Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky


# Porovnání bankovní digitální identity a self-sovereign digitální identity

BAKALÁŘSKÁ PRÁCE

Studijní program: Aplikovaná informatika

Studijní obor: Aplikovaná informatika

Autor: David Karlík

Vedoucí bakalářské práce: Ing. Jan Kučera, Ph.D.

Praha, červen 2021

***Prohlášení***

Prohlašuji, že jsem bakalářskou práci „Porovnání bankovní digitální identity a self-sovereign digitální identity“ vypracoval samostatně za použití v práci uvedených pramenů a literatury.

V Praze dne 1. června 2021

David Karlík

***Poděkování***

Tímto bych chtěl velmi poděkovat panu Ing. Janu Kučerovi, Ph.D. za velkou trpělivost a cenné rady při vedení mé práce.

### *Abstrakt*

Práce se zaměřuje na porovnání přístupů k digitální identitě známých jako self-sovereign identity a bankovní identita. Cílem práce je v první řadě stanovit kritéria vhodná k porovnání systémů digitální identity a následně realizovat samotné srovnání. Protože se především v případě self-sovereign identity jednotlivá řešení ještě stále velmi liší a je tím pádem složité vytvořit generalizovaný model, který by správně vystihoval přístup jako celek, bylo pro umožnění dosažení cílů práce srovnání omezeno na srovnání dvou konkrétních řešení reprezentující oba přístupy – BankID a Sovrin. Jako kritéria použita ke srovnání jsou primárně zvoleny tzv. Laws of Identity bývalého architekta společnosti Microsoft Kima Camerona. Srovnány jsou také jednotlivé architektury řešení.



### *Klíčová slova*

Digitální identita, self-sovereign identita, bankovní identita, Sovrin, BankID

### *Abstract*

This paper focuses on a comparison of approaches to digital identity known as self-sovereign identity and banking identity (also known as BankID). The aim of the thesis is first to establish criteria suitable for comparing digital identity systems and then to present the comparison itself. Since, especially in the case of self-sovereign identity, the individual systems are still very different and it is therefore difficult to create a generalized model that correctly describes the approach as a whole, to enable the achievement of the objectives of the thesis, the comparison was limited to a comparison of two specific systems representing both approaches – BankID and Sovrin. The criteria used for comparison are primarily the so-called Laws of Identity by former Microsoft digital architect Kim Cameron. Individual solution architectures are also compared.



### *Keywords*

Digital identity, self-sovereign identity, banking identity, BankID, Sovrin

# Obsah

**OBSAH** ..... **6**

**ÚVOD** ..... **8**

**2 METODY A ZPŮSOB DOSAŽENÍ CÍLE** ..... **10**

2.1 POSTUP ŘEŠENÍ PRÁCE ..... 10

**3 REŠERŠE** ..... **11**

3.1 VYHLEDÁVAČE VYUŽITÉ K REŠERŠI ..... 13
3.2 KLÍČOVÁ SLOVA PRO VYHLEDÁVÁNÍ LITERATURY ..... 13
3.3 KRITÉRIA PRO VÝBĚR LITERATURY ..... 14

**4 PŘEDSTAVENÍ POJMŮ** ..... **16**

4.1 IDENTITA ..... 17
4.2 DIGITÁLNÍ IDENTITA ..... 17
4.3 ENTITA ..... 18
4.4 ATRIBUT ..... 18
4.5 IDENTIFIKÁTOR ..... 19
4.7 DOMÉNA ..... 19
4.8 IDENTITY MANAGEMENT (IDM) ..... 19
4.9 IDENTITY MANAGEMENT SYSTÉM (IMS) ..... 20
4.10 BLOCKCHAIN A DLT ..... 20

**5 PŘÍSTUPY K ŘEŠENÍ DIGITÁLNÍ IDENTITY** ..... **21**

5.1 MODELY SYSTÉMŮ DIGITÁLNÍ IDENTITY ..... 21
*5.1.1 Izolovaný model* ..... *22*
*5.1.2 Centralizovaný model* ..... *23*
*5.1.3 Federativní model* ..... *24*
*5.1.4 User-centric model* ..... *25*
5.2 STANDARDY DIGITÁLNÍ IDENTITY ..... 26
*5.2.1 SAML 2.0* ..... *26*
*5.2.2 OAuth 2.0* ..... *26*
*5.2.3 OpenID Connect* ..... *26*
5.3 SHRNUTÍ ..... 27

**6 BANKOVNÍ IDENTITA A SELF-SOVEREIGN IDENTITY** ..... **27**

6.1 BANKOVNÍ IDENTITA ..... 27
6.2 SELF-SOVEREIGN IDENTITY ..... 28
6.3 SHRNUTÍ ..... 29

**7 PŘÍSTUP KE SROVNÁNÍ** ..... **29**

7.1 STANOVENÍ KRITÉRIÍ PRO SROVNÁNÍ ..... 31
*7.1.1 Srovnání podle Laws of Identity* ..... *31*
*7.1.2 Srovnání architektury řešení a použitých technologií* ..... *32*
7.2 VÝBĚR ŘEŠENÍ PRO SROVNÁNÍ ..... 33
7.3 SHRNUTÍ ..... 33

**8 ANALÝZA ŘEŠENÍ** ..... **33**

8.1 BANKID ..... 34
*Architektura řešení* ..... *34*
*Laws of Identity* ..... *35*
8.2 SOVRIN ..... 37

*Architektura řešení* ..... *37*
*Laws of Identity* ..... *39*

**9 SROVNÁNÍ A DISKUSE** ..... **41**

9.1 SROVNÁNÍ ARCHITEKTURY ..... 41
9.2 SROVNÁNÍ DLE LAWS OF IDENTITY ..... 42
9.3 DISKUSE ..... 44
9.4 POTENCIÁL PRO DALŠÍ PRÁCE ..... 44

**POUŽITÁ LITERATURA** ..... **46**

# Úvod

Tato práce se zabývá srovnáním dvou přístupů k digitální identitě, a to tzv. self-sovereign identity a bankovní identity. Motivací k tomu zabývat se digitální identitou je neustále rostoucí důležitost digitálního prostředí ve vztahu k prostředí fyzickému ve všech oblastech našeho života. Jeden ze základů ekonomického, finančního a sociálního pokroku v jakémkoliv prostředí je schopnost člověka prokázat, že je opravdu tím, za koho se vydává (1) a vzhledem k tomu, že se čím dál víc interakcí v našich životech přesouvá do digitálního prostředí je zřejmé, že téma digitální identity, tedy identity v digitálním prostředí, nabírá a stále bude nabírat na důležitosti.

Je možné také zaznamenat snahu a potřebu napříč různými obory pro využití systému digitální identity jako náhrady tradiční fyzické identity. Publikace Světového ekonomického fóra, věnující se zapojení finančních institucí do řešení digitální identity, uvádí, že absence vhodného řešení digitální identity znemožňuje fintech inovátorům přinášet bezpečné, efektivní a digitální inovace na poli fintech řešení. Stejně tak uvádí, že nutnost tradičních finančních institucí spoléhat se na prostředky fyzické identity je příčinou neefektivnosti a chybovosti procesů při poskytování běžných finančních produktů a služeb. Digitální identita má tedy dle Světového ekonomického fóra obrovský potenciál nejen tyto základní procesy finančních služeb zlepšit, ale také přinést nové příležitosti v oboru. (2)

Zajímavé, a podtrhující důležitost tématu digitální identity je dle mého také zjištění analýzy společnosti McKinsey, že správně zavedená digitální identita by se do roku 2030 mohla podílet na tvorbě ekonomické hodnoty odpovídající až 13 % HDP jednotlivých zemí. Stejně tak dle této analýzy může digitální identita výrazně přispět ke vzniku hodnot neekonomického charakteru, které nelze změřit kvantitativní analýzou, jako je inkluze občanů, ochrana práv, lepší přístup ke vzdělání, zdravotní péči a na trh práce. (3)

Výrazným impulzem ve vývoji řešení digitální identity může dle mého názoru být i současná pandemie Covid-19.

Zpráva britské technologické organizace TechUK zmiňuje, že bezpečný, důvěryhodný a interoperabilní systém digitální identity bude kritický pro obnovení ekonomiky po následcích krize a může být důležitý i v samotném boji proti pandemii. Konkrétním případem využití digitální identity v případě boje proti viru může být efektivnější trasování kontaktů, případně vázání certifikátu imunity, který dle autorů bude třeba v budoucnosti vyžívat, na digitální identitu člověka. (4) Příležitostí pro využiti digitální identity při vypořádávání se s následky pandemie může být potřeba efektivního a rychlého cílení vládní pomoci na lidi postižené pandemií. Takové systémy na národní úrovní se už osvědčily například v Chile, Thajsku, nebo Indii.(5)

Spokojíme-li se pro tento úvod s jednoduchou slovníkovou definicí identity, tedy, že identita člověka znamená jeho stejnost, skutečnost, že je sám sebou a nikým jiným, můžeme říct, že identita každého člověka jen jedna.(6)

V kontrastu s tím můžeme být svědky běžné situace na internetu, kdy má člověk několik odlišných digitálních identit ve formě přihlašovacích údajů a profilů na různých webových službách, ať už se

jedná o účty na internetových diskusních fórech, internetových obchodech, nebo sociálních sítích. Je však důležité upozornit, že existují desítky různých definicí identity a celý koncept identity je neustále diskutován napříč obory jako je psychologie a sociologie, proto při hlubším srovnávání pojmu identity a digitální identity by bylo třeba definici stanovit přesněji.

Ve fyzickém prostředí je většinou standardizováno prokazování identity na základě dokumentů vydaných univerzálně uznávanou autoritou – státem, jako je občanský průkaz, řidičský průkaz, nebo zkrátka fyzickými charakteristikami při osobním jednání. Ať už si zakládáme nový účet v bance, vyřizujeme financování nového vozu, vyřizujeme něco na úřadě, nebo proukazujeme náš věk při nákupu alkoholu v obchodě, stačí nám většinou vždy jen občanský průkaz, dokument vydaný univerzálně uznávanou autoritou, abychom dokázali, kdo jsme a byli obslouženi. V porovnání s tím na internetu chybí všeobecně standardizovaný způsob prokazování identity.

Impulzem k tomu, proč jsem se rozhodl ke srovnání zvolit právě bankovní identitu je to, že jsem téma bankovní identity v roce 2019 a 2020 v českém prostoru začal vnímat čím dál intenzivněji.

Ruku v ruce s tím se začaly objevovat první náznaky snahy zavedení bankovní identity do praxe a také začalo docházet k důležitým legislativním změnám, které vyvrcholily 1. ledna 2021 nabytím účinnosti tzv. zákona o bankovní identitě (č. 49/2020 Sb.). To umožnilo jednotlivým bankám začít zavádět služby bankovní identity pro své klienty, což se taky velmi rychle stalo, a ještě v lednu jsme mohli být svědkem spuštění služeb bankovní identity prvními bankami.(7)

Koncept bankovní identity je sice svým pojetím možné zařadit mezi tradičnější, centralizované, řešení, avšak je možné spatřit snahu v ČR a také napříč jinými zeměmi takové řešení v dnešní době přinášet. Další velkou motivací pro výběr přístupu bankovní identity ke srovnávání je projekt České bankovní asociace, pracovně nazýván jako projekt SONIA. (8)

Na druhé straně důvodem pro výběr self-sovereign identity ke srovnání je nepopíratelný trend v oboru IT prostředí přicházet s decentralizovanými řešeními různých problémů, za využití technologií jako je například blockchain. Příkladem může být velký nárůst popularity decentralizovaných kryptoměn jako je bitcoin, a to i mezi laickou veřejnost.

Přestože je koncept self-sovereign identity poměrně novým pojmem, motivací pro výběr tohoto přístupu je fakt, že je často považován jako nejnovější krok evoluce přístupů k digitální identitě a finální krok k decentralizaci digitální identity a přesunu kontroly nad vlastní digitální identitou do rukou uživatelů. (9) Řada odborníků i organizací jej považuje za potenciální budoucnost přístupů k digitální identitě.

## Cíl práce

Hlavním cílem této práce je **porovnat přístupy k digitální identitě označované jako bankovní identita a self-sovereign identity**. Z důvodů uvedených v části „Omezení práce“ budou pro potřeby naplnění hlavního cíle na základě rešerše zvolený dva konkrétní systémy digitální identity, přičemž jeden bude reprezentovat koncept self sovereign identity a jeden koncept bankovní identity.

Aby mohl být hlavní cíl naplněn, bude nutné nejprve na základě rešerše **vymezit kritéria pro porovnání bankovní identity a self-sovereign identity** (dílčí cil 2). Není mou ambicí v této práci kritéria pro srovnávání sám vymýšlet na zelené louce, ale na základě rešerše literatury a předchozích prací s podobným cílem kritéria najít, analyzovat, vhodně zvolit a případně dle potřeby upravit. Dílčím cílem práce bude také **analyzovat technologická řešení pro bankovní identitu a pro self-sovereign identity** (dílčí cíl 1)**.**

### Omezení práce

Vzhledem k tomu, že je self-sovereign přístup k digitální identitě poměrně novým fenoménem, existuje velké množství jednotlivých systémů od různých autorů, které se svým způsobem řešení někdy i velmi výrazně liší. Bylo by proto dle mého názoru obtížené a pro tuto práci příliš ambiciózní systémy generalizovat do jednoho řešení, tak, aby dávalo smysl, dobře celý koncept vystihovalo a bylo pro srovnávání vhodné.

Z toho důvodu budou pro potřeby srovnání v této práci na základě rešerše a analýzy dostupných řešení zvoleny dvě konkrétní řešení digitální identity – jedno spadající do konceptu bankovní identity, druhé spadající do konceptu self-sovereign identity a ty následně srovnány.

Také považuji za důležité zmínit, že ambicí této práce není v žádném případě postihnout všechny aspekty digitální identity, protože se nepochybně jedná o velmi komplexní, interdisciplinární téma, které je možné zkoumat z mnoha různých úhlů pohledu, ať už se jedná o pohled právní, humanitní, nebo ekonomický.

# 2 Metody a způsob dosažení cíle

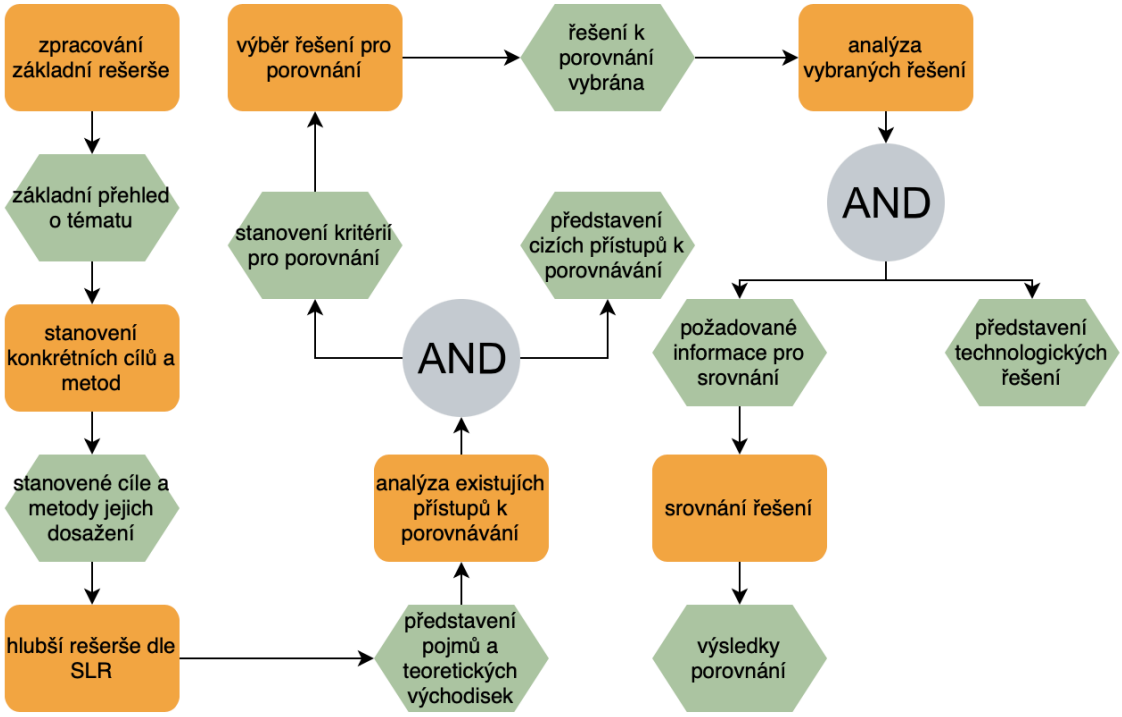
První metodou využitou k dosažení cílů bude rešerše dostupné literatury, elektronických článků, webových stránek a dokumentů dle zásad Systematc Literarature Review, tak jak jej popisuje článek Guidance on Conduction a Systematic Literature Review autorů Yu Xiao a Marie Watson. (10) Vzhledem k povaze a aktuálnosti tématu očekávám, že budou převažovat elektronické zdroje, často i články, které nejsou z odborných publikací, ale například webových stránek autorů jednotlivých řešení. Rešerši je věnovaná kapitola 3.

V návaznosti na rešerši dojde k analýze literatury a v rámci tvorby výstupů této práce k syntéze zjištěných poznatků. Využití syntézy přepokládám především pro potřeby stanovování kritérií ke srovnávání přístupů digitální identity.

V poslední bakalářské práce budou za využití metody srovnávání (komparativní analýzy) srovnány zvolené řešení digitální identity.

## 2.1 Postup řešení práce

Postup řešení práce se pokusím ilustrovat následujícím obrázkem.

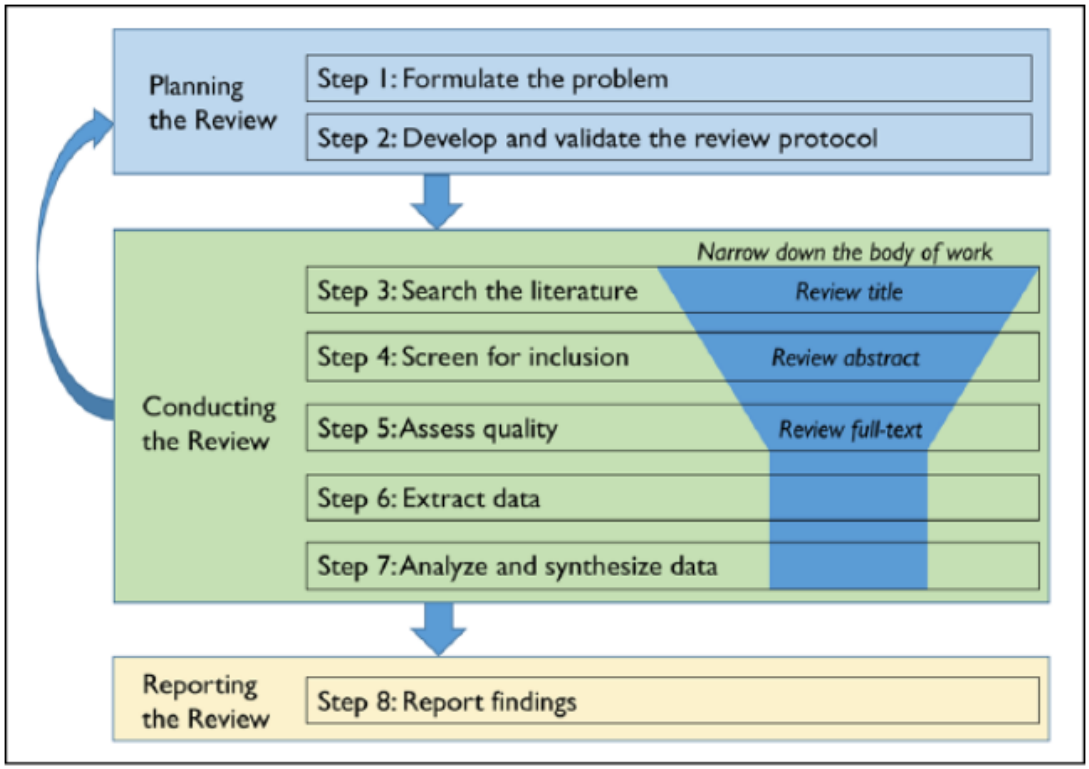



*Obrázek 1 - postup řešení práce, zdroj: autor*

# 3 Rešerše

Jak už bylo zmíněno v předchozí kapitole, při rešerši této bakalářské práci jsem se pokusil postupovat dle zásad procesu Systematic Literature Review, tak, jak je popsaný v článku Guidance on Conduction a Systematic Literature Review autorů Yu Xiao a Marie Watson. (10) Cílem však není postupovat naprosto přesně dle všech instrukcí autorů a využit všech doporučení, ale spíše respektovat základní pravidla a postupy, aby byla zajištěna alespoň elementární kvalita rešerše. Je tomu tak především z toho důvodu, že velmi často autoři pro optimální kvalitu doporučují práci dvou a více výzkumníku na rešerši, což v mém případě není možné.

Jednotlivé kroky procesu rešerše přehledně ilustruje Obrázek 2.




*Obrázek 2 - proces Systematic Literature Review (10)*

Celý proces ve svém článku autoři rozdělují na 3 části, přičemž první část, je určena k plánování rešerše a obsahuje 2 kroky, druhá část je samotné provádění rešerše a obsahuje 5 kroků a poslední část je složena jen z jednoho kroku, kterým je reporting výsledků rešerše.

Prvním krokem Systematic Literature Review je formulovat problém. Ten se v případě této práce shoduje s cíli práce, které byly popsány v úvodu.

Druhým krokem je dle autorů tvorba a validace rešeršního protokolu. Takový protokol by měl popisovat všechny elementy rešerše, včetně účelu studie, výzkumným otázek, kritérií pro výběr literatury, kritérii pro hodnocení kvality literatury, strategií pro získání, syntézu a vyhodnocení dat.

Třetím krokem je samotné vyhledávání literatury za použití vhodně stanovených klíčových slov.

Čtvrtý krok autoři popisují jako hlubší prohledání nalezené literatury. Doporučují se zaměřit na abstrakty prací a stanovit si kritéria na základě kterých zařadit nebo vyřadit jednotlivé práce z předchozího kroku.

Pátým krokem je ohodnocení kvality jednotlivých vybraných prací na základě celého textu. A představuje jakousi poslední šanci danou práci z výběru vyřadit.

U čtvrtého, pátého a šestého kroku autoři doporučují, aby se na něm pro větší kvalitu podíleli minimálně dva lidé. To pro tuto práci ze zřejmých důvodů není možné.

Šestý krok spočívá v získání potřebných informací z vybrané literatury a sedmý v analýze a syntéze daných informací. Posledním krokem je poté report výsledků a celého procesu rešerše tak, jak byl ve skutečnosti proveden.(10)

Při rešerši jsem přistupoval odděleně k vyhledávání obecných informací a podkladů o tématu digitální identity, jednotlivých zkoumaných přístupech (pro potřeby vysvětlení pojmů a stanovení teoretických východisek) a odděleně k pracím zabývajícím se srovnáváním systémů digitální identity, za účelem stanovení kritérií ke srovnání, a tedy naplnění dílčího i hlavního cíle této práce. Šlo mi o to nalézt co nejvíce relevantních prací zabývajících se srovnáním přístupů k digitální identitě, kvůli tomu, abych zjistil, jak k srovnávání přistupovali jiní autoři.

Jak už bylo zmíněno v úvodu, při rešerši jsem upřednostňoval vyhledávání internetových zdrojů, a to z toho důvodu, že se jedná především v případě konceptu self-sovereign identity o poměrně nové, stále zkoumané a rychle se vyvíjející téma.

Ve výjimečných případech, jako například v části věnující se definici identity, jsem využil i mimo oborovou literaturu. V případě definice identity se jedná o knihu Sociální psychologie od profesora Výrosta, doktora Slaměníka a kolektivu.(6)

## 3.1 Vyhledávače využité k rešerši

K rešerši zdrojů k této bakalářské práci jsem využil níže uvedené vyhledávače.

- Vyhledávač Google, k dispozici na adrese www.google.cz
- Vyhledávač Google Scholar, k dispozici na adrese scholar.google.com
- Vyhledávač zdrojů knihovny VŠE, k dispozici na adrese knihovna.vse.cz/zdroje/
- Vyhledávač vysokoškolských kvalifikačních prací Theses, k dispozici na theses.cz

Nejvíce jsem využíval a ocenil vyhledávač Google Scholar a to z důvodu největší relevance výsledků vyhledávání a celkové přehlednosti uživatelského rozhrání.

## 3.2 Klíčová slova pro vyhledávání literatury

V následující sekci stanovím klíčová slova, na základě, kterých budu hledat literaturu pro potřeby naplnění cílů této práce. Pro přehlednost uvedu klíčová slova zvlášť pro nalezení literatury k teoretickým informacím k problematice digitální identity a jednotlivých přístupů a zvlášť pro samotné srovnání a stanovení kritérií ke srovnání.

### Klíčová slova pro rešerši teoretických podkladů

V tomto případě budou využity následná klíčová slova a jejich případné variace.

- Digital identity
- Self-sovereign identity
- BankID
- Digital identity management

Při rešerší informací o bankovní identitě jsem převážně využíval pojem BankID. Jedná se sice původně o název konkrétního řešení bankovní identity ve Švédsku, velmi často se však používá různými autory k označovaní bankovní identity, jakožto obecného konceptu.(11)

Příkladem může být například článek společnosti PwC představující bankovní identitu. (12) Stejně tak se lze s použitím tohoto termínu při označování konceptu bankovní identity setkat v článcích internetových médií informujících o bankovní identitě. (13, 14)

#### Klíčová slova pro rešerši k potřebám naplnění cíle srovnání řešení

Pro tento účel byly stanoveny následující klíčová slova a jejich variace.

- identity management systems comparison
- identity management systems comparative analysis
- self-sovereign identity systems comparison
- BankID systems comparison

## 3.3 Kritéria pro výběr literatury

Jak už bylo zmíněno na začátku této kapitoly, podstatnou roli při hledání literatury za využití zásad Systematic Literature Review je stanovení kritérií, na základě, kterých bude rozhodnuto, zda daná literatura bude pro práci využita.

Kritéria jsem tedy zvolil na základě zaměření, a především cílů práce, tak, aby zvolená literatura bylo pro plnění cílů této práce co nejrelevantnější a nejužitečnější.

#### Kritéria pro výběr literatury pro potřeby stanovení teoretického základu

Kritéria pro akceptaci literatury k využití pro potřeby teoretické části jsem stanovil následující:

- Autor nebo instituce zaštiťující práci musí být kredibilní a jejich kredibilita ověřitelná
- Téma zaměření práce musí být digitální identita
- Práce musí popisovat koncept digitální identity, některý z přístupů k řešení digitální identity, nebo konkrétní systémy digitální identity
- Tvrzení uvedena v práci musí být korektně zdůvodněna
- Celý text práce musí být dostupný on-line

#### Kritéria pro výběr literatury pro potřeby srovnání řešení

Kritéria pro akceptaci literatury k využití pro potřeby srovnání řešení jsem stanovil následující:

- Výstupem práce musí být srovnání dvou nebo více konkrétních řešení digitální identity, nebo stanovení kritérií či rámce k takovému srovnání.
- Musí být popsáno technologické řešení jednotlivých porovnávaných řešení
- Celý text práce musí být dostupný on-line

## 3.4 Komentovaný přehled zdrojů

Jako stavební kámen práce, na základě, které jsem stanovoval a popisoval pojmy v této práci jsem zvolil knihu **Digital Identity, Unmasking Identity Management Architecture (IMA)** autora Phillipa J. Windleyho vydanou v roce 2005. Přestože se jedná o knihu poměrně starou, důvodem, proč jsem ji vybral je, to, že kromě splnění všech mých dříve stanovených kritérií má vysokou míru citovanosti dle Google Scholar (374 citací k 23.2.2021). Autor se sice v práci zaměřuje především na správu digitální identity v kontextu byznysu, institucí a společností, ale také dle mého názoru srozumitelně a přehledně vysvětluje základní koncepty digitální identity, správy digitální identity a některých jednotlivých systému, které už ale díky poměrné zastaralosti díla nemusí být příliš aktuální.(15)

Další kniha, kterou jsem především ke stanovení pojmů využil, je **Digital Identity Management**, na jejíž tvorbě se podílelo více autorů, přičemž editory jsou Maryline Laurent a Samia Bouzefrane. Kniha přehledně a poutavě představuje téma digitální identity, jednotlivé řešení a modely systémů digitální. Přidanou hodnotu práce také vidím v tom, že je kniha prací kolektivu autorů, mezi které nepatří jen IT odborníci, ale i odborníci z jiných oborů, jako je například ekonomie, sociologie, lingvistika a právo a nabízí tím pádem vhled do tématu digitální identity z pohledu jiným vědních oborů. (16) Takové odlišné pohledy sice pro mou práci rozhodně nejsou nutné, protože jak jsem zmiňoval dříve, určitě není mou snahou postihnout všechny aspekty digitální identity, ale jsem přesvědčen, že i pro mnou zkoumané aspekty můžou takové informace z jiných oborů přinést zajímavé obohacení.

Poslední knihu, kterou jsem velmi ocenil je kniha **Solving Identity Management in Modern Applications** autorů Yvonne Wilson a Abhishek Hingnikar. Tato kniha velmi srozumitelně komentuje jednotlivé systémy a přístupy k digitální identitě a jak napovídá podtitul knihy, zaměřuje se především na OAuth 2.0, OpenID Connect a SAML 2.0. Autoři také srozumitelně prezentují modely systému digitální identity. Ocenil jsem vysvětlení problematiky jednoduchým a srozumitelným způsobem. (17)

Jako velmi zajímavý a pro mou práci relevantní jsem shledal konferenční příspěvek **A comparative analysis of Identity Management Systems.** Autoři, kterými jsou Md Sadek Ferdous a Ron Poet, ve svém příspěvku stanovují konkrétní požadavky – kritéria identity management systémů, na základě, kterých poté zvolené identity management systémy srovnávají.

Md Sadek Ferdous je také spoluautorem článku **In Search of Self-Sovereign Identity Leveraging Blockchain Technology.** Tento článek se zaměřuje na problematikou self-sovereign identity a jak jej popisují samotní autoři, klade si za cíl přijít s prvním formálním a rigorózním pohledem na koncept self-sovereign identity za použití matematického modelu. Dle autora totiž v době psaní článku existovalo velmi málo literatury věnující se self-sovereign identitě a ta, která existovala nebyla nikterak metodologická a obsáhlá. Článek velmi dobře a formálně analyzuje dosavadní

definice konceptu self-sovereign identity a stanovuje vlastnosti, které jsou pro self-sovereign identity klíčové. Na základě těchto vlastností poté autor srovnává 4 konkrétní systémy self-sovereign identity, a to uPort, Jolo, Sovrin a Blockcerts. Článek také velmi dobře uvádí terminologii a různé dosud známé modely digitální identity.(18)

Podobné zaměření, tedy srovnání několika konkrétních systémů využívajících konceptu self-sovereign-identity na základě kritérií má také práce Paula Dunphyho a F.A.P. Petitcolase **A First Look at Identity Management Schemes on the Blockchain (19)** a článek Nitina Naika a Paula Jeninske **Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology**. (20)

### 3.5 Shrnutí

Při zkoumání literatury jsem došel k závěrů, že prací se stejným, či podobným cílem, jaký má moje, tedy srovnání konkrétních systému digitální identity je poměrně hodně a téměř vždy splňují základní formální požadavky, jakými jsou stanovení jasných kritérií, na základě, kterých jsou systémy srovnány. V žádném z těchto případu se však neobjevuje jakýkoliv systém bankovní identity a vždy jde o srovnání buď různých systémů na bázi self-sovereign konceptu, nebo systémů založených na jiném konceptu a modelu.

Dle mého názoru se jedná o vhodnou příležitost k tomu, aby moje práce přinesla nové zjištění.

V literatuře zabývající se self-sovereign identitou je velmi často možné se setkat s tvrzením, že toto téma nebylo ještě dostatečně prozkoumáno na odborné úrovni.

# 4 Představení pojmů

V následující kapitole se pokusím představit základní pojmy, které jsou relevantní pro téma digitální identity a následující části této práce. Základem pro výběr představovaných pojmů k této kapitole bude literatura zvolena na základě rešerše. Také byly využity další relevantní zdroje, jako je například mezinárodní standard ISO/IEC 24760-1:2019€ (dále také pouze jako mezinárodní standard ISO, nebo standard ISO). Cílem však není uvést naprosto všechny pojmy týkající se digitální identity, ale pouze ty, které budou dále využité v této práci a je tedy vhodné, aby s nimi byl čtenář seznámen.

Jelikož je naprostá většina zdrojů k tématu v angličtině a tato práce v českém jazyce, budou uvedené definice mnou přeložené. Výjimkou budou názvy obecně používaných termínů, jako je například Identity management system (IdM), které se běžné používají v anglickém znění i v české literatuře a jejich překlad mi nepřijde smysluplný.

## 4.1 Identita

Jak už bylo zmíněno v úvodu této práce, je pojem identita a samotný koncept identity velmi široký a existují desítky různých definic napříč mnoha obory. Stejně tak existuje spousta dimenzí identity, které jsou neustále diskutovány a zkoumány. Při hledání vhodné definice identity jsem prvně nahlédl do knihy Sociální psychologie.(6)

V kapitole 6.1, která se zabývá právě definicí identity, autoři přichází s tvrzením, že „Odborná literatura obsahuje desítky definic identity. Skutečnost, že termín identita znamená a vyjadřuje více jevů, platí i pro psychologii. Existující definice jsou nejen rozmanité, ale i protikladné, takřka vylučující se.“(6) Dále uvádí, že „nejednoznačné používání pojmu znepokojuje mnoho teoretiků identity“ v návaznosti na to parafrázují myšlenku Jamese D. Fearona, který tvrdí, že kvůli tomu, že badatelé napříč různými vědními obory usilují o to, identitu vysvětlit, nebo usilují pomoci identity vysvětlit jiné další jevy, tak pojem sám zůstává záhadou. (21)(6)

Protože pojem identity jako takové nebude pro tuto práci tolik důležitý, a dále v této práci budeme pracovat už především s pojmem digitální identita, tak se definici samotného pojmu identity dále věnovat nebudu. Jednak by to bylo vzhledem k výše uvedeným důvodům příliš složité, ale také pro naše potřeby zbytečné. Dále se proto pokusím věnovat pojmu Digitální identita.

Při rešerši literatury jsem také došel k zjištění, že definici pojmu identity se autoři v literatuře věnující se digitální identitě samostatně příliš nevěnují. Pokud pojem identita autoři používají, je zřejmé, že tím už často mluví o identitě v digitálním prostředí. Často se lze setkat také s tím, že pojmy identita a digitální identita autoři jasně nerozlišují. Příkladem může být právě zmiňovaná kniha autorů Wilson a Hingnikar.(17)

## 4.2 Digitální identita

Phillip J. Windley v části své knihy, věnující se definici digitální identity, digitální identitu popisuje jako něco, co obsahuje data, která jedinečně popisují osobu nebo věc (v jazyku digitální identity subjekt nebo entitu), ale také obsahují informace o vztahu subjektu s jinými entitami.(15)

Jak už bylo zmíněno v komentovaném přehledu zdrojů, autoři knihy Digital identity management, se digitální identitě věnují nejen z pohledu technologického, ale i sociologického a ekonomického.

V části věnující se sociologické dimenzi digitální identity autoři tvrdí, že existují dva odlišné sociologické přístupy vysvětlující digitální identitu. První přístup dle autorů předpokládá, že lidé využívají internetové nástroje k tomu, aby vytvořili svou digitální identitu. Naproti tomu druhý přístup předpokládá, že se lidé na internetu takoví, jakými opravdu v reálném životě jsou, pouze rozhodují o tom, jaké informace budou a nebudou sdílet.(16)

Relevantní pro tuto práci bude však pohled z technologického hlediska, který autoři následně nabízí. Autoři zde stanovují formální definici digitální identity. Digitální identita je dle nich sada digitálních dat, které reprezentují entitu v digitálním virtuálním světě (internet, informační systémy…).

Wilson a Hingnikar ve své knize identitu definují jako soubor atributů asociovaných s osobou nebo entitou v partikulárním kontextu.(17)

Zajímavý a rozšiřující je přístup k definici digitální identity Ferdouse a kolektivu. Ten digitální identitu definuje jako soubor všech částečných identit entity ve všech doménách.(22) Částečnou identitu poté definuje jako soubor atributů entity v jedné doméně. Tato definice Ferdouse je odlišná oproti definicím jiných autorů v zahrnutí pojmu částečné identity do definice. Ostatní autoři tento pojem příliš nevyužívají.

Mezinárodní standard ISO/IEC 24760-1 IT, Security and Privacy — A framework for identity management — Part 1: Terminology and concepts, identitu v kontextu správy digitální identity definuje jako sadu atributů vztahujících se k entitě. (23)

Identitu mohou mít i nelidské entity. Softwarové komponenty sloužící jako agenti, boti, či jiná chytrá zařízení mohou mít identity a mohou komunikovat s jiným softwarem nebo zařízeními způsobem, který vyžaduje ověření a autorizaci stejně jako lidské subjekty.

## 4.3 Entita

Jak popisuje Ferdous ve své práci, entita v kontextu digitální identity je fyzický, nebo logický objekt, který má samostatnou, rozlišitelnou existenci ve fyzickém, nebo logickém smyslu.
V kontextu tématu digitální identity můžou být entitou lidé, organizace, sítě, síťové elementy, software, hardware a webové služby. (24)

Jak popisuje Windley ve své knize, v kontextu digitální identity se entitou myslí osoba, organizace, software, program, stroj, nebo jiná věc, vytvářející požadavky pro přístup ke zdroji. Zdrojem dle Windleyho může být myšlena webová stránka, data v databázi, nebo třeba transakce na kreditní kartě.(15)

V naprosté většině případů lze říct, že každý funkční systém digitální identity obsahuje entity zastupující jednu z těchto rolí, přičemž v některých případech může jedna entita zastávat rolí více (například v případě izolovaného modelu splývá role IdP a SP).

- **Uživatel**: entita, jejíž částečná identita je uložena u IdP a která přistupuje ke službám SP.
- **Identity provider** (IdP, poskytovatel identity): jde o entitu zodpovědnou za ukládání částečné identity uživatele v rámci své domény a její sdílení mezi různými doménami.
- **Service provider** (SP, poskytovatel služby): entita zodpovědná za poskytování služeb uživateli na základě profilu uživatele, který obdržel od IdP.

## 4.4 Atribut

Ferdous popisuje atribut jako distinktivní, měřitelnou, fyzickou nebo abstraktní pojmenovanou vlastnost patřící entitě v dané doméně, jejíž hodnota může určena k identifikaci entity uvnitř dané domény.

Mezinárodní standard ISO/IEC 24760-1 IT atribut definuje jako charakteristiku, nebo vlastnost entity. Taková definice je dle mého názoru srozumitelná a dostatečná pro potřeby této práce.

Identity lidí mohou zahrnovat atributy, jako například jméno, věk, adresa, telefonní číslo, barva očí, nebo pracovní pozice. Nelidské identity mohou zahrnovat atributy, jako je vlastník, IP adresa a případně číslo modelu nebo verze. (17)

## 4.5 Identifikátor

Mezinárodní standard ISO/IEC 24760-1 IT identifikátor definuje jako sadu atributů, které jedinečně charakterizují entitu v doméně. Jako pseudonym poté označujeme identifikátor, který obsahuje minimální informace o identitě, které postačují k tomu, aby jej ověřovatel mohl použít jako odkaz na známou identitu.(23)

Ferdous identifikátor popisuje jako atribut, jehož hodnota může být použita k jedinečné identifikaci entity v rámci domény. (25)

Definice jiných autorů se nesou v podobném duchu a je tedy možné říct, že se autoři shodují na definici identifikátoru, jako atributu, nebo souboru atributů, který je dostatečný pro jednoznačnou identifikaci konkrétní entity v daném prostředí.

E-mailové adresy, čísla pasů, čísla řidičských průkazů a čísla zaměstnanců jsou příklady identifikátorů používaných pro osoby. Nelidské entity, jako jsou agenti, boti nebo zařízení, mohou být identifikovány alfanumerickým řetězcem znaků přiděleným v okamžiku jejich vytvoření nebo registrace v kontextu, ve kterém budou působit. Identifikátory nám umožňují odkazovat na konkrétní osobu nebo nelidskou entitu a pro identity management jsou nezbytné.(17)

V případě identifikátoru osob se můžeme setkat s termínem PII - Personally identifiable information.(26)

## 4.7 Doména

Mezinárodní standard ISO/IEC 24760-1 IT doménu definuje jako prostředí, kde může entita použít sadu atributů pro identifikaci a jiné účely.(23)

Ferdous doménu v kontextu tématu digitální identity definuje jako prostředí, ve kterém entita operuje a operuje. O doméně také mluví jako o kontextu, nebo aplikační doméně.(18)

V kontextu této práce tedy lze říct, že doména je prostředí, kde konkrétně identity systém existuje a funguje. Může se jednat například o internet, podnikovou, nebo jinou síť.

## 4.8 Identity management (IdM)

Mezinárodní standard ISO definuje identity management jako procesy a zásady zapojené do správy životního cyklu, hodnot, typu, nepovinných metadat atributů identit v určité doméně.(23)

Ferdous identity management popisuje jako proces umožňující správu (částečných) online identit. Skládá se z technologií a zásad pro reprezentaci a identifikaci entit jejich (částečnou) identitou a využití takových identit k přístupu k službám v dané doméně.(24)

Windley popisuje digital identity management jako tvorbu, správu, používání a eventuální zničení záznamů, které mohou sloužit k identifikaci entity.

Obecně se lze v literatuře setkat se používáním zkratky IdM. Tato zkratka bude využita i dále v této práci. V české literatuře se lze také setkat s přeloženým pojmem – správa (digitální) identity.

## 4.9 Identity management systém (IMS)

Identity management system, v literatuře často označovaný zkratkou IMS, je dle ISO standardu mechanismus skládající se ze zásad, procedur, technologií a dalších prostředků pro údržbu informací identit včetně asociovaných metadat.(23)

Jednoduchou, ale přitom dle mého názoru dostatečnou definici používá Ferdous. Ten zkrátka Identity management systém popisuje jako systém používaný ke správě identit. Vzhledem k tomu, že správu identit (identity management) jsme si již definovali, tak tuto definici považuji za dostatečnou.

V kontextu této práce lže říct, že pokud je použit termín „digital identity system“, „identity systém“, nebo „identity systém“, je tím v naprosté většině myšlen právě identity management system. S takovým přístupem je možné se setkat i v další odborné literatuře (např. (27)), kdy autoři termínem identity system popisují to, co ISO standard i ostatní autoři termínem identity management system.

V české literatuře se lze setkat jak s používáním anglického termínu identity management system, tak českým termínem systém správy identit.

## 4.10 Blockchain a DLT

Bitcoin, který byl představen v roce 2009, se stal první široce používanou digitální měnou na světě. Jeho technickým základem je mechanismus zvaný Distributed Ledger Technology (DLT, v češtině se lze setkávat s termínem technologie distribuované účetní knihy), známý také jako technologie blockchain.

Přestože se pojmy blockchain a DLT v literatuře často zaměňují, existuje mezi nimi rozdíl, který stojí za to zdůraznit. Jak tvrdí Ferdous, blockchain můžeme chápat jako určitý typ určitého typu ledgeru, v níž mohou být data uložena ve specifickém formátu. Existují i jiné typy ledgerů s různými formáty dat. Pokud je ledger (včetně blockchainu) distribuovaný v síti, lze jej definovat za distribuovaný ledger.(24)

Jak už název napovídá, základem DLT je samotný ledger. Distribuovaný ledger, nebo specificky blockchain je ledger sestávající z po sobě jdoucích bloků řetězených podle přísného souboru pravidel. Tento ledger je distribuován a ukládán uzly fungujících na principu peer to peer, kde je

každý blok vytvářen v předem definovaném intervalu decentralizovaně pomocí **konsenzuálního algoritmu**. Konsensuální algoritmus zaručuje vlastnosti souvisejících s integritou dat uvnitř ledgeru.

V praxi existují potom dva různé druhy, respektive dva různé způsoby nasazení blockchainu. Na základě těchto způsobu existují dva převládající typy ledgerů– veřejný a soukromý.

Veřejný blockchain, označovaný termínem **permisionless blockchain** (do češtiny přeložitelné jako blockchain bez povolení), umožňuje komukoli vytvářet a ověřovat bloky a také měnit stav ledgeru ukládáním a aktualizací dat prostřednictvím transakcí mezi zúčastněnými subjekty. Díky tomu je stav ledgeru a jeho transakce spolu s uloženými daty transparentní a přístupný všem. To může však vyvolávat obavy o ochranu soukromí v určitých kontextech, kde je třeba zachovat soukromí těchto dat, jako je třeba kontext digitální identity.

Soukromý blockchain, známý také jako **permissioned blockchain** (do češtiny přeložitelné jako blockchain s povolením), může být na rozdíl od svého veřejného protějšku omezen v tom smyslu, že se aktivit v rámci ledgeru mohou účastnit pouze autorizované a důvěryhodné subjekty. Tím, že se na činnostech v rámci ledgeru mohou podílet pouze oprávněné subjekty, může být zajištěno soukromí dat ledgeru, což může být v například v případu správy identity a jiných citlivých dat žádoucí.(24)

# 5 Přístupy k řešení digitální identity

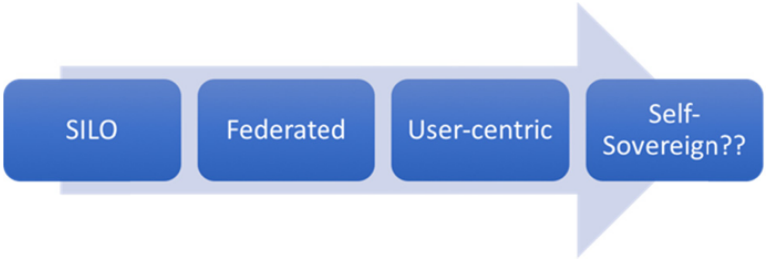
Smyslem této kapitoly je stručně prezentovat přehled existujících technologických řešení pro digitální identitu. To za tím cílem, aby byl vytvořen teoretický základ pro část práce věnující se architektuře jednotlivých řešení.

## 5.1 Modely systémů digitální identity

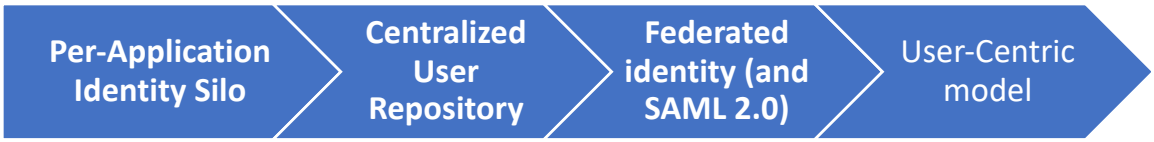
Na základě rešerše je možné říct, že v literatuře věnující se digitální identitě a správě digitální identity je možné najít styčný prvek v kategorizování přístupů k řešení digitální identity na základě modelů systémů digitální identity. Autoři se také veskrze shodují na tom, že systémy digitální identity procházely za dobu své existence určitou evolucí. Právě jednotlivé kroky této evoluce jsou dány odlišnými modely systémů digitální identity. Modely jde chápat jako jakési logické seskupení jednotlivých entit systému (respektive jejich typů) a jejich vzájemných vztahů.

To, jaké modely a v jakém pořadí autoři v popisu evoluce uvádí, se z velké části shoduje, a dle mého nejlépe je vystihující popis od Laurent a kolektivu.(16) Na základě něj budou modely popsány.

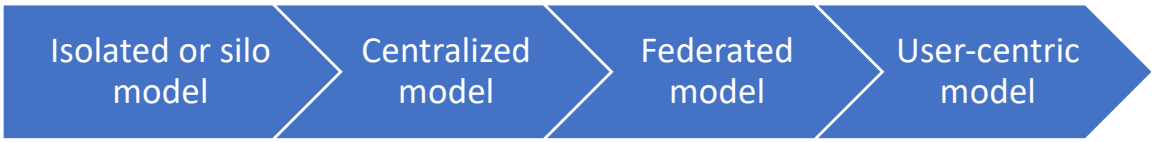
Informace o modelech byly čerpány z dvou knih a prací Ferdouse a kolektivu, tak, jak byly vybrány na základě rešerše.




Obrázek 3 - evoluce digitální idenity dle Ferdouse et al., převzato z:(24)




Obrázek 4 - evoluce digitální identity dle Hingnikar a Wilson, zdroj: (17), obrázek vytvořen autorem




Obrázek 5 - evoluce digitální identity dle Laurent et al. (16), obrázek vytvořen autorem

### 5.1.1 Izolovaný model

Izolovaný model představuje jakýsi původní, nejjednodušší přístup k řešení správy digitální identity. V tomto modelu musí uživatel spravovat tolik identifikátorů (například hesel), kolik je poskytovatelů služeb. Atributy spojené s každým identifikátorem jsou spravovány izolovaně každým SP.

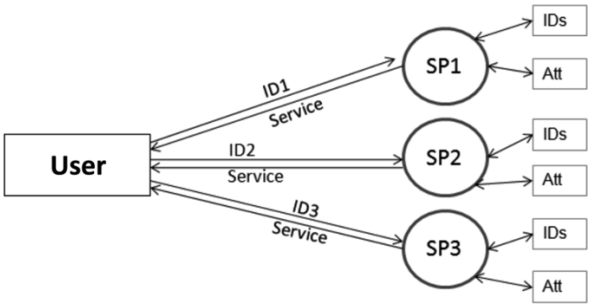
Bohužel i v dnešní době se lze setkat s velkým množstvím služeb, a tedy i uživatelů, které tento model využívají. Příkladem mohou být různé internetové služby, jakými jsou emaily, sociální sítě,

internetové obchody, kam se uživatelé velmi často přihlašují pouze svým uživatelským jménem (případně emailem) a heslem.

Nevýhodou tohoto modelu je velký počet přihlašovacích údajů, které si musí uživatel zapamatovat. Existuje tedy značné riziko, že si uživatel zvolí stejná přihlašovací jména a hesla pro několik svých účtů, což výrazně snižuje úroveň zabezpečení. V takové situaci se můžou stávat situace, kdy útočník napadne poskytovatele služeb, o němž ví, že je zranitelný, aby získal přístupové údaje, které poté použije k přístupu k několika uživatelským účtům umístěným na robustnějších webech.(16)

Důvodem, proč se tento způsob stále těší poměrně velké popularitě může dle mého názoru být právě jednoduchost využití pro koncového uživatele, kdy od něj není vyžadováno zkrátka nic jiného než si zapamatovat, případně zapsat na papírek, uživatelské jméno a heslo. To bohužel aniž by si uvědomoval dříve zmíněna velká rizika.

Izolovaný model ilustruje obrázek 6 od Laurent a koletivu. Lze vidět, že uživatel musí každému poskytovateli služeb předávat identifikátor (například přihlašovací údaje), který je specifický právě pro tohoto poskytovatele služeb. Jednotliví poskytovatelé služeb poté uchovávají atributy a identifikátory (respektive celé identity) uživatelů ve vlastních databázích nebo uložištích.




Obrázek 6 - izolovaný model – převzato z (16)

### 5.1.2 Centralizovaný model

Následný krok evoluce systémů digitální identity se vyznačuje existencí entity, která zastává roli IdP (Identity provider, poskytovatel identity). IdP v tomto případě funguje jako společný, centralizovaný repositář identit uživatelů.

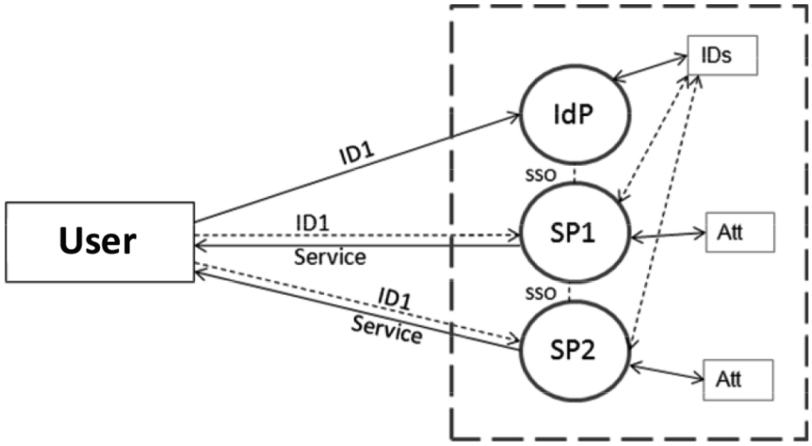
Uživatel se tak může u SP autentizovat stejnou identitou – stejnými údaji (identifikátory), a to bez nutnosti opakovat autentizaci pro každý další SP, jeho služby chce uživatel využívat. Laurent a kolektiv v tomto případě hovoří o tzv. Single Sign On (SSO), protože jediná autentizace u „centralizovaného“ IdP poskytuje přístup ke všem SP závislým na stejném IdP. Jako jednoduché open-source softwarové řešení tohoto modelu je možné uvést OpenAM. (16, 28)

Zranitelnost centralizovaného modelu spočívá v tom, že prozrazení jednoho identifikátoru s přidruženými údaji (za předpokladu, že jsou statické) stačí k tomu, aby byl najednou poskytnut neoprávněný přístup ke všem službám ve stejné doméně. Navíc centralizovaný aspekt tohoto modelu jej nečiní vhodným pro velký počet uživatelů nebo SP.

Windley ve své knize tvrdí, že představy, že centralizovaný přístup podpoří bezpečnost, úsporu nákladů nebo zjednodušení správy, se v praxi ukázaly jako nepravdivé. Zásadní problém

centralizovaných systémů digitálních identit vidí v jejich neschopnosti škálování. Vztahy identit mají ze své podstaty strukturu podobnou sítě, zatímco centralizované technologie, jako jsou adresáře, jsou hierarchické. Každá osoba může mít vztahy k mnoha dalším osobám, organizacím, aplikacím a službám. Každé prostředí, jako například podnik, se musí potýkat s mnoha sadami překrývajících se a často se měnících vztahů identit.(15)

Obrázek 5 ilustruje architekturu centralizovaného modelu.




Obrázek 7 - centralizovaný model – převzato z (16)

### 5.1.3 Federativní model

Federativní model představuje jakýsi přirozený vývoj centralizovaného modelu. Jak už název napovídám, podstatou tohoto modelu je existence tzv. federace. Federace v kontextu digitální identity znamená jakési sdružení více domén, respektive jednotlivých IdP a SP existujících v různých doménách.

Naprosto klíčový je v rámci této federace koncept důvěry. Pro to, aby mohla fungující federace existovat, musí si zkrátka její aktéři vzájemně důvěřovat. V praxi se může jednat o jednotlivé organizace, které mezi sebou (například na základě smluvních dohod) takovou důvěru vytváří. Součástí takové dohody může být kromě zavedení důvěry například stanovení technologických standardů, které usnadňují komunikaci mezi jednotlivými entitami a doménami. Pro označení vzájemné důvěry se v literatuře lze setkat s pojmem kruh důvěry (CoT, Circle of Trust).(16)

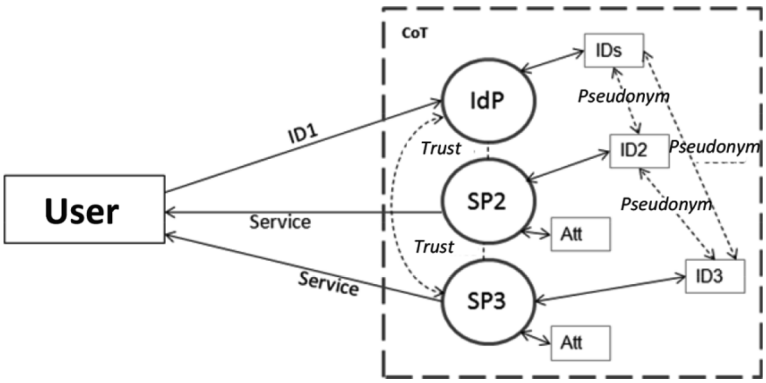
Windley ve své knize popisuje 5 základních komponent důvěry v kontextu federace identit. Dá se tedy i říct, že se jedná o 5 základních prvků, které je nutné stanovit pro fungující federace digitální identity.(15)

- Řízení, které popisuje pravidla fungování, role a odpovědnosti a právní platnost politiky.
- Osoby nebo jiné subjekty zapojené do vztahů důvěry.
- Procesy pro provádění operací a transakcí.

– Technologické nástroje, včetně softwaru a hardwaru.

– Funkční ekonomický model

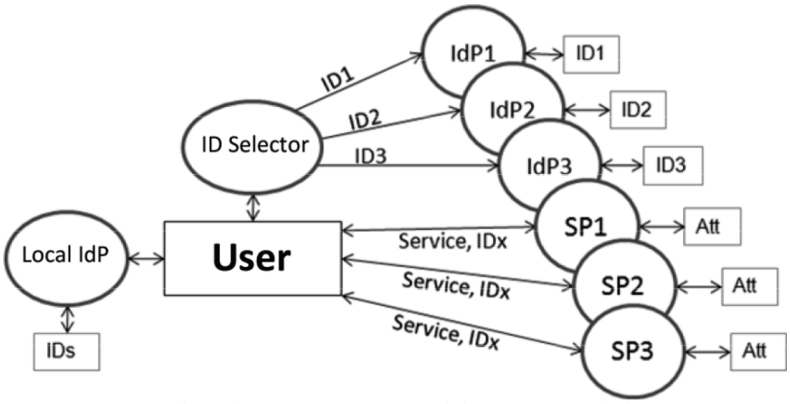
Stejně jako v případě centralizovaném modelu, tak i zde může být implementováno SSO tak, aby se uživatel mohl jednorázově autentizovat u IdP a získat tak přístup ke službám SP, které jsou součástí CoT. Na druhé straně je pak uživatel, který přistupuje k SP, odkazován SP pomocí pseudonymu. Ve skutečnosti se všechny výměny mezi SP a IdP, které se týkají uživatele, uskutečňují na základě těchto pseudonymů. Stejně tak předává uživatel IdP a SP své atributy a identifikátor a je nucen důvěřovat v to, že budou respektovat jeho soukromí.(16)




Obrázek 8 - federativní model – převzato z (16)

### 5.1.4 User-centric model

User-centric model dle Laurent a kolektivu poprvé nabídl uživateli plnou kontrolu nad svými vlastními atributy. Uživatel má ze svého zařízení, a to buď lokálně, nebo vzdáleně, u zvoleného IdP k dispozici portfolio svých digitálních identit. Na žádost SP, ke kterým přistupuje, si může vybrat identitu a rozhodnout, zda chtějí vydat určité atributy. Specifikem tohoto modelu je, že SP jednají samostatně a mohou nabízet vzájemně propojené služby. SP se dle Laurent stále častěji přiklánějí k tomu, aby navrhovali autentizaci uživatele s tím, že mu ponechají rozhodnutí o výběru IdP. (16)
S tím se můžeme dnes v praxi setkat nejčastěji při přihlašování k různým internetovým službám, e-hopům a podobně, které nabízejí přihlášení skrze vícero IdP, jako je Facebook, Google, Apple apod.




*Obrázek 9 – user-centric model – převzato z (16)*

## 5.2 Standardy digitální identity

Smyslem této části bude představit vybrané technologické standardy, na základě, kterých jsou systémy digitální identity založený. Cílem není samoúčelně popsat všechny dostupné standardy, ale především ty, které jsou využity v srovnávaných systémech.

### 5.2.1 SAML 2.0

Standard SAML 2.0 (Security Assertion Markup Language) byl standardizován v roce 2005 organizací OASIS. Definuje strukturu založenou na XML, která umožňuje výměnu autentizačních a autorizačních dat a atributů mezi IdP a SP, přičemž tato struktura může být sama o sobě zabezpečena protokolem SOAP, který může implementovat mechanismy šifrování a elektronického podpisu. Protokol SAML je velmi flexibilní, pokud jde o obsah výměny mezi IdP, SP a uživatelem, a identifikuje různé vzory výměny ve formě profilů (například SSO webového prohlížeče, Single Logout, Basic Attribute Profile).(16)

SAML 2.0 je modulární standard a skládá ze sady komponent, které definují, jak si aktéři mohou vyměňovat identity.(16) Jelikož je SAML 2.0 možné považovat za jeden z nejrozšířenější standardů, je zajimavé si všimnout, že komponenty protokolu z velké části korespondují s komponenty modelů.

Hlavními komponentami standardu SAML 2.0 dle Laurent a kolektivu jsou

- poskytovatel identity (IdP): komponenta spravující ověřování uživatelů a šíření identity uživatelů

- poskytovatel služeb (SP): komponenta delegující ověřování uživatelů na IdP a požadující identitu uživatele od IdP.

- assertion – token předávaný mezi IdP a SP ve formátu XML obsahující samotnou identitu (16)

### 5.2.2 OAuth 2.0

OAuth 2.0 je protokol, který umožňuje uživateli autorizovat jednu aplikaci, známou jako **klient (client),** aby jeho jménem odeslala požadavek na rozhraní API, známé jako server zdrojů **(resource server)** a získala data vlastněná uživatelem ze serveru zdrojů Za tímto účelem aplikace komunikuje s autorizačním serverem **(authorization server)**, který následně ověřuje uživatele v rámci získání jeho souhlasu s přístupem aplikace k jeho datům. Aplikace poté obdrží token, který jí následně umožní volat server zdrojů jménem uživatele. (16)

Naprosto typicky se s využitím protokolu OAuth 2.0 můžeme v praxi setkat při přihlašování se do internetových účtu skrze účty u služeb třetích stran, jako je Facebook, Google apod.

### 5.2.3 OpenID Connect

OpenID Connect můžeme chápat jako rozšíření protokolu OAuth 2.0, které jej rozšiřuje především o možnost snazší možnost autentizace.

I když jsou autorizační servery OAuth 2.0 schopny autentizovat uživatele, OAuth 2.0 neposkytuje standardní způsob, jak bezpečně předat identitu ověřeného uživatele aplikaci. Protokol OpenID Connect právě toto zajišťuje. OIDC byl navržen jako vrstva nad protokolem OAuth 2.0, která aplikacím poskytuje informace o identitě ověřeného uživatele ve standardizovaném formátu. To poskytuje aplikacím řešení pro autentizaci uživatelů, ale i autorizaci skrze API. (16)

## 5.3 Shrnutí

Způsobů, jak kategorizovat přístupy k řešení digitální identity je zajisté velká řada, ale v tomto případě bylo na základě rešerše literatury představeno dělení na 4 známé modely systémů digitální identity. Následně byly také prezentovány relevantní technologické standardy pro fungování takových systémů.

# 6 Bankovní identita a Self-sovereign identity

Následující kapitola je věnována definici a popisu konceptu bankovní identity a self-sovereign.

## 6.1 Bankovní identita

Pro pochopení toho, co vlastně bankovní identita je, jsem přistoupil ke zkoumání toho, jak samotné organizace zainteresované do provozování systémů bankovní identity bankovní identitu definují. Protože se dá říct, že téma bankovní identity je v současné době v české republice velké téma a velké množství bank, pod záštitou asociací, s takovým řešením přichází, nabízí se možnost hledat definici právě u těchto subjektů.

Níže bude uvedena definice třech největších bank (ČSOB, Česká spořitelna, Komerční Banka), které uvádí na svých webových stránkách v sekci věnující se bankovní identitě. Seznam zapojených bank, včetně odkazu na část webové stránku dané banky věnující se digitální identity nabízí webová stránka České bankovní asociace (29, 30).

### Česká spořitelna

Česká spořitelna webovou stránku věnovanou bankovní identitě má a jedna z prvních informací na dané webové stránce je odpověď na otázku, co bankovní identita je.

Dle České spořitelny bankovní je bankovní identita *„Jednoduchý a bezpečný způsob pro přihlašování a ověřování totožnosti na internetu.“* (31)

### ČSOB

ČSOB webovou stránku věnovanou stránku bankovní identity má. ČSOB bankovní identitu prezentuje pod názvem ČSOB Identita. V části „Časté otázky & odpovědi“ se lze setkat s dle mého názoru kvalitní a formální definicí bankovní identity.

*„Bankovní identitou se obecně rozumí digitální identita, kterou vydává některá z bank. Při splnění zákonných podmínek ji klient může využívat k ověřování své totožnosti v digitálním prostředí, a to vůči různým firmám či státu.“*(32)

### Komerční Banka

Komerční banka webovou stránku věnovanou bankovní identitě má a bankovní identitu popisuje následovně.

*„Jeden způsob pro ověření totožnosti a přihlašování do banky pro potvrzování plateb, pro veřejnou správu a komerční poskytovatele digitálních služeb.“(33)*

Nejvýstižnější je dle mého názoru definice banky ČSOB, proto takovou definici budu považovat za dostatečnou.

Důležitým faktorem fungování bankovní identity je také vysoká důvěra lidí vůči bankám jako institucím. Dá se předpokládat, že pokud lidé důvěřuji bankám ve správě svých peněz, budou tak stejně činit i v případě informací.

## 6.2 Self-sovereign identity

Koncept self-sovereign identity (SSI) spočívá v tom, že každý uživatel má plně pod kontrolou své vlastní informace. Uživatelé mohou přidávat, odebírat a sdílet atributy podle vlastního uvážení. Mohou sdílet svůj e-mail poskytovateli služeb a následně zrušit práva k používání tohoto e-mailu. Federované modely sice zpřístupnily některé z těchto možností tím, že umožnily uživatelům zaregistrovat se u jednoho poskytovatele a poté tuto identitu používat pro přístup k dalším službám, které akceptovaly stejný standard, ale jedním z hlavních problémů tohoto přístupu bylo, že federovaný poskytovatel, u kterého se uživatelé rozhodnou zaregistrovat, má všechny informace o uživateli a má nad nimi kontrolu. Podstatou modelu self-sovereign identity je tedy je to, že žádná identita nemůže být v držení jediného subjektu třetí strany.

Když byl Bitcoin v roce 2009 poprvé spuštěn, zavedl pojem decentralizovaného ledgeru (decentralizované účetní knihy). Technologie blockchain a decentralizované konsenzuální mechanismy nabídly technologické řešení problému důvěryhodnosti třetí strany. Přestože se většina průmyslového a akademického úsilí zaměřuje na měny a převod vlastnictví hodnoty, roste výrazně i zájem o využití blockchainu a souvisejících decentralizovaných technologií pro potřebu správu identity.(34)

Ledgery sice posunuly systémy identity o krok blíže k ideální samosprávné identitě, nadále se však potýkají s některými zásadními problémy. Většina navrhovaných a implementovaných systémů identity je postavena na infrastruktuře digitálních měn a interakce se sítí vyžaduje převod určité

peněžní hodnoty. Ty, které nejsou, jsou částečně centralizované za účelem řízení konsensu v síti. Ideální samosprávný systém identity by měl být svobodný a decentralizovaný a dnes navrhovaná a realizovaná řešení se dopouštějí kompromisů.(34)

Jako ideálně definici self-sovereign identity považuji následující od Dunphyho a Petitcolase.

Self-sovereign je *„…identita, kterou vlastní a kontroluje její vlastník, aniž by se musel spoléhat na jakoukoliv vnější správní autoritu, a aniž by mu tato identita mohla být odebrána. Může být realizována pomocí decentralizovaného ekosystému identity, který umožňuje zaznamenávání a výměnu atributů identity a šíření důvěry mezi zúčastněnými subjekty.“* (19) (překlad vlastní)

## 6.3 Shrnutí

V této kapitole byl stručně představen koncept bankovní identity a self-sovereign identity, přičemž hlouběji budou tyto koncepty představeny při analýze konkrétních řešení.

# 7 Přístup ke srovnání

Následující kapitola bude věnována analýze toho, jak ke srovnávání dvou a více konkrétních řešení digitální identity přistupovali jiní autoři. Na základě těchto zjištění bude zvolen přístup ke srovnávání, který bude využit v této práci.

V rámci provedené rešerše bylo zvoleno 5 prací, zabývajících se srovnáním konkrétních řešení digitální identity. Pro jasné pochopení toho, jak autoři ke srovnávání přistupovali bude cílem zjistit především následující informace.

- Jaké řešení autoři srovnávají?
- Jaká konkrétní kritéria ke srovnávání stanovují, respektive co přesně autoři chtějí porovnat a tím pádem zjistit?

V následujících odstavcích se pokusím jednotlivé práce podrobněji představit, a především v nich nalézt odpovědi na zmíněné otázky.

### Srovnání dle Dunphy a Petitcolas

Dunhpy a Petitcolas se ve svém článku A First Look at Identity Management Schemes on the Blockchain zaměřuje na srovnání více IdM systémů založených na technologii DLT (Distributed ledger technology, technologie distribuovaných záznamů), mezi které se řadí i self-sovereign identity systémy.(19)

Autoři ke srovnání zvolili následující systémy – uPort, ShoCard, Sovrin a Facebook Connect.

To, proč autoři zvolili tyto 4 systémy není dle jejich názoru náhoda, ale je tak tomu z toho důvodu, že každý ze 3 zvolených systémů reprezentuje mírně odlišný přístup řešení k IdM za využití DLT. Facebook Connect je pak dle autorů vybrán jaké zástupce tradičního řešení proto, aby byly při srovnání zdůrazněny rozdíly řešení.

Při stanovování kritérií autoři tvrdí, že neexistují žádná definitivní kritéria ke srovnávání IdM systémů. Proto se jako srovnávací rámec rozhodli využit tzv. Laws Of Identity autora Kima Camerona. Jedná se o 7 pravidel, autorem nazývaných jako zákony, které jsou dle něj kritické pro úspěch nebo neúspěch konkrétních systémů digitální identity.(35)

### Srovnání dle Ferdous a kolektivu

Md Sadek Ferdous je spoluautorem dvou prací, jejichž součástí je srovnávání systému digitální identity.

V práci In Search of Self-Sovereign Identity Leveraging Blockchain Technology srovnává 4 dle něj nejnadějnější self-sovereign identity systémy– uPort, Jolo, Sovrin, Blockcerts za využití svých vlastních stanovených zákonů, inspirovaných Cameronovými Laws of Identity, které ale však mají lépe vystihovat specifika SSI systémů. Jedná se o zákon existence, autonomie, vlastnictví, přístupu, jediného zdroje, ochrany, dostupnosti a trvalosti(24)

Druhou prací, která se zaměřuje na srovnání tradičních IdM systémů je A Comparative Analysis of Identity Management Systems, srovnávající řešení CardSpace, OpenID, Shibboleth, LA, PRIME a OAuth za využití několika sad obsahujících poměrně velké množství detailních kritérií. Definuje sady funkční, representační, řešící kontrolu uživatele, správu historie, bezpečnost, soukromí, interoperabilitu, ale například i právní aspekty.(36)

### Srovnání dle El Haddouti a El Kettani

Autoři studie Towards an Interoperable Identity Management Framework: a Comparative Study srovnávají vybrané populární IdM systémy, které jsou založeny na user-centric modelu. Konkrétně se jedná o CardSpace, Liberty Alliance, Shibboleth a OpenID. (37)

Pro srovnání využívají také Laws of Identity, které dále rozšiřují o vlastní definované požadavky pro IdM systémy. Svá kritéria zařazují do následujících sad: zabezpečení, soukromí, důvěryhodnost, použitelnost, obnovení identity, detekce kontextu, nezávislost na umístění, administrace identit (vytváření, aktualizace a mazání identit a souvisejících informací), digitální důkazy, uchování dat, cenová dostupnost a zajištění jednoduchosti systému.

### Srovnání dle Naik a Jenkins

Článek Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology Naika a Jenkinse se zaměřuje na srovnání dle nich dvou nejvýznamnějších self-sovereign řešení na bázi blockchainu – uPort a Sovrin. Autoři zmiňují dva existující rámce pro srovnávání IMS, a to už zmíněné Cameronovy Laws of Identity a Guiding Principles of SSI Christophera Allena. (20)

Tvrdí však, že pro evaluaci self-sovereign identity řešení je vhodné stanovit vlastní kritéria, která budou respektovat specifika self-sovereign identity systémů. Jedná se o následující kritéria: svrchovanost (sovereignty) nad vlastní digitální identitou, kontrola nad uložištěm, dlouhá životnost, ověřitelnost, možnost obnovy, bezplatnost, zabezpečení, soukromí, ochrana držitele identity, přístupnost, dostupnost, transparentnost, přenositelnost, interoperabilita a škálovatelnost systému. (38)

## 7.1 Stanovení kritérií pro srovnání

Tato kapitola je věnována stanovení kritérií, pomoci, kterých budou srovnána řešení v této práci. Níže budou jednotlivá kritéria představena.

### 7.1.1 Srovnání podle Laws of Identity

Na základě zjištění z předchozí kapitoly, že naprostá většina autorů ke srovnávání systému digitální identity přistupuje především na základě využití Laws of Identity, budou tyto „zákony“ využity právě i v našem případě. Přestože jsou tyto „zákony“ na poměry rychle se vyvíjejícího světa informačních technologií staré, tak to, že jsou jako základ ke srovnání systémů digitální identity používány dodnes, může svědčit o tom, že jsou stále relevantní a smysluplné. Stejně tak použití těchto pravidel dle mého názoru dává smysl proto, že jejich využití nabídne možnost srovnávat výsledky této práce s výsledky prací jiných autorů a tím pádem je zasadit do kontextu.

Níže budou uvedena jednotlivá pravidla společně s jejím plným přeloženým zněním a případně dalším nezbytným popisem.

1. Kontrola a souhlas uživatele

*„Systémy identity musí zveřejňovat informace identifikující uživatele pouze s jeho souhlasem.“* (35)(vlastní překlad)

Cameron při popisu tohoto pravidla také umocňuje důležitost důvěry uživatele v systém. Aby systém obstál, musí si především získat důvěru uživatele. Systém musí být navržen tak, aby měl uživatel kontrolu nad tím, jaké identifikační údaje jsou používány a jaké informace jsou předávány. (35)

Systém musí také chránit uživatele před podvodem a ověřovat totožnost všech stran, které žádají o informace. Pokud se uživatel rozhodne poskytnout informace o své identitě, nesmí být pochyb o tom, že je dostane na správné místo. A systém potřebuje mechanismy, které uživatele informují o účelech, pro které jsou informace shromažďovány.(35)

2. Minimální zveřejnění pro omezené použití

*„Dlouhodobě nejstabilnějším řešením je řešení, které zveřejňuje nejmenší množství identifikačních informací a nejlépe omezuje jejich použití.“* (35)(vlastní překlad)

3. Ospravedlnitelné (nezbytné) strany

*„Systémy digitální identity musí být navrženy tak, aby se zpřístupnění identifikačních údajů omezilo na strany, které mají v daném vztahu identity nezbytné a odůvodněné místo.“* (35)(vlastní překlad)

Cameron také dodává, že systém identit musí uživatele informovat o tom, s jakou stranou nebo stranami při sdílení informací komunikuje a požadavky na odůvodnění nezbytnosti strany se vztahují jak na subjekt, který informace poskytuje, tak na spoléhající se stranu, která na nich závisí.

4. Řízená identita

*„Univerzální systém identit musí podporovat jak "všesměrové" identifikátory pro použití veřejnými subjekty, tak "jedno směrové" identifikátory pro použití soukromými subjekty, což usnadní zjišťování a zároveň zabrání zbytečnému uvolňování korelačních údajů.“* (35)(vlastní překlad)

5. Pluralita provozovatelů a technologií

*„Univerzální systém identit musí zprostředkovávat a umožňovat vzájemnou spolupráci různých technologií identit provozovaných různými poskytovateli identit.“* (35)(vlastní překlad)

6. Lidská integrace

*„Univerzální systém identity musí definovat lidského uživatele jako součást distribuovaného systému integrovaného prostřednictvím jednoznačných komunikačních mechanismů mezi člověkem a strojem, které nabízejí ochranu proti útokům na identitu.“* (35)(vlastní překlad)

Kromě nutnosti plně integrovat uživatele – člověka do systému, která se už může jevit jako samozřejmá, Cameron v tomto zákonu zdůrazňuje důležitost uživatelské zkušenosti. Tvrdí, že koncept systémů digitální identity vyžaduje zásadní změnu uživatelské zkušenosti tak, aby byla dostatečně předvídatelná a jednoznačná a umožňovala plně informovaná rozhodnutí.

7. Konzistentní uživatelská zkušenost v různých kontextech

*„Sjednocující metasystém identit musí uživatelům zaručit jednoduchou a konzistentní zkušenost a zároveň umožnit oddělení kontextů prostřednictvím různých operátorů a technologií.“*(35)(vlastní překlad)

### 7.1.2 Srovnání architektury řešení a použitých technologií

Druhou skupinou kritérií, na základě, kterých budou systémy srovnané, budou kritéria zaměřená na architekturu konkrétního řešení.

Prvním bodem bude srovnání toho, jaké konkrétní subjekty jsou součástí daného řešení a jaké ze standardně definovaných rolí (IdP, SP…) takové subjekty zastávají.

Druhým bodem bude srovnání toho, jakým způsobem probíhá komunikace mezi jednotlivými entitami a jaké konkrétní technologie jsou pro komunikaci využity.

## 7.2 Výběr řešení pro srovnání

Jak už bylo zmíněno dříve práci, pro potřeby srovnání byly vybrány 2 řešení zastupující v jednom případě koncept self-sovereign identity a v druhém koncept bankovní identity.

Jako řešení reprezentující koncept bankovní identity byla zvolena česká služba **BankID** společnosti Bankovní Identita, a.s. Hlavním důvodem k tomu je fakt, že se jedná o české řešení bankovní identity, inspirované cizími, déle fungujícími řešeními, jako jsou například ve Švédsku a Dánsko. To, že se jedná o české řešení nabízí v kombinaci s veřejně dostupných vývojářským portálem možnost získat potřebné detailní a technické informace o řešení v českém jazyce. Výběr tohoto řešení vychází také už z motivace psaní této práce, kterou byl projekt České bankovní asociace, SONIA, který umožnil vzniku a zavedení bankovní identity do českého prostředí a vzniku služby BankID.

Protože v době psaní této práce neexistuje, nebo nebylo mnou nalezeno, žádné české řešení na bázi self-sovereign identity, byl k výběru tohoto řešení zvolen jiný přístup. Jelikož bylo v rámci analýzy odlišných přístupů ke srovnání systémů digitální identity nalezeno několik prací zabývajících se srovnáním i self-sovereign identity systémů, rozhodl jsem se k mému srovnání zvolit systém, který autoři srovnávají nejčastěji. Tím je systém **Sovrin**.

## 7.3 Shrnutí

Na základě analýzy 5 prací zabývajících se komparací systémů digitální identity byl zvolen přístup ke srovnání na základě tzv. Laws of Identity, doplněný přístupem srovnání architektur řešení. Následně byly vybrány 2 konkrétní systémy zastupující přístupy self-sovereign identity a bankovní identity – Sovrin a BankID.

# 8 Analýza řešení

V následující kapitole bude provedena analýza vybraných řešení na základě stanovených kritérií. Prvně bude každé řešení představeno, následovat bude analýza architektury řešení a použitých technologií (viz kap. 8.1.1) a analýza toho, jak jednotlivá řešení vyhovují Laws of Identity (viz 8.1.2).

V kapitole 10 budou získané informace srovnány a diskutovány.

## 8.1 BankID

Vývojářský portál BankID nabízí hned na svém úvodu odpověď na otázku „Co je BankID?“, proto toho využiji a definici autorů samotného systému prezentuji ve formě citace.

*„BankID funguje jako prostředník mezi poskytovatelem služeb (SeP) a bankou koncového uživatele. BankID dává uživateli možnost ověřit se proti SeP pomocí jeho přihlášení do banky a později umožňuje SeP získat Bankou ověřená data a osobní identifikační údaje (PII) koncového uživatele.*

*Hlavní cíle systému BankID jsou:*

- *Zjednodušit autentizaci koncového uživatele během počáteční registrace do SEP s již existujícím bankovním přihlášením koncového uživatele.*
- *Povolit poskytovatelům služeb přístup k osobním údajům ověřeným bankou pro*
- *Autorizace – například: Je koncový uživatel starší 18 let? Mohu jim prodat alkohol?*
- *Ověření PII – Je tento koncový uživatel tím, kým tvrdí, že je?*
- *Dodržování zákonů a předpisů proti praní peněz (AML) prostřednictvím používání rozhraní Know Your Customer (KYC) API.“(26)*

Primárním zdrojem k další analýze architektury bude právě oficiální dokumentace umístěna na vývojářském portálu BankID a oficiální webová stránka BankID. (39)

### Architektura řešení

V případě řešení BankID můžeme říct, že se jedná o jakousi variaci federativního modelu tak, jak byl představen v kapitole 5. Federace, respektive zmiňovaný kruh důvěry v tomto případě vzniká samotným zapojením bank, jako poskytovatelů identity na jedné straně a firem, které chtějí služeb BankID na straně druhé. Zapojení se do BankID je jak pro poskytovatel služeb, tak pro banky podmíněno podpisem smlouvy, což můžeme chápat jako formální vytvoření důvěry, a tedy kruhu důvěry, který je podstatnou části identitní federace.

Poskytovatelem identity (**IdP**) jsou v případě BankID jednotlivé banky, které drží údaje – identifikátory svých zákazníků primárně pro účely poskytování bankovních služeb.

Poskytovatelem služeb (**SeP**) je jakákoliv organizace, která se rozhodne do systému BankID zaregistrovat, implementovat systém do svých webových produktů nebo služeb a tím pádem nabízet pro své zákazníky možnost autentizace stejným způsobem, jako do internetového bankovnictví u své banky. Na rozdíl od uživatelů, pro které je služba BankID bankami poskytována zdarma, je zapojení se do systému pro SeP zpoplatněno.

Zjednodušeně řečeno, **uživatelem** může být každý klient banky, která je do systému BankID zapojená. To, jestli je třeba učinit ze strany klienta banky ještě nějaké další kroky, je stanovené pravidly dané banky. Nejčastěji se lze setkat s dvěma přístupy, které lze vidět u dvou největších českých bank – ČSOB a Česká spořitelna (30), které jsou zároveň do BankID zapojeny.

V prvním případě, s kterým se lze setkat u České spořitelna, je uživatel do systému zapojen automaticky už jen tím, že je klientem banky a využívá internetové bankovnictví. (31)

V druhém případě, který můžeme vidět u ČSOB, si uživatel musí v prvně vytvořit identitu v prostředí internetové bankovnictví. Ta opravňuje uživatele jen k autentizaci u služeb spadajících pod danou banku (v tomto případě ČSOB). Proto, aby mohl uživatel využívat bankovní identitu k přihlašování k externím službám, je třeba další aktivace služby v internetovém bankovnictví a potvrzení splnění všech zákonných podmínek.(32)

**BankID** můžeme chápat jako unikátní, specifickou entitu v tomto systému. BankID působí jako jakýsi prostředník v komunikaci mezi SeP a IdP (bankami).

Komunikaci v tomto systému tedy můžeme rozdělit na komunikaci mezi BankID a SeP a komunikaci mezi BankID a IdP a je založena na dříve představeném protokolu OAuth 2.0 a OpenID Connect. (26)

Princip komunikace aktérů upřesňuje technická dokumentace BankID.

*„BankID vystavuje dvě sady rozhraní REST – jednu pro banky a druhou pro poskytovatele služeb. Jsou založeny na specifikacích OpenID Connect a OAuth2. Specifikace je dodržována co nejpřesněji, aby byla zajištěna snadná interoperabilita se stávajícími řešeními a kódy – což by MĚLO snížit celkové náklady na vývoj a údržbu.*

*API jsou popsána pomocí sady specifikací OpenAPI, jmenovitě:*

- *BankID API pro API vystavená BankID, která má konzumovat SeP*
- *SeP RP front/back-channel API pro API vystavená SeP, která má konzumovat BankID*
- *BankID Authorization APIs pro API vystavená BankID pro SeP, pro účely podepisování*

*“(26)*

## Laws of Identity

V této části bude analyzováno, jak řešení BankID vyhovuje pravidlům Laws of Identity. Každé jednotlivé pravidlo bude ve vztahu k systému analyzováno jednotlivě.

### Kontrola a souhlas uživatele

Důvěra uživatele v systém, jež Cameron zmiňuje jako velmi důležitou, zde dle mého názoru výrazně tvoří důvěra lidí v samotné banky. Dá se předpokládat, že pokud lidé důvěřují bankám ve správě svých financí, budou stejně tak důvěřovat i ve správě informací.

Potřebné informace jsou poskytovateli služby předány jen na základě výslovného souhlasu uživatele, který potvrzuje přihlášením se v standardizovaném uživatelském rozhrání své banky.(26)

Problémem však může být, že uživatel nemá při autentizaci u SeP nemá žádnou přímou kontrolu nad tím, jaké konkrétní atributy se sdílí.

Nemůžeme tedy přímo určit, zda BankID tomuto zákonu vyhovuje.

### Minimální zveřejnění pro omezené použití

Ze strany uživatele není třeba zveřejňovat žádné údaje, jednoduše proto, že je banka už má. A to ať už na základě dokladů dodaných například při zakládání účtu, nebo získaných z registrů, ke kterým má banka díky novému zákonu o bankovní identitě přístup.

IdP SeP poskytuje jen vyžádané atributy a nic víc. Zákon BankID tedy splňuje.

### Ospravedlnitelné (nezbytné) strany

Součástí systému jsou nezbytné, standardně definované strany – banka jako IdP, SP jako poskytovatelé služeb – zapojené firmy nebo stát a uživatelé. Strana, která je oproti běžně definovaným navíc, je samotné BankID. Jelikož je existence strany BankID v systému zároveň jeho podstata – zajišťuje veškerou komunikaci mezi dalšími zúčastněnými stranami, můžeme ji označit jako nezbytnou.

Můžeme tedy říct, že všechny strany v systému jsou ospravedlnitelné a nezbytné.

### Řízená identita

To, zdali bude identifikátor všesměrový nebo jednosměrový (neboli soukromý nebo veřejný), záleží na tom, o jaké identifikátory se konkrétně bude jednat, tedy v principu, jaké atributy bude SeP vyžadovat. Mohou ale být obojího druhu.

### Pluralita provozovatelů a technologií

Jelikož je systém BankID založen na standardizovaných technologiích OAuth 2.0 a OpenID Connect a všichni zapojení aktéři se musí využívat jasně specifikované konfigurace těchto protokolů dle dokumentace (26), nemůžeme mluvit a žádné pluralitě technologií.

V případě plurality provozovatelů v kontextu systémy BankID se nabízí více interpretací. Pokud jako provozovatele chápeme poskytovatele identity – jednotlivé banky, můžeme říct, že pluralita provozovatelů v omezené míře existuje. Více bank je do systému už zapojená a další se můžou přidat. Avšak bank je velmi omezený počet, nevznikají často a žádné jiné entity, než banky se jako SeP do systému z podstaty věci nemohou přidat. Pokud však jako provozovatele považujeme samotnou entitu BankID, která je v systému unikátní, nemůžeme o existenci plurality provozovatelů vůbec mluvit.

### Lidská integrace

Uživatel je samozřejmě plně integrovanou entitou v BankID systému. BankID taky vyhovuje pravidlu kvalitní uživatelské zkušenosti. Úroveň uživatelské zkušenosti v tomto případě těží z faktu, že možnost autentizace banky dlouhodobě využívají v případě přihlašování do svých bankovních služeb, jako je například internetové bankovnictví. Tím pádem je možné říct, že s zajišťování kvalitní uživatelské zkušenosti mají dlouhodobou zkušenost a jsou ji schopni v dobré kvalitě poskytnout.

Samotná implementace u konkrétních služeb je sice především v ruce samotných poskytovatelů služeb, ale pro tyto potřeby BankID nabízí vývojářské podklady. Samotná autentizace uživatele poté probíhá již v prostředí tvořené jednotlivými bankami.(26)

BankID tedy tento zákon splňuje.

### Konzistentní uživatelská zkušenost v různých kontextech

Stejně jak u pravidla lidské integrace, konzistentní uživatelskou zkušenost zajišťuje uživatelské rozhraní, které je standardizované jednotlivými bankami. Konzistentní uživatelskou zkušenost je možné pozorovat i napříč různými zařízeními (PC, chytrý telefon, tablet), s kterými uživatelské rozhraní tvořené bankou v naprosté většině počítá

BankID tedy tento zákon splňuje.

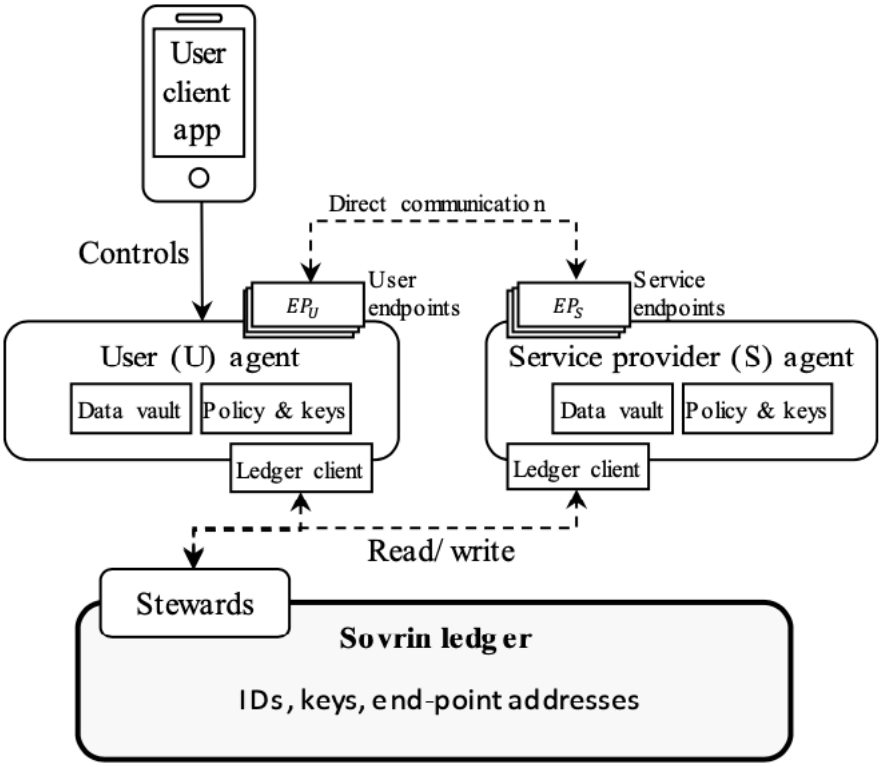
## 8.2 Sovrin

Sovrin je decentralizovaný systém digitální identity založený na open-source technologiích a postavený na technologii **DLT typu permissioned** (viz kapitola 4). Sovrin je veřejně přístupný systém, ale pouze důvěryhodné instituce, tzv. **stewardech/stewards** – což mohou být banky, univerzity, vlády apod. - mohou provozovat uzly, které se účastní konsensuálních protokolů – jedná se tedy o permissioned ledger. Nezisková nadace Sovrin Foundation zajišťuje řádné řízení stewardů a dodržování právních závazků spadajících pod tzv. Sovrin Trust Framework.

### Architektura řešení

Pokusit se zařadit řešení Sovrin do jedné z popsaných kategorií generalizovaných modelů na rozdíl od BankID není možné. To především z důvodu velké odlišnosti jednotlivých self-sovereign systémů, jejich relativní nevyspělosti a tím pádem neexistenci nějakého obecného self-sovereign identity modelu. Níže se tedy pokusím na základě analýzy oficiální dokumentace a dalších zdrojů popsat architekturu řešení Sovrin.

Architekturu systému Sovrin demonstruje obrázek 10 a už na první pohled je vidět zřejmé rozdíly oproti tradičním modelům představených dříve v této práci.




*Obrázek 10 - architektura systému Sovrin, zdroj: (20)*

Základem Sovrinu je ledger s povolením. Do tohoto Ledgeru mohou zapisovat a spravovat jej pouze tzv. stewardi, kteří jsou vázaní dodržovat soubor pravidel daných Sovrinem – tzv. Sovrin Trust Framework. Uživatelé a organizace se spoléhají na agenty, kteří jsou adresovatelnými body sítě. V ledgeru jsou uloženy identifikátory, klíče a adresy koncových bodů.

Sovrin umožňuje uživateli generovat tolik identifikátorů, kolik je potřeba k zachování kontextového oddělení identit pro účely ochrany soukromí; každý identifikátor je nepropojitelný a řízený jiným párem asymetrických klíčů. Samotné identifikátory jsou spravovány uživatelem nebo určenou službou – agentem a řídí se specifikací DID - Decentralized Identifiers konsorcia W3C.(40)

Volba ledgeru s povolením má v návrhu systému Sovrin dle Dunphyho a Petitcolase dva důležité důsledky. V první řadě k dosažení shody o stavu ledgeru není zapotřebí nákladný výpočet (tzv. proof-of-work, nejčastěji se s ním můžeme setkat v případě těžby Bitcoinu a jiných kryptoměn), což výrazně snižuje energetické náklady na provoz uzlu a výrazně zlepšuje propustnost transakcí.

Za druhé, důvěra v Sovrin je založená jak na lidech, tak na kódu. Důvěra vychází ze společné důvěry tvořené globálně distribuovaným ledgerem, ale jak se k síti připojují nové organizace a uživatelé, mohou se právě oni se stát tzv. kotvou důvěry (v kontextu systému Sovrin to především znamená, že mohou přidávat další uživatele a organizace).

Uživatelé komunikují se Sovrinem prostřednictvím mobilní aplikace a ovládají tzv. agenty, kteří jednají jejich jménem a realizují interakce s ostatními agenty v síti. **Agenty** v kontextu systému Sovrin chápeme jako jakési koncové body, které jsou vždy adresovatelné a přístupné. Uživatelé mohou provozovat agenty na svých vlastních serverech, ale předpokládá se, že požádají specializované zprostředkovatele, aby to dělali za ně. Agenti také poskytují zálohovací služby a šifrované ukládání specifických atributů.(19)

## Laws of Identity

V následující části bude stejně jak u řešení BankID analyzováno, jak řešení Sovrin splňuje jednotlivá pravidla Laws of Identity. Analýza bude realizována především za využití oficiální dokumentace Sovrin Foundartion (41) v kombinaci se sekundární analýzou prací, které se již analýzou systému Sovrin zabývaly (18, 19, 38, 42).

### Kontrola a souhlas uživatele

Samotnou podstatou systému Sovrin je umožnit uživatelům plně kontrolovat všechny aspekty jejich identity. Každý uživatel si tedy může vždy vybrat, jaké atributy vztahující se k jeho identitě chce s druhou stranou sdílet. To je možné také díky použití anonymních údajů. Zjednodušeně řečeno, uživatelé si sice mohou vybrat, zda své údaje uloží do Sovrin ledgeru, obecně se však počítá s využitím možnosti ukládání do svého mobilního telefonu, nebo ke svému agentovi, což umožňuje předávání atributů jiným stranám prostřednictvím zabezpečených komunikačních kanálů a k identifikaci správných koncových bodů sítě, který mají použít, použijí účetní knihu.(19)

Co se týče nutnosti důvěry uživatele v systém, kterou Cameron u tohoto pravidla zmiňuje, tak je řešena využitím modelu web-of-trust, řízením nadace Sovrin Foundation a pověstí stewardů. Je však otázkou, do jaké míry se tyto způsoby zajištěný důvěry v budoucnu ukážou jako dostatečné.

Můžeme tedy říct, že toto pravidlo Sovrin splňuje, avšak otázkou zůstává důvěra uživatelů v systém.

### Minimální zveřejnění pro omezené použití

V systému Sovrin se údaje vydávají vlastníkům identit, ale vlastníci identit následně celé údaje s ověřovatelem nesdílejí. Předložení všech údajů by logicky vedlo k odhalení více informací, než je nutné. Místo toho držitel identity předloží pouze tzv. zero-knowledge proof, tedy zjednodušeně důkaz o existenci a hodnoty určitého atributu, aniž by došlo k odhalení jakýchkoliv jiných.(42)

Tím pádem můžeme říct, že Sovrin pravidlo minimálního zveřejnění splňuje.

### Ospravedlnitelné (nezbytné) strany

V rámci systému Sovrin musí uživatelé chovat důvěru vůči agentům, kteří je budou v síti Sovrin zastupovat a vůči stewardům, kteří spravují ledger. V závislosti na výběru agenta a jeho implementaci může být v jeho rukou potenciálně mnoho informací, včetně případně nežádoucích. Protože však agenti jednají jménem uživatele, a především si jej uživatel volí uživatelé sami, můžeme říct, že mají ve vztahu k identitě nezbytné a opodstatněné místo.(19)

### Řízená identita

Protože je Sovrin založen na principech DID, který pracuje jak s veřejnými (všesměrovými), tak privátními(jedno směrovými) identifikátory, můžeme říct, že Sovrin pravidlo řízené identity splňuje.(40)

### Pluralita provozovatelů a technologií

Pravidlo plurality provozovatelů v kontextu systému Sovrin můžeme brát jako splněné z důvodu existence více stewardů spravující Sovrin ledger, jejich neustále rostoucího počtu, a především možnosti ostatních organizací se stewardy jednoduše na základě žádosti u Sovrin Foundation stát.(43)

### Lidská integrace a konzistentní uživatelská zkušenost v různých kontextech

Jak tvrdí Dunphy a Petitcolas, důležitou otázkou, kterou se vývojáři Sovrinu dosud příliš nezabývali, je uživatelská zkušenost. Integrace člověka do systému tak zůstává pro Sovrin otevřenou otázkou. Vzhledem k tomu, že Sovrin je stále v rané fázi vývoje, je jeho hodnocení podle těchto zákonů nepříliš smysluplné.  Indikátorem potencionálního problému může být fakt, že se mnoho prací zabývalo návrhem samotné architektury self-sovereign systému, ale téměř žádná se nezabývala přímo uživatelskou zkušeností.(19) Současně však můžeme říct, že tyto pravidla Sovrin nesplňuje.

# 9 Srovnání a diskuse

V rámci této kapitoly bude na základě provedené analýzy řešení provedeno srovnání obou řešení.

## 9.1 Srovnání architektury

V této části budou řešení srovnány na základě jejich architektury.

Zatímco BankID můžeme jako celek nazvat tradičním řešením a říct, že se svou architekturou blíží standardnímu federativnímu modelu, architektura Sovrin sice využívá fungujících a už i relativně dobře prověřených technologií jako je DLT, nebo DID, avšak jako celek vytváří na rozdíl od BankID unikátní, ničemu nepříliš podobný systém.

Jednotlivé entity a jejich role nelze vzájemné také příliš systematicky srovnat, protože jsou z povahy často založeny na naprosto odlišném principu.

V případě BankID roli poskytovale identity zastává banka, přičemž v případě Sovrinu je jakýmsi poskytovatel / zdrojem identit samotný ledger Sovrin, avšak je zřejmé, že obě entity roli plni odlišnými způsoby.

Poskytovatel služeb je v případě BankID firma nebo instituce, která se na základě uzavřené smlouvy, zaplacení poplatku a implementace technologií zařazuje do systému. V případě Sovrinu to může být prakticky kdokoliv, bez nutnosti jakéhokoliv smluvního vztahu, jelikož jednou z hlavních myšlenek systému Sovrin je jeho otevřenost.

Kde lze však v případě Sovrinu najít určitou podobnost s BankID / federativním modelem identity, je stále převládající nutnost důvěry uživatele v autority systému, které garantují jeho správnou funkčnost. V případě BankID to jsou jak samotné banky, tak BankID, přičemž v případě Sovrinu jsou to již zmínění tzv. Stewards, tedy vybírané Sovrin Foundation, které mají jako jediné možnost spravovat ledger, kde jsou umístěně samotné identifikátory.

| | *BankID* | *Sovrin* |
|---|---|---|
| *Poskytovatel identity* | Banka | Poskytovatelem (spíše zdrojem) identity můžeme nazvat ledger Sovrin |
| *Poskytovatel služby* | Smluvní zákazník BankID | Kdokoliv |
| *Komunikační technologie* | OAuth 2.0, OpenID Connect | DLT, DID |

Tabulka 1 – přehled rolí entit a použitých technologií

## 9.2 Srovnání dle Laws of Identity

V následující tabulce budou prezentovány výsledky srovnání na základě Laws of Identity. Ke každému zákonu bude uvedeno, zda jej dané řešení splňuje (zelené pozadí = splňuje, šedé pozadí = není jasné a červené pozadí = nesplňuje) a krátké zdůvodnění.

| Zákon / Řešení | BankID | Sovrin |
|---|---|---|
| **1 - Kontrola a souhlas uživatele** | Souhlas uživatele je vždy vyžadovaný, avšak kontrola předávaných dat je problematická. | Uživatel má plnou kontrolu nad svou identitou. |
| **2 - Minimální zveřejnění pro omezené použití** | K SeP se od bank dostávají jen vyžádané atributy a žádné jiné. | Díky využití zero-knowledge proof nejsou zveřejněný žádné jiné než nutné atributy. |
| **3 – Ospravedlnitelné (nezbytné) strany** | Mimo existenci běžných entit (IdP, SP) existuje entita BankID, která je plně ospravedlnitelná. | Je třeba chovat důvěru v stewardy a agenty, ale jejich místo v systému je plně ospravedlnitelná. |
| **4 – Řízená identita** | Identifikátor může být všesměrová i jednosměrový, záleží na konkrétním případu. | DID, které Sovrin v ledgeru ukládá může být jednosměrové i všesměrové |
| **5 – Pluralita provozovatelů a technologií** | Entita BankID je vždy jen jedna. SeP mohou být jen banky. IdP i SeP se musí při zapojení řídit pevně danými technickými specifikacemi. | Stát se stewardem ledgeru může jakákoliv instituce, která o to požádá a splní podmínky. |
| **6 – Lidská integrace** | Uživatel je plnohodnotná součást systému. Uživatelská zkušenost je odvozena od standardizovaného uživatelského rozhraní bank. | Uživatel je zamýšlen jako plnohodnotná součást systému, avšak kvůli rané a teoretické fázi projektu nelze hodnotit uživatelskou zkušenost |
| **7 – Konzistentní uživatelská zkušenost** | Konzistence uživatelské zkušenosti je dána standardizovaným uživatelským rozhraním bank napříč SeP a zařízeními. | Uživatelskou zkušenosti nelze současně stále dobře hodnotit. |

Tabulka 1 - výsledky srovnání systémů, zdroj: autor

## 9.3 Diskuse

Na základě srovnání obou systému v tom, jak si stojí vůči Laws of Identity, můžeme definovat 4 rozdíly.

Prvním rozdílem patrným v prvním zákoně je, že přestože v obou případech je například při autentizaci v rámci daného sytému nutný výslovný souhlas uživatele, jen u řešení Sovrin má uživatel plnou přímou kontrolu nad tím, jaké konkrétní data – atributy budou zveřejněné. Tato zdánlivá „nevýhoda“ systému BankID ale však může být kompenzována velkou důvěrou, kterou lidi v instituci jako jsou banky mají.

Druhý rozdíl je zřejmý u pravidla 5, kdy BankID je relativně rigorózní model, kdy se do systému mohou jako IdP přidávat pouze banky a samotná entita BankID je pro systém unikátní a nenahraditelná. Fungování Sovrinu závisí především na Stewardech – důvěryhodných registrovaných institucích, které mohou ale libovolně do systému na základě žádosti libovolně přibývat, a to bez ohledu na to, zda se jedná o banku nebo jinou organizaci.

Poslední 2, úzce spolu související rozdíly se týkají šestého a sedmého zákonu. Můžeme říct, že z hlediska integrace člověka a jeho uživatelské zkušenosti je systém BankID velmi pokročily a jak už bylo zmíněno, je tomu kvůli tomu, že všechny zúčastněné banky mají zavedené funkční uživatelské rozhraní pro autentizaci uživatele, které využívají pro poskytování svých bankovních služeb. V praxi to pak vypadá tak, že se uživatelé ke službám za využití bankovní identity přihlašují stejně tak, jak jsou zvyklí se již roky přihlašovat do svého internetového bankovnictví.

Oproti tomu v případě Sovrinu nemůžeme nic takového říct, protože systém je stále v poměrně rané fázi vývoje a hlavní orientaci vývoje je stále orientován na technické oblasti.

Zajímavé je však, že body týkající se uživatelského zážitku jsou jediné, které na základě analýzy Sovrin nesplňuje. Můžeme tedy odvodit, že pokud by v budoucnu došlo k implementaci kvalitní uživatelské zkušenosti pro uživatele – laickou veřejnost, má systém potenciál být velmi dobrý, snad i lepší, než systém BankID – tedy alespoň podle kritérií Kima Camerona.

## 9.4 Potenciál pro další práce

Možností pro navázání na tuto práci je několik. V první řadě se nabízí definování dalších, detailnějších kritérií, tak jak se s tím jde setkat u cizích autorů, kteří často Cameronovy Laws of Identity rozšiřují.

V druhé řadě se nabízí možnost aplikovat stejná kritéria na systémy, které ještě nebyly nijak zkoumány.

V poslední řadě se vzhledem k relativní nevyspělosti self-sovereign, ale i bankovních systému nabízí možnost analýzu opakovat za delší časový úsek, kdy se dá čekat, že řešení projdou určitým vývojem.

# Závěr

Práce se zabývala porovnáním bankovní identity a self-sovereign identity. Na úvod práce byla představena motivace ke psaní a čtenář byl uveden to základů tématu. Následně byl popsán průběh rešerše za využití principů SLR. Byly také představeny pojmy relevantní k práci a tématu digitální identity. Čtenář byl také seznámen s modely, standardy digitální identity.

Následně byl stručně představen koncept self-sovereign identity a bankovní identity, přičemž následovala hlubší analýza architektury řešení Sovrin a BankID a také toho, jak vyhovují definovaným pravidlům Laws of Identity Kima Camerona.

V poslední části práce byly představeny a diskutovány výsledky srovnání s indikací toho, kam by se mohl další výzkum ubírat.

Dílčí cíl 1 byl splněn v kapitole 8 provedenou analýzou řešení, dílčí cíl 2 v kapitole 7 stanovením kritérií a hlavní cíl v kapitole 9, srovnáním obou řešení.

# Použitá literatura


1. KENDE, Michael, Rory MACMILLAN a Theodorou YIANNIS. *Regulatory and policy trends impacting Digital Identity and the role of mobile* [online]. B.m.: GSMA. 26. říjen 2016. Dostupné z: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/10/Regulatory-and-policy-trends-impacting-Digital-Identity-and-the-role-of-mobile.pdf
2. WORLD ECONOMIC FORUM. *A Blueprint for Digital Identity: The role of Financial Institutions in building Digital Identity* [online]. B.m.: World Economic Forum. 2016. Dostupné z: http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf
3. WHITE, Olivia, Owen SPERLING, Anu MADGAVKAR, James MANYIKA, Jacques BUGHIN, Deepa MAHAJAN a Michael MCCARTHY. *Digital ID: A key to inclusive growth | McKinsey* [online]. [vid. 2021-03-05]. Dostupné z: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/Digital-identification-A-key-to-inclusive-growth?cid=other-eml-alt-mgi-mck&hlkid=ecd8822bafc44de78b1f2670c2979652&hctky=2259579&hdpid=0945f28e-3aa8-4f73-a111-6ba86e377b51
4. TECHUK. *Digital identities: the missing link in a UK digital economy* [online]. B.m.: techUK. 2020. Dostupné z: https://www.techuk.org/images/programmes/Digital_ID/digital_identities.pdf
5. PANGESTU, Mari Elka. How can digital ID systems make a difference? *World Economic Forum* [online]. 2020. Dostupné z: https://www.weforum.org/agenda/2020/08/harnessing-the-power-of-digital-id/
6. VÝROST, Jozef a Ivan SLAMĚNÍK. *Sociální psychologie*. Praha: Grada, 2008. ISBN 978-80-247-1428-8.
7. Bankovní identitu spouští první české banky, další je budou brzy následovat. *Česká bankovní asociace* [online]. [vid. 2021-03-07]. Dostupné z: https://cbaonline.cz/bankovni-identitu-spousti-prvni-ceske-banky-dalsi-je-budou-brzy-nasledovat
8. ČESKÁ BANKOVNÍ ASOCIACE. O projektu – bankovniidentita. *bankovniidentita* [online]. [vid. 2020-10-14]. Dostupné z: https://bankovni-identita.cz/o-projektu/
9. PWC. *Blockchain and Digital Identity: the path to Self Sovereign Identity* [online]. 2019. Dostupné z: https://www.pwc.com/it/it/publications/assets/docs/blockchain-and-digital-identity.pdf
10. XIAO, Yu a Maria WATSON. Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research* [online]. 2019, **39**(1), 93–112. ISSN 0739-456X. Dostupné z: doi:10.1177/0739456X17723971
11. *This is BankID* [online]. [vid. 2020-10-16]. Dostupné z: https://www.bankid.com/en/om-bankid/detta-ar-bankid
12. PRICEWATERHOUSECOOPERS. Bankovní identita. *PwC* [online]. [vid. 2020-10-16]. Dostupné z: https://www.pwc.com/cz/cs/odvetvove-specializace/bankovnictvi-a-financni-sluzby/BankID.html
13. SEDLÁK, Jan. E-government přes internetové bankovnictví. Vláda schválila zavedení BankID. *Lupa.cz* [online]. [vid. 2020-10-16]. Dostupné z: https://www.lupa.cz/aktuality/e-government-pres-internetove-bankovnictvi-vlada-schvalila-zavedeni-bankid/
14. VÁCLAVÍK, Lukáš. Česko zavede BankID, komunikace se státem bude jednodušší. *Cnews.cz* [online]. 27. srpen 2019 [vid. 2020-10-16]. Dostupné z: https://www.cnews.cz/portal-obcana-bankid-sonia-elektronicke-bankovnictvi/
15. WINDLEY, Phillip J. *Digital identity*. 1st ed. Beijing ; Sebastopol, CA: O'Reilly, 2005. ISBN 978-0-596-00878-9.
16. LAURENT, Maryline a Samia BOUZEFRANE, ed. *Digital identity management*. London: ISTE Press [u.a.], 2015. Information systems, web and pervasive computing. ISBN 978-1-78548-004-1.
17. WILSON, Yvonne a Abhishek HINGNIKAR. *Solving Identity Management in Modern*

*Applications: Demystifying OAuth 2. 0, OpenID Connect, and SAML 2. 0.* [online]. Berkeley, CA: Apress L.P., 2020 [vid. 2021-04-11]. ISBN 978-1-4842-5095-2. Dostupné z: https://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=5997230
18. FERDOUS, M. S., F. CHOWDHURY a M. O. ALASSAFI. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. *IEEE Access* [online]. 2019, **7**, 103059–103079. ISSN 2169-3536. Dostupné z: doi:10.1109/ACCESS.2019.2931173
19. DUNPHY, Paul a Fabien PETITCOLAS. A First Look at Identity Management Schemes on the Blockchain. *IEEE Security & Privacy* [online]. 2018, **16**. Dostupné z: doi:10.1109/MSP.2018.3111247
20. NAIK, N. a P. JENKINS. Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology. In: *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*: *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)* [online]. 2020, s. 90–95. ISSN 2573-7562. Dostupné z: doi:10.1109/MobileCloud48802.2020.00021
21. FEARON, James D. WHAT IS IDENTITY (AS WE NOW USE THE WORD)? nedatováno, 45.
22. FERDOUS, Md Sadek. *User-controlled Identity Management Systems using mobile devices* [online]. B.m., 2015 [vid. 2021-04-11]. PhD. University of Glasgow. Dostupné z: https://eleanor.lib.gla.ac.uk/record=b3126074
23. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION a INTERNATIONAL ELECTROTECHNICAL COMMISSION. *ISO/IEC 24760-1:2019 IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts* [online]. B.m.: International Organization for Standardization / International Electrotechnical Commission. 2019. Dostupné z: https://www.iso.org/standard/77582.html
24. FERDOUS, Md Sadek, Farida CHOWDHURY a Madini O. ALASSAFI. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. *IEEE Access* [online]. 2019, **7**, 103059–103079. ISSN 2169-3536. Dostupné z: doi:10.1109/ACCESS.2019.2931173
25. FERDOUS, Md. Sadek, Gethin NORMAN a Ron POET. Mathematical Modelling of Identity, Identity Management and Other Related Topics. In: *ACM International Conference Proceeding Series* [online]. 2014. Dostupné z: doi:10.1145/2659651.2659729
26. BANKOVNÍ IDENTITA, A.S. *Bank ID dev portal | Bank ID* [online]. 2021 [vid. 2021-06-15]. Dostupné z: https://developer.bankid.cz/docs
27. GOODELL, Geoff a Tomaso ASTE. A Decentralised Digital Identity Architecture. *arXiv:1902.08769 [cs]* [online]. 2019 [vid. 2021-04-27]. Dostupné z: doi:10.3389/fbloc.2019.00017
28. How OpenAM Works Simple Explanation · Open Identity Platform. *Open Identity Platform - Open Source Solutions for Access Management, Identity Management, Directory Services* [online]. [vid. 2021-05-04]. Dostupné z: https://www.openidentityplatform.org/blog/how-openam-works-simple-explanation
29. *Zapojené banky – Bankovní identita* [online]. [vid. 2021-05-06]. Dostupné z: https://bankovni-identita.cz/banky-a-reseni/
30. Největší banky v Česku. Žebříček podle počtu klientů i peněz. *Peníze.cz* [online]. [vid. 2021-06-22]. Dostupné z: https://www.penize.cz/bezne-ucty/425357-nejvetsi-banky-v-cesku-zebricek-podle-poctu-klientu-i-penez
31. ČESKÁ SPOŘITELNA, A. S. *Bankovní IDentita* [online]. [vid. 2021-05-06]. Dostupné z: https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bankovni-identita
32. ČSOB. *ČSOB Identita – bankovní identita od ČSOB | ČSOB* [online]. [vid. 2021-05-06]. Dostupné z: https://www.csob.cz/portal/csob/csob-identita
33. KOMERČNÍ BANKA. *Bankovní identita KB | Komerční banka* [online]. [vid. 2021-05-06]. Dostupné z: https://www.kb.cz/cs/podpora/bankovnictvi-a-nastroje/kb-bankovni-identita
34. SATYBALDY, Abylay, Mariusz NOWOSTAWSKI a Jørgen ELLINGSEN. Self-Sovereign Identity Systems: Evaluation Framework. In: [online]. 2020, s. 447–461. ISBN 978-3-030-42503-6. Dostupné z: doi:10.1007/978-3-030-42504-3_28
35. CAMERON, Kim. The Laws of Identity. 2005, 12.

36. FERDOUS, Md. Sadek a Ron POET. A comparative analysis of Identity Management Systems. In: [online]. 2012. Dostupné z: doi:10.1109/HPCSim.2012.6266958
37. EL HADDOUTI, Samia a Mohamed KETTANI. *Towards an Interoperable Identity Management Framework: a Comparative Study*. 2015.
38. NAIK, N. a P. JENKINS. Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology. In: *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*: *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)* [online]. 2020, s. 90–95. ISSN 2573-7562. Dostupné z: doi:10.1109/MobileCloud48802.2020.00021
39. BANKOVNÍ IDENTITA, A.S. *Dokumentace | Bank ID* [online]. 2021 [vid. 2021-06-16]. Dostupné z: https://developer.bankid.cz/docs/high_level_overview_sep
40. W3C. *Decentralized Identifiers (DIDs) v1.0* [online]. 2021 [vid. 2021-06-13]. Dostupné z: https://www.w3.org/TR/did-core/
41. SOVRIN FOUNDATION. Library. *Sovrin* [online]. [vid. 2021-06-23]. Dostupné z: https://sovrin.org/library/
42. WINDLEY, Phil. *The Laws of Identity* [online]. 7. leden 2019 [vid. 2021-06-21]. Dostupné z: https://www.windley.com/archives/2019/01/the_laws_of_identity.shtml
43. SOVRIN FOUNDATION. Stewards Archive. *Sovrin* [online]. 2021 [vid. 2021-06-13]. Dostupné z: https://sovrin.org/stewards/