

# ***Příloha č. 8***

Návrh řešení Plnění

# Obsah

---

1	Návrh architektury systému	5
1.1	Popis komponent řešení	5
1.1.1	Diagram komponent řešení	5
1.1.2	Mapování komponent řešení	6
1.1.3	Implementace komponent řešení Dodavatele - SW produkty a vývoj na zakázku	11
1.2	Popis rozhraní a datových toků	15
1.2.1	Diagram rozhraní a datových toků	15
1.2.2	Popis implementace rozhraní a datových toků	16
1.3	Popis parametrizace systému a způsobu řešení změn	24
1.4	Popis logování a monitoringu	27
2	Implementace procesů	33
2.1	Popis implementace procesů	33
3	Návrh Technické infrastruktury systému	41
3.1	Produkční prostředí	41
3.1.1	Schéma technické architektury	41
3.1.2	Popis technické architektury	43
3.1.3	Vysoká dostupnost	45
3.1.4	Bezodstávkový provoz Dozorové části	48
3.1.5	Požadavky na síťovou infrastrukturu	49
3.1.6	Kalkulace datových a diskových kapacit	54
3.1.7	Kalkulace výpočetního výkonu, paměti a systémových disků	56
3.2	Pre-produkční prostředí	57
3.2.1	Schéma technické architektury	57
3.2.2	Popis technické architektury	59
3.2.3	Kalkulace datových a diskových kapacit	61
3.2.4	Kalkulace výpočetního výkonu, paměti a systémových disků	62
3.3	Testovací/Vývojové prostředí	63
3.3.1	Schéma technické architektury	63
3.3.2	Popis technické architektury	65
3.3.3	Kalkulace datových a diskových kapacit	66
3.3.4	Kalkulace výpočetního výkonu, paměti a systémových disků	67
3.4	Souhrn požadavků na výpočetní výkon a diskové prostory a jejich časový vývoj	69

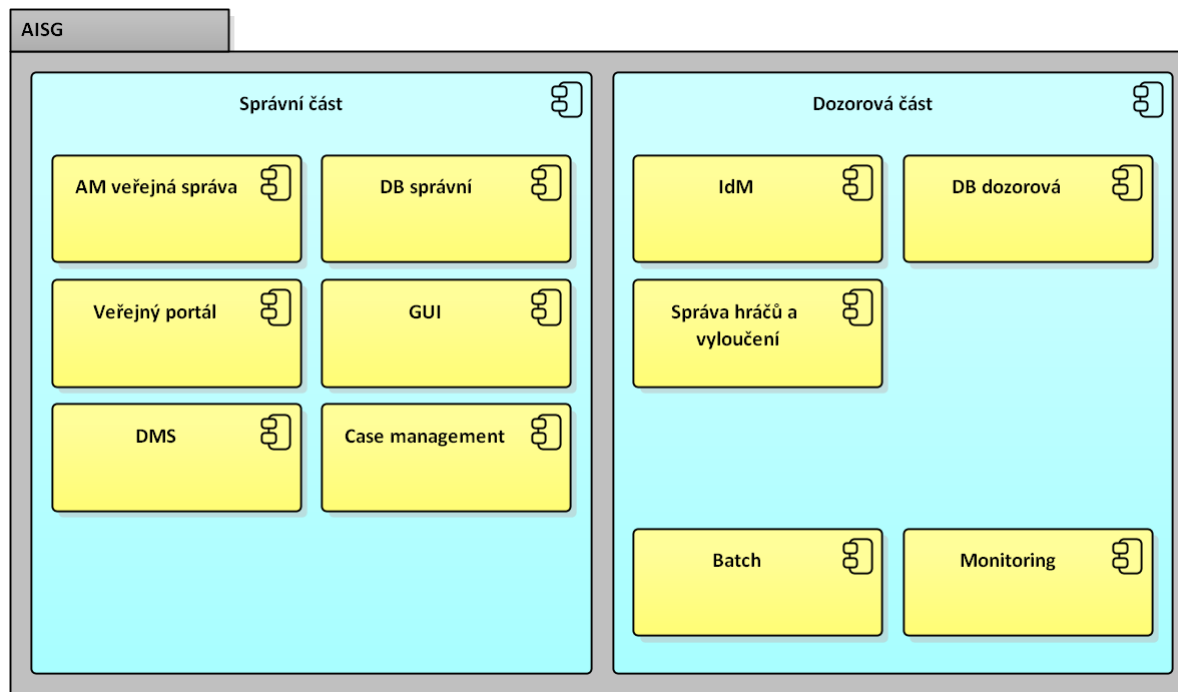
---

4	Seznam licencí, maintenancí a subskripcí SW produktů	70
4.1	Produkční prostředí	70
4.1.1	Etapa 1B	70
4.1.2	Etapa 2 a Servisní služby po ukončení Etapy1B	73
4.1.3	Servisní služby po ukončení Etapy 2	75
4.2	Neprodukční prostředí	78
4.3	Jednotkové ceny	80
5	Řešení bezpečnosti	81
5.1	Popis řešení bezpečnosti	81
5.2	Popis bezpečnostních prvků a mechanismů	82
5.3	Popis auditních logů a bezpečnostního monitoringu	93
6	Rámcový harmonogram realizace	99
6.1	Rámcový harmonogram realizace	99
6.2	Součinnosti	110
7	Servisní služby	120
7.1	Popis Servisních služeb	120
7.1.1	Přehled prováděných servisních služeb	121
7.1.2	Hotline	125
7.1.3	Typy incidentů	125
7.1.4	Garantované SLA	126

# 1 Návrh architektury systému

## 1.1 Popis komponent řešení

### 1.1.1 Diagram komponent řešení



## 1.1.2 Mapování komponent řešení

Komponenta řešení dle kapitoly 2.2 Přílohy č. 1 Smlouvy	Komponenty řešení Dodavatele	Naplnění požadavků v kapitole 2.2 Přílohy č. 1 Smlouvy
DB správní	DB správní, Batch, Monitoring	<p><b>DB správní</b> – databáze udržuje data o legálních provozovatelích, nelegálních provozovatelích a ostatních subjektech působících v rámci provozování hazardních her, včetně souvisejících řízení.</p> <p>DB správní udržuje kromě aktuálních dat i historii změn pro účely předávání historie změn do Analytického modulu a pro podporu procesu Archivace (viz proces 16. Archivace v Příloze č. 2 Smlouvy). Předávání do Analytického modulu a proces Archivace realizuje komponenta <b>Batch</b> (aplikace). Tato aplikace rovněž plní úlohu pravidelné aktualizace a exportů záznamů DB správní.</p> <p>Požadavek na provozní a bezpečnostní logování a monitoring komponent (viz 3.3.9 v Příloze č. 1 Smlouvy) plní komponenta <b>Monitoring</b> (logovací server), která bude integrována s nástroji SPCSS.</p> <p>Komponenty Batch a Monitoring jsou uvedeny v dozorové části, nicméně Dodavatel předpokládá jejich použití z obou částí systému – ve stejném smyslu, v jakém je použita komponenta IdM řešení dle kapitoly 2.2 Přílohy č. 1 Smlouvy.</p>
DB hráčů	DB dozorová, Správa hráčů a vyloučení, Batch, Monitoring	<p><b>DB dozorová</b> (plní požadavky DB hráčů a DB vyloučení dle kapitoly 2.2 přílohy č. 1 Smlouvy) – databáze udržující data o hráčích a jejich vazbách na provozovatele.</p> <p>DB dozorová udržuje kromě aktuálních dat i historii změn pro účely předávání historie změn do Analytického modulu a pro podporu procesu Archivace (viz proces 16. Archivace v Příloze č. 2 Smlouvy). Předávání do Analytického modulu a proces Archivace realizuje komponenta <b>Batch</b> (aplikace). Tato aplikace rovněž plní úlohu pravidelné aktualizace a exportů záznamů DB dozorová.</p> <p>Komunikační rozhraní komponenty <b>Správa hráčů a vyloučení</b> (aplikace) plní požadavky na vystavení služeb pro Registraci/z totožnění hráče a Aktualizaci údajů hráče v souladu s procesem 13. Registrace (viz Přílohu č. 2 Smlouvy).</p> <p>Požadavek na provozní a bezpečnostní logování a monitoring komponent (viz 3.3.9 v Příloze č. 1 Smlouvy) plní komponenta <b>Monitoring</b> (logovací server), která bude integrována s nástroji SPCSS.</p>

Komponenta řešení dle kapitoly 2.2 Přílohy č. 1 Smlouvy	Komponenty řešení Dodavatele	Naplnění požadavků v kapitole 2.2 Přílohy č. 1 Smlouvy
		Komponenty Batch a Monitoring jsou uvedeny v dozorové části, nicméně Dodavatel předpokládá jejich použití z obou částí systému – ve stejném smyslu, v jakém je použita komponenta IdM řešení dle kapitoly 2.2 Přílohy č. 1 Smlouvy.
DB vyloučení	DB dozorová, Správa hráčů a vyloučení, Batch, Monitoring	<p><b>DB dozorová</b> (plní požadavky DB hráčů a DB vyloučení dle kapitoly 2.2 přílohy č. 1 Smlouvy) – databáze udržující data o subjektech vyloučených z hraní (využívaná jak při registraci, tak při autorizaci hráče) a záznamy o transakcích služby ověření hráče.</p> <p>DB vyloučení udržuje kromě aktuálních dat i historii změn pro účely předávání historie změn do Analytického modulu a pro podporu procesu Archivace (viz proces 16. Archivace v Příloze č. 2 Smlouvy). Předávání do Analytického modulu a proces Archivace realizuje komponenta <b>Batch</b> (aplikace). Tato aplikace rovněž plní úlohu pravidelné aktualizace a exportů záznamů DB dozorová.</p> <p>Komunikační rozhraní komponenty <b>Správa hráčů a vyloučení</b> (aplikace) plní požadavek na vystavení služeb pro Autorizaci hráče v souladu s procesem 13. Registrace (viz Přílohu č. 2 Smlouvy). Grafické rozhraní této komponenty plní požadavek na manuální provádění zápisu a výmazu osob v rejstříku vyloučených osob pracovníky MF (viz kapitolu 1.2 Přílohy č. 1 Smlouvy).</p> <p>Požadavek na provozní a bezpečnostní logování a monitoring komponent (viz 3.3.9 v Příloze č. 1 Smlouvy) plní komponenta <b>Monitoring</b> (logovací server), která bude integrována s nástroji SPCSS.</p> <p>Komponenty Batch a Monitoring jsou uvedeny v dozorové části, nicméně Dodavatel předpokládá jejich použití z obou částí systému – ve stejném smyslu, v jakém je použita komponenta IdM řešení dle kapitoly 2.2 Přílohy č. 1 Smlouvy.</p>
Case Management	Case Management, Batch, Monitoring	<p>Komponenta <b>Case Management</b> řídí všechna workflow Správní části. Je součástí implementace všech uživatelských a automatických procesů Správní části využívajících logiku workflow.</p> <p>Každé workflow je složeno z jednotlivých úkolů. Ke každému úkolu je přiřazena odpovídající role, která jej vykonává. Při každém přechodu (úkol, stav) mohou být nadefinovány jednotlivé akce (například notifikace). Přehled workflow pokrytých systémem je uveden v Analytické dokumentaci.</p> <p>Pravidelné aktualizace záznamů (provolávání služeb eGSB, ADIS, aktualizace z ISZR) realizuje komponenta <b>Batch</b> (aplikace).</p>

Komponenta řešení dle kapitoly 2.2 Přílohy č. 1 Smlouvy	Komponenty řešení Dodavatele	Naplnění požadavků v kapitole 2.2 Přílohy č. 1 Smlouvy
		<p>Požadavek na provozní a bezpečnostní logování a monitoring komponent (viz 3.3.9 v Příloze č. 1 Smlouvy) plní komponenta <b>Monitoring</b> (logovací server), která bude integrována s nástroji SPCSS.</p> <p>Komponenty Batch a Monitoring jsou uvedeny v dozorové části, nicméně Dodavatel předpokládá jejich použití z obou částí systému – ve stejném smyslu, v jakém je použita komponenta IdM řešení dle kapitoly 2.2 Přílohy č. 1 Smlouvy.</p>
DMS	DMS, Monitoring	<p><b>Document Management System (DMS)</b> – systém pro správu dokumentů. Komponenta je součástí implementace všech uživatelských a automatických procesů Správní části pracujících s dokumenty.</p> <p>Udržuje dokumenty související s agendou systému, které jsou nahrány přímo do systému a nejsou udržovány v jiných systémech státní správy.</p> <p>V DMS budou fyzicky uloženy pouze dokumenty, které nebudou fyzicky uloženy v EPD (např. dokumenty obcí a krajů). Jeden dokument musí být na MF dlouhodobě autoritativně uchovávan pouze na jednom místě bez omezení pro oprávněného uživatele. Systém EPD nenabízí možnost vzdáleného přístupu pro jiné organizace než MF. Dokumenty mimo MF budou předávány zprostředkovaně dočasnou kopií v AISG, a to výhradně za účelem zobrazení.</p> <p>Podpora skenování není požadována. Počet ukládaných dokumentů do DMS bude maximálně 20 tisíc za jeden rok. Průměrná velikost dokumentu nepřekročí 1 MB.</p> <p>DMS bude v souladu s požadavky na ISSD (informační systém spravující dokumenty) dané Národním standardem pro elektronické systémy spisové služby (<a href="http://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx">http://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx</a>).</p> <p>Požadavek na provozní a bezpečnostní logování a monitoring komponent (viz 3.3.9 v Příloze č. 1 Smlouvy) plní komponenta <b>Monitoring</b> (logovací server), která bude integrována s nástroji SPCSS.</p> <p>Komponenta Monitoring je uvedena v dozorové části, nicméně Dodavatel předpokládá její použití z obou částí systému – ve stejném smyslu, v jakém je použita komponenta IdM řešení dle kapitoly 2.2 Přílohy č. 1 Smlouvy.</p>
GUI	GUI, Monitoring	<b>Graphical User Interface (GUI)</b> – Grafické rozhraní systému.

Komponenta řešení dle kapitoly 2.2 Přílohy č. 1 Smlouvy	Komponenty řešení Dodavatele	Naplnění požadavků v kapitole 2.2 Přílohy č. 1 Smlouvy
		<p>Jedná se o jednotné uživatelské rozhraní pro vykonávání agend v zodpovědnosti MF pro uživatele z resortu MF. Pro přístup k informacím toto rozhraní využívá i CS a FS (nicméně nemá oprávnění do systému zapisovat informace).</p> <p>GUI bude mít formu tenkého klienta (web aplikace). GUI bude provozovatelné na běžných kancelářských PC s rozlišením obrazovky 1024x768 a vyšším, operačních systémech MS Windows 7 (32-bit a 64-bit) a novějších a bude podporovat Internet Explorer a Firefox ve verzích podporovaných výrobcí.</p> <p>Požadavek na provozní a bezpečnostní logování a monitoring komponent (viz 3.3.9 v Příloze č. 1 Smlouvy) plní komponenta <b>Monitoring</b> (logovací server), která bude integrována s nástroji SPCSS.</p> <p>Komponenta Monitoring je uvedena v dozorové části, nicméně Dodavatel předpokládá její použití z obou částí systému – ve stejném smyslu, v jakém je použita komponenta IdM řešení dle kapitoly 2.2 Přílohy č. 1 Smlouvy.</p>
Veřejný portál	Veřejný portál, Monitoring	<p><b>Veřejný portál</b> slouží pro přístup veřejnosti a uživatelů mimo resort MF. Z tohoto důvodu je rozdělený na dvě části – veřejnou a privátní.</p> <ol style="list-style-type: none"> <li>1. Veřejná část <ul style="list-style-type: none"> <li>• Je určena pro přístup široké veřejnosti.</li> <li>• Slouží k zobrazování veřejně dostupných informací (včetně veřejně dostupných formulářů).</li> <li>• Je dále určena pro nepřihlášené provozovatele, resp. PAO, kteří mají možnost portál využít pro zadání žádosti a poskytnutí dokumentů, funkce předvyplnění údajů a přístup k historii žádostí získají až po přihlášení do privátní části portálu.</li> </ul> </li> <li>2. Privátní část <ul style="list-style-type: none"> <li>• Je určena pro přístup úředníků z obcí a krajů.</li> <li>• Úředníci se do ní hlásí přes své přístupové údaje v JIP/KAAS.</li> <li>• Funguje jako jediné uživatelské rozhraní pro obce a kraje.</li> <li>• Je dále určena pro přihlášené provozovatele, resp. PAO, kteří mají možnost portál využít pro zadání žádosti a poskytnutí dokumentů, včetně předvyplnění údajů a přístupu k historii svých žádostí.</li> </ul> </li> </ol> <p>Veřejný portál je web aplikace a bude podporovat prohlížeče Internet Explorer, Firefox, Chrome, Safari a Edge ve verzích podporovaných výrobcí.</p> <p>Požadavek na provozní a bezpečnostní logování a monitoring komponent (viz 3.3.9 v Příloze č. 1 Smlouvy) plní komponenta <b>Monitoring</b> (logovací server), která bude integrována s nástroji SPCSS.</p>



Komponenta řešení dle kapitoly 2.2 Přílohy č. 1 Smlouvy	Komponenty řešení Dodavatele	Naplnění požadavků v kapitole 2.2 Přílohy č. 1 Smlouvy
		Komponenta Monitoring je uvedena v dozorové části, nicméně Dodavatel předpokládá její použití z obou částí systému – ve stejném smyslu, v jakém je použita komponenta IdM řešení dle kapitoly 2.2 Přílohy č. 1 Smlouvy.
AM veřejná správa	AM veřejná správa, Monitoring	<p><b>AM veřejná správa</b> je modul, který slouží k řízení přístupu (AM – Access Management) uživatelů z veřejné správy (včetně obcí a krajů) k funkcím AISG.</p> <p>Pro správu identit a přístupových údajů uživatelů z veřejné správy a jejich základních rolí v AISG bude použit systém JIP/KAAS. Modul „AM veřejná správa“ v maximální možné míře využije autentizační a autorizační služby JIP/KAAS, včetně nastavení činnostních a přístupových rolí AIS, které doplní o nastavení lokálních rolí specifických pro jednotlivé komponenty AISG a použité SW produkty, včetně autorizace na základě územní působnosti, času a typu dokumentů apod.</p> <p>Pro zaměstnance resortu MF, kteří jsou běžnými uživateli AISG, platí požadavek na autentizaci prostřednictvím JIP/KAAS a zároveň požadavek integrace s Active Directory MF (single sign-on). Zaměstnanci resortu MF jsou vybaveni čipovými kartami s uloženými certifikáty v souladu se zákonem č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce a čtečkami čipových karet. Modul plní požadavek integrace autentizace čipovou kartou do AISG.</p> <p>Autentizace malého počtu technických administrátorů systému a jeho jednotlivých komponent bude implementována způsobem specifickým pro jednotlivé komponenty (lokální účet).</p> <p>Požadavek na provozní a bezpečnostní logování a monitoring komponent (viz 3.3.9 v Příloze č. 1 Smlouvy) plní komponenta <b>Monitoring</b> (logovací server), která bude integrována s nástroji SPCSS.</p> <p>Komponenta Monitoring je uvedena v dozorové části, nicméně Dodavatel předpokládá její použití z obou částí systému – ve stejném smyslu, v jakém je použita komponenta IdM řešení dle kapitoly 2.2 Přílohy č. 1 Smlouvy.</p>
IdM	IdM, DB dozorová, Monitoring	<p>Modul <b>IdM</b>, který slouží ke správě identit provozovatelů a PAO. Je využíván v Dozorové části (správa identit provozovatelů) i ve Správní části (správa identit provozovatelů i PAO), v diagramech je zařazen v Dozorové části z důvodů nejvyšších provozních požadavků této části.</p> <p>Pro přístup do Veřejného portálu budou provozovatelé a PAO využívat autentizaci pomocí autentizační služby Portálu veřejné správy, která ověřuje uživatele pomocí přístupových údajů datových schránek (ISDS – identifikace právnických osob).</p>

Komponenta řešení dle kapitoly 2.2 Přílohy č. 1 Smlouvy	Komponenty řešení Dodavatele	Naplnění požadavků v kapitole 2.2 Přílohy č. 1 Smlouvy
		<p>Předpokládá se dvouúrovňový systém, který naplňuje požadavky řešení bezpečnosti. Provozovatelé, resp. PAO budou přistupovat do několika částí AISG (veřejný portál ve správní části, dozorová část pro registraci a autorizaci hráčů, DB správní a DMS pro PAO). V prvním případě bude autentizace provozovatele založena na ISDS, ve zbylých případech se bude jednat o XML komunikaci s využitím HTTPS. Z legislativního hlediska není důležité, který konkrétní pracovník provozovatele, resp. PAO přistupuje k AISG, odpovědnost za předávání dat a dodržení ostatních pravidel dle zákona je na provozovateli, resp. PAO jako právnické osobě.</p> <p>IdM modul bude tedy evidovat provozovatele hazardních her, resp. PAO, a pro každého jednu až několik sad přístupových údajů pro Dozorovou část (včetně jejich certifikátů). IdM bude dále obsahovat údaj o datové schránce provozovatele, resp. PAO. Evidence bude vedena v komponentě <b>DB dozorová</b>.</p> <p>IdM kontroluje platnost uložených certifikátů a notifikuje administrátora o blížícím se termínu obnovy certifikátů.</p> <p>IdM bude umožňovat administrátorskou operaci strojově čitelného exportu údajů o provozovatelích a PAO (např. CSV, XML, samostatné soubory s certifikáty,...) za účelem využití stejných identit v jiných systémech Objednatele komunikujících s provozovateli a PAO.</p> <p>Požadavek na provozní a bezpečnostní logování a monitoring komponent (viz 3.3.9 v Příloze č. 1 Smlouvy) plní komponenta <b>Monitoring</b> (logovací server), která bude integrována s nástroji SPCSS.</p> <p>Komponenta Monitoring je uvedena v dozorové části, nicméně Dodavatel předpokládá její použití z obou částí systému – ve stejném smyslu, v jakém je použita komponenta IdM řešení dle kapitoly 2.2 Přílohy č. 1 Smlouvy.</p>

### 1.1.3 Implementace komponent řešení Dodavatele - SW produkty a vývoj na zakázku

Komponenta řešení Dodavatele	Použité SW produkty, míra pokrytí funkčních požadavků out-of-box Části vyvinuté na zakázku, programovací jazyk a typ aplikačních serverů
DB správní	<p><b>Použitý SW:</b> Databázový server PostgreSQL (Postgres) – relační SQL databáze</p> <p><b>Míra pokrytí funkčních požadavků out-of-the-box:</b> Žádné pokrytí, vývoj na zakázku.</p> <p><b>Části vyvinuté na zakázku, programovací jazyk:</b> Všechny funkční požadavky budou realizovány v jazycích SQL a PL/pgSQL. Použití SW uvedených produktů Dodavatel předpokládá tak, jak jsou, tedy bez úprav jejich zdrojového kódu. Produkty jsou nosnou platformou pro řešení vyvinuté na zakázku.</p>
Batch	<p><b>Použitý SW:</b> Aplikační server WildFly (Red Hat) – Java EE server</p> <p><b>Míra pokrytí funkčních požadavků out-of-the-box:</b> Žádné pokrytí, vývoj na zakázku.</p> <p><b>Části vyvinuté na zakázku, programovací jazyk:</b> Všechny funkční požadavky budou realizovány v jazyce Java. Použití SW uvedených produktů Dodavatel předpokládá tak, jak jsou, tedy bez úprav jejich zdrojového kódu. Produkty jsou nosnou platformou pro řešení vyvinuté na zakázku.</p>
Monitoring	<p><b>Použitý SW:</b> Logovací server Graylog – logovací server se strukturovanými logy, GUI, REST API, a dotazováním nad NoSQL databází, vstupy, filtrováním, alertingem a výstupy</p> <p><b>Míra pokrytí funkčních požadavků out-of-the-box:</b></p>

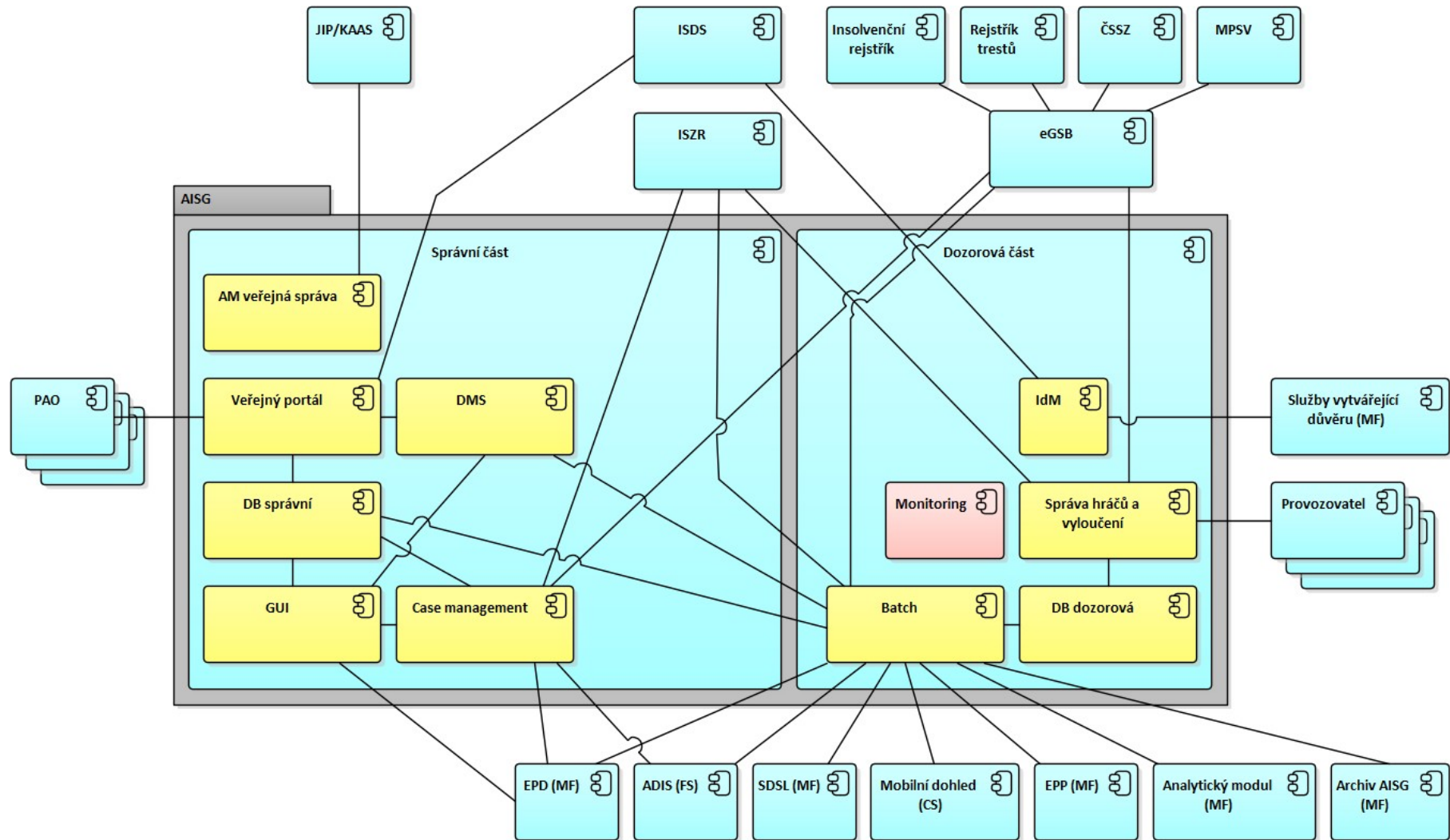
Komponenta řešení Dodavatele	Použité SW produkty, míra pokrytí funkčních požadavků out-of-box Části vyvinuté na zakázku, programovací jazyk a typ aplikačních serverů
	<p>Předpokládá se plné pokrytí pro účely napojení do monitoringu SPCSS podle požadavků MF a SPCSS.</p> <p><b>Části vyvinuté na zakázku, programovací jazyk:</b> Budou-li z konkrétních požadavků na logování a monitoring nutné úpravy na zakázku, budou vyvinuty jako plugin v jazyce Java. Použití SW uvedených produktů Dodavatel předpokládá tak, jak jsou, tedy bez úprav jejich zdrojového kódu. Produkty jsou nosnou platformou pro řešení vyvinuté na zakázku.</p>
Case Management	<p><b>Použitý SW:</b> Aplikační server WildFly (Red Hat) – Java EE server</p> <p><b>Míra pokrytí funkčních požadavků out-of-the-box:</b> Žádné pokrytí, vývoj na zakázku.</p> <p><b>Části vyvinuté na zakázku, programovací jazyk:</b> Všechny funkční požadavky budou realizovány v jazyce Java. Použití SW uvedených produktů Dodavatel předpokládá tak, jak jsou, tedy bez úprav jejich zdrojového kódu. Produkty jsou nosnou platformou pro řešení vyvinuté na zakázku.</p>
DMS	<p><b>Použitý SW:</b> DMS Alfresco Community Edition, Webový kontejner Apache Tomcat, Databáze Postgres (PostgreSQL)</p> <p><b>Míra pokrytí funkčních požadavků out-of-the-box:</b> Částečná – out-of-box je pokryt požadavek na ukládání/zobrazování dokumentů (rozhraní pro práci s dokumenty), administraci (administrační rozhraní) a konfigurovatelnost přístupových práv.</p> <p><b>Části vyvinuté na zakázku, programovací jazyk:</b> Přizpůsobení standardu NSESSS znamená vývoj na zakázku v programovacím jazyce Java. Použití SW uvedených produktů Dodavatel předpokládá tak, jak jsou, tedy bez úprav jejich zdrojového kódu.</p> <p>Požadavek na archivaci dokumentů je z pohledu operací s dokumenty v DMS plněn out-of-box skrze strojové aplikační rozhraní, samotnou archivaci provádí komponenta Batch. Produkty jsou nosnou platformou pro řešení vyvinuté na zakázku.</p>
GUI	<b>Použitý SW:</b>

Komponenta řešení Dodavatele	Použité SW produkty, míra pokrytí funkčních požadavků out-of-box Části vyvinuté na zakázku, programovací jazyk a typ aplikačních serverů
	<p>Aplikační server WildFly (Red Hat) – Java EE server</p> <p><b>Míra pokrytí funkčních požadavků out-of-the-box:</b> Žádné pokrytí, vývoj na zakázku.</p> <p><b>Části vyvinuté na zakázku, programovací jazyk:</b> Všechny funkční požadavky budou realizovány v jazyce Java a TypeScript. Použití SW uvedených produktů Dodavatel předpokládá tak, jak jsou, tedy bez úprav jejich zdrojového kódu. Produkty jsou nosnou platformou pro řešení vyvinuté na zakázku.</p>
Veřejný portál	<p><b>Použitý SW:</b> Aplikační server WildFly (Red Hat) – Java EE server</p> <p><b>Míra pokrytí funkčních požadavků out-of-the-box:</b> Žádné pokrytí, vývoj na zakázku.</p> <p><b>Části vyvinuté na zakázku, programovací jazyk:</b> Všechny funkční požadavky budou realizovány v jazyce Java a TypeScript. Použití SW uvedených produktů Dodavatel předpokládá tak, jak jsou, tedy bez úprav jejich zdrojového kódu. Produkty jsou nosnou platformou pro řešení vyvinuté na zakázku.</p>
AM veřejná správa	<p><b>Použitý SW:</b> Aplikační server WildFly (Red Hat) – Java EE server Keycloak – Identity and Access Management, na uvedeném aplikačním serveru WildFly</p> <p><b>Míra pokrytí funkčních požadavků out-of-the-box:</b> Částečné, SSO a standardní protokoly (OpenID, OAuth, SAML) jsou out-of-box.</p> <p><b>Části vyvinuté na zakázku, programovací jazyk:</b> Funkční požadavky specifické pro AISG, tedy napojení na JIP/KAAS a AD MF, budou realizovány v jazyce Java. Použití SW uvedených produktů Dodavatel předpokládá tak, jak jsou, tedy bez úprav jejich zdrojového kódu. Produkty jsou nosnou platformou pro řešení vyvinuté na zakázku.</p>
DB dozorová	<p><b>Použitý SW:</b> Databázový server Postgres (PostgreSQL) – relační SQL databáze</p>

Komponenta řešení Dodavatele	Použité SW produkty, míra pokrytí funkčních požadavků out-of-box Části vyvinuté na zakázku, programovací jazyk a typ aplikačních serverů
	<p>Load balancing a active-active HA řeší middleware PgPool-II (mezi DB serverem a DB klientem)</p> <p><b>Míra pokrytí funkčních požadavků out-of-the-box:</b> Žádné pokrytí, vývoj na zakázku.</p> <p><b>Části vyvinuté na zakázku, programovací jazyk:</b> Funkční požadavky budou realizovány v jazycích SQL a PL/pgSQL. Použití SW uvedených produktů Dodavatel předpokládá tak, jak jsou, tedy bez úprav jejich zdrojového kódu. Produkty jsou nosnou platformou pro řešení vyvinuté na zakázku.</p>
Správa hráčů a vyloučení	<p><b>Použitý SW:</b> Aplikační server WildFly (Red Hat) – Java EE server</p> <p><b>Míra pokrytí funkčních požadavků out-of-the-box:</b> Žádné pokrytí, vývoj na zakázku.</p> <p><b>Části vyvinuté na zakázku, programovací jazyk:</b> Všechny funkční požadavky budou realizovány v jazyce Java a TypeScript. Použití SW uvedených produktů Dodavatel předpokládá tak, jak jsou, tedy bez úprav jejich zdrojového kódu. Produkty jsou nosnou platformou pro řešení vyvinuté na zakázku.</p>
IdM	<p><b>Použitý SW:</b> Aplikační server WildFly (Red Hat) – Java EE server Keycloak – Identity and Access Management, na uvedeném aplikačním serveru WildFly</p> <p><b>Míra pokrytí funkčních požadavků out-of-the-box:</b> Částečné, SSO a standardní protokoly (OpenID, OAuth, SAML) jsou out-of-box.</p> <p><b>Části vyvinuté na zakázku, programovací jazyk:</b> Funkční požadavky specifické pro AISG, tedy napojení na ISDS a Služby vytvářející důvěru (MF), budou realizovány v jazyce Java. Použití SW uvedených produktů Dodavatel předpokládá tak, jak jsou, tedy bez úprav jejich zdrojového kódu. Produkty jsou nosnou platformou pro řešení vyvinuté na zakázku.</p>

## 1.2 Popis rozhraní a datových toků

### 1.2.1 Diagram rozhraní a datových toků



## 1.2.2 Popis implementace rozhraní a datových toků

Rozhraní dle kapitoly 2.3 Přílohy č. 1 Smlouvy		Implementované standardy aplikační nebo databázové komunikace Způsob autentizace a zabezpečení komunikací
Element A	Element B	
Provozovatel	DB hráčů	<p>Provozovatel komunikuje s komponentou <b>Správa hráčů a vyloučení</b>, která pracuje nad databází <b>DB dozorová</b> (jejíž součástí je DB hráčů), skrze SOAP 1.2 Webservice.</p> <p>Zprávy jsou předávány v XML zprávách elektronicky podepsaných dle standardu WS-security. Všechny používané certifikáty provozovatelů jsou registrovány v komponentě <b>IdM</b>.</p> <p>Komunikace Provozovatele probíhá šifrovaně přes HTTPS. Provozovatel se autentizuje svým certifikátem, registrovaným v IdM.</p> <p>Komponenta Správa hráčů a vyloučení se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>
Provozovatel	DB vyloučení	<p>Provozovatel komunikuje s komponentou <b>Správa hráčů a vyloučení</b>, která pracuje nad databází <b>DB dozorová</b> (jejíž součástí je DB vyloučení), skrze SOAP 1.2 Webservice.</p> <p>Zprávy jsou předávány v XML zprávách elektronicky podepsaných dle standardu WS-security. Všechny používané certifikáty provozovatelů jsou registrovány v komponentě <b>IdM</b>.</p> <p>Komunikace Provozovatele probíhá šifrovaně přes HTTPS. Provozovatel se autentizuje svým certifikátem, registrovaným v IdM.</p> <p>Komponenta Správa hráčů a vyloučení se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna</p>



Rozhraní dle kapitoly 2.3 Přílohy č. 1 Smlouvy		Implementované standardy aplikační nebo databázové komunikace Způsob autentizace a zabezpečení komunikací
Element A	Element B	
		šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.
PAO (Pověřená osoba)	DB Správní, DMS	<p>PAO komunikuje s komponentou <b>Veřejný portál</b>, která pracuje nad databází <b>DB správní</b>, skrze SOAP 1.2 WebService. Veřejný portál komunikuje s <b>DMS</b> skrze REST API (HTTP rozhraní) zabezpečené TLS na úrovni komunikačního protokolu.</p> <p>Zprávy jsou předávány v XML zprávách elektronicky podepsaných dle standardu WS-security. Všechny používané certifikáty PAO jsou registrovány v komponentě <b>IdM</b>.</p> <p>Komunikace PAO probíhá šifrovaně přes HTTPS. PAO se autentizuje svým certifikátem, registrovaným v <b>IdM</b>.</p> <p>Komponenta Veřejný portál se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>
DB hráčů	ISZR	<p>Komponenta <b>Správa hráčů a vyloučení</b> komunikuje se službami ISZR (v souladu s požadavky SZR). Komponenta pracuje nad databází <b>DB dozorová</b> (jejíž součástí je DB hráčů). Komponenta registruje komponentu <b>Batch</b> k aktualizacím údajů o subjektech.</p> <p>Komunikace s ISZR bude probíhat šifrovaně přes HTTPS jako SOAP 1.1 WebService s XML. Podle standardů SZR je zabezpečení webových služeb pomocí komunikační vrstvy (nepoužívá se WS-Security, XML-Signature a XML-Encryption, atd.)</p> <p>Komponenta Správa hráčů a vyloučení se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>
ISZR	DB hráčů	Komponenta <b>Batch</b> je registrována, aby přijímala aktualizace údajů o subjektech. Pracuje na databázi <b>DB dozorová</b> (jejíž součástí je DB hráčů).

Rozhraní dle kapitoly 2.3 Přílohy č. 1 Smlouvy		Implementované standardy aplikační nebo databázové komunikace Způsob autentizace a zabezpečení komunikací
Element A	Element B	
		<p>Komunikace s ISZR bude probíhat šifrovaně přes HTTPS jako SOAP 1.1 WebService s XML. Podle standardů SZR je zabezpečení webových služeb pomocí komunikační vrstvy (nepoužívá se WS-Security, XML-Signature a XML-Encryption, atd.)</p> <p>Komponenta Batch se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>
Case Management	ISZR	<p>Komponenta <b>Case Management</b> komunikuje se službami ISZR (v souladu s požadavky SZR). Komponenta pracuje nad databází <b>DB správní</b>. Komponenta registruje komponentu <b>Batch</b> k aktualizacím údajů o subjektech (PAO a provozovatelé).</p> <p>Komunikace s ISZR bude probíhat šifrovaně přes HTTPS jako SOAP 1.1 WebService s XML. Podle standardů SZR je zabezpečení webových služeb pomocí komunikační vrstvy (nepoužívá se WS-Security, XML-Signature a XML-Encryption, atd.)</p> <p>Komponenta Case management se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>
ISZR	DB správní	<p>Komponenta <b>Batch</b> je registrována, aby přijímala aktualizace údajů o subjektech. Pracuje na databázi <b>DB správní</b>.</p> <p>Komunikace s ISZR bude probíhat šifrovaně přes HTTPS jako SOAP 1.1 WebService s XML. Podle standardů SZR je zabezpečení webových služeb pomocí komunikační vrstvy (nepoužívá se WS-Security, XML-Signature a XML-Encryption, atd.)</p> <p>Komponenta Batch se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>

Rozhraní dle kapitoly 2.3 Přílohy č. 1 Smlouvy		Implementované standardy aplikační nebo databázové komunikace Způsob autentizace a zabezpečení komunikací
Element A	Element B	
ISZR	DB vyloučení	<p><b>Komponenta Batch</b> je registrována, aby přijímala aktualizace údajů o subjektech. Pracuje na databázi <b>DB dozorová</b> (jejíž součástí je DB vyloučení).</p> <p>Komunikace s ISZR bude probíhat šifrovaně přes HTTPS jako SOAP 1.1 Webservice s XML. Podle standardů SZR je zabezpečení webových služeb pomocí komunikační vrstvy (nepoužívá se WS-Security, XML-Signature a XML-Encryption, atd.)</p> <p>Komponenta Batch se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>
EPD	DB správní	<p>EPD předává informace o dokumentech určených pro AISG komponentě <b>GUI</b>, která pracuje nad databází <b>DB správní</b>.</p> <p>Komunikace s EPD bude probíhat, bude autentizována a zabezpečena dle standardů EPD a její návrh bude součástí Detailního návrhu Dodavatele.</p> <p>Komponenta GUI se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>
Case Management	EPD	<p>Komponenta <b>Case Management</b> pracuje pouze s odkazy na dokument v EPD (odkazy uložené v <b>DB správní</b>), který předloží uživateli k zobrazení v komponentě <b>GUI</b>. Zabezpečení a autentizace jsou řešeny v rámci standardů EPD s využitím SSO pracovníků MF.</p> <p>Komponenta Case management se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>

Rozhraní dle kapitoly 2.3 Přílohy č. 1 Smlouvy		Implementované standardy aplikační nebo databázové komunikace Způsob autentizace a zabezpečení komunikací
Element A	Element B	
Case Management	eGSB	<p>Komponenta <b>Case Management</b> komunikuje se službami eGSB (v souladu s požadavky eGSB). Komponenta pracuje nad databází <b>DB správní</b>.</p> <p>Komunikace s eGSB bude probíhat šifrovaně přes HTTPS jako SOAP 1.1 Webservice s XML. Podle standardů SZR je zabezpečení webových služeb pomocí komunikační vrstvy (nepoužívá se WS-Security, XML-Signature a XML-Encryption, atd.)</p> <p>Komponenta Case management se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>
Case Management	ADIS	<p>Komponenta <b>Case Management</b> komunikuje se službami ADIS. Komponenta pracuje nad databází <b>DB správní</b>. Pravidelné (dávkové) provolávání dotazů nad platnými záznamy zajišťuje komponenta <b>Batch</b> totožným způsobem.</p> <p>Komunikace s ADIS bude probíhat šifrovaně přes HTTPS jako SOAP 1.2 Webservice s XML. Zabezpečení webových služeb bude na úrovni komunikační vrstvy (nepoužívá se WS-Security, XML-Signature a XML-Encryption, atd.), autentizována bude obousměrnou SSL důvěrou (certifikáty).</p> <p>Komponenty Case management a Batch se k databázi autentizují svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>
JIP /KAAS	AM veřejná správa	<p>Komponenta <b>AM veřejná správa</b> komunikuje s JIP/KAAS podle standardu JIP/KAAS. Konkrétní návrh zabezpečení a autentizace komunikace bude součástí Detailního návrhu Dodavatele.</p> <p>Komponenta AM veřejná správa se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>

Rozhraní dle kapitoly 2.3 Přílohy č. 1 Smlouvy		Implementované standardy aplikační nebo databázové komunikace Způsob autentizace a zabezpečení komunikací
Element A	Element B	
DB vyloučení	eGSB	<p>Komponenta <b>Batch</b> komunikuje se službami eGSB (v souladu s požadavky eGSB). Komponenta pracuje nad databází <b>DB dozorová</b> (jejíž součástí je DB vyloučení).</p> <p>Komunikace s eGSB bude probíhat šifrovaně přes HTTPS jako SOAP 1.1 Webservice s XML. Podle standardů SZR je zabezpečení webových služeb pomocí komunikační vrstvy (nepoužívá se WS-Security, XML-Signature a XML-Encryption, atd.)</p> <p>Komponenta Batch se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>
EPP	DB správní	<p>Komponenta <b>Batch</b> je registrována, aby přijímala aktualizace údajů o subjektech. Pracuje na databázi <b>DB správní</b>.</p> <p>Komunikace s EPP bude probíhat šifrovaně přes HTTPS jako SOAP 1.2 Webservice s XML. Zabezpečení webových služeb bude na úrovni komunikační vrstvy (nepoužívá se WS-Security, XML-Signature a XML-Encryption, atd.), autentizována bude obousměrnou SSL důvěrou (certifikáty).</p> <p>Komponenta Batch se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>
Mobilní dohled	DB správní	<p>Komponenta <b>Batch</b> je registrována, aby přijímala aktualizace údajů o subjektech. Pracuje na databázi <b>DB správní</b>.</p> <p>Komunikace s Mobilním dohledem bude probíhat šifrovaně přes HTTPS jako SOAP 1.2 Webservice s XML. Zabezpečení webových služeb bude na úrovni komunikační vrstvy (nepoužívá se WS-Security, XML-Signature a XML-Encryption, atd.), autentizována bude obousměrnou SSL důvěrou (certifikáty).</p> <p>Komponenta Batch se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním</p>

Rozhraní dle kapitoly 2.3 Přílohy č. 1 Smlouvy		Implementované standardy aplikační nebo databázové komunikace Způsob autentizace a zabezpečení komunikací
Element A	Element B	
		na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.
SDSL (MF)	DB správní	<p>Komunikaci pro účely migrace dat mezi SDSL a <b>DB správní</b> bude zajišťovat komponenta <b>Batch</b>, která nad touto databází běží.</p> <p>V databázi SDSL bude ve spolupráci s Objednatelům zřízen migrační účet s minimálními právy pro Batch. Autentizace a zabezpečení komunikace bude taková, jakou databáze systému SDSL dovoluje. Její návrh bude součástí Detailního návrhu Dodavatele.</p> <p>Komponenta Batch se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>
DB správní	ADIS	<p>Komponenta <b>Batch</b> komunikuje se službami ADIS. Komponenta pracuje nad databází <b>DB správní</b>.</p> <p>Komunikace s ADIS bude probíhat šifrovaně přes HTTPS jako SOAP 1.2 Webservice s XML. Zabezpečení webových služeb bude na úrovni komunikační vrstvy (nepoužívá se WS-Security, XML-Signature a XML-Encryption, atd.), autentizována bude obousměrnou SSL důvěrou (certifikáty).</p> <p>Komponenta Batch se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>
DMS	EPD	Přesun dokumentů do EPD zprostředkovává komponenta <b>Batch</b> , která komunikuje také s komponentou <b>DMS</b> . Komponenty <b>Case Management</b> a <b>GUI</b> pracují pouze s odkazy na dokument v EPD (odkazy uložené v <b>DB správní</b> ), které předloží uživateli k zobrazení. Zabezpečení a autentizace jsou řešeny v rámci standardů EPD s využitím SSO pracovníků MF.

Rozhraní dle kapitoly 2.3 Přílohy č. 1 Smlouvy		Implementované standardy aplikační nebo databázové komunikace Způsob autentizace a zabezpečení komunikací
Element A	Element B	
		<p>Komunikace s EPD bude probíhat, bude autentizována a zabezpečena dle standardů EPD a její návrh bude součástí Detailního návrhu Dodavatele.</p> <p>Komponenty GUI, Case management a Batch se k databázi autentizují svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p> <p>Rozhraní mezi DMS a EPD bude v souladu s požadavky na rozhraní mezi ISSD (informační systém spravující dokumenty) a eSSL (elektronický systém spisové služby) dané Národním standardem pro elektronické systémy spisové služby (<a href="http://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx">http://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx</a>) s tím, že rozhraní bude implementovat události (operace) odpovídající charakteru a funkcionalitě komponenty DMS podle požadavků v přílohách Smlouvy.</p>
IdM	ISDS	<p>Autentizace majitelů datových schránek (primárně provozovatelů a PAO) pomocí autentizační služby Portálu veřejné správy, která ověřuje uživatele pomocí přístupových údajů datových schránek, bude probíhat šifrovaně přes HTTPS jako SOAP 1.2 WebService s XML, dle provozního řádu a požadavku ISDS. Komunikace bude mezi <b>IdM</b> a ISDS, komponenta IdM zprostředkovává přihlášení do ostatních komponent (např. Veřejného portálu).</p> <p>AISG bude registrován jako informační systém veřejné správy oprávněný využívat služby Portálu veřejné správy.</p> <p>Komponenta IdM se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>
Veřejný portál	ISDS	<p>Komunikace <b>Veřejného portálu</b> s ISDS bude probíhat šifrovaně přes HTTPS jako SOAP 1.2 WebService s XML, dle provozního řádu a požadavku ISDS. Autentizaci bude zprostředkovávat komponenta <b>IdM</b>.</p> <p>Komponenty Veřejný portál a IdM se k databázi autentizují svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna</p>

Rozhraní dle kapitoly 2.3 Přílohy č. 1 Smlouvy		Implementované standardy aplikační nebo databázové komunikace Způsob autentizace a zabezpečení komunikací
Element A	Element B	
		šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.
IdM	Služby vytvářející důvěru	<p><b>Komponenta IdM</b> komunikuje se Službami vytvářejícími důvěru prostřednictvím standardních protokolů pro danou službu (stahování certifikátů a CRL pro HTTPS), případně WebServices. <b>Konkrétní návrh zabezpečení a autentizace komunikace bude součástí Detailního návrhu Dodavatele.</b></p> <p><b>Komponenta IdM</b> se k databázi autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>
DB správní DB hráčů DB vyloučení	Analytický modul	<p><b>Komponenta Batch</b> odesílá pravidelně data do analytického modulu z databáze <b>DB dozorová</b> (jejíž součástí je DB hráčů a DB vyloučení) a z databáze <b>DB správní</b>.</p> <p><b>Komunikace s Analytickým modulem bude probíhat, bude autentizována a zabezpečena dle požadavků Analytického modulu a její návrh bude součástí Detailního návrhu Dodavatele. Předávaná data budou ve formě umožňující zpracování standardními ETL a návrh bude součástí Detailního návrhu Dodavatele.</b></p> <p><b>Komponenta Batch</b> se k databázím autentizuje svým vyhrazeným databázovým účtem s minimálními nutnými právy. Dodavatel nepředpokládá šifrování vnitřní komunikace s databází a komponentami AISG, dle specifikace v kapitole 3.3.2 Přílohy č. 1 Smlouvy. V případě bezpečnostního požadavku SPCSS v rámci Detailního návrhu může být komunikace zajištěna šifrováním na úrovni síťového protokolu (např. HTTPS) s algoritmy v souladu platnými právními předpisy a normami, například Kybernetickým zákonem.</p>

### 1.3 Popis parametrizace systému a způsobu řešení změn





## ***1.4 Popis logování a monitoringu***



# 2 Implementace procesů

## 2.1 Popis implementace procesů

ID	Procesní oblast	Způsob implementace Příslušné komponenty a rozhraní architektury řešení Míra pokrytí funkčních požadavků out-of-box použitými SW produkty
2.	Metodická činnost	<p>Implementace procesů popsaných v kapitole 3.3.2.2 (tabulka 5) Přílohy č.2 Smlouvy.</p> <p><b>Použité komponenty:</b></p> <ul style="list-style-type: none"><li>- GUI</li><li>- Veřejný portál</li><li>- DMS</li><li>- DB správní</li><li>- AM veřejná správa</li></ul> <p><b>Použitá rozhraní:</b></p> <ul style="list-style-type: none"><li>- JIP/KAAS – AM veřejná správa</li></ul> <p><b>Míra pokrytí funkčních požadavků out-of-box použitými SW produkty:</b> Částečná – pro komponentu DMS, out-of-box je pokryt požadavek na ukládání/zobrazování dokumentů (rozhraní pro práci s dokumenty), administraci (administrační rozhraní) a konfigurovatelnost přístupových práv. Ostatní funkční požadavky implementovány vývojem na zakázku.</p>
3.	Vyřizování dotazů	<p>Implementace procesů popsaných v kapitole 3.3.2.3 (tabulka 6) Přílohy č.2 Smlouvy.</p> <p><b>Použité komponenty:</b></p> <ul style="list-style-type: none"><li>- GUI</li><li>- DB správní</li><li>- DMS</li></ul>

ID	Procesní oblast	Způsob implementace Příslušné komponenty a rozhraní architektury řešení Míra pokrytí funkčních požadavků out-of-box použitými SW produkty
		<p><b>Použitá rozhraní:</b></p> <ul style="list-style-type: none"> <li>- DMS - EPD</li> </ul> <p><b>Míra pokrytí funkčních požadavků out-of-box použitými SW produkty:</b> Částečná – pro komponentu DMS, out-of-box je pokryt požadavek na ukládání/zobrazování dokumentů (rozhraní pro práci s dokumenty), administraci (administrační rozhraní) a konfigurovatelnost přístupových práv. Ostatní funkční požadavky implementovány vývojem na zakázku.</p>
4.	Pověřené osoby	<p>Implementace procesů popsaných v kapitole 3.3.2.4 (tabulka 7) Přílohy č.2 Smlouvy.</p> <p><b>Použité komponenty:</b></p> <ul style="list-style-type: none"> <li>- Veřejný portál</li> <li>- DMS</li> <li>- DB správní</li> <li>- GUI</li> <li>- Case Management</li> <li>- AM veřejná správa</li> <li>- IdM</li> </ul> <p><b>Použitá rozhraní:</b></p> <ul style="list-style-type: none"> <li>- PAO (Pověřená osoba) – DB správní, DMS</li> <li>- JIP/KAAS – AM veřejná správa</li> <li>- IdM – Služby vytvářející důvěru</li> </ul> <p><b>Míra pokrytí funkčních požadavků out-of-box použitými SW produkty:</b> Částečná – pro komponentu DMS, out-of-box je pokryt požadavek na ukládání/zobrazování dokumentů (rozhraní pro práci s dokumenty), administraci (administrační rozhraní) a konfigurovatelnost přístupových práv. Ostatní funkční požadavky implementovány vývojem na zakázku.</p>
5.	Řešení stížností	<p>Implementace procesů popsaných v kapitole 3.3.2.5 (tabulka 8) Přílohy č.2 Smlouvy.</p> <p><b>Použité komponenty:</b></p> <ul style="list-style-type: none"> <li>- Veřejný portál</li> <li>- GUI</li> <li>- Case Management</li> <li>- DMS</li> <li>- DB Správní</li> </ul>

ID	Procesní oblast	Způsob implementace Příslušné komponenty a rozhraní architektury řešení Míra pokrytí funkčních požadavků out-of-box použitými SW produkty
		<ul style="list-style-type: none"> <li>- AM veřejná správa</li> </ul> <p><b>Použitá rozhraní:</b></p> <ul style="list-style-type: none"> <li>- JIP/KAAS – AM veřejná správa</li> <li>- Veřejný portál - ISDS</li> </ul> <p><b>Míra pokrytí funkčních požadavků out-of-box použitými SW produkty:</b> Částečná – pro komponentu DMS, out-of-box je pokryt požadavek na ukládání/zobrazování dokumentů (rozhraní pro práci s dokumenty), administraci (administrační rozhraní) a konfigurovatelnost přístupových práv. Ostatní funkční požadavky implementovány vývojem na zakázku.</p>
6.	Spolupráce v daňové oblasti	<p>Implementace procesů popsanych v kapitole 3.3.2.6 (tabulka 9) Přílohy č.2 Smlouvy.</p> <p><b>Použité komponenty:</b></p> <ul style="list-style-type: none"> <li>- GUI</li> <li>- Case Management</li> <li>- DB správní</li> <li>- DMS</li> </ul> <p><b>Použitá rozhraní:</b></p> <ul style="list-style-type: none"> <li>- Case Management - ADIS</li> <li>- DB správní - ADIS</li> <li>- DMS - EPD</li> </ul> <p><b>Míra pokrytí funkčních požadavků out-of-box použitými SW produkty:</b> Částečná – pro komponentu DMS, out-of-box je pokryt požadavek na ukládání/zobrazování dokumentů (rozhraní pro práci s dokumenty), administraci (administrační rozhraní) a konfigurovatelnost přístupových práv. Ostatní funkční požadavky implementovány vývojem na zakázku.</p>
7.	Správa registrů	<p>Implementace procesů popsanych v kapitole 3.3.2.7 (tabulka 10) Přílohy č.2 Smlouvy.</p> <p><b>Použité komponenty:</b></p> <ul style="list-style-type: none"> <li>- Veřejný portál</li> <li>- GUI</li> <li>- DB správní</li> <li>- DMS</li> <li>- Case Management</li> <li>- AM veřejná správa</li> </ul>

ID	Procesní oblast	Způsob implementace Příslušné komponenty a rozhraní architektury řešení Míra pokrytí funkčních požadavků out-of-box použitými SW produkty
		<ul style="list-style-type: none"> <li>- IdM</li> </ul> <p><b>Použitá rozhraní:</b></p> <ul style="list-style-type: none"> <li>- Veřejný portál – ISDS</li> <li>- IdM - ISDS</li> <li>- JIP/KAAS – AM veřejná správa</li> <li>- IdM – Služby vytvářející důvěru</li> <li>- DMS - EPD</li> </ul> <p><b>Míra pokrytí funkčních požadavků out-of-box použitými SW produkty:</b> Částečná – pro komponentu DMS, out-of-box je pokryt požadavek na ukládání/zobrazování dokumentů (rozhraní pro práci s dokumenty), administraci (administrační rozhraní) a konfigurovatelnost přístupových práv. Ostatní funkční požadavky implementovány vývojem na zakázku.</p>
8.	Ohlášení hazardní hry	<p>Implementace procesů popsanych v kapitole 3.3.2.8 (tabulka 11) Přílohy č.2 Smlouvy.</p> <p><b>Použité komponenty:</b></p> <ul style="list-style-type: none"> <li>- Veřejný portál</li> <li>- DB správní</li> <li>- DMS</li> <li>- Case Management</li> <li>- GUI</li> <li>- IdM</li> </ul> <p><b>Použitá rozhraní:</b></p> <ul style="list-style-type: none"> <li>- Veřejný portál - ISDS</li> <li>- IdM – Služby vytvářející důvěru</li> </ul> <p><b>Míra pokrytí funkčních požadavků out-of-box použitými SW produkty:</b> Částečná – pro komponentu DMS, out-of-box je pokryt požadavek na ukládání/zobrazování dokumentů (rozhraní pro práci s dokumenty), administraci (administrační rozhraní) a konfigurovatelnost přístupových práv. Ostatní funkční požadavky implementovány vývojem na zakázku.</p>
9.	Kontrolní činnost	<p>Implementace procesů popsanych v kapitole 3.3.2.9 (tabulka 12) Přílohy č.2 Smlouvy.</p> <p><b>Použité komponenty:</b></p> <ul style="list-style-type: none"> <li>- GUI</li> </ul>

ID	Procesní oblast	Způsob implementace Příslušné komponenty a rozhraní architektury řešení Míra pokrytí funkčních požadavků out-of-box použitými SW produkty
		<ul style="list-style-type: none"> <li>- DB Správní</li> <li>- AM veřejná správa</li> <li>- DMS</li> <li>- Case Management</li> </ul> <p><b>Použitá rozhraní:</b></p> <ul style="list-style-type: none"> <li>- JIP/KAAS – AM veřejná správa</li> <li>- Mobilní dohled – DB Správní</li> <li>- EPP – DB Správní</li> <li>- EPD – DB Správní</li> <li>- DMS - EPD</li> <li>- Case Management – EPD</li> </ul> <p><b>Míra pokrytí funkčních požadavků out-of-box použitými SW produkty:</b> Částečná – pro komponentu DMS, out-of-box je pokryt požadavek na ukládání/zobrazování dokumentů (rozhraní pro práci s dokumenty), administraci (administrační rozhraní) a konfigurovatelnost přístupových práv. Ostatní funkční požadavky implementovány vývojem na zakázku.</p>
10.	Základní povolení	<p>Implementace procesů popsaných v kapitole 3.3.2.10 (tabulka 13) Přílohy č.2 Smlouvy.</p> <p><b>Použité komponenty:</b></p> <ul style="list-style-type: none"> <li>- Veřejný portál</li> <li>- DMS</li> <li>- DB Správní</li> <li>- Case Management</li> <li>- GUI</li> <li>- AM veřejná správa</li> <li>- IdM</li> </ul> <p><b>Použitá rozhraní:</b></p> <ul style="list-style-type: none"> <li>- Case Management - eGSB</li> <li>- ISZR – DB správní</li> <li>- Case Management - ISZR</li> <li>- JIP/KAAS – AM veřejná správa</li> <li>- IdM – Služby vytvářející důvěru</li> <li>- Case Management - ADIS</li> </ul>



ID	Procesní oblast	Způsob implementace Příslušné komponenty a rozhraní architektury řešení Míra pokrytí funkčních požadavků out-of-box použitými SW produkty
		<p><b>Míra pokrytí funkčních požadavků out-of-box použitými SW produkty:</b> Částečná – pro komponentu DMS, out-of-box je pokryt požadavek na ukládání/zobrazování dokumentů (rozhraní pro práci s dokumenty), administraci (administrační rozhraní) a konfigurovatelnost přístupových práv. Ostatní funkční požadavky implementovány vývojem na zakázku.</p>
11.	Povolení k umístění herního prostoru	<p>Implementace procesů popsanych v kapitole 3.3.2.11 (tabulka 14) Přílohy č.2 Smlouvy.</p> <p><b>Použité komponenty:</b></p> <ul style="list-style-type: none"> <li>- Veřejný portál</li> <li>- DB Správní</li> <li>- DMS</li> <li>- Case Management</li> <li>- GUI</li> <li>- IdM</li> </ul> <p><b>Použitá rozhraní:</b></p> <ul style="list-style-type: none"> <li>- IdM – ISDS</li> <li>- Veřejný portál – ISDS</li> </ul> <p><b>Míra pokrytí funkčních požadavků out-of-box použitými SW produkty:</b> Částečná – pro komponentu DMS, out-of-box je pokryt požadavek na ukládání/zobrazování dokumentů (rozhraní pro práci s dokumenty), administraci (administrační rozhraní) a konfigurovatelnost přístupových práv. Ostatní funkční požadavky implementovány vývojem na zakázku.</p>
12.	Vedení rejstříku fyzických osob vyloučených z účasti na hazardních hrách	<p>Implementace procesů popsanych v kapitole 3.3.2.12 (tabulka 15) Přílohy č.2 Smlouvy.</p> <p><b>Použité komponenty:</b></p> <ul style="list-style-type: none"> <li>- Správa hráčů a vyloučení</li> <li>- DB dozorová (DB vyloučení, DB hráčů)</li> <li>- Case Management</li> </ul> <p><b>Použitá rozhraní:</b></p> <ul style="list-style-type: none"> <li>- DB vyloučení (DB dozorová) – eGSB</li> <li>- Case Management - eGSB</li> <li>- ISZR - DB vyloučení (DB dozorová)</li> <li>- ISZR - DB hráčů (DB dozorová)</li> </ul>

ID	Procesní oblast	Způsob implementace Příslušné komponenty a rozhraní architektury řešení Míra pokrytí funkčních požadavků out-of-box použitými SW produkty
		<p><b>Míra pokrytí funkčních požadavků out-of-box použitými SW produkty:</b> Žádné pokrytí. Funkční požadavky implementovány vývojem na zakázku.</p>
13.	Registrace	<p>Implementace procesů popsaných v kapitole 3.3.2.13 (tabulka 16) Přílohy č.2 Smlouvy.</p> <p><b>Použité komponenty:</b></p> <ul style="list-style-type: none"> <li>- DB dozorová</li> <li>- Veřejný portál</li> <li>- DMS</li> <li>- DB správní</li> <li>- Case Management</li> <li>- GUI</li> <li>- IdM</li> </ul> <p><b>Použitá rozhraní:</b></p> <ul style="list-style-type: none"> <li>- Case management – ISZR</li> <li>- Provozovatel – DB hráčů</li> <li>- Provozovatel – DB vyloučení</li> <li>- IdM – Služby vytvářející důvěru</li> </ul> <p><b>Míra pokrytí funkčních požadavků out-of-box použitými SW produkty:</b> Částečná – pro komponentu DMS, out-of-box je pokryt požadavek na ukládání/zobrazování dokumentů (rozhraní pro práci s dokumenty), administraci (administrační rozhraní) a konfigurovatelnost přístupových práv. Ostatní funkční požadavky implementovány vývojem na zakázku.</p>

ID	Procesní oblast	Způsob implementace Příslušné komponenty a rozhraní architektury řešení Míra pokrytí funkčních požadavků out-of-box použitými SW produkty
14.	Řízení o přestupcích	<p>Implementace procesů popsaných v kapitole 3.3.2.14 (tabulka 17) Přílohy č.2 Smlouvy.</p> <p><b>Použité komponenty:</b></p> <ul style="list-style-type: none"> <li>- GUI</li> <li>- DB Správní</li> <li>- DMS</li> <li>- Case Management</li> </ul> <p><b>Použitá rozhraní:</b></p> <ul style="list-style-type: none"> <li>- Mobilní dohled – DB Správní</li> <li>- EPP – DB Správní</li> <li>- DMS – EPD</li> <li>- Case Management - EPD</li> <li>- DB správní - ADIS</li> </ul> <p><b>Míra pokrytí funkčních požadavků out-of-box použitými SW produkty:</b> Částečná – pro komponentu DMS, out-of-box je pokryt požadavek na ukládání/zobrazování dokumentů (rozhraní pro práci s dokumenty), administraci (administrační rozhraní) a konfigurovatelnost přístupových práv.</p> <p>Ostatní funkční požadavky implementovány vývojem na zakázku.</p>
16.	Archivace	<p>Implementace procesů popsaných v kapitole 3.3.2.16 (tabulka 19) Přílohy č.2 Smlouvy.</p> <p><b>Použité komponenty:</b></p> <ul style="list-style-type: none"> <li>- DMS</li> <li>- Case Management</li> <li>- DB hráčů</li> <li>- DB vyloučení</li> <li>- DB správní</li> </ul> <p><b>Použitá rozhraní:</b></p> <ul style="list-style-type: none"> <li>- DMS - EPD</li> <li>- Case Management – EPD</li> </ul> <p><b>Míra pokrytí funkčních požadavků out-of-box použitými SW produkty:</b> Částečná – pro komponentu DMS, out-of-box je pokryt požadavek na ukládání/zobrazování dokumentů (rozhraní pro práci s dokumenty), administraci (administrační rozhraní) a konfigurovatelnost přístupových práv.</p> <p>Ostatní funkční požadavky implementovány vývojem na zakázku.</p>

# ***3 Návrh Technické infrastruktury systému***



# ***4 Seznam licencí, maintenancí a subskripcí SW produktů***

## ***4.1 Produkční prostředí***

### ***4.1.1 Etapa 1B***

## ***4.2 Jednotkové ceny***

# ***5 Řešení bezpečnosti***

## ***5.1 Popis řešení bezpečnosti***

## ***5.2 Popis bezpečnostních prvků a mechanismů***

# 6 Rámcový harmonogram realizace

## 6.1 Rámcový harmonogram realizace

Příložený harmonogram předpokládá zahájení projektu (které následuje po podpisu smlouvy a jejím zveřejněním v registru smluv) k 2.1.2019. Celý harmonogram bude časově posunut podle skutečného termínu zahájení projektu.

Č.	Název úkolu	Doba trvání	Zahájení	Dokončení	Předchůdci
1	<b>Zahájení projektu</b>	0 dny	02.01.2019	02.01.2019	
2	Kick off meeting	1 den	02.01.2019	02.01.2019	1
3	<b>Etapa 1A</b>	<b>87 dny</b>	<b>03.01.2019</b>	<b>03.05.2019</b>	
4	<b>Plánování projektu</b>	26 dny	03.01.2019	07.02.2019	
5	<b>Rámcový harmonogram projektu (D)</b>	26 dny	03.01.2019	07.02.2019	
6	Tvorba Rámcového harmonogramu	10 dny	03.01.2019	16.01.2019	2
7	Předání Rámcového harmonogramu ke schválení	1 den	17.01.2019	17.01.2019	6



8	Schválení Rámcového harmonogramu	15 dny	18.01.2019	07.02.2019	7
9	<b>Plán výstupů a akceptací (D)</b>	<b>26 dny</b>	03.01.2019	07.02.2019	
10	Tvorba Plánu výstupů a akceptací	10 dny	03.01.2019	16.01.2019	2
11	Předání Plánu výstupů a akceptací ke schválení	1 den	17.01.2019	17.01.2019	10
12	Schválení Plánu výstupů a akceptací	15 dny	18.01.2019	07.02.2019	11
13	<b>Revize požadavků</b>	<b>41 dny</b>	03.01.2019	28.02.2019	
14	<b>Revize požadavků (D)</b>	41 dny	03.01.2019	28.02.2019	
15	Tvorba dokumentu Revize požadavků	25 dny	03.01.2019	06.02.2019	2
16	Předání dokumentu Revize požadavků ke schválení	1 den	07.02.2019	07.02.2019	15
17	Schválení dokumentu Revize požadavků	15 dny	08.02.2019	28.02.2019	16
18	<b>Návrh řešení</b>	<b>46 dny</b>	01.03.2019	03.05.2019	
19	<b>Návrh architektury řešení (D)</b>	46 dny	01.03.2019	03.05.2019	
20	Tvorba dokumentu Návrh architektury řešení	30 dny	01.03.2019	11.04.2019	17
21	Předání dokumentu Návrh architektury řešení	1 den	12.04.2019	12.04.2019	20
22	Schválení dokumentu Návrh architektury řešení	15 dny	15.04.2019	03.05.2019	21
23	<b>Návrh datové migrace (D)</b>	36 dny	08.03.2019	26.04.2019	
24	Tvorba dokumentu Návrh datové migrace	20 dny	08.03.2019	04.04.2019	20SS+5 dny
25	Předání dokumentu Návrh datové migrace	1 den	05.04.2019	05.04.2019	24
26	Schválení dokumentu Návrh datové migrace	15 dny	08.04.2019	26.04.2019	25
27	<b>Požadavky na vývojové a dokumentační prostředí (D)</b>	36 dny	08.03.2019	26.04.2019	
28	Tvorba dokumentu Požadavky na vývojové a dokumentační prostředí	20 dny	08.03.2019	04.04.2019	20SS+5 dny

29	Předání dokumentu Požadavky na vývojové a dokumentační prostředí	1 den	05.04.2019	05.04.2019	28
30	Schválení dokumentu Požadavky na vývojové a dokumentační prostředí	15 dny	08.04.2019	26.04.2019	29
31	<b>Bezpečnostní dokumentace – analýza a identifikace aktiv a rizik a bezpečnostní požadavky (D)</b>	36 dny	08.03.2019	26.04.2019	
32	Tvorba Bezpečnostní dokumentace	20 dny	08.03.2019	04.04.2019	20SS+5 dny
33	Předání Bezpečnostní dokumentace	1 den	05.04.2019	05.04.2019	32
34	Schválení Bezpečnostní dokumentace	15 dny	08.04.2019	26.04.2019	33
35	<b>Testovací strategie (D)</b>	36 dny	08.03.2019	26.04.2019	
36	Tvorba dokumentu Testovací strategie	20 dny	08.03.2019	04.04.2019	20SS+5 dny
37	Předání dokumentu Testovací strategie	1 den	05.04.2019	05.04.2019	36
38	Schválení dokumentu Testovací strategie	15 dny	08.04.2019	26.04.2019	37
39	<b>Etapa 1B</b>	<b>173 dny</b>	<b>06.05.2019</b>	<b>01.01.2020</b>	
40	<b>Detailní návrh řešení</b>	<b>34 dny</b>	<b>06.05.2019</b>	<b>20.06.2019</b>	
41	<b>Detailní návrh řešení (D)</b>	34 dny	06.05.2019	20.06.2019	
42	Tvorba dokumentu Detailní návrh řešení	18 dny	06.05.2019	29.05.2019	18
43	Předání dokumentu Detailní návrh řešení	1 den	30.05.2019	30.05.2019	42
44	Schválení dokumentu Detailní návrh řešení	15 dny	31.05.2019	20.06.2019	43
45	<b>Specifikace rozhraní pro pověřené osoby (D)</b>	29 dny	13.05.2019	20.06.2019	
46	Tvorba dokumentu Specifikace rozhraní pro pověřené osoby	13 dny	13.05.2019	29.05.2019	42SS+5 dny
47	Předání dokumentu Specifikace rozhraní pro pověřené osoby	1 den	30.05.2019	30.05.2019	46
48	Schválení dokumentu Specifikace rozhraní pro pověřené osoby	15 dny	31.05.2019	20.06.2019	47

49	<b>Návrh testů (D)</b>	29 dny	13.05.2019	20.06.2019	
50	Tvorba dokumentu Návrh testů	13 dny	13.05.2019	29.05.2019	42SS+5 dny
51	Předání dokumentu Návrh testů	1 den	30.05.2019	30.05.2019	50
52	Schválení dokumentu Návrh testů	15 dny	31.05.2019	20.06.2019	51
53	<b>Bezpečnostní dokumentace – návrhová část (D)</b>	29 dny	13.05.2019	20.06.2019	
54	Tvorba Bezpečnostní dokumentace - návrhová část	13 dny	13.05.2019	29.05.2019	42SS+5 dny
55	Předání Bezpečnostní dokumentace - návrhová část	1 den	30.05.2019	30.05.2019	54
56	Schválení Bezpečnostní dokumentace - návrhová část	15 dny	31.05.2019	20.06.2019	55
57	<b>Implementace systému</b>	91 dny	06.05.2019	09.09.2019	
58	Dodávka HW (SPCSS - 6 týdnů)	30 dny	06.05.2019	14.06.2019	22
59	Instalace HW (SPCSS - 4 týdny)	20 dny	17.06.2019	12.07.2019	58
60	Vývoj a konfigurace řešení	50 dny	21.06.2019	29.08.2019	40
61	<b>Zpráva o dokončení vývoje a provedení unit testů (Z)</b>	7 dny	30.08.2019	09.09.2019	
62	Tvorba dokumentu Zpráva o dokončení vývoje a provedení unit testů	1 den	30.08.2019	30.08.2019	60FF+1 den
63	Předání dokumentu Zpráva o dokončení vývoje a provedení unit testů	1 den	02.09.2019	02.09.2019	62
64	Schválení dokumentu Zpráva o dokončení vývoje a provedení unit testů	5 dny	03.09.2019	09.09.2019	63
65	<b>Testování systému</b>	65 dny	30.08.2019	28.11.2019	
66	Příprava testovacích dat pro funkční a integrační testy	12 dny	30.08.2019	16.09.2019	67SS-7 dny
67	Funkční testy (2 týdny testů + opravy a retesty)	12 dny	10.09.2019	25.09.2019	57
68	Integrační testy (2 týdny testů + opravy a retesty)	12 dny	26.09.2019	11.10.2019	67;66
69	<b>Zpráva o provedení funkčních a integračních testů (T)</b>	7 dny	14.10.2019	22.10.2019	
70	Tvorba dokumentu Zpráva o provedení funkčních a integračních testů	1 den	14.10.2019	14.10.2019	68FF+1 den

71	Předání dokumentu Zpráva o provedení funkčních a integračních testů	1 den	15.10.2019	15.10.2019	70
72	Schválení dokumentu Zpráva o provedení funkčních a integračních testů	5 dny	16.10.2019	22.10.2019	71
73	Příprava testovacích dat pro zátěžové testy, testy vysoké dostupnosti a bezpečnostní testy	15 dny	14.10.2019	01.11.2019	74SS-7 dny
74	Zátěžové testy	15 dny	23.10.2019	12.11.2019	72
75	<b>Zpráva o provedení výkonnostních testů (T)</b>	8 dny	12.11.2019	21.11.2019	
76	Tvorba dokumentu Zpráva o provedení výkonnostních testů	2 dny	12.11.2019	13.11.2019	74FF+1 den
77	Předání dokumentu Zpráva o provedení výkonnostních testů	1 den	14.11.2019	14.11.2019	76
78	Schválení dokumentu Zpráva o provedení výkonnostních testů	5 dny	15.11.2019	21.11.2019	77
79	Testy vysoké dostupnosti (SPCSS - 3 dny)	15 dny	23.10.2019	12.11.2019	72
80	<b>Zpráva o řešení vad z testů vysoké dostupnosti (T)</b>	8 dny	12.11.2019	21.11.2019	
81	Tvorba dokumentu Zpráva o řešení vad z testů vysoké dostupnosti	2 dny	12.11.2019	13.11.2019	79FF+1 den
82	Předání dokumentu Zpráva o řešení vad z testů vysoké dostupnosti	1 den	14.11.2019	14.11.2019	81
83	Schválení dokumentu Zpráva o řešení vad z testů vysoké dostupnosti	5 dny	15.11.2019	21.11.2019	82
84	Nezávislé bezpečnostní testy (Objednatel - 2 týdny testů + opravy a retesty)	20 dny	23.10.2019	19.11.2019	72
85	<b>Zpráva o řešení vad z nezávislých bezpečnostních testů (T)</b>	7 dny	20.11.2019	28.11.2019	
86	Tvorba dokumentu Zpráva o řešení vad z nezávislých bezpečnostních testů	1 den	20.11.2019	20.11.2019	84FF+1 den
87	Předání dokumentu Zpráva o řešení vad z nezávislých bezpečnostních testů	1 den	21.11.2019	21.11.2019	86
88	Schválení dokumentu Zpráva o řešení vad z nezávislých bezpečnostních testů	5 dny	22.11.2019	28.11.2019	87

89	<b>Datová migrace</b>	58 dny	30.08.2019	19.11.2019	
90	Migrace dat	30 dny	30.08.2019	10.10.2019	60
91	<b>Zpráva o dokončení datové migrace a ověření dat Dodavatelem (Z)</b>	11 dny	04.10.2019	18.10.2019	
92	Tvorba dokumentu Zpráva o dokončení datové migrace a ověření dat Dodavatelem	5 dny	04.10.2019	10.10.2019	90FF
93	Předání dokumentu Zpráva o dokončení datové migrace a ověření dat Dodavatelem	1 den	11.10.2019	11.10.2019	92
94	Schválení dokumentu Zpráva o dokončení datové migrace a ověření dat Dodavatelem	5 dny	14.10.2019	18.10.2019	93
95	Testování datové migrace (1 týden testů výsledků datové migrace + opravy a retesty)	15 dny	21.10.2019	08.11.2019	94
96	<b>Zpráva o provedení testů datové migrace (T)</b>	11 dny	05.11.2019	19.11.2019	
97	Tvorba dokumentu Zpráva o provedení testů datové migrace	5 dny	05.11.2019	11.11.2019	95FF+1 den
98	Předání dokumentu Zpráva o provedení testů datové migrace	1 den	12.11.2019	12.11.2019	97
99	Schválení dokumentu Zpráva o provedení testů datové migrace	5 dny	13.11.2019	19.11.2019	98
100	<b>Uvedení do provozu</b>	58 dny	14.10.2019	01.01.2020	
101	<b>Školící materiály (D)</b>	18 dny	14.10.2019	06.11.2019	
102	Tvorba Školících materiálů	2 dny	14.10.2019	15.10.2019	68
103	Předání Školících materiálů	1 den	16.10.2019	16.10.2019	102
104	Schválení Školících materiálů	15 dny	17.10.2019	06.11.2019	103
105	Školení uživatelů a administrátorů (viz kapitola 4.5 přílohy Smlouvy)	28 dny	07.11.2019	16.12.2019	104
106	<b>Zpráva o provedení školení (Z)</b>	7 dny	17.12.2019	25.12.2019	
107	Tvorba dokumentu Zpráva o provedení školení	1 den	17.12.2019	17.12.2019	105

108	Předání dokumentu Zpráva o provedení školení	1 den	18.12.2019	18.12.2019	107
109	Schválení dokumentu Zpráva o provedení školení	5 dny	19.12.2019	25.12.2019	108
110	<b>Bezpečnostní dokumentace – dokumentační a provozní část (D)</b>	<b>21 dny</b>	29.11.2019	27.12.2019	
111	Tvorba Bezpečnostní dokumentace - dokumentační a provozní část	5 dny	29.11.2019	05.12.2019	65
112	Předání Bezpečnostní dokumentace - dokumentační a provozní část	1 den	06.12.2019	06.12.2019	111
113	Schválení Bezpečnostní dokumentace - dokumentační a provozní část	15 dny	09.12.2019	27.12.2019	112
114	<b>Dokumentace systému (D)</b>	51 dny	14.10.2019	23.12.2019	
115	Tvorba Dokumentace systému	35 dny	14.10.2019	29.11.2019	68
116	Předání Dokumentace systému	1 den	02.12.2019	02.12.2019	115
117	Schválení Dokumentace systému	15 dny	03.12.2019	23.12.2019	116
118	Příprava a ověření Produkčního prostředí	3 dny	30.12.2019	01.01.2020	101;106;110;114
119	<b>Etapa 2</b>	<b>280 dny</b>	<b>06.05.2019</b>	<b>29.05.2020</b>	
120	<b>Detailní návrh řešení</b>	<b>82 dny</b>	<b>21.06.2019</b>	<b>14.10.2019</b>	
121	<b>Detailní návrh řešení (D)</b>	82 dny	21.06.2019	14.10.2019	
122	Tvorba dokumentu Detailní návrh řešení	66 dny	21.06.2019	20.09.2019	40
123	Předání dokumentu Detailní návrh řešení	1 den	23.09.2019	23.09.2019	122
124	Schválení dokumentu Detailní návrh řešení	15 dny	24.09.2019	14.10.2019	123
125	<b>Specifikace rozhraní pro provozovatele (D)</b>	31 dny	28.06.2019	09.08.2019	
126	Tvorba dokumentu Specifikace rozhraní pro provozovatele	15 dny	28.06.2019	18.07.2019	122SS+5 dny
127	Předání dokumentu Specifikace rozhraní pro provozovatele	1 den	19.07.2019	19.07.2019	126

128	Schválení dokumentu Specifikace rozhraní pro provozovatele	15 dny	22.07.2019	09.08.2019	127
129	<b>Návrh testů (D)</b>	31 dny	28.06.2019	09.08.2019	
130	Tvorba dokumentu Návrh testů	15 dny	28.06.2019	18.07.2019	122SS+5 dny
131	Předání dokumentu Návrh testů	1 den	19.07.2019	19.07.2019	130
132	Schválení dokumentu Návrh testů	15 dny	22.07.2019	09.08.2019	131
133	<b>Bezpečnostní dokumentace – návrhová část (D)</b>	31 dny	28.06.2019	09.08.2019	
134	Tvorba Bezpečnostní dokumentace - návrhová část	15 dny	28.06.2019	18.07.2019	122SS+5 dny
135	Předání Bezpečnostní dokumentace - návrhová část	1 den	19.07.2019	19.07.2019	134
136	Schválení Bezpečnostní dokumentace - návrhová část	15 dny	22.07.2019	09.08.2019	135
137	<b>Implementace systému</b>	208 dny	06.05.2019	19.02.2020	
138	Dodávka HW (SPCSS - 6 týdnů)	30 dny	06.05.2019	14.06.2019	22
139	Instalace HW (SPCSS - 4 týdny)	20 dny	17.06.2019	12.07.2019	138
140	Vývoj a konfigurace řešení	85 dny	15.10.2019	10.02.2020	120
141	<b>Zpráva o dokončení vývoje a provedení unit testů (Z)</b>	9 dny	07.02.2020	19.02.2020	
142	Tvorba dokumentu Zpráva o dokončení vývoje a provedení unit testů	3 dny	07.02.2020	11.02.2020	140FF+1 den
143	Předání dokumentu Zpráva o dokončení vývoje a provedení unit testů	1 den	12.02.2020	12.02.2020	142
144	Schválení dokumentu Zpráva o dokončení vývoje a provedení unit testů	5 dny	13.02.2020	19.02.2020	143
145	<b>Testování systému</b>	66 dny	31.01.2020	01.05.2020	
146	Příprava testovacích dat pro funkční a integrační testy	15 dny	31.01.2020	20.02.2020	147SS-7 dny
147	Funkční testy (2 týdny testů + opravy a retesty)	15 dny	11.02.2020	02.03.2020	140
148	Integrační testy (2 týdny testů + opravy a retesty)	15 dny	03.03.2020	23.03.2020	147
149	<b>Zpráva o provedení funkčních a integračních testů (T)</b>	7 dny	24.03.2020	01.04.2020	

150	Tvorba dokumentu Zpráva o provedení funkčních a integračních testů	1 den	24.03.2020	24.03.2020	148FF+1 den
151	Předání dokumentu Zpráva o provedení funkčních a integračních testů	1 den	25.03.2020	25.03.2020	150
152	Schválení dokumentu Zpráva o provedení funkčních a integračních testů	5 dny	26.03.2020	01.04.2020	151
153	Příprava testovacích dat pro zátěžové testy, testy vysoké dostupnosti a bezpečnostní testy	15 dny	24.03.2020	13.04.2020	154SS-7 dny
154	Zátěžové testy	15 dny	02.04.2020	22.04.2020	152
155	<b>Zpráva o provedení výkonnostních testů (T)</b>	8 dny	22.04.2020	01.05.2020	
156	Tvorba dokumentu Zpráva o provedení výkonnostních testů	2 dny	22.04.2020	23.04.2020	154FF+1 den
157	Předání dokumentu Zpráva o provedení výkonnostních testů	1 den	24.04.2020	24.04.2020	156
158	Schválení dokumentu Zpráva o provedení výkonnostních testů	5 dny	27.04.2020	01.05.2020	157
159	Testy vysoké dostupnosti (SPCSS - 3 dny)	15 dny	02.04.2020	22.04.2020	152
160	<b>Zpráva o řešení vad z testů vysoké dostupnosti (T)</b>	8 dny	22.04.2020	01.05.2020	
161	Tvorba dokumentu Zpráva o řešení vad z testů vysoké dostupnosti	2 dny	22.04.2020	23.04.2020	159FF+1 den
162	Předání dokumentu Zpráva o řešení vad z testů vysoké dostupnosti	1 den	24.04.2020	24.04.2020	161
163	Schválení dokumentu Zpráva o řešení vad z testů vysoké dostupnosti	5 dny	27.04.2020	01.05.2020	162
164	Nezávislé bezpečnostní testy (Objednatel - 2 týdny testů + opravy a retesty)	15 dny	02.04.2020	22.04.2020	152
165	<b>Zpráva o řešení vad z nezávislých bezpečnostních testů (T)</b>	8 dny	22.04.2020	01.05.2020	
166	Tvorba dokumentu Zpráva o řešení vad z nezávislých bezpečnostních testů	2 dny	22.04.2020	23.04.2020	164FF+1 den
167	Předání dokumentu Zpráva o řešení vad z nezávislých bezpečnostních testů	1 den	24.04.2020	24.04.2020	166



168	Schválení dokumentu Zpráva o řešení vad z nezávislých bezpečnostních testů	5 dny	27.04.2020	01.05.2020	167
169	<b>Uvedení do provozu</b>	42 dny	02.04.2020	29.05.2020	152
170	<b>Školící materiály (D)</b>	18 dny	02.04.2020	27.04.2020	
171	Tvorba Školících materiálů	2 dny	02.04.2020	03.04.2020	148
172	Předání Školících materiálů	1 den	06.04.2020	06.04.2020	171
173	Schválení Školících materiálů	15 dny	07.04.2020	27.04.2020	172
174	Školení uživatelů a administrátorů (viz kapitola 4.5 přílohy Smlouvy)	8 dny	28.04.2020	07.05.2020	173
175	<b>Zpráva o provedení školení (Z)</b>	7 dny	08.05.2020	18.05.2020	
176	Tvorba dokumentu Zpráva o provedení školení	1 den	08.05.2020	08.05.2020	174
177	Předání dokumentu Zpráva o provedení školení	1 den	11.05.2020	11.05.2020	176
178	Schválení dokumentu Zpráva o provedení školení	5 dny	12.05.2020	18.05.2020	177
179	<b>Bezpečnostní dokumentace – dokumentační a provozní část (D)</b>	21 dny	02.04.2020	30.04.2020	
180	Tvorba Bezpečnostní dokumentace - dokumentační a provozní část	5 dny	02.04.2020	08.04.2020	148
181	Předání Bezpečnostní dokumentace - dokumentační a provozní část	1 den	09.04.2020	09.04.2020	180
182	Schválení Bezpečnostní dokumentace - dokumentační a provozní část	15 dny	10.04.2020	30.04.2020	181
183	<b>Dokumentace systému (D)</b>	31 dny	02.04.2020	14.05.2020	
184	Tvorba Dokumentace systému	15 dny	02.04.2020	22.04.2020	148
185	Předání Dokumentace systému	1 den	23.04.2020	23.04.2020	184
186	Schválení Dokumentace systému	15 dny	24.04.2020	14.05.2020	185
187	Příprava a ověření Produkčního prostředí	2 dny	19.05.2020	20.05.2020	170;175;179;183
188	<b>Zpráva o přípravě a ověření Produkčního prostředí (Z)</b>	7 dny	21.05.2020	29.05.2020	

189	Tvorba dokumentu Zpráva o přípravě a ověření Produkčního prostředí	1 den	21.05.2020	21.05.2020	187
190	Předání dokumentu Zpráva o přípravě a ověření Produkčního prostředí	1 den	22.05.2020	22.05.2020	189
191	Schválení dokumentu Zpráva o přípravě a ověření Produkčního prostředí	5 dny	25.05.2020	29.05.2020	190
192	<b>Ukončení projektu</b>	1 den	01.06.2020	01.06.2020	191

## 6.2 Součinnosti

Č.	Název aktivity / výstupu	Zahájení	Dokončení	Předchůdci	Rozsah součinnosti Objednatele
1	<b>Zahájení projektu</b>	02.01.2019	02.01.2019		
2	Kick off meeting	02.01.2019	02.01.2019	1	Zajištění účasti pracovníků Objednatele a 3.stran na schůzce
3	<b>Etapa 1A</b>	03.01.2019	03.05.2019		
4	<b>Plánování projektu</b>	03.01.2019	07.02.2019		
5	<b>Rámcový harmonogram projektu (D)</b>	03.01.2019	07.02.2019		
6	Tvorba Rámcového harmonogramu	03.01.2019	16.01.2019	2	Předání výchozí verze Rámcového harmonogramu Dodavateli. Spolupráce s Dodavatelem na finalizaci dokumentace....
7	Předání Rámcového harmonogramu ke schválení	17.01.2019	17.01.2019	6	Předání finální verze Rámcového harmonogramu ke schválení ŘKO.
8	Schválení Rámcového harmonogramu	18.01.2019	07.02.2019	7	ŘKO - schválení Rámcového harmonogramu projektu.
9	<b>Plán výstupů a akceptací (D)</b>	03.01.2019	07.02.2019		

10	Tvorba Plánu výstupů a akceptací	03.01.2019	16.01.2019	2	Předání výchozí verze Plánu výstup a akceptací Dodavateli. <b>Spolupráce s dodavatelem na finalizaci dokumentace.</b>
11	Předání Plánu výstupů a akceptací ke schválení	17.01.2019	17.01.2019	10	Předání finální verze Plánu výstupů a akceptací ke schválení ŘKO.
12	Schválení Plánu výstupů a akceptací	18.01.2019	07.02.2019	11	ŘKO - schválení Plánu výstupů a akceptací.
13	<b>Revize požadavků</b>	03.01.2019	28.02.2019		
14	<b>Revize požadavků (D)</b>	03.01.2019	28.02.2019		
15	Tvorba dokumentu Revize požadavků	03.01.2019	06.02.2019	2	Poskytování konzultací pracovníky Objednatele. Zajištění konzultací 3. stran. Poskytování potřebné vstupní dokumentace a informací.
16	Předání dokumentu Revize požadavků ke schválení	07.02.2019	07.02.2019	15	Převzetí dokumentace ke schválení.
17	Schválení dokumentu Revize požadavků	08.02.2019	28.02.2019	16	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
18	<b>Návrh řešení</b>	01.03.2019	03.05.2019		
19	<b>Návrh architektury řešení (D)</b>	01.03.2019	03.05.2019		
20	Tvorba dokumentu Návrh architektury řešení	01.03.2019	11.04.2019	17	Poskytování konzultací pracovníky Objednatele. Zajištění konzultací 3. stran. Poskytování potřebné vstupní dokumentace a informací.
21	Předání dokumentu Návrh architektury řešení	12.04.2019	12.04.2019	20	Převzetí dokumentace ke schválení.
22	Schválení dokumentu Návrh architektury řešení	15.04.2019	03.05.2019	21	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
23	<b>Návrh datové migrace (D)</b>	08.03.2019	26.04.2019		
24	Tvorba dokumentu Návrh datové migrace	08.03.2019	04.04.2019	20SS+5 dny	Poskytování konzultací pracovníky Objednatele. Zajištění konzultací 3. stran. Poskytování potřebné vstupní dokumentace a informací.
25	Předání dokumentu Návrh datové migrace	05.04.2019	05.04.2019	24	Převzetí dokumentace ke schválení.
26	Schválení dokumentu Návrh datové migrace	08.04.2019	26.04.2019	25	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
27	<b>Požadavky na vývojové a dokumentační prostředí (D)</b>	08.03.2019	26.04.2019		
28	Tvorba dokumentu Požadavky na vývojové a dokumentační prostředí	08.03.2019	04.04.2019	20SS+5 dny	Poskytování konzultací pracovníky Objednatele. Zajištění konzultací 3. stran. Poskytování potřebné vstupní dokumentace a informací.

29	Předání dokumentu Požadavky na vývojové a dokumentační prostředí	05.04.2019	05.04.2019	28	Převzetí dokumentace ke schválení.
30	Schválení dokumentu Požadavky na vývojové a dokumentační prostředí	08.04.2019	26.04.2019	29	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
31	<b>Bezpečnostní dokumentace – analýza a identifikace aktiv a rizik a bezpečnostní požadavky (D)</b>	08.03.2019	26.04.2019		
32	Tvorba Bezpečnostní dokumentace	08.03.2019	04.04.2019	20SS+5 dny	Poskytování konzultací pracovníky Objednatele. Zajištění konzultací 3. stran. Poskytování potřebné vstupní dokumentace a informací.
33	Předání Bezpečnostní dokumentace	05.04.2019	05.04.2019	32	Převzetí dokumentace ke schválení.
34	Schválení Bezpečnostní dokumentace	08.04.2019	26.04.2019	33	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
35	<b>Testovací strategie (D)</b>	08.03.2019	26.04.2019		
36	Tvorba dokumentu Testovací strategie	08.03.2019	04.04.2019	20SS+5 dny	Poskytování konzultací pracovníky Objednatele. Zajištění konzultací 3. stran. Poskytování potřebné vstupní dokumentace a informací.
37	Předání dokumentu Testovací strategie	05.04.2019	05.04.2019	36	Převzetí dokumentace ke schválení.
38	Schválení dokumentu Testovací strategie	08.04.2019	26.04.2019	37	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
39	<b>Etapa 1B</b>	06.05.2019	01.01.2020		
40	<b>Detailní návrh řešení</b>	06.05.2019	20.06.2019		
41	<b>Detailní návrh řešení (D)</b>	06.05.2019	20.06.2019		
42	Tvorba dokumentu Detailní návrh řešení	06.05.2019	29.05.2019	18	Poskytování konzultací pracovníky Objednatele. Zajištění konzultací 3. stran. Poskytování potřebné vstupní dokumentace a informací.
43	Předání dokumentu Detailní návrh řešení	30.05.2019	30.05.2019	42	Převzetí dokumentace ke schválení.
44	Schválení dokumentu Detailní návrh řešení	31.05.2019	20.06.2019	43	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
45	<b>Specifikace rozhraní pro pověřené osoby (D)</b>	13.05.2019	20.06.2019		
46	Tvorba dokumentu Specifikace rozhraní pro pověřené osoby	13.05.2019	29.05.2019	42SS+5 dny	Poskytování konzultací pracovníky Objednatele. Zajištění konzultací 3. stran. Poskytování potřebné vstupní dokumentace a informací.

47	Předání dokumentu Specifikace rozhraní pro pověřené osoby	30.05.2019	30.05.2019	46	Převzetí dokumentace ke schválení.
48	Schválení dokumentu Specifikace rozhraní pro pověřené osoby	31.05.2019	20.06.2019	47	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
49	<b>Návrh testů (D)</b>	13.05.2019	20.06.2019		
50	Tvorba dokumentu Návrh testů	13.05.2019	29.05.2019	42SS+5 dny	Poskytování konzultací pracovníky Objednatele. Zajištění konzultací 3. stran. Poskytování potřebné vstupní dokumentace a informací.
51	Předání dokumentu Návrh testů	30.05.2019	30.05.2019	50	Převzetí dokumentace ke schválení.
52	Schválení dokumentu Návrh testů	31.05.2019	20.06.2019	51	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
53	<b>Bezpečnostní dokumentace – návrhová část (D)</b>	13.05.2019	20.06.2019		
54	Tvorba Bezpečnostní dokumentace - návrhová část	13.05.2019	29.05.2019	42SS+5 dny	Poskytování konzultací pracovníky Objednatele. Zajištění konzultací 3. stran. Poskytování potřebné vstupní dokumentace a informací.
55	Předání Bezpečnostní dokumentace - návrhová část	30.05.2019	30.05.2019	54	Převzetí dokumentace ke schválení.
56	Schválení Bezpečnostní dokumentace - návrhová část	31.05.2019	20.06.2019	55	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
57	<b>Implementace systému</b>	06.05.2019	09.09.2019		
58	Dodávka HW (SPCSS - 6 týdnů)	06.05.2019	14.06.2019	22	Zajištění dodávky potřebného HW.
59	Instalace HW (SPCSS - 4 týdny)	17.06.2019	12.07.2019	58	Zajištění instalace potřebného HW. Zajištění přístupů Dodavatele k předmětnému HW.
60	Vývoj a konfigurace řešení	21.06.2019	29.08.2019	40	Součinnost při konfiguraci řešení ve vztahu k navazujícím systémům a aplikacím. Zajištění součinnosti 3.stran.
61	<b>Zpráva o dokončení vývoje a provedení unit testů (Z)</b>	30.08.2019	09.09.2019		
62	Tvorba dokumentu Zpráva o dokončení vývoje a provedení unit testů	30.08.2019	30.08.2019	60FF+1 den	
63	Předání dokumentu Zpráva o dokončení vývoje a provedení unit testů	02.09.2019	02.09.2019	62	Převzetí zprávy ke schválení.
64	Schválení dokumentu Zpráva o dokončení vývoje a provedení unit testů	03.09.2019	09.09.2019	63	Zajištění připomínkování zprávy Objednatelem. Zajištění schválení zprávy Objednatelem.
65	<b>Testování systému</b>	30.08.2019	28.11.2019		
66	Příprava testovacích dat pro funkční a integrační testy	30.08.2019	16.09.2019	67SS-7 dny	Zajištění účasti pracovníků Objednatele a 3.stran při přípravě testovacích dat.

67	Funkční testy (2 týdny testů + opravy a retesty)	10.09.2019	25.09.2019	57	Zajištění účasti pracovníků Objednatele a 3.stran na testech....
68	Integrační testy (2 týdny testů + opravy a retesty)	26.09.2019	11.10.2019	67;66	Zajištění účasti pracovníků Objednatele a 3.stran na testech.
69	<b>Zpráva o provedení funkčních a integračních testů (T)</b>	14.10.2019	22.10.2019		
70	Tvorba dokumentu Zpráva o provedení funkčních a integračních testů	14.10.2019	14.10.2019	68FF+1 den	
71	Předání dokumentu Zpráva o provedení funkčních a integračních testů	15.10.2019	15.10.2019	70	Převzetí zprávy ke schválení.
72	Schválení dokumentu Zpráva o provedení funkčních a integračních testů	16.10.2019	22.10.2019	71	Zajištění připomínkování zprávy Objednatelem. Zajištění schválení zprávy Objednatelem.
73	Příprava testovacích dat pro zátěžové testy, testy vysoké dostupnosti a bezpečnostní testy	14.10.2019	01.11.2019	74SS-7 dny	Zajištění účasti pracovníků Objednatele a 3.strana součinnost na přípravě testovacích dat.
74	Zátěžové testy	23.10.2019	12.11.2019	72	Zajištění účasti pracovníků Objednatele a 3.stran na testech.
75	<b>Zpráva o provedení výkonnostních testů (T)</b>	12.11.2019	21.11.2019		
76	Tvorba dokumentu Zpráva o provedení výkonnostních testů	12.11.2019	13.11.2019	74FF+1 den	
77	Předání dokumentu Zpráva o provedení výkonnostních testů	14.11.2019	14.11.2019	76	Převzetí zprávy ke schválení.
78	Schválení dokumentu Zpráva o provedení výkonnostních testů	15.11.2019	21.11.2019	77	Zajištění připomínkování zprávy Objednatelem. Zajištění schválení zprávy Objednatelem.
79	Testy vysoké dostupnosti (SPCSS - 3 dny)	23.10.2019	12.11.2019	72	Zajištění účasti pracovníků Objednatele a 3.stran na testech. Součinnost při simulaci výpadků infrastruktury a zatížení systému.
80	<b>Zpráva o řešení vad z testů vysoké dostupnosti (T)</b>	12.11.2019	21.11.2019		
81	Tvorba dokumentu Zpráva o řešení vad z testů vysoké dostupnosti	12.11.2019	13.11.2019	79FF+1 den	
82	Předání dokumentu Zpráva o řešení vad z testů vysoké dostupnosti	14.11.2019	14.11.2019	81	Převzetí zprávy ke schválení.
83	Schválení dokumentu Zpráva o řešení vad z testů vysoké dostupnosti	15.11.2019	21.11.2019	82	Zajištění připomínkování zprávy Objednatelem. Zajištění schválení zprávy Objednatelem.

84	Nezávislé bezpečnostní testy (Objednatel - 2 týdny testů + opravy a retesty)	23.10.2019	19.11.2019	72	Zajištění realizace testů.
85	<b>Zpráva o řešení vad z nezávislých bezpečnostních testů (T)</b>	20.11.2019	28.11.2019		
86	Tvorba dokumentu Zpráva o řešení vad z nezávislých bezpečnostních testů	20.11.2019	20.11.2019	84FF+1 den	
87	Předání dokumentu Zpráva o řešení vad z nezávislých bezpečnostních testů	21.11.2019	21.11.2019	86	Převzetí zprávy ke schválení.
88	Schválení dokumentu Zpráva o řešení vad z nezávislých bezpečnostních testů	22.11.2019	28.11.2019	87	Zajištění připomínkování zprávy Objednatelem. Zajištění schválení zprávy Objednatelem.
89	<b>Datová migrace</b>	30.08.2019	19.11.2019		
90	Migrace dat	30.08.2019	10.10.2019	60	
91	<b>Zpráva o dokončení datové migrace a ověření dat Dodavatelem (Z)</b>	04.10.2019	18.10.2019		
92	Tvorba dokumentu Zpráva o dokončení datové migrace a ověření dat Dodavatelem	04.10.2019	10.10.2019	90FF	
93	Předání dokumentu Zpráva o dokončení datové migrace a ověření dat Dodavatelem	11.10.2019	11.10.2019	92	Převzetí zprávy ke schválení.
94	Schválení dokumentu Zpráva o dokončení datové migrace a ověření dat Dodavatelem	14.10.2019	18.10.2019	93	Zajištění připomínkování zprávy Objednatelem. Zajištění schválení zprávy Objednatelem.
95	Testování datové migrace (1 týden testů výsledků datové migrace + opravy a retesty)	21.10.2019	08.11.2019	94	Zajištění účasti pracovníků Objednatele a 3.stran na datových migracích. Součinnost při přípravě migrovaných dat, připomínkování výsledků migrace dat.
96	<b>Zpráva o provedení testů datové migrace (T)</b>	05.11.2019	19.11.2019		
97	Tvorba dokumentu Zpráva o provedení testů datové migrace	05.11.2019	11.11.2019	95FF+1 den	
98	Předání dokumentu Zpráva o provedení testů datové migrace	12.11.2019	12.11.2019	97	Převzetí zprávy ke schválení.
99	Schválení dokumentu Zpráva o provedení testů datové migrace	13.11.2019	19.11.2019	98	Zajištění připomínkování zprávy Objednatelem. Zajištění schválení zprávy Objednatelem.



100	<b>Uvedení do provozu</b>	14.10.2019	01.01.2020		
101	<b>Školicí materiály (D)</b>	14.10.2019	06.11.2019		
102	Tvorba Školicích materiálů	14.10.2019	15.10.2019	68	
103	Předání Školicích materiálů	16.10.2019	16.10.2019	102	Převzetí dokumentace ke schválení.
104	Schválení Školicích materiálů	17.10.2019	06.11.2019	103	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
105	Školení uživatelů a administrátorů (viz kapitola 4.5 přílohy Smlouvy)	07.11.2019	16.12.2019	104	Zajištění účastní školených pracovníků Objednatele a 3.stran na školeních. Zajištění školicích prostor včetně příslušného vybavení ke školení.
106	<b>Zpráva o provedení školení (Z)</b>	17.12.2019	25.12.2019		
107	Tvorba dokumentu Zpráva o provedení školení	17.12.2019	17.12.2019	105	
108	Předání dokumentu Zpráva o provedení školení	18.12.2019	18.12.2019	107	Převzetí zprávy ke schválení.
109	Schválení dokumentu Zpráva o provedení školení	19.12.2019	25.12.2019	108	Zajištění připomínkování zprávy Objednatelem. Zajištění schválení zprávy Objednatelem.
110	<b>Bezpečnostní dokumentace – dokumentační a provozní část (D)</b>	29.11.2019	27.12.2019		
111	Tvorba Bezpečnostní dokumentace - dokumentační a provozní část	29.11.2019	05.12.2019	65	
112	Předání Bezpečnostní dokumentace - dokumentační a provozní část	06.12.2019	06.12.2019	111	Převzetí dokumentace ke schválení.
113	Schválení Bezpečnostní dokumentace - dokumentační a provozní část	09.12.2019	27.12.2019	112	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
114	<b>Dokumentace systému (D)</b>	14.10.2019	23.12.2019		
115	Tvorba Dokumentace systému	14.10.2019	29.11.2019	68	
116	Předání Dokumentace systému	02.12.2019	02.12.2019	115	Převzetí dokumentace ke schválení.
117	Schválení Dokumentace systému	03.12.2019	23.12.2019	116	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
118	Příprava a ověření Produkčního prostředí	30.12.2019	01.01.2020	101;106;110;114	Součinnost při dokončení přípravy produkčního prostředí. Součinnost při ověření Produkčního prostředí. Zajištění součinnosti 3.stran. Součinnost Objednatele při předání řešení etapy 1A do produkčního provozu.
119	<b>Etapa 2</b>	06.05.2019	29.05.2020		

120	<b>Detailní návrh řešení</b>	21.06.2019	14.10.2019		
121	<b>Detailní návrh řešení (D)</b>	21.06.2019	14.10.2019		
122	Tvorba dokumentu Detailní návrh řešení	21.06.2019	20.09.2019	40	Poskytování konzultací pracovníky Objednatele. Zajištění konzultací 3. stran. Poskytování potřebné vstupní dokumentace a informací.
123	Předání dokumentu Detailní návrh řešení	23.09.2019	23.09.2019	122	Převzetí dokumentace ke schválení.
124	Schválení dokumentu Detailní návrh řešení	24.09.2019	14.10.2019	123	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
125	<b>Specifikace rozhraní pro provozovatele (D)</b>	28.06.2019	09.08.2019		
126	Tvorba dokumentu Specifikace rozhraní pro provozovatele	28.06.2019	18.07.2019	122SS+5 dny	Poskytování konzultací pracovníky Objednatele. Zajištění konzultací 3. stran. Poskytování potřebné vstupní dokumentace a informací.
127	Předání dokumentu Specifikace rozhraní pro provozovatele	19.07.2019	19.07.2019	126	Převzetí dokumentace ke schválení.
128	Schválení dokumentu Specifikace rozhraní pro provozovatele	22.07.2019	09.08.2019	127	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
129	<b>Návrh testů (D)</b>	28.06.2019	09.08.2019		
130	Tvorba dokumentu Návrh testů	28.06.2019	18.07.2019	122SS+5 dny	Poskytování konzultací pracovníky Objednatele. Zajištění konzultací 3. stran. Poskytování potřebné vstupní dokumentace a informací.
131	Předání dokumentu Návrh testů	19.07.2019	19.07.2019	130	Převzetí dokumentace ke schválení.
132	Schválení dokumentu Návrh testů	22.07.2019	09.08.2019	131	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
133	<b>Bezpečnostní dokumentace – návrhová část (D)</b>	28.06.2019	09.08.2019		
134	Tvorba Bezpečnostní dokumentace - návrhová část	28.06.2019	18.07.2019	122SS+5 dny	Poskytování konzultací pracovníky Objednatele. Zajištění konzultací 3. stran. Poskytování potřebné vstupní dokumentace a informací.
135	Předání Bezpečnostní dokumentace - návrhová část	19.07.2019	19.07.2019	134	Převzetí dokumentace ke schválení.
136	Schválení Bezpečnostní dokumentace - návrhová část	22.07.2019	09.08.2019	135	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
137	<b>Implementace systému</b>	06.05.2019	19.02.2020		
138	Dodávka HW (SPCSS - 6 týdnů)	06.05.2019	14.06.2019	22	Zajištění dodávky potřebného HW.
139	Instalace HW (SPCSS - 4 týdny)	17.06.2019	12.07.2019	138	Zajištění instalace potřebného HW. Zajištění přístupů Dodavatele k předmětnému HW.

140	Vývoj a konfigurace řešení	15.10.2019	10.02.2020	120	Součinnost při konfiguraci řešení ve vztahu k navazujícím systémům a aplikacím. Zajištění součinnosti 3.stran.
141	<b>Zpráva o dokončení vývoje a provedení unit testů (Z)</b>	07.02.2020	19.02.2020		
142	Tvorba dokumentu Zpráva o dokončení vývoje a provedení unit testů	07.02.2020	11.02.2020	140FF+1 den	
143	Předání dokumentu Zpráva o dokončení vývoje a provedení unit testů	12.02.2020	12.02.2020	142	Převzetí zprávy ke schválení.
144	Schválení dokumentu Zpráva o dokončení vývoje a provedení unit testů	13.02.2020	19.02.2020	143	Zajištění připomínkování zprávy Objednatelem. Zajištění schválení zprávy Objednatelem.
145	<b>Testování systému</b>	31.01.2020	01.05.2020		
146	Příprava testovacích dat pro funkční a integrační testy	31.01.2020	20.02.2020	147SS-7 dny	Zajištění účasti pracovníků Objednatele a 3.stran a součinnost při přípravě testovacích dat.
147	Funkční testy (2 týdny testů + opravy a retesty)	11.02.2020	02.03.2020	140	Zajištění účasti pracovníků Objednatele a 3.stran na testech.
148	Integrační testy (2 týdny testů + opravy a retesty)	03.03.2020	23.03.2020	147	Zajištění účasti pracovníků Objednatele a 3.stran na testech.
149	<b>Zpráva o provedení funkčních a integračních testů (T)</b>	24.03.2020	01.04.2020		
150	Tvorba dokumentu Zpráva o provedení funkčních a integračních testů	24.03.2020	24.03.2020	148FF+1 den	
151	Předání dokumentu Zpráva o provedení funkčních a integračních testů	25.03.2020	25.03.2020	150	Převzetí zprávy ke schválení.
152	Schválení dokumentu Zpráva o provedení funkčních a integračních testů	26.03.2020	01.04.2020	151	Zajištění připomínkování zprávy Objednatelem. Zajištění schválení zprávy Objednatelem.
153	Příprava testovacích dat pro zátěžové testy, testy vysoké dostupnosti a bezpečnostní testy	24.03.2020	13.04.2020	154SS-7 dny	Zajištění účasti pracovníků Objednatele a 3.stran a součinnost při přípravě testovacích dat.
154	Zátěžové testy	02.04.2020	22.04.2020	152	Zajištění účasti pracovníků Objednatele a 3.stran na testech. Součinnost při přípravě testovacích dat.
155	<b>Zpráva o provedení výkonnostních testů (T)</b>	22.04.2020	01.05.2020		
156	Tvorba dokumentu Zpráva o provedení výkonnostních testů	22.04.2020	23.04.2020	154FF+1 den	
157	Předání dokumentu Zpráva o provedení výkonnostních testů	24.04.2020	24.04.2020	156	Převzetí zprávy ke schválení.
158	Schválení dokumentu Zpráva o provedení výkonnostních testů	27.04.2020	01.05.2020	157	Zajištění připomínkování zprávy Objednatelem. Zajištění schválení zprávy Objednatelem.

159	Testy vysoké dostupnosti (SPCSS - 3 dny)	02.04.2020	22.04.2020	152	Zajištění účasti pracovníků Objednatele a 3.stran na testech. Součinnost při simulaci výpadků infrastruktury a zatížení systému.
160	<b>Zpráva o řešení vad z testů vysoké dostupnosti (T)</b>	22.04.2020	01.05.2020		
161	Tvorba dokumentu Zpráva o řešení vad z testů vysoké dostupnosti	22.04.2020	23.04.2020	159FF+1 den	
162	Předání dokumentu Zpráva o řešení vad z testů vysoké dostupnosti	24.04.2020	24.04.2020	161	Převzetí zprávy ke schválení.
163	Schválení dokumentu Zpráva o řešení vad z testů vysoké dostupnosti	27.04.2020	01.05.2020	162	Zajištění připomínkování zprávy Objednatelem. Zajištění schválení zprávy Objednatelem.
164	Nezávislé bezpečnostní testy (Objednatel - 2 týdny testů + opravy a retesty)	02.04.2020	22.04.2020	152	Zajištění realizace testů.
165	<b>Zpráva o řešení vad z nezávislých bezpečnostních testů (T)</b>	22.04.2020	01.05.2020		
166	Tvorba dokumentu Zpráva o řešení vad z nezávislých bezpečnostních testů	22.04.2020	23.04.2020	164FF+1 den	
167	Předání dokumentu Zpráva o řešení vad z nezávislých bezpečnostních testů	24.04.2020	24.04.2020	166	Převzetí zprávy ke schválení.
168	Schválení dokumentu Zpráva o řešení vad z nezávislých bezpečnostních testů	27.04.2020	01.05.2020	167	Zajištění účasti pracovníků Objednatele a 3.stran na testech. Součinnost při přípravě testovacích dat.
169	<b>Uvedení do provozu</b>	02.04.2020	29.05.2020	152	
170	<b>Školicí materiály (D)</b>	02.04.2020	27.04.2020		
171	Tvorba Školicích materiálů	02.04.2020	03.04.2020	148	
172	Předání Školicích materiálů	06.04.2020	06.04.2020	171	Převzetí dokumentace ke schválení.
173	Schválení Školicích materiálů	07.04.2020	27.04.2020	172	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
174	Školení uživatelů a administrátorů (viz kapitola 4.5 přílohy Smlouvy)	28.04.2020	07.05.2020	173	Zajištění účasti školených pracovníků Objednatele a 3.stran na školeních. Zajištění školicích prostor včetně příslušného vybavení ke školení.
175	<b>Zpráva o provedení školení (Z)</b>	08.05.2020	18.05.2020		
176	Tvorba dokumentu Zpráva o provedení školení	08.05.2020	08.05.2020	174	
177	Předání dokumentu Zpráva o provedení školení	11.05.2020	11.05.2020	176	Převzetí zprávy ke schválení.

178	Schválení dokumentu Zpráva o provedení školení	12.05.2020	18.05.2020	177	Zajištění připomínkování zprávy Objednatelem. Zajištění schválení zprávy Objednatelem.
179	<b>Bezpečnostní dokumentace – dokumentační a provozní část (D)</b>	02.04.2020	30.04.2020		
180	Tvorba Bezpečnostní dokumentace - dokumentační a provozní část	02.04.2020	08.04.2020	148	
181	Předání Bezpečnostní dokumentace - dokumentační a provozní část	09.04.2020	09.04.2020	180	Převzetí dokumentace ke schválení.
182	Schválení Bezpečnostní dokumentace - dokumentační a provozní část	10.04.2020	30.04.2020	181	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
183	<b>Dokumentace systému (D)</b>	02.04.2020	14.05.2020		
184	Tvorba Dokumentace systému	02.04.2020	22.04.2020	148	
185	Předání Dokumentace systému	23.04.2020	23.04.2020	184	Převzetí dokumentace ke schválení.
186	Schválení Dokumentace systému	24.04.2020	14.05.2020	185	Zajištění připomínkování dokumentace Objednatelem. Zajištění schválení dokumentace Objednatelem.
187	Příprava a ověření Produkčního prostředí	19.05.2020	20.05.2020	170;175;179;183	Součinnost při dokončení přípravy produkčního prostředí. Součinnost při ověření Produkčního prostředí. Zajištění součinnosti 3.stran.
188	<b>Zpráva o přípravě a ověření Produkčního prostředí (Z)</b>	21.05.2020	29.05.2020		
189	Tvorba dokumentu Zpráva o přípravě a ověření Produkčního prostředí	21.05.2020	21.05.2020	187	
190	Předání dokumentu Zpráva o přípravě a ověření Produkčního prostředí	22.05.2020	22.05.2020	189	Převzetí zprávy ke schválení.
191	Schválení dokumentu Zpráva o přípravě a ověření Produkčního prostředí	25.05.2020	29.05.2020	190	Zajištění připomínkování zprávy Objednatelem. Zajištění schválení zprávy Objednatelem.
192	<b>Ukončení projektu</b>	01.06.2020	01.06.2020	191	

# 7 Servisní služby

## 7.1 Popis Servisních služeb

Servisní služby zahrnují služby v oblasti technické podpory, správy a údržby AISG potřebné pro zajištění dostupnosti a správnosti všech funkcionalit AISG a jeho bezproblémový provoz. Servisní služby budou prováděny v součinnosti s Objednatelem a dalšími subjekty (např. Státní pokladna Centrum sdílených služeb, s. p.).

V rámci činností technické podpory je Dodavatel odpovědný za:

- dostupnost a správnost všech funkcionalit AISG,
- za řešení provozních incidentů (tzn. výskyt chování odlišného od dokumentace systému),
- za odstranění vad dodaného SW.

Další činnosti a odpovědnosti Dodavatele:

- Dodavatel bude dále vykonávat provozní požadavky a součinnosti vyžádané ostatními zúčastněnými subjekty, potřebné k zajištění provozu AISG a schválené Objednatelem.
- Dodavatel je plně odpovědný za dostupnost aplikace AISG dle níže uvedených parametrů Service Level Agreements a za záznam řešení incidentů v ServiceDesku SPCSS.
- Dodavatel odpovídá za incidenty způsobené vadou dodaného SW a to včetně proprietárního SW. Dokud není jednoznačně určena příčina incidentu, analyzuje a řeší Dodavatel incident jako vlastní incident v rámci SLA.

Dodavatel neodpovídá za:

- incidenty způsobené nefunkčností infrastruktury nebo některých jejích částí v odpovědnosti SPCSS,
- incidenty způsobené zásahem Objednatele do díla,

- incidenty způsobené nefunkčností spolupracujících externích systémů.

Řešení incidentů probíhá následujícími způsoby:

- včasný záznam incidentů a postupu jejich řešení v SD SPCSS,
- spolupráce na analýze incidentů (v případě požadavku schváleného Objednatelem spolupráce na řešení),
- v případě vady příprava dočasného náhradního řešení (**work-around**).

V rámci činností správy a údržby je Dodavatel odpovědný za kontroly a návrhy změn konfigurace, kontroly a analýzy logů, ladění a optimalizaci AISG, profylaxi a proaktivní údržbu potřebnou k předcházení incidentům a veškeré další administrátorské činnosti na aplikační úrovni potřebné pro provoz AISG. Dodavatel je povinen na základě analýzy incidentů navrhopvat, a po schválení objednatele na úrovni aplikace implementovat nové **metriky monitoringu a bezpečnostního dohledu** s cílem zrychlení detekce incidentů. Dodavatel je dále povinen navrhopvat a po schválení Objednatelem provádět upgrady a aktualizace použitých SW produktů s cílem udržení aktuálnosti a bezpečnosti AISG.

Součástí servisních služeb je i rozvoj a úprava mechanismů, které minimalizují vliv nefunkčnosti spolupracujících externích systémů na funkčnost AISG případně umožní při výskytu těchto externích chyb alespoň částečnou funkci systému.

### *7.1.1 Přehled prováděných servisních služeb*

## Úroveň L1

- Součinnost při telefonické podpoře uživatelů AISG
- Součinnost při vedení dokumentace popsanych problémů v SD SPCSS

## Úroveň L2

- Součinnost při analýze a řešení incidentů (Technická infrastruktura)
- Analýza a řešení incidentů (Aplikace, SW produkty a Data)
- Dokumentace řešení incidentů (Aplikace, SW produkty a Data)
- Uzavírání incidentů (Aplikace, SW produkty a Data)
- Součinnost při řešení metodických problémů a dotazů (AISG)
- Aktualizace číselníků (AISG)
- Součinnost při kontrole logů a stavu systému, identifikace vad a optimalizace (Technická infrastruktura)
- Kontroly logů a stavu systému, identifikace vad a optimalizace (Aplikace, SW produkty a Data)
- Opravy dat v AISG (duplicity, chyby dat)
- Správa databáze a migrace dat
- Návrhy na úpravy monitoringu (Aplikace, SW produkty a Data)
- Pokročilá správa uživatelů
- Metodická podpora a školení (včetně tvorby video návodů), šablony v AISG



## Úroveň L3

- Součinnost při analýze a řešení incidentů (Technická infrastruktura)
- Analýza a řešení incidentů (Aplikace, SW produkty a Data)
- Dokumentace řešení incidentů (Aplikace, SW produkty a Data)
- Uzavírání incidentů (Aplikace, SW produkty a Data)
- Zprostředkování podpory u výrobce SW (SW produkty)
- Legislativní znalost (správní řád a zákon o hazardu) při řešení incidentů
- Zajišťování ochrany a bezpečnosti AISG
- Zajišťování integrity dat v AISG a prvotní nastavení databáze
- Součinnost při kontrole logů a ladění konfigurace podle zkušeností z provozu (Technická infrastruktura)
- Kontroly logů a ladění konfigurace podle zkušeností z provozu (Aplikace, SW produkty a Data)
- Návrhy na úpravy monitoringu (Aplikace, SW produkty a Data)
- Součinnost při úpravě monitoringu a bezpečnostního monitoringu
- Součinnost při aktualizaci firmware a software (Technická infrastruktura)
- Součinnost při aktualizaci databázových serverů (patche, upgrady)
- Aktualizace SW produktů (SW produkty)
- Součinnost při propojení s okolními IS a DB dle technické dokumentace (Technická infrastruktura)
- Propojení s okolními IS a DB dle technické dokumentace (AISG)
- Součinnost při pokročilé zajištění a kontrole řádné synchronizace DB IS SDSL a DB AISG
- Aktualizace technické dokumentace (Aplikace, SW produkty a Data)

## Servis desk

- Součinnost při eskalaci stavu řešení incidentů
- Součinnost při zakládání incidentů a provozování monitoringu

## Provozní změny

- Řízení provozních změn a konfigurací (Aplikace, SW produkty a Data)
- Testování změn (Aplikace, SW produkty a Data)

## Řízení problémů

- Součinnost při analýze incidentů a identifikace problémů (Technická infrastruktura)
- Analýza incidentů a identifikace problémů (Aplikace, SW produkty a Data)
- Součinnost při evidenci problémů
- Součinnost při návrhování řešení problémů (Technická infrastruktura)
- Návrh řešení problémů (Aplikace, SW produkty a Data)
- Součinnost při řešení problémů (Technická infrastruktura)
- Řešení problémů (Aplikace, SW produkty a Data)

# Řízení rizik

- Identifikace rizik
- Součinnost při evidenci rizik a opatření
- Součinnost při navrhování opatření (Technická infrastruktura)
- Návrh opatření (Aplikace, SW produkty a Data)
- Součinnost při implementaci opatření (Technická infrastruktura)
- Implementace opatření (Aplikace, SW produkty a Data)

Pro realizaci výše uvedených servisních služeb bude mít dodavatel po celou dobu realizace plnění k dispozici tým servisních specialistů různých profesí (konzultant, analytik, programátor, DB a aplikační specialista, systémový inženýr a další).

## 7.1.2 Hotline

Dodavatel bude zajišťovat v provozní době systému (tj. V režimu 24/7) telefonickou podporu Hotline pro řešení incidentů a požadavků aplikační podpory. Služba Hotline bude využívána pracovníky SD SPCSS a oprávněnými pracovníky Objednatele k operativnímu informování o incidentech a operativnímu řešení incidentů a požadavků na činnosti provozní správy AISG.

## 7.1.3 Typy incidentů

### **Incident kategorie A (výpadek)**

AISG není použitelný ve svých základních a klíčových funkcích nebo není dostupný většině uživatelů. Tento stav kritickým způsobem ohrožuje klíčové odpovědnosti, procesy a aktivity Objednatele, případně způsobuje větší finanční nebo jiné kritické škody.

### **Incident kategorie B**

AISG je ve své funkcionalitě omezen tak, že tento stav významně omezuje běžné použití AISG ze strany uživatelů.

### **Incident kategorie C**

Drobné incidenty, které neomezují základní funkčnost a neomezují významně běžné použití AISG uživateli nebo způsobují omezení, které lze uživatelsky řešit jiným způsobem.

### 7.1.4 Garantované SLA

<b>Dozorová část AISG</b>			
<i>Provozní doba:</i>	7 x 24	<i>Minimální dostupnost</i> :	99,982%
	<b>Incident kategorie A</b>	<b>Incident kategorie B</b>	<b>Incident kategorie C</b>
<b>Maximální doba odezvy (v hodinách):</b>	0,25	1,5	4
<b>Maximální doba vyřešení (v hodinách):</b>	1,5	8	48
<b>Maximální počet incidentů:</b>	1 / rok	1 / měsíc	5 / měsíc

<b>Správní část AISG</b>			
<i>Provozní doba:</i>	6:00 – 20:00 v pracovních dnech	<i>Minimální dostupnost</i> :	99,00 %
	<b>Incident kategorie A</b>	<b>Incident kategorie B</b>	<b>Incident kategorie C</b>
<b>Maximální doba odezvy (v hodinách):</b>	0,5	6	14
<b>Maximální doba vyřešení (v hodinách):</b>	4	28	70
<b>Maximální počet incidentů:</b>	3 / rok	1 / měsíc	5 / měsíc

Pro zajištění garantovaných SLA bude mít dodavatel vytvořeny technické předpoklady (architektura využívá prvky vysoké dostupnosti –viz 3.1.3 - Vysoká dostupnost), nastaveny organizační parametry a zajištěny dostatečné lidské zdroje. Pro kritické části systému bude držena technická pohotovost 24/7. Jako prevence a předcházení fatálním chybám budou nastaveny kontinuální sledovací mechanismy provozu systému, které budou v reálném čase informovat o kondici aplikací/databází a budou vytvořeny krizové scénáře pro okamžité řešení nefunkčnosti.