INTEGROVANÝ OPERAČNÍ PROGRAM

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ

MINISTERSTVO PRO MÍSTNÍ ROZVOJ

Příloha č. 1
zadávací dokumentace veřejné zakázky
„Dlouhodobé ukládání digitálních dokumentů“
Technická dokumentace

Veškeré požadavky a ustanovení uvedené v této příloze jsou povinné, musí být obsaženy v nabídce a musí být uchazečem splněny.

Předmětem plnění veřejné zakázky s názvem „Dlouhodobé ukládání digitálních dokumentů“ jsou:

- Dodávka a implementace řešení **dlouhodobého úložiště digitálních dokumentů**
- Dodávka a implementace **HW garantovaného úložiště** do Technologického centra Plzeňského kraje

1 Řešení dlouhodobého ukládání digitálního obsahu

1.1 Obecný popis řešené oblasti

Pod pojmem „dlouhodobé uložení“ je v kontextu této zadávací dokumentace míněno důvěryhodné uložení elektronických (tzv. „digital-born“) nebo digitalizovaných (skenovaných, převedených nebo autorizovaně konvertovaných) dokumentů po dlouhou dobu tedy v řádu desítek let, případně natrvalo. Základním požadavkem je ochrana dokumentu a zajištění čitelnosti jeho obsahu po celou dobu uložení, přičemž ochranou dokumentu a jeho čitelností je myšlena především schopnost důvěryhodně uchovat a zobrazit informační obsah dokumentu po celou dobu uložení, a to nezávisle na použitém formátu či technologii.

Problematika dlouhodobého ukládání digitálního obsahu se v rámci výzvy IOP č. 08 řešila pro tři obecné skupiny obsahu, který pro který je důležité zajistit dlouhodobé bezpečné uložení na úrovni kraje:

1. uzavřené elektronické dokumenty a spisy ze spisové služby po dobu běhu jejich skartační lhůty (krajská digitální spisovna, KDS),
2. digitalizované dokumenty, fotografie a jiný materiál významné kulturní hodnoty (krajský digitální repozitář, KDR),
3. ostatní elektronické („digital-born“) nebo digitalizované soubory bez specifického zařazení (krajské digitální úložiště, KDÚ).

Poptávané řešení se soustřeďuje na první skupinu, tedy na **řešení krajské digitální spisovny (KDS)**, která je pro zadavatele klíčová. Zadavatel nicméně do budoucna předpokládá potřebu zajištění dlouhodobého a důvěryhodného ukládání i pro ostatní skupiny záznamů. Vzhledem k podobnosti uvedených tří typů úložišť a v souladu s doporučením zadavatel požaduje, aby nabídnuté **řešení bylo do budoucna svými technickými parametry schopno zajistit dlouhodobé ukládání všech tří uvedených skupin obsahu**, se všemi specifiky, které se k těmto skupinám obsahu vážou – viz požadavky typizovaného projektového záměru Digitalizace a ukládání z výzvy IOP č. 08 (viz http://www.osf-mvcr.cz/vyzvy/2-1-zavadeni-ict-v-uzemni-verejne-sprave-leden-2010). Vlastní rozšíření nabízeného řešení o funkcionality krajského digitálního repozitáře a krajského digitálního úložiště není v rámci této veřejné zakázky poptáváno, nicméně do budoucna musí být možné toto rozšíření zajistit pouze konfigurací a parametrickými úpravami řešení, bez nutnosti pořizovat nové licence. Hovoří-li se proto dále v této zadávací dokumentaci o „krajské digitální spisovně“ či zkráceně „KDS“, je tím myšleno „poptávané řešení dlouhodobého úložiště, nastavené jako krajská digitální spisovna“; obdobně to platí pro případné použití „KDR“ a „KDÚ“.

Dlouhodobé úložiště bude **komunikovat s dalšími informačními systémy**, provozovanými jednak původci ukládaného obsahu na jedné straně, a zpracovateli obsahu na straně druhé. Řešení proto musí být na tuto komunikaci připraveno. V případě krajské digitální spisovny se jedná především o elektronické spisové služby jednotlivých původců a na Národní digitální archiv. Významná bude také vazba na systém ePUSA, který bude vůči navrhovanému řešení zajišťovat centrální správu uživatelských identit. Zároveň musí řešení variantně umožnit provést všechny kroky životního cyklu uloženého záznamu plně manuálně (pro případ nerealizované nebo nefungující integrace).

Řešení bude sloužit pro kraj, obce v kraji, pro zřizované a zakládané organizace kraje a obcí, do budoucna není vyloučeno případné rozšíření o další subjekty veřejné správy na území kraje (v případě rozšíření funkcionality úložiště o další typy obsahu). Důležitým požadavkem proto je, aby **řešení bylo dostatečně robustní a jeho architektura odpovídala jeho rozsahu a významu** (počet a velikost ukládaných záznamů, velký počet uživatelů a jejich ověření proti centrálnímu systému správy identit kraje, distribuovaná správa, možnost hromadných změn, odpovídající zajištění auditní stopy atd.).

Součástí dodávky budou také **podpůrné nástroje, nutné pro zajištění důležitých funkcí KDS**. Tyto nástroje musí být implementovány jako samostatné moduly tak, aby byly využitelné i odděleně od dlouhodobého úložiště.

Záznamy, určené pro dlouhodobé uložení, je nutné před vlastním uložením většinou zpracovat. Součástí poptávaného řešení proto bude **pracovní úložiště** jako nástroj pro řízení logických úložišť nad souborovým úložištěm se základními vlastnostmi jednoduchého DMS systému, které umožní jednotlivým původcům pracovní uložení a přípravu dat, následně určených k dlouhodobému uložení. Jako součást řešení je požadována dodávka **samostatného nástroje pro konverzi datových formátů do PDF/A** pro zajištění převodu dokumentů do korektního archivního formátu, a dále **samostatný nástroj pro manuální tvorbu SIP balíčků** pro původce, kteří svoji spisovou službu nebudou mít na dlouhodobé úložiště napojenou.

1.2 Obecný popis stávajícího stavu

1.2.1 Původci obsahu a spisové služby v kraji

Největšími původci dokumentů na území kraje jsou Plzeňský kraj (krajský úřad) a Statutární město Plzeň (magistrát a úřady městských částí).

Krajský úřad používá elektronickou spisovou službu AthenA společnosti PilsCom.

Město Plzeň používá elektronickou spisovou službu eSpis společnosti ICZ.

Kraj dále provozuje hostovanou spisovou službu Galatea v rámci řešení VIRTUOS (www.evirtuos.cz), která je k dispozici obcím na území kraje a krajem zřizovaným organizacím. V současné době využívá tuto spisovou službu přes 100 obcí různé velikosti a několik desítek organizací kraje.

Větší města na území kraje používají různé spisové služby, ve velké většině se jedná o známá zavedená řešení elektronické spisové služby.

Malé obce většinou vedou spisovou službu v listinné podobě.

Cílem kraje je vybudovat řešení dlouhodobého ukládání digitálních dokumentů především pro výše uvedené původce a napojit na toto dlouhodobé úložiště jejich stávající elektronické spisové služby. Prioritou je přitom napojení největších původců a nejrozšířenějších el. spisových služeb.

Předpokládaný objem dokumentů, vyžadujících uložení v krajské digitální spisovně, byl ve studii proveditelnosti v roce 2010 odhadnut na 2 – 4 TB ročně, z toho zhruba polovina dokumentů se skartační lhůtou do 2 let.

1.2.2 Stávající řešení digitálních dokumentů

Elektronická spisová služba AthenA na KÚPK obsahuje modul spisovny, ten však v podobě, v jaké je nyní implementován, nesplňuje velkou část požadavků, kladených na řešení KDS v této zadávací dokumentaci. Jeho současná role je především evidenční. Nutnou podmínkou je proto propojení el. spisové služby AthenA s poptávaným řešením.

1.2.3 Správa uživatelských identit

Plzeňský kraj používá pro řízení uživatelských identit ve svých informačních systémech tři hlavní typy Identity Management systémů:

1. **Marbes EOS + MS Active Directory** pro identity uživatelů KÚPK a organizací, pro které odbor informatiky KÚPK zajišťuje svěřenou správu ICT (Správa a údržba silnic Plzeňského kraje, Centrální nákup Plzeňského kraje, Zdravotnický holding) – celkem cca 650 uživatelů.
2. **ePUSA** pro identity uživatelů z řad obcí a uživatelů z příspěvkových organizací kraje a obcí, kteří přistupují k informačním systémům kraje. Do ePUSA automaticky přenášeny identity uživatelů z MS AD. Identity z ePUSA jsou zároveň dále přenášeny do JIP (CzechPOINT) – řádově jde o tisíce uživatelů.
3. **SSO databáze** pro ostatní uživatele především z řad občanů a podnikatelů pro přístup do systémů, ve kterých není nutná garance důvěryhodnosti identity – řádově tisíce uživatelů.

Pro informační systémy, provozované jen pro vnitřní potřebu Krajského úřadu, je využita autentizace s využitím doménového přihlášení (MS AD). U celokrajských řešení, která jsou určena i pro uživatele mimo KÚ a kam bude patřit i poptávané dlouhodobé úložiště, je pro autentizaci uživatelů využívána aplikace **SSO**, která zajišťuje integrované ověření uživatelů a zachování principu jednoho přihlášení (single sign-on) do všech aplikací kraje, ke kterým má uživatel přidělená práva. Jedná se o proprietární řešení Plzeňského kraje pro ověřování uživatelů z více zdrojů, komunikující s aplikacemi prostřednictvím SOAP Web Services protokolem SAML.

1.3 Obecné požadavky na řešení

1.3.1 Kvalita řešení

Pro řešení dlouhodobého úložiště, které má být implementováno, jsou stanoveny následující cíle na požadovanou kvalitu:

- uživatelská přívětivost
- efektivita
- škálovatelnost a modularita
- kompatibilita procesů s modelem OAIS

Uživatelská přívětivost

Uživatelům musí být umožněno vykonávat svou práci maximálně efektivně. Na základě přiměřenosti musí být proto splněny následující požadavky:

- veškerá uživatelská rozhraní musí být v českém jazyce (pouze u rozhraní pro technickou administraci řešení je povolen i anglický jazyk)
- funkcionality systému musí být co nejvíce samovysvětlující, intuitivní, s relevantní nápovědou
- úplná dokumentace (administrátorská, uživatelská) v českém jazyce

Efektivita

Řešení musí uživateli maximálně zjednodušovat a automatizovat především činnosti, které se často opakují. Nesmí po uživateli vyžadovat opakované zadávání stejných dat. Všude tam, kde to přichází v úvahu, musí nabízené řešení nabízet možnost hromadného zpracování (vstup, vydávání, skartace, změna vlastníka nebo oprávnění) k více dokumentům najednou.

Škálovatelnost a modularita

Je požadována bezproblémová škálovatelnost řešení, jak co se týká množství dat (počtu dokumentů i jejich objemu), tak počtu původců (předávajících úřadů) a jejich uživatelů. Škálovatelnost nesmí být omezena

licenčně ani výkonově.

Je vyžadována modulární stavba řešení. Jednotlivé komponenty řešení mohou být odstaveny, upgradovány atd. nezávisle na fungování zbytku. Řešení se svým okolím komunikuje výhradně prostřednictvím definovaného a popsaného aplikačního rozhraní na bázi standardů a otevřených technologií.

OAIS-kompatibilita (Open Archival Information System, ISO Standard 14721:2003)

OAIS koncept je standardem ve formě referenčního modelu pro dynamický, rozšiřitelný archivní informační systém. S ohledem na uchazečem nabízené celkové řešení se očekává, že se uchazeč orientuje v systémovém řešení dle OAIS modelu a jeho řešení bude tento model respektovat.

Požadavek na kompatibilitu s konceptem OAIS se vztahuje pouze na vlastní dlouhodobé úložiště, ne na podpůrné nástroje.

1.4 Požadovaný rozsah realizace

Účelem této části veřejné zakázky je vytvoření a následná údržba dlouhodobého úložiště, implementovaného tak, aby plnilo funkci krajské digitální spisovny, vytvoření a následná údržba pracovního úložiště, implementace podpůrných nástrojů a dále návrh souvisejících procesů, organizačních změn a smluvního modelu užívání.

Uchazeč má v rámci zadaných rámcových podmínek nabídnout softwarovou a systémovou architekturu, která umožňuje zadavateli dlouhodobě zabezpečit stabilní provoz dlouhodobého úložiště s důsledným zaměřením na dlouhodobé a důvěryhodné uchování dat se zajištěním jejich přístupnosti v každém čase a vybudováním archivačních procesů podle OAIS modelu (ISO Standard 14721 :2003). Řešení musí být vysoce škálovatelným, flexibilním modulárně budovaným systémem, stabilním v datové disponibilitě a bezpečnosti.

Předmětem plnění je:

a) dodávka řešení a poskytnutí licence k jeho užívání, včetně pořízení případných dalších licencí, nezbytných pro řádné plnění předmětu veřejné zakázky,
b) implementace řešení,
c) technická podpora a údržba řešení.

Dále jsou jednotlivé body upřesněny.

Dodávka řešení a poskytnutí licence k jeho užívání, včetně pořízení případných dalších licencí …

- Licence dlouhodobého úložiště, zahrnující neomezený počet původců a jejich logických úložišť (předpokládá se v řádu tisíců), neomezený počet uživatelů (předpokládá se v řádu desítek tisíc), neomezený počet uložených objektů a pro neomezenou velikost úložiště (pro potřeby KDS se předpokládá velikost úložiště v řádech desítek TB)
- Licence pracovního úložiště za stejných podmínek jako v předchozím bodě
- Součástí dodávky jsou veškeré nutné licence produktů třetích stran, které neposkytne zadavatel (je upřesněno dále) a které jsou nezbytné pro řádný provoz řešení na zařízení zadavatele v souladu s touto zadávací dokumentací,
- Veškeré licence se poskytnou pro 3 oddělená prostředí (předpokládá se produkční, testovací/vývojové a školící instance) – platí zvlášť pro dlouhodobé úložiště a zvlášť pro samostatný nástroj pracovní úložiště
- V rámci licence dlouhodobého úložiště bude umožněno používat samostatný nástroj pro manuální tvorbu SIP balíčků na libovolném počtu počítačů zadavatele a jeho smluvních partnerů, kteří využívají služeb dlouhodobého úložiště

- Řešení nesmí být v žádném dalším ohledu licenčně nebo technicky omezeno (velikostí úložiště, počtem spisů, dokumentů, typem obsahu, počtem napojených aplikací apod.)
- Zadavatel požaduje hotové, plně funkční řešení (uchazeč prokáže nasnímanou prezentací produktu, přiloženou k nabídce na CD/DVD – viz požadavky na obsah nabídky v Zadávací dokumentaci)

Implementace řešení

Implementace bude zahrnovat následující činnosti:

- Zpracování prováděcího projektu (popíše technické, organizační a procesní potřeby a dopady a stanoví přesný harmonogram implementace) včetně rámcové vstupní analýzy,
- Dodávka testovacího a školícího prostředí, které bude oživeno jako první,
- Dodávka a implementace vlastního řešení,
- Instalace a konfigurace produkčního prostředí,
- Pilotní ověření integračního rozhraní formou realizace plně funkčního napojení těchto řešení elektronických spisových služeb původců na území kraje:
    - spisová služba Krajského úřadu Plzeňského kraje AthenA společnosti PilsCom,
    - Spisová služba GalateA společnosti PilsCom, kterou Plzeňský kraj hostuje pro obce a zřizované organizace jako součást řešení VIRTUOS,
    - Spisová služba eSpis společnosti ICZ zadavatelem vybraného původce,
    - Spisová služba IS RADNICE VERA zadavatelem vybraného původce.

  Zadavatel zajistí součinnost původců při ověřování napojení.
- Provedení školení správců dlouhodobého úložiště v rozsahu minimálně 2 školících dní a klíčových uživatelů (nejvýše 100 osob) v rozsahu 1 školicí den na skupinu (každá skupina 10-15 osob). Školení proběhne v prostorách zadavatele, po dohodě obou stran je možné provést školení i v jiných vhodných vybavených prostorách. Případné náklady na zajištění prostor nese v tom případě dodavatel.
- Zpracování dokumentace finálního vyhotovení včetně detailního popisu všech rozhraní a jejího předání před přechodem na produktivní provoz,
- Zajištění metodické i technické podpory,
- Zpracování kompletní provozní a bezpečnostní dokumentace řešení, včetně popisu pravidelné údržby řešení,
- příprava strategických plánů podle metodiky PLATTER,
- Poskytnutí součinnosti při aktualizaci informační koncepce, vnitřních směrnic úřadu a jiných interních dokumentů, na které má implementace řešení vliv,
- Poskytnutí podkladů a konzultací, potřebných pro provedení interního auditu dlouhodobého úložiště podle DRAMBORA (www.repositoryaudit.eu),
- Zpracování návrhu smlouvy s odběrateli služeb krajské digitální spisovny včetně provozních podmínek a SLA.

Technická podpora a údržba řešení

Na údržbu a podporu řešení bude s vybraným uchazečem uzavřena smlouva o technické podpoře na dobu neurčitou. Vybraný uchazeč bude v rámci této smlouvy povinen zajistit, že veškeré funkce řešení, popsané v této zadávací dokumentaci a dodané spolu s dílem a dokumentací díla budou odpovídat obecně platným právním předpisům ČR a platným standardům, které musí podle zákona nebo podle této zadávací dokumentace dodržovat.

Rozsah podpory a údržby je podrobněji specifikován dále v tomto dokumentu.

1.5 Funkční požadavky řešení

1.5.1 Dlouhodobé úložiště

Základní požadavky na vybudování dlouhodobého úložiště jsou následující

- vybudování dlouhodobého úložiště jako součásti TC Kraje v souladu s požadavky kladenými na důvěryhodnou instituci a stanovení a plnění podmínek udržitelnosti provozu v současnosti i budoucnosti.
- nastavení dlouhodobého úložiště pro potřeby krajské digitální spisovny (KDS), tedy systémového řešení dlouhodobého a důvěryhodného uchovávání a zpřístupňování úředních elektronických dokumentů vytvořených určenými původci
- všechny vyřízené spisy a jiné dokumenty určeného původce jsou po dobu trvání skartační lhůty uloženy ve spisovně. Po dobu uložení elektronického dokumentu musí být v souladu se zákonem o archivnictví a spisové službě a jeho prováděcími předpisy zajištěna ochrana uložených informací před ztrátou, důvěryhodnost uložených informací (nezměněnost a prokazatelnost vzniku v uvedeném čase) a čitelnost uložených informací v budoucnosti. Tedy uložený dokument má mít tyto charakteristiky (dle standardu ISO 15489 Records Management):
    - autenticity (authenticity) – pro dokument může být prokázáno, že je tím o čem se domníváme, že je (dokument neztratil smysl, význam), že byl vytvořen nebo odeslán danou osobou a že byl vytvořen nebo odeslán v daný čas,
    - hodnověrnosti (reliability) – na dokument se můžeme spolehnout, neboť jeho obsah je důvěryhodný, jelikož úplně a přesně vyjadřuje transakce, aktivity nebo fakta, která popisuje,
    - integrity (integrity) – dokument je kompletní a nezměněný od okamžiku vstupu do KDS,
    - použitelnosti (usability) – dokument může být dohledán, získán, prezentován a interpretován (je čitelný).
- přebírání, zpracování, uložení a zpřístupňování úředních dokumentů a jejich metadat ze systémů elektronických spisových služeb a dalších AIS smluvních původců na území Kraje
- vlastníkem dokumentů uložených v dlouhodobém úložišti zůstává příslušný původce. Kraj je správcem a provozovatelem dlouhodobého úložiště a s původci uzavírá smlouvy o uložení dokumentů (službě)
- možnost provádění skartačního řízení a to tak, že každý původce provádí vzdáleně skartační řízení nad svými dokumenty, které má v dlouhodobém úložišti uloženy. Skartační řízení (skartační proces) musí být prováděno podle platné legislativy a za podpory legislativou stanovených orgánů.

Řešení dlouhodobého úložiště jako systém na dlouhodobé a důvěryhodné uchovávání elektronických dokumentů musí odpovídat standardu OAIS (Open Archival Information System – norma ISO 14721:2003). 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.

Pro zabezpečení důvěryhodnosti a provozu dlouhodobého úložiště je nutné vypracovat a udržovat dlouhodobý strategický plán cílů. Tyto cíle, resp. plány (např. technologický, řízení lidských zdrojů, financování, krizový plán apod.) by měly vymezit všechna důležitá hlediska budování a provozu důvěryhodného úložiště a tím umožňují předem definovat cíle, postupy – aktivity a role, vedoucí k jejich naplnění.

Řešení dlouhodobého úložiště musí být dodáno tak, aby mohlo být pravidelně podrobováno internímu auditu a externí kontrole dle předem stanovené metodiky a vydefinovaných nástrojů.

Řešení KDS musí být v souladu s následujícími standardy:

- Zákon č. 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů
- Vyhláška č. 259/2012 Sb. o podrobnostech výkonu spisové služby
- Norma ISO 15489 – Records Management
- Národní standard pro elektronické systémy spisové služby (NSESSS)
- Norma ISO 14721:2003 – standard OAIS
- Dokumenty, struktura a metadata ukládána v balíčcích AIP dle platné legislativy a se strukturou dle otevřeného obecně uznávaného standardu (zadavatel předpokládá využití standardu METS – viz http://www.loc.gov/standards/mets)
- Podpora metadat ve formátech METS, NSESSS, PREMIS (http://www.loc.gov/standards/premis), případně i další formáty podle potřeb zákazníka, včetně souladu metadat s platnou legislativou
- Možnost aplikace časových razítek a elektronických značek, a to i více autorit na kompletní balíčky AIP nebo dávky balíčků, včetně možnosti opakované aplikace, s použitím standardu umožňujícího budoucí ověření platnosti razítka, podle zákona č. 227/2000 Sb. o elektronickém podpisu
- Vyhovuje provozu spisovny/archivu podle strategického plánu cílů směrnice PLATTER (viz např. http://www.ndk.cz/platter-cz či http://www.digitalpreservationeurope.eu/platter/)

KDS musí být otevřený systém, který bude poskytovat služby vůči okolním subjektům a dalším systémům a to zejména v oblastech:

1.5.1.1 Příjem dokumentů do spisovny

Tato funkční část řeší příjem elektronických dokumentů od původců ve stanoveném formátu a struktuře.

Komponenty této části mají za úkol přebírat heterogenní data od různých původců (úředních systémů), připravit je tak, aby byla schopna archivace a tato data předávat do části řešení Správa spisovny, administrace a bezpečné ukládání.

Dokumenty by měly být do spisovny předávány zejména elektronickými systémy spisových služeb a agendovými informačními systémy - pracujícími jako ERMS systémy s povinnými funkcemi uvedenými v Národním standardu, případně dalšími aplikacemi produkujícími dokumenty.

Řešení umožní manuální přípravu a příjem SIP balíčku s pomocí samostatného nástroje – viz dále.

Oblast **Příjmu** musí být v souladu s následujícími požadavky:

- Kontrola formální struktury SIP balíčků a kontrola na škodlivý obsah (antivirová kontrola) s použitím karanténní zóny
- Kontrola povinných položek popisných metadat a přípustných formátů souboru
- Kontrola vazeb mezi dokumenty a číselníkových položek
- Zjištění a evidence technických metadat
- Kontrola zda balíček obsahuje platné autentifikační prvky (třeba elektronický podpis a časové razítko).
- Generování balíčků AIP a jejich řízené ukládání, tj. konzistentní uložení metadat a obsahu archivních balíčků současně do archivního úložiště a systému správy dat podle OAIS

Předpokládá se, že v rámci implementace funkcionality krajské digitální spisovny budou dokumenty v SIP balíčcích typicky dodány v požadovaných výstupních datových formátech (podle §23 vyhlášky č. 259/2012 Sb.), tj. buď v těchto formátech již vznikly, nebo do nich byly převedeny původcem před příjmem balíčku. Řešení

však musí být schopno v rámci příjmu akceptovat i SIP balíčky, které budou kromě výstupních datových formátů obsahovat originální zdrojové formáty dokumentů.

Dlouhodobé úložiště samo o sobě musí obecně akceptovat balíčky s obsahem v jakémkoli formátu, který určí správce daného typu úložiště.

1.5.1.2 Správa spisovny, administrace a bezpečné ukládání

Cílem této funkční části je naplnění požadavků na dlouhodobost a důvěryhodnost uchování a zajištění transparentnosti vůči okolním subjektům.

Řešení archivace má za úkol převzít od komponent Příjem dokumentů do spisovny vstupní připravené archivní jednotky, předávat je do archivního úložiště, konfigurovatelnou část metadat spravovat v přístupové databázi (myslí se tím Data Management) a řídit systém ukládání. Vycházejíce z funkčních požadavků na SW řešení musí být nabídka vyhotovena z hlediska HW (server, datové úložiště), který je v TCK. HW se může případně rozšířit bez kapacitního omezení po celou dobu provozování dlouhodobého úložiště.

Pro každého původce je v systému KDS vytvořen logicky oddělený prostor (logický segment, logické úložiště) s vlastním řízením přístupových práv, kde je uložen kompletní jím předaný obsah. Administrace i přístup k obsahu balíčků spisovny je pro každého původce striktně oddělený, přičemž každý původce by měl mít definovaného vlastního správce, který administruje příjem balíčků, skartační řízení i další operace a spravuje číselníky i uživatele pro daného původce. Správci mohou správu svého obsahu dobrovolně delegovat na další uživatele mimo organizaci.

V rámci logického úložiště se mohou evidovat balíčky pro jednotlivé organizační jednotky původce.

Také použité číselníky (např. spisový a skartační plán) musí být definovány a spravovány pro každého původce odděleně.

Administrátor systému KDS zajišťuje technicky provoz pro všechny původce, ale nespravuje uložený obsah.

Dokument musí být považován za prověřený už v okamžiku, kdy vstupuje do spisovny. Spisovna nezaručuje autenticitu v tom smyslu, že by ověřovala samotný dokument, ale zaručuje nezměnitelnost dokumentů uložených v balíčcích od okamžiku předání do systému KDS a dlouhodobě umožňuje autenticitu uložených balíčků prokázat.

Autenticitu balíčků uložených v KDS a jejich nezměnitelnost je možné zajistit softwarovými i hardwarovými prostředky, třeba i externím autentifikačním způsobem prokazujícím daná data v čase a také příslušnými organizačními opatřeními.

Mimo všech prostředků ochrany balíčků proti neoprávněné modifikaci a smazání je nutné na uložené balíčky aplikovat i časová razítka. Ta umožní dlouhodobě prokázat autenticitu uložených balíčků a jejich existenci v čase bez ohledu na použitou technologii, i v případě budoucí změny technologií a přesunu dat na jiná média. Pravidelná aplikace časových razítek na kompletní obsah balíčků zajistí nezměnitelnost obsahu uloženého v libovolných, spisovnou akceptovaných, formátech. Zvolené technologie a formát časových razítek by měly odpovídat účelům dlouhodobé archivace, včetně korektního dodržení standardů v této oblasti (je vyžadován soulad se standardem XML Advanced Electronic Signatures).

Řešení musí umožňovat takovou variantu metody ochrany balíčků, která nevyžaduje aplikaci časového razítka na jeden každý balíček, ale zajistí důvěryhodnost jejich obsahu hromadě, jiným bezpečným algoritmem, který umožní hromadnou aplikaci časového razítka na společný hash, spočítaný na základě bezpečného, běžně používaného algoritmu.

Řešení musí umožňovat aplikaci časových razítek několika (minimálně tří) nezávislých autorit (TSA).

Zejména proti změnám obsahu zapříčiněným technickými problémy a degradací použitých médií aplikují systém KDS i periodické ověřování kontrolních součtů nad všemi uloženými balíčky AIP. Určité funkce bezpečnostního a

autentizačního charakteru je vhodné ponechat také na technologických funkcích úložiště, které na daném hardwarovém zařízení asi nejlépe provedou potřebné kroky a opatření.

Veškeré operace s balíčky – tzn. vstupní operace, výdej balíčků, operace ve skartačním řízení, operace pro zajištění autenticity balíčků musí být zaznamenány. Tyto záznamy budou obsahovat zejména čas provedení, popis operace a příslušného uživatele.

Tyto záznamy budou dlouhodobě uloženy stejným způsobem a se stejnou péčí jako primární obsah v archivním úložišti systému KDS. Jedině tak je možné zajistit dlouhodobost a důvěryhodnost uložení a jejich autenticitu.

Řešení musí být v souladu s následujícími požadavky pro **Bezpečné uložení:**

- Software KDS bude pro ukládání balíčků AIP umožňovat použití technologie typu NAS/CAS/diskové úložiště, případně i v kombinaci
- Součástí této veřejné zakázky je dodávka a implementace HW garantovaného úložiště. Řešení dlouhodobého úložiště bude pro úložiště typu CAS primárně využívat toto garantované úložiště, bude však umožňovat integraci na jiné typy bezpečných úložišť
- Možnost ukládání a kontroly integrity do více fyzických diskových úložišť přímo dlouhodobým úložištěm
- Periodické vytváření časových razítek a jejich zabezpečené uložení a evidence.
- Periodická kontrola konzistence uložených dat na aplikační úrovni.
- Administrátorem odsouhlasená automatická náhrada AIP balíčků, které byly zjištěny jako poškozené, z identických nepoškozených kopií na úrovni práce s úložištěm
- Neplatné SIP balíčky budou odmítnuty a původci vrácen chybový kód. Odmítnutí bude logováno.
- Dokumenty budou uloženy ve formě archivních balíčků AIP v archivním formátu, obsahujících obsah dokumentů společně s metadaty
- Jednotlivý AIP se nesmí děleně ukládat na více datových nosičích a to ani při nedostatečném množství místa na jednom médiu
- Řešení musí pracovat s úložišti tak, aby bylo možné je rozdílově zálohovat, a to i po delší době používání – uchazeč v nabídce popíše způsob práce s úložištěm, součástí plnění bude zpracování plánu zálohování
- Uložené balíčky AIP musí být dostupné i prostřednictvím standardního rozhraní úložiště i bez použití specifického SW pro účely migrace a obnovy.
- Autorizace - omezení přístupů na základě klasifikace dokumentu, původce, uživatelských skupin a rolí uživatelů. Modul povolí přístup ke čtení obsahu nebo metadat podle rolí přihlášeného uživatele a oprávnění příslušného balíčku.
- Provádění transakčních záznamů o přístupu k jednotlivým uloženým balíčkům – veškerý přístup k balíčkům bude důsledně logován
- Evidence veškerých přístupů k uloženým dokumentům v podobě auditních záznamů
- Auditní záznamy o veškeré manipulaci s informačními balíčky musí být ukládané do bezpečného úložiště podle volby zadavatele
- podpora syslog nebo SNMP traps

Systém KDS musí plnit veškeré funkce spisovny, tedy musí podporovat i skartační řízení včetně všech náležitostí ve smyslu NSESSS. Pro účely práce s analogovými a hybridními dokumenty bude podporována evidence a zařazování do fyzických ukládacích jednotek a spisoven, evidence zápůjček a nahlížení do spisu, tvorbu tiskových sestav založených nad ukládacími jednotkami potřebných pro schvalování skartačních návrhů, tedy věci obvyklé ve spisovnách papírových dokumentů/spisů.

Oblast **Správa spisovny** musí být v souladu s následujícími požadavky:

- Import, evidence a správa číselníků, zejména tyto číselníky - původci, spisový a a skartační plán, povolené souborové formáty, kategorizace dokumentů podle kritérií přístupnosti, požadavků na zachování důvěryhodnosti,
- Přehled přijímaných a uložených balíčků
- Kontrola konzistence uložených balíčků AIP nezávisle na vlastnostech použitého archivního úložiště
- Podpora skartačního řízení s přístupem schvalujícího archiváře
- Možnost migrace uložených formátů souborů
- Možnost exportu a předání do Národního digitálního archivu
- Oddělená správa a administrace technologie systému KDS (kterou provádí provozovatel) od správy a administrace datového obsahu (kterou provádí správci pověření jednotlivými původci)
- KDS je logicky rozděleno na jednotlivé logické segmenty (spisovny) pro jednotlivé původce
- KDS, resp. jeho modul archivního úložiště musí mít možnost nastavení ukládání balíčků AIP od jednotlivých původců do logicky, případně i fyzicky, oddělených částí úložiště.

Z pohledu **Administrace** musí být řešení v souladu s následujícími požadavky:

- Správa jednotlivých původců a jejich logických segmentů (v případě KDS spisoven jednotlivých původců)
- Skupiny uživatelů, uživatelé a role a oprávnění, navázané na Identity Management systémy kraje – přebírání uživatelských účtů, základních rolí oprávnění (minimálně na úrovni „přístup ano/ne“) a zařazení uživatelů do organizací ze systému ePUSA
- Ověřování uživatelů prostřednictvím řešení SSO Plzeňského kraje
- Historické a budoucí verze číselníků
- Centrální administrace a přístup pro správce původců
- Řízení procesu příjmu, přehled o stavu příjmu balíčků SIP, podpora řešení případných problémů se strukturou a obsahem balíčků při příjmu.
- Řízení procesů migrace, spouštění migrace souborových formátů v uložených balíčcích a přehled o provedených migracích. Samotné nástroje pro migraci formátů nejsou předmětem plnění, řešení však musí být připraveno na tento proces a na budoucí rozšíření o tyto nástroje.
- Skartační řízení, příprava návrhu a jeho schvalování, provedení skartace, případně exportu do jiného archivu v definovaném formátu (typicky NDA, do budoucna např. NDK).
- Správa funkcionality kontroly konzistence, včetně zajištění dokumentace tohoto procesu.
- Správa číselníků, zajišťuje pro administrátory původce aktualizaci číselníků používaných v rámci vstupní kontroly a vyhledávání.
- Důvěryhodné ukládání transakčních záznamů pro účely auditu, zaznamenávání veškerých provedených operací nad uloženými balíčky (příjem, kontrola, transformace, ukládání, čtení).
- Přístup k transakčním záznamům, zobrazení transakčních záznamů pro účely auditu.

1.5.1.3 Vyřazování dokumentů ze spisovny

V rámci této funkční části je řešena příprava návrhu a jeho schvalování, provedení skartace, případně exportu do Národního digitálního archivu (případně do jiného dlouhodobého úložiště) v definovaném formátu.

Na základě definovaných skartačních režimů systém navrhne příslušné operace v rámci skartačního řízení a umožní posouzení a změny ve skartačním návrhu oprávněným uživatelům. Přitom musí být zajištěna podpora i pro analogové dokumenty a hybridní dokumenty.

Po schválení skartačního návrhu systém jednotlivě provede nad digitálně uloženými dokumenty příslušné operace – tedy smazání obsahu dokumentů nebo export do NDA. V případě, že NDA neposkytne v době plnění této zakázky popsané rozhraní na NDA, bude realizace funkcionality předávání digitálních archiválií implementována až po zpřístupnění tohoto rozhraní v budoucnu, a to zdarma jako součást placené podpory.

Dokumenty jsou ve faktickém i právním vlastnictví původce a ten je za ně zodpovědný. Skartační řízení tedy prostřednictvím funkcí KDS provádí určený pracovník původce.

Do NDA jsou balíčky předávány po ukončení skartačního řízení ve formátu určeném v NSESSS. Tyto balíčky jsou vytvořeny z balíčků AIP uložených ve spisovně, přičemž jsou předávána pouze metadata požadovaná Národním archivem a příslušný digitální obsah. Konkrétní rozhraní a pravidla pro předávání nejsou v současné době stanovena.

Systém KDS by měl umožnit i následnou dlouhodobou archivaci pro potřeby původce u vybraných skupin digitálních dokumentů, které byly již předány do NDA nebo skartovány. Na rozdíl od analogových dokumentů je v případě digitálních dokumentů z principu možné uchovávat více instancí originálního dokumentu.

Pro podporu práce s digitálními i analogovými dokumenty musí KDS minimálně zajistit:

- příjem do spisovny (ve formě SIP balíčku obsahujícím pouze metadata o dokumentu/spisu)
- evidenci ve spisovně, minimálně v rozsahu:
    - základní metadata (zejména pro vyhledávání ve spisovně) + všechna metadata uložená spolu s dokumentem/spisem předaná do spisovny (dle vyhlášky č. 259/2012 Sb., metadata dle národního standardu)
    - přiřazení k věcné skupině podle spisového plánu
    - přirazení skartačního režimu (skartační znak, skartační lhůta)
    - místo uložení (slovní nebo číselníkové určení místa fyzického uložení)
    - další povinná či volitelná metadata podle specifikace zadavatele
- skartační řízení
    - informování o uplynutí skartačních lhůt
    - zařazení do skartačního návrhu
    - sestavení seznamu balíčků dokumentů/spisů k vyřazení (spolu s digitálními) podle skartačních operací S nebo A, vyřešení operací V
    - záznam o provedení skartačního řízení

Funkce skartačního řízení

- zobrazení všech dokumentů, kterým uplynula skartační lhůta,
- zařazení do skartačního řízení,
- kontrola konfliktů (hledání a řešení konfliktu skartačních režimů, vyřazování částí spisů nebo souvisejících spisů/dokumentů)
- sestavení a úprava skartačního návrhu
- kontrola a schválení skartačního návrhu
- sestavení seznamu balíčků dokumentů/spisů k vyřazení (spolu s digitálními) podle skartačních operací S nebo A
- na základě schválení skartačního návrhu provedení vyřazení:
    - přenos do národního archivu – export do požadované struktury digitálního archivu, po potvrzeném přenosu může nastat zničení dokumentů a některých metadat.
    - skartace - zničení dokumentů a některých metadat, ponechání základních údajů o dokumentu a údajů o skartaci.

- procesní řešení skartačního řízení části balíčku (možnost umístění více spisů s různými skartačními značkami v jednom AIP balíčku)
- záznam o provedení skartačního řízení

1.5.1.4 Přístup k obsahu spisovny

Základním cílem této funkční části je zpřístupnění uložených elektronických dokumentů pouze oprávněným uživatelům.

Přístup k datům v KDS by měl být možný prostřednictvím uživatelského rozhraní, které bude umožňovat vyhledávání podle evidovaných metadat a výdej obsahu ve formě balíčků DIP (Dissemination Information Package). Také by mělo být umožněno asistované znázornění dokumentu.

Vedle uživatelského rozhraní by měl být umožněn přístup i prostřednictvím popsaného aplikačního rozhraní pro zpřístupnění externími aplikacemi, například systémy ESSL, nebo portálovými systémy.

Každý přístup k uloženému balíčku oprávněnými uživateli původce i v případě nahlížení do spisu bude zaznamenán a trvale evidován. Přístup k dokumentům uloženým v KDS musí být omezen pouze na oprávněné uživatele na základě klasifikace dokumentu a uživatelské role.

U vybraných typů dokumentů může být vyžadováno i schválení zpřístupnění balíčku oprávněným uživatelem.

Přístup k obsahu spisovny musí být v souladu s následujícími požadavky“

- Možnost použití případného stávajícího systému DMS/ECM nebo stávajícího portálu pro přístup k dokumentům nezávisle na SW KDS.
- Programové rozhraní API pro přístup k dokumentům
- Vyhledání uložených balíčků na základě zvolených metadat.
- Možnost vyžádání a schvalování výdeje balíčků DIP, evidence výdeje balíčků DIP
- Postoupení uložených dokumentů ve formě DIP, systém umožní výběr dokumentů a jejich zaslání oprávněnému uživateli ve standardizované podobě.
- Zabezpečení přístupu a autentizace uživatelů. Zajištění přístupu uživatelů k uloženým metadatům a dokumentům.

1.5.2 Podpůrné nástroje

Dále jsou uvedeny nástroje, jejichž dodání je v rámci plnění požadováno. Nástroje musí být možné použít samostatně, odděleně od zbytku řešení. Musí být však se zbytkem řešení propojené v míře, nezbytné pro zajištění funkcionality celého řešení.

1.5.2.1 Pracovní úložiště

Součástí poptávaného řešení bude zřízení pracovního úložiště, které umožní jednotlivým původcům pracovní uložení a přípravu dat, následně určených k dlouhodobému uložení. Pracovní úložiště bude koncipováno tak, aby bylo případně využitelné i samostatně pro krátkodobé či střednědobé bezpečné uložení nestrukturovaných záznamů, bez vazby na dlouhodobé úložiště.

U pracovního úložiště se nepředpokládá fungování dle principů OAIS.

Funkční požadavky

Pracovní úložiště bude sloužit k přímému, rychlému ukládání dat vybraných kategorií po dohodě s jejich původci. Data budou ukládána přímo ve formě souborů. Soubory nebudou povinně obsahovat popisná

metadata v jednotně stanoveném formátu. Pracovní úložiště musí zajistit spolehlivé uložení, zálohování a případnou aplikaci základních retenčních politik.

V pracovním úložišti musí být možné jednoduchým způsobem zakládat a spravovat oddělená logická úložiště pro jednotlivé původce s vlastním řízením přístupových práv.

Není nutné, aby pracovní úložiště nabízelo funkcionalitu nad rámec běžného souborového systému (NFS, CIFS, FTP aj.) pouze se základním řízením uživatelských oprávnění na úrovni každého logického úložiště.

Neomezená licence

Je požadována neomezená licence pro jednu instalaci pracovního úložiště, umožňující neomezený počet původců (logických úložišť), neomezený počet uložených objektů, neomezený počet uživatelů s plným přístupem a bez licenčního omezení kapacity celého úložiště

Implementace

Prvním krokem implementace bude zpracování prováděcího projektu v nezbytně nutném rozsahu. Schválený prováděcí projekt bude sloužit jako zadání pro vlastní implementaci, popíše technické, organizační a procesní potřeby a dopady a stanoví přesný harmonogram implementace.

Součástí implementace bude dodávka testovacího a školicího prostředí, které bude oživeno jako první.

Následně proběhne implementace vlastního řešení do prostředí Technologického centra Plzeňského kraje a jeho postupné oživení.

Po celou dobu platnosti smlouvy o technické podpoře zajistí dodavatel technickou podporu nástroje.

Součástí implementace bude školení správy pracovního úložiště pro administrátory (dvě skupiny, každá do počtu 15 osob v rozsahu 1 den).

Součástí implementace je zpracování kompletní provozní a bezpečnostní dokumentace, včetně popisu pravidelné údržby řešení, havarijních plánů a plánu obnovy.

Zhotovitel poskytne součinnost při aktualizaci informační koncepce, vnitřních směrnic úřadu a jiných interních dokumentů, na které má implementace řešení vliv.

Před přechodem na produktivní provoz bude předána dokumentace finálního vyhotovení včetně podrobného popisu všech rozhraní v takové úrovni detailu, která umožní případnou budoucí integraci řešení bez nutné součinnost dodavatele.

Zhotovitel zpracuje v rámci této části plnění návrh smlouvy s odběrateli služeb KDÚ včetně provozních podmínek a SLA.

1.5.2.2 Samostatný nástroj pro konverzi datových formátů do PDF/A

Je požadován samostatný nástroj, běžící na serveru zadavatele, který bude sloužit pro automatizaci tvorby a skládání PDF souborů. Nástroj bude přes aplikační rozhraní (API) nabízet jiným informačním systémům službu konverze souborů z formátů jejich původních aplikací resp. z uznávaných standardních formátů do korektního formátu řady PDF/A. Nezbytnou podmínkou je plně korektní výstupní formát PDF/A v souladu se standardem ISO.

Nástroj bude poskytovat služby dlouhodobému úložišti a do budoucna potenciálně i dalším informačním systémům zadavatele.

Nástroj musí být schopen převést minimálně tyto vstupní formáty dokumentů:

- Microsoft Office 2000+, 2007+ (DOC, XLS, PPT,WPD, MPP, RTF, TXT, Microsoft Office Open XML formáty)
- Microsoft Visio 2003, 2007 (VSD)
- Microsoft Project 2003, 2007 (MPP)
- OpenOffice 2.0+ (ODT, ODS, DOP, ODG, ODF)
- Webové soubory (HTML)
- Obrazové formáty (JPEG, GIF, BMP, TIFF, PNG)
- PDF 1.3 až 1.7, PDF/A, PDF/X – včetně skenovaných bez textové složky

Nástroj musí do výstupního souboru automaticky vkládat potřebné typy písma a být schopen získat strukturované informace (např. značky přístupnosti) z původních aplikací, sloužící k vytváření PDF/A-1a souborů.

Proces konverze musí využívat technologii optického rozpoznávání znaků (OCR) v případě tak, aby výsledný PDF/A dokument zachoval stejný vzhled jako originál, ale na rozdíl od něj obsahoval text (označované jako „text over image PDF" nebo „searchable PDF"). Použitá OCR funkcionalita musí být schopna bez problémů zpracovat české texty s diakritikou.

Dodaná licence musí plně pokrývat prostředí, na kterém bude nástroj provozován (předpokládá se jeden vyhrazený virtuální server v prostředí, popsaném dále v tomto dokumentu). Zadavatel požaduje licenci bez omezení počtu konvertovaných dokumentů a bez omezení uživatelů. Do podpory dodávaného řešení uchazeč zahrne i právo na podporu a na nové verze tohoto nástroje.

Součástí implementace bude školení správy nástroje pro administrátory (jedna skupina cca 5 osob v rozsahu 1 den).

1.5.2.3 Tvorba SIP balíčků

Pro případ, kdy bude do dlouhodobého úložiště nutné uložit obsah, který není předáván automaticky prostřednictvím vstupního rozhraní z jiné integrované aplikace, bude dodán nástroj, který zajistí manuální vytváření vstupních SIP balíčků.

Tento nástroj vytvoří vstupní balíček SIP, zahrne do něj připravené soubory (komponenty) a umožní zadat popisná metadata. Přitom budou využívány číselníky evidované v dlouhodobém úložišti, což usnadní přípravu validních metadat.

Stejně jako v případě předávání do dlouhodobého úložiště prostřednictvím aplikačního rozhraní budou balíčky při vstupu automaticky kontrolovány.

Licenčně nebude nástroj jakkoli omezen, bude jej moci neomezeně využívat jakýkoli subjekt, který užívá dlouhodobé úložiště nebo toto užívání zvažuje, a to bezplatně. Podpora dlouhodobého úložiště se vztahuje i na tento nástroj.

Součástí implementace bude školení správy nástroje pro administrátory (jedna skupina cca 5 osob v rozsahu 0,5 dne).

1.6 Technická specifikace řešení

1.6.1 Dlouhodobé úložiště

Dlouhodobé úložiště, založené na principech OAIS, přistupuje k ukládaným dokumentům a spisům jako k balíčkům, obsahujícím předmětná data a současně jejich metadata za účelem dlouhodobého a důvěryhodného uložení. Podle fáze jejich životního cyklu se jedná o vstupní (SIP), archivní (AIP) a výstupní (DIP) balíčky.

Rozhraní pro přístup k těmto systémům je specificky navrženo pro příjem a výdej balíčků v příslušném formátu definovaném na základě standardů. Vzhledem k zajištění bezpečnosti a konzistence uložených dat probíhá příjem dat do úložiště asynchronně v rámci procesu, který se skládá z několika kontrolních a transformačních procedur.

1.6.1.1 Architektura řešení

Poptávané řešení dlouhodobého úložiště musí být postavené jako minimálně třívrstvé, s jasně oddělenou částí ukládání dat od aplikační logiky.

Pro provozní strukturovaná data bude využita relační databáze (RDBMS). Zadavatel nabízí k dispozici využití MS SQL Server 2012 Enterprise Edition a předpokládá jeho využití. V případě, že řešení uchazeče bude vyžadovat RDBMS jiného výrobce, je uchazeč do nabídky povinen zahrnout licence tohoto RDBMS ve srovnatelné edici a rozsahu, včetně podpory a maintenance a zajistit proškolení 3 pracovníků zadavatele v rozsahu 2 dní.

Vlastní ukládaný obsah (AIP balíčky) bude uložen ve vyhrazeném úložišti NAS (TIER2 nebo TIER3 Technologického centra kraje) nebo CAS, pro každé logické úložiště v oddělené struktuře. Rozhodnutí o použití úložiště NAS/CAS bude nastavitelné na úrovni každého logického úložiště minimálně v těchto variantách:

- Využití pouze úložiště NAS pro veškerý obsah
- Využití pouze úložiště CAS
- Využití úložiště NAS pro AIP balíčky a úložiště CAS pro vybrané bezpečnostní informace (hashe, časová razítka, auditní logy)

Veškerá integrační rozhraní a realizované vazby budou detailně popsány. Zadavatel požaduje, aby integrační vazby byly realizovány protokolem WS/SOAP, pokud tomu nebudou bránit vážné důvody mimo vliv dodavatele.

Součástí dodávky bude detailní popis struktury ukládaných dat tak, aby bylo možné v případě nouze porozumět datovému obsahu a přenést jej do jiného typu úložiště i v případě, kdy aplikační část řešení nebude funkční.

Řešení musí umožnit bezpečnostní klasifikaci dat a řízení bezpečnosti na základě této klasifikace.

U veškerých změn v ukládaném obsahu musí být možné držet historii.

Součástí dodávky budou havarijní plány, popisující minimálně procesy:

- Zálohy
- Obnovy ze zálohy
- Postupu v případě havárie
- Migrace úložiště na jiný hardware (při zachování stávajícího typu úložiště)
- Nouzový hromadný export dat pro přenos do jiného typu úložiště

1.6.1.2 Komponenty dlouhodobého úložiště

Systém digitální spisovny, implementovaný nad dlouhodobým úložištěm, se musí skládat z těchto softwarových komponent, které musí společně splňovat výše uvedené funkční požadavky:

Vstupní modul

- **Příjem dat**
  Zajišťuje komunikaci s původcem, autentizaci, autorizaci a uložení přijatých balíčků SIP do pracovního úložiště.
- **Kontrola kvality vstupních dat (kontrola datové struktury, kontrola na obsah škodlivého kódu)**
  Kontroluje formální strukturu balíčků a přítomnost virů a jiného škodlivého obsahu balíčků. V rámci tohoto modulu je zřízena i tzv. karanténní zóna pro zajištění spolehlivosti kontrol.
- **Řízení příjmu**
  Kontrola popisných a technických metadat, kontrola přípustnosti souborových formátů a jejich vnitřní validity, kontrola struktury balíčku SIP a vzájemného provázání balíčků.
- **Generování balíčků AIP**
  Automatické doplnění zejména technických metadat, konverze formátů metadat, možnost manuálního doplnění metadat, vstupní migrace formátů včetně generování náhledů pro prezentaci dat archivu v určeném formátu.
- **Řízení ukládání**
  Zajišťuje konzistentní uložení metadat a obsahu archivních balíčků současně do archivního systému, systému správy dat a systému pro přístup bezpečným a prokazatelným způsobem v souladu s Národním standardem elektronických spisových služeb.

Modul správy dat

- **Evidence číselníků**
  Zajišťuje ukládání a přístup k číselníkům používaným v rámci vstupní kontroly a vyhledávání. Jedná se zejména o tyto číselníky - původci, klasifikace, povolené souborové formáty, spisové plány jednotlivých původců, kategorizace dokumentů podle kritérií přístupnosti, požadavků na zachování důvěryhodnosti, doby uložení.
- **Evidence přijímaných a uložených balíčků.**
  Zajišťuje vedení a přístup ke katalogu uložených dokumentů včetně stavu příjmu a uložení.
- **Evidence kontroly konzistence.**
  Uložení kontrolních součtů jednotlivých uložených balíčků AIP na aplikační úrovni pro účely periodické kontroly konzistence uloženého obsahu nezávisle na vlastnostech použitého archivního úložiště.
- **Evidence procesů skartace a archivace.**
  Informace o stavu skartace a informace o stavu jednotlivých balíčků AIP zařazených do skartačního řízení.

Archivní systém

- **Bezpečné uložení**
  Zajišťuje vlastní bezpečné uložení obsahu balíčků AIP do zvoleného úložiště NAS/CAS

Modul administrace

- **Řízení procesu příjmu**

Pro administrátora zajišťuje přehled o stavu příjmu balíčků SIP, umožňuje řešení problémů se strukturou a obsahem balíčků při příjmu.

- **Řízení procesů migrace**
  Spouštění migrace souborových formátů v uložených balíčcích a přehled o provedených migracích.
- **Skartační řízení**
  Příprava návrhu a jeho schvalování, provedení skartace, případně exportu do Národního digitálního archivu (případně do jiného dlouhodobého úložiště) v definovaném formátu.
- **Správa kontroly konzistence**
  Přehled o průběhu ověřování kontrolních součtů a o nalezených problémech s uložením balíčků AIP.
- **Správa číselníků**
  Zajišťuje pro administrátory původce a archivu aktualizaci a čtení číselníků používaných v rámci vstupní kontroly a vyhledávání.
- **Ukládání transakčních záznamů.**
  Pro účely auditu zaznamenává veškeré provedené operace nad uloženými balíčky (příjem, kontrola, transformace, ukládání, čtení). Uložené záznamy jsou zároveň ukládány do úložiště ve formě AIP.
- **Přístup k transakčním záznamům**
  Zobrazení transakčních záznamů pro účely auditu v souladu s požadavky na logování viz dále.

Přístupový modul

- **Zabezpečení přístupu a autentizace uživatelů.**
  Zajištění přístupu uživatelů k uloženým metadatům a dokumentům. Identifikace a autentizace uživatelů bude realizována proti řešení SSO Plzeňského kraje. Identifikace uživatelů a jejich zařazení k organizaci (původci) bude přebírána z řešení ePUSA.
- **Autorizace - omezení přístupů na základě klasifikace dokumentu, původce, uživatelských skupin a rolí uživatelů.**
  Základní oprávnění (minimálně přístup ano/ne) bude přebírán z role v systému ePUSA, jemnější členění oprávnění bude řešení udržovat samostatně. Modul povolí přístup ke čtení obsahu nebo metadat podle rolí přihlášeného uživatele a oprávnění příslušného balíčku.
- **Vyhledání uložených balíčků na základě zvolených metadat.**
  Uživatel bude mít možnost vyhledávat nad metadaty zvoleného logického úložiště v rámci svých uživatelských oprávnění.
- **Postoupení uložených dokumentů ve formě DIP**
  výběr dokumentů a jejich zaslání oprávněnému uživateli ve standardizované podobě
- **Provádění transakčních záznamů o přístupu k jednotlivým uloženým balíčkům**
  Systém eviduje veškeré přístupy k uloženým dokumentům a archivuje je.
- **Programové rozhraní API na externí portál pro přístup**
  V případě, že bude nasazeno externí portálové řešení, umožňující publikaci vybraného obsahu, bude toto rozhraní použito pro jeho přístup do úložiště.

1.6.1.3 Otevřené rozhraní vůči dalším systémům

Rozhraní pro přístup k KDS musí být specificky navrženo pro příjem a výdej balíčků v příslušném formátu definovaném na základě standardů. Vzhledem k zajištění bezpečnosti a konzistence uložených dat probíhá příjem dat do úložiště asynchronně v rámci procesu, který se skládá z několika kontrolních a transformačních procedur.

Operace vstupního rozhraní minimálně zajistí:

- Přenos balíčků SIP do spisovny
- Poskytování informací o stavu zpracování přijatých balíčků
- Poskytování informací o stavu uložených balíčků
- Poskytování obsahu číselníků použitých při validaci vstupních dat a správě spisovny
- Vstup na fyzickém (doneseném) médiu
- Nástroj na přípravu formálních balíčku (viz dále).

Operace výstupního rozhraní minimálně zajistí:

- Výdej obsahu ze spisovny (balíčky DIP)
- Poskytování informací o stavu žádosti o výdej
- Poskytování informací o proběhlých skartačních řízeních
- Poskytování informací o skartaci a archivaci dokumentů

Integrace

- Otevřené rozhraní pro vstup dokumentů a jejich metadat podle specifikace XML formátu NSESSS pro předávání dokumentů a jejich metadat do archivu
- Komunikace na vstupu postavená na Web Services
- Výstup dat (archiválií) do Národního digitálního archivu podle specifikace Národního archivu
- Aplikace pro manuální vytváření vstupních SIP balíčků
- Integrační rozhraní vůči elektronickým spisovým službám, dostupným na trhu

1.6.2 Nástroje

1.6.2.1 Pracovní úložiště

Pracovní úložiště bude vybudováno jako úložiště se základní funkcionalitou, nabízející běžné základní služby souborového systému (FS). Typicky budou data uložena na vrstvě úložiště TIER2 nebo TIER3.

Požadavky na pracovní úložiště

- Bezpečnost – z pohledu dostupnosti, důvěrnosti a integrity uložených dokumentů
- Evidence typů ukládaných dat v katalogu pracovního úložiště
- Organizace dokumentů/dat do adresářů či složek;
- Práce s dokumenty pomocí více rozhraní (HTTP/S, S/FTP, CIFS, NFS)
- Možnost umístění celého logického úložiště na TIER2, TIER3 nebo CAS
- Podpora standardizovaných a otevřených typů filesystémů
- Podpora importu většího množství souborů, exportu a migrace dat na jiný HW
- Integrace funkcionality autentizace uživatelů s řešením SSO Plzeňského kraje
- Centrální administrace úložiště přímo z katalogu logických úložišť (logická úložiště, objemové kvóty, autonomní správa uživatelů)
- Možnost namapování úložiště nebo jeho části jako logického disku v MS Windows na počítači uživatele (např. CIFS)

Nepovinná funkcionalita pracovního úložiště

Tato funkcionalita není povinnou součástí řešení (řešení bude tímto směrem v budoucnu rozvíjeno):

- Plná podpora technik ILM a HSM pro ukládání dat

- Podpora elektronických podpisů a časových razítek
- Zaznamenávání historie práce s dokumenty pro účely auditu;
- Řízení uživatelských přístupových oprávnění na úrovni celého logického úložiště;

Vnitřní členění logických úložišť

Pracovní úložiště bude rozděleno na jednotlivé logické segmenty. Tyto logické segmenty (logická úložiště) budou definovány v katalogu pracovního úložiště a na jejich základě bude vytvořena logická struktura úložiště. Pro každý segment bude definován typ ukládaných dat, formát datových souborů, ukládací politika, původce datových souborů a přístupová pravidla. Segment bude samostatně upravovatelný z pohledu místa uložení a z pohledu řízení přístupových práv.

V katalogu budou evidovány jednotlivé logické segmenty úložiště s těmito parametry:

- Název logického segmentu a textový popis významu uložených dat
- Původce dat v logickém segmentu, jeho kontaktní osoby
- Typy ukládaných dat a formáty datových souborů v rámci logického segmentu
- Přístupové protokoly
- Pravidla řízení životnosti dat v logickém segmentu
- Pravidla ukládacích politik požadovaného způsobu uložení s ohledem na rychlost přístupu (má vliv na konfiguraci HSM).
- Definice skupin uživatelů oprávněných k přístupu k souborům daného logického segmentu.
- Podrobný popis souborových formátů (dokumentace, standard), kdo standard vydal a udržuje, kdo jiný standard ještě používá.
- Předpisy/normy podle kterých je třeba zajistit bezpečnost dat (osobní data, data chráněná autorským zákonem) v jednotlivých logických segmentech.
- Pravidla způsobu kryptování, periodicita obměny kryptovacích klíčů, dostupnost a způsob zajištění dostupnosti klíčů pro vybrané logické segmenty úložiště.

Katalog musí umožňovat přidávat, měnit a odebírat parametry administrátorem. Změny záznamů v katalogu musí být verzované, aby byl dohledatelný stav záznamů k určenému datu.

Data katalogu musí být uložena do databáze nebo jiným způsobem, který umožní jejich jednoduché zálohování.

Katalog musí umožňovat exporty a tiskové výstupy v nezbytném rozsahu.

Přístup do katalogu musí být umožněn jen oprávněným, Zajištění přístupu uživatelů k uloženým metadatům a dokumentům (dle předem definovaných rolí v Identity management, podpora SSO včetně přidělení oprávnění dle členství ve skupinách) s možností nastavení práv minimálně na úrovni nic/čtení/změna/admin všech záznamů katalogu.

1.6.2.2 Konverze datových formátů PDF/A

Nástroj bude fungovat jako centrální serverové řešení, které bude použité pro konverzi souborů z běžně používaných jiných formátů do formátu PDF/A. Komunikovat s dalšími informačními systémy bude prostřednictvím plně zdokumentovaného rozhraní (API), postaveného na běžně používaných technologiích, které umožní kontrolu těchto informačních systémů nad procesem konverze.

Pro konverzi z datových formátů aplikací třetích stran se předpokládá instalace těchto aplikací na server, na kterém bude nástroj provozován, nástroj je bude využívat pro převod. Licence aplikací třetích stran zajistí zadavatel, nejsou předmětem poptávky.

Nástroj musí chránit utajení a autenticitu dokumentů, jejichž obsah může být citlivý.

1.6.2.3 Tvorba SIP balíčků

Nástroj bude samostatně provozovatelný u jednotlivých původců – uživatelů dlouhodobého úložiště jako samostatná aplikace, spustitelná na klientském počítači. Pro svoji činnost nebude nutně požadovat on-line napojení na dlouhodobé úložiště (s omezeními, které off-line provoz přináší, jako nemožnost ověřovat strukturu metadat v aktuálních seznamech).

1.7 Bezpečnostní specifikace řešení

1.7.1 Vybrané bezpečnostní požadavky na dodávané řešení

- autentizace přístupu uživatelů s využitím řešení SSO
- centrální autorizace a řízení přidělování oprávnění
- přebírání uživatelů a základních autorizačních rolí z ePUSA (minimálně na úrovni přístup povolen/zamítnut)
- možnost distribuované správy oprávnění (delegace správy za jednotlivá logická úložiště)
- řešení zranitelností
    - součástí akceptace bude test zranitelnosti, provedený na náklady zadavatele
    - zadavatel bude po dobu provozování řešení průběžně kontrolovat zranitelnost řešení, dodavatel bude povinen provádět opravy nalezených problémů z bezpečnostních skenů v rámci údržby
    - zadavatel bude příležitostně po dobu provozování řešení objednávat externí testy zranitelnosti. V případě, že externí test objeví nedostatky dodávaného řešení, hradí zadavatel nejvýše jeden další opakovaný externí test zranitelnosti. Nebudou-li problémy odstraněny ani poté, zaplatí dodavatel smluvní pokutu za každý další externí test zranitelnosti ve výši ceny tohoto testu.

1.7.2 Požadavky na logování

- řešení musí generovat strojově čitelné, strukturované logy, které lze importovat do připravovaného systému řízení centrálního logování
- logy musí obsahovat informace, které jsou nezbytné pro audit činností libovolného uživatele
- v auditním logu se eviduje vždy minimálně:
    - vstup uživatele do systému (příp. opuštění)
    - změna oprávnění
    - změna konfigurace
    - vložení či změna vybraných dat
    - přístup k vybraným datům
- systémy musí dodržet strukturu logování nebo dodat "slovník" událostí

1.8 Požadavky na dokumentaci

V rámci plnění bude dodána minimálně tato dokumentace:

- prováděcí dokumentace (prováděcí projekt)
- provozní dokumentace
  - bezpečnostní dokumentace
  - systémová příručka
  - uživatelská příručka
- popis řešení havárií
- školicí dokumentace
- strategické plány dlouhodobého úložiště
- typová smlouva s původcem

V rámci placené údržby bude dodavatel zajišťovat aktuálnost dodané dokumentace.

1.8.1 Prováděcí dokumentace

Prováděcí dokumentace bude sloužit jako podklad pro implementaci řešení, bude zpracována v tomto minimálním rozsahu:

- schémata
  - síťová
  - datová
  - aplikační vč. integrace
- popis procesu nasazení aplikace vč. zpřesněného harmonogramu
- popis procesu migrace dat
- požadavky na součinnost v průběhu implementace
- návrh školení uživatelů
- návrh akceptačních testů
- popis údržby

1.8.2 Provozní dokumentace

Provozní dokumentace bude zpracována minimálně v rozsahu, definovaném pro ISVS v zákonu o ISVS a jeho prováděcích předpisech.

1.8.3 Popis řešení havárií

Popis řešení havárií bude zpracován v míře podrobnosti, použitelné pro zařazení do celkového plánu zotavení z havárie (Disaster Recovery Plan) KÚPK.

1.8.4 Strategické plány dlouhodobého úložiště

Budou zpracovány a udržovány aktuální strategické plány podle metodiky PLATTER.

1.8.5 Typová smlouva s původcem

Bude připravena typová smlouva Plzeňského kraje jakožto správce dlouhodobého úložiště s původcem (uživatelem) dlouhodobého úložiště. Smlouva bude zaměřena na využití dlouhodobého úložiště jako krajské digitální spisovny.

1.9 Popis prostředí zadavatele

Pro implementaci řešení vítězného uchazeče bude připraveno prostředí v dále definovaném rozsahu. Podrobnosti jsou uvedené v této kapitole.

1.9.1 Zajištění potřebného hardware

Obsahem této poptávky není dodání hardwaru, vyjma garantovaného úložiště, řešeného v jiné části této poptávky. Hardware bude zajišťovat v definovaném rozsahu zadavatel, s výjimkou HW garantovaného úložiště. Zadavatel k realizaci řešení je připraven v současné době zajistit:

1) umístění serverů ve virtuální prostředí datového centra (ESX vSphere 5. x)

   Limit pro celé prostředí (součet na všech serverech a podíl na SQL Serverech) vyčleněného pro realizaci řešení je 32GB RAM.

   Virtuální servery budou hostovány na společném virtuálním hostu, dimenzovaném pro až 50 virtuálních serverů. Virtuální host má 2 fyzické procesory s výkonem minimálně SPECint_rate2006: 490 bodů, SPECfp_rate2006: 350 bodů

2) umístění systémů a dat ve sdíleném diskovém úložišti NAS datového centra, určeného pro cca 100 serverů.
   Počáteční nastavení pro celé prostředí (součet na všech serverech a podíl na SQL Serverech) vyčleněného v NAS pro realizaci řešení:

   a. 4 TB na poli se výkonem max. 6000 IOP, minimálně 240 IOP na diskový oddíl.

   b. 10 TB na poli s výkonem max. 2000 IOP, minimálně 80 IOP na diskový oddíl.

3) Zajištění bezpečnosti serverů na úrovni síťového provozu (firewall).

V případě nutnosti se do budoucna předpokládá navýšení těchto kapacit po oboustranné dohodě.

1.9.2 Zajištění potřebného software

1.9.2.1 Serverová část

Obsahem této poptávky není dodání základního software, který bude zajišťovat v definovaném rozsahu zadavatel. Zadavatel k realizaci řešení je připraven v současné době zajistit:

1) Operační systém – předpokládány jsou 4 stroje (možné navýšení v odůvodněných případech, limitováno výší dostupné RAM) s operačním systémem Windows 2012 nebo 2008 R2 v edici Data Center

2) Databáze - přístup k jednomu serveru MS SQL 2012 nebo 2008 R2 v edici Standard či Workgroup. Bude poskytnut administrátorský přístup k databázím (vytvoření databáze zajistí zadavatel podle specifikace dodavatele – přímý přístup k operačnímu systému stroje s MS SQL nebude umožněn)

3) Anti-X ochranu, řešenou na úrovni datového centra pro každý server

Na všechen výše uvedený software pod body 1-3 bude zadavatel na své náklady zajišťovat podporu, tj. právo na nové verze a update minimálně z pohledu bezpečnosti po celou dobu provozování řešení. Doba upgrade na vyšší verze bude stanovena po oboustranné dohodě, nejzazší doba upgrade na úrovni operačního systému nebo databáze souvisí s ukončením podpory bezpečnostních update výrobce k dané verzi.

Zadavatel v této chvíli předpokládá zachování produktové řady základního software (vyšší verze MS Windows Server a MS SQL Server ve stejných nebo odpovídajících edicích), do budoucna si však z důvodu provozních nákladů vyhrazuje právo požadovat přenesení vlastního dlouhodobého úložiště, případně i pracovního úložiště do plně open-source prostředí. Uvedené části řešení proto musí toto prostředí podporovat (tj. být nativně provozovatelné v prostředí některé aktivně podporované rozšířené serverové distribuce GNU/Linux a alespoň jedné aktivně podporované rozšířené relační open-source SQL databáze).

Zadavatel preferuje, aby řešení bylo implementováno do výše popsaného prostředí. V případě, že řešení uchazeče bude vyžadovat pořízení dalšího software kromě vlastního poptávaného řešení a výše uvedeného základního software, zahrne do nabídky pořízení veškerých potřebných licencí, implementace, důkladné zaškolení všech správců a následná údržba ve stejném rozsahu (tj. právo na nové verze a bezpečnostní update) po celou dobu, po kterou bude poskytována podpora nabízeného řešení. V tom případě uchazeč do nabídky uvede veškerý takový software včetně jeho výrobce a licenční politiky, zahrne pořizovací náklady na pořízení licencí a na následnou údržbu do nabídkové ceny a software zahrne do smlouvy o poskytování technické podpory.

Řešení musí být ošetřeno proti náhlému výpadku serveru. Systém musí být schopen se v takovém případě automaticky vrátit ke konzistentnímu stavu. Software musí přistupovat ke konzistentním datům, sledovat výpadek, vrátit se automaticky v čase (na úrovni záloh i transakcí).

Administrace systému jako takového, tj. přidělování práv, správa účtů musí vycházet z obvyklých standardů zadavatele a modul správy to musí reflektovat.

1.9.2.2 Klientská část

Uživatelské rozhraní dlouhodobého úložiště musí být provozovatelné na tomto prostředí:

1) Windows XP a vyšší, podpora alespoň jedné aktivně podporované rozšířené distribuce GNU/Linux
2) Internet Explorer 8 a vyšší, Firefox 15 a vyšší

1.9.3 Dostupnost infrastruktury pro dodavatele

Zadavatel zajistí celkovou bezpečnost infrastruktury, na níž bude řešení provozováno.

Přístup dodavatele k infrastruktuře bude zajištěn

- fyzicky – běžně v pracovní době, po dohodě lze výjimečně domluvit rozšířený režim (noci, víkendy), pokud to projekt bude vyžadovat
- vzdálený přístup přes VPN na servery, vyhrazené na projekt
- oprávnění
    - přístupová práva k serverům, vyhrazeným pro projekt (v odůvodněných případech na úrovni administrátora)
    - admin přístup k databázi (nikoli k serveru)

1.9.4 Součinnost dodavatele

Dodavatel musí postavit nabídku bez předpokladu, že přenese některé práce na zadavatele. Zadavatel si vyhrazuje právo limitovat součinnost svých pracovníků jen na úkoly nezbytně nutné, které není možné spravedlivě požadovat po dodavateli.

1.10 Podpora provozu dlouhodobého úložiště

Zhotovitel se smluvně zaváže udržovat a podporovat řešení po celou dobu udržitelnosti projektu.

Na údržbu a podporu řešení bude s vybraným uchazečem uzavřena smlouva o technické podpoře na dobu neurčitou. Součástí smlouvy bude dodávka nových verzí produktu, oprava chyb, zohlednění změn legislativy, informační linka a garance úrovně služeb (SLA) při servisním zásahu.

Vybraný uchazeč bude v rámci této smlouvy povinen zajistit, že veškeré funkce řešení, popsané v této zadávací dokumentaci a dodané spolu s dílem a dokumentací díla budou odpovídat obecně platným právním předpisům ČR a platným standardům, které musí podle zákona nebo podle této zadávací dokumentace dodržovat.

Technická podpora a údržba zahrne především:

- právo zákazníka na nové verze produktu a zapracování požadovaných legislativních změn
    - poskytování legislativního update a upgrade ve vazbě na aktuálně platné právní předpisy s tím, že jejich distribuce bude provedena před termínem účinnosti změn právních předpisů,
    - poskytování update a upgrade produktu dle potřeby vzniklé požadavky zadavatele či samostatnou, nevynucenou inovační činností zhotovitele
    - v rámci placené údržby bude dodavatel zajišťovat i aktuálnost dodané dokumentace
- instalace a implementace update a upgrade řešení v prostředí zadavatele
    - bude prováděna pravidelně v termínech, odsouhlasených mezi oběma smluvními stranami, nejpozději však k datu, po kterém by byla ohrožena bezpečnost řešení, jeho plná funkcionalita nebo jeho soulad s legislativou
- přenos řešení do nového prostředí zajišťovaného zadavatelem (operační systém, databázový server)
    - v případě, že výrobce přestane podporovat některou část prostředí, ve kterém je řešení provozováno, dodavatel v rámci podpory provede přenos řešení do nového prostředí, připraveného zadavatelem s respektováním produktové řady komponent prostředí (vyšší verze stejných nebo srovnatelných edicí Microsoft Windows Server a Microsoft SQL Server)
- řešení provozních problémů
    - vzniklých při užití produktu zadavatelem a jednotlivými původci,
    - vzniklých při užití produktu na pracovišti zadavatele a původců,
    - při užití produktu vzdáleným přístupem k prostředkům zadavatele,
- služba Hot-line formou telefonické podpory pro zadavatele pro řešení technických problémů, poradenství a konzultace,
- služba Helpdesk pro zadavatele pro hlášení závad jednotlivých kategorií, poradenství a konzultace.

Technická podpora a údržba bude poskytována od převzetí řešení do rutinního provozu a jeho akceptace bez výhrad, a to po celou dobu účinnosti Smlouvy o servisní podpoře. Další informace o rozsahu technické podpory a údržby jsou uvedeny dále.

Pohotovost podpory je poskytována pracovní době, tj. v pracovních dnech od 8:00 do 16:00 (režim 5x8). Provozní doba služby bude v pracovních dnech v této době garantována.

Plánované přerušení provozu řešení oznámí zadavatel minimálně 5 pracovních dnů předem, závazkem protistrany je potvrdit tuto informaci.

Požadovaná úroveň služeb (SLA)

Priorita	Charakteristika problému	Reakční doba	Doba vyřešení požadavku od převzetí
Vysoká	Kategorie A	4 pracovní hodiny	7 pracovních dnů
Střední	Kategorie B	8 pracovních hodin	15 pracovních dnů
Nízká	Kategorie C	24 pracovních hodin	30 pracovních dnů

Problémem (závadou) se rozumí takový stav systému, který neumožňuje provádět jednotlivé funkce systému, nebo nejsou splněny podmínky stanovené v dokumentaci, nebo je ohrožena bezpečnost uložených dat. Závady jsou klasifikovány dle jejich závažnosti a provozních podmínek na tři kategorie důležitosti:

- Vysoká = závady vylučující užívání software nebo jeho důležité a ucelené části (tj. problémy, zabraňující provozu systému), provoz systému je zastaven.
- Střední = závady způsobující problémy při užívání a provozování informačního systému nebo jeho části, ale umožňující provoz systému. Provoz systému je omezen, ale činnosti mohou pokračovat určitou dobu náhradním způsobem.
- Nízká = provoz systému je závadou ovlivněn, ale může pokračovat jiným způsobem, např. organizačními opatřeními.

Požadavek na servisní zásah může být uplatněn zadavatelem na systému Helpdesk.

Po nahlášení a následném zpětném potvrzení požadavku kontaktuje řešitel případu zadavatele a dohodne podrobnosti a způsob řešení. Závady způsobené chybou aplikace jsou zahrnuty v poplatku za technickou podporu a údržbu.

2 HW garantovaného úložiště do TC Plzeňského kraje

Předmětem této části poptávky je řešení hardware garantovaného úložiště do Technologického centra Plzeňského kraje.

2.1 Popis předmětu plnění

Požadavky na garantované úložiště vycházejí z typizovaného projektového záměru Technologického centra kraje jako přílohy výzvy IOP č. 08 (viz http://www.osf-mvcr.cz/vyzvy/2-1-zavadeni-ict-v-uzemni-verejne-sprave-leden-2010).

Je požadována dodávka a implementace **2 ks** shodných úložišť s možností replikace, z nichž každé bude umístěno v samostatném datovém centru Technologického centra Plzeňského kraje.

Hardware garantované úložiště bude primárně sloužit pro potřeby dlouhodobého úložiště digitálních dokumentů, řešeného v rámci této veřejné zakázky. Zadavatel však do budoucna předpokládá využití garantovaného úložiště i pro jiné účely v rámci Technologického centra kraje.

Navržené zařízení musí splňovat základní parametry a charakteristiky:

- funkcionalita Content-addressable storage (CAS)
- minimální podporované protokoly CIFS, NFS, HTTP, HTTPS, WEBDAV.
- možnost ovládání úložiště přes popsané programové rozhraní (API)
- protokoly založené na HTTP (HTTP, HTTPS, WEBDAV) mohou být zajištěny out-of-box řešením zahrnutém v dodávce při zachování podpory výrobce.
- otevřené řešení, podpora otevřených standardů, standardní rozhraní souborového systému
- čistá využitelná úložná kapacita každého úložiště minimálně 8 TB
- úložiště musí zajistit dostatečnou ochranu dat i v případě závady dvou různých disků pole (např. RAID6 nebo RAID5 s hot-spare diskem)
- veškeré potřebné softwarové licence
- rozšiřitelnost minimálně na 40TB čisté kapacity
- garantovaná neměnnost uložených dat
- garantovaná jedinečnost dat
- garantovaná autentičnost a nepodvržitelnost obsahu archivu
- splnění požadavků na „důvěryhodné úložiště“, vyplývajících z legislativy (především zákona o archivnictví a spisové službě, autorského zákona, zákona o ochraně osobních údajů, správního řádu, daňového řádu a zákona o finanční kontrole, v platném znění, včetně prováděcích vyhlášek)
- vysoká bezpečnost dat - nikdy neexistuje tak privilegovaný administrátor, aby mohl získat přístup k obsahu objektů (mimo vybrané požadované vlastnosti, např. export/migrace dat do nového pole), případně objekty mazat nebo manipulovat s podpisy a obsahem.,
- možnost šifrování obsahu (minimálně AES)
- fulltextové indexování a vyhledávání v plné kapacitě, vyjma šifrovaného obsahu
- garantovaná nesmazatelnost uložených dat po definovanou dobu (retenční politika), po uplynutí doby variantně buď smazání záznamu, nebo pouze uvolnění zámku, bránícího smazat
- garantovaný skartační algoritmus
- replikace dat na stejné nebo nadřazené (podřízené) úložiště – nabídka musí obsahovat i druhé úložiště
- zachování názvů souborů a formátů

- možnost automatického vytváření více kopií uložených objektů v každém z garantovaných úložišť
- Možnost módu HA (high-availability) - řešení, které nemá žádný "single point of failure"
- Podpora Active Directory a LDAP autentifikace
- výrobcem garantovaný a popsaný proces exportu dat (v případě přechodu na úložiště jiného výrobce) a proces převodu dat do nového nebo náhradního zařízení stejného nebo vyššího modelu minimálně po dobu 10 let
- podpora virtuálních resp. logicky oddělených úložišť – podpora modelu využití a správy pro každé logické úložiště odděleně (minimálně vytváření a změny uživatelských účtů, složek)

Požadavky na poptávané řešení jako celek, tedy řešení dlouhodobého úložiště digitálních dokumentů s využitím HW garantovaného úložiště, musí dále splňovat následující požadavky:

- soulad s normou ISO 14721:2003 pro referenční model otevřeného archivačního informačního systému (OAIS)
- soulad s normou ISO 15801:2004, doporučení pro důvěryhodnost a spolehlivost elektronicky zobrazovaných a uchovávaných informací

2.1.1 Implementace

Zadavatel požaduje provést minimálně následující implementační práce. Uchazeč dle svého uvážení do nabídky doplní další práce, které jsou dle jeho názoru nezbytné pro úspěšnou realizaci této části zakázky.

- instalace obou úložišť a konfigurace HW a SW pro zajištění funkcionality garantovaného úložiště včetně jejich propojení
- otestování jednotlivých funkcionalit za přítomnosti pracovníků zadavatele
- kompletní nastavení 20 samostatně spravovaných oddělených logických úložišť pro potřeby krajského úřadu a obcí s rozšířenou působností
- zpracování provozní dokumentace minimálně pro čtyři role (hlavní správce, správce logického úložiště, operátor, uživatel) včetně popisu všech relevantních procesů.
- V rámci implementace musí být vytvořeny příslušné skupiny oprávnění pro jednotlivé role
- součinnost při zařazení do virtuální serverovny zadavatele (napojení na servery, pole, garantované uložiště, základní dohled/monitoring, VPN přístup, apod.)
- nastavení základního dohledu, monitoringu a logování přístupu k úložišti
- zpracování havarijních plánů a plánů obnovy
- zajištění školení, každé v rozsahu 1 den:
    - pro hlavního správce – vybraní pracovníci zadavatele – cca 5 uživatelů
    - pro správce logických úložišť – vybraní pracovníci zadavatele a obcí s rozšířenou působností – cca 20 uživatelů
    - školení proběhne v prostorách zadavatele nebo v jiných prostorách odsouhlasených zadavatelem

2.1.2 Školení

Na úrovni TC K a odboru informatiky krajského úřadu je potřeba, aby byli odpovědní pracovníci zaškoleni do základní úrovně administrátora instalovaných technologií. Preferovány jsou proto technologie, na které jsou

zaměstnanci odboru informatiky krajského úřadu již proškoleni a běžně plní roli operátora nebo administrátora systému. Součástí dodávky technologií proto bude rozdílové školení pro tyto zaměstnance.

Následující tabulka shrnuje minimální rozsah a témata školení pro jednotlivé administrátorské role. Nebude-li zajištěna zastupitelnost zaměstnanců jinak (externě, spoluprací s ORP apod.), musí všechna školení absolvovat 2 zaměstnanci. Proškolený zaměstnanec bude zastávat roli „technologického garanta“ a bude odpovědný za proškolení ostatních zaměstnanců – vlastními silami, spoluúčastí na školeních či konzultacích, samostudiem apod. Dále bude odpovědný za průběžnou aktualizaci znalostí zaměstnanců v dané oblasti, zejména za seznamování se známými problémy a postupy řešení a významnými změnami konfigurací či funkčností technologií.

Součástí implementace bude školení správy garantovaného úložiště pro administrátory (1 skupina do 5 lidí v rozsahu 1 den).

2.2 Podpora provozu HW garantovaného úložiště

Detaily požadovaného rozsahu podpory jsou uvedeny ve smlouvě o technické podpoře, zde je uvedeno jejich shrnutí:

- servis a záruka 5 let v režimu 9x5 s reakční dobou do 4 hod a opravou do 3 pracovních dní.
- do požadované doby provést opravu popř. výměnu zařízení tak, aby bylo plně funkční
- činnosti potřebné k zajištění požadované úrovně záruk, servisu, aktualizací. Tzn. přístup softwarovým aktualizacím dodaného hw a sw (firmware apod.), případně pravidelné servisní prohlídky (pokud ji mi výrobce či dodavatel podmiňuje záruku)
- náklady na maintenance musí obsahovat veškeré náklady potřebné k zajištění požadované úrovně záruk, servisu, aktualizací apod. a to včetně povinných servisních prohlídek, revizí apod.
    - zajištění maintenance na 5 let
- pokud jsou některé funkce správy vyhrazeny jen uživateli s plným přístupem, který nebude zadavateli poskytnut (superadministrátor), zajistí dodavatel činnosti, spojené s nutností přihlásit se pod tímto uživatelem (např. export všech dat) bezplatně, a to po celou dobu záruky
- v případě nutnosti výměny či opravy vadné části Garantovaného úložiště, obsahující jakákoli uložená data, musí dodavatel před odvezením této části mimo prostory zadavatele garantovat, že není možná rekonstrukce uložených dat z této části do čitelné podoby (ať už použitými kryptovacími metodami, nebo kvůli fyzickému zničení). V opačném případě musí vadná část zůstat u zadavatele.