

Příloha č. 1: Technická specifikace

V této příloze jsou uvedeny výchozí podmínky a požadavky na dodávku v rámci této veřejné zakázky.

OBSAH

Obsah.....	1
Využití zdroje	2
Seznam tabulek	2
Seznam zkratk a pojmů.....	3
1 Předmět plnění.....	5
2 Členění dokumentu	7
3 Požadavky na dodávky a související služby	8
3.1 Předmět a rozsah dodávky.....	8
3.1.1 Rozsah dodávky	8
3.1.2 Související služby a náležitosti dodávky	8
3.1.3 Dodávkou nedotčené oblasti stávajícího řešení	9
3.1.4 Vyloučení z dodávky	9
3.2 Východiska	9
3.2.1 Elektronická dokumentace	9
3.2.2 Ochrana osobních údajů	10
3.2.3 Certifikační autorita, certifikáty, nosiče certifikátů a čtečky a časová razítka	10
3.2.4 Karetní systém a související nastavení.....	10
3.2.5 Ostatní východiska.....	11
3.3 Koncept/architektura požadovaného řešení	11
3.3.1 Koncept/architektura řešení.....	11
3.3.2 Stručný popis konceptu řešení.....	11
3.4 Požadavky na dodávky	12
3.4.1 Obecné a společné požadavky.....	12
3.4.2 Dodávka elektronického archivu (EA).....	14
3.4.3 Úpravy a napojení EZD na elektronický archiv.....	21
3.4.4 Dodávka nezbytné provozní infrastruktury a systémového SW pro dodávané systémy.....	24
3.4.5 Auditní služby	27
3.4.6 Bezpečnostní požadavky.....	27
3.4.7 Implementační a provozní požadavky	29

3.5	Požadavky na služby.....	31
3.5.1	Realizace předmětu plnění	31
3.5.2	Seznámení s funkcionalitami, obsluhou dodávaného systému	34
3.6	Záruky.....	35
4	Harmonogram	36
5	Místa plnění.....	37
6	Výchozí stav.....	38
6.1	Zdravotnická záchraná služba Karlovarského kraje, příspěvková organizace (zadavatel)	38
6.2	Uživatelé	38
6.3	Počty a množství zpracovávaných dat	38
6.4	Stav informačních a komunikačních technologií.....	39
6.4.1	Informační systémy a aplikační software ZZS KVK.....	39
6.4.2	Datové sítě.....	41
6.4.3	Ostatní relevantní technologie	41
	Konec základní části dokumentu	42

VYUŽITÉ ZDROJE

[1] Nejsou

SEZNAM TABULEK

Tabulka 1: Seznam zkratk a pojmů	4
Tabulka 2: Předmět a rozsah dodávky	8
Tabulka 3: Stručný popis koncept řešení	12
Tabulka 4: Obecné požadavky	14
Tabulka 5: Požadavky: Dodávka elektronického archivu organizace (EA)	21
Tabulka 6: Požadavky: Úpravy a napojení EZD na elektronický archiv	24
Tabulka 7: Požadavky: Dodávka nezbytné provozní infrastruktury a systémového SW pro dodávané systémy	27
Tabulka 8: Auditní služby.....	27
Tabulka 9: Bezpečnostní požadavky	29
Tabulka 10: Provozní požadavky.....	31
Tabulka 11: Dokumentace – požadavky na zpracování	33
Tabulka 12: Harmonogram	36
Tabulka 13: Místa plnění	37
Tabulka 14: Výchozí stav: Uživatelé.....	38
Tabulka 15: Množství zpracovávaných dat.....	39

Tabulka 16: Výchozí stav: Informační systémy a aplikační software ZZS KVK.....	41
Tabulka 17: Datové sítě	41
Tabulka 18: Ostatní relevantní technologie.....	42

SEZNAM ZKRATEK A POJMŮ

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

Zkratka/pojem	Význam
OS	Operační systém
PD	Projektová dokumentace
PNP	Přednemocniční neodkladná péče
RA	Registrační autorita
RČ	Rodné číslo
SIP	SIP balíček je archivním digitálním nosičem dat („Submission Information Package“).
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 nebo výjezdová skupina (dle kontextu)
VZ	Veřejná zakázka
ZD	Zadávací dokumentace nebo zdravotnická dokumentace dle kontextu.
ZOS	Zdravotnické operační středisko
ZVZ / ZZVZ	Zákon o zadávání veřejných zakázek
ZZS	Zdravotnická záchranná služba (ve všeobecném významu)
ZZS KVK	Zdravotnická záchranná služba Karlovarského kraje, příspěvková organizace

Tabulka 1: Seznam zkratk a pojmů

1 PŘEDMĚT PLNĚNÍ

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

Zdravotnická záchranná služba Karlovarského kraje, příspěvková organizace je základní složkou IZS a v souladu s legislativou poskytuje přednemocniční neodkladnou péči (PNP). V rámci poskytování PNP je nyní zdravotnická dokumentace zpracovávána a archivována v souladu s legislativou v systému EZD v písemné (listinné) formě. ZZS KVK současně zpracovává a archivuje i ostatní dokumentaci organizace v písemné (listinné) formě. Veškerá uvedená dokumentace je nyní archivována v písemné podobě, nicméně ZZS KVK hodlá vybudováním EA a úpravami EZD a napojením EZD na EA přejít na zpracování a archivaci v elektronické podobě v souladu s legislativou. EZD tedy musí umožnit zpracování dokumentace pro přechodné období v kombinované formě (elektronická i papírová) a i v čistě elektronické formě s cílem dosažení „bezpapírové“ organizace.

Předmětem plnění v rámci této VZ je dodávka dlouhodobého bezpečného důvěryhodného elektronického archivu pro archivaci elektronické zdravotnické dokumentace a ostatní dokumentace v souladu s legislativou (EA). V tomto archivu bude ukládána elektronická dokumentace vzniklá v rámci provozu ZZS. Dále jsou předmětem plnění úpravy EZD tak, aby vytvářená zdravotnická dokumentace byla plně elektronická a umožnila archivaci v EA a výměnu zdravotnické dokumentace v rámci systémů eHealth. Součástí dodávky je dále veškerá nezbytná infrastruktura pro provoz a ukládání dat pro zajištění funkčnosti EA (servery, úložiště) neposkytovaná objednatelům.

Primárním požadavkem je efektivně vytvářet, 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.

Dále je součástí předmětu plnění automatizované napojení vybraných vnitřních informačních systémů ZZS KVK a to systému EZD (EKP/MZD) – komplexního systému pro zpracování elektronické zdravotnické dokumentace (bude napojen na EA) a zajištění technických prostředků pro vkládání a archivaci ostatní dokumentace zpracovávané v rámci organizace.

Dodané řešení musí kompletně zahrnovat plně automatizovaný systém práce s elektronickou zdravotnickou dokumentací, zpracovávanou v současném systému EZD (od vytvoření po archivaci a skartaci). Nicméně řešení musí také obsahovat datové (integrační) a aplikační (GUI) rozhraní, umožňující archivovat i ostatní druhy elektronických dokumentů z dalších perspektivních systémů či agend ZZS KVK (smlouvy, ekonomické, personální a další interní dokumenty organizace). Tato vlastnost je požadována na úrovni webové aplikace, poskytující schopnosti konzumace validního elektronického dokumentu, opatření metadaty, zaručení jeho neměnnosti a prokazatelnosti a vyhledání relevantního záznamu v rozsahu poskytnutých metadat včetně implementace skartačního řádu. Pro autentizaci uživatelů je požadováno využití platných komerčních

certifikátů včetně jejich nosičů (QSCD), které budou zavedeny v rámci ZZS KVK k autentizaci uživatelů v systému EZD a pro přístup do dalších systémů a technologií. Pro podepisování dokumentů budou využívány platné kvalifikované certifikáty v souladu s eIDAS na stejných nosičích jako komerční certifikáty. Autentizace uživatelů i podepisování bude podporováno ve všech částech EZD a EA.

Integrace dalších systémů (plně automatizovaný systém vzájemné komunikace) nad rámec integrace EA s EZD dle požadavků uvedených dále v tomto dokumentu není součástí dodávky.

Součástí předmětu plnění je dodávka nezbytné provozní infrastruktury a systémového SW pro běh dodávaného EA.

Předmět plnění (dílo) a související služby jsou detailně popsány v kap. 3.1 – 3.6.

Požadavky na provozní a servisní služby k tomuto Dílu jsou definovány v samostatném dokumentu.

2 ČLENĚNÍ DOKUMENTU

Tento dokument obsahuje jen a pouze požadavky na dodávku a související služby (Dílo) a je členěn následovně:

- **Kapitola 3 – Požadavky na dodávky a související služby** – kapitola obsahuje požadavky na dodávky a služby (Dílo), které musí zhotovitel splnit ve svém řešení a ve své nabídce. Kapitola obsahuje základní koncept řešení, legislativní požadavky, konkrétní funkční a technické požadavky na řešení předmětu plnění v rámci VZ.
- **Kapitola 4 - Harmonogram** – kapitola obsahuje harmonogram realizace předmětu plnění VZ.
- **Kapitola 5 – Místa plnění** – kapitola obsahuje místa plnění v rámci realizace předmětu plnění VZ.
- **Kapitola 6 – Výchozí stav** – kapitola obsahuje popis výchozího stavu pro realizaci předmětu VZ, tj. uvedení seznamu dotčených subjektů, jejich vztah k předmětu VZ, informační a komunikační technologie a vybavení, kterými subjekty disponují nebo které budou k dispozici pro realizaci VZ, případně další organizační a technické podmínky, které jsou důležité pro realizaci VZ.

Uvedené kapitoly a jejich obsah jsou uvedeny dále v tomto dokumentu.

Požadavky na servisní služby k tomuto Dílu jsou definovány v samostatném dokumentu, který v rámci VZ je přílohou ZD a současně se stane přílohou Servisní smlouvy.

3 POŽADAVKY NA DODÁVKY A SOUVISEJÍCÍ SLUŽBY

V této kapitole jsou uvedeny požadavky na dodávky a související služby v rámci této VZ.

3.1 PŘEDMĚT A ROZSAH DODÁVKY

V této kapitole je upřesnění předmětu a rozsahu dodávky v rámci této VZ.

3.1.1 Rozsah dodávky

Rámcový rozsah dodávky je následující:

Ozn.	Položka	Popis	Počet
1	Dodávka elektronického archivu (EA)	Dodávka dlouhodobého bezpečného důvěryhodného elektronického archivu pro archivaci elektronické zdravotnické dokumentace a ostatní dokumentace v souladu s legislativou. V tomto archivu bude ukládána elektronická dokumentace vzniklá v rámci provozu ZZS.	1 soubor
2	Úpravy a napojení EZD na elektronický archiv a sdílení zdravotnické dokumentace	Nezbytné úpravy EZD pro vytváření elektronické zdravotnické dokumentace a její archivace do elektronického archivu organizace a sdílení zdravotnické dokumentace prostřednictvím eHealth systémů s dalšími poskytovateli zdravotních služeb. Součástí budou i nástroje pro správu certifikátů, autentizaci uživatelů a podepisování dokumentů uživateli.	1 soubor
3	Dodávka nezbytné provozní infrastruktury pro dodávané systémy.	Dodávka nezbytné provozní infrastruktury pro běh dodávaných IS ZZS KVK, datové konektivity a zajištění bezpečného provozování. Jedná se o servery, disková úložiště apod., které jsou nezbytné pro dodávku a provoz nových částí IS ZZS KVK.	1 soubor
4	Dodávka nezbytného systémového SW pro dodávané systémy.	Dodávka nezbytného systémového SW pro běh dodávaných IS ZZS KVK, integrace a zajištění bezpečného provozování. Jedná se o OS, DB, licence, archivace apod., které jsou nezbytné pro dodávku a provoz nových částí IS ZZS KVK.	1 soubor

Tabulka 2: Předmět a rozsah dodávky

3.1.2 Související služby a náležitosti dodávky

Součástí dodávky jsou dále následující služby a náležitosti:

1. Projektové řízení dodávky řešení.
2. Zpracování Analýzy a návrhu řešení – konkretizace implementačního postupu, přesné konfigurace a instalačního a montážního návrhu řešení z nabídky, související konzultace k dodávanému řešení.
3. Dodávka, implementace, instalace, konfigurace HW a SW infrastruktury.
4. Vývoj/rozvoj informačního systému a jeho součástí.
5. Implementace informačního systému a jeho součástí.
6. Výchozí import datových zdrojů a metadat do systému (initial load, bude-li třeba dle výstupu implementační analýzy).
7. Ověření funkčnosti dodaného systému a jeho částí.

8. Dodávka dokumentace dodaného systému a jeho částí (min. uživatelská dokumentace, dokumentace skutečného provedení, systémová dokumentace, projektová dokumentace).
9. Zaškolení uživatelů a administrátorů – seznámení s funkcionalitami, obsluhou dodávaného systému a jeho budoucím provozem.
10. Zařazení do provozního prostředí Zadavatele (dohled, zálohování apod.).
11. Provedení zkušebního provozu.
12. Poskytnutí záruky 5 let na informační systém a 3 roky na provozní infrastrukturu a systémový SW.

Doplňující požadavky na implementaci:

1. Zajištění kontinuity provozu ZZS KVK. Po stránce nepřetržitého provozu ZZS KVK předpokládá plánovanou odstávku pouze na minimální nezbytnou dobu, neohrožující poskytování PNP významným snížením informační podpory dispečerů a pracovníků výjezdových skupin.
2. Požaduje se kontinuita (převzetí či využití) nastavených parametrů, všech číselníků, definic a jiných aspektů provozu. Nepředpokládá se investice do opětovného zadávání a pořizování těchto údajů.

3.1.3 Dodávkou nedotčené oblasti stávajícího řešení

Dodávkou nebudou dotčeny následující oblasti stávajícího řešení:

1. Současné funkcionality systémů, technologií a pracovišť stávajících systémů EZD a IS ZOS zůstanou zachovány a nebudou negativně dotčeny realizací projektu.

3.1.4 Vyloučení z dodávky

Předmětem dodávky není:

1. Zajištění **v rámci požadavků neuvedené** komunikační infrastruktury (sítě apod.) mezi jednotlivými prvky systému. ZZS zajistí nezbytná síťová propojení pro realizaci dodávek a provoz řešení.
2. Infrastruktura, HW a systémový SW poskytovaný Objednatel (ZZS KVK) uvedený ve výchozím stavu a neuvedený v požadavcích.
3. Integrace na další informační systémy ZZS KVK, které nejsou explicitně uvedeny v rámci dodávky. Tímto není dotčena dodávka integračního rozhraní, která umožní budoucí napojení dalších informačních systémů ZZS KVK.
4. Spotřební materiál využívaný v následném provozu informačního systému neuvedený v rámci požadavků na dodávky.

Koncept řešení, principy a požadavky na dodávky a služby jsou uvedeny dále v tomto dokumentu.

3.2 VÝCHODISKA

3.2.1 Elektronická dokumentace

Objednatel povede zdravotnickou dokumentaci jako čistě elektronickou, tj. jen v elektronické podobě. Z uvedeného plyne, že dokumentace se bude cílově kompletně pořizovat, zpracovávat a ukládat elektronicky od vytváření po archivaci a skartaci, které jsou předmětem dodávky.

Pozn.: Nad rámec elektronické formy bude systém jako celek nadále obsahovat navíc (také) vybrané dokumenty v papírové formě, jejichž obsah či procesní předání/převzetí protistranou je prokazováno podpisem (případně razítkem) přebírající protistrany (typicky ZOV, faktury apod.). Tyto dokumenty jsou generovány z elektronického systému jako výstup a jsou datově konzistentní s elektronicky uloženými daty. V rámci procesu zpracování a kontroly zdravotnické dokumentace budou konvertovány do elektronické podoby, jejich pravost je potvrzena odpovědným pracovníkem a tvoří součást zdravotnické dokumentace. Proto se bude jednat i přes existenci těchto dokumentů o plně elektronický systém zdravotnické dokumentace.

Ke zrušení tohoto typu (datově duplicitních) papírových dokumentů dojde po implementaci technologie pro zaručený biometrický podpis a tento proces je podmíněn právě zavedením systému důvěryhodného elektronického archivu ZD do rutinního provozu.

Elektronické verze dokumentů ze zdravotnické dokumentace (z EZD) bude podepsána uznávaným elektronickým podpisem, pokud se bude jednat o pracovníka Objednatele a nebude vyžadován podpis další osoby (ověření pravosti dokumentu pracovníkem). Pokud bude vyžadován podpis jiné osoby, bude dokument podepsán touto osobou nebo podepsán biometrickým/viditelným digitálním podpisem na zařízení a následně předán dále do zpracování jako platný elektronický dokument.

V případě, že by v provozu vznikl papírový dokument, bude takový dokument k elektronické dokumentaci zařazen následně pracovníkem Objednatele, který provede konverzi do elektronické formy a elektronicky podepíše.

Objednatel v rámci tohoto projektu bude pořizovat elektronický archiv organizace pro archivaci elektronické dokumentace v souladu s požadavky legislativy na vedení a archivaci plně elektronické zdravotnické dokumentace a ostatní dokumentace v souladu s platnou legislativou.

3.2.2 Ochrana osobních údajů

V rámci projektu je nezbytné zajištění ochrany osobních údajů a bezpečnosti v souladu s legislativou a moderními principy – Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob (GDPR), zákona č. 181/2014 Sb. – Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a požadavky kladené na KII.

3.2.3 Certifikační autorita, certifikáty, nosiče certifikátů a čtečky a časová razítka

V rámci souběžného projektu budou pro realizaci dodávky Díla zajištěno (součinnost Objednatele):

1. Certifikační autorita sloužící pro vydávání komerčních a kvalifikovaných certifikátů pro personál v souladu s eIDAS.
2. Nosiči certifikátů budou karty a tokeny v souladu s QESCD, tj. budou plnit podmínky pro kvalifikovaný prostředek.
3. Certifikační autorita bude vydávat kvalifikované elektronické pečeti pro elektronický archiv, případně pro EZD.
4. Certifikační autorita bude vydávat kvalifikovaná časová razítka pro elektronické dokumenty a poskytne k tomu rozhraní pro jejich automatizované čerpání z EA a EZD.
5. Tablety a pracovní stanice budou vybaveny čtečkami a ovladači pro čtení nosičů certifikátů dle předchozího bodu.
6. Tablety budou podporovat technologie biometrického podpisu.

Součástí souběžného projektu nebudou úpravy EZD sloužící pro autentizaci uživatelů a elektronické podepisování, tyto funkcionality včetně administrace jsou součástí Díla dle tohoto dokumentu.

Implementace a zprovoznění výstupů výše zmíněného souběžného projektu jsou nezbytnou podmínkou pro realizaci Díla dle tohoto dokumentu.

3.2.4 Karetní systém a související nastavení

V rámci souběžného projektu budou pro realizaci dodávky Díla zajištěno (součinnost Objednatele):

1. Dodávka SDK pro přístup ke kartám a certifikátům na kartách na koncových HW zařízeních a Middleware pro přístup EZD pro OS MS Windows pro potřeby čtení a ověřování certifikátů při ověřování identity a podepisování.
2. Součinnosti dodavatele karetního systému při implementaci napojení EZD na karetní systém.

3. Vydávání karet včetně nahrávání komerčních a kvalifikovaných certifikátů na karty bude zajišťovat karetní systém.
4. Poskytnutí testovacích karet s komerčními certifikáty a kvalifikovanými certifikáty pro ověřování funkcionalit v EZD.
5. Nahrávání veřejných klíčů z komerčních certifikátů do MS AD ke konkrétním uživatelům.

Další upřesnění jsou uvedena v konkrétních požadavcích v tomto dokumentu.

3.2.5 Ostatní východiska

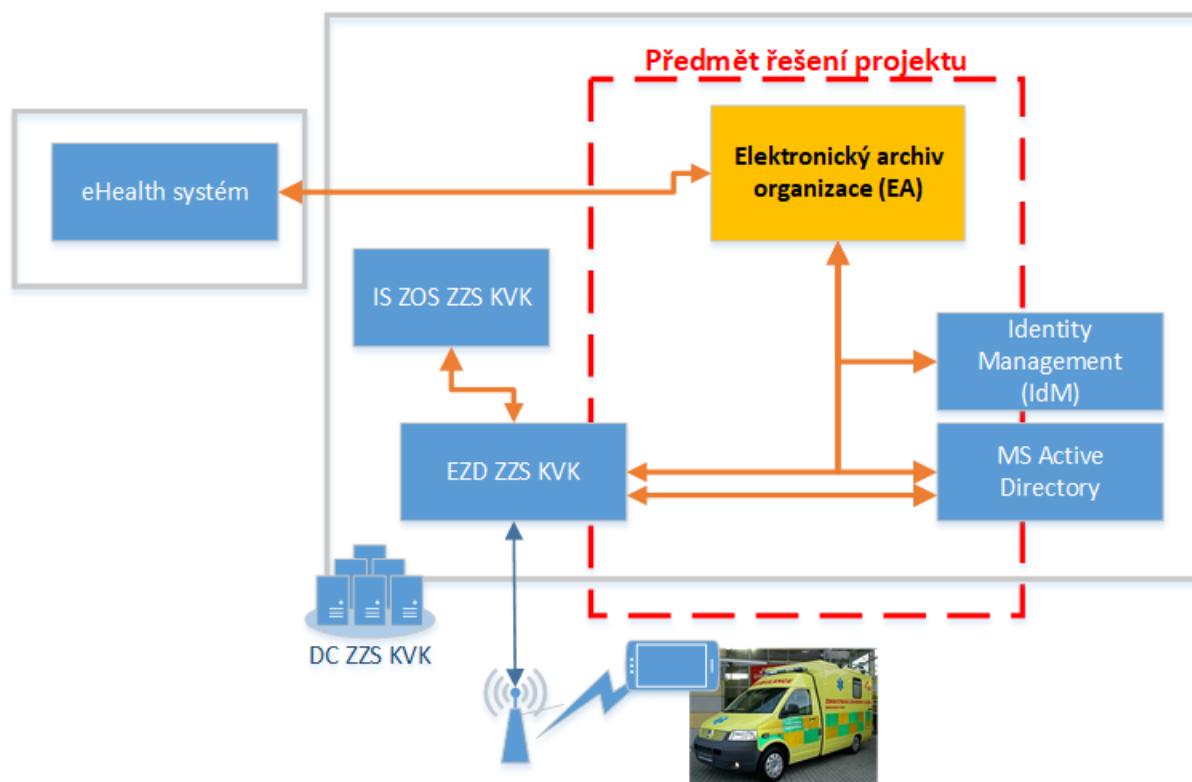
Další východiska jsou definována výchozím stavem uvedeným v kap. 6 – Výchozí stav.

3.3 KONCEPT/ARCHITEKTURA POŽADOVANÉHO ŘEŠENÍ

V této kapitole je uveden koncept/architektura požadovaného řešení.

3.3.1 Koncept/architektura řešení

Na následujícím schématu je uveden koncept řešení:



Obrázek 1: Koncept/architektura řešení

3.3.2 Stručný popis konceptu řešení

V následující tabulce je stručný popis konceptu řešení z předchozího schématu:

Prvek	Popis
Rozsah projektu	Červeně ohraničené vymezení předmětu řešení projektu.
DC ZKS KVK	Datové centrum pro umístění a provoz technologií ZKS KVK a tedy i technologií a IS EZD ZKS KVK a IS ZOS (SOS) ZKS KVK. V tomto DC budou realizovány dodávky, tj. dodávka úprav EZD a jeho napojení na EA a úpravy IS ZOS.

Prvek	Popis
IS ZOS ZZS KVK	Informační systém zdravotnického operačního střediska (IS ZOS) bude beze změny, bude poskytovat data systému EZD pro potřeby úplnosti dokumentace a následné archivace této dokumentace.
EZD ZZS KVK	Systém elektronické zdravotnické dokumentace zajišťující přebírání dat o výjezdu z IS ZOS (do EZD), předávání posádkám (do MZD), sběr patientských informací z výjezdů ZZS (z IS ZOS a MZD) a elektronickou podporu posádek v rámci výjezdů (MZD) a elektronické předávání dat z terénu do centrálního IS pro následné zpracování (v EZD). V této části bude zavedena archivace elektronické zdravotnické dokumentace do elektronického archivu organizace (EA). Součástí popínaného řešení je i zřízení sdíleného úložiště certifikátů (veřejná část komerčního certifikátu) jednotlivých uživatelů a prostředky provozní a systémové správy v rozsahu současného řešení v rámci EZD. Je požadován soulad s platnou národní i evropskou legislativou (eIDAS).
Elektronický archiv organizace (EA)	Nově dodávaný a budovaný elektronický archiv organizace (EA) pro archivaci elektronické zdravotnické dokumentace a ostatní dokumentace. Předmětem projektu je dodávka dlouhodobého bezpečného důvěryhodného elektronického archivu (EA) pro archivaci elektronické zdravotnické dokumentace a ostatní dokumentace v souladu s legislativou. V tomto archivu bude ukládána elektronická dokumentace vzniklá v rámci provozu ZZS KVK. Jedná se o nově budovanou součást IS ZZS KVK.
MS Active Directory	MS Active Directory tvoří základní identity management systémů ZZS KVK. Součástí popínaného řešení je i přebírání veřejných částí komerčních certifikátů uživatelů ze sdíleného úložiště certifikátů a nastavení synchronizace s AD. Je požadován soulad s platnou národní i evropskou legislativou (eIDAS).
Identity management	ZZS KVK buduje rozšířený identity management (IdM) systémů ZZS KVK. Součástí popínaného řešení je i integrace na IdM společně s integrací na MS AD.
eHealth systém (eMeDocS)	EZD ZZS KVK je napojen na systém výměny zdravotnické dokumentace mezi zdravotnickými zařízeními na území ČR provozovaným Krajem Vysočina (eMeDocS). Předmětem plnění je poskytování elektronické zdravotnické dokumentace v nové, čistě elektronické formě.

Tabulka 3: Stručný popis koncept řešení

Detailní popis požadavků na dodávky je uveden v následující kapitole.

3.4 POŽADAVKY NA DODÁVKY

V této kapitole jsou uvedeny požadavky na dodávky.

3.4.1 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).

#	Požadavek
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. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat 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"> 1. 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 2. 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
P.13	Soulad se zákonem č. 325/2021 Sb. o elektronizaci zdravotnictví a zákonem č. 326/2021 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronizaci zdravotnictví.
P.14	Soulad s Vyhláškou č. 98/2012 Sb., o zdravotnické dokumentaci, v rámci tohoto projektu zajištění primárního souladu s: <ol style="list-style-type: none"> 1. vymezením obsahu ZD – ZD zahrnuje také výsledky vyšetření včetně grafických, audiovizuálních, digitálních nebo jiných 2. pravidly pro skartační řízení

#	Požadavek
P.15	Soulad s Nařízením Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.
P.16	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.17	Zajištění jednotného času na všech pracovištích/zařízeních (synchronizace klientů a systému s Objednatelem určeným time serverem).

Tabulka 4: Obecné požadavky

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

3.4.2 Dodávka elektronického archivu (EA)

Požadavky na tuto část předmětu plnění jsou následující:

#	Požadavek
P.18	Dodávka dlouhodobého bezpečného důvěryhodného elektronického archivu pro archivaci elektronické zdravotnické dokumentace a ostatní dokumentace v souladu s legislativou.
P.19	EA musí zajistit minimálně následující služby: <ol style="list-style-type: none"> 1. uložení a fyzické zabezpečení dokumentů/dat, 2. archivace (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, 3. přístup k uloženým dokumentům přes integrační i aplikační rozhraní, 4. ověřování uživatelů primárně přes komerční certifikáty v kvalifikovaném prostředí, případně přes dočasné heslo (viz administrace EZD), návaznost na MS Active Directory Objednatele 5. zajištění přístupu k dokumentům jen oprávněným uživatelům a systémům 6. skartace dokumentů <p>Upřesňující požadavky následují.</p>
P.20	Řešení musí na aplikační úrovni disponovat mechanismy, které zajistí uložení dat ve shodě s národními normami pro důvěryhodné uložení dat a organizačními směrnici a nařízeními. <ol style="list-style-type: none"> 1. eIDAS – nařízení Evropské unie č. 910/2014 2. Zákon č. 297/2016 Sb., Zákon o službách vytvářejících důvěru pro el. transakce 3. Zákon č. 499/2004 Sb., Zákon o archivnictví a spisové službě a o změně některých zákonů 4. Národní standard pro vedení elektronického systému spisové služby NSESSS <p>Tato schopnost bude doložena certifikátem shody s výše uvedenými normami vydaným akreditovaným subjektem.</p>
P.21	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.22	Ukládání elektronické dokumentace vzniklé v rámci provozu ZZS do EA prostřednictvím:

#	Požadavek
	<ol style="list-style-type: none"> 1. datového (integračního) rozhraní – napojení EZD, možnost budoucího napojení dalších vnitřních, nyní neintegrovaných IS. 2. aplikačního (GUI) rozhraní pro uživatele. <p>Umožňující archivovat i ostatní druhy elektronických dokumentů z dalších perspektivních systémů či agend ZZS KVK (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.23	<p>Archivované elektronické dokumenty musí být důvěryhodné a musí mít po formální i po obsahové stránce stejně trvalou důkazní hodnotu jako papírové.</p> <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.24	<p>Dlouhodobá archivace elektronických dokumentů a zajištění jejich právní validity.</p>
P.25	<p>Validace platnosti bezpečnostních prvků (elektronické podpisy, elektronické pečete a časová razítka) založených na kvalifikovaných certifikátech. Pro účely archivace 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>
P.26	<p>Možnost nastavení požadované úrovně důvěry při ověřování platnosti bezpečnostních prvků (uznávaný, kvalifikovaný podpis/pečeť).</p>
P.27	<p>Funkce fixace dokumentu formou elektronické pečete/podpisu a/nebo časového razítka. Ověřování elektronické značky/podpisu/pečete a/nebo časového razítka.</p>
P.28	<p>Ověřování certifikátů, na nichž jsou založeny elektronický podpis/značka/pečeť, časové razítko.</p>
P.29	<p>Opatření dokumentů, případně skupiny dokumentů, časovým razítkem. Zajištění periodického prodloužení validity formou automatického přerazítkování.</p>
P.30	<p>Získávání a uchovávání všech relevantních důkazů validity uloženého dokumentu.</p>
P.31	<p>Archivace dokumentů v archivních balíčcích určených pro dlouhodobou archivaci včetně opatření časovým razítkem. Možnosti sdružování libovolných dokumentů do archivních balíčků.</p> <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>
P.32	<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>

#	Požadavek
	<i>Poznámka: Kontrola použití kvalifikovaných certifikátů s platností minimálně celého dotčeného dne je součástí úprav systému EZD.</i>
P.33	<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 hromadně. Při tomto nahrání bude možné pro všechny nahrávané dokumenty společně vybrat šablonu metadat (smlouva, faktura, pracovní výkaz atd.), nebo metadata zadat ručně pro všechny nahrávané dokumenty společně 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.34	<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 vytvářet na základě definované role (správce).</p>
P.35	<p>Notifikace v situacích, kdy z jakéhokoliv důvodu nebude možné nahrát celou dávku dokumentů, či vybraný dokument v této dávce:</p> <ol style="list-style-type: none"> 1. V případě chyby při nahrání dokumentů přes integrační rozhraní zajistí notifikaci uživatelů/správce integrovaný systém. 2. V případě EZD (integrovaný systém) zašle notifikaci EZD na definovanou distribuční skupinu (v případě zdravotnických dat). 3. V případě ručního nahrávání dokumentů uživatelem v rámci EA oznámí EA tuto skutečnost přímo uživateli, který dokument(y) nahrál přes webové rozhraní. <p>Pokud problém vznikne u jednotlivých dokumentů v dávce, budou tyto problematické dokumenty ze strany EA automaticky vyjmuty z dávky a zbytek dávky odešle EA do archivu. Problematické dokumenty pocházející z EZD budou po odstranění vady dokumentu systémem EZD automaticky zpracovány v rámci následující denní dávky. Problematické dokumenty nahrávané přes webové rozhraní budou uživateli vráceny s uvedením důvodu nemožnosti jejich zpracování.</p>
P.36	<p>Řešení umožňuje řízení procesu tvorby balíčků dle různých archivačních politik a charakteru dokumentů jednotlivých agend (více podpisů s různou časovou platností).</p>
P.37	<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.38	<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.39	<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.40	Systém musí zajistit dlouhodobé uložení dokumentů a zajištění čitelnosti uložených informací do doby jejich skartace. Systém musí zajistit důvěryhodné uložení elektronických dokumentů včetně jejich metadat.
P.41	Archiv musí podporovat ukládání a zpřístupňování dokumentace ve formě textových, grafických, audiovizuálních, digitálních nebo jiných obdobných záznamů.
P.42	Systém musí umožňovat archivaci a zobrazování zdravotnické dokumentace ve formátu PDF/A (A-1 – A-3). Mimo zdravotnickou dokumentaci možnost uložení libovolných formátů dokumentů.
P.43	Možnost konverze ukládaných dat do výstupního formátu – PDF/A (A-1 – A-3). V případě konverze dokumentů budou dokumenty uloženy jak v originálním, tak ve výstupním formátu. Konverze se bude vztahovat na dokumenty ve formátu PDF nesplňující výstupní formáty PDF/A a dokumenty ve formátu MS Office.
P.44	Ověřování všech AdES formátů podpisů.
P.45	Univerzální archivační systém umožňující napojení stávajících i v budoucnu pořízených produkčních systémů spravujících a pořizujících zdravotnickou, případně jinou dokumentaci k archivaci. 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. Automatizované vkládání dokumentů ze zdrojových IS pomocí webových služeb.
P.46	Musí být podporovány standardy pro výměnu (zdravotnické) dokumentace HL7, DASTA, SOAP, PDF/A (A-1 – A-3).
P.47	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. Vyhledávání a zpracování archivované zdravotnické dokumentace pacienta přes jeho identifikaci bude řešeno v EZD. Systém EA musí být plně připraven na přechod identifikace pacienta pomocí bezvýznamového identifikátoru po legislativním zavedení takového požadavku.
P.48	Možnost automatizované konverze dat do průmyslových standardů, které budou v budoucnosti požadovány.
P.49	Řešení musí umožnit pracovat se všemi formáty rozšířeného elektronického podpisu (AdES).
P.50	Systém musí zajistit automatické transformace dokumentů k zajištění dlouhodobé archivace a zajištění validity dokumentů v souladu s legislativou.
P.51	Uživatelsky nastavitelná archivační a skartační pravidla pro jednotlivé typy dokumentů. Nastavení archivačních a skartačních pravidel dle požadavků objednatele v rámci dodávky.

#	Požadavek
P.52	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.53	Elektronický archiv disponuje minimálně následujícími funkcemi: <ol style="list-style-type: none"> 1. Příjem SIP balíčku 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.54	Dokument lze smazat pouze auditovatelným způsobem, smazání bude zaznamenáno do logů v rámci auditních služeb (viz kap. 3.4.5).
P.55	Systém musí zahrnovat uživatelské rozhraní pro vkládání a přístup k dokumentaci provozované ve webovém prohlížeči bez nutnosti instalovat přídatné moduly či rozšíření. Uživatelské rozhraní kompatibilní s prostředím objednatele.
P.56	Možnost vyhledávat dokumenty dle metadat dokumentů prostřednictvím uživatelského rozhraní.
P.57	Možnost náhledu na archivované dokumenty prostřednictvím uživatelského rozhraní. Řešení musí umožnit náhled na dokument minimálně těchto formátů: PDF, PDF/A (A-1 – A-3). Ostatní, zde neuvedené formáty, musí uživatel stáhnout a otevřít v jiném prohlížeči mimo archiv.
P.58	Možnost manuálního (neautomatizovaného) vkládání dokumentů uživatelem přes aplikační rozhraní (GUI).
P.59	Řešení musí být napojeno na MS Active Directory a Identity Management Objednatele: <ol style="list-style-type: none"> 1. Synchronizace seznamu uživatelů z MS AD a IdM 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.61). 4. Zamezení přístupu uživateli do EA, který není v MS Active Directory / IdM aktivní, není členem definované skupiny, nebo byl v MS AD / IdM smazán. Není požadováno smazání

#	Požadavek
	<p>uživatele, ale jen zamezení přístupu (min. na úrovni přihlášení). Důvodem je zachování návaznosti dat a logů na uživatele.</p> <ol style="list-style-type: none"> 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 zařazeni jen v příslušné skupině, konkrétní oprávnění rolí bude nastaveno ve EA. 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 Objednatele bude šifrována.
P.60	Přebírání veřejných klíčů komerčních certifikátů uživatelů ze sdíleného úložiště certifikátů (viz kap. 3.4.3) pro potřeby autentizace uživatelů v EA.
P.61	<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 čtečky. c. Veřejný klíč komerčního certifikátu bude převzat z úložiště certifikátů, které je součástí dodávky (viz požadavek P.81). 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.62	Řešení musí umožňovat nastavení a řízení přístupových práv dle rolí uživatele a jeho organizačního zařazení v rámci svého nástroje pro správu oprávnění.

#	Požadavek
P.63	Řešení nesmí být licenčně omezeno na počet nebo typ připojených produkčních systémů; typ archivované dokumentace; počet dokumentů, počet uživatelů nebo zobrazovacích stanic.
P.64	Datové úložiště musí být dimenzováno min. na 5 let provozu a umožňovat následné budoucí rozšíření o další prostory. Úložiště musí umět růst společně s růstem množství ukládaných dat bez nutnosti migrace dat na nové technologie. 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.65	Rozšiřitelnost – EA umožní bezproblémovou a dlouhodobou rozšiřitelnost realizovatelnou bez ohrožení uložených dat.
P.66	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.67	Auditování a logování provozu jednotlivých prvků systému a možnost vyhodnocování min. 1 rok zpětně. Zabezpečení tzv. auditní stopy, řešení automatizovaných činností počínaje označováním dokumentů elektronickými značkami, časovými razítky, jejich validací apod. Auditní záznamy a logy zpřístupňovat ve strukturované formě s parametrizací zadání pro obsah auditního záznamu / logu pro definovanou roli.
P.68	Možnost exportu archiválií do souborového systému jednotlivě nebo hromadně.
P.69	Vstupní konektory: <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.70	Centrální mezipaměť (cache) <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.71	Komprese ukládaných dokumentů
P.72	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.73	Řešení musí vycházet z referenčního modelu OAIS a musí 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.74	Podpora definování intervalů, po které není možné dokument smazat ani nijak pozměnit (retenční doba).
P.75	Správa uživatelských účtů bude v EZD, včetně certifikátů potřebných pro autentizaci/přihlašování uživatelů do EA dle požadavku P.61. Napojení na správu uživatelů a na úložiště a správu certifikátů požadovaném v kap. 3.4.3, požadavku P.81.
P.76	Systém musí být připraven na provoz 24x7x365 (non-stop).

Tabulka 5: Požadavky: Dodávka elektronického archivu organizace (EA)

3.4.3 Úpravy a napojení EZD na elektronický archiv

Požadavky na tuto část předmětu plnění jsou následující:

#	Požadavek
Elektronické podepisování	
P.77	Zajištění přístupu k úložišti s kvalifikovanými certifikáty a podepisování dokumentů uznávaným elektronickým podpisem v souladu s legislativou. V případě, že je třeba dodat obslužný software nebo ovladače pro realizaci podpisu na základě certifikátu z úložiště, je součástí dodávky i tento SW pro všechna mobilní zařízení (tablety).
P.78	Pokud bude vyžadován podpis na dokumentu od jiné osoby (bez kvalifikovaného certifikátu), bude zajištěna možnost podepsat dokument biometrickým/viditelným digitálním podpisem na mobilním zařízení (tabletu). Následně bude podepsán uznávaným elektronickým podpisem oprávněného pracovníka ZZS, který tím potvrdí platnost dokumentu s viditelným el. podpisem.
P.79	Dokumenty po podpisu uznávaným elektronickým podpisem jsou pak uzamčeny proti změně a systém nesmí umožnit jejich úpravy (zamezení pozměňování dokumentace). Případné změny ve zdrojových datech bude vytvořena nová kompletní verze dokumentu nebo dodatek obsahující změny v dokumentu a výsledný dokument bude následně podepsán v souladu s dalšími požadavky.
Certifikáty	
P.80	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.81	Zajištění správy a ukládání komerčních certifikátů v EZD pro potřeby autentizace uživatelů: <ol style="list-style-type: none"> 1. Napojení úložiště komerčních certifikátů ve správcovském nástroji EZD. 2. Dodávka integračního rozhraní pro čtení certifikátů vnitřními systémy ZZS (např. EA). Zajištění čtení z integračního rozhraní na základě oprávnění daného IS. 3. Čtení a ověřování certifikátů v EZD vůči tomuto úložišti. <p>Další požadavky jsou uvedeny v kap. 3.4.6.</p>

#	Požadavek
Správa přístupů	
P.82	<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 EZD. Uživatelé EZD budou zařazeni do definované skupiny v MS AD, načítat se budou jen uživatelé zařazení do skupiny určené pro EZD. 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 EZD (EKP i MZD) budou přihlašovat svým komerčním certifikátem nebo dočasným heslem (viz požadavek P.84). 4. Zamezení přístupu uživateli do EZD, 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 / IdM a jeho následně aktivace se tyto změny musí projevit v EZD při zachování všech oprávnění a historických dat. 6. V MS AD budou uživatelé zařazení jen v příslušné skupině, konkrétní oprávnění rolí bude nastaveno ve EZD. 7. Pokud bude uživatel jen ve skupině MS AD pro přístup do EZD, ale v EZD mu nebudou nastavena konkrétní oprávnění, bude mu umožněno přihlášení, ale nebude mít k dispozici data a funkcionality. 8. Počet neúspěšných přihlášení 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 / IdM Objednatele bude šifrována.
P.83	<p>Přebírání veřejných klíčů komerčních certifikátů uživatelů ze sdíleného úložiště certifikátů (viz kap. 3.4.3) pro potřeby autentizace uživatelů v EZD.</p>
P.84	<p>Autentizace/přihlašování uživatelů do EZD:</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 čtečky. c. Veřejný klíč komerčního certifikátu bude převzat z úložiště certifikátů, které je součástí dodávky (viz požadavek P.81). 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 EZD (EKP). Toto heslo bude zasláno na email uživatele (vnitřní email Objednatele – z AD), který do EZD přistupuje (přihlašuje se). Platnost takto generovaného hesla musí být parametrizovatelná správcem. Vygenerované

#	Požadavek
	<p>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).</p> <p>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 EZD (notifikace na definovaný email), který bude moci vzdáleně příslušný účet odblokovat a vygenerovat nové dočasné heslo.</p>
Archivace dokumentace vytvořené v EZD	
P.85	<p>Vytváření, podepisování a předávání následujících typů dokumentů do EA:</p> <ol style="list-style-type: none"> 1. Záznam o výjezdu od posádky (jen elektronicky podepsaný originál). 2. Záznam o výjezdu po zpracování a podpisu kontrolním oddělením – po provedených úpravách, včetně skenu/konverze záznamu o výjezdu od posádky (pokud je dokument v listinné podobě), automatizované vytvoření a vyžádání elektronického podpisu uživatele. 3. 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). 4. 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.86	<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.87	<p>Součástí předávané dokumentace mohou být i nepodepsané přílohy, např. PDF, multimediální dokumentace (obrázky, videa, zvukový záznam) apod.</p>
P.88	<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.89	<p>Součástí archivované dokumentace budou následující údaje (metadata):</p> <ol style="list-style-type: none"> 1. Identifikace výjezdu, číslo události, 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 narození pacienta 4. Datum a čas vzniku dokumentu.

#	Požadavek
	<p>5. Autor dokumentu – identifikace uživatele z EZD, login z MS Active Directory, jméno, příjmení.</p> <p>6. Identifikace vozidel v rámci výjezdu (může být více vozidel, v tom případě budou čísla oddělena čárkou).</p> <p>V rámci implementační analýzy může dojít k doplnění metadat na základě procesních potřeb archivace.</p>
P.90	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.91	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 spojením 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.92	V EZD udržovat validní odkaz na dokumenty v EA.
P.93	Možnost zobrazit přehled archivované dokumentace k výjezdu v EZD (pouze na úrovni EKP).
P.94	Možnost vyhledávání v archivované dokumentaci dle uložených metadat (viz požadavek P.89).
P.95	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.96	<p>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.</p> <p>Pokud je dokument již stažen do dočasného úložiště EZD, nestahovat opakovaně a zobrazit z tohoto dočasného úložiště.</p> <p>Takto stažené dokumenty automaticky mazat po 5 dnech od jejich posledního zobrazení. Doba uložení bude konfigurovatelný parametry, výchozí hodnota bude 5 dnů.</p>
Ostatní požadavky	
P.97	Archivace dokumentace a práce s archivovanou dokumentací musí být realizována tak, aby výpadek EA neměl negativní dopad na poskytování ostatních služeb EZD.

Tabulka 6: Požadavky: Úpravy a napojení EZD na elektronický archiv

3.4.4 Dodávka nezbytné provozní infrastruktury a systémového SW pro dodávané systémy

V této kapitole jsou uvedeny požadavky na dodávky nezbytné provozní infrastruktury a nezbytného systémového SW pro dodávané systémy.

Žadatel nepředepisuje technologii, jen principy a požadavky na řešení. Technologie bude navržena dodavatelem v nabídce v rámci veřejné zakázky.

HW a SW infrastrukturu není možné v tomto dokumentu dostatečně specifikovat, protože jsou závislé na zvolené technologii v rámci řešení konkrétního uchazeče. Zde jsou stanoveny limitní podmínky, které musí

uchazeč splnit, tj. nejen technologické podmínky v DC, technologie využívané žadatelem, ale i požadavky na min. doby pro ukládání dat a v návaznosti na splnění těchto podmínek a potřeb technologie, uchazeč navrhne, nabídne a dodá vhodnou HW a SW infrastrukturu.

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

#	Požadavek
P.98	Infrastruktura pro IS ZOS zůstane beze změny, úpravy musí být funkční a provozované společně se stávajícím systémem na stávající infrastruktuře IS ZOS.
P.99	Infrastruktura pro EZD zůstane beze změny, úpravy musí být funkční a provozované společně se stávajícím systémem na stávající infrastruktuře EZD.
P.100	EA bude provozován jako jedna instance služby.
P.101	Infrastruktura pro Systém musí být připravena na provoz 24x7x365 (non-stop).
P.102	Infrastruktura a systémový SW musí být kompatibilní s prostředím objednatele uvedeném ve výchozím stavu.
P.103	<p>Zadavatel umožňuje dodavateli využít stávající HW infrastrukturu pro EA ve virtuálním prostředí VMware 6.0 v rozsahu max. 6 vCPU, 12 GB RAM, 500 GB v rámci dodávky a navýšení na 1 TB během provozu na disku pro všechny potřebné virtuální servery pro dodávané řešení společně (dále jen „poskytovaná HW infrastruktura“).</p> <p>V případě, že poskytovaná HW infrastruktura není dostatečná pro řešení dodavatele, případně není vhodná z důvodu specifického licencování systémového SW, dodavatel nabídne a dodá rozšíření HW infrastruktury tak, aby plnila uvedené požadavky a podmínky dodávaného řešení.</p>
P.104	<p>V případě, že dodavatel bude dodávat vlastní HW infrastrukturu, musí servery plnit následující minimální podmínky:</p> <ol style="list-style-type: none"> 1. Instalace do racku 2. Servery – minimální požadavky <ol style="list-style-type: none"> a. Min. 2 zdroje pro napájení b. Min. 2x 10 GB optické rozhraní c. Management karta 3. Diskové pole – minimální požadavky <ol style="list-style-type: none"> a. Redundantní diskové pole b. Připojení do virtualizačního prostředí (FB) c. Možnost dalšího rozšiřování 4. Dodávka včetně veškerého příslušenství pro zapojení 5. Záruka a servis min. 3 roky, NBD
P.105	<p>Zadavatel požaduje, aby všechny servery pro provoz dodávaného systému byly virtualizované na HW infrastruktuře.</p> <p>V případě, že dodavatel potřebuje pro své řešení fyzickou HW infrastrukturu, musí ve své nabídce toto řešení dostatečně odůvodnit (např. zásadně vhodnějšími licenčními podmínkami využívaného systémového SW), v případě, že takové řešení nebude dostatečně odůvodněné, bude zadavatel považovat tento požadavek za nesplněný.</p>

#	Požadavek
P.106	Virtualizace: V případě, že dodavatel dodá vlastní HW infrastrukturu, musí dodat licence a služby pro virtualizaci pro dodávanou HW/virtuální infrastrukturu, včetně servisních služeb po dobu záruky.
P.107	Zadavatel umožňuje dodavateli využít licence operačních systémů objednatele MS Windows 2019 pro EA v rozsahu poskytované HW infrastruktury dle požadavku P.103 (dále jen „poskytované licence OS“). V případě, že poskytovaná HW infrastruktura a poskytované licence OS nejsou dostatečné pro řešení dodavatele, případně nejsou vhodné z důvodu specifického licencování systémového SW (OS), dodavatel nabídne a dodá operační systémy tak, aby plnily uvedené požadavky a podmínky dodávaného řešení, včetně servisních služeb po dobu záruky.
P.108	Kapacita úložiště pro data bude stanovena dodavatelem dle parametrů uvedených v kap. 6.2, 6.3 a nároků a potřeb jeho řešení.
P.109	Dodávka licencí a instalace SW databází (DB): Pokud řešení vyžaduje dodávku licencovaného SW pro DB, jsou součástí dodávky i licence těchto DB (např. ORACLE, MS SQL). Dodávka DB SW pro potřeby dodávaného řešení tak, aby DB byla výkonově a kapacitně dostatečně dimenzovaná na 5 let provozu EA s uvedeným objemem dat a počtem uživatelů (kap. 6.2 a 6.3), včetně servisních služeb po dobu záruky.
P.110	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.111	Zálohování – systém (OS) a DB musí být schopny a připraveny na zálohování objednatelem, tj. pro OS a DB musí umožňovat zálohování. <i>Integrace do systému zálohování objednatele není součástí dodávky, konfiguraci si zajistí objednatel. Zhotovitel poskytne parametry, podmínky a součinnost při nastavení zálohování dodaného řešení.</i>
P.112	Prostředí pro Systém musí zajistit zabezpečené připojení jak integrovaných systémů, tak uživatelů Systému min. na úrovni SSL.
P.113	Zajištění administrátorských aplikací, konzolí pro všechny součásti systému (virtualizace, OS, DB atd.) pro zajištění konfiguračního managementu systému anebo jeho součástí.
P.114	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.115	Šifrování úložišť v rámci operačních systémů, kde jsou uložena data systému.
P.116	Dodávka, zapojení, instalace technologií, instalace a zprovoznění modernizovaného IS na dodaných technologiích.
P.117	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.118	Architektura řešení celého systému musí korespondovat s požadavky na jeho dostupnost.

#	Požadavek
P.119	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 po celou dobu dodávky dle SoD a poskytování služeb dle servisní smlouvy.

Tabulka 7: Požadavky: Dodávka nezbytné provozní infrastruktury a systémového SW pro dodávané systémy

3.4.5 Auditní služby

Požadavky na tuto část plnění jsou následující:

#	Požadavek
P.120	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.121	Řešení umožní poskytovat auditní reporty o přístupech uživatelů (kdo, kdy, období, kam) na základě parametrizace prováděné pověřeným auditorem.
P.122	Auditní (logovací) aparát je dostupný pouze určené roli (auditor). Není dostupný a manipulovatelný uživateli, administrátory ani správci.
P.123	System 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.124	Auditní systém musí být v souladu s nařízením EU o ochraně osobních dat (GDPR).

Tabulka 8: Auditní služby

3.4.6 Bezpečnostní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.125	Uživatelé systému jsou zavedeni v MS Active Directory a Identity Managementu (IdM) Objednatele (výchozí stav). Přístup do systému EZD (zařazení do relevantní role) je poskytován s využitím aplikace pro správu přístupů (viz požadavek na tuto aplikaci dále). Všichni uživatelé zůstávají v systému i po ukončení platnosti jejich účtu bez přístupu k systému. Uchování neaktivního uživatele (zánik objektu v MS AD / IdM) je pro potřeby uchování historie.
P.126	Autentizace uživatele bude probíhat primárně použitím komerčního certifikátu, uloženým společně s kvalifikovaným certifikátem pro elektronický podpis na úložišti pro kvalifikované a komerční certifikáty, alternativně použitím dočasného hesla (viz následující požadavek). Přihlašování pomocí komerčního certifikátu: EZD ověří shodu přístupového jména a vyžádá si poskytnutí privátní části komerčního certifikátu uloženého v kvalifikovaném úložišti certifikátů (zadání 6-ti místného PIN). Následně je ověřen proti aplikačnímu serveru, kde ověří příslušné role uživatele. Oba certifikáty budou mít stejnou časovou platnost. Informace o zbývajícím času platnosti certifikátu se po ověření uživatele budou zobrazovat uživateli v aplikaci MZD i aplikaci EKP.
P.127	Zavedení provozního módu pro práci při absenci certifikátu pro přihlášení – např. zapomenuté úložiště pro kvalifikované a komerční certifikáty. Systém musí umožňovat vygenerovat

#	Požadavek
	<p>pro uživatele dočasné přístupové heslo (automatický proces) a to na základě inicializace této žádosti uživatelem na stacionárním pracovišti EZD). Toto heslo bude zasláno na email uživatele (vnitřní email Objednatele – z AD), který do aplikace MZD, resp. EZD přistupuje (přihlašuje se). Platnost takto generovaného hesla musí být parametrizovatelná aplikačním administrátorem (viz tabulka rolí).</p> <p>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 aplikace (notifikace na definovaný email), který bude moci vzdáleně příslušný účet odblokovat a vygenerovat nové dočasné heslo.</p>
P.128	<p>Dodání a zavedení aplikace pro správce přístupů s následujícími funkcemi:</p> <ol style="list-style-type: none"> 1. Import uživatelů z AD 2. Zařadit/změnit uživatele do konkrétní role, případně více rolí 3. Povolit / zablokovat přístup danému uživateli do systému EZD 4. Zobrazit konec platnosti certifikátů 5. Zobrazení data/času zařazení uživatele do role 6. Zobrazení data/času posledního přihlášení uživatele 7. Třídění/filtrování podle všech atributů
P.129	<p>Dodání a zavedení aplikace pro správce certifikátů s následujícími funkcemi:</p> <ol style="list-style-type: none"> 1. Import uživatelů z AD, 2. Přiřadit/odebrat konkrétnímu uživateli certifikáty (komerční i kvalifikovaný) – veřejné části těchto certifikátů, 3. Zobrazit konec platnosti certifikátů, 4. Třídění/filtrování podle všech atributů
P.130	<p>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>
P.131	<p>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>
P.132	<p>Řešení musí být připraveno na plnění podmínek zákona č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů.</p>
P.133	<p>Autorizace: Poskytnutí přístupu autentizovaného uživatele k aktivu systému (data, aplikace), odpovídající pracovnímu zařazení uživatele a přidělené roli (rolím) v systému.</p> <p>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.</p>

#	Požadavek
P.134	Zabránění vstupu neautorizovaného subjektu do systému – zamezení možnosti přístupu neoprávněného subjektu.
P.135	Zajištění konfiguračního managementu a správy systému s eliminací rizika ovlivnění chodu systému změnou aplikací 3. stran (unifikace konfigurací serverů, řízený patch management).
P.136	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.137	Zajištění šifrované komunikace mezi všemi součástmi systému a pracovišti uživatelů, případně zajištění komunikace v odděleném síťovém prostředí.
P.138	<p>Veškeré komunikační kanály budou zdokumentovány v rámci matice komunikací a budou součástí dokumentace skutečného provedení a následně udržována jako aktuální v rámci provozu.</p> <p>Součástí matice bude minimálně zdrojový systém, cílový systém, IP adresy, případně názvy, porty, protokoly, způsob zabezpečení dané komunikace (např. SSL), autentizace a ověřování komunikace a účel dané komunikace.</p> <p>V rámci provozu systému budou povoleny jen a pouze komunikační kanály, které budou součástí schválené matice. Případné změny komunikačních kanálů podléhají schválení objednatele.</p> <p>Zpracování matice a principu správy komunikačních kanálů bude součástí implementační analýzy a návrhu řešení s tím, že v rámci dokumentace systému bude aktualizována a předána v konečné verzi.</p>
P.139	Evidence přístupů všech uživatelů do systému (logování) včetně časových údajů.
P.140	Veškeré přístupy k datům a aktivita 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.141	Veškerá komunikace je a bude zajišťována prostřednictvím zabezpečených (šifrovaných kanálů), případně zajištění komunikace v odděleném síťovém prostředí.
P.142	Zabezpečení dat – zabezpečení pomocí řízení přístupu k datům, použití šifrování a ostatních kryptografických prostředků, audit logových záznamů
P.143	Veškeré bezpečnostní logy budou dostupné i pro externí logmanager/SIEM.

Tabulka 9: Bezpečnostní požadavky

3.4.7 Implementační a provozní požadavky

V následující tabulce je seznam požadavků na tuto část dodávky:

#	Požadavek
P.144	Systém musí být připraven na provoz 24x7x365 (non-stop).

#	Požadavek
P.145	<p>V rámci řešení jsou požadované následující provozní podmínky řešení:</p> <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. Tento režim bude zajištěn objednatelem v rámci virtualizace. 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. 4. Odolnost proti katastrofě – systém bude provozován na vysoce dostupné, případně redundantní infrastruktuře – předmět dodávky. 5. Vysoká bezpečnost – viz předchozí kapitola.
P.146	<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. <p>Minimální požadované počty jsou uvedené v kap. 6.2 – Uživatelé. Dodávka musí zajistit funkčnost pro uvedený počet uživatelů.</p>
P.147	<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 hodnoty uvedené v 6.3. 2. EA – odhad objemu zpracovávaných dat je uveden v kap. 6.3 – Počty a množství zpracovávaných dat. <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. 5 let s možností rozšiřování kapacity.</p>
P.148	<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.149	<p>Instalace do prostředí objednatele a na požadovanou infrastrukturu dle kap. 3.4.4 – Dodávka nezbytné provozní infrastruktury a systémového SW pro dodávané systémy a 6.4 – Stav informačních a komunikačních technologií.</p>
P.150	<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</p>

#	Požadavek
	popíše postup přechodu systémů. Dodavatel je povinen přizpůsobit realizaci předmětu zakázky podmínkám objednatele.
P.151	Všechny součástí systému (OS, DB, IS, klientské aplikace) musí logovat svou činnost do logů s možností nastavit úroveň logování pro potřeby diagnostiky.
P.152	Zajištění zálohování a obnovy v souladu s legislativou a provozními požadavky na Systém a dodávané technologie. 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.153	Zajištění administrátorských aplikací, konzolí pro všechny součástí 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.154	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.155	Architektura řešení celého systému musí korespondovat s požadavky na jeho dostupnost, uvedenými v servisní smlouvě.
P.156	Synchronizace času všech zařízení s Objednatelem určeným time serverem nebo zprostředkovaně přes centrální systém.
P.157	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 10: Provozní požadavky

3.5 POŽADAVKY NA SLUŽBY

3.5.1 Realizace předmětu plnění

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

- 1) 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:
 - a) Implementační analýza – zjištění týkající se prostředí objednatele, bude obsahovat alespoň 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 alespoň:

- 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 4 - Harmonogram, 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 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 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 11: 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.

- 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.

3.5.2 Seznámení s funkcionalitami, obsluhou dodávaného systému

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

- 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 musí být zahrnuty v ceně odpovídající části předmětu dodávky.

3.6 ZÁRUKY

V této kapitole jsou uvedeny požadavky na záruky dodávky jako celku, případně specificky dílčích částí dodávky.

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

- a) 60 měsíců na informační systém(y), aplikace a služby spojené s realizací projektu,
- b) 36 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 opotřebením. 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 60-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 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.

4 HARMONOGRAM

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.

Tabulka 12: Harmonogram

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.

5 MÍSTA PLNĚNÍ

Realizace předmětu plnění bude probíhat v následujících místech plnění:

Místo	Adresa	Předmět realizace
Zdravotnická záchranná služba Karlovarského kraje, příspěvková organizace	Závodní 390/98C, Karlovy Vary PSČ: 360 06	<u>Datové centrum ZZS KVK</u> – návaznost na technologie umístěné v tomto datovém centru a dodávka technologie dodávané v rámci Díla. Dodávka EA a technologií a poskytnutí služeb k EA v rámci dodávky technologie umístěné do této lokality. <u>Sídlo ZZS KVK</u> – místo předání výstupů dodávek.
	<u>Území</u> <u>Karlovarského</u> <u>kraje</u>	Dodávka úprav EZD pro výjezdové skupiny a souvisejících technologií a poskytnutí služeb k EZD.

Tabulka 13: Místa plnění

6 VÝCHOZÍ STAV

V této kapitole je uveden výchozí stav a výchozí podmínky pro dodávku předmětu plnění.

6.1 ZDRAVOTNICKÁ ZÁCHRANNÁ SLUŽBA KARLOVARSKÉHO KRAJE, PŘÍSPĚVKOVÁ ORGANIZACE (ZADAVATEL)

Kontext ZZS KVK v rámci řešení projektu je následující:

1. ZZS KVK plní úkoly k zajištění zvláštní zdravotní péče fyzickým osobám, které se náhle nebo nečekaně ocitly v ohrožení zdraví či života, tedy nepřetržitě zabezpečuje odbornou přednemocniční neodkladnou péči včetně přednemocniční péče o dárce a příjemce orgánů v souladu s příslušnými právními předpisy a pokyny zřizovatele a za plnění těchto úkolů odpovídá.
2. V rámci svých činností ZZS zajišťuje kvalifikovaný příjem, zpracování a vyhodnocení tísňových výzev k odborné zdravotnické první pomoci a určení nejvhodnějšího způsobu poskytování přednemocniční neodkladné péče.
3. V rámci provozu ZZS KVK vzniká dokumentace, která vyžaduje archivaci. Jedná se o elektronickou zdravotnickou dokumentaci a ostatní dokumentaci, která vzniká v rámci běžného provozu ZZS.

V následujícím textu je uveden současný stav informačních systémů, aplikačního SW, pracovišť, technologií a další relevantní informace.

6.2 UŽIVATELÉ

V následující tabulce jsou uvedeny orientační počty současných uživatelů:

Skupina	Počet	Doplňující informace
Uživatelé/operátoři ZOS	5	Současně pracující operátoři na ZOS.
	35	Celkový počet operátorů v rámci zajištění směnného provozu.
Posádky/uživatelé EZD	400	Jedná se o maximální počet členů posádek v rámci směnného provozu pro systém EZD.
Uživatelé EA	100	Jedná se o maximální počet uživatelů přistupujících přes GUI do EA. Uživatelé EZD nepřistupují do EA přes GUI, ale cestou EZD.
Správci	5	Správci technologie a informačních systémů.

Tabulka 14: Výchozí stav: Uživatelé

6.3 POČTY A MNOŽSTVÍ ZPRACOVÁVANÝCH DAT

V této kapitole je uvedeno množství zpracovávaných dat:

Oblast	Množství
Počet výjezdů	Cca 150 / den (průměrně) Cca 55.000 / rok Roční nárůst cca 10 %

Oblast	Množství
Dokumenty z EZD (k výjezdům)	<p>Ke každému výjezdu/události/zásahu budou archivovány typicky 3 sady dokumentace (záznam o výjezdu, přílohy, change listy).</p> <p>Průměrná velikost kompletní sady dokumentace k jednomu výjezdu: 7 MB</p> <p>10 % výjezdů bude mít průměrně 6 sad dokumentace, tj. kompletní sada dokumentace bude mít 14 MB.</p> <p>Roční nárůst cca 10 %</p>
Ostatní dokumentace	<p>Cca 5.000 / rok</p> <p>Průměrná velikost sady dokumentace: 7 MB</p> <p>Roční nárůst cca 10 %</p>

Tabulka 15: Množství zpracovávaných dat

6.4 STAV INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

V této kapitole je uveden základní popis výchozího stavu jednotlivých systémů a prvků stávajícího řešení.

6.4.1 Informační systémy a aplikační software ZZS KVK

V této kapitole je uveden výchozí stav informačních systémů a aplikačního software ZZS KVK:

IS, SW, subsystém	Výchozí stav
IS ZOS / IS OŘ	<p>Jedná se o produkt SOS společnosti PER4MANCE s.r.o. využívaný u více ZZS v ČR a min. jedné zahraniční ZZS (Maďarsko), tj. jedná se o široce používaný a standardizovaný produkt/systém.</p> <p>SOS je systém pro operační řízení dispečinku Zdravotnické záchranné služby (ZZS). Systém byl vyvinut na základě dlouhodobých zkušeností s provozem krajských ZZS se zahrnutím moderních požadavků na efektivní řízení Krajských záchranných operačních středisek (ZOS). Poskytuje funkcionalitu pro všechny činnosti ZOS ZZS počínaje náběrem tísňové výzvy (calltaking) přes operační řízení po vyhodnocení činnosti ZOS.</p> <p>Součástí je řada dalších důležitých funkcionalit, které jsou popsány v dokumentaci k IS.</p> <p>IS ZOS je napojen na systém elektronické zdravotnické dokumentace (EZD) a předává do tohoto systému data k výjezdům pro posádky v terénu, které jsou následně v tomto systému zpracovány.</p> <p>Součástí předávaných informací jsou potřebné údaje získané z tísňové výzvy a nezbytné pro posádky v rámci poskytování PNP.</p> <p>Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.</p> <p>Funkcionalita nebude předmětem změny v rámci dodávky Díla.</p>
EZD	<p>Jedná se o produkt společnosti European Medical Distribution s.r.o. (EMD) dodaný a využívaný většinou ZZS v ČR.</p> <p>Systém EZD se skládá z centrální části nazvané Elektronické karta pacienta (EKP), která slouží pro zaznamenávání všech relevantních údajů o výjezdech a pacientech</p>

IS, SW, subsystém	Výchozí stav
	<p>v rámci těchto výjezdů, Mobilního zadávání dat (MZD) sloužící pro zadávání dat o pacientech v rámci výjezdu ZZS v terénu prostřednictvím mobilních zařízení (tabletů) a následně jejich předávání do centrálního systému EKP pro následné zpracování a IS Pojišťovna, který slouží pro vyúčtování poskytnuté zdravotnické péče zdravotním pojišťovnám.</p> <p>Data jsou na vstupu čerpána z IS ZOS/OŘ a následně během nebo po ukončení výjezdu z MZD, kontrolována a následně zpracována do formy pro vykazování pojišťovnám.</p> <p>Systémy poskytují následující funkce:</p> <ol style="list-style-type: none"> 1. Přebírání dat o výjezdu z IS ZOS/OŘ (integrace). 2. Posílání dat do mobilních zařízení posádek v terénu. 3. Funkčnost pro vyplnění posádkami v terénu. 4. Předání z MZD zpět do EKP. 5. Přebírání dat ze systému sledování vozidel (integrace). 6. Následné úpravy, dopracování, kontrola dat na výjezdových základnách. 7. Následné úpravy, dopracování, kontrola dat na oddělení pojišťoven. 8. Vykazování pojišťovnám. <p>Součástí je řada dalších důležitých funkcionalit, které jsou popsány v dokumentaci k IS.</p> <p>V rámci tohoto systému vzniká elektronická zdravotnická dokumentace v souladu s legislativou. Archivace této dokumentace je primárním cílem této dodávky a tvoří naprostou většinu objemu elektronické dokumentace k archivaci.</p> <p>Subsystém je plně funkční a jeho funkčnost musí být zachována min. v rámci současného stavu, a to jak v rámci realizace projektu, tak v případě mimořádných událostí a krizových situací.</p> <p>Funkcionalita musí být doplněna dle požadavků uvedených v kap. 3.4.3 – Úpravy a napojení EZD na elektronický archiv.</p>
Elektronický archiv organizace (EA)	ZZS KVK nedisponuje žádným elektronickým archivem organizace (EA) pro archivaci elektronické zdravotnické dokumentace a ostatní dokumentace.
Sdílené úložiště certifikátů	ZZS KVK v současné době nedisponuje samostatným systémem pro uchovávání certifikátů.
Registrační certifikační autorita	ZZS KVK v rámci jiného projektu zajistí registrační certifikační autoritu. Certifikační autorita bude vystavovat pro personál jak kvalifikované certifikáty pro uznávaný elektronický podpis v EZD, případně jiných IS, tak komerční certifikáty, které budou využívány pro autentizaci uživatelů do EZD.
Certifikáty	Certifikáty budou nahrány na kvalifikovaných prostředcích ve standardu QESCD v souladu s legislativou. Tyto prostředky jsou připojovány k PC/notebookům přes čtečky.
Infrastruktura	Stávající infrastruktura IS ZOS a EZD zůstane zachována beze změny, tj. nebude dotčena dodávkou a není tedy relevantní.

Tabulka 16: Výchozí stav: Informační systémy a aplikační software ZZS KVK

6.4.2 Datové sítě

V rámci projektu budou využity následující sítě:

Datová síť	Popis
LAN + WAN ZZS	Bude využita pro komunikaci mezi IS ZOS a EZD, EZD a EA a pro přístup uživatelů k EA. LAN ZZS je propojena s KI a tím i zprostředkovaně k dalším externím sítím. Základem LAN infrastruktury lokality Karlovy Vary jsou dva vysoce dostupné stohy přepínačů HPE, z nich jeden tvoří jádro sítě a zajišťuje vzájemnou komunikaci serverů rychlostí 10 Gb a druhý tvoří distribuční vrstvu LAN pro napojení dalších technologií a koncových zařízení rychlostí 1 Gb. Celkově je v LAN provozováno 6 síťových přepínačů HPE 1950 a HP5120.
Internet	Bude povolena jen zabezpečená komunikace na stanovené IP adresy, případně rozsahy adres. Připojení prostřednictvím KI k ISP O2 Czech Republic je využíváno jak pro primární připojení do sítě Internet tak i pro VPN přístup a realizaci VPN sítě ZZS. Sekundární (záložní) internetové konektivita je zajišťována společností Wolfnet.

Tabulka 17: Datové sítě

6.4.3 Ostatní relevantní technologie

V následující tabulce jsou uvedeny ostatní technologie relevantní pro dodávku předmětu plnění:

Oblast	Technologie	Doplňující informace
Pracovní a klientské stanice uživatelů	MS Windows 10 Google Chrome v aktuální verzi MS Edge v aktuální verzi	Aplikace (klient EA) pro uživatele musí být funkční na těchto technologiích.
Tablety a mobilní prostředky	MS Windows 10 MS Windows 8.1	Systém EZD nadále musí být funkční na těchto OS.
Servery – výrobci	Dell R740	Pokud bude dodavatel dodávat vlastní infrastrukturu, musí být infrastruktura kompatibilní s těmito servery a musí zajistit obdobnou správu.
Disková pole	HP P4300 Storage	Pokud bude dodavatel dodávat vlastní infrastrukturu, musí být infrastruktura kompatibilní s těmito servery a musí zajistit obdobnou správu.
Virtualizační platforma	VMware vSphere 6.0 a HPE StoreVirtual	Pokud bude dodavatel dodávat tuto technologii, požaduje objednatel v rámci dodávky kompatibilní řešení.
Zálohování a dostupnost	Veeam	Pokud bude dodavatel dodávat tuto technologii, požaduje objednatel v rámci dodávky kompatibilní řešení.

Oblast	Technologie	Doplňující informace
Operační systémy na serverech	Objednatel provozuje systémy na OS MS Windows (Datacenter, Standard 2012R2 a vyšší), Linux Ubuntu	Je požadována dodávka na těchto operačních systémech.
Správa uživatelů	MS Active Directory (MS AD) Identity Management (IdM)	Objednatel využívá pro autentizaci Active Directory se stromovou i doménovou úrovní Windows Server 2012. V rámci souběžného projektu bude dodán Identity Management systém, typ a integrační rozhraní budou poskytnuty v rámci implementační analýzy. Objednatel poskytne přístup k těmto systémům pro propojení a případná nastavení.
Certifikační autorita	Bude doplněna v rámci dodávky	Certifikační autorita a způsob jejího napojení bude doplněno v rámci dodávky.
Dohled	Nevyužívá se, bude zaveden mimo dodávku	Zhotovitel poskytne vstupy pro dohled nad během systému jako celku, nastavení dohledu zajistí objednatel.
Vzdálený přístup	VPN	Konkrétní typ a podmínky využití budou poskytnuty v rámci součinnosti. Vzdálený přístup pro management prostředí bude umožněn pomocí VPN objednatele.
Databáze	Objednatel využívá databázové technologie MS SQL pro EZD a ORACLE DB pro ZOS.	Pokud bude dodavatele dodávat databázovou technologii, jedná se o preferovanou technologii.

Tabulka 18: Ostatní relevantní technologie

KONEC ZÁKLADNÍ ČÁSTI DOKUMENTU