Stanovisko NASES k návrhom odbornej verejnosti k téme mobilnej autentifikácie a autorizácie

Dňa 27. júla 2018 zorganizovala Národná agentúra pre sieťové a elektronické služby (NASES), za prítomnosti Úradu podredsedu vlády pre investície a informatizáciu (ÚPPVII) - stretnutie so zástupcami združení odbornej verejnosti (menovite združení IT asociácia Slovenska (ITAS) a Slovensko.Digital) na tému pripravovaného projektu mobilnej autentifikácie a autorizácie (ďalej skrátene mobileID). Zástupcovia odbornej verejnosti vzniesli na stretnutí po odprezentovaní základných východísk k téme niektoré otázky a návrhy, pričom bolo dohodnuté, že združenia ich zašlú ako oficiálne dokumenty. Od Slovensko.Digital NASES obdržal tieto návrhy 7. augusta 2018, za ITAS 27. augusta 2018.

Z oboch vyjadrení nás teší potvrdenie, že téma odstraňovania bariér využívania elektronických služieb je veľmi dôležitá, a že je potrebné hľadať pre ňu riešenia dosiahnuteľné v čo možno najkratšom čase a pri čo možno najefektívnejšie vynaložených prostriedkoch. Zároveň sme si dovolili vyextrahovať z oboch stanovísk jednotlivé témy, okolo ktorých sa sústredili otázky a návrhy oboch združení.

Téma č.1: MobilnéID a miera jeho previazanosti s eID.

Komentár za S.D.: *Mobilné ID nemá byť priamo naviazané na eID. Má byť od začiatku plánovaný scenár získania mobilného ID pre osobu, ktorá nemá eID – ale samozrejme nemusí byť realizovaný v prvej etape. Vydávanie a používanie autentifikačných certifikátov nie je priamo naviazané na eID, ale je to nezávislý spôsob autentifikácie – podľa zákona, je to tak implementované aj používané. Funkčnosť mobilného ID má byť nezávislá od stavu eID (stratený, zneplatnený), ktoré používateľ využil na jeho zriadenie.*

Komentár za ITAS.: *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.*

Vyjadrenie NASES: Vítame každú snahu, ktorej výsledkom môže byť zjednodušenie alebo odstránenie bariéry využívania el. služieb. Takým je aj návrh umožniť aktivovať mobileID aj pre skupinu občanov, ktorí dnes nedisponujú eID/eDoPP – pričom aktivácia by bola možná na niektorom z obslužných miest eGov, ktoré sú blízko ich domova (Pošta, Obecný úrad), a ktoré môžu vykonať stotožnenie. Predpokladáme však k takejto iniciatíve širšiu diskusiu a zatiaľ zotrvávame na pôvodnom stanovisku, ktoré bolo prezentované aj na stretnutí – teda aj v obslužných scenároch plánujeme využívať eID (eDoPP) kartu a znalosť BOK kódu pri prvej aktivácii mobileID.

Téma č.2: Úroveň autentifikácie vo väzbe na eIDAS.

Komentár za S.D.: *Autentifikáciu žiadame implementovať pre úroveň eIDAS „pokročilá" = ŠTD ISVS level 3, Tento projekt opäť poukazuje na potrebu zjednotenia ŠTD ISVS s platnými požiadavkami pre úrovne autentifikácie podľa eIDASID nemá byť priamo naviazané na eID.*

Komentár za ITAS.: *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, 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.*

Vyjadrenie NASES: Sme radi, že v tomto bode panuje zhoda, a že prístup na všetky služby cez autentifikačnú úroveň „vysoká" je už prekonaný. S odporúčaním samozrejme súhlasíme (riešenie mobileID bude vychádzať z autentifikácie podľa eIDAS na úrovni „pokročilá"), a legitímnu požiadavku na zosúladenie Výnosu o štandardoch ISVS a eIDAS-u do budúcnosti postupujeme na ÚPPVII.

Téma č.3: Ako určiť vhodný vyžadovaný autentifikačný stupeň pre eGov služby.

Komentár za S.D.: *Potrebné je pracovať so správcami aby určili vhodný vyžadovaný stupeň autentifikácie pre svoje služby - navrhujeme zvoliť „reverznú“ úvahu: služba, ktorej použitie smeruje k vytvoreniu podania pre ktorý podľa ZeGov je možné použiť autorizáciu kliknutím, nemôže vyžadovať úroveň autentifikácie vyšší ako „pokročilá“/3.*

Komentár za ITAS.: *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.*

Vyjadrenie NASES: Súčasná legislatíva hovorí len o dvoch úrovniach pri vyjadrovaní vôle občanmi alebo podnikateľmi – vlastnoručnom podpise a úradne overenom vlastnoručnom podpise. Rozumieme logike návrhu zo strany ITAS-u, no zároveň dodávame, že uvedený návrh sa týka existujúceho stavu legislatívy (ktorej zmene predchádzali práve diskusie na túto tému a dnešná legislatíva je výsledkom dohody). Projekt zavedenia mobileID tento stav nijakým spôsobom nezhoršuje, ani nezlepšuje. Pre praktické usmernenie – OVM majú aj v tejto chvíli účinný nástroj na „reguláciu“ spôsobov autorizácie v prípade podaní, ktoré vnímajú ako príliš rizikové pre iné formy autorizácie než je autorizácia pomocou kvalifikovaného elektronického podpisu. V zásade je možné zadefinovať pre takéto podania (ich vypracovanie v samoobslužnom režime) úroveň autentifikácie „vysoká“.

Téma č.4: Požiadavka na podporu plne mobilného scenára pre prihlásenie od začiatku projektu.

Komentár za S.D.: *Plne mobilný scenár má byť jedna z priorít tohto projektu Žiadame plne mobilný scenár riešiť už v prvej fáze projektu. V prípade implementácie scenáru „prístup k elektronickej schránke“ budú musieť byť vytvorené*

všetky architektonické aj implementačné komponenty pre plne mobilný scenár, preto nie je dôvod jeho podporu odsúvať. Plne mobilný scenár má byť podporovaný, aj podľa NKIVS a strategických dokumentov. V súčasnosti už viac ako tretina prístupov k službám cez internet je v SR vykonávaná prostredníctvom mobilných platforiem. Ak nebude podporovaný plne mobilný scenár, autorizáciu nemá vôbec zmysel riešiť a vynechajme ju z projektu úplne - bez plne mobilného scenára totiž nie je situácia, kde by sa autorizácia na mobilnom zariadení dala využiť.

Komentár za ITAS.: *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.*

Vyjadrenie NASES: Už na stretnutí sme vysvetlili, že samotná pripravenosť všetkých úrovní a komponentov riešenia na plne mobilný scenár prihlásenia vyplýva už zo záväzku spustiť hneď od začiatku prihlásenie do eDesk schránky priamo z natívnej mobilnej aplikácie. Takže ešte raz a formálne deklarujeme, že súhlasíme a plne mobilný scenár prihlásenia (bez využitia iného zariadenia, QR kódu) bude podporovaný od začiatku projektu.

Téma č.5: Výklad formulácie o autentifikačných certifikátoch podľa súčasného zákona č. 305/2013 resp. ich využitie v rámci mobilného ID.

Komentár za S.D.: Chápeme snahu naviazať riešenie na koncept autentifikačného certifikátu podľa súčasnej legislatívy, potom však z dlhodobého hľadiska je potrebné oblasť autentifikačných certifikátov presnejšie upraviť pre jednotlivé spôsoby použitia – integrácie OVM, OpenAPI, Mobilné ID. Vyjasniť rolu autentifikačného certifikátu v koncepte OpenAPI a jeho zlučiteľnosť s plánovaným použitím v Mobilnom ID. Zjednodušiť prístup používateľa k autentifikačnému certifikátu, najmä jeho vydanie, až po úplnú automatizáciu tohto procesu vydania pre používateľa disponujúceho eID a už registrovanú službu. Vydať vyhlášku o autentifikačných certifikátoch podľa §59.2.f ZeGov

Komentár za ITAS.: *Považujeme za dôležité najprv objasniť výklad súčasného znenia §22a a §22aa spomínaného zákona, 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 a tiež odporúčaniami Európskou agentúrou pre informačnú a sieťovú bezpečnosť (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.

a) 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.

b) 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."

Vyjadrenie NASES (výklad zákona č. 305/2013 v spolupráci s ÚPPVII): Na účely autentifikácie ustanovuje § 19 ods. 5 a 6 zákona o e-governemente dva spôsoby jej vykonania, v závislosti od toho, či ide o prístup do informačného systému verejnej správy (ďalej len „ISVS") alebo

o elektronickú úradnú komunikáciu. Keďže na účely mobileID je autentifikácia v procese elektronickej úradnej komunikácie irelevantná, resp. je mimo rámec projektu, venujeme sa len prvému spôsobu.

Autentifikácia sa primárne deje overením deklarovanej identity (teda identifikátora osoby) a následne použitého autentifikátora [§ 19 ods. 5 písm. b) ZoEG]. Tento spôsob autentifikácie ZoEG ustanovuje pre úradný autentifikátor a pre alternatívny autentifikátor. Pokiaľ ide o autentifikačný certifikát, ako nástroj autentifikácie, tento v sebe obsahuje identifikátor osoby (§ 22a a 22aa ods. 2 ZoEG) a pri jeho použití sa podľa § 19 ods. 5 písm. a) zákona o e-governemente overuje „len“ jeho platnosť. V spojení s § 22b ods. 5 zákona o e-governemente sa platnosť autentifikačného certifikátu overuje voči zoznamu platných autentifikačných certifikátov, ktorý vychádza z registra autentifikačných certifikátov a zverejňuje sa denne, vždy s platnosťou na nasledujúcich 24 hodín. Keďže z hľadiska mobileID je podstatnou práve autentifikácia s použitím autentifikačného certifikátu, budeme sa ďalej venovať len tomuto spôsobu autentifikácie.

Z hľadiska použitia autentifikačného certifikátu § 22a zákon o e-governemente umožňuje jeho použitie na prístup k ISVS (prístupovému miestu alebo spoločnému modulu) a na prístup a disponovanie s elektronickou schránkou. V oboch prípadoch sa podľa § 22a zákona o e-governemente predpokladá automatizovaný spôsob prístupu s použitím technického alebo programového prostriedku. Z hľadiska podmienky použitia technického alebo programového prostriedku ide o podmienku existencie „zariadenia alebo aplikácie“, ktoré v prístupe alebo komunikácii „figurujú medzi“ užívateľom a prístupovým miestom, spoločným modulom alebo elektronickou schránkou. V skratke, nejde o prístup s využitím užívateľského rozhrania na to určeného konkrétnym prístupovým miestom. Z hľadiska použitého pojmu „automatizovaný spôsob“ ide o podmienku, kedy jednotlivé časti procesu a komunikáciu, potrebné na prístup, zabezpečuje ono „zariadenie alebo aplikácia“ a nie užívateľ priamo. Pritom, z povahy veci, nie je možné vylúčiť akúkoľvek interakciu užívateľa, keďže už samotný „úmysel“ pristúpiť

k elektronickej schránke či prístupovému miestu je nevyhnutne viazaný na prejav vôle užívateľa – v skratke, užívateľ určuje, kedy a kam chce pristúpiť. Rovnako tak nie je z hľadiska zákona vylúčené, aby „iniciáciu alebo pokyn na použitie“ autentifikačného certifikátu zadával, či potvrdzoval užívateľ. Podstatné z hľadiska automatizovaného spôsobu je, že potrebné kroky a komunikáciu zabezpečujú „zariadenie alebo aplikácia“ a nie manuálne užívateľ. Tieto sa dejú sa v priamej komunikácii dvoch IS a nie na to určeným užívateľským rozhraním daného prístupového miesta, či elektronickej schránky. Z hľadiska zákona je následne irelevantné, aký technologický prístup sa zvolí pre konkrétny mechanizmus autentifikácie.

V prípade autentifikácie s použitím autentifikačného certifikátu zákon o e-governemente nevyžaduje osobitné deklarovanie identifikátora osoby, užívateľa a ani overovanie jeho správnosti a platnosti [§ 19 ods. 5 písm. a)], keďže informácia od identifikátora je priamo obsiahnutá v certifikáte. Zároveň platí, že autentifikáciu zabezpečuje v tomto prípade NASES, keďže overenie platnosti autentifikačného certifikátu sa deje voči zoznamu platných autentifikačných certifikátov. Z toho vyplýva, že všetky informácie, ktoré sú obsahom autentifikačného certifikátu, spracúva z pohľadu zákona vždy NASES a samotný „poskytovateľ služby“, na ktorej použitie autentifikácia slúži, dostáva len informáciu o úspešnom overení identity užívateľa – o úspešnej autentifikácii. Zákon ďalej nepredpisuje, aké konkrétne informácie o užívateľovi majú byť poskytovateľovi služby sprístupnené, preto všetko, čo je poskytovateľovi služby sprístupnené, má vždy plne pod kontrolou ten, kto autentifikáciu vykonáva (v tomto prípade NASES) a nie samotný poskytovateľ služby.

Na základe vyššie uvedeného máme za to, že na autentifikáciu v rámci projektu mobileID je možné použiť autentifikačný certifikát, keďže

- podmienka použitia technického alebo programového prostriedku je splnená tým, že medzi užívateľom a prístupovým miestom či elektronickou schránkou v procese vystupuje technické zariadenie a aplikácia užívateľa,

- podmienka automatizovaného spôsobu je splnená tým, že komunikácia pri autentifikácii prebieha priamo medzi zariadením, resp. aplikáciou a ISVS na strane autentifikujúceho orgánu a poskytovateľa služby,
- proces autentifikácie využíva zákonom predpokladaný inštitút registra autentifikačných certifikátov a zoznamu platných autentifikačných certifikátov, voči ktorému v konečnom dôsledku k overeniu platnosti použitého autentifikačného mechanizmu dochádza.

Zároveň z pohľadu budúcnosti plánujeme nasledovné (sú to však témy, ktoré určite teraz nebránia využitiu autentifikačných certifikátov):

- Uvažujeme o otvorení autentifikačných certifikátov, ale nie spôsobom, kde nejaká tretia strana neregulovaným a potenciálne nebezpečným spôsobom „generuje“ a „podpisuje“ prihlasovacie výzvy. Generovanie a samotný podpis výzvy sa bude diať v kontrolovanom prostredí za IAM-om. Fasáda IAM sama o sebe zaručuje, že smerom k poskytovateľovi nejakej služby (teda využívateľovi služby eGov autentifikácie) pôjdu len tie informácie, ktoré občan/podnikateľ chce zverejniť (napríklad že ich poskytnutie autorizuje v rámci flow-u protokolu Oauth2). Ďalej do kontrolovaného prostredia za IAM-om nebude môcť treťostranný poskytovateľ nejakej metódy autentifikácie (čo bude zväčša iný subjekt, než vyššie spomínaný poskytovateľ nejakej služby) s využitím autentifikačných certifikátov nasadiť svoje riešenie len tak. Bude to možné až po splnení kritérií definovaných certifikačným procesom, ktorý bude okrem iného pre každé riešenie auditovať spôsob generovania a nakladania s výzvami, mieru požadovania autentifikačných údajov a spôsob práce s nimi. Inými slovami zabezpečia sa rovnaké podmienky, ktorých splnenie predpokladáme pri spustení autentifikácie pomocou riešenia pre mobilné ID s využitím autentifikačných certifikátov.
- Zjednodušenie manažmentu autentifikačných certifikátov (v registri autentifikačných certifikátov) plánujeme zase riešiť v rámci rozvoja tém OpenAPI, ApiGW (rovnako v spolupráci s ÚPPVII, ktorý je gestorom modulu procesnej integrácie a integrácie údajov,

v rámci ktorého téma OpenAPI a APIGW patrí) a Oauth2/OpenIDConnect podpora pre IAM.

Téma č.6: Úprava IAM UPVS pri autentifikácii.

Komentár za S.D.: (Tejto téme sa stanovisko nevenuje)

Komentár za ITAS.: *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: a) Identifikácia, Autentifikácia – Identity provider, b) 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.*

Vyjadrenie NASES:

Návrhom sa budeme zaoberať v pri ďalšom rozvoji modulu IAM ÚPVS, resp. aj pri rozvoji témy OpenAPI. Z pohľadu spustenia projektu mobileID nejde o kritickú podmienku, no do budúcna plánujeme túto tému adekvátne adresovať.

Téma č.7: Vytvárať centrálny komponent pre autorizáciu (podpisovanie) CPK.

Komentár za S.D.: *V zmysle legislatívy nerealizuje ÚPVS podpisovaciu službu a nie je známa potreba aby táto služba bola na ÚPVS zavedená. Vytváranie elektronického podpisu (najmä KEP) má byť lokálny úkon vykonaný na strane používateľa. (Špecifická výnimka sú vzdialené podpisy.) V súčasnosti ÚPVS používateľovi poskytne podporné nástroje (stiahnutie aplikácie) pre vytváranie KEP. V oblasti vytvárania KEP existuje na trhu viacero aplikácií, ktoré si navzájom konkurujú, viaceré z nich dokážu použiť eID. Ak by ÚPVS implementoval „centrálny podpisovací komponent“,*

spôsobilo by to zásadné narušenie tohto trhu, na ktoré nevidíme dôvod (už aj súčasné riešenie takéto narušenie trhu spôsobuje). Do budúcnosti je vhodný prístup otvoriť ÚPVS pre použitie ľubovoľných aplikácií pre vytváranie KEP tretích strán, ktoré má používateľ lokálne nainštalované, pomocou ich jednoduchej integrácie. V prípade autorizácie kliknutím je vhodné prepoužiť v čo najväčšej miere súčasné postupy implementované v ÚPVS pri službách s de-facto autorizáciou kliknutím.

Ďalej.: Nemá byť vytváraný „centrálny komponent" pre autorizáciu kliknutím. V zmysle ZeGov môže každé prístupové miesto (napr. špecializovaný portál) samostatne sprístupňovať elektronické služby a preberať autorizované elektronické podania. Taktiež môže každý OVM podľa vlastného uváženia (a v rozsahu svojich kompetencií) vytvárať služby ktoré nie sú výkonom verejnej moci. Je správne, ak si každý správca služby v rámci vlastných elektronických služieb môže implementovať autorizáciu kliknutím (ak je to efektívne). Zodpovedá to aj formulácii z §23.1.a.2 ZeGov „použitím na to určenej funkcie informačného systému prístupového miesta". Požiadavky na autorizáciu kliknutím sú v legislatíve úmyselne zvolené tak, aby ich splnenie bolo možné s nízkymi nákladmi. Vyššie uvedené zodpovedá aj dnešnému stavu, kedy množstvo služieb verejnej správy, špecificky takých, ktoré sú spojené iba s nízkymi nárokmi na bezpečnosť, implementuje de-facto mechanizmus autorizácie kliknutím, napr. vo forme potvrdzovacieho tlačítka „žiadam", „odoslať", „potvrdiť" a pod. Nie je preto potrebné ani efektívne vytvoriť povinne používaný centrálny komponent implementujúci autorizáciu kliknutím. ÚPVS má implementovať autorizáciu kliknutím iba pre elektronické podania prostredníctvom neho doručované jednotlivým OVM (viď. §29-33 ZeGov). Pre autorizáciu kliknutím je možné vytvoriť a prijať štandardy upravujúce technické a bezpečnostné požiadavky tak, aby bola zaistená právna istota a minimalizácia nákladov pri jej implementácii jednotlivými OVM.

Komentár za ITAS.: (Tejto téme sa stanovisko nevenuje).

Vyjadrenie NASES: V zmysle legislatívy je ÚPVS jedným z centrálnych prístupových miest. Vzťahuje sa naň aj ustanovenie o autorizácii § 23, odsek 1, písmeno a) bod 2 a písmeno b) (v nadväznosti potom ten istý paragraf, odsek 2) – pričom „podpisovanie", resp. využívanie el. podpisov je jedným z legitímnych (a podľa eIDAS aj interoperabilných) spôsobov. V širšom význame môžeme pokojne uvažovať o „centrálnom autorizačnom komponente", pričom na zabezpečenie nemennosti obsahu dokumentu sa dnes využíva takmer výhradne nejaká forma podpisu alebo pečate. V prvom priblížení ide viac o „podpisovací" (ale do budúcnosti v širšom význame autorizačný) komponent. V legislatíve nie je vymedzené, že podpisovanie má byť len „lokálne", určite by sme mali nastoľovať otázku, čo je pre verejnú správu a vynakladanie verejných prostriedkov optimálne. Azda ťažko za optimálny označiť stav, v ktorom každý OVM

obstaráva a implementuje „vlastné“ riešenie problému, ktorý môže byť efektívne vyriešený pre celé prostredie e-Governmentu len raz. Výhodou centrálneho riešenia (ale z pohľadu metódy poskytovania neutrálneho, resp. otvoreného) je však okrem nákladovej optimalizácie (ktorá môže byť vecou subjektívneho pohľadu, resp. „viery“ v efektivitu jedného a nedôvere k druhému princípu) nesporne schopnosť efektívne a plošne v budúcnosti zavádzať akýkoľvek nový spôsob autorizácie úkonu. Nemusíme ísť tak ďaleko do minulosti, aby sme vedeli oceniť úžitkovú hodnotu takejto možnosti – stačí sa pozrieť na odhalenú zraniteľnosť pri generovaní podpisovacích kľúčov na eID. Schopnosť „pružne“ reagovať bola pre SR limitovaná, najmä kvôli „lokálnemu“ prístupu k podpisovaniu.

Téma č.8: Legislatívna podpora autorizácie pri zavedení mID.

Komentár za S.D.: *Autorizáciu žiadame implementovať pre úroveň „použitím na to určenej funkcie informačného systému“ aka. „autorizácia kliknutím“. Legislatíva rozoznáva iba dva paušálne spôsoby autorizácie pri výkone verejnej moci elektronicky – KEP a autorizáciu kliknutím. Úroveň KEP je nákladná, je v protiklade s plánom pokryť iba vybrané služby a v protiklade s rýchlym efektívnym riešením. Konštrukcia §23.1 ZeGov presne určuje, ktoré podania vyžadujú akú úroveň autorizácie, nie je to závislé na zmenách legislatívy alebo „určení“ zo strany OVM. Autorizácia je vykonávaná na ÚPVS, ktorý realizuje doručovaciu službu, nie podpisovaciu službu. Z dlhodobého hľadiska považujeme za nevyhnutné upraviť ÚPVS na režim „elektronická doručovacia služba pre registrované zásielky“ v zmysle eIDAS z dôvodov mimo projektu Mobilné ID. Či je potrebné resp. vhodné túto službu realizovať ako kvalifikovanú nie je podľa nášho názoru v súčasnosti možné jednoznačne zodpovedať, potrebné je zvážiť náklady a prínosy takéhoto postupu. Pri implementácii autorizácie kliknutím nepovažujeme vhodné použiť AdES používateľa - nie je v slovenskej legislatíve zavedený, nie je verejnou správou akceptovateľný, jeho použitie by si vyžadovalo zvýšené náklady organizačné (nutnosť certifikačnej autority) aj technické (napr. ďalší kľúč/certifikát a ich manažment) a to aj na strane prijímateľov podaní (overovanie podpisu iným mechanizmom ako KEP), pre interoperabilitu doručovacích služieb eIDAS predpisuje iné bezpečnostné mechanizmy, naopak interoperabilita AdES prináša nové komplikácie. V súčasnosti je na ÚPVS implementovaných viacero služieb s de-facto autorizáciou kliknutím, napr. potvrdenie doručenky v schránke, udelenie oprávnenia na disponovanie so schránkou, vloženie správy do dlhodobého úložiska, ... – ich implementácia nepoužíva techniku elektronického podpisu používateľa a je dlhodobo považovaná za dostatočne spoľahlivú.*

Komentár za ITAS.: *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.

- *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 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.*
- *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 XXX.*

Vyjadrenie NASES: Autorizáciou je podľa § 3 písm. o) zákona o e-Governmente vyjadrenie súhlasu s obsahom a vykonaním právneho úkonu. Spôsoby autorizácie zo strany osoby, ktorá nie je orgánom verejnej moci, sú ustanovené v § 23 ods. 1 písm. a) zákona o e-Governmente. Predmetné ustanovenie upravuje tri spôsoby – (i) kvalifikovaný elektronický podpis, resp. pečať, (ii) podpis s použitím na to určenej funkcie IS prístupového miesta (ďalej len „Podpis klikom“) a (iii) uznaný spôsob autorizácie. Autorizáciu kvalifikovaným elektronickým podpisom, resp. pečaťou na účely tohto stanoviska nebudeme posudzovať, keďže s ňou Projekt nepočíta. Ak by ju NASES implementoval, ide o podrobne regulovanú oblasť, ktorá nepotrebuje v konečnom dôsledku právne posúdenie, ale posúdenie správnosti technickej realizácie. Rovnako sa nebudeme venovať uznanému spôsobu autorizácie, keďže ten je podľa § 59 ods. 1 písm. g) zákona o e-Governmente viazaný na vydanie vykonávacieho predpisu, ktorý takéto spôsoby definuje a tento predpis dnes vydaný nie je, čiže uznané spôsoby autorizácie neexistujú. Inštitút uznaného spôsobu autorizácie sa javí ako vhodný nástroj na prebratie inštitútov eIDAS, ktoré by na účely autorizácie mohli slúžiť, napríklad aj zdokonaleného elektronického podpisu. Inštitúty, ktoré nariadenie eIDAS pozná a ktorým priamo z nariadenia nie sú ustanovené účinky rovnaké ako napríklad kvalifikovanému elektronickému podpisu, by tak tieto účinky mohli získať a na účely autorizácie by bolo možné využiť viacero inštitútov, ktoré zároveň zabezpečujú aj interoperabilné riešenia v rámci členských štátov EÚ.

Pokiaľ ide o Podpis klikom, podľa § 23 ods. 1 písm. a) zákona o e-Governmente ide o spôsob autorizácie, ktorý je rovnocenný vlastnoručnému podpisu nevyžadujúcemu úradné osvedčenie. Inými slovami, nedá sa platne použiť na taký právny úkon, ktorý podľa osobitného predpisu vyžaduje úradné osvedčenie podpisu konajúcej osoby. Z hľadiska jeho definície ustanovuje zákon o e-Governmente nasledovné podmienky, ktoré musí spĺňať – (i) vyhotovuje sa s použitím na to určenej funkcie informačného systému prístupového miesta, (ii) vyžaduje úspešnú autentifikáciu osoby, ktorá autorizáciu vykonáva, zodpovedajúcej najmenej úrovni zabezpečenia „pokročilá“ podľa nariadenia eIDAS, (iii) musí byť zabezpečené uvedenie podpisujúcej osoby ako odosielateľa

elektronickej správy s autorizovaným dokumentom, (iv) musí byť zabezpečená nemennosť obsahu autorizovaného dokumentu do momentu uloženia v elektronickej schránke adresáta, a (v) musí byť zabezpečené spojenie autorizovaného dokumentu s identifikátorom osoby odosielateľa a zachovanie väzby medzi nimi. Podpis klikom je možné použiť vždy, ak to osobitný predpis nezakazuje.

Z hľadiska podmienky vyhotovovania prostredníctvom určenej funkcie prístupového miesta platí, že samotný Podpis klikom musí byť vytváraný v podmienkach prístupového miesta. Ide z povahy veci primárne o tri prístupové miesta – ÚPVS, špecializovaný portál a IOM – keďže funkcie ústredného kontaktného centra nie sú zamerané na elektronickú komunikáciu smerom k orgánu verejnej moci (aj keď nie je vylúčené jeho použitie napr. pri autorizácii nahlasovaného technického problému). Ustanovením tejto podmienky sa sledujú dva hlavné ciele – (i) odbremeniť používateľa služby od potreby vynakladania osobitných nákladov ma obstaranie si a udržiavanie prostriedku autorizácie a (ii) zveriť vytvorenie a kontrolu nad prostriedkom autorizácie „do rúk štátu“ s tým, aby nebola potrebná žiadna ďalšia regulácia konkrétnych technických podrobností s tým spojených (ako by to bolo v prípade „otvorenia“ Podpisu klikom pre akéhokoľvek poskytovateľa). Svojím spôsobom teda išlo primárne o snahu vybudovať centralizovaný komponent na podpisovanie najmä na ÚPVS a v druhom rade dať túto možnosť aj pre konkrétne agendové systémy. Samozrejme, uvedené neznamená, že napr. aplikácia, ktorú si užívateľ inštaluje na účely autentifikácie, nemôže zároveň obsahovať nástroj na autorizáciu. Vyššie uvedené dôvody uvádzame na dokreslenie motivácie gestora zákona, nie ako obmedzenie alebo príkaz, ktorý zákon ukladá.

Podmienka autentifikácie najmenej na úrovni „pokročilá“ odkazuje na podmienky, vymedzené čl. 8 ods. 2 písm. c) a súvisiacimi článkami nariadenia eIDAS. Z hľadiska zákona o e-Governmente je dôležité, že úspešná autentifikácia je podmienkou autorizácie v zmysle, že musí byť „viazaná“ k autorizácii. Inými slovami, musí ísť o autentifikáciu, ktorej jediným dôvodom je s tým spojená autorizácia konkrétneho dokumentu. Z tohto pohľadu je teda podmienka splnená, ak po tom, ako

používateľ zvolí dokument, ktorý chce autorizovať, musí absolvovať úspešnú autentifikáciu, ktorej bezprostredným „následkom“ je autorizácia dokumentu.

Uvedenie autorizujúcej osoby ako odosielateľa elektronickej správy súvisí s podmienkou zviazania identity odosielateľa s autorizovaným dokumentom a vytvorením väzby medzi nimi. Dôvod je zrejmý, ide o deklarovanie identity autorizujúcej osoby vo vzťahu k autorizovanému dokumentu. Takýto spôsob autorizácie nie je možné využiť v prípadoch, kedy je autorizujúca osoba odlišná od odosielateľa správy – alebo presnejšie povedané od osoby, ktorá je ako odosielateľ správy uvedená. Aj keď nie je vylúčené a je možné použiť Podpis klikom aj bez „okamžitého“ odoslania správy s autorizovaným dokumentom, bez ohľadu na to, kedy k odoslaniu tejto správy dôjde, autorizujúca osoba musí byť uvedená ako jej odosielateľ. Zákon nepredpisuje konkrétne technologické riešenie na vytvorenie väzby medzi dokumentom a informáciou o identite toho, kto ho autorizoval. Dôležité je len to, že takáto väzba bude existovať a bude „nepochybná“ a určujúca identitu autorizujúcej osoby.

Poslednou podmienkou je zabezpečenie nemennosti obsahu autorizovaného dokumentu, pričom zákon túto podmienku vyžaduje splniť minimálne do doby uloženia v elektronickej schránke adresáta. Napriek tomu, že sa v náležitostiach Podpisu klikom uvádza elektronická schránka adresáta, je potrebné upozorniť na to, že Podpis klikom je autorizáciou, a teda separátnym, oddeleným úkonom od doručovania. Inými slovami, nejde o jeden a ten istý úkon, rovnako ako nejde o úkony podmienené. Podpis klikom môže spĺňať zákonné náležitosti aj v prípade, ak k odoslaniu autorizovaného dokumentu nikdy nedôjde, alebo ak s ním bude naložené iným spôsobom ako doručením do elektronickej schránky adresáta. Ide totiž o podmienku, ktorá je kladená na „kvalitu“ Podpisu klikom a nie o podmienku alebo náležitosť jeho použitia.

Zákon nepredpisuje konkrétne technologické riešenie Podpisu klikom, z čoho vyplýva, že podstatným pre posúdenie splnenia náležitostí Podpisu klikom je posúdenie splnenia podmienok

podľa § 23 ods. 1 písm. a) druhého bodu zákona o e-Governmente. Z technologického hľadiska je teda možností realizácie niekoľko, vrátane využitia už existujúcich a štandardizovaných riešení, akými sú aj elektronické podpisy podľa nariadenia eIDAS – zákon o e-Governmente tomuto žiadnym spôsobom nebráni. Vzhľadom na existujúce podmienky a obmedzenia vo vzťahu ku kvalifikovaným certifikátom na vyhotovenie kvalifikovaného elektronického podpisu a ich umiestneniu, resp. kvalitatívnych podmienkach kladených na zariadenie, v ktorom sú umiestnené, sa ako vhodný vždy javil zdokonalený elektronický podpis podľa čl. 26 nariadenia eIDAS. Podľa predmetného článku musí zdokonalený elektronický podpis spĺňať nasledovné podmienky – (i) musí byť jedinečne spojený s podpisovateľom, (ii) musí umožňovať určiť totožnosť podpisovateľa, (iii) musí byť vyhotovený s pomocou údajov, ktoré s vysokou mierou dôveryhodnosti podpisovateľ používa pod svojou výlučnou kontrolou a (iv) musí byť spojený s podpisovanými údajmi spôsobom, ktorý umožňuje každú dodatočnú zmenu údajov zistiť. Prvé dve podmienky súvisia s určením totožnosti autorizujúcej osoby a vo vzťahu k Podpisu klikom je ich splnenie zároveň splnením podmienky spojenia identifikátora autorizujúcej osoby s autorizovaným dokumentom. Podmienka kontroly nad údajmi, použitými na vyhotovenie zdokonaleného elektronického podpisu zároveň predstavuje splnenie podmienky autentifikácie podpisovateľa, ktorá je podmienkou autorizácie Podpisom klikom. Nariadenie eIDAS nevyžaduje, aby údaje potrebné na vyhotovenie zdokonaleného elektronického podpisu boli pod výlučnou kontrolou podpisujúceho – postačuje vysoká miera dôveryhodnosti v tom, že použitie týchto údajov na vyhotovenie podpisu je pod výlučnou kontrolou podpisovateľa. Inými slovami, že je s vysokou mierou dôveryhodnosti možné tvrdiť, že zvolený mechanizmus zabezpečí, že podpis vyhotoví práve a len ten, „komu podpis patrí“, resp. kto je s podpisom „jedinečne spojený“. Táto požiadavka na zdokonalený elektronický podpis by teda mohla zároveň splniť aj zákonom o e-Governmente vyžadovanú autentifikáciu na účely podpisu a jeho vyhotovenia. Podmienka umožniť zistenie dodatočnej zmeny údajov súvisí so zachovaním integrity dokumentu, ktorý je autorizovaný. Nejde pritom o objektívnu nemožnosť zmeny, ale o ochranu pred dodatočnou zmenou, zmenou po podpísaní dokumentu. Požiadavku nemennosti obsahuje aj Podpis klikom, pričom táto požiadavka rovnako nie je formulovaná ako objektívna nemožnosť zmeny, ale ako vlastnosť zvoleného technologického riešenia, ktoré slúži na ochranu integrity dokumentu po

jeho podpísaní. Požiadavka zdokonaleného elektronického podpisu, viazaná na ochranu integrity dokumentu, by teda rovnako mohla spĺňať požiadavku zákona o e-Governmente na zabezpečenie nemennosti obsahu autorizovaného dokumentu.

Na základe vyššie uvedeného máme za to, že na autorizáciu v prípade mobileID je možné použiť Podpis klikom, keďže ide o spôsob autorizácie, ktorý zákon o e-Governmente pripúšťa:

- použiť ľubovoľné technologické riešenie Podpisu klikom, ak sa zabezpečí splnenie zákonom ustanovených podmienok,
- nie je vylúčené (z hľadiska interoperability je to dokonca vhodné a pri príprave zákona s tým bolo uvažované) aby sa využilo technologicky rovnaké riešenie ako na elektronické podpisy podľa nariadenia eIDAS, pričom ako vhodný sa javí najmä zdokonalený elektronický podpis.
- Parametre ako finančná náročnosť, používateľská prívetivosť a miera jednoduchosti adaptácie existujúceho eGov prostredia na nový spôsob autorizácie by mali byť predmetom posudzovania pri konkrétnych kandidátskych riešeniach. Napríklad už teraz si dovoľujeme nesúhlasiť s predpokladom S.D., že zdokonalený el. podpis vygeneruje vysoké dodatočné náklady pre jeho akceptáciu v existujúcich systémoch eGov – už len na báze argumentu, že ide o riešenie architektonicky veľmi príbuzné (ak nie takmer totožné) s aktuálne zavedeným a podporovaným riešením na báze kvalifikovaných elektronických podpisov.

Vyjadrenie k využitiu kvalifikovaných dôveryhodných služieb pre mobileID:

Nariadenie eIDAS dáva členským štátom možnosť definovať si vlastné dôveryhodné služby, a to aj na účely autentifikácie alebo autorizácie. Ich následné využitie na účely mobileID nie je samozrejme vylúčené, tento koncept však má dve slabiny.

Prvou je fakt, že z právneho hľadiska neprinesie nič nové do dnešnej situácie, keďže právny základ pre mobileID existuje už dnes. Diskusia o tom, že projekt mobileID môže byť postavený na inom právnom základe, je síce možná, avšak mala by zmysel v prvom rade vtedy, ak by súčasný právny

základ nebol plnohodnotne použiteľný. Zastávame názor, že k takejto situácii nedošlo a preto aj argument použitia dôveryhodných kvalifikovaných služieb nie je argumentom proti realizácii projektu mobileID ako takej.

Druhou slabinou je paradoxne samotná interoperabilita, keďže definovanie vlastných dôveryhodných kvalifikovaných služieb namiesto využitia (v časti autorizácie) interoperabilného riešenia priamo predpokladaného nariadením eIDAS by viedlo práve k nemožnosti potenciálneho využitia výstupov projektu mobileID vo vzťahu k zahraničiu.

Argument smerujúci k nahradeniu autorizácie dôveryhodnou kvalifikovanou službou elektronického doručovania registrovaných zásielok je legitímny, jeho uplatnenie v praxi však vyžaduje zmenu nielen zákonnej úpravy, ale aj nastavenia procesov. Podstatou úpravy zákona o e-Governmente je okrem iného aj to, že vo vzťahu k podaniam a rozhodnutiam nezasahuje do ich obsahových náležitostí, ale ustanovuje ich „vyjadrenie“ v elektronickej komunikácii. Z toho vyplýva, že v súčasnej situácii je autorizácia oddeleným inštitútom od doručovania – ide o dva osobitné úkony. Právna fikcia, spočívajúca v „nahradení podpisu odoslaním“ nie je vylúčená, ale jej zavedenie nie je triviálne. Zároveň v situácii, ak sa tým má nahradiť z hľadiska nariadenia eIDAS plne interoperabilné riešenie autorizácie zdokonaleným elektronickým podpisom, je otázne, nakoľko prevratný prínos by pre projekt mobileID samotný takéto nahradenie malo.

Tento návrh je možné vnímať ako legitímny smer diskusie k systémovej zmene elektronickej komunikácie so štátom. Samotné nariadenie eIDAS poskytuje základ k jeho možnej implementácii, avšak ani toto nariadenie neustanovuje fikciu podpisu doručovaného dokumentu jeho odoslaním. Podľa čl. 43 ods. 2 nariadenia eIDAS sa ustanovuje „len“ domnienka integrity, garancie identity odosielateľa a adresáta a dátumu a času odoslania a doručenia. Nariadenie eIDAS nekonštituuje právnu domnienku, či fikciu vyjadrenia vôle s obsahom zásielky len jej odovzdaním na prepravu. Nebráni to samozrejme úprave takejto domnienky, či fikcie v slovenskom práve, avšak z hľadiska interoperability to len na základe nariadenia eIDAS nezaručuje akceptovanie doručovaného dokumentu ako dokumentu, vo vzťahu ku ktorému bol prejavený súhlas s jeho obsahom – čo použitie elektronického podpisu zabezpečuje.

V záverečnej skratke, vychádzajúc len z nariadenia eIDAS je dôveryhodná kvalifikovaná služba elektronického doručovania registrovaných zásielok len „poštár, ktorému môžem veriť“, bez vzťahu k prejavu vôle k obsahu doručovanej zásielky.

Téma č.9: Využívanie mobileID mimo verejnej správy a otvorenosť využívania služieb autentifikácie a autorizácie aplikáciami tretích strán cez OpenAPI.

Komentár za S.D.: *Primárne má riešenie slúžiť pre verejnú správu v SR, nemajme veľké oči. Autentifikačná služba má byť použiteľná aj mimo verejnej správy. Odporúčame vytvoriť možnosť čo najjednoduchšieho použitia tejto služby tretími stranami – redukovať povinnosti pri integrácii. Cieľ však nie je, aby táto služba bola použiteľná pre „všetky“ služby v komerčnej sfére – prvoradé je vytvorenie efektívneho riešenia pre verejnú správu, komerčné subjekty si sami vyhodnotia, či toto riešenie je dostatočné pre ich službu. Na základe našej skúsenosti sme presvedčení, že aj v „komerčnom“ prostredí je podstatne viac / častejšie používaných služieb vyžadujúcich nižšie požiadavky na bezpečnosť ako „najvyššiu úroveň“, prípadne by bolo vhodné vykonať prieskum dopytu po autentifikačnej službe mimo verejnej správy. Z dlhodobého hľadiska je vhodný štandardný postup otvorenia tejto služby mechanizmom podľa eIDAS.*

Riešenie má byť jednoducho interoperabilné pre aplikácie tretích strán. Najmä pre aplikácie pre vytváranie KEP na mobilných platformách – tak, aby ich bolo možné jednoducho integrovať do plne mobilného scenára použitia služieb eGov. Téma integrácie iných (komerčných) služieb identifikácie/autentifikácie nie je doriešená.

Komentár za ITAS.: *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. Pre inštitúcie finančného sektora to záleží najmä od rešpektovania záväzného legislatívneho rámca – minimálne v rozsahu:*

a) zákon č. 297/2008 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 o platobných službách (transponovaná PSD2 smernica) - § 3c Silná autentifikácia používateľa platobných služieb podľa regulatívneho technického štandardu od European Banking Authority. 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.

Vyjadrenie NASES:

Jedným z cieľov projektu je aj otvorenie využívania služieb autentifikácie a autorizácie tretími stranami, a tým vytvorenie predpokladu pre rozšírenie využívania štátom garantovanej identity aj v komerčnom sektore. V prvej etape ide o vytvorenie základných predpokladov, t. z. čo najjednoduchšie pripojenie a využívanie služieb autentifikácie a autorizácie (napríklad redukovaním povinností pri integrácii). Uvedené už umožní občanom a podnikateľom využívanie v scenároch komerčného sektora, ktoré sú z nášho pohľadu najčastejšie (napríklad prihlasovanie do klientskych zón či autorizácia väčšiny transakcií. Samozrejme, budeme sa následne zaoberať aj možnosťou využívať mobileID aj pri (z pohľadu legislatívy) špecializovaných scenároch (napríklad založenie účtu online).

Téma č.10: Prezentácia rozpracovaného zámeru mobile ID na pracovnej skupine UPPVII

Komentár za S.D.: (Tejto téme sa stanovisko nevenuje)

Komentár za ITAS.: *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.*

Vyjadrenie NASES:

Počas jesene predpokladáme prezentáciu detailnejšie rozpracovaného zámeru mobileID na pracovnej skupine Lepšie služby.

Téma č.11: Mobilná aplikácia ako open source

Komentár za S.D.:

Aplikácia na mobile má byť vyvíjaná ako OpenSource, t.j. zverejnený zdrojový kód, ktorý môže každý použiť, vrátane možnosti vytvárať odvodené diela. Je to aj požiadavka z úlohy č. 16 Akčného plánu OGP 2017-19 „Pre novovytvárané ... a klientskych aplikácií umožniť zverejnenie ich zdrojového kódu a vývoj metódou otvoreného kódu (open source)“

Komentár za ITAS.: (Tejto téme sa stanovisko nevenuje)

Vyjadrenie NASES:

Súhlasíme a budeme sa snažiť túto požiadavku v maximálnej miere zohľadniť. Výnimkou pre zverejňovanie zdrojových kódov môžu byť prípadné bezpečnostné mechanizmy riešenia.