# Doručené pripomienky k návrhu štruktúry pre potvrdenie autorizácie vykonanej podľa § 23 ods. 1 písm. a) bod 2 (tzv. "autorizácia klikom")

Obsah

[Doručené pripomienky k návrhu štruktúry pre potvrdenie autorizácie vykonanej podľa § 23 ods. 1 písm. a) bod 2 (tzv. "autorizácia klikom") 1](#_Toc56466613)

[Pripomienky od Jozefa Jankoviča v zastúpení Združenie miest a obcí Slovenska 1](#_Toc56466614)

[Pripomienky od Juraja Hájeka v zastúpení Ardaco, a.s. 4](#_Toc56466615)

[Pripomienky od Pavla Friča v zastúpení DITEC, a.s. 8](#_Toc56466616)

[Pripomienky od Martina Blaška v zastúpení Globaltel a.s. 12](#_Toc56466617)

[Pripomienky od Ľubora Illeka v zastúpení Spoločnosť pre otvorené informačné technológie 15](#_Toc56466618)

[Pripomienky od Michala Kevického v zastúpení za Národná agentúra pre sieťové a elektronické služby 16](#_Toc56466619)

[Pripomienky od Emila Fitoša v zastúpení za IT Asociáciu Slovenska 18](#_Toc56466620)

[Princíp „Autorizácie klikom“ 18](#_Toc56466621)

[Pripomienky k navrhovanej štruktúre 20](#_Toc56466622)

[Ďalšie odporúčania 22](#_Toc56466623)

## Pripomienky od Jozefa Jankoviča v zastúpení Združenie miest a obcí Slovenska

* V texte dokumentu sa uvádza medzi základnými požiadavkami „väzba na autorizovaný dokument vo forme jeho digitálneho odtlačku“
  + pri porovnaní s PPT máme za to, že sa nejedná o povinnú položku, zrejme ide o doplňujúci údaj k autorizácii (authorization data)

Š.Szilva: Pokiaľ je doložka spoločne autorizovaná s podaním, digitálny odtlačok sa nachádza priamo v podpise.

Uvádzanie digitálneho odtlačku v doložke môže byť predmetom diskusie pre prípad potreby oddelenia elektronického podania a doložky.

* K PPT:
  + Delegation – máme za to, že by sa nemalo jednať o povinný údaj.

 Š. Szilva: Ide o nepovinný údaj v prípade, ak osoba vykoná autorizáciu klikom vo vlastnom mene. Povinný je tento údaj v prípade, ak osoba koná v mene inej osoby.

Autentifikovaná osoba:

* A) prihlásená v zastúpení inej osoby (napr. štatutár, zákonný zástupca) môže autorizáciu klikom vykonať s uvedením prihlásenej osoby a zastupovanej osoby v autorizačnej doložke.   
  V zmysle § 23 ods. 1 písm. a) bod 2 platí povinnosť uviesť autorizujúcu osobu ako odosielateľa elektronickej správy (elektronického podania).   
  V zmysle prílohy č. 10 Vyhlášky č. 78/2020 Z. z. je SubjectID v SAML Assertion osoba, v mene ktorej sa proces vykonáva.

Generálne zastupovanie podľa všeobecne záväzného právneho predpisu je v zmysle prílohy č. 10 iba v prípade DelegationType = 0.

* B) prihlásená vo vlastnom mene.

Používateľské prostredie pre vykonanie autorizácie musí používateľa informovať, v koho mene je autorizácia vykonávaná. V prípade prihlásenia v zastúpení inej osoby sa v používateľskom prostredí zobrazuje informácia, v koho mene je osoba prihlásená, čo by mohlo používateľa uviesť do omylu. Príkladom je aj portál [www.dcom.sk](http://www.dcom.sk) .

* + Ďalej.:
    - celý formulár doložky obsahuje primárne údaje o autentifikovanej osobe, ktorá vykonáva autorizáciu (v zmysle IAM UPVS to je Actor, ktorý má ActorID). V tejto časti by sa malo jednať o zastupovaný subjekt, čiže Subject

Š.Szilva:   
  
V zmysle prílohy č. 10 Vyhlášky č. 78/2020 Z. z. o štandardoch pre IT VS je SubjectID: *„Samotný identifikátor identity v roli subjekt. Subjektom je konkrétna osoba, v mene ktorej sa vykonáva proces.  
Hodnotou je identifikátor právnickej osoby alebo identifikátor fyzickej osoby. V prípade, že používateľ koná vo svojom mene, hodnota je totožná s ActorID.“*

V prípade autentifikácie použitím autentifikačného certifikátu sa v ActorID v súčasnosti uvádza identifikátor technického účtu. Identifikátor držiteľa autentifikačného certifikátu je v prípade prihlásenia vo vlastnom mene uvedený v SubjectID a v prípade prihlásenia v mene inej osoby je uvedený v DerivedFromID.

* + - chýbajú informácie o zastupovanom subjekte – meno, priezvisko, identifikator (RČ v zmysle zákona), UPVS\_ID resp. údaje právnickej osoby aj s UPVS\_ID

Š.Szilva:   
Ide o základný návrh do diskusie, takéto detailné údaje preto v štruktúre zatiaľ uvádzané neboli.

* + Navrhujeme štruktúru informácií rozdeliť nasledovne (viď schéma ako priložený obrázok, žltou zvýraznené informácie, ktoré si myslíme že zaslanému návrhu chýbajú):
    - Údaje autorizujúcej osoby (ktorá bola autentifikovaná)
      * Meno, priezvisko, formátované meno
      * Identifikátor osoby, Issuer\_country, Typ identifikátora
        + Podla zakona to moze byt pri fyzickej osobe len rodne cislo alebo zahranicny identifikator.
      * PersonGUID - Univerzalny identifikator identity v eGov

Š.Szilva:   
Môžeme o návrhu diskutovať. UPVSIdentityID je však interný identifikátor vytváraný v ÚPVS IAM, nie je definovaný v zákone ani používaný v referenčných registroch.

* + - Popis autentifikácie osoby (Authentication\_method)
      * Identifikator autentifikacneho prostriedku osoby
      * Typ autentifikacneho prostriedku (PersonAuthResourceType) - Kod z ciselnika - povolene hodnoty 2 = eID, 4 = Certifikat, 9 = eIDAS, 10 = mID

Š.Szilva MIRRI: O návrhu je možné diskutovať. Táto miera detailu v návrhu nebola uvedená.   
Vami uvedené hodnoty sú z číselníka ÚPVS IAM authResourceType.  
Prosím rozviesť, čo konkrétne máte na mysli identifikátorom autentifikačného prostriedku v jednotlivých prípadoch?

* eID - číslo občianskeho preukazu? Upozorňujem, že dnes číslo občianskeho preukazu nie je v SAML tokene vydávanom UPVS IAM. Obsahuje však PČO.
* autentifikačný certifikát – CN z certifikátu alebo digitálny odtlačok certifikátu?
* eIDAS – Jedinečný identifikátor vytvorený na účely cezhraničnej identifikácie? V zmysle Vykonávacieho rozhodnutia [Komisie EÚ č. 2015/1501](https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:32015R1501&from=EN) a ani v zmysle špecifikácie [eIDAS SAML Attribute Profile](https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20SAML%20Attribute%20Profile%20v1.2%20Final.pdf) nie je takýto údaj pri cezhraničnej identifikácie k dispozícii.
* mID – jedinečné číslo generované pre mobilné zariadenie?
  + - * Issuer\_country

Š.Szilva:   
V prípade eIDAS prostriedkov je k dispozícii iba údaj Issuer\_country pre jedinečný identifikátor. V prípade eID, autentifikačného certifikátu a mID by predpokladám bola hodnota SK.

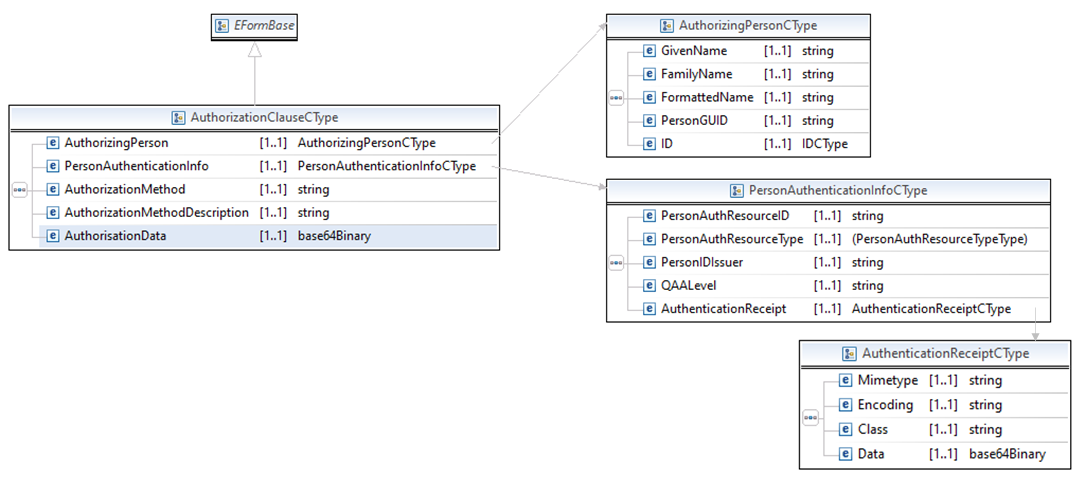
* + - * QAAlevel - eIDAS\_Level autentifikácie (3 = substantial alebo 4= high)
      * Authentication\_receipt - Vysledok autentifikacie (moze byt dodatocnej), ktora bola pouzita pred ukonom autorizacie. Napr. SAML alebo Oauth2 token vydany pristupovym miestom. Obsahuje „potvrdenku“ o vydani autentifikacnych informacii pri dodatocnej autentifikacii. Je to dokaz, ze bol dany pouzivatel autentifikovany, v pripade potreby overitelny (rucne, automatizovane – je              na pristupovom mieste). Moze to byt cislo transakcie pre dohladavanie v logoch mechanizmu pristupoveho miesta.
        + Mimetype, encoding, class, data
    - Popis autorizácie (Authorization\_method)
      * Hodnota z ciselnika pre sposob autorizacie klikom.

Š.Szilva:   
Na zváženie je použitie centrálneho číselníka pre spôsoby autorizácie klikom.

* + - * Description
      * Authorization\_method\_data - optional
    - Údaje zastupovanej osoby – optional (Delegation)
      * Meno, priezvisko, formátované meno
      * Identifikátor osoby, Issuer\_country, Typ identifikátora
        + Podla zakona to moze byt pri fyzickej osobe len rodne cislo alebo zahranicny identifikator.
      * SubjectGUID - Univerzalny identifikator identity v eGov
      * Identifikátor osoby, Issuer\_country, Typ identifikátora – RČ, IČO

Š.Szilva:   
Duplicita - údaje o zastupovanej osobe ste už uvádzali vyššie.

**Technická schéma:**



## Pripomienky od Juraja Hájeka v zastúpení Ardaco, a.s.

1. Samotnú autorizáciu klikom považujeme za nesystémový a v súčasnosti prekonaný prvok.

Š.Szilva: Ide o spôsob autorizácie definovaný v § 23 ods. 1 písm. a) bod 2 zákona č. 305/2013 Z. z. o e-Governmente od 1. novembra 2017. Cieľom aktuálneho návrhu je definovanie štandardu pre potvrdenie o vykonaní takejto autorizácie. Diskusiu o aktuálnosti tohto spôsobu autorizácie navrhujeme presunúť aj na pracovnú skupinu k NKIVS - Lepšie služby.

1. Za vhodnejšie považujeme riešenia založené na normách STN EN 41 9241-1  a STN EN 41 9241-2 (Dôveryhodné systémy podporujúce podpisovanie na strane servera).
2. Ak sa vrátime ku pôvodným zdôvodneniam, prečo sa téme autorizácie klikom venoval taký priestor, malo ísť napr. o *,,,de facto o jediné dnes v zákone upravené riešenie, ktoré je použiteľné na autorizáciu a zároveň je technologicky neutrálne v zmysle, že je na jeho vytvorenie možné použiť rôzne a viaceré postupy a nástroje a neodkazuje na konkrétne, resp. konkrétnym spôsobom štandardizované riešenie".* Tieto a podobné zdôvodnenia dnes neplatia. STN normy vyššie priamo adresujú potrebu autorizácie, sú technologicky neutrálne, v ničom postupy a nástroje neobmedzujú (s výnimkou bezpečnostných aspektov), sú  súlade s legislatívou a zároveň umožňujú autorizáciu (aj, nie však výlučne) až na stupeň kvalifikovaný. Zároveň nevyžadujú žiadny špeciálny HW na strane podpisovateľa (eID, smart karta, token).

Š.Szilva:

Vami uvedený návrh je z môjho pohľadu možné použiť pre autorizáciu podľa § 23 ods. 1 písm. a) bod 1 aj bod 2 zákona o e-Governmente t.j. pre autorizáciu kvalifikovaným elektronickým podpisom alebo pečaťou ako aj pre autorizáciu klikom.   
Autorizácia podľa § 23 ods. 1 písm. a) bod 2 zákona poskytuje možnosť využiť technicky jednoduchšie riešenie, v rámci zodpovednosti správcu príslušného prístupového miesta.

Dovolím si citovať z dôvodovej správy zákona č. 238/2017 Z. z. (novela zákona o e-Governmente) k autorizácii klikom:

*„Zmeny v ustanoveniach o autorizácii sú dvojakého charakteru. Hlavnou zmenou je možnosť autorizovať podanie („podpisovať“) aj s použitím funkcionality prístupového miesta, bez nutnosti využiť elektronický podpis. Ide o spôsob, ktorý sa dnes používa napríklad na potvrdzovanie prijatia správ v elektronickej schránke a rozširuje sa aj v osobitných konaniach ako alternatíva k „bežnému podpisovaniu“. Vzhľadom na to, že identita osoby je v danom prípade preukázaná prostredníctvom autentifikátora (dnes najmä občianskeho preukazu) a nie je sporná, je predpoklad, že takýto spôsob autorizácie sprístupní využívanie elektronických služieb aj pre osoby, ktoré z rôznych dôvodov nedisponujú elektronickým podpisom. Navyše, touto zmenou sa dosiahne aj to, že postačí aj občiansky preukaz s elektronickým čipom a osoba bude môcť cez ústredný portál verejnej správy využívať elektronické služby v plnom rozsahu, bez potreby obstarávania ďalších technických, či programových prostriedkov.“*

1. Ak vychádzame z predpokladu, že aj autorizácia konkrétneho úkonu bude vyžadovať nejaké dodatočné overenie, že ho skutočne robí daná osoba (t.j. nie, že sa používateľ niekam prihlási a počas platnej session útočník na zariadení autorizuje N dokumentov), tak tento spôsob nie je o nič menej komfortný ako autorizácia klikom.
2. V zmysle predošlých bodov pečatenie doložiek o autorizácii klikom podľa nášho názoru nie je vôbec potrebné. Nič nebráni tomu, aby podpisovateľ podpísal priamo požadovaný dokument a to vlastným kľúčom umiestneným v prostredí Trusted Service Provider (TSP). Mali by sme sa skôr zamerať na to, aby bolo vydanie takýchto kľúčov čo najjednoduchšie (napr. prístup TSP do registrov za konkrétnym účelom – overnie identity a pod).

Š.Szilva:

V prípade podpisovania na strane servera je možné využívať aj autorizáciu podľa § 23 ods. 1 písm. a) bod 1. V takom prípade nie je potrebné postupovať podľa bodu 2 a ani vyhotovovať doložku.

Témy dostupnosti údajov z registrov je vhodné riešiť na príslušných pracovných skupinách.

1. Za omnoho užitočnejšie a systémovejšie by sme považovali, ak by štát otvoril ekosystém pre autorizáciu. Tým myslíme, nech definuje komunikačný protokol, ktorý musí spĺňať aplikácia pre autorizáciu, aby ju mohlo vyvolať ľubovoľné prístupové miesto, napr. ÚPVS. Zvyšok je na TSP a výrobcoch aplikácií, aký komfort používateľovi poskytnú a z akých platforiem, vrátane mobilných.

Š.Szilva:

Vami uvedený návrh považujem za užitočný. Odporúčam predložiť návrh na posúdenie štandardu do pracovnej skupiny.

1. Náročnosť tejto zmeny je podľa názoru s vysokou pravdepodobnosťou porovnateľná resp. výrazne nižšia, ako meniť IS tak, aby vedeli generovať a spracovávať špecifické doložky, atď.
2. Návrh podobných ,,SK špecifických" postupov a štandardov nepovažujeme za dobrý krok.

K samotnému návrhu:

1. Konkrétny úkon je autorizovaný mechanizmami, ktoré podpisovateľ nemá pod svojou výlužnou kontrolou. Dôkazom, že ho autorizoval, má byť pečať iného subjektu. Je relevatné sa spýtať, akú istotu má občan, že prístupové miesto nevydá pečať aj na dokument, ktorý v skutočnosti neautorizoval.

Š. Szilva:

Ide o zodpovednosť príslušného správcu prístupového miesta.

Obdobným spôsobom je možné „autorizovať“ alebo potvrdzovať na to určenou funkciou ústredného portálu verejnej správy úkony definované v zákone (napr. § 16 ods. 6 alebo § 30 ods. 3 zákona) ako je napríklad udelenie oprávnenia na disponovanie s elektronickou schránkou, aktivácia schránky na doručovanie alebo potvrdenie doručenky.

1. Inak povedané, to, že sa podpisovateľ niekam prihlásil nejakým eIDAS stupňom autentifikácie a po jeho prihlásení prístupové miesto niečo podpísalo vlastnou pečaťou nerovná sa prejav jeho vôle.

Š.Szilva:

Kvalifikovaná pečať potvrdzuje, že správca prístupového miesta eviduje prejavenie vôle konkrétnej osoby. Napríklad autorizačný prostriedok používaný podľa § 16 ods. 6 zákona o e-Governmente používa vlastný spôsob, kedy v odoslanej správ uchováva SAML token osoby (podpis.xml)

1. Spojili sa dve dôveryhodné služby, ale spôsobom, ktorý sám o sebe dôveryhodný nie je. Takéto spojenie nie je (podľa našich vedomostí) predmetom žiadnej akreditácie. Vychádza sa zrejme z toho, že prístupové miesto je dôveryhodné. Vyvoláva to v nás ale otázku, kto a na základe akého štandardu takúto kombináciu služieb posúdi.

Š. Szilva:

V súčasnosti ide o kompetenciu a zodpovednosť správcu prístupového miesta.

1. Pre porovnanie, v STN EN 41 9241-1 a 2 je jasne uvedené, aký stupeň výlučnej kontroly môže mať podpisovateľ , za akých okolností, aké sú požiadavky na prostredie, mechanizmy, atď.
2. Súhlasíme s pripomienkami p. Friča k obsahu položiek. Z pohľadu prijímateľa/spracovateľa je jedno, či používateľ vykonal autorizáciu na mobile, akým spôsobom a detaily k tomu. Ak vznikne spor, tieto položky nebude ručne overovať prijímateľ. Tomu v zásade podľa návrhu postačuje, že tam bude nejaké ID operácie a pečať prístupového miesta. Ak sa pôjde v spore tak ďaleko, že sa spochybní tá, bude potrebné aj tak preverovať forézne záznamy na strane prístupového miesta a dôveryhodných služieb, ktoré využíva.

Š. Szilva:

Doložka môže obsahovať voliteľné údaje, do ktorých môže prístupové miesto priamo zapisovať napríklad dôkaz o vykonanej autorizácii, k čomu môže byť potrebné uvádzať aj súvisiace metaúdaje. Ide o možnosť pre niektoré technické riešenia, ktoré by takú funkčnosť zužitkovali (napr. vložený nekvalifikovaný elektronický podpis).

1. Podobne nerozumieme, odkiaľ sa zoberie informácia o zastupovaní.

Š. Szilva:

Informácia o zákonnom generálnom zastupovaní je údaj z registrov (napr. štatutár).

Myšlienka autorizácie klikom vznikla v čase, keď neexistovali uvedené normy a zároveň prebiehali diskusie o tom, či musí byť všetko autorizované KEP-om, ako adresovať požiadavky na podpisovacie zariadenia, čo s mobilnými platformami, atď.

Odvtedy sa štandardizácia a technológie výrazne posunuli.

## Pripomienky od Pavla Friča v zastúpení DITEC, a.s.

Podla mna je potrebne vychadzat z poziadaviek zakona a povodneho zameru a v tomto kontexte definovat minimalnu sadu udajov, ktore su potrebne pre vyhodnotenie takejto formy autorizacie pri dalsom spracovani podania. Podla mojho nazoru netreba do tejto struktury davat udaje, ktore overovatel aj tak nepouzije, resp. su mu zbytocne (aj ked mozno by sa niekedy v pripade sporu mohli zist). Ak treba zhromazdovat dokazne prostriedky, dajme tuto povinnost radsej prevadzkovatelovi pristupoveho miesta, ktory ma zodpovednost za preukazanie ze takato autorizacia bola pre dany dokument autorizujucoiu osobou vykonana (on potvrdzuje platnost udajov v autorizacnej dolozke). A kedze spracovatel podania doveruje prevadzkovatelovi pristupoveho miesta, nic viac nepotrebuje.

V tomto kontexte komentujem jednotlive polozky navrhu, ktore sa mi zdaju zbytocne a zbytocne tuto autorizacnu dolozku komplikuju.

* eIDAS uroven autorizacie – treba si uvedomit, ze v sucasnosti nase standardy definuju 4 urovne autentifikacie. Do standardu je potrebne doplnit prevodnu tabulku, nakolko mozu byt medody autentifikacie pouzivane na pristupovom mieste hodnotene urovnami z tychto standardov

Š.Szilva:

Súhlasím. Téma úrovní autentifikácie elektronických služieb a úrovní zabezpečenia podľa Nariadenia EP a Rady EÚ č. 910/2014 (eIDAS) je aj otvorených témach pracovných skupín.

* description – priznam sa ze nerozumiem co tym autor myslel „autorizacia klikom z mobilneho telefonu“. Toto je podla mna irelevantne, pouzivatel sa ma autorizovat na pozadovanej urovni a je uplne jedno, aky prostriedok zabezpecujuci minimalnu uroven pouzil. Druhou vecou je, ze niekde by malo byt povedane ze sa jedna o autorizacnu dolozku pre podpis klikom, aby vedel spracovatel toto automatizovane vyhocnotit, t.j. ze prave toto je autorizacia klikom

Š. Szilva:

Skutočnosť, že sa jedná o autorizačnú doložku, je možné zistiť z XML namespace elektronického formulára.

Je to napríklad možné riešiť tým spôsobom, že jednotný elektronický formulár pre autorizačnú doložku bude sprístupnený v module elektronických formulárov.

Description mal slúžiť aj na slovné vysvetlenie účelu doložky. Môže byť riešené aj ako súčasť prezentačnej schémy.

* delegation – opatovne nerozumiem ucelu. Opravnenie k zastupovaniu sa vacsinou priklada k podaniu ako samostatny doklad (ak napr. nevyplyva zo zakona) a netusim odkial by ho pristupove miesto ziskavalo a spracovalo, aby ho vedelo vlozit do tejto struktury (a teda za neho aj nieslo zodpovednost). Ak sa bavime o UPVS, tak tento eviduje iba opravnenie pristupu do schranky, co vsak rozhodne nie je opravnenie k uskutocnovaniu ukonov v mene vlastnika schranky

Š. Szilva:

V súvislosti s autorizáciou klikom je položka delegation cielená pre prípad, ak ide o úkon v mene inej osoby na základe zákonného zastupovania - generálne zastupovanie podľa všeobecne záväzného právneho predpisu (na ÚPVS ide o DelegationType = 0).

V zmysle § 23 ods. 1 písm. a) bod 2 platí povinnosť uvádzať ako odosielateľa osobu, ktorá vykonala autorizáciu. V prípade prihlásenia v zastúpení inej osoby je potrebné, aby správy bola odoslaná v mene identity uvedenej v SAML tokene v SubjectID, t.j. v mene zastupovanej identity.

Citát z prílohy č. 10 Vyhlášky č. 78/2020 Z. z. o štandardoch pre IT VS:

*„DelegationType“*

„*0 – generálne zastupovanie podľa všeobecne záväzného právneho predpisu, napríklad konateľ právnickej osoby, alebo súdom určený zástupca nesvojprávnej osoby,“*

Používateľské prostredie pre vykonanie autorizácie by malo používateľa informovať, v koho mene je autorizácia vykonávaná. V prípade prihlásenia v zastúpení inej osoby sa v používateľskom prostredí obvykle zobrazuje informácia, v koho mene je osoba prihlásená, čo by mohlo používateľa uviesť do omylu.

* authentication method – tu by som videl skor identifikaciu „identity providera, na koho sa obratit v pripade pripadneho riesenia sporov

Š. Szilva:

V princípe ide o tento účel. Môžeme diskutovať, aký najvhodnejší údaj zvoliť. Správca prístupového miesta bude identifikovateľný prostredníctvom pečate.

* authentication method receipt – opat pochybujem o zmysluplnom pouziti tohto udaja v autorizacnej dolozke. Toto nech uchovava prevadzkovatel pristupoveho miesta v logoch (definovany cas). Ale v autorizacnej dolozke toto nema zmysel. To tam mozeme pridat aj fotku podpisovatela 😊

Š. Szilva:

Obdobne ako sú v prípade archívnej formy podpisov uchovávané „dôkazy“, obdobne môžu byť pre niektoré systémy užitočné nepovinne uchovávané konkrétne dôkazy o vykonaní autorizácie klikom. Nepovažujem za potrebné tomu brániť.

Pokiaľ však budú zásadné výhrady, je možné vypustiť.

* authorisation method data – opat nie celkom chapem zmysel. Ak niekto podpisuje na mobile (a je to zakonom uznany podpis), tak nemusi robit autorizaciu klikom. A podpis ktory nema ziadnu pravnu vahu je uplny nezmysel davat do autorizacnej dolozky. Nevyhodnocuje sa a nic neriesi. Ma sa pri autorizacii klikom autentifikovat, nie podpisovat dokument na mobile.

Š. Szilva:

Autorizácia klikom nevylučuje použitie ľubovoľnej formy elektronického podpisu pre dosiahnutie účelu (napr. zachovanie nezmenenosti dokumentu). Pokiaľ daná technológia prístupového miesta takúto funkciu potrebuje a chce uchovávať údaje v autorizačnej doložke (napríklad pre svoje vlastné potreby pri overovaní), nepovažujem to za problém.

Takze ked to zhrniem, postacujuce su nasledujuce polozky

* udaj ze sa jedna o autorizacnu dolozku pre podpis klikom
* identifikacia osoby vykonavajucej autorizaciu
* identifikacia sposobu autentifikacie (identity providera, napr eID, eIDAS schema, mID atd)
* uroven pouzitej autentifikacie
* a mozno zvazit cas vykonania autentifikacie

Niekolko dalsich poznamok

* boli diskusie ze postaci prvotna autentifikacia pouzivatela (pri pristupe k pristupovemu miestu) a nasledne pri autorizacii klikom autentifikacia nie je potrebna. Toto povazujem za dost nebezpecne, nakolko potom na pristupovom mieste moze pouzivatel autorizovat aj „omylom“, bez toho ze by to explicitne vedel potvrdil. Toto moze mat rozne dopady (nechcem pisat ze potom je mozne autorizovat aj bez vole pouzivatela a nie je to cim preukazat – aspon autorizacny token bude pristupove miesto mat)

Š.Szilva:

Podľa zákona je podmienkou úspešná autentifikácia. Požiadavka na opakovanú autentifikáciu by mala byť predmetom diskusie pracovnej skupiny.

* povinnost prijimat takuto autorizaciu – ta je zo zakona pre vsetkych, nerozumiem textu v dovodovej sprave (ak pristupove miesto poskytuje). Nie je to podla mna ani na rozhodnuti organu, iba ze by organ vo vlastnej legislative (myslim v zakone !!! pre danu agendu) takyto sposob autorizacie vylucil

Š.Szilva:

Podmienkou je, že bude takúto autorizáciu poskytovať prístupové miesto.

Nič však nebráni tomu, aby prístupové miesto konfiguračne umožnilo autorizáciu klikom len pre vybrané elektronické služby.

* k diskutovanym alternativam v zdovodneni sa nevyjadrujem, su podla mna mimo ucelu takehoto sposobu autorizacie jeho spracovania

Pozrel som … Ale o tom, ako by to malo fungovat sa stale len dohadujem, ale skusim:

1. pouzivatel sa autentifikuje na portali OVM, alebo na slovensko.sk – proste pristupovom mieste napr pomocou elektronckeho obcianskeho a autentifikacneho certifikatu vydaneho SVK eID PCA (musi zadat BOK)
2. . vyhlada si sluzbu – povedzme, ze ta sluzba nevyzaduje autorizaciu KEPom, ale "autorizaciu klikom"
3. vyplni prislusny elektronicky formular sluzby a "klikne" na podpisat
4. vtedy system moze vyziadat dodatocnu autentifikaciu pouzivatela (teda znovu zada BOK, pozn. k Authorization\_method\_data – Výstupom niektorých autent. metód môže byť uistenie, že pokyn k úkonu podpisu klikom (a dodatočnej autentifikácii) vznikol práve k danému dokumentu a na zariadení, ktoré má priamo pod kontrolou občan) – mimochodom, nema tam byt Autehnitication\_method\_data?

Š.S.

Nie, tento element mal slúžiť pre voliteľné údaje prístupového miesta, ktoré by potrebovalo ukladať ako dôkazový materiál o vykonanej autorizácii (napr. nejaká forma podpisu).

1. alebo system pouzije existujuci Authentication\_method\_receipt („výsledok“ autentifikácie (môže byť dodatočnej), ktorá bola použitá pred úkonom – napr. SAML alebo Oauth2 token vydaný prístupovým miestom)

Š. Szilva:

V tomto elemente sa predpokladalo ukladanie dôkazu o dodatočnej autentifikácii (SAML/JWT) resp. o vyžiadanej autentifikácii pre naplnenie účelu tohto ustanovenia.

1. system automatizovane vytvori Autorizačnú doložku potvrdzujúcu autorizáciu klikom
   * pozn. k obsahu autorizacnej dolozky: v sucasnosti certifikat pre autentifikaciu na slovensko.sk, ktory vydava SVK eID PCA, neobsahuje: Meno, priezvisko, **Identifikátor osoby**, Issuer\_country,**Typ identifikátora (dnes: zásadne len SK (PAS, IDC, PNO, NTR, PSD, atd)**)

Š.S.:

Požadované údaje je možné získať na základe úspešnej autentifikácie, nie je potrebný certifikát PCA.

* + Priklad: SERIALNUMBER = 00000000000000457603, CN = Róbert Vittek, C = SK, L = Senec
  + uvedeny identifikator obsahuje az QC vydany SVK eID ACA, pristup ku ktoremu je ale chraneny PINom
  + alebo uvedeny identifikator osoby bude obsahovat Authentication\_method\_receipt?

Š.S. :

Áno, očakáva sa, že by mal byť v tokene potvrdzujúcom úspešnú autentifikáciu na úrovni pokročilá alebo vysoká. Údaje je však možné získať aj volaním príslušných webových služieb IAM UPVS.

1. system zapecati spolocne elektronicky formular vyplneny pouzivatelom a autorizacnu dolozku KEPe – teda kvalifikovanou el. pecatou pristupoveho miesta

Pochopil som to spravne?

Š.S.:

Áno.

------

Dalsie poznamky:

- v strukture autorizacnej dolozky som nenasiel: väzbu na autorizovaný dokument vo forme digitálneho odtlačku, resp. to je to uplne dole AuthorizationFile, co sa javi byt sucast nepovinneho Authorization\_method\_data?

Š.S:

Ide o voliteľný element na diskusiu, pre účely možnosti prenášať v samostatných objektoch doložku a podanie.

@ je ich možné overiť v bežných podateľniach, rozdiel je v tom, že údaje o autorizujúcej osobe klikom sú v doložke a nie v pečati, ktorou iba prístupové miesto potvrdzuje úspešný a plnohodnotný úkon autorizácie klikom.

- cize podatelna musi vediet identifikovat podpisovatela z autorizacnej dolozky

Š.S.:

Podateľňa alebo iný system spracúvajúci prijímané podania a identifikujúci autorizujúcu osobu.

@ umožniť vytvorenie (aj) centrálnej funkcie autorizácie klikom využiteľnú pre rôzne elektronické služby, ktorých gestori sa rozhodnú takúto možnosť autorizácie povoliť.

- je uz predstava, ktoreho modulu to bude centralna funkcia?

Š.S.: Nie je.

@ ak ma byt cielom:

- umožniť jednotný spôsob preukazovania a automatizovaného vyhodnocovania vykonanej autorizácie klikom v rôznych systémoch,

- umožniť jednotné zobrazenie informácií o vykonanej autorizácii v elektronickej schránke používateľa,

..tak by tam nemali byt vagne specifikovane veci, ako napr: dôkaz, že bol daný používateľ autentifikovaný a je vydaný pre neho. Kľudne môže byť číslo transakcie pre dohľadávanie v logoch mechanizmu prístupového miesta

## Pripomienky od Martina Blaška v zastúpení Globaltel a.s.

Účelom návrhu je definovať štandard, ktorý umožní jednotným spôsobom preukazovať vykonanú autorizáciu klikom.

Navrhovaný štandard umožňuje vykonať autorizáciu klikom použitím rôznych technických postupov, pričom výsledkom je štandardizovaná doložka potvrdzujúca tento úkon, autorizovaná kvalifikovanou elektronickou pečaťou prístupového miesta spoločne s podaním. Návrh aktuálne počíta s tým, že sa bude doložka odosielať súčasne s podaním.

Cieľom štandardu je:

* + - umožniť jednotný spôsob preukazovania a automatizovaného vyhodnocovania vykonanej autorizácie klikom v rôznych systémoch,
    - umožniť jednotné zobrazenie informácií o vykonanej autorizácii v elektronickej schránke používateľa,
    - umožniť vytvorenie (aj) centrálnej funkcie autorizácie klikom využiteľnú pre rôzne elektronické služby, ktorých gestori sa rozhodnú takúto možnosť autorizácie povoliť,
    - technologická neutralita - t.j. umožniť vykonanie autorizácie klikom použitím rôznych technických prostriedkov (eID, mobileID, rôznorodé špecifické portálové riešenia).

Základné požiadavky:

* + - vykonanú autorizáciu klikom preukazuje doložka o vykonanej autorizácii,
    - doložka má charakter štandardného elektronického formulára, ktorý je vypĺňaný a autorizovaný automaticky systémom prístupového miesta,
    - doložka obsahuje identifikačné údaje o osobe, ktorá autorizáciu klikom vykonala, väzbu na autorizovaný dokument vo forme jeho digitálneho odtlačku, údaje o autentifikácii minimálne na úrovni pokročilá, informáciu o vykonanej autorizácii, nepovinné údaje o ďalšom použitom prostriedku ak ich dané špecifické riešenie potrebuje (napríklad zdokonalený podpis a podobne),
    - doložka spolu s vyplnenými údajmi podľa elektronického formulára podania sú zapečatené kvalifikovanou elektronickou pečaťou prístupového miesta,

Ďalšie možnosti využitia:

* + - návrh potenciálne umožňuje:
      * + autorizáciu jedného dokumentu aj viacerými osobami pripojením viacerých doložiek,
        + autorizáciu v zastúpení inej osoby (predvolene len so zákonným zastupovaním, k riešeniu splnomocnení by bolo potrebné doriešiť koncept zastupovaní na ÚPVS),

Dopady na existujúce systémy:

* + - keďže pri tomto riešení vzniká podpisový ASiC kontajner v súlade so štandardmi podľa eIDAS a Vyhlášky o štandardoch, je možné jeho platnosť overiť v elektronických podateľniach, rozdiel je v tom, že údaje o autorizujúcej osobe klikom sú uvedené v doložke a nie v pečati, ktorou iba prístupové miesto potvrdzuje úspešný a plnohodnotný úkon autorizácie klikom,
    - systémy, ktoré potrebujú automatizovane spracúvať prijaté potvrdenie o autorizácii klikom vytvorené prístupovým miestom (napr. z UPVS), musia počítať s prijímaním doložky,
    - systémy musia počítať so spoločne autorizovanými dvoma dokumentami v jednom kontajneri v prijímanom podaní (v class=FORM): doložka a elektronické podanie.

Autorizáciu klikom má orgán verejnej moci povinnosť akceptovať len v prípade, ak prístupové miesto pre elektronickú službu umožňujúcu elektronické podanie danému orgánu poskytuje takúto možnosť autorizácie. Môže sa používať pre všetky elektronické podania (t.j. údaje vyplnené podľa elektronického formulára), pri ktorých sa nevyžaduje úradne overený podpis.

Zákon o e-Governmente neupravuje požiadavky na autorizáciu príloh elektronických podaní. Požiadavky na autorizáciu príloh elektronických podaní upravujú osobitné predpisy. Akceptovanie autorizácie klikom na prílohách je teda na rozhodnutí orgánu verejnej moci, ak osobitné predpisy nestanovujú konkrétnu požiadavku na spôsob autorizácie.

 Alternatívy zvažované pred výberom riešenia:

* + - Zapisovanie digitálneho odtlačku autorizovaného dokumentu v autentifikačnom tokene podpísanom v IAM, pričom takýto token by sa prikladal ako príloha podania (rovnako ako dnes na ÚPVS pri použití autorizačnej funkcie UPVS - t.j. opakovanej autentifikácie)
    - Alternatíva by si vyžadovala pripravenosť spracúvať tokeny z prílohy podania v rôznych systémoch, t.j. overovať ich platnosť, zahrnutý digitálny odtlačok dokumentu a parsovať z tokenov dáta.
    - Pre čitateľnú vizualizáciu takéhoto potvrdenia by bolo potrebné vytvorenie XSLT transformácie, ktorá by však nemohla byť zaregistrovaná ako elektronický formulár v MEF.

**Autorizačná doložka potvrdzujúca autorizáciu klikom ÚPVS (XML súbor) - má podobu elektronického formulára s položkami:**

* Meno, priezvisko, Identifikátor osoby, Issuer\_country, Typ identifikátora (zvážiť len SK – z IAM/RFO vs z certifikátu PAS, IDC, PNO, NTR, PSD, atd)),
* eIDAS\_Level autentifikácie (substantial alebo high)
* Description (ľudsky čitateľný popis použitej metódy autorizácie – napr.: autorizácia klikom pomocou mobilného telefónu - Autorizácia podľa § 23 ods. 1 písm. a) bod 2 zákona č. 305/2013 Z.z.).
* Delegation (údaje o zastupovaní) – DelegationType (typ zastupovania), ActorId (zastupujúca osoba)
* Authentication\_method (metóda autentifikácie, ktorá bola použitá pred úkonom)
* Authentication\_method\_receipt („výsledok“ autentifikácie (môže byť dodatočnej), ktorá bola použitá pred úkonom – napr. SAML alebo Oauth2 token vydaný prístupovým miestom)
  + Obsahuje „potvrdenku“ o vydaní autentifikačných informácií pri autentifikácaii. Nebude sa automatizovane overovať pri overovaní platnosti autorizácie klikom, pretože sa vychádza z toho, že pečať je dostatočná garancia.
  + Je to dôkaz, že bol daný používateľ autentifikovaný a je vydaný pre neho. Kľudne môže byť číslo transakcie pre dohľadávanie v logoch mechanizmu prístupového miesta
  + Dôkaz v prípade potreby overiteľný (ručne, automatizovane – je na prístupovom mieste). V zásade je to base64 encoded string rozumnej dĺžky.
* Authorization\_method\_data: (NEPOVINNÉ). Výstupom niektorých autentifikačných metód môže byť uistenie, že pokyn k úkonu autorizácie klikom (a dodatočnej autentifikácii) vznikol práve k danému dokumentu a na zariadení, ktoré má priamo pod kontrolou občan (čo v prípade autorizácie klikom, kde sa občan musí spoľahnúť na bezchybnú implementáciu prístupového miesta, má dodatočnú mieru uistenia).
  + Tieto údaje nevaliduje prístupové miesto, ani agendové systémy, slúžia na prípadnú dodatočnú, ručnú kontrolu.
  + Napríklad pre autorizáciu pomocou mobilného telefónu slúži pre dodatočnú kontrolu, či pri „autorizácii klikom“ participovalo aj zariadenie, ktoré má občan pod kontrolou (mobilný telefón).:
  + Návrh: mať jeden element, v ktorom môže byť nepovinne umiestnený súbor s dôkazom. Aká bude štruktúra daného súboru a či bude obsahovať vnorené elementy nechávame na jednotlivé implementácie. Celé ako kódovanie base64, čiže ak tam chcú mať viacero elementov, môžu si na to spraviť štruktúru. Napr.:
  + <AuthorizationFile Class="mobileIDSignature-XAdES" MimeType="application/xml" Encoding="http://www.w3.org/2000/09/xmldsig#base64"> PHh6ZXA6RGF0YUVudmVsb3BlIHhtbG5zOnh6ZXA9Imh.................</AuthorizationFile>
    - Digest\_method, digest value, document name
    - Podpis použitý pre digest\_value (typ, mimetype, encoding)

## Pripomienky od Ľubora Illeka v zastúpení Spoločnosť pre otvorené informačné technológie

Žiadam o rozdelenie materiálu k "autorizácii klikom" na metodický materiál a záväzný štandard, a následne zopakovať ich pripomienkovanie - v súčasnej podobe nie je presne jasné, čo a v akých situáciách má byť pre koho povinné. Zároveň až takto bude možné rozlíšiť, ktoré časti materiálu sú iba úvaha predkladateľa, ktoré majú byť odporúčané, a ktoré záväzné.

Zároveň žiadam, aby k tejto téme bolo vykonané štandardné stretnutie pracovnej skupiny (prípadne vzhľadom na epidemiologické opatrenia online formou), kde bude možné tento návrh diskutovať, a to najmä s jeho tvoracmi. Rovnako žiadam, aby tento návrh bol prerokovaný v PS Lepšie služby.

Z materiálu žiadam vypustiť odsek: "Autorizáciu klikom má orgán verejnej moci povinnosť akceptovať len v prípade, ak prístupové miesto pre elektronickú službu umožňujúcu elektronické podanie danému orgánu poskytuje takúto možnosť autorizácie. Môže sa používať pre všetky elektronické podania (t.j. údaje vyplnené podľa elektronického formulára), pri ktorých sa nevyžaduje úradne overený podpis." Toto je riešené jednoznačne v zákone.

Žiadam, aby vytvorenie autorizačnej doložky podľa uvedeného návrhu bolo povinne vyžadované iba v prípade, ak z povahy súvisiaceho úkonu je zrejmé, že autorizované podanie sa má prenášať medzi viacerými OVM. Podstatným zmyslom zavedenia možnosti realizovať autorizáciu klikom totiž bolo zníženie technických požiadaviek na jeho realizáciu, a taktiež zlepšenie používateľskej prívetivosti pri výkone autorizácie. Vytvárať navrhnutú autorizačnú doložku však nie je jednoduché, opäť tým vznikne problém najmä pre "malé" OVM alebo agendy. Zároveň za povšimnutie stojí, že doteraz vytváranie takejto doložky nebolo vyžadované nikde - a nikomu nechýbala. Rovnako v súčasnosti už existujú ISVS, v rámci ktorých je autorizácia kliknutím používaná a zavedenie autorizačnej doložky by bolo neúmerne nákladné. Ako príklad je možné uviesť napr. žiadosti podávané v rámci aplikácie Elektronický súdny spis (ktoré v žiadnom prípade nie sú banálne - realizuje sa nimi výkon niektorých závažných práv v rámci súdnych konaní), pri ktorých je používaná autorizácia kliknutím a do schránky je doručovaná informácia o samotnom podaní vo vizuálne vhodnej forme.  
V prípadoch, kedy podľa predošlého bodu nemá byť potrebné vytváranie autorizačnej doložky, žiadam štandardom určiť jednoduchý zoznam položiek, ktoré má obsahovať dokument dokladujúci vykonanie autorizácie klikom ukladaný do elektronickej schránky.  
  
Žiadam ako súčasť ďalšieho posudzovania priložiť aj vizuálnu podobu autorizačnej doložky. Jedným z cieľom autorizácie klikom je totiž podstatne zvýšiť  používateľskú prívetivosť služieb eGov, doložka podľa predloženého návrhu však vzbudzuje pochybnosti, či tento cieľ dosiahne.  
  
K predloženej štruktúre autorizačnej doložky uvedenej v dokumente "AutorizaciaKlikomNavrhStandardu\_pripomienkovanie.pptx": pred možnosťou finálneho pripomienkovania žiadam detailnejšie vysvetliť uvedené skratky, a koncepty. Zároveň žiadam vypustiť všetky parametre, ktoré sú zbytočné pre používateľa a neslúžia na preukázanie vykonanej autorizácie, t.j. najmä parametre Delegation, Authentication\_method, Authentication\_method\_receipt, Authorization\_method\_data.  
  
V rámci navrhovaného štandardu žiadam určiť ktoré údaje má prevádzkovateľ prístupového miesta v súvislosti s vykonávanou autorizáciou kliknutím vytvárať a uchovávať vo forme záznamov (logy). Tu je priestor pre uvedenie položiek, ktoré žiadam vypustiť v predchádzajúcom bode.

## Pripomienky od Michala Kevického v zastúpení za Národná agentúra pre sieťové a elektronické služby

**Návrh štruktúry pre potvrdenie autorizácie vykonanej podľa § 23 ods. 1 písm. a) bod 2**

**(tzv. "autorizácia klikom")**

Účelom návrhu je definovať štandard, ktorý umožní jednotným spôsobom preukazovať vykonanú autorizáciu klikom.

Navrhovaný štandard umožňuje vykonať autorizáciu klikom použitím rôznych technických postupov, pričom výsledkom je štandardizovaná doložka potvrdzujúca tento úkon, autorizovaná kvalifikovanou elektronickou pečaťou prístupového miesta spoločne s podaním. Návrh aktuálne počíta s tým, že sa bude doložka odosielať súčasne s podaním.

Cieľom štandardu je:

- umožniť jednotný spôsob preukazovania a automatizovaného vyhodnocovania vykonanej autorizácie klikom v rôznych systémoch,

- umožniť jednotné zobrazenie informácií o vykonanej autorizácii v elektronickej schránke používateľa,

- umožniť vytvorenie (aj) centrálnej funkcie autorizácie klikom využiteľnú pre rôzne elektronické služby, ktorých gestori sa rozhodnú takúto možnosť autorizácie povoliť,

- technologická neutralita - t.j. umožniť vykonanie autorizácie klikom použitím rôznych technických prostriedkov (eID, mobileID, rôznorodé špecifické portálové riešenia).

Základné požiadavky:

- vykonanú autorizáciu klikom preukazuje doložka o vykonanej autorizácii,

- doložka má charakter štandardného elektronického formulára, ktorý je vypĺňaný a autorizovaný automaticky systémom prístupového miesta,

- doložka obsahuje identifikačné údaje o osobe, ktorá autorizáciu klikom vykonala, väzbu na autorizovaný dokument vo forme jeho digitálneho odtlačku, údaje o autentifikácii minimálne na úrovni pokročilá, informáciu o vykonanej autorizácii, nepovinné údaje o ďalšom použitom prostriedku ak ich dané špecifické riešenie potrebuje (napríklad zdokonalený podpis a podobne),

- doložka spolu s vyplnenými údajmi podľa elektronického formulára podania sú zapečatené kvalifikovanou elektronickou pečaťou prístupového miesta,

Ďalšie možnosti využitia:

návrh potenciálne umožňuje:

- autorizáciu jedného dokumentu aj viacerými osobami pripojením viacerých doložiek,

- autorizáciu v zastúpení inej osoby (predvolene len so zákonným zastupovaním, k riešeniu splnomocnení by bolo potrebné doriešiť koncept zastupovaní na ÚPVS),

Dopady na existujúce systémy:

- keďže pri tomto riešení vzniká podpisový ASiC kontajner v súlade so štandardmi podľa eIDAS a Vyhlášky o štandardoch, je možné jeho platnosť overiť v elektronických podateľniach, rozdiel je v tom, že údaje o autorizujúcej osobe klikom sú uvedené v doložke a nie v pečati, ktorou iba prístupové miesto potvrdzuje úspešný a plnohodnotný úkon autorizácie klikom,

- systémy, ktoré potrebujú automatizovane spracúvať prijaté potvrdenie o autorizácii klikom vytvorené prístupovým miestom (napr. z UPVS), musia počítať s prijímaním doložky,

- systémy musia počítať so spoločne autorizovanými dvoma dokumentami v jednom kontajneri v prijímanom podaní (v class=FORM): doložka a elektronické podanie.

Autorizáciu klikom má orgán verejnej moci povinnosť akceptovať len v prípade, ak prístupové miesto pre elektronickú službu umožňujúcu elektronické podanie danému orgánu poskytuje takúto možnosť autorizácie. Môže sa používať pre všetky elektronické podania (t.j. údaje vyplnené podľa elektronického formulára), pri ktorých sa nevyžaduje úradne overený podpis.

Zákon o e-Governmente neupravuje požiadavky na autorizáciu príloh elektronických podaní. Požiadavky na autorizáciu príloh elektronických podaní upravujú osobitné predpisy. Akceptovanie autorizácie klikom na prílohách je teda na rozhodnutí orgánu verejnej moci, ak osobitné predpisy nestanovujú konkrétnu požiadavku na spôsob autorizácie.

Alternatívy zvažované pred výberom riešenia:

- Zapisovanie digitálneho odtlačku autorizovaného dokumentu v autentifikačnom tokene podpísanom v IAM, pričom takýto token by sa prikladal ako príloha podania (rovnako ako dnes na ÚPVS pri použití autorizačnej funkcie UPVS - t.j. opakovanej autentifikácie)

- Alternatíva by si vyžadovala pripravenosť spracúvať tokeny z prílohy podania v rôznych systémoch, t.j. overovať ich platnosť, zahrnutý digitálny odtlačok dokumentu a parsovať z tokenov dáta.

- Pre čitateľnú vizualizáciu takéhoto potvrdenia by bolo potrebné vytvorenie XSLT transformácie, ktorá by však nemohla byť zaregistrovaná ako elektronický formulár v MEF.

## Pripomienky od Emila Fitoša v zastúpení za IT Asociáciu Slovenska

Uvedený spôsob autorizácie je v legislatíve už dlhšiu dobu a MIRRI až teraz predkladá návrh na štandardizáciu štruktúry vyjadrujúcej tento spôsob autorizácie. ITAS po internej diskusii zasiela pripomienky k tomuto návrhu.

### Princíp „Autorizácie klikom“

ITAS chápe, že účelom „podpisu klikom“ je zjednodušenie procesu autorizácie pre používateľov. Takéto zjednodušenie však nemôže byť vykonané na úkor výrazného zníženia úrovne bezpečnostných záruk pre takýto spôsob autorizácie. Z týchto dôvodov je vhodné pri implementácii tohto bezpečnostného mechanizmu zohľadniť nasledujúce skutočnosti:

* Súčasná legislatíva explicitne nepredpisuje, či sa autentifikácia používateľa má vykonať v procese autorizácie, alebo pri autentifikácii používateľa pri prvotnom prístupe k prístupovému miestu/službe. Absenciu viacfaktorového potvrdenia procesu autorizácie považujeme za vysoké bezpečnostné riziko, kde pôvodný autentifikačný token pri prístupe k prístupovému miestu je používaný na akúkoľvek autorizáciu úkonu Požadujeme proces autorizácie explicitne viazať na opätovnú autentifikáciu (pri každej autorizácii samostatne).
* Návrh dátovej štruktúry autorizačnej doložky pre „podpis klikom“ nerieši základný deficitný aspekt, kedy celý mechanizmus závisí od bezpečnej a korektnej implementácie. Kvalifikovaná elektronická pečať prístupového miesta použitá na autorizáciu doložky túto nedokonalosť neadresuje. Dokazovanie by muselo vychádzať z overovania logov a overovania implementácie v rámci systému konkrétneho prístupového miesta (a ani nie je určené na koho strane bude dôkazné bremeno v prípade sporu spočívať). Preto je dôležité v návrhu štandardu neriešiť iba návrh dátovej štruktúry, ale taktiež definovať ktoré udaje z procesu autentifikácie a autorizácie je prevádzkovateľ prístupového miesta povinný uchovávať a preukazovať v prípade sporu o autorizácii. Domnievame sa, že dôkazné bremeno v prípade sporu nemá byť na používateľovi (vykonávajúcou autorizáciu, ktorá nie je plne pod jeho kontrolou), ale práve na prevádzkovateľovi prístupového miesta
* Najmä v kontexte existujúceho právneho ukotvenia „podpisu klikom“ považujeme za nevyhnutný predpoklad dôvery v technologicky neutrálne spôsoby autentifikačných schém aspoň na úrovni bezpečnostných záruk „Pokročilá“, ktorá má predchádzať autorizácii klikom, vytvorenie národného jednotného rámca posudzovania bezpečnostných záruk autentifikačných schém a určenie kvalifikovaného a kompetentného úradu alebo orgánu pre túto špecifickú oblasť. Zhoda každej autentifikačnej schémy s požiadavkami plynúcimi z rámca na úrovne „Pokročilá“ a „Vysoká“ musí byť nezávisle posúdená týmto orgánom alebo úradom ešte pred jeho sprístupnením pre autorizáciu klikom (špeciálne pre centralizované sprístupnenie autorizácie klikom aj na UPVS), ak autentifikačná schéma už nebola potvrdená na príslušnej úrovni bezpečnostných záruk v rámci plnohodnotného notifikačného procesu pre cezhraničné uznávanie podľa nariadenia eIDAS.
* V rámci kompetencií kvalifikovaného orgánu alebo úradu by tento mal ešte pred uvedením do používania funkcie prístupového miesta pre „autorizáciu klikom“ povinne overiť bezpečnú a korektnú implementáciu v rámci daného prístupového miesta a súlad so zákonnými normami alebo vtedy definovanými štandardami, vrátane diskutovaného návrhu.
* Súčasná legislatíva umožňuje každému používateľovi využívať pre akúkoľvek službu vyžadujúci v listinnej forme autorizáciu vlastnoručným podpisom autorizáciu „podpisom klikom“.. Preto legislatívne nie je možné na úrovni prístupového miesta obmedzovať použitie „podpisu klikom“ pre vybranú množinu služieb a poskytovateľ služby nemá možnosť takúto autorizáciu odmietnuť, nakoľko legislatíva nedáva možnosť prihliadať na povahu daného typu podania. Z tohto dôvodu považujeme zosúladiť text návrhu s platným legislatívnym stavom, ktorý obmedzenia použitia „podpisu klikom“ vylučuje.
* Na druhej strane, najmä v kontexte poskytovaných bezpečnostných záruk“ si uvedomujeme možné riziká použitia takéhoto spôsobu autorizácie pre vybrané služby. Z tohto dôvodu považujeme za prioritu otvoriť diskusiu o zmene prístupu k autorizácii v elektronickom prostredí.

K vlastnému zdôvodneniu predkladaného návrhu pripájame nasledujúce poznámky:

* V návrhu sa spomína, že vykonanie „autorizácie klikom“ sa má realizovať použitím rôznych technických prostriedkov (eID, mobileID, rôznorodé špecifické portálové riešenia). Jednak toto nie sú technické prostriedky, zámer autora bol asi vymenovať autentifikačné prostriedky. Tu je potom však potrebné uvádzať všetky zákonné spôsoby autentifikácie použiteľné pri výkone elektronickej moci elektronicky. MobileID je len názov projektu a nie spôsob autentifikácie, tento pojem nie je vhodné uvádzať. V zásade sú to:
  + Autentifikácia úradným autentifikátorom
  + Autentifikácia alternatívnym autentifikátorom
  + Autentifikácia autentifikačným certifikátom
  + Prostriedok eIDAS
* „Základné požiadavky“ uvádzané v dokumente nie sú vo svojej podstate požiadavky ale skôr pre/dstavujú návrh riešenia ako naplniť ustanovenia z legislatívy. Navrhujeme zmeniť názov na „Návrh riešenia“, resp. bolo by vhodné prehodnotiť štruktúru dokumentu
* V dopadoch na existujúce systémy absentuje potreba rozšírenia služieb centrálnej el. podateľne (CEP). OVM v súčasnosti spracovávajú výsledok overenia platnosti autorizácie, ktorý im poskytuje CEP a ktorý v súčasnosti neposkytne informáciu o údajoch z autorizačnej doložky. Toto platí aj pre fyzické osoby a právnické osoby, ktoré v elektronickej schránke informatívne overujú platnosť autorizácie volaním služieb CEP
* V dopadoch chýba nasledovný dopad: Prístupové miesta musia byť schopné vykonať autorizáciu klikom v zmysle tohto návrhu. To znamená naplniť doložku predpísaným spôsobom a spoločne je autorizovať pečaťou prístupového miesta. Pričom toto musia realizovať dôveryhodným, aj spätne preukázateľným spôsobom pre prípad sporu. Za týmto účelom musia uchovávať informácie o vykonanej autorizácii (v púredpísanom rozsahu).

### Pripomienky k navrhovanej štruktúre

Pri návrhu štandardu na reprezentáciu „autorizácie klikom“ doporučujeme vychádzať z pôvodného legislatívneho zámeru a zo zásady uvedenie minimálnych požiadaviek, ktoré sú potrebné pre vyhodnotenie autorizácie prijímajúcou osobou. Prebvádzkovateľ prístupového miesta, ako dôveryhodná osoba, garantuje vykonanie autorizácie dokumentu uvedenou osobou. A toto potvrdí zapečatením autorizovaného dokumentu a „autorizačnej doložky“. Všetky ďalšie údaje, ktoré by mohli byť použiteľné v prípade sporu uchováva prevádzkovateľ prístupového miesta (a nie je potrebné ich nezmyselne vkladať do „autorizačnej doložky“.

V tomto kontexte v „autorizačnej doložke“ postačuje uvedenie nasledujúcich údajov:

* Že sa jedná o „autorizáciu klikom“
* identifikácia osoby vykonávajúcej autorizáciu, t.j. osoby ktorá sa pri autorizácii autentifikovala, resp. identifikátor osoby v mene ktorej sa osoba autentifikovala. Tento identifikátor je potrebný pre naplnenie nasledovnej legislatívnej požiadavky:
  + „(prístupové miesto) zabezpečí uvedenie tejto osoby ako odosielateľa elektronickej správy“ a „spojenie autorizovaného dokumentu s identifikátorom osoby odosielateľa„. V prípade odoslania podania z PO schránky je totiž odosielateľom správy PO, osobou ktorá sa v skutočnosti autentifikovala je FO, typicky štatutár.
* potvrdenie o tom, že daná osoba sa autentifikovala a uvedenie úrovne autentifikácie (údaje o vlastnom procese autentifikácie nie je portrebné uvádzať, postačí ak ich uchováva prevádzkovateľ prístupového miesta),
* čas vykonania autorizácie.

Komentáre k navrhovaným údajom v autorizačnej doložke pripájame:

* Znenie „Autorizačná doložka potvrdzujúca autorizáciu klikom ÚPVS (XML súbor) - má podobu elektronického formulára s položkami“ upraviť tak, aby bolo zrejmé, že sa má použiť jeden spoločný formulár na tento účel registrovaný v MEF a že každé prístupové miesto nemá registrovať vlastný formulár
* **Meno, priezvisko, identifikátor osoby** – je potrebné doplniť, že sa jedná o osobu, ktorá sa úspešne autentifikovala v procese „autorizácie klikom“. Teda sa jedná vždy o fyzickú osobu.
  + Okrem tohto je potrebné uviesť aj identifikátor osoby v mene ktorej sa autentifikovala (t.j. napríklad Právnická osoba). Tento identifikátor je potrebné pre naplnenie nasledovnej náležitosti: „(prístupové miesto) zabezpečí uvedenie tejto osoby ako odosielateľa elektronickej správy“ a „spojenie autorizovaného dokumentu s identifikátorom osoby odosielateľa„. V prípade odoslania podania z PO schránky alebo podaním v mene PO je totiž odosielateľom správy PO, osobou ktorá sa v skutočnosti autentifikovala je FO, typicky štatutár.
  + Znenie „Typ identifikátora (zvážiť len SK – z IAM/RFO vs z certifikátu PAS, IDC, PNO, NTR, PSD, atd)“ navrhujeme vypustiť, nakoľko toto nie sú identifikátory v zmysle Zákona o eGovernmente a je otázna ich použiteľnosť OVM pri overení autorizácie klikom.
* **eIDAS úroveň autorizácie** – v súčasnosti štandardy platné v SR definujú 4 úrovne autentifikácie. Do návrhu je potrebné doplniť prevodnú tabuľku, nakoľko môžu byť metódy autentifikácie používane na prístupovom mieste hodnotené v súlade so štandardami SR nie podľa eIDAS, ktoré referencuje legislatíva
* **description** – navrhujeme neuvádzať. Z definície „autorizačnej doložky“ je jasné, že sa jedná o „autorizáciu klikom“. Uvedený príklad „ autorizácia klikom z mobilného telefónu“ je mätúci, nakoľko spôsob autorizácie pri dodržaní minimálnej požadovanej úrovne autorizácie je irelevantný pre platnosť takejto autorizácie. „Autorizáciu klikom“ v zmysle zákona realizuje prístupové miesto, pričom úspešná autentfikácia (ako nutný predpoklad) bola v tomto prípade realizovaná ľubovoľným povoleným spôsobom autentifikácie.
* **delegation** – navrhujeme neuvádzať. Oprávnenie zastupovania sa nedeleguje v procese autentifikácie alebo autorizácie a vo väčšine prípadov prístupové miesto ani takúto informáciu nemá. A táto informácia nie je určujúca pre vyhodnotenie platnosti „autorizácie klikom“.

Oprávnenie k zastupovaniu sa väčšinou prikladá k podaniu ako samostatný doklad (ak toto oprávnenie nevyplýva zo zákona) a prístupové miesto touto informáciou spravidla nedisponuje tak, aby ho bolo schopné vložiť do štruktúry „autorizačnej doložky“. V prípade UPVS sú evidované výhradne oprávnenia pre prístup do schránky, čo však rozhodne nie je oprávnenie k uskutočňovaniu úkonov v mene vlastníka tejto elektronickej schránky.

* **Authentication\_method** – v tejto položke podľa nášho názoru postačuje uviesť použitú úroveň autentifikácie (a v tomto zmysle premenovať aj názov položky). Je možné diskutovať o jej použití, kde je možné zvažovať uvedenie typu použitého autentifikačného prostriedku, použitím ktorého prebehla identifikácia osoby v zmysle platnej legislatívy 305/2013 a QAA level.
* **Authentication\_method\_receipt** – navrhujeme túto položku nepoužívať, nakoľko pochybujeme o použiteľnosti tohto údaja pri vyhodnocovaní platnosti „autorizácie klikom“. Samozrejme, tento výsledok by mal uchovávať prevádzkovateľ prístupového miesta z dôvodu možného použitia v prípade riešenia prípadných sporov o vykonaní tohto spôsobu autorizácie.

Konštatovanie, že táto položka „obsahuje potvrdenku...“ je príliš všeobecná, lebo nie je zrejmé čo sa takouto „potvrdenkou“ chápe, Z technického pohľadu by mal byť postačujúci autentifikačný token, i keď i toto je nad rámec legislatívnych náležitostí. Ak nebudú existovať služby pre overenie tokenu vydaného správcom daného autentifikačného prostriedku (aj po exspirácii tokenu) tak to i tak stráca význam. Navyše OVM má zo zákona pri tomto spôsobe autorizácie dôverovať prístupovému miestu a doložke, už nebude skúmať token, t.j. dôkazový materiál na základe ktorého bola doložka vydaná. Preto ukladanie na prístupovom mieste v logoch naviazaných na konkrétne vykonanú autorizáciu ako dôkazný materiál pre prípad sporu.

Textácia „Je to dôkaz...“ je opätovne mätúca. Ako dôkaz je možné považovať „autorizačnú doložku“ autorizovaná pečaťou prístupového miesta spoločne s podaním. Adresát podania t.j. OVM je spoliehajúca sa strana, nebude skúmať token, bude veriť doložke.

* Navrhujeme doplniť položku určujúcu čas vykonania autorizácie, prípadne identifikátor autorizácie, prostredníctvom ktorého by bolo možné „napárovať“ autorizáciu na zaznamenané údaje použiteľné v prípade riešenia sporov.
* **Authorization\_method\_data** – túto položku navrhujeme zrušiť, nakoľko jej význam pre overovateľa platnosti autorizácie je nulový a aj v zmysle zákona nemá zmysel. V tejto položke má zmysel možno iba uvedenie referencie na autorizovaný dokument ( „digest\_method“, „digest value“, „document name“). Pripomíname však, že väzba doložky na autorizovaný dokument je zabezpečená spoločnou autorizáciou pečaťou prístupového miesta.

Nesúhlasíme s konštatovaním o „nepovinných údajoch o ďalšom použitom prostriedku ak ich dané špecifické riešenie potrebuje (napríklad zdokonalený podpis a podobne)“. Autorizácia klikom nemá vôbec adresovať špecifické riešenia pojednávajúce o akýchkoľvek typoch elektronických podpisov definovaných v nariadení eIDAS, nevynímajúc zdokonalený podpis. Buď sa podanie autorizuje na to určenou funkciou prístupového miesta (kliknutím) alebo iným platným spôsobom uvedeným v zákone o e-Governmente. Súčasné znenie zákona však neumožňuje využitie zdokonaleného podpisu pre autorizáciu podaní a teda jeho uvádzanie ako „nepovinná položka“ nemôže mať žiadny význam pri vyhodnocovaní autorizácie. V tom prípade je nutné iniciovať zmenu legislatívy s cieľom stanoviť dodatočné úrovne bezpečnostných záruk alebo právneho účinku a umožniť autorizáciu podaní aj explicitne zdokonaleným podpisom, pretože nie je možný koexistenčný režim, kedy autorizácia klikom spadá pod nariadenie eIDAS (autorizácia zdokonaleným podpisom) a zároveň je proprietárna a nespadá pod nariadenie eIDAS (na to určená funkcia prístupového miesta s vytvorením doložky). Odlišovanie režimov, právnych účinkov a spôsobov autorizácie by malo byť jasné a konzistentné.

### Ďalšie odporúčania

Koncept „podpisu klikom“ ITAS už v rámci pripomienkovania navrhovanej legislatívnej zmeny kritizoval ako krok, ktorý zavádza nesystémové riešenie, nakoľko predstavuje národné špecifikum aplikovateľné výhradne v kontexte e-Governmentu a výhradne pre autorizáciu podaní (a nie ani príloh k podaniam). Nie je nám v súčasnosti známe, že by iná krajina Európskej Únie (EÚ) využívala obdobný proprietárny mechanizmus s právnym účinkom vlastnoručného podpisu pre vyjadrenie súhlasu fyzickej osoby s podaním resp. úkonom a jeho obsahom v elektronickej forme.

Naopak, krajiny Európskej únie v praxi využívajú a spoliehajú sa na inštitúty a štandardy definované v nariadením Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu („eIDAS“) a súvisiacich vykonávacích nariadení Komisie EÚ. eIDAS priamo a komplexne adresuje prejav súhlasu fyzickej osoby v elektronickom svete pomocou elektronického podpisu. Explicitne stanovuje, že právny účinok kvalifikovaného elektronického podpisu (KEP) je rovnocenný s vlastnoručným podpisom. Členské štáty môžu okrem toho určiť na národnej úrovni, ktorý iný typ elektronického podpisu podľa eIDAS okrem KEP (elektronický podpis, zdokonalený podpis, zdokonalený podpis s kvalifikovaným certifikátom) je pre nich rovnocenný s vlastnoručným podpisom. Ale autorizácia klikom je funkciou prístupového miesta a ako sa uvádza v dôvodovej správe ku novelizácii zákona č. 305/2013 pri jeho zavádzaní do legislatívneho rámca, „hlavnou zmenou je možnosť autorizovať podanie aj s použitím funkcionality prístupového miesta, bez nutnosti využiť elektronický podpis“. Nejedná sa teda o žiadny z elektronických podpisov podľa eIDAS, ale o na to určenú funkciu prístupového miesta a nevzťahuje sa na ňu eIDAS.

Podľa nášho názoru „autorizácia klikom“, s ohľadom na všeobecne priradený právny účinok vlastnoručného podpisu, predstavuje dodatočné riziká a má podstatné nedostatky, na ktoré je potrebné upozorniť a vziať do úvahy pri zavádzaní do praxe spôsobom, aký definuje existujúcí legislatívny rámec:

* Autorizačná schéma nie je interoperabilná v cezhraničnom kontexte, ani nie je priamo použiteľná v komerčnom sektore.
* Legislatívne je ekvivalentom vlastnoručného podpisu, čo ju kladie na rovnocenné postavenie s kvalifikovaným elektronickým podpisom. Bezpečnostne (aj v spojení s autentifikáciou na úrovni pokročilá vyžadovanou v procese autorizácie) však poskytuje výrazne nižšie bezpečnostné záruky ako kvalifikovaný elektronický podpis. Nie je vytvorený národný jednotný rámec posudzovania bezpečnostných záruk všetkých autentifikačných schém pre účely využitia v e-Government prostredí (a teda aj pre „podpis klikom“) a zhody so všetkými požiadavkami vyplývajúcimi z vykonávacieho nariadenia EÚ č. 1502/2016, prípadne ďalšími relevantnými právnymi aktmi alebo odporúčaniami orgánov EÚ a jej agentúr v oblasti autentifikácie (napr. Guidance on LoA which support the eIDAS regulation, Európskej agentúry pre sieťovú a informačnú bezpečnosť - ENISA atď.). Stanovenie úrovne autentifikácie nem§že byť postavené na deklarácii dodávateľa, resp. poskytovateľa takejto služby.
* Nie je definovaná na národnej úrovni ako (kvalifikovaná) dôveryhodná služba, čo by umožňovalo kontrolovať a auditovať spôsob implementácie a tak výrazným spôsobom redukovať existujúce bezpečnostné riziká. Spoľahlivosť a dôveryhodnosť je do značnej miery priamo úmerná korektnosti implementácie v rámci konkrétneho prístupového miesta orgánu verejnej moci. Chýba kompetenčný rámec, vrátane režimu dohľadu so stanovenou periodicitou hodnotenia súladu implementácie autorizácie kliku prístupového miesta so zákonnými normami alebo štandardami.
* Nie je určené, na koho strane je v prípade sporu o autorizácii dôkazné bremeno, nakoľko eIDAS sa na tento spôsob autorizácie nevzťahuje. Autorizujúca osoba je v tomto prípade v nevýhode, pretože jediným zdrojom dôkazov je samotné prístupové miesto a jeho správna implementácia (autentifikačný token, monitoring, logy, bezpečné ukladanie údajov pre vyhotovenie kvalifikovanej pečate pre autorizáciu doložky atď.). A platnosť takejto autorizácie je podľa nášho názoru možné efektívne spochybniť.
* Definícia v legislatíve je pomerne vágna, čoho dôsledkom je priestor na rôznorodú, flexibilnú interpretáciu spôsobu realizácie, o čom nasvedčujú rozsiahle a rozporuplné pohľady odbornej verejnosti a dokazuje to aj diskusia ku prvému riešeniu, ktoré deklaruje „úplnú“ zhodu s legislatívnym rámcom pre autorizáciu „klikom“, konkrétne DEUS mID.
* Autorizujúca osoba nemá autorizačný prostriedok pod svojou výlučnou kontrolou, pretože sa jedná o funkciu prístupového miesta, nie o koncept elektronického podpisu. Na základe toho sa nedá s vysokou mierou istoty vylúčiť, že podanie bolo autorizované bez jej vedomia čo môže byť problematické pri preukazovaní neodmietnuteľnosti autorizovaného právneho úkonu a vytvára priestor pre právnu neistotu.

Rozumieme motivácii zjednodušiť spôsob autorizácie v prípade tých elektronických služieb a podaní, kde je autorizácia prostredníctvom KEP s ohľadom na ich povahu a potenciálny dopad na práva a povinnosti neprimeraná. Avšak nie sme presvedčení, že ekvivalencia právneho účinku pre diametrálne odlišné spôsoby autorizácie v elektronickom priestore s rozdielnymi úrovňami bezpečnostných záruk pre všetky elektronické služby je racionálny prístup.

Apelujeme na čo možno najskoršie napravenie nekonzistentného legislatívneho stavu, ktorého cieľom by malo byť zavedenie dodatočnej kategórie právneho účinku resp. „úrovní“ autorizácie elektronickými metódami s nižšími bezpečnostnými zárukami (vrátane autorizácie klikom, zdokonaleného podpisu s alebo bez kvalifikovaného certifikátu a pod.) a dosiahnutie flexibility technologických možností pre autentifikačné a autorizačné mechanizmy s rôznymi úrovňami bezpečnostných záruk. V praxi toto môže spôsobovať problémy v akceptácii „podpisu klikom pre vybrané služby“ napriek skutočnosti, že legislatíva toto všeobecne vyžaduje

Na MIRRI je k dispozícii legislatívny návrh zmien v oblasti autorizácie, ktorý zavádza pre autorizáciu v elektronickom prostredí rôzne úrovne autorizácie v závislosti od nimi poskytovaných bezpečnostných záruk. Následne predpokladá pre každú službu stanovenie minimálnej požadovanej úrovne pre autorizácie. Odporúčame rozpracovanie tohto princípu, ktorý zavádza konzistentný a systematický prístup k zavádzaniu nových inovatívnych prostriedkov pre autorizáciu úkonov v elektronickom prostredí.