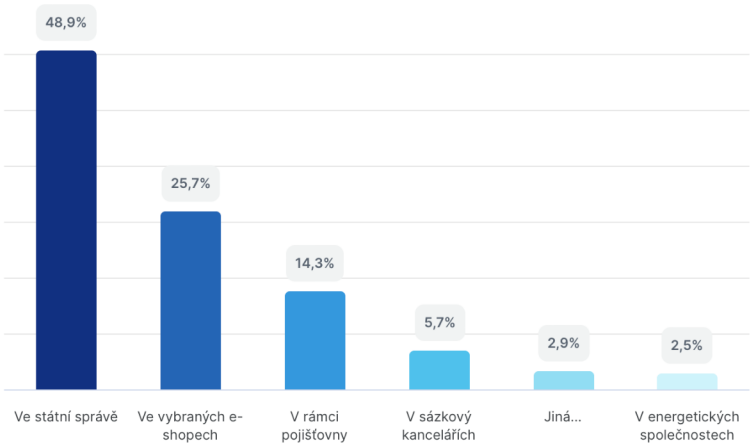
Další otázka měla za cíl zjistit, jaký postoj a názor mají využívající respondenti ohledně bankovní identity v porovnání s klasickým způsobem ověřování. Na výběr bylo z možností: ano, spíše ano, nejsem si jistý, ne a spíše ne. Celkem 59,6 % respondentů odpovědělo ano, přičemž dalších 31,6 % odpovědělo spíše ano. Dohromady se tedy jednalo o 91,2 % dotazovaných, kteří vidí využití bankovní identity jako praktičtější způsob ověřování. Výsledek není překvapivý, jelikož se jedná o analýzu odpovědí respondentů, kteří

aktivně bankovní identitu využívají. Avšak částečně to nasvědčuje tomu, že se jedná o inovaci v oblasti ověřování.

Kde využíváte bankovní identitu nejčastěji?

Praktická část práce se zabývala analýzou možností využití bankovní identity jak ve státní, tak soukromé sféře. S touto problematikou se též pojí následující otázka, která zkoumala, v jakých oblastech je z hlediska respondentů nejvíce využívána. Dotazovaný mohl vybrat jednu či více odpovědí. Výsledek pak popisuje graf, jenž lze vidět na obrázku 23. Na základě odpovědí bylo zjištěno, že nejvyšší využití má BankID ve státní správě. Odpovědi tvořily v poměru k ostatním jasnou většinu, a to 48,9 %. Zmíněnou možnost zvolilo 137 respondentů. Státní správa byla jedním z míst, kde se dalo a dá ověřit prostřednictvím bankovní identity. Zároveň se do portálů státní správy uživatel nepřihlásí jinak než prostřednictvím datové schránky, nebo některou z ověřených identit. Jedná se nejspíše o hlavní důvody výše zmíněného výsledku. Je trochu překvapením, že 72 respondentů uvedlo, že využívají bankovní identitu ve vybraných e-shopech, jelikož v této oblasti není ještě tolik rozšířená. Jednalo se o 25,7 % odpovědí. Třetí nejvíce využívanou oblastí jsou pojišťovny. Ty představují 14,3 % z celkového počtu odpovědí, což není tak dominantní číslo, ale je vidět, že i v této oblasti je bankovní identita využívána.

Obrázek 23: Graf – nejvíce využívané oblasti z hlediska bankovní identity



Zdroj: Vlastní (2022)

Využil(a) jste již někdy bankovní identitu pro přihlášení do státní správy (např. Portál občana, Sčítání lidu apod.)?

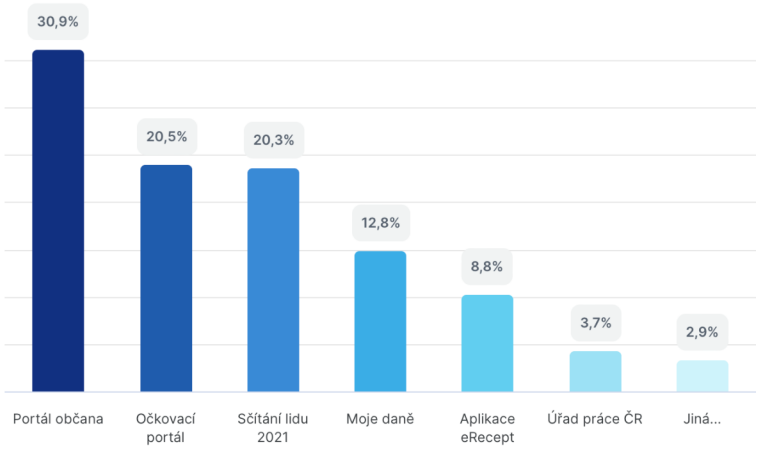
Jak již bylo zmíněno výše, státní správa je jedním z prvních míst, kde se dala bankovní identita využít. Zároveň existuje všeobecné povědomí o tom, že právě v této oblasti je

nejvíce využívána. To potvrdily i výsledky odpovědí respondentů na předchozí otázky. Následující dotaz měl za cíl zjistit, zda uživatelé pomocí BankID přistupují i do státní správy. Dotazovaný měl na výběr ze dvou odpovědí – ano, či ne, přičemž 71,1 % uvedlo, že ji již někdy pro přihlášení do státní správy využilo. Zbývajících 28,9 % ji ve státní správě nevyužívá. Výsledek není nijak překvapivý, protože v předchozí otázce měla státní správa též dominantní postavení. Všech 160 respondentů, kteří uvedli ano, bylo přesměrováno k další otázce, a sice kde přesně ji ve státní sféře využili. Zbývajícím 65 se otázka vůbec nezobrazila.

Kde konkrétně jste bankovní identitu ve státní správě využil(a)?

V praktické části byly popsány vybrané portály státní správy, kde lze bankovní identitu využít. Většina z nich byla použita jako možné odpovědi na následující otázku. Ta má za cíl zjistit, kde konkrétně je nejvíce využívána bankovní identita ve státní sféře. Na výběr měli respondenti ze 7 možností, které lze vidět i s poměrovými hodnotami na obrázku 24. Na základě odpovědí bylo zjištěno, že nejvíce respondentů ve státní sféře využívá Portál občana, tak odpovědělo 30,9 % dotazovaných. Lze tedy říct, že je Portál občana mezi uvedeným vzorkem občanů nejznámějším místem ve státní sféře, kde se ověřují prostřednictvím bankovní identity. Druhou nejuváděnější volbou byl Očkovací portál s poměrem 20,5 % k celkovému počtu 160 respondentů, přičemž hned za ním je Sčítání lidu 2021 s téměř stejnou hodnotou 20,3 %. Tyto portály byly vytvořeny z důvodu dvou největších událostí posledních let, které se týkaly celé České republiky, a to pandemie covidu-19 a celorepublikového sčítání lidu v roce 2021. Zmíněné události mohou být i důvodem výše uvedeného výsledku.

Obrázek 24: Graf – v jaké oblasti státní správy se bankovní identita využívá nejvíce



Zdroj: Vlastní (2022)

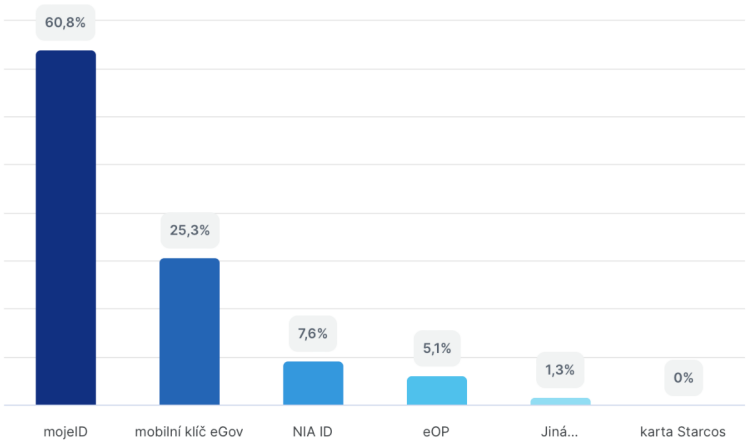
Používáte některé z alternativ bankovní identity?

Poslední část, jež byla zkoumána u využívajících respondentů, jsou alternativy bankovní identity a jejich míra využití. Alternativami se zabývala i praktická část před kapitolou Dotazníkové šetření. Hlavním cílem otázky bylo zjistit, zda uživatelé bankovní identity využívají ještě některé její alternativy. Možnosti odpovědí byly ano, nebo ne. Přičemž ano odpovědělo 71,1 % z celkového počtu 225 respondentů, zatímco ne odpovědělo 28,9 %. Jedná se o poměrně překvapivé číslo, jelikož se zdá zbytečné používat alternativy, které poskytují podobnou, ne-li stejnou službu jako bankovní identita. Avšak mohou být uživatelé, kteří si zřídili jinou identitu ještě před zavedením BankID, nebo alternativy využívají tam, kde bankovní identitu využít nelze. Jestliže dotazovaný uvedl ano, byl přesměrován na další otázku zabývající se tématem, o kterou alternativu se přesně jedná.

Kterou z alternativ bankovní identity využíváte?

Na následující otázku odpovědělo 160 respondentů. Jde o ty, kteří v předchozím kroku uvedli, že využívají některé z alternativ bankovní identity. Obě alternativy ověřování, jež byly detailněji popsány v předchozí části praktické části, byly zařazeny do možných odpovědí. Cílem otázky bylo zjistit, které alternativy nejvíce využívají uživatelé, kteří se již bankovní identitou aktivně ověřují. Všechny možnosti a výsledky lze vidět v grafu na obrázku 25, viz níže. Největší poměr 60,8 % respondentů uvedl, že využívá ještě službu mojeID. Ta, jak byla zanalyzována v předešlé části, funguje z hlediska využití velice podobně jako BankID. Druhou nejvyužívanější alternativou, kterou uvedlo 25,3 % respondentů, je Mobilní klíč eGov. Tedy obě alternativy, které byly zanalyzovány v praktické části, se u uživatelů bankovní identity řadí mezi oblíbené alternativy.

Obrázek 25: Graf – nejvíce využívané alternativy



Zdroj: Vlastní (2022)

4.6.2 Analýza odpovědí nevyužívajících respondentů

Výše došlo k rozboru odpovědí respondentů, kteří bankovní identitu aktivně využívají. Tato kapitola se bude zabývat analýzou odpovědí druhé skupiny, jež je tvořena respondenty, kteří na otázku ohledně využívání bankovní identity odpověděli, že ji nevyužívají. Celkem se jedná o 130 dotazovaných. Hlavním cílem otázek a celé kapitoly je popsat a zjistit, zda respondenti využívají některé z alternativ, pokud ano, tak jaké, z jakých důvodů BankID nevyužívají a zda mají v plánu v blízké době bankovní identitu využívat. Všechny tyto oblasti budou popsány v rámci analýzy odpovědí níže.

Používáte některé z alternativ bankovní identity (eOP, mojeID apod.)?

První dotaz se týkal využití alternativ bankovní identity. Hlavním cílem bylo zjistit, zda občané, kteří bankovní identitu nepoužívají, využívají například některé z jejích alternativ. Na základě odpovědí tak lze částečně rozlišit respondenty z toho hlediska, zda se spíše přiklánějí k novodobějšímu ověřování, jako je bankovní identita, mojeID či Mobilní klíč eGov, nebo mají raději klasický způsob ověřování (jméno a heslo). V rámci dotazu byly nabídnuty dvě jednoznačné možnosti odpovědí, a to ano, nebo ne. Z celkového počtu 130 dotazovaných odpovědělo 69,2 %, že využívá některou z alternativ bankovní identity. Z toho lze usoudit, že důvodem, proč respondenti nevyužívají BankID je, že k ověřování volí právě některou z jejích alternativ. Touto problematikou se ale ještě bude zabývat jedna z následujících otázek. Všichni respondenti, kteří odpověděli pozitivně, byli přesměrováni na otázku, jež detailněji zkoumala, o kterou z alternativ se jedná, viz níže.

Kterou z alternativ bankovní identity využíváte?

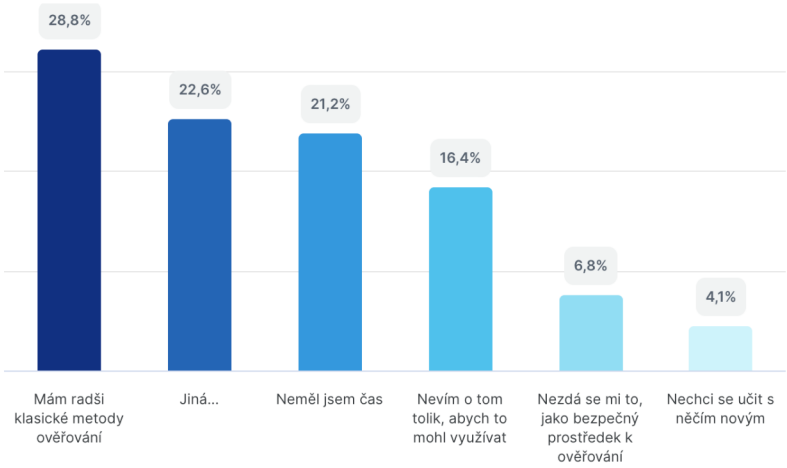
Všech 69,2 % respondentů, kteří v předchozí otázce odpověděli, že využívají některou z alternativ bankovní identity, bylo přesměrováno na následující otázku. Tu zodpovědělo celkem 90 dotazovaných. Na výběr měli stejné možnosti jako využívající respondenti na obrázku 25. Hlavním cílem bylo zjistit, kterou z alternativ využívají respondenti nepoužívající k ověřování identity BankID. Odpovědi byly téměř totožné jako u využívajících klientů. Nejvíce respondentů využívá mojeID. Jednalo o 53,2 % z celkového počtu. Druhou nejčastější volbou, kterou vybralo 25,5 % dotazovaných, byl Mobilní klíč eGov. Důvody těchto výsledků jsou nejspíše stejné, jako byly zmíněny v odstavci výše, jenž se též týkal konkrétních alternativ. Zajímavostí je, že u nevyužívajících občanů je větší poměr respondentů, celkem 14,9 %, kteří více využívají k ověřování eOP, než byl u využívajících. U nich bylo na třetím místě ověřování prostřednictvím NIA ID. Zároveň

z výsledků průzkumu vyplynulo, že jak využívající, tak nevyužívající respondenti vůbec nepoužívají k ověřování kartu Starcos.

Z jakých důvodů bankovní identitu nevyužíváte?

Jednou z nejzásadnějších otázek a cílů této části práce bylo zjistit, z jakých důvodů respondenti bankovní identitu nevyužívají. Touto problematikou se zabývá právě otázka, na základě jejíchž výsledků by mohlo dojít k doporučení, jak ještě lépe získávat nové uživatele bankovní identity. Respondentům bylo navrženo 6 základních možností odpovědí na zmíněnou otázku. Výsledky lze vidět v grafu na obrázku 26. Celkem 28,8 % respondentů uvedlo, že bankovní identitu nevyužívá, protože má raději klasické metody ověřování. To přibližně odpovídá i počtu respondentů, kteří odpověděli, že nepoužívají ani alternativy bankovní identity. Druhou nejpočetnější a zároveň zajímavou odpovědí byla možnost jiná, kde dotazovaný mohl napsat jiný z důvodů, než byl předem uvedený. Ze získaných odpovědí byly vybrány ty nejzajímavější. Tady jsou: *„Alternativní metody jsou lepší. Nechápu proč by banka měla být prostředníkem pro přístup ke státní správě“; „Moje banka zatím nepodporuje“; „Mám datovou schránku a vše řeším jejím prostřednictvím“; „Moje ID umožňuje Windows Hello“; „Nebyla možnost, proto jsem zvolil ověření skrze Mobilní klíč eGov“; „Nemá „vysokou“ úroveň zabezpečení. Nejde používat jako e-občanka“; „Neověřuje to nic, neručí za unikátnost. Můžu mít klidně 10 bankovních účtů a 10 BankID identit, což je jako mít 10 pasů“; „Využívám již její alternativy“* a *„Zatím jsem nepotřeboval*“. Další z odpovědí, již zvolilo 21,2 % dotazovaných, byla skutečnost, že nemají čas. Naopak nejméně respondentů uvedlo, že se nechce učit novým věcem a že se jim bankovní identita nezdá být bezpečným prostředkem k ověřování. Z toho lze vyvodit, že respondenti, co se týká bezpečnosti, mají v bankovní identitě většinou důvěru. Tomu se ale bude věnovat poslední část dotazníkového šetření níže. Ze získaných dat a výsledků lze pro získání většího množství uživatelů bankovní identity doporučit, aby lépe a více docházelo k představování benefitů bankovní identity, aby je ti, kdo stále využívají klasické metody nebo neměli čas nebo o ní tolik neví, viděli, pochopili a začali tak bankovní identitu využívat. Zároveň bylo mnoho odpovědí respondentů, které uváděly, že tuto službu jejich banka zatím neposkytuje. S rostoucím počtem bank by tedy mohl narůstat i počet dalších uživatelů. Jednotky respondentů též uvedly, že důvodem pro nepoužívání BankID je, že nedosahuje úrovně „vysoká“. Jedná se tedy o možné budoucí rozšíření této služby, jež by mohlo přitáhnout další uživatele. V bankovním prostředí jde ale o hodně složitý krok.

Obrázek 26: Graf – důvody nevyužívání bankovní identity

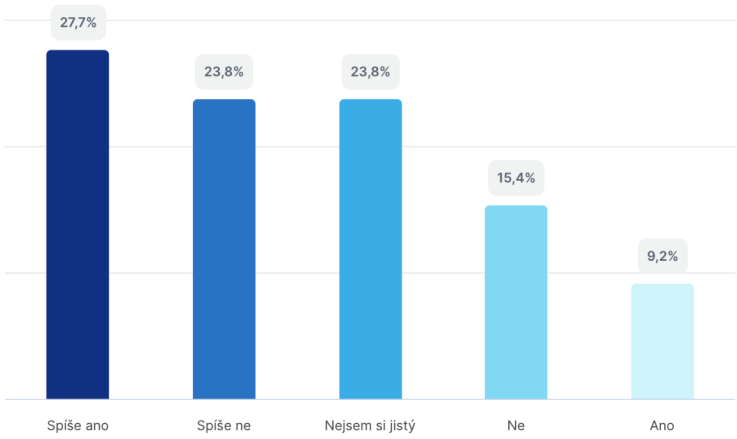


Zdroj: Vlastní (2022)

Máte v plánu v blízké době bankovní identitu začít používat?

Jedním z cílů dotazníku bylo též zjistit, zda lidé, kteří bankovní identitu nevyužívají, mají v plánu její budoucí používání. Díky analýze získaných výsledků by pak mohlo být zřejmé, kolik procent respondentů se do budoucna může stát aktivními uživateli bankovní identity. Dotazovaní měli na výběr z 5 odpovědí. Všechny odpovědi i s procentuálním rozložením lze vidět na obrázku 27. Z výsledků dotazníku je zřejmé, že většina nevyužívajících respondentů si s budoucím využíváním bankovní identity není stoprocentně jistá. Celkem 27,7 % respondentů uvedlo, že ji v budoucnu spíše využívat začne. Naopak 23,8 % uvedlo, že bankovní identitu spíše využívat nebude. Stejné procento respondentů si není odpovědí jisto. Jenom 9,2 % s jistotou odpovědělo, že v budoucnu mají v plánu bankovní identitu využívat. Na základě této skutečnosti lze říct, že nevyužívající respondenti mají své důvody bankovní identitu nevyužívat, proto neplánují v budoucnu její aktivní používání, nebo si nejsou jistí.

Obrázek 27: Graf – názor na možné budoucí využití bankovní identity



Zdroj: Vlastní (2022)

4.6.3 Názor na budoucnost a bezpečnost

Poslední oblast dotazníkového šetření se zabývá získáním a vyhodnocením informací ohledně názoru na budoucnost bankovní identity v České republice a její bezpečnost. Jelikož se nejedná o hlavní oblasti výzkumu, byly respondentům položeny pouze tři otázky. Odpovědi na ně by ale měly podat alespoň základní přehled ohledně mínění veřejnosti ve zmíněných dvou oblastech. Dotazy zodpovědělo celkem 355 respondentů, kteří v úvodu dotazníku uvedli, že mají povědomí o tom, co je bankovní identita.

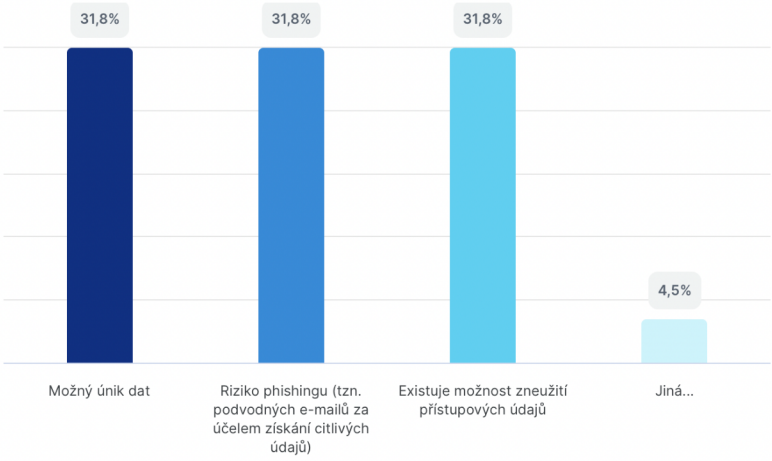
Myslíte si, že je bankovní identita bezpečným způsobem ověřování identity?

První a druhá otázka z této oblasti se zabývá výzkumem názorů na bezpečnost bankovní identity. Banky si pro poskytování této služby musí uchovávat množství soukromých informací o jednotlivých svých klientech. Bezpečnost takových informací zajišťují samotné systémy banky. Vyvstává tedy otázka, zda respondenti mají pocit, že jsou jejich osobní údaje v bezpečí a že je BankID bezpečným ověřováním identity. Na otázku bezpečnosti odpovědělo celkem 355 respondentů. Z toho 43,1 % odpovědělo ano a 42,5 % odpovědělo spíše ano. Převážná většina respondentů má pocit, že jsou jejich osobní údaje zcela v bezpečí. Na základě výsledků lze konstatovat, že většinový vzorek respondentů dotazníkového šetření nemá s bezpečností bankovní identity žádný problém. Jestliže dotazovaný odpověděl, že bankovní identita spíše nebo vůbec není bezpečným prostředkem ověřování, byl přesměrován na otázku, která se zabývala konkrétními důvody.

Proč se Vám bankovní identita nezdá být bezpečným prostředkem ověřování?

Celkem 14 respondentů v předchozím dotazu uvedlo, že spíše, nebo vůbec nevěří v bezpečnost bankovní identity. Jedná se o velice malý vzorek, tudíž jsou výsledky uváděné spíše pro zajímavost. Po analýze bankovní identity na webových stránkách a portálech došlo k vytvoření tří možných odpovědí, jež představují nejznámější potenciální hrozby bankovní identity. Pokud si respondent nevybral z těchto tří možností, mohl uvést svůj vlastní důvod. Z výsledků na obrázku 28 je patrné, že se dotazovaní obávají všech tří uvedených hrozeb úplně stejně, tedy jak možného úniku dat, tak rizika phishingu i možnosti zneužití přístupových údajů, což činí 31,8 %. Zbývající 4,5 % dotazovaných uvedla jiný důvod, proč v bezpečnost BankID nemají důvěru. Konkrétně se jednalo o jednoho respondenta, jenž uvedl: „*Banka vystupuje vůči státu jako moje osoba.*“

Obrázek 28: Graf – bezpečnostní hrozby bankovní identity



Zdroj: Vlastní (2022)

Věříte, že je bankovní identita budoucností ověřování identity v České republice?

Závěr dotazníku byl věnován otázce, která se zabývala názorem respondentů na budoucnost bankovní identity jako způsobu ověřování v České republice. Na výběr byla klasická škála odpovědí, přičemž 41,1 % z celkového počtu 355 respondentů spíše věří, že se jedná o budoucnost ověřování, a 32,1 % uvedlo, že věří úplně. Dalších 17,5 % dotazovaných si nebylo odpovědí jisto a 9,3 % odpovědělo, že v to spíše nebo vůbec nevěří. Z výsledků je na první pohled patrné, že dominantní většina respondentů v budoucnost bankovní identity v České republice věří. Podle názoru respondentů, lze tedy v následujících letech předpokládat další rozšiřování a využívání BankID v různých segmentech.

5 Výsledky a diskuse

Kapitola se bude zabývat souhrnem a popisem výsledků praktické části práce. V úvodu bude zhodnocena analýza stavu a připravenosti bankovní identity v rámci tří největších bank v České republice. Dále dojde k interpretaci výsledků z analýzy možností využití, jež byla provedena jak ve státní, tak soukromé sféře. Následným bodem bude porovnání bankovní identity s jejími alternativami. Souhrnný výstup dotazníkového šetření popíše výsledky výzkumu mínění veřejnosti ohledně bankovní identity, které tvořilo závěr praktické části. Závěr kapitoly popíše přínosy a doporučení k bankovní identitě a uvede možná rozšíření diplomové práce.

5.1 Zhodnocení připravenosti jednotlivých bank

Jeden z dílčích cílů práce obnášel analýzu aktuálního stavu bankovní identity v rámci českých bank. Pojmem připravenosti bank bylo myšleno shrnutí jejich aktuálního stavu a definování závěrů plynoucích z provedené analýzy u tří největších bank v České republice. Jedná se o Komerční banku, ČSOB a Českou spořitelnu.

V rámci každé z nich došlo ke zmínění zásadních událostí, které v průběhu zavádění bankovní identity nastaly. Například Komerční banka spustila pilotní provoz jejího řešení 26. ledna v roce 2021, přičemž samotným klientům byla bankovní identita zprostředkována 24. března 2021. Jednalo se o termín, jenž byl těsně před sčítáním lidu v roce 2021. Zmíněná banka aktuálně umožňuje i řešení pro firmy, kde nabízí tři základní formy BankID. Co se týká ČSOB, tak jde o banku, která jako první získala v roce 2020 akreditaci od Ministerstva vnitra. Dalším zásadním krokem ČSOB bylo zpřístupnění bankovní identity pro ověření u služeb soukromých poskytovatelů (tzv. SONIA), jenž se uskutečnilo 1. června v roce 2021. Jednou z posledních inovací banky ve zkoumané problematice byl digitální podpis smluv či dokumentů, a to u soukromých společností, jež jsou začleněné do řešení BankID. Poslední bankou byla Česká spořitelna. Ta jako první v České republice začala zprostředkovávat svým klientům bankovní identitu a jako druhá získala akreditaci od Ministerstva vnitra pro ověřování svých klientů u služeb veřejné správy. Postupem času své portfolio míst, kde lze bankovní identitu využít, rozšířila například o společnost ČEZ nebo o Generali Českou pojišťovnu. V říjnu 2021 jako první banka spustila digitální podpis dokumentů prostřednictvím BankID SIGN.

Jedním z možných kritérií, podle kterého lze připravenost dílčích řešení bank zhodnotit, je fakt, že za dobu fungování a zavádění bankovní identity v České republice nenastal žádný zásadní bezpečnostní ani jiný problém, jež by s ní byl pojen. Důvodem je nejspíše skutečnost, že banky musí získat od státu potřebnou akreditaci a musí splňovat tzv. Zákon o bankovní identitě. Základní principy zákona byly též objasněny v praktické části práce.

Na základě praktických ukázek došlo k představení procesu použití bankovní identity u jednotlivých bank. Proces byl u všech téměř totožný a probíhal v principu ve dvou krocích. Každá banka má vlastní aplikaci zvanou Klíč, pomocí níž se klient ověřuje. Podobnost řešení je nejspíše důsledkem skutečnosti, že banky na projektu Bankovní identity vzájemně spolupracují. Zajímavým faktem, díky němuž se řešení České spořitelny odlišovalo od ostatních, bylo zprostředkování aplikace Správa třetích stran, kde má klient možnost kontrolovat svá jednotlivá ověřování nebo bankovní identitu zneaktivnit.

5.2 Zhodnocení možností využití bankovní identity

Zavádění bankovní identity se v České republice realizuje rychlým tempem. Aktuálně ji k roku 2022 zprostředkovává 7 bank, jak bylo podrobněji vyloženo v úvodu praktické části. Jejím prostřednictvím se lze ověřit nejen ve státní správě na jednotlivých portálech, ale i v soukromé sféře na vybraných stránkách a e-shopech. Na základě zmíněných skutečností byla v praktické části provedena analýza možností využití bankovní identity v jednotlivých sférách. Pro výzkum bylo využíváno ověřování u Komerční banky, protože se jedná o jednu z nejvyužívanějších bank, což potvrdil i výsledek dotazníkového šetření.

5.2.1 Analýza v soukromé sféře

Na počátku příchodu bankovní identity bylo její využití převážně na jednotlivých portálech státní správy. Na základě jejího rozšiřování se dostává více i do soukromé sféry, která se uživatelům může zdát atraktivnější, jelikož se jedná o e-shopy a stránky, které využívají někdy i na denní bázi. Jedná se o část bankovní identity s názvem SONIA, jenž byla podrobněji popsána v teoretické části.

První ukázka se zaměřila na analýzu využití bankovní identity u společnosti Alza.cz. Firma byla vybrána, jelikož se jedná o jeden z největších e-shopů v České republice, který má bohatou klientelu. Společnost využívá bankovní identitu pro ověření identity svých klientů pro službu Třetinka. Ta umožňuje zákazníkovi zaplatit pouze třetinu ceny, přičemž zbytek doplatí později. Způsob využití bankovní identity u zmíněné služby pak popisuje

ukázka v praktické části. Největší výhodou a přínosem bankovní identity v této oblasti je fakt, že si společnost prostřednictvím získaných údajů ověřuje bonitu uživatele. Ten tak nemusí chodit na pobočku a urychluje se celý proces zprostředkovávané služby.

Možnost ověření identity pomocí BankID umožňuje i řada pojišťoven a investičních společností. V rámci práce byla pro praktickou ukázku vybrána společnost Avant.cz, která se zabývá hlavně rozvojem fondů a investičními příležitostmi. Využívá bankovní identitu pro vstup svých zákazníků do portálů společnosti. Uživatelé se pak nemusí složitě registrovat, ale stačí jim prostřednictvím bankovní identity nasdílet údaje dané společnosti.

Poslední oblastí, kde byly zmíněny možnosti využití bankovní identity v soukromé sféře, byla energetika. Konkrétně došlo k výběru portálu Pražské plynárenské. Ta dává své klientele možnost se při registraci do zákaznického portálu nebo při uzavírání smluv na nekomoditní produkty ověřit prostřednictvím své banky. Jedinou a zásadní podmínkou je, že uživatel musí být již zákazníkem Pražské plynárenské a mít podepsanou smlouvu. Z toho plyne, že se stejně musí osobně dostavit a potřebné náležitosti zařídit. Naopak výhodou, kterou přináší samotné ověření prostřednictvím bankovní identity, je možnost registrace, přihlášení a uzavírání smluv na nekomoditní produkty. S ohledem na energetickou krizi a zvýšení poptávky po fotovoltaice může tato služba ušetřit klientům mnoho času.

Po komunikaci a tiskových zprávách společnosti BankID, jež se podílí na ověření pomocí bankovní identity, je zřejmé, že v soukromém sektoru přibývá společností, které umožňují svým klientům službu využívat. Způsob využití je, jak popisují jednotlivé praktické ukázky, pro uživatele jednoduchý, jelikož se jedná o velmi podobný proces přihlášení jako do internetového bankovnictví. Mezi jednotlivými implementacemi na rozebraných stránkách se nevyskytoval žádný markantní rozdíl.

5.2.2 Analýza ve státní sféře

Druhou oblastí, kde byly analyzovány možnosti využití bankovní identity v České republice, byla státní sféra. Obecně se jedná o připojení k Národnímu bodu pro identifikaci (tzv. NIA). Jelikož v ní bylo ověření pomocí BankID či jiných jejích alternativ umožňováno dříve než ve sféře soukromé, jsou zde možnosti jejího využití o něco výraznější. Důkazem je, že většina portálů dílčích ministerstev nabízí ověření identity právě prostřednictvím bankovní identity. Došlo tedy k popisu způsobů jejího využití na předem vybraných portálech.

Prvním analyzovaným portálem byl Portál občana. Před samotnou praktickou ukázkou byl kontaktován tým Portálu občana s dotazy na bankovní identitu. Nejzásadnějšími výstupy z odpovědí bylo, že identifikační prostředky s úrovní záruky značná (BankID, NIA ID, mojeID…) představují více než polovinu přihlášení do Portálu občana a samotná bankovní identita České spořitelny je na druhém místě jako nejoblíbenější elektronický prostředek k přihlašování k online službám veřejné správy s 2,8 miliony použití. Dále kupříkladu bylo poznamenáno, že BankID představuje jednoduchý přístup k online službám státu, a proto se tak rychle v poslední době rozšiřuje. Výsledek praktické ukázky, jež se týkala samotného procesu využití na portálu, ukázal, že uživatel na rozdíl od soukromé sféry komunikuje prostřednictvím tzv. Identity občana, a to u všech portálů státní sféry. Na něm například uživatel uděluje souhlas pro výdej osobních údajů. Přihlášení a výběr banky pak probíhaly podobně jako u sféry soukromé.

Většina lidí se setkává ať už přímo, či nepřímo s nutností platit daně. Proto došlo k popisu využití portálu Moje daně, jenž se touto problematikou zabývá. Z analýzy vyplynulo, že stejně jako u ostatních portálů využívá k ověřování Identitu občana. Naopak zajímavou odlišností je Daňová informační schránka, která je určená daňovým subjektům k nejrůznějším činnostem v rámci daní a představuje, dá se říct, tzv. „Online finanční úřad“. V rámci práce došlo tedy k její aktivaci a následnému popisu.

Posledním představeným portálem byl klientský portál MPSV. Jedná se o novou službu vzniklou v roce 2022 kvůli krizi. Jejím prvotním cílem bylo zabezpečit vyplácení příspěvku na dítě v hodnotě 5 000 Kč. Do aplikace Jenda, která je problematice určena, se uživatel může přihlásit pomocí bankovní identity. Nemusí tak chodit na úřad a zařizovat věci osobně. V rámci práce došlo k popisu toho, jak se o dávku dalo požádat a jak se do portálu lze přihlásit pomocí BankID. Jde o další příklad z praxe, který potvrzuje, jak užitečná a nápomocná je bankovní identita.

Státní sféra způsoby ověřování, jako je například bankovní identita, využívá a asi využívat bude i u dalších potenciálně vytvořených portálů. Samotné přihlášení či registrace se na jednotlivých portálech příliš neliší, jelikož je implementovaná tzv. Identita občana. To představuje velkou výhodu pro uživatele, který se přihlašuje v již známém prostředí na všech portálech.

5.3 Bankovní identita v porovnání s alternativami

Bankovní identita má v České republice několik alternativ. Proto je na místě je v souvislosti s jejím postupným zaváděním definovat. Většina z nich byla totiž vytvořená ještě před jejím zavedením. To může mít dopad na míru jejího využití, jelikož jsou někteří lidé zvyklí používat jiné metody a nové se nechtějí učit, nebo se jim to může zdát zbytečné. Dvě nejznámější alternativy byly popsány v praktické části. Výsledky pak popisují, jaké jsou hlavní rozdíly mezi BankID a zmíněnými alternativami.

První vybranou alternativou byla služba mojeID. Na základě analýzy se došlo k závěru, že proces ověření se zdá být z hlediska pohledu uživatele téměř totožný. Jako negativum oproti bankovní identitě lze zmínit fakt, že si uživatel musí mojeID založit a následně se ještě ověřit pomocí další metody, jako je například datová schránka. Celý postup založení identity mojeID popisuje praktická ukázka využití v kapitole mojeID. Jako pozitivum lze zmínit například fakt, že mojeID umožňuje Windows Hello, na což bylo poukázáno respondentem v rámci dotazníkového šetření. Dalším pozitivem oproti bankovní identitě je možnost úrovně záruky. Jelikož mojeID zprostředkovává až úroveň záruky „vysoká“, přičemž bankovní identita pouze úroveň „značná“.

Druhou alternativou, jež byla popsána v praktické části, je Mobilní klíč eGovernmentu. Zde se narazilo na zajímavou metodu ověření uživatele, a to možnost nastavení si obrázkového hesla. Co se týká porovnání s BankID, z popisu v praktické ukázce vyplývá, že se jedná o jednodušší způsob ověření. Uživateli stačí v mobilní aplikaci oskenovat QR kód a nemusí zadávat žádné další přihlašovací údaje. Naopak nevýhodou je, že si musí Mobilní klíč eGovernmentu založit. Proces samotného založení byl popsán v praktické části. Dalším negativem je skutečnost, že oblast využití služby je oproti BankID pouze ve státní sféře.

5.4 Zhodnocení výsledků dotazníkového šetření

Pro získání základního povědomí veřejnosti o bankovní identitě a jejích alternativách byl vytvořen dotazník, jehož výsledky byly popsány v závěru praktické části. Získání účastníků probíhalo od 17. července do 28. srpna 2022 a cílovou skupinou byli lidé, kteří mají alespoň základní povědomí o bankovní identitě. Dotazníkového šetření se zúčastnilo celkem 460 respondentů, přičemž 52,2 % odpovídajících byly ženy a 47,8 % představovali muži. Nejpočetnější věkovou skupinu představovali lidé ve věku od 18–25 let, jednalo se o 49,1 % všech dotazovaných. Otázky v dotazníku korespondovaly s osnovou praktické části. To

znamená, že nejprve se otázky týkaly využití bank v České republice. Následně byl zkoumán názor respondentů na bankovní identitu v soukromé a státní sféře. Další část se věnovala dotazům na téma alternativ a závěr dotazníku se zaměřil na budoucnost a bezpečnost BankID.

Z výsledků dotazníkového šetření se zjistilo, že nejvíce respondentů využívá účet u Komerční banky. Konkrétně se jednalo o 19,7 % dotazovaných. Další v pořadí byla Česká spořitelna a ČSOB. Výsledek napomáhá ukázkám v praktické části, jelikož v jejich rámci bylo zvoleno ověření právě prostřednictvím Komerční banky. Jak již bylo zmíněno výše, cílovou skupinou byli občané, kteří mají alespoň základní povědomí o bankovní identitě. Tou se zabývala následující otázka, jež měla respondenty roztřídit. Pokud respondent odpověděl, že o bankovní identitě nic neví, byl přesměrován rovnou na konec dotazníku. Celkově 355 respondentů mělo povědomí o tom, co bankovní identita je. Zbývajících 105 dotazovaných odpovědělo, že o ní nic neví. Většina ale bankovní identitu zná, avšak stále mají banky nezanedbatelný počet klientů, jež je třeba oslovit. Nejvíce respondentů, kteří měli povědomí o bankovní identitě, mělo vedený účet u ČSOB.

Respondenti informovaní o bankovní identitě byli v následující části roztříděni do dvou skupin a na základě toho jim byly pokládány další otázky. Celkově 225 dotazovaných odpovědělo, že BankID využívá a 130 ji nevyužívá. Z analýzy odpovědí bylo zjištěno, že nejčastější bankou, prostřednictvím které respondenti bankovní identitu aktivně využívají, je ČSOB. Jednalo se o 25,9 % z celkového počtu 225 respondentů. Za ní byla Komerční banka (24,8 %) a následně Česká spořitelna (23,3 %). Z čísel plyne, že rozdíl ve výsledcích tří největších bank je téměř zanedbatelný. Dalším cílem bylo zjistit, v jaké míře je bankovní identita využívána. Největší množství respondentů uvedlo, že je to několikrát v měsíci (24,4 %) a méně než jednou měsíčně (20 %). Z výsledků lze říct, že pro respondenty není bankovní identita služba, kterou by využívali na denní bázi. Další zjištěnou skutečností u využívajících klientů bylo, že 59,6 % se zdá být bankovní identita praktičtějším způsobem ověření identity, než je klasický způsob (registrace, zadání jména a hesla). Přičemž 31,6 % uvedlo, že spíše ano. Jedná se tedy o převážnou většinu, které se zdá být BankID výhodnější. Z dotazů na uživatele se též zjistilo, v jaké oblasti využívají bankovní identitu nejčastěji. Celkem 48,9 % z nich uvedlo, že ji nejčastěji využívají ve státní sféře, což není zas tak překvapivá skutečnost, jelikož má v této oblasti největší možnosti využití. Překvapením bylo, že druhou nejčastější odpovědí bylo ve vybraných e-shopech (25,7 %), protože se v této oblasti teprve začíná rozrůstat. Ze získaných dat lze též říct, že 71,1 % z 255

respondentů někdy bankovní identitu využilo ve státní sféře. Této skupině o 160 respondentech byla položena další otázka, a to na jakém portálu ji ve státní sféře využili. Celkem 30,9 % uvedlo Portál občana, 20,5 % Očkovací portál a 20,3 % Sčítání lidu v roce 2021. Z výsledků lze říct, že nejvyužívanějším portálem ve státní správě u vybrané skupiny respondentů je právě Portál občana, jenž byl též popsán a zanalyzován s ohledem na bankovní identitu v rámci praktické části. Poslední dotazy, které byly pokládány pouze na vytříděnou skupinu využívajících respondentů, se týkaly alternativ. Dotazovaný měl na výběr pouze dvě možnosti, a sice zda některou alternativu BankID využívá, či ne. Výsledkem bylo, že 71,1 % z 255 dotazovaných některou alternativu využívá, 28,9 % nevyužívá. Ze získaných 160 respondentů pak uvedlo 60,8 %, že k bankovní identitě využívá ještě mojeID a 25,3 % Mobilní klíč eGovernmentu. Závěrem lze tedy říct, že se jedná o dvě nejvyužívanější alternativy u vybrané skupiny respondentů, které byly také podrobněji popsány v praktické části práce.

Druhou skupinu, jak již bylo zmíněno výše, tvořili respondenti, kteří o bankovní identitě mají povědomí, ale nevyužívají ji. Celkově se jednalo o 130 dotazovaných. Hlavním cílem dotazů bylo zjistit, zda daná skupina respondentů místo bankovní identity využívá některé z jejích alternativ, jaký je hlavní důvod, proč bankovní identitu nevyužívají a zda mají v plánu ji někdy v budoucnu začít využívat. Z analýzy dat lze říct, že 69,2 % nevyužívajících respondentů používá některé z jejích alternativ. Zbytek tedy nevyužívá BankID, ani žádnou alternativu a asi se přiklání ke klasickému způsobu ověřování. Zmíněných 69,2 % respondentů pak nejvíce využívá jako alternativu službu mojeID (53,2 % z celkového počtu 90) a Mobilní klíč eGovernmentu (25,5 %). Výsledky nejsou tedy od využívaných respondentů příliš odlišné. Nejzajímavější zkoumanou částí v této oblasti byly důvody nevyužívání bankovní identity. Zde odpovědělo 28,8 % respondentů, že má raději klasické metody ověřování. Další nejčastější odpovědí byla možnost „Jiná“, kam dotazovaní psali vlastní názor. Jako hlavní důvody například uvedli, že již využívají některé z jejích alternativ, že to jejich banka zatím nepodporuje nebo že nemá „vysokou“ úroveň zabezpečení a nezaručuje unikátnost. Dalších 21,2 % pak uvedlo, že ještě neměli čas si ji vyzkoušet. Nejméně respondentů odpovědělo, že se nechce učit novým věcem. Z toho plyne příležitost pro oslovení nových potenciálních uživatelů bankovní identity. Z analýzy výsledků se dále zjistilo, že 27,7 % bankovní identitu spíše využívat začne. Naopak 23,8 % ji využívat spíše nebude. Větší část respondentů si tedy s jejím budoucím využíváním není

zatím stoprocentně jistá. Pouze 9,2 % respondentů má v plánu bankovní identitu do budoucna začít využívat.

Poslední část dotazníkového šetření se zabývala budoucností a bezpečností bankovní identity v České republice. Na dotazy ve zmíněné oblasti odpovědělo 335 respondentů, kteří v úvodu uvedli, že mají povědomí o tom, co je to bankovní identita. Získaná data pak ukázala, že 43,1 % věří, že je bankovní identita bezpečným prostředkem ověření, zatímco 42,5 % tomu spíše věří. Jedná se tedy o převážnou většinu respondentů. Ti, kdo v ni nemají plnou důvěru (14 respondentů) byli přesměrováni na další otázku, jež měla za cíl zjistit důvody, proč se jim nezdá být BankID bezpečným prostředkem ověření. Tři nejčastěji zvolené důvody byly: možný únik dat, riziko phishingu a možnost zneužití přístupových údajů. Některý z respondentů též uvedl svůj vlastní důvod, a sice že banka vystupuje vůči státu jako jeho osoba. Poslední dotaz šetření se věnoval otázce budoucnosti bankovní identity, kde 41,1 % z 355 respondentů spíše věří, že se jedná o budoucnost ověřování v České republice, 32,1 % věří zcela. Celkem 17,5 % si nebylo odpovědí jisto. Z interpretovaného výsledku je patrné, že většina respondentů má víru v bankovní identitu a lze v nadcházejících letech předpokládat další její rozšiřování.

5.5 Přínosy a doporučení

Kapitola se bude zabývat vybranými přínosy diplomové práce a budou též uvedena některá doporučení, jež byla zjištěna na základě jejího zpracovávání. Hlavními přínosy práce jsou:

- Základní přehled o současné situaci v ČR – diplomová práce udává základní přehled o největších bankách v České republice, o společnosti BankID, která bankovní identitu provozuje, a způsobu implementace bankovní identity v České republice.
- Analýza řešení bankovní identity v rámci jednotlivých bank a interpretace výsledků – práce představuje zásadní události, které se pojí se zaváděním bankovní identity a konkrétní bankou. Popisuje způsoby využití u jednotlivých bank a definuje jejich aktuální stav.
- Analýza možností využití jak ve státní, tak soukromé sféře – v rámci práce bylo analyzováno využití na několika portálech a stránkách jak už státní, tak soukromé sféry. Z toho vyplynuly různé závěry a názory, které byly popsány

v praktické části práce. Přínosem je též zajištění přehledu, kde se dá bankovní identita využít a jakým způsobem.

- Procesní diagramy pro představení fungování bankovní identity – na základě analýzy v obou sférách byly vytvořeny procesní diagramy, jež podrobněji popisují proces ověření pomocí bankovní identity. Diagramy jsou též popsány slovně.
- Popis procesu založení a využití alternativ bankovní identity – v rámci práce bylo popsáno založení a praktické využití dvou nejznámějších alternativ bankovní identity. Byly tak představeny další možnosti ověření, které může lze využít. Zároveň došlo k porovnání se samotnou bankovní identitou, takže byla podána i základní představa o plusech a mínusech jednotlivých alternativ.
- Přehled mínění veřejnosti ohledně bankovní identity a jejích alternativ – závěr praktické části se zabýval výzkumem mínění veřejnosti. Dotazy na respondenty byly sestaveny v souvislosti s řešenou problematikou. Následně došlo ke stanovení závěrů, jež objasňují aktuální názor na bankovní identitu ve společnosti, její míru využití a další. Zároveň na základě ohlasů z dotazníku byli nalezeni respondenti, kteří na jeho základě zjistili, co je vlastně bankovní identita, a přemýšlejí o jejím využívání.

Při zpracovávání jednotlivých již zmíněných analýz a vyhodnocování dat z dotazníku byla vyvozena některá doporučení. Prvním problémem, na který se při psaní narazilo, je skutečnost, že bankovní identita nemá „vysokou“ úroveň zabezpečení, a proto ji někteří lidé nevyužívají. Nachází se zde možnost pro společnost BankID, ačkoli je velmi složitá, zvýšit pro klienty, kteří si to žádají, úroveň jejího zabezpečení. Další doporučení směřuje přímo na jednotlivé banky, které bankovní identitu zprostředkovávají, a to aby více komunikovali se svými klienty, kteří ji zatím nikdy nevyužili. Na základě dotazníku došlo k nalezení nemalého počtu klientů, kteří neměli vůbec povědomí o bankovní identitě. To by se pomocí e-mailové nebo telefonické komunikace dalo zlepšit. Kromě výše zmíněných dvou doporučení nebyly zaznamenány žádné další výtky. Naopak převládá názor, že se bankovní identita bude dále rychlým tempem rozšiřovat, a to jak ve státní sféře, tak ve vybraných e-shopech, pojišťovnách, energetických společnostech a dalších sférách.

5.6 Možná rozšíření práce

Jak již bylo několikrát zmíněno, bankovní identita se v posledních letech velmi rozšířila, a to do několika segmentů. Uchopit tak téma a obsah diplomové práce lze z několika hledisek a pohledů. Práce byla tvořena tak, aby podala přehled o zavádění bankovní identity v ČR, kde a jak ji lze využít a jaké jsou její nejznámější alternativy. Zároveň byly představeny názory veřejnosti a týmu Portálu občana. Práce by mohla být dále rozšířena o více technický popis fungování bankovní identity nebo o názory dalších portálů a jejich spokojenosti s bankovní identitou. Problémem u podrobnějšího technického popisu je, že banky ani společnost BankID tyto informace příliš neposkytují.

6 Závěr

Hlavním cílem práce bylo provést analýzu zavádění bankovní identity v České republice. Tím je myšleno: představit jednotlivé banky, které bankovní identitu zprostředkovávají, popsat a interpretovat její aktuální stav u vybraných bank, analyzovat možnosti jejího využití a na základě analýzy vytvořit přehledný způsob, jak vysvětlit její chování v různých sférách. Pro větší orientaci v problematice měly být též představeny její alternativy a měl být proveden výzkum mínění veřejnosti o této oblasti. Zmíněné skutečnosti pak stojí na zpracovaném teoretickém základu, jenž předcházel samotné praktické části. Všechny získané závěry byly interpretovány v kapitole Výsledky a diskuse.

Teoretická část se zabývala popisem bankovní identity a souvisejících problematik. Úvodní kapitola představila pojetí bankovní identity jako takové a vysvětlila základní pojmy jako NIA nebo SONIA. Vysvětleny byly též její alternativy jako například: eOP, mojeID, Karta Starcos a Mobilní klíč eGovernmentu. V následující kapitole došlo k popsání e-governmentu. V souvislosti s tím byly mimo jiné definovány i pojmy jako Czech POINT, datové schránky a základní registry. Bankovní identita je prostředkem pro ověřování identity a s tím souvisí i pojem kryptografie. Tomu se též teoretická část věnovala. Jelikož se práce zabývala částečně i bezpečností bankovní identity, byla představena v rámci zmíněné kapitoly i hrozba phishingu. Příchod a rozšiřování nových moderních technologií, jako je bankovní identita, je obecně spojen s digitalizací, a to jak ve společnosti, ekonomice, tak v samotném bankovnictví. Právě touto problematikou se zabývaly poslední dvě kapitoly teoretické části. Nejprve došlo k objasnění pojmu digitalizace, bankovních produktů, technologií a budoucnosti plateb, jež představují jednu z nejzásadnějších činností bank. Další část popisovala otevřené bankovnictví a aktuální stav digitalizace českých bank. Poslední kapitola Digitalizace v ekonomice a společnosti objasnila ekonomické přínosy digitalizace, její rizika, obchodování na internetu a incidenty, jež jsou s ní spojeny.

Praktická část byla sestavena v několika krocích. Jednalo se o: představení aktuální situace bankovního trhu v České republice, průzkum a analýzu stavu bankovní identity ve vybraných bankách, analýzu možností využití bankovní identity ve státní a soukromé sféře, vysvětlení jejího principu využití a fungování prostřednictvím procesních diagramů, analýzu alternativ a výzkum mínění veřejnosti ve zmíněných oblastech.

V úvodu praktické části došlo k popisu současné situace v České republice. Z vybraných zdrojů byly představeny největší banky a došlo k uvedení informací o tom, které z bank

zprostředkovávají svým klientům ověření pomocí bankovní identity. Závěr kapitoly se zabýval společností BankID, která se úzce pojí s řešením bankovní identity v České republice.

Navazující problematikou praktické části bylo provedení analýzy stavu a připravenosti bankovní identity u tří největších bank v České republice. Jednalo se o Komerční banku, ČSOB a Českou spořitelnu. V rámci každé z nich došlo ke zmínění důležitých událostí, jež v průběhu zavádění bankovní identity nastaly. Jako jedno z možných kritérií, podle kterého lze definovat připravenost vybraných bank, byl uveden fakt, že za dobu fungování bankovní identity nebyla nalezena žádná větší veřejná komplikace. Jako důvod pak byla zmíněna skutečnost, že všechny banky musí získat od státu potřebnou akreditaci a musí splňovat tzv. Zákon o bankovní identitě, jehož základní principy byly též objasněny v rámci praktické části. Na základě praktických ukázek ověření u každé z bank se došlo závěru, že jejich řešení bankovní identity je téměř totožné, jelikož se podílejí na projektu Bankovní identita společně.

Se zaváděním bankovní identity se též pojí její možnosti využití v jednotlivých oblastech. Došlo tedy k popisu způsobů jejího využití v České republice prostřednictvím praktických ukázek jak ve státní, tak soukromé sféře. Analýza v soukromé sféře se zaměřila například na společnost Alza, kde ověření pomocí BankID lze použít pro kontrolu bonity u služby Třetinka. Další oblastí, kde lze bankovní identitu v soukromé sféře využít, jsou pojišťovny a investiční společnosti. Proto byla vybrána společnost Avant, jež se zaměřuje hlavně na rozvoj fondů a investičních příležitostí. Praktická ukázka se pak zabývala popisem využití bankovní identity pro registraci a vstup do portálu společnosti. Poslední praktická ukázka, jež úzce souvisí s aktuální energetickou krizí, byla provedena na webu Pražské plynárenské. Samotný způsob využití bankovní identity byl na jednotlivých stránkách téměř totožný, změny se projevovaly pouze u volby konkrétní banky pro ověření.

Pro analýzu možností využití bankovní identity ve státní sféře byly vybrány celkem 3 portály. Samotná analýza se pojí s pojmem NIA, jenž byl představen v teoretické části. Prvním byl Portál společnosti, kde došlo ke kontaktování jeho týmu a získání odpovědí v oblasti bankovní identity. Největším rozdílem oproti soukromé sféře bylo předávání ověřených osobních informací, jelikož se ve státní sféře k této činnosti využívá tzv. Identita občana, a to u všech portálů. Další volbou pro praktickou ukázku byl portál Moje daně, kde byla v rámci práce založena a popsána tzv. Daňová informační schránka, jež představuje tzv. „Online finanční úřad“. Jako poslední byl zmíněn klientský portál MPSV, jenž byl vybrán

z důvodu jeho aktuálnosti, protože sloužil v roce 2022 jako místo, kde si mohli rodiče zažádat v době krize o příspěvek na dítě v hodnotě 5 000 Kč.

Na základě informací a zkušeností z analýz v obou sférách došlo k vytvoření BPMN diagramů, které detailněji popisují proces ověření prostřednictvím bankovní identity. Jelikož jsou procesy od vybrání metody přes odsouhlasení předávaných údajů až po úspěšné ověření v soukromé a státní sféře v něčem odlišné, došlo k vytvoření a popisu celkem dvou diagramů. Ty dávají ucelený přehled, jak v aktuálním stavu bankovní identita funguje.

Dalším tématem bylo představení a popis využití alternativ bankovní identity. Důvodem je skutečnost, že alternativy byly přítomné ještě před jejím zavedením a mohou též ovlivňovat její řešení a míru využití. Pro tuto problematiku byly zvoleny dvě nejznámější alternativy mojeID a Mobilní klíč eGovernmentu. V rámci praktických ukázek došlo k registraci a založení obou alternativ a následně ke zkoušce jejich využití na různých portálech. Na základě získaných výsledků pak došlo ke stanovení rozdílů dané alternativy v porovnání s bankovní identitou.

Závěr praktické části se zabýval výzkumem mínění veřejnosti v oblasti bankovní identity a jejích alternativ. Získávání respondentů probíhalo od 17. července do 28. srpna 2022, přičemž celkově dotazník vyplnilo 460 respondentů. Ti byli dále roztříděni podle toho, zda měli, či neměli povědomí o tom, co je bankovní identita. Celkem 355 respondentů, kteří odpověděli kladně, tvořilo cílovou skupinu dotazníku. Ostatních 105 dotazovaných bylo přesměrováno rovnou na jeho konec. Otázky byly pokládány v souvislosti s osnovou praktické části. Ještě před roztříděním respondentů byly získány informace v oblasti aktivního využívání účtů u jednotlivých bank. Z hlediska využití bankovní identity byli respondenti rozděleni do dvou skupin, a to na využívající a nevyužívající. Podle skupin jim byly pokládány specifické dotazy. První skupinu představovalo 225 využívajících respondentů. Dotazy na tuto skupinu se týkaly zejména bank, s jejichž pomocí bankovní identitu využívají, jak často ji využívají, zda se podle nich jedná o praktičtější způsob ověřování v porovnání s klasickým (jméno, heslo nebo nutnost registrace), kde ji využívají nejčastěji, zda ji využívají ve státní sféře, případně na jakém portále a jaký je jejich postoj k jejím alternativám. Druhá skupina byla tvořena 130 nevyužívajícími respondenty. Jednotlivé otázky pak zkoumaly, zda používají některé z alternativ, případně které to jsou, proč se pomocí bankovní identity neověřují a jestli mají v plánu ji do budoucna začít využívat. Poslední část dotazníku se zaměřovala na obě skupiny a zkoumala oblasti budoucnosti a bezpečnosti bankovní identity.

7 Seznam použitých zdrojů

ALZA.CZ, 2022. Třetinka od Alzy bezkontaktně? Ano, díky BankID [online]. 1 [cit. 2022-08-27]. Dostupné z: https://www.alza.cz/tretinka-bankid

AVANTFUNDS.CZ, 2022. O společnosti [online]. 1 [cit. 2022-08-27]. Dostupné z: https://www.avantfunds.cz/cs/o-spolecnosti/

BANKID.CZ, 2022. Jak bankovní identitu získat [online]. 1 [cit. 2022-07-18]. Dostupné z: https://www.bankid.cz/

BANKID.CZ, 2022. Kde můžete bankovní identitu použít? [online]. 1 [cit. 2022-08-01]. Dostupné z: https://www.bankid.cz/budoucnost

BARTŮŇKOVÁ, Eva, 2020. České banky a digitalizace: Co nás v následujících letech čeká na poli online služeb? [online]. 1 [cit. 2021-10-23]. Dostupné z: https://www.dreport.cz/blog/ceske-banky-a-digitalizace-co-nas-v-nasledujicich-letech-ceka-na-poli-online-sluzeb/

BHARADWAJ, Lipi, 2018. Technology in Banking: 10 Innovations That Will Impact Future of Banking [online]. 1 [cit. 2021-07-15]. Dostupné z: https://www.wowso.me/blog/technology-in-banking#5

BIRCH, David G.W., 2020. Bezhotovostní budoucnost je hotová věc. Jak zajistit, aby byla spravedlivá pro všechny? [online]. 1 [cit. 2021-10-17]. Dostupné z: https://forbes.cz/bezhotovostni-budoucnost-je-hotova-vec-jak-zajistit-aby-byla-spravedliva-pro-vsechny/

BOUŠKA, Petr, 2014. Kerberos protokol a Single sign-on [online]. 1 [cit. 2021-10-12]. Dostupné z: https://www.samuraj-cz.com/clanek/kerberos-protokol-a-single-sign-on/

BRADY, Scott, 2015. What is OpenID Connect? [online]. 1 [cit. 2021-10-13]. Dostupné z: https://www.scottbrady91.com/openid-connect/openid-connect-overview

BURDA, Karel, 2019. Kryptografie okolo nás. Praha: CZ.NIC, z.s. p.o. CZ.NIC. ISBN 978-80-88168-49-2.

BUREŠ, Michal, 2021. Bankovní identita vám pomůže vyřídit věci z banky i úřadů z tepla domova [online]. 1 [cit. 2021-09-16]. Dostupné z: https://www.finance.cz/537529-bankovni-identita-vyhody/

BUSINESSINFO.CZ, 2020. Základní registry veřejné správy [online]. 4 [cit. 2021-10-01]. Dostupné z: https://www.businessinfo.cz/navody/zakladni-registry-verejne-spravy-ppbi/#h-d-vody-vzniku-a-obecn-charakteristika-z-kladn-ch-registr

BUSINESSINFO.CZ, 2021. Bankovní identita – jednoduchý způsob přihlašování k online službám státu i komerčních subjektů [online]. 4 [cit. 2021-09-07]. Dostupné z: https://www.businessinfo.cz/navody/bankovni-identita-ppbi

ČESKÁ BANKOVNÍ ASOCIACE, 2019. Projekt SONIA prošel druhým čtením [online]. 1 [cit. 2021-09-11]. Dostupné z: https://cbaonline.cz/projekt-sonia-prosel-druhym-ctenim

ČESKÁ BANKOVNÍ ASOCIACE, 2021. Jeden z největších digitalizačních projektů českého bankovního sektoru [online]. 1 [cit. 2021-09-14]. Dostupné z: https://bankovni-identita.cz/o-projektu/

ČESKÁ SPOŘITELNA, A.S., 2021. Klienti Spořitelny mohou nově využít Bankovní identitu pro online sjednání produktů u ČEZu a Generali České pojišťovny. Celkem mohou BankID použít již u 35 firem [online]. 1 [cit. 2022-11-06]. Dostupné z: https://www.csas.cz/cs/o-nas/pro-media/tiskove-zpravy/2021/09/29/klienti-sporitelny-mohou-nove-vyuzit-bankovni-identitu-pro-online-sjednani-produktu-u-cezu-a-generali-ceske-pojistovny#

ČESKÁ SPOŘITELNA, A.S., 2021. Spořitelna jako první banka na trhu spouští digitální podpis dokumentů pomocí BankID SIGN [online]. 1 [cit. 2022-11-06]. Dostupné z: https://www.csas.cz/cs/o-nas/pro-media/tiskove-zpravy/2021/10/12/sporitelna-jako-prvni-banka-na-trhu-spousti-digitalni-podpis-dokumentu-pomoci-bankid-sign#

ČESKÁ SPOŘITELNA, A.S., 2022. Jak mohu zkontrolovat, jestli někdo nepoužívá moji Bankovní IDentitu? [online]. 1 [cit. 2022-11-06]. Dostupné z: https://www.csas.cz/cs/caste-dotazy/Jak-mohu-zkontrolovat-jestli-nekdo-nepouziva-moji-bankovni-identitu

ČSOB, 2020. ČSOB má jako první akreditaci pro bankovní identitu, klientům se otevírají i služby státu [online]. 1 [cit. 2022-11-06]. Dostupné z: https://www.csob.cz/portal/-/tz201026b

ČSOB, 2021. ČSOB spouští přihlašování přes bankovní identitu i ke službám soukromých poskytovatelů [online]. 1 [cit. 2022-11-06]. Dostupné z: 1. června 2021

ČSOB, 2021. S bankovní identitou od ČSOB je možné digitálně podepsat dokumenty. A s bankovní identitou jiné banky taky jednoduše založit nový účet u ČSOB [online]. 1 [cit. 2022-11-06]. Dostupné z: https://www.csob.cz/portal/-/tz211206

DUOFINANCE, 2021. Co je to bankovní identita, a jaké výhody a nevýhody jsou s jejím užíváním spojené? [online]. 1 [cit. 2021-10-14]. Dostupné z: https://www.statnisprava.cz/rstsp/clanky.nsf/i/co_je_to_bankovni_identita_a_jake_vyhody_a_nevyhody_jsou_s_jejim_uzivanim_spojene__21062909_05284199

EZDRAV.CZ, 2019. EGovernment – co to je a jak u nás funguje [online]. [cit. 2021-07-12]. Dostupné z: http://ezdrav.cz/egovernment-co-to-je-a-jak-u-nas-funguje/

FELIX, Ondřej, Jiří KAUCKÝ, Jindřich KOLÁŘ et al., 2015. Jak se (z)rodil eGON: reforma a elektronizace veřejné správy. Praha: CEVRO Institut. ISBN978-80-87125-28-1.

FINANČNÍ SPRÁVA ČR, 2022. Příručka uživatele Online finančního úřadu [online]. 28 [cit. 2022-08-27]. Dostupné z: https://adisspr.mfcr.cz/dpr/adis/idpr_pub/dpr_info/prirucka_uzivatele_dis_plus.pdf

GENERÁLNÍ FINANČNÍ ŘEDITELSTVÍ, 2020. Online finanční úřad [online]. 1 [cit. 2022-08-27]. Dostupné z: https://adisspr.mfcr.cz/pmd/home

GRIMES, Roger a Josh FRUHLINGER, 2019. What is OAuth? How the open authorization framework works [online]. 1 [cit. 2021-10-12]. Dostupné z: https://www.csoonline.com/article/3216404/what-is-oauth-how-the-open-authorization-framework-works.html

HASSELL, Jonathan, 2003. Radius. Vyd. 1. New York: O´Reilly, 190 s. ISBN 0-596-00322-6.

HEX, 2021. Co je bankovní identita, jak funguje a které banky ji podporují? [online]. 1 [cit. 2021-09-06]. Dostupné z: https://www.skutecnost.cz/rubriky/finance/co-je-bankovni-identita-jak-funguje-a-ktere-banky-ji-podporuji_852.html

IANNACCONE, Marco, 2021. Bankovní digitalizace v Česku nabírá nový vítr. Extrémně zrychlujeme, zní z UniCredit Bank. Forbes [online]. 1 [cit. 2021-10-23]. Dostupné z: https://forbes.cz/bankovni-digitalizace-v-cesku-nabira-novy-vitr-extremne-zrychlujeme-zni-z-unicredit-bank/

IRSHIVANGINI, 2020. Authentication vs. Authorization Defined: What's the Difference? [online]. 1 [cit. 2021-10-08]. Dostupné z: https://securityboulevard.com/2020/06/authentication-vs-authorization-defined-whats-the-difference-infographic/

JOGANI, Anil, 2019. Business digitalization risk & change management [online]. 1 [cit. 2021-10-25]. Dostupné z: https://www.wegalvanize.com/risk/business-digitalization-risk/

KANTNEROVÁ, Liběna, 2016. Základy bankovnictví: teorie a praxe. V Praze: C.H. Beck. Beckovy ekonomické učebnice. ISBN 978-80-7400-595-4.

KELLY, Andrew, 2021. Finance Explainer: What is open banking? [online]. 1 [cit. 2021-10-22]. Dostupné z: https://www.reuters.com/business/finance/what-is-open-banking-2021-07-09/

KOMERČNÍ BANKA, 2021. Komerční banka spustila pilotní provoz Bankovní identity [online]. 1 [cit. 2022-11-06]. Dostupné z: https://www.kb.cz/cs/o-bance/pro-media/tiskove-zpravy-2021/komercni-banka-spustila-pilotni-provoz-bankovni-id

KOMERČNÍ BANKA, 2021. Komerční banka naplno spustila Bankovní identitu, využít ji lze pro daňové přiznání i Sčítání lidu [online]. 1 [cit. 2022-11-06]. Dostupné z: https://www.kb.cz/cs/o-bance/pro-media/tiskove-zpravy-2021/komercni-banka-naplno-spustila-bankovni-identitu

KOMERČNÍ BANKA, 2022. Bankovní identita KB pro firmy [online]. 1 [cit. 2022-11-06]. Dostupné z: https://www.kb.cz/cs/podpora/bankovnictvi-a-nastroje/bankovni-identita-kb-pro-firmy

KORBEL, František a Dalibor KOVÁŘ, 2021. Právní úprava tzv. bankovní identity [online]. 1 [cit. 2022-11-06]. Dostupné z: https://advokatnidenik.cz/2021/05/09/pravni-uprava-tzv-bankovni-identity-2/

KOUTNÝ, Petr, 2019. Banky se digitalizují. Jaké novinky připravují do roku 2019 [online]. 1 [cit. 2021-10-22]. Dostupné z: https://www.bankovnipoplatky.cz/banky-se-digitalizuji-jake-novinky-pripravuji-do-roku-2019-37535

KUČERA, Petr, 2021. Služba mojeID nabídne i nejvyšší stupeň ověření [online]. 1 [cit. 2021-09-19]. Dostupné z: https://www.penize.cz/spotrebitel/425018-sluzba-mojeid-nabidne-i-nejvyssi-stupen-overeni

KUMAR, Puneet, Vinod Kumar JAIN a Kumar Sambhav PAREEK, 2018. The Stances of e-Government: Policies, Processes and Technologies. 1st Edition. Boca Raton: CRC Press. ISBN 978-1-138-30490-1.

LANGEROVÁ, Jana, 2021. COVID-19: Digitalizace přispěje k oživení ekonomiky [online]. 1 [cit. 2021-10-23]. Dostupné z: https://www.cfoworld.cz/clanky/covid-19-digitalizace-prispeje-k-oziveni-ekonomiky/

LUTKEVICH, Ben, 2020. Access control [online]. 1 [cit. 2021-07-13]. Dostupné z: https://searchsecurity.techtarget.com/definition/access-control

MAŠEK, Adam, 2021. Pojištění i nákup solárů on-line. Startuje bankovní identita pro firmy, využije ji třeba Pražská plynárenská [online]. 1 [cit. 2022-08-27]. Dostupné z: https://archiv.hn.cz/c1-66929170-pojisteni-i-nakup-solaru-on-line-startuje-bankovni-identita-pro-firmy-vyuzije-ji-treba-prazska-plynarenska

MAŠÍNOVÁ, Sára, 2019. Czech POINT, co to je a jak to funguje? [online]. 1 [cit. 2021-09-27]. Dostupné z: https://saramasinova.blog.idnes.cz/blog.aspx?c=713574

MEDIAGURU, 2021. Šest hlavních trendů v retailu v roce 2021 [online]. 1 [cit. 2021-10-25]. Dostupné z: https://www.mediaguru.cz/clanky/2020/12/sest-hlavnich-trendu-v-retailu-v-roce-2021/

MEHL, Bernhard, 2018. Authentication Protocols: LDAP vs Kerberos vs OAuth2 vs SAML vs RADIUS [online]. 1 [cit. 2021-10-10]. Dostupné z: https://www.getkisi.com/blog/authentication-protocols-overview

MERTOVÁ, Jana, 2021. Konec běhání po úřadech a pobočkách. Bankovní identita nahradí v online světě občanky. Forbes [online]. 1 [cit. 2021-09-02]. Dostupné z: https://forbes.cz/konec-behani-po-uradech-a-pobockach-bankovni-identita-nahradi-v-online-svete-obcanky/

MINISTERSTVO PRÁCE A SOCIÁLNÍCH VĚCÍ, 2022. Klientský portál pro žádost o příspěvek na dítě běží bez omezení [online]. 1 [cit. 2022-08-27]. Dostupné z: https://www.mpsv.cz/documents/20142/2786931/TZ_%C5%BE%C3%A1dosti_Jenda_15082022.pdf/e2f8f9a1-cdfe-337a-d9d4-b6b1d3caeb5a

MINISTERSTVO VNITRA, 2022. Portál občana [online]. 1 [cit. 2022-08-27]. Dostupné z: https://portal.gov.cz/caste-dotazy/portal-obcana

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, 2020. Nové možnosti elektronické identifikace [online]. 1 [cit. 2021-09-20]. Dostupné z: https://www.datoveschranky.info/-/nove-moznosti-elektronicke-identifikace?inheritRedirect=true

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, 2020. Akreditace pro Českou spořitelnu. Dalších 1,7 mil. klientů bude moci využívat služby veřejné správy přes internetové bankovnictví [online]. 1 [cit. 2022-11-06]. Dostupné z: https://www.mvcr.cz/clanek/akreditace-pro-ceskou-sporitelnu-dalsich-1-7-mil-klientu-bude-moci-vyuzivat-sluzby-verejne-spravy-pres-internetove-bankovnictvi.aspx

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, 2021. Portál občana [online]. 1 [cit. 2021-09-26]. Dostupné z: https://www.mvcr.cz/clanek/portal-obcana.aspx?q=Y2hudW09Mg%3D%3D

MONIOVÁ, Eva, 2019. Doba poplatková. Na čem vydělávají české banky [online]. 1 [cit. 2021-10-22]. Dostupné z: https://www.seznamzpravy.cz/clanek/odmitame-euro-banky-nam-za-to-mohou-dekovat-83129

PETERKA, Jiří, 2020. EObčanky ztratily monopol na přihlašování ke službám eGovernmentu. Jak funguje karta Starcos? [online]. 1 [cit. 2021-09-20]. Dostupné z: https://www.lupa.cz/clanky/eobcanky-ztratily-monopol-na-prihlasovani-ke-sluzbam-egovernmentu-jak-funguje-karta-starcos/

PETERKA, Jiří, 2021. Bankovní identita startuje. Potrvá jí to nejspíše celý leden [online]. 1 [cit. 2021-09-09]. Dostupné z: https://www.lupa.cz/clanky/bankovni-identita-startuje-potrva-ji-to-nejspise-cely-leden/

PETERKA, Jiří, 2021. Bankovní identita: 1,6 milionu aktivovaných identit, (snad) jen jedna SONIA a první ceník jejích služeb [online]. 1 [cit. 2021-09-14]. Dostupné z: https://www.lupa.cz/clanky/bankovni-identita-1-6-milionu-aktivovanych-identit-snad-jen-jedna-sonia-a-prvni-cenik-jejich-sluzeb/

PETERKA, Jiří, 2021. MojeID už funguje i s úrovní záruky „vysoká“. K čemu je dobrá a jak ji aktivovat? [online]. 1 [cit. 2022-11-06]. Dostupné z: https://www.lupa.cz/clanky/mojeid-uz-funguje-i-s-urovni-zaruky-vysoka-k-cemu-je-dobra-a-jak-ji-aktivovat/

PETERSEN, Thieß, 2019. Digital Economy: How is digitalization changing global competitiveness and economic prosperity? [online]. 1 [cit. 2021-10-25]. Dostupné z: https://ged-project.de/digitization-and-innovation/digital-economy-how-is-digitalization-changing-global-competitiveness-and-economic-prosperity/

POLOUČEK, Stanislav, 2013. Bankovnictví. 2. vyd. V Praze: C.H. Beck. Beckovy ekonomické učebnice. ISBN978-80-7400-491-9.

PORTÁLDIGI | DIGISTRATEGIE, 2020. Digitalizace [online]. 1 [cit. 2021-07-14]. Dostupné z: https://portaldigi.cz/digislovnik/digitalizace/

RADA, Michal, 2021. Co zásadního čeká veřejnou správu v eGovernmentu? [online]. 1 [cit. 2021-10-04]. Dostupné z: http://www.openczeg.cz/clanky/2021/03/15/co-nas-ceka.html

SAHU, Saurabha, 2020. Redefining Banking With Augmented Reality and Virtual Reality [online]. 1 [cit. 2021-10-15]. Dostupné z: https://www.finextra.com/blogposting/19257/redefining-banking-with-augmented-reality-and-virtual-reality

SANG, Ashlee, 2021. How Do Banks Make Money? [online]. 1 [cit. 2021-10-22]. Dostupné z: https://www.clevergirlfinance.com/blog/how-do-banks-make-money/

SEZNAM.CZ, 2022. Ověření účtu bankovní identitou [online]. 1 [cit. 2022-08-27]. Dostupné z: https://napoveda.seznam.cz/cz/bankid-overeni/

SKALKOVÁ, Olga, 2022. Největší banky v Česku. Nové žebříčky podle klientů a peněz [online]. 1 [cit. 2022-07-16]. Dostupné z: https://www.penize.cz/osobni-ucty/432939-nejvetsi-banky-v-cesku-zebricek-podle-poctu-klientu-a-spravovanych-penez

SLÍŽEK, David, 2021. Základní registry fungují na hranici kapacity, mohou přijít výpadky či kolaps, varuje vnitro [online]. 1 [cit. 2021-10-04]. Dostupné z: https://www.lupa.cz/aktuality/zakladni-registry-funguji-na-hranici-kapacity-mohou-prijit-vypadky-ci-kolaps-varuje-vnitro/

SOLITEA A.S., 2020. Datová schránka. K čemu slouží, jak ji založit a na co si dát pozor [online]. 1 [cit. 2021-09-30]. Dostupné z: https://money.cz/novinky-a-tipy/podnikani/datova-schranka-k-cemu-slouzi-zalozit-si-dat-pozor/

SPRÁVA ZÁKLADNÍCH REGISTRŮ, 2020. NIA ID (Jméno, heslo a SMS kód) [online]. 1 [cit. 2021-09-06]. Dostupné z: https://info.eidentita.cz/ups/

SPRÁVA ZÁKLADNÍCH REGISTRŮ, 2020. EObčanka [online]. 1 [cit. 2021-09-19]. Dostupné z: https://info.eidentita.cz/eop/

SULLIVAN, Tom, 2018. Authentication vs. authorization: Differences and methods [online]. 1 [cit. 2021-10-08]. Dostupné z: https://plaid.com/resources/banking/authentication-vs-authorization/

TAAFFE, Ouida, 2019. Banking on Change: The Development and Future of Financial Services. 1. West Sussex, England: Wiley, 248 s. ISBN 978-1-119-60998-8.

ÚSTAV ZDRAVOTNICKÝCH INFORMACÍ A STATISTIKY ČR, 2022. Očkovací portál občana [online]. 1 [cit. 2022-08-27]. Dostupné z: https://www.nzip.cz/doporuceny-zdroj/299-ockovaci-portal-obcana

VANÍČEK, Zdeněk a Stanislav A. MARCHAL, 2011. Právní aspekty eGovernmentu v ČR. Praha: Linde. ISBN978-80-7201-855-0.

VEBER, Jaromír, 2018. Digitalizace ekonomiky a společnosti: výhody, rizika, příležitosti. Praha: Management Press. ISBN 978-807-2615-544.

VODIČKA, Milan, 2014. 3D: Data, daně digitálně, aneb, Ajťákem i proti své vůli. Praha: Wolters Kluwer. ISBN978-80-7478-671-6.

VODIČKA, Milan, 2021. Jaká jsou rizika digitalizace? [online]. 1 [cit. 2021-10-25]. Dostupné z: https://solitea.com/cs-cz/rizika-digitalizace

VOKŘÁL, Jiří, 2021. Přehledně: Jak založit datovou schránku a na co si dát pozor [online]. 1 [cit. 2021-09-30]. Dostupné z: https://www.seznamzpravy.cz/clanek/zrizeni-datove-schranky-147602

VOKŘÁL, Jiří, 2021. Základ, bez kterého se člověk už neobejde. Běžný účet [online]. 1 [cit. 2021-10-23]. Dostupné z: https://www.seznamzpravy.cz/clanek/bezne-ucty-155479

WICKES, Peter, 2021. The Future of Payments [online]. 1 [cit. 2021-10-17]. Dostupné z: https://www.finextra.com/the-long-read/129/the-future-of-payments

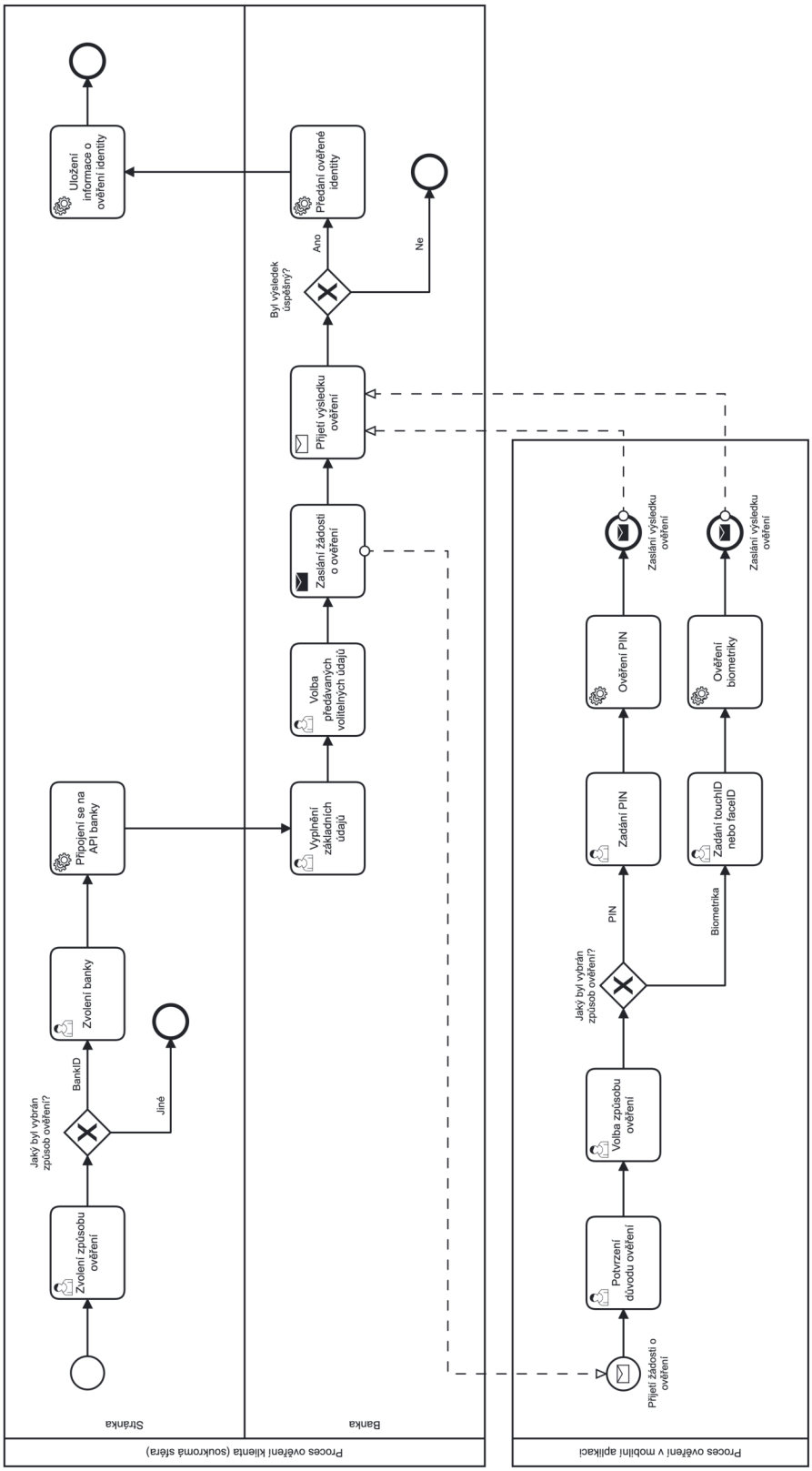
ZMEŠKAL, Kamil, 2021. Bankovní identita je dobrý sluha. Existují ale i důvody, proč ji nechtít [online]. 1 [cit. 2021-09-19]. Dostupné z: https://www.lupa.cz/clanky/bankovni-identita-je-dobry-sluha-existuji-ale-i-duvody-proc-ji-nechtit/

Seznam obrázků

Obrázek 1: Největší banky v ČR 47
Obrázek 2: Přihlášení do KB 50
Obrázek 3: Potvrzení v aplikaci KB klíč 50
Obrázek 4: Přihlášení do ČSOB 52
Obrázek 5:Potvrzení v aplikaci Smart klíč 52
Obrázek 6: Aplikace Správa třetích stran 54
Obrázek 7: Využití BankID na stránce Alza.cz 57
Obrázek 8: Využití BankID u společnosti Avant 58
Obrázek 9: Nastavení volitelných údajů při ověřování 59
Obrázek 10: Registrace na zákaznickém portálu Pražské plynárenské 60
Obrázek 11: Volba ověření identity na Portálu občana 63
Obrázek 12: Udělení souhlasu pro výdej údajů na Portálu občana 63
Obrázek 13: Využití Daňové informační schránky 65
Obrázek 14: Aplikace Jenda 66
Obrázek 15: BPMN diagram procesu ověření v soukromé sféře 68
Obrázek 16: BPMN diagram procesu ověření ve státní sféře 69
Obrázek 17: Možnost nastavení obrázkového hesla 72
Obrázek 18: Graf – věkové kategorie respondentů 74
Obrázek 19: Graf – nejvíce využívané banky 75
Obrázek 20: Graf – povědomí o bankovní identitě 76
Obrázek 21: Graf – banky, u kterých je bankovní identita nejvíce využívána 77
Obrázek 22: Graf – jak často respondenti využívají bankovní identitu 78
Obrázek 23: Graf – nejvíce využívané oblasti z hlediska bankovní identity 79
Obrázek 24: Graf – v jaké oblasti státní správy se bankovní identita využívá nejvíce 80
Obrázek 25: Graf – nejvíce využívané alternativy 81
Obrázek 26: Graf – důvody nevyužívání bankovní identity 84
Obrázek 27: Graf – názor na možné budoucí využití bankovní identity 85
Obrázek 28: Graf – bezpečnostní hrozby bankovní identity 86

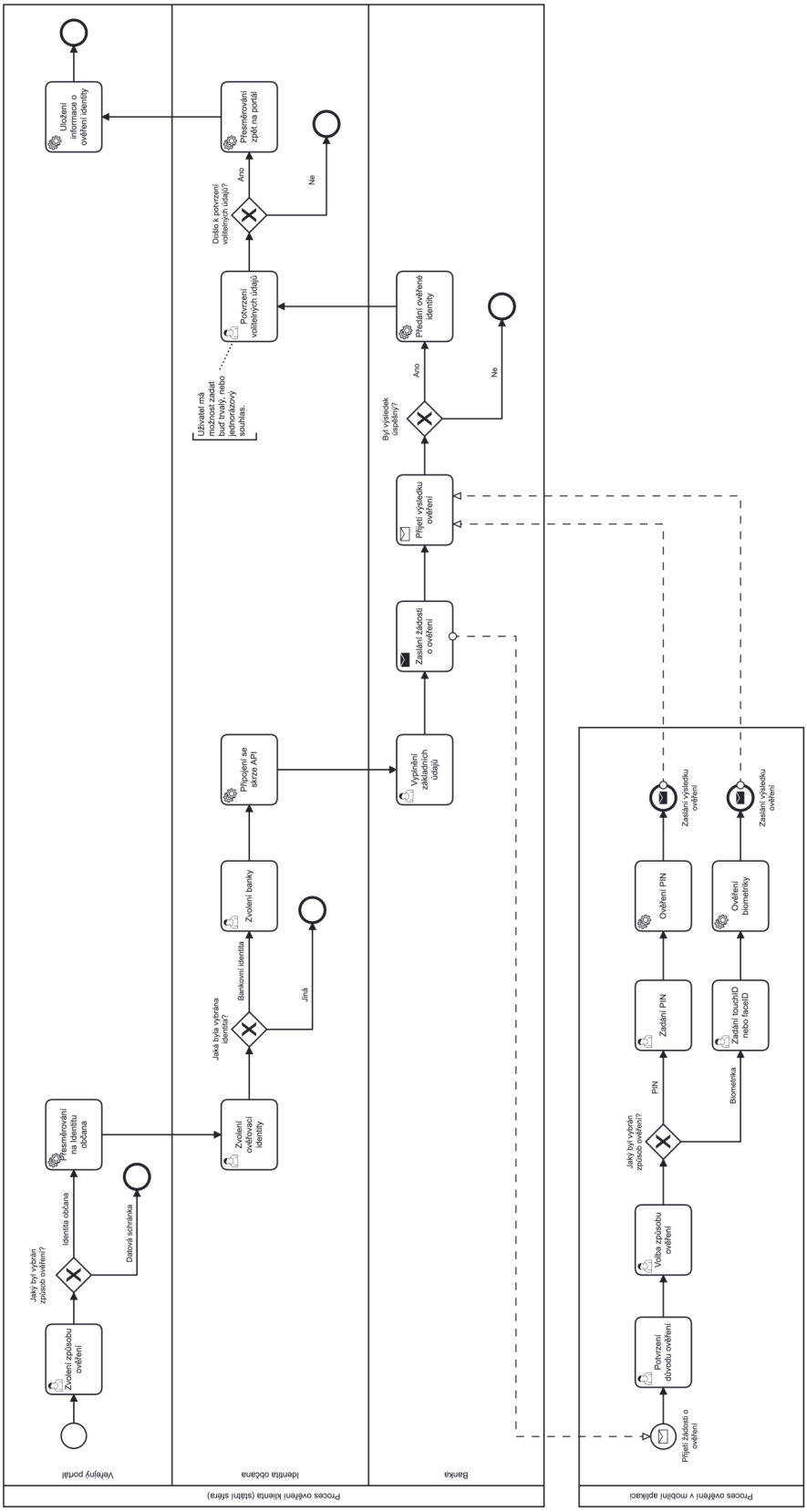
Přílohy

Příloha A BPMN diagram – soukromá sféra



Zdroj: Vlastní (2022)

Příloha B BPMN diagram – státní sféra



Zdroj: Vlastní (2022)