

Příloha č. 2 – Návrh na řešení Díla

Popis nabízeného technického řešení zpracovaný dle požadavků Přílohy 5 - Technická specifikace.

Popis nabízeného technického řešení je zpracovaný v níže uvedeném členění:

- (a) Detailní návrh cílového stavu respektující požadavky podle Přílohy 5 - Technická specifikace (zejména kapitoly 3) včetně uceleného detailního popisu jednotlivých částí systému a jejich vzájemných vazeb. Detailní návrh cílového stavu musí dále obsahovat detailní popis postupu implementace předmětu plnění včetně detailního popisu způsobu realizace implementačních služeb uvedených v kapitole 3.4 Přílohy 5 - Technická specifikace.
- (b) Detailní popis funkčních vlastností nabízeného plnění ve struktuře a rozsahu uvedených v kapitole 3 Přílohy 5 - Technická specifikace.
- (c) Detailní harmonogram projektu (vycházející a dodržující lhůty ze základního harmonogramu viz kapitola 4 Přílohy 5 - Technická specifikace) včetně popisu jednotlivých činností v dostatečném detailu. Z harmonogramu vyplývá, že realizace předmětu zakázky proběhne v požadovaných termínech.
- (d) Detailní popis záručního a pozáručního servisu v rozsahu požadovaném v kapitole 3.6 Přílohy 5 - Technická specifikace.
- (e) Detailní popis podpory provozu, tzn. servisních služeb, v rozsahu dle kapitoly 3 Přílohy 6 – Servisní služby.

1 DETAILNÍ NÁVRH CÍLOVÉHO STAVU

V této kapitole je uveden detailní návrh cílového stavu respektující požadavky podle Přílohy 5 - Technická specifikace (zejména kapitoly 3) včetně uceleného detailního popisu jednotlivých částí systému a jejich vzájemných vazeb. Detailní návrh cílového stavu obsahuje detailní popis postupu implementace předmětu plnění včetně detailního popisu způsobu realizace implementačních služeb uvedených v kapitole 3.5 Přílohy 5 - Technická specifikace.

1.1 DODÁVKA ELEKTRONICKÉHO ARCHIVU (EA)

Předmětem dodávky v této části předmětu plnění je dodávka dlouhodobého bezpečného důvěryhodného elektronického archivu elektronické zdravotnické dokumentace a ostatní dokumentace v souladu s legislativou (EA). V tomto archivu bude ukládána elektronická dokumentace vzniklá v rámci provozu ZZS. Součástí dodávky je veškerá nezbytná infrastruktura pro provoz a ukládání dat pro zajištění funkčnosti EA (servery, úložiště).

Primárním požadavkem je efektivně zpracovávat a dlouhodobě archivovat elektronické dokumenty a zajistit jejich právní validitu. Elektronické dokumenty musí být důvěryhodné a musí mít po formální i po obsahové stránce stejně trvalou důkazní hodnotu jako papírové.

Archivace dokumentace zajistí dlouhodobé a důvěryhodné uložení elektronických dokumentů podle zákona č. 499/2004 Sb., o archivnictví a spisové službě, Národního standardu pro elektronické systémy spisové služby (NSESSS) a podle úrovně technického řešení problematiky obvyklého v Evropské unii.

Stručný popis konceptu řešení:

Požadavek na archiv elektronické dokumentace (EA) plníme dodávkou produktu OBELISK Trusted Archive (OB-TA). Služby důvěryhodného elektronického archivu poskytované produktem OB-TA odpovídají požadavkům služby vytvářející důvěru „uchovávání elektronických podpisů a pečeti“ dle nařízení eIDAS. OB-TA nabízí řešení pro dlouhodobou archivaci elektronických dokumentů, které zajišťuje jejich čitelnost a důvěryhodnost po celou dobu jejich životního cyklu. Řešení je založené na aplikaci moderních technických standardů s využitím principů asymetrické kryptografie v podobě elektronické pečeti a časových razítek. Proces archivace vychází z obecných zásad pro práci s dokumenty a legislativních požadavků.

Nezávislost na vstupním formátu

Díky dodržení principů OAIS OB-TA umožňuje archivaci jakéhokoliv souboru bez ohledu na nástroj, aplikaci nebo systém, kterým byl vytvořen.

Validace

Veškeré dokumenty jsou při vstupu do archivu ověřeny, kdy se zkoumá přítomnost elektronických podpisů, pečeti a časových razítek. Validace je provedena dle principů nařízení eIDAS a zákona 297/2016. Výstupem validace jsou validační reporty a další podpůrná data (tj. certifikáty, CRL/OCSP, TSL seznamy, apod.), archivovaná společně s příslušným elektronickým dokumentem, tak aby bylo možné kdykoli v budoucnu prokázat v jakém stavu byl dokument do archivu předán.

Balíčkování

OB-TA nabízí možnost sdružování dokumentů do archivních balíčků, což minimalizuje požadavky na kvalifikovanou časovou razítka.

- Libovolný počet dokumentů lze seskupit do jednoho balíčku a výrazně optimalizovat potřebný počet časových razítek. Lze tak použít koncept jednoho kvalifikovaného časového razítka na celou skupinu ošetřených dokumentů. Obvyklé použití je zařazení 1000 dokumentů do jednoho archivního balíčku.

- Prokázání platnosti dokumentu a jeho podpisů/razítek bez nutnosti existence ostatních dokumentů ve stejném balíčku nebo přístupu k nim.

Balíčkování dokumentů lze parametrizovat dle počtu dokumentů, velikosti nebo časového intervalu.

Přerazítkování

OB-TA sleduje platnost časových razítek v archivních balíčcích. Automaticky prodlužuje jejich platnost přerazítkováním, kdy na archivní balíčky přidává nové časové razítko v okamžiku přiblížení konce platnosti předchozího.

Poskytování důkazního materiálu

V případě potřeby poskytuje OB-TA ve formě DIP důkazní materiál obsahující veškeré relevantní informace pro potřeby prokázání platnosti dokumentu a jeho bezpečnostních prvků.

Logování a audit

OB-TA průběžně zaznamenává operace týkající se činnosti v archivu.

Součástí je i **OBELISK Digitální spisovna** (OB-DS), která nabízí specifické funkce, které naplňují požadavky na provoz spisovny jako funkční složky elektronické spisové služby vyplývající ze zákona 499/2004 Sb. o archivnictví a spisové službě, vyhlášky 259/2012 Sb. o podrobnostech výkonu spisové služby a národního standardu pro elektronické systémy spisové služby NSESSS.

V rámci skartačního řízení OB-DS poskytuje následující operace:

- Příjem dokumentů k provedení skartačního řízení v podobě SIP dle NSESSS
- Sestavení skartačního návrhu
- Vyjmutí určených dokumentů ze skartačního návrhu
- Schválení skartačního návrhu
- Export skartačního návrhu ve formě SIP bez komponent dle NSESSS pro potřeby provedení skartačního řízení v nadřazeném archivu původce
- Zpracování odpovědní dávky z nadřazeného archivu dle NSESSS
- Export SIP dle NSESSS včetně komponent pro uložení v nadřazeném archivu
- Vymazání dokumentů a spisů, které prošly skartačním řízením
- Vyhledávání a prohlížení historie provedených skartačních řízení

Součástí je dále i produkt **OBELISK Storage** (OB-St), což je softwarově definované úložiště, které se stará o komplexní správu a řízení ukládání dat a dokumentů. Umožňuje zdrojovým systémům ukládat dokumenty do různých typů úložišť a konsolidovat tak přístup k dokumentům v rámci celé organizace. Prostřednictvím jednotného aplikačního rozhraní nabízí ale i řadu nadstavbových služeb. OBELISK Storage poskytuje zdrojovým systémům základní služby pro operace s dokumenty prostřednictvím jednotného aplikačního rozhraní (API). Služby mohou být skládány / kombinovány do jednoduchých procesů, a to bez ohledu na to, zda se jedná o služby synchronní či asynchronní. Jedním zavoláním API tak může být vyvolána celá souslednost služeb, které dokument zpracují do cílové podoby.

Typickými operacemi, které lze kombinovat jsou:

- Uložení dokumentu
- Validace dokumentu
- Pečetění dokumentu
- Archivace dokumentu

- Šifrování dokumentu v cílovém úložišti
- Stažení dokumentu

1.2 ÚPRAVY A NAPOJENÍ EZD NA ELEKTRONICKÝ ARCHIV

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 Kompletního záznamu o výjezdu (KZOV).
4. Implementace procesu průběžné aktualizace KZOV 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 KZOV.
6. Úpravy MZD a EKP, které zabrání podepsání zdravotnické dokumentace certifikátem s blížícím se koncem platnosti.
7. Vyčlenění úložiště a jeho správy komerčních certifikátů mimo EZD.
8. Úpravy integrace EZD na nové úložiště certifikátů.
9. Integrace EZD s digitálním archivem.

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

Pro přechod do plně elektronické zdravotní dokumentace ZZS HMP 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.

1.2.2 Přebírání nových údajů ze záznamu operátora v IS ZOS

Mezi IS ZOS a EZD je integrace, v rámci které jsou předávány informace týkající se tísňové výzvy ze záznamu operátora ZOS. Na straně IS ZOS dojde k rozšíření datového setu přenášených údajů o datum, čas a pořadové číslo tísňového volání.

Tyto nové informace budou převzaty do KZOV a stanou se jeho součástí. KZOV bude následně digitálně archivován.

Úprava bude realizována tak, aby případný výpadek EA nebo EZD neměl negativní vliv na provoz systému IS ZOS.

1.2.3 Zařazení nových údajů ze záznamu operátora v IS ZOS do Kompletního záznamu o výjezdu (KZOV)

Mezi IS ZOS a EZD je integrace, v rámci které jsou předávány informace týkající se tísňové výzvy ze záznamu operátora ZOS. Na straně IS ZOS dojde k rozšíření datového setu přenášených údajů o datum, čas a pořadové číslo tísňového volání.

Tyto nové informace budou převzaty do KZOV a stanou se jeho součástí. KZOV bude následně digitálně archivován. Takto bude pořízen a na jednom místě udržován ucelený záznam o výjezdu včetně související dokumentace a záznamu operátora ZOS z dispečerského deníku ZOS.

1.2.4 Implementace procesu průběžné aktualizace Kompletního záznamu o výjezdu (KZOV) a jeho podepisování uživateli, kteří provedli zápis / změnu v dokumentaci.

Úpravy budou provedeny v rámci Elektronické karty pacienta (EKP).

KZOV bude obsahovat kompletní záznam o výjezdu. Tato dokumentace úvodně vzniká při vytvoření ZOV, který je pořízen posádkou ZZS. ZOV prochází v organizaci dalším workflow zpracování.

V rámci oddělení kontrolingu dochází ke konverzi dokumentace související s výjezdem z papírové podoby do elektronické a její komplectaci, případně dílčím změnám dokumentace především v oblasti identifikace pacienta.

V rámci oddělení OZP může opět dojít ke změně identifikace pacienta na základě kontroly s registry pojištěnců.

Veškeré změny, ke kterým dojde v průběhu výše uvedeného workflow budou zahrnuty do KZOV včetně změnových logů (change list), které drží informace o tom, kdy a jaké položky byly v dokumentaci změněny. Změnové logy budou obsahovat seznam změn údajů, tj. původní hodnotu, novou hodnotu, datum a čas změny, autora změny případně další metadata, která budou identifikována v rámci implementační analýzy.

V rámci změnového logu budou vizuálně označeny okamžiky vytvoření a archivace dokumentace a tím odděleny změny v různých typech a verzích dokumentace

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

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 KZOV a zároveň digitálně podepsána uživatelem, který danou změnu provedl. Modul POJ nově zajistí promítnutí těchto změn do KZOV a zároveň digitální podpis uživatelem, který tuto změnu provedl. Adekvátním způsobem dojde i k záznamu změn do změnových logů.

1.2.6 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 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).

1.2.7 Vyčlenění správy a úložiště komerčních certifikátů mimo EZD

V současné době používá pouze systém EZD pro autentizaci a autorizaci komerční certifikáty uložené na QSCD prostředku.

Systém pro autentikaci je součástí EZD a integrovaný s AD organizace. Tento způsob ověření uživatele je aktuálně dostupný pouze v EZD. S nasazením digitálního archivu se rozšíří okruh uživatelů i mimo uživatele EZD, kteří budou rovněž pro autentikaci a autorizaci používat QSCD prostředky. Z tohoto důvodu bude třeba vyčlenit systém pro správu a ukládání komerčních certifikátů mimo EZD a zpřístupnit ho pro autentikaci a autorizaci vůči digitálnímu archivu i ostatním uživatelům.

V rámci vyčlenění dojde i k definici a implementaci rozhraní, které umožní ostatním systémům ZZS HMP autentikovat uživatele s využitím QSCD prostředků.

Součástí dodávky bude integrace úložiště komerčních certifikátů s archivem zdravotnické dokumentace tak, aby bylo možné přihlašování do archivu přes komerční certifikáty nebo dočasným heslem dle požadavků ZD.

1.2.8 Úpravy integrace EZD na nové úložiště certifikátů

EZD bude upraveno tak, aby mohlo využít pro autentikaci nově vytvořené úložiště komerčních certifikátů viz 1.2.7. Pro integraci s tímto úložištěm bude použito rozhraní, které umožňuje okolním systémům využít autentikaci a autorizaci na základě QSCD prostředků.

1.2.9 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.

1.2.9.1 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. Záznam o výjezdu po zpracování a podpisu oddělením kontrolingu – po provedených úpravách, včetně skenu záznamu o výjezdu od posádky, automatizované vytvoření a vyžádání podpisu uživatele.
3. Pokud v rámci vykazování péče zdravotním pojišťovnám dojde ke změně údajů pacienta, bude vytvořen a podepsán aktualizovaný záznam o výjezdu (doplnění funkčnosti do modulu pojišťovny).
4. 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.

1.2.9.2 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

1.2.9.3 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.

1.2.9.4 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

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.

1.3 ÚPRAVY IS ZOS PRO POSKYTNUTÍ KOMPLETNÍCH DAT DO EZD PRO NÁSLEDNOU ARCHIVACI

Tyto úpravy umožní doplnění údajů ze záznamu operátora k tísňové výzvě přenášných mezi IS ZOS a EZD o datum, čas a pořadové číslo tísňového volání. Díky tomu bude EZD vybaveno dostatečnými údaji pro sestavení Záznamu operátora, který jako součást Kompletního záznamu o výjezdu bude digitálně archivován.

Údaje budou přenášeny v rámci stávající integrace z IS ZOS do EZD, která bude rozšířena o uvedené údaje (datum, čas a pořadové číslo tísňového volání).

Úprava bude realizována tak, aby případný výpadek EA nebo EZD neměl negativní vliv na provoz systému IS ZOS.

1.4 DODÁVKA NEZBYTNÉ PROVOZNÍ INFRASTRUKTURY PRO DODÁVANÉ SYSTÉMY.

Dodávané systémy pro provoz elektronického archivu budou nasazeny do cloudového prostředí Amazon AWS, které zajistí veškeré potřebné komponenty pro provoz elektronického archivu v podobě aplikačních serverů, databázových serverů, síťové infrastruktury a zálohovacích a dohledových nástrojů. Bližší specifikace jednotlivých služeb je v kapitole 1.7.4.

1.5 DODÁVKA NEZBYTNÉHO SYSTÉMOVÉHO SW PRO DODÁVANÉ SYSTÉMY.

Produkty OBELISK jsou dodávány v podobě softwarové appliance, v níž je předpřipravena kompletní sada softwarového vybavení, nutného k provozu archivu. Veškerý potřebný software je tedy nedílnou součástí dodávky.

Stávající infrastruktura ZOS a EZD se nemění.

1.6 ČASOVÁ RAZÍTKA

Časové razítko zaručuje, že uvedená data v elektronické podobě existovala v určitý časový okamžik v dané podobě. Systémový čas, který se zaznamenává v dokumentech je lehce zmanipulovatelný, jediné časové razítko poskytuje nezpochybnitelný důkaz o tom, jak dokument vypadal v okamžiku, kdy byl orazítkován. Časové razítko navíc prodlouží ověřitelnost dokumentu s elektronickým podpisem.

V rámci archivace v OBELISK Trusted Archive jsou časová razítka využívána pro časové zafixování jednotlivých archivních balíčků. Archivační proces probíhá následovně:

1. OBELISK Trusted Archive přijímá dokumenty k archivaci.
2. Přijaté dokumenty dle nastavených pravidel (např. 1 archivní balíček pro 1000 dokumentů, nebo 1 archivní balíček za 24 hodin) zařazuje do archivních balíčků.
3. Při naplnění kapacity archivního balíčku je tento opatřen elektronickou pečetí archivu časovým razítkem.
4. OBELISK Trusted Archive automaticky sleduje platnost časových razítek ve vytvořených archivních balíčcích a provádí přerazítkování, jakmile se přiblíží datum vypršení platnosti časových razítek.

1.7 IMPLEMENTACE PŘEDMĚTU PLNĚNÍ

1.7.1 Dodávka elektronického archivu (EA)

1.7.1.1 Nasazení produktů OBELISK

Elektronický archiv bude realizován produkty OBELISK, který bude nasazen do cloudového prostředí Amazon AWS, za využití služeb popsanych v kapitole 1.7.4. OBELISK je postaven na vícevrstvé architektuře, takže budou zvlášť nasazeny:

1. Aplikační server v podobě produktové virtuální appliance postavené na CentOS Linuxu. Aplikační server bude nasazen jako instance virtuálního serveru služby EC2.
2. Databázový server bude hostovat databázovou logiku produktu OBELISK. Databáze bude nasazena ve službě RDS. Jako databázová technologie je použit PostgreSQL.
3. Objektové úložiště bude sloužit pro ukládání binárních souborů dokumentů předaných k archivaci. K tomu bude využita služba S3.

Totožné součásti se použijí jak pro primární tak i standby lokalitu.

1.7.1.2 Přístup ke službám OBELISKU

Integrace se službami OBELISKU bude realizována prostřednictvím produktového API SOAP webových služeb. Endpointy webových služeb budou dostupné pouze přes site-to-site VPN (realizovanou službou AWS VPC Site-to-Site VPN) po zabezpečeném https kanále. Dokumenty k uložení a archivaci budou předávány v rámci volání jako MTOM přílohy jednotlivých requestů.

1.7.1.3 Role jednotlivých součástí systému

OBELISK Trusted Archive

Úlohou OBELISK Trusted Archive je realizovat archivační proces předaných dokumentů. To se skládá z následujících hlavních činností:

- Validace dokumentů přijatých k archivaci – provádí automatizovanou validaci platnosti bezpečnostních prvků (elektronické podpisy, pečeti a časová razítka) u dokumentů vkládaných do archivu, přičemž počítá s grace periodami vydávání informací o odvolání. Výsledky provedených validací se v archivu ukládají společně s příslušnými dokumenty minimálně v rozsahu:
 - validační reporty,
 - certifikáty a certifikační cesty, na nichž byly založeny jednotlivé podpisy, pečeti nebo časová razítka,
 - informace o revokacích prokazující, že dotčené certifikáty byly, nebo nebyly odvolány v podobě CRL nebo OCSP odpovědí příslušných autorit,
 - TSL, které se k validaci daných certifikátů logicky vztahuje.
- Archivace – probíhá sdružováním dokumentů do množin (tzv. balíčkování) a jejich hromadné opatření elektronickou pečetí a opatření kvalifikovaným časovým razítkem.
- Přerazítkování – zajištění periodického prodloužení validity formou automatického přerazítkování archivních balíčků.

- Důkazní materiál – možnost stažení relevantních důkazů validity uloženého dokumentu minimálně v rozsahu:
 - soubor archivovaného dokumentu,
 - metadata dokumentu,
 - validační reporty dokumentu,
 - certifikáty podpisů/pečetí/časových razítek,
 - revokační data,
 - důvěryhodné kotvy v podobě TSL,
 - archivní balíček dokumentu.

OBELISK Storage

Je součástí systému OBELISK, zajišťující obsluhu integračních API a ukládání dokumentů do S3 objektového úložiště.

OBELISK Digitální Spisovna

Zajišťuje funkce skartace elektronických dokumentů v souladu s požadavky na skartace, které jsou uvedené v požadavku P.51 zadávací dokumentace.

1.7.2 Úpravy a napojení EZD na elektronický archiv

1.7.2.1 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 HMP. Tento deployment není možné udělat OTA aktualizací ale instalací závislých komponent na tablety v provozu ZZS HMP.

1.7.2.2 Přebírání nových údajů ze záznamu operátora v IS ZOS

V rámci této úpravy je řešeno získání a zpracování nových datových položek ze záznamu operátora, které budou nově předávány v rámci stávajícího interface IS ZOS – EZD. Úprava zahrnuje následující oblasti:

- **Úprava interface IS ZOS – EZD**
Jedná se o úpravu WCF rozhraní na straně EZD a příjem nových datových položek ze záznamu operátora
- **Úprava datového modelu MZD/EKP**
Nové datové položky budou začleněny do datového modelu dokumentace tzv. epcrDocument, který je využíván v MZD a EKP
- **Úprava business logiky aplikačního serveru a klientských aplikací MZD /EKP**
Jedná se o úpravu mezivrstev systému, které zprostředkovávají interakci mezi klientskými aplikacemi MZD a EKP a datovým modelem.
- **Úprava GUI MZD/EKP**
Úprava uživatelského rozhraní klientských aplikací MZD a EKP a zahrnutí nových položek do vizualizace datového modelu

1.7.2.3 Zařazení nových údajů ze záznamu operátora v IS ZOS do Kompletního záznamu o výjezdu (KZOV)

V rámci této úpravy dojde k úpravě designu Kompletního záznamu o výjezdu a doplnění nově přebíraných datových položek ze záznamu operátora IS-ZOS. Díky tomu může být výsledný dokument považován za plnohodnotný záznam operátora v elektronické podobě a následně digitálně archivován.

1.7.2.4 Implementace procesu průběžné aktualizace KZOV 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 oddělení kontrolingu či změny identifikace ošetřeného pacienta v rámci procesů OZP. Každá úprava dat musí být opatřena elektronickým podpisem osoby, která změnu provedla a pro jednoznačnou identifikaci změnovaných dat i changelovem, který popisuje, jaké datové položky byly změněny, jaká byla jejich původní a nová hodnota. Nově vygenerovaný KZOV bude následně digitálně archivován a vytvoří novou verzi již dříve uloženého KZOV v digitálním archivu organizace. Úpravu je třeba provést v následujících oblastech.

- **Úprava workflow práce s dokumentací při změně dat záznamu o výjezdu**
 - **Automatické generování KZOV při uložení**
Vytvoření nové verze KZOV při uložení změněné dokumentace
 - **Implementace podpisu nově vygenerovaného KZOV 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

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

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 KZOV při změnách identifikace pacienta na dokladech POJ**
Veškeré změny údajů KZOV, které mohou proběhnout v rámci modulu POJ budou zahrnuty do KZOV
 - **Implementace podpisu nově vygenerovaného KZOV uživatele**
Změny provedené v modulu POJ, které jsou promítány do KZOV 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

1.7.2.6 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)
- **Úprava GUI MZD, EKP a POJ**
Úprava uživatelského rozhraní aplikace implementace vizualizace notifikace uživatelům

1.7.2.7 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
- **Implementace OAuth standardu a distribuce JWT tokenů**
Pro zajištění SSO mezi EZD a DA bude implementován OAuth standard a modul bude úspěšně

přihlášeným uživatelům přidělovat JWT tokeny ve kterých budou prohlášení o jejich autorizaci k využívání externích systémů. Tyto tokeny budou zpracovávány v okolních systémech a na základě oprávnění, která v nich budou uvedena bude umožněn přístup k funkcínostem okolních systémů

1.7.2.8 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

1.7.2.9 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.

1.7.3 Úpravy IS ZOS pro poskytnutí kompletních dat do EZD pro následnou archivaci

Datový set předávaný v rámci integrace IS ZOS a EZD bude rozšířen o datum, čas a pořadové číslo tísňového volání. Tyto informace budou poskytnuty ze záznamu operátora, který je vedený v IS ZOS.

Úprava bude realizována tak, aby na straně IS ZOS neměla negativní vliv na provoz IS ZOS. Rovněž bude zajištěno, aby případný výpadek EA nebo EZD neměl negativní vliv na provoz systému IS ZOS.

1.7.4 Dodávka nezbytné provozní infrastruktury pro dodávané systémy

Dodávané systémy pro provoz elektronického archivu budou nasazeny do cloudového prostředí Amazon AWS. Přístup k infrastruktuře EA v cloudu bude zajištěn za pomoci síťových prvků ZZS HMP a služby AWS VPC Site-to-Site VPN Connection. Služby nebudou přímo dostupné z internetu. Provozní infrastruktura EA v cloudu se nebude sdílet účet s žádnou jinou službou a je provozována v režimu active-passive.

Použitá cloudová infrastruktura se bude skládat ze dvou částí, využívající různé služby AWS:

- 1) Výkonná aplikační část
 - a. Virtuální aplikační servery Elastic Compute Cloud (EC2), které budou hostovat aplikační část elektronického archivu.
 - b. Virtuální databázové servery služby Relational Database Service (RDS), které budou hostovat databázovou část elektronického archivu.
 - c. Objektové úložiště Simple Storage Service (S3), které bude sloužit, jako koncové dlouhodobé úložiště dokumentů předaných k archivaci.

- 2) Management část (bude sloužit ke správě jednotlivých služeb i celé cloudové infrastruktury elektronického archivu)
- a. Amazon Virtual Private Cloud (VPC) – slouží jako síťová vrstva pro EC2 a zajišťuje zejména služby správy adresního prostoru, sítě jako takové a site-to-site VPN.
 - b. AWS Identity and Access Management (IAM) – slouží ke správě uživatelů a přístupových práv.
 - c. AWS Key Management Service (KMS) – služba zajišťující správu šifrovacích klíčů, provozována dle pravidel FIPS 140-2.
 - d. AWS CloudWatch – služba pro sledování a monitoring infrastruktury a jejich jednotlivých služeb.
 - e. AWS Lambda – služba zajišťující provádění skriptů pro údržbu infrastruktury a zálohování infrastruktury a uložených dat.

Pro poskytování služeb Amazon AWS bude využíváno následujících lokalit:

- eu-central-1 (datacentrum Frankfurt, Německo) – pro primární i standby instance elektronického archivu včetně S3 objektového úložiště.
- eu-west-1 (datacentrum Dublin, Irsko) – pro ukládání záloh v podobě kopií snapshotů EC2 a RDS instancí a replikace S3 bucketu s dokumenty.

Tímto je zajištěno, že zpracovávaná ani ukládaná data v žádném případě neopustí území EU/EHS.

Amazon AWS plní všechny požadavky na ISO certifikace, uvedené v požadavku P.100 zadávací dokumentace. Jednotlivé certifikáty jsou dostupné na následujících adresách:

AWS ISO/IEC 27001:2013 ISO Compliance	<u>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</u>
AWS ISO/IEC 27017:2015 ISO Compliance	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
AWS ISO/IEC 27001:2013 ISO Compliance	<u>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</u>

V souladu s požadavkem P.115 zadávací dokumentace Amazon AWS zveřejňuje i SOC reporty. Ty jsou dostupné na adrese: XXXXXXXXXXXXXXXXXXXXXXXXXXXX.

1.7.5 Dodávka nezbytného systémového SW pro dodávané systémy

Produkty OBELISK jsou dodávány v podobě softwarové appliance, v níž je předpřipravena kompletní sada softwarového vybavení, nutného k provozu archivu. Veškerý potřebný software je tedy nedílnou součástí dodávky.

1.7.6 Časová razítka

OBELISK Trusted Archive pro získání časových razítek podporuje jakoukoli kvalifikovanou časovou autoritu, která splňuje protokol RFC 3161 Time-Stamp Protocol. Autentizace vůči službě časových razítek může být realizována jménem/heslem, nebo certifikátem.

Pro potřeby dodávky do doby předání a akceptace plnění v objemu na 100 dnů (mezi fázemi 5 až 10 harmonogramu dle kap. 3), bude dodáno

- 100 ks časových razítek pro balíčky elektronické zdravotnické dokumentace
- 100 ks časových razítek pro ostatní dokumentaci

Časová razítka pro potřeby provozu od doby předání a akceptace plnění jsou součástí servisních služeb uvedených v samostatném dokumentu. Účtována budou jen a pouze skutečně spotřebovaná časová razítka.

1.8 ZPŮSOB REALIZACE IMPLEMENTAČNÍCH SLUŽEB

Popis řešení:

Způsob realizace implementačních služeb bude plně odpovídat specifikaci uvedené v kapitole 3.5 Přílohy 5 - Technická specifikace Zadávací dokumentace viz požadavky uvedené níže.

- 1) Před zahájením implementačních prací bude zpracována **Implementační analýza včetně návrhu řešení** (konkretizace implementačního postupu, přesné konfigurace a instalačního a montážního návrhu řešení z nabídky), která bude zahrnovat informace pro všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění. Implementační analýza včetně návrhu řešení musí být před zahájením prací schválena objednatelem. Implementační analýza včetně návrhu řešení zohlední podmínky stávajícího stavu, požadavky cílového stavu a bude obsahovat tyto části:
 - a) Implementační analýza – zjištění týkající se prostředí objednatele, bude obsahovat následující:
 - i) Seznam technologií, které mají vliv/dopad na dodávku
 - ii) Identifikace zdrojů dat využitých pro dodávku
 - iii) Evaluace bezpečnosti systému a rizikových faktorů
 - iv) Implementační upřesnění specifikace požadavků
 - v) Výstupy z analýzy okolí – sběr a analýza informací vztahujících se k dodávce (např. součinnosti apod.)
 - b) Detailní popis cílového stavu (instalační a montážní upřesnění návrhu řešení z nabídky)
Popis bude obsahovat:
 - i) Rozpracování návrhu řešení z nabídky zhotovitele z pohledu instalací a montáže dle informací z implementační analýzy
 - ii) Upřesnění rozhraní pro integraci na IS a technologie třetích stran (v případě nutnosti)
 - iii) Způsob zajištění projektového řízení na straně zhotovitele pro realizaci předmětu plnění (harmonogram, projektový tým, koordinační mechanismy apod.)
 - iv) Detailní návrh a popis postupu implementace, instalace a montáže předmětu plnění
 - v) Detailní popis zajištění bezpečnosti systému a informací
Detailní harmonogram projektu včetně uvedení kritických milníků. Kritické milníky jsou termíny dosažení určitých fází projektu, které jsou pro naplnění cílů projektu klíčové. Kritické milníky budou obsahovat minimálně aktivity vedené v kapitole 3 - Detailní harmonogram projektu, s uvedením konkrétních termínů, zhotovitel vhodným způsobem může rozšířit kritické milníky o další aktivity, které mohou být pro projekt klíčové.
 - vi) Detailní popis navrhovaného seznámení s funkcionalitami, obsluhou dodávaného zařízení a budoucím provozem

Implementační analýza bude detailně popisovat způsob naplnění veškerých požadavků. Její akceptace je nezbytnou podmínkou pro realizaci dalších etap dodávky. Její nezbytnou součástí je dále konkretizovaný rozsah požadované součinnosti ze strany Objednatele.

- 2) **Zajištění projektového vedení/řízení** realizace předmětu plnění ze strany zhotovitele a jeho případných subdodavatelů.
- 3) **Vývoj, implementace a nastavení** informačních a komunikačních technologií odpovídající schválenému návrhu řešení uvedenému v Implementační analýze a příprava pro ověření ze strany objednatele, alespoň v následujícím rozsahu:
 - a) Vývoj na straně zhotovitele – vývoj jednotlivých systémů, úpravy existujících produktů, jejich parametrizace a nastavení, vývoj a ověřování integračních rozhraní, součinnost se třetími stranami v souvisejících oblastech.
 - b) Instalace a implementace do prostředí objednatele v testovacím režimu.
 - c) Interní ověření na straně zhotovitele a příprava podkladů pro ověření na straně objednatele (dokumentace, organizace testování a další).
 - d) Příprava a naplnění základních dat – z integračních úloh, číselníky, uživatelé a další.

Provedením těchto činností bude zajištěna připravenost pro ověření ze strany objednatele.

- 4) **Dodávka předmětu plnění.** Součástí dodávky musí být instalace, upgrade a sestavení předmětu zakázky včetně:
 - a) Instalace a nastavení infrastruktury a SW budou provedeny kvalifikovanými osobami pro dané typy zařízení
 - b) Nastavení infrastruktury, SW a aplikací
- 5) **Zajištění instalace všech součástí dodávky** v určených lokalitách a prostorách objednatele.
- 6) **Zajištění instalace a připojení** k zařízením a technickým prostředkům zajištěným objednatelem.
- 7) **Realizace pilotního provozu** k ověření funkčnosti systému na menším objemu dat, s menším počtem uživatelů a na menším počtu zařízení.
- 8) **Převedení systémů do zkušebního provozu** a plná podpora uživatelů v rámci zkušebního provozu včetně technické podpory. V této etapě budou realizována požadovaná seznámení s funkcionalitami, obsluhou dodávaného zařízení a budoucím provozem.
- 9) **Zpracování dokumentace skutečného provedení, systémové a provozní dokumentace** – součástí předmětu plnění je zajištění systémové a provozní dokumentace související s realizací předmětu plnění minimálně v následujícím rozsahu:

Název	Popis
Uživatelská dokumentace	Bude popisovat konkrétní funkčnost z pohledu uživatele tak, aby byl uživatel schopen práce s informačním systémem a pochopil význam jednotlivých částí systému a vazeb mezi nimi. V uživatelské příručce bude popisován způsob práce s jednotlivými částmi systému, vazby mezi nimi včetně popisu součástí jednotlivých částí systému. K usnadnění práce bude sloužit popis jednotlivých obrazovek, ovládacích prvků na obrazovkách a jejich významů, který bude uveden v rámci uživatelské dokumentace.
Dokumentace skutečného provedení	a Obsahuje popis informačního systému (rozhraní a služby) včetně popisu správy informačního systému, definování uživatelů, jejich oprávnění a povinností a detailní popis údržby systému.

Název	Popis
systémová/provozní dokumentace	
Bezpečnostní dokumentace	Účelem bezpečnostní dokumentace je definovat závazná pravidla pro zajištění informační bezpečnosti včetně stanovení bezpečnostních opatření. Součástí této dokumentace bude uveden seznam, který bude obsahovat seznam všech externích zdrojů, ke kterým se jednotlivé servery (součásti systému) připojují, včetně uvedení síťových protokolů, pomocí kterých se s daným externím zdrojem komunikuje. V případě, že na servery (součásti systému) existuje vzdálený přístup, musí být tento přístup jasně specifikován (vzdálené zařízení, síťový protokol) a popsán zdůvodnění takovéhoho přístupu (dohled, správa DB atd.)
Disaster & Recovery Plan	Plán řešení situací v případě výpadků a obnovy funkčnosti systému. Součástí je plán a způsob provádění zálohy a případného způsobu obnovy a obnovy funkčnosti i v případě jiných technických výpadků. Dokument bude vytvářen v součinnosti s objednatelem.
Projektová dokumentace	Smluvní dokumentace, harmonogram realizace projektu, analýzy a prováděcí projekty, zápisy z jednání, protokoly (předávací, akceptační)

Tabulka 1: Dokumentace – požadavky na zpracování

Dokumentace bude dodána v relevantním rozsahu na všechna místa plnění projektu.

Dokumentace bude v souladu se zákonem č. 365/2000 Sb. o informačních systémech veřejné správy a prováděcích právních předpisů, v platném znění.

Dokumenty budou zpracovávány v následujících programech elektronicky a uloženy v následujících formátech:

- MS Office 2016 (MS Word 2016, MS Excel 2016, MS PowerPoint 2016)
- MS Project 2016
- WinZip (formát .zip)
- Portable Document Format (formát .pdf).

Preferovaná forma předávaných dokumentů, které nebudou vyžadovat podpisy konkrétních osob je elektronicky a to na elektronických nosičích (CD, DVD, flash disk, atp.). K předávání a k archivaci souborů se používají média s možností pouze zápisu, nikoliv přepisovatelná.

Veškerá dokumentace bude podléhat schvalování (akceptaci) při převzetí ze strany objednatele.

Veškerá dokumentace bude zhotovena výhradně v českém jazyce, bude dodána ve 2x kopiích v elektronické formě ve standardních formátech (MS Office a PDF) používaných objednatelem na datovém nosiči a 1x kopii v papírové formě.

- 10) **Provedení akceptačních testů.** Zhotovitel je povinen kompletně připravit podklady pro akceptaci dodaného řešení. Součástí akceptace bude akceptační protokol a kompletní předávací dokumentace.
- 11) **Uvedení systému do produkčního provozu,** zajištění potřebných nastavení a přístupů pro všechny pracovníky objednatele, minimalizace dopadů na provoz objednatele při přechodu a zvýšená podpora bezprostředně po přechodu do produkčního provozu.
- 12) Zhotovitel dle svého uvážení doplní v nabídce další služby, které jsou dle jeho názoru nezbytné pro úspěšnou realizaci zakázky.

- 13) Veškeré náklady na zajištění služeb souvisejících s realizací předmětu plnění musí být zahrnuty v ceně odpovídající části předmětu dodávky.

1.8.1 Seznámení s funkcionalitami, obsluhou dodávaného systému

- 1) Zhotovitel proškolí pracovníky objednatele se všemi typy dodaných zařízení a aplikací a problematikou jejich užití, provozu a obsluhy. Zhotovitel se zavazuje poskytnout informace minimálně k následujícím tématům v dostatečném detailu pro porozumění činnosti zařízení a způsobu provozu:
 - a) Základní produktové seznámení s jednotlivými dílčími technologickými celky.
 - b) Celkové schéma součinnosti jednotlivých zařízení a jejich návaznosti.
 - c) Obsluha jednotlivých dílčích modulů, aplikací a technologických celků
 - d) Použitá nastavení zařízení, detailnější rozbor použitých konfigurací.
 - e) Základní kroky správy, diagnostiky a elementární postupy pro řešení problémů.
- 2) Poskytnuté informace zajistí seznámení pracovníků objednatele se všemi podstatnými částmi dodávky v rozsahu potřebném pro obsluhu, provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
- 3) Vše uvedené bude probíhat v prostorách objednatele s využitím vybavení dodaného v rámci této veřejné zakázky, případně zajištěné ze strany objednatele.
- 4) Konkrétní termíny určí objednatel dle postupu v rámci realizace projektu a dostupnosti zainteresovaných osob.
- 5) Seznámení s funkcionalitami, obsluhou dodávaného systému se týká klíčových uživatelů, ostatní uživatelé budou proškoleni klíčovými uživateli.

Veškeré náklady na zajištění těchto činností jsou zahrnuty v ceně odpovídající části předmětu dodávky.

2 POPIS PLNĚNÍ POŽADAVKŮ TECHNICKÉ SPECIFIKACE NA DODÁVKU

V této kapitole je uveden detailní popis funkčních vlastností nabízeného plnění ve struktuře a rozsahu uvedených v kapitole 3 Přílohy 5 - Technická specifikace.

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v této kapitole.

2.1.1 Obecné a společné požadavky

#	Požadavek
P.1	Dodávaný systém musí svojí architekturou splňovat obecné zásady informační bezpečnosti v míře, odpovídající charakteru užití a kategorii zpracovávaných dat (GDPR).
P.2	Veškeré nabízené SW i HW prvky musí být plně kompatibilní se stávajícími systémy uvedenými v kap. 6.4 – Stav informačních a komunikačních technologií.
P.3	Součástí implementace musí být i veškeré potřebné licence a služby nezbytné pro dodávku a provoz EA, SW a HW prvků.
P.4	Zaručená perspektiva provozu, rozvoje a podpory je minimálně po dobu dalších 10 let od uvedení do provozu.
Legislativa a další normy	
P.5	Soulad s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR – General data protection regulation) v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
P.6	Soulad se Zákonem č. 110/2019 Sb., o ochraně osobních údajů a o změně některých dalších zákonů, ve znění pozdějších předpisů.
P.7	Soulad se Zákonem č. 181/2014 Sb., o kybernetické bezpečnosti v aktuálním znění a vyhláškou Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti v aktuálním znění.
P.8	Soulad se Zákonem č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů v aktuálním znění.
P.9	Soulad se Zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
P.10	Soulad se Zákonem č. 499/2004 Sb., o archivnictví a spisové službě, ve znění zákona č. 190/2009 Sb.
P.11	Soulad s Národním standardem pro elektronické systémy spisové služby, vyhlášený Ministerstvem vnitra dle zmocňovacího ustanovení Zákona o archivnictví a spisové službě.
P.12	Soulad se Zákonem č. 372/2011 Sb., o zdravotních službách, v rámci tohoto projektu zajištění primárního souladu s: <ol style="list-style-type: none"> podmínky vedení ZD: zajištěna neměnnost provedených záznamů, veden seznam identifikátorů záznamů, bezpečnostní kopie každý den, archivní kopie každý rok, migrace formátů a datových nosičů, výstupy autorizovanou konverzí nahlížení do ZD, výpisy a kopie: široká škála osob, které smí nahlížet do ZD, pacient má právo nahlížet, obdržet kopii, o nahlížení a kopii je nutno vést záznamy

#	Požadavek
P.13	Soulad s Vyhláškou č. 98/2012 Sb., o zdravotnické dokumentaci, v rámci tohoto projektu zajištění primárního souladu s: <ol style="list-style-type: none"> vymezením obsahu ZD – ZD zahrnuje také výsledky vyšetření včetně grafických, audiovizuálních, digitálních nebo jiných pravidly pro skartační řízení
P.14	Dokumentace bude v souladu se zákonem č. 365/2000 Sb. o informačních systémech veřejné správy a prováděcích právních předpisů, v platném znění.
Ostatní obecné požadavky	
P.15	Zajištění jednotného času na všech pracovištích/zařízeních (synchronizace klientů a systému s Objednatelem určeným time serverem).

Tabulka 2: Obecné požadavky

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

Pro konkrétní oblasti jsou uvedeny specifické požadavky samostatně v dílčích podkapitolách.

2.1.2 Dodávka elektronického archivu (EA)

Požadavky na tuto část předmětu plnění jsou následující:

#	Požadavek
P.16	Dodávka dlouhodobého bezpečného důvěryhodného elektronického archivu pro archivaci elektronické zdravotnické dokumentace a ostatní dokumentace v souladu s legislativou.
P.17	EA musí zajistit minimálně následující služby: <ol style="list-style-type: none"> uložení a fyzické zabezpečení dokumentů/dat, validace (opatření časovým razítkem na úrovni dokumentu, případně denní sady dokumentů, pro které je prováděno ověření platnosti elektronického podpisu), uchovávání a prokazování platnosti a věrohodnosti podpisů a časových razítek, přístup k uloženým dokumentům přes integrační i aplikační rozhraní, ověřování uživatelů přes MS Active Directory Objednatele a zajištění přístupu k dokumentům jen oprávněným uživatelům a systémům, skartace dokumentů <p>Upřesňující požadavky následují.</p>
P.18	Řešení musí na aplikační úrovni disponovat mechanismy, které zajistí uložení dat ve shodě s národními normami pro důvěryhodné uložení dat a organizačními směrnicemi a nařízeními. <ol style="list-style-type: none"> eIDAS – nařízení Evropské unie č. 910/2014 Zákon č. 297/2016 Sb., Zákon o službách vytvářejících důvěru pro el. transakce Zákon č. 499/2004 Sb., Zákon o archivnictví a spisové službě a o změně některých zákonů Národní standard pro vedení elektronického systému spisové služby NSESSS

#	Požadavek
	Tato schopnost bude doložena certifikátem shody s výše uvedenými normami vydaným akreditovaným subjektem.
P.19	Řešení musí být plně v souladu s platnou legislativou ohledně vedení zdravotnické dokumentace v elektronické podobě a ochrany osobních údajů (viz jiné části tohoto dokumentu).
P.20	Ukládání elektronické dokumentace vzniklé v rámci provozu ZZS do EA prostřednictvím: <ol style="list-style-type: none"> 1. datového (integračního) rozhraní – napojení EZD, možnost budoucího napojení dalších vnitřních, nyní neintegrovaných IS. 2. Aplikační (GUI) rozhraní pro uživatele. <p>Umožňující archivovat i ostatní druhy elektronických dokumentů z dalších perspektivních systémů či agend ZZS HMP (smlouvy, ekonomické, personální a další interní dokumenty organizace).</p> <p>Tato vlastnost je požadována na stupni schopnosti konzumace validního elektronického dokumentu, opatření metadaty, zaručení jeho neměnnosti a prokazatelnosti a vyhledání relevantního záznamu v rozsahu poskytnutých metadat.</p>
P.21	Archivované elektronické dokumenty musí být důvěryhodné a musí mít po formální i po obsahové stránce stejně trvalou důkazní hodnotu jako papírové. <p>Dlouhodobé důvěryhodné uchování jednotlivých prvků, které mohu být v budoucnu použity jako důkazní materiál k danému elektronickému dokumentu (certifikáty, pečete, včetně certifikačních cest, CRL, OCSP).</p>
P.22	Dlouhodobá archivace elektronických dokumentů a zajištění jejich právní validity.
P.23	Validace platnosti bezpečnostních prvků (elektronické podpisy, elektronické pečete a časová razítka) založených na kvalifikovaných certifikátech. Zadavatel připouští z důvodu minimalizace nákladů na časová razítka metodu validace na úrovni ověření denní množiny dokumentů, opatřených elektronickým podpisem při zajištění prokazatelného a nezaměnitelného journal takto validované skupiny dokumentů. Další podmínkou použití této metody je implementace nástroje pro prokázání důvěryhodnosti a nezaměnitelnosti takto archivovaných dokumentů.
P.24	Možnost nastavení požadované úrovně důvěry při ověřování platnosti bezpečnostních prvků (uznávány, kvalifikovaný podpis/pečet).
P.25	Funkce fixace dokumentu formou elektronické pečete/podpisu a/nebo časového razítka. Ověřování elektronické značky/podpisu/pečete a/nebo časového razítka.
P.26	Ověřování certifikátů, na nichž jsou založeny elektronický podpis/značka/pečet, časové razítko.
P.27	Opatření dokumentů, případně skupiny dokumentů, časovým razítkem. Zajištění periodického prodloužení validity formou automatického přerazítkování.
P.28	Získávání a uchovávání všech relevantních důkazů validity uloženého dokumentu.
P.29	Archivace dokumentů v archivních balíčcích určených pro dlouhodobou archivaci včetně opatření časovým razítkem. Možnosti sdružování libovolných dokumentů do archivních balíčků. <p>Elektronické dokumenty je možné balíčkovat nezávisle na jejich typu, významu, různých přístupových právech a bez jejich vzájemného vztahu. Systém umožňuje mazání jednotlivých dokumentů z balíčku, bez narušení možnosti prokázat důvěryhodnost ostatních dokumentů z balíčku.</p>

#	Požadavek
P.30	<p>Elektronická zdravotnická dokumentace z EZD (viz kap. 3.4.3) bude archivována v balíčcích po kalendářních dnech (jeden balíček bude obsahovat veškerou dokumentaci z daného kalendářního dne). Balíček bude opatřen časovým razítkem. V případě, že v daném dni nebude žádná dokumentace, balíček nebude vytvořen.</p> <p><i>Poznámka: Zajištění použití kvalifikovaných certifikátů s platností minimálně celého dotčeného dne je součástí úprav systému EZD.</i></p>
P.31	<p>Ostatní dokumentace bude archivována jednotlivě nebo v balíčcích dle typu dokumentu, dokument nebo balíček budou opatřeny časovým razítkem.</p> <p>Ostatní dokumentaci bude možné nahrát přes webové rozhraní po jednotlivých souborech, či hromadě (např. vybráním adresáře, či jednorázovým výběrem více souborů). Při tomto nahrání bude možné vybrat šablonu metadat (smlouva, faktura, pracovní výkaz atd.), nebo metadata zadat ručně bez výběru předdefinované šablony. Takto nahraná data budou opatřena právě jedním časovým razítkem (bez ohledu na počet nahraných dokumentů) v okamžiku odeslání dat uživatelem k archivaci. O stavu nahrání (úspěch, neúspěch) bude uživatel interaktivně informován.</p>
P.32	<p>Systém EA umožní tvorbu šablon metadat (smlouva, faktura, pracovní výkaz atd.), které uživatelům předvyplní metadata k často využívaným typům dokumentů. Tyto šablony bude možné uživatelsky vytvářet na základě definované role.</p>
P.33	<p>V případě, že z jakéhokoliv důvodu nebude možné nahrát celou dávku dokumentů, či vybraný dokument v této dávce, zašle systém notifikaci na definovanou distribuční skupinu (v případě zdravotnický dat), či tuto skutečnost oznámí přímo uživateli, který dokument(y) nahrál přes webové rozhraní.</p> <p>Pokud problém vznikne kvůli jednotlivým dokumentům v dávce, budou tyto dokumenty vyjmuty z dávky a zbytek dávky se odešle do archivu. Problematické dokumenty pocházející z EZD budou po odstranění vady systémem automaticky zpracovány v rámci následující denní dávky. Problematické dokumenty nahrávané přes webové rozhraní budou uživateli vráceny s uvedením důvodu nemožnosti jejich zpracování.</p>
P.34	<p>Řešení umožňuje řízení procesu tvorby balíčků dle různých archivačních politik a charakteru dokumentů jednotlivých agend (více podpisů s různou časovou platností).</p>
P.35	<p>Udržování ověřitelnosti bezpečnostních prvků elektronického dokumentu v čase, tak aby byla realizována aktivní péče o elektronické dokumenty, které zabezpečuje jejich dlouhodobou platnost (digitální kontinuita).</p>
P.36	<p>Poskytování důkazního materiálu pro prokázání platnosti uloženého elektronického dokumentu. Důkazní materiál je poskytován k jednotlivým elektronickým dokumentům bez ohledu na ostatní dokumenty v balíčku, bez jejich kompromitace a bez ohledu, zda v čase poskytnutí důkazního materiálu existují.</p>
P.37	<p>Archivace dokumentace zajistí dlouhodobé a důvěryhodné uložení elektronických dokumentů a specifické funkce podle zákona č. 499/2004 Sb., o archivnictví a spisové službě, vyhlášky 259/2012 Sb., o podrobnostech výkonu spisové služby, Národního standardu pro elektronické systémy spisové služby (NSESSS) a podle úrovně technického řešení problematiky obvyklého v Evropské unii.</p>

#	Požadavek
P.38	<p>Systém musí zajistit dlouhodobé uložení dokumentů a zajištění čitelnosti uložených informací do doby jejich skartace.</p> <p>Systém musí zajistit důvěryhodné uložení elektronických dokumentů včetně jejich metadat.</p>
P.39	<p>Archiv musí podporovat ukládání a zpřístupňování dokumentace ve formě textových, grafických, audiovizuálních, digitálních nebo jiných obdobných záznamů.</p>
P.40	<p>Systém musí umožňovat archivaci a zobrazování zdravotnické dokumentace ve formátu PDF/A (A-1 – A-3). Mimo zdravotnickou dokumentaci možnost zpracování a archivace libovolných formátů dokumentů.</p>
P.41	<p>Možnost konverze ukládaných dat do formátu PDF/A (A-1 – A-3).</p>
P.42	<p>Ověřování všech AdES formátů podpisů.</p>
P.43	<p>Univerzální archivační systém umožňující napojení stávajících i v budoucnu pořízených produkčních systémů spravujících a pořizujících zdravotnickou, případně jinou dokumentaci k archivaci.</p> <p>Zajištění integračního rozhraní pro napojení dalších produkčních systémů a archivaci dat (dokumentů) z nich dle platné legislativy včetně jeho přesného detailního popisu umožňující využít integrační rozhraní bez nákupu služeb dodavatele.</p> <p>Automatizované ukládání dokumentů ze zdrojových IS pomocí webových služeb.</p>
P.44	<p>Musí být podporovány standardy pro výměnu (zdravotnické) dokumentace HL7, DASTA, SOAP, PDF/A (A-1 – A-3).</p>
P.45	<p>Elektronická zdravotnická dokumentace v EA bude identifikována také bezvýznamovým identifikátorem, který bude poskytován z jiných částí IS ZZS. EA nebude pracovat pouze s identifikací pacienta (RČ, číslo pojištěnce), ale primárně s předaným bezvýznamovým identifikátorem.</p> <p>Vyhledávání a zpracování archivované zdravotnické dokumentace pacienta přes jeho identifikaci bude řešeno v EZD.</p> <p>Systém EA musí být plně připraven na přechod identifikace pacienta pomocí bezvýznamového identifikátoru po legislativním zavedení takového požadavku.</p>
P.46	<p>Možnost automatizované konverze dat do průmyslových standardů, které budou v budoucnosti požadovány.</p>
P.47	<p>Řešení musí umožnit pracovat se všemi formáty rozšířeného elektronického podpisu (AdES).</p>
P.48	<p>Systém musí zajistit automatické transformace dokumentů k zajištění dlouhodobé archivace.</p>
P.49	<p>Uživatelsky nastavitelná archivační a skartační pravidla pro jednotlivé typy dokumentů. Nastavení archivačních a skartačních pravidel dle požadavků objednatele v rámci dodávky.</p>
P.50	<p>Řízená skartace dle legislativy a skartačního řádu objednatele. Systém musí umožňovat také řízenou skartaci postavenou dle platných předpisů, která na základě metadat určují životnost dokumentu a termín jeho skartace a dále protokoly o uskutečněných skartacích.</p>
P.51	<p>Elektronický archiv disponuje minimálně následujícími funkcemi:</p> <ol style="list-style-type: none"> 1. Příjem SIP balíčku

#	Požadavek
	<ol style="list-style-type: none"> 2. Parametrizovatelné sestavení skartačního návrhu 3. Manuální sestavení skartačního návrhu jen z vybraných entit 4. Vyjmutí určených entit ze skartačního návrhu 5. Schválení skartačního návrhu 6. Export entit zahrnutých ve skartačním návrhu ve formě SIP bez komponent dle NSESSS pro potřeby provedení skartačního řízení v nadřazeném archivu původce 7. Hromadné i jednotlivé generování SIP pro všechny entity zařazené ve skartačním návrhu, nebo pro jednotlivé vybrané entity 8. Načtení a zpracování odpovědní dávky (vytvořené dle požadavků a technické struktury NSESSS) z nadřazeného archivu 9. Export entit ve formě SIP včetně komponent pro uložení v nadřazeném archivu 10. Vymazání dokumentů a spisů, které prošly skartačním řízením 11. Vyhledávání a prohlížení historie provedených skartačních řízení.
P.52	Dokument lze smazat pouze auditovatelným způsobem, smazání bude zaznamenáno do logů v rámci auditních služeb (viz kap. 3.4.6).
P.53	<p>Systém musí zahrnovat uživatelské rozhraní pro vkládání a přístup k dokumentaci provozované ve webovém prohlížeči bez nutnosti instalovat přídatné moduly či rozšíření.</p> <p>Uživatelské rozhraní kompatibilní s prostředím objednatele.</p>
P.54	Možnost vyhledávat dokumenty dle metadat dokumentů prostřednictvím uživatelského rozhraní.
P.55	Možnost náhledu na archivované dokumenty prostřednictvím uživatelského rozhraní. Řešení musí umožnit náhled na dokument minimálně těchto formátů: PDF, PDF/A (A-1 – A-3), MS Office (DOC, DOCX, PPT, PPTX, XLS, XLSX, RTF), JPG, GIF, PNG, XML.
P.56	Možnost manuálního (neautomatizovaného) vkládání dokumentů uživatelem přes aplikační rozhraní (GUI).
P.57	<p>Řešení musí být napojeno na MS Active Directory Objednatele:</p> <ol style="list-style-type: none"> 1. Synchronizace seznamu uživatelů z MS Active Directory do EA. Uživatelé EA budou zařazeni do definované skupiny v MS AD, načítat se budou jen uživatelé zařazení do skupiny určené pro EA. Systém musí umožnit rekurzivní prohledávání skupin. 2. Synchronizace uživatelů bude probíhat v nastavitelném intervalu nebo bude možné definovat čas, kdy bude prováděna synchronizace nebo možnost ručního vynucení synchronizace správcem. Výchozí nastavení na bude synchronizace každou 1 hodinu. 3. Uživatelé se do EA budou přihlašovat svým komerčním certifikátem nebo dočasným heslem (viz požadavek P.59). 4. Zamezení přístupu uživateli do EA, který není v MS Active Directory aktivní, není členem definované skupiny, nebo byl v MS AD smazán. Není požadováno smazání uživatele, ale jen zamezení přístupu (min. na úrovni přihlášení). Důvodem je zachování návaznosti dat a logů na uživatele. 5. V případě deaktivace účtu v MS AD a jeho následně aktivace se tyto změny musí projevit v EA při zachování všech oprávnění a historických dat. 6. V MS AD budou uživatelé zařazení jen v příslušné skupině, konkrétní oprávnění rolí bude nastaveno ve EA.

#	Požadavek
	<ol style="list-style-type: none"> 7. Pokud bude uživatel jen ve skupině MS AD pro přístup do EA, ale v EA mu nebudou nastavena konkrétní oprávnění, bude mu umožněno přihlášení, ale nebude mít k dispozici data a funkcionality. 8. Počet neúspěšných přihlášení do webového rozhraní musí být omezen na 5 pokusů a následně bude účet uzamčen a odemčení bude moct provést pouze správcem systému. 9. Možnost odblokování uživatele správcem. 10. Integrace na MS AD Zadavatele bude realizována pomocí MS Azure, nebo ADFS (Active Directory Federation Services) a tato komunikace bude šifrována. Systém musí podporovat obě varianty a konečný způsob ověřování bude řešen v rámci analýzy a návrhu řešení.
P.58	Přebírání veřejných klíčů komerčních certifikátů uživatelů ze sdíleného úložiště certifikátů (viz kap. 3.4.3) pro potřeby autentizace uživatelů v EA.
P.59	<p>Autentizace/přihlašování uživatelů do EA:</p> <ol style="list-style-type: none"> 1. Komerčními certifikáty (primární způsob autentizace): <ol style="list-style-type: none"> a. Prostřednictvím komerčního certifikátu uloženého na kvalifikovaných prostředcích ve standardu QESCD. b. Kvalifikované prostředky budou připojeny z PC/notebooku prostřednictvím USB. c. Veřejný klíč komerčního certifikátu bude převzat z úložiště certifikátů, které je součástí dodávky (viz požadavek P.79). 2. Dočasným heslem: <ol style="list-style-type: none"> a. Zavedení provozního módu pro práci při absenci certifikátu pro přihlášení (např. zapomenuté úložiště pro certifikáty). b. Systém musí umožňovat vygenerovat pro uživatele dočasné přístupové heslo (automatický proces) a to na základě inicializace této žádosti uživatelem v rámci GUI EA. Toto heslo bude zasláno na email uživatele (vnitřní email Objednatele – z AD), který do EA přistupuje (přihlašuje se). Platnost takto generovaného hesla musí být parametrizovatelná správcem. Vygenerované heslo bude mít vlastnost povinné změny při prvním použití. Tuto funkcionalitu lze zajistit buď pomocí mailového serveru Objednatele (bude přístupné rozhraní vyžadující autentifikaci), či pomocí vlastního systému dodavatele (nesmí se jednat o mailové služby sloužící k rozesílání newsletterů). c. Počet pokusů zadání dočasného hesla bude omezen, aby se zabránilo neoprávněnému přístupu do aplikace. Po opakovaném chybném zadání hesla (počet pokusů bude konfigurovatelný parametr správcem aplikace) bude příslušný účet zablokován. O této události bude systémem informován správce EA (notifikace na definovaný email), který bude moct vzdáleně příslušný účet odblokovat a vygenerovat nové dočasné heslo.
P.60	Řešení musí umožňovat nastavení a řízení přístupových práv dle rolí uživatele a jeho organizačního zařazení v rámci svého nástroje pro správu oprávnění.
P.61	Řešení nesmí být licenčně omezeno na počet nebo typ připojených produkčních systémů; typ archivované dokumentace; počet dokumentů, počet uživatelů nebo zobrazovacích stanic.
P.62	Datové úložiště musí být dimenzováno na 4 roky provozu a umožňovat následné budoucí rozšíření o další prostory.

#	Požadavek
	<p>Úložiště musí umět růst společně s růstem množství ukládaných dat bez nutnosti migrace dat na nové technologie.</p> <p>Musí umět adaptovat nové technologie za chodu (růst kapacity disků, zvyšování rychlosti infrastruktury apod.) Při rozšiřování se nesmí měnit způsob ukládání, není tedy třeba modifikovat aplikaci. Musí umožňovat bezproblémovou a dlouhodobou rozšiřitelnost realizovatelnou bez ohrožení uložených dat.</p>
P.63	Rozšiřitelnost – EA umožní bezproblémovou a dlouhodobou rozšiřitelnost realizovatelnou bez ohrožení uložených dat.
P.64	Replikace dat – EA musí být vybaveno systémem pro replikaci dat. Sekundární, případně n-tá lokalita musí být schopna dočasně převzít veškeré funkce lokality primární, jak z pohledu přístupu k uloženým dokumentům, tak z pohledu ukládání nových dokumentů.
P.65	<p>Auditování a logování provozu jednotlivých prvků systému a možnost vyhodnocování min. 1 rok zpětně.</p> <p>Zabezpečení tzv. auditní stopy, řešení automatizovaných činností počínaje označováním dokumentů elektronickými značkami, časovými razítky, jejich validací apod.</p> <p>Auditní záznamy a logy zpřístupňovat ve strukturované formě s parametrizací zadání pro obsah auditního záznamu / logu pro definovanou roli.</p>
P.66	Možnost exportu archiválií do souborového systému jednotlivě nebo hromadně.
P.67	<p>Vstupní konektory:</p> <ol style="list-style-type: none"> 1. standardní vstupní rozhraní SOAP/REST nebo REST pro příjem požadavků, 2. možnost ovlivnit chování vstupního rozhraní konfigurací (skriptem), např. pro účely orchestrace s dalšími IS (např. ve formě volání jiného IS), 3. možnost ručního vkládání dokumentů (např. ze souborového systému).
P.68	<p>Centrální mezipaměť (cache)</p> <ol style="list-style-type: none"> 1. uložení často používaných dokumentů pro rychlý přístup 2. v případě nedostupnosti cílového úložiště dočasně dokument pocházející z EZD (denní dávka) i s metadatami uchová a uloží do cílového úložiště při jeho opětovné dostupnosti
P.69	Komprese ukládaných dokumentů
P.70	<p>Centrální monitorování sleduje stav/výkon integračních procesů:</p> <ol style="list-style-type: none"> 1. stav a výkon integrace s dokumentovými úložišti, 2. stav sítě, dostupnost a odezva jednotlivých koncových zařízení, 3. stav/výkon aplikačních serverů – odezva, kapacita (paměť, diskový prostor).
P.71	Řešení musí umožnit napojeným IS pracovat s dokumenty z různých typů dokumentových úložišť, jako např. ze systémů pro správu dokumentů (DMS/ECM), souborových systémů (ať už lokálních, nebo vzdálených NFS/CIFS), objektových úložišť, úložišť typu NAS, CAS a jiných specializovaných hardwarových úložišť.
P.72	Řešení musí vycházet z referenčního modelu OAIS a být založeno na rozdělení systému elektronické archivace na dvě základní části řešení: logická (softwarová) část starající se o procesy v archivu a fyzická (hardwarová) část starající se o bezpečné uložení dat.

#	Požadavek
P.73	Podpora definování intervalů, po které není možné dokument smazat ani nijak pozměnit (retenční doba).
P.74	<p>Dodávka časových razítek:</p> <ol style="list-style-type: none"> Pro potřeby dodávky do doby předání a akceptace plnění v objemu na 100 dnů (mezi fázemi 5 až 10 harmonogramu dle kap. 4), tj. <ol style="list-style-type: none"> Časová razítka pro balíčky elektronické zdravotnické dokumentace: 100 ks Časová razítka pro ostatní dokumentaci: 100 ks Pro potřeby provozu od doby předání a akceptace plnění je součástí servisních služeb uvedených v samostatném dokumentu. <p>Účtována budou jen a pouze skutečně spotřebovaná časová razítka.</p>
P.75	Správa uživatelských účtů, certifikátů a jejich propojení v návaznosti na úložiště a správu certifikátů požadovaném v kap. 3.4.3
P.76	Systém musí být připraven na provoz 24x7x365 (non-stop).

Tabulka 3: Požadavky: Dodávka elektronického archivu organizace (EA)

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.3 Úpravy a napojení EZD na elektronický archiv

Požadavky na tuto část předmětu plnění jsou následující:

#	Požadavek
Integrace na IS ZOS	
P.77	<p>Doplnění údajů ze záznamu operátora k tísňové výzvě přenášených mezi IS ZOS a EZD o datum, čas a pořadové číslo tísňového volání.</p> <p>Údaje budou přenášeny v rámci stávající integrace z IS ZOS do EZD, která bude jen rozšířena o uvedené údaje.</p> <p>Totožný požadavek na IS ZOS je požadavek P.93.</p>
Certifikáty	
P.78	Neumožnit elektronicky podepsat dokument v definovaný počet dnů před koncem platnosti kvalifikovaného certifikátu. Bude se jednat o systémový parametr, výchozí hodnota bude 1 den před koncem platnosti.
Úložiště a správa certifikátů	
P.79	<p>Změna ukládání komerčních certifikátů v EZD:</p> <ol style="list-style-type: none"> Vyčlenění úložiště komerčních certifikátů z EZD do samostatného úložiště. Migrace stávajících certifikátů z EZD do nově vytvořeného úložiště. Změna ukládání certifikátů ze správcovského nástroje EZD do nově vytvořeného úložiště při zachování všech stávajících kontrol a funkcí správcovského nástroje.

#	Požadavek
	<ol style="list-style-type: none"> 4. Vytvoření integračního rozhraní pro čtení certifikátů vnitřními systémy ZZS. Zajištění čtení z integračního rozhraní na základě oprávnění daného IS. 5. Úprava čtení certifikátů v EZD na primární zdroj v nově vytvořeném úložišti. 6. Toto úložiště bude umístěné do DMZ Objednatele a umožněn přístup pouze pro konkrétní veřejné IP adresy (subnet).
Archivace dokumentace	
P.80	<p>Vytváření a předávání následujících typů dokumentů do EA:</p> <ol style="list-style-type: none"> 5. Záznam o výjezdu od posádky (jen elektronicky podepsaný originál). 6. Záznam o výjezdu po zpracování a podpisu oddělením kontrolingu – po provedených úpravách, včetně skenu záznamu o výjezdu od posádky, automatizované vytvoření a vyžádání podpisu uživatele. 7. Pokud v rámci vykazování péče zdravotním pojišťovněm dojde ke změně údajů pacienta, bude vytvořen a podepsán aktualizovaný záznam o výjezdu (doplnění funkčnosti do modulu pojišťovny). 8. Veškeré ostatní elektronicky podepsané dokumenty systému EZD, tvořící soubor zdravotnické dokumentace. <p>Dokumenty mohou vznikat opakovaně, v případě, že budou prováděny úpravy zdrojových dat v rámci kontrolních procesů na straně ZZS nebo zdravotních pojišťoven.</p> <p>Pokud vznikne dokument opakovaně, bude do EA vložen jako nová verze téhož typu dokumentu.</p>
P.81	<p>Součástí archivace dokumentů budou vždy i samostatné změnové logy (change list) nového stavu dokumentu oproti prvotnímu záznamu o výjezdu od posádky. Změnové logy budou obsahovat min. seznam změn údajů, tj. původní hodnotu, novou hodnotu, datum a čas změny, autora změny.</p> <p>V rámci změnového logu budou vizuálně označeny okamžiky vytvoření a archivace dokumentace a tím odděleny změny v různých typech a verzích dokumentace.</p>
P.82	<p>Součástí předávané dokumentace mohou být i nepodepsané přílohy, např. PDF, multimediální dokumentace (obrázky, videa, zvukový záznam) apod.</p>
P.83	<p>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.</p>
P.84	<p>Součástí archivované dokumentace budou následující údaje (metadata):</p> <ol style="list-style-type: none"> 6. Identifikace výjezdu, datum a čas výjezdu, pořadové číslo výjezdu. 7. Bezvýznamový identifikátor pacienta – v rámci EA nebude mít význam, bude se jednat o identifikátor z EZD, který nebude rodným číslem. 8. Datum a čas vzniku dokumentu. 9. Autor dokumentu (identifikace uživatele) 10. Identifikace vozidel v rámci výjezdu (může být více vozidel) <p>V rámci implementační analýzy může dojít k doplnění metadat na základě procesních potřeb archivace.</p>
P.85	<p>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.</p>

#	Požadavek
P.86	Doplnění systému EZD o možnost vyhledání a následného podepsání dokumentu definovanou autoritou pro případy vypršení platnosti elektronických podpisů na dokumentu a jejich předání do EA (ošetření stavu výpadku spojení EA s EZD spojeném s vypršením platnosti certifikátu). EA tedy poskytne nástroj, který tyto dokumenty na vyžádání vypíše, případně pro každý takový dokument zašle notifikaci na předem definovaný distribuční seznam.
Práce s archivovanou dokumentací	
P.87	V EZD udržovat validní odkaz na dokumenty v EA.
P.88	Možnost zobrazit přehled archivované dokumentace k výjezdu v EZD (pouze na úrovni EKP).
P.89	Možnost vyhledávání v archivované dokumentaci dle uložených metadat (viz požadavek P.84).
P.90	Udržování kopií archivovaných dokumentů v EZD po dobu min. 3 roky (konfigurovatelný parametr systému). Po této době odmazání dokumentů z EZD a možnost jen odkazování do EA.
P.91	Při požadavku na zobrazení dokumentu v EZD, primárně zobrazovat z EZD, pokud již není v EZD uloženo, upozornit uživatele na možnou delší dobu stažení dokumentu a následně stáhnout dokument z EA do dočasného úložiště EZD. Pokud je dokument již stažen do dočasného úložiště EZD, nestahovat opakovaně a zobrazit z tohoto dočasného úložiště. Takto stažené dokumenty automaticky mazat po 5 dnech od jejich posledního zobrazení. Doba uložení bude konfigurovatelný parametry, výchozí hodnota bude 5 dnů.
Ostatní požadavky	
P.92	Archivace dokumentace a práce s archivovanou dokumentací musí být realizována tak, aby výpadek EA neměl negativní dopad na poskytování ostatních služeb EZD.

Tabulka 4: Požadavky: Úpravy a napojení EZD na elektronický archiv

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.4 Úpravy IS ZOS pro poskytnutí kompletních dat do EZD pro následnou archivaci

Požadavky na tuto část předmětu plnění jsou následující:

#	Požadavek
P.93	Doplnění údajů ze záznamu operátora k tísňové výzvě přenášených mezi IS ZOS a EZD o datum, čas a pořadové číslo tísňového volání. Údaje budou přenášeny v rámci stávající integrace z IS ZOS do EZD, která bude jen rozšířena o uvedené údaje. Totožný požadavek na EZD je požadavek P.77.
P.94	Úprava musí být realizována tak, aby výpadek EA nebo EZD neměl negativní dopad na poskytování ostatních služeb IS ZOS.

Tabulka 5: Požadavky: Úpravy IS ZOS pro poskytnutí kompletních dat do EZD pro následnou archivaci

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.5 Dodávka nezbytné provozní infrastruktury a systémového SW pro dodávané systémy

V následující tabulce jsou uvedeny min. parametry pro dodávku infrastruktury (HW a systémového SW):

#	Požadavek
P.95	Infrastruktura pro IS ZOS zůstane beze změny, úpravy musí být funkční a provozované společně se stávajícím systémem na stávající infrastruktuře IS ZOS.
P.96	Infrastruktura pro EZD zůstane beze změny, úpravy musí být funkční a provozované společně se stávajícím systémem na stávající infrastruktuře EZD.
P.97	EA bude provozován jako dvě instance služby. Instance budou provozovány v režimu aktivní/pasivní, kdy v provozu bude vždy jedna lokalita, druhá bude připravena převzít služby v případě výpadku aktivní lokality.
P.98	EA bude umístěn a provozován v rámci cloudových služeb formou IaaS (Infrastruktura jako služba), které zajistí dodavatel a to včetně provozu těchto služeb po dobu dodávky a poskytování provozních a servisních služeb dle servisní smlouvy. <i>Upozornění: Poskytovatel cloudových služeb, který zajišťuje prostředky a platformu a jedná jménem zákazníka cloudových služeb, se považuje za zpracovatele údajů. Dodavatel podáním nabídky stvrzuje, že s tímto souhlasí a bude se řídit platnou legislativou ČR/EU.</i>
P.99	Cloudové služby budou zajištěny a provozovány v zemích EU/EHP, umístění ani přesun mimo země EU/EHP není přípustný z důvodu ochrany osobních údajů uložených v systému. <i>Dodavatel v rámci dodávky a následně poskytování servisních služeb poskytne objednateli informace o lokalitě umístění EA a to při každé změně, případně na vyžádání.</i>
P.100	Datové centrum, kde budou umístěny Cloudové služby musí mít dostatečné fyzické zabezpečení, stejně tak ochranu proti výpadkům napájení, či případným kybernetickým útokům a splňovala standardy ISO 27001, 27017 a 27018.
P.101	Zajištění úplné sady cloudových služeb pro provoz dodávaného řešení v souladu s požadavky uvedenými v tomto dokumentu a nároky navrhovaného SW řešení, tj. běhové prostředí/platformu, servery, virtuální servery, kapacita úložiště pro data (viz kap. 6.2, 6.3), vysokou dostupnost, zálohování a další služby nezbytné pro řešení dodavatele.
P.102	Kapacita úložiště pro data a požadavky na datové přenosy budou stanoveny dodavatelem dle parametrů uvedených v kap. 6.2, 6.3 a nároků a potřeb jeho řešení. Součástí dodávky je kapacita úložiště a datové přenosy na období dodávky a následně na 4 roky provozu (úhrada v rámci provozu bude v rámci servisní smlouvy).
P.103	Dodávka OS pro servery umístěné v rámci cloudových služeb, včetně instalace do prostředí cloudových služeb, vč. potřebných licencí, pokud se jedná o licencovaný OS.
P.104	Dodávka a instalace SW databází (DB): Pokud řešení vyžaduje dodávku licencovaného SW pro DB, jsou součástí dodávky i licence těchto DB (např. ORACLE, MS SQL).

#	Požadavek
P.105	Dodávka a instalace jiného systémového SW, pokud jej řešení dodavatele vyžaduje, součástí dodávky jsou i licence tohoto systémového SW, pokud se jedná o licencovaný SW.
P.106	Pokud pro provozování systému bude Poskytovatel potřebovat pomocný server v DMZ Objednatele (např. pro zajištění komunikace mezi cloudovými službami a interní sítí Objednatele), tak součástí dodávky je i zajištění potřebných licencí SW pro tento server a jeho konfigurace. Tento server musí splňovat všechny požadavky (bezpečnostní, na audit atd.), které jsou kladeny na systém jako celek (nesmí zde vzniknout slabý článek dodávaného systému).
P.107	Prostředí pro Systém musí zajistit zabezpečené připojení jak integrovaných systémů, tak uživatelů Systému přes internet min. na úrovni SSL. <i>Poznámka: dostatečnou kapacitu linky zajistí objednatel na min. garantované úrovni 20 Mbit/s symetricky.</i>
P.108	Prostředí, kde je provozován Systém bude s DC Objednatele propojeno s využitím Site-to-Site VPN. Dodavatel zajistí technologii na straně Cloudového systému.
P.109	Na všech serverech bude nastaveno dostatečné zabezpečení dle Best Practices výrobce SW, jak na úrovni šifrování (pouze bezpečné šifrovací algoritmy a protokoly), na úrovni komunikace (zakázání nepoužívaných a málo bezpečných služeb), tak i síťového provozu (omezení komunikace pro předem definované rozsahy adres).
P.110	Šifrování úložišť v rámci operačních systémů, kde jsou uložena data systému.
P.111	Dodávka, zapojení, instalace technologií, instalace a zprovoznění modernizovaného IS na dodaných technologiích.
P.112	Objednatel připouští registraci cloudových služeb na Objednatele v rámci dodávky a servisních služeb, nicméně úhrada za služby po dobu dodávky a platnosti servisní služby bude poskytovateli prováděna dodavatelem (cena za provoz systému dle uzavřené servisní smlouvy bude konečná)
P.113	Součástí nabídky bude popis konfigurace a umístění cloudových služeb v rozsahu, umožňujícím ověření splnění uvedených požadavků.
P.114	Součástí nabídky bude i seznam osob dodavatele a systémů, které mají jakýkoliv přístup k poskytovaným zdrojům a systémům a na jaké úrovni. Tento seznam bude udržován aktuální o celou dobu dodávky dle SoD a poskytování služeb dle servisní smlouvy. <u>Doplnění požadavku dodavatelem v rámci nabídky:</u> <u>V době dodávky bude mít k systému přístup tým dodavatele tj. následující osoby</u> <u>xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx</u> <u>V průběhu poskytování servisních služeb bude seznam osob udržován v aktuální podobě</u>
P.115	Poskytovatel bude v rámci služeb poskytovat reporty SOC 3.

Tabulka 6: Požadavky: Dodávka nezbytné provozní infrastruktury a systémového SW pro dodávané systémy

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.6 Auditní služby

Požadavky na tuto část plnění jsou následující:

#	Požadavek
P.116	Dodávané systémy a technologie umožní provádět audity užití na základě interních logů aplikace, které zaznamenávají a ukládají údaje o změnách či nahlížení na osobní údaje podle identity uživatelů.
P.117	Řešení umožní poskytovat auditní reporty o přístupech uživatelů (kdo, kdy, období, kam) na základě parametrizace prováděné pověřeným auditorem.
P.118	Auditní (logovací) aparát je dostupný pouze určené roli (auditor). Není dostupný a manipulovatelný uživateli, administrátory ani správci.
P.119	Systém musí umožnit automatizované i manuální vystoupení logových záznamů do externích systémů pro správu logů (log management, SIEM) a do tabulek MS Excel (.csv, .xlsx)
P.120	Auditní systém musí být v souladu s nařízením EU o ochraně osobních dat (GDPR).

Tabulka 7: Auditní služby

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.7 Bezpečnostní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.121	Řešení bude pracovat s identifikací pacienta v souladu s legislativou a prováděcími předpisy platnými ke dni dokončení realizace řešení, vč. zajištění připravenosti na postupné opuštění rodných čísel jako jediného a výměnného identifikátoru a zavedení bezvýznamových identifikátorů během doby trvání servisní smlouvy, pokud nebude možné tento přechod realizovat během realizace projektu. Maximální doba pro realizaci takového požadavku v rámci servisní smlouvy je 6 měsíců od jeho uplatnění, zkrácení tohoto termínu je možné pouze v situaci legislativního určení bližšího termínu.
P.122	Systém bude chránit osobní údaje pacientů a bude v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR) v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
P.123	Řešení musí být připraveno na plnění podmínek zákona č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů.
P.124	Autorizace: Poskytnutí přístupu autentizovaného uživatele k aktivu systému (data, aplikace), odpovídající pracovnímu zařazení uživatele a přidělené roli (rolím) v systému. Systém umožní řídit přístupová oprávnění jednotlivých subjektů jen k údajům, ke kterým mají a mohou mít přístup. Návrh množiny rolí a jejich konkrétních oprávnění bude předmětem implementační analýzy.

#	Požadavek
P.125	Zabránění vstupu neautorizovaného subjektu do systému – zamezení možnosti přístupu neoprávněného subjektu.
P.126	Zajištění konfiguračního managementu a správy systému s eliminací rizika ovlivnění chodu systému změnou aplikací 3. stran (unifikace konfigurací serverů, řízený patch management).
P.127	Dostupnost: <ol style="list-style-type: none"> 1. Zajištění dostupnosti jednotlivých částí systému podle požadavků uvedených v této dokumentaci a servisní smlouvě. 2. Odpovídající architektura řešení pro zajištění této dostupnosti. 3. Dekompozice SLA na jednotlivá aktiva podle kategorizace jejich důležitosti/dopadu na dostupnost systému
P.128	Zajištění šifrované komunikace mezi všemi součástmi systému a pracovišti uživatelů, případně zajištění komunikace v odděleném síťovém prostředí.
P.129	Evidence přístupů všech uživatelů do systému (logování) včetně časových údajů.
P.130	Veškeré přístupy k datům a aktivity uživatelů budou logovány tak, aby byly zřejmé přístupy k jednotlivým údajům a zpětná kontrola těchto údajů. V systému bude evidována jednoznačná identifikace kdo, kdy provedl zápis do systému nebo provedl náhled do dokumentace. Tyto logy budou zabezpečeny proti změnám.
P.131	Veškerá komunikace je a bude zajišťována prostřednictvím zabezpečených (šifrovaných kanálů), případně zajištění komunikace v odděleném síťovém prostředí.
P.132	Zabezpečení dat – zabezpečení pomocí řízení přístupu k datům, použití šifrování a ostatních kryptografických prostředků, audit logových záznamů
P.133	Veškeré bezpečnostní logy budou dostupné i pro externí logmanager/SIEM.

Tabulka 8: Bezpečnostní požadavky

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.8 Implementační a provozní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.134	Systém musí být připraven na provoz 24x7x365 (non-stop).
P.135	V rámci řešení jsou požadované následující provozní podmínky řešení: <ol style="list-style-type: none"> 1. Active/passive – lokality budou provozovány v režimu aktivní/pasivní, kdy v provozu bude vždy jedna lokalita, druhá bude připravena převzít služby v případě výpadku aktivní lokality. 2. Izolovanost – přístup do systému a přístup ze systému ven je možný pouze přes definované přístupové body. 3. Autonomnost – systém není a nebude v kritických oblastech závislý na dostupnosti funkcionality a dat jiných informačních systémů.

#	Požadavek
	<ol style="list-style-type: none"> 4. Odolnost proti katastrofě – systém se bude provozován na vysoce dostupné, případně redundantní infrastruktuře – předmět dodávky. 5. Vysoká bezpečnost – viz předchozí kapitola.
P.136	<p>Počet uživatelů:</p> <ol style="list-style-type: none"> 1. EZD – počet uživatelů systému se zásadně nezmění, potenciální změna počtu uživatelů nepřekročí 10 % po dobu požadované podpory systému. 2. EA – počet uživatelů přistupujících přes GUI je uveden v kap. 6.2 – Uživatelé. 3. IS ZOS – počet uživatelů systému se nezmění. <p>Minimální požadované počty jsou uvedené v kap. 6.2 – Uživatelé. Dodávka musí zajistit funkčnost pro uvedený počet uživatelů.</p>
P.137	<p>Počty a množství zpracovávaných dat:</p> <ol style="list-style-type: none"> 1. EZD – objem zpracovávaných dat v systému se zásadně nezmění, potenciální změna nepřesáhne 10 % ročně. 2. EA – odhad objemu zpracovávaných dat je uveden v kap. 6.3 – Počty a množství zpracovávaných dat. 3. IS ZOS – objem zpracovávaných dat v systému se nezmění. <p>Minimální požadované objemy dat jsou uvedené v kap. 6.3 – Počty a množství zpracovávaných dat. Dodávka musí zajistit kapacity a funkčnost pro uvedený objem dat na dobu min. 4 let s možností postupného rozšiřování min. na 11 let.</p>
P.138	<p>Předmětem zakázky jsou i veškeré služby související s dodávkou – doprava, instalace, implementace do stávající infrastruktury, konfigurace a zprovoznění komunikace, nastavení datových toků, seznámení s obsluhou a správou systému, testování, bezplatné preventivní prohlídky v rámci poskytování servisních služeb. Veškeré seznámení s obsluhou bude probíhat v prostorách objednatele a v českém jazyce.</p> <p>Součástí nabídkové ceny musí být i veškeré práce či činnosti, které v této zadávací dokumentaci nejsou explicitně uvedeny, ale které musí dodavatel s ohledem na jím nabízený předmět veřejné zakázky a jeho řádnou a úplnou realizaci provést k dosažení objednatelem požadovaného cílového stavu.</p>
P.139	<p>Instalace do prostředí objednatele a na požadovanou infrastrukturu dle kap. 3.4.5 – Dodávka nezbytné provozní infrastruktury a systémového SW pro dodávané systémy a 6.4 – Stav informačních a komunikačních technologií.</p>
P.140	<p>V rámci implementace musí dodavatel zajistit plnohodnotný provoz dodávaného řešení současně s provozem stávajících systémů, to vše bez jakéhokoliv omezení provozu. Dodavatel do nabídky popíše postup přechodu systémů. Dodavatel je povinen přizpůsobit realizaci předmětu zakázky podmínkám objednatele.</p>
P.141	<p>Všechny součásti systému (OS, DB, IS, klientské aplikace) musí logovat svou činnost do logů s možností nastavit úroveň logování pro potřeby diagnostiky.</p>
P.142	<p>Zajištění zálohování a obnovy v souladu s legislativou a provozními požadavky na Systém a dodávané technologie.</p>

#	Požadavek
	Konkrétní zálohované části a podmínky zálohování budou navrženy v rámci implementační analýzy a návrhu řešení. Požadavek na zálohování se nevztahuje na části, jejichž zálohování bude zajišťovat Objednatel.
P.143	Zajištění administrátorských aplikací, konzolí pro všechny součásti systému (OS, DB, IS, ...) pro zajištění konfiguračního managementu systému anebo jeho součástí, zajištění konfigurace na jednom místě s případnou vnitřní distribucí nastavení do jednotlivých částí systému.
P.144	Dohled – systém musí předávat informace o svém stavu (stavu služeb apod.) na žádosti SNMP GET. Zhotovitel poskytne parametry, podmínky a součinnost při nastavení dohledu dodaného řešení.
P.145	Architektura řešení celého systému musí korespondovat s požadavky na jeho dostupnost, uvedenými v servisní smlouvě.
P.146	Synchronizace času všech zařízení s Objednatelem určeným time serverem nebo zprostředkovaně přes centrální systém.
P.147	V případě ukončení servisní smlouvy musí Systém a provozní infrastruktura umožnit převedení veškerých aktiv, spravovaných dodavatelem, vč. smluvních vztahů k zajištění provozní infrastruktury a uložených dat na Objednatele, případně možnost zajištění migrace Systému na jinou infrastrukturu zajištěnou Objednatelem.

Tabulka 9: Provozní požadavky

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v předcházející tabulce

2.1.9 Požadavky na služby

2.1.9.1 Realizace předmětu plnění

Součástí předmětu plnění je zajištění služeb souvisejících s realizací předmětu plnění minimálně v následujícím rozsahu:

- 14) Objednatel požaduje před zahájením implementačních prací zpracování **Implementační analýzy včetně návrhu řešení** (konkretizace implementačního postupu, přesné konfigurace a instalačního a montážního návrhu řešení z nabídky), která bude zahrnovat informace pro všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění. Implementační analýza včetně návrhu řešení musí být před zahájením prací schválena objednatelem. Implementační analýza včetně návrhu řešení musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:

- c) Implementační analýza – zjištění týkající se prostředí objednatel, bude obsahovat alespoň následující:
- vi) Seznam technologií, které mají vliv/dopad na dodávku
 - vii) Identifikace zdrojů dat využitých pro dodávku
 - viii) Evaluace bezpečnosti systému a rizikových faktorů
 - ix) Implementační upřesnění specifikace požadavků

- x) Výstupy z analýzy okolí – sběr a analýza informací vztahujících se k dodávce (např. součinnosti apod.)
- d) **Detailní popis cílového stavu** (instalační a montážní upřesnění návrhu řešení z nabídky)
Popis bude obsahovat alespoň:
 - vii) Rozpracování návrhu řešení z nabídky zhotovitele z pohledu instalací a montáže dle informací z implementační analýzy
 - viii) Upřesnění rozhraní pro integraci na IS a technologie třetích stran (v případě nutnosti)
 - ix) Způsob zajištění projektového řízení na straně zhotovitele pro realizaci předmětu plnění (harmonogram, projektový tým, koordinační mechanismy apod.)
 - x) Detailní návrh a popis postupu implementace, instalace a montáže předmětu plnění
 - xi) Detailní popis zajištění bezpečnosti systému a informací

Detailní harmonogram projektu včetně uvedení kritických milníků. Kritické milníky jsou termíny dosažení určitých fází projektu, které jsou pro naplnění cílů projektu klíčové. Kritické milníky budou obsahovat minimálně aktivity vedené v kapitole 3 - Detailní harmonogram projektu, s uvedením konkrétních termínů, zhotovitel vhodným způsobem může rozšířit kritické milníky o další aktivity, které mohou být pro projekt klíčové.

- xii) Detailní popis navrhovaného seznámení s funkcionalitami, obsluhou dodávaného zařízení a budoucím provozem

Implementační analýza bude detailně popisovat způsob naplnění veškerých požadavků. Její akceptace je nezbytnou podmínkou pro realizaci dalších etap dodávky. Její nezbytnou součástí je dále konkretizovaný rozsah požadované součinnosti ze strany Objednatele.

- 15) **Zajištění projektového vedení/řízení** realizace předmětu plnění ze strany zhotovitele a jeho případných subdodavatelů.
- 16) **Vývoj, implementace a nastavení** informačních a komunikačních technologií odpovídající schválenému návrhu řešení uvedenému v Implementační analýze a příprava pro ověření ze strany objednatele, alespoň v následujícím rozsahu:
 - e) Vývoj na straně zhotovitele – vývoj jednotlivých systémů, úpravy existujících produktů, jejich parametrizace a nastavení, vývoj a ověřování integračních rozhraní, součinnost se třetími stranami v souvisejících oblastech.
 - f) Instalace a implementace do prostředí objednatele v testovacím režimu.
 - g) Interní ověření na straně zhotovitele a příprava podkladů pro ověření na straně objednatele (dokumentace, organizace testování a další).
 - h) Příprava a naplnění základních dat – z integračních úloh, číselníky, uživatelé a další.

Provedením těchto činností bude zajištěna připravenost pro ověření ze strany objednatele.

- 17) **Dodávka předmětu plnění.** Součástí dodávky musí být instalace, upgrade a sestavení předmětu zakázky včetně:
 - c) Instalace a nastavení infrastruktury a SW budou provedeny kvalifikovanými osobami pro dané typy zařízení
 - d) Nastavení infrastruktury, SW a aplikací
- 18) **Zajištění instalace všech součástí dodávky** v určených lokalitách a prostorách objednatele.
- 19) **Zajištění instalace a připojení** k zařízením a technickým prostředkům zajištěným objednatelem.
- 20) **Realizace pilotního provozu** k ověření funkčnosti systému na menším objemu dat, s menším počtem uživatelů a na menším počtu zařízení.

- 21) **Převedení systémů do zkušebního provozu** a plná podpora uživatelů v rámci zkušebního provozu včetně technické podpory. V této etapě budou realizována požadovaná seznámení s funkcionalitami, obsluhou dodávaného zařízení a budoucím provozem.
- 22) **Zpracování dokumentace skutečného provedení, systémové a provozní dokumentace** – součástí předmětu plnění je zajištění systémové a provozní dokumentace související s realizací předmětu plnění minimálně v následujícím rozsahu:

Název	Popis
Uživatelská dokumentace	Bude popisovat konkrétní funkčnost z pohledu uživatele tak, aby byl uživatel schopen práce s informačním systémem a pochopil význam jednotlivých částí systému a vazeb mezi nimi. V uživatelské příručce bude popisován způsob práce s jednotlivými částmi systému, vazby mezi nimi včetně popisu součástí jednotlivých částí systému. K usnadnění práce bude sloužit popis jednotlivých obrazovek, ovládacích prvků na obrazovkách a jejich významů, který bude uveden v rámci uživatelské dokumentace.
Dokumentace skutečného provedení a systémová/provozní dokumentace	Obsahuje popis informačního systému (rozhraní a služby) včetně popisu správy informačního systému, definování uživatelů, jejich oprávnění a povinností a detailní popis údržby systému.
Bezpečnostní dokumentace	Účelem bezpečnostní dokumentace je definovat závazná pravidla pro zajištění informační bezpečnosti včetně stanovení bezpečnostních opatření. Součástí této dokumentace bude uveden seznam, který bude obsahovat seznam všech externích zdrojů, ke kterým se jednotlivé servery (součásti systému) připojují, včetně uvedení síťových protokolů, pomocí kterých se s daným externím zdrojem komunikuje. V případě, že na servery (součásti systému) existuje vzdálený přístup, musí být tento přístup jasně specifikován (vzdálené zařízení, síťový protokol) a popsán zdůvodnění takového přístupu (dohled, správa DB atd.)
Disaster & Recovery Plan	Plán řešení situací v případě výpadků a obnovy funkčnosti systému. Součástí je plán a způsob provádění zálohy a případného způsobu obnovy a obnovy funkčnosti i v případě jiných technických výpadků. Dokument bude vytvářen v součinnosti s objednatelem.
Projektová dokumentace	Smluvní dokumentace, harmonogram realizace projektu, analýzy a prováděcí projekty, zápisy z jednání, protokoly (předávací, akceptační)

Tabulka 10: Dokumentace – požadavky na zpracování

Dokumentace bude dodána v relevantním rozsahu na všechna místa plnění projektu.

Dokumentace bude v souladu se zákonem č. 365/2000 Sb. o informačních systémech veřejné správy a prováděcích právních předpisů, v platném znění.

Dokumenty budou zpracovávány v následujících programech elektronicky a uloženy v následujících formátech:

- MS Office 2016 (MS Word 2016, MS Excel 2016, MS PowerPoint 2016)
- MS Project 2016

- WinZip (formát .zip)
- Portable Document Format (formát .pdf).

Preferovaná forma předávaných dokumentů, které nebudou vyžadovat podpisy konkrétních osob je elektronicky a to na elektronických nosičích (CD, DVD, flash disk, atp.). K předávání a k archivaci souborů se používají média s možností pouze zápisu, nikoliv přepisovatelná.

Veškerá dokumentace bude podléhat schvalování (akceptaci) při převzetí ze strany objednatele.

Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána ve 2x kopiích v elektronické formě ve standardních formátech (MS Office a PDF) používaných objednatelem na datovém nosiči a 1x kopii v papírové formě.

- 23) **Provedení akceptačních testů.** Zhotovitel je povinen kompletně připravit podklady pro akceptaci dodaného řešení. Součástí akceptace bude akceptační protokol a kompletní předávací dokumentace.
- 24) **Uvedení systému do produkčního provozu,** zajištění potřebných nastavení a přístupů pro všechny pracovníky objednatele, minimalizace dopadů na provoz objednatele při přechodu a zvýšená podpora bezprostředně po přechodu do produkčního provozu.
- 25) Zhotovitel dle svého uvážení doplní v nabídce další služby, které jsou dle jeho názoru nezbytné pro úspěšnou realizaci zakázky.
- 26) Veškeré náklady na zajištění služeb souvisejících s realizací předmětu plnění musí být zahrnuty v ceně odpovídající části předmětu dodávky.

2.1.9.2 Seznámení s funkcionalitami, obsluhou dodávaného systému

V této kapitole jsou uvedeny požadavky na seznámení s funkcionalitami, obsluhou dodávaného zařízení a jeho budoucím provozem:

- 6) Zhotovitel proškolí pracovníky objednatele se všemi typy dodaných zařízení a aplikací a problematikou jejich užití, provozu a obsluhy. Zhotovitel se zavazuje poskytnout informace minimálně k následujícím tématům v dostatečném detailu pro porozumění činnosti zařízení a způsobu provozu:
 - f) Základní produktové seznámení s jednotlivými dílčími technologickými celky.
 - g) Celkové schéma součinnosti jednotlivých zařízení a jejich návaznosti.
 - h) Obsluha jednotlivých dílčích modulů, aplikací a technologických celků
 - i) Použitá nastavení zařízení, detailnější rozbor použitých konfigurací.
 - j) Základní kroky správy, diagnostiky a elementární postupy pro řešení problémů.
- 7) Poskytnuté informace zajistí seznámení pracovníků objednatele se všemi podstatnými částmi dodávky v rozsahu potřebném pro obsluhu, provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
- 8) Vše uvedené bude probíhat v prostorách objednatele s využitím vybavení dodaného v rámci této veřejné zakázky, případně zajištěné ze strany objednatele.
- 9) Konkrétní termíny určí objednatel dle postupu v rámci realizace projektu a dostupnosti zainteresovaných osob.
- 10) Seznámení s funkcionalitami, obsluhou dodávaného systému se týká klíčových uživatelů, ostatní uživatelé budou proškoleni klíčovými uživateli.

Veškeré náklady na zajištění těchto činností musí být zahrnuty v ceně odpovídající části předmětu dodávky.

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené výše

3 DETAILNÍ HARMONOGRAM PROJEKTU

V této kapitole je uveden detailní harmonogram projektu (vycházející a dodržující lhůty ze základního harmonogramu viz kapitola 4 Přílohy 5 - Technická specifikace) včetně popisu jednotlivých činností v dostatečném detailu. Z harmonogramu vyplývá, že realizace předmětu zakázky proběhne v požadovaných termínech.

Následující tabulka obsahuje požadovaný časový harmonogram realizace dodávky (T ~ datum účinnosti smlouvy o dílo):

#	Fáze	Termín	Doplňující informace
1	Zahájení realizace	0	Zahájení realizace bude dnem podpisu smlouvy na dodávku.
2	Analýza a návrh řešení	60	Zpracování analýzy a návrhu řešení pro potřeby upřesnění podmínek realizace (implementační analýza)
3	Dodávka, implementace, instalace, konfigurace HW a SW infrastruktury.	90	Dodávka a implementace HW, SW a síťové infrastruktury.
4	Vývoj a implementace SW, dodávka dokumentace k SW.	120	Vlastní vývoj a implementace dle analýzy a návrhu řešení.
5	Výchozí import datových zdrojů a metadat do systému (initial load)	130	
6	Ověření funkčnosti dodaného systému a jeho částí.	170	Otestování systému a ověření jeho plné funkčnosti.
7	Zaškolení uživatelů a administrátorů.	170	Součástí je i zaškolení způsobu převedení provozu do záložní lokality.
8	Dodávka dokumentace dodaného systému a jeho částí.	170	Min. uživatelská dokumentace, dokumentace skutečného provedení, systémová dokumentace, projektová dokumentace.
9	Převedení do zkušebního provozu.	170	Převedení do zkušebního provozu, odstranění všech vad a nedodělků, dokončení realizace a převedení do ostrého provozu.
10	Ukončení realizace dodávky.	230	Součástí je zahájení doby provozu dodaného systému a poskytování servisních služeb.

Doplňující informace:

- Pod pojmem „den“ je míněn kalendářní den.
- Zhotovitel má možnost v rámci zpracování implementační analýzy definovat kratší termíny plnění (v rámci dodávky), nelze zkrátit dobu zkušebního provozu, která musí být min. 30 dnů. Zkušební dobu lze zkrátit jen na písemnou žádost Objednatele v rámci dodávky.

4 DETAILNÍ POPIS ZÁRUČNÍHO A POZÁRUČNÍHO SERVISU

V této kapitole je uveden detailní popis záručního a pozáručního servisu v rozsahu požadovaném v kapitole 3.6 Přílohy 5 - Technická specifikace.

Popis řešení:

Nabízené řešení splňuje veškeré požadavky uvedené v této kapitole.

Objednatel požaduje záruku na veškeré dodané technologie včetně nezbytných provozních a servisních služeb v délce trvání minimálně:

- a) 48 měsíců na informační systém(y), aplikace a služby spojené s realizací projektu,
- b) 48 měsíců – u provozní infrastruktury a systémového SW, pokud není u konkrétního vybavení uvedeno jinak. Delší záruka je uvedena jen u částí, kde je na trhu běžné poskytování delší záruky v pořizovací ceně.
- c) 12 měsíců na spotřební materiál, případně drobné vybavení podléhající rychlému opotřebení. Případný spotřební materiál musí být explicitně označen v nabídce a smlouvě a musí být prokázáno, že splňuje tento charakter.

Další požadavky na záruky:

1. Záruka začíná běžet od okamžiku předání do ostrého (produkčního) provozu.
2. Veškeré opravy po dobu záruky budou bez dalších nákladů pro provozovatele (objednatele). Veškeré komponenty, náhradní díly a práce budou poskytnuty bezplatně v rámci záruky.
3. Zadavatel uvádí u jednotlivých komodit požadovanou min. záruku, popř. podporu. Uváděné parametry byly průzkumem trhu zjištěny jako standardní, tj. poskytovány výrobcí jako součást standardní dodávky a ceny.
4. Nabídne-li Dodavatel v rámci svého řešení zboží, na něž výrobce standardně (tj. v rámci standardní dodávky a ceny) poskytuje horší záruku, popř. podporu, požaduje Zadavatel zahrnout do nabídky (nabídkové ceny) cenu povýšení záruky, popř. podpory na jím požadovanou úroveň.
5. Zadavatel požaduje bezplatný (zahrnutý v ceně zakázky) přístup k aktualizacím software a firmware dodaných komodit minimálně po dobu záruky.
6. Po dobu 48-ti měsíců od předání díla jako celku do plného provozu musí zhotovitel nebo výrobce všech zařízení garantovat běžnou dostupnost náhradních komponentů a dostupnost servisu.
7. Součástí záruky je i shoda dodávaných systémů s platnou legislativou.
8. Max. doba na odstranění vady díla je 15 dnů od prokazatelného oznámení dodavateli
9. Zhotovitel uvede provozní služby požadovaného předmětu plnění veřejné zakázky včetně parametrů, které budou předmětem dodávek v rámci záruky systému a v rámci poskytování servisních služeb.
10. Zhotovitel ve své nabídce výslovně uvede všechny podmínky záruk.
11. Pro hlášení servisní požadavků zajistí Dodavatel Zhotoviteli přístup ke svému helpdeskovému systému s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Detailní popis helpdeskového systému a jeho obsluhy musí být součástí nabídky. Provozní doba helpdeskového systému musí být minimálně 7-17 hod. v pracovních dnech.

Po skončení záruky budou náhradní komponenty hrazeny Objednatelem, služby související s jejich instalací a uvedením systému do provozu jsou součástí servisních služeb v rámci provozu, které jsou popsány v samostatném dokumentu.

Popis řešení:

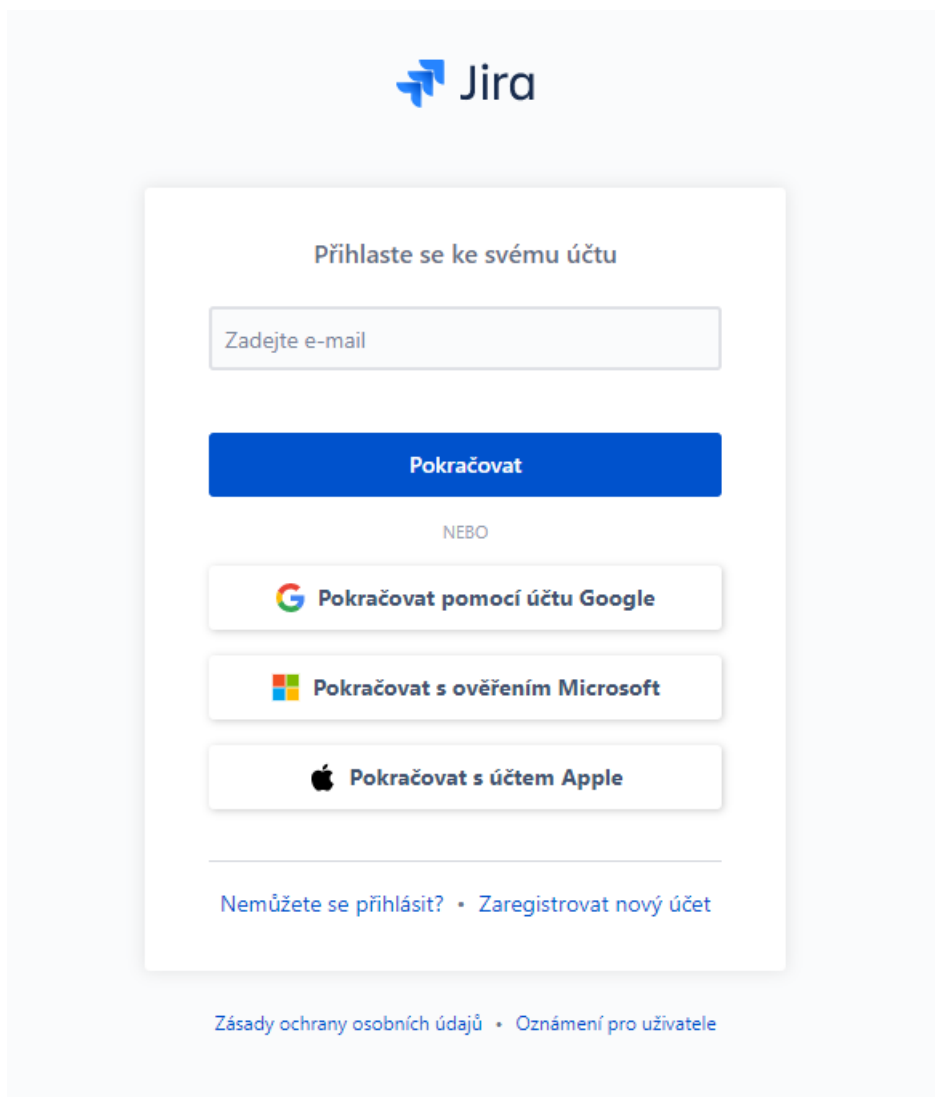
Pro záruční a pozáruční servis bude využíván stejný systém helpdeskového systému skládajícího se z následujících komponent:

- *www aplikace helpdeskového systému*
- *email helpdeskového systému*
- *telefonní linka helpdeskového systému*

Nabízené řešení splňuje veškeré požadavky uvedené v této kapitole a v požadavcích následující kapitoly (Detailní popis podpory provozu).

Helpdeskový systém WWW Aplikace

Jedná se o standardní WWW aplikaci pro účely evidence požadavků jejich průběhu a reportingu. Aplikace je provozována prostřednictvím šifrovaného přístupu pomocí protokolu https. Přístup do aplikace mají jak jednotliví dodavatelé a poddodavatelé technologií tak oprávněné osoby Zadavatele.



Jednotlivé požadavky je možné zadávat do systému jak pomocí WWW rozhraní aplikace, tak odesláním emailu z definovaných emailových adres Zadavatele. Dalším způsobem je zadání přes telefonního operátora po telefonickém nahlášení požadavku.

Vlastní rozhraní nabízí přehled jak aktuálně řešených požadavků, tak již vyřešený s možností definování uživatelských filtrů a vytvářet tak i specifické reporty.

Time to resolution	S	Klíč	Stav	Souhrn	Vytvořeno	Zadavatel	Termín	Přifazený řešitel
		ICCI-355	WAITING FOR CUSTOMER	Kontrola backup a synchro ICCI vs Gdrive	30/Srp/19
		ICCI-303	PENDING	Password reset on inactive user status change ...	14/Li/18
		ICCI-371	WAITING FOR CUSTOMER	Access to Nish's One drive	15/Led/20
		ICCI-237	PENDING	Establish ICCI Virtual Data room	20/Úno/19
		ICCI-375	PENDING	unable to change the Contact Manager and Owner of contact created from webservice.	13/Úno/20

Proto je možné systém využít jak na reportování dodržování SLA jednotlivých služeb tak na podrobné sledování průběhu řešení jednotlivých požadavků včetně doplňování dalších potřebných informací během řešení požadavků.

ICCI-355
Kontrola backup a synchro

Typ: IT Help | Stav: WAITING FOR CUSTOMER | Priorita: Medium | Stav řešení: Nevřešeno

Slouhoví SLA
7:59 ✓ Time to first response do 8 h

Popis
Kontrola backup a synchro

Přílohy
Přetáhnout soubor pro přílohu, nebo procházet počítač.

- 2019-04-10.png (18 kB)
- 2019-09-13_zaplneni_googl... (19 kB)
- 20190920.png (18 kB)
- 2019-10-18.png (18 kB)
- 2019-11-08.png (14 kB)
- ICCI-355.png (59 kB)

Termíny
Vytvořeno: 30/Srp/19 1:10 odp.
Aktualizováno: 06/Pro/19 8:58 dop.

O vytvoření incidentů a změnách stavů a jsou jednotliví uživatelé helpdeskového systému informováni E-mailem.

Helpdeskový systém – Email

Pro účely poskytování služeb Zadavateli je zřízena helpdesková emailová adresa, pomocí které jsou vytvářeny přímo požadavky v HelpDeskové aplikaci (od definovaných uživatelů Zadavatele) a je zaslán i operátorovi HotLine.

Helpdeskový systém – Telefon

Pro účely poskytování služeb Zadavateli je zřízena telefonní linka operátora HotLine, který je schopen přijímat jednotlivé požadavky a zajistit jak jejich evidenci v helpdeskovém systému tak i distribuci technickým pracovníkům pro jejich včasné řešení.

Helpdeskový systém – způsob komunikace

Zadavatel při zadávání jednotlivých požadavků musí dodržovat pravidla s nakládáním s osobními údaji (v souladu s GDPR) a do požadavků zadávaných jakýmkoliv způsobem (aplikace, mail a

telefon) nesmí vkládat osobní ani citlivé údaje. Zadavatel pro specifikaci požadavků vždy uvádí pouze obecné číselníkové údaje jako je číslo akce apod. tak, aby v rámci poskytování Helpdeskového systému nebyly ukládány osobní údaje.

5 DETAILNÍ POPIS PODPORY PROVOZU

1. Předmětem zajišťování provozu Systému je zajištění dostupnosti a zálohování EA na infrastrukturu zajišťované Poskytovatelem dle SoD.
 - a. Poskytovatel cloudové infrastruktury je Amazon AWS.
 - b. Zálohování je řešeno prostředky AWS. Provádí se snapshoty úložišť instancí aplikačních a databázových serverů, které jsou drženy po stanovenou dobu v primární lokalitě a zároveň v geograficky oddělené lokalitě. V prostoru objektového úložiště je zapnuté verzování objektů, které udržuje minulou verzi objektů, včetně těch odstraněných.
 - c. Přístup do administrace cloudových služeb AWS je možné dvěma způsoby:
 - i. Webové GUI - AWS Management Console
 - ii. CLI - AWS Command Line Interface
 - d. Pro sledování kapacity a výkonu je určena služba AWS CloudWatch ve spolupráci se zasíláním notifikací AWS Simple Notification Service při dosažení hodnot překračujících stanovené meze.
2. Systémy EZD a IS ZOS nejsou předmětem zajišťování provozu Systému, jejich provoz zůstane zachován ve stávajícím DC a bude zajišťován Objednatelem.
3. Dodávka časových razítek pro provoz Systému v objemu 1400 / 1 kalendářní čtvrtletí. Účtována budou jen a pouze skutečně spotřebovaná časová razítka. Služba odběru časových razítek bude dostupná na následujícím URL xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
4. V případě ukončení servisních služeb Poskytovatel převede smluvní vztahy k zajištění provozní infrastruktury na Objednatele, případně poskytne veškerou potřebnou součinnost pro migraci Systému na jinou infrastrukturu zajištěnou Objednatelem.
5. Poskytování služby Hotline včetně základní servisní technické podpory Systému při zajištění provozu a odstraňování závad Systému. Hotline bude k dispozici v režimu 24 x 7, nicméně služby budou poskytovány dle úrovně v kap. 4 – Úroveň požadovaných služeb z dokumentu Specifikace servisních služeb, která je přílohou servisní smlouvy
6. Poskytování pravidelné profylaxe Systému vč. indikace a předcházení možných problémů při užívání Systému min. 1x čtvrtletně. Profylaxe bude spočívat minimálně v následujících krocích:
 - a. Kontrola funkčnosti infrastruktury (aplikační servery, databázové servery, objektová úložiště) – kontroluje se, zda monitoring provozu nevykazuje anomální chování v žádné součásti infrastruktury systému.
 - b. Kontrola zálohování – kontroluje se, zda zálohování probíhá dle stanovených pravidel, ve stanovených intervalech.
 - c. Kontrola archivace – kontroluje se, zda OBELISK Trusted Archive nevykazuje anomální chování, tzn. že:
 - i. běží všechny součásti systému,
 - ii. probíhá příjem dokumentů k archivaci,
 - iii. probíhá balíčkování přijatých dokumentů,
 - iv. probíhá uzavírání archivních balíčků a jejich opatření elektronickou pečetí a časovým razítkem,
 - v. probíhá přerazítkování.
7. Bude zajištěn soulad funkčnosti a vlastností systému s aktuální legislativou vč. bezplatného provádění nezbytných úprav systémů pro splnění tohoto požadavku.
8. Poskytování aktualizací Softwarových produktů a technologií a opravných patchů produktů OBELISK bude probíhat následujícím způsobem:
 - a. Aktualizace produktů OBELISK jsou vydávány cca 4x ročně.

- b. Před instalací aktualizace bude se zákazníkem dohodnuta odstávka systému pro instalaci.
 - c. Dodavatel pak následně nasadí update na aplikační servery, databázové servery a provede další nezbytné úkon pro aktualizaci systémů.
 - d. Dodavatel zkontroluje funkčnost aktualizovaného systému a následně jej přepne zpět do produkčního provozu.
9. Bude dodána dokumentace k aktualizacím Softwarových produktů a technologií, aktualizace provozní dokumentace Systému tak, aby odpovídala aktuálnímu stavu provozovaného Systému.
10. Bude prováděna aplikace service packů a hotfixů nutných pro bezchybný chod systému, které budou identifikovány na základě profylaxe a jejich aplikace bude dohodnuta s Objednatelem.

6 REALIZAČNÍ TÝM

Následující tabulka uvádí členy realizačního týmu a jejich role.

Členové realizačního týmu	Jméno a příjmení osoby, která se bude podílet na realizaci veřejné zakázky jako člen realizačního týmu
a) Projektový manažer	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
b) Technický specialista – mobilní zadávání dat a elektronická zdravotnická dokumentace	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
c) Technický specialista – zdravotnické operační středisko	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
d) Technický specialista – elektronizace dokumentů	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
e) Technický specialista – důvěryhodný archiv dokumentace	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Tabulka 11

7 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
EAEA	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
HMP	Hlavní město Praha
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
KZOV	Kompletní záznam o výjezdu
MHMP	Magistrát hl. m. Prahy
MS	Microsoft

Zkratka/pojem	Význam
MZD	Mobilní zadávání dat
OAuth	Otevřený standard pro delegaci přístupů mezi různými systémy
OŘ	Operační řízení
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 HMP	Zdravotnická záchranná služba hl. m. Prahy