## Detailný popis požiadaviek k Dodatku č. 8 k Zmluve na úpravu informačných systémov a zabezpečenie služieb ich prevádzky

Predmetom úpravy je zabezpečenie časti legislatívnych požiadaviek na úpravu spoločných modulov ÚPVS v súvislosti so zmenami, ktoré vyplývajú zo zákona č. 238/2017 Z. z. účinného od 1. 11. 2017 a nasledujúcimi platnými novelami, najmä zákona č. 211/2019 Z. z, ktorými sa mení a dopĺňa zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente). Ďalšie úpravy sa týkajú optimalizácie a zmeny existujúcich funkcionalít ÚPVS z dôvodu zmeny zákona o e-Governmente a rozšírenia funkcionality aplikácií na podporu prevádzky ÚPVS.

Najdôležitejšie témy, ktorých sa týka úprava funkcionalít jednotlivých modulov a komponentov ÚPVS:

**Autentifikačný modul (IAM)**

Predmetom úpravy sú zmeny súvisiace s budovaním mobilného riešenia. Tie sa týkajú rozšírenia registra autentifikačných certifikátov o registráciu a evidenciu certifikátov fyzických osôb a umožnenie ich využívania pri prihlasovaní používateľov v mobilnom riešení.

V súvislosti s novým mobilným riešením je potrebná nielen úprava modulu IAM, ale aj modulu elektronických schránok a ostatných dotknutých modulov ÚPVS. Súčasne je potrebné služby IAM upraviť tak, aby mohli byť zverejnené na OpenApi platforme.

Mobilné riešenie bude predstavovať otvorený systém federácie identít, čo v praxi znamená, že umožní trhu podieľať sa na sprístupnení existujúcich identít v ÚPVS, ktoré sú dôveryhodné. Pre zabezpečenie otvoreného systému a schopnosti sprístupniť na jednom mieste viacerých prevádzkovateľov identít je potrebné zriadiť federačnú autoritu, ktorou má byt’ NASES. Federačná autorita bude podľa stanovených podmienok a pravidiel pripájať štátnych aj komerčných prevádzkovateľov identít do jedného identitného systému.

Úlohou mobilného riešenia je umožniť používateľovi prihlásiť sa prostredníctvom autentifikačného certifikátu cez špecializovanú mobilnú aplikáciu pre prihlasovanie, ktorú bude mať používateľ inštalovanú na mobilnom zariadení. Používateľovi bude umožnené prihlásiť sa aj z viacerých mobilných zariadení. Používateľ si bude môcť zaregistrovať svoje mobilné zariadenie pomocou eID karty na portáli ÚPVS alebo asistovane na integrovanom obslužnom mieste (IOM).

Mobilné riešenie bude v čo najväčšej miere využívať existujúce funkcionality a rozhrania poskytované spoločnými modulmi ÚPVS. Riešenie poskytne integračné rozhrania pre pripojenie ďalších providerov mobilných ID riešení pre plnohodnotné a rovnocenné prihlasovanie autentifikačným certifikátom používateľa, rozhrania pre registráciu autentifikačného certifikátu do centrálneho registra autentifikačných certifikátov pre IOM.

Tieto integračné rozhrania spoločne s univerzálnym rozhraním pre pripojenie autentifikačných serverov 3tích strán budú predstavovať otvorený systém federácie identít, ktorý umožní sprístupňovať identity z externých systémov (aj z komerčného sveta ako napr. banky a pod.) v ÚPVS ak sú tieto systémy a poskytované údaje o identitách dôveryhodné. Príkladom sú napríklad identity advokátov s možnosťou autentifikácie alternatívnym autentifikátorom.

Súčasťou mobilného riešenia bude aj špecializovaná mobilná aplikácia pre zobrazenie obsahu elektronickej schránky. Táto umožní zobraziť na mobilnom zariadené jednotlivé priečinky, zoznamy prijatých správ, detail správ s prechodom na predchádzajúcu alebo ďalšiu správu. Umožní prihlásiť sa v mene iného subjektu podľa existujúcich zastupovaní evidovaných v IAM a prehliadať obsah schránky tohto subjektu. Aplikácia umožní prevzatie doručovanej správy cez autorizáciu doručenky. Aplikácia bude integrovaná na mechanizmus push notifikácií o uložení novej správy v schránke.

Súčasťou mobilného riešenia je aj poskytnutie možnosti autorizácie elektronických správ prostredníctvom novovybudovanej funkcionality podpisu klikom pre fyzické o právnické osoby ako funkcionality centrálneho podpisového komponentu. Prístupové miesta nebudú nútené budovať a prevádzkovať vlastné riešenia pre podpis klikom, nakoľko centrálny podpisový komponent poskytne rozhrania pre integráciu informačných systémov prístupových miest za účelom využitia jeho autorizačných funkcií.

Zavedenie mobilného riešenia do produkčnej prevádzky bude mať výkonnostné dopady aj na ostatné moduly ústredného portálu. Z tohto dôvodu bude preto nutné optimalizovať modul elektronických schránok spôsobom, ktorý by eliminoval vzájomné výkonnostné interakcie medzi rozhraniami a službami modulu. Navrhovaná optimalizácia bude realizovaná zmenou architektúry modulu na koncepciu mikroslužbieb. Ďalšie úpravy sa týkajú rozšírenia vybraných služieb o  funkcionalitu vyhľadávania podľa viacerých kritérií a podporu stránkovania a hromadných akcií a zverejnenie týchto služieb na OpenApi. Úpravy IAM zahŕňajú doplnenie údajov vedených o autentifikačnom certifikáte v registri autentifikačných certifikátov a vytvorenie služieb, ktorými bude sprístupnený výsledok autentifikácie úradným autentifikátorom aj pre vybrané komerčné subjekty (napr. banky, poštové podniky a iné).

Vyššie uvedené zmeny majú dopad aj na modul centrálneho monitorovacieho nástroja a na modul zberu a vyhodnocovania údajov (DWH), preto je potrebné doplniť zber, ukladanie a vyhodnocovanie relevantných dát do týchto modulov.

**Modul elektronických schránok (eDesk)**

Zahŕňa úpravy spojené so zriaďovaním elektronických schránok pre neplnoletých a schránok pre orgány verejnej moci na základe osobitného účelu. Na zriadenie schránky pre maloleté osoby budú dostupné elektronické formuláre v anonymnom a neanonymnom režime a bude rozšírená a upravená integrácia na register fyzických osôb.

Rovnako budú sprístupnené žiadosti o vytvorenie a zrušenie elektronickej schránky orgánom verejnej moci, ktoré v rozsahu ustanovenom osobitným predpisom plnia úlohy vo veciach ochrany ústavného zriadenia, vnútorného poriadku a bezpečnosti štátu, a to na účely plnenia jeho úloh. Za týmto účelom bude doplnená nové špecifické oprávnenie (rola) v IAM.

**Modul centrálnej elektronickej podateľne (CEP)**

Doplnenie funkcionalít sa týka možnosti vyhotovenia autorizácie klikom tak, aby po úspešnej autentifikácii osoby, ktorá autorizáciu vykonáva bolo zabezpečené uvedenie tejto osoby ako odosielateľa elektronickej správy, nemennosť obsahu autorizovaného dokumentu do momentu uloženia v elektronickej schránke adresáta a spojenie autorizovaného dokumentu s identifikátorom osoby odosielateľa a zachovanie väzby medzi nimi.

Nová funkcionalita autorizácie klikom umožní  fyzickým a právnickým osobám autorizáciu elektronického podania na prístupových miestach klikom a to v prípade ak nie je ustanovený iný spôsob autorizácie alebo ak je podľa osobitného predpisu náležitosťou podania vlastnoručný podpis.

Autorizácia klikom pre prístupové miesta bude funkciou centrálneho komponentu. Súčasťou konceptu je preto aj vybudovanie centrálneho podpisového komponentu (CPK), ktorá by v prvej fáze centrálne zabezpečovala autorizáciu klikom, neskôr sa môže rozširovať o nové autorizačné funkcie. CPK sprístupní rozhrania umožňujúce prístupovým miestam integrácie svojich systémov a umožní im tak využívanie jeho autorizačných funkcií.  Tým sa docieli to, že prístupové miesta nebudú nútené budovať a prevádzkovať vlastné riešenia, postačujúca bude ich integrácia na CPK.

Služby CEP pre overenie podpisov budú rozšírené o overenie autorizácie klikom.

## Obsah

[Časť Diela IAM – 2017/2019 5](#_Toc29934597)

[Časť Diela - Mobilná aplikácia MeID 27](#_Toc29934598)

[Časť Diela eDESK - 2019 30](#_Toc29934599)

[Časť Diela CEP - 2017 32](#_Toc29934600)

### Časť Diela IAM – 2017/2019

Zoznam požiadaviek IAM – 2017/2019 je uvedený v tabuľke.

| **Požiadavka** | **Názov požiadavky** | **Popis** | **Legislatíva** | **Závislosť** |
| --- | --- | --- | --- | --- |
| R19-IAM-004 | Rozšírenie centrálneho registra autentifikačných certifikátov o fyzické osoby | Úprava a rozšírenie Registra autentifikačných certifikátov tak, aby poskytol dostatočnú kapacitu a výkon na ukladanie, uchovávanie a poskytovanie údajov o autentifikačných certifikátov aj pre fyzické osoby. | § 22a ods. 1 |  |
| R19-IAM-007 | Mobilné riešenie a jeho integrácia | Sprístupnenie autentifikácie a autorizácie k službám e-Governmentu prostredníctvom mobilného zariadenia. Úprava rozhraní na účely pripojenia iného spôsobu autentifikácie pri prístupe k ÚPVS. Požiadavka je fázovaná a zahŕňa aj dopady MeID riešenia na IAM, G2G a eForm. Ďalej sprístupnenie push notifikácií, integráciu riešení tretích strán a pripojenie IOM. |  | R19-IAM-004 |
| R19-IAM-014 | Rozšírenie údajov vedených o autentifikačnom certifikáte v centrálnom registri | Úprava a rozšírenie Registra autentifikačných certifikátov o údaje v zmysle § 22a ods. 3. | § 22a ods. 3 písm. b) |  |
| R19-IAM-015 | Autentifikácia klientov komerčných subjektov úradným autentifikátorom | Nová služba pre vybrané komerčné subjekty definované zákonom, ktorá umožní získať vybrané údaje o prihlásenej identite. | Čl. VI - X |  |
| R19-IAM-016 | Autentifikácia alternatívnymi autentifikátormi a zakladanie schránok advokátov | Nová funkcionalita prihlasovania na ÚPVS a do elektronických schránok pre vybranú skupinu fyzických osôb, ktoré sa budú prihlasovať identifikačnou kartou advokáta. | §21 ods. 6 |  |
| R19-ALL-004 | Jednotný postup pri detekcii elektronického formulára | Zoznam pravidiel pre detekciu elektronického formulára. |  | R19-IAM-004 |
| R19-EDESK-002 | Optimalizácia služieb modulu eDesk - prechod na mikroslužby | Prechod služieb modulu na mikroslužby. |  | R19-IAM-004, R19-IAM-007 |
| R19-EDESK-003 | Škálovanie databáz modulu eDesk | Úprava riešenia zamedzenia výkonnostnej interakcie jednotlivých rozhraní eDesku. |  | R19-IAM-004, R19-IAM-007 |
| R19-EDESK-004 | Definovanie nezávislých skupín schránok modulu eDesk pre samostatné nasadenie | Úprava riešenia pri práci s jednotlivými skupinami schránok. |  | R19-IAM-004, R19-IAM-007 |
| R19-EDESK-005 | Domigrácia správ z existujúcich schránok modulu eDesk do OST | Migrácia všetkých správ modulu eDesk do OST. |  | R19-IAM-004, R19-IAM-007 |
| R19-EDESK-008 | Použitie OST v konštruktore správ | Úprava konštruktora správ na ukladanie správ do OST. |  | R19-IAM-004, R19-IAM-007 |
| R19-EDESK-009 | Optimalizácia a rozšírenie služieb EKR modulu eDesk | Úprava metód EKR o funkcionalitu na vyhľadávanie podľa viacerých kritérií, stránkovanie a hromadné akcie. |  | R19-IAM-004, R19-IAM-007 |
| R19-DWH-001 | Konsolidácia DWH | Zmena architektúry na úrovni dátových štruktúr DWH z dôvodu zvýšených nárokov na rýchlosť spracovania a rastúci objem dát. |  | R19-IAM-004 |
| R19-MON-001 | Vytvorenie zobrazenia pre MUK-P a prípadné ďalšie nové komponenty | Rozšírenie informačných panelov pre modul MUK-P. |  | R19-IAM-004 |

##### **R19-IAM-004** **Rozšírenie centrálneho registra autentifikačných certifikátov o fyzické osoby**

**Súčasný stav**

Register autentifikačných certifikátov je v súčasnosti z výkonnostného a kapacitného pohľadu dimenzovaný na ukladanie, uchovávanie a poskytovanie údajov o autentifikačných certifikátov nasledovných typov identít:

* právnické osoby
* fyzické osoby - podnikateľov
* orgány verejnej moci

**Požadovaný stav**

Technologicky a infraštruktúrne je potrebné upraviť/rozšíriť Register autentifikačných certifikátov tak, aby poskytol dostatočnú kapacitu a výkon na ukladanie, uchovávanie a poskytovanie údajov o autentifikačných certifikátov aj pre fyzické osoby. Súčasťou požadovaného stavu je aj prípadný dopad na procesy služby modulu CRAC (napríklad tie, ktoré zapisujú/poskytujú údaje o autentifikačných certifikátoch). Autentifikačné certifikáty fyzických osôb budú primárne použité na účel prihlasovania (napr. mobileID autentifikácia). Z tohto dôvodu je potrebné zabezpečiť zvýšenie výkonnosti a priepustnosti modulu IAM, ktorého služby sú pre prihlasovanie využívané a to vytvorením nových NOD-ov modulu IAM.

##### **R19-IAM-007** **Mobilné riešenie a jeho integrácia**

**Súčasný stav**

V súčasnom stave nie je možné prihlásiť sa do elektronickej schránky  pomocou mobilného zariadenia. Používateľ je pre prihlasovanie nútený používať eID kartu s čítačkou (prípadne iný úradný alebo alternatívny autentifikátor) a musí mať na svojom zariadení nainštalovaný obslužný SW.

**Požadovaný stav**

**Úvod**

Umožniť používateľovi prihlásiť sa autentifikačným certifikátom cez špecializovanú mobilnú aplikáciu pre prihlasovanie (mID) inštalovanú v mobilnom zariadení a to v nasledovných scenároch:

* z mobilnej aplikácie 3tej strany (MA3S),
* z webovej aplikácie 3tej strany (WA3S), pričom webová aplikácia v ktorej používateľ pracuje môže bežať v mobilnom zariadení (i na tom istom na ktorom beží mID) alebo na osobnom počítači. Webová aplikácia môže byť integrovaná na IAM buď ako oAuth2 klient (využíva openID connect) alebo ako service provider (využíva saml2 websso).

Umožniť používateľovi registrovať autentifikačný certifikát a mobilné zariadenie nasledovnými scenármi:

* samoregistrácia autentifikačného certifikátu prostredníctvom prihlásenia eID kartou (prípadne čipovou kartou povolenia k trvalému pobytu, alebo podporovaným alternatívnym autentifikátorom),
* asistovaná registrácia autentifikačného certifikátu na integrovanom obslužnom mieste.

Umožniť používateľovi odregistrovať autentifikačný certifikát a mobilné zariadenie vrátane zrušenia autentifikačného certifikátu (zmazanie privátneho kľúča zo zariadenia a zrušenie certifikátu v registri autentifikačných certifikátov (CRAC) nasledovnými scenármi:

* samoobslužná odregistrácia prihláseným používateľom,
* asistovaná odregistrácia.

Umožniť mobilnej aplikácii 3tej strany overiť údaje o identite, pričom pre autentifikáciu identity sa využije mID, ktorá s integráciou na IAM vytvára koncept mobileID.

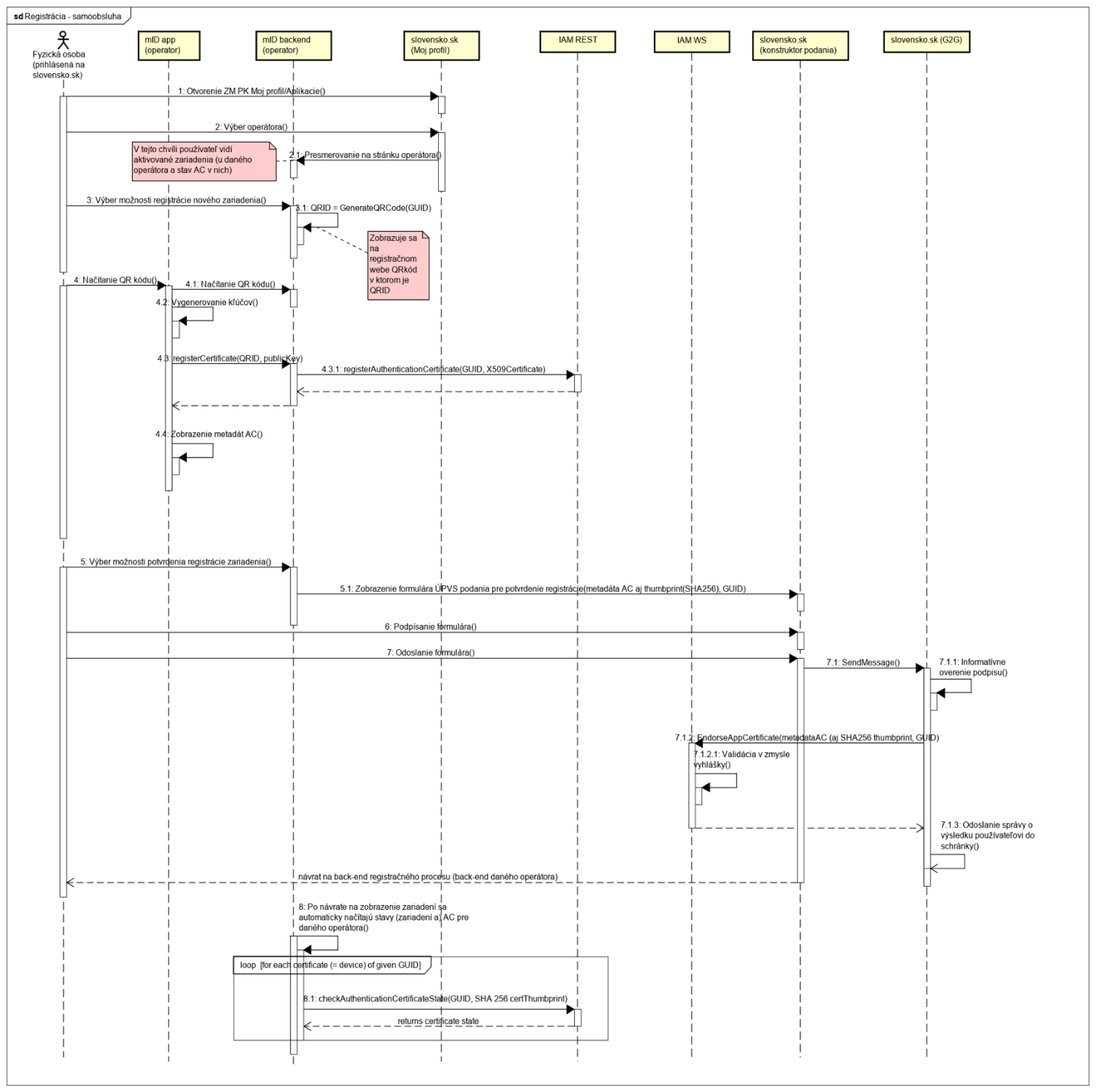
Pri budovaní mobileID riešenia, musí byť kladený dôraz na splnenie nasledovných požiadaviek:

* **Požiadavky týkajúce sa celého mobileID riešenia:** 
  + v čo najväčšej miere využiť jestvujúce funkcionality a rozhrania poskytované spoločnými modulmi ÚPVS vrátane IAM oAuth2 servera s openID connect budovaného v MUK-P (využitie možných synergií)
  + prevádzkovať celé riešenie mobileID výhradne na infraštruktúre v správe NASES
  + umožniť prihlásenie používateľa z viacerých mobilných zariadení
  + vybudovať a poskytnúť integračné rozhrania pre:
    - pripojenie mobileID DEUS (používajúce vlastný autentifikačný server a mID) pre plnohodnotné a rovnocenné prihlasovanie autentifikačným certifikátom dvoma nezávislými štátnymi mobileID riešeniami : mobileID NASES a mobileID DEUS
    - pripojenie mobileID DEUS (používajúce vlastný autentifikačný server a mID) pre plnohodnotné a rovnocenné získanie údajov identity nezávislými mobile ID riešeniami: mobileID NASES a mobileID DEUS
    - pripojenie mobileID a integrovaného obslužného miesta pre registráciu a odregistráciu (zrušenie) autentifikačného certifikátu do/z CRAC
  + rozšíriť koncept jednotného prihlásenia o nasledovné scenáre:
    - presmerovanie prihláseného používateľa z oAuth2klienta na iného oAuth2klienta na tom istom zariadení, pričom používateľ ostáva prihlásený
    - presmerovanie prihláseného používateľa zo service providera na iného oAuth2klienta, pričom používateľ ostáva prihlásený
    - nasledovný scenár nebude podporovaný: presmerovanie prihláseného používateľa z oAuth2 klienta na service providera, pričom používateľ by zostal prihlásený. V tomto prípade nebude používateľ po presmerovaní prihlásený.
    - dobudovanie konfigurácie oAuth2 klientov po vzore service providerov: Cieľom je umožniť jednotlivým oAuth2 klientom konfigurovať autentifikačné prostriedky zobrazované na prihlasovacej obrazovke IAM ÚPVS
    - dobudovať podporu pre dodatočnú autentifikáciu pre oAuth2
  + Vybudovať publish-subscribe mechanizmuz pre kanál push notifikácii, v ktorom eDesk vystupuje v roli pubslihera a mEdesk v roli subscribera. Súčasťou požiadavky však nie je posielanie push notifikácia tým používateľom, ktorí majú v IAM nastavené čiastočný prístup (zastupovanie) k danej elektronickej schránke. Dôvodom tohto obmedzenia sú komplikácie spojené s možnosťou nastavovania oprávnení na konkrétnej priečinky pre tento typ zastupovania. Rozšírenie push notifikácie aj na tieto prípady bude predmetom ďalšej rozvojovej fázy. Publish-subscribe mechanizmus bude vybudovaný tak, aby vytvoril predpoklady pre budúce rozšírenie o:
    - ďalšie udalosti, ktoré by mohli byť v budúcnosti predmetom notifikácií (napr. CUET novinky, zmeny v údajoch identít a pod.) a integráciu systémov, ktoré ich generujú (nový publisheri)
    - nové komunikačné kanály, ktorými bude prebiehať notifikácia (napr. sms, email, elektronická schránka, rozhranie)
    - nové typy subscription.
* **Požiadavky súvisiace s procesom  registrácie mobileID NASES:** 
  + zabezpečiť zaregistrovanie autentifikačného certifikátu a súvisiacich meta údajov potrebných pre prihlásenie: privátna časť kľúča ostáva uložená v mobilom zariadení, verejná časť a meta údaje budú zaregistrovaná v IAM/CRAC.
  + vytvorenie používateľského rozhrania ako rozšírenie profilu identity, kde:
    - * používateľ bude mať možnosť inicializovať a vykonať registráciu mobileID NASES alebo presmerovať sa na mobileID DEUS registráciu
      * používateľ bude mať možnosť zobraziť zoznam registrovaných mobilných zariadení s mID NASES
      * používateľ bude mať možnosť inicializovať a vykonať samoobslužnú odregistráciu mobileID NASES

**Dopady na UPVS**

**IAM a CRAC**

**Samoobslužná registrácia:** v IAM a CRAC budú implementované rozhrania a funkcionality vyplývajúceho z nasledovného procesu:



**Asistovaná registrácia na IOM:** v IAM a CRAC budú implementované rozhrania a funkcionality z procesu asistovanej registrácie, ktorá vychádza z procesu samoobslužnej registrácie, takže detailnejšie je možné realizáciu niektorých krokov odsledovať aj pomocou relevantných častí sekvenčného diagramu samoobslužnej registrácie - viď diagram vyššie.

Popis krokov relevantných pre samoobslužnú registráciu:

1. Obslužný systém registrátora (IOM) volá mID backend daného operátora s požiadavkou na registráciu používateľa (REST služba). Parametre volania, nutné k vytvoreniu autentifikačného a podpisového certifikátu:
2. mobilID systém (back-end) naštartuje registráciu používateľa, poskytne obslužnému systému registrátora aktivačný kód, ktorý obslužný systém registrátora zobrazí ako QR kód. Spolu s aktivačným kódom vráti aj identifikáciu požiadavky pre budúce párovanie (transactionID).
3. Scenár pokračuje aktiváciou mID aplikácie tak ako pri samoobsluhe (používateľ zadá/vyberie si svoj PIN kód, mID systém operátora (pozostávajúci z mobilnej aplikácie aj back-end) vygeneruje autentifikačný a podpisový certifikát používateľa (v prípade ak operátor okrem autentifikácie podporuje podpis pre komerčnú sféru – viď príslušné scenáre). Autentifikačný certifikát je uložený v registri AC (zatiaľ neaktivovaný). Jeho thumbprint je vrátený do back-endu obslužného systému registrátora (spárovanie cez transactionID). Týmto krokom sa považuje aktivácia podpisovacieho certifikátu za ukončenú (informácia ide do obslužného sytému registrátora).
4. Operátor obslužného systému registrátora skonštruuje pre dané GUID a thumbprint certifikátu podanie – ktoré v mene občana na IOM je podpísané a odoslané na spracovanie.
5. Operátor obslužného systému po čase (asynchrónne spracovanie podania) vidí, že daný AC je finálne aktivovaný.

**Samoobslužná odregistrácia prihláseným používateľom:**v IAM a CRAC budú implementované rozhrania a funkcionality vyplývajúceho z nasledovného procesu:

Popis krokov relevantných pre samoobslužnú odregistráciu prihláseným používateľom v mobilnom zariadení:

1. Prihlásený používateľ v mID aplikácii prejde do nastavení aplikácie
2. Používateľ klikne na tlačidlo odregistrovania autentifikačného certifikátu
3. Aplikácia otvorí pop up okno so žiadosťou o potvrdenie vykonania odregistrácie
4. Používateľ potvrdí odregistrovanie
5. Aplikácia zavolá mobileID systém (back-end) s požiadavkou o odregistrovanie AC
6. Aplikácia zneplatní AC v mobilnom zariadení

Popis krokov relevantných pre samoobslužnú odregistráciu prihláseným používateľom v PK - profil identity na ÚPVS:

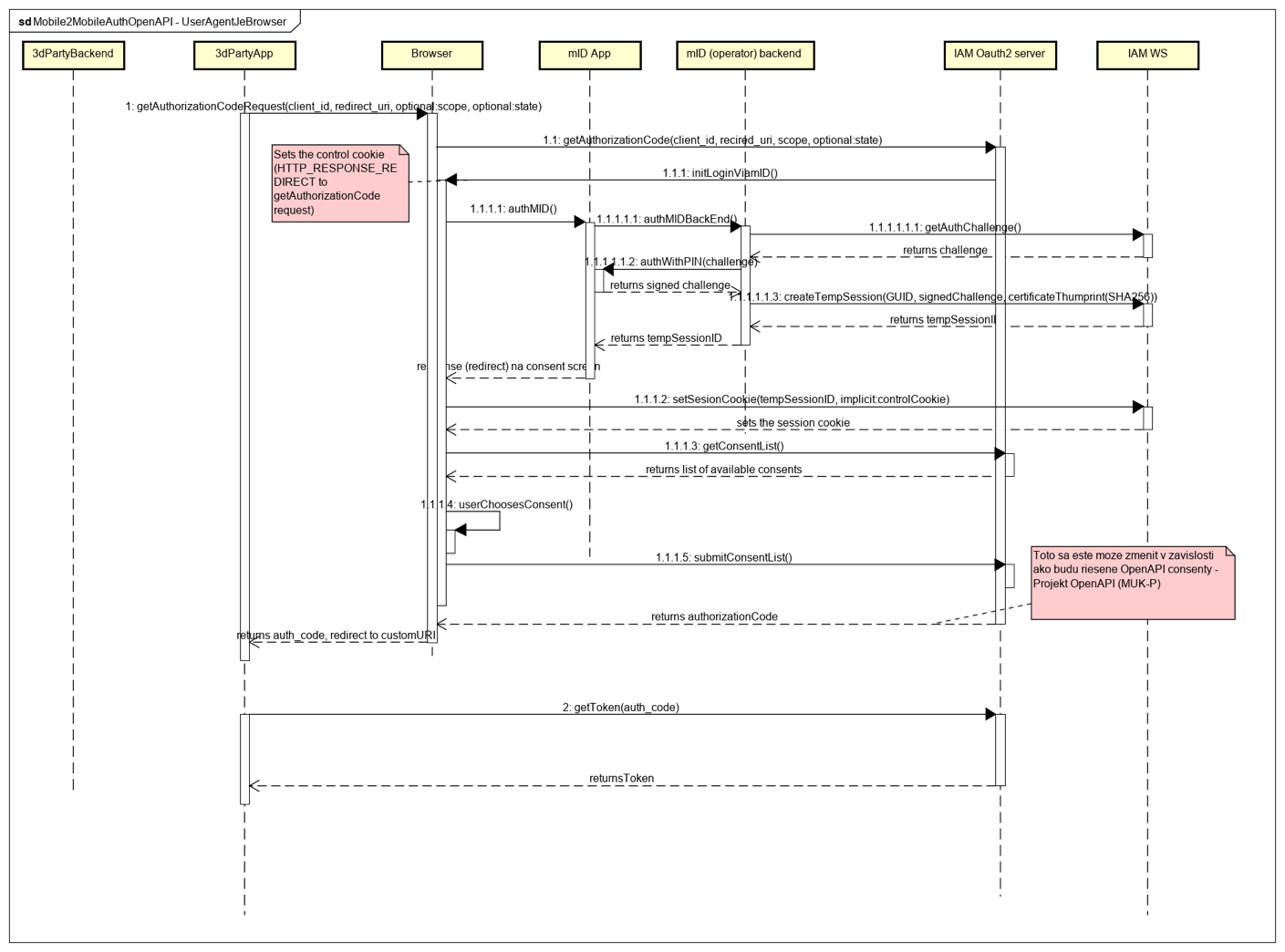
1. Prihlásený používateľ v PK ÚPVS prejde do sekcie Môj profil/Mobilné zariadenia
2. Používateľ klikne na tlačidlo odregistrovania autentifikačného certifikátu na konkrétnom mobilnom zariadení
3. Aplikácia otvorí pop up okno so žiadosťou o potvrdenie vykonania odregistrácie
4. Používateľ potvrdí odregistrovanie
5. Aplikácia zavolá mobileID systém (back-end) s požiadavkou o odregistrovanie AC
6. Po prijatí úspešnej odpovede zo strany mobileID systému (back-end) aplikácia je zobrazené zariadenie resp. AC na danom zariadený zobrazovaný v PK ako neplatný
7. V prípade ak sa používateľ pokúsi o prihlásenie v mID app, nepodarí sa mu to z dôvodu neplatného AC v IAM / CRAC a zneplatní AC aj v mobilnom zariadení

**Asistovaná odregistrácia na IOM:** v IAM a CRAC budú implementované rozhrania a funkcionality vyplývajúceho z nasledovného procesu:

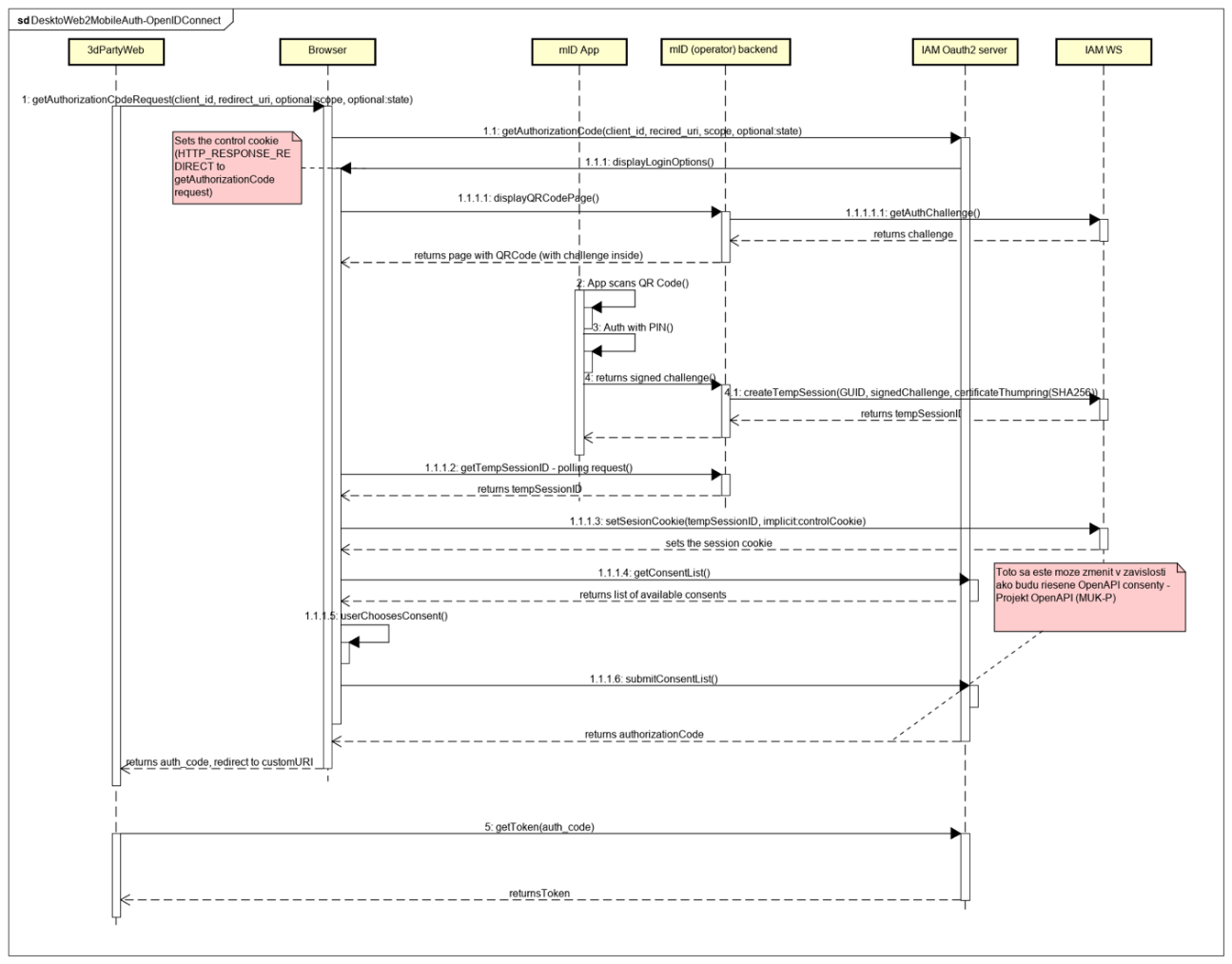
 Popis krokov relevantných pre asistovanú odregistráciu prihláseným používateľom:

1. Obslužný systém registrátora (IOM) volá mID backend daného operátora s požiadavkou na odregistráciu používateľa (REST služba). Parametre volania, nutné k vytvoreniu autentifikačného a podpisového certifikátu:
2. Operátor obslužného systému vidí, že daný AC je deaktivovaný v IAM / CRAC.
3. V prípade ak sa používateľ pokúsi o prihlásenie v mID app, nepodarí sa mu to z dôvodu neplatného AC v IAM / CRAC a zneplatní AC aj v mobilnom zariadení

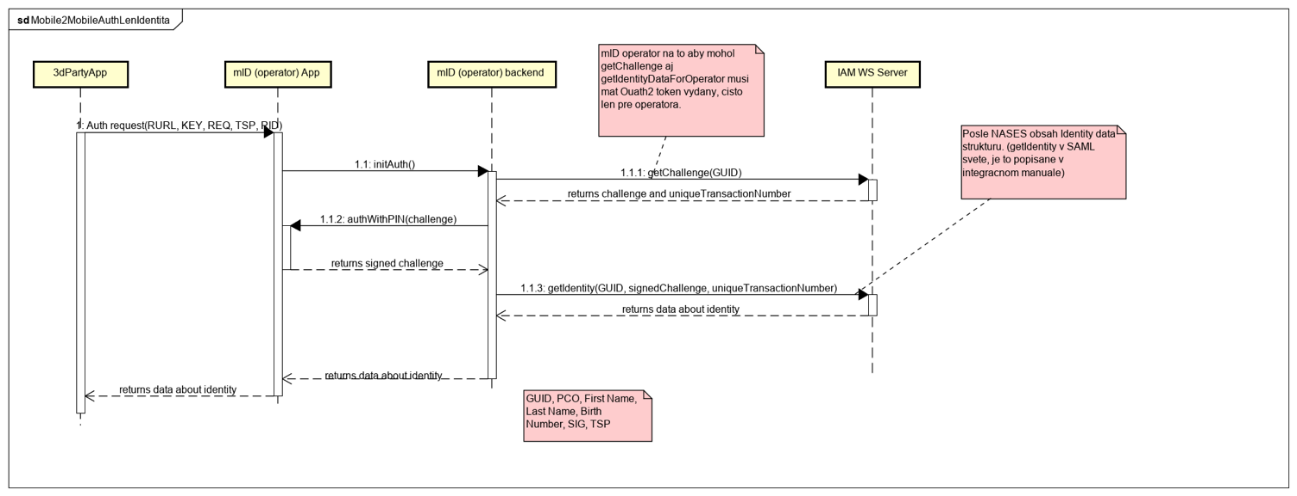
**Prihlasovanie z mobilnej aplikácie 3tej strany (MA3S):** v IAM a CRAC budú implementované rozhrania a funkcionality vyplývajúceho z nasledovného procesu:



**Prihlasovanie z webovej aplikácie 3tej strany (WA3S):** v IAM a CRAC budú implementované rozhrania a funkcionality vyplývajúceho z nasledovného procesu:



**Získanie údajov o identite z  mobilnej aplikácie 3tej strany (MA3S):** v IAM a CRAC budú implementované rozhrania a funkcionality vyplývajúceho z nasledovného procesu:



**Ďalšie rozšírenia funkcionality týkajúce sa prihlásenia cez mobileID**

* rozšírenie konceptu jednotného prihlásenia o nasledovné scenáre:
  + prechod prihláseného používateľa z oAuth2klienta na iného oAuth2klienta na tom istom zariadení, pričom používateľ ostáva prihlásený
  + prechod prihláseného používateľa zo service providera na iného oAuth2klienta na tom istom zariadení, pričom používateľ ostáva prihlásený
  + dobudovanie konfigurácie oAuth2 klientov po vzore service providerom: Cieľom je, umožniť jednotlivým service providerom konfigurovať autnetifikačné prostriedky zobrazované na prihlasovacej obrazovke
* dobudovať podporu pre opakované prihlasovanie pre oAuth2
* rozšíriť login obrazovky IAM o možnosť prihlásenia cez mobileID NASES a mobileID DEUS
* zavedenie nových typov autentifikačných prostriedkov pre mobileID NASES a mobileID DEUS
* rozšíriť login obrazovku pre prihlasovanie cez oAuth2 na vstupe o zoznam podporovaných autentifikčných prostriedkov (načítaných z konfigurácie oAuth2 klientov, nakoľko service providerom v tomto scenári je vždy oAuth2 server)

**Modul G2G**

**Samoobslužná registrácia:** v G2G bude vytvorená orchestrácia vyplývajúceho z procesu - viď diagram samoregistrácie uvedený v dopadoch na IAM a CRAC. Tá zahŕňa:

* validáciu podpisu na žiadosti: či je podpis kvalifikovaný a či je platný
* validáciu žiadateľa: súlad identity žiadateľa s identifikátorom prihlásenej osoby
* integráciu na WS IAM pre zaregistrovanie certifikátu
* vytvorenie a odoslanie notifikácie o výsledku registrácie do schránky žiadateľa

**Asistovaná registrácia:** v G2G bude vytvorená orchestrácia pre spracovanie žiadosti o registráciu autentifikačného certifikátu na IOM. Tá zahŕňa:

* + validáciu podpisu na žiadosti: či je podpis platný a či sa jedná o kvalifikovanú elektronickú pečať IOM
  + validáciu identity prihlásenej osoby: či sa jedná o identitu typu OVM s priradenou rolou oprávňujúcou vykonávať asistovanú registráciu autentifikačného certifikátu
  + integráciu na WS IAM pre zaregistrovanie certifikátu
  + vytvorenie a odoslanie notifikácie o výsledku registrácie do schránky žiadateľa

**Elektronické formuláre**

Budú vytvorené a v module elektronických formulárov (MEF) zaregistrované nasledovné elektronické formuláre:

* elektronický formulár žiadosti o samoobslužnú registráciu
* elektronický formulár žiadosti o asistovanú registráciu
* elektronický formulár notifikácie o výsledku registrácie

**eDesk**

Budú realizované nasledovné rozšírenia:

* Integrácia na službu publish v momente uloženia novej správy do schránky,
* optimalizácia EKR služby pre získanie nových správ.

**Publish-subscribe**

Pre push notifikácie do mobilnej aplikácie bude vybudovaný publish-subscribe mechanizmus, ktorý bude poskytovať služby pre

* publikovanie udalostí - zatiaľ sa budú publikovať udalosti v module eDesk o novej správe v schránke,
* subscribe klienta - mobilná aplikácia mEdesk sa prihlási k odoberaniu push notifikácii o nových správach v schránke pre danú schránku.

Samotný komponent bude naintegrovaný na systémových poskytovateľov push notifikácii do mobilu pre operačné systémyu iOS a Android.

Bude vyhodnocovať dané eventy (nová správa v schránke) a spracovávať ich, to znamená preposielať na push notifikácie pre subscriberov.

Komponent bude integrovaný aj na služby IAM za účelom získania aktuálnych údajov o identite resp. zastupovaní.

##### **R19-IAM-014 Rozšírenie údajov vedených o autentifikačnom certifikáte v centrálnom registri**

**Súčasný stav**

Register autentifikačných certifikátov spoločne s modulom IAM v terminológii ÚPVS má uchovávať nasledovné údaje o autentifikačných certifikátoch právnických osôb, fyzických osôb podnikateľov a OVM:

1/ certifikát a údaje v ňom uvedené ako napr. CN, DN, použitý algoritmus, vydavateľ, platnosť, verzia, identifikátor držiteľa certifikátu a pod.

2/ údaj o autentifikačnom certifikáte uvádzaný na technickom účte

3/ zastupovanie medzi technickým účtom a identitou držiteľa certifikátu vrátane rozsahu oprávnení, ktoré identita delegovala technickému účtu (role a typ zastupovania medzi identitou a technickým účtom)

Po nasadení IAM OAUTH2 autentifikácie a dodaní projektu MUK-P do prevádzky bude modul IAM a MUK-P uchovávať nasledovné údaje:

4/ identifikátor a certifikát aplikácie 3tej strany pre prístup k rozhraniam (službám) zverejneným na MUK-P

5/ oprávnenia aplikácie 3tej strany k rozhraniam (službám) zverejneným na MUK-P

6/ rozsah tzv. SCOPES (účelov), o ktoré je aplikácia 3tej strany oprávnená koncového používateľa žiadať a po odsúhlasení s nimi disponovať

**Požadovaný stav**

V zmysle §22a, ods.3 zákona o e-Governmente má správca komunikačnej časti autentifikačného modulu evidovať v registri autentifikačných certifikátov o autentifikačnom certifikáte nasledovné informácie:

* údaje, potrebné na vykonanie identifikácie a autentifikácie s jeho použitím, a to počas celej doby jeho platnosti a vo vzťahu k všetkým **účelom** a informačným systémom, pre ktoré má byť používaný,
* **identifikáciu aplikačného rozhrania** podľa § 25 ods. 7 (vysvetlenie: jedná sa o rozhrania, ktoré je správca ÚPVS a správca špecializovaného portálu povinný vytvoriť a zverejniť za účelom vytvorenia a podanie elektronického podania automatizovaným spôsobom a to pre všetky prípady, v ktorých umožňujú vytvorenie a podanie elektronického podania prostredníctvom používateľského rozhrania; to platí aj pre doplnkové služby k vytváraniu elektronického podania prostredníctvom používateľského rozhrania, ak ich správca ústredného portálu alebo správca špecializovaného portálu vytvára), **údaje o programovom prostriedku**, ktorý má byť na prístup k nemu používaný, **údaje o prevádzkovateľovi programového prostriedku** a **identifikátor osoby** každého, v mene koho je prevádzkovateľ programového prostriedku oprávnený konať, ak má byť autentifikačný certifikát používaný na autentifikáciu na účely podľa odseku 1 prostredníctvom aplikačného rozhrania podľa § 25 ods. 7.

Zjednotenie pojmov

* **účelom** rozumieme rozsah tzv. SCOPES (účelov), o ktoré je aplikácia/systém 3tej strany oprávnená/ý koncového používateľa žiadať a po odsúhlasení s nimi disponovať
* **Identifikáciou aplikačného rozhrania** rozumieme identifikáciu rozhrania (služby) zverejnenej v MUK-P. Z pohľadu ÚPVS služieb sa jedná najmä napr.  EKR, službu pre príjem sk-talk správ typu podanie ale aj volanie služieb ďalších spoločných modulov
* **programovým prostriedkom** rozumieme aplikáciu alebo systém tretej strany pristupujúci k službám zverejneným na MUK-P, prípade v zmysle dohody o integračnom zámere pristupujúci k službám zverejnených na zberniciach ÚPVS.
* **prevádzkovateľom programového prostriedku** rozumieme výrobcu/prevádzkovateľa aplikácie resp. systému tretej strany.

Evidencia údajov v registri autentifikačných certifikátov a súvisiace údaje uložené v MUK-P, OAUTH2 server a IAM už v aktuálnom stave pokrývajú rozsah údajov požadovaný v §22a, ods.3 zákona o e-Governemnte. Výnimkou je evidencia účelov vo vzťahu k identite reprezentovanej autentifikačným certifikátom a vo vzťahu k programovému prostriedku. Z tohto dôvodu bude potrebné dobudovať v OAUTH2 serveri evidenciu scope/identita/aplikácia a súvisiace obslužné procesy. V praxi sa jedná o uloženie zapamätaného rozsahu účelov (SCOPES), ktoré identita odsúhlasila jednotlivým aplikáciám a možnosť získať a zmeniť tieto údaje bezpečným spôsobom.

**Dopady na ÚPVS**

Rozšírenie funkcionality OAUTH2 IAM v zmysle požadovaného stavu

##### **R19-IAM-015** **Autentifikácia klientov komerčných subjektov úradným autentifikátorom**

**Súčasný stav:**

Banky, CDCP a poštový podnik nie sú so zákona oprávnený použiť pre identifikáciu fyzických osôb úradný autentifikátor. Technicky je však možné, aby sa zapojili do konceptu single sign on tým, že budú zaregistrovaný v module IAM ako service provider a naintegrovaný na služby IAM. Takéto zapojenie, však natívne umožňuje presmerovanie prihláseného používateľa na webové portály iných service providerov bez obmedzenia. V konečnom dôsledku by tak používateľ bankového systému po úspešnej autentifikácii fyzickej osoby úradným autentifikátorom  v IAM mohol pristúpiť v mene tejto fyzickej osoby do jej elektronickej schránky (presmerovaním web elektronických schránok).

**Požadovaný stav**

V IAM vznikne nová kategória service providerov, ktorým v prípade úspešného prihlásenia identity v module IAM (cez login obrazovku IAM) bude vydaný špeciálny druh jednorazového tokenu. Takýto token nebude možné použiť v koncepte single sign on a bude slúžiť výhradne pre potreby informačných systémov service providera. Token bude obsahovať identifikátor prihlásenej identity a identifikátor zastupovanej identity, použitý typ autentifikačného prostriedku, jeho QAA level, typ zastupovania a prípadne ďalšie údaje, ktoré sú súčasťou štandardného websso tokenu.

Okrem toho bude potrebné v IAM zriadiť novú službu, ktorá bude publikovaná v MUK-P. Táto služba bude určená výhradne pre banky, CDCP a poštový podnik za účelom získania ďalších údajov. Vstupom do služby bude jednorazový token prihláseného používateľa popísaný vyššie a výstupom budú doplnkové údaje o prihlásenej identite a prípadne aj zastupovanej identite, ktorých identifikátory sú uvedené v tokene. Napríklad:

* údaje týkajúce sa prihlásenej zastupovanej osoby ako:
* rodné číslo (v prípade právnickej osoby IČO)
* meno a priezvisko (v prípade právnickej osoby názov)
* adresa

##### **R19-IAM-016 Autentifikácia alternatívnymi autentifikátormi a zakladanie schránok advokátov**

**Súčasný stav**

IAM je za účelom autentifikácie vybranými autentifikátormi integrovaný na rôzne autentifikačné servery. V procese autentifikácie prostredníctvom vzájomnej integrácie žiada modul IAM tieto servery o vydanie autentifikačného rozhodnutia (protokol SAML2). Finálnym výsledkom autentifikačného procesu v IAM je vydanie tzv. WebSSO SAML2 tokenu, vďaka ktorému je realizovaný koncept jednotného prihlasovania v e-Governmente (single sign on).

Jednotlivé autentifikačné servery, ktoré IAM žiada o vydanie autentifikačného rozhodnutia vystupujú voči IAM v roli IDP (identity data provider), sú zavedené v konfigurácii IAM a sú pre ne stanovené bezpečnostné a komunikačné pravidlá.

Jednotlivé podporované autentifikačné prostriedky sú zavedené v module IAM a majú svoju konfiguráciu – napr. určenie hodnoty QAA levelu. Zároveň sú implementované v konfigurácii jednotlivých SP (service provider), aby bolo možné daný prostriedok zobraziť v prihlasovacej obrazovke vyvolanej daným SP.

Aktuálne je modul IAM za účelom autentifikácie legislatívou stanovenými autenifikačnými prostriedkami integrovaný na nasledovné autentifikačné servery:

* Autentifikačný server pre eID, ktorého správcom je MVSR. Zabezpečuje autentifikáciu nasledovnými prostriedkami:
  + úradný autentifikátor, ktorým je eID kartou, alebo čipové karta povolenia k trvalému pobytu.
  + alternatívny autentifikátor, ktorým je čipová karta vydávaná MVSR zahraničným štatutárom právnických osôb pre prístup k schránke právnickej osoby
* eIDAS NODE, ktorého správcom je Úrad podpredsedu vlády pre informatizáciu. Zabezpečuje autentifikáciu prostriedkom elektronickej identifikácie vydaného v rámci schémy elektronickej identifikácie (eIDAS prostriedok). Autentifikačným serverom je v tomto prípade eIDAS NODE, pre ktorý je autentifikačným serverom systém prevádzkovaný správcom príslušného zahraničného eIDAS prostriedku.

Okrem týchto bol v novele vyhlášky Ministerstva vnútra Slovenskej republiky č. 29/2017 Z. z., ktorou sa ustanovujú podrobnosti o alternatívnom autentifikátore zavedený nový typ alternatívneho autentifikátora. Tým je čipová karta vydávaná MSSR fyzickým osobám (tuzemským i zahraničným) pre prístup k schránke advokáta (ďalej len ako identifikačná karta advokáta). Autentifikačným serverom pre autentifikáciu týmto autentifikátorom je autentifikačný server Ministerstva spravodlivosti SR. Tento autentifikačný server nie je v súčasnosti integrovaný na modul IAM a teda nie je možné použiť identifikačnú kartu advokáta pre prihlásenie do elektronickej schránky advokáta resp. k službám spoločných modulov ÚPVS, resp. zapojenie do konceptu jednotného prihlasovania.

Naviac aktuálne nie je v integrácii IAM na RPO pripojený zoznam advokátov. Zakladanie identít a schránok advokátov v ÚPVS neprebieha automatizovane, prebieha na základe manuálnych importov.

**Požadovaný stav**

Modul IAM bude potrebné naintegrovať na autentifikačný server MSSR po vzore integrácie eID servera MVSR, tak aby bolo umožnené fyzickým osobám prihlasovať sa identifikačnou kartou advokáta. Navyše v súvislosti s tým, bude v IAM potrebné realizovať také úpravy, ktoré zabezpečia, aby bolo  možné jednoduchým spôsobom integrovať ďalšie autentifikačné servery 3tích strán (IDP) protokolom SAML2 a to tak, aby  každá ďalšia integrácia vyvolala minimálne zmeny v IAM, či už v aplikácii alebo v integračných rozhraniach.

Pre naplnenie tejto požiadavky bude potrebné na strane IAM zabezpečiť:

* Možnosť zavedenia nového IDP konfiguračne
* Možnosť zavedenia nového autentifikačného prostriedku konfiguračne s automatickým rozšírením konfigurácie SP o nový autentifikačný prostriedok
* Štandardizácia komunikačného rozhrania medzi IDP a IAM: Komunikácia medzi systémom IDP a modulom IAM bude realizovaná prostredníctvom štandardu SAML2.0. Komunikácia bude šifrovaná a bude prebiehať zabezpečeným kanálom (SSL).
* Štandardizácia procesu jednotného prihlasovania: vydanie webSSO SAML2 tokenu modulom IAM na základe autentifikačného rozhodnutia (tiež SAML2 token) prijatého od autentifikačného servera. SAML2 token generovaný autentifikačným serverom bude štandardizovaný – bude obsahovať PČO (alebo iný dohodnutý identifikátor) autentifikovanej osoby a prípadne ďalšie dohodnuté atribúty (určí detailná analýza, napr. QAA level). Štandardizovaný bude aj scenár neúspešného prihlásenia – t.j.  spôsob akým bude autentifikačný server hlásiť modulu IAM neúspešné prihlásenie

Napriek štandardizácii a rozšíreniu konfigurovateľnosti modulu IAM, bude pri integrácii každého nového IDP potrebné realizovať:

* Úprava login obrazovky: zmena dizajnu obrazovky a integrácia login obrazovky na API IDP (nedá sa totiž predpokladať, že každý IDP bude poskytovať identické integračné rozhrania)
* Práce súvisiace s prepojením infraštruktúry ÚPVS s IDP
* Práce súvisiace s konfiguráciou modulu IAM

Ďalšia požiadavka sa týka procesu zakladania schránok advokátov v ÚPVS. V súvislosti s tým bude potrebné realizovať nasledovné úpravy:

* pripojenie zoznamu advokátov do integrácie IAM s RPO takým spôsobom aby
  + schránky advokátov (a identity) reprezentované IČOm vznikali a boli aktualizované automatizovane na základe dávok z RPO (údaje zo zdrojového registra "Zoznam advokátov")
  + boli automatizovane vytvárané / aktualizované zastupovania na fyzické osoby pre prístup do schránok advokátov (zákonné zastupovania). Podmienkou úspešného vytvorenie zastupovania je existencia fyzickej osoby ako identity v module IAM. Identifikácia tejto osoby v IAM prebehne na základe PČO, ktoré musí byť uvedené v dávke RPO ako štatutár danej identity advokáta (daného IČO). V prípade, že sa jedná o PČO tuzemskej FO (resp. FO s trvalým pobytom), tak je možné predpokladať, že identita s týmto PČO už existuje v IAM – bola v IAM založená jestvujúcou integráciou s RFO. Ak sa však jedná o PČO zahraničnej FO, tak bude nutné na strane ÚPVS upraviť proces spracovania dávky RPO (údaje o advokátoch zo zoznamu advokátov) nasledovne:
    - pre každé PČO overiť, či existuje v IAM identita
    - ak neexistuje, tak zavolať online službu RFO pre získanie údajov o fyzickej osobe
    - založiť identitu v IAM na základe získaných údajov a aj schránku pre túto osobu
    - označiť osobu ako záujmovú osobu v RFO
* proces zakladania schránok advokátov bude podstavený na nasledovných predpokladoch:
  + pri založení zahraničnej FO bude automaticky zároveň zriadená elektronickú schránka obdobne ako je zriaďovaná tuzemským FO
  + bude potrebné ako určiť, ako bude generované URI pre zahraničnú FO, nakoľko nemusí mať v RFO vyplnené rodné číslo. Pri generovaní URI bude potrebné zohľadniť skutočnosť, že v IAM nesmú existovať dve aktívne identity so zhodným URI
  + pri zriaďovaní schránok advokátov bude potrebné stanoviť pravidlá pre tvorbu URI tak, aby v SAK a IAM bolo evidované zhodné URI pre schránku advokáta
* pred pripojením zoznamu advokátov do integrácie IAM s RPO bude potrebné porovnať existujúce údaje o advokátoch v IAM so záznamami o advokátoch v RPO. Prípadné rozdiely v údajoch bude potrebné v IAM dorovnať.

**Dopady na ÚPVS**

MODUL IAM

* realizovať úpravy súvisiace so zjednodušením integrácie autentifikačných serverov 3tích strán (IDP) protokolom SAML2 a to tak, aby  každá ďalšia integrácia vyvolala minimálne zmeny v IAM, či už v aplikácií alebo v integračných rozhraniach. Viď požiadavky v časti "Požadovaný stav"
* porovnať existujúce údajov o advokátoch v IAM so záznamami o advokátoch v RPO. Prípadné rozdiely v údajoch bude potrebné v IAM dorovnať (realizovať migráciu údajov)
* práce súvisiace s pripojením autentifikačné servera MSSR:
  + Úprava login obrazovky: zmena dizajnu obrazovky a integrácia login obrazovky na API IDP (nedá sa totiž predpokladať, že každý IDP bude poskytovať identitické integračné rozhrania)
  + Práce súvisiace s prepojením infraštruktúry ÚPVS s IDP
  + Práce súvisiace s konfiguráciou modulu IAM

IMPORTOOL

* úprava  spracovania záznamov zo zdrojového registra Zoznamu advokátov v dávkach RPO. Viď požiadavky v časti "Požadovaný stav" a s tým súvisiaca:
  + integrácia na služby RFO (pre získanie údajov o identite a pre označenie záujmovej osoby)
  + úprava procesu zakladania zahraničnej fyzickej osoby: generovanie URI FO podľa dohodnutého pravidla

RPO KONEKTOR

* rozšírenie o mapovanie údajov:  dávka zo zdrojového registra Zoznam adokátov v RPO → údaje v štruktúre pre importTool podľa dohodnutých pravidiel a s tým súvisaca analýza údajov RPO

##### **R19-ALL-004 Jednotný postup pri detekcii elektronického formulára**

**Súčasný stav**

Určovanie, či daný objekt v elektronickej správe je elektronický formulár sa definuje na základe class, mimetype, prípadne namespace v XML. Pravidlá sú ale napevno určené v eDesk spracovaní a podobne aj v iných moduloch.

**Požadovaný stav**

Je potrebné tieto pravidlá mať pružnejšie a konfigurovateľné a tak, aby ich jednoducho vedeli použiť aj ostatné moduly, prípadne aj externé subjekty.

**Dopady na ÚPVS**

Potrebné zmeny

* vypracovať pravidlá - aké mimetype, aké namespace určujú elektronický formulár a tieto sprístupniť
* elektronický formulár určovať podľa týchto pravidiel vo všetkých moduloch ÚPVS (eDesk, CUET, MDURZ, ...)

##### **R19-EDESK-002 Optimalizácia služieb modulu eDesk - prechod na mikroslužby**

##### **R19-EDESK-003** **Škálovanie databáz modulu eDesk**

##### **R19-EDESK-004** **Definovanie nezávislých skupín schránok modulu eDesk pre samostatné nasadenie**

**Súčasný stav**

Aktuálne je aplikácia eDesk implementovaná ako monolitická aplikácia využívajúca jednu centrálnu SQL databázu na ukladanie metadát. Neštruktúrovaný obsahu v podobe formulárov a príloh správ sa ukladá v OST. Každý dotaz na čítanie či zápis z/do eDesku či už je realizovaný cez GUI, EKR či interné API pre ktorý sú potrebné metadáta je teda realizovaný voči tejto jednej  SQL databáze.  SQL databáza zo svojej podstaty ako taká natívne nepodporuje horizontálne škálovanie a teda rozloženie do viacerých inštancií. Z toho dôvodu sa často stáva, že databáza je preťažená cez niektorý typ rozhrania a tým sú výrazne spomalené aj ostatné typy rozhraní. Napríklad, ak je vyťažená používateľmi cez GUI a cez EKR spomalia sa tým odozvy interného API na zápis správ do schránok, napr. pri procese elektronického doručovania. Prípadne výrazná komunikácia integrovaného subjektu zo svojou schránkou cez EKR neúmerne spomalí prácu so všetkými ostatnými schránkami. Vo všeobecnosti povedané sa rôzne typy rozhraní vzájomne výkonovo ovplyvňujú. Rovnako sa vzájomne výkonovo ovplyvňuje práca s jednotlivými schránkami a v tomto prípade nie je možné ani rozkladať výkon na prácu s definovanými skupinami schránok.

**Požadovaný stav**

Upraviť existujúce riešenia tak, aby sa jednotlivé typy rozhraní vzájomne výkonovo neovplyvňovali, resp., aby sa toto vzájomné ovplyvňovanie minimalizovalo. Je potrebné dosiahnuť, aby ktorékoľvek z rozhraní poskytujúce služby ÚPVS externým subjektom/používateľom (GUI, EKR) ani v prípade preťaženia nijakým spôsobom nespomalilo API pre vnútorné procesy ÚPVS. Rovnako je potrebné definovať skupiny schránok, ktorých údaje budú uložené v separátnych databázach tak, aby práca so schránkami určených skupiny nemala výkonnostný dopad na prácu zo schránkami iných skupín.

**Dopady na ÚPVS**

Potrebné zmeny

* Návrh a implementácia riešenia zamedzenia výkonovej interakcie jednotlivých rozhraní eDesku
* Návrh a implementácia riešenia zamedzenia výkonovej interakcie jednotlivých pri práci s jednotlivými skupinami schránok
* Analýza služieb poskytovaných aplikáciou
* Návrh štruktúry a granularity mikroslužieb
* Návrh aplikácie s využitím architektúry založenej na mikroslužbách
* Implementácia resp. reimplementácia aplikácie s využitím architektúry založenej na mikroslužbách

##### **R19-EDESK-005 Domigrácia správ z existujúcich schránok modulu eDesk do OST**

**Súčasný stav**

Pri realizácii optimalizácie podľa dodatku č. 5 PRK bola realizovaná implementácia objektového úložiska - OST, do ktorého sú ukladané formuláre a prílohy správ ukladané do eDesku. Táto zmena bola realizovaná tak, že nové úložisko sa používa len pre správy, ktoré boli v eDesku ukladané až po nasadení tejto optimalizácie. Správy v eDesku uložené pred optimalizáciou majú formuláre a prílohy uložené v pôvodnom úložisku realizovanom nad súborovým systémom (FS).

**Požadovaný stav**

Požaduje sa zmigrovať formuláre a prílohy všetkých správ eDesku do nového OST úložiska a zbaviť sa závislosti na FS.

**Dopady na ÚPVS**

* Navrhnúť a implementovať migračnú procedúru z FS do OST s potrebnou úpravou metadát v SQL DB eDesku
* Vykonať migráciu s následným preverením jej úspešnosti

##### **R19-EDESK-008 Použitie OST v konštruktore správ**

**Súčasný stav**

V súčasnosti konštruktor podania pri vytváraní správy vkladá do odosielanej SkTalk správy jej objekty v podobe formulárov a príloh message kontajnera v celom rozsahu a takáto správa je zasielaná na vstupný nárazník. Ten tieto objekty vyberie, vloží do OST a v správe ich nahradí len referenciami z OST, t.j. správu dekomponuje. Tým pádom sú medzi komponentami prenášané veľké objemy údajov, ktoré systém vyťažujú.

**Požadovaný stav**

Požadujeme aby konštruktor správ objekty v podobe formulárov a príloh message kontajnera ešte pred odoslaním na vstupný nárazník uložil do OST a v správe ich nahradil referenciami, teda vykonal dekompozíciu. Až následne takúto dekomponovanú správu zaslal na vstupný nárazník. Rovnaké správanie je potrebné aj na ukladanie rozpracovaných správ v module eDesk.

**Dopady na ÚPVS**

Potrebné zmeny

* Úprava konštruktora správ v súlade s požadovaným stavom.

##### **R19-EDESK-009 Optimalizácia a rozšírenie služieb EKR modulu eDesk**

**Súčasný stav**

Počas existujúcej prevádzky systému vznikla potreba na doplnenie funkcií, ktoré aktuálna sada metód EKR neposkytuje. Jedná sa o funkcionalitu v prípadoch použitia ako je vyhľadávanie podľa viacerých kritérií, stránkovanie, filtrovanie a hromadné akcie. Vykonanie niektorých operácií, za istých okolností pri využití existujúcej sady metód nie je z pohľadu výkonu optimálne, keďže je potrebné veľké množstvo volaní, ktoré zaťažujú systém.

**Požadovaný stav**

Požadujeme rozšírenie metód EKR o funkcionalitu na vyhľadávanie podľa viacerých kritérií, stránkovanie, filtrovanie a hromadné akcie.

**Dopady na ÚPVS**

Potrebné zmeny

* Návrh a implementácia rozšírenie metód EKR o požadovanú funkcionalitu.

##### **R19-DWH-001  Konsolidácia DWH**

**Súčasný stav**

Súčasné riešenie DWH a Reportingu je postavené na platforme MS SQL Server 2012. Nakoľko  Microsoft zabezpečuje suport na 10 ročné obdobie, je nutný pre MS SQL platformu upgrade jednotlivých jeho častí MS DB, SSRS, SSAS, SSIS na novšiu verziu MS SQL server 2017 pre zachovanie bezpečnostných štandardov a aktuálnosti SW vybavenia. Upgrade SW vybavenia. DWH momentálne pokrýva údaje prevažne z modulov G2G, modulu IAM a eDESK .V rámci nových požiadaviek na rozšírenie DWH budú do dátového skladu spracované dáta z modulov MED CUD a MUK-P.

**Požadovaný stav**

Kvôli plánovaným zmenám zdrojových systémov je nutné prerobiť importné loady, ETL procesy, prípadne štruktúru stage vrstvy DWH na nový zdroj, ktorým bude ElasticSearch prípadne Kafka. Takéto riešenie uľahčí zaťaženiu primárnych systémov pri každodennom loade dát do DWH.

Rozšírenie riešenia o ďalšie dáta

Modul eDESK: Bude vytvorený proces pre spracovanie dát z modulu eDesk do dátového skladu, ktorý zabezpečí load, transformáciu a historizáciu a prípravu dát pre následný Reporting (relačná schéma prípadne OLAP).

Modul MED-CUD: Bude vytvorený proces pre spracovanie dát z modulu CUD do dátového skladu, ktorý zabezpečí transformáciu a historizáciu dát týkajúcich sa evidovaných podaní a ich stavov. Na základe požiadaviek bude následne z dát uložených v DWH vytvorená OLAP kocka pre multidimenzionálnu analýzu dát. Dáta z DWH bude možné využívať aj na vytváranie reportov a ich pravidelnú distribúciu napr. pre export reportov a súborov pre rôzne inštitúcie.

Modul MUK-P: Bude vytvorený proces pre spracovanie dát z modulu MUK-P do dátového skladu, ktorý zabezpečí transformáciu a historizáciu dát týkajúcich sa volaní služieb a ich konzulmentov a poskytovateľov. Na základe požiadaviek bude následne z dát uložených v DWH vytvorená OLAP kocka pre multidimenzionálnu analýzu dát. Dáta z DWH bude možné využívať aj na vytváranie reportov a ich pravidelnú distribúciu napr. pre export reportov alebo datasetov.

Modul IAM: existujúci export údajov z IAM bude rozšírený o ďalšie údaje, ktoré majú význam pre budúcu tvorbu reportov alebo pre vypracovanie analýz údajov a štatistík.

Dátový sklad a jeho báza údajov ma rastúcu tendenciu. Vzhľadom na to, že do DWH budú pritekať aj iné zdroje údajov bude nutné rozšírenie diskového priestoru.

Optimalizácia spracovania DWH (partitioning)

Vzhľadom na stále väčšie nároky na rýchlosť spracovania a rastúceho objemu dát v DWH, sú požadované zmeny architektúry na úrovni dátových štruktúr DWH. Zavedením partitioningu tabuliek v rámci DWH s očkávaným nasledovným prínosom:

* Ľahší manažment dát – urýchlenie práce s dátami
* Prehľadnejší backup/recovery – netreba narábať s obrovskými tabuľkami
* Faktové tabuľky môžu narásť do väčších objemov dát

Optimalizácia spracovania a prístupu k dátam (relačným a OLAP)

Je požadované sprístupnenie a prezeranie aj relačných dát obsiahnutých v rámci DWH pomocou prezentačnej vrstvy. Súčasné OLAP databázy obsahujú rádovo desiatky GB dát ročne, preto je nutná aj optimalizácia spracovania OLAPu. V rámci optimalizácie spracovania relačných dát a OLAPu bude cieľovým stavom spracovanie dát v DWH a aktualizácia OLAP kociek a dimenzií v nižšej granularite (napr. dennej báze).

Prezentačná vrstva

Rozšírenie prezentačnej vrstvy o relačné prezeranie dát (ktoré napomôže skoršiemu dohľadávaniu dát (denné)), automatizované reporty a analytický nástroj. Analytický nástroj bude slúžiť ako alternatívny nástroj k súčasnému riešeniu MS Excelom pre prezeranie MS OLAP kociek, tvorenia analýz. Takisto bude využívaný na účely relačného reportingu nad menším množstvom dát. MS Reporting Services – bude slúžiť na vytvorenie zoznamov údajov (list reportov) s preddefinovanými filtrami z relačných dát. Vhodné aj pre vytvorenie a následne zasielanie pravidelných reportov nad relačnými ako aj OLAP štruktúrami.

##### **R19-MON-001**  **Vytvorenie zobrazenia pre MUK-P a prípadné ďalšie nové komponenty**

**Súčasný stav**

V rámci centrálneho monitorovacieho nástroja sú okrem štandardných zobrazení monitorovaných parametrov definované špeciálne vlastné informačné panely pre jednotlivé moduly, ktoré zobrazujú špecifické monitorované vlastnosti systému.

**Požadovaný stav**

Je nutné navrhnúť a špecifikovať vlastné informačné panely pre modul MUK-P a prípadné nové komponenty, ktoré vzniknú počas implementácie. Implementovať zber špecifických monitorovaných vlastností systému a prehľadne ich zobraziť v informačnom panely.

### Časť Diela - Mobilná aplikácia MeID

**Súčasný stav**

V súčasnom stave nie je možné prihlásiť sa do elektronickej schránky  pomocou mobilného zariadenia. Používateľ je pre prihlasovanie nútený používať eID kartu s čítačkou (prípadne iný úradný alebo alternatívny autentifikátor) a musí mať na svojom zariadení nainštalovaný obslužný SW.

**Požadovaný stav**

Umožniť používateľovi prihlásiť sa autentifikačným certifikátom cez špecializovanú mobilnú aplikáciu pre prihlasovanie (mID NASES) inštalovanú v mobilnom zariadení. Požiadavky týkajúce sa mID NASES:

* dizajn má byť intuitívny, vytvorený v súlade so všeobecne platnými štandardmi pre tvorbu mobilných aplikácii danej platformy (iOS, android). NASES v spolupráci s UPVII dodá dizajn manuál pre tvorbu grafického rozhrania mobilných aplikácií
* zabezpečiť, dostupnosť mID NASES cez distribučné kanály podporovanej mobilnej platformy: app store pre iOS, google play pre Android. Dostupnosť mID NASES pre windows mobile nie je predmetom tejto požiadavky
* zabezpečiť generovanie autentifikačného certifikátu a uloženie privátneho kľúča certifikátu v úložisku na mobilnom zariadení
* integrácia na IAM / CRAC za účelom registrácie mobilného zariadenia a autentifikačného certifikátu
* integrácia na IAM oAuth2 za účelom prihlásenia
* poskytnúť rozhranie pre MA3S za účelom overenia údajov o identite a s tým súvisiaca integrácia na IAM za účelom poskytnutia údajov o identite
* podporu viacerých používateľov pracujúcich cez profily na jednom mobilnom zariadení (každému používateľovi - FO je vygenerovaný vlastný autentifikačný certifikát s ktorým je možné sa prihlásiť)
* lokalizácia aplikácie v slovenskom a anglickom jazyku

Umožniť používateľovi zobraziť obsah elektronickej schránky prostredníctvom samostatnej špecializovanej mobilnej aplikácie (mEdesk) nainštalovanej v mobilnom zariadení. Požiadavky na mEdesk:

* dizajn má byť intuitívny, vytvorený v súlade so všeobecne platnými štandardmi pre tvorbu mobilných aplikácii danej platformy (iOS, android). NASES v spolupráci s UPVII dodá dizajn manuál pre tvorbu grafického rozhrania mobilných aplikácií
* zabezpečiť, dostupnosť mEdesk cez distribučné kanály podporovanej mobilnej platformy: app store pre iOS, google play pre Android. Dostupnosť mEdesk pre windows mobile nie je predmetom tejto požiadavky
* pre prihlásenie používateľa bude využívať prihlásenie cez mobileID (mobileID NASES alebo mobileID DEUS)
* umožní zobraziť zoznam priečinkov
* umožní zobraziť zoznam správ v jednotlivých priečinkoch
* umožní zobraziť detail vybranej správy s podporou prechodu na predchádzajúcu / ďalšiu správu
* umožní používateľovi prihlásiť sa v mene iného subjektu podľa existujúcich zastupovaní v IAM a prezerať obsah schránky tohto subjektu.
* umožní v manuálnom i automatickom režime (pri spustení a na pozadí v definovaných časových intervaloch) aktualizáciu obsahu schránky o novo prijaté správy
* umožní prevzatie doručovanej správy autorizáciou doručenky: používateľ bude po zvolení možnosti prevziať správu nad notifikačnou doručenku vyzvaný na dodatočnú autentifikáciu. Po úspešnom prihlásení mEdesk zavolá EKR službu autorizácie doručenky
* bude integrovaná na mechanizmus push notifikácii cez zabudovanú službu push notifikácie v iOS a android. Cieľom je aby, bol používateľ v mobilnom zariadení informovaný push notifikáciou o uložení novej správy v schránke.
* lokalizácia aplikácie v slovenskom a anglickom jazyku

**Dopady na UPVS**

**Vytvorenie mobilnej aplikácie mID, ktorá bude obsahovať**

* funkcionalitu generovania autentifikačného certifikátu a ukladania privátneho kľúča v úložisku mobilného zariadenia, s podporou viacerých používateľov pracujúcich cez profily na jednom mobilnom zariadení (každému používateľovi - FO je vygenerovaný vlastný autentifikačný certifikát)
* integráciu na IAM / CRAC za účelom registrácie a odregistrácie mobilného zariadenia a autentifikačného certifikátu v zmysle diagramov uvedených v časti dopady na IAM a CRAC
* integráciu na IAM oAuth2 cez openID connect ako oAuth2 klient za účelom prihlásenia v zmysle diagramov uvedených v časti dopady na IAM a CRAC
* rozhranie pre MA3S za účelom získania údajov o identite a s tým súvisiaca integrácia na IAM za účelom poskytnutia údajov o identite v zmysle diagramov uvedených v časti dopady na IAM a CRAC
* aplikácia bude vytvorená pre mobilné zariadenia na platforme: Android, iOS
* lokalizácia aplikácie v slovenskom a anglickom jazyku.

**Vytvorenie mobilnej aplikácie mEdesk**

* GUI pre prezeranie obsahu schránky v zmysle požiadaviek
* integrácia na EKR služby registrované v MUK-P pre získanie zoznamu priečinkov, zoznamu správ, detailu správy a pre vykonanie autorizácie doručenky. Pri autorizácii doručenky bude používateľ vyzvaný na dodatočnú autentifikáciu. Po úspešnom prihlásení mEdesk zavolá EKR službu autorizácie doručenky
* integrácia na mechanizmus push notifikácii cez zabudovanú službu push notifikácie v iOS a android. Zaregistrovanie k odberu push notifikácii (subscriber) - po inicializácii aplikácie zaregistruje pre odber notifikácií o nových správach pre danú schránku . Spracovanie push notifikácie - po kliknutí používateľa na notifikáciu presmerovanie používateľa do mEdesk, pričom po štarte mEdesk dôjde k synchronizácii nových správ cez EKR.
* registrácia mEdesk ako oAuth2 klient s integráciou na openIDconnect za účelom prihlasovania a integráciou na službu zmeny zastupovania. mEdesk umožní používateľovi prihlásiť sa v mene iného subjektu podľa existujúcich zastupovaní v IAM a prezerať obsah schránky tohto subjektu.
* aplikácia bude vytvorená pre mobilné zariadenia na platforme: Android, iOS
* lokalizácia aplikácie v slovenskom a anglickom jazyku.

### Časť Diela eDESK - 2019

Zoznam požiadaviek eDesk – 2019 je uvedený v tabuľke.

| **Požiadavka** | **Názov požiadavky** | **Popis** | **Legislatíva** | **Závislosť** |
| --- | --- | --- | --- | --- |
| R19-EDESK-014 | Zriadenie schránky pre maloletých na žiadosť | Vytvorenie nových žiadostí, procesu a pravidiel zakladania identít a schránok pre danú skupinu používateľov. | § 12 ods. 4 písm. d) |  |
| R19-EDESK-015 | Zriaďovanie schránok na žiadosť OVM v rozsahu ustavnovenom osobitným predpisom | Vytvorenie nových žiadostí, procesu a pravidiel zakladania identít a schránok pre danú skupinu používateľov. | § 12 ods. 6 |  |

##### **R19-EDESK-014** **Zriadenie schránky pre maloletých na žiadosť**

**Súčasný stav**

Doteraz boli schránky fyzických osôb zriaďované automaticky po dosiahnutí 18. roku veku na základe informácií a údajov z referenčného registra (register fyzických osôb).

**Požadovaný stav**

Je potrebné zabezpečiť možnosť zriadenia schránky aj maloletým osobám a to na základe žiadosti a za podmienok definovaných v zákone o e-Governmente (autorizácia žiadosti o zriadenie schránky a následné úkony spojené so správou schránky musia byť autorizované rodičmi alebo zákonným zástupcom maloletého). Na základe uvedeného je potrebné pripraviť žiadosti (elektronické formuláre v anonymnom a neanonymnom režime) a funkcionalitu na podporu zriaďovania schránok aj pre osoby mladšie ako 18 rokov (rozšírenie a úprava integrácie na referenčný register RFO).

**Dopady na ÚPVS**

MEF - žiadosť o zriadenie schránky s uvedením všetkých potrebných náležitostí - bude confirm-ovaná  
G2G - spracovanie pre vytvorenie schránky maloletej osoby  
G2G/IAM - integrácia na RFO pre označenie záujmovej osoby  
IAM - označenie osoby v IAM, aby sa neprebili zákonní zástupcovia po nahlásení údajov z RFO  
IAM - prechod na normálnu schránku (zmena zákonných zástupcov (zrušenie existujúcich + nastavenie samého seba; odstránenie vyššie uvedeného označenia v IAM) po dovŕšení 18 roku

##### **R19-EDESK-015 Zriaďovanie schránok na žiadosť OVM v rozsahu ustanovenom osobitným predpisom**

**Súčasný stav**

Elektronické schránky zriaďuje správca elektronických schránok aj na základe žiadosti. Jedná sa však vždy o zriaďovanie schránky na žiadosť MAJITEĽA schránky (OVM) a musí sa jednať o situácie popísané v ustanoveniach zákona o e-Governmente. Ide najmä o prípady zriadenia schránky nezapísanej organizačnej zložky na účely doručovania, zriadenie schránky pre osoby, ktoré sa nezapisujú do zákonom stanovenej evidencie a pod.

**Požadovaný stav**

Sprístupnenie žiadostí pre orgány verejnej moci, ktoré v rozsahu ustanovenom osobitným predpisom (Slovenská informačná služba) plní úlohy vo veciach ochrany ústavného zriadenia, vnútorného poriadku a bezpečnosti štátu, a to na účely plnenia jeho úloh. Za týmto účelom vznikne elektronická žiadosť, prostredníctvom ktorej úrad so špecifickým oprávnením (rolou) vyplní údaje o novej elektronickej schránke požadovaného typu (fyzická osoba, fyzická osoba podnikateľ, právnická osoba, OVM) a odošle ju na ÚPVS. Ďalej vznikne elektronický formulár žiadosti o zrušenie takto zriadenej elektronickej schránky - rovnako platí, že žiadosť môže vyplniť a odoslať len úrad so špecifickým oprávnením (rolou). Obe žiadosti budú odosielané do elektronickej schránky správcu ÚPVS. Samotné zriadenie schránky nebude realizované automaticky, ale bude realizované zásahom L2 (napr. z dôvodu špecifických požiadaviek na schránku: určenie špecifického identifikátora schránky, špecifického stavu schránky a pod).

Súčasťou žiadosti o zriadenie schránky budú aj údaje o zákonnom zástupcovi.

**Dopady na ÚPVS**

MEF - vytvorenie a registrácia nových formulárov (žiadosť o vytvorenie a zrušenie elektronickej schránky)

G2G - zriadenie a konfigurácia nových tried správ

IAM - zriadenie špecifickej role a jej priradenie oprávnenému OVM

### Časť Diela CEP - 2017

Zoznam požiadaviek CEP – 2017 je uvedený v tabuľke.

| **Požiadavka** | **Názov požiadavky** | **Popis** | **Legislatíva** | **Závislosť** |
| --- | --- | --- | --- | --- |
| R19-CEP-002 | Autorizácia klikom | Vytvorenie novej funkcionality na autorizáciu v rámci centrálneho podpisového komponentu. | § 23 ods. 1 | R19-IAM-007 |
| R19-CEP-031 | Zosúladenie obsahu Úplného overenia podpisov s obsahom Informatívneho overenia podpisov | Zjednotenie a zosúladenie formátu správ o výsledku overenia podpisov. |  | R19-CEP-002 |

##### **R19-CEP-002 Autorizácia klikom v CPK**

**Súčasný stav**

Funkcionalita autorizácie klikom nie je momentálne na ÚPVS poskytovaná. Existuje obdobná funkcionalita modulu eDesk - autorizácia opakovaným prihlásením (a zadaním BOK), ktorú ÚPVS interne využíva pre potvrdenie doručenky a autorizáciu technických žiadostí typu aktivácia elektronickej schránky na doručovanie. Vyžadovaný spôsob autorizácie je evidovaný v Lokátore služieb ako súčasť údajov o registrovanej službe. Podporované možnosti sú: buď KEP/KEPe alebo opakované prihlásenie.

**Požadovaný stav**

Poskytnutie novej funkcionality za účelom autorizácie elektronických podaní na prístupových miestach osobami, ktoré nie sú orgánmi verejnej moci. V zmysle zákona o e-Governmente ÚPVS ako prístupové miesto má umožniť  fyzickým a právnickým osobám autorizáciu elektronického podania klikom a to v prípade, ak tento zákon neustanovuje iný spôsob autorizácie alebo ak je podľa osobitného predpisu náležitosťou podania vlastnoručný podpis. Nová funkcionalita má zabezpečiť autorizáciu tak, aby bola dostupná po úspešnej autentifikácii osoby (zodpovedajúcej najmenej úrovni zabezpečenia pokročilá), nemennosť obsahu autorizovaného dokumentu do momentu uloženia v elektronickej schránke adresáta, spojenie autorizovaného dokumentu s identifikátorom osoby odosielateľa a zachovanie väzby medzi nimi. Povinnosť uvádzania autentifikovanej osoby ako odosielateľa elektronickej správy je požadovanou funkcionalitou prístupového miesta.

Cieľom požadovaného riešenia je realizovať taký koncept, ktorý by:

* sprístupnil autorizáciu klikom prístupovým miestam ako funkciu centrálneho komponentu. Súčasťou konceptu je preto aj vybudovanie centrálneho podpisového komponentu (CPK), ktorá by v prvej fáze centrálne zabezpečovala autorizáciu klikom. Koncept CPK je potrebné navrhovať s ohľadom na potrebu neskoršieho rozširovania CPK o nové autorizačné funkcie (nie je súčasťou tejto požiadavky). Jedná sa napríklad o podpisovanie KEPom prostredníctvom integrácie s klientskymi podpisovačmi, vyhotovenie elektronickej pečate a pod. CPK by teda mala poskytnúť potrebné rozhrania umožňujúce prístupovým miestam integráciu svojich systémov a umožniť im tak využívanie jej autorizačných funkcií.  Tým sa docieli to, že prístupové miesta nebudú nútené budovať a prevádzkovať vlastné riešenia.
* funkciu autorizácie klikom realizoval spôsobom, ktorý bude minimalizovať dopady na IS VS a v maximálnej miery využije jestvujúce princípy a služby - najmä  v oblastí podateľní.

Požiadavky na funkcionalitu CPK:

* vytvorenie a sprístupnenie sady webových služieb cez MUK-P pre prístupové miesta primárne za účelom nahratia dokumentov určených k autorizácii a prevzatie autorizovaných dokumentov (výsledok autorizácie). Prípadne ďalšie, ktoré určí detailná analýza.
* CPK bude budovaná ako webová aplikácia s responzívnym používateľským rozhraním. Podklady dodá NASES v spolupráci s ÚPVII obdobne ako v prípade redizajnu eDesk: dizajn manuál, html šablóny, štýly..
* CPK bude registrovaná ako oauth2 klient s openID connect na  IAM za účelom prihlásenia používateľa resp. za účelom zapojenia CPK do IAM single sign on pre oAuth2. To predpokladá rozšírenie funkcionality IAM v zmysle požiadavky R19-IAM-007 , časť Dopady na ÚPVS → Ďalšie rozšírenia funkcionality týkajúce sa prihlásenia cez mobileID
* CPK umožní používateľovi autorizáciu klikom. Proces autorizácie klikom bude prebiehať nasledovným spôsobom (poznámka: v prípade ÚPVS sa prístupovým miestom rozumie konštruktor správ):
  1. prístupové miesto nahrá predmetné dokumenty do CPK prostredníctvom integrácie s CPK. Súčasťou sú aj meta údaje nevyhnutné pre vykonanie autorizácie klikom napr. ID odosielateľa správy, a pod (ďalšie určí detailná analýza).
  2. prístupové miesto presmeruje používateľa na používateľské rozhranie CPK. Ak bol používateľ prihlásený, tak aj v CPK ostáva prihlásený: CPK ako oauth2 klient je integrovaný na IAM oauth2 server
  3. CPK zobrazí používateľovi názvy dokumentov s možnosťou ich vizualizácie. Vizualizácia podpisovaného elektronického formulára (typicky podania) bude zabezpečená aplikovaním podpisovej transformácie. Vizualizácia iného elektronického dokumentu bude realizovaná nasledovne: Zobrazený bude iba názov súboru s možnosťou stiahnutia. S obsahom dokumentu sa môže používateľ oboznámiť tak, že si elektronický dokument stiahne a vizualizuje jeho obsah v asociovanej aplikácii v závislosti od formátu dokumentu
  4. používateľ v CPK zvolí možnosť autorizácie klikom
  5. CPK požiada  o opakovanú autentifikáciu  prostredníctvom login obrazovky IAM. Výsledkom je, že CPK získa tzv. AA token. To predpokladá rozšírenie IAM o funkcionalitu o opakovanej autentifikácie pre oAuth2 v zmysle požiadavky  R19-IAM-007  . V rámci budúcich plánovaných rozvojov bude AA token podpisovaný kvalifikovaným podpisom (nie je súčasťou tejto požiadavky), viď dopady na IAM v  **R19-EDESK-001**
  6. CPK preverí, že subjectID v tokene z bodu 5 korešponduje s odosielateľom správy
  7. CPK vyplní formulár autorizačnej doložky, pričom použije údaje z tokenu z bodu 5. Formulár autorizačnej doložky bude za týmto účelom vytvorený a zaregistrovaný v module eForm a bude obsahovať najmä údaj o identifikátore identity (napr. meno, priezvisko, identifikátor, typ identifikátora, krajina vydávajúca identifikátor), QAA level, typ autentifikačné prostriedku a prípadne ďalšie údaje získateľné z tokenu, prípadne element kde bude možné uviesť zdokonalený podpis (alebo iný) alebo prípadne celý token z bodu 3 pre účely dokazovania prípadných sporov, pričom potrebu uvádzania tokeny určí detailná analýza
  8. CPK prostredníctvom služby CEP - serverové podpisovanie vykoná spoločnú autorizáciu dokumentov spoločne s vyplneným formulárom doložky za použitia na to dedikovaného kvalifikovaného certifikátu elektronickej pečate. Ten si za týmto účelom vygeneruje NASES v module HSM. Výsledkom spoločnej autorizácie bude štandardný ASiC podpisový kontajner v zmysle EIDAS. CPK uloží autorizovaný dokument vo svojom úložisku
  9. CPK zaloguje vykonanie autorizácie klikom: najmä identifikátor správy, token, identifikátor identity, dátum a čas vykonania autorizácie, prípadne iné údaje, ktorú budú identifikované počas detailnej analýzy
  10. prístupové miesto vyžiada od CPK autorizovaný dokument
* Funkcia autorizácie klikom ďalej umožní:
  1. podpísať klikom už raz autorizovaný dokument, pričom predchádzajúca autorizácia mohla byť vykonaná nasledovnými spôsobmi. Prípadné obmedzenia pre úspešný vykonanie takejto autorizácie klikom sú dané aktuálnymi možnosťami serverovej podpisovacej služby modulu CEP
     + PaDES
     + ASiC XaDES
     + ASiC CaDES
     + ASiC XaDES, ASiC CaDES obsahujúci autorizáciu klikom. V tomto prípade CPK pri autorizácii klikom doplní ďalšiu autorizačnú doložku
* Predmetom požiadavky nie je vytvorenie mobilnej aplikácie podporujúcej autorizáciu klikom.
* Ďalšie funkcie dostupné na používateľskom rozhraní: zobrazenie informácií o podpise

Požiadavky na funkcionalitu ostatných modulov:

* bude potrebné vytvoriť nové služby pre overenie autorizácie klikom v službách úplného overenia (i ako výsledok služby zaevidovania podania) a informatívneho overenia a tým súvisiace rozšírenie výstupu týchto služieb a reintegrovať existujúce moduly ÚPVS (G2G, eDesk, MDURZ) na tieto nové služby.
* na prístupovom komponente bude sprístupnená nová služba informatívneho overenia podpisov za účelom overenia aj autorizácií klikom.
* bude potrebné upraviť evidenciu Lokátora služieb tak, aby bolo možné definovať nové typy autorizácie (integrácia na novozriadený spoločný číselník) a túto informáciu poskytovať cez služby Lokátora služieb. Doplniť do POSP o možnosť určiť požadované typy autorizácie ako rozšírenie súčasnej možnosti vyžadovania prítomnosti KEP/KEPe.
* bude potrebné upraviť eDesk (konštruktor správ) tak, aby pri podaniach poskytoval tie možnosti autorizácie, ktoré zodpovedajú požadovaným typom autorizácie, ktoré sú pre danú službu povolené v Lokátore služieb a ktoré majú funkčnú podporu v konštruktore správ. V tomto zmysle bude potrebné upraviť aj autorizačnú službu G2G.  Pre vykonanie autorizácie klikom bude potrebné eDesk (konštruktor správ) integrovať na rozhrania CPK

**Dopady na ÚPVS**

CPK:

Implementovať komponentu CPK ako webovú aplikáciu v zmysle požiadaviek uvedených v časti "požadovaný stav":

* vytvorenie rezponzívneho GUI podľa podkladov (dizajn manuál, šablóny, štýly) od NASES
* vytvorenie integračných rozhraní a ich sprístupnenie cez MUK-P, konečná sada potrebných rozhraní bude vyšpecifikovaná v detailnej analýze:
  + Štart session
  + Nahratie dokumentov k autorizácii
  + Prevzatie autorizovaných dokumentov (výsledok autorizácie)
* integrácia na IAM oAuth2 server ako oAuth2 klient pre:
  + prihlásenie používateľa
  + zapojenie do websso
  + dodatočnú autentifikáciu
* integrácia na IAM službu STS za účelom získania STS tokenu pre volanie služieb na internej zbernici ÚPVS vyžadujúcich autorizáciu STS tokenom
* integrácia ma modul eForm za účelom vizualizácie elektronických formulárov
* integrácia na CEP:
  + serverová služba podpisovania
  + vrátenie podpísaných údajov
  + zistenie typu a formátu podpisu
  + informatívne overenie podpisu (nová služba)
* prípadne podporné nástroje/knižnice CEP pre prácu s ASiC ako napr. Asic factory ak to bude potrebné pre viacnásobnú autorizáciu
* integrácia na OST a centrálny log

CEP

* nové služby pre overenie autorizácie klikom v službách úplného overenia (ako výsledok služby zaevidovania podania) a informatívneho overenia a tým súvisiace rozšírenie výstupu týchto služieb. Pri overení sa bude kontrolovať, či pečať boha vyhotovená niektorým z povolených certifikátov - module CEP bude obsahovať zoznam povolených certifikátov. Síce sa počíta s tým, že pri autorizácii klikom sa vždy použije jeden certifikát, ktorý si NASES/UPVII vygeneruje v HSM, avšak v dôsledku exspirácie bude potrebné evidovať v CEP viacero certifikátov

EDESK (konštruktor správ)

* poskytovať všetky typy autorizácie, ktoré povoľuje definícia služby v LS a ktoré majú podporu v konštruktore správ
* reintegrácia na LS: rozšírený výstup služieb o požadované typy autorizácie
* integrácia na CPK pri autorizácii klikom podľa popisu (proces) tejto funkcie v časti "Požadovaný stav"
* možnosť odobratia autorizácie klikom
* reintegrácia na novú službu informatívneho overenia podpisov

ELEKTRONICKÉ FORMULÁRE

* vytvorenie nových el. formulárov pre zobrazenie výsledku úplného a informatívneho overenia a ich registrácia v MEF
* vytvorenie a zaregistrovanie elektronického formulára autorizačnej doložky v MEF
* rozšírenie POSP o možnosť určiť požadované typy autorizácie a jeho nasadenie v MEF

LOKÁTOR SLUŽIEB

* úprava dátového modelu a rozhraní poskytujúcich informácie o službách a inštanciách z dôvodu zavedenia číselníka autorizácií
* integrácia na spoločný číselník typov autorizácie

G2G

* úprava autorizačnej služby o overovanie autorizácie podania voči požadovaným typom, ktoré sú definované v POSPe formulára
* reintegrácia na novú službu informatívneho overenia podpisov, úplného overenia podpisov a a zaevidovania podania s novým typom odpovede

PRÍSTUPOVÝ KOMPONENT

* rozšírenie jestvujúcej služby, ktorá umožňuje na používateľskom rozhraní zavolať službu informatívneho overenia KEP a zobraziť výsledok a to preintegrovaním na novú službu informatívneho overenia KEP

MDURZ:

* reintegrácia na novú službu úplného overenia podpisov
* reintegrácia na novú službu informatívneho overenia podpisov

SPOLOČNÉ ČÍSELNÍKY

* konfigurácia nového číselníka typov autorizácie

##### **R19-CEP-031 Zosúladenie obsahu Úplného overenia podpisov s obsahom Informatívneho overenia podpisov**

**Súčasný stav**

Na úrovni xml sú obsahy rozdielne. ISIGN\_VERIFY\_RESULT (PrijatieVysledkuOverenia, PrijatieVysledkuOverenia4) a Informatívne overenie 3.

**Požadovaný stav**

CEP musí zabezpečiť zjednotenie formátu správ o výsledku (asynchrónneho/synchrónneho) predbežného/úplného overenia elektronického podpisu, alebo časovej pečiatky a informatívneho overenia (synchrónna služba). Súčasťou je teda aj uvádzanie zoznamu referencií na podpísané biznis objekty, aby v prípade spoločnej autorizácie boli vo výsledku overenia uvedené údaje o popise iba raz aj keď ním bolo autorizovaných viac biznis objektov. V prípade viacnásobnej autorizácie je potrebné uvádzať údaje o podpísanom biznis objekte iba raz, aj keď bol autorizovaný viacerými podpismi.

**Dopady na ÚPVS**

Potrebné zmeny

* zjednotenie schém - ale až po zapracovaní všetkých zmien
* zapracovanie rozšírenej schémy úplného overenia MDURZ, MED (časť CUD)