Dobrý deň,

za Slovensko.Digital sa zasadnutia pracovnej skupiny zúčastním ja. Pre informáciu, tento materiál už bol pred cca. 2 týždňami predstavený v pracovnej skupine Governance, kde bolo uvedené že najbližším krokom MIRRI je po odbornej diskusii rozhodnutie, či navrhovaný prístup bude použitý, alebo nie. V tomto duchu posielam aj nasledovné stanovisko:

Tému autorizácie nemá zmysel riešiť úplne izolovane, je silne prepojená s témami identifikácie, autentifikácie a prideľovania oprávnení (authentication / authorization / access control).

V týchto oblastiach je predložený dokument jedna z mála viditeľných centrálnych aktivít. Aj v tomto kontexte navrhnutú zmenu legislatívy vnímam mimoriadne negatívne. Vítam možnosť diskusie ešte v tomto skorom štádiu pripravovanej zmeny, vopred posielam tieto pripomienky / otázky:

·         Nie je jasné, aký problém navrhovaná legislatívna zmena má riešiť. V oblasti autentifikácie/autorizácie samozrejme v súčasnosti vidím viaceré výzvy, avšak žiadnu z nich nie je potrebné riešiť „zmenou legislatívy“ a navyše takouto zásadnou. Práve naopak, zásadne obmedzené zdroje ktoré máme (najmä čas = ľudské kapacity x potrebné zmeny) má zmysel investovať do riešenia práve tých akútnych problémov.

·         Navyše efekt legislatívnej zmeny sa nevyhnutne dostaví až v dlhodobom horizonte, minimálne 2 rokov, najmä ak ide o takto rozsiahlu zmenu. Čiže navrhovaná zmena nemôže vyriešiť žiadne akútne problémy.

·         Rozumiem plánu na „dlhodobé zmeny“, avšak v súčasnosti sme natoľko pozadu v nasadení toho čo „je možné teraz“ a v skutočnom riešení dnes známych problémov, že podľa mňa nedokážeme dobre odhadovať ani potrebu a zameranie dlhodobých zásadných zmien. Sústreďme sa najbližšie 2 roky na akútne problémy a následne bude jasnejšie čo/ako je vhodné meniť dlhodobo.

·         Pri poslednej väčšej novelizácii z.305/2013 bolo deklarované, že jedných z jej účelov je vyriešenie všetkých potrebných zmien týkajúcich sa autentifikácie/autorizácie, a to aj z pohľadu interakcie IS-IS. Je preto prekvapivé, že práve teraz prichádza návrh na ďalšie a zásadné zmeny v tejto oblasti, hoci zatiaľ ani to čo už v zákone je uvedené dnes nie je poriadne využívané.

·         Materiál správne konštatuje, že v prostredí verejnej správy je vhodný „konzervatívny prístup k autorizácii“. Jeden z aspektov tejto konzervatívnosti je minimalizácia nákladov, a to tak na riešenia komunikácie s FO/PO, rovnako aj v rámci verejnej správy interne. Práve podpora iba vhodnej minimálnej sady technologických riešení k takejto minimalizácii nákladov povedie – čo je presne opačný prístup ako je predpokladaný v predkladanom návrhu.

·         Predkladaný návrh bude práveže mimoriadne náročný na zdroje, pričom odhad v tejto oblasti absentuje. Pôjde o náklady tak na technologické riešenia, ako aj organizačné zabezpečenie – samotná zmena legislatívy, súvisiace predpisy, centrálna správa metód autorizácie, posúdenia jednotlivých nových spôsobov autorizácie. Ak by sa v návrhu na legislatívnu zmenu malo pokračovať, je potrebné do neho už v súčasnosti doplniť odhad potrebných zdrojov.

·         V súčasnosti už jeden prístup založený na „úrovniach“ máme – v autentifikácii (tak v SK Výnose o štandardoch, ako aj v nariadení eIDAS) a vidíme ako mimoriadne slabo je pochopený/uplatňovaný zo strany OVM.

·         V neposlednom rade navrhovaná legislatívna úprava vyzerá byť mimoriadne podrobná, s čím je pri legislatívnych zmenách potrebné narábať veľmi opatrne (napr. vlastnoručný podpis nie je legislatívne definovaný) a taktiež navrhovaný postup nemá zrejme vo svete obdobu.

·         Rovnako negatívne vnímam možnosť „výberu metódy autorizácie“ zo strany každého OVM. Oproti súčasnému stavu by išlo o významné rozšírenie možností rozhodovania orgánov VS na úkor zákonodarnej moci. Aj na základe doterajších skúseností je zrejmé, že tendenciou OVM bude povoliť iba najstriktnejšie možné úrovne, čo bude zásadne znižovať použiteľnosť.

·         V súčasnosti pri listinne realizovaných úkonoch má VS dobre (historicky) stanovené a legislatíve zakotvené požiadavky na autorizáciu.  To zahŕňa aj ošetrenie rizík pri rôznych neštandardných situáciách (podvody, falšovania, vynútená autorizácia a pod.). Preto považujem za mimoriadne vhodné elektronické spôsoby autorizácie presne zacieliť na charakteristické metódy autorizácie z listinného sveta. Z tohto hľadiska je vo VS najširšie používaná úroveň „vlastoručný podpis“ a „osvedčený podpis“. Presne týmto úrovniam zodpovedajú dnes v legislatíve zachytené elektronické metódy „autorizácia kliknutím“ (presnejšie autorizácia použitím funkcie informačného systému) a KEP. V duchu zásady „prostriedok s vyššími zárukami je použiteľný tam kde stačia nižšie záruky“ je možné KEP použiť aj tam, kde je postačujúci iba vlastnoručný podpis – rovnako ako je takto možné využiť osvedčený podpis.

·         Nevidím teda ani z tohto hľadiska dôvod na zásadné zmeny v oblasti autorizácie z pohľadu legislatívy. Skôr je potrebné sa sústrediť na implementáciu všetkých možností ktoré nám už súčasná legislatíva poskytuje a vyriešenie súvisiacich problémov – z ktorých niektoré sú známe aj viac ako 10 rokov.

·         Metóda autorizácie kliknutím poskytuje vo všetkých aspektoch (aspekty v zmysle predkladaného návrhu) vyššie bezpečnostné záruky ako vlastnoručný podpis. Pri identifikácii konajúceho, integrite úkonu, zachytení času vykonania úkonu, ako aj nespochybniteľnosti úkonu poskytuje vlastnoručný podpis iba minimálne záruky, čo aj doteraz bolo pre VS dostatočné. Z tohto hľadiska je možné bez obáv plošne nasadiť autorizáciu kliknutím všade tam, kde je vyžadovaný (iba) vlastnoručný podpis – odhadom ide o viac ako 80% všetkých úkonov pri interakcii s VS. Ako som už uviedol vyššie, na riešenie pochybností sa použijú doterajšie metódy formálne / právne / znalecké.

·         Mechanizmus použitia používateľom lokálne vytváraného „elektronického podpisu“ sa celosvetovo ukazuje ako veľmi slabo používané riešenie. QES/AdES má pri interakcii FO/PO s VS viaceré podstatné slabé miesta, najmä:

o    slabá možnosť automatickej identifikácie podpisujúceho

o    závislosť na tretích stranách (CA v rámci celej certifikačnej cesty)

o    mimoriadne komplikované overovanie platnosti podpisu

o    mimoriadne široké možnosti podpisových formátov/kontajnerov

o    prenesenie všetkej zodpovednosti na používateľa ktorý podpis vytvára, pričom tento de-facto je vo veľmi nevýhodnom postavení (vie iba veľmi slabo overiť čo podpisuje)

·         Naopak, špeciálne v asymetrických vzťahoch (t.j. kde neide o voľnú dohodu viacerých rovnocenných strán, ale o použitie schematickej služby poskytovanej jednou stranou v štandardizovaných formálnych aj technických rámcoch) stále viac rozšírené metódy sú založené na silnej identifikácii „používateľa“ a zachytenie prejavu vôle sa realizuje technickými prostriedkami výlučne pod kontrolou poskytovateľa služby. Výhodou tohto prístupu je mimoriadna flexibilnosť na strane poskytovateľa služby, tak v oblasti „servisu“ pre používateľa (t.j. spraviť implementáciu jednoducho použiteľnou), ako aj v úrovni bezpečnostných záruk za jeho časť riešenia.

·         V navrhovanej úprave kľúčovým miestom je definovanie úrovní pre jednotlivé aspekty bezpečnostných záruk. Pritom sa navrhujú binárne kritériá pre splnenie určitého aspektu záruk – áno/nie = spĺňa/nespĺňa. Je potrebné uvedomiť si, že v realite je situácia odlišná; každá reálna implementácia v uvedených aspektoch poskytuje záruky do určitej výšky a nikdy nie úplne. Preto pri zavedení navrhovaného konceptu bude potrebné stanoviť hranicu, kedy už určité záruky sú „splnené“. Táto hranica bude arbitrárna a do budúcnosti bude spôsobovať podstatné obmedzenia deklarovanej flexibility.

·         Zároveň v niektorých aspektoch v súčasnosti vnímané záruky sú de-facto iluzórne. Najlepším príkladom je deklarácia, kedy pri vytváraní KEP má údajne používateľ „pod svojou kontrolou prostriedky, ktorými sa autorizácia vykonáva“. V skutočnosti táto premisa platí iba teoreticky, reálne používateľ použije hardvér a softvér, ktorý nemá úplne pod svojou kontrolou a nevie overiť ako funguje, rovnako nevie overiť aký dokument v skutočnosti podpisuje – z jeho pohľadu ide „iba“ o súhlas s tým, čo vidí na obrazovke a dôveru v poskytovateľa nástrojov ktoré používa.

Do diskusie k téme autentifikácii/autorizácii však chcem pristúpiť konštruktívne. Mali by sme sa spoločne zamyslieť, ktoré problémy a ciele pred nami sú a je potrebné ich riešiť. Navrhujem nasledovné aktivity z krátkodobého hľadiska:

·         Rozšírenie nasadenia metódy autorizácie kliknutím všade tam, kde to už súčasná legislatívna úprava umožňuje. V tejto téme má samozrejme zmysel postupovať tiež koordinovane, nasledovným spôsobom:

o   „toolkit“ pre čo najjednoduchšie nasadenie v nových službách

o    úprava existujúcich služieb podľa priorít, najmä používanosti služby

o    najskôr tam, kde nie je „odpor úradníkov“, prípadné výhrady

·         Vydať štandard pre preukazovanie autorizácie kliknutím, najmä pri komunikácii medzi OVM navzájom

·         Reálna klasifikácia elektronických služieb do úrovní autentifikácie, špecificky do úrovne „pokročilá“ podľa eIDAS

·         Zmena SK štandardu pre úrovne autentifikácie na 3 úrovne kompatibilné s eIDAS

·         Pri identifikačných schémach podľa eIDAS doriešiť, aby SK implementácia nebola iba Potemkinova dedina, t.j. po prihlásení ne-SK schémou vedel občan aj reálne nejaké služby použiť

·         Doriešiť skutočné akceptovanie KEP, nielen založeného na certifikátoch z eID, vrátane opustenia prítomnosti RČ v certifikáte pre KEP v eID.

A taktiež nasledovné aktivity z dlhodobého hľadiska:

·         Strategické riešenie pre komunikáciu IS-IS, špecificky čo s registrom autentifikačných certifikátov, ktorý považujem za legislatívny archaizmus.

·         Naopak, asap riešenia pre udeľovanie oprávnení na zastupovanie – špeciálne centrálny register elektronických plnomocenstiev

·         Zmysel a uplatnenie úrovne autentifikácie „nízka“ podľa eIDAS a systematický prístup jej využitia. Napr. autentifikácia pomocou verejne používaných schém – Google, Facebook...

·         Funkčné riešenia pre dlhodobé uchovávanie autorizovaných elektronických dokumentov. Špecificky modul MDUERZ ÚPVS nie je jasné aké funkcie v súčasnosti plní a akým spôsobom

Ľubor Illek  
Slovensko.Digital