**Charakteristika projektu mID**

(analýza ÚPVII)

**Ciele projektu MID**

Hlavným cieľom projektu mID je odstrániť jednu z bariér vo využívaní elektronických služieb verejného sektora. Užívateľsky komplikované prihlasovanie a podpisovanie na báze občianskeho preukazu (ďalej len eID) bude doplnené o mobilnú alternatívu pre rozhodujúcu časť služieb. Pokiaľ pre veľkú časť eGov služieb budú eID a mID rovnocenne použiteľné ako pri prihlasovaní, tak aj pri podpisovaní – záber mID bude zúžený o tie scenáre, ktoré si explicitne vyžadujú KEP, resp. najvyššiu úroveň autentifikácie. Etablovanie mID súčasne otvára cestu sprístupniť služby štátu väčšiemu počtu občanov efektívnejšie prostredníctvom mobilných technológií. Navrhnutý koncept mobilného ID predstavuje otvorený systém federácie identít, čo v praxi znamená, že umožní trhu podieľať sa na sprístupnení už raz vytvorených identít občanov v systémoch, ktoré sú dôveryhodné. Pre zabezpečenie otvoreného systému a schopnosti sprístupniť na jednom mieste viacerých prevádzkovateľov identít je potrebné zriadiť federačnú autoritu, ktorou má byt’ NASES (prevádzkovateľ) pod vedením UPVII (správca). Federačná autorita bude podľa stanovených podmienok a pravidiel pripájať’ štátnych aj komerčných prevádzkovateľov identít do jedného identitného ekosystému.

**Zvýšenie záujmu občanov o zriadenie mID – nevyhnutné sú synergie s komerčným sektorom**

Samotné zjednodušenie aktivácie, resp. využívania štátnej mobilnej identity je nutným, nie však postačujúcim predpokladom toho, že si ju viac občanov aktivuje. Je potrebné zabezpečiť, aby mal občan viac dôvodov pre jej aktiváciu. Napriek vysokej snahe zo strany OVM poskytovať kvalitné agendové el. služby, štát tu v porovnaní s komerčným sektorom implicitne ťahá za kratší koniec.: Priemerný občan potrebuje komunikovať so štátom maximálne 2-5x ročne. Pričom ten istý občan komunikuje so svojou bankou, poisťovňou, telekomunikačným operátorom, či utilitnou spoločnosťou násobne viac krát do roka. ÚPVII si uvedomuje, že v súčasnosti je motivácia občana vykonať zriadenie a aktiváciu elektronickej identity veľmi nízka. História ukázala, že motivačné náklady na zriadenie eID pre štatutárov stáli štát na marketingu 4€ za identitu, čo v prípade 230 tisíc štatutárov bol náklad viac ako 900 tisíc €.

Prvým a jednoduchším riešením, ktorého rýchlosť zavedenia má štát veľmi dobre pod kontrolou - je zabezpečiť, aby sa občan „stretol“ s možnosťou využiť (a aktivovať si) štátnu mobilnú identitu častejšie, teda v scenároch komerčného sektora. Vzhľadom na dnes už nezanedbateľný počet aktivovaných eID, rozsah údajov evidovaných ku každej identite a štátom garantovanú dôveryhodnosť – je v určitých scenároch (typicky onboarding) pre komerčný sektor a aj občanov veľmi atraktívne využiť štátnu identitu.: Občan potom nemusí ísť do kamennej predajne či pobočky a organizácia vie obslúžiť občana cez elektronické kanály (najmä moderné mobilné aplikácie). ÚPVII dnes eviduje veľmi silný záujem zo strany bánk, a tento sa nepochybne ešte zvýši aj o iné organizácie. Stačí k službe spustiť cielenú komunikáciu smerom na trh. Štát potrebuje etablovať na ÚPVII kanceláriu lepších služieb, ktorá službu mobilnej elektronickej identity gestorsky zastreší.

Už dnes existujúca báza aktivovaných eID dáva samozrejme príležitosť pre štát monetizovať poplatkami jeho využívanie pomocou mobilnej identity. No najmä dáva štátu príležitosť vyjednávať a presvedčiť (zaujímavými podmienkami, či dohodami) ďalšie komerčné subjekty, aby naopak priniesli svoje identity do štátom federovaného prostredia. Občan tak získa alternatívnu možnosť prístupu k službám eGov, resp. za určitých okolností (napr. ak riešenie komerčného subjektu má potrebnú eIDAS certifikáciu) možnosť komfortného vytvorenia mID z pohodlia svojho domova aj bez predchádzajúceho zriadenia eID alebo návštevy registračného miesta pre mID. Benefit pre štát je jasný – každou integráciou ďalšieho externého prevádzkovateľa identít sa rozširuje okruh občanov, ktorí sa vedia prihlásiť k využívaniu elektronických služieb verejného sektora. Pre zabezpečenie otvoreného systému a schopnosti sprístupniť na jednom mieste viacerých prevádzkovateľov identít je potrebné zriadiť federačnú autoritu (FA), ktorou by sa stal NASES pod vedením ÚPVII Kancelárie lepších služieb. FA by za vopred stanovených podmienok a pravidiel pripájala komerčných prevádzkovateľov identít do jedného identitného ekosystému. ÚPVII sa rozhodlo, že zároveň so spustením služby sprístupnenia štátnej mobilnej identity (aj pre komerčný sektor) - vybuduje predpoklady pre fungujúcu FA.

Na to, aby bolo možné federovať identity od rôznych prevádzkovateľov identít, je pre tento účel nevyhnutné zriadiť inštitút certifikácie riešení mobilných identít. Každé riešenie mobilnej identity musí prejsť certifikáciou a klasifikáciou, čím daná mobilná identita získa kategóriu podľa úrovne dôveryhodnosti. Certifikačná a klasifikačná schéma musí byť nastavená v súlade s nariadením eIDAS. Garantom certifikačného procesu bude ÚPVII Kancelária lepších služieb. Očakáva sa, že v prvom kroku budú certifikované riešenia od DEUS ako aj od NASES. Komerční prevádzkovatelia identít dostanú certifikáciu podľa EIDAS čím sa aj následne budú od seba konkurenčne odlišovať. Z pohľadu pridanej hodnoty komerčného prevádzkovateľa identít je pre štát zaujímavý jednoznačne počet už aktívnych mobilných identít komerčného prevádzkovateľa. Nemá zmysel sa zaoberať prevádzkovateľom, ktorý má síce technologicky kvalitné riešenie ale nemá v systéme aktuálne žiadnu identitu. Takýto partner len zaťažuje administratívne štát s tým, že nepridá pridanú hodnotu a tou je rýchla penetrácia mobilných identít pre štátne služby.

**Aby mohol štát od začiatku demonštrovať svoju pripravenosť zohrávať úlohu FA, je potrebné ukázať fungovanie minimálne dvoch prevádzkovateľov identít.** **Vzhľadom na fakt, že štát pri zabezpečovaní svojej pripravenosti nemôže byť závislý od vôle komerčných subjektov (či sa chcú alebo nechcú so svojimi identitami pripojiť) - spúšťa ÚPVII projekt mobilnej identity s dvoma prevádzkovateľmi el. identity (DEUS a NASES), zapojenými do jedného federovaného identitného ekosystému. Obaja prevádzkovatelia prinášajú mobilné identity odvodené od štátnej (eID) identity (ale aj identity odvodené od „domácich“ dokladov totožnosti, zaregistrované registračnou autoritou s príslušnými oprávneniami danými legislatívou - napr. IOM). Týmto sa funkcionalita FA stane kompletnou.**

**Diferencované služby pre verejný a komerčný sektor a postupnosť ich zavádzania**

ÚPVII Kancelária lepších služieb (ÚPVII KLS) – bude mať vo svojom portfóliu, ako pre OVM tak aj pre komerčný sektor produkt „Overenie identity“. Službu „podpis klikom“ bude mať vo svojom portfóliu len pre OVM (pre komerčný sektor nemá podpis klikom legislatívnu oporu). Služba Pokročilý elektronický podpis v prvej fáze nebude súčasťou portfólia ÚPVII mID, pokročilý elektronický podpis môžu jednotliví poskytovatelia mobilných identít ponúkať pre komerčné subjekty ako svoju vlastnú dodatočnú službu. V druhej fáze sa pokročilý podpis pre komerčný sektor stane súčasťou portfólia ÚPVII. Pre motiváciu komerčných prevádzkovateľov mobilných identít bude potrebné nastaviť vhodný business model, kde bude zohľadnená motivácia prevádzkovateľa mobilnej identity integrovať sa do identitného ekosystému eGov. Súčasťou tohoto business modelu by mal byť aj cenník pre služby Overenia identity.

**Organizačné zabezpečenie (kompetenčný model pre mID)**

1. **ÚPVII kancelária lepších služieb** (KLS) **je produktový manažér pre jednu, jednotnú službu mID v štáte (aj smerom ku komerčnému sektoru).** Je teda jedno, že federovaní prevádzkovatelia identít budú od začiatku už dvaja, je to stále jedna jediná služba, ktorú gestoruje a jej produktovým manažérom je ÚPVII KLS. To prakticky znamená.:
	1. **Vzťah ÚPPVII (KLS) a NASES bude upravený zmluvne.** Súčasťou bude vyššie spomínaný záväzný template zmluvy o pripojenie, a fixované práva a povinnosti ÚPPVII ako „produktového manažéra“ a rovnako práva a povinnosti NASES ako „servisnej organizácie“ zabezpečujúcej „operatívu“ služby mID (prevádzku mID pod centrálnou autentifikáciou a autorizáciou v štáte a prevádzku federačnej autority).
	2. **ÚPVII KLS je prvý a základný bod, s ktorým komunikujú OVM, resp. organizácie komerčnej sféry o využívaní mID** (nie s NASES, nie s DEUS). ÚPVII zaeviduje záujem organizácie o využívaní služby mID, a podľa typu využívania služby (len využívanie mobilnej identity (prihlasovanie, podpisovanie), alebo neskôr vo fáze 2 aj publikovanie vlastného identitného systému a identít do federovaného riešenia. Cez pracovníka (produktového manažéra) bude daná organizácia.:
		1. **Poučená ísť uzavrieť zmluvu o pripojení k službe mID s NASES.** ÚPVII KLS definuje základné a všetky dôležité parametre tejto zmluvy (napr. cena, SLA, reklamačné podmienky, rozsah poskytovaných služieb, podmienky aktualizácie) formou záväzného „štandardného template-u“. V prípade (vo fáze 2), že organizácia chce publikovať svoj identitný systém v rámci federovaného - budú súčasťou zmluvy aj ďalšie náležitosti k tejto téme, opäť definované z ÚPVII formou záväzného štandardhého template-u. Od organizácii komerčného sektora bude NASES vyberať poplatok (flat fee) za využívanie služby mID, podľa podmienok definovaných KLS.Každá organizácia komerčného sektora tak bude mať garantované zmluvou s NASES využívanie všetkých zapojených prevádzkovateľov mobilnej identity. Na naštartovanie tohto procesu bude mať NASES publikovanú žiadosť na ktorú ÚPVII KLS vo svojom poučení bude odkazovať (a bude ju vedieť pomôcť s organizáciou vyplniť).
		2. **Informovaná o jednotnom logickom rozhraní (bod 2.b) a v prvej fáze o dvoch dostupných prevádzkovateľoch mobilnej identity, ktorých riešenia sú pripojené**. Súčasťou odovzdanej informácie bude aj poučenie, ako proces integrácie po podpise zmluvy (s NASES) – naštartovať.
	3. **ÚPVII KLS zabezpečí, aby smerom na organizácie (komerčné, OVM) využívajúce služby mID, bolo vypublikované jedno logické rozhranie (a aj ho definuje).** V praxi to znamená nasledovné.
		1. **Pre každého prevádzkovateľa mobilnej idenity bude existovať autonómna (mobilná) aplikácia mobilnej identity (v prvej fáze jedna od NASES a druhá od DEUS).** Občanovi stačí, aby mal aktivovanú jednu z nich (môže si aj viac ak sa tak rozhodne), a môže využívať služby mID či už v scenároch podporovaných el. služieb štátu, alebo scenároch komerčného sektora.
		2. **Pre „čisto mobilný“ scenár.:** **Vyvolanie autentifikácie alebo autorizácie z treťostrannej mobilnej aplikácie organizácie** (či už OVM, alebo komerčný sektor) **sa bude diať cez „logické“ (štandardizované) rozhranie - pomocou custom URI.** **Toto rozhranie definuje ÚPVII KLS, prevádzkovatelia sa mu následne v plnej miere podriadia.** Vyvolávajúca aplikácia tretej strany tak nemá (a nepotrebuje) vedomosť o tom, ktoré riešenie má občan na svojom mobile inštalované, len „vyšle“ štandardnú požiadavku, na ktorú sa jedna z dostupných mobilných aplikácií „chytí“ a vybaví. Ak sú nainštalované viaceré aplikácie mobilnej identity od viacerých prevádzkovateľov mID, je na štandardom mechanizme platformy (Android, iOS) – ako sa ponúkne občanovi výber, ktorou aplikáciou chce danú požiadavku spracovať.
		3. **Pre scenár desktop-mobil** (používateľ je na desktope, ale na úkon autentifikácie, alebo autorizácie v podporovanom scenári chce využiť mobil) **definuje UPVII KLS štandardné rozhranie pre autentifikáciu** (v spolupráci s NASES, nakoľko sa jedná o Oauth2 pripravované rozhranie nad IAM – spomínané už v rozbehnutom projekte MUK-P). Bude sa jednať o predpísanú špecifikáciu, ktorú následne musia operátori presne splniť.
	4. **KLS vytvorí a bude manažovať katalóg služieb OVM,** ktoré bude možné využívať aj s vyjadrovaním vôle pomocou tzv. „podpisu klikom“. Vo fáze pilotu (pri ostrom štarte) to budú minimálne služby.:
		1. **NASES.: služby eDesku**
		2. **DEUS.:**
			1. Oznamovanie o vzniku, zániku alebo zmene daňovej povinnosti k dani za psa
			2. Ohlasovanie vzniku, zániku alebo zmeny poplatkovej povinnosti za komunálne odpady a drobné stavebné odpady
			3. Podávanie daňového priznania k dani z nehnuteľností
	5. **KLS vypracuje plán kampane pre spustenie jednotnej služby mID** – zatiaľ predpokladáme, že kampaň a komunikáciu (férovú) oboch prevádzkovateľov identity riadi a koordinuje UPVII KLS, pričom jednotliví prevádzkovatelia nesmú robiť vlastnú kampaň (pokiaľ sa oficiálne nedohodne inak a UPVII KLS zverejní podmienky za akých to môžu operátori robiť).
	6. **KLS vypracuje metodické usmernenie – akým spôsobom bude prevádzkovateľ IOM (definovaný v 305/2013 Z.z., §7 odsek 2) ako registračná autorita - registrovať ľudí, ktorí prídu bez preferencie aktivácie konkrétneho operátora.** Prevádzkovateľ IOM ako registračná autorita pre aktiváciu a deaktiváciu mobilnej identity bez použitia čítačky (či dokonca bez eID) bude technologicky pripojený na prevádzkovateľov mobilnej identity a ich aktivačné a deaktivačné služby. Ako zabezpečiť fair play prístup (aby sa neponúkalo „implicitne“ riešenie len jedného operátora, pretože to je pre druhého „likvidačné“) bude úlohou ÚPVII KLS zadefinovať.
	7. **KLS vypracuje postup certifikácie komerčného poskytovateľa identít do federovaného systému.**
		1. Zatiaľ navrhnuté body.:
			1. Posúdenie bezpečnosti od ÚPVII CSIRt-u pre príslušnú úroveň autentifikácie a autorizácie podľa eIDAS. Je potrebné strpieť audit UPVII CSIRT a penetračné testy.
			2. Servre v EU (GDPR).
			3. Živá referencia na technológiu – minimálne 10K aktívnych identít (preukázané jednou transakciou nad danou identitou aspoň raz za 3 mesiace) ktoré preniesie daný poskytovateľ do federovaného prostredia.
			4. Poistenie zodpovednosti za škodu do 1-5 mil ročne (spresní ÚPVII), závisí od stupňa eIDAS pre daného poskytovateľa identít.

 **Pre DEUS ÚPVII zabezpečí nasledovné.:**

1. **ÚPVII zoberie záväzok, že do konkrétneho termínu spustí jednotnú službu mID v štáte (pre OVM overenie identity a podpis klikom a pre komerčný sektor overenie identity) aj s operátormi DEUS a NASES** v prípade, že splnia kritériá certifikácie. Predpokladáme, že GR Jaro Kmeť pošle v mene ÚPVII oficiálny list do DEUS aj NASES aj s uvedenou informáciou a následne že bude NASES zo strany ÚPVII v tejto veci koordinovaný.
2. **ÚPPVII potvrdí formálne mandát pre nový setup DEUS vs. NASES** (pošle kladnú odpoveď na list z DEUS) – pretože došlo k úprave pôvodného scope-u DEUS-u.