# **Stanovisko ITAS ku zámeru Mobilné ID v gescii UPVII prezentované NASES**

Na základe poverenia od UPVII prezentovala Národná agentúra pre sieťové a elektronické služby (NASES) zámer, čo najskôr implementovať tzv. Mobilné ID s cieľom eliminovať limity súčasného stavu využívania úradných autentifikátorov (eID karta a eDoPP karta) a podporiť tak zvýšenie miery využívania elektronických služieb poskytovaných orgánmi verejnej moci prostredníctvom výkonu verejnej moci elektronickým spôsobom (eGovernment). Medzi zásadné prekážky praktického a frekventovaného používania súčasných prostriedkov pre autentifikáciu patrí komplikovaná používateľská skúsenosť vyplývajúca z nutnosti používať čipovú kartu v kombinácii s čítačkou čipových kariet a klientskym softvérom (eID klient) na osobnom počítači, ktoré vyžadujú pre inštaláciu pokročilé IT zručnosti. Zároveň je používateľsky komplikované aj vyjadrenie vôle (autorizácie) prostredníctvom vytvorenia kvalifikovaného elektronického podpisu (KEP), ktorý okrem spomenutých komponentov vyžaduje inštaláciu ďalšieho dodatočného softvéru (D.suite).

Zámer Mobilné ID bol prezentovaný trom nominovaným členom IT Asociácie Slovenska (ITAS) na stretnutí uskutočnenom v piatok 27. júla 2018 v priestoroch detašovaného pracoviska NASES v Bratislave. Okrem ITAS boli prítomný aj delegáti za NASES, ÚPVII a aj z občianskeho združenia Slovensko.digital. Mrzí nás striktná limitácia počtu osôb na tri osoby, ktoré sa mohli za jednotlivé organizácie zúčastniť a vyjadriť tak kvalifikovaný názor počas produktívneho dialógu.

ITAS víta ambíciu agentúry NASES adresovať v čo najkratšom možnom časovom horizonte súčasné nedostatky uznaných autentifikátorov pre prístup k elektronickým službám. Téma implementácie riešenia pre jednoduchšiu autentifikáciu a autorizáciu je aktuálna a vnímaná ako kľúčové opatrenie pre zvýšenie záujmu občanov o elektronické služby poskytované štátom. Pozitívne hodnotíme tiež úsilie zohľadniť aj potreby komerčného sektora, pre ktorý je táto téma rovnako atraktívna. Skúsenosti z iných európskych krajín jasne preukazujú, že riešenie pre autentifikáciu / autorizáciu, ktoré nebude otvorené pre použitie aj v komerčnom sektore, má výrazne nižšiu šancu na úspech pre prirodzene nízku frekvenciu komunikácie občanov so štátom. Kladne hodnotíme intenciu využívania mobilných zariadení ako reakciu na rastúci trend mobility.

Oceňujeme, že môžeme konštruktívnymi názormi formulovanými v tomto stanovisku prispieť ku komunikovanému zámeru tak, aby boli v čo najvyššej možnej miere naplnené očakávané prínosy plynúce zo zavedenia mobilného ID z perspektívy občanov, štátu a aj komerčných subjektov. Sme presvedčení, že naše pripomienky by mohli byť presnejšie formulované, pokiaľ by sme dostali k dispozícii konkrétne dokumenty popisujúce prezentovaný zámer. Navrhujeme predloženie takéhoto dokumentu na rokovanie PS UPVII, aspoň na pracovné skupiny Lepšie služby a Bezpečnosť.

## **1. Autentifikačná časť**

* 1. **Plne mobilný scenár:** Mobilné ID by malo od začiatku podporovať plne mobilný scenár pre konzumáciu elektronickej služby priamo natívnym spôsobom z toho istého mobilného zariadenia, ktoré slúži pre autentifikáciu s mobilným ID, teda bez využitia iného zariadenia (osobný počítač atď.) a potreby snímania QR kódu. Súčasný popisovaný scenár vychádza z predpokladu, že interakcia a konzumácia elektronickej služby prebieha na inom zariadení (osobný počítač) a mobilné zariadenie sa použije len na autentifikáciu, ale nie na konzumáciu služby. Plne mobilný scenár by mal byť od začiatku implementácie dostupný, preto ho navrhujeme zakomponovať do zámeru. Práve takýto scenár je podľa nášho názoru nevyhnutný pre plošné využitie v komerčnej sfére, ktorá široko využíva práve natívne mobilné aplikácie a nie len prístup na mobile prostredníctvom prehliadača. Bez doriešenia tohto scenára a prepracovania modulu IAM (viď nižšie) má riešenie iba malú pridanú hodnotu pre súčasných používateľov.
	2. **Registrácia a aktivácia mobilné eID asistovane s eID/eDoPP:** Pre asistovaný spôsob aktivácie bola diskutovaná preferencia overenia totožnosti žiadateľa na základe dokladu totožnosti, teda aj občana, ktorý nedisponuje elektronickým identifikačným dokladom. Navrhujeme uplatňovať princíp vyššej opatrnosti realizáciou dokazovania fyzickej prítomnosti žiadateľa využitím eID/eDoPP karty a bezpečnostného osobného kódu (BOK) pre elimináciu rizika výskytu interného podvodného konania (podobné opatrenia zavádzajú napr. banky a zdravotníci). V prípade, ak žiadateľ nedisponuje eID/eDoPP, navrhujeme, aby sa zvážila možnosť previazať proces asistovanej registrácie mobilného eID a aktivácie jeho eID/eDoPP.Nevyhnutným predpokladom samoobslužnej online aktivácie je úspešné vykonanie autentifikácie občana eID/eDoPP kartou.
	3. **Výklad formulácie o autentifikačných certifikátoch podľa súčasného zákona č. 305/2013 resp. určenie legislatívneho základu mobilného ID:** Považujeme za dôležité najprv objasniť výklad súčasného znenia [§22a a §22aa spomínaného zákona](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2013/305/20180401#predpis.clanok-1.cast-tretia.skupinaParagrafov-osobitne_ustanovenia_o_identifikacii_osoby_a_autentifikacii_prostrednictvom_informacneho_systemu), pretože existuje odôvodnená obava, že použitie autentifikačných certifikátov podľa tejto legislatívy pre účely Mobilné ID je nesprávne interpretované a neaplikovateľné v praxi v prípade interaktívnej dvojfaktorovej autentifikácie osoby (bez automatizovaného spôsobu). Zároveň odporúčame posúdiť, či spôsob opisovanej autentifikácie s využitím autentifikačných certifikátov podľa tohto zákona nie je v rozpore s [výkladom nariadenia eIDAS Európskou komisiou](https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas) a tiež [odporúčaniami Európskou agentúrou pre informačnú a sieťovú bezpečnosť](https://www.enisa.europa.eu/publications/eid-cards-en/at_download/fullReport) (ENISA), pretože protistrana je identifikovaná priamo z certifikátu s poskytnutím všetkých osobných údajov obsiahnutých v certifikáte (bez kontroly používateľa) a vytvoreného podpisu výzvy prislúchajúcim kľúčovým párom. Ako uvádza ENISA, tento spôsob obmedzuje možnosti ochrany súkromia a osobných údajov. V súvislosti s tým upozorňujeme, že nariadenie eIDAS (recitál 11 a článok 5) by sa malo uplatňovať v úplnom súlade so zásadami ochrany osobných údajov ustanovených v nariadení GDPR – z tohto hľadiska by sa autentifikácia služby online mala týkať spracovania len tých identifikačných údajov, ktoré sú primerané, relevantné a nie sú nadbytočné na účely poskytnutia prístupu. Plný súlad znamená dodržiavanie všetkých princípov (zákonnosť, spravodlivosť, transparentnosť, obmedzenie účelu, minimalizácia údajov, správnosť, minimalizácia uchovávania, integrita a dôvernosť, zodpovednosť), vrátane prístupu formulovaného ako „Privacy by default“ a „Privacy by design“. Preto ak existujú mechanizmy, ktoré zaručujú dodržiavanie GDPR, mali by byť aplikované.

	Navyše pre využitie autentifikácie autentifikačnými certifikátmi sa predpokladá vyhovieť špecifickým požiadavkám, napríklad uzavretie dohody o integračnom zámere atď. Preto navrhujeme otvoriť túto tému v relevantných pracovných skupinách Úradu podpredsedu vlády pre investície a informatizáciu. Ak má byť Mobilné ID „náhradou“ eID a nie „doplnkom“ ku eID, potom z pohľadu právnej istoty dávame do budúcna na zváženie zadefinovanie samostatného pojmu v legislatíve. Zamedzilo by sa tak akýmkoľvek špekuláciám (sporným právnym výkladom), ktoré by mohli hlavne pre využívanie v komerčnom sektore z pohľadu compliance manažérov znamenať právnu neistotu a mať za následok zamietnutie akceptácie Mobilného ID v praxi.
		1. V prípade, že z výkladu vyplynie stanovisko, že napriek uvedeným úskaliam a odporúčaniam je možné využiť túto formuláciu pre právne zakotvenie Mobilného ID, potom je potrebné otvoriť a kvalitne podporovať rozhranie pre použitie autentifikačného certifikátu vo všeobecnosti, teda umožniť využitie nie len aplikácie od štátu, ale aj aplikácii rôznych iných poskytovateľov. Cieľom takéhoto otvoreného rozhrania je dosiahnuť, aby nebolo použitie autentifikačného certifikátu limitované na konkrétne riešenie, ale poskytovalo efektívny spôsob autentifikácie používateľov. Za zváženie stojí možnosť využitia kvalifikovaných autentifikačných certifikátov, ktorá zjednoduší proces registrácie certifikátu pre autentifikáciu. Zároveň by bolo potrebné legislatívne umožniť uznávanie tohto spôsobu overovania identity komerčnými subjektami, najmä finančnými inštitúciami, prostredníctvom doplnenia zákona č. 297/2008 o ochrane pred legalizáciou príjmov z trestnej činnosti a financovaním terorizmu.
		2. V prípade, že z výkladu vyplynie zamietavé stanovisko pre možnosť využitia tohto inštitútu, potom je nutné využiť inú alebo zaviesť novú legislatívnu bázu. Tiež platí, že by zároveň bolo potrebné legislatívne umožniť uznávanie tohto spôsobu overovania identity komerčnými subjektami, najmä finančnými inštitúciami, prostredníctvom doplnenia zákona č. 297/2008 o ochrane pred legalizáciou príjmov z trestnej činnosti a financovaním terorizmu.
	4. **Úprava IAM UPVS**: Prehodnotiť a podľa potreby upraviť súčasnú implementáciu IAM UPVS a výslednej autorizácie prístupu prostredníctvom SAML assertion pre dosiahnutie korektného spôsobu implementácie použiteľného univerzálne aj pre komerčný sektor. Navrhujeme oddeliť proces identifikácie a autetifkácie používateľa od procesu jeho autorizácie (t.j. určenia jeho role, resp. oprávnení pre prístup ku schránke atď.). V súčasnosti je tento proces spojený s pridelením prístupu ku schránke, čoho dôsledkom je potreba opätovného použitia eID pri prístupe k inej schránke. Tento spôsob odporuje princípu Single-Sign-On. Slovensko.sk toto realizuje pre získanie oprávnenia pre prístup do schránky, táto informácie je však pre ostatné subjekty nepotrebná a môže viesť k publikovaniu informácií, ktoré môžu byť následne zneužité. Navrhujeme poskytovať SAML token len s overením identity, ktorý spoliehajúca sa strana následne použije na pridelenie oprávnení podľa svojej potreby.
	Z architektonického pohľadu by bolo vhodné jasne definovať, akú funkcionalitu rieši IAM ÚPVS:
	 - Identifikácia, Autentifikácia – Identity provider
	 - Autorizácia – Attribute provider
	Pre obe oblasti (min. však pre identifikáciu a autentifikáciu) by bolo vhodné definovať ako ich bude možne rozšíriť o iné možnosti poskytnutia funkcionality od tretích strán.
	5. **Určenie cieľovej bezpečnostnej úrovne autentifikácie Mobilné eID a klasifikácia služieb podľa úrovne autentifikácie:** Je potrebné stanoviť cieľovú bezpečnostnú úroveň pre autentifikáciu na základe Mobilného ID s rešpektovaním [vládou schválených výstupov pracovných skupín ÚPVII, konkrétne skupiny Lepšie služby – Multikanálový prístup](http://www.informatizacia.sk/ext_dok-uppvii_sp_multikanalovy_pristup_vfinal/24195c), ktorá približuje možnosti dosiahnutia bezpečnostných úrovní, výber stratégie a odôvodnenie a dokonca uvádza: „*Okrem určenia technického spôsobu prevedenia mobilnej autentifikácie v súlade s bezpečnostnými požiadavkami, bude vykonaná biznis analýza koncových služieb v gescii jednotlivých orgánov verejnej moci za účelom revízie požadovanej úrovne autentifikácie s jej potenciálnym znížením na úroveň, ktorá zabezpečí čo najrýchlejší prístup aj z mobilných zariadení.*“ S ohľadom na deklarovanú motiváciu a sledované ciele nie je nevyhnutná realizácia Mobilnej ID s bezpečnostnou úrovňou „Vysoká“ a sprístupnenie všetkých služieb. Pre prístup ku službám kritickej povahy z pohľadu dopadu na práva a povinnosti občana slúži a naďalej bude slúžiť úradný autentifikátor eID/eDoPP. Navyše, bezpečnostné prvky eID a navrhovaného Mobilné ID nie sú porovnateľné resp. ekvivalentné. Popis súčasného návrhu riešenia a prvkov naznačuje, že úroveň „Vysoká“ je málo pravdepodobne dosiahnuteľná ak berieme do úvahy najmä vykonávacie nariadenie [eIDAS 1502/2015](https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32015R1502) s väzbou (viď recitál 4) na [STORK](https://joinup.ec.europa.eu/sites/default/files/document/2014-12/STORK%20Deliverable%20D2.3%20-%20Quality%20authenticator%20scheme.pdf), ISO/IEC 29115 atď. Predpokladá sa tiež kategorizácia služieb podľa ich povahy a požadovanej úrovne autentifikácie. Rovnako by sa mali zosúladiť lokálne bezpečnostné úrovne autentifikácie vyplývajúce zo štandardov IS VS a nariadenia eIDAS a súvisiaceho vykonávacieho nariadenia eIDAS č. 2015/1502.
	6. **Využiteľnosť Mobilného ID komerčným sektorom podľa legislatívnych požiadaviek:** Aby bolo umožnené komerčné využívanie Mobilného ID v súlade s ambíciami formulovanými v zámere, je potrebná analýza aspoň základných prípadov použitia a tiež aspoň stručná legislatívna analýza takéhoto používania za účelom identifikácie dodatočných technických požiadaviek
		1. **Pre inštitúcie finančného sektora** to záleží najmä od rešpektovania záväzného legislatívneho rámca – minimálne v rozsahu:

**a)** [**zákon č. 297/2008**](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2008/297/20180315#paragraf-7) o ochrane pred legalizáciou príjmov z trestnej činnosti a pred financovaním terorizmu (transponovaná AML4 smernica). Najmä §7 a §8 špecificky pre prípad založenia účtu – tzv. online onboarding, ktorý je pre banky veľmi atraktívny a aktuálny, pričom vyžaduje aj typ a číslo dokladu totožnosti, ale pre prípad použitia na prihlasovanie do mobilného resp. elektronického bankovníctva (pre banky menej atraktívne) už typ a číslo dokladu nie je nevyhnutné. Bolo by žiadúce vykonanie kontroly platnosti deklarovaného čísla dokladu totožnosti a overenie stavu v agende dokladov Ministerstva Vnútra SR.

**b)** [**zákon č. 492/2009**](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2009/492/20180113#paragraf-3c) o platobných službách (transponovaná PSD2 smernica) - § 3c Silná autentifikácia používateľa platobných služieb podľa [regulatívneho technického štandardu od European Banking Authority](https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=uriserv:OJ.L_.2018.069.01.0023.01.SLK&toc=OJ:L:2018:069:TOC). Z uvedeného legislatívneho rámca vyplývajú technické aspekty rozhodujúce o relevantnosti a akceptácii Mobilného ID vo finančnom sektore – najmä vo väzbe na viacúčelové zariadenia (vrátane mobilov) a dynamickú autorizáciu transakcií.

* + 1. **Pre ostatné menej regulované inštitúcie** (utility, zdravotníctvo....) záleží od očakávaní a prípadov použitia, či už dvojfaktorové prihlasovanie, online onboarding, dokazovanie prítomnosti a iné

## **Autorizačná časť**

V tejto časti sme na pôde ITASu diskutovali dve relevantné alternatívy, ktoré sa ponúkajú v zmysle doteraz realizovaných krokov v oblasti eGovernmentu a informácií vyplývajúcich z prezentácie zámeru.  Ide o takzvanú autorizáciu „klikom“ a zdokonalený elektronický podpis (AdES podľa eIDAS). Tieto alternatívy by mali byť ekvivalentne zvážené a vyhodnotené z pohľadu možnosti ich využitia pre účely autorizácie. K obom vyššie spomínaným alternatívam si dovoľujeme uviesť hodnotenie ich momentálnej pripravenosti k nasadeniu a návrh opatrení pre ich implementovateľnosť.

* 1. **Alternatíva 1 - autorizácia „klikom“**

Autorizácia „klikom“ je už zakomponovaná v súčasnej legislatíve, konkrétne v [§23 ods. 1, písm. a, bod 2.) zákona č. 305/2013 o eGovernmente](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2013/305/20180401#paragraf-23) v súlade s vládou schváleným výstupom „Multikanálový prístup“ pracovnej skupiny ÚPVII „Lepšie Služby“. Autorizácia klikom má potenciál na to, aby zjednodušila úkon autorizácie pre tie služby, ktoré nevyžadujú prihlásenie na bezpečnostnej úrovni eIDAS „Vysoká“. Avšak identifikujeme deficity v súvislosti s autentifikáciu „klikom“ ako je definovaná dnes v zákone, ktoré by mali byť vyriešené pre dosiahnutie vlastnostní potrebných pre cieľovú použiteľnosť:

* Vágna interpretácia a absentujúca bližšia definícia obsahu služby. Riešením tohto problému by mohlo vypracovanie metodického a technologického štandardu pre autorizáciu klikom.
* Nejasná právna zodpovednosť za centrálne prevádzkovanie služby. Jednou z možností eliminovania tohto problému je etablovanie novej kvalifikovanej dôveryhodnej službu pre podpisovanie klikom. Takto by bolo možné dosiahnuť a garantovať bezpečnosť, spoľahlivosť, vymedzenie zodpovedností a hlavne nespochybniteľnosť úkonu autorizácie týmto spôsobom.
	1. **Alternatíva 2 – autorizácia zdokonaleným podpisom**

Súčasné znenie zákona o eGov explicitne nehovorí priamo o možnosti využitia zdokonaleného elektronického podpisu, definovaného v eIDAS v článku 26 a článku 27, ako jednej z možných alternatív k autorizácii kvalifikovaným elektronickým podpisom. A to napriek tomu, že eIDAS má povahu nariadenia, a teda jeho ustanovenia sú pre Slovenskú republiku priamo záväzné. Problém je v tom, že eIDAS nedefinuje podmienky aplikovateľnosti zdokonaleného elektronického podpisu (pre ktoré agendy resp. podania je vhodný, a kde je nevyhnutné použitie kvalifikovaného elektronického podpisu). Rámec použiteľnosti iného spôsobu autorizácie, ako využitím kvalifikovaného elektronického podpisu, zase definuje slovenský zákon o eGov v §23 v odseku 1, písmeno a, bodoch 2 a 3.

Máme tak dve legislatívne normy, ktoré síce v súčte vytvárajú nevyhnutné predpoklady pre využitie zdokonaleného elektronického podpisu podľa eIDAS, ale chýba im vzájomné prepojenie.

Pre odstránenie akýchkoľvek pochybností o možnosti používania zdokonaleného elektronického podpisu na Slovensku navrhujeme UPVII túto medzeru preklenúť jedným z dvoch nižšie uvedených návrhov:

* Spracovať právny výklad, ktorý potvrdí, že autorizácia prostredníctvom zdokonaleného elektronického podpisu definovaného v článkoch 26 a 27 eIDAS spĺňa požiadavky zákona o eGov uvedené v zákon o eGov v §23 v odseku 1, písmeno a, bode 2 , alebo
* Vydať jednoduchú vyhlášku pre aplikovateľnosť zdokonaleného elektronického podpisu podľa zákona o eGov v §23 v odseku 1, písmeno a, bod 3 s odvolaním sa na definíciu zdokonaleného elektronického podpisu v článkoch 26 a 27 eIDAS a v nadväzujúcich technických normách

**Všeobecné konštatovanie k autorizácii**

Bez ohľadu na to, ktorá z vedených alternatív bude v budúcnosti aplikovaná, dovoľujeme si upozorniť na skutočnosť, že filozofia negatívneho vymedzovania elektronických podaní, ktoré môžu byť autorizované iným spôsobom, ako kvalifikovaným elektronickým podpisom, je síce implementačne veľmi jednoduchá, ale prináša so sebou nové riziká. Túto novú filozofiu zaviedla novela zákona o eGov z roku 2017 v bodoch 2 a 3. v §23, odseku 1, písmeno a. Chápeme zámer zákona, čo najrýchlejšie odbúrať legislatívne bariéry pre používanie užívateľsky jednoduchšej formy autorizácie, ako je kvalifikovaný elektronický podpis, avšak nie sme si istí, či to neprinieslo neprimerané zvýšenie rizika.

Dávame preto na zváženie návrat k filozofii pozitívneho vymedzenia, ale v spojení s výrazným implementačným zjednodušením jeho aplikácie pre OVM a základnou metodickou podporou pri rozhodovaní o tom, kde je pre autorizáciu nevyhnutný kvalifikovaný elektronický podpis, a kde bude postačujúca niektorá z jeho jednoduchších alternatív.

OVM by mali na základe zrozumiteľnej metodiky kategorizovať všetky ponúkané elektronické služby občanom podľa požadovanej úrovne autorizácie vychádzajúc z analýzy povahy služieb na základe objektívnych kritérií, ako sa to uvádza aj v spomínanom dokumente o multikanálovom prístupe: *„Okrem určenia technického spôsobu prevedenia iného spôsobu autorizácie v súlade s bezpečnostnými požiadavkami bude vykonaná biznis analýza koncových služieb v gescii jednotlivých orgánov verejnej moci za účelom revízie požadovaného spôsobu autorizácie s jeho potenciálnou zmenou na spôsob, ktorý zabezpečí prístup aj z mobilných zariadení.“*

Na základe kategorizácie podľa úrovne autorizácie by OVM identifikovali množiny elektronických služieb vyžadujúcich príslušnú úroveň a akceptovaný spôsob resp. prostriedok autorizácie - napríklad najvyššiu úroveň autorizácie vyžadujúcu kvalifikovaný elektronický podpis (KEP), nižšiu úroveň autorizácie prostredníctvom niektorej z alternatívnych možností.

Sme presvedčení, že je možné pripraviť efektívne fungujúcu filozofiu pozitívneho vymedzenia tak, aby nebola brzdou v používaní jednoduchších foriem autorizácie.

## **Záver**

Na záver by sme ešte radi upozornili, že takýto projekt bez zváženia súvislostí a dopadov sa môže z plánovaného „quick-win“ preklopiť do plošne kritizovaného projektu s malou pridanou hodnotou, ktorý môže byť považovaný za zbytočne minuté peniaze bez očakávaných prínosov.

Na druhej strane sme presvedčení, že zohľadnenie vyššie uvedených postrehov zvýši celkovú kvalitu a komfort prístupu ku elektronickým službám a výraznou mierou prispeje ku naplneniu sledovaných cieľov a očakávaní plánovaného „quick-winu“. Radi budeme pokračovať v konštruktívnej spolupráci pri príprave kvalitného návrhu, ktorý bude v prospech celej spoločnosti.

Do budúcna sme pripravení ponúknuť odborné kapacity členov ITAS do pracovných skupín na rozpracovanie alternatív pre oblasť autentifikácie alebo autorizácie.



Emil Fitoš 24. august 2018

Prezident ITAS