Predmet zákazky: „**Centrálny podpisový komponent a implementácia vymenovaných možností autorizácie**“

1 SKRATKY

Skratka	**Popis**
AFPM	Autorizácia funkciou prístupového miesta (historicky používané označenie "Klik")
API	Application programming interface [Angl.], Aplikačné programovacie rozhranie
ASiC	Associated signature containers [Angl.], Pridružené podpisové kontajnery
BOK	Bezpečnostný osobný kód
CAdES	CMS advanced electronic signatures [Angl.], sada rozšírení podpísaných údajov syntaxe kryptografických správ
CAMP	Centrálna API manažment platforma
CEP	Centrálna elektronická podateľňa
CPK	Centrálny podpisový komponent
DTBS	Data to be signed representation [Angl.], hash dokumentu
eDoPP	Elektronický doklad o povolení pobytu
eID	Elektronický občiansky preukaz
eIDAS	Electronic IDentification, authentication and trust services [Angl.], Európsky štandard pre elektronickú komunikáciu
ESI	Electronic signatures and infrastructures [Angl.], Elektronické podpisy a infraštruktúry
FO	Fyzická osoba
G2G	Government to government [Angl.], komunikácia verejnej správy medzi sebou pomocou middleware platformy
GUI	Graphical user interface [Angl.], grafické užívateľské rozhranie
HSM	Hardware security module [Angl.], špecializované hardvérové zariadenia, ktoré využívajú silné fyzické a logické bezpečnostné techniky na ochranu dôležitých kľúčov pred nezákonným prístupom a zmenami.
IAM	Identity access management [Angl.], zabezpečenie centrálnej správy identít, autentifikačných údajov a autorizácií
IS	Informačný systém
ISVS	Informačný systém verejnej správy
KCCKB	Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
KEP	Kvalifikovaný elektronický podpis
META IS	Centrálny metainformačný systém verejnej správy
MVP	Minimum viable product [Angl.], produkt v minimálnom použiteľnom hu
NBU	Národný bezpečnostný úrad

NFC	Near field communication [Angl.], technológia na bezpečnú a rýchlu bezdrôtovú komunikáciu do vzdialenosti 4 cm.
OPZ	Opis predmetu zákazky
OVM	Orgán verejnej moci
PAdES	PDF advanced electronic signatures [Angl.], PDF dokument vhodný pre zdokonalený elektronický podpis
PO	Právnická osoba
PTK	Prípravná trhová konzultácia
RPO	Recovery Point Objective [Angl.], akceptovateľná doba od poslednej zálohy
RTO	Recovery Time Objective [Angl.], cieľový čas obnovy business procesu
QA	Quality assurance [Angl.], zabezpečenie/posúdenie kvality
QSCD	Qualified signature creation device [Angl.], kvalifikované zariadenia na vyhotovenie elektronického podpisu
REST API	Representational state transfer API, aplikačné programovacie rozhranie ktoré spĺňa obmedzenia architektonického štýlu REST
SDK	Software development kit [Angl.], súbor nástrojov pre vývoj softvéru
SSO	Single sign-on [Angl.], jednotné prihlásenie pre prihlásenie pomocou jedného ID do ktoréhokoľvek z niekoľkých súvisiacich, ale nezávislých softvérových systémov.
SW	Software
ÚPVS	Ústredný portál verejnej správy
WebSSO	IAM služba Single Sign-On (SSO) - „jednotné prihlásenie sa“
XAdES	XML advanced electronic signatures [Angl.], sada rozšírení odporúčania XML-DSig vhodná pre zaručené elektronické podpisy
ZEP	Zaručený elektronický podpis

2 PREDMET ZÁKAZKY

Prax a skúsenosti pri vybavovaní životných situácii (v zmysle § 3 písm. q) zákona č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene na doplnení niektorých zákonov v znení neskorších predpisov, ďalej ako „zákon č. 95/2019“) elektronicky občanmi ukazujú, že z pohľadu používateľa je podpisovanie podaní najnáročnejšou činnosťou pri vytváraní podania a to na portáli slovensko.sk a na špecializovaných portáloch (v zmysle § 5 ods. 3 zákona č. 305/2013 Z.z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, ďalej ako „zákon č. 305/2013 o e-Governmente“), ktoré majú implementovaný mechanizmus podpisovania prostredníctvom podpisových aplikácií (poskytovaných na stiahnutie na ÚPVS), a to najmä z dôvodu komplikovanej inštalácie komponentov určených na podpisovanie, obmedzenia prehliadačov pri inicializácii podpisovej aplikácie z webového prehliadača ako aj nutnosti poznať viaceré unikátne identifikátory ako je BOK či KEP PIN. Pri vytváraní podania je najviac neúspešných krokov z dôvodu zlyhania podpisovania.

Alternatívou, ktorá by zabezpečila jednotné, jednoduché, intuitívne a komfortné používateľské prostredie, v ktorom sa bude podpisovanie realizovať, je implementácia spoločného modulu, t.j. Centrálny podpisový komponent (CPK), v rámci jeho poskytovania sú viaceré možností vyhotovenia kvalifikovaného elektronického podpisu bez nutnosti použitia čítačky čipových kariet, a to s pomocou mobilných zariadení (s možnosťou autorizácie s využitím eID 2.0), Remote Signing ako aj zjednodušenej formy autorizácie (autorizácia funkciou prístupového miesta), ktorá zabezpečí rýchlejší a používateľsky komfortnejší spôsob podpisovania vybraných úkonov a služieb nevyžadujúcich autorizáciu na úrovni KEP, a to bez nutnosti inštalovania osobitného SW, či poznania unikátnych identifikátorov (ako napr. KEP PIN).

Riešenie bude slúžiť pre všetky komunikačné kanály a prístupové miesta ako napríklad (Slovensko v mobile, ÚPVS, špecializované portály, ISVS) a zároveň bude umožňovať využívanie nielen pre verejný, ale aj komerčný sektor, tretie strany. Verejný obstarávateľ zároveň poskytuje prílohu č. 4 „Katalóg požiadaviek“, ako podporný dokument, ktorý poukazuje na služby, ktoré sa očakávajú v rámci dodania a poskytnutia požadovaných služieb.

3 ROZSAH ZÁKAZKY

V rámci CPK verejný obstarávateľ požaduje nasledovné hlavné funkcie:

i) **implementácia CPK**, ktorý umožní výber podpisovej aplikácie na desktope, aktuálne D.Signer a Autogram a ľubovoľnej inej cez jednotné rozhrania a integračné komponenty (knižnice) CPK, podpisovanie kvalifikovaným a zdokonaleným elektronickým podpisom ako aj kvalifikovanou elektronickou pečaťou. Súčasťou podpisu môže byť aj elektronická časová pečiatka. CPK bude podporovať aj možnosť viacnásobného podpisovania, ale riadenie viacnásobného podpisovania podľa požiadaviek koncovej služby (napr. kto autorizuje a v akom poradí) bude realizované funkcionalitou konštruktora správ mimo CPK.

ii) **Implementácia autorizácie funkciou prístupového miesta** (AFPM, tiež používané označenie "Klik"), ktorá predstavuje autorizáciu v zmysle § 23 ods. 1 písm. a) bod 2 zákona č. 305/2013 Z.z. o e-Governmente. Jej funkčnosť bude zabezpečovať nový požadovaný komponent AFPM.

iii) implementácia autorizácie prostredníctvom eID 2.0 a eDoPP 2.0 (NFC KEP), ktorá predstavuje autorizáciu v zmysle § 23 ods. 1 písm. a) bod 1 zákona č.305/2013 Z.z. o e-Governmente.

iv) **implementáciu autorizácie s využitím prostriedku Remote Signing**, ktorá predstavuje autorizáciu v zmysle § 23 ods. 1 písm. a) bod 1 zákona č. 305/2013 Z.z. o e-Governmente.

v) **Vytvorenie elektronického podpisu odosielaného elektronického dokumentu**, ktorá predstavuje vytváranie kvalifikovaných pečatí pracovníkom OVM cez používateľské rozhranie v zmysle § 23 ods. 1 zákona č. 305/2013 Z.z. o e-Governmente - náhrada alebo prepoužitie (integrácia) jestvujúcej funkcionality CEP (Modul centrálnej elektronickej podateľne, aplikačná služba METAIS kód=sluzba_is_1370).

CPK poskytne integrácie, prostredníctvom ktorým bude možné po schválení a potrebných úkonoch jednoducho pridať ďalších poskytovateľov služieb spojených s podpisovaním a zároveň nebude multiplicitne implementovať funkcionalitu, ale využije integračné služby na príslušné komponenty.

4 FÁZY DODANIA PRODUKTU

Verejný obstarávateľ požaduje dodanie diela a jeho nasadenie na produkčné prostredie sa bude realizovať v troch fázach:

- 1. Fáza MVP (MVP -Minimal Viable Product) - fáza s predpokladaným termínom dodania a nasadenia do 4 mesiacov odo dňa nadobudnutia účinnosti ZMLUVY
- 2. Fáza - ďalší rozvoj po realizácii MVP fázy s predpokladaným termínom dodania a nasadenia do 10 mesiacov odo dňa nadobudnutia účinnosti ZMLUVY
- 3. Fáza – Remote signing – s predpokladaným termínom dodania a nasadenia do 16 mesiacov odo dňa nadobudnutia účinnosti ZMLUVY

Nižšie uvedené výstupy projektu sú detailne popísané v rozsahu požiadaviek, ktoré tvoria neoddeliteľnú súčasť tohto OPZ.

Verejný obstarávateľ požaduje nasledovný rozsah v rámci 1. fázy MVP (MVP-Minimal Viable Product):

- Implementácia a produkčné nasadenie aplikačných komponentov CPK
- Sprístupnenie API CPK na Centrálnej API manažment platforme (CAMP)
- Poskytnutie súčinnosti pri integrácii služieb CPK do konštruktora správ na ÚPVS
- Poskytnutie súčinnosti pri zmenách v UPVS umožňujúcich Podpis lokálneho súboru podporovanými formami autorizácie (eID a/alebo eID 2.0 a/alebo Remote signing)
- Podpísanie súboru v CPK bez možnosti prihlásenia
- Viacnásobné podpísanie dokumentu bez možnosti prihlásenia
- Implementácia SDK (pluginu do web prehliadača podporovanej verzie webového prehliadača" podľa §16 písm. d) Vyhlášky č. 78/2020) povinného pre integráciu na lokálne podpisové aplikácie poskytovateľov
- Poskytnutie súčinnosti zo strany verejného obstarávateľa pri integrácii súčasných (D.Signer, Autogram) a nových podpisových komponentov
- Integrácia na IAM a UPVS za účelom využitia štátom garantovanej identity na prihlásenie do CPK pomocou WebSSO
- Vytvorenie náhľadu na podpisovanie dát podľa vizualizačných schém (v zmysle Diagramu č. 1) pre formulár a podpisované súbory
- Vytvorenie MessageDigest - digitálny odtlačok dát určených na podpisovanie
- Overenie povolených možností autorizácie evidovaných pre danú službu v MetaIS
- Návrh dátovej štruktúry pre AFPM a vloženie príslušného formulára do MEF
- Vytvorenie autorizácie prostredníctvom funkcie prístupového miesta a jej implementácia v CPK
- Implementácia overovania auditných záznamov v CPK

- Prepoužitie (integrácia) služby pre vytvorenie elektronického podpisu odosielaného elektronického dokumentu (aplikačná služba METAIS kód=sluzba_is_1370 v CEP)
- Pripájanie časovej pečiatky (k dokumentu a/alebo k podpisu),
- Vrátenie autorizovaných objektov späť do žiadateľského systému
- Technická, produktová a projektová dokumentácia CPK podľa Vyhlášky Ministerstva investícií, regionálneho rozvoja a informatizácie SR č. 401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy (ďalej len „Vyhláška MIRRI SR č. 401/2023 Z.z.“ (https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2023/401/)

Verejný obstarávateľ v rámci 2. fázy - Rozvoj požaduje nasledovné:

- Komponent “Autorizácia prostredníctvom eID 2.0” a jeho integrácia do CPK viac info v kapitole 5.1.4
    - Autorizácia prostredníctvom eID 2.0 je modernizovaný spôsob elektronickej autentifikácie občanov, ktorý využíva čipové karty (elektronické občianske preukazy) vybavené pokročilými bezpečnostnými prvkami. Tento systém umožňuje bezpečný prístup k elektronickým službám štátu a iných OVM.
    - Integráciou eID 2.0 do CPK sa zjednoduší autentifikácia a autorizácia používateľov, ktorí sa budú môcť pomocou svojich eID kariet (elektronických občianskych preukazov) jednoducho a bezpečne autentifikovať svoju identitu a autorizovať operácie, čo uľahčuje prístup k elektronickým službám a transakciám.
- Viacnásobná autorizácia funkciou prístupového miesta
    - Podpis viacerými osobami funkciou prístupového miesta (viac oprávnených osôb podpisuje jedno podanie v korektnom poradí).

Verejný obstarávateľ v rámci 3. fázy- Remote signing požaduje nasledovné –:

- Rozšírenie vystavených API o “Remote signing” viac info v kapitole 5.6.
    - Implementovanie funkcie vzdialeného podpisovania dokumentov. Remote signing je proces, pri ktorom používateľ môže podpísať dokumenty elektronicky, z akéhokoľvek miesta a zariadenia s pripojením na internet bez nutnosti fyzického pripojenia podpisovacieho zariadenia (napr. Elektronický občiansky preukaz) k počítaču alebo inému zariadeniu.

Verejný obstarávateľ uvádza súvisiace časti k riešeniu CPK, ktoré nie sú predmetom zákazky podľa tohto zadania, ale nakoľko musí byť zabezpečená kompatibilita medzi dodávaným riešením z prvých 3 fáz a nižšie uvedenými bodmi:

- Úprava alebo implementácia konštruktora podania (vypĺňacej funkcie formulára podania)
- Prijatie a spracovanie správy s podaním autorizovaným funkciou prístupového miesta na rozhraní G2G ÚPVS a zobrazenie v schránke správ modulu eDesk na ÚPVS
- Overenie autorizácie funkciou prístupového miesta s využitím komponentu CEP pri doručovaní a preberaní takto autorizovaného podania v schránke v eDesk na ÚPVS

MIRRI SR, NASES a úspešný uchádzač zabezpečia súčinnosť pri integrácií dodávaných komponentov.

5 POŽADOVANÉ RIEŠENIE

5.1 Popis požadovaného riešenia

CPK, ktorý verejný obstarávateľ požaduje a ktorý je predmetom zákazky, má poskytnúť služby pre centrálne podpisovanie a riadenie procesu podpisovania. Bude teda otvorený pre dynamické pridávanie nových komponentov alebo modulov zabezpečujúcich podpisovanie (vrátane vzdialeného podpisovania). CPK má poskytnúť definované rozhranie cez ktoré integrovaná podpisová služba bude môcť poskytnúť informácie o rozsahu služieb a formáte podpisov ktoré poskytuje.

Verejný obstarávateľ požaduje, aby komponent CPK pozostával z grafického webového používateľského rozhrania (GUI), servisnej vrstvy – služby vystavené cez REST API a backend časti. Webová aplikácia bude slúžiť na vytváranie podpisov pre používateľov pri podpisovaní ľubovoľných elektronických úradných dokumentov ako aj pri tvorbe elektronických podaní a bude prístupná z ktoréhokoľvek bodu ISVS. Tieto ako aj všetky ostatné funkcionality, budú mať reprezentáciu vo forme REST služieb sprístupnených cez integračnú platformu. Produkt odbremení používateľa, ktorý si už ďalej nemusí inštalovať rôzne typy podpisových aplikácií.

CPK umožní podpísať elektronický dokument alebo podanie kvalifikovaným alebo zdokonaleným elektronickým podpisom alebo pečaťou. V prípade použitia pečate využitím HSM modulu musí byť používateľ autentifikovaný, overené jeho zastupovanie PO alebo OVM a musí mať priradenú rolu R_EDESK_SIGN. Používateľ musí mať možnosť výberu z jestvujúcich certifikátov a filtrovať zoznam certifikátov podľa typu (mandátny certifikát, KEP, KEPe pečať – HSM modul). Formáty podpisovaného dokumentu aj podpísaného dokumentu sú definované štandardmi uvedenými v kapitole 7 „Nutné legislatívne požiadavky“ (Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy, ďalej ako „Vyhláška ÚPVII č. 78/2020 Z.z.“ § 46, § 47 a § 48).

Podporované nepodpísané súbory:

.pdf .doc .docx .odt .txt .xml .rtf .png .gif .tif .tiff .bmp .jpg .jpeg

Podporované podpísané súbory:

.pdf .xml .asics .scs .asice .sce .p7m .zep .zepx .xzep

Verejný obstarávateľ požaduje, aby každá služba si mohla konfiguračne nastaviť zoznam povolených typov súborov na podpis.

CPK umožní aj podpísanie lokálneho elektronického súboru. Produkt umožní nahratie dokumentu a možnosť konverzie do povinných formátov PDF/A-2 až 4. Maximálna veľkosť

lokálneho súboru bude konfigurovateľná. Poskytovateľ služby bude mať k dispozícii nastavenie konfigurácie, ktorá umožní alebo zakáže konverziu konkrétnych formátov určených na podpisovanie.

CPK tiež umožní a poskytne funkcionalitu pre hromadné podpisovanie elektronických úradných dokumentov či viacerými používateľmi (viacnásobné podpísanie elektronických dokumentov alebo podaní). Zároveň umožní aj spoločnú autorizáciu viacerých dokumentov konfiguračne podľa typu osoby používateľa vzhľadom na povinnosť vytvárať spoločnú autorizáciu zo strany OVM a nemožnosť vytvárania spoločne autorizovaných podaní zo strany FO/PO.

CPK integráciou na službu vytvorenia časovej pečiatky zabezpečí jej pridanie pre každý podpis do podpisovaného dokumentu alebo podania.

Je požadovaná implementácia funkcionality pre zobrazenie podpisov predchádzajúcich osôb pri viacnásobnom podpisovaní spolu s kvalifikovanou elektronickou časovou pečiatkou.

CPK podporuje nasledujúce formáty podpisov a podpisových kontajnerov.

- XAdES
- PAdES
- CAdES
- ASiC
- a do budúcna ďalšie definované a rozšírené v rámci eIDAS

Po úspešnom a kompletnom podpísaní dokumentu nastane kontrola všetkých už vytvorených podpisov a vráteniu podpísaného objektu do komponentu, ktorý inicializoval volanie CPK. CPK bude preberať podmienky autorizácie podľa informácií k už poskytovaným službám v systéme METAIS, obsahujúce požadovanú úroveň autentifikácie, typ používateľa (FO/PO, OVM), minimálnu úroveň autorizácie podania a zoznam metód autorizácii, ktoré budú na základe tejto konfigurácie služby používateľovi dostupné. Kontrola podpisov na prílohách podania bude konfigurovateľná v zmysle podmienok poskytovania služby v METAIS.

Overovanie podpísaných dokumentov a podaní bude možné vykonať prostredníctvom služby Centrálnej elektronickej podateľne, ale aj pomocou ľubovoľnej inej kvalifikovanej služby, ktorá je vystavená na centrálnej integračnej platforme. CPK musí zabezpečiť používateľsky prijateľnú vizualizáciu výsledku overenia.

Súčasťou predmetu zákazky CPK bude JavaScript knižnica, ktorú bude možné poskytnúť správcom ISVS a prevádzkovateľom iných portálových riešení, ktorý bude integrovať služby CPK do ich informačných systémov. Súčasťou predmetu zákazky riešenia CPK je aj návrh jednotného integračného štandardu a súčinnosť pre zabezpečenie integrácie nových verzií existujúcich podpisovacích aplikácií D.Signer a Autogram, ako aj možnosť integrácií ďalších aplikácii, ktoré budú spĺňať navrhnutý integračný štandard.

Realizácia procesu podpísania sa požaduje výhradne v online režime, tzn. že pri využívaní CPK komponentu je potrebné mať internetové spojenie so službami CPK. Pred vytváraním podpisu

je nutné vykonať validáciu certifikátu, ktorý k úkonu chceme využiť. Požadujeme, aby pri realizácii podpisu bolo možné do podpisu súboru (dokumentu, dát formulára podania) vložiť časovú pečiatku (využitím služby centrálnej podateľne CEP alebo akéhokoľvek iného dôveryhodného poskytovateľa služby časovej pečiatky).

CPK vystaví API pre integráciu a registráciu nových služieb zabezpečujúcich funkcionalitu elektronického podpisu a remote signing-u. Možnosť integrácie služieb remote signingu bude naviazané na predchádzajúci proces posúdenia a schválenia integrácie tejto služby. Informácie o poskytovateľovi služieb remote signingu budú uložené v systéme Meta IS.

CPK bude vytvárať systémové aj aplikačné záznamy o svojej činnosti. Záznamy budú distribuované do centrálneho systému zberu logov a prevádzkového dohľadu v NASES. Vybrané aplikačné záznamy aktivít budú poskytované aj pre používateľov aplikácie, aby si sami mohli skontrolovať záznamy, ktoré vykonali alebo boli vykonané v ich zastúpení. Záznamy o aktivitách, ktoré budú určené aj pre používateľov musia používateľsky zrozumiteľne popisovať zaznamenanú aktivitu: čas aktivity, meno používateľa a zástupcu, ich ID, výsledok aktivity, zrozumiteľný popis aktivity alebo chyby, identifikácia objektu, s ktorým bola aktivita vykonaná.

KCCKB (NBU) bude validovať (posudzovať) Detailný návrh riešenia a auditovať nasadenú implementáciu riešenia.

5.2 Predpoklady

Aby sa mohli realizovať všetky scenáre použitia, je nutné mať splnené nasledujúce predpoklady:

1. Používateľ bude autentifikovaný do prostredia ÚPVS
2. Používateľ je oprávnený v zmysle prístupu k službám
3. Používateľ úspešne vytvorí elektronické podanie
4. ISVS OVM využívajúci služby CPK je integrovaný s ÚPVS
5. Pre niektoré spôsoby podpisovania je nutné mať aktivovanú mobilnú aplikáciu, ktorá nie je predmetom dodávky
6. CPK po zrealizovaní poslednej autorizácie neuchováva podpísané dokumenty ani podania

5.3 Aplikačná architektúra pre biznis architektúru

Po splnení vyššie uvedených predpokladov bude možné prostredníctvom kanála, v ktorom podanie vzniká, vyvolať služby vystavené na novom CPK komponente. CPK bude implementovať viaceré spôsoby autorizácie, pričom ale tieto spôsoby autorizácie nebudú navzájom plne zastupiteľné. Možné spôsoby autorizácie pre konkrétnu službu budú poskytované podľa údajov evidovaných na príslušných biznis službách v Meta IS. Pre každú službu bude v METAIS evidované, akými spôsobmi je možné ju autorizovať.

Úlohou komponentu CPK nie je zabezpečiť vytváranie formulárov podaní a príloh. Komponent CPK vie autorizovať jeden alebo viac objektov, v rámci jedného podania, ktoré vyžadujú podpis v závislosti od kontextu (identifikácia služby, povinné osoby, spôsob autorizácie). Komponent

vystavuje rozhranie, pomocou ktorého získa odkaz alebo priamo zoznam objektov na autorizáciu.

Komponent CPK pracuje v štyroch krokoch:

1. prijme objekt alebo objekty na autorizáciu a kontext podpisu (identifikácia služby, povinné osoby, spôsob autorizácie)
2. zvolí spôsob autorizácie a vyberie vhodný certifikát podľa konfigurácie služby v MetaIS
3. zabezpečí vytvorenie podpísaného objektu buď vlastnou funkcionalitou, alebo pomocou vystavených služieb podpisovej aplikácie
4. a následne vráti podpísané objekty do volajúceho informačného systému, alebo v prípade Autorizácie funkciou prístupového miesta (AFPM) odošle Sk-Talk správu.

V CPK v súčasnosti počítame s týmito možnosťami autorizácie v zmysle vyjadrenia vôle / podpisovaním:

- Autorizácia prostredníctvom KEP alebo AdES-QC (t.j. uznaného spôsobu autorizácie) na desktope. V tomto prípade sa očakáva integrácia CPK na podpisové aplikácie zabezpečujúce vytvorenie elektronického podpisu v prostredí ÚPVS:
  - D.Signer,
  - Autogram,
  - Iný podpisový software integrovaný v CPK
- Autorizácia funkciou prístupového miesta (AFPM)
- Autorizácia prostredníctvom KEP na mobile pomocou eID 2.0 alebo eDoPP a NFC
- Autorizácia formou Remote Signing
- Autorizácia OVM - vytvorenie elektronického podpisu/elektronickej pečate odosielaného elektronického dokumentu (rozhodnutia)

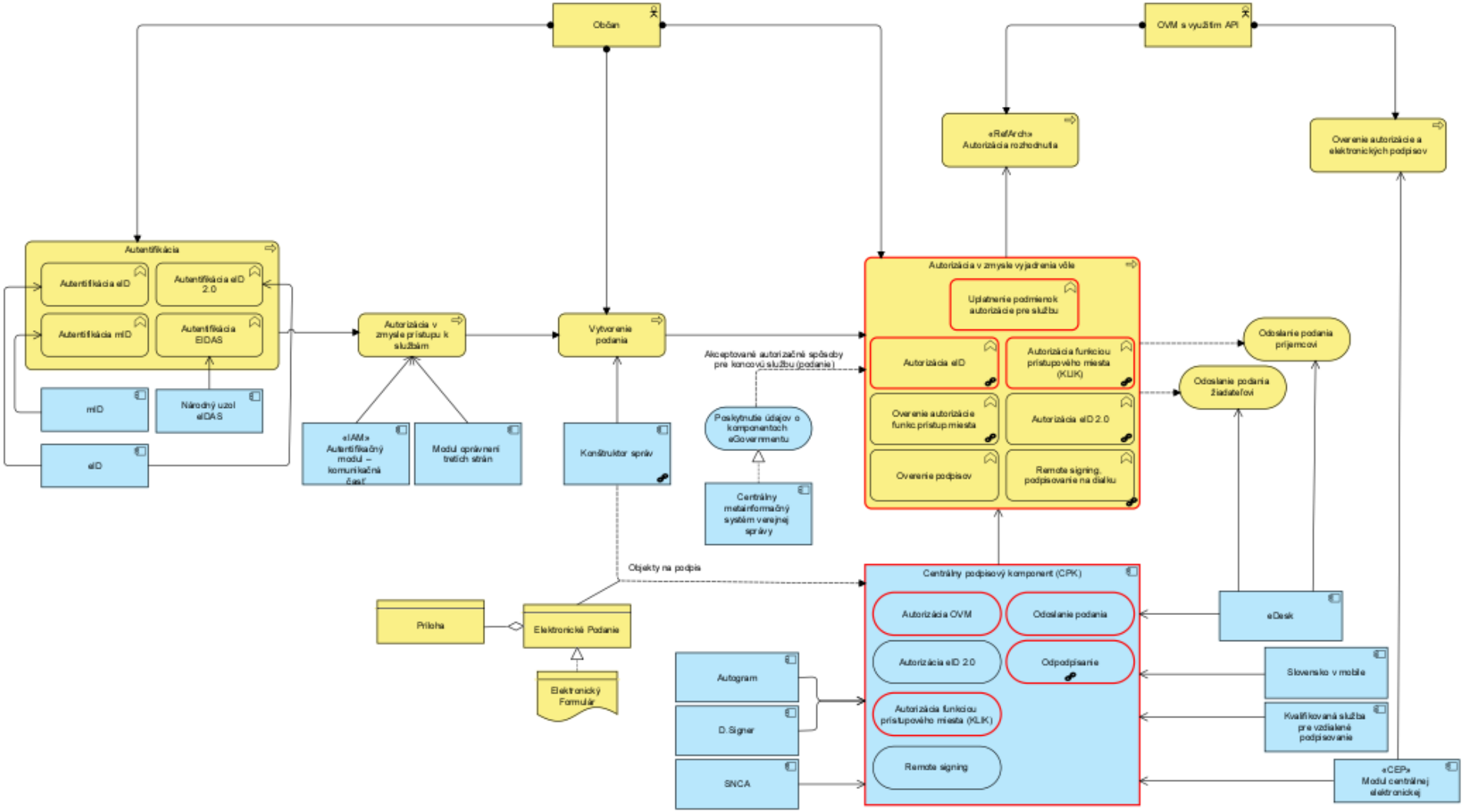


Diagram 1: *Architektúra CPK – Proces podpísania všeobecne*

Medzi konštruktorom správ a samotným CPK je zvýraznený tok dát, ktorý umožni výmenu objektov na podpis. CPK má k dispozícii dátový tok do podpisovej aplikácie ako je Autogram alebo D.Signer, prípadne iný software, vhodný na podpisovanie.

5.3.1 Proces autorizácie podania – všeobecne

Zovšeobecnený popis procesu vykonania autorizácie jednou osobou v CPK nad jedným objektom:

1. Aktivácia CPK, počas ktorého konštruktor správ doručí do CPK
    a. objekt na autorizáciu, alebo odkaz na ich umiestnenie v úložisku,
    b. kontext autorizácie, čiže dodatočné informácie o koncovej službe (identifikácia služby, povinné osoby, spôsob autorizácie)
2. Výber z povolených spôsobov autorizácie na základe údajov z Meta IS
3. V prípade autorizácie (vytvorenia el. podpisu) podpisovou aplikáciou (napr. d.Signer, Autogram):
    a. Overenie dostupnosti podpisovej aplikácie (overenie, že aplikácia je nainštalovaná a pripravená na komunikáciu s CPK)
    b. Výmena informácií o poskytovaných službách podpisovej aplikácie (napr. poskytovaná služba vizualizácie, overenia certifikátov atď.)
    c. Inicializácia podpisovacieho procesu v podpisovej aplikácií
4. Výber poskytovateľa a certifikátu
    a. je nutné overiť, či so zvolenými certifikátmi možno realizovať autorizáciu a pri negatívnom výsledku umožniť novú voľbu spôsobu a poskytovateľa,
5. Zobrazenie objektu na autorizáciu vo formáte podľa prezentačnej schémy (*ak sú v objekte už iné podpisy alebo pečate, zobrazí stručnú informáciu o ich stave*). V prípade autorizácie funkciou prístupového miesta sa okrem zobrazenia dát na podpis zobrazí aj upozornenie, že autorizácia bude vykonaná funkciou prístupového miesta.
6. Overenie či prihlásená osoba je oprávnená vytvoriť podpis:
    a. V prípade autorizácie funkciou prístupového miesta opätovným prihlásením
    b. V ostatných prípadoch zadaním BOK a PIN k QSCD
7. Vytvorenie MessageDigest - digitálny odtlačok dát určených na podpis
8. Zašifrovanie MessageDigestu vybraným poskytovateľom podpisových služieb a vybratým privátnym kľúčom používateľa.
9. Vytvorenie autorizovaného objektu podľa zvoleného spôsobu autorizácie:
    a. Napríklad podpisového kontajnera vo formáte ASiC, alebo
    b. Vytvorenie a odoslanie Sk-Talk správy v prípade autorizácie funkciou prístupového miesta (AFPM)
10. Vrátenie výsledku autorizácie do komponentu, ktorý inicioval autorizáciu (napr. konštruktor podaní, konštruktor správ)
11. Vrátenie riadenie konštruktoru s informáciou o výsledku autorizácie a/alebo odoslania.

Samotná práca s podpisovaným objektom môže byť celá alebo čiastočne vykonaná na strane CPK alebo podpisovej aplikácie.

Podrobný popis

Po úspešnej autentifikácii do prostredia ÚPVS prostredníctvom jedného z kanálov a zároveň po úspešnom vytvorení konkrétneho podania sa používateľ rozhodne, či potrebuje autorizovať toto podanie alebo iba prílohu dokumentu k samotnému podaniu. CPK mu podľa definície používateľskej služby v METAIS ponúkne zoznam akceptovaných autorizačných spôsobov. Používateľovi bude zobrazené GUI rozhranie komponentu CPK, v ktorom bude ponúknutý ucelený zoznam prípustných foriem autorizácie.

Užívateľ vyberie želanú formu, CPK realizuje potrebnú integráciu (detailnejšie uvedené v kapitole 5.3.2 k príslušnému spôsobu), zabezpečia sa kontroly ako overenie tokenov, kontrola autentifikácie minimálne na úrovni QAA L3, QA kontroly a podobne.

Následne sa vykoná samotné podpísanie podania a zapečatenie. V ďalšom kroku prebehne overenie všetkých podpisov na podaní, vrátane podpisov na prílohách (ak sú podpísané). Používateľ bude mať možnosť aj v tomto kroku ešte podpisy odobrať a vrátiť sa späť.

V prípade že používateľom zvolený objekt nebude môcť byť podpísaný, pretože pre želanú formu podpisu nemá vyhovujúci certifikát, CPK vráti používateľa na zoznam akceptovaných autorizačných spôsobov.

CPK následne podpísané objekty vráti späť do systému, ktorý o podpis žiadal. Alternatívne bude možné si kópiu autorizovaného objektu stiahnuť na vlastné úložisko. Pri každej aktivite, ktorá sa bude týkať podpísania vznikne auditný záznam.

Spôsoby autorizácie

5.4 Autorizácia podania elektronickým podpisom používateľa pomocou eID alebo eDoPP

Autorizácia KEP v zmysle § 23 ods. 1 písm. a) bod 1 zákona č. 305/2013 Z.z. o e-Governmente a Autorizácia Uznaným spôsob autorizácie podľa § 1 ods.1 písm. a) v zmysle Vyhlášky MIRRI SR č. 511/2022 Z.z. o uznaných spôsoboch autorizácie (ďalej ako „Vyhláška MIRRI SR č. 511/2022 Z.z.).

Prostredníctvom KEP bude možné podpísať každé elektronické podanie, rozhodnutie a ich prílohy, ktoré sa nachádzajú v ÚPVS. Pre výber a overenie možnosti použiť uznaný spôsob autorizácie bude zavedený krok pre overenie možnosti spôsobov autorizácie na základe údajov o službe z Meta IS repozitára. Po výbere spôsobu autorizácie (KEP, alebo uznaný spôsob autorizácie) bude požívateľovi pri realizácii podpisu ponúknutá možnosť výberu z jeho dostupných certifikátov. Po realizácii výberu bude vyzvaný na zadanie PIN k podpisovaciemu kľúču. V prípade, že boli predchádzajúce kroky úspešné, bude vytvorený elektronický podpis a podpisový kontajner podpisovaného objektu (podania, rozhodnutia, alebo prílohy). Používateľ dostane možnosť stiahnuť si už podpísaný objekt do lokálneho súboru.

5.4.1 Autorizácia funkciou prístupového miesta (AFPM)

Autorizácia použitím na to určenej funkcie ústredného portálu alebo špecializovaného portálu v zmysle § 23 ods. 1 písm. a) bod 2 zákona č.305/2013 Z.z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e Governmente).

Jedná sa o zjednodušený proces autorizácie vybraných podaní a služieb odoslaním elektronického podania do elektronickej schránky orgánu verejnej moci prostredníctvom ÚPVS alebo prostredníctvom špecializovaného portálu po opätovnej autentifikácii do prostredia ÚPVS. Osoba je autentifikovaná najmenej na úrovni „pokročilá“. CPK poskytne GUI pre zabezpečenie svojej funkcionality.

Pri volaní tejto služby CPK dôjde k nasledujúcim kontrolám:

- Volanie Služby CPK vykonal systém s príslušným oprávnením
- Zhoda SenderId / SubjectId - autentifikovaná osoba je zhodná s odosielateľom správy
- Minimálny QAA Level 3 / Level of Assurance prihlásenia používateľa
- Opätovné prihlásenie pred odoslaním podania sa bude kontrolovať vekom tokenu
- Validácia nakonfigurovaných akceptovaných autorizačných prostriedkov pre službu a formulár v MetaIS (kód služby v METAIS)
- Kontrola zastupovania v prípade PO

Autorizácia funkciou prístupového miesta nebude k dispozícii pre lokálne nahratý súbor (bez podania). Prílohy obsahujúce iné podpisy sa pomocou AFPM neautorizujú. Popis krokov pri AFPM:

ID	Krok	Realizátor
1.	Používateľ vyplní podanie	Konštruktor
2.	Používateľ sa rozhodne autorizovať	Konštruktor
3,	Aktivácia CPK, CPK preberie dokumenty a kontext	CPK
4.	Používateľ vyberie AFPM	CPK
5.	Zobrazenie náhľadu podania s odkazom na prílohy.	CPK
5.1	Zobrazenie upozornenia, že používateľ si vybral AFPM, bude vyzvaný na opätovné prihlásenie a že autorizáciou bude podanie aj odoslané.	CPK
6.	Používateľ klikne na “Autorizovať a odoslať”	CPK
7.	Používateľ sa autentifikuje minimálne na úrovni „pokročilá“ (pomocou eID alebo mID)	CPK
8.	CPK overí autentifikáciu, identitu odosielateľa a zastupovanie	CPK
8.1	CPK vytvorí pečate CPK/MIRRI pre každý objekt ktorý nebol podpísaný	CPK

8.2	CPK vytvorí autorizačnú informáciu, ktorú tiež zapečatí pečaťou CPK/MIRRI	CPK
8.3	CPK vytvorí a odošle Sk-Talk správu do schránky adresáta v eDesk s rolou ktorá mu umožni odoslať do G2G a odoslané podanie vloží do priečinka odoslaných správ prihláseného používateľa (SaveApplicationToOutbox)	CPK
9	CPK odošle informáciu o realizácii autorizácie AFPM	CPK

Autorizačná informácia z bodu 8.2 bude realizovaná novou dátovou štruktúrou. Dátová štruktúra bude prenášaná ako objekt v správe s Class AUTHORIZATION, v ktorej uvedie údaje o autorizovaných dokumentoch, použitom spôsobe autorizácie ako aj údaje o samotnej autorizácii. Štruktúra je navrhnutá tak, aby ju bolo možné v budúcnosti využiť aj pre iné spôsoby autorizácie. Detailný popis je v Prílohe č. 1 Opisu predmetu zákazky „Návrh dátovej štruktúry pre AFPM“.

Prijatie, spracovanie a overenie podania na strane G2G rozhrania ÚPVS, zobrazenie informácie o tomto spôsobe autorizácie v eDesk a overenie autorizácie v CEP **nie sú predmetom zákazky podľa tohto zadania.**

Podpis viacerými osobami funkciou prístupového miesta (viac oprávnených osôb podpisuje jedno podanie v korektnom poradí) bude súčasťou fázy 2 v zmysle kapitoly 4.

5.5 Autorizácia eID 2.0 alebo eDoPP 2.0 s NFC rozhraním (podpisovanie na mobile)

Autorizácia KEP v zmysle § 23 ods. 1 písm. a) bod 1 zákona č.305/2013 Z.z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente).

Predpokladom pre tento scenár podpisovania:

- ✓ Aktivovaná mobilná aplikácia previazaná s konkrétnou identitou z IAM modulu
- ✓ Podania, dokumenty, prílohy budú ukladané do momentu odoslania na dočasnom úložisku podporujúcom S3 protokol
- ✓ V momente úspešnej autorizácie budú súbory z dočasného úložiska odstránené

Proces podpísania prostredníctvom eID 2.0 prvku je podpisovaním KEP. Certifikáty budú však v tomto prípade prístupné prostredníctvom komunikačného protokolu NFC.

Existujúci eID framework v mobilnej aplikácii „Slovensko v mobile“ umožňuje komunikovať cez NFC s eID 2.0 a podpísať ľubovoľný textový reťazec pomocou certifikátov uložených na eID 2.0 zariadení s NFC chipom. Od používateľa si vypýta BOK a KEP PIN. Pre podpísanie dokumentu sú potrebné tieto ďalšie funkčnosti:

- Získanie a vytvorenie DTBS/R reprezentácie dokumentu (Data To Be Signed Representation) podľa ETSI EN 319 102-1). Aktivitu vykoná backend CPK.
- Zobrazenie podpisovaného dokumentu používateľovi spolu s údajmi o podaní, type a názvu dokumentu a prípadnými už existujúcimi podpismi. Môže byť samotný

dokument, alebo vygenerovaný náhľad. Návrh riešenia musí podporovať pravidlá prístupnosti.

- Vytvorenie bezpečného komunikačného kanálu a relácie medzi CPK a mobilnou aplikáciou.
    - Mobilná aplikácia musí čítať URL uvedené v Push notifikácii a QR kóde a následne komunikovať s poskytnutými URL
- Verifikácia platnosti podpisového certifikátu. Vykonávať sa bude na backende CPK.
- Konverzia dokumentu do štandardizovaného formátu. Vykonávať sa bude na backende CPK.
- Vytvorenie podpisu (zašifrovanie dát na podpis) v mobilnej aplikácii pomocou eID frameworku.
- Vloženie podpisu do dokumentu. Vykonávať sa bude na backende CPK.
- Získanie časovej pečiatky z CEP Vloženie časovej pečiatky volaním komponentu CEP, služby „PrevodEPESNaTFormu“. Vykonávať sa bude na backende CPK**.**

Identifikované boli 4 požadované scenáre:

1) **Desktop2App** – Vytvorenie dokumentu na portáli, napr. slovensko.sk na desktope, podpis na mobile v mobilnej aplikácii pomocou eID 2.0 alebo eDoPP 2.0 s využitím čítania certifikátu cez NFC.
2) **Web2App** – Vytvorenie dokumentu na portáli s využitím internetového prehliadača na mobile. Podpis sa bude realizovať prostredníctvom mobilného zariadenia s aktivovanou mobilnou aplikáciou a certifikátom z eID 2.0 alebo eDoPP 2.0 čítaním certifikátu cez NFC.
3) **App2App** – Dokument alebo podanie sa vytvorí v mobilnej aplikácii, podpis sa bude realizovať v mobilnej aplikácii pomocou certifikátu z eID 2.0 alebo eDoPP 2.0 s využitím NFC
4) **Podpis lokálneho súboru**

Scenár Desktop2Application

Po vytvorení dokumentu / podania sa používateľovi na desktope zobrazí vygenerovaný QR kód obsahujúci deeplink smerujúci do mobilnej aplikácie, kde sa zobrazí žiadosť o podpis obsahujúca základné údaje o podaní či dokumente, ako aj vizualizáciu obsahu s možnosťou audiokomentáru pre zrakovo postihnutých a nevidiacich. Ak je používateľ na desktope autentifikovaný a jeho identita je previazaná s aktivovanou mobilnou aplikáciou, odošle sa do mobilného zariadenia aj push notifikácia s rovnakým mechanizmom ako pri QR kóde. Deeplink bude obsahovať identifikačný token podania / dokumentu, pomocou ktorého si aplikácia stiahne náhľady, DTBS/R, ako aj URL adresu , kam má odoslať požadovaný výstup.

Scenár Web2Application

Po vytvorení dokumentu či podania vo webovom prehliadači na mobile je používateľ presmerovaný do mobilnej aplikácie využitím deeplinku, kde aplikácia zobrazí žiadosť o podpis. Zobrazené budú aj základné údaje o podaní alebo dokumente s vizualizáciou obsahu. Po realizácii podpisu je pomocou rovnakého mechanizmu používateľ presmerovaný späť do pôvodného okna internetového prehliadača na mobile, aby mohol pokračovať v podaní.

Deeplink bude obsahovať identifikačný token podania/dokumentu, pomocou ktorého si aplikácia stiahne potrebné dáta ako napr. náhľady, DTBS/R, a URL adresu, kam sa má odoslať výsledok procesu.

Scenár Application2Application

Dokument alebo podanie sa vytvorí v mobilnej aplikácii, ktorá nie je predmetom obstarávania, podpis sa bude realizovať v mobilnej aplikácii pomocou certifikátu z eID 2.0 alebo eDoPP 2.0 s využitím NFC.

Mobilná aplikácia pracuje s identifikačným tokenom, ktorý dostane z webview a pomocou ktorého si aplikácia stiahne náhľady, DTBS/R a URL adresu kam má odoslať výstup. DTBS/R podpíše pomocou eID 2.0 alebo eDoPP 2.0 cez NFC. Po odoslaní výsledku podpisu a jeho overení môže používateľ pokračovať v aplikácii v podaní.

Scenár Podpis lokálneho súboru

CPK poskytne používateľom webstránku so službou pre vytvorenie elektronického podpisu alebo viacerých podpisov na súbore štandardizovaného formátu. Používateľ do služby nahrá súbor zo súborového systému svojho zariadenia (desktop alebo mobil) a zvolí spôsob vytvorenia elektronického podpisu nahratého objektu (KEP, KEP s eID 2.0, uznaný spôsob autorizácie, remote signing). CPK (v spolupráci s podpisovou aplikáciou) zabezpečí vytvorenie alebo pridanie elektronického podpisu pomocou niektorého z vyššie uvedených spôsobov vytvorenia elektronického podpisu. V prípade, že je potrebná autentifikácia používateľa (napr. pre použitie remote signing) CPK autentifikuje používateľa alebo pre už prihláseného používateľa využije WebSSO. CPK pred vytvorením alebo pridaním elektronického podpisu overí existenciu a platnosť existujúceho podpisu na nahratom súbore. CPK po vytvorení podpisu umožní používateľovi stiahnutie podpísaného súboru. Portál CPK dokument neuchováva - zmaže ho na príkaz používateľa alebo po ukončení relácie s používateľom.

5.6 Vzdialené podpisovanie – Remote Signing

Pri remote signing procese ide o autorizáciu kvalifikovaného elektronického podpisu, a teda KEP alebo AdES, s tým že certifikáty a privátne podpisovacie kľúče pre vyhotovenie podpisu sú uložené na vzdialenom zabezpečenom serveri s HSM. Výhodou je eliminácia potreby osobného QSCD zariadenia (eID, hardverový token), inštalácie čítačky a ovládača QSCD zariadenia. Pri remote signing procese počítame s podporou pre štandardne podporované komunikačné kanály, t. j. mobilné zariadenia, web prehliadače ako aj desktop integrované aplikácie.

Remote signing musí byť implementovaný podľa vykonávacích predpisov nariadenia eIDAS.

5.6.1 Autorizácia OVM

Pri Autorizácii OVM ide o nasledovné spôsoby a služby autorizácie vykonávanej pracovníkmi OVM:

- Vytvorenie elektronického podpisu odosielaného elektronického dokumentu, ktorá predstavuje autorizáciu-vytváranie kvalifikovaných pečatí v zmysle § 23 ods. 1 zákona č.305/2013 Z.z. o e-Governmente náhradou alebo prepoužitím (integráciou) jestvujúcej funkcionality CEP (Modul centrálnej elektronickej podateľne, aplikačná

služba METAIS kód=sluzba_is_1370, služby DITEC_CEP_PODPISANIE_DOKUMENTOV a DITEC_CEP_PODPISANIE_DOKUMENTOV2 podľa integračného manuálu CEP).

- Vytvorenie elektronického podpisu odosielaného elektronického dokumentu, ktorá predstavuje autorizáciu v zmysle § 23 ods. 3 zákona č.305/2013 Z.z. o e-Governmente - vytváranie kvalifikovaného podpisu konkrétnou osobou alebo osobou v konkrétnom postavení, kedy orgán verejnej moci na autorizáciu použije kvalifikovaný elektronický podpis vyhotovený s použitím mandátneho certifikátu, ku ktorému sa pripojí kvalifikovaná elektronická časová pečiatka. Vtedy musí CPK realizovať autorizáciu podľa kapitoly 4.4.2 Autorizácia podania elektronickým podpisom používateľa pomocou eID alebo eDoPP alebo kapitoly 4.4.4 Autorizácia eID 2.0 alebo eDoPP 2.0 s NFC rozhraním (podpisovanie na mobile) tohto dokumentu.

5.7 Overovanie podpisov

CPK komponent bude podporovať viacnásobné podpisovanie (pridanie podpisu ďalšej osoby). Pri viacnásobnom podpisovaní treba overiť a zobraziť už existujúce podpisy na podpisovanom objekte. CPK preto integruje službu CEP pre overenie podpisov a overenie autorizácie funkciou prístupového miesta tak, aby bola k dispozícii v procesoch a službách poskytovaných CPK. Overenie autorizácie funkciou prístupového miesta bude nová funkcionalita implementovane v CEP. **Rozšírenie funkcionality CEP pre overenie autorizácie funkciou prístupového miesta a jej využitie v procese zasielania podaní do eDesk nie je predmetom dodávky.**

Overenie autorizácie funkciou prístupového miesta bude riešené rozšírením služieb CEP tak, aby služba overenia podpisu rozoznávala tento spôsob autorizácie podania. Overenie tohto typu autorizácie bude tiež doplnené do štandardného procesu overovania podpisov na správach zasielaných do eDesk, aby OVM mohli využiť výsledok overenia vo svojich procesoch spracovania podania podobným spôsobom, ako podania autorizované el. podpisom klienta

5.8 Odstránenie podpisov na nepodanom podaní- Odobratie podpisu

Komponent CPK bude vystavovať aj službu, ktorá zabezpečí zrušenie podpisov na predtým podpísaných dokumentoch, tzv. odpodpísanie. Táto služba je implementovaná a poskytovaná v CEP a CPK ju realizuje príslušnou integráciou, nebude ju duplicitne implementovať.

6 OČAKÁVANÉ VYSTAVENÉ SLUŽBY

#	Sémantický názov služby	Krátky popis
1	Získanie informácie o koncovej službe	Informácia, akým spôsobom je prípustné autorizovať podanie v koncovej službe
2	Získanie poskytovateľov podpisových služieb	Vráti zoznam dostupných poskytovateľov podpisových služieb (podpisové aplikácie), ktorí sú integrovaní a inštalovaní na koncovom zariadení používateľa a sú schopní poskytnúť akceptované

		autorizačné služby (vytvorenie elektronického podpisu)
3	Získanie informácie o poskytovateľovi podpisových služieb	Získa a poskytne používateľovi údaje, aké typy podpisu je integrovaný podpisový aplikačný komponent schopný vytvoriť / overiť
4	Vytvorenie elektronického podpisu	Vykoná autorizáciu zvoleného typu a spôsobu (vytvorenie el. podpisu) s vybraným poskytovateľom podpisových služieb podľa podľa §23 ods. 1.a (okrem bodu 2) a ods. 1.b. Ako výsledok autorizácie vráti podpísaný objekt spolu s informáciou o výsledku autorizácie. CPK neuchováva podpísané objekty.
5	Vytvorenie podpisu funkciou autorizácie prístupovým miestom (AFPM)	Vykoná autorizáciu funkciou prístupového miesta podľa §23 ods. 1.a.2, ktorá je podmienená úspešnou autentifikáciou zodpovedajúcou najmenej úrovni zabezpečenia „pokročilá“. Výsledok autorizácie odošle adresátovi podania a volajúcemu systému/portálu vráti výsledok autorizácie.
6	Stiahnutie podpísaného objektu	Podanie / dokument bude možné stiahnuť ako podpísaný objekt
7	Pridanie poskytovateľa autorizačných služieb	Služba bude slúžiť na zaregistrovanie nového poskytovateľa autorizačnej funkcie, spolu s parametrami, akou formou a aké výstupy je schopný poskytnúť. Po úspešnej registrácii bude môcť byť služba poskytovateľa využívaná prostredníctvom CPK
8	Aktualizácia / odstránenie poskytovateľa autorizačných služieb	Umožňuje zo zoznamu evidovaných poskytovateľov odobrať subjekt alebo aktualizovať jeho parametre
9	Odstránenie podpisov na objekte – zrušenie podpisov	Na podaní, ktoré ešte nebolo odoslané alebo v samostatnom dokumente, bude poskytovateľovi umožnené odstrániť svoj podpis

10	Kontrola podpisov na objekte	Služba skontroluje existenciu, počet, poradie, formát a platnosť podpisov aplikovaných na kontrolovanom objekte
11	Vytvorenie podpisu nahratého súboru	Služba umožní cez webové používateľské rozhranie vytvoriť elektronický podpis na nahratom podporovanom formáte súboru a stiahnuť podpísaný súbor. Služba bude poskytovaná aj pre neprihláseného používateľa.
12	Vytvorenie viacnásobného podpisu	Služba pridá podpis na už podpísaný objekt

7 POŽADOVANÉ LEGISLATÍVNE POŽIADAVKY

Legislatívne požiadavky na produkt vychádzajú z legislatívy Slovenskej republiky a Európskej Únie, ďalších technických špecifikácií a produkt musí byť v súlade s nasledujúcou legislatívou/reguláciou:

1) Štandardy a legislatívne normy stanovené vo Vyhláške Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu z z 9. októbra 2023 o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy401/2023 Z. z.
2) Vyhláška ÚPVII č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov.
3) Vyhláška MIRRI SR z 14. novembra 20222 č. 385/2022 Z. z. o jednotnom formáte elektronických správ v znení neskorších predpisov.
4) Vyhláška MIRRI SR z 19. decembra 2022 č. 511/2022 Z. z. o uznaných spôsoboch autorizácie v znení neskorších predpisov
5) Aktuálna Podpisová politika zverejňovaná Národným bezpečnostným úradom
6) ETSI TS 119 101 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation
7) ETSI TS 103 171 Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile
8) ETSI TS 103 172 Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile
9) ETSI TS 103 173 Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile
10) ETSI TS 103 174 Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile
11) ETSI TR 102 038: "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies
12) ETSI TR 102 272: "Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies
13) Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu, dostupná na webovom sídle Národného bezpečnostného úradu
14) Dokumentácia TL X.509 XML schémy pre dôveryhodný zoznam, zverejnená na webovom sídle Národného bezpečnostného úradu.

15) Nariadenie Európskeho parlamentu a Rady EÚ č. 910/2014 o elektronickej identifikácii a dôveryhodných službách
16) Zákon č. 272/2016 Z.z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)
17) Vyhláška MIRRI SR z 12. februára 2021 č. 70/2021 Z.z. o zaručenej konverzii v znení neskorších predpisov
18) 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)
19) Zákon č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
20) Pravidlá publikovania elektronických služieb do multikanálového prostredia verejnej správy č. 3204/2018/oAeG-1 (dokument zverejnený v centrálnom metainformačnom systéme)

Odporúčané požiadavky z pohľadu legislatívny a štandardov

1) ETSI TS 101 733 Electronic Signatures and Infrastructures (ESI), CMS Advanced Electronic Signatures (CAdES)
2) ETSI TS 101 903 Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)
3) ETSI TS 102 778 Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; PAdES
4) ETSI EN 319 132-1 Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
5) ETSI EN 319 142-1 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
6) ETSI EN 319 122-1 Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures
7) ETSI EN 319 162-1 Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers

Príloha 1: Návrh dátovej štruktúry pre AFPM:

Navrhovaná štruktúra sa bude používať aktuálne pre autorizáciu odoslaním podania po predchádzajúcej autentifikácii. Štruktúra je navrhnutá tak, aby ju bolo možné využiť aj pre iné spôsoby autorizácie v budúcnosti.

<u>Zdôvodnenie potreby vytvorenia dátovej štruktúry:</u>

Štandard pre elektronické správy Sk-Talk a jednotný formát elektronických správ MessageContainer majú v súčasnosti pevne stanovené elementy, ktoré nie je možné využiť pre uvádzanie údajov o použitom spôsobe autorizácie. V prípade autorizácie vo formátoch zdokonalených elektronických podpisov ASiC, PAdES alebo v slovenských formátoch XAdES_ZEP, ZEPf (používaných podľa legislatívy účinnej do 30.6.2016) sa autorizácia objektu vyznačuje v atribúte IsSigned, na základe ktorého sa určuje, či sa má daný objekt považovať za

autorizovaný a overiť štandardnými overovacími nástrojmi v elektronickej podateľni podporujúcimi tieto formáty podpisov. (V podateľniach sa štandardne overujú kvalifikovaný elektronický podpis/pečať, zdokonalený elektronický podpis založený na kvalifikovanom certifikáte, zdokonalený elektronický podpis kvalifikovanej služby validácie alebo kvalifikovanej služby uchovávania.)

Preto sa pre tieto prípady navrhuje vytvoriť novú dátovú štruktúru prenášanú ako objekt v správe s Class AUTHORIZATION, v ktorej daný informačný systém (špecializovaný portál) uvedie údaje o použitom spôsobe autorizácie ako aj údaje o samotnej autorizácii.

Orgány verejnej moci si pre účely automatizovaného spracovania takejto formy autorizácie musia upraviť svoje informačné systémy tak, aby v doručenej správe vyhľadávali dátovú štruktúru v Class AUTHORIZATION a vyhodnocovali resp. zobrazovali jej obsah obdobne, ako v prípade výsledku overenia podpisov.

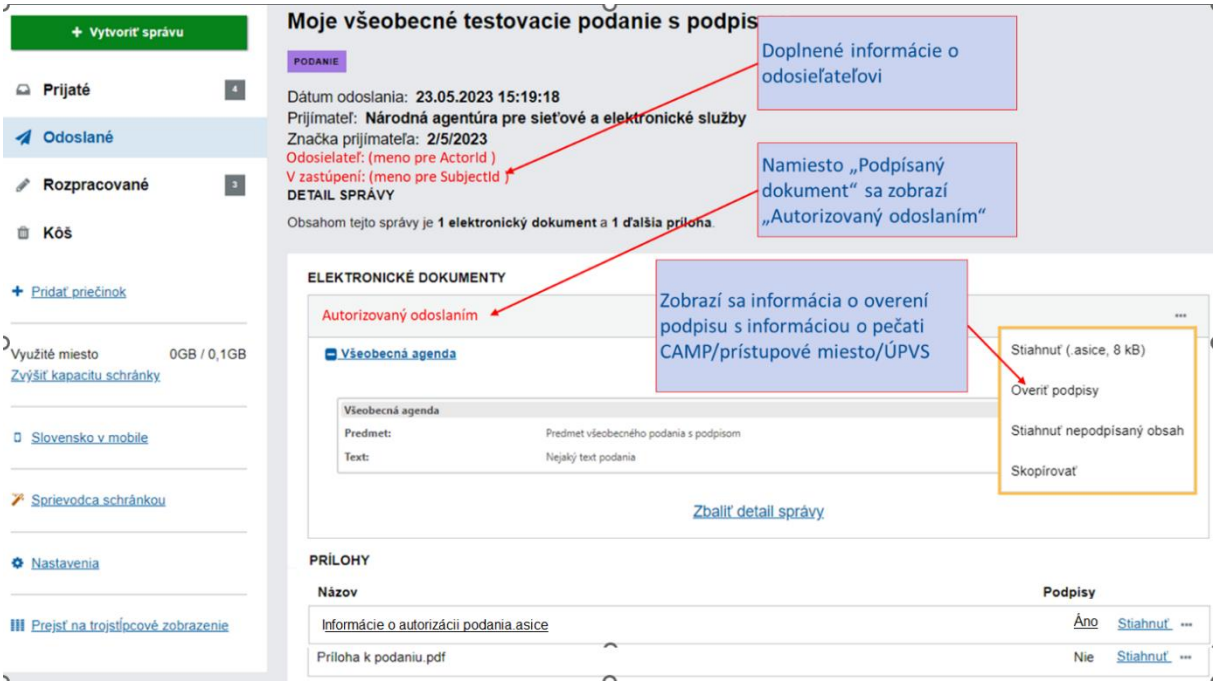
Za týmto účelom sa navrhuje aj úprava zobrazenia elektronickej správy v elektronickej schránke, aby zobrazovala v čitateľnej forme informáciu o použitom spôsobe autorizácie odoslaním.

Názov elementu	Typ	Kardinalita	Popis
AuthorizationInfo	Zložený typ	1	Štruktúra vkladaná do Sk-Talk pre identifikáciu typu autorizácie a súvisiacich údajov
Authorization	Zložený typ	1..n	Obsahuje údaje o jednej autorizácii. Umožňuje viacnásobný výskyt pre každý autorizovaný dokument v správe.
AuthorizedObjectId	Text	1	Identifikátor objektu v správe - v MessageContainer.
AuthorizationType	Zložený typ	1	Typ autorizácie - povinný údaj. Číselníková hodnota podľa číselníka v METAIS Do budúcna môžu pribúdať rôzne ďalšie formy autorizácie. Poznámka: V prípade autorizácie s KEP / AdES-QC sa nevypĺňa, nakoľko v takom prípade sa zohľadňuje atribút IsSigned pre daný objekt, z čoho vyplýva, že sa daný objekt má spracovať v elektronickej podateľni ako štandardný formát podpisu s kvalifikovaným certifikátom.

CodelistCode			Použitý spôsob autorizácie (CL009011 - Základný číselník spôsobov autorizácie v METAIS)
CodelistItem	Zložený typ	1	Položka číselníka
ItemCode	Text	1	Kód položky
ItemName	Text	1	Slovný názov typu autorizácie
AuthorizationDateTime	DateTime	1	Dátum a čas autorizácie. Povinný udaj.
SystemId	Text	0..1	Identifikácia informačného systému, pomocou ktorého bola vykonaná autorizácia (primárne by mal byť použitý kód ISVS podľa METAIS). Povinný v závislosti od typu autorizácie. V prípade autorizácie odoslaním podania po opakovanej autentifikácii sa uvádza povinne.
AuthorizedBy	Zložený typ	1	Identifikačné údaje osoby, ktorá autorizovala dokument. V prípade autorizácie vo vlastnom mene sa v položkách ActorId a SubjectId uvádza rovnaká hodnota. V prípade autorizácie odoslaním podania s opakovanou autentifikáciou v zastúpení sa uvádza údaj o zastupujúcej osobe v ActorId aj o zastúpenej osobe v SubjectId.
Actor	Zložený typ	1	
ActorID	Text		
Actor.FormattedName	Text		
Actor.IssuerForeignerID	Text		Kód krajiny vydávajúcej identifikátor osoby
Delegation	Číslo		Typ zastupovania – používa sa najmä zákonné zastupovanie, potrebné pre spracovanie niektorých typov žiadostí (napr. § 16 ods. 6 zákona eGov).
Subject	Zložený typ	1	
SubjectID	Text		
Subject.FormattedName	Text		

AuthorizationDocument	Zložený typ	1..n	Povinný min. 1 súbor preukazujúci vykonanú autorizáciu - obsah elektronického podpisu (pečate) autorizovaného dokumentu. V ďalšom preukazujúcom dokumente môže byť poskytnutý ďalší dôkaz, napr. záznam v LogFile
Type	Text	1	Typ preukazujúceho súboru (vymenované hodnoty): Signature (preferovaný typ), LogFilerecord
Document	Text	1	Hodnota preukazujúceho dokumentu zakódovaná do base64 (pre preferovaný typ Signature bude preukazujúcim dokumentom META-INF*signature*.* z ASIC kontajnera alebo export podpisu z PDF dokumentu vo formáte PADES príslušného autorizovaného objektu.)

Príloha 2: Návrh zobrazenia informácie o autorizácii odoslaním v schránke eDesk



Poznámka: V časti “prílohy” sa bude zobrazovať ako samostatný objekt / súbor formulár v ASiC vložený v správe v Class AUTHORIZATION štandardne ako bežný podpísaný formulár. Predpokladaný názov: “Informácie o autorizácii podania“.

8 POŽIADAVKY NA PREVÁDZKOVÚ PODPORU SYSTÉMU (SLA)

Poskytovateľ služby je povinný zabezpečiť prevádzkovú podporu dodávaného diela a všetkých jeho súčastí na obdobie dvoch (2) rokov s možnosťou opcie na nasledujúce dva (2) roky.

Úrovne podpory používateľov

Verejný obstarávateľ požaduje, aby poskytovateľ služby realizoval Help Desk nasledovnej úrovne podpory, s nasledujúcim označením:

- **L1 podpora:** (Level 1) – Jednotný priamy kontakt pre používateľov nového riešenia. Zabezpečené zamestnancami objednávateľa a/alebo ním určených osôb
- **L2 podpora:** (Level 2) – Postúpenie požiadaviek od L1 podpory. Zabezpečené Poskytovateľom služby na základe zmluvy.
- **L3 podpora:** (Level 3) – Postúpenie požiadaviek od L2, prípadne L1 podpory. Zabezpečené Poskytovateľom služby na základe zmluvy.

Pre prevádzkovú podporu sú definované takéto SLA:

- Help Desk je dostupný prostredníctvom telefonického kontaktu alebo e-mailu.
- Dostupnosť L2 a L3 podpory pre IS je 10x7 (10 hodín x 7 dní v týždni od 8:00h do 18:00h).

Riešenie incidentov – SLA parametre

Za incident je považovaná chyba IS, t.j. správanie sa v rozpore s prevádzkovou a používateľskou dokumentáciou.

- **označenie naliehavosti incidentu:**

Označenie naliehavosti incidentu	Závažnosť incidentu	Popis naliehavosti incidentu
A	**Kritická**	Kritické chyby, ktoré spôsobia úplné zlyhanie systému ako celku a nie je možné používať ani jednu jeho časť, nie je možné poskytnúť požadovaný výstup z IS. Za kritickú chybu sa považuje nemožnosť podpísať podanie akýmkoľvek spôsobom, teda chyba na úrovni CPK.
B	**Vysoká**	Chyby a nedostatky, ktoré zapríčinia čiastočné zlyhanie systému a neumožňujú používať časť systému.
C	**Stredná**	Chyby a nedostatky, ktoré spôsobia čiastočné obmedzenia používania systému.
D	**Nízka**	Kozmetické a drobné chyby.

- **možný dopad:**

Označenie závažnosti incidentu	Dopad	Popis dopadu
1	**katastrofický**	katastrofický dopad, priamy finančný dopad alebo strata dát,
2	**značný**	značný dopad alebo strata dát
3	**malý**	malý dopad alebo strata dát

- **výpočet priority incidentu je kombináciou dopadu a naliehavosti v súlade s best practices ITIL V3 uvedený v nasledovnej matici:**

Matica priority incidentov	Dopad		
	Katastrofický - 1	**Značný - 2**	**Malý - 3**

Naliehavosť	**Kritická - A**	1	2	3
	Vysoká - B	2	3	3
	Stredná - C	2	3	3
	Nízka - D	3	3	3

- **<u>vyžadované reakčné doby:</u>**

Označenie priority incidentu	**Reakčná doba[(1)] od nahlásenia incidentu po začiatok riešenia incidentu**	**Doba konečného vyriešenia incidentu od nahlásenia incidentu (DKVI) [(2)]**
1	Do 10 min.	Do 4 hodín
2	Do 30 min.	Do 12 hodín
3	Do 60 min.	Do 10 dní

- Za odstránenie chyby sa považuje aj nasadenie dočasného náhradného riešenia umožňujúceho pokračovať v prevádzke.

(1) Reakčná doba je čas medzi nahlásením incidentu verejným obstarávateľom (objednávateľom) (vrátane užívateľov IS, ktorí nie sú v pracovnoprávnom vzťahu s verejným obstarávateľom) na helpdesk úrovne L2 a L3 a jeho prevzatím na riešenie.

(2) Doba konečného vyriešenia incidentu (DKVI) znamená obnovenie štandardnej prevádzky - čas medzi nahlásením incidentu Objednávateľom a vyriešením incidentu Poskytovateľom služby (do doby, kedy je funkčnosť prostredia znovu obnovená v plnom rozsahu). Doba konečného vyriešenia incidentu od nahlásenia incidentu Objednávateľom (DKVI) sa počíta počas celého dňa. Do tejto doby sa nezarátava čas potrebný na nevyhnutnú súčinnosť Objednávateľa, ak je potrebná pre vyriešenie incidentu. V prípade potreby je Poskytovateľ služby oprávnený požadovať od Objednávateľa schválenie riešenia incidentu.

Incidenty nahlásené verejným obstarávateľom (objednávateľom)uchádzačovi, ktorý poskytuje služby (poskytovateľom) v rámci testovacieho prostredia:

a) Majú prioritu 3 a nižšiu.
b) Vzťahujú sa výhradne k dostupnosti testovacieho prostredia.
c) Za incident na testovacom prostredí sa nepovažuje incident vztiahnutý k práve testovanej funkcionalite.

Vyššie uvedené SLA parametre pre prevádzkovú podporu nebudú použité pre nasledovné služby:

- Služby systémovej podpory na požiadanie (nad paušál).
- Služby realizácie aplikačných zmien vyplývajúcich z legislatívnych a metodických zmien (nad paušál).

“Náhradné riešenie” je riešenie, ktoré nahradí poskytovanú Službu do doby opravy pôvodných prostriedkov potrebných na funkcionalitu Služby. Náhradné riešenie je poskytnuté na dohodnutý, alebo nevyhnutný čas.

8.1 Výkonnosť a dostupnosť služieb

Popis	***Parameter***	***Poznámka***
Prevádzkové hodiny	24 hodín	24 hodín x 7dní od 00:00h do 24:00:hvrátane sviatkov
Servisné okno	8 hodín	• Plánovaný výpadok je oznámený minimálne 14 dní vopred. • Plánovaný výpadok nie je dlhší ako 8 hodín a je prioritne medzi 22:00 – 06:00, sobota alebo nedeľa.
Dostupnosť produkčného prostredia IS	99,95%	• 99,95 % z 24/365 dní, t.j. max výpadok je 4.4 hodín. • Maximálny týždenný výpadok je v rozsahu do1 hodiny. • Nedostupnosť IS sa počíta od momentu zaevidovania incidentu Objednávateľom Do dostupnosti IS nie sú započítané servisné okná a plánované odstávky IS. • V prípade nedodržania dostupnosti IS bude každý ďalší začatý pracovný deň nedostupnosti braný ako deň omeškania bez odstránenia vady alebo incidentu.
RPO	Od 8 do 24 hodín	Poskytovateľ služby vie zabezpečiť riešenia tak, aby boli minimalizované časy pre obnovenie riešenia a minimalizovaná doba výpadku.
RTO	Do 24 hodín	Poskytovateľ služby vie zabezpečiť riešenia tak, aby boli minimalizované časy pre obnovenie riešenia a minimalizovaná doba výpadku.
Zálohovanie	5 predchádzajúcich dní	Záloha databázy bude vykonávaná pravidelne, garantovaná bude dostupnosť vždy k verziám z piatich (5) predchádzajúcich dní
Prístup k logom	n/a	Zabezpečenie logov systému, ktoré umožnia Objednávateľovi vyhodnotiť splnenie požiadaviek na úroveň služieb (SLA) a dostupnosti systému (odozva systému, dokončenie spracovania v definovaných lehotách, dostupnosť systému, atď.).
Odozva služieb pri testovaní záťaže systému	n/a	• 80% z meraných testovacích volaní v pomere zápis a čítanie 1:2 má odozvu kratšiu alebo rovnú 2 sekundy, • 15% z meraných testovacích volaní v pomere zápis a čítanie 1:2 má odozvu kratšiu alebo rovnú 5 sekúnd, • 5% z meraných testovacích volaní v pomere zápis a čítanie 1:2 má odozvu najviac 10 sekúnd,

		• Simulácia sa vykonáva podľa dát z reálnej prevádzky existujúcich služieb ÚPVS (podklad poskytne Objednávateľ), • V prípade volania externých služieb sa meria iba overhead na strane dodaného systému a nie čas odozvy. • Počet volaní a interakcia s koncovými používateľmi je určená podľa špičiek v prevádzke Pondelok – Piatok, 07:00 – 13:00 prebehne 90% všetkých volaní služieb, z toho v pondelok prebehne 25% všetkých volaní.

8.2 Služby riadenia systémovej a aplikačnej podpory (paušál)

Servisné služby vzťahujúce sa na produkčné aj testovacie prostredie systému, ktoré je prevádzkované v infraštruktúre vládneho cloudu medzi ktoré patria: činnosti správy a údržby systémového softvéru a systému (vrátane kontroly príslušných operačných systémov, kontroly logov, naplnenosti diskového priestoru, operačnej pamäte, správy komunikačnej matice pre jednotlivé služby produktov, sledovania informácií výrobcov a dodávateľov zariadení, príslušných bezpečnostných riešení, patchov a nutných aktualizácií, správa služieb infraštruktúry (DNS, NTP, VPN), monitorovanie vyťaženosti systému, monitorovanie sieťovej komunikácie, monitorovanie naplnenosti databáz, správa certifikátov interných/externých, prideľovanie systémových prostriedkov (CPU, Disk, RAM), vytváranie záloh, nasadzovanie nových verzií, riešenie úloh, vykonávanie preventívnej údržby, udržiavanie systému v súlade s bezpečnostnou dokumentáciou, súčinnosť a odstraňovanie zistení z bezpečnostného auditu.

Servisné služby budú realizované so zámerom:

- Uvedenie systému do plne funkčného stavu alebo poskytnutie náhradného riešenia (po poruchách, chybách) podľa definovaných parametrov pre produkčné prostredie pre nové riešenie CPK .
- Podpora systémového softvéru a aplikačného softvéru v produkčnom aj testovacom prostredí (vrátane riešenia vzniknutých problémov).
- Nasadzovanie nových verzií aplikačného programového vybavenia do testovacieho a produkčného prostredia.
- Lokalizácia potenciálnych problémov pri používaní prostredia.
- Optimalizácia prevádzky na základe odsúhlasených návrhov riešení.
- Aktualizácia prevádzkovej, používateľskej a bezpečnostnej dokumentácie vyplývajúcej z aktuálneho nastavenia systému.
- Poskytovanie podpory pri integrácii CPK s inými systémami a aplikáciami používanými objednávateľom.

8.3 Činnosti správy a údržby systémového softvéru a aplikačného softvéru vykonávané priebežne (paušál)

Priebežná správa a údržba CPK

Tieto činnosti sa vykonávajú v pravidelných intervaloch s cieľom preventívne identifikovať možné problémy. Ide zväčša o monitorovanie a kontrolovanie definovaných parametrov na základe vopred definovaného profylaktického plánu. Výsledky kontrol budú evidované v reporte s návrhom preventívnych akcií na elimináciu neštandardných stavov systému.

Evidencia a reportovanie

- **Spracovávanie požadovaných reportov a operatívnych informácií**: O stave prevádzky, poskytovania služieb, výsledkoch monitoringu, kontrol a auditov.
- **Vedenie technických a prevádzkových evidencií**: Vrátane technickej dokumentácie, nastavení parametrov, evidencie technických prostriedkov, používateľských príručiek, evidencie dodávateľov a kontaktných osôb.
- **Poskytovanie štatistických informácií**: Pre Objednávateľa a ním určené osoby.

Zabezpečovanie kvality služieb

Predkladanie návrhov opatrení na zlepšenie kvality služieb prevádzky a implementáciu schválených opatrení:

- **Plánovanie a riadenie preventívnej údržby**
- **Riadenie preventívnej údržby a opráv**: Vrátane prevádzkových a bezpečnostných auditov.
- **Riadenie vnútorných procesov**: A spolupráce s ostatnými zložkami.

Administrácia a manažment:

- konfigurovanie a správa diskových subsystémov,
- vytváranie, konfigurovanie a rušenie prístupových účtov v OS,
- vytváranie a rušenie adresárových štruktúr,
- prideľovanie, odoberanie a správa prístupových práv,
- správa bezpečnostnej a skupinovej politiky,
- rekonfigurácia parametrov operačných systémov a systémového aplikačného vybavenia,
- plánovaný a neplánovaný shutdown, reštart alebo štart systému, odpájanie a zapájanie systémov,
- inštalácia aktualizácií a patchov štandardného systémového softvéru,
- vytváranie a evidencia firewallových pravidiel,
- konfigurovanie integrácií na iné informačné systémy verejnej správy.
- Implementácia a udržiavanie bezpečnostných opatrení na ochranu údajov spracovávaných prostredníctvom CPK, vrátane šifrovania a kontrol prístupu.

Zálohovanie a obnova:

- konfiguračný manažment zálohovacieho systému,
- zálohovanie a obnova systémového softvéru,
- vytváranie, konfigurácia a správa zálohovacích scriptov,
- vykonávanie pravidelných a nepravidelných záloh systému,

- evidencia a správa systému záloh,
- obnova systémového softvéru (OS + systémové utility),
- obnova konfigurácie a parametrov komponentov,
- zálohovanie a obnova databáz.

Monitoring:

- dostupnosť a funkčnosť hardvérového vybavenia,
- diskových subsystémov,
- vyťaženia operačnej pamäte a CPUs,
- výkonnosti sieťových subsystémov,
- výskytu varovných a chybových hlásení HW a OS,
- prírastkov databáz a transakčných logov,
- indexov a konzistencie databáz,
- vykonávania pravidelných Backupov,
- vykonávania pravidelných systémových procesov,
- prevádzkových udalostí,
- kontrola behu systémových procesov,
- kontrola behu aplikačných procesov,
- kontrola logov aplikačného servera,
- kontrola integrity kritických systémových súborov.

8.4 Požiadavky služby systémovej podpory na požiadanie (nad paušál)

Prevádzkové činnosti , ktoré budú poskytované nad rámec služieb v rámci systémovej a aplikačnej podpory (SLA):

- Riešenie systémových a prevádzkových chýb súvisiacich s potrebou funkčnej úpravy nastavených procesov;
- Školenia garantov a používateľov;
- Poskytovanie služieb odborných a technických konzultácii nad rámec činností uvedených v rámci SLA (tento dokument) v kapitole 1.1.1;
- Ďalšie činnosti a služby aplikačnej podpory súvisiace so zabezpečením prevádzky systému;
- Aktualizácia používateľskej a technickej dokumentácie po každej zmene systému;

8.5 Požiadavky služby realizácie aplikačných zmien vyplývajúcich z legislatívnych a metodických zmien (nad paušál)

Činnosti súvisiace s rozvojom systému. Tieto činnosti zahŕňajú implementáciu schválených požiadaviek používateľov na zmenu funkčnosti systému najmä:

- Rozširovanie funkcionality systému - Analýza, návrh a vývoj rozšírenia, vylepšenia a/alebo modifikácie aplikačného softvéru, na základe metodických a/alebo legislatívnych zmien;
- Vykonanie úprav v nastavení modulov systému voči implementovanej funkčnosti a existujúcim nastaveniam;

- Programovanie nových funkcií v rámci existujúcich modulov systému;
- Vykonávanie úprav do existujúcich integračných rozhraní;
- Programovanie a implementácia nových integračných rozhraní;
- Realizácia testov podľa testovacích scenárov;
- Projektové riadenie zmien v zmysle Vyhlášky MIRRI SR z 9. októbra 2023 č. 401/2023 o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy
- Aktualizácia používateľskej a technickej dokumentácie po každej zmene systému.

Zmena funkčnosti zahŕňa pridanie, modifikáciu alebo zrušenie akejkoľvek časti systému a súvisiacej dokumentácie. Zmena funkčnosti môže byť vyvolaná legislatívnou požiadavkou a/alebo požiadavkou používateľov na zlepšenie existujúcej funkcionality alebo zavedenie novej funkcionality v novom riešení CPK.