

Elektronické odesílání dat zdravotnické dokumentace

Příloha č. 2: Návrh Zhotovitele – Popis nabízeného technického řešení

Předmětem plnění veřejné zakázky (dílem) je komplexní dodávka a implementace elektronického archivu organizace (EA) pro ZZS KVK, nezbytné úpravy informačního systému elektronické zdravotnické dokumentace (EZD), zahrnující jak systém pro mobilní zadávání dat v terénu (MZD), tak elektronickou kartu pacienta (EKP) v oblasti vytváření elektronické zdravotnické dokumentace a napojení EZD na elektronický archiv pro archivaci elektronické zdravotnické dokumentace Zdravotnické záchranné služby Karlovarského kraje (ZZS KVK), dodávka souvisejících technologií, SW, systémového SW a provozní infrastruktury neposkytovaná Objednatelem a souvisejícího vybavení a služeb. Součástí plnění VZ jsou dále provozní a servisní služby pro zajištění provozu dodaných systémů, jejich úprav a technologií na dobu neurčitou.

1 DETAILNÍ NÁVRH CÍLOVÉHO STAVU

V této kapitole je uveden detailní návrh cílového stavu respektující požadavky podle Přílohy 3 - Technická specifikace (zejména kapitoly 3) včetně uceleného detailního popisu jednotlivých částí systému a jejich vzájemných vazeb.

1.1 PRODUKTY A TECHNOLOGIE

1.1.1 Elektronický archiv

Elektronický archiv (EA) ZZS KVK bude založen na produktu **ICZ DESA** s licencí Multicompany a multiuser – jedná se o licenci bez omezení na počet subjektů a bez omezení na počet uživatelů přistupujících k archivu.

který kompletně řeší potřeby kladené na dlouhodobý důvěryhodný archiv. Jedná se o produkt vyvinutý společností ICZ pro střednědobé až dlouhodobé důvěryhodné uložení elektronických dokumentů a spisů v organizacích v souladu s legislativou i potřebami organizací. Jedná se o mnoha lety ověřené řešení nasazené u zákazníků ve zdravotnictví, státní správě i komerční sféře.

ICZ DESA umožňuje ukládat velmi velké množství dat různorodého obsahu, a to nejenom jednotlivé dokumenty, ale také například velmi složité struktury dokumentů a komplexní spisy (zdravotnické dokumentace, pojistné dokumentace, fotografie atd.).

Důvěryhodná elektronická spisovna **ICZ DESA edice DES** je úložištěm, kam se dostávají elektronické dokumenty z původních aplikací (jedná se o dokumenty úředního charakteru, tj. i zdravotnická dokumentace vedená podle legislativy). Uložená dokumentace zde čeká na standardní skartační řízení. Po uplynutí příslušných lhůt, se dokumenty skartují nebo přesouvají do nadřazeného archivu.

Hlavní funkce systému:

- Zajištění neměnnosti uložených informací
- Kontrola konzistence uložených balíčků
- Zajištění důvěryhodnosti
- Transakční protokol
- Zajištění čitelnosti uložených informací v budoucnosti v dlouhodobě udržitelném formátu
- Metoda migrace formátů
- Předcházení problémům vzniklým generačními změnami HW a SW

Elektronické odesílání dat zdravotnické dokumentace

Softwarové technologie:

Celé řešení je postaveno na přenositelných technologiích (Java, XML) a je jej tedy možné provozovat na různých HW a SW platformách, které podporují prostředí Java.

Nabízené řešení bude postaveno na architektuře tvořené dvojicí serverů, kde jeden z nich bude fungovat jako databázový. Servery budou zapojeny přímo do interní sítě Objednatele. Pro komunikaci budou využívat běžného TCP/IP protokolu.

Databázový server bude dodán s operačním systémem Microsoft Windows a dále pak s licencí relačního databázového stroje, který má v sobě integrovánu podporu pro fulltextové vyhledávání. Bude využita databáze MS SQL Server (2019 a vyšší).

Aplikační server je po softwarové stránce postaven na operačním systému s podporou provozního prostředí Java 2 Standard Edition ve verzi nejméně 1.8 a na aplikačním serveru Tomcat, který je šířen pod licencí GNU/GPL. Bude dodán operační systém Microsoft Windows server 2022.

Další software, jako jsou např. antivirové programy, software pro firewall, síťové komunikační programy apod. není vyžadován. Tento typ systémového software je plně v kompetencích odpovědných pracovníků Objednatele.

Aplikace DESA má webové uživatelské rozhraní. Na pracovní stanice nejsou kladeny žádné speciální požadavky. Postačující je pracovní stanice s instalovaným operačním systémem Microsoft Windows a běžným internetovým prohlížečem splňujícím standardy HTML 4.0 a CSS1, např. Mozilla Firefox verze 4.5 a vyšší, Microsoft Edge, Google Chrome. Je-li tedy na koncové stanici nainstalován operační systém s funkčním internetovým prohlížečem, lze říci, že daná specifikace softwarového vybavení na straně koncového uživatele je splněna. V prohlížečích je nutná podpora Java. Není podporován 64bit Internet Explorer (OS Win XP a vyšší - dle verze instalace).

Hardwarové technologie:

Pro provoz řešení předpokládáme využití vyhrazeného aplikačního serveru pro aplikaci ICZ DESA a samostatného databázového serveru. Je možné také servery virtualizovat.

Požadavky na hardwarovou konfiguraci jsou definovány v závislosti na počtu paralelně pracujících uživatelů. Paralelně pracujícími uživateli se rozumí uživatelé aplikací, kteří v jednom okamžiku aktivně v aplikaci pracují.

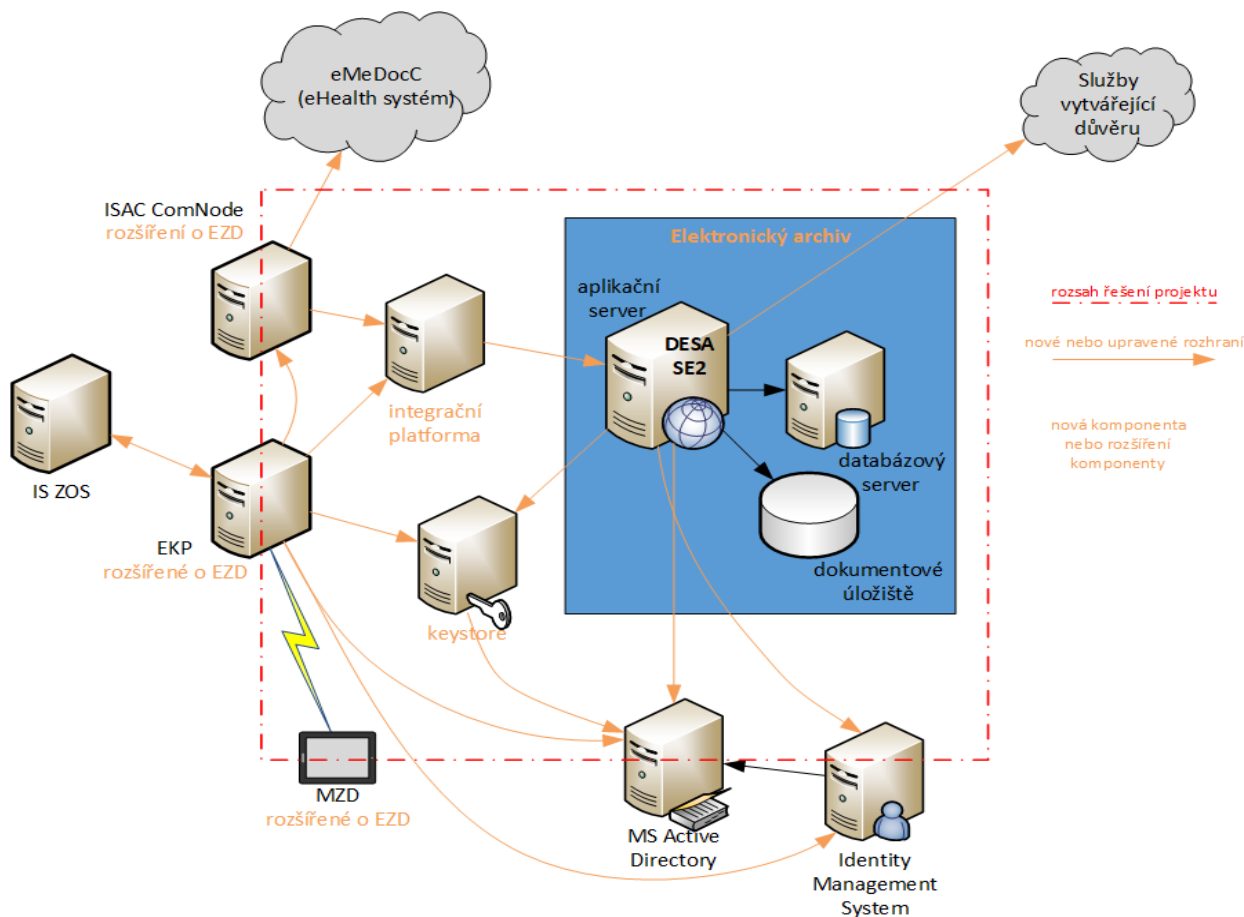
Dalším důležitým parametrem navrženého hardware je odhad potřebné diskové kapacity.

Pro režijní informace dokumentového úložiště, které jsou tvořeny především metadaty a full-text indexy.

1.2 ARCHITEKTURA A POPIS NUTNÉ PROVOZNÍ INFRASTRUKTURY A SYSTÉMOVÉHO SW PRO SYSTÉM

Na následujícím obrázku Obrázek 1 je zobrazena architektura řešení s vyznačeným rozsahem nových nebo rozšířených stávajících komponent a nových nebo rozšířených integračních a komunikačních rozhraní. Následuje pak popis komponent architektury.

Elektronické odesílání dat zdravotnické dokumentace



Obrázek 1: Architektura komponent řešení

V následující tabulce uvádíme popis dodávaných komponent.

Typ	Položka	Popis	Technologie
Infra	EA (App server)	Server poskytuje běhové prostředí pro aplikaci ICZ DESA a její modul SecureElement (SE2), které jsou součástí řešení EA.	Instalováno na serveru
Infra	EA (DB server)	Server poskytuje běhové prostředí pro databázový systém, který poskytuje databázové služby aplikačním komponentám EA.	Instalováno na serveru
Infra	EA (Úložiště)	Datové úložiště pro dlouhodobé ukládání dokumentů	Instalováno na serveru
Infra	Integrační platforma	Server je běhovým prostředím pro integrační platformu ICZ eHSB, která zprostředkovává komunikaci s EA, umožňuje provádět transformace pro přizpůsobení integračních API a datových zpráv, umožňuje orchestraci workflow apod.	Instalováno na serveru
APP	EA (DESA & SE2)	Aplikační software ICZ DESA včetně modulu SecureElement, který poskytuje služby ověřování, pečetení a razítkování.	SW a licence jsou součástí dodávky Uchazeče

Elektronické odesílání dat zdravotnické dokumentace

Typ	Položka	Popis	Technologie
APP	EA (DB)	Databázový systém pro uchovávání a správu metadat archivu.	SW a licence
APP	ISAC CN	Jedná se o rozšíření SW ISAC CN umožňující odesílání ZOV obsahující podepsané PDF prostřednictvím výměnné sítě eMeDocS.	SW
API	EA (DESA)	Integrační rozhraní DESA je součástí dodávky SW DESA - integrační API pro IS původců - webové uživatelské rozhraní - integrační rozhraní na MS AD a IdM - integrační rozhraní k úložišti autentizačních klíčů a certifikátů	SW
API	EA (SE2)	Komunikační služby pro komunikaci s externími službami Poskytovatelů kvalifikovaných služeb vytvářejících důvěru.	SW
API	IP eHSB	Integrační a komunikační rozhraní sběrnice eHSB	SW
API	ISAC CN	Úprava, rozšíření integračních a komunikačních rozhraní komunikačního uzlu ISAC - aby umožňovaly přenos POV ve formě PDF, - aby umožňovaly vyhledání a získání PDF z EA	SW

1.3 SEZNAM PRACÍ ČI ČINNOSTÍ DODAVATELE, KTERÉ JSOU SOUČÁSTÍ DODÁVKY

Uchazeč uvádí, že mu v době podání nabídky není známo, že v rámci realizace VŘ proveden práce či činnosti, které jsou součástí dodávky, které nejsou v zadávací dokumentaci explicitně uvedeny, ale které musí s ohledem na námi nabízený předmět veřejné zakázky a jeho řádnou a úplnou realizaci provést k dosažení objednatelům požadovaného cílového stavu a které jsou tedy součástí dodávky, a tedy i ceny.

Nad rámec požadavků bude samostatně evidovat možné rozvojové požadavky na celé komplexní řešení. Řízení změn bude prováděno dle zásad obecného change managementu.

2 DETAILNÍ NÁVRH CÍLOVÉHO STAVU

Níže je popsán detailnější návrh řešení. Uchazeč explicitně deklaruje, že implementuje technologie, software, úpravy nezbytných aplikací a provede další činnosti požadované Objednatelem tak, aby dodané řešení bylo plně funkční a splňovalo požadavky Objednatele.

2.1 DODÁVKA ELEKTRONICKÉHO ARCHIVU (EA)

Ozn.	Položka	Popis	Počet
1	Dodávka elektronického archivu (EA)	Dodávka dlouhodobého bezpečného důvěryhodného elektronického archivu pro archivaci elektronické zdravotnické dokumentace a ostatní dokumentace v souladu s legislativou. V tomto archivu bude ukládána elektronická dokumentace vzniklá v rámci provozu ZZS.	1 soubor

Dodávka elektronického archivu bude splňovat níže uvedené požadavky a bude mít následující vlastnosti.

2.1.1 Legislativa a normy

Legislativní požadavky a normy, které nabízené řešení splňuje:

- Zákon č. 499/2004 Sb.,
- Vyhláška č. 259/2012 Sb.
- Zákon 300/2008 Sb.
- Národní standard z Věstníku MV 57/2017
- ISO 14721:2003, které přešlo na ISO 14721:2012 Open archival information system (OAIS) — Reference model

2.1.2 Ochrana uložených informací

- Dlouhodobá čitelnost
 - Vstup v dlouhodobě udržitelném formátu
 - Metoda migrace formátů
- Neměnnost
 - Kontrola konzistence uložených balíčků
 - Aplikace elektronických pečeti a časových razítek
- Věrohodnost
 - Transakční protokol

2.1.3 Základní vlastnosti:

- DESA je oddělená od ostatních systémů
- V DESA neexistuje funkcionalita, která mění nebo maže uložená data
- DESA eviduje a archivuje všechny operace v transakčních záznamech
- DESA využívá omezená skupina uživatelů s vymezenými rolmi
- DESA ukládá data ve více kopiích a kontroluje jejich konzistenci

Elektronické odesílání dat zdravotnické dokumentace

2.1.4 Cíle a hlavní úlohy

Ztráta dokumentů, dokladujících vnitřní procesy organizace, nebo ztráta jejich důvěryhodnosti představuje obecné riziko související s právní jistotou, jednoznačností a vymahatelností. Elektronické dokumenty pak svojí nematerializovanou podstatou představují další rizika - technologická. Kterým technologickým rizikům čelí elektronické dokumenty při dlouhodobé archivaci?

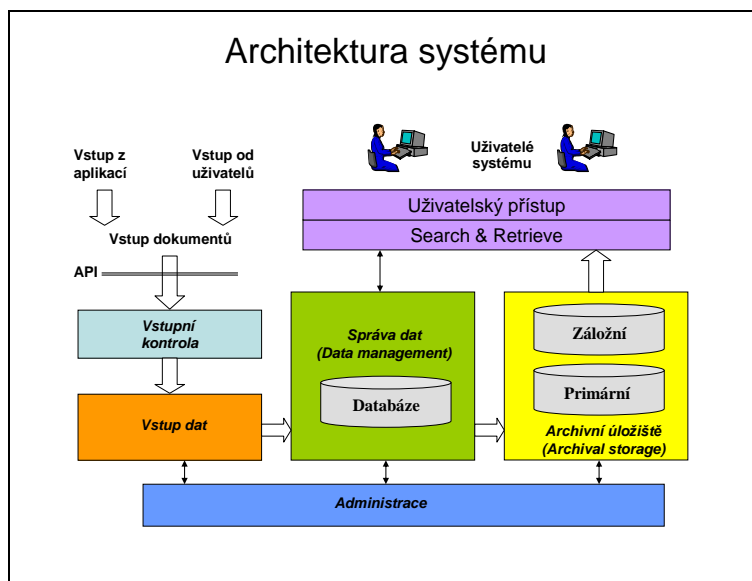
Běžná technologická rizika uchovávání elektronických informací (nejen dokumentů):

- Nefungující software
- Nefungující hardware
- Změna obsahu
- Smazání obsahu

Technologická rizika, kterým čelí elektronické dokumenty při dlouhodobém uložení:

- degradace nosiče
- zastarávání hardware
- zastarávání formátu
- zastarávání SW technologií a principů
- ztráta autenticity – platnost autentizačních prvků

Odstranění uvedených technologických rizik, jejich eliminace a zajištění průkaznosti uchovávaných dokumentů – to jsou hlavní cíle a úkoly ICZ DESA.



Obrázek 2: Architektura řešení DESA

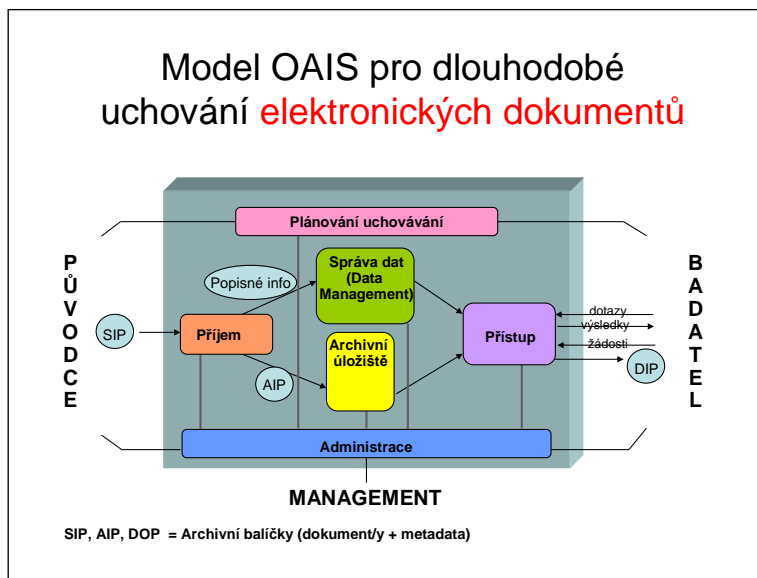
Na obrázku uvedené Archivní úložiště není předmětem nabídky. Předmětem nabídky je úložiště typu NAS, na které mohou být archivní dokumenty ukládány. Toto úložiště bude umístěno v primárním datovém centru, pokud si Objednatel nezajistí jeho uložení a propojení s primárním v jiné lokalitě.

2.1.5 Architektura systému ICZ DESA

Architektura vychází z mezinárodně uznávaného standardu OAIS (ISO 14721:2003 - Open Archival Information System). Tento standard vymezuje základní koncepci archivu pro uložení elektronických dokumentů. Standard definuje hlavní funkce, které má archiv zajišťovat. Jedná se o příjem dokumentů,

Elektronické odesílání dat zdravotnické dokumentace

správu dat, archivní uložení, přístup, administraci a plánování uchovávání. Základní model OAIS je na následujícím obrázku.



Obrázek 3: Model OAIS

Podle standardu OAIS je elektronický dokument a všechny informace, které jsou spolu s ním ukládány v Digitálním archivu zabalen do balíčku s jednotnou strukturou. Podle standardu OAIS jsou tyto balíčky nazývány SIP – Submission Information Package (balíčky přijímané od původců), AIP - Archival Information Package (archivní balíčky) zahrnující ukládaný obsah a jeho příslušné popisné informace pro uchovávání (archivní a technické informace) a DIP - Dissemination Information Package (balíčky vytvořené na základě badatelského dotazu).

Podle OAIS je dlouhodobé uchovávání definováno jako:

- Uchování dat v podobě posloupnosti bitů (Bit Streams) v průběhu jakéhokoli kopírování.
- Schopnost kdykoli v budoucnosti interpretovat informace uchované v této posloupnosti bitů.
- Schopnost kdykoli v budoucnosti prezentovat informace uchované v posloupnosti bitů uživateli.

Pracovní postup při ukládání elektronických dokumentů do ICZ DESA je následující:

- Elektronický dokument je nejprve připraven u původce (DMS či agendy ve které dokument vznikl) do vhodné podoby pro předání do archivu.
- Dokumenty převzaté k archivaci v ICZ DESA jsou zkontrolovány dle stanovených pravidel (na integritu, neškodnost, validitu, kvalitu apod.). Elektronické dokumenty jsou dále doplněny metadaty podporujícími procesy řízení, uchovávání a zpřístupňování (viz dále); každému dokumentu je přidělena jednoznačná identifikace a vše je zabalen do archivního informačního balíčku (všechna metadata a elektronické soubory). Archivní balíček je poté uložen do archivního úložiště. ICZ DESA pak zajišťuje bezpečné uložení archivních balíčků. Na základě uchovávací strategie provádí činnosti pro udržení čitelnosti a životaschopnosti elektronických dokumentů.

Základem dlouhodobého uložení je volba vhodné uchovávací metody. Uchovávací metoda je způsob jak dlouhodobě (po neomezenou dobu) zajistit zpřístupnění elektronických dokumentů pořízených původními počítačovými technologiemi, které se již nepoužívají. Díky ní je možno reagovat na nepředvídatelný vývoj technických i programových prostředků a udržovat archivované elektronické dokumenty neustále čitelné a prezentovatelné.

Elektronické odesílání dat zdravotnické dokumentace

Jak již bylo uvedeno, každý uložený dokument bude doplňován metadaty. Metadata obsahují vlastnosti dokumentu, jeho strukturu a další informace, potřebné pro archivaci.

- Popisná metadata (například název, popis, autor, původce, typ, kategorie a další) slouží převážně pro popis elektronických dokumentů a jsou využívána pro vyhledávání objektu a zjištění základních údajů o objektu. Popisná metadata vycházejí ze standardu Moreq2.
- Uchovávací metadata slouží pro podporu uchovávání a pro archivační aktivity. Uchovávací metadata obsahují údaje o formátu, technické údaje o uložených digitálních objektech. Dále obsahují informace o činnostech či změnách provedených s elektronickým obsahem.
- Strukturální metadata slouží pro sdružení všech částí informačního balíčku do jednoho logického celku.

Použitá technologie dlouhodobé archivace, kromě ochrany před ztrátou dat, zachovává čitelnost dokumentů, jejich autenticitu a nezměnitelnost. Je zajištěno, že budou prováděny pouze kontrolovatelné a autorizované zásahy a ty budou prokazatelně dokladované. Veškeré procesy s dokumenty jsou dokumentovány tak, aby budoucí uživatel mohl v případě potřeby vyhodnotit, jaké zásahy byly provedeny, kdo, kdy a z jakého důvodu je prováděl.

2.1.6 Vkládání dokumentů

Pracovní postupy při ukládání elektronických dokumentů do ICZ DESA je následující:

- Elektronický dokument, který je určen pro uložení do ICZ DESA, musí být nejprve připraven do vhodné podoby pro předání. Tuto přípravu zajistí buď určený uživatel původce manuálně, ve speciálním nástroji, nebo je příprava provedena automatickou službou zajišťující integraci aplikace, ve které dokumenty vznikají s ICZ DESA. Připravené dokumenty v podobě informačních balíčků SIP jsou přes aplikační rozhraní přeneseny do ICZ DESA. Balíčky SIP obsahují kromě souborů s dokumenty také určená popisná metadata.
- Dokumenty převzaté k archivaci v DESA jsou zkontrolovány dle stanovených pravidel (na integritu, neškodnost, validitu, kvalitu apod.). Elektronické dokumenty jsou dále doplněny technickými metadaty podporujícími procesy řízení, uchovávání a zpřístupňování. Každému dokumentu je přidělena jednoznačná identifikace a vše je zabaleno do archivního informačního balíčku AIP (všechna metadata a elektronické soubory). Archivní balíček je poté uložen do archivního úložiště.
- ICZ DESA pak zajišťuje bezpečné uložení archivních balíčků. Na základě uchovávací strategie provádí činnosti pro udržení čitelnosti, důvěryhodnosti a životaschopnosti elektronických dokumentů.

2.1.7 Zajištění důvěryhodnosti

Je zajištěno, že ICZ DESA bude provádět pouze kontrolovatelné a autorizované zásahy a ty budou prokazatelně dokladované. Veškeré procesy s dokumenty jsou dokumentovány tak, aby budoucí uživatel mohl v případě potřeby vyhodnotit, jaké zásahy byly provedeny, kdo, kdy a z jakého důvodu je prováděl.

2.1.8 Zajištění dlouhodobosti

Opatření proti zastarávání formátu (uchovávají metoda).

Z řady v současnosti známých metod byla vybrána metoda **migrace formátu**. Dokumenty musí být na vstupu v dlouhodobě udržitelném formátu, nebo jsou do něj na vstupu konvertovány. Pro systém ICZ DESA existuje číselník (seznam) povolených (akceptovatelných) formátů souborů s dokumenty. Příklady formátů ze současného světa dokumentů jsou PDF/A, XML pro text a tabulky, TIFF, PNG pro rastrovou grafiku, SVG pro vektorovou grafiku, AIFF, WAV pro zvuk, MPEG-2 pro video. Tento seznam je možno aktualizovat podle budoucího vývoje počítačových technologií.

Opatření proti degradaci a zastarávání nosiče

Elektronické odesílání dat zdravotnické dokumentace

Veškerý obsah archivu bude ukládán paralelně, alespoň ve dvou identických fyzických kopiích.

ICZ DESA obsahuje mechanismy pravidelné kontroly integrity uloženého obsahu a řešení situace, kdy je zjištěno, že jedna z kopií obsahu má porušenou integritu.

Konkrétní specifikace fyzických úložišť je záležitostí implementační procedury.

Opatření proti zastarávání systémového hardware a operačního systému

S vývojem počítačových technologií je nutno počítat s tím, že se fyzická úložiště a média budou měnit.

S vývojem počítačových technologií je nutno počítat s tím, že se bude měnit systémový hardware a jeho operační systém. Pro dlouhodobý archiv je nutno počítat s tím, že v nějakém období bude nutno celý archiv přemigrovat ze starého na nový systém. Proto provoz systému je rozdělen na tzv. provozní cykly odpovídající životnosti jednoho infrastrukturního systému (hw+os). Délku trvání provozních cyklů není možné předvídat. Pravděpodobně nebude kratší než 10let. Většinou se počítá s délkou 15 let.

Opatření proti zastarávání SW principů

S vývojem počítačových technologií je nutno počítat s tím, že se budou měnit použité metody pro různé moduly systému. Pro některé použité metody, u kterých je předpoklad rychlého vývoje, je možnost změny přímo zintegrována v systému (např. pro tzv. hashovací funkce - funkce pro výpočet kontrolních součtů zajišťujících integritu dat a jejich bezpečnost. Identifikace funkce použité pro konkrétní data/dokument je vždy uložena spolu s vypočítanou hodnotou). Změnu ostatních metod je nutno řešit individuálně podle situace (například odložením řešení na konec provozního cyklu a jeho vyřešení v rámci migrace na nový systém).

2.1.9 Řízení přístupu k dokumentům

Kromě správců systému v roli archiváře, mohou ostatní uživatelé vždy jen číst uložené informace. Uživatel, který nemá přístup ke konkrétnímu dokumentu se ani nedozví, že dokument existuje. Podle stupně oprávnění může uživatel číst popisná metadata, číst všechna metadata dokumentu a zobrazit vlastní dokument.

2.1.10 Vyhledání a získání dokumentu

Pokud uživatel systému ICZ DESA potřebuje získat dokument, musí příslušný dokument nejprve vyhledat. Vyhledání dokumentu/ů je možné buď podle jednoznačného identifikátoru dokumentu, nebo pomocí zadání vyhledávacích kritérií (kombinace hodnot metadat). Na základě zadaného dotazu systém vyhledá odpovídající dokumenty, ověří přístup k nim pro přihlášeného uživatele a zobrazí seznam nalezených dokumentů. Ke zvolenému dokumentu má uživatel možnost zobrazit jeho další podrobnosti - uchovávané hodnoty metadat, historii.... Dále je možno si vyžádat důvěryhodnou kopii dokumentu.

2.1.11 Vyřazení dokumentu ze systému

Po vypršení archivační lhůty může být dokument ze systému vyřazen.

Vyřazením se rozumí zničení obsahu skartovaných dokumentů, resp. export dokumentů a jejich metadat do formátu vhodného pro přenos do nadřazeného archivu. Podle nastavení systému se dokumenty předané prokazatelně do nadřazeného archivu také zničí, nebo zůstávají jako kopie nadále v systému. O vyřazení se pořizuje skartační, resp. předávací protokol.

2.1.12 Provoz systému

Důvěryhodný elektronický archiv je systém složený z hardwarové a softwarové části a činnosti lidí-administrátorů, správců a archivářů. Pro důvěryhodnost uložených dokumentů je nezbytné zajistit ze strany provozovatele dodržování závazných metodických předpisů.

Elektronické odesílání dat zdravotnické dokumentace

2.1.13 Rozsah funkcí systému ICZ DESA

Systém ICZ DESA bude zajišťovat následující funkce v oblasti ukládání a přístupu k dokumentům:

- Vstup dokumentů prostřednictvím definovaného API
- Vstupní kontrola proti škodlivému obsahu, kontrola formátu metadat a validace číselníkových hodnot.
- Uložení dokumentů ve formě balíčků AIP v úložišti ve dvou nezávislých kopiích (předpokládá se použití diskového pole).
- Periodická kontrola integrity uložených balíčků na aplikační úrovni oproti systému správy dat ICZ DESA
- Ukládání transakčních logů ve formě balíčků AIP.
- Vyhledání dokumentů podle základních metadat podporovaných aplikací (zejména typ dokumentu, identifikátor dokumentu a datum vzniku).
- Výdej obsahu dokumentu uživateli či výdej dokumentů jinému systému pomocí API rozhraní.
- Vyřazování dokumentů.

Systém ICZ DESA bude dále zajišťovat tyto administrační funkce:

- Správa uživatelů.
- Správa rolí.
- Správa číselníků (formou importu číselníků pro definovaný rozsah platnosti v předdefinovaném XML formátu). Zejména se jedná o klasifikaci dokumentu, typ dokumentu a spisový znak.

Přístupová oprávnění k jednotlivým dokumentům budou určena typem dokumentu a rolí uživatele, definovanou v systému ICZ DESA.

2.1.14 Uživatelské funkce systému ICZ DESA

Tato kapitola uvádí seznam funkcí ICZ DESA, které budou k dispozici uživatelům. Funkce jsou rozděleny do skupin: 1. vstup, 2. Výstup, 3. Přístup.

1. Ukládání dokumentů do archivu

- zobrazení stavu zpracování vstupních balíčků
- možnost individuálního uložení dokumentu do archivu mimo automatický import prostřednictvím klientské aplikace (nutná instalace na platformě podporující běh aplikací v prostředí Java SE 5)
 - uživatel zapíše potřebná metadata a klasifikuje dokument
 - před vlastním uložením proběhnou některé kontroly a vstupní zpracování

2. Vyřazování záznamů

- příprava skartačního řízení
 - zobrazení všech dokumentů, kterým uplynula skartační lhůta,
 - zařazení do skartačního řízení, sestavení skartačního návrhu
 - schválení skartačního návrhu
- skartační řízení
 - kontrola skartačního návrhu
 - na základě schválení skartačního návrhu provedení vyřazení:
 - přenos do národního archivu
 - skartace - zničení dokumentů a některých metadat, ponechání základních údajů o dokumentu a údajů o skartaci

3. Přístup uživatelů k uloženým záznamům

Elektronické odesílání dat zdravotnické dokumentace

- vyhledání dokumentů podle vybraných popisných metadat s respektováním nastavených oprávnění na dokument a na uživatele
- zobrazení metadat a obsahu dokumentů podle oprávnění
- vyžádání kopie uložených archivních balíčků (AIP)
- Příjem vyžádané kopie
 - generování jednotného výstupu (DIP – poskytovaný balíček metadata a obsah)
 - distribuce – elektronický kanál (e-mail)

4. Správa systému ICZ DESA

- Správa uživatelů

Uživatele pracující s digitální spisovnou a archivem můžeme rozdělit do čtyř základních rolí:

- Centrální administrátor (např. správce ICZ DESA) – tato role spravuje celkovou konfiguraci archivu a spravuje záznamy a jejich seskupování, provádí údržbu, ...
 - Posuzovatel – toto je speciální role, která je primárně zodpovědná za přípravu a vyřazování záznamů na základě definovaných skartačních plánů.
 - Uživatel spisovny a archivu – tato role má základní úroveň přístupových práv k záznamům, rutinně používá archiv pro hledání záznamů, popř. pro individuální přidávání záznamů. Možnost řízení oprávnění k dokumentům podle příslušnosti uživatele k původci
- Správa rolí
 - Práva a omezení jednotlivých rolí pro základní funkce spisovny - prvotní návrh vychází ze specifikace MoReq2.
 - Správa číselníků (formou importu a exportu číselníků pro definovaný rozsah platnosti v předdefinovaném XML formátu). Zejména se jedná o klasifikaci dokumentu, typ dokumentu a spisový znak.

2.1.15 Souhrn parametrů

Níže uvádíme souhrn parametrů řešení DESA.

System bude poskytnut v multilicenčním režimu, tj. bez omezení počtu přihlášených uživatelů, a bez omezení z pohledu jakýchkoliv provozních licencí (např. licence run-time).

Uživatelská vrstva je tvořena webovou aplikací a uživatelské rozhraní je zobrazováno v prohlížečích:

- Mozilla Firefox verze 110 a vyšší,
- Microsoft Edge, Google Chrome

System vychází z platné legislativy v oblasti správy dokumentů, minimálně s níže uvedeným výčtem právních předpisů. Zároveň System implementuje pracovní postupy, procesy a datové formáty ve shodě s platnou legislativou pro dlouhodobé a důvěryhodné ukládání dat. Konkrétně se řídí těmito předpisy:

- Zákon č. 499/2004 Sb., o archivnictví a spisové službě, v platném znění, ve znění pozdějších předpisů,
- Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů,
- Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, ve znění pozdějších předpisů,
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů,
- Národní standard z věstníku MV 57/2017

Elektronické odesílání dat zdravotnické dokumentace

- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů. A jeho doprovodný změnový Zákon č. 298/2016, ve znění pozdějších předpisů.

Řešení, jako systém na dlouhodobé uchovávání elektronických dokumentů, odpovídá mezinárodnímu standardu pro dlouhodobé ukládání informací OAIS (Open Archival Information System – norma ISO 14721:2003, ISO 14721:2012). Ten specifikuje základní funkční části otevřeného archivu, komunikaci s okolím, procesy a informační model ve formě informačních balíčků přijímaných, poskytovaných, a především uložených v úložišti.

Zejména pak musí splňovat tyto požadavky:

- Dokumenty a jejich metadata tvoří v rámci systému jeden balíček a jsou tak uloženy po celou dobu, po kterou je dokument přítomen v systému
- Systém umožní příjem, uchování a výdej dokumentů ve formě balíčků SIP, AIP, DIP
- Řešení není svázáno s konkrétním formátem dokumentu nebo technologií a je připraveno na změnu těchto technologií.
- Systém musí podporovat migrační strategie na jiné formáty, technologie nebo kompletně jiný systém.
- Informace jsou v datovém balíčku uchovávány v otevřené podobě, tedy v takovém formátu, který lze číst běžně dostupnými prostředky, které nejsou závislé na dodávaném systému-
- Data jsou organizována na úrovni ukládacích jednotek, které odpovídají fyzickému uložení dokumentů ve spisovně/archivu.

Archiv bude vybudován takovým způsobem, který zajistí nezávislost spravovaných dat na použitých SW a HW technologiích a také na dodavateli tohoto systému. Mezi požadavky, které pomohou zajistit splnění této podmínky patří zejména:

- Řízení veškeré funkcionality na aplikační úrovni systému bez využití speciálních vlastností HW úložišť či Výpočetního vybavení.
- Ukládání dat v podobě datových balíčků dle příslušných norem uvedených výše.
- Systém podporuje migrační strategie na jiné formáty, technologie nebo kompletně jiný systém.
- Data jsou organizována na úrovni ukládacích jednotek, které odpovídají fyzickému uložení dokumentů ve spisovně/archivu.
- Pokud popisná metadata obsahují výsledek nějaké obecně popsané funkce (například hash/otisk), je třeba uložit identifikaci této funkce použité pro konkrétní data/dokument vždy uložena spolu s vypočítanou hodnotou.
- Řízením se standardy.

Systém ukládá data systémem datových balíčků, což jsou soubory obsahující elektronické dokumenty, které jsou dále doplněny metadaty podporujícími procesy řízení, uchovávání a zpřístupňování. Každému dokumentu je přidělena jednoznačná identifikace a vše je zabaleno do archivního informačního balíčku (všechna metadata a elektronické přílohy/soubory/dokumenty). Datové balíčky, ve kterých jsou dokumenty ukládány, musí splňovat následující požadavky:

- Dokumenty a jejich metadata tvoří v rámci systému jeden balíček a jsou tak uloženy po celou dobu, po kterou je dokument přítomen v systému.
- Systém umožňuje příjem, uchování a výdej dokumentů ve formě balíčků SIP, AIP, DIP (více v normě OAIS).
- Řešení není svázáno s konkrétním formátem dokumentu nebo technologií a je připraveno na změnu těchto technologií.

Elektronické odesílání dat zdravotnické dokumentace

<ul style="list-style-type: none">• Informace jsou v datovém balíčku uchovávány v otevřené podobě, tedy v takovém formátu, který lze číst běžně dostupnými prostředky, které nejsou závislé na dodávaném systému, ani na použitém formátu.
<p>System na aplikační úrovni, tedy nezávisle na použitém HW, umožňuje distribuci přijatých datových balíčků na více připojených úložišť.</p> <ul style="list-style-type: none">• Počet těchto úložišť nebude nijak omezen a bude možné úložiště přidávat a odebírat pouze změnou konfiguračních parametrů systému.• Jednotlivá úložiště mohou být heterogenní, vzájemně nezávislá, nepropojená a bez replikace na úrovni HW, ovladačů nebo operačních systémů.• Při přidání dalšího úložiště systém automaticky vytvoří kopie spravovaných datových balíčků na toto nové úložiště.• Systém bude podporovat úložiště komunikující minimálně protokoly CIFS a NFS.• Systém umožní konfigurovat tato úložiště nezávisle pro různé původce dat.• Pro jednotlivá datová úložiště bude možné nastavit prioritu čtení, tzn. To, které z připojených datových úložišť bude přednostně využito pro čtení datových balíčků.
<p>System bude provádět pravidelnou kontrolu konzistence jednotlivých datových balíčků na připojených datových úložištích.</p>
<p>Při zjištění nekonzistence nebude systém automaticky vyhodnocovat a provádět opravu, ale pouze dostatečně zaznamená tento stav, který bude následně řešit pověřený správce systému.</p>
<p>System nebude na aplikační úrovni poskytovat žádné funkce k mazání dokumentů a datových balíčků ani žádné nástroje na změnu obsahu dokumentů.</p>
<p>System bude disponovat mechanismy, které zajistí odolnost proti změnám obsahu a zajistí důvěru v pravost a neporušenost uloženého obsahu. Tento stav zajistí využitím systému časových razítek ve spolupráci s akreditovanou certifikační autoritou, která tato časová razítka vydává. Konkrétně bude DDÚ v této oblasti disponovat těmito vlastnostmi:</p> <ul style="list-style-type: none">• Integrací s akreditovanou certifikační autoritou zajistí automatické vydávání časových razítek a jejich aplikaci na uložené datové balíčky.• Bude pravidelně (v konfiguračně nastavitelných intervalech) kontrolovat platnost časových razítek jednotlivých uložených datových balíčků a s dostatečným, konfiguračně nastavitelným předstihem, zajistí vydání časových razítek nových a jejich aplikaci na související datové balíčky.• Umožní aplikaci časových razítek na celou skupinu datových balíčků najednou. Bude možné konfiguračně nastavit velikost této skupiny. Zároveň bude možné konfiguračně nastavit, jak dlouho mohou datové balíčky čekat na příjem, než jejich počet dosáhne stanovené velikosti skupiny. Po uplynutí této lhůty dojde k aplikaci časového razítka na balíčky aktuálně čekající na příjem, přesto že jejich počet nebude odpovídat nastavené velikosti skupiny.• Systém skupinového razítkování nebude nijak omezovat možnost provést řízenou skartaci jednotlivých balíčků ze skupiny, na kterou je aplikováno jedno časové razítko. I po skartaci části datových balíčků ze skupiny nebude porušena integrita a důvěryhodnost ostatních datových balíčků.

Elektronické odesílání dat zdravotnické dokumentace

<ul style="list-style-type: none">• Možnost napojení na nejméně na dvě akreditované certifikační autority najednou jako zálohu v případě nedostupnosti jedné z nich.• Možnost aplikovat na jeden datový balíček časová razítka od více certifikačních autorit.
Data nelze v systému nijak měnit ani mazat. Jediným způsobem, jak data vyřadit je plánovaná skartace dle platné legislativy. I pak mohou být dokumenty v systému přítomny.
Při opravě dokumentu nebo jeho metadat dojde vždy k vytvoření další verze dokumentu. Všechny předchozí verze jsou vždy dostupné.
Při příjmu datového balíčku se stejnou identifikací na úrovni systému bude tento uložen vždy jako nová verze tohoto datového balíčku.
Pokud DDÚ podporuje funkci konverzí mezi datovými formáty uloženého obsahu, musí být konvertovaná verze obsahu vždy uložena jako nová verze datového balíčku.
Uživatelské i aplikační rozhraní poskytne přístup ke všem existujícím verzím datového balíčku.
Přístup do systému budou mít jen oprávnění uživatelé. Přihlašování uživatelů do systému bude probíhat ověřením přihlašovacích údajů za využití protokolu LDAP na adresářové služby zadavatele (MS Active Directory).
Přístup uživatelů k funkcím a obsahu bude možné nastavit na úrovni uživatele, jemuž bude možné přiřadit předem definované role s příslušnými oprávněními k funkcím systému. Oprávnění k používání systému musí být možné rozdělit dle činností do těchto skupin/rolí: <ul style="list-style-type: none">• Centrální správce - spravuje celkovou konfiguraci systému, provádí údržbu systému a centrální dohled.• Lokální správce - spravuje a konfiguruje vlastnosti spojené s jedním původcem dat a spravuje uživatele tohoto původce.• Archivář - nakládá s balíčky na příjmu a při skartaci na základě skartačních plánů.• Uživatel - běžný uživatel, který může vyhledávat a zobrazovat balíčky dle přidělených oprávnění
Systém poskytne nástroje k evidenci zápůjček a nahlížení do obsahu oprávněným žadatelům v tomto rozsahu: <ul style="list-style-type: none">• Uživatelské rozhraní bude obsahovat funkce pro výdej datových balíčků těmito formami:• Zapůjčení fyzických dokumentů uložených ve spisovných/archivech s generováním zápůjčních protokolů.• Vyžádání datového balíčku. Oprávněný uživatel bude mít možnost vybrat skupinu datových balíčků a tu buď exportovat na lokální disk.• Evidence totožnosti osob, které si dokumenty půjčili nebo do archivu nahlíželi.• Evidence dokumentů, které jsou zapůjčeny a těch, do kterých bylo nahlíženo.• Evidence data a času, ve kterých k zápůjčkám, nahlížení, nebo výdeji datového balíčku došlo.
Systém poskytne funkci uživatelského rozhraní, pomocí které bude mít uživatel možnost upravit popisná metadata datového balíčku a opravit tak případné chyby z předchozího zpracování. Výsledkem této úpravy bude nová verze datového balíčku s upravenými metadaty.

Elektronické odesílání dat zdravotnické dokumentace

2.2 ÚPRAVY A NAPOJENÍ EZD NA ELEKTRONICKÝ ARCHIV

2	Úpravy a napojení EZD na elektronický archiv a sdílení zdravotnické dokumentace	Nezbytné úpravy EZD pro vytváření elektronické zdravotnické dokumentace a její archivace do elektronického archivu organizace a sdílení zdravotnické dokumentace prostřednictvím eHealth systémů s dalšími poskytovateli zdravotních služeb. Součástí budou i nástroje pro správu certifikátů, autentizaci uživatelů a podepisování dokumentů uživateli.	1 soubor
---	---	--	----------

Úpravy EZD, které umožní napojení na digitální archiv se dají rozdělit do následujících oblastí:

1. Rozšíření MZD o funkčnosti odběru biometrického podpisu pořízeného Záznamu o výjezdu (ZOV)
2. Přebírání nových údajů ze záznamu operátora v IS ZOS.
3. Zařazení nových údajů ze záznamu operátora v IS ZOS do Záznamu o výjezdu (ZOV).
4. Implementace procesu průběžné aktualizace ZOV a jeho podepisování uživateli, kteří provedli zápis / změnu v dokumentaci. Úpravy budou provedeny v rámci Elektronické karty pacienta (EKP).
5. Úpravy modulu Pojišťovna (POJ) tak, aby případná změna identifikačních údajů pacienta v POJ byla digitálně podepsána a promítnuta do ZOV.
6. Úpravy MZD a EKP, které zabrání podepsání zdravotnické dokumentace certifikátem s blížícím se koncem platnosti.
7. Integrace EZD s digitálním archivem.

2.2.1 Rozšíření MZD o funkčnosti odběru biometrického podpisu pořízeného Záznamu o výjezdu (ZOV)

Pro přechod do plně elektronické zdravotní dokumentace ZZS KVK je třeba, aby potvrzení převzetí pacienta přijímacím lékařem ZZ bylo zachyceno v elektronické podobě. V rámci realizace tohoto požadavku dojde k implementaci odběru biometrického podpisu přímo v MZD v okamžiku, kdy je předáván pacient do ZZ. Přijímací lékař provede potvrzení převzetí pacienta podpisem na tabletu MZD.

Obdobně bude biometrický podpis využíván pro podpis pacienta v případě odmítnutí poskytnuté péče – negativního reversu, potvrzení příjmu faktury za poskytnutou péči či potvrzení informovaného souhlasu.

Biometrický podpis bude zaznamenán do záznamu o výjezdu a nadále budou v rámci ZoV udržovány informace nezbytné pro zajištění validity biometrického podpisu.

2.2.2 Úpravy modulu Pojišťovna (POJ) tak, aby případná změna identifikačních údajů pacienta v POJ byla digitálně podepsána a promítnuta do Záznamu o výjezdu

V rámci procesů OZP dochází mimo jiné i k ztotožnění neznámého pacienta či doplnění nebo opravě zadaných identifikačních údajů pacienta. Aktualizace takových údajů musí být promítnuta do ZOV a zároveň digitálně podepsána uživatelem, který danou změnu provedl. Modul POJ nově zajistí promítnutí těchto změn do ZOV a zároveň digitální podpis uživatelem, který tuto změnu provedl. Adekvátním způsobem dojde i k záznamu změn do změnových logů.

2.2.3 Úpravy MZD, EKP a POJ, které zabrání podepsání zdravotnické dokumentace certifikátem s blížícím se koncem platnosti

Ne vždy je možné předat digitálně podepsanou dokumentaci do DA případně může dojít k situaci, kdy DA aplikuje pečeť na předanou dokumentaci s časovým odstupem. Teoreticky může nastat situace, kdy je dokument elektronicky podepsán certifikátem, kterému před zpracováním v DA vyprší platnost. Aby se

Elektronické odesílání dat zdravotnické dokumentace

zamezilo takovým případům, bude v rámci MZD, EKP a POJ implementována funkčnost, která neumožní digitální podpis certifikátem, jehož platnost nastane v dohledné době (konfigurovatelný časový interval).

2.2.4 Integrace EZD s digitálním archivem

Integrace EZD s digitálním archivem umožní následující funkčnosti:

1. Vytváření a předávání dokumentů z EZD do EA
2. Poskytnutí dodatečných metadat týkající se předávané dokumentace do EA
3. Vytvoření fronty dokumentů pro předání do EA
4. Vytvoření dočasného úložiště archivovaných dokumentů

Archivace dokumentace a práce s archivovanou dokumentací bude realizována tak, aby výpadek EA neměl negativní dopad na poskytování ostatních služeb EZD.

2.2.4.1 Vytváření a předávání dokumentů z EZD do EA

Do EA budou předávány následující typy dokumentů:

1. Záznam o výjezdu od posádky (jen elektronicky podepsaný originál).
2. Pokud v rámci vykazování péče zdravotním pojišťovám dojde ke změně údajů pacienta, bude vytvořen a podepsán aktualizovaný záznam o výjezdu (doplnění funkčnosti do modulu pojišťovny).
3. Veškeré ostatní elektronicky podepsané dokumenty systému EZD, tvořící soubor zdravotnické dokumentace.

Dokumenty mohou vznikat opakovaně, v případě, že budou prováděny úpravy zdrojových dat v rámci kontrolních procesů na straně ZZS nebo zdravotních pojišťoven.

Pokud vznikne dokument opakovaně, bude do EA vložen jako nová verze téhož typu dokumentu.

EA vrátí při archivaci dokumentu do EZD odkaz na archivované dokumenty pro následné zobrazování náhledů. EZD si uloží odkaz na dokument v EA pro zajištění vzájemné provázanosti systémů.

2.2.4.2 Poskytnutí dodatečných metadat týkající se předávané dokumentace do EA

Součástí archivované dokumentace budou následující údaje (metadata):

1. Identifikace výjezdu, datum a čas výjezdu, pořadové číslo výjezdu.
2. Bezvýznamový identifikátor pacienta – v rámci EA nebude mít význam, bude se jednat o identifikátor z EZD, který nebude rodným číslem.
3. Datum a čas vzniku dokumentu.
4. Autor dokumentu (identifikace uživatele)
5. Identifikace vozidel v rámci výjezdu (může být více vozidel)

EZD umožní vyhledávání v archivované dokumentaci dle uložených metadat.

V rámci implementační analýzy může dojít k doplnění metadat na základě procesních potřeb archivace

2.2.4.3 Vytvoření fronty dokumentů pro předání do EA

Dokumenty budou do EA předávány bezprostředně po svém vzniku a podpisu oprávněnou osobou. V případě, že nebude funkční připojení na EA, budou dokumenty z EZD předány po opětovném připojení EA.

2.2.4.4 Vytvoření dočasného úložiště archivovaných dokumentů

Při požadavku na zobrazení dokumentu v EZD se budou tyto dokumenty primárně zobrazovat z EZD. V EZD budou udržovány kopie archivovaných dokumentů po dobu min. 3 roky (konfigurovatelný parametr systému). Po této době odmazání dokumentů z EZD a možnost jen odkazování do EA.

Elektronické odesílání dat zdravotnické dokumentace

Pokud již uběhla doba pro smazání dokumentů v EZD a ty již nejsou v EZD uloženy, bude po upozornění uživateli dokument stažen z EA do dočasného úložiště v EZD.

Pokud bude dokument již stažen do dočasného úložiště EZD bude uživateli nabídnut z tohoto úložiště.

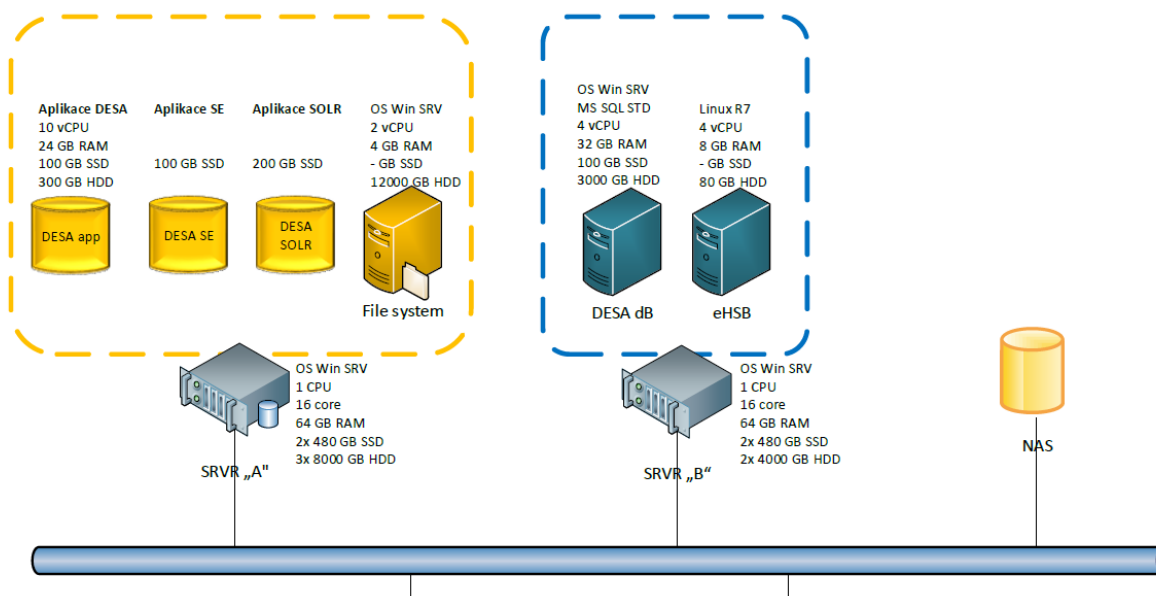
Takto stažené dokumenty budou automaticky smazané po 5 dnech od jejich posledního zobrazení. Doba uložení bude konfigurovatelný parametry, výchozí hodnota bude 5 dnů.

2.3 DODÁVKA NEZBYTNÉ PROVOZNÍ INFRASTRUKTURY PRO DODÁVANÉ SYSTÉMY

3	Dodávka nezbytné provozní infrastruktury pro dodávané systémy.	Dodávka nezbytné provozní infrastruktury pro běh dodávaných IS Chyba! Neznámý název vlastnosti dokumentu., datové konektivity a zajištění bezpečného provozování. Jedná se o servery, disková úložiště apod., které jsou nezbytné pro dodávku a provoz nových částí IS Chyba! Neznámý název vlastnosti dokumentu..	1 soubor
---	--	--	----------

Objednatel dal k dispozici prostředky na provoz EA definované v ZD. Tyto prostředky jsou pro provoz nedostačující, proto Uchazeč nabízí dodání nezbytné infrastruktury. Stávající infrastruktura pro provoz EZD se nemění.

Architektura infrastruktury je dobře patrná z níže uvedeného obrázku.



Obrázek 4: Architektura infrastruktury

Pro provoz EA dodáme 2 kusy server **Dell PowerEdge R550** v následujících konfiguracích:

Server „A“

- 1x CPU Intel Xeon Silver 4314 2.4G, 16C
- 2x 32 GB RDIMM 3200MT/s
- 2x 480GB SSD
- 3x 8000GB HDD
- 1x DualPort 10GbE SFP+
- 1x DualPort 1Gb

Elektronické odesílání dat zdravotnické dokumentace

- 2x HotPlug Power supply 700W

Server „B“

- 1x CPU Intel Xeon Silver 4314 2.4G, 16C
- 2x 32 GB RDIMM 3200MT/s
- 2x 480GB SSD
- 2x 4000GB HDD
- 1x DualPort 10GbE SFP+
- 1x DualPort 1Gb
- 2x HotPlug Power supply 700W

NAS - Synology RS288RP+ (4x HDD 4TB)

2.4 DODÁVKA NEZBYTNÉHO SYSTÉMOVÉHO SW PRO DODÁVANÉ SYSTÉMY

4	Dodávka nezbytného systémového SW pro dodávané systémy.	Dodávka nezbytného systémového SW pro běh dodávaných IS, integrace a zajištění bezpečného provozování. Jedná se o OS, DB, licence, archivace apod., které jsou nezbytné pro dodávku a provoz nových částí IS.	1 soubor
---	---	---	----------

Pro provoz dodávaných systémů dodáme:

- 2x MS SQL Server Standard 2Core SLng LSA OLV 2L NL 3Y Aq Y1 AP
- 2x Windows Server 2022,Standard,16core

3 POSTUP PŘECHODU SYSTÉMŮ A DOPAD DO PROVOZU OBJEDNATELE

V rámci implementace zajistí Dodavatel plnohodnotný provoz dodávaného řešení současně s provozem stávajících systémů, to vše bez jakéhokoliv omezení provozu.

3.1 DODÁVKA ELEKTRONICKÉHO ARCHIVU (EA)-POSTUP IMPLEMENTACE

- Analýza
- Dovývoj požadovaných funkcí
- Implementace
- Napojení poskytnutého rozhraní
- Školení
- Zkušební provoz
- Přechod do rutinního provozu

3.2 ÚPRAVY A NAPOJENÍ EZD NA ELEKTRONICKÝ ARCHIV-POSTUP IMPLEMENTACE

3.2.1 Rozšíření MZD o funkčnosti odběru biometrického podpisu pořízeného Záznamu o výjezdu (ZOV)

Implementace rozšíření MZD o funkčnosti odběru biometrického podpisu zahrnuje následující úpravy EZD:

- **Zalicensování Signotec SignoAPI a Implementace SignoAPI SDK**
Signotec je dodavatel řešení pro odběr biometrického podpisu. Integrace tohoto produktu do EZD umožní pořizování a přikládání odebraného biometrického podpisu k dokumentům, které jsou v EZD vytvářeny. Jedná se především o záznam o výjezdu, ale biometrický podpis je možné připojit i k ostatním dokumentům jako je odmítnutí péče pacientem – negativní reverz či faktura pro samoplátce
- **Úprava GUI MZD / EKP**
V souvislosti s odběrem biometrického podpisu je třeba adekvátně přizpůsobit uživatelské rozhraní MZD a EKP a začlenit komponentu pro odběr podpisu a následně i zobrazení odebraného podpisu v uživatelském rozhraní MZD a EKP
- **Úprava designu tiskových výstupů EZD**
Grafická reprezentace odebraného biometrického podpisu se musí stát součástí tiskových výstupů EZD. Jedná o Záznam o výjezdu, negativní reverz a faktura pro samoplátce
- **Úprava formátu tiskových výstupů (PDF/A)**
Pro umožnění dlouhodobé elektronické archivace biometricky a elektronicky podepsaných dokumentů je nutné, aby jejich výchozí formát byl ve standardu PDF/A. Dojde k úpravám formátu dokumentů, které se stávají součástí záznamu o výjezdu
- **Úprava image MZD určeného pro tablety**
Implementace Signotec SignoApi řešení do MZD si vynucuje nutnost vytvoření nového specializovaného image pro tablety, který v sobě bude obsahovat potřebné binární soubory nutné pro odběr a zpracování biometrického podpisu. Toto rozšíření není možné udělat OTA aktualizací. Je tedy třeba doinstalovat tuto komponentu do standardního image, který je využíván tablety a používán pro přípravu nových tabletů, či tabletů vrácených ze servisního střediska
- **Distribuce nového image na tablety**
V souvislosti s vytvořením nového image je třeba dořešit i jeho distribuci na stávající tablety v provozu ZZS. Tento deployment není možné udělat OTA aktualizací ale instalací závislých komponent na tablety v provozu ZZS.

Elektronické odesílání dat zdravotnické dokumentace

3.2.2 Implementace procesu průběžné aktualizace ZOV a jeho podepisování uživateli, kteří provedli zápis / změnu v dokumentaci. Úpravy budou provedeny v rámci Elektronické karty pacienta (EKP)

Cílem této úpravy je průběžná tvorba kompletního záznamu o výjezdu, který bude obsahovat úvodní záznam o výjezdu včetně všech souvisejících příloh, ale také i další změny, které proběhly v dokumentaci následně po ukončení výjezdu. Mohou to být činnosti související se změnami a úpravami dat v rámci procesů OZP. Každá úprava dat musí být opatřena elektronickým podpisem osoby, která změnu provedla a pro jednoznačnou identifikaci změněných dat i changelogem, který popisuje, jaké datové položky byly změněny, jaká byla jejich původní a nová hodnota. Nově vygenerovaný ZOV bude následně digitálně archivován a vytvoří novou verzi již dříve uloženého ZOV v digitálním archivu organizace. Úpravu je třeba provést v následujících oblastech.

- **Úprava workflow práce s dokumentací při změně dat záznamu o výjezdu**
 - **Automatické generování ZOV při uložení**
Vytvoření nové verze ZOV při uložení změněné dokumentace
 - **Implementace podpisu nově vygenerovaného ZOV uživatele**
Každá změna dokumentace bude vyžadovat autorizaci elektronickým podpisem uživatele.
- **Úprava GUI EKP**
Úprava uživatelského rozhraní aplikace pro možnosti autorizace změn dat elektronickým podpisem uživatele

3.2.3 Úpravy modulu Pojišťovna (POJ) tak, aby případná změna identifikačních údajů pacienta v POJ byla digitálně podepsána a promítnuta do ZOV

V rámci procesů OZP dochází někdy ke ztotožnění neznámého pacienta či k aktualizaci identifikace ošetřeného pacienta. V rámci této úpravy budou do klientské aplikace POJ implementovány následující úpravy

- **Úprava workflow práce s dokumentací při změně dat záznamu o výjezdu**
 - **Automatické generování ZOV při změnách identifikace pacienta na dokladech POJ**
Veškeré změny údajů ZOV, které mohou proběhnout v rámci modulu POJ budou zahrnuty do ZOV
 - **Implementace podpisu nově vygenerovaného ZOV uživatele**
Změny provedené v modulu POJ, které jsou promítány do ZOV budou obdobně jako v EKP autorizovány elektronickým podpisem uživatele, který změny provedl
- **Úprava GUI POJ**
Úprava uživatelského rozhraní aplikace pro možnosti autorizace změn dat elektronickým podpisem uživatele

3.2.4 Úpravy MZD, EKP a POJ, které zabrání podepsání zdravotnické dokumentace certifikátem s blížícím se koncem platnosti

V rámci této úpravy budou implementovány omezení, která zabrání podpisu dokumentace certifikátem s blížícím se koncem platnosti. Předpokládáme nejprve notifikaci uživateli o blížící se expiraci certifikátu, která bude notifikovat uživatele několik dní před vlastním znemožněním provedení elektronického podpisu.

- **Změny business logiky aplikací MZD, EKP a POJ:**
 - Notifikace uživatelům o blížící se expiraci certifikátu (konfigurovatelný interval)
 - Znemožnění uživateli podepsat dokumentaci, pokud dojde v následujícím období k expiraci certifikátu (konfigurovatelný interval)

Elektronické odesílání dat zdravotnické dokumentace

- **Úprava GUI MZD, EKP a POJ**
Úprava uživatelského rozhraní aplikace implementace vizualizace notifikace uživatelům

3.2.5 Vyčlenění úložiště a jeho správy komerčních certifikátů mimo EZD

Autentizační subsystém používaný v rámci EZD umožňuje autentizaci uživatelů prostřednictvím komerčního certifikátu na QSCD prostředku a pinem případně dočasným heslem. Tento typ autentizace bude nově dostupný okolním systémům, proto je třeba pro jeho vyčlenění z EZD provést následující úpravy

- **Implementace nového samostatného modulu identity managementu využívajícího koncept komerčních certifikátů**
Vytvoření nového modulu, který bude řešit identity management na základě komerčních certifikátů
- **Vyjmutí logiky stávajícího úložiště certifikátů a jeho správy ze systému EZD**
tato logika bude implementována do samostatného modulu nezávislého na EZD. Stejně tak bude implementována správa tohoto nového úložiště
- **Integrace s Active Directory organizace**
Organizace bude nadále spravovat přístupy uživatelů k jednotlivých interním systémům (autorizace) prostřednictvím Active directory. V rámci této integrace budou synchronizováni uživatelé a jejich definované přístupy v AD s nově vzniklým modulem identity managementu, který bude autentikovat a autorizovat uživatele

3.2.6 Úpravy integrace EZD na nové úložiště certifikátů

V rámci této úpravy dojde k integraci EZD a nově vytvořeného úložiště pro autentikaci a autorizaci uživatelů k přístupu do EZD.

Budou provedeny následující úpravy

- Implementace integračního rozhraní s úložištěm certifikátů
- Úprava business logiky EKP
- Úprava aplikačního serveru MZD

3.2.7 Integrace EZD s digitálním archivem

Napojení EZD na digitální archiv využije rozhraní, které je aktuálně v rámci EZD podporované. Integrace bude umožňovat následující funkčnosti.

- Vytváření a předávání dokumentů z EZD do EA
- Poskytování dodatečných metadata týkající se předávané dokumentace
- Vytváření nových verzí již dříve předané dokumentace

Předávání dokumentů do archivu bude probíhat asynchronně. Bude vytvořena fronta dokumentů předávaných do archivu, která bude monitorována a v případě problému s uložením dílčích dokumentů dojde k notifikaci správců systému s možností alternativního řešení uložení dokumentu v digitálním archivu.

Pro rychlý náhled dokumentů z digitálního archivu bude vytvořena v EZD dočasné úložiště (cache), kam bude dříve získaný dokument z digitálního archivu uložen tak, aby byl k dispozici pro následně zobrazení v EZD a nebylo nutno dokument opět získávat z archivu.

4 POŽADAVKY NA SOUČINNOST OBJEDNATELE

Pro včasnou a řádnou realizaci předmětu nabídky je nezbytné ze strany zadavatele poskytnout uchazeči aktivní součinnost. Níže je uveden výčet vybraných součinností, které jsou ze strany zadavatele nutné poskytnout pro zdárné provedení předmětu nabídky.

1. Podmínky pro instalaci a zprovoznění dodávaného HW a SW (VPN, prostor v racku, napájení, zajištění zálohování, zapojení do síťové infrastruktury ZZS)
2. Delegování administrátorů a správců – zajistit delegování IT pracovníků zodpovědných za správu HW a síťové infrastruktury
3. Zajištění prostupů mezi jednotlivými servery, tak aby na sebe viděly, byly přístupné pro pracovníky Dodavatele a zároveň měly přístup do internetu a do sítě GOV
4. Zajištění dostatečných oprávnění pro pracovníky Dodavatele pro provedení instalace a konfigurace jednotlivých částí systémů
5. Zajištění vzdáleného přístupu pro pracovníky Dodavatele pro vzdálenou konfiguraci, testování a další operace v systému (platí i pro testovací prostředí)
6. Zajištění přístupu pracovníků Dodavatele do budov, kde budou školení organizována
7. Zajištění smlouvy pro odběr časových razítek a pečeti
8. Součinnost při integraci AD objednatel. Dostupnost komerčních certifikátů pro vyčítání a import do úložiště certifikátů.
9. Zajistit akceptační proceduru na straně Objednatel/Zadavatel pro zajištění akceptace jednotlivých dílčích plnění převzetí jednotlivých dodávek.
10. Plnění operativních úkolů - realizovat a zabezpečovat operativní úkoly stanovené na jednotlivých úrovních řízení (na základě zápisů z jednání, rozhodnutí Řídícího výboru a vyplývající z ostatní projektové dokumentace)
11. Součinnost v rámci Zkušební provozu – delegovat osoby Objednatel (testery) a zajistit organizaci zkušební provozu (kdo, kdy bude prověřovat Systém, jaká funkcionality a jak dlouhou dobu bude prověřována)
12. Součinnost při školení - pro zdárný průběh školení poskytnout potřebnou infrastrukturu: zajištění školící místnosti, počítačového vybavení a projektoru po celou dobu školení. Delegovat osobu zodpovědnou za organizaci školení na straně Objednatel/Zadavatel. Delegovat pracovníky na školení a zajistit jejich rozdělení do skupin.

5 SEZNAM ZKRATEK A POJMŮ

Zkratka/pojem	Význam
365x7x24	Poskytování služeb 365 dní v roce, 24 hodiny denně, 7 dnů v týdnu
AD	Active Directory
CD / CD-ROM / DVD / USB	Datový nosič
ČR	Česká republika
DB	Databáze
DC	Datové centrum
EA	Elektronický archiv organizace
eIDAS	Nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu.
EKP	Elektronická karta pacienta
EZD	Elektronická zdravotnická dokumentace
NSESSS	Národní standard pro elektronické systémy spisové služby
EU	Evropská unie
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob
GUI	Grafické uživatelské rozhraní
HW	Hardware
IaaS	Infrastruktura jako služba
ICT	Informační a komunikační technologie
IS	Informační systém
IS ZOS	Informační systém zdravotnického operačního střediska
IZS	Integrovaný záchranný systém
JWT	JSON web token
KII	Kritická informační infrastruktura
ks	Počet kusů
MS	Microsoft
MZD	Mobilní zadávání dat
OAuth	Otevřený standard pro delegaci přístupů mezi různými systémy
OŘ	Operační řízení

Elektronické odesílání dat zdravotnické dokumentace

Zkratka/pojem	Význam
OS	Operační systém
OTA	Over the air
OZP	Oddělení zdravotních pojišťoven
PD	Projektová dokumentace
PNP	Přednemocniční neodkladná péče
POJ	Modul Pojišťovna – určený pro vykazování poskytnuté zdravotní péče plátcům
QSCD	Qualified Electronic Signature Creation Device
RA	Registrační autorita
RČ	Rodné číslo
SLA	Úroveň a podmínky poskytování služeb technické a technologické podpory
SQL	Strukturovaný dotazovací jazyk pro práci v relačních databázích
SW	Software
VŘ	Výběrové řízení
VS	Veřejná správa
VZ	Veřejná zakázka
ZD	Zadávací dokumentace nebo zdravotnická dokumentace dle kontextu.
ZOS	Zdravotnické operační středisko
ZOV	Záznam o výjezdu ZZS
ZVZ / ZZVZ	Zákon o zadávání veřejných zakázek
ZZ	Zdravotnické zařízení
ZZS	Zdravotnická záchranná služba (ve všeobecném významu)
ZZS KVK	Zdravotnická záchranná Karlovarského kraje