Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Převzetí identifikace v prostředí PSD2

Diplomová práce

Autor: Bc. Kateřina Kvapilová

Studijní obor: IM2

Vedoucí práce: Ing. Pavel Čech, Ph.D.

Hradec Králové listopad 2017

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracovala samostatně a s použitím uvedené literatury.

V Hradci Králové dne 29. 4. 2018 Kateřina Kvapilová

Anotace

Evropský bankovní trh čelí jedné z největších změn za posledních 20 let. Ještě do nedávné doby výhradně banky vlastnily data o svých klientech a jejich finančních pohybech, byla to jedna z největších konkurenčních výhod na trhu platebních služeb. To se ale mění od 13. 1. 2018, kdy vstoupila v účinnost nová směrnice o platebních službách, známá pod zkratkou PSD2, která má za cíl otevření bankovních dat směrem ke třetím stranám. Banky tak mohou ztratit svůj primární vztah s klientem, tím svou největší konkurenční výhodu. Jednou z možností, jak mohou reagovat, je udržet s inovacemi krok, a nabídnout ještě lepší klientský služby. Diplomová práce se snaží najít jednu takovou příležitost, jak díky PSD2 poskytnout kvalitnější klientský zážitek, a to zjednodušit a zrychlit proces online identifikace klienta jiné banky, aniž by musel navštívit pobočku nebo pobočka navštívila jeho.

Annotation

Title: Non client identification in PSD2 environment

The European banking is facing one of the biggest change over the last 20 years. Until recently, only banks had data about their clients and their financial movements, it was one of the biggest competitive advantage in the payment services market. However, it has changed since 13 January 2018, when the new Payment Services Directive, known as the PSD2, aimed at opening banking data to third parties, entered into force. Thus, banks can lose their primary relationship with the client and thus their biggest competitive advantage. One way how banks can react is to keep pace with innovation and offer even better client services. The diploma thesis seeks to find one such opportunity for PSD2 to provide a better client experience by simplifying and speeding up the process of online identification of the client of another bank without having to visit a branch or a branch to visit him.

Poděkování

Chtěla bych poděkovat Ing. Pavlovi Čechovi, Ph.D., vedoucímu mé diplomové práce, za vedení, zájem, připomínky a čas, který mi věnoval.

Obsah

1 Úvod

„Know Your Customer“, termín, který popisuje proces ověření identity uživatele. Nejvíce je tento termín ale skloňovaný v souvislosti s finančními institucemi a praním špinavých peněz. Banky v tomto období prochází velkou digitální transformací, pobočka se stává pouze jedním z kanálů a je rovnocenným soupeřem digitálního bankovnictví. Svého klienta dnes umí finanční instituce E2E obsloužit od personalizované nabídky po modelaci finančního produktu, podpis smlouvy a distribuci. Klíčovým slovem je zde spojení „svého klienta“. Banka totiž nejdříve musí fyzicky ověřit identitu potenciálního klienta, kde slovo fyzicky znamená poslat za klientem kurýra, ale u většiny klientů návštěvu obchodního místa. Dokonce banky musí fyzicky ověřit identitu klienta, který je již klientem jiné banky, byl již tedy jednou fyzicky ověřen.

Pokud se má stát digitální svět bance rovnocenným partnerem pro distribuci jejích produktů, musí umět online identifikovat a ověřit identitu svého potenciálního klienta, ne pouze klienta stávajícího. Český zákon tomu ale nevychází vstříc. Společně s Polskem jsme jediná země z našich sousedů, která si vyložila a transponovala evropský zákon proti praní špinavých peněz tak, že nový klient musí být vždy fyzicky ověřen. Ostatním zemím vypadl termín „fyzicky“, a tedy umí dnes nového klienta ověřit například přes videochat, jako banka N26.

Dnes evropský bankovní trh čelí s příchodem nové směrnice o platebních službách nové výzvě.

Posledních 50 let bylo pro evropské banky obdobím velkých změn, nejdříve nástup telefonního bankovnictví v 80. letech, internetového bankovnictví v 90. letech a dnes rozvoj finančních technologií tzv. fintech. Je zajímavé, že ač řada prognóz vždy předvídala konec bankovnictví tak, jak ho známe dnes, tedy udržování sítě poboček, tento tradiční model zůstal beze změny.

PSD2 směrnice reguluje evropské banky a poskytovatele platebních služeb. Reflektuje aktuální rozvoj informačních a komunikačních služeb a má za cíl zajistit silnější ochranu spotřebitele, posílit konkurenční prostředí, zjednodušit a podpořit zavádění inovací v sektoru finančních služeb a standardizovat pravidla na unijní úrovni.

Největší změnou PSD2 je právě otevřené sdílení bankovních dat, které tak urychlí vznik nových produktů a služeb, jaké jsme si v nedávné době ani nedokázali představit. Dodnes právě banky vlastnily vztah s klientem, tedy především klientská data.

Vlastnictví těchto dat dlouhodobě poskytovalo bankám významnou konkurenční výhodu. To se nyní mění, neboť ve stále větší míře bude docházet ke sdílení dat se třetími stranami. A to není všechno – tato data bude potenciálně možné využít i k poskytování inovativních bankovních služeb s další přidanou hodnotou.

Data budou poskytovat prostřednictvím tzv. API, speciální komunikační rozhraní pro programování aplikací, kde banky otevírají trh novým hráčům prostřednictvím právě dvou zcela nových služeb

- služba nepřímého udělení platebního příkazu,
- služba informování o platebním účtu.

Třetí strana tak nově umožní přes uživatelské rozhraní své aplikace iniciovat online platbu, aniž by se uživatel musel přihlašovat do svého online bankovnictví, anebo použít platební kartu. Umožní také třetí straně poskytnout klientovi přehled bankovních účtů vedených u různých bank, a mnohé další informace o účtech klienta.

Právě bankovnictví bylo hlavním komunikačním kanálem banky, tím, že nově uživatel bude moci zadávat platbu ze své banky i přes jiné hráče na trhu, ztrácí banka tuto strategickou výhodu. Banky ale mohou být proaktivní, rozeznat příležitost i pro sebe a upevnit své místo na bankovním i fintechovém trhu. Banka má totiž oproti třetím stranám stále jednu velkou výhodu, a to je důvěryhodnost, již existující vztah ke klientovi a schopnost operativně nabízet komplexní finanční produkty.

2 Cíl práce

Cílem diplomové práce je návrh řešení s oporou v legislativě, jak zjednodušit a zrychlit dnešní proces online identifikace nového klienta banky, který byl jednou fyzicky ověřen jinou finanční institucí.

Proces identifikace bude zasazen do kontextu online zřízení platebního účtu. Zřízení účtu je jedna z nejčastějších každodenních operativ v retailové bance. Jen v České spořitelně se za měsíc zřídí cca 16 000 platebních účtů, z toho na online svět především kvůli složitosti procesu spadají pouze jednotky kusů, zbytek zbývá na pobočkovou síť.

Návrh možného řešení pro zjednodušení a zrychlení procesu bude vycházet z modelace aktuálního stavu a identifikace slabých míst a překážek procesu online identifikace.

Možná řešení budou vycházet z obsahové analýzy:

1. Zákona 253/2008 Sb. stanovující pravidla pro dnes používaný model první identifikace a ověření totožnosti, viz kapitola 3.4, a na základě kterého identifikujeme slabá místa celého procesu identifikace, viz kapitola 3.5;
2. Směrnice Evropského parlamentu a Rady EU o platebních službách tzv. PSD2 a její transpozice do českého právního řádu Zákonem 370/2017 o platebním styku, kde se budeme snažit najít oporu v zákoně, jak mitigovat nedostatky dnes existujícího procesu online první identifikace vycházejícího ze zákona 253/2008 Sb., viz kapitola 4.2;
3. Technického standardu pro silnou autentizaci a bezpečnou komunikaci, popisující, jak využít služby PSD2 z pohledu bezpečnosti, viz kapitola 4.4;
4. Českého standardu pro Open Banking, kde se již podíváme na praktické využití služeb vycházejících z PSD2 v českém bankovním sektoru, viz kapitola 5.3.

Konkrétní návrh zjednodušení a zrychlení celého procesu online identifikace opírající se o zjištění z obsahové analýzy výše bude shrnut v kapitole 6.

3 Převzetí identifikace

3.1 Identifikace klienta dnes

"*Do roku 2020 bude 95 procent všech interakcí mezi klientem a bankou probíhat digitálně a banky v Evropě zruší 40 procent svých poboček. Proměna je iniciována samotnými zákazníky, kteří ji už teď vyžadují.*", říká zpráva mezinárodní konzultační společnosti Bain & Company. [1]

Je ale zavádějící, že dnes v době nezpomalující se digitalizace, první taková interakce banky s klientem probíhá ve většině případů právě na pobočce. Proč? Příčinou je především evropská směrnice snažící se zamezit legalizaci výnosů z trestné činnosti, ale především také transpozice směrnice do českého práva ve formě zákona 253/2008 Sb., který je ještě striktnější a přísnější než transpozice stejného nařízení do vnitřního práva v Německu, Rakousku nebo třeba na Slovensku.

Ověření totožnosti klienta musí finanční či úvěrová instituce provést vždy, identifikuje-li nového klienta za účelem uskutečnění obchodního vztahu. Ve většině případů dle vlastní zkušenosti dochází k této první identifikaci na kamenných pobočkách cílové instituce, kde ověření totožnosti je plně metodicky v rukou pracovníka dané pobočky.

3.2 Regulatorní požadavky na online převzetí identifikace klienta

Pro první identifikaci klienta se musí finanční a úvěrové instituce v České republice řídit právními předpisy, které tuto činnost regulují, především ve snaze rozkrýt výnosy z trestné činnosti tzv. Anti-money laundering (AML).

3.2.1 AML

Legalizace výnosů v podstatě znamená zahlazení stop po trestné činnosti a znemožnění dohledání zdrojů finančních prostředků. Nejčastěji formou přesunů peněz mezi účty, či změnou formy těchto prostředků.

Boj proti praní špinavých peněz se celosvětově skrývá pod pojmem AML/ CFT neboli Anti-money landering/ Combating teh financing of terrorism – snaha o rozkrytí, nahlášení a vyšetřování činu praní špinavých peněz a financování terorismu.

Proces praní špinavých peněz má většinou 3 fáze:

- ✓ umístění prostředků
- ✓ zakrytí původu prostředků
- ✓ převedení prostředků zpět k jeho původnímu majiteli

A právě finanční a úvěrové instituce mohou v tomto procesu hrát nevědomky roli zprostředkovatele. AML/ CTF má tedy celosvětově za cíl:

- ✓ zabránění zneužití finančního systému pro legalizaci výnosů z trestné činnosti a financování terorismu
- ✓ uchování stop po přesunech prostředků, včetně záznamů od koho, prostřednictvím koho a kam putují

V návaznosti na mezinárodní závazky vycházející především ze členství v Evropské unii je problematika výnosů z trestné činnosti a financování terorismu upravena i v České republice. Pro potřeby této práce se zaměříme na Zákon 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, který upravuje podmínky pro proces první identifikace klienta.

3.2.2 Zákon 253/2008 Sb.

Prevenci a opatření proti legalizaci výnosů z trestné činnosti a financování terorismu reguluje v České republice Zákon 253/2008 Sb. Zákon vymezuje tzv. povinné osoby a povinnosti při realizaci opatření pro praní špinavých peněz a financování terorismu, pod které zejména pro potřeby této práce patří např.:

- ✓ povinnost identifikace;
- ✓ provádění identifikace;
- ✓ kontrola klienta;
- ✓ zprostředkovaná identifikace;
- ✓ převzetí identifikace;
- ✓ zjednodušená identifikace a kontrola klienta;
- ✓ výjimky z povinnosti identifikace a kontroly klienta;
- ✓ neuskutečnění obchodu. [2]

Pro potřeby této práce dále rozebereme, jaké jsou povinnosti identifikace, jejího provádění a možnosti jejího převzetí.

3.2.2.1 Povinnost identifikace

Finanční i úvěrové instituce jsou povinny provést identifikaci v případě:

- ✓ hodnota obchodu překročí částku 1000 EUR
- ✓ bez ohledu na tento limit, když se jedná o:
  - podezřelý obchod;
  - vznik obchodního vztahu;
  - uzavření smlouvy o nájmu bezpečnostní schránky nebo smlouvy o úschově;
  - nákup nebo přijetí kulturních památek, předmětů kulturní hodnoty, použitého zboží nebo zboží bez dokladu o jeho nabytí ke zprostředkování jejich prodeje anebo přijímání věcí do zástavy, nebo výplatu zůstatku zrušeného vkladu z vkladní knížky na doručitele. [2]

Jak je tedy z textu výše patrné, platební instituce musí provést identifikaci klienta vždy, když se jedná o nový obchod např. založení běžného účtu, pokud zákon nestanovuje jinak, viz kapitola výjimky z provedení identifikace.

3.2.2.2 Provádění identifikace

Tato část zákona nám především říká, že:

- ✓ povinná osoba musí provést identifikaci klienta za jeho fyzické přítomnosti;
- ✓ povinná osoba zaznamená identifikační údaje a ověří je z dokladů totožnosti;
- ✓ povinná osoba ověří shodu podoby s vyobrazením na dokladu totožnosti;
- ✓ povinná osoba zaznamená, zda klient není politicky exponovanou osobou;
- ✓ klient musí poskytnout povinné osobě doklady totožnosti nezbytné k provedení identifikace. [2]

Údaje, které musí povinná osoba na daných dokladech totožnosti kontrolovat, jsou:

- ✓ druh a číslo průkazu totožnosti;
- ✓ stát, popřípadě orgán, který doklad vydal;
- ✓ dobu platnosti. [2]

3.2.2.3 Převzetí identifikace

Práce hledá příležitost, jak zjednodušit a zrychlit proces převzetí identifikace klienta jiné banky v prostředí nové regulace platebních služeb. V české regulaci je online první identifikace striktně vymezena částí zákona 253/2008 Sb. o provádění a převzetí identifikace, kde je stanoveno, že pro provedení identifikace musí být klient vždy fyzicky přítomen, pokud zákon nestanoví jinak.

Povinná osoba ale nemusí první identifikaci klienta provést za jeho fyzické přítomnosti v případě, že tyto úkony byly již provedeny jinou finanční či úvěrovou institucí známé jako tzv. převzetí identifikace a zároveň:

- ✓ banka má přístup k těmto informacím;
- ✓ banka má kopii příslušných dokladů o identifikaci klienta, účelu a zamýšlené povaze obchodního vztahu. [2]

Zákon také stanovuje proces, jakým má být převzetí identifikace vykonáno. Klient zasílá povinné osobě kopie dokladů a provádí iniciační platbu pro dokázání existence účtu vedeného u jiné finanční instituce na jeho jméno:

- ✓ *klient zašle povinné osobě kopie jednoho průkazu totožnosti a nejméně jednoho podpůrného dokladu totožnosti, z nichž lze získat údaje viz kapitola Provádění identifikace;*
- ✓ *klient zašle povinné osobě kopii dokladu potvrzující existenci účtu vedeného na jméno klienta u jiné finanční nebo úvěrové instituce;*
- ✓ *první platba z nově vznikající smlouvy s povinnou osobou se uskuteční prostřednictvím účtu vedeného na jméno klienta u jiné finanční nebo úvěrové instituce.* [2]

Klient využije služeb kvalifikovaného poskytovatele služeb vytvářející důvěru:

- ✓ *klient sdělí povinné osobě své identifikační údaje;*
- ✓ *povinná osoba ověří totožnosti majitele u kvalifikovaného poskytovatele služeb vytvářející důvěru dle předpisu eIDAS.* [2]

3.3 On-line identifikace a ověření identity klienta

Potenciální klient finančních služeb má dnes v sektoru bankovnictví několik možností, jak získat určitý finanční produkt vyžadující plné AML ověření, pokud ho dané platební instituce umožňuje zřídit online E2E včetně podpisu smluvní dokumentace, lišící se především v tom, zda mám možnost se digitálně autentizovat v digitálním prostředí banky a autorizovat určitou operaci např. podpis smlouvy na produkt:

- ✓ Jsem již klientem finanční instituce, která již v minulosti ověřila mou fyzickou totožnost a vydala mi tzv. digitální identitu, se kterou se pohybuji v jejím digitálním prostředí, která mě jednoznačně identifikuje a se kterou mohu elektronicky podepsat dokument
- ✓ Jsem již klientem finanční instituce, která již v minulosti ověřila mou fyzickou totožnost, ale nevlastním žádnou tzv. digitální identitu, která by mě jednoznačně identifikovala v jejím digitálním prostředí a umožňovala mi podepisovat elektronicky dokumenty
- ✓ Nejsem klientem finanční instituce

V prvním případě je řešení jednoduché. Pokud banka na svých stránkách nabízí E2E online proces zakoupení finančního produktu vyžadujícího plné AML ověření, klient se v daném digitálním prostředí autentizuje svou digitální identitou (většinou je představeno jednoznačným identifikátorem tzv. uživatelským jménem, který identifikuje klienta, a bezpečnostním klíčem např. heslem, kterým klient ověří svou totožnost), namodeluje si finanční produkt a stejným či jiným bezpečnostním klíčem, kterým se již autentizoval v digitálním světě, autorizuje podpis smluvní dokumentace k produktu.

Ve druhém a třetím případě ale klient žádný identifikátor pro prostředí digitálního světa nevlastní, v tom případě má pouze dvě možnosti:

- ✓ navštívit kamennou pobočku pro dokončení nákupu;
- ✓ projít procesem převzetí identifikace online z jiné finanční instituce, kde jsem již jednou fyzicky identifikován byl a kde vlastním osobní účet.

Pro potřeby této diplomové práce se budeme dále zabývat druhým bodem – procesem převzetí identifikace online.

3.4 On-line zřízení finančního produktu

Platební instituce se pro plné online ověření totožnosti klienta, kterého vidí poprvé, musí řídit českými právními předpisy, viz Zákon 253/2008 Sb.

Nejčastější formou převzetí identifikace je dnes tzv. penny transfer, kde klient musí během procesu zaslat platbu na svůj nově zřizovaný účet u platební instituce z účtu, u kterého kopií dokladu prokazuje cílové platební instituci své majitelství např. proces online zřízení účtu u mBank.

Proces online převzetí identifikace u českých finančních institucí je nejčastěji spojen s nákupem finančního produktu online, například zřízení platebního účtu on-line. Proces je složen z kroků, jejichž pořadí se v závislosti na bankovní instituci může měnit:

1. Modelace osobního účtu
2. Výběr formy uzavření smlouvy na osobní účet
    a. Uživatel vlastní digitální identitu, díky které ho banka autentizuje a vlastní autorizační metodu, kterou může elektronicky podepsat smlouvu na produkt
        i. Validace digitální identity uživatele
    b. Uživatel nevlastní digitální identitu
        i. Zadání základních osobních údajů uživatele
            - Jméno, příjmení
            - Státní občanství
            - Rodné číslo / datum narození
            - Místo narození
            - Pohlaví
        ii. Zadání trvalé adresy uživatele
        iii. Přiložení kopie přední a zadní strany dokladu totožnosti, který obsahuje:
            - druh a číslo průkazu totožnosti
            - stát, popřípadě orgán, který doklad vydal
            - dobu platnosti

iv. Přiložení kopie přední strany podpůrného dokladu totožnosti, který obsahuje:
    - druh a číslo průkazu totožnosti
    - stát, popřípadě orgán, který doklad vydal
    - dobu platnosti
v. Přiložení kopie výpisu z účtu/ smlouvy o účtu, vůči kterému je uživatel ve vztahu majitel

3. Získání informací o účelu a zamýšlené povaze zřizovaného osobního účtu
4. Podpis smlouvy o osobním účtu
5. Ověření existence platebního účtu na jméno uživatele
6. Úspěšné dokončení zřízení osobního účtu

Většina bank dnes založení účtu online nijak veřejně nepropaguje, na svých oficiálních stránkách tuto možnost ale uvádí. České banky se dělí na dva bazény. Jeden bazén komunikuje na potenciální klienty zřízení účtu online, ale k podpisu smlouvy se musí uživatel stejně nakonec dostavit na pobočku, nebo vyčkat na příjezd kurýra. To nabízí například Air Bank, Komerční banka, Raiffeisenbank a Equa bank. Druhý bazén umožňuje dokončit žádost online včetně podpisu smlouvy, ale uživatel již musí mít zřízen účet u jiné banky a zřízení trvá 1-3 pracovní dny. Možnost zřízení online bez návštěvy pobočky nebo kurýra dnes poskytuje právě Československá obchodní banka, mBank, Fio banka a MONETA Money bank.

3.5 Identifikace slabých míst procesu převzetí identifikace

V prostředí zákona 253/2008 Sb. online převzetí identifikace ztrácí hlavní výhody, které nám přináší digitální svět – úspora času, kdy klient získá čas, který by jinak strávil cestou na pobočku a zpět, případně čekáním ve frontě.

Slabá místa převzetí identifikace dnes:

1) Nutnost přerušení a opuštění procesu identifikace pro zadání platby specifikované dle požadavků viz kapitola 1.2.2.3. Převzetí identifikace
2) Čas nutný pro připsání platby (1–2 dny)

3) Nutnost získat a doložit v procesu kopii dokladu stvrzující existenci účtu na jméno žadatele

Z výše uvedeného vyplývá, že pro žadatele přináší proces několik překážek, z nichž dnes ty nejviditelnější jsou především nemožnost dokončit proces v řádu několika minut (v České spořitelně, a.s. trvá zřízení účtu online, pokud již nejsem klientem banky, několika dnů), a zároveň opuštění procesu z důvodu získání příslušného dokladu stvrzujícího existenci účtu (nejčastěji stažení výpisu z účtu původní banky). Pro platební instituci je bolestivým bodem část procesu, kdy uživatel přerušuje identifikaci a je nucen přihlásit se do prostředí své původní banky, kde ztrácí platební instituce kontakt s uživatelem a může tak přijít o potenciálního klienta.

Všechny tři překážky v převzetí identifikace zmíněné výše ale mohou být odstraněny v době platnosti PSD2, čímž se zabývá poslední kapitola.

4 Nová směrnice Evropského parlamentu a Rady Evropské unie o platebních službách

4.1 Úloha Evropského orgánu pro bankovnictví

European Banking Authority neboli EBA je jeden z regulatorních orgánů Evropské unie dohlížející na evropský bankovní sektor. Jeho cílem je prostřednictvím jednotného regulatorního rámce zajistit integritu, stabilitu a řádné fungování evropského bankovního trhu. [6]

EBA aktuálně pracuje na několika nových regulatorních standardech, které mají za cíl vytvořit jednotný předpis Evropské unie o bankovnictví. Součástí tohoto předpisu mají být i jednotlivé rámce, přičemž mezi nejvíce diskutované v českých bankách aktuálně můžeme zařadit

- ✓ The Revised Payment Services Directive (PSD2),
- ✓ The Mortgage Credit Directive (MCD),
- ✓ The Payment Accounts Directive (PAD),
- ✓ The Fourth Anti-money Laundering Directive (AMLD). [6]

Specifické právní akty, pro tuto práci především ve formě směrnic, jsou včleňovány do právního řádu jednotlivých členských států Evropské unie. Říkají, co by mělo být danou směrnicí naplněno za cíl, ale již neuvádí, jakými prostředky má tohoto cíle členský stát dosáhnout.

Jelikož jsou směrnice závazné, tak v okamžiku jejich přijetí je členským státům stanovena lhůta, v rámci které musí být dané směrnice transponovány do právního řádu konkrétního státu. Liší se tedy od nařízení, které je přímo účinné a tedy přímou implementaci do právního řádu nevyžaduje.

Jeden z problémů, které EBA v rámci tvorby jednotného předpisu Evropské unie o bankovnictví řeší, je i zvýšení bezpečnosti během zadávání platebních transakcí, podpora inovací a ochrana zákazníka. Tento dílčí cíl se snaží popsat a naplnit směrnicí známou pod zkratkou PSD2, neboli Payment Services Directive 2 s účinností od 13. 1. 2018. Směrnicí PSD2 se blíže zabývají následující kapitoly této práce.

4.2 Směrnice Evropského parlamentu a Rady EU o platebních službách

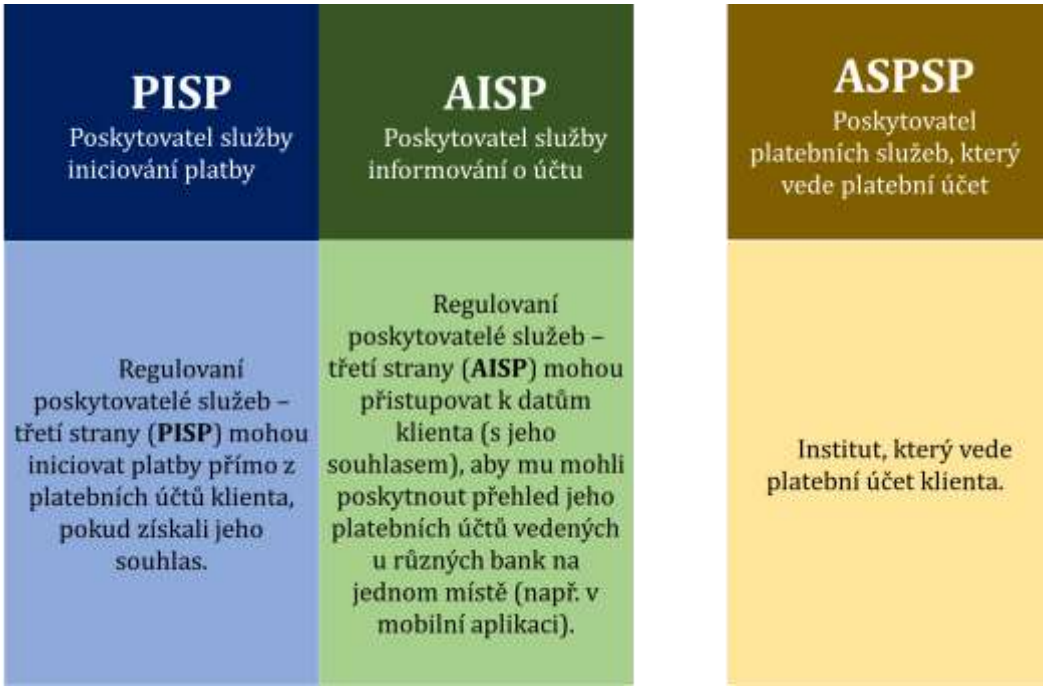
Směrnice PSD2, jejíž celý název zní „Směrnice Evropského parlamentu a Rady EU 2015/2366 ze dne 25. 11. 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení EU č.1093/2010 a zrušuje směrnice 2007/64/ES.", upravuje podmínky pro poskytování platebních služeb a stanovuje pravidla pro provádění platebních transakcí při platbě elektronickými penězi. [7]

4.2.1 Čím se zabývá nová směrnice Evropského parlamentu a Rady EU o platebních službách

PSD2 popisuje povinnost poskytovatelů platebních služeb a rozděluje je následovně:

- poskytovatele platebního účtu tzv. ASPSPs (Account servicing payment service providers),
- poskytovatele služby nepřímého udělení platebního příkazu tzv. PISPs (Payment initiation service provider),

- poskytovatele služby informování o účtu tzv. AISPs (Account information service providers),
- ostatní poskytovatelé platebních služeb tzv. PSPs (Payment service providers). [7]



Obrázek 1 - Subjekty PSD2

Cílem Evropské komise je prostřednictvím této směrnice vylepšit a posílit ochranu spotřebitelů, zlepšit bezpečnost plateb na internetu a přístup k účtu v rámci Evropské unie, posílit konkurenční prostředí a usnadnění zavádění inovací ve finančním sektoru. [8]

Jejím hlavním záměrem je umožnit klientům bank, respektive finančních institucí, správu jejich financí prostřednictvím rozhraní třetích stran. Ve výsledku to znamená, že klienti budou moci provádět platby a sledovat/analyzovat své výdaje prostřednictvím aplikace poskytnuté třetí stranou např. Googlem, přičemž jejich peníze budou stále bezpečně uložené na bankovním účtu v „jejich" bance. [8]

Jelikož k dosažení tohoto záměru je nutné, aby byla třetím stranám bankou zpřístupněna infrastruktura a potřebná data, stanovuje PSD2 bankám povinnost poskytnout přístup k bankovním účtům klientů, a to přes rozhraní pro programování aplikací (tzv. API). [8]

4.2.2 Poskytovatelé platebních služeb a platební služby

Výše zmíněná směrnice se vztahuje především na všechny poskytovatele platebních služeb poskytovaných v rámci EU, tj. na úvěrové instituce, poštovní žirové instituce, platební instituce, instituce elektronických peněz, Evropskou centrální banku a národní centrální banky. [7]

Dle PSD2 je platebními službami myšleno následující:

- ✓ Služby umožňující vložení hotovosti na platební účet, jakož i veškeré operace nutné pro vedení platebního účtu,
- ✓ provádění platebních transakcí, včetně převodu peněžních prostředků, na platebním účtu vedeném u poskytovatele,
- ✓ platebních služeb uživatele nebo u jiného poskytovatele platebních služeb,
- ✓ provádění inkasa, včetně jednorázového inkasa,
- ✓ provádění platebních transakcí prostřednictvím platební karty nebo podobného prostředku,
- ✓ provádění úhrad, včetně trvalých příkazů,
- ✓ provádění platebních transakcí, u nichž se peněžní prostředky čerpají z úvěru pro uživatele platebních služeb,
- ✓ provádění úhrad, včetně trvalých příkazů,
- ✓ vydávání platebních prostředků nebo akceptace platebních transakcí,
- ✓ poukazování peněz,
- ✓ služby iniciování platby,
- ✓ služby informování o účtu. [7]

Je tedy zřejmé, že platební směrnice PSD2 se vztahuje na drtivou většinu všech dnes poskytovaných platebních služeb na českém trhu.

4.2.3 Porovnání PSD2 a PSD

Nová směrnice PSD2 reviduje směrnici PSD z roku 2009. Jelikož finanční trh je čím dál komplexnější, stává se jak pro poskytovatele finančních služeb, tak pro konzumenty méně přehledný.

Studie konzultantské společnosti PWC poukazuje na slabá místa stávající směrnice platebních služeb PSD a následné řešení těchto slabin prostřednictvím PSD2, viz níže.

Nedostatky PSD jsou:

- ✓ Nekonzistentní aplikace PSD a dalších evropských směrnic v rámci jednotlivých členských států,
- ✓ Několik generických výjimek ve směrnici,
- ✓ Mnoho operátorů a neregulovaných zprostředkovatelů,
- ✓ Nedostatek standardizace řešení platebních služeb a bezpečnostních systémů,
- ✓ Použití rozdílných poplatků napříč členskými státy. [9]

Řešení nedostatků vyplývající z PSD2 je:

- ✓ Posílení ochrany spotřebitele,
- ✓ Vývoj nových platebních řešení,
- ✓ Regulace nových účastníků na trhu,
- ✓ Jednotné poplatky za platby kartou v souladu s regulací mezibankovních poplatků (tzv. MIF),
- ✓ Zvýšení úrovně hospodářské soutěže,
- ✓ Překonání rozdílů mezi členskými státy,
- ✓ Obecné zvýšení efektivity prostřednictvím standardizace infrastruktury. [9]

Na základě výše uvedeného je zřejmé, že Evropská unie směřuje k sjednocení postupů a pravidel na bankovním trhu, k posílení bezpečnosti systému a zajištění vysoké úrovně hospodářské soutěže a transparentnosti vůči spotřebitelům.

Ke zvýšení úrovně hospodářské soutěže dochází právě umožněním vstupu třetích stran do oblasti platebních služeb, nicméně spolu s tím se zvyšuje riziko týkající se bezpečnosti dat, především citlivých údajů o klientech.

Aby bylo toto riziko sníženo na minimum, jsou poskytovatelé platebních služeb povinni provádět při elektronických platbách tzv. silné ověření klienta. Konkrétní postupy pro silné ověření jsou blíže vymezeny v jedné z regulačních technických norem připravovaných Evropským orgánem pro bankovnictví (EBA), a to konkrétně normou „Draft Regulatory Technical Standards on Strong Customer Authentication

and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)", které je věnována samostatná podkapitola.

4.2.4 Obsah PSD2

V rámci PSD2 směrnice jsou nově platební instituce povinny poskytovat služby licencovaným třetím stranám (Third Part Provider tzv. TPP):

- informování o platebním účtu (Account Information Service), kdy třetí strana (AISP) poskytne klientovi přehled bankovních účtů vedených u různých platebních institucí,
- nepřímého udělení platebního příkazu (Payment Initation Service), kdy třetí strana (PISP) umožní klientovi iniciovat platbu online ze svého platebního účtu bez přímého přístupu do bankovnictví. [7]

Banky musí nově poskytovat stejné množství informací o účtu, jaké klientovi vzdáleně online dnes poskytuje sama. Výjimkou jsou citlivé údaje, které by mohly být zneužity k podvodu. Blíže již se ale vymezením citlivých údajů směrnice nezaobírá.

4.2.4.1 Služba informování o platebním účtu

V prostředí PSD2 musí nově poskytovatelé platebních služeb poskytovat službu informování o platebním účtu, která dle 370/2017 Sb. Zákonu o platebním styku říká:

„*Udělil-li uživatel souhlas se sdělením informací o platebním účtu, sdělí poskytovatel, který mu vede platební účet, informace o platebním účtu uživatele poskytovateli služby informování o platebním účtu v rozsahu, v jakém jsou přístupné uživateli prostřednictvím internetu.*“ [8]

Vybrané povinnosti poskytovatele platebního účtu:

- Musí umožnit sdílení stejných informací AISP o platebním účtu uživatele v rozsahu, jaké jsou přístupné uživateli v prostředí internetu (banka musí poskytnout třetí straně všechny informace o platebním účtu, jaké dnes poskytuje svému uživateli ve svém bankovnictví, tedy pokud například ve svém bankovnictví může uživatel vidět transakční historii za 3 roky, banka nemůže třetí straně poskytnout transakční historii pouze za 2 roky, musí ji poskytnout v celém rozsahu).

- Nesmí dělat žádné rozdíly mezi žádostmi o informace o platebním účtu, ať jdou ze strany AISP, tak ze strany vlastního internetového rozhraní tzv. princip nediskriminace, (například banka nemůže mít různou odezvu služby pro získání informací o transakční historii uživatele ze strany vlastního rozhraní bankovnictví nebo rozhraní třetí strany).
- Nesmí si účtovat žádné poplatky za poskytnutí informací o účtu. [7]

Vybrané povinnosti poskytovatele služby informování o platebním účtu:

- Poskytuje službu informování o platebním účtu uživatele pouze na základě výslovného souhlasu uživatele.
- Nevyžaduje po uživateli ani nijak nezpracovává citlivé údaje, čímž se zde myslí jakýkoliv údaj, který dle Zákona o platebním styku: „*může být zneužit k podvodu v oblasti platebních služeb, s výjimkou jedinečného identifikátoru a jména majitele platebního účtu*“. [8] Kdy jedinečným identifikátorem je zde myšlena jedinečná kombinace písmen, číslic nebo symbolů, kterými se identifikuje uživatel nebo jeho účet při provádění platebních transakcí.
- Při každém dotazu pro sdělení informací o platebním účtu uživatele ověří svou totožnost poskytovateli platebních služeb daného uživatele.
- AISP může přistupovat pouze k datům, ke kterým získal od uživatele výslovný souhlas.
- Zpracovává pouze ty údaje o uživateli, které potřebuje pro poskytnutí služby informování o platebním účtu. [7]

4.2.4.2 Služba nepřímého udělení platebního příkazu

Poskytovatel platebního účtu musí nově umožnit také službu nepřímého udělení platebního příkazu, která je dle 370/2017 Sb. Zákonu o platebním styku definována takto:

„*Službou nepřímého dání platebního příkazu služba spočívající v dání platebního příkazu k převodu peněžních prostředků z platebního účtu jménem plátce poskytovatelem rozdílným od poskytovatele, který pro plátce vede daný platební účet, je-li platební příkaz dán prostřednictvím internetu.*“ [8]

Vybrané povinnosti poskytovatele platebního účtu podle článku 46-49 PSD2:

- Ihned po iniciování, přijetí i provedení platebního příkazu sdělí poskytovateli služby dostupné informace o zadaném platebním příkazu jako je (článek 46, 48, 49 PSD2):
    - Potvrzení o úspěšném iniciování platebního příkazu;
    - Referenční údaje transakce umožňující plátci identifikovat danou transakci, a příjemci umožňující identifikovat plátce;
    - Částku platební transakce;
    - Veškeré poplatky s platební transakcí spojené;
    - Datum přijetí platebního příkazu;
    - Směnný kurz použitý při platební transakci;
    - Den připsání částky na účet.
- Nesmí dělat rozdíly ve zprocesování platby, ať již byla přijata nepřímo přes službu nepřímého dání platebního příkazu, či přímo přes vlastní služby podání platebního příkazu tzv. princip nediskriminace (např. nesmí se lišit doba zpracování platby či proces pro zamítnutí nebo přijetí platby). [7]

Vybrané povinnosti poskytovatele služby nepřímého dání platebního příkazu:

- Nepřijímá žádné peněžní prostředky k provedení platby.
- Osobní bezpečnostní prvky pro autentizaci uživateli a autorizaci platby zpřístupní pouze poskytovateli platebního účtu a plátci.
- Neuchovává žádné citlivé údaje o plátci, které mohou být zneužity pro podvod v oblasti platebních služeb.
- Požaduje po plátci pouze ty údaje k nepřímému dání platebního příkazu, které pro podání příkazu potřebuje. [7]

4.3 Licencování

Aby třetí strana mohla poskytovat nové služby definované směrnicí PSD2, musí získat povolení od České národní banky (dále ČNB). Seznam všech licencovaných subjektů poskytující platební služby nepřímého udělení platebního příkazu nebo informování o účtu zveřejňuje ČNB na svých webových stránkách [6].

Dále musí získat certifikát, kterým se bude prokazovat poskytovateli platebního účtu. Certifikát ale bude povinný až od účinnosti Regulatorního technického standardu k říjnu 2019. Dnes se tedy aplikace třetích stran certifikáty neprokazují.

Třetí strana pro získání povolení vystupovat jako poskytovatel platebních služeb v roli PISP nebo AISP musí doložit k žádosti také:

- popis, jaké platební služby plánuje třetí strana poskytovat,
- obchodní plán včetně kalkulace předpokládaného rozpočtu na první tři účetní období,
- doklad o tom, že platební instituce má počáteční kapitál (min vždy 20 000 EUR),
- popis opatření přijatých za účelem ochrany peněžních prostředků,
- popis postupu pro sledování a řešení bezpečnostních incidentů a stížností klientů,
- popis postupu pro zaznamenávání citlivých údajů o platbách a omezování přístupu k nim,
- popis organizačního uspořádání žadatele, aj. [7]

4.4 Technický standard pro silnou autentizaci a bezpečnou komunikaci

Na PSD2 navazuje řada norem jak návody (Guidelines) popisující implementaci a řízení se PSD2 v určitých oblastech, tak i technické standardy (Regulatory Technical Standards). Tato kapitola se zabývá přiblížením technického standardu pro silnou autentizaci a bezpečnou komunikaci tzv. Regulatory technical standards on strong authentication and secure communication tzv. RTS.

4.4.1 Hlavní cíle Regulatorního technického standardu pro silnou autentizaci a bezpečnou komunikaci

RTS je technický standard vznikající pod regulací PSD2, který má za úkol zvýšit ochranu spotřebitele, podpořit rozvoj a inovace, a zajistit vyšší míru bezpečnosti v prostředí online platebních služeb. Standard byl vytvořen Evropskou centrální bankou ve spolupráci s Evropským orgánem pro bankovnictví. [11]

Finální znění RTS bylo schváleno Evropskou komisí v únoru roku 2018, účinnosti dle PSD2 nabývá 18 měsíců po nabytí v platnost, tedy říjen 2019.

RTS obsahuje:

- Požadavky na silnou autentizaci;
- Výjimky z povinnosti provádět silné ověření klienta;
- Zásady ochrany uživatele platebních služeb během všech fází ověření totožnosti a přenosu a zobrazení informací o účtu;
- Požadavky na bezpečnou komunikaci;
- Závěrečná ustanovení. [11]

4.4.2 Požadavky na silnou autentizaci

RTS přináší standard pro vzdálené ověření totožnosti uživatele. Klient k takovému úkonu musí dát výslovný souhlas. Třetí strana má nad to ještě právo přistupovat pouze k těm údajům klienta, které slouží pouze požadovanému účelu klienta.

Výslovný souhlas zahrnuje:

- Identitu třetí strany, se kterou chce klient sdílet své údaje;

- Rozsah dat, která budou se třetí stranou sdílena;
- Délku trvání udělení výslovného souhlasu s přístupem na data definovaná výše. [11]

Každý souhlas s přístupem k účtu, iniciace elektronické platby, nebo jakákoliv další operace online, která znamená potenciální riziko zneužití dat o klientovi či zneužití jeho platebního účtu, až na výjimky popsané v kapitole 4.4.3, musí být následně potvrzen tzv. SCA (Strong Customer Authentication) metodou neboli silně ověřen [11].

SCA jednoduše znamená, že každé ověření totožnosti uživatele musí být založeno minimálně na dvou na sobě navzájem nezávislých faktorech (dále 2FA), a to:

- Něco znám („Knowledge“) např. Heslo
- Něco mám („Possession“) např. Klientský certifikát
- Něco jsem („Inherence“) např. Otisk prstu

Uživatel se tedy s každou žádostí o přístup ke svému účtu, či během autorizace platební operace musí prokázat min dvěma faktory. Už dnes mají uživatelé možnost využít 2FA přihlašování a ověřování svých platebních transakcí, např. pro přihlášení do svého bankovnictví zadávají nejen heslo („Knowledge“), ale také jednorázový OTP kód („One Time Password“), který jim přijde na jejich mobilní zařízení („Possession“).

V praxi to znamená, že na základě těchto dvou faktorů systém zodpovědný za ověření totožnosti uživatele platebního účtu generuje autentizační kód. Tento kód se smí použít pro autentizaci uživatele a autorizaci přístupu k jeho datům pouze jednou. Systém pro každé další ověření, např. iniciování nové platby, generuje nový kód, vyžaduje od uživatele, aby se prokázal znovu svými dvěma bezpečnostními faktory.

To je v dnešním rychlém digitálním světě pro spoustu uživatelů značně nepohodlné, pomalé. Proto RTS definuje i určité výjimky pospané v kapitole níže, za kterých je možné od SCA upustit.

4.4.3 Výjimky z povinnosti provádět SCA

Poskytovatel platebních služeb má možnost nevyžadovat po plátci silné ověření totožnosti (SCA) v těchto případech:

1) Jedna platební transakce nepřekročí částku 30 EUR (Article 16 RTS), kdy plátce může schválit max 5 takto za sebou jdoucích low – value transakcí bez nutnosti SCA autorizace.
2) Kumulativně platební transakce nepřekročí částku 100 EUR (Article 16 RTS), kdy plátce může schválit max 5 takto za sebou jdoucích low – value transakcí bez nutnosti SCA autorizace.
3) Platba mezi tzv. důvěryhodnými příjemci (Article 13 RTS), tedy kde číslo účtu příjemce platby je uvedeno na seznamu důvěryhodných příjemců, který si již dříve plátce vytvořil.
4) Opakující se platba na stejnou částku a stejné číslo účtu (Article 14 RTS)
5) Platba mezi vlastními účty, které jsou vedeny v rámci jedné fyzické či právnické osoby (Article 15 RTS).
6) Platební transakce iniciované ze speciálního dedikované prostředí zabezpečeného dle standardů Directive 2015/2366 (Article 17 RTS).
7) Platba vyhodnocená jako nízkoriziková na základě analýzy rizik tzv. Transaction risk analysis, kdy zároveň nepřekročí částku danou dle tzv. ETV (Exemption Threshold Value), maximálně může být schválena platba bez nutnosti využít SCA až do 500 EUR dle míry rizika (Article 18 RTS). [7]

4.4.4 Zásady ochrany uživatele platebních služeb během všech fází ověření totožnosti a přenosu a zobrazení informací o účtu

Kapitola 5.2. popisuje povinnosti na ochranu uživatele, jeho bezpečnostních přihlašovacích údajů a autentizačního kódu během celého procesu online autentizace včetně přenosu, zobrazení a ukládání dat.

Blíže je tato problematika přiblížena v kapitole 5.2.2, kde jsou shrnuty požadavky na API vycházející z PSD2, potažmo RTS.

4.4.5 Požadavky na bezpečnou komunikaci

Kapitola 5 RTS již detailně specifikuje povinnosti

- ASPSPs,
- PISPs,
- AISPs,
- PSPs

pro zajištění bezpečné komunikace mezi nimi, plátci, příjemci a ostatními poskytovateli platebních služeb.

Blíže je tato problematika přiblížena v kapitole 5.2, kde jsou shrnuty požadavky na API vycházející z PSD2, potažmo RTS.

4.5 Plán implementace PSD2 a RTS

Směrnice PSD2 již vstoupila v platnost 13. 1. 2016. Jednotlivé členské státy Evropské unie měly dva roky na to, transponovat evropskou směrnici do své národní legislativy. V České republice se tak stává zákonem 370/2017 Sb., o platebním styku. Tento zákon nabyl účinnosti k 13. 1. 2018.

Obrázek 2 - Harmonogram

Od 13. 1. 2018 jsou tedy banky povinny umožňovat svým klientům nepřímé podání platebního příkazu přes licencovanou třetí stranu. Platební instituce jsou také povinny těmto třetím stranám se souhlasem klienta podat informace o platebním účtu aj.

K 13. 1. 2018 ale nebude účinná většina prováděcích předpisů EU (standardy, vyhlášky a doporučení), které jsou nutné pro zajištění fungování nových služeb, podléhajících regulaci. [12]

Jedním z těchto prováděcích předpisů je regulatorní technický standard (NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU), kterým se doplňuje směrnice Evropského parlamentu a Rady 2015/2366), který definuje detailní technické parametry a principy silného ověření klienta včetně definice zabezpečení komunikace mezi klientem, bankou a třetí stranou. Jeho finální verze byla publikována v listopadu 2017. Tedy účinnost regulatorních technických standardů se nekryje s datem účinnosti směrnice. RTS již byla přijata Evropskou komisí, předpokládaný termín účinnosti je říjen 2019. Od oficiálního přijetí RTS Evropskou komisí opět běží lhůta, než nabude standart účinnosti, což je 12 měsíců po zveřejnění dokumentace a zpřístupnění

testovacích rozhraní, ale nejdéle 18 měsíců od oficiálního přijetí Evropskou komisí. Nařízení vstupuje v platnost prvním dnem po vyhlášení v Úředním věstníku EU.

5 Standardizace komunikace platebních institucí s aplikacemi třetích stran

Dnešní technologie nabízí dva způsoby, jak zajistit přístup k účtu klienta přes třetí stranu – prostřednictvím zvláštního dedikovaného rozhraní určeného pro programování aplikací (API) a prostřednictvím strojového čtení uživatelského rozhraní (screen scraping), kdy počítačový program kopíruje data z webové stránky a umožňuje tak třetí straně přistupovat ke všem informacím, jaké jsou uživateli na stránce dostupné. Ministerstvo financí i Česká národní banka považují vzhledem k výše uvedenému za preferovaný způsob zpřístupnění účtu třetím stranám pomocí API.

V rámci finálního znění RTS publikovaného v listopadu 2017 byl tradiční screen scraping zakázán a tento zákaz vstoupí v účinnost spolu s tímto standardem, tedy přibližně říjen 2019. Proto budu dále v této práci rozebírat standard komunikace založený na API. [12]

5.1 API

API neboli Application Programming Interface je v softwarovém inženýrství obecný pojem pro soubor funkcí a procedur, které umožňují vývojářům využívat funkce nějaké knihovny nebo jiného softwaru. API umožňuje rychlejší vývoj softwaru využitím již existujících komponent jiných poskytovatelů, typicky například funkce operačního systému, databází nebo grafických knihoven atd.

V kontextu práce se pod pojmem API rozumí specificky Web API – rozhraní pro komunikaci s webovými službami, tj. službami poskytovanými po internetu. Upřesnění, že jde o „Web“ API se dnes již často nepoužívá, jelikož bývá z kontextu zřejmé, že se jedná o webové služby, a tak se již běžně pojem „Web“ vynechává. Tomu je tak pak i u dalších typů API jako například Open API, Google Maps API a podobně.

5.1.1 Proč API?

S rozmachem internetu a postupně i výrazně zvyšující se rychlostí a výpočetní kapacitou služeb připojených k internetu doznal velkých změn i způsob vývoje softwaru. Historicky monolitické aplikace a jejich architektura se postupně začaly přizpůsobovat novým možnostem počítačových a síťových technologií. Software

instalovaný z CD je postupně nahrazován formou konkrétní koncové nepřetržitě fungující služby – takzvané SaaS – Software as a Service. Příkladů je v každém odvětví mnoho, ať už to jsou e-commerce řešení (platformy pro eshopy jako shoptet.cz, shopify.com, Amazon…), CRM systémy (Microsoft Dynamics, Salesforce…), marketingové nástroje (Adobe Marketing Cloud, Google Analytics…), nástroje datové analýzy (GoodData, Keboola…). Tato změna byla na jedné straně způsobená právě možností využívat již hotové služby dostupné online od jiných poskytovatelů, a zároveň tyto služby dál urychlují vývoj nových a nových služeb tím, že jsou dostupné zase online prostřednictvím API dalším vývojářům. API jsou proto v dnešním prostředí naprosto zásadním prvkem, který dnes v mnohém definuje celé odvětví online služeb, i jejich ekonomiku (s využíváním API vzniklo i mnoho nových obchodních modelů, které nicméně nejsou pro tuto práci natolik podstatné).

Jako příklad takových „všudepřítomných“ služeb využívaných přes jejich API je Google Maps a Facebook. Dnes je již těžké najít online službu, která nevyužívá registraci a přihlášení uživatelů pomoc Facebooku – jinými slovy využití API Facebooku pro získání informací o uživateli a ověření jeho identity. V tomto případě jde o API poskytované zdarma, zjevnou hodnotou pro vývojáře služeb je rychlá implementace funkcí spojených se získáním uživatelských informací a ověřování uživatelů. Hodnotou pro Facebook je znalost, kam se konkrétní uživatelé přihlašují a jaký typ služeb využívají, což dále Facebook využívá pro cílení reklamy. Google Maps je pak příkladem freemium obchodního modelu, kdy využívání map přes Google Maps API je od určité četnosti volání rozhraní již zpoplatněno. Zase se jedná o hezký příklad běžné, velmi užitečné a přitom implementačně extrémně náročné funkčnosti (rychlá vizualizace map online, optimalizace vysokého datového toku, cenné mapové podklady), která je tímto způsobem snadno dostupná téměř komukoliv.

Je proto zřejmé, proč je o API takový zájem i u tradičnějších odvětví a korporací, jako je třeba bankovnictví a proč i sem vstupuje regulace, které má na jedné straně zájem chránit uživatele v online prostředí, a na straně druhé umožnit a zrychlit možné inovace.

5.1.2 Architektura API

V roce 1998 Microsoft uvedl nový komunikační protokol SOAP. Šlo na tehdejší dobu o revoluční řešení, které umožňovalo výměnu dat ve formátu XML mezi systémy

komunikující po síti. Aplikace, jednotlivé webové služby, na sobě mohou být navzájem nezávislé, nezávislé na programovacím jazyce, ve kterém jsou napsány, ale přesto si mezi sebou díky standardizovanému protokolu pro výměnu dokumentů rozumí. Výměna dat ve formátu XML vystavená na standardu SOAP je popsána jazykem WSDL (Web Services Description Language), který popisuje, jak má vypadat komunikace mezi jednotlivými webovými službami. WSDL vychází z XML.

V dnešní době se od protokolu SOAP již upouští. Dnešní webové služby jsou až na výjimky vystavěné ve stylu REST. SOAP služby dnes již využívají pouze velké firmy, pro které by byl přechod na RESTful komunikaci příliš náročný a drahý.

Nevýhody komunikačního protokolu SOAP tkví především v povinném formátu pro výměnu dat XML a absence standardizovaného architektonického stylu. Což přináší omezení:

- Některé klientské aplikace neumí data ve formátu XML zpracovat;
- XML soubory jsou pro jednoduché příkazy příliš náročné a zbytečně zatěžují komunikaci po síti;
- Vzniká obrovské množství služeb napsaných v jazyce WSDL, které pokud nejsou jasně zdokumentované, nikdo neví, co má daná služba dělat.

5.1.3 Rest API

V roce 2000 Roy Fielfing reagoval na tehdejší problém se škálovatelností WWW a ve své disertační práci popsal nový architektonický přístup světa fungování webových aplikací, nazval ho Representational State Transfer (REST). [17]

REST je architektonický styl komunikace klient – server, založená na principu požadavek – odpověď. Pravidla REST vychází z bezstavového http protokolu, který historicky popisuje výměnu dat všech formátů na webu. Na rozdíl od protokolu SOAP, který byl založen na systému volání procedur, je architektura REST vystavěná na jednotlivých jedinečně identifikovaných zdrojích, neboli resources. Resource je objekt, který je jednoznačně identifikovatelný a adresovatelný na webu pomocí URL (Unified Resource Identifier) např. účet klienta. [17]

Webová služba umožňuje klientovi provádět operace nad resources pomocí metod vycházejících z http protokolu. Většina webových aplikací si dnes vystačí

s metodami GET a POST. REST ale využívá i další metody popsané standardem http, též známe pod zkratkou CRUD (Create, Read, Update, Delete):

- Metoda GET vykresluje data, např. zobrazí formulář
- Metoda POST posílá data na server, např. zasílá vyplněný formulář zpět na server
- Metoda PUT updatuje data na serveru, např. změna uživatelského jména uživatele
- Metoda DELETE maže data na serveru, např. smazání uživatele

V requestu si může klient sám vyžádat, v jaké formátu očekává response aplikace (JSON, XML, HTML,…), případně v jakém formátu zasílá na server data. I response zprávy obsahuje informaci, v jakém formátu klient nakonec data získal. S response zprávy se pojí také stavový kód, kdy server sděluje klientovi výsledek jeho žádosti. Například server takto informuje klienta, že byl překročen maximální limit počtu požadavků/ min stavovým kódem 429, případně zašle stavový kód 403 v případě, že vyhodnotí, že se jedná o neautorizovaný přístup na daný resource.

5.2 Požadavky na API vycházející z PSD2

PSD2 a její prováděcí předpisy kladou především důraz na bezpečnost a dostupnost dat, které banky nově povinně musí poskytnout certifikovaným třetím stranám.

Dosavadní strojové čtení, které znamenalo, že klient poskytnul své přihlašovací údaje třetí straně, představovalo riziko pro zachování bezpečnosti dat klienta. Nově je toto riziko mitigováno jednotlivými požadavky směrnice RTS na přístup, přenos a dostupnost dat, které popisuji níže.

Požadavky na identifikaci uživatele platebních služeb v digitálním prostoru rozebírala kapitola 2.1.4.3, následující shrnutí popisuje již samotné bezpečnostní nároky na API.

5.2.1 Obecné požadavky pro zpřístupnění rozhraní

Poskytovatel platebního účtu musí umožnit AISP a PISP bezpečnou komunikaci se svým rozhraním systému platebních služeb (Article 30 RTS). Dále také například:

- Umožnit AISP, PISP, že mají možnost se identifikovat směrem k poskytovateli platebních služeb
- Poskytnout dokumentaci API min 6 měsíců před účinností RTS, anebo samotným spuštěním API
- Poskytnout testovací prostředí min 6 měsíců před účinností RTS, anebo samotným spuštěním API
- Mít na internetu k dispozici kvartálně statistiku dostupnosti a výkonnosti API (Article 32 RTS) [11]

5.2.2 Bezpečnost

Požadavky na bezpečnost využití definovaného rozhraní banky třetí stranou je vymezeno jak pravidly pro ověření totožnosti klienta dle SCA, tak dalšími nároky na API jako je například:

- Třetí strana (TPP) se vždy musí identifikovat vůči subjektu, který vede platební účet (ASPSP)
- Přístup k účtu uživateli musí být dočasně či trvale blokován po min 5 neúspěšných pokusech o autorizaci přístupu

- Maximální čas nečinnosti na webové či mobilní stránce po úspěšně provedené autorizaci přístupu je 5min
- Platební služba musí vždy uživateli během celého procesu autorizace platební transakce zobrazovat následující údaje:
    - Částka
    - Identifikace příjemce (typicky se bude využívat číslo účtu příjemce) [11]

Autentizační kód, kterým uživatel autorizuje platební transakci, musí být dynamicky propojen s informacemi o příjemci a částky. Pokud se jakýkoliv z těchto dvou vstupů změní, musí dojít také ke změně autentizačního kódu. [11]

5.2.3 Komunikace systému platební instituce s aplikací třetí strany

Požadavky komunikaci řešení umožňující přístup třetích stran přes dedikované rozhraní k API bankovní instituce se opírá především o dostupnost a odezvu bankovních aplikací, aby žádným způsobem nediskriminovala třetí stranu.

Vybrané požadavky na úroveň poskytovaných služeb:

- Celková dostupnost služeb
- Výkon
- Podpory pro řešení problémů
- Zátěžové testy rozhraní, které jsou vykonány ostatními subjekty služeb na trhu platebních služeb a orgánem trhu
- Zveřejnění technických specifikací svých rozhraní a to nejpozději 6 měsíců před datem účinnosti RTS
- Zpřístupnění testovacího prostředí pro všechny poskytovatele platebních služeb, které o to požádali [11]

Pokud banka neposkytne dedikované rozhraní dle standardů výše, má třetí strana možnost využít přístup k účtu klienta přes zákaznické rozhraní. Jedná se o nouzové opatření, které může představovat i tzv. screen scraping. [11]

5.3 Požadavky na API vycházející z Českého standardu pro Open Banking

Na základě schválení směrnice PSD2, na kterou navazuje řada norem a návodů, která přináší na bankovní trh spoustu různorodých řešení, přistoupila Česká bankovní asociace k vydání tzv. Českého standardu pro Open Banking (ČOBS) vycházejícího z již zmiňovaného zákona o platebním styku. [12]

5.3.1 Co je Česká bankovní asociace?

Česká bankovní asociace (ČBA) je sdružení právnických osob, kde členství je vyhrazeno bankám a pobočkám zahraničních bank s licencí ČNB. Vznikla v roce 1990. V současné době sdružuje 38 členů.

Role ČBA:

- zastupuje a prosazuje společné zájmy členů ve vztahu k Parlamentu, vládě, České národní bance a dalším právním subjektům;
- prezentuje roli a zájmy bankovnictví vůči veřejnosti a zahraničí;
- podílí se na standardizaci postupů v bankovnictví a na vytváření odborných usancí, podporuje harmonizaci bankovní legislativy s legislativou Evropské unie. [13]

5.3.2 Český standard pro Open Banking

Nová směrnice PSD2 přinesla s sebou i řadu různých výkladů, proto řešení jednotlivých poskytovatelů platebních účtů a licencovaných třetích stran mohou být velmi různá. To může vést k tomu, že jednotlivá řešení, která budou vybudována na základech PSD2 značně složitá, nákladná, nepřepoužitelná. Jednotlivé banky sdružené v asociaci ČBA je proto rozhodly svá řešení standardizovat pod Českým standardem pro Open Banking. [15]

ČOBS definuje technickou specifikaci pro přístup třetích stran k informacím o účtu, pro nepřímé dání platebního příkazu a pro ověření dostatku prostředků na platebním účtu. Cílem standardu je především zjednodušit integraci TPP na rozhraní jednotlivých bank. [15]

Standard je dobrovolný. Každá banka může zvážit, zda se jím bude řídit, nebo ne.

ČOBS obsahuje:

- Technický popis definující základní parametry komunikace a zdůvodnění jejich použití;
- Bezpečnostní standard definující průběh ověření totožnosti uživatele pro přístup třetí strany ke službám banky;
- Definici API pro službu informování o účtu;
- Definici API pro službu nepřímého dání platebního příkazu;
- Definici API pro službu ověření dostatku na účtu;
- Příklady request a response jednotlivých zdrojů API ve formátu JSON;
- Definici bezpečnostních principů;
- Specifikace datového obsahu jednotlivých služeb. [15]

5.3.3 Technické požadavky na API vycházející z Českého standardu pro Open Banking

ČOBS popisuje, jak má vypadat rozhraní platebních institucí spadajících pod regulaci PSD2 pro přístup třetích stran k informacím a službám bank.

Vybrané požadavky na komunikaci poskytovatele platebního účtu s aplikací třetí strany:

- Jako transportní protokol komunikace se využívá verze HTTP 1.1 nebo HTTP 2.0
- Využívané http metody jsou:
    - POST např. pro vytvoření nové platební transakce;
    - PUT např. pro změnu parametru transakce;
    - DELETE např. pro smazání zprávy;
    - GET např. pro volání seznamu účtů klienta;
- Design komunikačního rozhraní je navržen v REST (Representational State Transfer);
- Formát zápisu dat je dotazu a odpovědi je využit JSON (JavaScript Object Notation);
- Kódování obsahu je ve formátu UTF-8. [15]

5.3.4 Požadavky na bezpečnou komunikaci

ČOBS nedefinuje, jak má dojít k ověření přihlašovacích údajů uživatele (ověření, že ta osoba, která přistupuje k API, je skutečně tou, za kterou se vydává, to je plně v kompetenci banky), ale specifikuje, jak má dojít k ověření, že osoba, která k API přistupuje, má k tomu právo. ČOBS popisuje, jak má dojít k prověření oprávnění přístupu klienta na konkrétní resource. Takové autorizační flow, kde uživatel vznese požadavek (request) pro přístup k nějaké informaci o účtu (např. zůstatek) a čeká na odpověď, je zabezpečeno protokolem OAuth2.0 a OpenID.[15]

5.3.4.1 Protokol OpenID

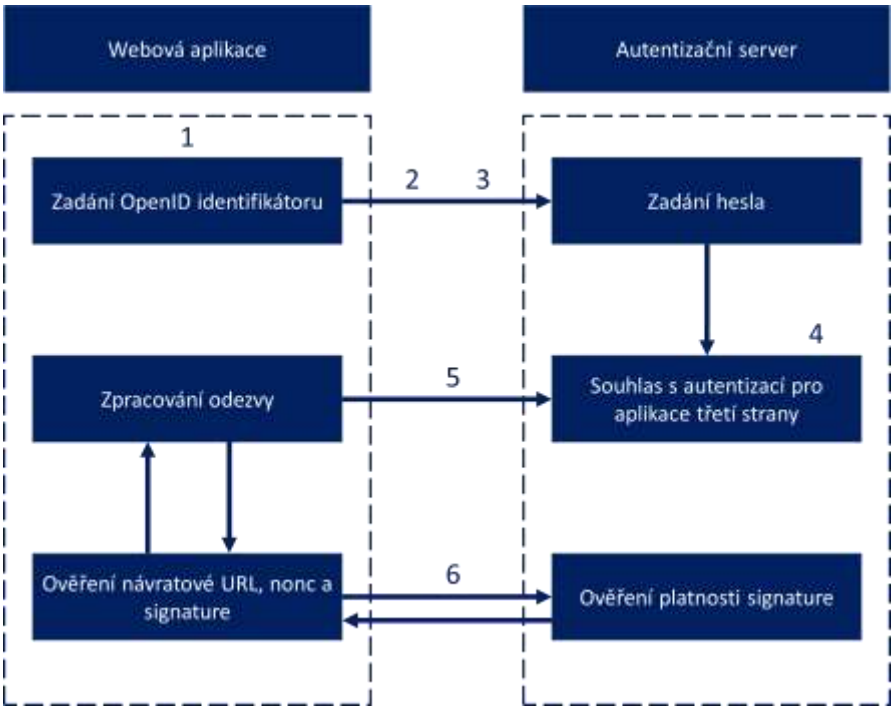
OpenID je otevřený standard, který umožňuje uživateli používat jedny přístupové údaje (například uživatelské jméno a heslo) pro více různých na sobě nezávislých webových služeb.

Jedná se decentralizovaný protokol, který nespoléhá na jednoho centrálního poskytovatele autentizace (například pouze FacebookID), ani neurčuje, jak má být konkrétní identita ověřena (zda má využít heslo nebo například jednorázový SMS kód), pouze umožňuje aplikaci třetí strany implementovat různé autentizační řešení různých poskytovatelů identity, aniž by musela celé řešení vyvíjet a spravovat sama.

OpenID standard dnes podporují velké globální společnosti jako je Google, Microsoft, facebook nebo Twitter. Mezi předními českými poskytovateli CZ.NIC poskytující službu mojeID.cz.

Uživatel si potřebuje pouze založit identitu u jednoho z poskytovatelů OpenID autentizace např. Google účet. Tak získá svůj OpenID identifikátor, který následně využívá pro přihlášení do všech webových služeb, které OpenID podporují.

Samotná komunikace aplikace s poskytovatelem Open ID identity je znázorněna na obrázku níže:



Obrázek 3 - OpenIS komunikace [16]

1. Uživatel iniciuje autentizaci do aplikace třetí strany vyplněním svého OpenID identifikátoru do webového formuláře.
2. Aplikace třetí strany vyhledá URL adresu konkrétního poskytovatele OpenID identity dle OpenID IDntifikátoru.
3. Aplikace třetí strany přesměrovává uživatele na autentizační server poskytovatele identity, kterému předává autentizační požadavek.
4. Uživatel se autentizuje na webové stránce providera a uděluje souhlas s poskytnutím informace o ověření své identity aplikaci třetí strany.
5. Autentizační server přesměrovává uživatele zpět do aplikace třetí strany spolu s informací, zda byla autentizace provedena, anebo selhala.
6. Aplikace třetí strany ověří informace předané z autentizačního serveru – návratové URL, parametry nonce a signature, neboli sdílený klíč mezi aplikací třetí strany a autentizačním serverem, který se generuje během zaslání requestu. [16]

5.3.4.2 Protokol OAuth 2.0

Protokol OAuth 2.0 je otevřený standard umožňující řídit přístup aplikace třetí strany na konkrétní webovou službu. Popisuje autorizační procesy pro webové, mobilní či jiná koncová zařízení a pomáhá řídit přístup aplikace třetí strany pouze na konkrétní resources.

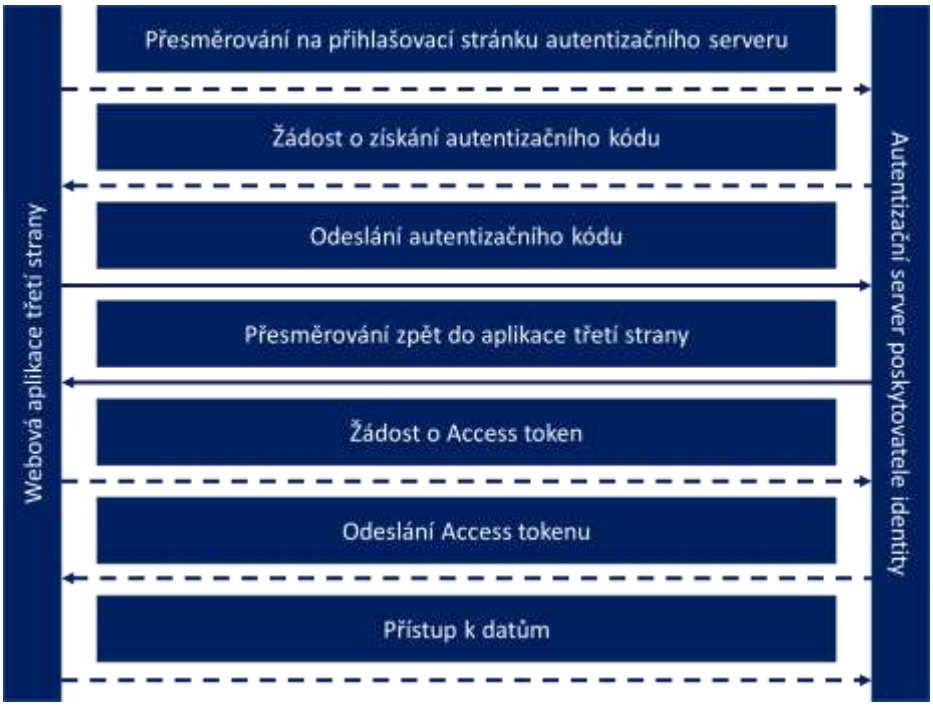
Standard OAuth 2.0 dnes využívá například Facebook, Twitter, Microsoft nebo Google pro řízení autorizovaného přístupu na svá API. Jedna z nejznámějších webových služeb je „Log in with Facebook" API, která poskytuje aplikaci třetí strany službu ověření uživatele přihlašovacími údaji Facebooku, aniž by aplikaci třetí straně tyto přihlašovací údaje poskytla a zároveň řídí přístup aplikace třetí strany pouze na ty údaje, které chce uživatel přes službu „Login with Facebook" sdílet.

OAuth umožňuje poskytnout v případě služeb pod PSD2 třetí straně přístup ke klientským datům, aniž by klient musel poskytnout třetí straně přihlašovací údaje (například uživatelské jméno a heslo do svého bankovnictví) ke službě. Aplikace třetí strany může přistupovat k datům klienta (například údaje o transakční historii), pokud jí k tomu dá klient explicitní souhlas, což je v případě PSD2 2faktorové ověření. Klientská aplikace se také dostane pouze k takové podmnožině dat, ke které dostala výše udělený explicitní souhlas. [15]

Samotná komunikace aplikace třetí strany s autentizačním serverem vypadá podobně jako v případě protokolu OpenID. Uživatel je přesměrován na webovou stránku ve správě poskytovatele služby ověření identity, kam zadává své přihlašovací údaje. Oproti protokolu OpenID je zde ale uživatel dotázán, jaké údaje chce aplikaci třetí strany poskytnout. Uživatel tedy může schválit přístup aplikace třetí strany ke svým datům, anebo zamítnout. Následně je přesměrován zpět do aplikace třetí strany. [16]

U protokolu OAuth je vždy klientská aplikace svázána s autentizačním serverem poskytovatele identity. Pokud autentizace proběhla úspěšně, autentizační server předává aplikaci třetí strany client_id, secret a autentizační kód.

Technicky je řešení OAuth vystavěno na výměně kódů mezi aplikací třetí strany a webovou službou tzv. code grant:



Obrázek 4 - OAuth 2.0 komunikace [16]

1. Aplikace třetí strany přesměrovává uživatele do webové aplikace poskytovatele identity s požadavkem pro autentizaci uživatele
2. Probíhá autentizace uživatele zcela v režii poskytovatele identity
3. Pokud autentizace proběhla úspěšně, autentizační server vystavuje autentizační kód a přesměrovává uživatele zpátky do aplikace třetí strany
4. Aplikace třetí strany zasílá požadavek na autentizační server pro výměnu získaného autentizačního kódu za dlouhodobý refresh token. Během dotazu se aplikace třetí strany identifikuje svým client_id a client_secret.
5. Aplikace třetí strany si ukládá refresh token
6. Aplikace třetí strany žádá získání krátkodobého access tokenu za refresh token
7. Autentizační server validuje, zda refresh token je stále platný pro dané client_id a pokud ano, vydává aplikaci třetí strany access token
8. Krátkodobý access tokenu aplikace třetí strany využívá pro komunikaci s API webové službou [15]

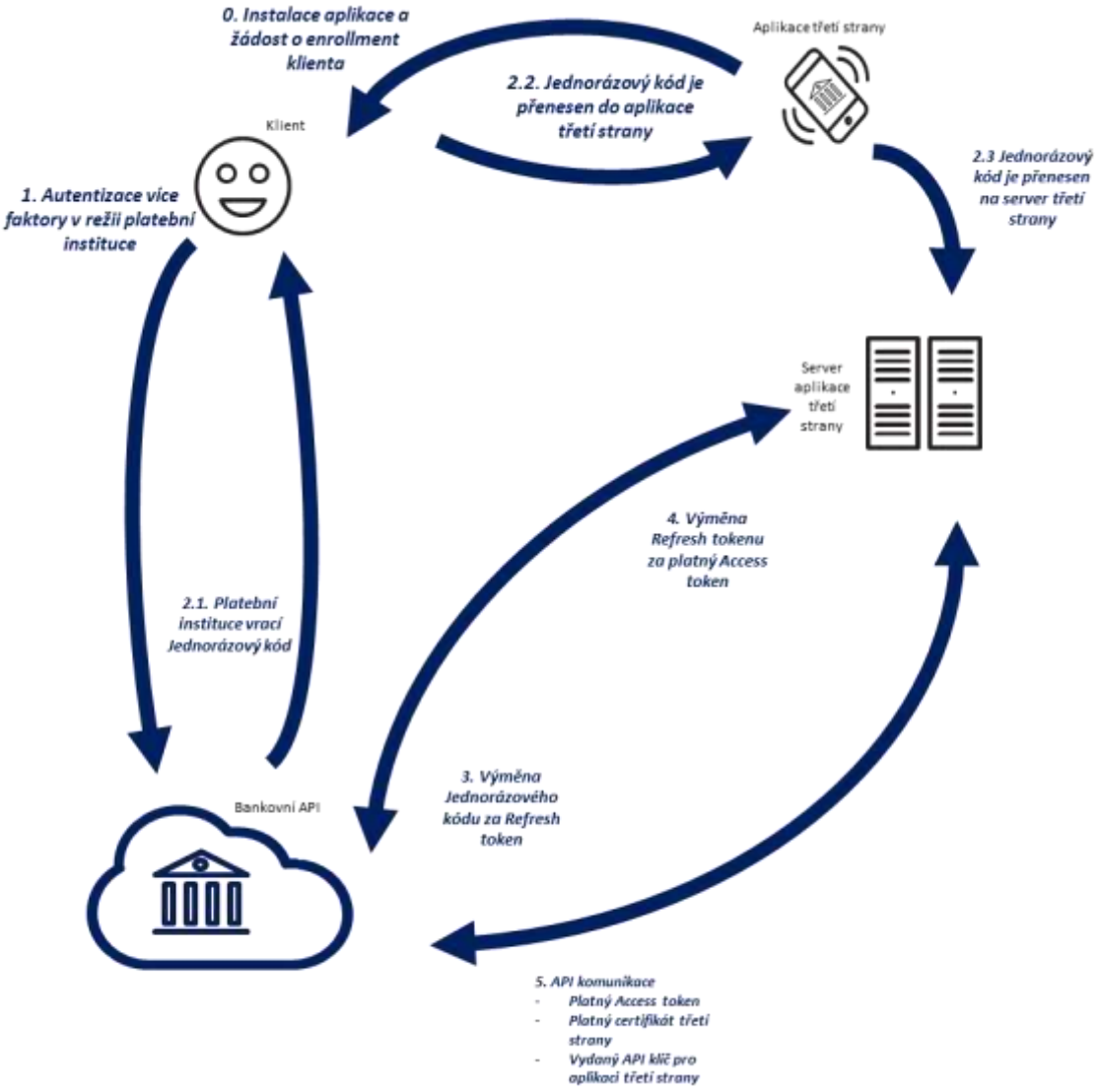
5.3.5 Enrollment klienta do aplikace třetí strany pod OAuth 2.0 protokolem

Standard ČOBS se také zabývá procesem enrollmenu platebního účtu banky do aplikace třetí strany. Celý proces enrollmentu popsaný níže, ale i další komunikace aplikace třetí strany s API banky je zabezpečená standardem OAuth 2.0 a vychází z otevřeného standardu OpenID.

Proces má 0-6 kroků:

0. Klient banky iniciuje přidání produktu do aplikace třetí strany;
1. Banka ověří klientovu totožnost prostřednictvím svého autentizačního; procesu, který je např. federovaný, tzn. v režimu každé banky
   Klient banky dává souhlas, jaké účty/ konkrétní data chce poskytnout třetí straně
2. Banka generuje jednorázový kód, který předává aplikaci třetí strany;
3. Aplikace třetí strany si vyměňuje jednorázový kód za tzv. refresh token, který je unikátní pro daného klienta a konkrétní třetí stranu;
4. Pro samotnou komunikaci aplikace třetí strany s bankou musí mít aplikace třetí strany vydaný platný access token, aplikace třetí strany vyměňuje refresh token za access token;
5. Aplikace třetí strany komunikuje s bankou s platným access tokenem a svým certifikátem třetí strany, který získala od ČNB. [15]

Proces začíná tzv. nultým krokem, krokem, kdy uživatel instaluje a používá aplikaci třetí strany a do kterého banka vůbec nevstupuje.



Obrázek 5 - Proces enrollmentu [15]

Refresh token je dlouhodobě vydaný token (vydaný až na 90 dní dle RTS), který získává aplikace třetí strany na základě jednorázového kódu. Pro samotnou komunikaci s bankou potřebuje aplikace třetí strany access token, který má krátkou dobu expirace (např. 3600s). Platný access token slouží k autorizaci konkrétního requestu na API banky. Jakmile access token expiruje, může aplikace třetí strany využít refresh token a získat tak access token nový. [15]

Banka tedy v procesu enrollmentu a využívání služeb banky v aplikaci třetí strany vystavuje jednotlivé resource pro vydání:

- jednorázového kódu,
- refresh tokenu a
- access tokenu. [15]

Třetí strana v procesu iniciuje napojení služeb banky vyžádáním si dlouhodobého refresh tokenu, který během komunikace s bankou mění za krátkodobý access token.

Jak banka, tak aplikace třetí strany musí umožnit klientovi vydané přístupy revokovat, tedy zrušit přístup třetí strany ke službám banky pro konkrétního klienta. [11]

6 Možnosti využití PSD2 API v prostředí online převzetí identifikace klienta

První část práce popisovala, jak se mění svět online plateb v prostředí nové směrnice PSD2, jaké nové povinnosti směrnice platebním institucím ukládá.

Ve druhé části byly popsány zásady převzetí identifikace v prostředí zákona proti praní špinavých peněz tzv. AML. Zásady prvního ověření klienta v digitálním světě, které musí povinné osoby dodržovat. Jasným závěrem této kapitoly bylo, že pro klienty je dnes obtížné prokázat svou totožnost online bez nutnosti návštěvy kamenné pobočky povinné osoby, a zároveň pro banky je obtížné celý proces klientovi E2E zprocesovat.

Poslední část práce se již zabývá konkrétní oportunitou využití směrnice PSD2 v procesu online převzetí identifikace na konkrétním procesu online zřízení platebního účtu.

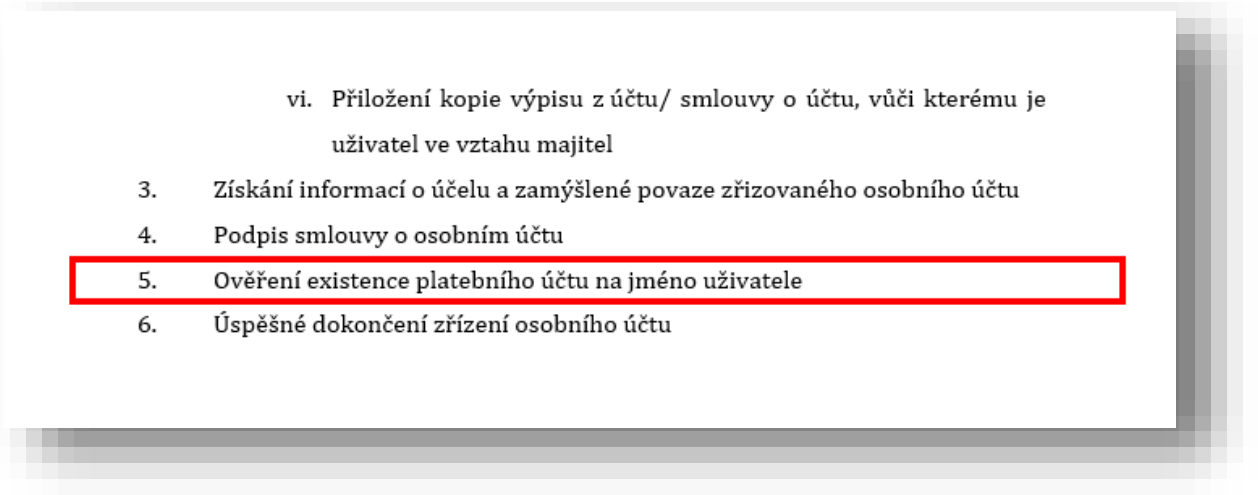
Návrh praktického začlenění konkrétního API do procesu online identifikace vychází z Českého standardu pro Open Banking.

6.1 Převzetí identifikace jako jeden spojitý proces

Identifikace skutečného majitele účtu u původní finanční instituce je nejsložitější částí procesu KYC („Know your customer“).

Zákon 253/2008 Sb. ověřuje identitu žadatele o produkt u finanční instituce tak, že žadatel v procesu prokáže své vlastnické spojení s účtem vedeným u původní finanční instituce, která již uživatele jednou fyzicky ověřila. Žadatel toto spojení prokazuje právě:

- Doložením kopie dokladu potvrzující existenci účtu u jiné finanční instituce na jeho jméno;
- Provedením iniciační platby na svůj nově zřizovaný účet.



Obrázek 6 - Ověření existence účtu

Právě služba pro nepřímé dání platebního příkazu umožní žadateli provést platbu přímo v nákupním procesu, aniž by se musel žadatel sám přihlašovat do internetového bankovnictví, vyplnit platební příkaz a zaslat ho bance.

6.1.1 Aplikace služby nepřímého dání platebního příkazu v procesu převzetí identifikace u finanční instituce

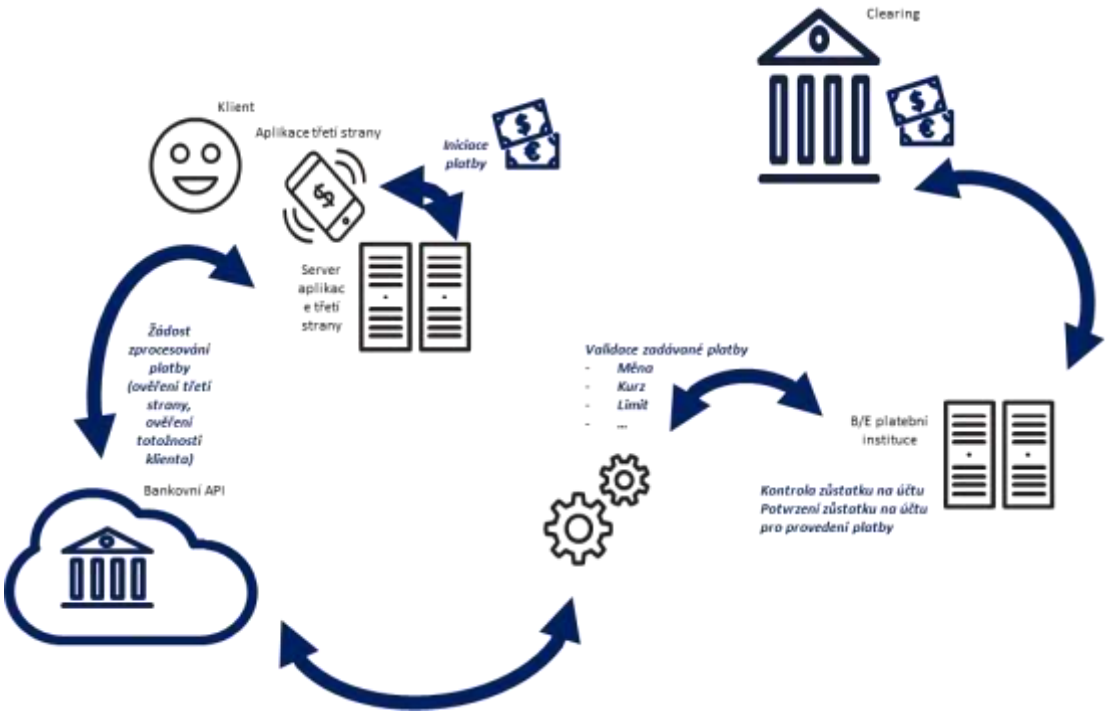
Služba nepřímého dání platebního příkazu umožňuje nahradit krok, kdy žadatel opouští nákupní proces, aby zadal a provedl platbu.

Aplikace služby nepřímého dání platebního příkazu

1. PISP vybízí uživatele, aby vyplnil povinné údaje o iniciační platbě:

a. Částku;
b. Číslo účtu příjemce;
c. Typ platby (domácí/ zahraniční v rámci EHP/ zahraniční mimo EHP/ SEPA);
d. Měnu; [7]

2. PISP zasílá požadavek pro iniciaci platby, která vyžaduje
   a. Autorizaci uživatele;
   b. Použití kvalifikovaného certifikátu třetí strany;
3. ASPSP požaduje po uživateli autorizaci platby na základě 2FA ověření totožnosti iniciátora platby;
4. Uživatel autorizuje platbu;
5. ASPSP odesílá informaci PISP o stavu autorizace platby;
6. PISP zobrazí uživateli informaci o úspěšně provedené platbě. [15]



Obrázek 7 - Iniciace platby [15]

U služby iniciace platby přibyl jeden krok, a to je samotná autorizace platby, kterou si implementují samy banky. Autorizace může být řešena přesměrováním klienta z aplikace třetí strany na URL federované autorizační stránky platební instituce. Dalším řešením je autorizace platby řešená přímo v aplikaci třetí strany bez dalšího

přesměrovávání, a to tak, že platební instituce zasílá uživateli jedinečný jednorázový kód na jeho mobilní telefonní číslo, který uživatel zadává do aplikace třetí strany. Aplikace třetí strany následně odesílá kód zpět platební instituce, která ho validuje.

6.1.2 Výhody aplikace služby nepřímého dání platebního příkazu v procesu převzetí identifikace

Právě využití služby nepřímého dání platebního příkazu přináší možnost:

- Iniciovat platbu přímo v prostředí nákupního procesu;
- Nenutit klienta opustit nákupní proces;
- Vyplnit platební příkaz za žadatele, žadatel zadává pouze číslo účtu u původní finanční instituce;
- Silně ověřit totožnost žadatele 2FA metodou.

6.1.3 Nevýhody aplikace služby nepřímého dání platebního příkazu v procesu převzetí identifikace

Platební instituce nemají povinnost zasílat třetí straně informaci o stavu platby, informaci, kterou dnes musí povinně poskytovat, je, že platba byla přijata ke zpracování, či nikoliv.

Může se ale stát, že banka přijme platbu ke zpracování, ale v mezidobí mezi požadavkem na zpracování, kdy je ověřena informace o dostatečném zůstatku na účtu, a samotných zpracování dojde k vypořádání jiných plateb (např. platba na cizí účet zadaná v pátek večer po uzavření clearingu bude zpracovávána až v další pracovní den), a platba nakonec nebude vypořádána, protože zůstatek se za tu dobu snížil a již nestačí pro pokrytí transakce. Třetí strana si musí tedy sama řídit dotazování se na stav přijaté platby.

6.2 Rychlejší a pohodlnější proces převzetí identifikace

Zákon AML požaduje od žadatele v procesu vzdáleného převzetí identifikace doložit doklad identifikující skutečného majitele účtu u jiné finanční instituce, která již uživatele dříve fyzicky ověřila.

Doklad je v procesu většinou reprezentován

- Výpisem z bankovního účtu, anebo
- Smlouvou o osobním účtu.

Získání a přiložení kopie dokladu je pro spoustu uživatelů časově náročné. Uživatel ve většině případů musí opustit nákupní proces, aby se přihlásil do svého internetového bankovnictví, kde kopii dokladu musí stáhnout do svého PC a přiložit zpět do procesu, kam se musí znovu přihlásit.

I pokud uživatel provede všechny kroky správně, kopie dokladu může být nepoužitelná, protože nebude obsahovat bankou vyžadovaná povinná pole, či je doklad zcela strojově nebo lidsky nečitelný.

Bance tento krok přináší překážku v digitalizaci, kdy pokud chce banka nákupní proces plně automatizovat, musí investovat do technologie optického rozpoznávání textu, což může být značně náročné, protože co banka, to jiný formát výpisů, který se také v čase neustále mění. V opačném případě musí banka zaměstnávat fyzickou osobu, která bude jednotlivé výpisy rozpoznávat a verifikovat dokument jako:

- Dokument je čitelný a podařilo se identifikovat skutečného majitele,
- Dokument je čitelný, ale nepodařilo se identifikovat skutečného majitele,
- Dokument je nečitelný.

Právě krok nákupního procesu pro přiložení dokladu, viz výše, může být nahrazen službou informování o platebním účtu, což je popsáno v nadcházející kapitole.

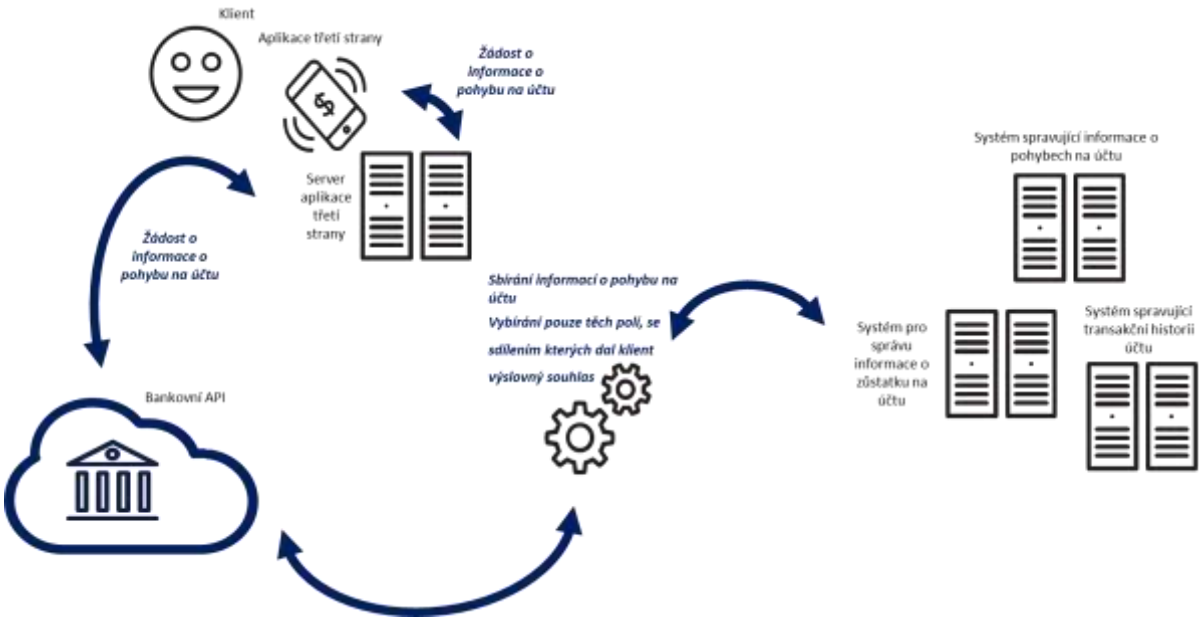
6.2.1 Využití služeb informování o platebním účtu v procesu převzetí identifikace

Doklad identifikující skutečného majitele účtu, o kterém mluví zákon 253/2008 Sb., by mohl být v procesu nahrazen službou informování o platebním účtu. Služba stejně jako doklad umožní získat informace o účtu klienta banky, samozřejmě s jeho

výslovným souhlasem, který je představován 2FA potvrzením. Třetí strana tak získá nejen informaci o tom, že platební účet skutečně existuje, ale také, že daný žadatel vlastní k účtu silné autorizační přístupy.

Aplikace služby informování o platebním účtu

1. PISP vybízí uživatele, aby vybral ze seznamu svou původní banku, u které je na jeho jméno zřízen platební účet;
2. Uživatel zvolí bankovní instituci;
3. PISP zasílá požadavek pro získání informací o účtu, který vyžaduje:
   a. Autorizaci uživatele;
   b. Použití kvalifikovaného certifikátu třetí strany;
4. ASPSP požaduje po uživateli autorizaci dotazu na základě dvou faktorových ověření totožnosti iniciátora platby;
5. Uživatel autorizuje dotaz;
6. ASPSP vybízí uživatele, aby vybral informace, které chce s třetí stranou sdílet;
7. Uživatel vybírá set informací, které chce poskytnout třetí straně;
8. ASPSP odesílá informace PISP;
9. PISP zobrazí uživateli informaci o úspěšně provedeném dotazu. [15]



Obrázek 8 - Získání informace o účtu [15]

Díky službě informování o účtu aplikace třetí strany metodou GET získává seznam platebních účtů klienta, zůstatek na účtu či přehled transakcí k danému účtu.

6.2.2 Výhody využití služeb informování o účtu v procesu převzetí identifikace

Právě využití služby informování o účtu přináší možnost získat výpis z účtu bez nutnosti dokládat jeho analogovou verzi do procesu:

- Nenutit klienta opustit nákupní proces;
- Nenutit klienta získat výpis z účtu příp. smlouvu o účtu a přiložit ji do procesu;
- Silně ověřit existenci a informace o účtu 2FA metodou.

6.2.3 Nevýhody využití služeb informování o účtu v procesu převzetí identifikace

Jednou z hlavních nevýhod takto získaného výpisu je skutečnost, že banky se společně dohodly, že nebudou v rámci transakční historie k účtu poskytovat také informaci o majiteli účtu, tedy žádnou informaci, která by mohla danou transakci s majitelem účtu spojit. Jedná se o zásadní nedostatek z pohledu ověření, že daný výpis patří právě k osobě a platebnímu účtu, u kterého si chceme potvrdit majitele.

7 Shrnutí výsledků

Práce se zabývala právní problematikou povinnostmi identifikace klienta online v prostředí platebních institucí. Pro modelaci aktuálního procesu online identifikace jsme vycházeli ze zákona 253/2008 Sb. o AML, kde jsou jasně stanovená pravidla a vymezený postup, jak má první identifikace klienta probíhat, a ze zkušenosti na českém a slovenském trhu platebních služeb, kde banky první identifikaci uživatele online též nabízejí.

Konkrétně povinnostmi provádění identifikace online se zabývala kapitola 3, jejímž závěrem byla analýza procesu a identifikace jeho slabých míst:

- Uživatel musí min dvakrát opustit nákupní proces;
- Uživatel nemá okamžitou zpětnou vazbu, že nahraný dokument je čitelný a použitelný jako doklad identifikující majitele platebního účtu;
- Uživatel nemá okamžitou zpětnou vazbu, že byla úspěšně provedena platba;
- Uživatel musí žádat o výpis z účtu, příp. smlouvu o účtu a doložit dokument v procesu, což značně prodlužuje proces a zřízení účtu online se tak stává uživatelsky nepřívětivý.

Práce přiblížila dále problematiku nové platební směrnice a navazujících technických směrnic a standardů, které přináší především nové povinnosti pro platební instituce otevřít bankovní data a práva konzumovat je pro vlastníky aplikací licencovaných třetích stran.

Aplikace služby nepřímého dání platebního příkazu a informování o platebním účtu vycházející ze směrnice PSD2 vstupuje do nákupního procesu zřízení běžného účtu online takto:

1. Modelace osobního účtu;
2. Výběr formy uzavření smlouvy na osobní účet;
    a. Uživatel vlastní digitální identitu, díky které ho banka autentizuje a vlastní autorizační metodu, kterou může elektronicky podepsat smlouvu na produkt;
        i. Validace digitální identity uživatele;

b. Uživatel nevlastní digitální identitu;
    i. Zadání základních osobních údajů uživatele
        - Jméno, příjmení;
        - Státní občanství;
        - Rodné číslo / datum narození;
        - Místo narození;
        - Pohlaví;
    ii. Zadání trvalé adresy uživatele;
    iii. Přiložení kopie přední a zadní strany dokladu totožnosti, který obsahuje:
        - Druh a číslo průkazu totožnosti;
        - Stát, popřípadě orgán, který doklad vydal;
        - Dobu platnosti;
    iv. Přiložení kopie přední strany podpůrného dokladu totožnosti, který obsahuje:
        - Druh a číslo průkazu totožnosti;
        - Stát, popřípadě orgán, který doklad vydal;
        - Dobu platnosti;
    v. Online získání informace o účtu prostřednictvím služby informování o účtu;

3. Získání informací o účelu a zamýšlené povaze zřizovaného osobního účtu;
4. Podpis smlouvy o osobním účtu;
5. Provedení iniciační platby na nový účet žadatele z jeho původního účtu prostřednictvím služby nepřímého dání platebního příkazu.

Výsledek aplikace služby nepřímého dání platebního příkazu a informování o účtu přináší uživateli:

- Uživatel nemusí opouštět nákupní proces, všechny kroky procesu dokončuje na jednom místě;
- Uživatel nemusí shánět kopii výpisu z účtu či smlouvy o účtu, zaslání jednotlivých informací o účtu potvrzuje online přímo v procesu;
- Uživatel má okamžitou informaci, zda banka získala všechny potřebné informace o účtu rovnou v procesu online;
- Uživatel má okamžitou informaci, zda byla přijata platba pro zpracování rovnou v procesu online.

Výsledek aplikace služby nepřímého dání platebního příkazu a informování o účtu přináší bance:

- Banka nemusí složitě implementovat nákladově i znalostně náročnou technologii OCR pro rozpoznávání textu dokumentů;
- Banka má okamžitou informaci o úspěšné či neúspěšné identifikaci žadatele o účet;
- Banka má okamžitou informaci o tom, zda byla autorizována platba a bez nutnosti dodatečného souhlasu žadatele o účet může zjistit, zda platba byla provedena;
- Banka nemusí složitě na back office párovat příchozí transakce na účet s číslem účtu odesílatele, u něhož potřebujeme identifikovat, že je majitelem účtu.

Využití služeb nepřímého dání platebního příkazu a informování o účtu může zrychlit proces až v řádu několika hodin až dnů, pokud odpadne nutnost manuálně na back office banky porovnávat kopie dokladů potvrzující existenci účtu na jméno žadatele a zároveň povinnost žadatele tyto kopie získat a doložit.

Současně dnes banky připravují řešení instantních plateb, kdy platby mezi účty různých bank budou zprocesované v řádu několika vteřin, ne dnů, jako je tomu dnes. Banky tedy umožní zadávat okamžité platby celých 24 hodin denně, 7 dnů v týdnu, 365 dnů v roce. Okamžité platby by dle vyjádření ČNB měly být implementovány ke konci

roku 2018 a jejich řešení by mělo být zahrnuto do standardu ČOBS. Nevýhodou této služby pro klienty bude zpoplatnění této služby. [14]

8 Závěry a doporučení

Dle predikce společnosti Deloitte povede stále větší tlak na otevřenost a dostupnost klientských dat platebních institucí ke vzniku netradičních finančně technologických řešení a online tržišť, kde dnes tradiční banky budou s nově příchozími hráči navzájem bojovat o kontakt se svými klienty.

Jednou z možností, jak uspět na nově se formujícím trhu finančních služeb, je využít také příležitosti spojené s otevřeným bankovnictvím, vyjít vstříc potřebám stávajících i potenciálních klientů, a zachovat si tak s nimi primární vztah.

Tato práce měla za cíl najít příležitost, jak tlak na otevřenost dat ve formě nové směrnice o platebních službách přináší platebním institucím možnost, jak zrychlit a zjednodušit proces online ověření identity klienta jiné banky dle AML, a umožnit mu tak dokončit E2E online nákupní proces finančního produktu bez návštěvy pobočky.

Vycházeli jsme z toho, že dnešní stav vzdáleného ověření identity klienta jiné banky může trvat min 2-3 pracovní dny. Proces dnes nutí klienta opustit nákupní flow a složitě prokazovat, že je vlastníkem účtu u jiné finanční instituce, která již jeho fyzické ověření v minulosti jednou provedla.

Právě možnost využití služeb nepřímého udělení platebního příkazu a informování o platebním účtu přímo v procesu identifikace a ověření totožnosti klienta dle AML a jejich aplikace na slabá místa procesu potvrdily možný směr, jak finanční instituce mohou využít služby pro urychlení celého procesu identifikace a tím také online nákupního procesu svých bankovních produktů.

Zrychlení spočívá v jednoduchém využití služby nepřímého udělení platebního příkazu přímo v nákupním procesu, kdy dle AML musí povinná osoba ověřit, že žadatel je majitelem účtu a tedy byl již jednou fyzicky ověřen u původní banky. Žadatel už nemusí opouštět nákupní proces a zadávat první platbu z bankovnictví původní banky, ale v nákupním procesu pouze metodou, kterou již dnes ve své původní bance autorizuje platby, potvrdí platbu přímo v nákupním procesu.

Ještě k zajímavějšímu využití služeb PSD2 v procesu identifikace je aplikace služby informování o účtu, kde místo doložení kopie dokladu stvrzující, že žadatel je majitelem daného účtu, si banka vzdáleně vyžádá přes službu informování o účtu

informace od původní banky online, a žadatel jako v předchozím kroku potvrdí vydání těchto informací metodou, kterou již dnes ve své původní bance autorizuje platby či jiné operace vyžadující silnou autentizaci. Banky dnes ale nechtějí spolu s informací o účtu sdělovat informaci o majiteli daného účtu

Aplikace služeb směrnice PSD2 přináší nejen zjednodušení a obrovské zrychlení procesu identifikace klienta, ale také zvýšení bezpečnosti, kdy k platební operaci, ale i k vydání informací o účtu prokazuje majitel účtu svou totožnost dvěma na sobě nezávislými bezpečnostními faktory. Již nestačí pro zadání platby prolomit heslo, vždy jeden faktor doplňuje faktor druhý - otisk prstu na bezpečném zařízení ve vlastnictví klienta, hlas spojený s nadiktováním PINu, heslo spolu s jednorázovým kódem v SMS, klientský certifikát spolu se 4místným PINem, verifikace obličeje kombinovaná s dalším faktorem, ať už potvrzujícím, že něco mám, nebo něco znám.

Diplomová práce našla příležitost využití služeb PSD2 v procesu identifikace, kde vzniká výhoda na obou stranách nabídky i poptávky – banka může rychle, bezpečně a jednoduše nabízet svůj účet či jiný finanční produkt spadající pod AML povinnosti identifikace, a zároveň klient může díky jednoduchému mapování nově vznikajících cenových srovnávačů služeb bank přecházet mezi účty, aniž by musel navštívit pobočku, anebo složitě vyplňovat žádost online a čekat 2-3 dny, než bude moci využívat svůj nový účet, nebo načerpat úvěr.

Tento rok banky umožní svým klientům zadávat okamžité platby, kdy platba bude připsána na účet vedený u jiné banky za pár vteřin a tato služba bude dostupná 24hodin denně 7 dní týdnu a 365 dní v roce. To umožní zrychlení procesu identifikace z hodin na vteřiny, stále zde ale zůstává překážka, kdy potenciální klient musí být majitelem účtu u jiné banky a v nákupním procesu zasílat ověřovací platby.

Diplomová práce vycházela z aktuální legislativní situace na českém bankovním trhu. Evropská i česká legislativa se dnes ale připravuje na další velký krok z pohledu otevřenosti a dostupnosti veřejných služeb a veřejných dat, známé pod zkratkou eIDAS. Nařízení přináší nový standard pro elektronickou identifikaci, elektronické podpisy a další možnosti elektronické autentizace. Nařízení je přejaté do české legislativy pod zákonem č. 250/2017 Sb. o elektronické identifikaci a zákonem č. 297/2016 o službách vytvářející důvěru pro elektronické transakce a umožní úplně

jiný přístup k ověření totožnosti uživatele. Aby byl uživatel plně fyzicky AML ověřen a mohl se tak bez omezení pohybovat v digitálním světě finančních ale i veřejných služeb, prokáže se identifikačním prostředkem, který si bude moci zřídit u jakéhokoliv kvalifikovaného poskytovatele identifikačních služeb. Takovým prostředkem bude nový elektronický občanský průkaz vydávaný od léta 2018.

Budoucnost vzdáleného ověřování totožnosti pravděpodobně už nebude ve fyzické návštěvě pobočky, ani v zasílání plateb mezi původní a novou finanční institucí. Každý občan EU bude mít do pár let jeden elektronický průkaz totožnosti, kterým prokáže svou identitu jak ve fyzickém světě (banky, úřady, atd.), tak vzdáleně ve světě digitálních služeb. Už žádné zasílání ověřovací platby a vytváření kopií dokladů totožnosti, pouze vyplnění jednoduchého formuláře a použití elektronického identifikátoru, což může vypadat tak, že uživatel připojí kartu ke svému počítači a zadá ověřovací PIN, či pouze otiskem prstu potvrdí svou totožnost ve své bezpečnostní aplikaci. Identifikace a ověření totožnosti bude jednou záležitostí pár vteřin.

Ač směřování bankovnictví i veřejného sektoru v oblast vzdálené identifikace jde pravděpodobně jiným směrem než je zasílání ověřovacích plateb mezi bankami, směrnice PSD2 umožňuje nečekat na den, kdy všichni občané EU budou mít po ruce svůj elektronický občanský průkaz či jiný identifikační prostředek (což může trvat ještě několik let), a již dnes urychlit celý proces a získat tak na nově se formujícím konkurenčním trhu otevřených bankovních dat důležitou konkurenční výhodu.

9 Seznam použité literatury

[1] BAIN & COMPANY. Bain retail bank study finds most lag in digital services customers want, face threat of disruption, obsolescence: Bain & Company. *Bain & Company* [online]. 15.7.2014 [cit. 2018-04-11]. Dostupné z: http://www.bain.com/about/press/press-releases/retail-bank-of-the-future-2014-press-release.aspx

[2] ČESKÁ REPUBLIKA. 253. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. In: *Sbírka zákonů*. Praha: Tiskárna Ministerstva vnitra, 2008, ročník 2008, částka 80.

[3] MBank: mKonto. *MBank* [online]. [cit. 2018-04-19]. Dostupné z: https://www.mbank.cz/osobni/ucty/mkonto/

[4] Osobní účet - Slovenská sporiteľňa: Osobní účet. *Slovenská sporiteľňa* [online]. [cit. 2018-04-19]. Dostupné z: https://www.slsp.sk/sk/ludia/ucty/osobny-ucet3

[5] MůjÚčet. *Komerční banka* [online]. [cit. 2018-04-19]. Dostupné z: https://www.kb.cz/cs/obcane/ucty/pro-dospele/mujucet

[6] EUROPEAN BANKING AUTHORITY. *THE EUROPEAN BANKING AUTHORITY AT A GLANCE* [online]. Luxembourg: Publications Office of the European Union, 2016 [cit. 2018-04-09]. ISBN 978-92-95086-80-7. Dostupné z: http://www.eba.europa.eu/documents/10180/1401372/EBA+AT+A+GLANCE.pdf/e8686db2-6390-4c52-ad06-bc8d24b7aeb5

[7] *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES*. In: . Štrasburku: Úřední věstník Evropské unie, 2015. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32015L2366

[8] ČESKÁ REPUBLIKA. 370 Zákon o platebním styku. In: *Sbírka zákonů*. Praha: Tiskárna Ministerstva vnitra, 2017, ročník 2017, částka 129.

[9] JENNINGS, Mike, Vincent SANTAMARIA, Martin VURM a Radoslav RATKOVSKÝ. *PSD2 v kostce* [online]. Září 2016 [cit. 2018-04-09]. Dostupné z: https://www.pwc.com/cz/cs/bankovnictvi/assets/psd2-v-kostce-n02-cz.pdf

[10] ČESKÁ NÁRODNÍ BANKA. Seznamy a evidence. *Česká národní banka* [online]. [cit. 2018-04-09]. Dostupné z: http://www.cnb.cz/cs/dohled_financni_trh/seznamy/index.html

[11] *NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU): kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace*. In:Brusel, 2017, číslo 389.

[12] ČBA. SDĚLENÍ ČBA K PŘECHODNÉMU OBDOBÍ PSD 2 A NOVÉHO ZÁKONA O PLATEBNÍM STYKU. *Česká bankovní asociace* [online]. 10. 01. 2018 [cit. 2018-04-

11]. Dostupné z: https://www.czech-ba.cz/cs/sdeleni-cba-k-prechodnemu-obdobi-psd-2-noveho-zakona-o-platebnim-styku

[13] ČBA. O ČBA. *Česká bankovní asociace* [online]. [cit. 2018-04-11]. Dostupné z: https://www.czech-ba.cz/cs/o-cba

[14]ZEMAN, Marek. Rok 2018 by měl být ve znamení okamžitých plateb. *Česká národní banka* [online]. 22.12.2017 [cit. 2018-04-09]. Dostupné z: http://www.cnb.cz/cs/verejnost/pro_media/tiskove_zpravy_cnb/2017/20171222_okamzite_platby.html

[15] MICHALÍK, Petr. *Standardy bankovních aktivit: Česká standard pro Open Banking* [online]. ČBA, 1.12.2017 [cit. 2018-04-11]. Dostupné z: file:///C:/Users/cen83684/Documents/ceskystandardproopenbankingv021.pdf

[16] PLAŠIL, Matouš. *Autentizace uživatelů webových služeb* [online]. Brno, 2013 [cit. 2018-04-21]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=68026. Bakalářská práce. Vysoké učení technické v Brně. Vedoucí práce Doc. Ing. KAREL BURDA, CSc.

[17] MASSÉ, Mark. *REST API Design Rulebook: Designing Consistent RESTful Web Service Interfaces*. Sebastopol: O'Reilly Media, 2011. ISBN 1449319904.

10 Seznam obrázků

11 Zadání práce

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2017/2018

Studijní program: Systémové inženýrství a informatika
Forma: Kombinovaná
Obor/komb.: Informační management (im2-k)

Podklad pro zadání DIPLOMOVÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Bc. Kvapilová Kateřina	Leoše Janáčka 729, Lázně Bohdaneč	I15500764

TÉMA ČESKY:

Možnosti bankovních API pro online převzetí identifikace v prostředí PSD2 regulace

TÉMA ANGLICKY:

Non client identification in PSD2 environment

VEDOUCÍ PRÁCE:

Ing. Pavel Čech, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem diplomové práce je návrh řešení s oporou v legislativě, jak zjednodušit a zrychlit dnešní proces online identifikace nového klienta banky, který byl jednou fyzicky ověřen jinou finanční instituci.

Osnova práce:

1) Úvod
2) Cíl práce
3) Převzetí identifikace
4) Nová směrnice Evropského parlamentu a Rady Evropské unie o platebních službách
5) Technický standard pro silnou autentizaci a bezpečnou komunikaci
6) Standardizace komunikace pomocí API
7) Český standard pro Open Banking
8) Možnost využití PSD2 služeb v procesu online identifikace
9) Shrnutí výsledků
10) Závěry a doporučení
11) Seznam použité literatury
12) Seznam obrázků
13) zadání práce

SEZNAM DOPORUČENÉ LITERATURY:

1) ČESKÁ REPUBLIKA. 253. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. In: Sbírka zákonů. Praha: Tiskárna Ministerstva vnitra, 2008, ročník 2008, částka 80.
2) SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES. In: . Štrasburku: Úřední věstník Evropské unie, 2015. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32015L2366
3) ČESKÁ REPUBLIKA. 370 Zákon o platebním styku. In: Sbírka zákonů. Praha: Tiskárna Ministerstva vnitra, 2017, ročník 2017, částka 129.
4) NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU): kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace. In:Brusel, 2017, číslo 389.

Podpis studenta: ..... Datum: 26.4.2018

Podpis vedoucího práce: ..... Datum: .....