Príloha č. 1 – Opis predmetu zákazky

Opis predmetu zákazky

Verejný obstarávateľ: Národná agentúra pre sieťové a elektronické služby

Názov zákazky: **„Vytvorenie a nasadenie Komponentu sprístupňovania doručovaných rozhodnutí“**

TRVANIE:
Termín dodania je do **14 mesiacov** od účinnosti Zmluvy.

KOMPLEXNOSŤ:
Hospodársky subjekt je povinný predložiť ponuku na celý predmet zákazky.

Zoznam skratiek

Tabuľka 1 - Zoznam skratiek

skratka	popis
API GW	Brána API - prijíma všetky volania API od klientov a potom ich smeruje do príslušnej mikroslužby
CEER	Centrálna evidencia elektronických rozhodnutí
CEP	Centrálna elektronická podateľňa
CUD	Centrálne úradné doručovanie (modul elektronického doručovania ÚPVS)
CUET	Centrálna elektronická úradná tabuľa
eDesk	Modul elektronických schránok ÚPVS
eIDAS	electronic IDentification, Authentication and trust Services - nariadenie Európskej únie č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom európskom trhu
EK	Európska komisia
ETL	Extract, transform, load (programovací nástroj súvisiaci s databázami)
EUD	Elektronický úradný dokument
FIX	Testovacie prostredie
GUI / UI	Graphic user interface (grafické používateľské rozhranie)
IAM	Autentifikačný modul ÚPVS
IDP	Identity provider
IOMO	Integrované obslužné miesto občana
IS	Informačný systém
KSDR	Komponent sprístupňovania doručovaných rozhodnutí
MEF	Modul elektronického formulára
MetaIS	Centrálny metainformačný systém verejnej správy
MoID	Mobilné ID
OP II	Operačný program integrovaná infraštruktúra
OST	Úložisko ÚPVS
OVM	Orgán verejnej moci
OWASP	Open Web Application Security Project
PROD	Produkčné prostredie
SNCA	Slovenská národná certifikačná autorita
SP	Service provider

Východisková situácia a zámer vytvorenia KSDR

Projekt je súčasťou reformy v zmysle reformného zámeru Transparentné rozhodovanie vo verejnej správe – fáza I (nový prístup k rozhodnutiam verejnej správy), schváleného 12.3.2018. Bude prvým z komponentov systému Centrálnej evidencie elektronických rozhodnutí (ďalej len CEER) - tzv. Komponent zdieľania doručovaných rozhodnutí (ďalej len KSDR). Projekt bude prvým krokom k naplneniu tejto reformy.

V KSDR bude na jednom mieste pre občana a podnikateľský subjekt zjednodušeným spôsobom dostupný prehľad o všetkých elektronických úradných dokumentoch (rozhodnutiach), ktoré verejná správa doručuje prostredníctvom IS CÚD (Informačný systém centrálneho úradného doručovania).

V tomto kontexte je realizácia hlavných aktivít projektu vo vecnom súlade s B. Zavedením inovatívnych elektronických služieb VS pre občanov a podnikateľovi v zmysle oprávnených aktivít OPII v rámci špecifického cieľa 7.3 a 7.4., pretože umožní pre občanov, podnikateľov a tretie osoby inovatívnym spôsobom zvýšiť efektívnosť, výkonnosť a kvalitu služieb pre vyhľadávanie, zobrazovanie, zdieľanie a sprístupňovanie právoplatných rozhodnutí všetkým zainteresovaným stranám. Táto skutočnosť sa prejaví najmä zvýšením počtu vybavených rozhodnutí a znížením času potrebného na vybavenie veci. Druhým, rovnako dôležitým cieľom je zvýšenie kvality a nezávislosti prijímania rozhodnutí, ako aj zníženie počtu chýb pri prijímaní rozhodnutí.

V súčasnosti sa k rozhodnutiam občan alebo podnikateľský subjekt dostane troma spôsobmi: sú mu doručené vo forme elektronického dokumentu do elektronickej schránky, sú mu poštou doručené ako úradný list alebo sú mu poštou doručené ako rovnopis elektronického dokumentu.

Pre orgány verejnej moci je zákonná povinnosť všetky úradné dokumenty doručovať v elektronickej podobe, takže po splnení si zákonných povinností zo strany všetkých OVM, alternatíva doručenia úradného listu v listinnej podobe v réžii OVM prestane byť aktuálna, preto ju ďalej nerozoberáme.

Nedostatkami súčasného riešenia sú:

- rozhodnutia (úradné dokumenty) sú distribuované u pôvodcov a adresátov;
- rozhodnutia doručené do elektronickej schránky sa nedajú preposielať v ľahko čitateľnej a zároveň bezpečnej podobe;
- rozhodnutia zasielané vo forme rovnopisov neobsahujú tradičné autorizačné prvky (pečiatka, podpis, nerozdeliteľné viazanie a podobne);
- pri rozhodnutiach, ktoré sú vytvárané bez zápisu do registra resp. zákonnej evidencie je ich potrebné predkladať úradom, čím je popretý princíp „Jedenkrát a dosť“.

Nedostatky neovplyvňujú dôveryhodnosť dokumentu pre adresáta, ktorý na základe dôveryhodného doručenia verí nezmeniteľnosti obsahu počas cesty medzi pôvodcom a adresátom. V prípade tretej strany však môže dôjsť k nedôvere voči adresátovi, ktorý práve pre absenciu autorizačných prvkov má možnosť s obsahom dokumentu manipulovať, a to bez ohľadu na to, či je treťou stranou OVM alebo iný typ subjektu. V takýchto prípadoch je občan často nútený vykonať zaručenú konverziu pôvodného elektronického dokumentu do papierovej podoby prostredníctvom IOMO, ktorý má počas obmedzenej doby prístup k pôvodnému elektronickému dokumentu na základe identifikátora rovnopisu, vytlačeného na samotnom rovnopise.

Biznisové požiadavky na riešenie KSDR

Riešenie KSDR bude poskytovať služby verejnosti. Z tohto dôvodu musí architektúra riešenia (bližší popis v časti "Architektúra"- budúci stav v Štúdii uskutočniteľnosti) rešpektovať najmä princípy:

- bezpečného používania osobných údajov,
- bezpečného oddelenia interných údajov a údajov určených pre verejnosť.

Po splnení nevyhnutných predpokladov bude rozhranie OpenAPI poskytované prostredníctvom API GW.

V rámci projektu budú vybudované služby pre občanov a služby pre podnikateľov. Aktivity budú následne realizované vo viacerých fázach v zmysle štandardov pre riadenie informačno-technologických projektov:[1]

V analytickej časti:

- Analýza a špecifikácia potrieb sprístupňovania, vyhľadávania a navigácie z hľadiska najvhodnejších riešení navigácie za účelom dosiahnutia čo najefektívnejšej a intuitívnej práce s grafickým rozhraní ako aj využívania aplikačných rozhraní.
- Analýza a špecifikácia pre zdieľanie a sprístupňovanie pre tretie strany: analýza a špecifikácia funkcionalít KSDR, ktoré sprostredkujú zápis evidencie oprávnení tretích strán (v zmysle tretia strana-používateľ-služba), čím sa zabezpečí realizácia princípov NKIVS v oblasti podpory Open API konceptu a v praxi sa podporia aj nové možnosti konkurencieschopnosti podnikov získavajúci nové údaje a služby (gov tech aplikácie a pod.).
- Poskytované aplikačné služby bude možné využívať na udelenie oprávnenia tretej strane konať v mene občana a podnikateľa v procesoch prístupu pre doručované rozhodnutia. Návrh testov a testovacích scenárov - v rámci tejto činnosti budú vytvorené popisy postupov pre jednotlivé testované oblasti (budú obsahovať vstupné podmienky, postupnosť krokov a očakávaných výstupov, resp. akcií a očakávaných reakcií), ktorými sa bude overovať, že skutočné funkcie testovanej oblasti (alebo jej

[1] Vyhláška č.78/2020 Z.z. o štandardoch pre ITVS, Vyhláška č.85/2020 Z.z. o riadení projektov, Vyhláška č.179/2020 Z.z. o obsahu bezpečnostných opatrení ITVS (ktoré nahradili 55/2014 Z.z.).

určitej časti) sú v súlade s požadovanou funkčnosťou (zadefinovanou v schválených analytických dokumentoch).

- Bezpečnostný zámer[2] - v rámci tejto činnosti budú vymedzené základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na zabezpečenie ochrany riešenia a spracúvaných údajov pred ohrozením ich bezpečnosti. Budú špecifikované technické, personálne a organizačné opatrenia na zabezpečenie ochrany údajov. Budú tiež vymedzené okolia ÚPVS / CÚD a hranice určujúce zostatkové riziká,

- Analýza bezpečnosti[3] - v rámci tejto činnosti bude vykonaný podrobný rozbor dôsledkov implementácie na bezpečnosť ÚPVS / CÚD. Bude vykonaná kvalitatívna analýza rizík, v rámci ktorej budú identifikované hrozby pôsobiace na aktíva ÚPVS / CÚD, spôsobilé narušiť ich bezpečnosť alebo funkčnosť. Výsledkom kvalitatívnej analýzy rizík bude najmä zoznam rizík, ktoré môžu ohroziť dôvernosť, integritu a dostupnosť ÚPVS / CÚD a spracúvaných osobných údajov, spolu s ohodnotením závažnosti dopadov realizácie rizika a popisom opatrení, ktoré eliminujú alebo minimalizujú vplyv rizík,

- Počas vývoja jednotlivých funkcionalít KSDR sa bude realizovať testovanie, ktoré je rozdelené na dve hlavné časti, a to na prípravu testovacej stratégie a testovacích prípadov na strane jednej a na samotný výkon užívateľsko-akceptačných testov. Následne bude v rámci testovacieho prostredia otestovaná vnútorná prepojiteľnosť jednotlivých funkcionalít a častí riešenia, schopnosť ich komunikácie, interný prenos dát a prenos dát s ÚPVS / CÚD. Finálne otestovanie plnej funkcionality riešenia (tzv. end-to-end process) zabezpečia užívateľské akceptačné testy (user acceptance test), pozostávajúce z testov funkčnosti a bezpečnosti jednotlivých oblastí riešení a záťažových testy, ktoré majú za cieľ preveriť kompletný proces poskytovania každej jednej funkcionality a jej bezporuchový priebeh.

- Testovanie bude realizované v nasledovných oblastiach:

    - Funkčné testovanie,
    - Identifikácia nedostatkov, konsolidácia a oprava chýb,
    - Záťažové testovanie,
    - Akceptácia riešenia.

- Po úspešnom otestovaní bezpečnosti, funkcionality a vzájomnej prepojiteľnosti jednotlivých komponentov bude systém nasadený do pilotnej a produkčnej prevádzky. Riešenie bude potrebné na nevyhnutný čas podporovať a reagovať na prípadné zistenia resp. vplyvy, ktoré neboli podchytené v rámci testovania, nakoľko v testovacom prostredí nemuseli vzniknúť podmienky na ich vznik.

    - Budú vykonané školenia pre používateľov a prevádzkovateľov, ktoré sú nevyhnutné k úspešnej prevádzke.

[2] Súčasť Bezpečnostného projektu
[3] Súčasť Bezpečnostného projektu

- Bude vytvorená prevádzková dokumentácia.
- Bude zabezpečená podpora užívateľom.

KSDR po nasadení do prevádzky zabezpečí:

- vedenie evidencie všetkých úradných dokumentov (rozhodnutí), doručovaných prostredníctvom ÚPVS bez ohľadu na spôsob doručenia (listinne, elektronicky);
- sprístupnenie rozhodnutí pôvodcom, aby nad nimi mohli vyhľadávať, zobrazovať si ich a ukladať si ich na lokálne zariadenie;
- sprístupnenie rozhodnutí adresátom, aby nad nimi mohli vyhľadávať, zobrazovať si ich a ukladať si ich na lokálne zariadenie pri autentifikácii eID alebo iným autentifikačným prostriedkom (napr. MoID);
- sprístupniť konkrétne rozhodnutie adresátovi bez potreby eID, iba zadaním (nasnímaním) čísla rozhodnutia a uvedením osobných údajov adresáta;
- umožniť adresátovi sprístupniť rozhodnutie tretej strane. Adresát požiada o vygenerovanie sprístupňovacieho kódu pre tretiu stranu a tento potom tretej strane poskytne (zaslanie e-mailom, zobrazenie na displeji mobilného telefónu a pod.);
- sprístupniť konkrétne rozhodnutie tretej strane bez potreby eID, iba zadaním (nasnímaním) sprístupňovacieho kódu , ktorý má jednorazovú resp. krátkodobú platnosť;
- Prístup ku službe poskytovanie rozhodnutia bude prostredníctvom API, publikovaného cez API GW, ako aj cez GUI. GUI bude vytvorené tak, aby bolo dostupné cez profil portfólia klienta na ÚPVS a v zmysle jednotného prístupu k osobným údajom (tzv. Moje dáta).

Riešenie sprístupnením originálnych elektronických rozhodnutí doručovaných rovnopisov rozhodnutí vrátane ich autorizačných prvkov (elektronické podpisy, časové pečiatky) výrazne zvýši dôveryhodnosť doručovaných rozhodnutí pre adresátov a tretie strany.

Navrhované riešenie nerieši vyznačovanie právoplatnosti rozhodnutí, sprístupňovanie rozhodnutí doručovaných inou cestou, životný cyklus rozhodnutí ani sprístupňovanie historických rozhodnutí. Je však prvým základným blokom pre vytvorenie budúcej centrálnej evidencie elektronických rozhodnutí, zabezpečujúcim služby pre potreby konzumentov informácií z rozhodnutí.

Pre prípady, kedy tretia strana bude vyžadovať kvôli svojmu spôsobu spracovania resp. ukladania dokumentov naďalej papierovú verziu, bude aj naďalej dostupná možnosť konverzie do papierovej podoby prostredníctvom IOMO (napríklad keď zamestnávateľ mimo OVM vyžaduje výpis z registra trestov a osobné spisy si stále vedie v papierovej podobe).

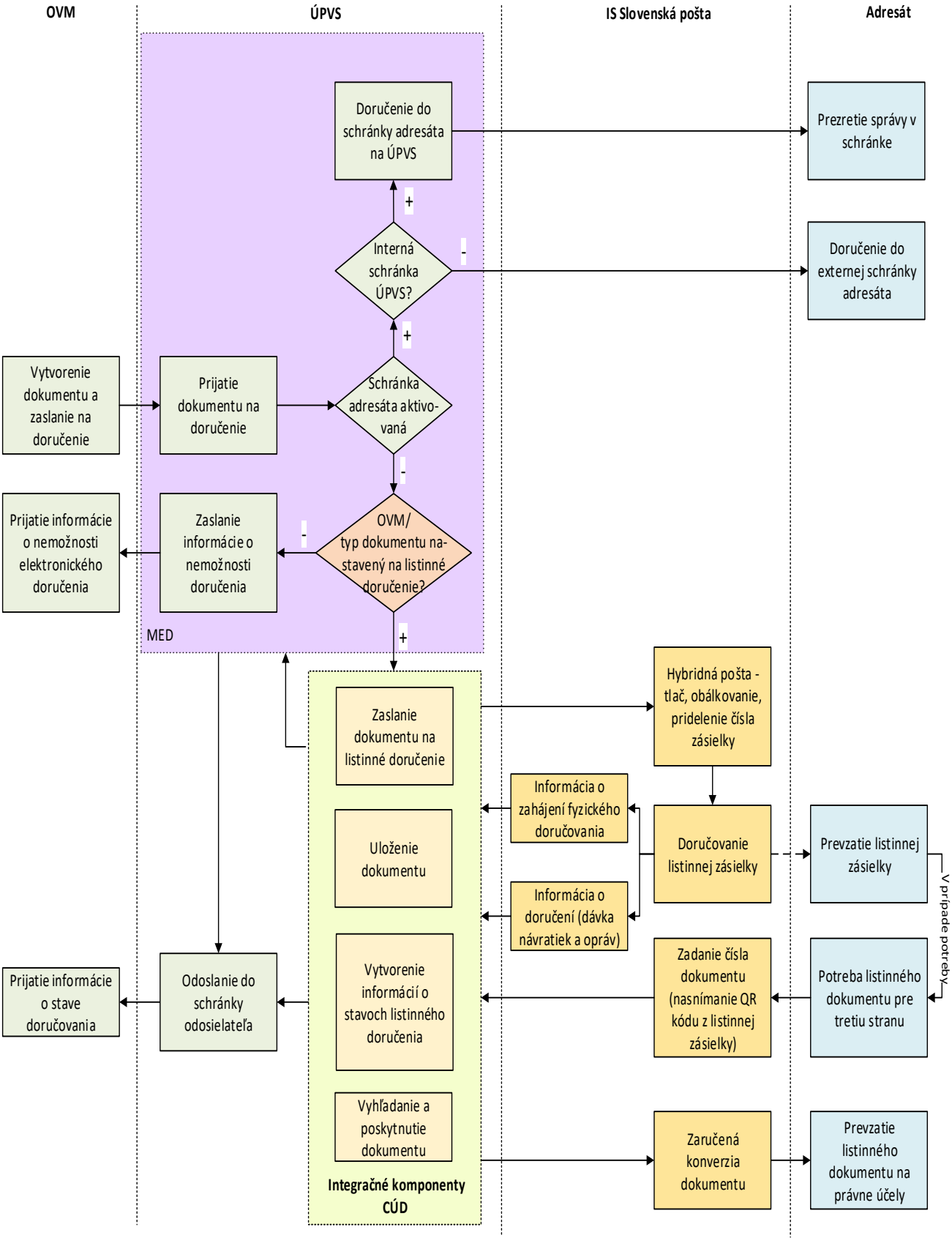
Detailný popis požiadaviek

Osoby v súčasnosti nemôžu vyhľadávať im doručené rozhodnutia na jednom mieste a sprístupňovať ich tretím stranám prostredníctvom tohto miesta.

Znamená to pre nich často stratený čas a ostatné prostriedky, ktoré musia vynaložiť na zabezpečenie príloh k ďalšiemu podaniu, ktoré potrebujú uskutočniť vo verejnej správe. Pritom všetky potrebné rozhodnutia už sú vydané inými OVM, ktoré ich ale nevedia sprístupniť na základe požiadavky občana alebo podnikateľa ďalším OVM alebo iným tretím stranám, čo spôsobuje prerušenie podania alebo jeho zastavenie a nutné znovuobnovenie zo strany občana alebo podnikateľa po doplnení potrebných rozhodnutí (príloh konania).

Súčasný proces je nakreslený na nasledujúcom obrázku:

Obrázok 1 – Aktuálny stav


OVM
ÚPVS
IS Slovenská pošta
Adresát
Doručenie do schránky adresáta na ÚPVS
Prezretie správy v schránke
+
Interná schránka ÚPVS?
-
Doručenie do externej schránky adresáta
+
Vytvorenie dokumentu a zaslanie na doručenie
Prijatie dokumentu na doručenie
Schránka adresáta aktivo-vaná
-
Prijatie informácie o nemožnosti elektronického doručenia
Zaslanie informácie o nemožnosti doručenia
-
OVM/ typ dokumentu na-stavený na listinné doručenie?
MED
+
Hybridná pošta - tlač, obálkovanie, pridelenie čísla zásielky
Zaslanie dokumentu na listinné doručenie
Informácia o zahájení fyzického doručovania
Doručovanie listinnej zásielky
Prevzatie listinnej zásielky
Uloženie dokumentu
Informácia o doručení (dávka návratiek a opráv)
V prípade potreby
Prijatie informácie o stave doručovania
Odoslanie do schránky odosielateľa
Vytvorenie informácií o stavoch listinného doručenia
Zadanie čísla dokumentu (nasnímanie QR kódu z listinnej zásielky)
Potreba listinného dokumentu pre tretiu stranu
Vyhľadanie a poskytnutie dokumentu
Zaručená konverzia dokumentu
Prevzatie listinného dokumentu na právne účely
Integračné komponenty CÚD

Požiadavky na zosúladenie implementácie a prevádzky KSDR v rámci ÚPVS

Nefunkčné požiadavky – legislatívne

- Všetky funkcionality KSDR budú koncovému používateľovi plne dostupné prostredníctvom štandardného webového prehliadača, bez potreby inštalácie akéhokoľvek dodatočného softvéru. Štandard prehliadača je určený Vyhláškou č. 78/2020 o štandardoch pre ITVS.
- Dielo musí byť dodané v súlade s platnými právnymi predpismi EÚ a SR, zoznam právnych predpisov a štandardov je uvedený v záložke Legislatíva a štandardy.
- Pri dodávke Diela sa budú uplatňovať všetky zásady a postupy v zmysle ISO 27001 Systém manažérstva bezpečnosti informácií.
  V úvodnej fáze projektu dodávateľ vykoná predbežnú analýzu rizík v súlade so smernicou pre riadenie rizík informačnej bezpečnosti NASES. Na základe požiadaviek na bezpečnosť navrhne Dodávateľ adekvátne opatrenia. Od Zhotoviteľa požadujeme, aby v priebehu projektu priebežne dopĺňal zoznam aktív v súčinnosti s Objednávateľom a tým aj aktualizoval zoznam požiadaviek a opatrení.
- Grafická prezentácia musí rešpektovať všetky zákonné normy pre systémy štátnej správy vrátane vyhlásenia o prístupnosti (blind-friendly).
- Komponent by mal zabezpečiť implementáciu opatrení OWASP Top 10 (www.owasp.org).
- Grafická prezentácia musí rešpektovať všetky zákonné normy pre systémy štátnej správy (najmä Vyhlášku č.78/2020) vrátane vyhlásenia o prístupnosti (blind-friendly). Riešenie musí byť v súlade s WCAG 2.1 úroveň AA (smernica EÚ č. 2016/2102). Riešenie musí byť v responzívnom dizajne a musí zabezpečiť dodržanie dizajnového manuálu pre štátnu správu ID-SK. Vyhlásenie o prístupnosti bude podporené posudkom UNSS.

Nefunkčné požiadavky - UX/UI/UCD

- Zabezpečiť zjednodušenie práce a ovládania KSDR. KSDR musí byť používateľsky príjemný, ľahko pochopiteľný a jeho ovládanie musí byť intuitívne a ľahko zvládnuteľné aj pre výrazne neskúseného používateľa. Kladie sa dôraz na UX a usability systému, nápovedu, help v rámci aplikácie a pod.
- Pri návrhu riešenia musí byť využitý tzv. user-centered dizajn (UCD) tak, aby sa zabezpečila zmysluplnosť a použiteľnosť služieb zo strany koncového používateľa – občana, podnikateľa a tretieho sektora ako aj používateľa OVM. Na základe UX stratégie budú navrhnuté používateľské rozhrania pre KSDR.

  Všetky časti KSDR musia byť navrhnuté v súlade s dizajn manuálom ID-SK a zároveň tak, aby bolo možné v prípade potreby zabezpečiť súlad s novým dizajn manuálom bez potreby preprogramovania. Každá požiadavka bude implementovaná s ohľadom na potreby používateľa s využitím metodiky UCD.

  NASES v spolupráci s MIRRI SR a dodávateľom predmetu tejto zákazky vytvorí tím,

ktorý vykoná uvedené analytické činnosti ktorých okrem iných výstupov bude aj UX stratégia. Je požadované, aby za stranu zhotoviteľa boli súčasťou tímu odborníci na:
    - _UX a behaviorálne inovácie,
    - _návrh grafického používateľského rozhrania a
    - _biznis architekt tohto projektu.
- Počas analýzy zabezpečiť prieskum navrhovaného riešenia s účasťou relevantných cieľových skupín (napr. občan, podnikateľ, OVM) koncových používateľov, ktoré overia navrhovaný spôsob riešenia požiadaviek, doplnia očakávania občanov a zanalyzujú ich motivácie, problémy, znalosti a potreby.
- Realizované používateľské rozhranie musí byť tvorené v súlade s dizajnovým manuálom pre štátnu správu ID-SK, musí podporovať úplnú prístupnosť pre zdravotne postihnutých občanov a musí byť tvorené v aktívnej kooperácii s koncovými používateľmi tak, aby projekt zabezpečil jeho úplnú použiteľnosť. Používatelia musia byť zapojení (napr. použitím card sortingu - používatelia navrhnú roztriedenie informácií do logicky usporiadaných tematických okruhov) do tvorby informačnej architektúry (štruktúra obsahu Front-End časti služby) a štruktúry navigácie. Tá by mala byť testovaná kvantitatívne so zapojením všetkých účastných cieľových skupín s dôrazom aj na prístupnosť pre znevýhodnených občanov. Informačná architektúra musí zohľadňovať slovník, ktorý je definovaný v Jednotnom dizajn manuáli elektronických služieb.
  Prototyp grafického rozhrania (GUI) jednotlivých častí KSDR (klikateľné používateľské rozhranie a navigácia) musí byť testovaný počas jeho prípravy so zástupcami všetkých relevantných cieľových skupín metódou formatívneho testovania použiteľnosti počas každého šprintu (iteratívnej dodávky). Zistenia z testovania musia byť zapracované do prototypu. Grafický dizajn a front-end programový kód musí zohľadňovať ID-SK.
- Pred uvedením KSDR do prevádzky musí byť KSDR otestovaný sumatívnym testovaním použiteľnosti s účasťou všetkých relevantných skupín určených NASESom. Počas testovania budú zdokumentované metriky použiteľnosti (čas úlohy, chybovosť úlohy, efektivita úlohy, SUS skóre) pre kľúčové prípady použitia. Zároveň bude vykonané testovanie prístupnosti systému zohľadňujúce aspoň WCAG 2.0 AA štandard.

Nefunkčné požiadavky - vizuálne komponenty (GUI)

- Pri vývoji Diela v intenciách funkčných požiadaviek požadujeme, aby navigácia v KSDR, ovládanie menu, presun medzi obrazovkami, dizajnové prevedenie, atď. boli konzistentné v celom komponente a v súlade s dizajn manuálom ID-SK podľa voľne dostupnej verzie v čase návrhu a implementácie riešenia v príslušnej iterácii.
- V intenciách funkčných požiadaviek musí používateľské rozhranie informovať používateľa o potrebe alebo výsledku vykonania/nevykonania operácie.
- Komponent musí umožňovať nastavenie podľa typu prihláseného prehliadača, napríklad musí rozlíšiť, či je prihlásené zariadenie typu smartphone alebo PC a podľa toho zobraziť stránku v príslušnom dizajne. Táto požiadavka, ak je to vhodné, môže byť riešená, napríklad responzívnym dizajnom.

Nefunkčné požiadavky – školenia

- Zhotoviteľ je povinný navrhnúť rozsah a štruktúru školení (pracovných workshopov) vrátane podrobného harmonogramu. Rozsah jednotlivých školení musí zodpovedať pokrytiu potrieb všetkých používateľov jednotlivých častí KSDR, ktoré sú súčasťou Diela. V rámci dodávky jednotlivých častí Diela je potrebné pokryť minimálne nasledujúci rozsah:
    - _Všeobecné funkcionality jednotlivých častí KSDR z pohľadu používateľov.
    - _Prevádzka, obsluha a dohľad KSDR z pohľadu prevádzkovateľa.

  Školenia sa vykonávajú v školiacom prostredí, ktoré pripraví Zhotoviteľ. Školiace prostredie má rovnakú funkcionalitu ako aktuálne predprodukčné, resp. produkčné prostredie. Školiace prostredie obsahuje školiace dáta. Zmeny, ktoré účastník školenia vykoná v školiacom systéme, môže administrátor odvolať a obnoviť prednastavené školiace prostredie. Alternatívne je možné využiť na školenia predprodukčné alebo testovacie prostredie. Súčasťou dodávky školení je dodávka školiacich materiálov a výstupov.

Technické požiadavky

- KSDR musí byť navrhnutý a realizovaný tak, aby sa dal prevádzkovať s dostupnosťou najmenej 99,0%, 24x7.
- KSDR musí byť dimenzovaný tak, aby umožnil prihlásiť 10 000 používateľov a pracovať v KSDR v rovnakom čase. Priemerný odhadovaný mesačný počet prístupov k elektronickým dokumentom: 45 000.
- KSDR bude poskytovať možnosť zobrazenia webových stránok optimalizovaných pre mobilné zariadenia (smart mobilný telefón, tablet) s rôznymi rozlíšeniami obrazoviek. Dostupnosť môže byť zabezpečená, ak je to vhodné, napríklad aj responzívnym dizajnom.
- Maximálny čas odozvy stránky (odpovede na HTTP dotaz) KSDR je 3 sekundy. Maximálny čas nesmie byť prekročený pre 95% volaní. V prípade vypočítavaného, alebo generovaného obsahu, ktorého zobrazenie trvá z povahy zobrazenia dlhšie ako 3 sekundy je potrebné používateľovi zobraziť informáciu o tom, že sa daný obsah pre neho pripravuje.
  Oznam bude zobrazený podobe zrozumiteľnej pre používateľa tak, aby používateľ vedel, čo sa deje.
- Požiadavka na IT a Kyber. Bezpečnosť:
    - _architektúra, oddeľujúca jednotlivé vrstvy riešenia s využitím overených návrhových vzorov ako napr. MVC, API first a podobne,
    - _voľba správnych frameworkov a prostriedkov, ktoré už svojim dizajnom predchádzajú bezpečnostným chybám (napr. SQL injekciám, XSS, pretečeniu buffra a podobne),
    - _použitie dôveryhodných a aktuálnych verzií frameworkov a knižníc,
    - _minimálna nutná množina komunikačných rozhraní,
    - _statická prezenčná vrstva (html+css+javascript) bez potreby a možnosti akejkoľvek server-side logiky, je nutné adresovať injekčné chyby (XSS, javascript injection, DOM injection, JSON injection),
    - _všetky služby aplikačnej vrstvy majú vystavené IBA API rozhrania, nikdy nie priamo vizuálnu stránku, preferované sú REST rozhrania,

- _všetky API volania sú autentifikované a autorizované (s výnimkou úplne verejných API rozhraní a prihlásenia), autentifikácia a autorizácia je riešená ako samostatný modul, nikdy nie vo vnútri konkrétnych funkčných modulov,
- _API podporujú ochranu pred DOS /rate limiting, atď.),
- _striktná kontrola všetkých vstupov od používateľa aj od externých IS na strane servera (v žiadnom prípade nie spoliehanie sa na „perimetrovú bezpečnosť“ nadradeného projektu), táto kontrola sa týka napr. aj HTTP hlavičiek, cookies a podobne,
- _ošetrovanie výstupov na predchádzanie injekciám (sql, xml, shell, xss, ldap, xpath, xsl(t), javascript,url/rest, iné),
- _nezobrazovanie chybových správ systému, runtime či frameworku do používateľského výstupu - max. zobrazovanie používateľsky prístupného chybového hlásenia bez akýchkoľvek technických detailov,
- _pokiaľ je potrebné ukladať autentifikačné údaje, musia byť uložené vo forme salted hash, s hashovacou funkciou minimálne SHA256. Žiadne autentifikačné údaje nesmú byť pevnou súčasťou zdrojového kódu,
- _citlivé údaje (najmä osobné údaje) je potrebné ukladať v šifrovanej forme (na úrovni DB alebo úložiska), zvážiť end-to-end šifrovanie vybraných údajov tak, aby databázový backend nemal žiadny prístup k ukladaným údajom (napr. browser-side šifrovanie asymetrickou kryptografiou pomocou kľúčov, ktoré sa neukladajú na serveri),
- _používateľmi vkladané prílohy je nutné kontrolovať na prítomnosť vírusov a iného spustiteľného, či inak škodlivého obsahu. Je potrebné definovať povolené typy vkladaných súborov. Taktiež je nutné identifikovať prílohy obsahujúce osobné údaje, či už automaticky podľa druhu prílohy (napr. doklad o dosiahnutom vzdelaní), manuálne označením používateľom, alebo pristupovať ku všetkým prílohám ako keby obsahovali osobné údaje. Následne je potrebné s týmito prílohami zaobchádzať podľa pravidiel narábania s osobnými údajmi.
- _transakcie aplikácie je potrebné zabezpečiť najmä proti opakovaniu rovnakej transakcie (či už neúmyselnému, napr. refresh v prehliadači, ako aj úmyselnému,
- _súbežne so softvérom vyvíjať automatizované testy, ktoré testujú
- _korektné správanie so stopercentným pokrytím API volaní, vysokým pokrytím kódu, vysokým pokrytím GUI komponentov
- _bezpečnostné vlastnosti, stanovené v bezpečnostnom návrhu (odolnosť voči určitým typom útokov, neautentifikovanému prístupu a podobne)
- _všetky identifikované a odstránené chyby (regresné testy),
- _čistotu zdrojového kódu (lint)
- _zabezpečiť proces bezpečnostných aktualizácií počas celej životnosti projektu, vrátane
- _aktualizácií vlastného software (odhalenie novej bezpečnostnej slabiny, prelomenie použitého šifrovacieho algoritmu a podobne)
- _jeho závislostí (pravidelne alebo podľa potreby aplikovať bezpečnostné patche použitých produktov, kontajnerov, knižníc)
- _úprav softvéru z dôvodu ukončenia bezpečnostnej podpory pre platformu, na ktorej je prevádzkovaná (operačný systém, "veľkej verzie" frameworku a podobne)

    - _proces bezpečného nasadzovania s minimalizovaním rizika supply chain útokov (bezpečné podpisovanie aktualizácií, oddelené prostredia s kontrolovaným upgradom)
- KSDR vrátane endpointov musí byť zabezpečený voči neoprávnenému prístupu k dátam a chránený voči SQL injection. Riadenie prístupu k obsahu je na základe autentifikačného rozhodnutia a pridelenej príslušnej role napárovanej na oprávnenú osobu.
- V procese vývoja KSDR zabezpečiť:
  _bezpečnosť pri vývoji,
  __bezpečnostné povedomie programátorov,
  __použitie verzionovacieho nástroja na správu zdrojového kódu,
  __použitie automatizovaných testov,
  __priebežnú tvorbu vývojárskej dokumentácie,
  _pri testovaní KSDR sa nesmú použiť údaje z produkčného prostredia,
  _prezentovať a konzultovať s NASES architektúru a bezpečnostný návrh KSDR pred samotným začiatkom vývoja, a pri každej zásadnej zmene architektúry

Funkčné požiadavky

- Migrácie, synchronizácie a preberanie údajov z existujúcich modulov, komponentov a rozšírení ÚPVS do KSDR je súčasťou dodávky Diela.
- Integráciu pre tretie strany zabezpečiť prostredníctvom API GW tak, aby bol poskytnutý jednotný prístup ku KSDR. Každá služba bude publikovaná na používanie cez API Gateway (API GW nie je predmetom dodávky). Súčasťou Diela nie je pripájanie poskytovaných služieb IS VS tretích strán na API GW.
- Súčasťou dodávky Diela je aj vybudovanie nových integračných rozhraní na systémy, ktoré bude potrebovať KSDR pre svoju funkcionalitu. Medzi nosné systémy patria najmä CSRÚ, SNCA, data.gov.sk. Samotné integrácie sú spomenuté vždy pri tých častiach KSDR, ktoré ich pre svoju činnosť potrebujú.
- Webové stránky KSDR budú integrované s používateľskými rozhraniami modulov ÚPVS tak, aby z používateľského hľadiska prechod medzi modulmi a webovými stránkami KSDR v rámci tohto Diela dodržiaval manuál ID-SK a boli zachované rozpracované procesy používateľa (napr. rozpracované elektronické podanie).
- Dodané dielo a jeho časti musia spĺňať nasledujúce požiadavky:
    - _na monitorovanie aplikácií využívalo existujúce nástroje monitoringu,
    - _na všetkých koncových a aplikačných službách automaticky monitorovať a reportovať SLA parametre,
    - _na logovanie využívalo centrálny logovací komponent,
    - _na využitie akejkoľvek funkcionality, ktorá nie je týmto projektom nahrádzaná využívalo funkcionalitu Portfólio klienta,
    - _riešenie musí byť funkčné vo všetkých prostrediach ÚPVS, nasadzovanie riešenia do prostredí sa musí riadiť predpismi pre ÚPVS.
- KSDR bude poskytovať údaje pre "Moje dáta". Centrálny systém pre manažment osobných údajov nie je súčasťou tohto projektu. V prípade, že do dokončenia implementácie projektu tento systém nebude k dispozícii, v rámci projektu sa vytvoria všeobecné integračné rozhrania na báze otvorených štandardov a s integráciou na API GW pre potreby budúcej integrácie.

- Zobrazenie údajov KSDR v Portfóliu klienta bude pridané ako generický zásuvný modul, nakonfigurovaným nasledujúcimi nastaveniami:
    - _formulár pre vyhľadávanie nad zdrojom údajov,
    - _formulár pre zobrazovanie výsledkov vyhľadávania,
    - _formulár pre detailný pohľad na údaj,
    - _transformáciu pre uloženie výsledku vyhľadávania so základnými metaúdajmi do súboru (csv, a používateľsky jednoducho dostupný formát napr. pdf, xlsx + ods),
    - _transformáciu pre tlač detailného pohľadu,
    - _rozhranie pre prístup k zdroju údajov.
- Pre KSDR, v rámci Portfólia klienta, bude možnosť využívať odosielanie notifikácií a proaktívnych správ.
  Záujem a formu zasielania (SMS,email, push) pre notifikácie a proaktivne správy, si manažuje používateľ KSDR v Portfóliu klienta.
- KSDR bude využívať samostatný komponent ÚPVS (Portfólio klienta) pre možnosť zberu, vyhodnocovania a publikovania spätnej väzby od používateľa.
- KSDR musí byť vytvorené tak, aby bolo možné použiť ho ako súčasť Workdesk identity prostredia Portfólia klienta.
- Workdesk identity je prostredie, v ktorom si používateľ môže definovať jednotlivé komponenty, s ktorými chce pracovať, resp. ktoré plánuje používať vo forme premiestňovateľných záložiek určených na rýchle spustenie komponentu (napríklad konštruktor, zoznam služieb, preferované služby, eDesk, portál slovensko.sk a podobne). Je to jednotná úvodná stránka používateľa, na ktorej v responzívnom dizajne bez ohľadu na systém z ktorého pristupuje (PC, mobil) vidí a ovláda grafické komponenty (pridáva, odoberá, premiestňuje a podobne). Táto stránka sa bude objavovať pri voľbe portálu vždy vtedy, keď ju bude mať používateľ nastavenú. Jednotlivé záložky musia byť vytvorené tak, aby boli použiteľné aj na iných webových stránkach.
- KSDR musí byť vytvorený tak, aby umožňoval využitie funkcionality štátneho messengera pre svoje potreby.
- Ak by používateľ (aj napriek intuitívnej navigácii) hľadanú informáciu predsa len nenašiel, môže sa okamžite cez štátny messenger obrátiť na zamestnanca, ktorý mu pomôže vyriešiť jeho požiadavku.
- KSDR zabezpečí riadenie prístupu k JÚEÚD pre interných používateľov ako aj pre autentifikovaných používateľov s príslušnou rolou.
- Riešenie dodané v rámci Diela musí zabezpečiť, aby všetky údaje obsiahnuté v KSDR, ktoré nepodliehajú ochrane osobných údajov alebo nie sú utajovanými skutočnosťami a majú hodnotu pre potrebu ďalšieho využitia v zmysle právnych noriem a smernice PSI, boli exportované vo forme otvorených údajov a automaticky umiestňované a aktualizované na portáli pre otvorené údaje data.gov.sk. Objednávateľ zabezpečí súčinnosť strán potrebných pre integráciu s projektom Otvorené údaje 2.0 (v prípade, že nebude Otvorené údaje 2.0 v realizácii, je potrebné zabezpečiť publikovanie na existujúcom systéme Otvorené údaje 1.0).
- KSDR musí podporovať ľubovoľný počet jazykových verzií bez potreby tvorby vlastných stromov pre jednotlivé mutácie. Počas dodania Diela sa predpokladá grafické používateľské rozhranie minimálne v slovenskej a anglickej verzii. Prepnutie jazykovej verzie musí zachovať aktuálnu pozíciu na portáli - t. j. ak sa používateľ preklikne na konkrétnu stránku a zmení jazyk, tak sa aktívna stránka

zobrazí v požadovanom jazyku (inými slovami zmena jazyka nesmie používateľa automaticky presmerovať na úvodnú stránku).
Systém tiež musí zabezpečovať prípady, kedy pre vybranú jazykovú mutáciu neexistuje vyplnený obsah. V prípade, že niektorá položka menu nemá definovanú jazykovú mutáciu v požadovanom jazyku, tak sa nezobrazí. V prípade, ak stránka nemá zadefinovanú jazykovú mutáciu v požadovanom jazyku, zobrazí sa všeobecná informácia o chýbajúcom preklade s možnosťou odkliku na ľubovoľnú inú jazykovú mutáciu, ktorej obsah existuje.
Vyhľadávanie – KSDR musí zabezpečiť funkčné vyhľadávanie v rámci ktorejkoľvek jazykovej mutácie – pokiaľ sú k danému výsledku vyhľadávania (napr. v anglickom jazyku) pridané tagy v požadovanom jazyku, výsledky vyhľadávania musia poskytnúť relevantné výsledky v požadovanej jazykovej mutácii.
Preklady názvov tlačidiel, jednotlivých nadradených častí – systém musí zabezpečiť jazykové mutácie nadradených častí a tlačidiel.

- Riešenie musí umožňovať nastavenie odberu notifikácií používateľom (napr. v prípade tretích strán notifikácie o sprístupnených rozhodnutiach). Rozsah bude upresnený vo fáze analýzy.
- Obsah každej obrazovky (webovej stránky) KSDR bude možné tlačiť, pričom v tlačovom výstupe je iba samotný vecný obsah, nie všetky zobrazené prvky (hlavička, pätička, menu, atď.)
- Základnými funkčnými celkami vyhľadávania v KSDR budú:
    - _textové vyhľadávanie,
    - _navigácia na základe atribútov a tagov (vyhľadávanie cez filtre).
- Je potrebné, aby používateľ vyhľadával informácie v KSDR jemu prirodzeným jazykom a na druhej strane dostával relevantné odpovede (sémantické vyhľadávanie).
  Pre účely sémantického vyhľadávania budú zhotoviteľom vytvorené ontológie webového obsahu KSDR.
- Vyhľadávanie bude odolné voči preklepom, alebo gramatickým chybám vo vyhľadávanom výraze, ktorý zadal používateľ. V prípade jednoduchých preklepov (zámena písmen a pod.), ktoré by inak dávali prázdne výsledky, upovedomení používateľa o spôsobe opravy. Bude poskytovať zoznam najčastejších výrazov začínajúcich rovnako ako hľadaný výraz (nápoveda pre vyhľadávanie), ktoré bude používateľovi ponúkať. Zároveň sa budú po zadaní preddefinovaného počtu znakov a/alebo po určenom intervale nečinnosti zobrazovať priebežné výsledky. KSDR takisto umožní, aby duplicitné frázy, používané pre vyhľadávanie, boli automaticky spájané pre účely efektívneho dopĺňania hľadaných výrazov. V prípade, že hľadaná fráza obsahuje slovo alebo frázu, pre ktoré nie sú výsledky, pri vyhľadávaní sa toto slovo (fráza) vynechá a pri zobrazení výsledkov sa označí (napr. prečiarknuté písmo).
- Procesná mapa ako predpripravený zoznam krokov sprístupnenia rozhodnutí tretím stranám (aj vrátane zobrazenia a použitia sprístupneného rozhodnutia treťou stranou).
  Procesná mapa by mala jednoduchým a intuitívnym spôsobom sprevádzať aj neprihláseného používateľa a ukazovať potrebu následných krokov alebo možnosť súčasných krokov.

Funkčné požiadavky – samotný modul KSDR

Riešenie zabezpečí jednotné úložisko všetkých elektronických úradných dokumentov (JÚEÚD), doručovaných prostredníctvom ÚPVS, bez ohľadu na spôsob doručovania. JÚEÚD bude:

- viesť metaúdaje jednotlivých rozhodnutí a bude integrované na úložisko, ktoré bude v čase implementácie projektu KSDR k dispozícii (ďalej len OST, upresnenie úložiska bude špecifikované v rámci analýzy);
- spĺňať všetky náležitosti zabezpečenia ochrany osobných údajov, ako aj iných legislatívnych noriem, ktorých nariadenia niektorým spôsobom ukladajú požiadavky na ochranu údajov iného charakteru (obchodné tajomstvo a pod.);
- v rámci riadenia životného cyklu správ (a ich metaúdajov), obsahovať aj funkcionalitu aktualizácie platnosti autorizačných prvkov po vypršaní času ich platnosti (elektronická pečať/ kvalifikovaná elektronická pečať, elektronický podpis/ kvalifikovaný elektronický podpis.
- podľa potreby KSDR zamykať záznamy.

Ďalšia potrebná funkcionalita

- Prevzatie metaúdajov správy triedy EGOV_DOCUMENT, doručovanej do elektronickej schránky, z ÚPVS MED
- Zapísanie metaúdajov správy triedy EGOV_DOCUMENT, doručovanej do elektronickej schránky, do JÚEÚD
- Nastavenie zablokovania vymazania elektronickej správy triedy EGOV_DOCUMENT, doručovanej do elektronickej schránky, v ÚPVS OST, vrátane kategórie správ v rámci CUET (kde sú zverejnené rozhodnutia pre všetkých v rámci miestnej príslušnosti)
- Prevzatie metaúdajov správy triedy EGOV_DOCUMENT_CUD, doručovanej listinne prostredníctvom centrálneho úradného doručovania (CÚD), z ÚPVS MED
- Zapísanie metaúdajov správy triedy EGOV_DOCUMENT_CUD, doručovanej listinne prostredníctvom CÚD, do JÚEÚD
- Nastavenie zablokovania vymazania elektronickej správy triedy EGOV_DOCUMENT_CUD, doručovanej listinne prostredníctvom CÚD, v ÚPVS OST
- Riadenie životného cyklu správ (ich metaúdajov) v JÚEÚD, vrátane ukončenia poskytovania a odblokovania správ voči zmazaniu v ÚPVS OST
- Indexovanie metaúdajov správ pre rýchle vyhľadávanie
- Cache metaúdajov správ, prípadne cache samotných správ
- API pre prístup k správam
- API pre vyhľadávanie nad správami

Riešenie zabezpečí riadenie prístupu k JÚEÚD pre pôvodcov a adresátov úradných dokumentov na základe autentifikačného rozhodnutia, vydaného ÚPVS IAM. Potrebná funkcionalita (ako pre API, tak aj grafické rozhranie) je:

- kontrola platnosti a správnosti vydaného autentifikačného rozhodnutia, vydaného ÚPVS IAM (autentifikačného tokenu)
- kontrola úrovne autentifikácie používateľa (QAA level), autorizácia iba pre povolené QAA level úrovne a autentifikačné prostriedky (na základe výsledkov analýzy)

- kontrola úrovne zastupovania subjektu, prípadne kontrola rolí pre zastupovania v prípade, že prihlasovaný používateľ (user) zastupuje iný subjekt ako sám seba
- kontrola scopes (rozsahu) a oprávnení aplikácie, cez ktorú používateľ pristupuje v roli tzv. univerzálneho pôvodcu bude môcť vystupovať aj OVM/IS VS, ktoré bude mať pridelenú špecifickú rolu pre prístup (napríklad polícia, portál oversi.sk, IOM a podobne)

Tieto kontroly je možné pre API rozhranie vykonať aj poskytovaním API cez API GW a nastavením kontrol na API GW (prostredníctvom integrácie na API GW). Presné nastavenie jednotlivých parametrov kontrol bude súčasťou funkčnej špecifikácie.

Riešenie zabezpečí grafické rozhranie pre manipuláciu so správami, uloženými v JÚEÚD, pre adresátov a pôvodcov autentifikovaných tokenom nasledovnou funkcionalitou (pre API aj grafické rozhranie):

- vyhľadávanie nad správami, kde je pôvodcom alebo adresátom subjekt autentifikačného tokenu
    - V KSDR nemajú byť danej osobe dostupné (vyhladateľné) EUD doručované do vlastných rúk, kým nepríde k ich doručeniu tejto osobe. (Spôsoby doručovania: - Fikcia doručenia - Za doručenie sa považuje aj uplynutie úložnej lehoty a fikcia doručenia. V takom prípade sa do schránky adresáta ukladá dané rozhodnutie, aj keď legislatíva takéto uloženie nevyžaduje. - V prípade doručovania do vlastných rúk bez fikcie - po uplynutí úložnej lehoty sa považuje za nedoručené. - V prípade doručovania nie do vlastných rúk (pre PO/FO) sa považuje za doručené až ďalší deň po reálnom uložení v schránke
    - Taktiež nemajú byť v KSDR uložené také EUD, ktoré nie sú zobraziteľné (Keďže UPVS nemá dostatočné vstupné validácie, v prípade chybných EUD neuložiteľných do eDesk sa ich UPVS pokúša doručiť a až kým nepríde k pokusu o prevzatie plynie doručovacia lehota. Keď nastane fikcia doručenia (adresát sa nepokúsil o prebratie rozhodnutia), dokument sa považuje za doručený ale KSDR ho nemusí byť schopný spracovať / zobraziť. Je potrebné buď zaviesť vstupné validácie do UPVS alebo vytvoriť validácie samostatne pre KSDR (tieto by však museli byť zladené s validáciami uplatňovanými v eDesk alebo CUET)
- Fulltextové vyhľadávanie nad elektronickými úradnými dokumentami (nad ich celým obsahom a štandardizovanými elementmi)[4]
- poskytnutie zoznamu výsledku vyhľadávania, funkcionalita zoznam sa neposkytne ak autentifikovaným je univerzálny pôvodca
- poskytnutie metaúdajov správy na základe zadanej referencie správy, získanej z výsledku vyhľadávania, elektronickej schránky alebo listinne doručeného úradného dokumentu
- poskytnutie samotnej správy, načítanej z ÚPVS OST, na uloženie na lokálne zariadenie na základe referencie správy

[4] Príloha č. 1 Vyhlášky č. 78/2020 Z.z. - 2.3.7. Dátová štruktúra elektronického formulára elektronického úradného dokumentu obsahuje najmenej údaje uvedené vo forme samostatných dátových prvkov, ktorými sú a) názov orgánu riadenia, ktorý konanie či úkon uskutočnil, b) identifikátor orgánu riadenia, ktorý konanie či úkon uskutočnil, c) dátum vydania elektronického úradného dokumentu, d) identifikačné údaje elektronického úradného dokumentu, e) predmet konania. Tento rozsah údajov sa vzťahuje aj na prípady podľa osobitného predpisu. 38) 2.3.8 Dátová štruktúra podľa bodu 2.3.7 zároveň spravidla obsahuje a) typ elektronického úradného dokumentu, b) poštovú doručovaciu adresu.

- poskytnutie samotnej správy, načítanej z ÚPVS OST, na prezeranie na lokálnom zariadení, na základe referencie správy
- zaznamenanie prístupu k správe alebo k jej metaúdajom s uložením pristupujúceho subjektu, používateľa, času prístupu a vykonanej činnosti so správou
- vedenie záznamov prístupu a ich ukladanie pre budúce poskytovanie prostredníctvom systému pre manažment osobných údajov (v prípade, že do dokončenia implementácie projektu systém „manažment osobných údajov“ nebude k dispozícii, v rámci projektu sa vytvoria všeobecné integračné rozhrania na báze otvorených štandardov a s integráciou na API GW pre potreby budúcej integrácie)

Pre potreby vyhľadávania a zobrazenia bude vytvorené grafické rozhranie pre používateľa. Grafické rozhranie zabezpečí:

- výber spôsobu prihlásenia
    - prostredníctvom autentifikačných prostriedkov (eID, mID a prípadne ďalších na základe výsledkov analýzy)
    - prostredníctvom identifikátora správy (napr. vytlačeného na rovnopise)
- autentifikáciu používateľa prostredníctvom ÚPVS IAM
- single sign on (SSO) v prípade, že používateľ už autentifikovaný je
- vyhľadávanie nad správami, kde je používateľ pôvodca alebo adresát
- nastavovanie filtrov pre vyhľadávanie
- rozhranie pre zadanie identifikátora správy
- rozhranie pre načítanie identifikátora správy z QR kódu doručovanej správy
- zobrazenie metaúdajov správy na základe
    - zvolenej položky zo zoznamu
    - zadaného identifikátora správy
    - načítaného identifikátora z QR kódu
- zobrazenie obsahu správy resp. jednotlivých príloh na základe voľby vykonanej v zobrazení metaúdajov správy
- uloženie samotnej správy, ľubovoľnej prílohy alebo celej správy vrátane príloh na lokálne úložisko (pevný disk, USB kľúč a podobne)
- informatívne overenie platnosti elektronického podpisu/elektronických podpisov na správe alebo ľubovoľnej prílohe
- zobrazovanie chybových hlásení v prípade chýb pri vyhľadaní, zobrazení a podobne
- uloženie dokumentu v pôvodnej elektronickej forme autorizovaný (ASIC), ale aj v PDF formáte pre potreby vizualizácie, alebo tlače
- Realizáciu zaručenej konverzie (prostredníctvom SNCA, CEP a MEF).

Veľa adresátov, ktorým sú úradné dokumenty doručované listinne, nepristupuje k elektronickej schránke, pretože:

- nemá eID
- nemá aktivovanú autentifikáciu na eID
- nepozná autorizačné kódy (BOK) pre autentifikáciu prostredníctvom eID
- nedôveruje používaniu eID
- nepracuje s eID

Pre túto skupinu používateľov je potrebné zabezpečiť prístup k rozhodnutiu na základe identifikátora listinne doručeného rozhodnutia a zadania osobných údajov, ktoré sú viazané s adresátom rozhodnutia a sú vedené v ÚPVS IAM (napríklad meno, priezvisko, rodné číslo, dátum narodenia, adresa trvalého bydliska). Grafické rozhranie pre túto funkcionalitu obsahuje:

- výber spôsobu prihlásenia
    - prostredníctvom autentifikačných prostriedkov (eID, mID a prípadne ďalších na základe výsledkov analýzy)
    - prostredníctvom identifikátora správy (napr. vytlačeného na rovnopise)
- rozhranie pre zadanie náhodne vybraného osobného údaju prihlasujúceho sa
- rozhranie pre zadanie identifikátora správy
- rozhranie pre načítanie identifikátora správy z QR kódu doručovanej správy
- kontrolu správnosti zadaných osobných údajov voči údajom adresáta správy, vedeným v metaúdajoch správy a údajom adresáta, vedeným v ÚPVS IAM
- zobrazenie metaúdajov správy na základe
    - zadaného identifikátora správy
    - načítaného identifikátora z QR kódu
- zobrazenie obsahu správy resp. jednotlivých príloh na základe voľby vykonanej v zobrazení metaúdajov správy
- uloženie samotnej správy, ľubovoľnej prílohy alebo celej správy vrátane príloh na lokálne úložisko (pevný disk, USB kľúč a podobne)
- informatívne overenie platnosti elektronického podpisu/elektronických podpisov na správe alebo ľubovoľnej prílohe
- zobrazovanie chybových hlásení v prípade chýb pri vyhľadaní, zobrazení a podobne

Adresát rozhodnutia bude môcť povoliť sprístupnenie úradného dokumentu tretej strane. Sprístupnenie bude zabezpečené alebo jednorazovým alebo časovo obmedzeným prístupovým kódom alebo jednorazovým prístupovým kódom s obmedzenou časovou platnosťou po prvom použití. Spôsob zabezpečenia sprístupnenia na základe niektorej z možností bude určený počas fázy analýza a dizajn projektu. Bude to môcť urobiť pre správu, u ktorej sa mu zobrazia metaúdaje bez ohľadu na spôsob prihlásenia. Funkcionalita potrebná pre túto činnosť je:

- zadanie požiadavky na vygenerovanie prístupové kódu
- vygenerovanie náhodného neuhádnuteľného prístupového kódu vrátane počtu opakovaní a dĺžky životnosti (podľa toho, čo je relevantné)
- priradenie prístupového kódu ku určenej správe
- kontrola životného cyklu prístupového kódu
- zobrazenie prístupového kódu na obrazovku s možnosťou skopírovania
- zaslanie prístupového kódu na zadanú adresu elektronickej pošty
- zobrazenie vytvorených prístupových kódov k správe a stav ich využitia

Ktokoľvek, kto bude mať prístupový kód, bude môcť jeho prostredníctvom pristupovať k úradnému dokumentu, ku ktorému je prístupový kód priradený. Potrebná funkcionalita prostredníctvom grafického rozhrania je:

- overenie prístupového kódu

    - overenie platnosti
    - overenie použiteľnosti
    - určenie správy
- zaznamenanie použitia prístupového kódu vrátane
    - zrušenie možnosti použitia prístupového kódu (v prípade jednorázovosti prístupového kódu alebo posledného využitia prístupového kódu)
    - nastavenie konca časovej platnosti prístupového kódu (v prípade obmedzenej životnosti prístupového kódu po jeho prvom použití)
    - zníženie možného počtu použití kódu (v prípade možnosti viacnásobného použitia prístupového kódu)
- zobrazenie metaúdajov správy
- zobrazenie obsahu správy resp. jednotlivých príloh na základe voľby vykonanej v zobrazení metaúdajov správy
- uloženie samotnej správy, ľubovoľnej prílohy alebo celej správy vrátane príloh na lokálne úložisko (pevný disk, USB kľúč a podobne)
- informatívne overenie platnosti elektronického podpisu/elektronických podpisov na správe alebo ľubovoľnej prílohe
- zobrazovanie chybových hlásení v prípade chýb pri vyhľadaní, zobrazení a podobne

Pre tretie strany budú služby poskytované aj prostredníctvom API, pričom bude potrebné zabezpečiť:

- overenie prístupového kódu
    - overenie platnosti
    - overenie použiteľnosti
    - určenie správy
- zaznamenanie použitia prístupového kódu vrátane
    - zrušenie možnosti použitia prístupového kódu (v prípade jednorázovosti prístupového kódu alebo posledného využitia prístupového kódu)
    - nastavenie konca časovej platnosti prístupového kódu (v prípade obmedzenej životnosti prístupového kódu po jeho prvom použití)
    - zníženie možného počtu použití kódu (v prípade možnosti viacnásobného použitia prístupového kódu)
- poskytnutie celej správy vrátane metaúdajov a príloh

Funkcionality popísané pre grafické rozhrania môžu byť zabezpečené jedným alebo viacerými grafickými rozhraniam, ktoré poskytne/poskytnú všetku požadovanú funkcionalitu. Grafické rozhranie musí byť dodané tak, aby tvorilo celok s portálom ÚPVS[5]. Grafické rozhranie bude poskytované v dvoch jazykových mutáciách, slovenskej a anglickej. V prípade grafického rozhrania pre mobilné telefóny je možné riešiť grafické rozhranie samostatnou aplikáciou[6], ktorá nebude súčasťou portálu ÚPVS, pri dodržaní požadovanej funkcionality pre grafické

[5] V súlade s aktuálnou verziou ID-SK - https://idsk.gov.sk/, https://www.mirri.gov.sk/sekcie/oddelenie-behavioralnych-inovacii/jednotny-dizajn-manual-elektornickych-sluzieb-verejnej-spravy/index.html, https://www.mirri.gov.sk/sekcie/oddelenie-behavioralnych-inovacii/index.html.

[6] Ak bude na základe výsledkov analýzy nutná natívna mobilná aplikácia (napr. načítanie QR kódu prostredníctvom fotoaparátu mobilného telefónu, alebo push notifikácie, a pod), tak bude zo strany obstarávateľa preferencia pre mobilné operačné systémy s aktuálne najväčším podielom na trhu (Android s trhovým podielom cca 85% a iOS s podielom cca 10%). Nevytvárať samostatnú novú mobilnú aplikáciu, ale urobiť ako súčasť „Slovensko v mobile“

rozhranie. Grafické rozhranie pre mobilné telefóny musí byť vytvorené tak, aby umožňovalo snímanie QR kódu a jeho automatické zadanie pre vyhľadanie správy s následným zobrazením správy (v prípade už autentifikovaného používateľa).

Riešenie vrátane dátového modelu musí byť vybudované v súlade so všetkými relevantnými štandardami vydanými na základe zákona č. 95/2019 Z.z. o ITVS, platnými v čase ukončenia funkčnej špecifikácie projektu.

Riešenie musí poskytnúť funkcionalitu aj pre zobrazenie vyhľadanej, alebo lokálne uloženej správy a jej príloh (rozhodnutia) aj po exspirácií platnosti autorizačných prvkov (elektronická pečať/ kvalifikovaná elektronická pečať, elektronický podpis/ kvalifikovaný elektronický podpis)

Riešenie musí poskytovať (API aj pre ďalšie použitie mimo KSDR) funkcionalitu pre konverziu rozhodnutia (rozhodnutia sú štandardne v XML formáte) do PDF formátu (aby si aj cudzinec vedel zobraziť rozhodnutie, pre slovenských občanov je funkcionalita zobrazenia rozhodnutia súčasťou elektronickej schránky).

- Vrátane možnosti zaručenej elektronickej konverzie, ako je uvedené v časti funkčných požiadaviek na grafické rozhranie.

Nefunkčné požiadavky

- Grafické rozhranie (portál) musí podporovať responzívny dizajn – stránky musia byť optimalizované pre rôzne druhy zariadení. To znamená, že stránky musia byť vždy prehľadne, zrozumiteľné a vyzerať príjemne esteticky nie len na klasickom počítači, ale i na notebooku, mobilnom telefóne alebo tablete (responzívny web rozpozná, na akom zariadení sa práve zobrazuje a aká je šírka displeja, a podľa toho prispôsobí svoj obsah)[7];
- Pre mobilné operačné systémy s aktuálne najväčším podielom na trhu (Android s trhovým podielom cca 85%, iOS s podielom cca 10%) vytvoriť samostatné grafické rozhranie (mobilnú aplikácia pre mobilné zariadenia/ mobilné telefóny) obsahujúce základnú/ kľúčovú a najpoužívanejšiu funkčnosť[8];
- Riešenie musí byť v súlade s „Cloud Native“[9];
- Riešenie musí zabezpečiť bezpečné používanie osobných údajov;

[7] V súlade s aktuálnou verziou ID-SK - https://idsk.gov.sk/.

[8] Ak bude na základe výsledkov analýzy nutná natívna mobilná aplikácia.

[9] Rámcové inštrukcie, ktoré je potrebné dodržať napríklad ako uvedené na https://thenewstack.io/10-key-attributes-of-cloud-native-applications/.

- Riešenie musí zabezpečiť poskytovanie vhodnej formy otvorených údajov v podobe štatistických prehľadov bez zverejnenia osobných údajov (napr. počty rozhodnutí podľa odosielateľa/ OVM, počty sprístupnení tretím stranám, počty zobrazení);
- Taktiež musí byť realizované bezpečné oddelenia interných údajov a údajov urečených pre verejnosť;
- KSDR realizovať v súlade s aktuálne platnými štandardami, ktorými sú:
    - Vyhláška č.78/2020 Z.z. o štandardoch pre ITVS,
    - Vyhláška č.85/2020 Z.z. o riadení projektov,
    - Vyhláška č.179/2020 Z.z. o obsahu bezpečnostných opatrení ITVS.

Integračné požiadavky

Z pohľadu využívania existujúcich komponentov ÚPVS je potrebné, aby pre svoje správne fungovanie bol komponent sprístupňovania doručovaných rozhodnutí integrovaný na nasledovné časti ÚPVS prípadne iné IS VS:

- komponent centrálneho úradného doručovania (CÚD)
    - identifikátor listinne doručovaného dokumentu
    - identifikátor pôvodnej správy
- modul elektronického doručovania (MED)
    - identifikátor doručovanej správy
    - metaúdaje doručovanej správy
- modul pre identifikáciu a autentifikáciu (IAM)
    - autentifikácia
    - načítanie údajov identity
- spoločné objektové úložisko ÚPVS (OST)
    - správa
    - prílohy
    - zablokovanie vymazania
- centrálnu elektronickú podateľňu (CEP)
    - overenie elektronického podpisu
    - realizácia zaručenej konverzie
- Modul elektronického formulára (MEF)
    - realizácia zaručenej konverzie
- portál ÚPVS (PK)
    - prihlásenie (SSO)
    - zakomponovanie GUI v podobe zásuvného modulu
    - jednotný dizajn
- Portfólio klienta
    - Zobrazovanie EUD pre užívateľa
    - Iné
- CSRÚ

    - PSČ z registra adries pre potreby úplnosti zobrazovanej doručovanej adresy z listinného doručovania CÚD
- SNCA
    - validácia kvalifikovaného elektronického podpisu a kvalifikovanej elektronickej pečate pri zaručenej konverzií
    - zobrazenie platnosti kvalifikovaných elektronických podpisov

Požiadavky na bezpečnosť

Riešenie bude v oblasti bezpečnosti a ochrany dát na technologickej úrovni využívať existujúce bezpečnostné politiky, komponenty a technológie nasadzované centralizovane v rámci ÚPVS.

Z hľadiska týchto komponentov budú v bezpečnostnej architektúre využívané nasledujúce mechanizmy:

- Autentifikácia používateľov prostredníctvom modulu IAM
    - eID
    - alternatívne spôsoby autentifikácie (napríklad MoID, alternatívny autentifikátor[10])
    - autentifikácia zamestnancov VS
- Autentifikácia prostredníctvom čísla rovnopisu a zadaním osobných údajov – bude umožnený prístup iba ku konkrétnemu rozhodnutiu
- Riadenie prístupu pre tretie strany – na základe uvedenia čísla rovnopisu a prístupového kódu pre tretie strany, prístupový kód bude nastavený tak, aby sa minimalizovala možnosť jeho zneužitia (napríklad jednorazové použitie, hodina platnosti po prvom použití a podobne)
- Riadenie prístupu pre oprávnených používateľov – na základe rolí používateľa vychádzajúcej z organizačného začlenenia, podporované autentifikačným modulom,
- Logovanie činností – bude zabezpečené centralizované zaznamenávanie činnosti jednotlivých používateľov s využitím mechanizmov na vyhodnocovanie záznamov a identifikácie bezpečnostných incidentov,
- Zabezpečenie sieťovej komunikácie pri prístupe k systému – budú využité mechanizmy pre budovanie sietí NASES,
- Ochrana proti škodlivému kódu a bezpečnostným prienikom – budú využívané centralizované riešenia na ochranu prevádzkového prostredia, v ktorom bude aplikácia prevádzkovaná,

Základnými východiskami pre riešenie bezpečnosti IS sú v súčasnosti platné právne predpisy najmä zákon č. 122/2013 o ochrane osobných údajov, zákon č. 95/2019 o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (zákon o ITVS) a

[10] Alternatívny autentifikátor napr. v podobe autentifikácie prostredníctvom čísla rovnopisu a zadaním osobných údajov (osoba, ktorá sa autentifikuje, pozná svoje osobné údaje). Alternatívna autentifikácia v prípade tretích strán: zadanie čísla rovnopisu a vygenerovaného prístupového kódu pre tretie strany (obmedzená časová platnosť, alebo jednorazové použitie, ..).

s ním súvisiace vyhlášky[11] a ďalej ISO/IES 27000, Common Criteria a OWASP Guides a dodatočných požiadaviek prevádzkovateľa systému - NASES. Bezpečnostná architektúra bude vychádzať z týchto pravidiel a v rámci pripraveného Bezpečnostného projektu, ktorého vypracovanie a aplikovanie bude podmienkou sprevádzkovania predovšetkým registrov a evidencií združených v Module evidencie osobných údajov.

Zabezpečenie prevádzky bude realizované ako rozšírenie prevádzky ÚPVS, ktorú NASES zabezpečuje a na ktorú má NASES rozpočtované finančné prostriedky. Dodávateľ rozšíri bezpečnostný plán ÚPVS tak, aby pokryl aj funkcionalitu a systémy Komponentu sprístupňovania doručovaných rozhodnutí.

Harmonogram realizácie

Budovanie KSDR sa bude realizovať vo viacerých etapách v zmysle štandardov pre riadenie informačno-technologických projektov.

Etapa 1: Analýza a dizajn
(08/2021 – 10/2021)

- Organizačné zriadenie projektového vedenia a komunikačných pravidiel,
- Dôsledná príprava a zabezpečenie metodiky riešenia jednotlivých fáz,
- Analýza požiadaviek a detailná analýza,
- Detailný návrh riešenia,
- Návrh migrácie ER (inicializačné ETL, pravidelné inkrementy)
- Iné (v zmysle návrhu dodávateľa)

Etapa 2: Implementácia a testovanie
(11/2021 – 07/2022)

- Príprava prostredia,
- Implementácia modulov na základe nastavených procesov,
- Implementácia interných integrácii,
- Implementácia rozhraní pre externé integrácie,
- Implementácia migračných ETL,
- Nasadenie služieb KSDR do testovacieho prostredia.
- Iné (v zmysle návrhu dodávateľa)

Testovanie
(05/2022 – 07/2022)

- Funkčné testovanie (FAT),
- Systémové a integračné testovanie (SIT),
- Testovanie migračných ETL (inicializácia, pravidelný inkrement),

[11] Vyhláška č.78/2020 Z.z. o štandardoch pre ITVS, Vyhláška č.85/2020 Z.z. o riadení projektov, Vyhláška č.179/2020 Z.z. o obsahu bezpečnostných opatrení ITVS (ktoré nahradili 55/2014 Z.z.).

- Záťažové a výkonnostné testovanie,
- Bezpečnostné testovanie,
- Používateľské testy funkčného používateľského rozhrania (UX),
- Užívateľské akceptačné testovanie (UAT),
- Identifikácia nedostatkov, konsolidácia a oprava chýb,
- Akceptácia riešenia,
- Príprava a realizácia školení.

Etapa 3: Nasadenie a post-implementačná podpora
(08/2022 – 09/2022)

- Spustenie produktívnej prevádzky,
- Zvýšená podpora používateľom.

Technická infraštruktúra

Riešenie bude prevádzkované vo virtuálnom prostredí na infraštruktúre, pripravenej NASES. Infraštruktúra bude pripravená ako rozšírenie infraštruktúry ÚPVS.

Požiadavky na dokumentáciu

V zmysle vyhlášky 85/2020 Z. z. a vzhľadom na rozsah a kontext KSDR je pre účely implementácie projektu požadovaná nasledovná dokumentácia v súlade s aktuálnymi formulármi vydanými MIRRI[12]:

Analýza a dizajn

- Detailný návrh riešenia (DNR) mapovaný na Katalóg požiadaviek
- Plán testov
- Predbežná analýza rizík
- Prieskum navrhovaného riešenia s účasťou relevantných cieľových skupín (napr. občan, podnikateľ, OVM)

Implementácia a testovanie

- Vývoj, migrácia údajov a integrácia
    - vyhotovenie dokumentácie k podporným prostriedkom a konverzným programom (ak budú pri realizácii použité)
    - vyhotovenie kompletnej podkladovej dokumentácie k používateľskému rozhraniu (UX),
- Testovanie
    - Testovacie scenáre

[12] https://www.mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/riadenie-kvality-qa/index.html

    - Testovacie protokoly
- Iná dokumentácia
    - Aplikačná príručka
    - Používateľská príručka
    - Inštalačná príručka a pokyny na inštaláciu (úvodnú/opakovanú)
    - Konfiguračná príručka a pokyny pre diagnostiku
    - Integračná príručka
    - Prevádzkový opis a pokyny pre servis a údržbu
    - Pokyny pre obnovu v prípade výpadku alebo havárie (Havarijný plán)
    - Bezpečnostný projekt (v súlade s vyhláškou ÚPVII č. 179/2020 Z.z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy)
    - Zoznam funkčných zdrojových kódov (vrátane)
    - Zoznam licencií (vrátane)
- Školenia
    - Harmonogram a štruktúra školení
    - Školiace materiály a výstupy

Nasadenie a post-implementačná podpora
    - DFŠ (as implemented)

Požiadavky na riešiteľský tím
Experti:

Riešiteľský tím má pozostávať z nasledovných pozícií:

- **IT architekt - senior**
- **IT architekt - junior**
- **IT analytik – senior**
- **IT analytik - junior**
- **IT programátor / vývojár – senior**
- **IT programátor / vývojár - junior**
- **UX/UI Dizajnér – senior**
- **Špecialista pre integrácie - senior**
- **IT tester - senior**
- **IT tester - junior**
- **Projektový manažér IT projektu - senior**
- **Špecialista pre IT bezpečnosť - senior**

IT architekt – senior

Navrhuje dizajn a architektúru Diela ako celku. Vyberá jednotlivé komponenty ÚPVS, technológie, ich vzájomné usporiadanie a prepojenie a pod. Dizajnér systémovej architektúry je zodpovedný za škálovateľnosť výkonu ÚPVS, jeho komplementaritu, možnosti ďalšieho rozvoja a rozširovania, kvalitu ÚPVS na technologickej úrovni a pod. Dizajnér systémovej architektúry je oprávnený zmeniť, zadefinovať konfiguráciu jednotlivých komponentov

architektúry z dôvodu optimalizácie a ladenia výkonu, stability Diela a pod. Typické činnosti dizajnéra systémovej architektúry sú najmä:

- návrh a aktualizácia architektúry ÚPVS,
- kontinuálna optimalizácia architektúry počas celého životného cyklu ÚPVS,
- tvorba architektonickej dokumentácie,
- v prípade nutnej zmeny architektúry ÚPVS, výber vhodnej alternatívy a manažovanie zmeny v rámci architektúry Diela,
- spolupráca pri zabezpečení požadovanej kvality a štandardov vývojárskych výstupov,
- spolupráca pri integrácii zdrojových kódov a riešenie konfliktov zdrojového kódu dodávaných jednotlivými vývojármi,
- údržba build systému ÚPVS,
- informuje Objednávateľa o jednotlivých zmenách a rizikách v architektúre ÚPVS,
- eskalácia problémov a otvorených otázok súvisiacich s návrhom dizajnu,
- reportovanie projektovému manažérovi o stave vykonanej práce.

Minimálna požadovaná úroveň štandardov:

- minimálne 5 rokov odbornej praxe v oblasti návrhu architektúry riešenia informačných systémov,
- minimálne 3 profesionálne praktické skúsenosti v oblasti návrhu architektúry a dizajnu informačných systémov v rámci projektov realizácie informačných systémov, pričom v rámci projektov boli využité nasledujúce technológie/jazyky/frameworky: Apache, Java Spring, php frameworks, alebo ekvivalentné; HAProxy alebo ekvivalentné (napr. Apache HTTPD, Nginx...); Elastic Search alebo ekvivalentné (napr. Apache SOLR...); IntelliJ IDEA, Visual Studio Code, Eclipse alebo ekvivalentné (napr. MS Visual Studio...); PostgreSQL alebo ekvivalentné (napr. Oracle DB, MS SQL Server...); Git; jazyk Java, php alebo ekvivalentné;
- získaný a platný certifikát pre oblasť návrhu architektúry IT TOGAF alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou
- preukazuje sa životopisom alebo údajom o odbornej praxi preukazujúcej splnenie požiadavky a príslušným certifikátom.

IT architekt - junior

Navrhuje dizajn a architektúru Diela ako celku z pozície IT architekta juniora. Vyberá jednotlivé komponenty ÚPVS, technológie, ich vzájomné usporiadanie a prepojenie a pod. Dizajnér systémovej architektúry je zodpovedný za škálovateľnosť výkonu ÚPVS, jeho komplementaritu, možnosti ďalšieho rozvoja a rozširovania, kvalitu ÚPVS na technologickej úrovni a pod. Dizajnér systémovej architektúry je oprávnený zmeniť, zadefinovať konfiguráciu jednotlivých komponentov architektúry z dôvodu optimalizácie a ladenia výkonu, stability Diela a pod. Typické činnosti dizajnéra systémovej architektúry z pozície juniora sú najmä:

- návrh a aktualizácia architektúry
- kontinuálna optimalizácia architektúry počas celého životného cyklu,
- tvorba architektonickej dokumentácie,
- v prípade nutnej zmeny architektúry riešenia , výber vhodnej alternatívy a manažovanie zmeny v rámci architektúry Diela,

- spolupráca pri zabezpečení požadovanej kvality a štandardov vývojárskych výstupov,
- spolupráca pri integrácii zdrojových kódov a riešenie konfliktov zdrojového kódu dodávaných jednotlivými vývojármi,
- údržba build systému ÚPVS,
- informuje Objednávateľa o jednotlivých zmenách a rizikách v architektúre riešenia,
- eskalácia problémov a otvorených otázok súvisiacich s návrhom dizajnu,
- reportovanie projektovému manažérovi o stave vykonanej práce.

Minimálna požadovaná úroveň štandardov:

- minimálne 1 rok odbornej praxe v oblasti návrhu architektúry riešenia informačných systémov,
- minimálne 1 profesionálna praktická skúsenosť v oblasti návrhu architektúry a dizajnu informačných systémov v rámci projektov realizácie informačných systémov, pričom v rámci projektov boli využité nasledujúce technológie/jazyky/frameworky: Apache, Java Spring alebo ekvivalentné; HAProxy alebo ekvivalentné (napr. Apache HTTPD, Nginx...); Elastic Search alebo ekvivalentné (napr. Apache SOLR...); IntelliJ IDEA, Visual Studio Code, Eclipse alebo ekvivalentné (napr. MS Visual Studio...); PostgreSQL alebo ekvivalentné (napr. Oracle DB, MS SQL Server...); Git; jazyk Java, php alebo ekvivalentné;
- preukazuje sa životopisom alebo údajom o odbornej praxi preukazujúcej splnenie požiadavky

IT analytik - senior

Je zodpovedný za riadenie analytického tímu. Podieľa sa na plánovaní projektu. Poskytuje odhady činností a prideľuje kapacitné zdroje analytickým úlohám. Reportuje projektovému manažérovi stav a priebeh analýz a eskaluje problémy súvisiace s tvorbou analýz. Činnosti sú nasledovné:

- riadenie analytického tímu,
- poskytovanie odhadov prác a prideľovanie analytických kapacít na jednotlivé úlohy,
- poskytovanie informácií o stave prác a problémoch v oblasti analýzy aplikačného programového vybavenia,
- zabezpečenie požadovanej kvality a štandardov analytických výstupov,
- reportovanie projektovému manažérovi a Objednávateľovi.

Minimálna požadovaná úroveň štandardov:

- minimálne 4 rokov odbornej praxe v oblasti analýzy informačných systémov,
- minimálne 2 profesionálne praktické skúsenosti zamerané na analýzu informačných systémov v projektoch realizácie informačných systémov, pričom ich súčasťou bolo aj riadenie analytického tímu a spracovanie analytickej dokumentácie,
    - z toho minimálne 1 profesionálna praktická skúsenosť v oblasti analýzy informačného systému umožňujúceho fulltextové vyhľadávanie,
    - z toho minimálne 1 profesionálna praktická skúsenosť v oblasti analýzy informačného systému umožňujúceho tvorbu elektronických formulárov,
- získaný a platný certifikát OMG-Certified UML Professional 2 Foundation level alebo vyšší (Unified Modeling Language) alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou – preukazuje sa

u minimálne jedného IT analytika – seniora, ktorý garantuje tvorbu softvérových analýz v zmysle štandardov a metodík,
- preukazuje sa životopisom alebo údajom o odbornej praxi preukazujúcej splnenie požiadavky a príslušným certifikátom.

IT analytik - junior

Analyzuje požiadavky v príprave analyticko-technickej dokumentácie na vyvíjané Dielo. V prípade potreby sa podieľa na plánovaní projektu a poskytuje odhady prácnosti k analytickým činnostiam. Zabezpečuje najmä tieto činnosti:

- komunikácia so zákazníkom pri zisťovaní funkčných a nefunkčných požiadaviek,
- zdokumentovanie funkčných a nefunkčných požiadaviek zákazníka,
- analýzu a špecifikáciu riešenia jednotlivých funkčných a nefunkčných požiadaviek,
- príprava analytickej dokumentácie a zabezpečenie požadovanej kvality a štandardov analytických výstupov,
- konzultácie s UX dizajnérom pri analýze,
- upozorňuje objednávateľa na možné riziká riešenia funkčnej a nefunkčnej požiadavky,
- konzultácie pre objednávateľa týkajúce sa riešenia funkčných a nefunkčných požiadaviek,
- konzultácie pre vývojový tím týkajúce sa riešenia funkčných a nefunkčných požiadaviek,
- podporu pri návrhu a definícii testovacích scenárov,
- súčinnosť pri základnom funkčnom manuálnom testovaní,
- eskalácia problémov/otvorených otázok súvisiacich s analýzou,
- reportovanie projektovému manažérovi o stave vykonanej práce,

Výsledkom činností je najmä špecifikácia správania sa systému. Úzko spolupracuje so všetkými expertmi projektového tímu podieľajúcimi sa na dodávke Diela.

Minimálna požadovaná úroveň štandardov:

- minimálne 1 rok odbornej praxe v oblasti biznis analýzy alebo analýzy softvérových riešení,
- minimálne 1 profesionálna praktická skúsenosť v oblasti biznis analýzy a analýzy softvérových riešení v projektoch realizácie informačných systémov
- preukazuje sa životopisom alebo údajom o odbornej praxi preukazujúcej splnenie požiadavky.

IT programátor/vývojár - senior

Je zodpovedný za riadenie vývojového tímu. Podieľa sa na plánovaní projektu. Poskytuje odhady činností a prideľuje zdroje vývojovým úlohám. Spolupracuje s manažérom plánovania verzií pri tvorbe obsahu verzie a časovom pláne verzie. Reportuje projektovému manažérovi stav a priebeh realizácie a eskaluje problémy súvisiace s vývojom. Činnosti sú nasledovné:

- riadenie vývojového tímu,
- poskytovanie odhadov prác a prideľovanie vývojárskych kapacít na jednotlivé úlohy,
- identifikuje a analyzuje možné technické problémy,
- spolupracuje s IT architektom na zabezpečení kvality kódu,
- podieľa sa na tvorbe dokumentácie k vytvorenému softvéru,
- poskytovanie informácií o stave prác a problémoch v oblasti vývoja,
- reportovanie projektovému manažérovi a Objednávateľovi.

Minimálna požadovaná úroveň štandardov:

- minimálne 4 roky odbornej praxe v oblasti programovania informačných systémov,
- minimálne 3 profesionálne praktické skúsenosti na projekte realizácie informačného systému, v rámci ktorého boli využité nasledujúce technológie/jazyky/frameworky:
  BE developer: Java 8 alebo vyššie; Spring, Spring boot alebo ekvivalentné (napr. JEE); Apache Tomcat alebo ekvivalentné (napr. IBM WebSphere, JBoss AS, Oracle WebLogic); Maven alebo ekvivalentné (napr. Gradle); IntelliJ Idea, alebo ekvivalentné (napr. Eclipse, NetBeans); PostgreSQL alebo ekvivalentné (napr. Oracle DB, IBM DB2, Maria DB, MySQL); Git, Git-flow alebo ekvivalentné (napr. SVN);

  FE developer: PHP 7, symfony3+ alebo ekvivalentné (napr. Laravel) alebo DRUPAL 8+, Javascript (framework napr. vue.js, React.js), HTML5, CSS3, CSS pre pocesory (Sass),

  - z toho minimálne 1 profesionálna praktická skúsenosť v oblasti programovania informačného systému umožňujúceho fulltextového vyhľadávania,
  - z toho minimálne 1 profesionálna praktická skúsenosť v oblasti programovania informačného systému umožňujúceho tvorbu elektronických formulárov,
- preukazuje sa životopisom alebo údajom o odbornej praxi preukazujúcej splnenie požiadavky alebo príslušným certifikátom.

IT vývojár/programátor - junior

Je odborník-junior v programovaní aplikačného programového vybavenia. Transformuje návrh riešenia od IT analytika seniora, na základe detailnej špecifikácie a vývojových diagramov, do podoby uceleného a korektne pracujúceho softwarového riešenia. Kódovanie vykonáva v programovacom jazyku, výsledkom čoho je textový kód, ktorý následne kompiluje do podoby spustiteľného programu/aplikácie. V prípade potreby sa podieľa na plánovaní projektu a poskytuje odhady prácnosti k programátorským činnostiam Typické činnosti sú najmä:

- implementácia pridelenej funkcionality,
- príprava diagramov popisujúcich vstupy/výstupy a logiku systému,
- identifikácia a analýza možných technických problémov,
- upozorňuje zákazníka na možné riziká implementovanej časti,
- kódovanie s dodržiavaním štandardov vývoja softvéru,
- unit testovanie funkčnosti vlastnej časti kódu a oprava identifikovaných chýb a nedostatkov,
- zmena definovaných špecifikácií v priebehu vývoja,
- tvorba technickej dokumentácie k vytvorenému softwaru alebo jeho častí,
- súčinnosť pri testovaní a zapracovanie zistených pripomienok,
- zabezpečenie požadovanej kvality a štandardov vývojárskych výstupov,
- integrácia zdrojových kódov a riešenie konfliktov zdrojového kódu,
- eskalácia problémov súvisiacich s vývojom,
- reportovanie projektovému manažérovi o stave vykonanej práce.

Minimálna požadovaná úroveň štandardov:

- minimálne 1 rok odbornej praxe v oblasti programovania informačných systémov,
- minimálne 1 profesionálna praktická skúsenosť na projekte realizácie informačného systému, v rámci ktorého boli využité nasledujúce technológie/jazyky/frameworky:

BE developer: Java 8 alebo vyššie; Spring, Spring boot alebo ekvivalentné (napr. JEE); Apache Tomcat alebo ekvivalentné (napr. IBM WebSphere, JBoss AS, Oracle WebLogic); Maven alebo ekvivalentné (napr. Gradle); IntelliJ Idea, alebo ekvivalentné (napr. Eclipse, NetBeans); PostgreSQL alebo ekvivalentné (napr. Oracle DB, IBM DB2, Maria DB, MySQL); Git, Git-flow alebo ekvivalentné (napr. SVN);

FE developer: PHP 7, symfony3+ alebo ekvivalentné (napr. Laravel) alebo DRUPAL 8+, Javascript (framework napr. vue.js, React.js), HTML5, CSS3, CSS pre pocesory (Sass)

- preukazuje sa životopisom alebo údajom o odbornej praxi preukazujúcej splnenie požiadavky

Expert pre UX/UI dizajn - senior

UX/UI dizajnér je zodpovedný za návrh a dizajn používateľského rozhrania. V spolupráci s dedikovaným tímom na strane Objednávateľa pripravuje UX stratégiu, kvalitatívny a kvantitatívny prieskum, definuje cieľové skupiny, vytvára persóny, user stories a použitím výskumných metód zisťuje a priorizuje potreby užívateľov. Získané dáta spracúva a využíva pri tvorbe klikateľných prototypov, ktoré následne overuje formou užívateľského testovania.

Minimálna požadovaná úroveň štandardov:

- minimálne 3 roky odbornej praxe pri tvorbe návrhu a dizajnu používateľského rozhrania,
- preukazuje sa životopisom alebo údajom o odbornej praxi preukazujúcej splnenie podmienky účasti.

Špecialista pre integrácie - senior

Spravuje, pripravuje a zodpovedá za integračnú dokumentáciu. Zabezpečuje komplexné práce súvisiace s riadením integrácií informačných systémov. Je zodpovedný za proces integrácie vo fáze prechodu integračných projektov do produkčnej prevádzky, komunikuje so všetkými zúčastnenými subjektmi pri realizácii integrácii v rámci dodávky Diela. Je zodpovedný za návrh a optimalizáciu integračných rozhraní.

Minimálna požadovaná úroveň štandardov:

- minimálne 3 roky odbornej praxe pri integrácii informačných systémov,
- minimálne 2 profesionálne praktické skúsenosti v oblasti návrhu integrácií informačných systémov v rámci projektov realizácie informačných systémov,
- preukazuje sa životopisom alebo údajom o odbornej praxi preukazujúcej splnenie požiadavky.

IT tester - senior

Overuje kvalitu produktu. Štruktúra činností testera - seniora je podobná ako pri vyššie spomínaných pozíciách, t.j. príprava podmienok pre testovanie, vlastné testovanie,

vyhodnotenie výsledkov a ich postúpenie relevantným členom tímu. Tester senior, prípadne ďalší členovia tímu, testujú systém v rámci alfa fázy, to sa považuje za interné testovanie. V rámci beta testovania sa systém dáva k dispozícii osobám z externého prostredia, najmä zákazníkovi, prípadne iným relevantným osobám. Typické činnosti sú najmä:

- tvorba testovacích scenárov pre manuálny a/alebo automatizovaný spôsob testovania a ich pravidelná aktualizácia,
- vykonávanie a zodpovednosť za integračné testy, smoke testy, regresné testy, funkčné a nefunkčné testy,
- programovanie skriptov / testov pre automatizované testovanie a záťažové testy,
- testovanie softvérového produktu – funkčnosť, výkonnosť/záťaž, bezpečnosť, použiteľnosť,
- odhaľovanie a izolovanie chýb a nedostatkov softvérového produktu,
- reportovanie nájdených chýb a ich analýza/interpretácia,
- eskalácia problémov súvisiacich s testovaním,
- reportovanie projektovému manažérovi o stave vykonanej práce.

Minimálna požadovaná úroveň štandardov:

- minimálne 3 roky odbornej praxe s testovaním aplikácií a dizajnovaním testovacích scenárov na základe dokumentácie písanej v UML jazyku alebo jeho ekvivalent,
- minimálne 2 profesionálne praktické skúsenosti v oblasti testovania informačných systémov na projektoch realizácie informačného systému,
- získaný a platný certifikát ISTQB alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou - preukazuje sa u minimálne jedného IT testera - seniora, ktorý garantuje testovanie softvéru v zmysle štandardov a metodík,
- preukazuje sa životopisom alebo údajom o odbornej praxi preukazujúcej splnenie požiadavky a príslušným certifikátom.

IT tester - junior

Overuje kvalitu produktu. Štruktúra činností testera - juniora je podobná ako pri vyššie spomínaných pozíciách, t.j. príprava podmienok pre testovanie, vlastné testovanie, vyhodnotenie výsledkov a ich postúpenie relevantným členom tímu. Tester - junior, prípadne ďalší členovia tímu, testujú systém v rámci alfa fázy, to sa považuje za interné testovanie. V rámci beta testovania sa systém dáva k dispozícii osobám z externého prostredia, najmä zákazníkovi, prípadne iným relevantným osobám. Typické činnosti sú najmä:

- tvorba testovacích scenárov pre manuálny a/alebo automatizovaný spôsob testovania a ich pravidelná aktualizácia,
- vykonávanie a zodpovednosť za integračné testy, smoke testy, regresné testy, funkčné a nefunkčné testy,
- programovanie skriptov / testov pre automatizované testovanie a záťažové testy,
- testovanie softvérového produktu – funkčnosť, výkonnosť/záťaž, bezpečnosť, použiteľnosť,
- odhaľovanie a izolovanie chýb a nedostatkov softvérového produktu,
- reportovanie nájdených chýb a ich analýza/interpretácia,
- eskalácia problémov súvisiacich s testovaním,
- reportovanie projektovému manažérovi o stave vykonanej práce.

Minimálna požadovaná úroveň štandardov:

- minimálne 1 rok odbornej praxe s testovaním aplikácií a dizajnovaním testovacích scenárov na základe dokumentácie písanej v UML jazyku alebo jeho ekvivalent,
- minimálne 1 profesionálna praktická skúsenosť v oblasti testovania informačných systémov na projektoch realizácie informačného systému,
- preukazuje sa životopisom alebo údajom o odbornej praxi preukazujúcej splnenie požiadavky.

Projektový manažér IT projektu - senior

Projektový manažér je hlavný koordinátor a manažér v rámci celého procesu dodávky. Koordinuje a zodpovedá za výkon činnosti všetkých pracovných tímov a ich expertov podieľajúcich sa na dodávke Diela. Projektový manažér má zodpovednosť za plánovanie, realizáciu a ukončenie projektu. Projektový manažér sa často zúčastňuje aktivít, ktoré produkujú konečný výsledok a tým sa snaží zabezpečiť pokrok, vzájomné interakcie a úlohy jednotlivých strán tak, že znižuje riziko celkového zlyhania projektu, maximalizuje výhody, pridanú hodnotu projektu a minimalizuje náklady. Je zodpovedný za prípravu detailného projektového plánu, sleduje jeho dodržiavanie a vykonáva jeho aktualizáciu. Projektový manažér je zodpovedný za sledovanie pokroku projektu, reportovanie pokroku, identifikáciu a elimináciu rizík. Projektový manažér zostavuje projektový tím Zhotoviteľa, je zodpovedný za výber osôb a ich kvalitatívne vlastnosti. Projektový manažér má oprávnenie vykonať personálne zmeny v projektovom tíme. Projektový manažér má oprávnenie vykonať zmeny v organizácii a riadení projektového tímu Zhotoviteľa. Projektový manažér je zodpovedný za korektné vykazovanie kapacít v projektovom nástroji vrátane vykonávania pravidelnej kontroly. Projektový manažér je zodpovedný za pridelenie, sledovanie, odpočtovanie úloh členom projektového tímu vrátane vykonávania pravidelnej kontroly. Zodpovedá za výstupy z pohľadu procesov OPII a správnosť dodávky Diela.

Minimálna požadovaná úroveň štandardov:

- minimálne 3 rokov odbornej praxe v riadení projektov v oblasti informačných technológií,
- minimálne 3 profesionálne praktické skúsenosti s riadením projektov v oblasti realizácie informačných systémov zameraných na analýzu, návrh a implementáciu softvérového riešenia v pozícii projektového manažéra
- získaný a platný certifikát (napr. PRINCE 2, IPMA, PMI, PMP alebo obdobný certifikát) na odbornú spôsobilosť pre riadenie projektov alebo ekvivalent daného certifikátu vydaný medzinárodnou uznávanou akreditačnou a certifikačnom autoritou,
- preukazuje sa životopisom alebo údajom o odbornej praxi preukazujúcej splnenie požiadavky a príslušným certifikátom.

Špecialista pre IT bezpečnosť – senior

Vykonáva analýzu bezpečnostných rizík v IT oblasti, spravuje nástroje IT bezpečnosti (napr. antivírus, bezpečnostné skeny, nástroje na zaznamenávanie zmien atď.). Vyšetruje bezpečnostné incidenty a ich riešenie v spolupráci so systémovými administrátormi. Zodpovedá za konfiguráciu a vykonávanie pravidelných bezpečnostných skenov (VUL skeny /PEN testy). Pravidelne pripravuje reporty a revíziu existujúcich bezpečnostných dokumentov.

Minimálna požadovaná úroveň štandardov:

- minimálne 5 rokov odbornej praxe ochrany bezpečnosti informačných systémov,
- minimálne 3 profesionálne praktické skúsenosti v oblasti návrhu architektúry bezpečnosti informačných systémov v rámci projektov realizácie informačných systémov,
- získaný a platný certifikát CISM alebo ekvivalent daného certifikátu vydávaný medzinárodne uznávanou organizáciou,
- preukazuje sa životopisom alebo údajom o odbornej praxi preukazujúcej splnenie požiadavky a príslušným certifikátom.

Príloha č. 1 - Katalóg požiadaviek