**Archiv elektronické zdravotnické dokumentace Kraje Vysočina**

Technické podmínky

Cílem projektu (předpoklad financování z výzvy 80. IROP eHealth – SC 1.1 (ČR) v roce 2024) je dodávka on-premise softwarového řešení a souvisejících služeb systému pro dlouhodobé a důvěryhodné uložení elektronických dokumentů, zejména pak zdravotnické dokumentace v elektronické podobě. Toto řešení musí být v souladu s požadavky zákona 325/2021 Sb. o elektronizaci zdravotnictví a také zákona č. 499/2004 Sb., o archivnictví a spisové službě (z důvodu neexistence příslušné vyhlášky MZ a předpokladu, že její budoucí podoba se bude blížit požadavkům zákona 499/2004).

Systém musí respektovat architekturu otevřeného archivu dle metodologie a architektury OAIS a základní funkce dle specifikace doporučení EU/CEF projektu E-ARK3 ([https://eark.online](https://eark.online/), a refereční architektura el. archivu <https://kc.dlmforum.eu/earchiving-ra20/>) a IHE ITI-41 (<https://profiles.ihe.net/ITI/TF/Volume2/ITI-41.html>) . Cílem je dodávka a provoz řešení s otevřenou, dlouhodobě udržitelnou architekturou, umožňující průběžné a dlouhodobé důvěryhodné uložení zdravotnických dat (zdravotnické dokumentace) při důrazu na interoperabilitu SW řešení i uložených dat.

Systém bude dodán jako multitenantní řešení, funkčně a licenčně plně pokrývající potřeby Kraje Vysočina - Krajského úřadu a příspěvkových organizací kraje (zejména s činností v oblasti zdravotnictví a sociálních služeb). Systém bude provozován v prostředí Technologického centra Kraje Vysočina (TCK) a Datové centra Nemocnice Jihlava (DCNemJi). Tato datacentra budou pro provoz archivu poskytovat prostředky výpočetního výkonu, sítí a datových úložišť prostřednictvím virtualizační technologie VMWare. Součástí dodávky SW není dodávka hardware. Ta bude řešena případně samostatnou zakázkou pro posílené HW a SW vybavení TCK a DCNemJi. Alternativou pro uložení dat je využití národní repozitářové platformy (NRP - <https://www.eosc.cz/projekty/narodni-repozitarova-platforma-pro-vyzkumna-data-os-i-nrp/nrp>) případně možnost dodatečného přepnutí na NRP.

Licence dodaného systému bude časově neomezená, perpetuální, určená pro libovolný počet organizací zřizovaných a zakládaných Krajem Vysočina (tenantů), Krajský úřad Kraje Vysočina a repozitáře budoucí akreditované afinitní domény (AafD) eMedocs II.; dále je součástí nabídky cenové ujednání (ceník) pro organizace zapojených do výměnné afinitní domény (výměnné sítě zdravotnických dat) Kraje Vysočina eMeDocS II. (aktuálně 50+ subjektů) a pro neomezený počet uživatelů, ukládaných dokumentů i integrovaných informačních systémů. Součástí ceny licence jsou i náklady na úvodní konfiguraci tenantů níže zmíněných osmi organizací.

Součástí dodávky řešení bude jeho obousměrná integrace (uložení dat do archivu i jejich získání) s pěti samostatnými nemocničními informačními systémy Fons Enterprise (NIS, ukládání textové a strukturované zdravotnické dokumentace; Nemocnice Jihlava, Nemocnice Třebíč, Nemocnice Nové Město na Moravě, Nemocnice Havlíčkův Brod, Nemocnice Pelhřimov), NIS FONS Akord Psychiatrické nemocnice Havlíčkův Brod, dispečerským systémem ZZS Kraje Vysočina (SOS), systémem podpory posádek ZZS (MZD) a sítí výměny zdravotnické dokumentace eMeDocS (případně novou AAfD kraje; služby archivace pro repozitáře ZD v rámci AAfD)

Požadavky zadavatele – technické podmínky, jsou dále obsaženy v „technickém listu“, který tvoří součást tohoto dokumentu; seznam dalších technických požadavků a závaznost požadavku:

* P1 - funkce musí být dostupná a prezentovatelná v době podání nabídky
* P2 - funkce musí být dostupná v době dokončení implementace
* R - nepovinný rozšiřující požadavek (součást kvalitativního hodnocení nabídek)
* **Etapa E1 - do 6ti měsíců od podpisu smlouvy**
* **Etapa E2 - do 18ti měsíců od podpisu smlouvy**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID požadavku** | **Popis požadavku** | **Závaznost požadavku** | **Etapa** |
| A1 | Dodané řešení umožní prostřednictvím webového uživatelského rozhraní definovat základní nastavení prostředí organizace (tenantu) včetně klasifikace dokumentů, integračních rozhraní, retenčních a skartačních pravidel, oddělených složek/oblastí (repozitářů), místa uložení (storage) s možností definice přístupů pro různé skupiny uživatelů vůči různý skupinám dokumentů | P1 | E1 |
| A2 | Ukládání a zpřístupňování zdravotnické dokumentace ve formě textových, grafických, audiovizuálních, digitálních nebo jiných obdobných záznamů. | P1 | E1 |
| A3 | Archivace textové i obrazové dokumentace PACS (dat uložených v PACSu typicky ve formátu DICOM; zvukové nahrávky, videonahrávky) | P2 | E2 |
| A4 | Podpora komunikačních protokolů DASTA a HL7 (CDA i FHIR R4) včetně uložení (archivace) a zpřístupnění dokumentů v těchto formátech | P2 | E2 |
| A5 | Vstupní a výstupní rozhraní v souladu s Národním standardem pro elektronické systémy spisové služby (ERMS) | P2 | E2 |
| A6 | Možnost vyhledání a získání uložené dokumentace dle identifikace pacienta (identifikace dle čísla pojištěnce a resortním identifikátorem pacienta) a to jak ve webovém frontendu (tam včetně zobrazení) tak v prostřednictvím API.  Včetně možnosti vyhledat dokumentaci a zpřístupnit data (formou archivní zápůjčky); zaznamenat tyto úkony do dokumentace a opět dokumentaci uložit. | P2 | E1 |
| A7 | Scénáře automatické transformace dokumentů (změny formátu) k zajištění dlouhodobého uložení a čitelnosti dokumentů. | R | E2 |
| A8 | Skartace na základě metadat určují životnost dokumentu a termín jeho skartace. Protokoly o uskutečněných skartacích. | P2 | E2 |
| A9 | Automatické vyhodnocování skartační lhůty na uložených dokumentech. Po uplynutí skartační lhůty musí vyhotovit seznam relevantních dokumentů, které nabídne oprávněnému uživateli ke skartaci. Uživatel může dokumenty smazat nebo jim prodloužit skartační lhůtu. Skartační protokol musí být automaticky uchováván. Skartací je myšleno mazání dokumentů na úrovni důvěryhodného elektronického archivu. | P1 | E2 |
| A10 | Nástroj na zobrazení/prohlížení/renderování zdravotnické dokumentace uložených ve formátech DASTA a HL7 (CDA i FHIR) - implementace národního referečního zobrazováního nástroje MZ (v případě jeho nedostupnosti není požadována dodávka vlastního řešení) | P2 | E2 |
| A11 | Nástroj pro kontrolu formátů uložených dokumentů (minimálně analýza verze PDF) a analýzu formy el. podpisu nebo pečeti dokumentu (LTV, nonLTV, platnost certifikátu) s možností definice pravidel příjmu dokumentů dle formátu a podpisu. | P2 | E1 |
| A12 | Proces automatické kontroly platnost systémového certifikátu časového razítka, před jeho expirací; automatická kontrola integrity dokumentu, stažení CRL vybraných certifikačních autorit a jejich, kořenových certifikátů, uložení informace o ověření, přidání aktuálního časového razítka a opětovné uložení do archivu. | P2 | E1 |
| A13.1 | Auditování a logování provozu jednotlivých prvků systému a možnost vyhodnocování min. 2 roky zpětně a to včetně manipulace s uloženými objekty, činnosti uživatelů a integrovaných systémů | P1 | E1 |
| A13.2 | Logování v souladu s doporučením IHE profilu ATNA | R | E2 |
| A14 | Zajištění interoperability archivu dle doporučení <https://www.dilcis.eu/> pro zdravotní záznamy - <https://www.dilcis.eu/content-types/cits-ehealth1-patient-medical-records> | R | E2 |
| A15 | Podpora provozu s vysokou dostupností v režimu active-pasive ve dvou datacentrech (TCK, DC NemJi) | P2 | E1 |
| A16 | Pro ověření uživatele (autentizaci) je vyžadována integrace na nástroje ověřování SSO KV = autentizační brána Authgate od společnosti Autocont (AC Identita), která spravuje federaci Idp viz VysocinaID <https://vysocinaid.kr-vysocina.cz> Ověřovací prostředí poskytuje službu autentizační brány (protokoly SAML2 a OpenID Connect/OIDC/), kde služba centrálně ověřuje uživatele proti identitním prostorům. | P2 | E2 |
| A17 | Podpora autorizace IDM AC Identita. Pro získání oprávnění uživatelů je provedena autorizace proti databází uživatelských oprávnění na identity management KV (IDM). Databáze uživatelských oprávnění má vystaveno uživatelské rozhraní (API) ve formě web služeb SOAP (WS). Systém získává profil daného uživatele včetně oprávnění (rolí) prostřednictvím API na IDM KV, ukládá tyto parametry do svého interního nástroje správy uživatelů a v proceduře autorizace přiděluje na základě úspěšné autorizace příslušná oprávnění. | P2 | E2 |
| A18 | Součástí implementace bude i testovací prostředí archivu | P2 | E1 |
| A19 | Integrace s eMedocs II.- za účelem předání uložené ZD dalším poskytovatelům zdrav. služeb a za účelem předání dat pro pacienta prostřednictvím NCPeH ([www.nixzd.cz](http://www.nixzd.cz)), Portálu občana (obcan.gov.cz), EZ-Karty a pro další afinitní domény. | P2 | E2 |
| A20 | Vlastní systém identifikace (číslování pomocí OID) uložených dokumentů a hlášení jejich existence do registru (indexu) zdravotnické dokumentace do příslušného indexu afinitních domén (minimálně eMedDocS II.). Možnost parametrického nastavení funkce (včetně možnosti přebírání OID z integrovaného provozního systému) per tenant a repozitář. | P2 | E2 |
| A21 | Nástroj pro automatické pečetění dokumentů na vstupu per tentant a repozitář pomocí funkcí pečeť jako služba. Možno řešit samostatnou licencí per tenant. V nabídce indikativně naceněno pro 2 tenanty. | P2 | E2 |
| A22 | Nástroj pro dodatečné uživatelské el. podepisování (PDF, LTV kvalifikovaný el. podpis) a časové razítkování zdravotnické dokumentace pro organizace kde není provozní systém vybaven těmito nástroji. Možno řešit samostatnou licencí per tenant. V nabídce indikativně naceněno pro 2 tenanty. | P2 | E2 |
| A23 | Funkce archivních časových razítek (ATSA) | P2 | E2 |
| A24 | Napojení systému logů na logovací nástroje typu SIEM/LogManager per tenant | P2 | E1 |
| A25 | Dokumentované (OpenAPI/SWAGGER nebo obdoba) REST API pro obsluhu řešení ze strany jiných integrovaných systém jak pro uložení tak získání dokumentů včetně podpory vyhledávání dokumentů minimálně dle OID, RID a čísla pojištěnce. | P2 | E1 |
| A26 | Funkce jednoznačného URL (linku) pro získání/zobrazení daného dokumentu | P2 | E1 |
| A27 | Nástroj pro provedení autorizované konverze listinných dokumentů na digitální. | R | E2 |
| A28 | Funkčnost celého řešení bez dostupnosti veřejného internetu jen v prostředí sítí ROWANet a CMS 2.0 | P2 | E1 |
| A29 | Využití národní repozitářové platformy (NRP) | R | E2 |
| A30 | Uživatelské rozhraní (UI) pro uložení a získání dat do/z archivu. | P2 | E2 |
| A31 | Online statistiky využití archivu - počty spotřebovaných časových razítek, počty objektů, počty typů dokumentů, využitá kapacita; za období i na tenant; grafické i tabulkové výstupy. | P2 | E2 |
| A32 | Podpora IHE profilů pro uložení a získání dat XDS, XCA a XDR | P2 | E2 |
| A33 | Řešení pro automatickou obnovu certifikátů (protokol ACME a obdobné) | P2 | E2 |
| A34 | Funkce zotavení z chyb nedostupnosti služeb typu CA (nedostupná časová autorita, nedostupný seznam odvolaných certifikátů, nedostupná CA, SMTP server) typicky vytvořením fronty požadavků pro následné automatické odbavení po obnově dostupnosti služby | P2 | E2 |
| A35 | Nástroj hromadné změny skartační lhůty uložených dokumentů. | P2 | E2 |
| A36 | Funkce prodlužování platnosti (autenticity) dokumentu přerazítkováváním časovými razítky na konci platnosti. | P1 | E1 |
| A37 | Funkce identifikace dokumentů (typicky hashovacími funkcemi) pro zamezení jejich duplicitnímu výskytu | R | E2 |
| A38 | Všechny použité kryptografické funkce, algoritmy a prostředky musí být v souladu s Doporučením v oblasti kryptografických prostředků v aktuálním znění, které vydává Národní úřad pro kybernetickou a informační bezpečnost, a to tak, že musí být použity pouze schválené, nikoliv dosluhující kryptografické prostředky. | P2 | E1 |
| A39 | Dodání provozně bezpečnostní dokumentace minimálně v tomto rozsahu:   * Bezpečnostní specifikace systému (Cíl dokumentu: popsat a zdokumentovat veškeré bezpečnostní mechanizmy a opatření za účelem identifikace toho, jaká data jsou jakým způsobem chráněna.) * Základní konfigurace (Cíl dokumentu: popsat a zdokumentovat postupy, které vedou k nastavení systému do takového stavu, aby bylo možné systém po instalaci provozovat na základní úrovni.) * Záloha, obnova, restart (Cíl dokumentu: popsat a zdokumentovat strategii zálohování systému, jakým způsobem, kdy, kam a jak často jsou zálohována data v rámci daného informačního systému a jakým způsobem se provádí obnova systému po havárii nebo ze zálohy, postupy a konkrétní kroky, které povedou k bezpečnému restartu systému.) * Vazby na jiné systémy, rozhraní, datové vztahy a struktury (Cíl dokumentu: popsat, jakým způsobem je daný systém navázán na jaké systémy, popsat všechna rozhraní a popsat datové vztahy a struktury) * Monitoring (Cíl dokumentu: popsat a zdokumentovat mechanizmus monitorování a zaznamenávání bezpečnostních a provozních logů a auditních událostí.) * Základní uživatelská a administrátorská příručka * Popis klíčových komponent (Cíl dokumentu: popsat a zdokumentovat účel, význam, úlohu a způsob použití klíčových komponent systému) | P2 | E1 |
| A40 | REST API systému musí podporovat autentizovaná i autorizovaná volání rozhraní | P2 | E1 |

Součástí dodávky bude úvodní analýza včetně detailní architektury, návrhu integrační vazeb, akceptačních testů včetně testů interoperability, školení administrátorů (10 osob) a uživatelů (6x20 osob), administrátorská, uživatelské a technická dokumentace.

Součástí analýzy bude také návrh provozních podmínek a typových vnitřních procesů (včetně popisu způsobu archivace dokumentů a výběru dokumentů z archivu) a nezbytných předpisů uživatelů archivu, dokumentace API pro integraci zdrojových systémů a bezpečnostní dokumentace dle požadavků přílohy č. 2 smlouvy o dílo tvořící přílohu č. 4 zadávací dokumentace. Popis způsobu uložení dokumentů/objektů v archivu po jeho jednotlivých vrstvách.

Systém bude provozován v režimu významného IS (VIS) dle konvence současného zákona o kybernetické bezpečnosti

**Součástí akceptace bude otestování akceptačních scénářů:**

* uložení a načtení dokumentu z/do jednotlivých integrovaných systémů do archivu
* razítkování časovým razítkem a jeho kontrola
* provedení vzorové skartace
* prodloužení platnosti/nepopiratelnosti dokumentu
* funkční obousměrná integrace NIS Nemocnice Jihlava