

I. Technická a funkční specifikace

Technická a funkční specifikace vychází z dokumentu Studie proveditelnosti projektu „Výstavba, implementace a technická podpora ICIS OZP“ (dále jen „**Studie proveditelnosti**“) a předkládá souhrn strategických požadavků na dílo. Dále obsahuje popis prostředí (infrastruktury) do něhož bude dílo nasazeno. Studie proveditelnosti včetně všech příloh tvoří přílohu a nedílnou součást této podrobné specifikace předmětu veřejné zakázky. Vlastní „tělo“ Studie proveditelnosti (tj. popisná část Studie proveditelnosti bez příloh) je přikládána k zadávacím podmínkám veřejné zakázky pouze jako „informativní a nezávazná“ příloha. Jednotlivé přílohy Studie proveditelnosti však představují závazné požadavky na dílo.

A. Funkční specifikace

1. Strategické požadavky na ICIS

Mezi primární strategické požadavky na ICIS, které zásadním způsobem mění stávající postupy, patří následující požadavky:

- a) Nový ICIS musí mít minimálně stejný rozsah funkcí a vlastností jako stávající systém OZP. ICIS musí zajistit rozšíření a zefektivnění stávajících funkcí a jejich optimalizaci a implementaci nových klíčových podpůrných procesů.
- b) Návrh datové struktury (DB modelu) ICIS musí být proveden tak, aby bylo zamezeno vzniku duplicit a nekonzistence dat v celém systému s důrazem na registry.
- c) Nový ICIS musí být navržen tak, aby byla zajištěna standardizace a prokazatelnost základních procesů zdravotní pojišťovny.
- d) Proces náhrady stávajícího CIS za nový ICIS nesmí ohrozit ani omezit kvalitu a plynulost činnosti OZP vůči všem typům partnerů.
- e) Veškerý vývoj uživatelských rozhraní a výstupů, obsah a uspořádání menu, formát a grafika formulářů, ovládání a navigace, budou řešeny pro každý modul, funkcionalitu či formulář vždy na základě předem odsouhlaseného návrhu, pokud to bude např. s ohledem na potřebu ergonomie vhodné, ve formě funkčního prototypu (v intencích globálně dohodnutých pravidel zohledňujících technické možnosti SW platformy) s naznačením chování ovládacích prvků, popř. výběrem možných variant.
- f) Strategické požadavky na oblast Registry OZP:
 - přístup k registrům - do určité úrovně musí být základní evidence subjektu společná – tzv. „Zobecněné registry“ (např. IČ, RČ), od určité úrovně pak mohou existovat specifické evidenční nadstavby v rámci jednotlivých agend, pro specifické role téhož subjektu (např. IČZ-IČP),
 - registr (PZS a i jiné) musí umožnit více odlišných vztahů s různou analytickou a fondovou evidencí.
- g) Strategické požadavky na oblast Výdajová část:
 - požaduje se řešení zpracování kontroly vykázané péče, včetně provádění závěrečného vyúčtování a regulací standardizovaným a transparentním způsobem na uživatelské úrovni s protokolováním všech změn a úprav,
 - požaduje se, aby všechny předpisy na pohledávky a závazky související s úhradami zdravotních služeb vznikaly ve výdajové části na základě různého vstupního rozhraní

včetně všech smluvních a specifických výdajů např. i na základě ručního zadání (např. faktury za očkovací látky od dodavatele).

h) Strategické požadavky na oblast Produktová část:

- požaduje se podpora ICIS produktům OZP (např. AS, Vitakarta, řízená péče, bonusový systém, preventivní programy, atd.). Pojištěnci mohou mít v daném okamžiku k pojišťovně více vztahů, z nichž mohou vyplývat platební pohledávky nebo úhradové závazky vůči pojištěncům nebo třetím stranám včetně účtování zdravotní péče.

i) Strategické požadavky na oblast Příjmová část:

- požaduje se vytvořit řešení celého procesu kontroly a vymáhání pohledávek za plátcí pojistného od vzniku pohledávky až po její zánik,
- řešení by mělo být realizováno nad předpisy vznikajícími v účetní části a mělo by odstranit současná omezení pro realizaci kontrol.

j) Strategické požadavky na oblast Finanční část:

- požaduje se vznik předpisů na pojistné a příslušenství a s tím souvisejících předpisů v účetní části, tyto předpisy využívá příjmová část,
- požaduje se, aby všechny účetní předpisy pohledávek a závazků související s úhradami zdravotních služeb (ZFZP, FPrev) vznikaly ve výdajové části,
- dále se požaduje finanční účetnictví, zajištění bankovního styku a hotovostních plateb (např. ČS, Česká pošta, Poštovní spořitelna), tvorba souborů pro export,
- požaduje se vytvoření workflow účetních dokladů,
- požaduje se, aby implementace požadavků finanční části byla v souladu se zákonem o účetnictví a zákonem o finanční kontrole.

k) Strategické požadavky na oblast Řízení vztahu s pojištěncem:

- nový proces řízení vztahu s pojištěncem - bude vytvořen sjednocující proces, který umožní sjednocenou kontrolu a řízení vztahu s pojištěnci napříč všemi agendami,
- požaduje se možnost periodických procesů zpřesňujících očekávanou nákladovou rizikovost pojištěnců s vazbou na eliminace rizik a nákladové prognózy skupin pojištěnců, regionů a OZP.

l) Strategické požadavky na oblast Podpora řízení (BI):

- požaduje se nový proces plánování a řízení bilance - bude vytvořen podpůrný mechanismus umožňující plánování a řízení bilance pojišťovny. Za tím účelem budou vytvořeny obousměrné vazby do ostatních "provozních" procesů,
- požaduje se podpora pro identifikaci „nežádoucích“ vazeb a procesů včetně chybně vykazovaných zdravotních služeb a identifikace pojistných podvodů s využitím prvků umělé inteligence,
- požaduje se podpora modelování a predikce pro plánování a reporting,
- v rámci analytického systému je požadováno mít i možnost pro ad hoc výběry dat zadavatelem.

m) Strategické požadavky společné pro všechny oblasti:

- požaduje se implementace schvalovací procedury a vazby požadavků dle zákona o finanční kontrole,

- i když není po právní stránce zřejmé, zda zadavatel musí tyto podmínky plnit, požaduje se, aby technické vlastnosti systému plnily podmínky stanovené právními předpisy o kybernetické bezpečnosti, a to nejméně v rozsahu významného informačního systému.

n) Strategické nefunkční požadavky na ICIS:

- Strategie nasazení nového ICIS musí zohlednit také potřebu tzv. nefunkčních požadavků na systém (Service Level Requirements), které mohou mít také kritický vliv na systém, ale jejich samotným úkolem však není podpořit věcnou náplň činnosti a procesy OZP, ale vyvinout kvalitní stabilní systém a jeho kvalitu měřit podle kritérií,
- Mezi základní nefunkční požadavky, které nový ICIS musí zohledňovat, jsou:
 - výkon,
 - škálovatelnost,
 - spolehlivost,
 - rozšiřitelnost,
 - kompaktnost
 - udržitelnost,
 - parametrizovatelnost a administrovatelnost zadavatelem,
 - spravovatelnost tj. schopnost řídit systém a zajistit tak jeho bezproblémový běh,
 - bezpečnost.

Konkrétní seznam nefunkčních požadavků je uveden v příloze Studie proveditelnosti, v dokumentu OZP-ICIS-Studie-P20-Seznam-nefunkčních-požadavků.xlsx.

2. Seznam požadavků na funkce ICIS

- Požadavky jsou pro přehlednost a zachování čitelnosti informací uloženy v přílohách Studie proveditelnosti ve zdrojových souborech XLSX.
- Požadavky jsou rozděleny podle oblastí řešení do jednotlivých samostatných příloh podle následujícího schématu:

	Kód	Oblast / Název přílohy
Zdravotní pojišťovna	P01	Finance OZP-ICIS-Studie-P01-Seznam-požadavků-Finance.xlsx
	P02	Podpora řízení OZP-ICIS-Studie-P02-Seznam-požadavků-Podpora-řízení.xlsx
	P03A	Produktová část OZP-ICIS-Studie-P03A-Seznam-požadavků-Produktová-část.xlsx
	P03B	Výdajová část OZP-ICIS-Studie-P03B-Seznam-požadavků-Výdajová-část.xlsx
	P04	Registry OZP-ICIS-Studie-P04-Seznam-požadavků-Registry.xlsx
	P05A	Servis – Agendy OZP-ICIS-Studie-P05A-Seznam-požadavků-Servis-Agendy.xlsx
	P05B	Servis – Technologie OZP-ICIS-Studie-P05B-Seznam-požadavků-Servis-Technologie.xlsx
	P06	Výběr pojistného OZP-ICIS-Studie-P06-Seznam-požadavků-Výběr-pojistného.xlsx

3. Specifikace požadovaných procesů realizovaných systémem ICIS

- a) V rámci zpracování analýzy procesů byla využita notace BPMN (Business Process Model and Notation) včetně doporučené metodiky přístupu k této analýze. Na nosiči dat dle bodu 1 této přílohy jsou uvedena jednotlivá schémata spolu s popisy roztržiděné podle základních oblastí, které jsou v rámci činnosti zdravotní pojišťovny požadovány.
- b) Podle syntaxe BPMN existuje hierarchie v procesech, tj. existují tzv. vyšší procesy a nižší procesy v tom smyslu, že vyšší procesy se skládají z nižších procesů, resp. obráceně nižší procesy se skládají do vyšších procesů. Z terminologického hlediska je vedle pojmu „rozklad procesů“ používán také pojem „rozklad oblastí řešení“. Jedná se o dva typy diagramů:
 - diagram rozkladu oblastí řešení (v této úrovni ještě neobsahuje procesní schéma),
 - diagram popisu procesu.
- c) Metodika zpracování procesního modelu je uvedena v bodu C této přílohy s názvem „Studie proveditelnosti“.
- d) Procesní model je vytvořen v nástroji Enterprise Architect a schémata na uvedeném nosiči jsou ve formátu DOCX.
- e) Procesní model je rozdělen podle první úrovně rozkladu oblastí řešení do jednotlivých samostatných příloh podle následujícího schématu:

	Kód	Oblast / Název přílohy
Zdravotní pojišťovna	P07	Finance OZP-ICIS-Studie-P07-Procesní-model-Finance.docx
	P08	Podpora řízení OZP-ICIS-Studie-P08-Procesní-model-Podpora-řízení.docx
	P09A	Produktová část OZP-ICIS-Studie-P09A-Procesní-model-Produktová-část.docx
	P09B	Výdajová část OZP-ICIS-Studie-P09B-Procesní-model-Výdajová-část.docx
	P010	Registry OZP-ICIS-Studie-P10-Procesní-model-Registry.docx
	P011A	Servis – Agendy OZP-ICIS-Studie-P11A-Procesní-model-Servis-Agendy.docx
	P011B	Servis – Technologie OZP-ICIS-Studie-P11B-Procesní-model-Servis-Technologie.docx
	P012	Výběr pojistného OZP-ICIS-Studie-P12-Procesní-model-Výběr-pojistného.docx

4. Funkční specifikace systému ICIS

- a) V této příloze jsou specifikovány funkce ICIS resp. pro přehlednost a zachování čitelnosti dokumentu jsou funkce uloženy v samostatných přílohách ve zdrojových souborech XLSX. Funkce jsou rozděleny podle oblastí řešení do jednotlivých samostatných příloh podle následujícího schématu:

	Kód	Oblast / Název přílohy
Zdravotní pojišťovna	P13	Finance OZP-ICIS-Studie-P13-Seznam-funkcí-Finance.xlsx
	P14	Podpora řízení OZP-ICIS-Studie-P14-Seznam-funkcí-Podpora-řízení.xlsx
	P15A	Produktová část OZP-ICIS-Studie-P15A-Seznam-funkcí-Produktová-část.xlsx
	P15B	Výdajová část OZP-ICIS-Studie-P15B-Seznam-funkcí-Výdajová-část.xlsx
	P16	Registry OZP-ICIS-Studie-P16-Seznam-funkcí-Registry.xlsx
	P17A	Servis – Agendy OZP-ICIS-Studie-P17A-Seznam-funkcí-Servis-Agendy.xlsx
	P17B	Servis – Technologie OZP-ICIS-Studie-P17B-Seznam-funkcí-Servis-Technologie.xlsx
	P18	Výběr pojistného OZP-ICIS-Studie-P18-Seznam-funkcí-Výběr-pojistného.xlsx

- b) Popis funkcí vychází ze schématu procesů (viz bod 3). Při jeho sestavování byly procházeny jednotlivé aktivity v procesech (se snahou zachovat jejich následnost). Poté byly procházeny jednotlivé požadavky, a pokud některý nebyl pokryt funkcí vyplývající z aktivity procesu, byl doplněn popis funkce vycházející z požadavku. Znamená to tedy, že při návrhu funkcí byla provedena křížová kontrola pokrytí procesů a požadavků funkcemi ICIS.
- c) Z důvodu přehlednosti a srozumitelnosti byl do XLSX tabulek s funkcemi vložen do každé sekce odkaz na kapitulu příloh P01 – P06, kde jsou popsány požadavky a odkaz na kapitulu P07 - P12, kde jsou popsány procesy.

B. Technická specifikace

1. Specifikace HW prostředků

- a) Dodavatel již v rámci zadávacího řízení předloží návrh HW, licenčního SW a zajištění napojení na stávající infrastrukturu tak, aby byl zajištěn provoz a správa ICIS s požadovanými parametry. V samostatné kapitole č. V tohoto dokumentu jsou podrobně specifikovány požadavky zadavatele na uvedený návrh dodavatele. Dodavatel je povinen zpracovat a v nabídce předložit svůj návrh v souladu s uvedenými požadavky zadavatele. Změny vůči návrhu musí odsouhlasit zadavatel.
- b) Dodavatel systému ICIS vypracuje specifikaci HW, na kterém bude nový ICIS provozován. OZP bude realizovat nákup HW samostatně mimo dodávku ICIS (jiný dodavatel). Soupis HW a jeho specifikace musí být natolik detailní, aby dodavatel garantoval provoz systému na HW splňujícím uvedenou konfiguraci po dobu minimálně 4 let. Náklady na HW nebudou zahrnuty do ceny dodávky, avšak náklady na licence potřebného SW (včetně operačních systémů) do ceny dodávky zahrnuty budou. Vzhledem ke skutečnosti, že požadovaný HW bude zadavatel zadávat v zadávacím řízení dle zákona, musí být veškeré požadavky dodavatele na tento HW v návrhu formulovány takovým způsobem, který bude plně v souladu se ZVZ, resp. s novým zákonem o zadávání veřejných zakázek (a to primárně s požadavky obsaženými v § 44 odst. 11 ZVZ a § 45 ZVZ, resp. obdobnými požadavky vymezenými v novém zákoně o zadávání veřejných zakázek).

- c) Dodavatel přebírá garanci za výkonové nastavení navrhovaného řešení dle požadavků zadavatele na SLA. V případě, že navržený systém nebude splňovat požadované SLA, bude doplnění kapacit v režii dodavatele.

2. Architektura ICIS

- a) Nový ICIS by měl být vystaven na jednotné, koncepčně moderní, výrazně pro-klientsky orientované, technologicky dlouhodobě perspektivní a v ČR i celosvětově široce podporované ERP platformě se zajištěnou technickou, vývojovou a legislativní podporou v ČR v horizontu min. 10 let, kde obecně používané funkcionality není třeba programovat, ale převážně pouze customizovat a parametrizovat v modulech ERP systému standardně dodávaných jeho výrobcem. Musí se jednat o takovou ERP platformu, která bude splňovat minimálně následující požadavky zadavatele:
1. minimálně třicet (30) realizovaných instalací SW platformy ERP nabízeného řešení pro informační systém v období posledních 3 let před zahájením zadávacího řízení předmětné veřejné zakázky „Výstavba, implementace a technická podpora Integrovaného Centrálního Informačního Systému (ICIS) OZP“;
 2. existence minimálně sto (100) certifikovaných konzultantů a systémových inženýrů k SW platformě ERP nabízeného řešení pro informační systém;
 3. existence minimálně deseti (10) certifikovaných integrátorů k SW platformě nabízeného řešení pro informační systém. Integrátorem se rozumí právnická osoba či podnikající fyzická osoba (OSVČ) zajišťující systémovou integraci, nikoli profesní skupina.
- b) ICIS musí mít vícevrstvou klient / server architekturu s minimálními nároky na koncová zařízení.
- c) ICIS musí zajišťovat jednotné grafické uživatelské rozhraní všech modulů a jednotnou ergonomii ovládání s vysokým stupněm provázanosti informací napříč aplikačními moduly. Pro specifické uživatelské role bude ICIS řešit rozhraní, resp. skladbu vstupních menu postavených „na míru“.
- d) Systém musí respektovat geografické rozložení působnosti zdravotní pojišťovny.

3. Dimenzování ICIS

- a) Nový ICIS jako plně integrovaný informační systém musí podporovat následující objemy při zachování deklarovaných odezev systému. Požadovaný stav musí ICIS splnit při náběhu systému. Podporovaný stav obsahuje možný nárůst objemu v novém ICIS, pro který musí být řešení rozšiřitelné posílením HW infrastruktury bez nutnosti zásahu do programového řešení ICIS. Tím je mj. zajištěna perspektivnost nového systému a jeho pružnost vůči změnám v prostředí zdravotního pojištění v ČR a zadavateli tak ICIS poskytuje konkurenční výhodu.

Parametr	Požadovaný stav	Podporovaný stav
Počet uživatelů	400, z toho 300 současně pracujících	800, z toho 500 současně pracujících
Počet pojištěnců	1 milión	5 miliónů
Počet poskytovatelů zdravotních služeb	25 tisíc	50 tisíc
Počet plátců zdravotního pojištění v kategoriích OSVČ, zaměstnavatel	200 tisíc	500 tisíc

- b) Při akceptaci HW infrastruktury navržené dodavatelem musí systém splňovat následující odezvy při zachování objemu dat požadovaného stavu po dobu minimálně 4 let provozu:

Parametr	Požadovaná hodnota	Přijatelná hodnota
Zpracování požadavku uživatele na přepážce (při interakci s klientem)	1 sekunda (80% případů), 2 sekundy (15% případů)	10 sekund (5% případů)
Zpracování online požadavku externího systému	1 sekunda	5 sekund (5% případů)
Zpracování požadavku uživatele u jednoho případu	1 sekunda (80% případů), 2 sekundy (15% případů)	10 sekund (5% případů)
Zpracování požadavku dávkové úlohy	Není explicitně stanoveno, běh dávkových úloh nesmí omezit provoz systému a musí počítat s časovými okny servisních zásahů (alespoň 4 hodiny denně).	Délka zpracování dávkové úlohy nebrání procesu zpracování údajů.

4. Dostupnost ICIS

- a) Systém ICIS musí být trvale dostupný (365x7x24) minimálně pro vyřizování online dotazů externích aplikací (Portál OZP ONLINE¹, Portál ZP). Za účelem vysoké dostupnosti předpokládá zadavatel využití technologií pro eliminaci výpadku z důvodu HW chyby (záložní zdroje, motorgenerátor, cluster, redundantní propojení). Řešitel musí navrhnout takové technické řešení, které bude toto plně podporovat a bude využívat moderních trendů v oblasti řešení systémů s vysokou dostupností s efektivním využíváním zdrojů (virtualizace).
- b) Akceptovatelná doba neplánovaného výpadku systému je 4 hodiny v celku, v provozní době (7:00-17:00), maximálně 1x za měsíc.
- c) Plná funkčnost systému ICIS pro uživatele musí být dostupná v provozní době (7:00-17:00). Mimo provozní dobu mohou probíhat plánované i jednorázové dávkové úlohy jako je načítání dat z externích systémů, ELT (ETL) procedury pro plnění datového skladu, zpracování různých výkazů, generování výstupních dat, zpráv a protokolů, dále v tuto dobu mohou probíhat plánované servisní úkony systému včetně procesů zálohování atd. V této době je po dohodě se zadavatelem možné provádět servisní práce, opravy a nasazování nových funkcí případně další potřebné zásahy do systému.
- d) Součástí poptávané dodávky řešení je také návazná technická podpora po nasazení ICIS do provozu. Technická podpora bude zakotvena ve Smlouvě o podpoře, která řeší základní podporu systému rozdělenou do jednotlivých služeb. Tyto služby jsou přehledně uvedeny v následujících tabulkách:

Kód	Název	Popis služby
S01	Technická podpora	Technická podpora ICIS zahrnuje služby: - Servisní podpory. - Podpory Licenčního SW (maintenance). - Podpory ASW, to je Údržby ASW a Vývoje ASW. Součástí je v obou případech tvorba a aktualizace uživatelské, bezpečnostní, projektové a provozní dokumentace, testování, školení apod.
S02	Profylaktická kontrola	Zahrnuje preventivní a funkční prohlídky ASW a LSW s cílem predikce nesrovnalostí a závad.

¹ Portál OZP ONLINE je od 1.4.2014 nazýván VITAKARTA ONLINE. Z důvodu přehlednosti ve vazbě na Studii proveditelnosti, je v zadávací dokumentaci ponecháno původní pojmenování.

Kód	Název	Popis služby
S03	Systémová podpora ICIS	Zahrnuje systémové služby k zajištění provozu a správy ICIS. Jedná se zejména o instalace SW, konfigurace, migrace apod. Jedná se o služby v rámci Servisní podpory. Požadavky na služby a zásahy v rámci systémové podpory mohou být typu „Havarijní“ a „Normální“.
S04	Školení a konzultace	Zahrnuje služby k zajištění školení, prezentací, seminářů uživatelů a správců ICIS lektory anebo formou e-learningu. Pozn.: služby školení, konzultace a prezentace jsou vyžadovány jen jako součást dodávky nových modulů a úprav funkcí ASW ICIS. V rámci Smlouvy o technické podpoře nebude standardní školení poptáváno.
S05	Projektové řízení	Zahrnuje služby spojené s řízením projektů, vedením příslušné projektové dokumentace, účast na kontrolních dnech, řídicích výborech projektů apod.
S06	Monitoring	Zahrnuje služby periodické kontroly stanovených parametrů ICIS, obvykle technickými prostředky.
S07	Služby Hot-line	Zahrnuje podporu uživatelům a správcům při vyřízení požadavků na krátké dotazy spojené s provozem a užíváním ICIS podaných obvykle telefonem, emailem či jinými elektronickými kanály apod.
S08	Podpora Licenčního software (maintenance)	Zahrnuje služby dle licenčních smluv výrobců LSW (maintenance LSW).
S09	ServiceDesk / HelpDesk	Zahrnuje služby řešení a eskalace zjištěných nesrovnalostí a vad ICIS (jeho ASW, LSW) vedoucí k jejich vyřízení/odstranění. Součástí je též přístup žadatelů o servisní zásah na ServiceDesk/HelpDesk dodavatele. Jedná se o požadavky na řešení vad (zásahy) typu „Havarijní“ a „Normální“.
S10	Reklamáce	Zahrnuje služby dle reklamačního řádu výrobce (prodejce / distributora) příslušného LSW a dodavatele ASW.
S11	Reporting	Služba pravidelného měsíčního reportingu o plnění sjednaných SLA. Slouží k zajištění kontroly plnění SLA.
S12	Podpora ASW ICIS	Zahrnuje upgrade a update dodaného ASW, jak od dodavatelů třetích stran, tak k produktům specificky vytvořeným a dodaným pro ICIS. Obsahuje: - právo na nové verze systémů třetích stran, součástí jejichž dodávky je služba maintenance resp. Software Assurance resp. podpory daného ASW - právo na upgrade a update - legislativní servis systému ICIS Maintenance legislativy (legislativní servis) zahrnuje sledování změn legislativy ve spolupráci se zadavatelem s dopadem na podporovaný systém ICIS a zapracování změn této legislativy.

e) Minimální požadavky na úroveň služeb jsou rozděleny na následující oblasti:

- Parametry SLA pro služby poskytované na vyžádání prostřednictvím ServiceDesk / HelpDesk dodavatelů (poskytovatelů služby),
- Parametry SLA pro služby poskytované paušálně.

5. HW infrastruktura

- Zadavatel předpokládá, že ICIS bude provozován na nově dodané HW infrastruktuře, jejíž specifikaci určí dodavatel. HW prvky budou rozmístěny ve třech nezávislých lokacích, přičemž dvě lokace budou sloužit pro redundanci HW prvků a budou výkonově a funkčně ekvivalentní. Třetí lokace bude určena jako geografická záloha systému ICIS.
- Na dodané HW infrastruktuře budou provozovány tři kopie systému ICIS – ostrý provoz (produkční), testovací provoz (předávací) a školící provoz (cvičný). Tato infrastruktura musí

být pokryta kompletně licencemi tak, aby nedošlo k žádnému zpochybnění OZP jako provozovatele.

- c) Součástí specifikace HW infrastruktury budou požadavky na zadavatele (v detailu minimálně dle lokací):
- požadovaný příkon elektrické sítě,
 - prostorové nároky HW prvků,
 - hmotnost HW prvků,
 - požadavky na chladicí jednotky,
 - požadavky na síťovou infrastrukturu pro propojení lokací, uživatelských stanic.
- d) ICIS bude podporovat stávající tiskárny provozované v prostředí zadavatele. Bude-li některá z funkcí ICIS vyžadovat použití specifického typu tiskárny, musí být tato informace explicitně uvedena. Výčet používaných typů tiskáren je uveden v souboru OZP-ICIS-Studie-P22-HW-Typy-tiskáren.docx.
- e) ICIS bude podporovat čtečky čárových kódů provozované v prostředí zadavatele. Bude-li ICIS vyžadovat specifickou čtečku čárových kódů, musí být tato informace explicitně uvedena. Výčet používaných čteček čárových kódů je uveden v příloze OZP-ICIS-Studie-P23-HW-Čtečky.docx.
- f) ICIS bude podporovat terminály pro bezhotovostní platby provozované v prostředí zadavatele. Výčet používaných terminálů bezhotovostních plateb je uveden v příloze OZP-ICIS-Studie-P24-HW-Terminály-bezhotovostních-plateb.docx.

6. Komunikační infrastruktura

- a) Výpočetní systém bude umístěn v jednom místě - v sídle zadavatele. K výpočetnímu systému se uživatelé připojují jak v místě přes LAN, tak z poboček přes WAN síť. Rychlost jednotlivých LAN lokalit 10/100 Mbps. Páteřní rozvody v datových centrech jsou 1Gbps Kapacita linek je v níže uvedené tabulce:

Lokality, včetně identifikátoru, rychlosti v jednotlivých lokalitách

Služba	Identifikátor	Adresa	upgrade na
IOL Fixed Digital 4 Mbps	IOL26903	Roškotova 1225/1 14200 Praha Braník	20 Mbps
IP Connect CMA	OS5928616		
IP Connect Trunk 1024 kbit/s	10010002130	Praha Nové Město (Praha 1), Na příkopě 8	2048
IP Connect Trunk 2048 kbit/s	10010002131	Tusarova 1152/36 17000 Praha Holešovice	12 Mbps
IP Connect Trunk 256 kbit/s	10010002132	Praha Smíchov, Radlická 1170/61	1024
IP Connect Trunk 256 kbit/s	10010002217	Palackého 31/2 26601 Beroun -Centrum	1024
IP Connect Trunk 2048 kbit/s	10010003116	Brno Zábrdovice (Brno-střed), Příkop 843	4096
IP Connect Trunk 512 kbit/s	10010004049	Dr. Jiřího Procházky 5281/ 58601 Jihlava	1024
IP Connect Trunk 512 kbit/s	10010005111	Olomouc, Denisova 345/2	1024
IP Connect Trunk 256 kbit/s	10010005113	Dolní náměstí 304/22 74601 Opava Město	1024
IP Connect Trunk 512 kbit/s	10010005114	Ostrava Moravská Ostrava, Přívozká 949/	1024
IP Connect Trunk 512 kbit/s	10010007122	Zlín, Zarámí 92/	1024
IP Connect Trunk 512 kbit/s	10010008121	Pardubice, Hronovická 1470	1024
IP Connect Trunk 512 kbit/s	10010010055	Plzeň Jižní Předměstí, Purkyňova 736/17	1024

IP Connect Trunk 256 kbit/s	10010011066	nám. F. Křížika 2840/ 39002 Tábor	1024
IP Connect Trunk 512 kbit/s	10010011067	České Budějovice, K. Weisse	1024
IP Connect Trunk 512 kbit/s	10010012061	Hradec Králové, Pražské předměstí 40/7	1024
IP Connect Trunk 512 kbit/s	10010014090	Liberec, Jablonecká 264/16a	1024
IP Connect Trunk 512 kbit/s	10010016117	Ústí nad Labem Ústí nad Labem-centrum, K	1024
IP Connect Trunk 512 kbit/s	10010024076	Karlovy Vary, T.G.Masaryka	1024
IP Connect Trunk 256 kbit/s	MO1179241	Dolní 165/1 59101 Žďár nad Sázavou 1	1024
IP Connect Trunk 8192 kbit/s	MO1215572	Roškotova 1225/1 14200 Praha Braník	20480

7. Bezpečnost dat

a) Nový ICIS musí splňovat požadavky na bezpečnost dat:

- dohledatelnost a právní prokazatelnost údajů a jejich změn v ICIS, právní prokazatelnost účetnictví,
- dohledatelnost a právní prokazatelnost dokumentů distribuovaných ICIS – standardní používání certifikátů, šifrované komunikace a elektronických podpisů s časovým razítkem,
- ochranu údajů proti zneužití (neoprávněnému přístupu), včetně logování přístupu uživatelů,
- ochranu proti neoprávněnému přístupu nástroji mimo systém ICIS,
- ochranu proti neoprávněné změně dat a funkcí,
- ochranu konzistence dat uvnitř ICIS i v rámci komunikačních kanálů a protokolů s okolními systémy,
- kontrolu proti vnitřnímu fraudu – ICIS bude podporovat nástroje pro identifikaci podezřelých situací indikujících možné snahy o neoprávněné obohacení ze strany pracovníků pojišťovny,
- výstupy pro interní a externí bezpečnostní audit,
- ochranu proti úniku informací neoprávněným uživatelům.

b) Zabezpečení dat uvnitř systému ICIS není explicitně vyžadováno. Serverové prostředí ICIS včetně datových úložišť bude považováno za důvěryhodné, není nutné šifrovat data na datovém úložišti nebo při komunikaci mezi systémy. Systém musí být připraven na možnou změnu legislativy v oblasti vnitřního zabezpečení dat (např. nový zákon o kybernetické bezpečnosti).

c) Bude-li nový ICIS ukládat důvěrná data mimo samotný systém (serverovou infrastrukturu), musí být tato funkce explicitně zdůvodněna a schválena zadavatelem. Toto se netýká ostatních interních systémů zadavatele, které jsou také považovány za důvěryhodné.

d) Uživatelé budou k datům přistupovat prostředky ICIS, případně budou mít pro reporting přístup do definovaného datového skladu. Přímý přístup k datům transakčních částí systému musí být uživatelům zamezen s výjimkou odpovědných pracovníků odboru informatiky.

e) Oprávněný uživatel bude moci data přenášet na PC zadavatele. Řízení přístupu k datům mimo systém ICIS není součástí poptávky.

f) Datové úložiště by mělo být pro celý systém ICIS na jedné technologické platformě. Datové úložiště musí zajistit požadavky na zabezpečení, výkon a integritu spravovaných dat. Nový ICIS musí v maximální míře omezit duplicitu dat.

- g) Datové úložiště musí umožnit propojení na stávající datový sklad provozovaný na platformě Microsoft SQL Server, a to zaměstnanci odboru informatiky zadavatele. Pro tvorbu sestav zadavatel předpokládá, že součástí ICIS bude datový prostor pro provádění analýz, ke kterému bude přístup z technologií Microsoft SQL Server (SSIS, SSAS, SSRS) za účelem vlastních analýz a tvorby vlastních sestav zadavatele.
- h) Pro specifické aplikace uvedené v návrhu systému musí ICIS umožnit zaměstnancům odboru informatiky zadavatele vytvořit vlastní programy zpracování dat, které budou postaveny na technologiích Microsoft.NET. Nový ICIS musí minimálně podporovat vzájemnou výměnu dat za použití standardních služeb (SOAP, REST, XML).

8. Řízení přístupu uživatelů

- a) Přihlašování do systému ICIS bude řešeno technologií Single Sign-On s využitím Microsoft Active Directory (dále také Active Directory) provozované zadavatelem. Active Directory je aktuálně na technologické úrovni Windows 2008 R2. Bude-li dodavatel požadovat jinou technologickou úroveň, musí být tato informace explicitně uvedena a náklady na tuto změnu musí být součástí nabídkové ceny. Ochrana specifických částí systému (heslo, certifikát, HW token) musí být explicitně uvedena. Dodavatel může navrhnout vlastní způsob realizace Single Sign-On s využitím stávající Active Directory, např. v kombinaci s dalšími identifikačními nástroji, avšak správa uživatelů musí být napříč řešením jednotná a probíhat nad Active Directory.
- b) Zabezpečení přístupu k funkcím ICIS bude řízeno víceúrovňovou definicí oprávnění. Základní autentizační jednotkou bude identita uživatele v prostředí Active Directory. Pro řízení přístupu k prostředkům systému ICIS zadavatel předpokládá využití bezpečnostních skupin, uživatelé budou zařazováni do připravených skupin dle rolí, které budou vykonávat.
- c) ICIS bude pro vybrané agendy podporovat řízení přístupu až k jednotlivým datovým záznamům (např. filtrovat přístup k datům dle vybraného atributu), viz požadavky na funkce systému.
- d) ICIS bude podporovat ověřování identity klientů v externích aplikacích uvedených v tabulce bodu č. 11 a č. 12.
- e) ICIS bude obsahovat víceúrovňovou administraci uživatelských oprávnění. ICIS umožní vybraným uživatelům spravovat uživatelské přístupy jemu podřízených zaměstnanců.

9. Klientské stanice

- a) Systém ICIS bude podporovat stávající klientské stanice uživatelů, s následující specifikací:
 - operační systém: Microsoft Windows (verze 7, 8 a novější),
 - kancelářský balík: Microsoft Office (2007, 2010, 2013 a novější),
 - internetový prohlížeč: Microsoft Internet Explorer verze 7 a vyšší, FireFox verze 4 a vyšší,
 - HW splňuje požadavky na provoz daného operačního systému.
- b) Dodavatel bude specifikovat dodatečné nároky na klientské stanice uživatelů, jak na centrálním pracovišti, tak na vzdálených pobočkách.

10. Integrace na stávající SW

- a) ICIS musí podporovat komunikaci se stávajícími aplikacemi zadavatele, které nebudou systémem ICIS nahrazeny. ICIS primárně obousměrně a přímo, bez využití vnějšího interface, komunikuje s okolními systémy, které se nachází ve vnitřním zabezpečeném prostředí OZP.
- b) ICIS musí podporovat plnou integraci na produkty provozované u zadavatele:

Interní IS	Popis
DMS SAFE	Systém spisové služby a důvěryhodného dlouhodobého úložiště dokumentů. Správa dokumentů (generované dokumenty z ICIS pro účely vypravení, příchozí elektronické dokumenty související s agendami ICIS).
MS Office SharePoint Server	Úložiště interních dokumentů (pracovní verze dokumentů před jejich uložením do spisové služby, kopie oficiálních dokumentů uložených ve spisové službě, dokumentace nepodléhající evidenci ve spisové službě v souladu se spisovým a skartačním plánem, ...).
MS Exchange	Brána pro tvorbu alertů, správu událostí v kalendáři a podpory hromadné emailové komunikace.
Security	Spojení MS Active Directory a Single Sign On (SSO) slouží pro centrální správu uživatelů a jejich oprávnění k přístupu do ICIS.
Tel. Ústředna (TIC)	Systém pro podporu evidování tel. komunikace v rámci ICIS.
Reportovací prostředí	Reportovací prostředí v rámci OZP postavené na MS-SQL a Reporting Services. Po implementaci ICIS by toto prostředí mělo být napojeno na budoucí jádro tzv. „business 12ntelligence“ části informačního systému (tedy datový sklad) sloužící jako datová základna pro analýzy, reporting, predikci vývoje.
Komunikační infrastruktura	Komunikační rozhraní, přes které je vedena veškerá komunikace s externími systémy, založena na on-line webových službách.
MS CRM	Podpora pro vedení agendy a komunikaci s klienty v rámci asistenční služby OZP.
DRG Wiever	Podpora pro vyhodnocení úhrad zdravotních služeb dle DRG.

11. Externí portály se sdílenou identitou

- a) ICIS aktivně, pomocí striktně definovaného interface², zahajuje komunikaci s portály, kdy na základě požadavků a odpovědí probíhá aktivní on-line komunikace.
- b) ICIS musí podporovat komunikaci s externími portály:

Portály	
Portál OZP ONLINE	Primární komunikační kanál s pojištěnci, který může být dále rozšiřován pro komunikaci se zdravotnickými zařízeními, plátcí či lékaři. Primárně se přenáší data o pojištěncích, jejich vykázané péči (Individuální účet) a další informace týkající se zdravotního stavu pojištěnců (projekt VítaKarta). Mezi jeho hlavní služby patří například: Osobní účet pojištěnce, Osobní deník pojištěnce, Individuální zdravotní plán pojištěnce, KHN lékaře, e-Formuláře jako Přehled OSVČ, Přihláška k asistenční službě apod.
Portál ZP	Primární komunikační kanál sdružení více ZP pro komunikaci se zdravotnickými zařízeními, plátcí, exekutory, policií apod. Mezi hlavní agendy, pro které je využíván, patří: načítání Dávek vykázané péče, HOZ, Hlášení úrazů, Požadavky na součinnost, Žádosti o výpis vykázané zdravotní péče, Výpisy registrovaných pojištěnců k lékaři, ověřování zaměstnavatelů a pojištěnců na portále na základě předávaných seznamů a nově příjem tzv. Příloh2 a další agendy. Vstupní brána pro přístup k produktu VítaKarta+ pro lékaře. Na Portál ZP je napojen Portál OZP ONLINE přes komunikační rozhraní (Kobra).
Portál ČSOB	Napojení Portálu OZP ONLINE na službu elektronického bankovníctví ČSOB a ERA v oblasti předávání údajů o klientech OZP.
Portál Vitalitas	Napojení Portálu OZP ONLINE na službu cestovního pojištění společnosti Vitalitas v oblasti předávání údajů o klientech OZP.

² Popisy interface (rozhraní) budou Dodavateli předány v rámci realizace díla.

- c) Součástí dodávky je i obměna komunikačního rozhraní mezi Portálem OZP ONLINE a Portálem ZP, tzv. Kobra.

12. Externí systémy

- a) ICIS musí podporovat komunikaci s existujícími systémy partnerů zadavatele. Popis externích systémů je uveden v tabulce bodu 11. ICIS musí umožnit budoucí rozvoj systému, aby bylo možné realizovat nově poptávanou komunikaci, minimálně s využitím stávajících standardů: WS, SOAP, REST, XML.
- b) Komunikace s externími systémy do vnitřního prostředí ICIS musí být řešena v off-line režimu. On-line požadavky nesmí vstupovat do ICIS přímo (např. přímé dotazy na data na úrovni databázového stroje), nýbrž budou zpracovány v asynchronním módu, tj. budou zařazovány do front pro zpracování, které následně ICIS zpracuje.
- c) Zadavatel předpokládá využití některé z ESB platform pro zajištění bezpečné a customizovatelné platformy pro implementaci integračních řešení.
- d) ICIS aktivně, pomocí striktně definovaného interface, zahajuje komunikaci s externími systémy, kdy na základě požadavků a odpovědí probíhá aktivní on-line komunikace. S některými externími systémy probíhá komunikace jednostranně (data jsou pouze načítána či odesílána), s jinými oboustranně.
- e) ICIS musí podporovat komunikaci s externími systémy:

Externí subjekt / systém	Popis
Banky	Komunikace primárně z modulu Finance (bankovní výpisy, příkazy k úhradě). Obousměrná komunikace (načítání výpisů, vytváření příkazů) pomocí externích programů konkrétních bank.
Call centrum	Komunikace primárně pro potřeby Asistenční služby o realizovaných hovorech s pojištěnci. Obousměrná komunikace (seznam pojištěnců evidovaných v AS, seznam uskutečněných hovorů a urgentní dotazy). Nyní poloautomaticky, v budoucnu by bylo vhodné komunikovat prostřednictvím webových služeb a data zasílat automatizovaně (záleží na smluvních podmínkách).
Centrální registr pojištěnců (CRP)	Komunikace primárně pro modul Registrů o stavech pojištěnců v rámci INFO souborů. Oboustranná komunikace o evidovaných pojištěncích (odesílá např. OZN, SP, ZUP; načítá např. INFO, VZP, ZP ad.) pomocí generování souborů a jejich zasílání emailem.
Centrální systém účetních informací státu (CSÚIS)	Komunikace primárně pro modul Finance – zasílání elektronických Státních výkazů, případně dalších zpracovávaných výkazů. Obousměrná komunikace, načítání výkazů a zpětná informace v případě chyb.
Centrum mezistátních úhrad (CMÚ)	Komunikace primárně pro modul Registrů (výpomocné registrace) a modul Produktové části (přeúčtování péče v rámci EU). Obousměrná komunikace (výpomocné registrace, přeúčtování péče) pomocí WS.
Český statistický úřad (ČSÚ)	Jednosměrná komunikace – hlášení tzv. národních zdravotních účtů z Produktové části
Datové schránky (DS)	Komunikace v rámci dohledávání a ověřování DS osob a obyvatel. Jednosměrná komunikace (ověřování existence DS) pomocí WS.
Externí tiskárna dokumentů	Komunikace primárně pro modul Registrů a Příjmové části pro možnost tisku dokumentů pojištěnci nebo pro potřeby platební morálky zaměstnavatelů. Jednosměrná komunikace (zasílání podkladů pro tisky) pomocí generování souborů a zasílání emailem. V budoucnu, dle smluvních podmínek, možnost vystavení souboru na rozhraní. V produktové části systému je na externí tisk zasílán hromadný soubor Zúčtovacích zpráv.
Externí tiskárna průkazu	Komunikace primárně pro modul Registrů pro možnost hromadných tisků průkazů pojištěnců. Jednosměrná komunikace (zasílání podkladů pro tisky) pomocí generování souborů a zasílání emailem. V budoucnu, dle smluvních podmínek, možnost vystavení souboru na rozhraní.
Finanční úřad (FÚ)	Komunikace primárně pro modul Finance, oblast DPH, elektronická podání hlášení v režimu přenesené daňové povinnosti (PDP). Další komunikace probíhá pouze zasíláním souborů přes datové schránky – daňová přiznání,

Externí subjekt / systém	Popis
	případně další dokumenty. Komunikace je obousměrná, zpětně jsou posílány informace o chybách.
Insolvenční rejstřík (ISIR)	Komunikace primárně pro kmenové evidence o osobách a obyvatelích o návrzích a insolvenčních řízeních, která jsou vedena ve vztahu na subjekty evidované. Jednosměrná komunikace (ověřování insolvenčních řízení nad evidovanými subjekty) pomocí WS. V budoucnu by mohla být doplněna na oboustrannou (příhláška k insolvenčnímu řízení.)
Interní IS smluvních exekutorů	Napojení na IS smluvně zajištěných exekutorských úřadů (např. IS Aura).
Ministerstvo financí (MF ČR)	Komunikace probíhá pouze v rámci výměny souborů přes datové schránky.
Ministerstvo Průmyslu a Obchodu (MPO)	Komunikace primárně pro modul Registrů v rámci JRF dotazníku.
Ministerstvo zdravotnictví (MZ ČR)	Komunikace probíhá pouze v rámci výměny souborů přes datové schránky.
Národní referenční centrum (NRC)	Komunikace primárně pro modul Produktové části ohledně DRG, očkování apod. pro možnost statistického vyhodnocování a určování trendů. Obousměrná komunikace (vyžádaná data, statistiky na základě srovnání republikových dat) pomocí XLS statistik.
Portál Vitalitas	Portál pojišťovny Vitalitas, která v rámci smluvního vztahu s OZP nabízí pojištěncům výhodné komerční pojištění. Primárně se předávají osobní data o pojištěncích pro možnost jejich rychlého pořizování. Obecně jsou však tyto IS autonomní.
Státní ústav pro kontrolu léčiv (SÚKL)	Komunikace primárně pro modul Produktové části pro potřeby revizí receptů (eRecepty s možností náhledů na papírový doklad). Jednosměrná komunikace (načítání eReceptů pro možnost revizí) pomocí WS.
Ústav zdravotních informací a statistik (ÚZIS)	Neprobíhá elektronická komunikace pro modul Finance. Probíhá jednosměrná komunikace pro modul Produktová část - reportovací nástroje napojené na produktovou část zasílají statistické informace o čerpání zdravotní péče a léků ve formě generování souborů zasílaných mailem.
VAKUS	Komunikace primárně v rámci modulu Finance, načítání poštovních poukázek. Jednosměrná komunikace (načítání poukázek) pomocí datových souborů.
Základní registry (ZR)	Komunikace v rámci kmenové evidence o osobách (poskytovatelé zdravotní péče, zaměstnavatelé, ...) a obyvatelích (pojištěnci, zákonní zástupci ...) a jejich datech. V rámci ZR je pak možnost ověřovat i adresy proti RÚIAN a ROB. Jednosměrná komunikace (ověřování osob, obyvatel a adresních míst) pomocí WS.

C. Studie proveditelnosti

Studie proveditelnosti, včetně detailu popisu požadovaných služeb a funkcí, je přílohou a nedílnou součástí tohoto dokumentu.

II. Orientační seznam několika hlavních právních předpisů, kterými se zejména, nikoli však výlučně, činnost zadavatele řídí

Pro vyloučení pochybností zadavatel předkládá demonstrativní výčet základních právních předpisů, které jsou účinné ke dni uveřejnění oznámení o zahájení zadávacího řízení a vytváří základní (nikoli komplexní) legislativní rámec pro jeho činnost.

a) V oblasti zdravotnictví:

Číselné označení	Název / Nadpis / Význam
551/1991 Sb.	Zákon o Všeobecné zdravotní pojišťovně České republiky
280/1992 Sb.	Zákon o resortních, oborových, podnikových a dalších zdravotních pojišťovnách
592/1992 Sb.	Zákon o pojistném na veřejné zdravotní pojištění
48/1997 Sb.	Zákon o veřejném zdravotním pojištění
59/1997 Sb.	Vyhláška, kterou se stanoví indikační seznam pro zdravotní péči v odborných dětských léčebnách
134/1998 Sb.	Vyhláška MZ, kterou se vydává seznam zdravotních výkonů s bodovými hodnotami
101/2000 Sb.	Zákon o ochraně osobních údajů a o změně některých zákonů
268/2014 Sb.	Zákon o zdravotnických prostředcích a o změně zákona o správních poplatcích
618/2006 Sb.	Vyhláška, kterou se vydávají rámcové smlouvy
63/2007 Sb.	Vyhláška MZ o úhradách léčiv a potravin pro zvláštní lékařské účely
378/2007 Sb.	Zákon o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech)
464/2008 Sb.	Vyhláška o stanovení hodnot bodu, výše úhrad zdravotní péče hrazené z veřejného zdravotního pojištění a regulačních omezení objemu poskytnuté zdravotní péče hrazené z veřejného zdravotního pojištění pro rok 2009
471/2009 Sb.	Vyhláška o stanovení hodnot bodu, výše úhrad zdravotní péče hrazené z veřejného zdravotního pojištění a regulačních omezení objemu poskytnuté zdravotní péče hrazené z veřejného zdravotního pojištění pro rok 2010
396/2010 Sb.	Vyhláška o stanovení hodnot bodu, výše úhrad zdravotní péče hrazené z veřejného zdravotního pojištění a regulačních omezení objemu poskytnuté zdravotní péče hrazené z veřejného zdravotního pojištění pro rok 2011
372/2011 Sb.	Zákon o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)
373/2011 Sb.	Zákon o specifických zdravotních službách
374/2011 Sb.	Zákon o zdravotnické záchranné službě
376/2011 Sb.	Vyhláška, kterou se provádějí některá ustanovení zákona o veřejném zdravotním pojištění
425/2011 Sb.	Vyhláška o stanovení hodnot bodu, výše úhrad zdravotní péče hrazené z veřejného zdravotního pojištění a regulačních omezení objemu poskytnuté zdravotní péče hrazené z veřejného zdravotního pojištění pro rok 2012
39/2012 Sb.	Vyhláška Ministerstva zdravotnictví (MZ) o dispenzární péči
70/2012 Sb.	Vyhláška o preventivních prohlídkách
92/2012 Sb.	Vyhláška MZ o požadavcích na minimální technické a věcné vybavení zdravotnických zařízení a kontaktních pracovišť domácí péče
99/2012 Sb.	Vyhláška MZ o požadavcích na minimální personální zabezpečení zdravotních služeb
307/2012 Sb.	Nařízení vlády o místní a časové dostupnosti zdravotních služeb

b) V oblasti veřejné správy a její elektronizace:

Označení	Název / Nadpis / Význam
89/1995 Sb.	Zákon o státní statistické službě
106/1999 Sb.	Zákon o svobodném přístupu k informacím
227/2000 Sb.	Zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)
365/2000 Sb.	Zákon o informačních systémech veřejné správy a o změně některých dalších zákonů
320/2001 Sb.	Zákon o finanční kontrole
416/2004 Sb.	Prováděcí vyhláška k zákonu o finanční kontrole
499/2004 Sb.	Zákon o archivnictví a spisové službě a o změně některých zákonů
500/2004 Sb.	Správní řád
137/2006 Sb.	Zákon o veřejných zakázkách
469/2006 Sb.	Vyhláška o informačním systému o datových prvcích
528/2006 Sb.	Vyhláška o informačním systému o informačních systémech veřejné správy
529/2006 Sb.	Vyhláška o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy)
594/2006 Sb.	Nařízení vlády o přepisu znaků do podoby, ve které se zobrazují v informačních systémech veřejné správy
53/2007 Sb.	Vyhláška o referenčním rozhraní
64/2008 Sb.	Vyhláška o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti)
300/2008 Sb.	Zákon o elektronických úkonech a autorizované konverzi dokumentů
111/2009 Sb.	Zákon o základních registrech
193/2009 Sb.	Vyhláška o stanovení podrobností provádění autorizované konverze dokumentů
194/2009 Sb.	Vyhláška o stanovení podrobností užívání a provozování informačního systému datových schránek
458/2011 Sb.	Zákon o změně zákonů související se zřízením jednoho inkasního místa a dalších změnách daňových a pojistných zákonů

c) V oblasti účetnictví a personálních agend:

Označení	Název / Nadpis / Význam
563/1991 Sb.	Zákon o účetnictví
586/1992 Sb.	Zákon o daních z příjmů
593/1992 Sb.	Zákon o rezervách
503/2002 Sb.	Prováděcí vyhláška k účetnictví pro zdravotní pojišťovny
503/2002 Sb.	Vyhláška, obsahující české účetní standardy pro účetní jednotky
418/2003 Sb.	Vyhláška, kterou se stanoví podrobnější vymezení okruhu a výše příjmů a výdajů fondů veřejného zdravotního pojištění zdravotních pojišťoven, podmínky jejich tvorby, užití, přípustnosti vzájemných převodů finančních prostředků a hospodaření s nimi, limit nákladů na činnost zdravotních pojišťoven krytých ze zdrojů základního fondu včetně postupu propočtu tohoto limitu.
235/2004 Sb.	Zákon o dani z přidané hodnoty
262/2006 Sb.	Zákoník práce
284/2009 Sb.	Zákon o platebním styku
190/2004 Sb.	Zákon o dluhopisech

d) Dalšími dokumenty, které určují pravidla relevantní k ICIS, jsou tyto:

- Metodika pro pořizování a předávání dokladů VZP ČR,
- Datové rozhraní VZP ČR – číselníky,
- Datové rozhraní VZP ČR – individuální doklady,
- Datové rozhraní VZP ČR – speciální rozhraní,
- Pravidla pro vyhodnocování dokladů ve VZP ČR,
- České účetní standardy pro zdravotní pojišťovny.

III. Pravidla pro vytvoření harmonogramu plnění, na základě kterých dodavatel připraví příslušnou přílohu Smlouvy o vytvoření

1. Nabídka dodavatele musí obsahovat časový harmonogram plnění předmětu smlouvy s uvedením jednotlivých dílčích plnění (etap/fází) a termínů jejich plnění.
2. Maximální doba realizace projektu od data účinnosti této smlouvy do okamžiku nasazení celého ICIS v plném rozsahu technické a funkční analýzy do ostrého provozu akceptovaná zadavatelem je 30 měsíců (pro účely tohoto zadávacího řízení se 30 kalendářních měsíců považuje za 913 kalendářních dnů). Nedodržení tohoto limitu v nabídce znamená vyřazení nabídky. Uvedený termín je nejzazší možný, avšak neznemožňuje nasazování po částech. Zadavatel preferuje nasazení díla k prvnímu lednu.
3. Zadavatelem je požadována fáze ostrého provozu se zvýšenou podporou a trvalou přítomností zástupce řešitelského týmu dodavatele na pracovišti zadavatele po dobu po dobu 90 kalendářních dnů od uvedení do rutinního provozu.
4. Zadavatelem je v harmonogramu požadován minimální předstih akceptace závazné specifikace HW před termínem jeho instalace a konfigurace min. 10 měsíců, a to včetně HW nezbytného pro testování, přípravu a provádění migrace dat.
5. Z harmonogramu musí být zřejmý časový průběh všech základních fází projektu dle přílohy 3 Smlouvy o vytvoření (Pravidla řízení projektu), způsob a průběh nasazení ICIS (jako celek nebo po částech), způsob testování a nasazování systému ICIS v souladu se zajištěním souběhu s původními aplikacemi a kontinuity fungování zadavatele jako celku (zohlednit například: roční účetní uzávěrku, období implementace úhradové vyhlášky do praxe, období pro přehlašování pojištěnců mezi zdravotními pojišťovnami apod.). Ideálně by měl být v takových obdobích i minimalizován požadavek na součinnost zadavatele.
6. V případě, že bude dodavatel předkládat harmonogram s postupným náběhem dílčích modulů do produkčního provozu, měl by také detailně a věrohodně popsat, jak zajistí v daný okamžik technologické napojení těchto částí na další, doposud původní části řešení CIS. Dodavatel nesmí takovéto zajištění nezbytného propojení apod. deklarovat jako očekávanou součinnost od zadavatele.
7. Termíny budou navrženy v relativních hodnotách vůči termínu účinnosti smlouvy „T“ (např. T+60 dnů).
8. Harmonogram musí zahrnovat minimálně tyto uvedené milníky projektu:
 - a) Akceptace iniciační fáze projektu (metodika, technika a organizace řízení projektu, týmové role).
 - b) Akceptace globální analýzy a návrhu (Deadline pro předložení dokumentů fáze 1-6 a rozhodnutí o pokračování / ukončení realizace).
 - c) Akceptace dopracované globální analýzy a návrhu (v případě předchozí neakceptace zadavatelem).
 - d) Akceptace detailního návrhu ICIS (detailní návrh ICIS vychází ze studie proveditelnosti výměny ICIS, fáze 7) včetně požadavků na součinnost.
 - e) Akceptace závazných požadavků na zajištění potřebného HW (případně po etapách – testování a školení, migrace, ostrá implementace).
 - f) Předání SW licencí (najednou nebo po etapách).
 - g) Akceptace provedené instalace a konfigurace HW (najednou nebo po etapách).

- h) Akceptace provedení instalace a implementace ASW (fáze 8 až 13).
 - i) Akceptace provedené migrace dat (přípravných a finální).
 - j) Rozpis termínů zahájení a ukončení jednotlivých fází testování a ověřovacího provozu.
 - k) Akceptace předání ICIS do ostrého provozu.
 - l) Akceptace ukončení ostrého provozu se zvýšenou podporou a přítomností zástupce řešitelského týmu dodavatele na pracovišti zadavatele.
 - m) Ukončení projektu (akceptace díla).
 - n) V rámci přechodové fáze CIS-ICIS definovat v rámci harmonogramu také všechny podstatné milníky řešící změny organizačního charakteru, tj. změny procesů vyvolané přípravou a implementací ASW a migrací dat.
9. Zadavatel požaduje plánovat a popsat v harmonogramu také dostatečné časové rezervy v kritických fázích projektu.

IV. Pravidla pro vytvoření seznamu doporučeného HW pro provoz, správu a technickou podporu díla, souvisejícího licenčního SW a zajištění napojení na stávající infrastrukturu, na základě kterých dodavatel připraví příslušnou přílohu Smlouvy o vytvoření

1. Dodavatel v rámci zadávacího řízení předloží návrh doporučeného HW, licenčního SW a zajištění napojení na stávající infrastrukturu tak, aby byl zajištěn provoz a správa ICIS s požadovanými parametry. Zde je podrobně specifikován požadavek na uvedený návrh. Dodavatel je povinen při zpracování svého návrhu tyto požadavky zadavatele na uvedený návrh akceptovat a zohlednit.
2. Dodavatel předloží návrh parametrů HW a další infrastruktury (zejména operačních systémů a virtualizační platformy) nezbytných pro běh ICIS pro dosažení dostupnosti požadované v bodě 5 této přílohy. Uvedené parametry dostupnosti musí systém splňovat při dimenzování na „Požadovaný stav“ dle bodu 4. Dimenzování ICIS, plný „Podporovaný stav“ musí být dosažitelný pouze doplněním HW, např. doplněním diskové kapacity nebo interní paměti, nikoli jeho výměnou či navýšením SW licencí. Změna tohoto návrhu proti parametrům uvedených v nabídce dodavatele je možná pouze v důvodných případech nově zjištěných skutečností v průběhu analýzy majících dopad do potřebného výkonu hardware. Změna bude v takovém případě provedena k tíži zadavatele, jen pokud nedostatek návrhu dodavatele vznikl ze zavinění zadavatele.
3. Systém ICIS musí být trvale dostupný (365x7x24) minimálně pro vyřizování online dotazů externích aplikací (Portál OZP ONLINE, Portál ZP). Za účelem vysoké dostupnosti předpokládá zadavatel využití technologií pro eliminaci výpadku z důvodu HW chyby (záložní zdroje, motorgenerátor, cluster, redundantní propojení). Akceptovatelná doba neplánovaného výpadku systému je 4 hodiny v celku, v provozní době (7:00-17:00), maximálně 1x za měsíc. Plná funkčnost systému ICIS pro uživatele musí být dostupná v provozní době (7:00-17:00). Mimo provozní dobu mohou probíhat plánované i jednorázové dávkové úlohy jako je načítání dat z externích systémů, ELT (ETL) procedury pro plnění datového skladu, zpracování různých výkazů, generování výstupních dat, zpráv a protokolů, dále v tuto dobu mohou probíhat plánované servisní úkony systému včetně procesů zálohování atd. V této době je po dohodě se zadavatelem možné provádět servisní práce, opravy a nasazování nových funkcí případně další potřebné zásahy do systému.
4. ICIS jako plně integrovaný informační systém musí podporovat následující objemy při zachování deklarovaných odezev systému. Požadovaný stav musí ICIS splnit při náběhu systému. Podporovaný stav obsahuje očekávaný nárůst objemu dat v ICIS, pro který musí být řešení rozšiřitelné posílením HW infrastruktury bez nutnosti zásahu do programového řešení ICIS.

Parametr	Požadovaný stav	Podporovaný stav
Počet uživatelů	400, z toho 300 současně pracujících	800, z toho 500 současně pracujících
Počet pojištěnců	1 milión	5 miliónů
Počet poskytovatelů zdravotních služeb	25 tisíc	50 tisíc
Počet plátců zdravotního pojištění v kategoriích OSVČ, zaměstnavatel	200 tisíc	500 tisíc

5. Při akceptaci HW infrastruktury navržené dodavatelem, a dále po dobu platnosti Smlouvy o vytvoření a Smlouvy o podpoře, musí systém splňovat následující odezvy při zachování objemu dat požadovaného stavu:

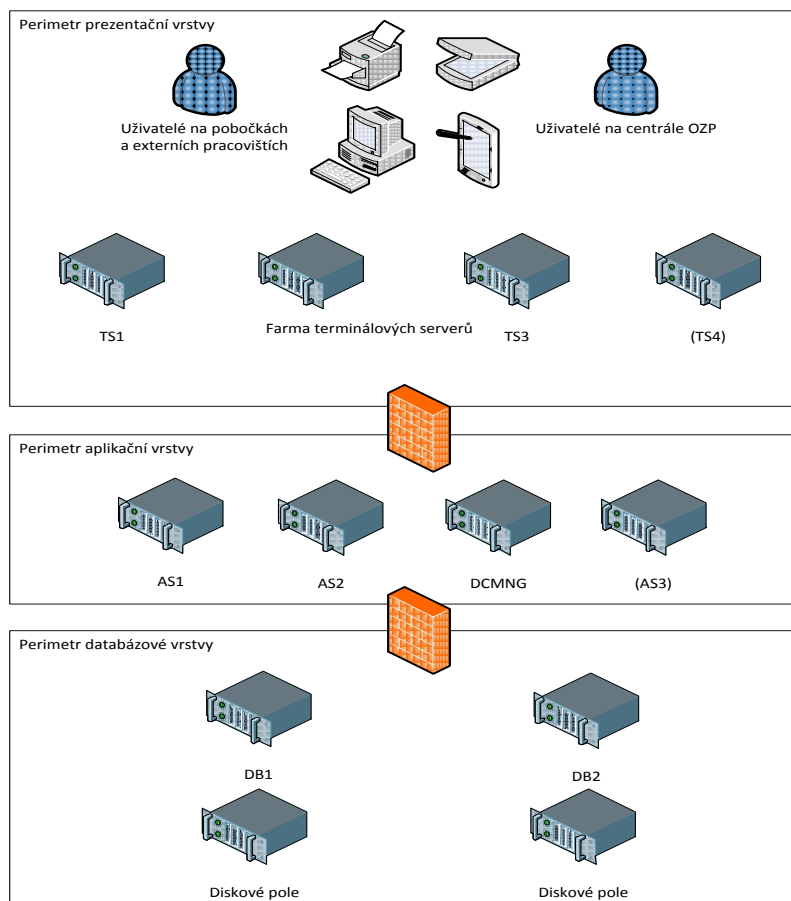
Parametr	Požadovaná hodnota	Přijatelná hodnota
Zpracování požadavku uživatele na přepážce (při interakci s klientem)	1 sekunda (80% případů), 2 sekundy (15% případů)	10 sekund (5% případů)
Zpracování online požadavku externího systému	1 sekunda	5 sekund (5% případů)
Zpracování požadavku uživatele u jednoho případu	1 sekunda (80% případů), 2 sekundy (15% případů)	10 sekund (5% případů)
Zpracování požadavku dávkové úlohy	Není explicitně stanoveno, běh dávkových úloh nesmí omezit provoz systému a musí počítat s časovými okny servisních zásahů (alespoň 4 hodiny denně).	Délka zpracování dávkové úlohy nebrání procesu zpracování údajů.

6. Zadavatel předpokládá, že ICIS bude provozován na nově dodané HW infrastruktuře, jejíž specifikaci určí dodavatel. HW prvky budou rozmístěny ve třech nezávislých lokacích, přičemž dvě lokace budou sloužit pro redundanci HW prvků a budou výkonově a funkčně ekvivalentní. Třetí lokace bude určena jako geografická záloha systému ICIS.
7. Na dodané HW infrastruktuře budou provozovány tři kopie systému – ostrý provoz, testovací provoz (předávací) a školící provoz (cvičný). Tato infrastruktura musí být pokryta kompletně licencemi tak, aby nedošlo k žádnému zpochybnění zadavatele jako provozovatele.
8. Součástí specifikace HW infrastruktury budou požadavky na zadavatele (v detailu minimálně dle lokací):
 - a) Požadovaný příkon elektrické sítě.
 - b) Prostorové nároky HW prvků.
 - c) Hmotnost HW prvků.
 - d) Požadavky na chladicí jednotky.
 - e) Požadavky na síťovou infrastrukturu pro propojení lokací, uživatelských stanic.
9. ICIS bude podporovat stávající tiskárny provozované v prostředí zadavatele. Bude-li některá z funkcí ICIS vyžadovat použití specifického typu tiskárny, musí být tato informace explicitně uvedena. Výčet používaných typů tiskáren je uveden v příloze studie proveditelnosti.
10. ICIS bude podporovat čtečky čárových kódů provozované v prostředí zadavatele. Bude-li ICIS vyžadovat specifickou čtečku čárových kódů, musí být tato informace explicitně uvedena. Výčet používaných čteček čárových kódů je uveden v příloze studie proveditelnosti.
11. ICIS bude podporovat terminály pro bezhotovostní platby provozované v prostředí zadavatele. Výčet používaných terminálů bezhotovostních plateb je uveden v příloze studie proveditelnosti.
12. Dodavatel nového ICIS vypracuje specifikaci HW, na kterém bude nový ICIS provozován. Zadavatel bude realizovat nákup HW samostatně mimo dodávku ICIS (jiný dodavatel). Soupis HW musí být natolik detailní, aby dodavatel garantoval provoz systému na HW splňujícím uvedenou konfiguraci. Náklady na HW nejsou zahrnuty do ceny dodávky (této zadávané veřejné zakázky), avšak náklady na licence potřebného SW (včetně operačních systémů) do této ceny zahrnuty budou. Vzhledem ke skutečnosti, že požadovaný HW bude zadavatel zadávat v zadávacím řízení dle zákona, musí být veškeré požadavky dodavatele na tento HW v návrhu formulovány takovým způsobem, který bude plně v souladu se ZVZ, resp. s novým zákonem o zadávání veřejných zakázek (a to primárně s požadavky obsaženými v § 44 odst. 11 ZVZ a § 45 ZVZ, resp. obdobnými požadavky vymezenými v novém zákoně o zadávání veřejných zakázek).
Celková výše nákladů na pořízení nového HW dle specifikace dodavatele nesmí přesáhnout 22.200.000,- Kč bez DPH.

13. V další části je uvedena specifikace očekávané struktury prvků infrastruktury a HW pro zajištění chodu ICIS. Jde o návrh prvků infrastruktury pro zajištění chodu systému a jeho průběžný rozvoj, testování a zálohování.

a) Požadavky zadavatele na HW infrastrukturu ICIS

Následující schéma obsahuje logické HW schéma prostředí serverů navrhovaného systému ICIS ve zjednodušené, přehledné formě. Neuvádí odpovídající aktivní prvky sítí LAN, WAN a SAN, které jsou dodavateli jako odborníkovi (technikovi) zřejmé a celé schéma by značně znehlednily.



Celé řešení ICIS požadujeme rozdělit do tří základních bezpečnostních perimetrů odpovídajících jednotlivým vrstvám aplikace:

- Prezentační vrstva – zahrnuje v sobě uživatele systému ICIS, jejich pracovní stanice, tiskárny, čtečky kódů a další periferie včetně případných přenosných zařízení. Dále obsahuje farmu serverů prezentační vrstvy ICIS tvořené čtyřmi fyzickými uzly terminálových serverů (konkrétně Remote Desktop Session Host). Součástí tohoto perimetru je i existující doména adresáře MS Active Directory obsahující mimo jiné účty uživatelů, stanic a případně dalších periferních zařízení, která to umožňují. Uživatelé přistupují k prezentační vrstvě ze svých stanic pomocí vzdáleného terminálového připojení (Remote Desktop Client).
- Aplikační vrstva je tvořena trojicí fyzických serverů hostujících virtualizované prostředí aplikačních serverů (viz dále) a fyzickým serverem pro management a primární doménový řadič centra.

- Databázová vrstva je tvořena dvojicí fyzických databázových serverů a společnou sítí SAN obsahující sdílenou diskovou kapacitu a dále zálohovací zařízení. Databázová a aplikační vrstva jsou též členy společné domény Active Directory centra podřízené hlavní doméně v rámci jednostranného vztahu důvěry oddělující z bezpečnostních důvodů serverové a aplikační účty centra.

Pro účely testovacího a školicího prostředí přibude jeden fyzický server v aplikační vrstvě (AS3), který bude hostovat kompletní prostředí odpovídajících virtuálních serverů. Prezentační vrstva poskytne pro účely testování a školení jeden z fyzických uzlů farmy (TS4). Databázová vrstva bude společná – testovací a školicí prostředí bude mít svoje vlastní, oddělené databáze. Fyzické servery pro testovací a školicí prostředí (AS3 a TS4) budou zároveň zálohou pro prostředí provozní v případě výpadku nebo pro období maximální zátěže (sezónní či jiný důvod).

S ohledem na aktuální možnosti virtualizace a fakt, že je potřebné poskytnout vysoký komfort uživatelům v centrále i na odloučených pracovištích a zároveň se jedná o systém s velmi vysokými nároky na celkovou bezpečnost je navrženo využití infrastruktury virtuálních desktopových sezení (Remote Desktop Sessions) zpřístupněných terminálovým přístupem. Zásadními výhodami tohoto řešení jsou:

- Vysoká bezpečnost – koncové zařízení uživatele neobsahuje žádná data systému (tedy ani osobní a citlivá), případné pracovní výstupy uživatele formou exportů, dokumentů apod. jsou též bezpečně uloženy v centru. Případná krádež či ztráta mobilního koncového zařízení tak neznamená ohrožení bezpečnosti dat.
- Snadná centrální správa – nároky kladené na prostředí LAN koncových stanic jsou minimalizovány. Stanice musí umožnit spuštění terminálového klienta a zpřístupnit lokálně umístěné periferie. Neobsahují však žádnou z komponent ICIS. Celé prostředí ICIS je v centru, je snadno spravovatelné, lze provádět bezpečně jeho upgrade a další rozvoj, minimalizuje se dopad heterogenity prostředí klientských stanic.
- Předvídatelné a dlouhodobě stabilní nároky na kapacitu WAN sítě pro vzdálená pracoviště. Podobné bezpečnostní prostředí pro přístup i mimo lokality OZP.

b) Informativní odhad objemů ukládaných dat ze strany zadavatele

Diskové pole bude ukládat data dle následující tabulky:

Typ ukládaných dat	Odhad objemu	Způsob uložení
Virtuální disky virtuálních serverů	19 x 40GB + rezerva = 1TB	RAID5
Roaming user profily	400 x 2GB = 800GB	RAID5
Data CRM	150 GB*	RAID5
Data ERP	800 GB*	RAID5
Data výdajové části	1TB	RAID5
Business Intelligence	1TB	RAID5
CELKEM	4,75TB	RAID5

Poznámka: Odhad objemu se týká provozního systému. Celkovou kapacitu je třeba vynásobit počtem kopií systému (záložní, testovací, školicí systém).

c) Centrální výpočetní výkon - kapacity přenosových linek

Pro síť LAN v sídle OZP předpokládáme dnes již standardní strukturovanou kabeláž a aktivní prvky pro Ethernet 100 Mbit/s. Páteřní síťové prvky by proto měly mít kapacitu 1 Gbit/s.

Navrhované řešení nebude klást zvýšené nároky na kapacitu LAN oproti běžnému provozu – nepředpokládáme přenosy velkého objemu dat po LAN.

Síť WAN pro připojení poboček a odloučených pracovišť bude pro navrhované řešení klíčová. Vzhledem k navržené virtualizaci desktopových sezení (využití terminálů s protokolem RDP) bude třeba zajistit malou latenci sítě. Pro síť WAN doporučujeme:

- Dostatečnou kapacitu pro připojení každého terminálového uživatele (pro základní odhad lze vyjít z kapacity 64 Kbit/s na uživatele u malého počtu uživatelů, při počtu 10 a více klesne postupně průměr na uživatele k 32 Kbit/s vzhledem k nestejněměrnému využití terminálového desktopu jednotlivými uživateli v čase) se zohledněním dodatečných požadavků na kapacitu pro přenos skenovaných dokumentů a další neterminálový provoz.
- Zajištění nízké latence sítě, pokud bude po WAN i jiný než terminálový provoz (např. tisky, skenování, přenosy souborů apod.) doporučujeme uplatnit nějakou formu řízení sítě a QoS.
- Zajištění záložních linek pro ta pracoviště, kde by výpadek primární linky znamenal zásadní problém.

d) Další požadavky

Navrhované řešení předpokládá využití následujících služeb stávající infrastruktury OZP (případně jejich realizaci):

- Prostředí zálohování v SAN infrastruktuře (zálohovací server a software NetWorker, páskovou knihovnu a média), licence pro zálohování nově pořízených fyzických a případně i virtuálních serverů.
- Dostatečné prostory datového centra pro umístění nové techniky se zajištěným přívodem elektrické energie, UPS, klimatizací, volné místo v RACK skříních.
- Zajištěnou objektovou (fyzickou) bezpečnost datového centra a jeho kvalifikovanou obsluhu a správu.
- Síťovou infrastrukturu centra (aktivní prvky sítě), volné porty pro připojení navrhovaných fyzických serverů řešení.
- Prostředky pro zabezpečení sítě a oddělení bezpečnostních perimetrů – firewally, možnost zřízení VLAN a řízení provozu mezi nimi.
- Zabezpečené připojení do Internetu a dalších privátních sítí budou-li potřeba pro provoz řešení.
- Periferie dle zadávací dokumentace (tiskárny, scannery, čtečky čárových kódů apod.).
- Základní síťové služby (DNS, DHCP apod.).
- Systém elektronické pošty se standardním API rozhraním.
- Adresářovou službu MS Active Directory pro zajištění vzdálené správy stanic, jednotné identity uživatelů – pro aplikační a databázovou vrstvu navrženého řešení předpokládáme vytvoření oddělené AD domény s jednostranným vztahem důvěry pro ochranu aplikačních účtů centra (pokud již neexistuje).

e) Bezpečnost dat

Nový ICIS musí splňovat požadavky na bezpečnost dat:

- Dohledatelnost a právní prokazatelnost údajů a jejich změn v ICIS, právní prokazatelnost účetnictví.

- Dohledatelnost a právní prokazatelnost dokumentů distribuovaných ICIS – standardní používání certifikátů, šifrované komunikace a elektronických podpisů s časovým razítkem.
- Ochranu údajů proti zneužití (neoprávněnému přístupu), včetně logování přístupu uživatelů.
- Ochranu proti neoprávněnému přístupu nástroji mimo systém ICIS.
- Ochranu proti neoprávněné změně dat a funkcí.
- Ochranu konzistence dat uvnitř ICIS i v rámci komunikačních kanálů a protokolů s okolními systémy.
- Kontrolu proti vnitřnímu fraudu – ICIS bude podporovat nástroje pro identifikaci podezřelých situací indikujících možné snahy o neoprávněné obohacení ze strany pracovníků pojišťovny.
- Výstupy pro interní a externí bezpečnostní audit.
- Ochranu proti úniku informací neoprávněným uživatelům.

Zabezpečení dat uvnitř systému ICIS není explicitně vyžadováno. Serverové prostředí ICIS včetně datových úložišť bude považováno za důvěryhodné, není nutné šifrovat data na datovém úložišti nebo při komunikaci mezi systémy. Systém musí být připraven na možnou změnu legislativy v oblasti vnitřního zabezpečení dat. Funkce ICIS však musí zajistit logování veškerých aktivit uživatelů a správců v souvislosti s modifikací a čtením dat včetně historie a zajistit podporu pro vyhodnocení logů. Aktivace logování nesmí snížit odezvy systému ICIS mimo požadované provozní parametry.

Bude-li nový ICIS ukládat důvěrná data mimo samotný systém (serverovou infrastrukturu), musí být tato funkce explicitně zdůvodněna a schválena zadavatelem. Toto se netýká ostatních interních systémů zadavatele, které jsou také považovány za důvěryhodné.

Uživatelé budou k datům přistupovat prostředky ICIS, případně budou mít pro reporting přístup do definovaného datového skladu. Přímý přístup k datům transakčních částí systému musí být uživatelům zamezen s výjimkou odpovědných pracovníků IT.

Oprávněný uživatel bude moci data přenášet na PC zadavatele. Řízení přístupu k datům mimo systém ICIS není součástí poptávky.

Datové úložiště by mělo být pro celý systém ICIS na jedné technologické platformě. Datové úložiště musí zajistit požadavky na zabezpečení, výkon a integritu spravovaných dat. Nový ICIS musí v maximální míře omezit duplicitu dat.

Datové úložiště musí umožnit propojení na stávající datový sklad provozovaný na platformě Microsoft SQL Server, a to zaměstnanci IT oddělení zadavatele. Pro tvorbu sestav zadavatel předpokládá, že součástí ICIS bude datový prostor pro provádění analýz, ke kterému bude přístup z technologií Microsoft SQL Server (SSIS, SSAS, SSRS) za účelem vlastních analýz a tvorby vlastních sestav zadavatelem.

Pro specifické aplikace uvedené v návrhu systému musí ICIS umožnit IT oddělení OZP vytvořit vlastní programy zpracování dat, které budou postaveny na technologiích Microsoft.NET. Nový ICIS musí minimálně podporovat vzájemnou výměnu dat za použití standardních služeb (SOAP, REST, XML).

f) Řízení přístupu uživatelů a správců

Přihlašování do systému ICIS bude řešeno technologií Single Sign-On s využitím Microsoft Active Directory provozované zadavatelem. MS Active Directory je aktuálně na technologické úrovni Windows 2008 R2. Bude-li Dodavatel požadovat jinou technologickou úroveň, musí být tato informace explicitně uvedena a náklady na tuto změnu musí být součástí nabídkové ceny. Ochrana specifických částí systému (heslo, certifikát, HW token) musí být explicitně uvedena. Dodavatel může navrhnout vlastní způsob realizace Single Sign-On s využitím stávající MS Active Directory, např. v kombinaci s dalšími identifikačními nástroji, avšak správa uživatelů musí být napříč řešením jednotná a probíhat nad MS Active Directory.

Zabezpečení přístupu k funkcím ICIS bude řízeno víceúrovňovou definicí oprávnění. Základní autentizační jednotkou bude identita uživatele v prostředí Active Directory. Pro řízení přístupu k prostředkům systému ICIS zadavatel předpokládá využití bezpečnostních skupin, uživatelé budou zařazováni do připravených skupin dle rolí, které budou vykonávat.

Nový ICIS bude pro vybrané agendy podporovat řízení přístupu až k jednotlivým datovým záznamům (např. filtrovat přístup k datům dle vybraného atributu), viz požadavky na funkce systému.

Nový ICIS bude podporovat ověřování identity klientů v externích aplikacích uvedených v tomto dokumentu.

Nový ICIS bude obsahovat víceúrovňovou administraci uživatelských oprávnění. ICIS umožní vybraným uživatelům spravovat uživatelské přístupy jemu podřízených zaměstnanců.

Základní bezpečnostní cíle, které ICIS musí zajistit, jsou:

- Integrita
- Důvěrnost
- Dostupnost
- Autenticita
- Prokazatelnost odpovědnosti
- Nepopiratelnost odpovědnosti
- Spolehlivost

ICIS musí podporovat zavedení identity managementu (IDM), které zadavatel plánuje.

Přílohy: Studie proveditelnosti projektu „Výstavba, implementace a technická podpora ICIS OZP“