

Cenová analýza EUDIW

Zpracovaná pro Digitální a informační agenturu

Dodavatel:

Ernst & Young, s.r.o.

Na Florenci 2116/15

110 00 Praha 1 – Nové Město

IČ: 26705338



1 Obsah

1	Obsah	2
2	Cíl a účel analýzy	5
3	Východiska	6
3.1	Hlavní cíle nařízení eIDAS 2.0	7
3.2	Významné změny oproti původnímu nařízení eIDAS	8
3.3	Výzvy implementace	9
4	Porovnání mezinárodní praxe ve způsobech poskytování EUDIW nebo obdobných řešení (z pohledu ekonomického, organizačního, procesního, ale i z pohledu smluvního zajištění poskytovatele)	10
4.1	Národní řešení	11
4.1.1	Estonsko	11
4.1.2	Řecko	12
4.1.3	Rakousko	14
4.2	Nadnárodní projekty a konsorcia	15
4.2.1	Projekt POTENTIAL	15
4.2.2	Projekt NOBID (Nordic-Baltic eID Project)	20
4.2.3	European Wallet Consortium	20
4.3	Shrnutí a přehled hybridních modelů spolupráce vlády a soukromého sektoru dle typů spolupráce	25
4.3.1	Porovnání modelů	26
4.3.2	Další příklady spolupráce	27
5	Variantní posouzení	29
5.1	Přístup k tvorbě cenového modelu	30
5.1.1	Implementační náklady	34
5.1.2	Provozní náklady	34
5.2	(nadpis neposkytnut)	35
5.3	(nadpis neposkytnut)	35
5.4	(nadpis neposkytnut)	36
5.5	(nadpis neposkytnut)	37
5.6	Návrh / oponentura metrik (SLA) a způsob jejich vykazování ve vztahu k povinnostem poskytovatele, včetně motivace k onboardingu uživatelů i spoléhajících se stran	38
5.7	Dopady na současné uživatele eDokladů (jak z pohledu frontend, tak i z backend). A zároveň posouzení dopadů na scénáře, kdyby eDoklady fungovaly paralelně s EUDIW.	42

5.7.1	Současný stav systému eDoklady.....	42
5.7.2	Scénáře po spuštění EUDIW	43
5.8	Identifikace souvisejících nákladů na straně státu	45
5.8.1	Posílení Národní identifikační autority (NIA).....	45
5.8.2	Posílení Informačního systému sdílené služby (ISSS)	45
6	Závěry a rekapitulace.....	49
6.1	Doplnění a shrnutí faktorů ovlivňujících cenový model.....	50
6.1.1	Potenciální příjmy z provozu EUDIW	50
6.1.2	Doplňkové komerční služby.....	50
6.1.3	Faktory ovlivňující nepřesnosti a rizika napříč variantami	50
6.2	Celkové shrnutí monopolního postavení dodavatele	52
6.3	Další doporučení k minimalizaci rizik monopolního postavení a vendor lock-in	53
6.3.1	Zajištění služeb nezávislého arbitra.....	53
6.4	Příklady dobré praxe.....	55
6.4.1	V České republice	55
6.4.2	V Evropské unii.....	55
6.4.3	V jiných zemích:	55
6.5	Další poznámky a doporučení.....	56
6.6	Manažerské shrnutí	57
6.6.1	K variantě 1 - Poskytovatelem je stát:.....	57
6.6.2	K variantě 2 - Poskytovatelem je soukromý subjekt – dodávka formou služby.....	57
6.6.3	K variantě 3 - Poskytovatelem je soukromý subjekt – koncese	57
6.6.4	K variantě 4 - Poskytovatelem je subjekt s majetkovým podílem státu	58
7	Výhrady a omezení.....	61
8	Zdroje.....	62
9	Příloha 1: Technologie Split Key	63

Datum:	12.11.2024	Verze dokumentu:	1.6
Autor:	Ernst & Young, s.r.o. (EY)		
Klient:	Digitální a informační agentura (DIA)		

2 Cíl a účel analýzy

Analýza je zpracována za účelem stanovení předpokládané hodnoty EUDIW – Evropské digitální peněženky pro Digitální a informační agenturu a klade si za cíl představit komplexní pohled na ekonomickou, organizační a procesní náročnost zajištění fungování evropské digitální peněženky, v souvislosti se zajištěním povinnosti poskytovat alespoň jednu EUDIW v ČR dle nařízení eIDAS 2.0.

Analýza poslouží Digitální a informační agentuře jako podklad pro účely návrhu řešení realizace poskytování EUDIW v České republice.

3 Východiska

Nařízení (EU) 2024/1183, známé jako eIDAS 2.0, bylo přijato s cílem harmonizovat digitální identifikační systémy napříč Evropskou unií a vytvořit spolehlivý, bezpečný a interoperabilní rámec pro digitální identity. Tato revize původního nařízení eIDAS (EU) 910/2014 zavádí nový koncept Evropské peněženky digitální identity (EUDI Wallet, dále jen EUDIW), která umožní občanům a podnikům bezpečné uchovávání a sdílení osobních údajů a elektronických dokumentů (elektronických potvrzení atributů) napříč členskými státy ^{1,2}.

¹ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401183

² <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/About%2Bthe%2Binitiative>

3.1 Hlavní cíle nařízení eIDAS 2.0

1. **Zvýšení důvěry a bezpečnosti digitální identity:** eIDAS 2.0 reaguje na potřebu bezpečnější a univerzálněji přijímané digitální identity v EU, která má být dostupná občanům i podnikům pro přístup k veřejným i soukromým službám.
2. **Interoperabilita mezi členskými státy:** Nové nařízení zavádí systém, který zajistí jednotné uznávání digitálních identit ve všech členských státech, což usnadní přeshraniční transakce a sníží právní a technické překážky.
3. **Zajištění kontroly uživatelů nad svými daty:** EUDIW poskytne uživatelům plnou kontrolu nad svými osobními údaji a umožní sdílení pouze těch dat, která jsou potřebná pro konkrétní účely. Tento koncept podporuje ochranu soukromí a soulad s GDPR.
4. **Podpora digitální ekonomiky:** Evropská digitální identita by měla vytvořit nové obchodní příležitosti a zvýšit efektivitu veřejné správy. Zavedení digitální peněženky by mělo mít pozitivní dopad na digitální ekonomiku a obchodní vztahy napříč EU.

3.2 Významné změny oproti původnímu nařízení eIDAS

1. **EUDIW:** Tento nový nástroj bude sloužit k ukládání a správě elektronických identifikačních údajů a elektronických potvrzení atributů. Občané tak budou moci bezpečně sdílet dokumenty ve formě elektronických potvrzení atributů jako jsou řidičské průkazy, diplomy nebo další různá osvědčení či povolení.
2. **Nové služby vytvářející důvěru:** Nařízení eIDAS 2.0 zavádí nové typy služeb vytvářejících důvěru, včetně elektronických záznamů knih a archivačních služeb, které zajišťují bezpečné uchovávání a integritu elektronických dat.
3. **Požadavky na poskytovatele služeb:** Stejně jako v původním znění nařízení eIDAS, kvalifikovaní poskytovatelé služeb vytvářejících důvěru budou povinni podstupovat pravidelné audity, aby prokázali splnění požadavků například na kybernetickou bezpečnost a ochranu dat v souladu s novými standardy nařízení.

3.3 Výzvy implementace

Implementace eIDAS 2.0 představuje několik výzev:

- **Technologické a organizační požadavky:** Zavedení EUDIW bude vyžadovat vývoj a harmonizaci technických standardů mezi členskými státy, zejména s ohledem na interoperabilitu a zabezpečení systémů.
- **Legislativní a právní aspekty:** Dodržování pravidel ochrany osobních údajů a kybernetické bezpečnosti bude hrát klíčovou roli v úspěšném zavedení EUDIW a dalších důvěryhodných služeb.

Celkově nařízení eIDAS 2.0 (Nařízení (EU) 2024/1183), harmonizuje digitální identifikační systémy napříč členskými státy EU a zavádí EUDIW. Tato digitální peněženka poskytne uživatelům možnost bezpečně spravovat a sdílet své osobní údaje a dokumenty (elektronická potvrzení atributů). Nařízení klade důraz na interoperabilitu, ochranu dat a soulad s GDPR. Zároveň zavádí nové služby vytvářející důvěru, které posilují kybernetickou bezpečnost a digitální infrastrukturu v EU.

4 Porovnání mezinárodní praxe ve způsobech poskytování EUDIW nebo obdobných řešení (z pohledu ekonomického, organizačního, procesního, ale i z pohledu smluvního zajištění poskytovatele)

Tato část analýzy se zaměřuje na porovnání mezinárodní praxe v poskytování digitálních identit a obdobných řešení, a to jak z ekonomického, organizačního, procesního, tak i smluvního pohledu.

Analýza rozděluje zjištěné poznatky do dvou celků, kdy v první části jsou popsány příklady jednotlivých členských zemí EU, ve druhé následně řešení zastřešené nadnárodními projekty, či konsorcií.

4.1 Národní řešení

4.1.1 Estonsko

Estonský přístup k EUDIW vychází z dlouhodobých zkušeností s digitalizací veřejné správy. Projekt řídí Estonian Information System Authority (RIA), která spolupracuje se společností **Cybernetica**, specialistou na kryptografii a digitální identity. **Cybernetica** získala kontrakt v hodnotě **6 milionů eur** na vývoj digitální peněženky kompatibilní s estonským národním systémem digitální identity a splňující standardy EU eIDAS.

Tento projekt spadá pod vládní zakázku zaměřenou na vývoj a podporu technologického řešení. Cybernetica je zodpovědná za vývoj a technické zajištění projektu, včetně bezpečnosti dat a identit. Peněženka bude integrována do národních systémů digitální identity a veřejných služeb, přičemž provoz bude pod správou **RIA**.

Cybernetica dodává technologické řešení a poskytne dlouhodobou podporu prostřednictvím servisních smluv. Přesto však nebude přímo provozovat celý systém, správa a údržba digitální peněženky budou pravděpodobně zajištěny státem.³ Zakázka tedy zahrnuje vývoj, implementaci a dlouhodobou technologickou podporu, ale nikoliv přímý provoz systému samotnou Cyberneticou.

Klíčovým prvkem tohoto řešení je technologie SplitKey, která zajišťuje bezpečnost dat pomocí kryptografických klíčů a zabraňuje jejich neoprávněnému kopírování. Tento projekt má za cíl umožnit uživatelům bezpečně spravovat a sdílet své identity napříč hranicemi, což je klíčovým cílem celoevropského programu EUDIW.

Technologie SplitKey, kterou využívá Estonsko a společnost Cybernetica, je navržena pro bezpečné uchovávání a sdílení digitálních identit bez závislosti na hardwarově založených bezpečnostních prostředcích, jako jsou čipy Secure Enclave. SplitKey funguje na principu kryptografických klíčů, které jsou rozděleny mezi uživatele a poskytovatele služby, což zajišťuje vysokou úroveň bezpečnosti při podepisování dokumentů a ověřování identity.

³ Informace o tom, kdo bude dlouhodobě zajišťovat správu a údržbu digitální peněženky v Estonsku, zatím není zcela jasná. Současný kontrakt s **Cyberneticou** se soustředí na vývoj a implementaci digitální peněženky, ale správa systému by měla zůstat v rukou **RIA**, která je vládní institucí zodpovědnou za dohled nad digitálními identitami a veřejnými službami. Pravděpodobně bude tento model hybridní, což znamená, že stát by měl spravovat systém, zatímco **Cybernetica** poskytne technickou podporu a servisní smlouvy.

Konečné rozhodnutí o provozu by mělo být učiněno po ukončení implementační fáze projektu, což se obvykle stává po úspěšném testování a nasazení digitální peněženky do ostrého provozu. Přesný termín tohoto rozhodnutí může záviset na výsledcích pilotních projektů a testovacích fázích, které jsou nyní v běhu.

Více informací o technologii SplitKey je uvedeno v Příloze 1.

Estonsko se rozhodlo pro hybridní model, ve kterém stát zajišťuje klíčové funkce, jako je infrastruktura a správa digitálních identit, zatímco soukromý sektor, reprezentovaný společností Cybernetica, přináší technologické inovace. Tento model funguje na základě dlouhodobé spolupráce mezi státními institucemi a soukromými firmami, což umožňuje rychlou implementaci nových technologií a zároveň zaručuje bezpečnost a důvěryhodnost vládních služeb.

Cybernetica má bohaté zkušenosti s významnými estonskými projekty, jako je X-Road, který umožňuje bezpečnou výměnu dat mezi státními institucemi. v rámci EUDIW projektu Cybernetica přispívá technologiemi, jako je SplitKey, které zabezpečují digitální identitu pomocí pokročilých kryptografických metod. Nicméně, provoz a správa systému digitálních identit zůstávají v rukou RIA (Estonian Information System Authority), která má na starosti dohled nad celou infrastrukturou.

Tento hybridní model je efektivní, protože spojuje flexibilitu a technologickou inovativnost soukromého sektoru s důvěryhodností a stabilitou státních systémů. Cybernetica se tedy zaměřuje na vývoj inovativních řešení a poskytování konzultačních služeb v oblasti kryptografie, zatímco stát zajišťuje provozní správu digitálních identit. Tento přístup umožňuje státu těžit z technologických pokroků a odbornosti Cyberneticy, aniž by ztratil kontrolu nad klíčovými aspekty systému.

Estonsko by bylo nejlépe přiřazeno k Variantě 1 (režie státu), jelikož zde stát (Estonian Information System Authority – RIA) zajišťuje klíčové funkce a spolupracuje se soukromým sektorem na technologických řešeních, jako je SplitKey. Klíčové části systému jsou provozovány státem, i když vývoj technologií zajišťuje soukromý sektor.

4.1.2 Řecko

Řecko je na dobré cestě k integraci své digitální peněženky s požadavky EUDIW. Řecko již má zavedenou svou Gov.gr Wallet, která od roku 2020 umožňuje digitální správu občanských průkazů a řidičských průkazů. Nyní je v plánu rozšířit funkčnost této peněženky o elektronické platby, otevírání bankovních účtů a další služby, které budou v souladu s evropskými standardy eIDAS.

Řecké ministerstvo digitální správy ve spolupráci s organizací GRNET S.A. (Národní infrastruktura pro výzkum a technologie) zajišťuje technickou realizaci řecké verze digitální peněženky v rámci projektu EUDIW. GRNET je **státní podnik**, který funguje pod záštitou ministerstva a zaměřuje se na poskytování technologických služeb a infrastruktury pro veřejnou správu, vzdělávání a výzkum. Nejedná se tedy o komerční společnost, ale o státní organizaci.

Formou veřejné zakázky (otevřené výběrové řízení) byla zajištěna spolupráce na technickém vývoji a implementaci, přičemž GRNET využívá své odborné znalosti k zajištění interoperability a pokročilých digitálních služeb. Tento model umožňuje státu kontrolovat infrastrukturu, zatímco **státní podnik**

GRNET poskytuje technologické řešení a jeho následnou podporu.⁴ Hodnota kontraktu zatím nebyla zveřejněna.

Současný plán Řecka zahrnuje rozšíření funkcionalit, aby byla národní peněženka interoperabilní s celoevropským systémem, což zahrnuje především schopnost elektronického podpisu, přeshraniční použití digitální identity a další digitální služby. Cílem je umožnit občanům bezpečně a snadno přistupovat ke službám napříč celou Evropskou unií, jak ve veřejném, tak soukromém sektoru, včetně například otevírání bankovních účtů, registrace SIM karet nebo přístupu k eGovernment službám.

Spolupráce mezi řeckým Ministerstvem digitální správy a organizací GRNET je příkladem efektivního propojení veřejného a akademického sektoru při realizaci technologicky náročných projektů, jako je digitální peněženka EUDIW. GRNET funguje jako klíčový technologický partner státu, přičemž využívá své odborné znalosti v oblasti návrhu digitální infrastruktury, bezpečnostních mechanismů a zajištění interoperability digitálních identit. Soustředí se na to, aby řešení splňovala evropské standardy, jako je eIDAS, a zároveň umožňovala bezpečné digitální transakce na národní i mezinárodní úrovni.

Podobně jako český CESNET⁵, GRNET čerpá svou sílu z akademického sektoru a je zapojen do mezinárodních sítí jako GÉANT a REFEDS, které podporují inovace v oblasti výzkumných a vzdělávacích infrastruktur. Tyto organizace se zaměřují na zajištění robustní digitální infrastruktury, která je schopna podporovat náročné výzkumné a vzdělávací aktivity na mezinárodní úrovni. v tomto kontextu je GRNET, stejně jako CESNET, klíčovým hráčem při tvorbě digitálních řešení, které podporují digitalizaci veřejné správy prostřednictvím odborných znalostí a technologických inovací vycházejících z akademické sféry.⁶

Tento model spolupráce umožňuje nejen rychlou implementaci technologických řešení, ale i vysokou úroveň bezpečnosti a důvěryhodnosti, což je zásadní pro digitální projekty, jako jsou digitální identity a peněženky v rámci celé EU.

GRNET se zapojuje do širokého spektra aktivit spojených s digitální transformací v Řecku a jeho hlavní zodpovědnost spočívá v poskytování infrastruktury pro cloudové služby, datová centra a kybernetickou bezpečnost. v rámci projektu EUDIW bude GRNET spolupracovat na technické realizaci, včetně zapojení dalších řeckých subjektů, které se podílejí na budování systému digitální identity. Významnou součástí této spolupráce je rovněž jejich účast v evropských konsorciích, jako je European Wallet Consortium (EWC), které podporují přeshraniční interoperabilitu digitálních identit a peněženek.

⁴ https://grnet.gr/en/2024/03/14/pr_eu_wallet_en/

⁵ Oba jsou součástí mezinárodních sítí, jako je GÉANT a REFEDS.

⁶ https://grnet.gr/en/2024/03/14/pr_eu_wallet_en/

Soukromé firmy budou zapojeny do procesu prostřednictvím veřejných výběrových řízení, která umožní flexibilní a rychlou implementaci technologií, což je běžný postup při zavádění technologických inovací v rámci státní správy.

Řecký model zahrnuje státní kontrolu nad infrastrukturou prostřednictvím GRNET, což odpovídá Variantě 1. GRNET však funguje jako státní podnik, což by mohlo také odpovídat Variantě 4, kde státní instituce a podniky zajišťují technologické služby, přičemž kontrola zůstává u státu. Tato situace je tedy na pomezí těchto dvou variant.

4.1.3 Rakousko

Rakouský systém ID Austria je již funkčním nástrojem digitální identity, který umožňuje přístup k široké škále veřejných služeb, včetně elektronického podepisování dokumentů, digitálního řidičského průkazu a dalších vládních aplikací. Rakousko plánuje tento systém rozšířit, aby byl plně kompatibilní s celoevropskými standardy EUDIW. ID Austria je vyvinut ve spolupráci mezi Rakouským federálním kancléřstvím a Ministerstvem vnitra a představuje krok k plné integraci digitální identity v celé Evropě.

Rakousko pravděpodobně zvolí vládní model správy své digitální identity, kdy stát zajistí základní infrastrukturu a technologické řešení, přičemž klíčová bude spolupráce se soukromým sektorem na inovacích a implementaci nových funkcí. Tento hybridní model je nápodobný Estonsku – hybridní model správy digitální identity, který kombinuje státní kontrolu s využitím inovací ze soukromého sektoru. Umožňuje tak rychlou implementaci inovací při zachování plné kontroly nad citlivými údaji a bezpečností ze strany státu^{7, 8}.

V případě Rakouska rozhoduje o zvoleném modelu především historická důvěra v státní správu digitálních identit. Rakousko má dlouholetou tradici v oblasti digitálních služeb a digitální identity, kde stát zajišťuje základní infrastrukturu pro elektronickou identifikaci a správu osobních údajů. Tento model podporuje důvěru občanů v to, že jejich osobní data jsou spravována transparentně a bezpečně, což je klíčový prvek, zvláště v kontextu zvyšujících se požadavků na ochranu soukromí podle evropského nařízení GDPR.

Rakousko zajišťuje základní infrastrukturu a provoz systému ID Austria přímo státem. I když soukromý sektor může přispět technologickými inovacemi, kontrola a správa systému digitálních identit zůstává státní, což je typické pro variantu 1.

⁷ <https://www.digitalaustria.gv.at/eng/>

⁸ <https://www.oesterreich.gv.at/en/id-austria.html>

4.2 Nadnárodní projekty a konsorcia

4.2.1 Projekt POTENTIAL

Projekt POTENTIAL je jedním z hlavních pilotních projektů podporovaných Evropskou komisí v rámci iniciativy na vytvoření EUDIW. Tento projekt zahrnuje více než 140 partnerů z 19 členských států EU a Ukrajiny. Hlavním cílem je testovat interoperabilitu a technickou proveditelnost digitální peněženky, která by umožnila občanům EU bezpečný přístup ke službám napříč hranicemi. Projekt se zaměřuje na různé případy použití, včetně digitálních řidičských průkazů, otevírání bankovních účtů, registrace SIM karet a vzdáleného elektronického podpisu.

Projekt POTENTIAL představuje důležitý krok směrem k vytvoření jednotného evropského systému digitální identity, který umožní občanům EU bezpečný a pohodlný přístup k digitálním službám po celé Evropě. Každý členský stát a jeho partneři přispívají k rozvoji a testování různých funkcionalit, což zajišťuje široké pokrytí klíčových scénářů pro budoucí nasazení EUDIW.

POTENTIAL konsorcium bylo vybráno Evropskou komisí k realizaci pilotů a je financováno z programu Digital Europe, který podporuje inovace v digitální infrastruktuře v EU. Cílem je vytvořit společné standardy pro digitální identitu, aby občané mohli bez problémů využívat digitální služby napříč členskými státy EU.

Vybraní členové projektu POTENTIAL a jejich prioritní zájmy:

- **Francie:** Zaměřuje se na digitální bankovní služby a ověřování identity pro online přístup k vládním službám. Prioritou je interoperabilita a bezpečnost dat při přístupu k soukromým a státním službám.
- **Německo:** Hlavní prioritou je testování digitálních řidičských průkazů a jejich integrace do systému EUDIW. Německo také pracuje na možnostech elektronického podpisu a na tom, jak mohou být digitální dokumenty používány napříč hranicemi.
- **Litva:** Litva testuje integraci digitálních řidičských průkazů a spolupráci s poskytovateli služeb, jako je car-sharing. Prioritou je ověřit technickou proveditelnost peněženky v rámci veřejného a soukromého sektoru.
- **Lotyšsko:** Lotyšsko se zaměřuje na interoperabilitu a technickou infrastrukturu pro digitální identitu s důrazem na zabezpečení a bezpečnost. Důležitou roli zde hraje integrace s národními systémy a testování SIM registrace.
- **Kypr:** Používá řešení zavedené v Řecku prostřednictvím mezivládní dohody pro první fázi zavádění digitální peněženky. Prioritou Kypru je rychlá implementace základního systému a následné rozšíření funkcí, které budou v souladu s evropskými standardy.

4.2.1.1 Německo a Francie

Projekt POTENTIAL hraje významnou roli v testování různých scénářů využití EUDIW, přičemž Francie a Německo zastávají klíčové postavení jako vedoucí státy. Obě země se soustředí na vývoj funkcí peněženky zahrnující přístup k vládním službám, digitálním řidičským průkazům, bankovním účtům a registraci SIM karet, s cílem zajistit přeshraniční interoperabilitu. Tento proces je zásadní pro budoucí implementaci systému napříč členskými státy EU.

Francie a Německo rozdělily své zaměření. Zatímco Francie se orientuje na využití digitální identity pro online služby a bankovníctví, Německo testuje digitální řidičské průkazy a jejich propojení s národními systémy a evropskými standardy. Výsledkem je ukázka funkčnosti digitální peněženky jak na národní, tak mezinárodní úrovni.

Obě země volí hybridní model spolupráce, kde se propojuje státní dohled nad bezpečností a ochranou osobních údajů s technologickými inovacemi soukromého sektoru. Tento přístup umožňuje efektivní vývoj digitálních řešení, jako jsou šifrovací technologie a cloudové platformy. Klíčovým aspektem je schopnost státu zajistit důvěryhodnost a vysokou úroveň ochrany, zatímco soukromý sektor se zaměřuje na rychlou a efektivní implementaci.

Francie spolupracuje s technologickými partnery, jako je IDEMIA, která se specializuje na biometrické technologie a digitální identity, a Thales, jenž poskytuje šifrovací a bezpečnostní řešení. Dalším významným partnerem je IN Groupe, která přispívá řešeními v oblasti digitální identifikace, a iProov, specializující se na biometrickou autentizaci. **Tento model urychluje nasazení digitálních technologií, aniž by došlo ke snížení bezpečnosti osobních údajů.**

Podobně Německo spolupracuje se soukromým sektorem na vývoji digitální infrastruktury, přičemž klíčové státní instituce zajišťují správu a bezpečnost dat. Německé úsilí směřuje k testování digitálních řidičských průkazů, které jsou integrovány do širších systémů digitální identity. **Tento přístup umožňuje rychle reagovat na nové technologické požadavky a zároveň zajišťuje vysokou úroveň zabezpečení dat.**

Hybridní model spolupráce mezi státem a technologickými partnery tak poskytuje optimální řešení pro rozvoj komplexních digitálních infrastruktur, které odpovídají požadavkům evropských standardů a předpisů, jako je nařízení eIDAS. Tento model kombinuje výhody flexibilního technologického vývoje s důvěryhodným a regulovaným prostředím státních institucí.

Ve Francii a Německu model spadá nejvíce k Variantě 1 (režie státu) s prvky Varianty 3 (koncese). Prvky Varianty 3 (koncese) jsou patrné skrze zapojení soukromých firem, které poskytují technologická řešení a nesou část rizika spojeného s implementací digitálních identit. Stát si ponechává kontrolu nad klíčovými oblastmi, ale spoléhá na soukromý sektor pro inovace a provoz technologií, což se blíží koncesnímu modelu.

4.2.1.2 Litva

Litva se v rámci projektu POTENTIAL zaměřuje na testování digitálních řidičských průkazů a jejich integraci do EUDIW. Tento pilotní projekt zahrnuje několik veřejných institucí, jako je Centrální registr, ale i soukromé společnosti, například poskytovatele služby sdílení automobilů. Cílem je ověřit technickou proveditelnost digitální peněženky a zajistit její interoperabilitu v rámci evropského kontextu. Pilot také zahrnuje testování použití peněženky v oblastech, jako je otevírání bankovních účtů, registrace SIM karet, a kvalifikovaný elektronický podpis, což jsou některé z klíčových funkcí, které má peněženka podporovat.

Litva pravděpodobně zvolí model veřejně-soukromé spolupráce, kde stát bude zajišťovat správu identity a bezpečnost, zatímco technologická řešení budou dodávána soukromými firmami. Model Litvy se de facto neliší od hybridního modelu v Estonsku. Oba zahrnují veřejně-soukromou spolupráci, kde stát zajišťuje správu identity a bezpečnost, zatímco technologická řešení poskytuje soukromý sektor. Tento přístup je pro Litvu výhodný, protože soukromý sektor může poskytnout flexibilitu a rychlost implementace, což je obzvláště důležité pro pilotní projekty financované z evropských fondů. Zvolený model by měl přispět k rychlejší inovacím a zároveň snížit náklady pro státní sektor. Soukromé firmy mohou rovněž zajistit technické a inovační prvky, jako je vývoj mobilních aplikací a integrace s národními ID kartami, i když detaily ohledně této integrace zatím nejsou plně specifikovány.

Tento přístup umožňuje Litvě rychle nasadit funkční řešení a následně systém rozšířit o další funkcionality, včetně těch, které budou reflektovat finální evropské standardy pro digitální peněženky.

Litva se zaměřuje na Variantu 1 (režie státu) s prvky Varianty 2 (dodávka komerčním poskytovatelem). Stát zajišťuje správu digitálních identit, zatímco technologická řešení poskytuje soukromý sektor. Tento přístup podporuje flexibilitu a rychlost inovací.

4.2.1.3 Lotyšsko

Lotyšsko je součástí konsorcia NOBID (Nordic-Baltic eID Project)⁹, které se zaměřuje na rozsáhlé testování EUDIW s důrazem na platby. Tento projekt zahrnuje šest zemí, včetně Lotyšska, a má za cíl nejen vytvořit a testovat digitální peněženku, ale také zkoumat její schopnost podporovat platby, včetně rychlých převodů mezi účty a akceptace plateb v kamenných prodejnách a online.

V rámci tohoto projektu se používá existující infrastruktura pro bankovní platby, kterou v Lotyšsku spravuje Latvian State Radio and Television Centre, spolu s dalšími významnými partnery v oblasti technologií a financí. Projekt je podporován z programu Digital Europe a zahrnuje testovací období, během kterého se očekává zapojení tisíců uživatelů a provedení více než deseti tisíc transakcí. Celkový

⁹ <https://www.nobidconsortium.com/kick-off-for-nobid-and-large-scale-piloting-of-the-eu-digital-wallet/>

rozpočet konsorcia NOBID činí 20 milionů EUR, které budou využity na vývoj a implementaci řešení včetně interoperability a zabezpečení v souladu s požadavky eIDAS 2.0¹⁰.

Lotyšsko nedávno dokončilo veřejnou zakázku na pilotní projekt EUDIW, který se zaměřuje na vytvoření centralizované platformy pro digitální identitu a elektronické podpisy.

Veřejná zakázka pro pilotní projekt EUDIW v Lotyšsku byla realizována formou otevřeného výběrového řízení, což umožnilo účast několika potenciálních dodavatelů¹¹. Tento proces zajistil transparentnost a efektivní výběr technologického partnera s potřebnými zkušenostmi.

Zakázka byla udělena jedné z největších lotyšských softwarových společností, která se specializuje na vládní projekty a integraci národních registrů – společnosti **TietoEVERY Latvia**¹². Celková hodnota zakázky činí 826 440 EUR. Projekt zahrnuje klíčové funkce, jako je vydávání verifikovatelných pověření (Verifiable Credentials – VC), vývoj mobilních aplikací pro systémy iOS a Android a podpora kvalifikovaných elektronických podpisů (Qualified Electronic Signatures – QES). **Tento pilotní projekt má zajistit interoperabilitu s celoevropským systémem digitální identity, což Lotyšsko přibližuje k integraci s evropskými normami eIDAS.**

Důvodem pro volbu hybridního modelu v Lotyšsku, kde základní infrastrukturu spravuje stát a technologické služby zajišťují soukromé firmy, je nutnost zapojení odborníků na specifické technologie. Hybridní model v tomto případě znamená spolupráci mezi veřejným sektorem, který spravuje základní infrastrukturu (například Latvian State Radio and Television Centre), a soukromým sektorem, který poskytuje technologické inovace a odborné znalosti. Soukromé společnosti se podílejí na vývoji technologií, jako jsou šifrování a správa digitálních identit, zatímco stát si ponechává kontrolu nad bezpečností a ochranou osobních údajů¹³.

Vybraný dodavatel má zkušenosti a know-how, které umožňují rychlou implementaci a inovaci při zachování souladu s evropskými bezpečnostními a technickými normami. **Partnerství mezi veřejným a soukromým sektorem umožňuje nižší náklady na provoz a zrychluje nasazení nových technologií, zatímco stát si ponechává kontrolu nad klíčovými aspekty, jako je bezpečnost dat a řízení identity.**

Právě v Lotyšsku budou spoléhající se strany, tedy organizace, které využívají digitální identitu (např. banky nebo poskytovatelé online služeb), pravděpodobně zpoplatněny. Tento model umožní komerčním partnerům zapojit se do ekosystému digitální identity, přičemž budou hradit poplatky za přístup k verifikovaným službám, jako je ověřování identity či elektronické podpisy.

¹⁰ <https://www.financelatvia.eu/en/news/the-nobid-consortium-chosen-to-launch-pan-european-payments-pilot-for-eu-digital-id-wallet/>

¹¹ <https://company.lursoft.lv/en/tietoevry-latvia/40203458747>, <https://www.iub.gov.lv/en>

¹² <https://www.prakse.lv/enterprise/profile/73/tietoevry-in-latvia>, <https://company.lursoft.lv/en/tietoevry-latvia/40203458747>

¹³ <https://www.prakse.lv/enterprise/profile/73/tietoevry-in-latvia>

Lotyšský projekt se soustředí na rozvoj centrální platformy pro digitální identitu a používá stejná technologická řešení, která jsou testována v rámci projektu POTENTIAL, jako jsou **verifikovatelné pověření (VC)** a **kvalifikované elektronické podpisy (QES)**.

Lotyšsko implementuje Variantu 3 (koncesní model), kde stát spravuje základní infrastrukturu, ale technologické služby jsou outsourcovány soukromým firmám. Tento model umožňuje rychlejší inovace, přičemž stát si udržuje kontrolu nad bezpečností dat.

4.2.1.4 Kypr

Kypr přistoupil k zavedení digitální peněženky EUDIW pomocí dvoufázového modelu. v první fázi využívá technologii vyvinutou v Řecku na základě mezivládní dohody, což mu umožňuje rychlejší nasazení bez nutnosti vypisování náročných veřejných zakázek. Tím Kypr dosahuje **rychlé implementace základní verze peněženky**, která zahrnuje digitální úložiště pro osobní doklady, jako jsou občanské a řidičské průkazy. Tato verze peněženky již umožňuje digitalizaci základních vládních služeb a snížení byrokracie.

V další fázi Kypr plánuje vypsat tendr na řešení, které bude plně vyhovovat finálním evropským standardům pro EUDIW. Tato budoucí fáze zahrnuje rozšíření funkcionalit o služby, jako jsou elektronické platby, interoperabilitu v rámci EU a rozšíření digitálního podpisu. Tento přístup umožňuje Kypru nejprve rychle nasadit funkční řešení, zatímco si ponechává flexibilitu pro budoucí rozšíření, která budou reflektovat konečné evropské požadavky.

Kypr tímto způsobem minimalizuje počáteční investice a zároveň využívá osvědčené technologie, které již byly zavedeny v Řecku. Tento model mu umožňuje udržet kontrolu nad vývojem a zároveň profitovat z řešení, která byla úspěšně nasazena v jiném členském státě EU. v pozdější fázi, kdy bude na úrovni EU zcela finalizován rámec pro EUDIW, bude Kypr moci systém snadno přizpůsobit novým požadavkům.

Kypr začíná s Variantou 1 (režie státu) v první fázi a plánuje postup k Variantě 2 nebo Variantě 3 v pozdější fázi. Aktuálně využívá řešení vyvinuté Řeckem, ale v budoucnu plánuje tender na rozšíření funkcí digitální peněženky podle evropských standardů.

4.2.2 Projekt NOBID (Nordic-Baltic eID Project)

Projekt NOBID hraje klíčovou roli v rámci iniciativy EUDIW (European Digital Identity Wallet), kde se zaměřuje zejména na testování přeshraničních plateb prostřednictvím digitální peněženky. Konsorcium zahrnuje šest zemí: Dánsko, Německo, Island, Itálii, Lotyšsko a Norsko, a jeho cílem je pilotně otestovat platební funkce digitální peněženky nejen v domácím, ale i v přeshraničním kontextu.

V rámci tohoto pilotního projektu se používá stávající infrastruktura pro bankovní platby, která zahrnuje okamžité platby (SCT Instant Payments) a tradiční převody z účtu na účet. Testují se různé formy autorizace plateb, včetně QR kódů, push notifikací a propojení na mobilní aplikace. Tento přístup umožňuje propojit digitální identity s platebními funkcemi, což má potenciál sloužit jako základ pro digitální euro a další inovace v oblasti digitálních financí¹⁴.

Každá zúčastněná země přináší do projektu své specifické zkušenosti a zájmy:

- Norsko se soustředí na integraci plateb do stávající národní ID brány, kterou denně používá více než 90 % norských občanů. Prioritou je zlepšení platební infrastruktury, která již funguje digitálně.
- Lotyšsko se v rámci NOBID zaměřuje na infrastrukturu digitální identity a propojení s platebními funkcemi. Jejich cílem je umožnit využití digitální identity nejen na národní úrovni, ale i pro přeshraniční služby, jako je registrace SIM karet.
- Itálie využívá digitální identitu (SPID a CIE) k digitální transformaci veřejných služeb a zaměřuje se na integraci platebních funkcí do svého systému digitálních identit.

NOBID tak hraje zásadní roli při testování a implementaci platebních funkcí v rámci EUDIW a přispívá k vytvoření standardizovaného přeshraničního digitálního ekosystému v EU.

4.2.3 European Wallet Consortium

European Wallet Consortium (EWC) hraje klíčovou roli v EUDIW tým, že se zaměřuje na pilotní testování a ověřování různých scénářů použití této peněženky. Mezi hlavní oblasti, na které se EWC soustředí, patří cestování, organizace digitálních identit (ODI) pro podniky a platby.

Konsorcium EWC zahrnuje partnery ze všech 27 členských států EU, ale i některé nečlenské země, a jeho cílem je demonstrovat, jak může digitální peněženka EUDIW usnadnit přeshraniční aktivity. v rámci cestovních případů použití se testuje například sdílení informací o cestujících a ověřování identity na hranicích. Platby jsou další důležitou součástí, kde EWC zkoumá možnosti použití peněženky pro přeshraniční platby a bezpečné elektronické transakce. Dále se zaměřuje na organizaci

¹⁴ <https://www.nobidconsortium.com/>

digitálních identit podniků, což zahrnuje ověřování pravosti a autorizace pro osoby jednající za společnosti nebo stroje.

EWC se snaží ukázat, jak může digitální peněženka EUDIW zjednodušit online nakupování a komunikaci mezi občany, podniky a vládními institucemi po celé Evropě, přičemž důraz je kladen na bezpečnost a spolehlivost těchto procesů.

4.2.3.1 *Polsko*

Polsko je součástí **European Wallet Consortium (EWC)**. Implementaci EUDIW v Polsku řídí **Ministerstwo Cyfryzacji (Ministerstvo digitalizace)**, které spolupracuje s národními i mezinárodními partnery na vývoji a implementaci digitální peněženky v souladu s evropskými standardy. Ministerstvo digitalizace zajišťuje legislativní rámec a dohled nad projektem, zatímco soukromé firmy poskytují technologická řešení a inovace.

Veřejná zakázka na vývoj a implementaci EUDIW byla realizována formou otevřeného výběrového řízení. Zakázka byla udělena konsorciu společností **Asseco Poland** a **Comarch**, které patří mezi největší IT firmy v Polsku a mají bohaté zkušenosti s dodávkou systémů pro veřejný sektor¹⁵.

Polsko plánuje integraci funkcí EUDIW s existující mobilní aplikací **mObywatel**. I zde jsou zakázky pravděpodobně zadávány prostřednictvím veřejných výběrových řízení, ale konkrétní částky nebo podrobnosti o vítězných dodavatelích nebyly veřejně oznámeny.

Polsko se rozhodlo integrovat funkce EUDIW do své stávající aplikace mObywatel, místo toho, aby provozovalo dvě samostatné aplikace. Tento krok umožní, aby občané mohli využívat jednu aplikaci jak pro národní, tak pro celoevropské digitální služby – přístup reflektuje širší strategii digitální transformace, která má zvýšit komfort uživatelů tím, že eliminuje potřebu mít více aplikací.

Aplikace mObywatel, kterou již používá více než 10 milionů lidí, poskytuje digitální verze osobních dokladů, jako jsou občanské průkazy a řidičské průkazy, a umožňuje občanům komunikovat s vládními úřady, provádět online platby za veřejné služby a získávat důležité informace, například o svých

¹⁵ https://euc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fpeople.ey.com%2Fpersonal%2Fflukas_klucka_cz_ey_com%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F626b49aa29664eeb9190cc496afef67e&wdenableroaming=1&mssc=1&wdodb=1&hid=61F755A1-008A-A000-125E-3EA703CD0308.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=4612dcf0-98ca-15d1-bed7-5609920e3b4b&usid=4612dcf0-98ca-15d1-bed7-5609920e3b4b&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fpeople.ey.com%22%2C%22pms%22%3Atrue%7D&ctp=L eastProtected&rct=Normal&wdorigin=ItemsView&wdhostclicktime=1727873499255&instantedit=1&wopicomplete=1&wd redirectionreason=Unified_SingleFlush#user-content-fn-4

vozidlech či lékařských předpisech. v roce 2023 se **mObywatel 12.0**¹⁶ stala rovnocennou s fyzickými doklady, což znamená, že digitální dokumenty v aplikaci jsou právně uznávané ve stejném rozsahu jako ty papírové.

V rámci integrace s EUDIW bude aplikace **mObywatel** rozšířena o další funkce, jako jsou **verifikovatelná pověření (VC)** a **kvalifikované elektronické podpisy (QES)**. Plán je nabídnout jednotnou aplikaci, která bude podporovat celoevropskou interoperabilitu digitálních identit.

Co se týče finančního aspektu, mObywatel je primárně financován z evropských fondů, včetně European Funds for Digital Development (EFDD), které pro období 2021–2027 poskytly Polsku značné prostředky na podporu digitální transformace, včetně zlepšení přístupu k digitálním službám a posílení kybernetické bezpečnosti.¹⁷

Co se týče soukromoprávních partnerů, Polsko plánuje zapojit do ekosystému mObywatel různé poskytovatele služeb, zejména finanční instituce a poskytovatele veřejných služeb. Tímto způsobem budou moci občané používat svou digitální identitu nejen při styku se státními úřady, ale také při komerčních transakcích, jako je otevírání bankovních účtů, přístup k pojištění nebo registrace SIM karet.

Finanční model pro integraci soukromého sektoru není v tuto chvíli detailně zveřejněn, ale očekává se, že poskytovatelé služeb budou zapojeni prostřednictvím partnerství. Pod pojmem partnerství se v tomto případě pravděpodobně myslí spolupráce mezi státem a soukromými poskytovateli služeb. Tato spolupráce by spočívala v tom, že by Polsko pravděpodobně získávalo příjmy ze **zpoplatnění ověřovacích služeb**. Soukromé společnosti by tedy vskutku typicky platily za přístup k validaci digitálních identit svých zákazníků. Tento systém by měl přinést **finanční výnosy** a současně umožnit státu rozšířit digitální infrastrukturu s podporou evropských fondů, jako jsou prostředky z programu **Digital Europe Programme** a **European Funds for Digital Development**.

(K získání přístupu k programům, jako je **Digital Europe Programme** nebo **European Funds for Digital Development (EFDD)**, musí být žadatelé oprávněnými organizacemi (veřejné instituce, firmy, univerzity) a připravit projekt v souladu s cíli programu. Projekty často vyžadují mezinárodní partnerství a doložení finanční způsobilosti.)

¹⁶ <https://www.gov.pl/web/primeminister/prime-minister-mateusz-morawiecki-mobywatel-means-digitisation-in-the-service-of-everyday-life> , <https://ux-design-awards.com/winners/2024-1-mobywatel-2-0> , <https://www.digitality.org/blog/mobywatel>

¹⁷ <https://www.digitality.org/blog/mobywatel>

Polsko plánuje další expanzi funkcí aplikace a propojení se službami veřejné správy, čímž chce vytvořit jednotné řešení pro všechny digitální potřeby občanů.

Polsko zde integruje funkce EUDIW do své stávající aplikace mObywatel, což naznačuje model mezi *Variantou 1* (režie státu) a *Variantou 2* (komerční poskytovatel). Stát zajišťuje legislativní rámec a dohled nad projektem, zatímco technologická řešení jsou poskytována soukromými firmami. Tento model odpovídá Varianta 1, kde stát řídí klíčové funkce a infrastrukturu, ale s prvky Varianty 2, protože implementace a rozvoj technologií jsou outsourcovány soukromým firmám.

4.2.3.2 Slovensko

Slovensko je aktivním účastníkem iniciativy EUDIW a zapojuje se do pilotních projektů zaměřených na testování a implementaci. Je součástí konsorcia **EWC (European Wallet Consortium)**.

V rámci projektu EWC se Slovensko zaměřuje na vytvoření centralizované platformy pro digitální identitu a elektronické podpisy. Implementaci EUDIW na Slovensku řídí **Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (MIRRI SR)**, které spolupracuje s národními i mezinárodními partnery na vývoji a testování digitální peněženky.

Veřejná zakázka na pilotní projekt EUDIW byla realizována formou otevřeného výběrového řízení. Tento proces zajistil transparentnost a efektivní výběr technologického partnera s potřebnými zkušenostmi. **Zakázka byla udělena společnosti DXC Technology Slovakia**, která má zkušenosti s implementací digitálních řešení pro veřejný sektor¹⁸.

Slovensko má aplikaci podobnou polské aplikaci **mObywatel** s názvem **Slovensko v mobile**. Aplikace Slovensko v mobile v současnosti slouží primárně pro přihlašování k vládním službám a usnadnění přístupu k elektronickým službám státu, jako je portál slovensko.sk, prostřednictvím mobilního klíče nebo QR kódu. Není zatím ovšem určena pro prokazování identity pomocí elektronických verzí osobních dokladů (např. občanského průkazu nebo řidičského průkazu), jak je tomu u aplikace **mObywatel** v Polsku. Ovšem stejně jako v Polsku, Slovensko postupně rozšiřuje funkce této aplikace,

¹⁸ https://euc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fpeople.ey.com%2Fpersonal%2Fflukas_klucka_cz_ey_com%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F626b49aa29664eeb9190cc496afef67e&wdenableroaming=1&mssc=1&wdodb=1&hid=61F755A1-008A-A000-125E-3EA703CD0308.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=4612dcf0-98ca-15d1-bed7-5609920e3b4b&usid=4612dcf0-98ca-15d1-bed7-5609920e3b4b&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fpeople.ey.com%22%2C%22pms%22%3Atrue%7D&ctp=L eastProtected&rct=Normal&wdorigin=ItemsView&wdhostclicktime=1727873499255&instantedit=1&wopicomplete=1&wd redirectionreason=Unified_SingleFlush#user-content-fn-1

aby usnadnilo přístup k eGovernment službám, jako jsou podání daňových přiznání nebo žádosti o různé úřední dokumenty.

Slovensko plánuje rozšířit funkcionalitu své aplikace na jednotnou platformu, která bude propojena se službami veřejné správy i komerčními subjekty, podobně jako polská aplikace **mObywatel**.

Finanční model není detailně zveřejněn, ale očekává se, že soukromoprávní subjekty budou zapojeny prostřednictvím partnerství a budou platit za přístup k ověřovacím službám. z tohoto důvodu Slovensko plánuje získávat finanční výnosy ze zpoplatnění těchto služeb a rozšířit digitální infrastrukturu s podporou evropských fondů. Tento model partnerství je tedy téměř stejný jako u Polska.

Důvodem pro volbu hybridního modelu na Slovensku je potřeba zapojení odborníků na specifické technologie a zároveň zachování kontroly nad bezpečností a ochranou osobních údajů. **Hybridní model** zde znamená spolupráci mezi veřejným sektorem, který spravuje základní infrastrukturu (například Národní agentúra pre sieťové a elektronické služby – NASES), a soukromým sektorem, který poskytuje technologické inovace a odborné znalosti¹⁹.

Slovenský model se přiklání k Variantě 1 (režie státu), jelikož stát zajišťuje správu identity a infrastrukturu, ale s prvky Varianty 2, protože soukromé firmy poskytují technologická řešení a inovace.

¹⁹ <https://www.trade.gov/country-commercial-guides/slovakia-digital-economy> , <https://dig.watch/resource/national-digital-decade-strategic-roadmap-of-slovakia>

4.3 Shrnutí a přehled hybridních modelů spolupráce vlády a soukromého sektoru dle typů spolupráce

Většina států EU preferuje hybridní modely, které kombinují státní kontrolu nad bezpečností a správou identity s technologickými inovacemi poskytovanými soukromými firmami. Tento přístup umožňuje rychlejší implementaci inovací a zároveň snižuje náklady na rozvoj digitálních peněženek.

I. Hybridní model – Stát zajišťuje klíčové funkce, soukromý sektor dodává řešení a technologické inovace, na jejichž správu a řízení mají vliv orgány členských států

• Estonsko

Stát (Estonian Information System Authority – RIA) spravuje digitální identitu, zatímco soukromá společnost Cybernetica vyvíjí technologická řešení, jako je technologie SplitKey.

• Francie

Stát dohlíží na bezpečnost a ochranu dat, soukromé firmy jako IDEMIA, Thales a IN Groupe poskytují technologické inovace v oblasti biometrie a šifrování.

• Německo

Státní instituce zajišťují správu a bezpečnost dat, soukromý sektor přispívá k vývoji digitální infrastruktury, zejména v oblasti digitálních řidičských průkazů.

• Lotyšsko

Stát spravuje základní infrastrukturu (Latvian State Radio and Television Centre), soukromá firma TietoEVERY Latvia vyvíjí technologická řešení pro digitální identitu.

• Litva

Stát zajišťuje správu identity a bezpečnost, technologická řešení dodávají soukromé společnosti zapojené do pilotního projektu.

II. Vládní model – Státní instituce nebo státní podniky zajišťují jak správu, tak technologická řešení

• Řecko

Ministerstvo digitální správy spolupracuje se státním podnikem GRNET S.A., který poskytuje technologická řešení a infrastrukturu bez zapojení komerčních společností.

III. Dvofázový model s mezivládní spoluprací

- **Kypr**

V první fázi využívá technologii vyvinutou v Řecku na základě mezivládní dohody. v další fázi plánuje vypsat veřejnou zakázku na řešení plně vyhovující evropským standardům.

Jako možné řešení varianty 1 lze model mezivládní spolupráce uvažovat v režimu G to G, nicméně tomuto by musela předcházet v prostředí České republiky legislativní úprava a pravděpodobně pověření vybrané státní agentury pro zajištění veškeré související podpory analogicky jako tomu bylo u přípravy obdobného režimu u zakázek v oblasti obrany a zřízení agentury AMOS. Současně by musela být provedena podrobná analýza, zdali je vhodné obdobný model využívat v oblasti ICT, zdali existuje potenciál obdobného řešení pro digitalizaci více oblastí, aby úsilí vynaložené k této aktivitě bylo účelné, zdali existuje vhodné řešení, které by bylo možné tímto způsobem převzít a zdali vláda země, ve které by toto řešení bylo k dispozici byla přístupná spolupráci v režimu G to G.

IV. Hybridní model v rámci pilotních projektů financovaných EU

- **Projekt POTENTIAL**

Země jako **Francie, Německo, Litva a Lotyšsko** testují různé scénáře použití EUDIW, kombinují státní dohled s technologickými inovacemi soukromého sektoru.

- **Projekt NOBID**

Země jako **Dánsko, Německo, Island, Itálie, Lotyšsko a Norsko** spolupracují na testování platebních funkcí EUDIW, využívají hybridní model spolupráce.

4.3.1 Porovnání modelů

Hybridní modely (Estonsko, Francie, Německo, Lotyšsko, Litva) umožňují kombinovat flexibilitu a inovativnost soukromého sektoru s důvěryhodností a kontrolou státní správy. Stát zajišťuje bezpečnost a správu klíčových funkcí, zatímco soukromé firmy dodávají technologické inovace a rychlou implementaci.

Vládní model (Řecko) spoléhá na státní instituce nebo státní podniky pro veškeré aspekty vývoje a správy digitální identity. Tento model může posílit důvěru občanů ve státní správu dat, ale může být méně flexibilní a pomalejší v implementaci inovací.

Dvofázový model s mezivládní spoluprací (Kypr) umožňuje rychlou implementaci osvědčených řešení z jiných zemí a zároveň zachovává možnost pozdějšího přizpůsobení a rozšíření funkcionalit dle finálních evropských standardů.

4.3.2 Další příklady spolupráce

Finsko – Hybridní model

Finsko pracuje na digitální peněženice v rámci projektu EU, kde státní instituce spolupracují se soukromými firmami, jako je Finnish Digital Agency a soukromí poskytovatelé služeb. Stát zajišťuje správu identity, soukromý sektor přispívá technologickými řešeními.

Belgie – Hybridní model s důrazem na soukromý sektor.

Belgická mobilní aplikace itsme^{®20} byla vyvinuta konsorciem belgických bank a telekomunikačních společností ve spolupráci s vládou. Stát uznává itsme[®] jako oficiální prostředek digitální identity pro přístup k vládním službám.

Aplikace itsme[®] v Belgii není koncesní projekt v tradičním smyslu. Je financována z prostředků konsorcia, které tvoří čtyři největší belgické banky a tři hlavní telekomunikační operátoři, kteří vytvořili konsorcium Belgian Mobile ID. Tyto společnosti do projektu vložily vlastní kapitál, přičemž vláda do něj vstoupila přes státní investiční fond (FPIM/SFPI) s podílem 20 %. Tento podíl je výsledkem investice 14,5 milionu EUR z celkových 24,7 milionu EUR, které byly do projektu vloženy pro další rozvoj aplikace.²¹

Nizozemsko – Veřejně-soukromé partnerství

Nizozemsko využívá model, ve kterém státní správa spolupracuje s komerčními poskytovateli digitálních identit (eHerkenning²²). Stát stanovuje standardy a akredituje poskytovatele, kteří pak nabízejí služby podnikům a občanům.

Španělsko – Vládní model s prvky hybridního přístupu.

Španělsko využívá systém Cl@ve²³, který kombinuje různé metody autentizace, včetně spolupráce s bankami a mobilními operátory pro ověřování uživatelů. Stát spravuje centrální infrastrukturu, ale využívá technologie a služby soukromého sektoru.

Systém Cl@ve slouží k autentizaci a ověřování občanů pro přístup k vládním online službám. Tento systém však není založen na koncesi, ale na certifikaci a uznávání různých způsobů autentizace, které zahrnují spolupráci s bankami a mobilními operátory. Stát spravuje centrální infrastrukturu pro Cl@ve a nabízí různé metody autentizace, jako jsou digitální certifikáty, PIN kódy a cloudové podpisy. Soukromé firmy se podílejí na poskytování těchto technologií, ale ne formou koncese.

20 <https://www.itsme-id.com/en-BE/get-started>

21 <https://thepayers.com/digital-identity-security-online-fraud/belgian-identity-app-itsme-gets-eur-247-mln-to-finance-growth-plans--1250122> , <https://press.telenet.be/belgian-banks-and-mobile-network-operators-launch-itsmer> , <https://nordic9.com/news/itsme-in-a-247-million-investment-round/>

22 <https://www.eherkenning.nl/en>

23 <https://clave.gob.es/clave/Home/clave.html>

Hybridní modely jsou nejčastěji využívané, kombinují výhody státní kontroly a důvěryhodnosti státu a inovačního potenciálu soukromého sektoru včetně flexibility pro přirozený rozvoj daného řešení. **Vládní modely** poskytují vysokou míru důvěry v bezpečnost dat, ale mohou být méně flexibilní. A jsou preferovány v zemích, kde je silná důvěra v státní správu a schopnost státu poskytovat technologická řešení. **Partnerství veřejného a soukromého sektoru** umožňují aktivní zapojení soukromého sektoru při zachování státní regulace a standardů. **Mezivládní spolupráce** umožňuje sdílení osvědčených postupů a technologií mezi státy, urychluje implementaci.

Každý model má své výhody a nevýhody, volba závisí na národních prioritách, legislativním rámci a úrovni důvěry mezi státem, občany a soukromým sektorem. Obecně lze shrnout tak, že zásadním rozdílem uvažovaných modelů je na jedné straně je institucionální pevnost čistě vládních řešení s různě intenzivním vlivem soukromého sektoru v oblasti rozvoje, inovací a hledání obchodních příležitostí na straně hybridních a PPP modelů, kdy PPP modelem se myslí především IPPP.

5 Variantní posouzení

Variantní posouzení analyzuje výhody a nevýhody jednotlivých variant, kterými jsou:

Varianta 1: Poskytovatelem je stát; tedy všechny součásti peněženky jsou provozovány státem i za předpokladu, že dílčí dodávky jsou zajišťovány dodavateli.

Varianta 2: Poskytovatelem je soukromý subjekt – dodávka formou služby; EUDIW peněženka je dodávána soukromým subjektem jako služba dle předem stanovených podmínek v rámci VZ na služby.

Varianta 3: Poskytovatelem je soukromý subjekt – koncese; realizace prostřednictvím poskytnutí koncese soukromému subjektu, dle předem stanovených podmínek v režimu ZZVZ.

Varianta 4: Poskytovatelem je subjekt s majetkovým podílem státu. Vytvoření nového subjektu s majetkovou účastí státu a soukromého kapitálu (nejedná se o státní podnik).

5.1 Přístup k tvorbě cenového modelu

Implementace EUDIW představuje velkou organizační výzvu a značnou finanční zátěž pro státní rozpočet, bez ohledu na zvolenou variantu řešení. Všechny varianty – od plně státem řízeného modelu po modely s partnerstvím se soukromým sektorem – budou vyžadovat zásadní investice do IT infrastruktury, náboru a školení odborníků, bezpečnostních opatření a integrace s národními digitálními systémy. Základní náklady spojené s vývojem a implementací zůstávají vysoké napříč variantami a i v případě, že bude soukromý sektor zapojen, stát bude muset financovat velkou část těchto nákladů. Hlavní rozdíl mezi variantami spočívá v míře zapojení soukromého sektoru a jeho podílu na provozních rizicích, nikoliv ve významném snížení celkových investičních nákladů současně s mírou flexibility umožňující průběžný rozvoj, inovace a hledání obchodních příležitostí, což je z povahy věci doménou soukromého sektoru. Přístup k tvorbě cenového modelu byl strukturován na základě následujícího postupu:

1. **Aplikace metody PERT** – Pro kalkulaci byla zvolena metoda PERT²⁴, která umožňuje pracovat s maximálními a minimálními hodnotami a generovat kontrolovaný průměr výsledných veličin. Tímto postupem byla vygenerována robustní predikce nákladových položek.
2. **Zohlednění specifík státní správy** – v rámci modelu byly využity praktické zkušenosti se státní správou, zejména s přihlédnutím k finančním údajům z tvorby eDokladů a vývoj základních registrů, jejichž nákladovost byla významným vstupním parametrem.
3. **Faktor důvěry** – Klíčovým prvkem v analýze byla kalkulace nákladů na implementaci certifikátů a infrastruktury spojené s jejich správou, kterou standardně hradí stát. Tento faktor byl zásadní pro určení nákladové základny.
4. **Validace odhadů** – Následně proběhlo systematické ověřování, zda jsou uvedené predikce v souladu s odhady stanovenými na úrovni EU, k čemuž byl mimo jiné použit referenční ceník ICT prací²⁵ a odhady nákladů z jiných členských států EU.

Při hodnocení jednotlivých variant analýza vychází z předpokladu, že základní pořizovací náklady na zajištění očekávaného řešení jsou ve všech variantách obdobné. Hlavní rozdíly se projevují v nákladech na straně státu na správu a řízení dodávky a provozu a současně na straně případných dodavatelů s ohledem na zohlednění souvisejících finančních položek, které se liší podle způsobu implementace.

24 <http://books.fs.vsb.cz/SystAnal/texty/26.htm#:~:text=Je%20zobecn%C4%9Bn%C3%ADm%20metody%20kritick%C3%A9%20cesty%20prom%C4%9Bn%C3%A1%20maj%C3%ADe%C3%AD%20ur%C4%8Dit%C3%A9%20rozlo%C5%BEen%C3%AD%20pravd%C4%9Bpodobnosti>

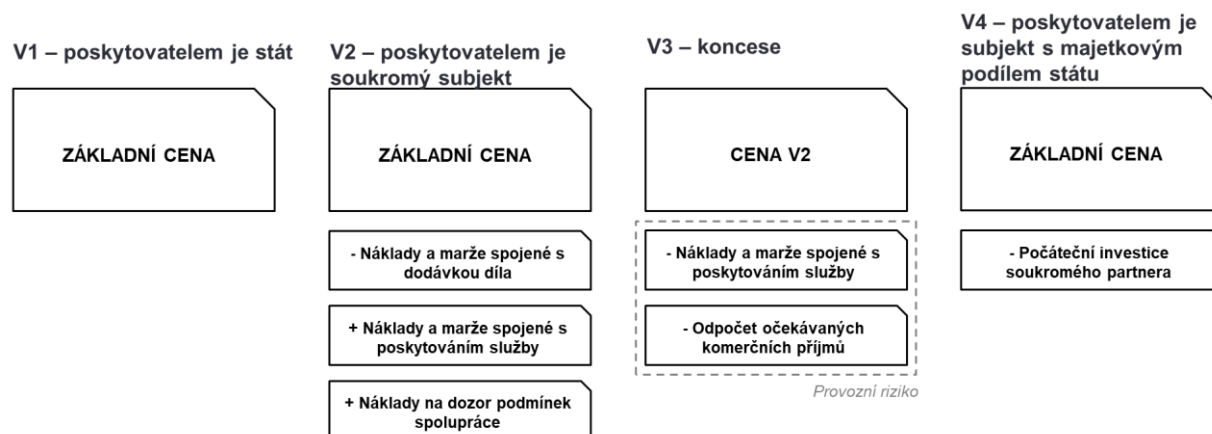
25 Přehled obvyklých cen ICT prací – Ministerstvo vnitra České republiky (mvcr.cz)

EUDIW, především s ohledem na marže a alokaci rizikových položek. Na tomto základě byl vytvořen koncept základní ceny, která je dále modifikována podle specifických parametrů jednotlivých variant.

Stejný přístup byl aplikován při identifikaci příjmových složek cenového modelu. U variant 1 a 2 bylo kalkulováno s příjmy, které lze jednoznačně identifikovat a kvantifikovat již v počátečních fázích. Příkladem může být smlouva s poskytovatelem digitální Peněženky, která naplňuje definiční znaky koncese dle § 174 ZZVZ, za podmínky, že zadavatel definuje parametry služby a vybere poskytovatele, který bude inkasovat platby od uživatelů (např. komerční subjekty či organizace využívající ověřovací služby). Tento model je rovněž spojen s provozním rizikem poskytovatele, přičemž stát neručí za případné ztráty poskytovatele. U variant 3 a 4 jsme naopak předpokládali širší spektrum komerčních aktivit a příjmů.

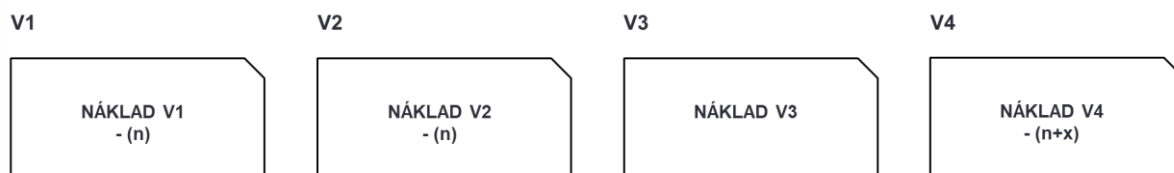
Tento přístup k tvorbě cenového modelu zajišťuje vyvážené a flexibilní financování mezi státem a komerčními subjekty, přičemž důraz byl kladen na optimalizaci nákladů a maximalizaci možných příjmů podle konkrétních variant řešení.

Koncese podle § 174 ZZVZ znamená, že poskytovatel služby nese provozní riziko a inkasuje platby od uživatelů za službu, kterou poskytuje. Zadavatel (stát) definuje parametry služby, ale nenese odpovědnost za případné ztráty poskytovatele. Tento model tedy umožňuje komerčnímu poskytovateli generovat příjmy, přičemž stát má nižší finanční odpovědnost a riziko je přesunuto na poskytovatele.



Stejný přístup byl aplikován při identifikaci příjmových složek cenového modelu. U variant 1 a 2 jsme kalkulovali s příjmy, které lze jednoznačně identifikovat a kvantifikovat již v počátečních fázích. Příkladem může být smlouva s poskytovatelem digitální Peněženky, která naplňuje definiční znaky koncese dle § 174 ZZVZ, za podmínky, že zadavatel definuje parametry služby a vybere poskytovatele, který bude inkasovat platby od uživatelů. Tento model je rovněž spojen s provozním rizikem

poskytovatele, přičemž stát neručí za případné ztráty poskytovatele²⁶. U varianty jsou 3 příjmy kalkulovány v rámci provozního rizika, a nejsou tedy již zahrnuty. Varianta 4 předpokládá možnost rozvoje komerčních aktivit a škála potenciálních příjmů je tedy širší.



²⁶ Smlouva s poskytovatelem Peněženky bude naplňovat definiční znaky koncese podle § 174 ZZVZ, pokud zadavatel definuje parametry služby a bude vybírat nejvhodnějšího poskytovatele, přičemž tato služba může být spojená i s úplatou ze strany zadavatele. Vždy ale musí být spojena s možností inkasovat platby od přímých uživatelů služby (tím není vyloučeno vymezení okruhu uživatelů, kterým bude určitá část služeb dostupná bezplatně) a spojená s provozním rizikem na straně poskytovatele (tj. zadavatel negarantuje, že poskytovatel nebude v provozní ztrátě, přičemž tato případná ztráta nesmí být pouze zanedbatelná). V případě, že by provozní riziko koncesionáře bylo příliš nízké, jednalo by se v daném případě typicky o zadání veřejné zakázky, spíše než koncese. ZZVZ ukládá povinnost postupovat v zadávacím řízení (typicky koncesní řízení, které lze pro tento účel považovat za nejvhodnější), pokud předpokládaná hodnota koncese (kterou se rozumí celkový obrát koncesionáře při poskytování služeb, které jsou předmětem koncese) přesáhne částku 20 mil. Kč bez DPH. Při nižší předpokládané hodnotě se bude jednat o koncesi malého rozsahu, kterou je zadavatel oprávněn zadat mimo zadávací (koncesní) řízení.

V rámci cenového modelu byly identifikovány níže uvedené nákladové položky, kdy ne všechny jsou relevantní pro každou z uvažovaných variant.

(tabulka nákladových položek neposkytnuta)

V rámci cenového modelu byly identifikovány níže uvedené příjmové položky, kdy ne všechny jsou relevantní pro každou z uvažovaných variant.

(tabulka nákladových položek neposkytnuta)

Nad rámec uvedeného je nutné zmínit, že cenový model pracuje s příjmy z komerčních služeb. Zdali budou tyto služby v plném, či částečném rozsahu poskytovány za úplatu a v jaké má být tato úplata výši je rozhodnutí, které musí učinit politická reprezentace a může se v čase vyvíjet a měnit. Níže jsou ve větším detailu popsány přístupy ke stanovení nákladů:

5.1.1 Implementační náklady

(část 5.1.1 neposkytnuta)

5.1.2 Provozní náklady:

(část 5.1.2 s výjimkou následujícího odstavce neposkytnuta)

Nad rámec popsaného je nutné zmínit, že cenový model pracuje s příjmy z komerčních služeb. Zda-li budou tyto služby v plném, či částečném rozsahu poskytovány za úplatu a v jaké má být tato úplata výši je rozhodnutí, které musí učinit politická reprezentace a může se v čase vyvíjet a měnit. Uvažovaný model rovněž nezohledňuje inflaci.

5.2 (nadpis neposkytnut)

(část 5.2 neposkytnuta)

5.3 (nadpis neposkytnut)

(část 5.3 neposkytnuta)

5.4 (nadpis neposkytnut)

(část 5.4 neposkytnuta)

5.5 (nadpis neposkytnut)

(část 5.5 neposkytnuta)

5.6 Návrh / oponentura metrik (SLA) a způsob jejich vykazování ve vztahu k povinnostem poskytovatele, včetně motivace k onboardingu uživatelů i spoléhajících se stran

Pro úspěšnou implementaci EUDIW je klíčové nastavit jasné metriky výkonnosti (SLA) a KPI, které budou dodavatele motivovat k dosažení strategických cílů, včetně aktivního onboardingu uživatelů a spoléhajících se stran. Ve Variantě 1 mají níže uvedené metriky státu sloužit jako vrcholné metriky pro nastaveních SLA dílčích dodavatelů, případně jednoho dodavatele. U Variant 2 – 4 mají být metrikami dodávané služby.

Tyto metriky by měly:

1. **Reflektovat strategické cíle státu:** Měřit aspekty, které jsou pro stát a uživatele nejdůležitější.
2. **Motivovat poskytovatele k excelentnímu výkonu:** Nastavit cíle tak, aby podporovaly neustálé zlepšování služeb a aktivní přístup k onboardingu nových uživatelů a spoléhajících se stran.

Vztah mezi SLA a KPI:

1. **SLA (Service Level Agreement):** Dohoda o úrovni poskytovaných služeb, stanovuje konkrétní metriky a standardy.
2. **KPI (Key Performance Indicators):** Klíčové ukazatele výkonnosti, měří dosažení strategických cílů.

5.6.1.1 Návrh metrik (SLA)

1. **Dostupnost služby:**
 - **Cíl:** 99,8 % dostupnost v režimu 24x7 měsíčně.
 - **Měření:** Automatizované monitorování s měsíčními reporty.
 - **Výjimky:** Plánovaná údržba s předchozím oznámením, výpadky mimo kontrolu poskytovatele (např. ISZR).
 - **Bezodstávkové release:** Podpora nasazení nových verzí bez přerušení služby.
 - **Plánovaná údržba:** Max 1 hodina každé 2 měsíce v době nejnižšího provozu.
2. **Výkonnost a odezva:**
 - **Cíl:** Maximální doba odezvy na uživatelský požadavek **2 sekundy**. Služba zvládne obsloužit cílový počet uživatelů bez degradace výkonu.
 - **Měření:** Testování výkonu v různých podmínkách.
3. **Bezpečnost:**
 - **Cíl:** Žádné kritické bezpečnostní incidenty.
 - **Měření:** Pravidelné bezpečnostní audity, sledování incidentů.
4. **Spolehlivost a chybovost:**

- **Cíl:** Max **0,5 %** chybovost transakcí.
- **Měření:** Analýza logů a uživatelských hlášení.
- **Výjimky:** Chyby na straně spoléhajících se stran nebo trust listů.

5. Přístupnost:

- **Cíl:** Splnění ETSI normy pro QTSP na přístupnost stránek a obsahu a zajištění shody s Úmluvou Organizace spojených národů o právech osob se zdravotním postižením a s požadavky na přístupnost obsaženými ve směrnici (EU) 2019/882.

6. Podpora uživatelů:

- **Cíl:** Rychlost reakce na dotazy L1 podpory do **30 sekund** při telefonickém kontaktu.
- **Měření:** Statistiky call centra, zákaznická spokojenost.

7. Onboarding uživatelů a spoléhajících se stran:

- **Cíl:** Přidání minimálně **500 000** nových uživatelů ročně.
- **Cíl:** Integrace **60** nových spoléhajících se stran ročně.
- **Měření:** Počet aktivních uživatelů a partnerů, měsíční reporty.

5.6.1.2 SLA na fyzický onboarding a podporu

1. Dostupnost onboarding:

- **Cíl:** Onboardingové místo dostupné do 30 minut pro 95 % obyvatel ČR.

2. Dostupnost podpory:

- **L1 podpora:** 24x7 (callcentrum, CzechPOINT, supportní portál).
- **L2 podpora:** 8x7.
- **L3 podpora:** 8x5.

3. Čas na vyřešení incidentů: Standartně dle SLA.

4. Další navrhované metriky:

- **Finanční výkonnost**
 - **Celkové příjmy:** Sledování generovaných příjmů z provozu EUDIW a doplňkových služeb.
 - **Provozní náklady:** Kontrola nákladů spojených s provozem a údržbou systému.
 - **Ziskovost:** Hodnocení čistého zisku nebo ztráty společnosti za dané období.

5. Způsob vykazování:

- **Měsíční reporty:** Detailní zprávy o plnění SLA a KPI.
- **Automatizované systémy monitorování:** Implementace nástrojů pro sledování výkonu a dostupnosti v reálném čase.
- **Audit a ověřování:** Pravidelné nezávislé audity pro ověření přesnosti reportů.

5.6.1.3 *Motivace k onboardingu uživatelů a spoléhajících se stran*

- **Finanční incentivy**
 - **Bonusy za překročení cílů:** Poskytovat finanční odměny za překročení stanovených KPI v oblasti nárůstu uživatelů a partnerů.
- **Marketingová podpora**
 - **Společné marketingové kampaně:** Spolupráce na propagačních aktivitách zvyšujících povědomí o EUDIW.
- **Technická a konzultační podpora**
 - **Snadná integrace:** Poskytování SDK, API a dokumentace pro rychlou integraci spoléhajících se stran.
 - **Školení a workshopy:** Organizace vzdělávacích akcí pro partnery.

Doporučení:

- **Good practices z jiných projektů digitální identity:** Úspěšné programy jako estonský e-Residency ukazují, že klíčovým faktorem pro rozšíření uživatelské základny je uživatelská přívětivost a aktivní podpora zapojení třetích stran.²⁷
- **Flexibilní a škálovatelné řešení:** Systém musí být navržen tak, aby zvládal rostoucí počet uživatelů a transakcí bez ztráty výkonu nebo kvality.
- **Spolupráce s komunitou:** Zapojení uživatelské komunity a partnerů do vývoje a zlepšování služeb může zvýšit jejich loajalitu a angažovanost.

5.6.1.4 *Action points:*

1. **Detailní definice SLA a KPI ve smlouvě**
 - **Přesná formulace metrik:** Zajistit, aby metriky byly jasně definované, měřitelné a dosažitelné.
 - **Sankce a odměny:** Stanovit, jak budou metriky propojeny se sankcemi a incentivy.
2. **Implementace monitorovacích nástrojů**
 - **Technické řešení pro sběr dat:** Zavést spolehlivé systémy pro monitorování a reportování metrik.
 - **Automatizace:** Minimalizovat manuální zásahy pro zvýšení přesnosti a efektivity.
3. **Pravidelná komunikace a zpětná vazba**
 - **Setkání s DIA:** Pravidelné schůzky pro projednání výsledků a plánování zlepšení.
 - **Zpětná vazba od uživatelů:** Využívat průzkumy a další nástroje pro získání názorů uživatelů.

²⁷ <https://www.e-resident.gov.ee/>

4. Podpora inovací

- **Vývoj nových funkcionalit:** Aktivně pracovat na vylepšování EUDIW na základě potřeb trhu.
- **Spolupráce s vývojáři:** Poskytovat podporu nezávislým vývojářům při tvorbě aplikací a služeb využívajících EUDIW.

5.6.1.5 Navrhované KPI

- **Nárůst uživatelů**
 - Cíl: 500 000 nových uživatelů ročně.
 - Celkový cíl: 2 500 000 uživatelů za 5 let.
- **Počet spoléhajících se stran**
 - Cíl: 300 soukromoprávních/státních subjektů využívajících EUDIW po 5 letech.

Jasně definované SLA a KPI spolu s efektivním systémem vykazování a motivace jsou klíčové pro dosažení strategických cílů projektu EUDIW. Poskytují rámec pro monitorování výkonnosti, zajišťují odpovědnost poskytovatele a podporují aktivní zapojení uživatelů a partnerů.

5.7 Dopady na současné uživatele eDokladů (jak z pohledu frontend, tak i z backend). A zároveň posouzení dopadů na scénáře, kdyby eDoklady fungovaly paralelně s EUDIW.

Implementace EUDIW mohou mít dopady na současné uživatele systému eDoklady, a to jak z pohledu uživatelského rozhraní (frontend) – jak osoby prokazující se, tak subjekty ověřující, tak z hlediska systémové infrastruktury (backend). Je také nezbytné posoudit scénáře, kdy by eDoklady a EUDIW fungovaly paralelně, a zvážit možnosti jejich integrace či postupného přechodu.

5.7.1 Současný stav systému eDoklady

Systém eDoklady byl navržen a vyvíjen v roce 2023 s plánovaným spuštěním na začátku roku 2024. Při návrhu architektury byl inspirován ranou architekturou EUDIW, konkrétně verzemi EDIW ARF 1.0.0 (leden 2023), ARF 1.1.0 (duben 2023) a ARF 1.2.0 (červen 2023). Systém eDoklady rovněž implementuje požadavky dle normy ISO18013-5 pro scénář předávání dokladů v blízkosti (proximity) prostřednictvím Bluetooth mezi mobilními zařízeními.

Podle dostupné dokumentace a veřejných informací systém eDoklady implementuje následující prvky EUDIW:

- **Doklad občanského průkazu jako mdoc atestací dle normy ISO18013-5**
- **Vydávání dokladů do mobilní aplikace**
- **Předávání dokladů scénářem mobil-mobil dle normy ISO18013-5**
- **Vzdálené předávání dokladů OpenID4VP**
- **Bezpečnostní mechanismy řešení dle normy ISO18013-5**
- **Architektonická a technická příbuznost s EUDIW**

Systém EUDIW je mnohem komplexnější a jeho standardy ještě nejsou finálně ukotveny. Nicméně architektonická a technická příbuznost mezi systémy eDoklady a EUDIW bude mít pozitivní dopad na jednodušší přechod a migraci uživatelů, ať už držitelů dokladů nebo čtenářů dokladů, ze systému eDoklady na EUDIW. Tato podobnost otevírá možnost uvažovat o systému eDoklady také jako o záložní variantě pro projekt EUDIW v České republice, za předpokladu dodatečných investic do tohoto systému.

Aby bylo možné eDoklady využít jako záložní řešení pro EUDIW, je nutné detailně rozpracovat analýzu a návrh takového řešení. Tento návrh by měl zahrnovat zejména:

1. **Gap analýzu architektury systému eDoklady z pohledu EUDIW:** Identifikaci prvků cílové architektury EUDIW, které jsou v eDokladech již implementovány, a těch, které chybí.

2. **Návrh a implementaci požadavků EUDIW do eDokladů pro záložní variantu:** Realizaci minimálně nutných požadavků dle nařízení eIDAS2.0, aby systém eDoklady mohl sloužit jako záložní řešení EUDIW. To je v souladu s požadavkem:

"Stát bude provozovat vlastní záložní řešení EUDIW, které bude realizovat minimálně nutné požadavky eIDAS2.0 a bude připraveno k zahájení provozu do dvou měsíců po inicializaci kritického stavu..."

- **Aktivační plán:** Plán aktivace v rámci systému eDoklady na EUDIW, včetně časového harmonogramu a komunikační strategie.

5.7.2 Scénáře po spuštění EUDIW

Po spuštění systému EUDIW se nabízejí následující scénáře týkající se provozu eDokladů:

1. Pokračování provozu eDokladů bez rozšíření na záložní řešení EUDIW

- Různé chování aplikací eDoklady a EUDIW může vést k nejednotné uživatelské zkušenosti pro držitele i čtenáře dokladů.
- Komplikace při integraci systémů třetích stran (relying parties), které by musely podporovat oba systémy.
- **Legislativní dopady:** Potřeba udržovat dva systémy v souladu s legislativou může zvýšit komplexnost právního rámce.
- **Dopad na náklady:** Zvýšené finanční náklady na provoz a údržbu dvou paralelních systémů.
- **Odhad adopce:** Možné zmatení uživatelů může zpomalit adopci EUDIW.

2. Pokračování provozu eDokladů s rozšířením na záložní řešení EUDIW

- Umožňuje využití stávajícího systému eDoklady jako záložního řešení pro EUDIW.
- Zajišťuje kontinuitu služeb a efektivní využití již vynaložených investic.
- Usnadňuje migraci uživatelů díky známému prostředí a funkcionalitám.
- **Legislativní dopady:** Integrace eDokladů do EUDIW může být legislativně méně náročná díky architektonické podobnosti. Nutná úprava legislativy ve vztahu k eDokladům.
- **Dopad na náklady:** Optimalizace nákladů díky využití stávající infrastruktury a technologií.
- **Odhad adopce:** Vyšší důvěra uživatelů a plynulejší přechod mohou zvýšit míru adopce EUDIW.
- **Dopad na profit z EUDIW:** Efektivní využití stávajícího systému může zvýšit finanční přínosy z implementace EUDIW.

3. Úprava ověřovacích aplikací eDokladů pro využívání EUDIW

- Ověřovací aplikace v ekosystému eDokladů budou upraveny tak, aby umožnily ověřovat také evropské peněženky.
- **Legislativní dopady:** Integrace části eDokladů do EUDIW může být legislativně méně náročná díky architektonické podobnosti. Nutná úprava legislativy ve vztahu k eDokladům.
- **Dopad na náklady:** Využití části dosavadní investice.
- **Odhad adopce:** Může být pozitivně vnímáno u ověřujících subjektů,

4. Ukončení provozu eDokladů a přeregistrace uživatelů do EUDIW

- Nutnost přeregistrace všech stávajících uživatelů do nového systému, což může být administrativně náročné a může vést ke ztrátě části uživatelské základny.
- Ztráta investic do stávajícího systému eDoklady.
- Riziko porušení udržitelnost EU podpory – riziko sankcí.
- **Legislativní dopady:** Potřeba zajistit soulad s legislativou během přechodu a ukončení starého systému. **Rozpor s Článkem 5a odst. 15 revize Nařízení.**
- **Dopad na náklady:** Náklady spojené s ukončením provozu eDokladů a migrací uživatelů.
- **Odhad adopce:** Riziko snížení důvěry uživatelů a pomalejší adopce EUDIW.

5.7.2.1 Posouzení variant

Z pohledu posouzení jednotlivých výše uvedených možností se jeví jako optimální Pokračování provozu eDokladů s rozšířením na záložní řešení EUDIW, jelikož:

- Kombinuje využití stávajícího řešení eDoklady a zajišťuje záložní řešení pro EUDIW, což je v souladu s požadavky nařízení eIDAS2.0.
- Minimalizuje dopady na uživatele a čtenáře dokladů, kteří nebudou nuceni provádět zásadní změny v používání aplikace.
- Efektivně využívá již vynaložené investice do vývoje a provozu systému eDoklady.
- Snižuje rizika spojená s legislativními změnami a náklady na migraci.

V patrnosti by rovněž měla být možnost kdy dojde k Úpravě ověřovacích aplikací eDokladů pro využívání EUDIW.

Integrace systému eDoklady jako záložního řešení pro EUDIW představuje strategickou příležitost pro Českou republiku. Tento přístup podporuje hladký přechod na EUDIW, minimalizuje legislativní a finanční rizika a zajišťuje kontinuitu digitálních služeb pro občany. Realizace vyžaduje důkladnou analýzu, plánování a aktivní komunikaci se všemi zainteresovanými stranami.

5.8 Identifikace souvisejících nákladů na straně státu

Implementace EUDIW v režii státu s sebou nese nejen přímé investice do vývoje a provozu systému, ale také řadu souvisejících nákladů. Tyto náklady jsou spojené s posilováním stávajících národních infrastruktur, jako je Národní identifikační autorita (NIA), integrací s dalšími systémy, zajištěním kybernetické bezpečnosti, legislativními úpravami a vzděláváním veřejnosti. Identifikace a plánování těchto nákladů je klíčové pro úspěšnou realizaci projektu a minimalizaci rizik spojených s jeho provozem.

5.8.1 Posílení Národní identifikační autority (NIA)

5.8.1.1 Technické aspekty

- **Kapacitní rozšíření:** NIA bude muset zvládnout zvýšený objem autentizačních požadavků a transakcí spojených s EUDIW.
 - *Náklady:* Investice do serverové infrastruktury, databází a síťových technologií.
- **Technologické upgrady:** Modernizace systémů NIA pro zajištění kompatibility a interoperability s EUDIW.
 - *Náklady:* Vývoj a implementace nových softwarových modulů, licenční poplatky.

5.8.2 Posílení Informačního systému sdílené služby (ISSS)

5.8.2.1 Technické aspekty

- **Kapacitní rozšíření:** ISSS bude muset zvládnout zvýšený objem požadavků a transakcí spojených s EUDIW (získávání údajů z publikačních AIS).
 - *Náklady:* Investice do serverové infrastruktury, databází a síťových technologií.
- **Technologické upgrady:** Modernizace systémů ISSS pro zajištění kompatibility a interoperability s EUDIW (ověřování atributů)
 - *Náklady:* Vývoj a implementace nových softwarových modulů.

5.8.2.2 Personální aspekty

- **Nábor odborníků:** Zvýšená potřeba IT specialistů, bezpečnostních analytiků a administrátorů.
 - *Náklady:* Mzdy, školení, benefity pro nové zaměstnance.
- **Školení stávajícího personálu:** Aktualizace znalostí a dovedností současných zaměstnanců DIA.
 - *Náklady:* Vzdělávací programy, certifikace.

5.8.2.3 *Integrace s existujícími systémy a službami*

- **Propojení s eGovernment službami:** Zajištění hladké komunikace mezi EUDIW a národními elektronickými službami.
 - *Náklady:* Vývoj integračních rozhraní (API), testování a ladění systémů.
- **Datová migrace:** Přenos a synchronizace dat mezi stávajícími databázemi a novým systémem.
 - *Náklady:* Analýza dat, vývoj migračních nástrojů, ověření integrity dat.
- **Pokročilá bezpečnostní opatření:** Implementace nejmodernějších technologií pro ochranu proti kybernetickým hrozbám.
 - *Náklady:* Nákup bezpečnostních řešení, jako jsou firewall systémy, intrusion detection/prevention systémy.
- **Bezpečnostní audit a certifikace:** Pravidelné kontroly zranitelností a souladu s bezpečnostními standardy.
 - *Náklady:* Služby externích auditorů, poplatky za certifikace.
- **Koordinace mezi úřady:** Spolupráce různých státních institucí pro sjednocení procesů a standardů.
 - *Náklady:* Projektový management, meziresortní komise, administrativní podpora.
 - **Kybernetická bezpečnost**
- **Incident Response Team:** Vytvoření specializovaného týmu pro rychlou reakci na bezpečnostní incidenty.
 - *Náklady:* Mzdy, školení, vybavení týmu.
 - **Legislativní a regulační náklady**
- **Úprava legislativy:** Aktualizace zákonů a vyhlášek pro podporu a regulaci EUDIW.
 - *Náklady:* Práce legislativců, právní analýzy, veřejné konzultace.
- **Soulad s evropskými předpisy:** Zajištění plné kompatibility s nařízeními EU.
 - *Náklady:* Právní poradenství, překlady dokumentace, účast na evropských pracovních skupinách.

5.8.2.4 *Veřejná osvěta a vzdělávání*

1. Marketingové aspekty

- **Informační kampaně:** Zvýšení povědomí občanů o EUDIW, jejích výhodách a způsobu použití.
 - *Náklady:* Reklamní spoty, online kampaně, tiskové materiály.

2. Vzdělávací aspekty

- **Školení pro veřejnost:** Organizace workshopů, webinářů a příruček pro uživatele.
 - *Náklady:* Vývoj vzdělávacích programů, honoráře lektorů.
 - **Školení a rozvoj kapacit**

3. Personální aspekty

- **Školení zaměstnanců veřejné správy:** Zajištění, aby úředníci rozuměli EUDIW a uměli jej integrovat do své agendy.
 - *Náklady:* Interní školení, externí kurzy, e-learningové platformy.

4. Technické aspekty

- **Podpora spoléhajících se stran:** Poskytnutí nástrojů a dokumentace pro integraci EUDIW do jejich systémů.
 - *Náklady:* Technická podpora, vývoj SDK, konzultační služby.
 - **Operační náklady a infrastruktura**
- **Údržba a aktualizace:** Pravidelné servisní práce na infrastruktuře EUDIW a souvisejících systémech.
 - *Náklady:* Servisní smlouvy, aktualizace softwaru, náhradní díly.

5. Organizační aspekty

- **Administrativní podpora:** Zvýšení administrativní zátěže vyžaduje navýšení personálu.
 - *Náklady:* Mzdy administrativních pracovníků, kancelářské potřeby.

5.8.2.5 Rezerva na nepředvídané náklady

Finanční aspekty

- **Kontingenční fond:** Finanční rezerva pro pokrytí neočekávaných výdajů, jako jsou bezpečnostní incidenty nebo technické závady.
 - *Náklady:* Alokace části rozpočtu pro krizové situace.

Příklady z praxe:

Německo

- **Posílení Bundesdruckerei:** Německá vláda investovala i do státní tiskárny, která spravuje národní identifikační systémy, aby zvládla integraci s EUDIW.
 - *Náklady:* Modernizace technologií, nábor IT odborníků.

Rakousko

- **Kampaně na zvýšení povědomí:** Rakousko investovalo do rozsáhlých informačních kampaní pro podporu adopce digitálních identit, což se promítlo v adopci.
 - *Náklady:* Reklama v médiích, veřejné akce, online platformy.

Celkové související náklady na straně státu mohou výrazně navýšit investice potřebné pro implementaci a provoz EUDIW. Tyto náklady jsou však nezbytné pro zajištění funkčnosti, bezpečnosti a široké adopce systému mezi občany a spoléhajícími se stranami. Důkladné plánování a alokace zdrojů do těchto oblastí je klíčové pro úspěch projektu a dosažení strategických cílů v oblasti digitalizace veřejné správy.

5.8.2.6 Doporučení

- **Komplexní rozpočtování:** Zahrnout související náklady do celkového rozpočtu projektu EUDIW.
- **Fázová implementace:** Rozložit investice do jednotlivých fází projektu pro efektivnější řízení nákladů.
- **Meziresortní spolupráce:** Využít synergie mezi různými státními institucemi pro optimalizaci nákladů.
- **Vyhledávání externího financování:** Aktivně hledat možnosti financování z fondů EU nebo mezinárodních grantů.

Plánování a identifikace souvisejících nákladů umožní státu připravit se na výzvy spojené s implementací EUDIW a zajistí, že systém bude dlouhodobě udržitelný, bezpečný a užitečný pro všechny zúčastněné strany.

6 Závěry a rekapitulace

Implementace EUDIW v prostředí České republiky bude představovat zajisté technologickou, organizační i finanční výzvu. Sumarizace výsledků je uvedena v manažerském shrnutí. Níže jsou uvedena další doplnění a shrnutí.

6.1 Doplnění a shrnutí faktorů ovlivňujících cenový model

Níže jsou uvedeny souhrnné faktory ovlivňující cenový model.

6.1.1 Potenciální příjmy z provozu EUDIW

Ve všech variantách je možné počítat s potenciálními příjmy z provozu EUDIW. Ty mohou zahrnovat paušální poplatky pro spoléhající se strany za připojení do systému, což je standardní model u digitálních identit. Varianta 3 a 4 nabízí větší potenciál příjmů, protože komerční partneři budou motivováni maximalizovat efektivitu systému a komercializovat doplňkové služby, současně díky tomu, že smluvní modely umožňují ponechat prostor pro rozvoj obchodních příležitostí.

6.1.2 Doplňkové komerční služby

Varianty 3 a 4 mohou nabídnout komerčním subjektům možnost poskytování doplňkových služeb. Mohou zahrnovat např. personalizované řešení pro bankovní sektor nebo rozšířené verze EUDIW pro soukromé firmy. Tyto doplňkové služby mohou generovat další příjmy pro poskytovatele a zvýšit atraktivitu systém.

6.1.3 Faktory ovlivňující nepřesnosti a rizika napříč variantami

Regulační změny mohou vyžadovat úpravy systému a zvýšit náklady. Aby se minimalizovalo toto riziko, je nezbytné aktivně sledovat legislativu. To zahrnuje pravidelné monitorování změn v národní a evropské legislativě a zapojení se do legislativního procesu prostřednictvím připomínek a konzultací. Tím lze předcházet nepředvídaným legislativním požadavkům a zajistit, že systém bude v souladu s aktuálními právními normami.

Významnou mírou nepřesnosti je absence, nepřesnost, či budoucí změny implementačních aktů. Tuto nejistotu je možné řešit několika způsoby. Částečně může být ošetřeno v rámci řízení o inovačním partnerství, ale především určitým rozvojovým budgetem (Varianty 1, 2 a 4), který by navazující změny pokryl. Paušální požadavek na dodavatele pro průběžné zohledňování změn v implementačních aktech považujeme za nereálný, jelikož představuje enormní finanční riziko. U Varianty 3 je možné tento faktor zohlednit jako riziko koncesionáře.

Technologický vývoj může vyvolat potřebu integrace nových technologií, což může ovlivnit původní finanční plány a způsobit dodatečné náklady. Řešením je udržovat technologickou agilitu tím, že se investuje do flexibilních systémů a otevřených standardů. Udržování partnerských vztahů s technologickými lídry umožní rychle reagovat na nové trendy a začleňovat inovace do systému bez výrazného narušení jeho fungování.

Bezpečnostní hrozby mohou vyžadovat dodatečné investice do zabezpečení a mohou ohrozit důvěru uživatelů v systém. Proaktivní bezpečnostní strategie je klíčová pro minimalizaci těchto rizik. To zahrnuje implementaci nejnovějších bezpečnostních standardů a postupů a pravidelné provádění bezpečnostních auditů a penetračních testů. Tím lze odhalit a odstranit potenciální zranitelnosti dříve, než dojde k jejich zneužití.

Nízká uživatelská akceptace může snížit očekávané příjmy a ohrozit udržitelnost projektu. Efektivní komunikační strategie může tento problém řešit. Realizace osvětových kampaní o výhodách a bezpečnosti EUDIW zvýší povědomí a důvěru veřejnosti. Zapojení uživatelů do vývoje prostřednictvím pilotních projektů a sběru zpětné vazby umožní lépe přizpůsobit systém jejich potřebám a zvýší míru jeho přijetí.

Makroekonomické podmínky mohou ovlivnit dostupnost financí a náklady na provoz a rozvoj systému. Finanční plánování s rezervami je proto nezbytné. Zahrnutí rezerv pro nepředvídané ekonomické výkyvy do finančních plánů umožní lépe zvládat nejistoty. Diversifikace zdrojů financování, včetně hledání možností spolufinancování z evropských fondů, jako jsou například fondy Evropské unie, může také pomoci rozložit finanční rizika a zajistit stabilitu projektu v dlouhodobém horizontu.

Identifikace možných zdrojů nepřesností a rizikových faktorů je zásadní pro úspěšnou implementaci EUDIW. Každá varianta přináší specifické výzvy pro stát, komerční partnery i uživatele. Implementace navržených řešení v bodech umožní minimalizovat nepřesnosti v odhadech a zvýšit pravděpodobnost úspěchu projektu. Rozhodovací proces by měl zohlednit nejen finanční aspekty, ale také strategické cíle, technologické trendy a potřeby občanů.

6.2 Celkové shrnutí monopolního postavení dodavatele

Riziko monopolního postavení poskytovatele EUDIW je významné zejména u variant, kde je služba svěřena komerčnímu subjektu nebo společnosti s majetkovou účastí státu. Níže uvádíme několik klíčových zásad pro minimalizaci těchto rizik.

1. Transparentní a férové smluvní podmínky

Umožňují flexibilitu a chrání zájmy státu i uživatelů. Jasné definované smlouvy s možností změny poskytovatele snižují riziko závislosti na jednom dodavateli.

1. Efektivní regulační dohled

Nezávislé orgány monitorují činnost poskytovatele a mohou zasáhnout při zneužití postavení. Regulační dohled zajišťuje dodržování smluvních podmínek a ochranu veřejného zájmu.

3. Podpora konkurenčního prostředí

Motivuje poskytovatele k inovacím a poskytování kvalitních služeb. Umožnění vstupu dalších subjektů na trh zabraňuje vzniku monopolů.

4. Oddělení rolí státu

Zabraňuje střetu zájmů a narušení trhu. Jasné vymezení rolí státu jako vlastníka a regulátora podporuje férovou soutěž.

Obecně lze konstatovat, že Varianty 2 a 3 nutně poskytnou subjektu, který zvítězí ve veřejné soutěži, komerční výhodu a náskok oproti ostatním účastníkům. Stát musí zajistit, aby smluvní podmínky zajišťovali, aby tato komerční výhoda byla co nejmenší a byla vyvážena přínosy pro stát. Pro zajištění zmenšení této výhody je nutné v rámci soutěže a smluvního zajištění aplikovat doporučení z této kapitoly. Situace se může dotýkat i Varianty 1 v případě, že stát nebude schopen a) zajistit si vývoj vlastními silami (což lze předpokládat); b) v rámci výběru dodavatele jednotlivých součástí nebude dodržena potřebná granularita a distribuce řešení mezi více dodavateli.

6.3 Další doporučení k minimalizaci rizik monopolního postavení a vendor lock-in

Napříč všemi variantami je důležité zaměřit se na strategické oblasti:

- **Využití open-source technologií:** Upřednostnění open-source softwaru a technologií při vývoji EUDIW snižuje závislost na jednom dodavateli a umožňuje komunitní podporu a vývoj.
- **Poskytnutí vytvořených produktů jako open-source:** Vymezení součástí EUDIW, které mají být poskytovatelem zpřístupněny jako open-source.
- **Stanovení podmínek veřejné soutěže:** V rámci veřejné soutěže je nutné nastavit takovou sadu opatření a podmínek, aby bylo možné zneužití postavení subjektu, který byl soutěží vybrán.
- **Standardizace a interoperabilita na evropské úrovni:** Aktivní účast České republiky v pracovních skupinách EU zajistí kompatibilitu mezi systémy různých zemí a usnadní přeshraniční služby²⁸.
- **Pravidelné bezpečnostní audity:** Provádění nezávislých bezpečnostních auditů.
- **Implementace flexibilních smluvních ustanovení:** Zařazení inovačních klauzulí do smluv umožní integraci nových technologií během trvání smlouvy, což zajistí aktuálnost systému.²⁹ (Za předpokladu dodržení regulačních a dalších požadavků, např. smluvních.)

6.3.1 Zajištění služeb nezávislého arbitra

Využití služeb nezávislého arbitra pro dohled nad implementací EUDIW z hlediska předcházení rizik monopolního postavení a vendor lock-in po celou dobu provozu.

- **Nezávislý dohled:** Arbitr není přímo spojen s žádným z dodavatelů ani s vládními orgány odpovědnými za implementaci, což mu umožňuje objektivně posuzovat situaci.
- **Odborné znalosti:** Disponuje hlubokými znalostmi v oblasti IT či veřejných zakázek, legislativy a standardů, aby mohl kvalifikovaně posoudit technické a právní aspekty projektu.
- **Předcházení monopolizaci:** Sleduje, aby žádný dodavatel nezískal dominantní postavení, které by mu umožnilo ovlivňovat trh nebo omezovat konkurenci.
- **Ochrana investic:** Předchází vendor lock-inu. Zajišťuje, že stát může v budoucnu snadno upravovat nebo rozšiřovat systém bez závislosti na jediném dodavateli.

²⁸ Evropská komise (2020): eIDAS Cooperation Network. <https://digital-strategy.ec.europa.eu/en/policies/european-digital-identity-cooperation-group>

²⁹ Evropská komise (2018): Guidance on Innovation Procurement. <https://ec.europa.eu/docsroom/documents/29261>

- **Otevřenost a transparentnost:** Podporuje používání technologií a řešení, která umožňují snadný přechod k jiným dodavatelům, pokud by to bylo potřeba.
- **Podpora inovací:** Otevřená konkurence motivuje dodavatele k inovacím a poskytování kvalitnějších služeb za lepší cenu.

6.4 Příklady dobré praxe

6.4.1 V České republice

- **Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB):** Funguje jako nezávislý orgán dohledu nad kybernetickou bezpečností a může poskytovat doporučení a metodiky pro minimalizaci rizik vendor lock-inu.
- **Úřad pro ochranu hospodářské soutěže (ÚOHS):** Dohlíží na transparentnost veřejných zakázek a může zasahovat v případech, kdy hrozí monopolizace trhu nebo neférové praktiky.

6.4.2 V Evropské unii

- **Evropská komise – Direktorát pro hospodářskou soutěž:** Sleduje a reguluje trh, aby zabránila monopolnímu postavení firem, zejména v oblasti digitálních služeb.
- **Evropská agentura pro kybernetickou bezpečnost (ENISA):** Poskytuje doporučení pro bezpečnou a interoperabilní implementaci digitálních řešení v EU, podporuje používání otevřených standardů.
- **Projekt eIDAS Observatory:** Slouží jako platforma pro sdílení informací a sledování implementace eIDAS 2.0 napříč členskými státy, zajišťuje transparentnost a výměnu osvědčených postupů.

6.4.3 V jiných zemích:

Spojené království – Government Digital Service (GDS): Organizace, která dohlíží na digitální projekty vlády, zajišťuje, že jsou dodržovány principy otevřených standardů a minimalizuje se riziko vendor lock-inu.

6.5 Další poznámky a doporučení

- **Vyloučení zvýhodnění³¹:** Je nutné zajistit vyloučení zvýhodnění dle Nařízení Komise.
- **Expertní poradenství a externí dozor:** Zapojení nezávislých expertů z akademické i soukromé sféry při klíčových rozhodnutích přináší **nový pohled a pomáhá předcházet přehlédnutí potenciálních rizik.**
- **Finanční transparentnost a kontrola nákladů:** Detailní rozpočtování a průběžné monitorování nákladů zabrání překročení rozpočtu a pomůže identifikovat oblasti pro úspory.
- **Právní analýzy:** Pravidelné právní kontroly zajistí, že všechny kroky projektu jsou v souladu s aktuální legislativou, což předchází právním sporům a možným sankcím.
- **Mezinárodní spolupráce a sdílení know-how:** Zapojení do evropských iniciativ, jako je Connecting Europe Facility (CEF) Digital³⁰, umožní České republice těžit z kolektivních zkušeností a inovací.

Úspěšná implementace EUDIW v České republice bude vyžadovat kombinaci pečlivého plánování, transparentnosti, odbornosti a široké spolupráce mezi veřejným a soukromým sektorem. Klíčové je udržovat flexibilitu projektu, aby mohl reagovat na rychle se měnící technologické prostředí a legislativní požadavky. Bezpečnost a ochrana uživatelských dat musí být samozřejmě prioritou ve všech fázích projektu.

³⁰ Evropská agentura pro provozní řízení rozsáhlých IT systémů (eu-LISA): <https://www.eulisa.europa.eu/>

³¹ PRÁVNÍ ANALÝZA SOUVISEJÍCÍ S REVIZÍ NAŘÍZENÍ EIDAS

6.6 Manažerské shrnutí

Implementace EUDIW v prostředí České republiky bude představovat zajisté technologickou, organizační i finanční výzvu. Analýza shrnuje potenciální nevýhody a výhody jednotlivých variant, kterými jsou:

- **Varianta 1: Poskytovatelem je stát;**
- **Varianta 2: Poskytovatelem je soukromý subjekt – dodávka formou služby;**
- **Varianta 3: Poskytovatelem je soukromý subjekt – koncese;**
- **Varianta 4: Poskytovatelem je subjekt s majetkovým podílem státu.**

6.6.1 K variantě 1 - Poskytovatelem je stát:

Varianta předpokládá, že poskytovatelem EUDIW bude stát s tím, že jednotlivé komponenty si zajistí dodavatelsky. Na dodavatele rovněž může přenést část rizik spojených s dodržováním SLA. Co se týče realizace, jednalo by se o extrémně náročný projekt jak z pohledu řízení projektu, TD a QA. Cenově vychází jako třetí nejvýhodnější, nicméně je nutné zdůraznit jeden aspekt, který může do modelu výrazně vstoupit a tím je případná investiční dotace ze strany EU, která by mohla pokrýt významnou část investičních nákladů. Zatím vhodný dotační titul nebyl identifikován.

6.6.2 K variantě 2 - Poskytovatelem je soukromý subjekt – dodávka formou služby

Druhá varianta předpokládá, že si stát zajistí poskytování EUDIW jako službu u komerčního poskytovatele v režimu ZZVZ formou služby. s ohledem na předpoklad, že si dodavatel do nabídkové ceny zohlední k celkovým nákladům na vybudování řešení provozní marže, řízení rizik i položku pro financování, jeví se tato varianta jako nejnákladnější. Tento aspekt by se dále prohluboval při prodloužení posuzovaného období. Současně je nutné zmínit, že dle názoru zpracovatele neumožňuje tento model využití platformy pro rozvojové komerční služby, které nebude možné definovat před zahájením zadávacího řízení.

6.6.3 K variantě 3 - Poskytovatelem je soukromý subjekt – koncese

Třetí varianta předpokládá využití koncese pro zajištění poskytovatele EUDIW. Tato varianta by zajistila koncesionáři relativní volnost pro rozvoj obchodních příležitostí, která by měla být vyváжена snížením nákladů na straně státu a to včetně přenesení rizik. Převážnou část těchto rizik by měl koncesionář vyvážit vlastními obchodními příležitostmi. Tato varianta vychází jako druhá nejvýhodnější.

Provozní riziko je v tomto cenovém modelu kalkulováno jako součet očekávané marže a veškerých potenciálních komerčních příjmů ze stanovené hodnoty paušální platby za poskytování služby, ekvivalentně dle Varianty 2. Model je pro Variantu 3 nastaven tak, aby koncesionář pro dosažení ekonomických indikátorů případného budoucího dodavatele ve Variantě 2 musel příjmy za poskytování komerčních služeb pokrýt přibližně 30 % ze stanovené hodnoty paušální platby za poskytování služby.

Úplata v rámci koncesní smlouvy = Vypočtená hodnota paušální platby za poskytování služby – (očekávaná marže + potenciální komerční příjmy)

6.6.4 K variantě 4 - Poskytovatelem je subjekt s majetkovým podílem státu

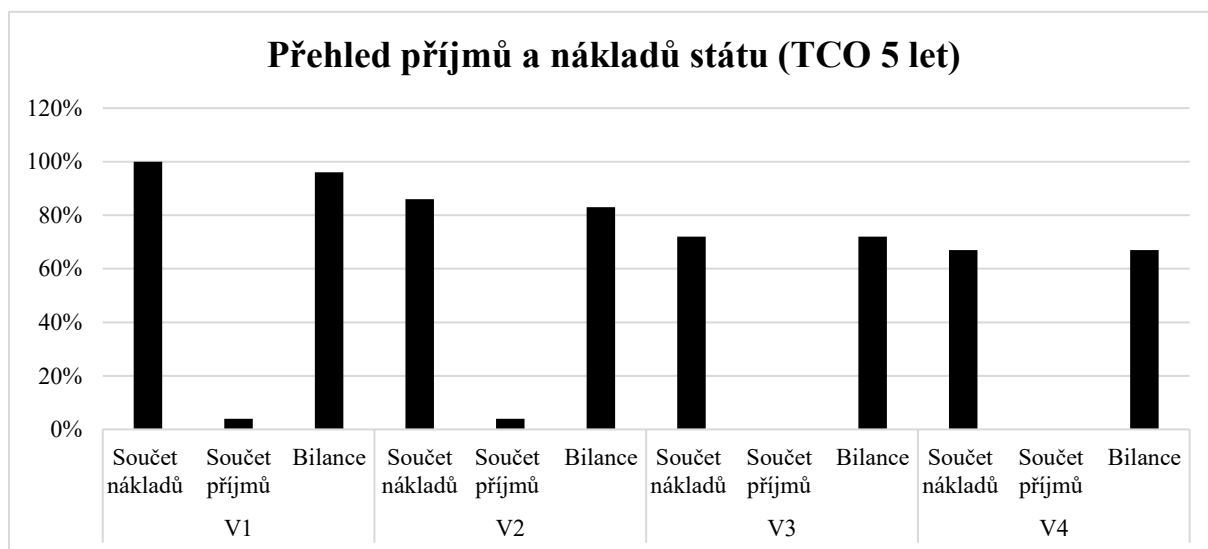
Poslední posuzovaná varianta je variantou institucionální spolupráce mezi státem a soukromým sektorem. Model vychází jako cenově nejvýhodnější, jelikož předpokládá proinvestování úvodních investičních nákladů ze strany soukromého sektoru oproti závazku státu využívat služby tohoto podniku po stanovenou dobu. Zásadním problémem je legislativní neukotvení tohoto režimu. Alternativou pro toto řešení není státní podnik.

K cenovému modelu je nutné zmínit faktor inflace a tzv. „ceny peněz“, kdy je nutné vzít v potaz náklady na financování státního dluhu, v případě přípravy veřejné zakázky, postupů finanční kontroly a nutné alokace finančních prostředků již před zahájením plnění kontraktu a náklady všech variant můžou být těmito dvěma faktory ovlivněny.

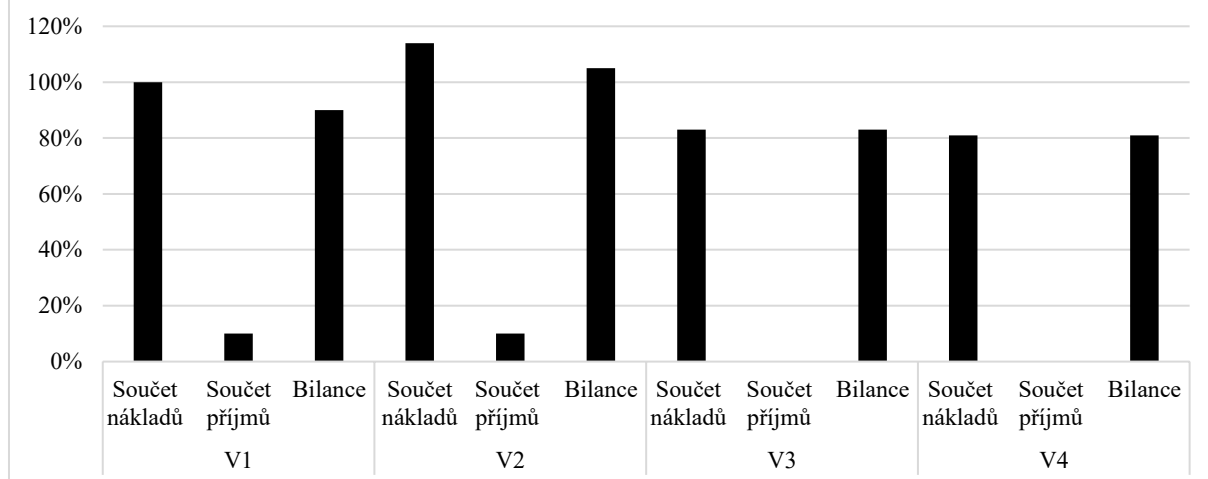
Co se posouzení předložených variant týče, nelze jednoznačně identifikovat cenově nejvýhodnější variantu. s jistotou s přihlédnutím ke zbývajícím třem variantám lze konstatovat, že nejméně cenově výhodná je varianta 2 – dodávka formou služby. Nákladový rozdíl mezi variantou 3 – Poskytovatelem je soukromý subjekt – koncese a variantou 4 – Poskytovatelem je subjekt s majetkovým podílem státu není dle této analýzy významný, nicméně může být ovlivněn na jedné straně soutěží v rámci koncesního řízení, na druhé straně ochotou akceptovat přísné, státem stanovené podmínky pro vstup do společného podniku. Významným faktorem, který limituje využití varianty 4 – Poskytovatelem je subjekt s majetkovým podílem státu, je časový aspekt a stávající legislativní rámec. Varianta 1 je standardní dodávkou řešení pro stát a to jak v režii dílčích dodávek, tak řešení na klíč, s čímž má stát již dostatečné zkušenosti. Významný faktor ve prospěch této varianty může hrát případná investiční dotace pro pokrytí investičních nákladů. Současně je nutné zmínit, že riziko potencionálních komerčních příjmů jde u variant 1 a 2 za státem, u variant 3 a 4 je přeneseno na dodavatele.

Tabulka: Příjmy a náklady na straně státu

		TCO 5 let	TCO 10 let
V1	Součet nákladů (základní cena)	100 %	100 %
	Součet příjmů	4 %	10 %
	<u>Bilance</u>	<u>96 %</u>	<u>90 %</u>
V2	Součet nákladů	86 %	114 %
	Součet příjmů	4 %	10 %
	<u>Bilance</u>	<u>82 %</u>	<u>104%</u>
V3	Součet nákladů	72 %	83 %
	Součet příjmů	0 %	0 %
	<u>Bilance</u>	<u>72 %</u>	<u>83 %</u>
V4	Součet nákladů	67 %	81 %
	Součet příjmů	0 %	0%
	<u>Bilance</u>	<u>67 %</u>	<u>81 %</u>



Přehled příjmů a nákladů státu (TCO 10 let)



7 Výhrady a omezení

Společnost EY jako zpracovatel této studie si vyhrazuje uvést níže uvedené skutečnosti:

1. Cenové údaje představují odborné odhady expertního týmu, které vycházejí z dosavadních zkušeností EY a zdrojů napříč EU. Je důležité ovšem zmínit, že řešení EUDIW je ve své podstatě unikátní a může docházet k dalším úpravám cen a to i s ohledem na průběžné změny a úpravy dokumentace EUDIW ze strany EU.
2. Tato analýza byla zpracována v limitovaném časovém okně 28 dnů (od 6. 9. 2024 do 3. 10. 2024), což byla podmínka stanovená v rámci veřejné zakázky Digitální informační agenturou. Analýza vychází ze skutečností, které mohly být v tomto období dostupné a přístupné, nebo je bylo možné ve výše uvedené lhůtě obstatat.
3. Analýza plně reflektuje výstupy PRÁVNÍ ANALÝZY SOUVISEJÍCÍ S REVIZÍ NAŘÍZENÍ EIDAS ODPOVĚDI NA DOTAZY DIA K EVROPSKÉ PENĚŽENCE DIGITÁLNÍ IDENTITY, kdy závěry uvedené v tomto dokumentu nejsou replikovány, ale je nutné oba dokumenty pro celkový kontext vnímat jako celek.
4. Při dalším užívání cenového modelu je nutné zohlednit finálně definované hranice mezi státní částí EUDIW a částí EUDIW, která je primárně řešena touto analýzou (také nazývána jako komerční část EUDIW).
5. V analýze ani manažerském shrnutí není zmíněna pravděpodobnost možnosti získání provozní dotace na provoz systému, protože o potřebných detailech získávání těchto dotací nemělo EY v době zpracování analýzy dostatečné informace. V tomto dokumentu jsou tedy zmíněny pouze okrajově.

8 Zdroje

(část 8 neposkytnuta)

9 Příloha 1: Technologie Split Key

Komprehensivní brief na technologii SplitKey a aktivity společnosti Cybernetica^{31, 32, 33}

Technologie SplitKey je pokročilá kryptografická technologie vyvinutá společností Cybernetica po dlouholetých zkušenostech se státní správou³⁴ pro zabezpečení digitální identity, elektronického podpisu a verifikace v prostředí, které nemusí být vybaveno hardwarově chráněnými prvky, jako jsou Secure Enclave nebo Trusted Execution Environments (TEE). SplitKey je navržen tak, aby poskytoval bezpečné, hardwarově agnostické řešení pro mobilní platformy, což umožňuje jeho širokou implementaci v aplikacích digitální identity, zejména v projektech jako je EUDIW.

Principy fungování SplitKey

Technologie SplitKey rozděluje kryptografické klíče mezi uživatele a poskytovatele služeb. Tento mechanismus umožňuje vysokou úroveň bezpečnosti, protože žádná ze stran nemá přístup k celému klíči. Tento přístup je odolný vůči útokům, protože klíč je vždy rozdělen, a samotný proces ověřování probíhá pouze tehdy, pokud jsou obě části klíče správně zrekonstruovány a ověřeny.

1. **SplitKey Signature Creation:** v tomto procesu se vytvoří podpis tím, že uživatelská strana a serverová strana společně generují kryptografické klíče, které jsou později rozděleny. Výhoda tohoto přístupu je, že umožňuje podepisování a ověřování identity i na platformách, které nevyužívají bezpečnostní čipy.
2. **Bezpečnost a odolnost:** Klíče jsou rozděleny, což zaručuje, že ani uživatel, ani poskytovatel služby nemá kompletní přístup k podpisovému klíči. Toto zajišťuje ochranu i proti potenciálnímu zneužití či útoku, pokud by jedna ze stran byla ohrožena. Tento model zároveň podporuje GDPR principy ochrany osobních údajů.
3. **Cloudová kompatibilita:** SplitKey je navržen tak, aby byl plně kompatibilní s cloudovými systémy a poskytoval bezpečné podepisování dokumentů a autentizaci bez nutnosti specifického hardwaru. To jej činí flexibilním řešením pro digitální identity v různých scénářích použití, včetně mobilních zařízení, kde hardware s vyšší úrovní ochrany není vždy dostupný.

³¹ Cybernetica SplitKey White Paper: https://cyber.ee/uploads/Split_Key_White_Paper_3506f03c34.pdf

³² Cybernetica Digital Identity Brochure: https://cyber.ee/uploads/digital_identity_brochure_60c8639fdc.pdf

³³ Cybernetica Comparison of SplitKey and Cloud Solutions:

https://cyber.ee/uploads/Split_Key_and_Cloud_Based_Signature_Solutions_Comparison_0bf2d00544.pdf

³⁴ Společnost Cybernetica má dlouholetou historii inovací v oblasti digitálních identit a kryptografických technologií. Byla zodpovědná za vývoj mnoha klíčových technologií, které jsou dnes nedílnou součástí digitální infrastruktury Estonska, včetně systému X-Road, který umožňuje bezpečnou výměnu dat mezi vládními a soukromými subjekty. Kromě toho Cybernetica vyvinula estonský internetový volební systém, jeden z prvních na světě, který umožňuje online volby. V oblasti digitálních identit se Cybernetica zaměřuje na další vývoj technologií, jako je SplitKey, které poskytují bezpečné, škálovatelné a interoperabilní řešení pro moderní digitální infrastruktury.

Srovnání SplitKey a tradičních cloudových řešení

Na rozdíl od tradičních cloudových řešení elektronických podpisů, která se spoléhají na servery a infrastrukturu třetích stran, SplitKey nabízí výhody decentralizovaného přístupu. Tradiční cloudová řešení často zahrnují, že poskytovatel služby má plný přístup k podpisovému klíči, což představuje potenciální bezpečnostní riziko. SplitKey naproti tomu umožňuje, aby byly kryptografické operace prováděny přímo na uživatelském zařízení, což znamená, že ani poskytovatel služby nemůže podepisovat jménem uživatele, aniž by měl přístup k jeho zařízení.

Výhody SplitKey technologie

- a) **Bez hardwarové závislosti:** SplitKey je navržen pro použití na platformách, které nemusí být vybaveny Secure Enclave nebo TEE, což z něj činí univerzální řešení pro mobilní zařízení.
- b) **Bezpečnostní vlastnosti:** Rozdělení klíčů mezi poskytovatele služby a uživatele zajišťuje, že ani jedna strana nemá úplnou kontrolu nad podpisovým klíčem, což chrání proti možnému zneužití.
- c) **Kompatibilita s evropskými standardy:** SplitKey je plně navržen pro integraci s požadavky na EUDIW a evropskou regulaci eIDAS, což zajišťuje interoperabilitu a kompatibilitu s dalšími digitálními řešeními v rámci EU.

Informace o EY

EY je předním celosvětovým poskytovatelem odborných poradenských služeb v oblasti auditu, daní, transakčního a podnikového poradenství. Znalost problematiky a kvalita služeb, které poskytujeme, přispívají k posilování důvěry v kapitálové trhy i v ekonomiky celého světa. Výjimečný lidský a odborný potenciál nám umožňuje hrát významnou roli při vytváření lepšího prostředí pro naše zaměstnance, klienty i pro širší společnost.

Název EY zahrnuje celosvětovou organizaci a může zahrnovat jednu či více členských firem Ernst & Young Global Limited, z nichž každá je samostatnou právnickou osobou. Ernst & Young Global Limited, britská společnost s ručením omezeným garancí, služby klientům neposkytuje. Pro podrobnější informace o naší organizaci navštivte prosím naše webové stránky ey.com.

© 2024 Ernst & Young, s.r.o.

Všechna práva vyhrazena.

ey.com