Příloha č. 1

Technická dokumentace

Obsah

Tato příloha Smlouvy obsahuje technické požadavky na řešení Plnění.

1 Celkový přehled řešení

Řešení systému pro dohled nad sázkovými hrami a loteriemi (AISG) je rozděleno na část správní a část dozorovou.

1.1 Správní část

Správní část podporuje procesy související s vydáváním povolení, státním dozorem a vedením řízení. Jmenovitě se jedná o procesy:

2. Metodická činnost
3. Vyřizování dotazů
4. Pověřené osoby (PAO)
5. Řešení stížností
6. Spolupráce v daňové oblasti
7. Správa registrů
8. Ohlášení hazardní hry
9. Kontrolní činnost
10. Základní povolení
11. Povolení k umístění herního prostoru
14. Řízení o přestupcích
16. Archivace (v části související s DB správní a DMS)

Správní část poskytuje rozhraní pro uživatele (obce, kraje, MF, CS, FS, provozovatele, PAO), kteří budou výše zmíněné procesy vykonávat. Její součástí je nástroj pro řízení těchto procesů a databáze pro ukládání dat a dokumentů souvisejících s výkonem procesů.

1.2 Dozorová část

Dozorová část je určena především pro služby pro registraci a autorizaci hráčů a pro správu dat o hráčích.

Jmenovitě Dozorová část podporuje následující procesy:

12. Vedení rejstříku fyzických osob vyloučených z účasti na hazardních hrách
13. Registrace
16. Archivace (v části související s DB hráčů, DB vyloučení)

Tato část je primárně technická, bez rozhraní pro uživatele, výjimkou je možnost zápisu (a výmazu) osoby do rejstříku vyloučených osob, kde pracovníci MF musí mít možnost tento úkon provést i manuálně přes uživatelské rozhraní. Součástí části jsou vystavené služby, přes které budou systémově komunikovat provozovatelé:

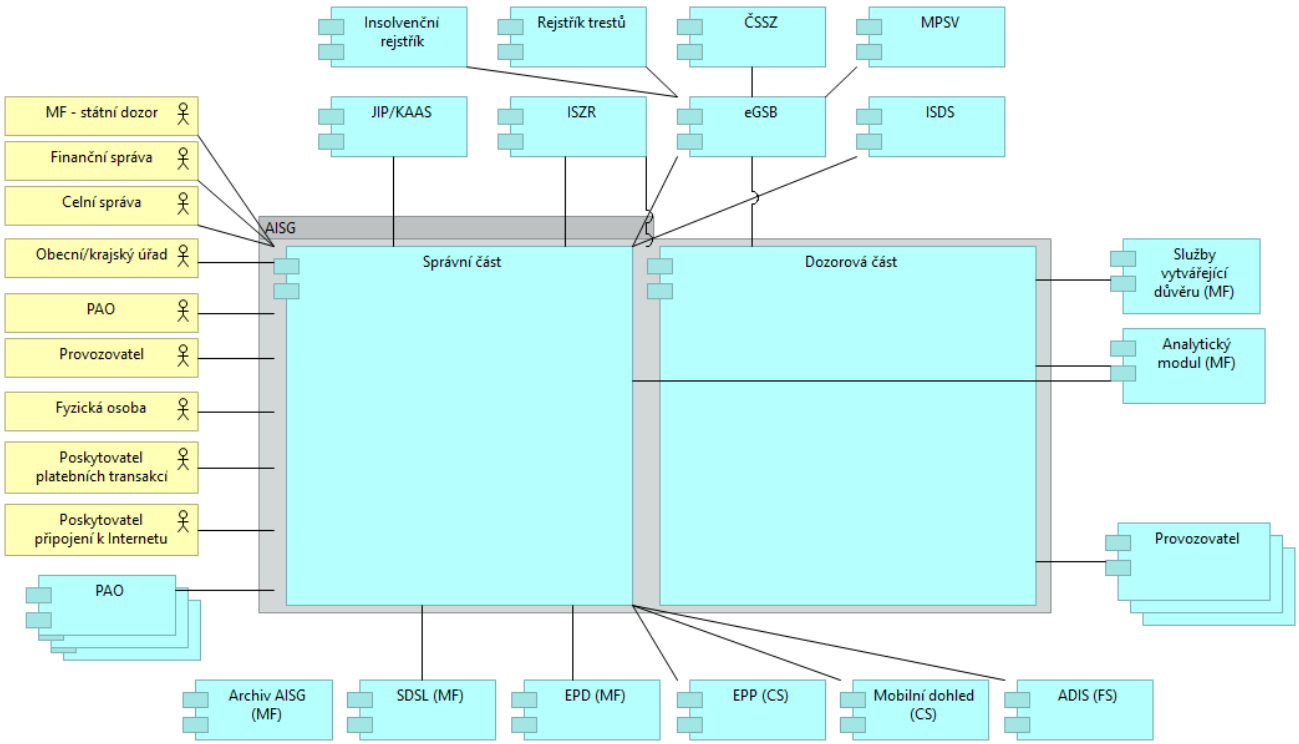
- Služba registrace hráče.
- Služba autorizace hráče.
- Služba změny údajů hráče.

2 Architektura systému

Diagramy v této kapitole definují klíčové pojmy používané v celé Smlouvě a jejích přílohách jako základ pro popis požadavků Objednatele. Dodavatel může ve výsledném řešení použít odlišnou architekturu (vyplývající např. ze struktury použitých SW produktů), nicméně pro účely nabídky, resp. smlouvy musí takovou architekturu namapovat na termíny a názvy komponent použité v této kapitole, aby bylo jasně prokázáno splnění všech požadavků. Rozdělení na Správní a Dozorovou část má navíc dopady i do požadavků na návrh řešení technické infrastruktury a provozních podmínek a jako takové je závazné.

2.1 Kontext systému

Sub-system context diagram popisuje zapojení AISG a jeho základních modulů v kontextu jeho uživatelů a okolních systémů, které s AISG interagují.



Popis elementů sub-systém context diagramu

Název elementu	Typ elementu	Popis elementu
Provozovatel	«Ostatní systém»	Informační systémy řádně registrovaného provozovatele.
PAO	«Ostatní systém»	Pověřená osoba dle § 110 ZHH. *Pozn: Pověřená osoba hraje roli uživatele AISG při manuálním vkládání osvědčení i externího systému při využití automatizovaného rozhraní. Obě varianty přístupu PAO jsou podporované.*
Služby vytvářející	«Ostatní systém»	K zajištění důvěrnosti, integrity a nepopiratelnosti komunikace systému

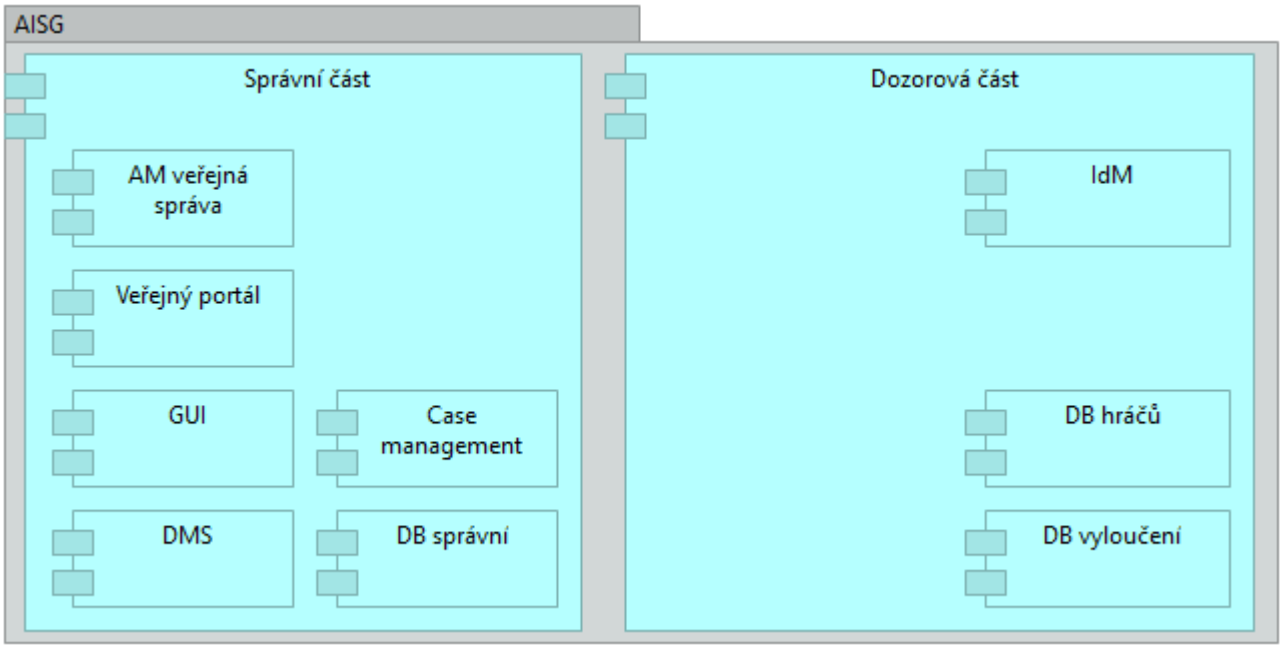
Název elementu	Typ elementu	Popis elementu
důvěru		provozovatele, resp. PAO s AISG bude sloužit systém založený na elektronických podpisech a pečetích. Objednatel v rámci modulu Služby vytvářející důvěru zajistí sadu podpůrných nástrojů a funkcí - služby jedné nebo více certifikačních autorit - certifikáty Objednatele, certifikáty provozovatelů a PAO, certifikáty CA, CRL.
Archiv AISG (MF)	«Ostatní systém»	Interní archiv AISG je cílovou komponentou pro archivované soubory a data podle procesu 16. Archivace. Implementace interního archivu AISG je v odpovědnosti Objednatele, odpovědností Dodavatele je výběr a příprava dat a souborů pro uložení do interního archivu a jejich následné smazání z databází a DMS. Komunikace s interním archivem bude probíhat formou předávání souborů. Archivace dat z databází bude probíhat formou uložení dat v XML souborech, pro každý běh archivace budou vytvořeny nové soubory.
Analytický modul	«Ostatní systém»	Analytický modul Objednatele získává od provozovatelů (mimo systém AISG) a zpracovává data o hazardních hrách a k jejich zpracování využívá i data z DB správní, DB hráčů a DB vyloučení. Vybudování Analytického modulu proběhne paralelně k dodávce AISG, je ale samostatnou aktivitou na straně Objednatele a není součástí integračního projektu přípravy AISG.
SDSL (MF)	«Ostatní systém»	Informační systém, který byl vyvinut k výkonu státního dozoru nad loteriemi a sázkami v souvislosti s plněním úkolů vyplývajících primárně ze zákona č. 202/1990 Sb., o loteriích a jiných podobných hrách ve znění pozdějších předpisů, částečně i ze zákona č. 186/2016 Sb., o hazardních hrách.
EPD (MF)	«Ostatní systém»	Systém spisové služby MF (EPD).
EPP (CS)	«Ostatní systém»	IS Evidence porušení předpisů využívaný Celní správou.
Mobilní dohled (CS)	«Ostatní systém»	IS Mobilní dohled využívaný Celní správou.
ADIS (FS)	«Ostatní systém»	Informační systém Finanční správy.
JIP/KAAS	«Ostatní systém»	Jednotný identitní prostor veřejné správy. Bude sloužit jako jediný identitní prostor pro všechny uživatele systému z veřejné správy (včetně obcí a krajů), uchovává přihlašovací údaje (uživatelské jméno, heslo) a uživatelské role pro přístup do AISG. *Pozn: Neplatí pro administrátory systému AISG, viz popis komponenty AM veřejná správa.*
ISZR	«Ostatní systém»	Informační systém základních registrů – součást systému Základních registrů realizovaných na základě zákona č. 111/2009 Sb.
eGSB	«Ostatní systém»	eGON Service Bus – ve spolupráci s ISZR slouží k výměně informací mezi

Název elementu	Typ elementu	Popis elementu
		AIS. Viz dokumentaci na http://www.mvcr.cz/clanek/dokumentace-egsb.aspx. *Poznámka: Zadávací dokumentace předpokládá dostupnost definice a implementace potřebných eGSB služeb rezortů MSp a MPSV prostřednictvím eGSB v termínech odpovídajících harmonogramu implementace AISG. V případě nedodržení tohoto předpokladu dojde formou změnového požadavku k definici a implementaci náhradního řešení, pravděpodobně přímé komunikace mezi AIS s využitím ISZR služeb E175 a E176 pro mapování AIFO.*
ISDS	«Ostatní systém»	Informační systém datových schránek provozovaný Českou poštou na základě zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentu. Je přímo využíván pouze pro autentizaci provozovatelů a PAO pomocí autentizační služby Portálu veřejné správy, která ověřuje uživatele pomocí přístupových údajů datových schránek, a pro odesílání datových zpráv pomocí Odesílací brány ISDS. *Pozn: Ostatní způsoby využití ISDS jsou nepřímé prostřednictvím EPD.*
Insolvenční rejstřík (MSp)	«Ostatní systém»	Agendový informační systém Ministerstva spravedlnosti o osobách v insolvenci.
Rejstřík trestů (MSp)	«Ostatní systém»	Rejstřík trestů je vede evidenci osob pravomocně odsouzených soudy v trestním řízení a dále evidenci jiných skutečností významných pro trestní řízení. Údaje z evidence slouží pro potřebu trestního, občanskoprávního nebo správního řízení a k prokazování bezúhonnosti.
ČSSZ	«Ostatní systém»	Informační systém České správy sociálního zabezpečení.
MPSV	«Ostatní systém»	Agendový informační systém Ministerstva práce a sociálních věcí obsahující informace o osobách pobírajících dávky hmotné nouze.
MF – státní dozor	«Uživatel»	Odbor 34 Ministerstva financí
Provozovatel	«Uživatel»	Provozovatel hazardní hry
Obecní úřad	«Uživatel»	Obecní úřad je orgán obce. Ve městech se tento úřad nazývá městský úřad, v městech úřad městský, ve městech statutárních pak magistrát.
Krajský úřad	«Uživatel»	Krajský úřad je jedním z orgánů kraje (vedle zastupitelstva kraje, rady kraje, hejtmana kraje a zvláštního orgánu kraje). Krajský úřad projednává zejména odvolání proti rozhodnutí obecního úřadu.
Celní správa (CS)	«Uživatel»	Celní správa České republiky je bezpečnostním sborem zajišťujícím výkon kompetencí v oblasti správy cel a některých daní, jakož i dalších svěřených nefiskálních činností ve prospěch státu i jeho občanů. Je podřízena Ministerstvu financí ČR.

Název elementu	Typ elementu	Popis elementu
Finanční správa (FS)	«Uživatel»	Finanční správa vykonává správu daní, provádí daňové řízení, převádí výnosy daní, které vybírá a vymáhá pohledávky v oblasti hazardních her.
Fyzická osoba	«Uživatel»	Občan, uživatel veřejné části Veřejného portálu
Poskytovatel platebních transakcí/operací	«Uživatel»	Aktér poskytující platební transakce/operace dle zákona o platebním styku.
Poskytovatel připojení k Internetu (ISP)	«Uživatel»	Poskytovatel internetového připojení (používána zkratka ISP z anglického Internet service provider) je firma nebo organizace zprostředkující přístup do Internetu, tj. poskytující telekomunikační služby.

2.2 Komponenty systému

Diagram komponent popisuje hlavní systém a moduly, ze kterých se skládá, a dále rozhraní hlavního systému na ostatní systémy.



Popis elementů diagramu komponent

Název elementu	Typ elementu	Popis elementu
DB správní	«Modul systému»	DB správní – databáze udržuje data o legálních provozovatelích, nelegálních provozovatelích a ostatních subjektech působících v rámci provozování hazardních her, včetně souvisejících řízení. 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).
DB hráčů	«Modul systému»	DB hráčů – databáze udržující data o hráčích a jejich vazbách na provozovatele. DB hráčů 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).
DB vyloučení	«Modul systému»	DB vyloučení – databáze udržující data o subjektech vyloučených z hraní (využívaná jak při registraci, tak při autorizaci hráče) a záznamy o transakcích služby ověření hráče 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).

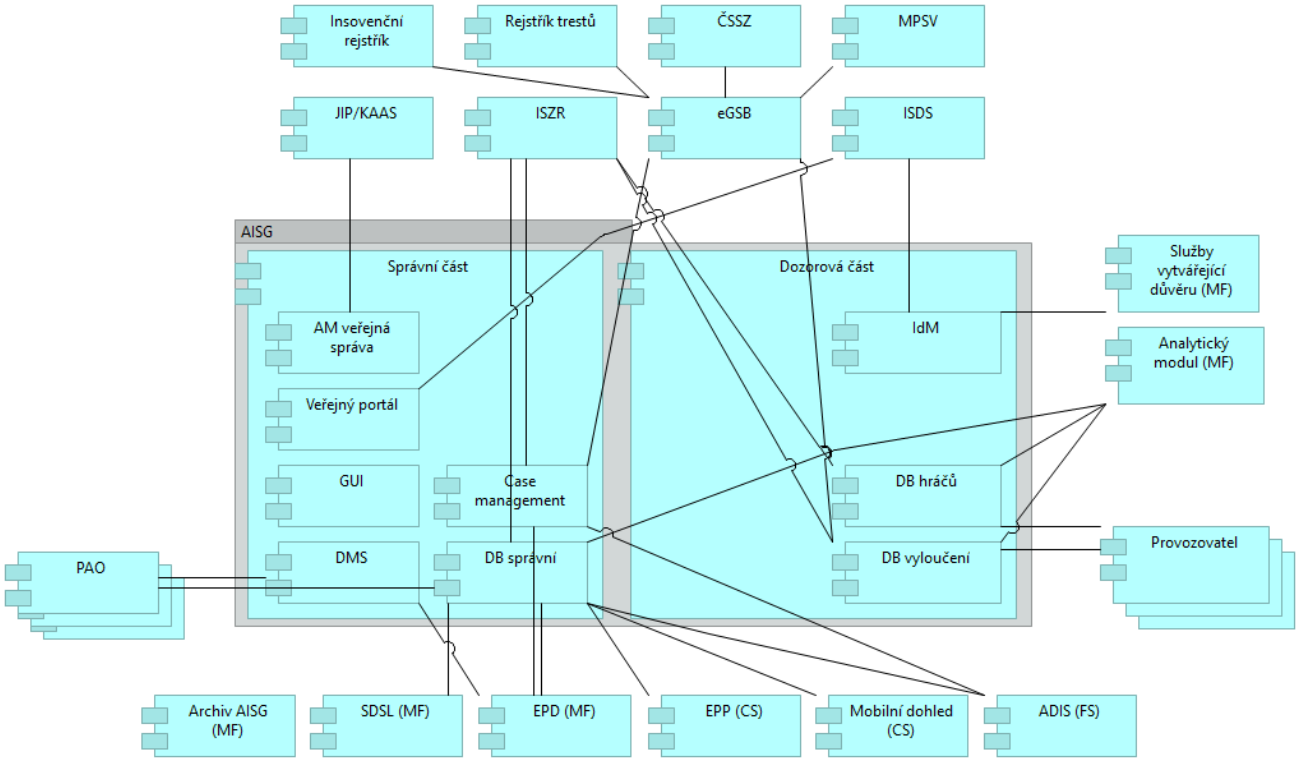
Název elementu	Typ elementu	Popis elementu
Case Management	«Modul systému»	Tento modul řídí všechna workflow Správní části. Komponenta je součástí implementace všech uživatelských a automatických procesů Správní části využívajících logiku workflow. Každé workflow je složeno z jednotlivých úkolů. Ke každému 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.
DMS	«Modul systému»	Document Management System – systém pro správu dokumentů. Komponenta je součástí implementace všech uživatelských a automatických procesů Správní části pracujících s dokumenty. Udržuje dokumenty související s agendou systému, které jsou nahrány přímo do systému a nejsou udržovány v jiných systémech státní správy. 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 uchováván pouze na jednom místě bez omezení pro oprávněného uživatele. Systém EPD nenabízí možnost vzdáleného přístupu pro jiné organizace než MF. Povoleným řešením je vytvoření dočasné kopie dokumentu v AISG. Kopie dokumentů v AISG budou určeny pouze pro zobrazení, nebude možné je jakkoliv editovat či mazat. Podpora skenování není požadována. Počet ukládaných dokumentů do DMS bude maximálně 20 tisíc za jeden rok. Průměrná velikost dokumentu nepřekročí 1 MB. DMS musí být v souladu s požadavky na ISSD (informační systém spravující dokumenty) dané Národním standardem pro elektronické systémy spisové služby (http://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx).
GUI	«Modul systému»	Graphical User Interface – Grafické rozhraní systému. 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). GUI může mít formu tlustého klienta (Windows aplikace) nebo tenkého klienta (web aplikace). GUI musí být provozovatelné na běžných kancelářských PC s rozlišení obrazovky 1024x768 a vyšším, operačních systémech MS Windows 7 (32-bit a 64-bit) a novějších. Pokud je GUI web aplikací, musí podporovat Internet Explorer a Firefox ve verzích podporovaných výrobci.
Veřejný portál	«Modul systému»	Portál slouží pro přístup veřejnosti a uživatelů mimo resort MF. Z tohoto důvodu je rozdělený na dvě části – veřejnou a privátní. 1. Veřejná část

Název elementu	Typ elementu	Popis elementu
		• Je určena pro přístup široké veřejnosti. • Slouží k zobrazování veřejně dostupných informací (včetně veřejně dostupných formulářů). • Je dále určena pro nepřihlášené provozovatele, resp. PAO, kteří mají možnost portál využít pro zadání žádostí a poskytnutí dokumentů, funkce předvyplnění údajů a přístup k historii žádostí získají až po přihlášení do privátní části portálu. 2. Privátní část • Je určena pro přístup úředníků z obcí a krajů. • Úředníci se do ní hlásí přes své přístupové údaje v JIP/KAAS. • Funguje jako jediné uživatelské rozhraní pro obce a kraje. • Je dále určena pro přihlášené provozovatele, resp. PAO, kteří mají možnost portál využít pro zadání žádostí a poskytnutí dokumentů, včetně předvyplnění údajů a přístupu k historii svých žádostí. Veřejný portál je web aplikace a musí podporovat prohlížeče Internet Explorer, Firefox, Chrome, Safari a Edge ve verzích podporovaných výrobci.
AM veřejná správa	«Modul systému»	Modul, který slouží k řízení přístupu (AM – Access Management) uživatelů z veřejné správy (včetně obcí a krajů) k funkcím AISG. 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. 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. Je požadována integrace autentizace čipovou kartou do AISG. Autentizace malého počtu technických administrátorů systému a jeho jednotlivých komponent může být implementována způsobem specifickým pro jednotlivé komponenty.
IdM – Identity management	«Modul systému»	Modul, který slouží ke správě identit provozovatelů a PAO. Modul 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. 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). Předpokládá se dvouúrovňový systém, který naplňuje požadavky řešení bezpečnosti. Provozovatelé, resp. PAO budou přistupovat do několika části

Název elementu	Typ elementu	Popis elementu
		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. 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. IdM kontroluje platnost uložených certifikátů a notifikuje administrátora o blížícím se termínu obnovy certifikátů. IdM musí 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. *Pozn: Přestože funkční procesy provozovatele a PAO a jejich vazba na vnitřní komponenty AISG jsou zcela odlišné, z technického hlediska pro ně předpokládáme automatizovaná XML rozhraní založená na stejných principech a stejný princip autentizace. Proto je jejich identita spravována ve stejné komponentě řešení.*

2.3 Rozhraní a datové toky

Diagram datových a datových toků popisuje datové toky mezi komponentami AISG a ostatními systémy, které jsou na něj napojeny (informační systémy resortu MF, veřejné správy a systémy provozovatelů a PAO).



Poznámka: rozhraní a datové toky jsou zobrazené a popsané z pohledu komponent AISG jako logické, popisují zdroje a cíle dat předávaných na rozhraní. Z technického pohledu nereprezentují přímou komunikaci, např. přímý přístup do DB. Pro implementaci rozhraní mohou být v návrhu Dodavatele využity další funkční komponenty implementující např. WebServices rozhraní apod.

Dodavatel je povinen v rámci Detailního návrhu řešení a implementace systému definovat a implementovat mechanismy, které minimalizují vliv nefunkčnosti spolupracujících externích systémů na funkčnost AISG (např. ošetření chybových stavů, opakování neúspěšných operací, využití nakešovaných nebo „starých" informací – v případech, kde je to možné a umožní alespoň částečnou funkci systému). Funkcionalita AISG může být v případě nefunkčnosti spolupracujících systémů omezena pouze ve funkcionalitách, které jsou přímo závislé na zmíněných systémech. Tyto funkcionality musí mít pro takový případ předem definované chybové stavy, tj. jaký dopad má nefunkčnost spolupracujícího systému na konkrétní funkcionality AISG.

V Detailním návrhu řešení Dodavatel podrobně popíše chybové stavy jednotlivých rozhraní, analyzuje jejich příčiny a navrhne způsob jejich ošetření na straně AISG.

Popis elementů diagramu rozhraní a datových toků

Tabulka nepopisuje obecně rozhraní jako směrová, logika iniciace a směrování komunikací mezi Elementem A a Elementem B vždy vyplývá z konkrétních požadavků a způsobu implementace daného rozhraní.

Element A	Element B	Typ	Popis rozhraní
Provozovatel	DB hráčů	Online	Mezi systémem provozovatele a AISG jsou vystaveny následující služby

Element A	Element B	Typ	Popis rozhraní
			v souladu s definicí procesu 13. Registrace (viz Přílohu č. 2 Smlouvy): 1. Registrace / ztotožnění hráče 2. Aktualizace údajů hráče Viz též sekce Obecný popis rozhraní k provozovatelům a PAO pod touto tabulkou.
Provozovatel	DB vyloučení	Online	Mezi systémem provozovatele a AISG jsou vystaveny následující služby v souladu s definicí procesu 13. Registrace (viz Přílohu č. 2 Smlouvy): 1. Autorizace hráče Viz též sekce Obecný popis rozhraní k provozovatelům a PAO pod touto tabulkou.
PAO (Pověřená osoba)	DB Správní, DMS	Batch	Automatizované rozhraní pro evidence osvědčení (včetně předání dokumentů). Viz též sekce Obecný popis rozhraní k provozovatelům a PAO pod touto tabulkou.
DB hráčů	ISZR	Online	1. Ztotožnění hráče - Rozhraní je postaveno v souladu s požadavky SZR. - AISG volá základní službu s identifikačními údaji daného hráče (jméno, příjmení, místo narození, datum narození, bydliště) - ISZR vrací kompletní evidovanou sadu údajů k danému subjektu, případně vrací informaci, že na základě poskytnutých údajů není možné hráče jednoznačně ztotožnit (existuje více subjektů se stejnými údaji; neexistuje žádný subjekt odpovídající údajům). - AISG se registruje k aktualizaci údajů o subjektu.
ISZR	DB hráčů	Batch	Rozhraní je postaveno v souladu s požadavky SZR. U fyzických osob registrovaných v AISG bude AISG dávkově (1x denně) dostávat informace o aktualizaci jejich referenčních údajů v základních registrech.
Case Management	ISZR	Online	1. Validace / stažení údajů o provozovateli nebo PAO - Rozhraní je postaveno v souladu s požadavky SZR. - AISG volá základní službu s IČO provozovatele nebo PAO. - ISZR vrací kompletní evidovanou sadu údajů k danému subjektu, případně vrací informaci, že na základě poskytnutých údajů není možné subjekt jednoznačně ztotožnit (existuje více subjektů se stejnými údaji; neexistuje žádný subjekt odpovídající údajům). - AISG se registruje k aktualizaci údajů o subjektu.
ISZR	DB správní	Batch	Rozhraní je postaveno v souladu s požadavky SZR. U právnických osob registrovaných v AISG bude AISG dávkově (1x týdně) dostávat informace o aktualizaci jejich referenčních údajů v základních registrech.
ISZR	DB vyloučení	Batch	Rozhraní je postaveno v souladu s požadavky SZR. U fyzických osob uvedených DB vyloučení bude AISG dávkově (1x denně) dostávat informace o

Element A	Element B	Typ	Popis rozhraní
			aktualizaci jejich referenčních údajů v základních registrech.
EPD	DB správní	Online	1. Předání informace o dokumentech určených pro AISG - EPD předává do AISG informaci o dokumentech, které byly do EPD předány pro účely výkonu agendy AISG. Informace jsou minimálně v rozsahu: • jedinečný identifikátor dokumentu (číslo jednací, PID), • typ dokumentu (z číselníku), • verze dokumentu, • subjekt, který dokument předal, • název dokumentu, • odkaz na dokument, • stav dokumentu (nový, smazaný, atd.). - Forma rozhraní odpovídá standardům EPD. - V rámci rozhraní neprobíhá samostatné předání dokumentu – ten je umístěn a spravován v EPD. V AISG se evidují pouze výše uvedená metadata dokumentu. Pro správní část AISG platí, že elektronická komunikace bude probíhat primárně přes EPD s využitím ISDS. Pokud je na MF doručen elektronicky podepsaný dokument emailem, je zanesen do EPD obdobně jako v případě, že by dorazil s využitím ISDS. Ověřování elektronických podpisů u přijatých dokumentů bude kompletně řešit EPD, tedy správní část AISG podpisy ověřovat nebude.
Case Management	EPD	Online	Zobrazení dokumentu z EPD
Case Management	eGSB	Online	1. Předávání informace o bezdlužnosti u ČSSZ. - Rozhraní je postaveno v souladu s požadavky eGSB. - Jedná se o eGSB službu vystavenou nad systémem ČSSZ – registr dlužníků na sociálním pojištění. - AISG přes eGSB službu zasílá IČO. - eGSB služba vrací informaci, zda je dané IČO vedeno v registru dlužníků. - Pozn.: Služba se provolává jak v okamžiku zadávání daného subjektu do AISG, tak pravidelně (1x za týden) pro všechny právnické osoby (provozovatelé, PAO), které mají platný záznam v AISG. 2. Předávání informace o bezúhonnosti - Rozhraní je postaveno v souladu s požadavky eGSB. - Jedná se o eGSB službu vystavenou nad systémem Rejstřík trestů. - AISG přes eGSB službu zasílá IČO / AIFO (u fyzických osob). - eGSB vrací informaci, zda je dané IČO / AIFO vedeno v Rejstříku trestů. - Pozn.: Služba se provolává jak v okamžiku zadávání daného subjektu do AISG, tak pravidelně (1x za týden) pro všechny právnické osoby (provozovatelé, PAO), které mají platný záznam v AISG. 3. Předávání informace o osobách v úpadku - Rozhraní je postaveno v souladu s požadavky eGSB. - Jedná se o eGSB službu vystavenou nad systémem Insolvenční rejstřík.

Element A	Element B	Typ	Popis rozhraní
			- AISG přes eGSB službu zasílá IČO. - eGSB vrací informaci, zda je dané IČO vedeno v Insolvenčním rejstříku. - Pozn.: Služba se provolává jak v okamžiku zadávání daného subjektu do AISG, tak pravidelně (1x za týden) pro všechny právnické osoby (provozovatelé, PAO), které mají platný záznam v AISG.
Case Management	ADIS	Online	Předávání informace o bezdlužnosti u FS - Rozhraní je založeno na výměně XML zpráv formou Web Service - Na straně IS FS se jedná a službu registru osob s nedoplatkem u Finanční správy. - AISG zasílá IČO (v případě zahraničních subjektů vlastní číslo plátce (VČP)), ISFS vrací informaci, zda je dané IČO/VČP vedeno v registru dlužníků. - Pozn.: Služba se provolává jak v okamžiku zadávání daného subjektu do AISG, tak pravidelně (1x za týden) pro všechny právnické osoby (provozovatelé, PAO), které mají platný záznam v AISG (cca 100 subjektů).
JIP /KAAS	AM veřejná správa	Online	1. Autentizace a autorizace uživatelů z veřejné správy pracujících s AISG - JIP/KAAS předává token a role ke konkrétní osobě při jejím přihlášení. - Forma komunikace je podle standardu JIP/KAAS.
DB vyloučení	eGSB	Batch	1. Identifikace osob pobírajících dávky v hmotné nouzi - Rozhraní je postaveno v souladu s požadavky eGSB. - Jedná se o eGSB službu vystavenou nad systémem MPSV – registr osob pobírajících dávky v hmotné nouzi. - MPSV 1x denně (dávkovou replikací) předává AISG údaje z registru osob pobírajících dávky. 2. Identifikace osob v úpadku - Rozhraní je postaveno v souladu s požadavky eGSB. - Jedná se o eGSB službu vystavenou nad systémem Insolvenční rejstřík. - Insolvenční rejstřík 1x denně (dávkovou replikací) předává AISG údaje z registru osob v úpadku.
EPP	DB správní	Online	1. Předání dat o správním řízení - IS EPP volá WebService AISG a předává data o realizovaném správním řízení vedeném v systému EPP a pokutách. Minimální obsah předávaných dat: • unikátní ID správního řízení / pokuty, • základní informace o správním řízení / pokutě (účastníci správního řízení, údaje ztotožněné vůči ISZR), • unikátní ID kontroly, ke kterému se správní řízení / pokuta váže, • částka, • stav správního řízení, • právní kvalifikace, • výsledek správního řízení, • přílohy (soubory).

Element A	Element B	Typ	Popis rozhraní
			Pozn: Rozhraní je online ve smyslu synchronního volání jedné WebService pro každé správní řízení. Rozhraní lze použít kdykoliv, ale předpokládá se jeho volání v plánovaném režimu, např. 1x denně pro všechna správní řízení realizovaná v daný den. *Pozn: Předávané přílohy jsou uloženy v DMS jako kopie originálních příloh uložených (a dlouhodobě archivovaných) ve spisové službě CS eSAT. Přímé spojení AISG do eSAT není, AISG pracuje s kopiemi.*
Mobilní dohled	DB správní	Online	1. Předání dat o realizovaných kontrolách - IS Mobilní dohled volá WebService AISG a předává data o realizované kontrole. Minimální obsah předávaných dat: • unikátní ID kontroly, • základní údaje o kontrole (kdo, kde, kontrolovaný subjekt; údaje ztotožněné vůči ISZR), • typ kontroly (z číselníku), • výsledek kontroly (z číselníku), • komentář, • přílohy (soubory). - Vzhledem k časovému rozdílu mezi zadáním kontroly do systému a uzavřením kontroly se předpokládá předání údajů minimálně v okamžiku zadání kontroly a v okamžiku jejího uzavření. *Pozn: Rozhraní je online ve smyslu synchronního volání jedné WebService pro každou kontrolu. Rozhraní lze použít kdykoliv, ale předpokládá se jeho volání v plánovaném režimu, např. 1x denně pro všechny kontroly zadané a uzavřené v daný den.* *Pozn: Předávané přílohy jsou uloženy v DMS jako kopie originálních příloh uložených (a dlouhodobě archivovaných) ve spisové službě CS eSAT. Přímé spojení AISG do eSAT není, AISG pracuje s kopiemi.*
SDSL (MF)	DB správní	Batch	Rozhraní mezi stávajícím systémem pro státní dozor (SDSL) a AISG. Detailnější informace jsou obsaženy v Příloze č. 3 Smlouvy.
DB správní	ADIS	Batch	1. Zajištění podkladů pro kontrolu daňových přiznání k dani z hazardních her Systém bude předávat informace pro kontrolu údajů uvedených v daňových přiznáních provozovatelů. Údaje o: • jednotlivých provozovatelích – DIČ/VČP, název provozovatele, sídlo, včetně státu sídla u zahraničních provozovatelů • druhu hazardní hry a způsobu jejího provozována (land-based/internet) • základním povolení – číslo jednací, datum nabytí právní moci, platnost povolení (od-do), typ rozhodnutí (povolení, změna, zrušení) • povolení k umístění herního prostoru – číslo jednací povolení, datum nabytí právní moci, platnost povolení (od –do), uvedení

Element A	Element B	Typ	Popis rozhraní
			typu rozhodnutí (povolení, změna, zrušení), provozovna s uvedením adresy • názvu a adrese herního prostoru ve vazbě na základní povolení/povolení k umístění herního prostoru • adrese místa, kde bude ohlašovaná hazardní hra provozována • počtu herních pozic jednotlivých povolených koncových zařízení uvedených v povolení k umístění herního prostoru pro výpočet minimální daně u technických her • údaje o herním prostoru – obec/město; ulice; č. popisné/orientační; PSČ; kód obce 2. Zajištění podkladů pro převod daní obcím Systém bude předávat podíl jednotlivých obcí vyjádřený v procentech, kterým se jednotlivé obce podílejí na části celostátního hrubého výnosu daně plynoucího ve zdaňovacím období, což se určí v závislosti na poměru: a) součtu herních pozic jednotlivých povolených koncových zařízení uvedených v povolení k umístění herního prostoru, které jsou povoleny na území dané obce k prvnímu dni bezprostředně předcházejícího zdaňovacího období, k b) celkovému součtu herních pozic jednotlivých povolených koncových zařízení uvedených v povolení k umístění herního prostoru, které jsou povoleny k prvnímu dni bezprostředně předcházejícího zdaňovacího období (tj. podle § 7 odst. 3 zákona č. 187/2016 Sb., o dani z hazardních her). Všechny výše uvedené údaje se budou předávat nejpozději 1. den následujícího měsíce po uplynutí každého zdaňovacího období. Data budou předávána ve formátu XML přes webové rozhraní.
DMS	EPD	Online	Rozhraní pro přesun dokumentů a vytváření kopií, mj. pro vytvoření dočasné kopie dokumentu z EPD v AISG. Rozhraní mezi DMS a EPD musí být 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 (http://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx) s tím, že rozhraní musí implementovat události (operace) odpovídající charakteru a funkcionalitě komponenty DMS podle požadavků v přílohách Smlouvy.
IdM	ISDS	Online	Autentizace majitelů datových schránek (primárně provozovatelů a PAO) pomocí autentizační služby Portálu veřejné správy, která ověřuje uživatele pomocí přístupových údajů datových schránek. *Pozn: Využíváno v rámci Správní části AISG, viz popis komponenty IdM*
Veřejný portál	ISDS	Online	Odesílací brána ISDS
IdM	Služby vytvářející	Online	Komunikace se službami modulu Služby vytvářející důvěru prostřednictvím standardních protokolů pro danou službu (stahování certifikátů a CRL po

Element A	Element B	Typ	Popis rozhraní
	důvěru		HTTPS apod), případně WebServices.
DB správní DB hráčů DB vyloučení	Analytický modul	Batch	Předávání aktuálního stavu DB a změn za předchozí den 1x denně. Data budou předávány způsobem umožňujícím zpracování standardními ETL nástroji, tj. ve formě strukturovaných souborů nebo separátní sady tabulek. AISG musí dále podporovat předání historie změn za určité období (manuální operace administrátora AISG)

Obecný požadavek na rozhraní k IS provozovaným v resortu MF

Spojení musí být navázáno prostřednictvím kryptografických prostředků, samostatně předávané soubory musí být šifrovány v souladu s minimálními požadavky na kryptografické algoritmy uvedené ve vyhlášce č. 316/2014.

Obecný popis rozhraní k IS provozovatelů a PAO

Přenos dat mezi systémy provozovatele/PAO a AISG je vždy šifrován. Půjde o HTTPS komunikaci s přenosem elektronicky podepsaných XML zpráv dle standardu WS-security (nebo obdobným způsobem). Všechny používané certifikáty provozovatelů/PAO budou registrovány v IdM.

XML zprávy v obou směrech budou opatřeny elektronickým podpisem (pečetí). Elektronické podpisy (pečetě) budou vytvářeny a ověřovány přímo na serverech AISG s využitím klíčů a certifikátů získaných prostřednictvím modulu Služeb vytvářejících důvěru Objednatele a uložených v softwarových úložištích IdM,

3 Technická infrastruktura

3.1 Vymezení odpovědností Dodavatele

V souladu se strategií ICT resortu Ministerstva financí bude AISG vybudován a provozován v prostředí Národního datového centra (dále jen „NDC“) resortního dodavatele služeb infrastruktury a provozu Státní pokladny Centra sdílených služeb, s.p. (dále jen „SPCSS“). Dodávku, implementaci a provoz síťové, HW a SW infrastruktury (dále jen Technické infrastruktury, v rozsahu upřesněném v této kapitole přílohy Smlouvy) a související provozní služby (zálohování, monitoring) zajistí Objednatel prostřednictvím SPCSS. Cílem této strategie je dosažení maximální efektivity sdílených služeb IT infrastruktury v resortu Ministerstva financí a soulad se strategií rozvoje eGovernmentu ČR.

SPCSS bude poskytovat Technickou infrastrukturu a související provozní služby formou provozních služeb na svých sdílených platformách, včetně přípravy těchto služeb v rámci implementace AISG. Konkrétně jde o oblasti:

- Služby datového centra
- Bezpečné propojení a připojení do Internetu (síťové služby)
- Poskytování výpočetního výkonu (včetně virtualizace)
- Poskytování diskového prostoru
- Správa operačních systémů
- Správa databází (pouze provozní služby v rámci Servisních služeb, dodávka, SW licence včetně maintenance a implementace v odpovědnosti Dodavatele)
- Zálohování a archivace dat
- CKB, SOC a bezpečnostní monitoring
- Provozní monitoring
- ServiceDesk

Návrh kompletní Technické infrastruktury AISG je odpovědností Dodavatele. Dodavatel navrhne a popíše Technickou infrastrukturu včetně jejího kapacitního návrhu v Příloze č. 8 Smlouvy na základě požadavků uvedených ve Smlouvě a jejích přílohách. V návrhu Technické infrastruktury Dodavatel použije výhradně standardy a stavební bloky SPCSS, uvedené v kapitole 3.3 této přílohy Smlouvy a popíše ji podle požadavků uvedených v Příloze č. 8 Smlouvy.

Součástí Technické infrastruktury jsou veškeré HW komponenty potřebné pro provoz AISG. Součástí Technické infrastruktury jsou pouze takové softwarové produkty a aplikace, které jsou nedílnou součástí HW zařízení (firmware) nebo uvedené v popisu standardů a stavebních bloků dále v této kapitole (virtualizační software, operační systémy, software dohledových systémů a ServiceDesk). Ostatní software a aplikace jsou součástí Díla, a v této a ostatních přílohách Smlouvy jsou označovány jako „SW produkty“ (Proprietární software nebo Open source software dle odst. 11 Smlouvy), „Aplikace“ (vyvinuté na zakázku pro AISG) a „Data“ (data SW produktů a Aplikací). Souhrnně jsou také obecně označovány jako „aplikační komponenty“ nebo „aplikační úroveň“, jejich správa z pohledu provozu pak jako „aplikační správa“.

V rámci realizace Díla a poskytování Servisních služeb a Služeb rozvoje bude Dodavatel spolupracovat s Objednatelem a SPCSS způsobem uvedeným v přílohách č. 4 a č. 5 Smlouvy, včetně plnění součinností souvisejících s implementací a provozem technické infrastruktury a souvisejících provozních služeb SPCSS. Rozdělení odpovědností Dodavatele a Objednatele v implementaci i provozu vychází primárně z výše uvedeného vymezení Technické infrastruktury. Detailní rozdělení odpovědností mezi Dodavatele a SPCSS a rozsah součinností při realizaci Díla (implementaci AISG) a poskytování Servisních služeb a Služeb rozvoje (provozu AISG) je uvedeno v přílohách č. 4 a č. 5 Smlouvy.

3.2 Prostředí

Požadována je implementace tří prostředí AISG: Produkční, Pre-produkční a Testovací/vývojové prostředí. Součástí Testovacího/Vývojového prostředí je i vývojové a dokumentační prostředí popsané v kapitole 4.2 Přílohy č. 4 Smlouvy.

Redundance HW i SW komponent Produkčního prostředí musí umožnit splnění SLA dostupnosti i všech výkonnostních požadavků i v případě výpadku jedné HW komponenty. V případě Správní části AISG je možno a doporučeno použít mechanismy vysoké dostupnosti na úrovni virtualizace. V případě Dozorové části AISG je požadováno active-active řešení na úrovni Aplikace i databází, případně dalších SW produktů.

Pro Dozorovou část je požadováno umístění části systému do druhého datového centra (geografická redundance) s cílem zajištění parametrů SLA pro tuto část i v případě kompletního výpadku primárního datového centra. Mechanismus přechodu provozu do druhého datového centra musí splňovat parametry RTO a RPO dle specifikace nefunkčních požadavků v kapitole 5 této přílohy Smlouvy.

Využití záložní lokality je možné pro všechny části řešení podle návrhu Dodavatele.

Pro neprodukční prostředí není Objednatelem požadován stejný výkon a disková kapacita jako u produkčního prostředí, musí ale splňovat následující požadavky:

- Návrh Pre-produkčního prostředí musí replikovat mechanismy redundance HW a SW produkčního prostředí na úrovni stavebních bloků i na úrovni aplikační a databázové architektury, a to včetně replikace architektury rozmístění serverů, resp. uzlů jednotlivých clusterů do primární a záložní lokality.
- Výkon a datové kapacity Pre-produkčního prostředí musí odpovídat potřebám funkčního testování oprav a změn v rámci Servisních služeb a Služeb rozvoje. Čisté datové kapacity úložišť Pre-produkčního prostředí musí odpovídat minimálně 10 % čistých datových kapacit Produkčního prostředí - platí pro každé dílčí úložiště (DB hráčů, DB vyloučení, DB správní a DMS) samostatně.
- Návrh Testovacího/vývojového prostředí musí odpovídat požadavkům na testování a školení popsaným v kapitolách 4.3 a 4.5 Přílohy č. 4 Smlouvy.
- Návrh Testovacího/vývojového prostředí musí obsahovat vývojové a dokumentační prostředí, popsané v kapitole 4.2 Přílohy č. 4 Smlouvy.
- Návrh neprodukčních prostředí musí umožnit po dobu Implementace Release 2 (Etapa 2) nezávislé testování oprav a změn Release 1 paralelně k celému vývojovému a testovacímu cyklu Release 2.

Přepokládaný způsob využití neprodukčních prostředí v době provozu je následující:

- Pre-produkční prostředí je funkční replikou Produkčního prostředí a je využíváno pro testy drobných oprav a změn a finální testy větších změn před nasazením do Produkčního prostředí.
- Testovací/vývojové prostředí je využíváno na vývoj a testování rozsáhlejších změn.

Způsob využití neprodukčních prostředí v době implementace i provozu bude upřesněn ve spolupráci Dodavatele s Objednatelem v Etapě 1A (Návrh architektury řešení, Testovací strategie).

Zátěžové testy budou provedeny na budoucím Produkčním prostředí před spuštěním ostrého provozu, nebo na Pre-produkčním prostředí s dočasně realokovanými HW zdroji z budoucího Produkčního prostředí.

3.3 Standardy a stavební bloky SPCSS

Standardy služeb a stavebních bloků výpočetního výkonu a diskového úložiště SPCSS uvedené v této kapitole jsou pro Dodavatele závazné.

3.3.1 Specifikace NDC

Národní datové centrum (NDC) SPCSS se nachází na adrese Na Vápence 915/14, Žižkov, 130 00 Praha 3. Hlavní parametry NDC jsou prostředí dle normy TIER III ANSI/TIA – 942/the Uptime Institute a možnost provádění servisních prací za plného provozu datového centra SPCSS bez dopadu na zákazníky a jejich zařízení. NDC nabízí redundanci všech kritických systémů a fyzickou bezpečnost, která je zajišťována nepřetržitou fyzickou ostrahou a evidencí vstupu a monitoring oprávněných osob uvnitř datového centra.

Druhé datové centrum NDC Zeleneč je ve výstavbě a bude v provozu od roku 2019. NDC Zeleneč bude připojeno dostatečnou kapacitou pro zajištění LAN a SAN konektivity mezi lokalitami. Vzdálenost NDC Zeleneč bude dostatečně malá pro použití mechanismů synchronní replikace diskových polí.

Pro podporu geografické redundance, požadované pro Dozorovou část, zajistí SPCSS dočasné umístění systémů určených pro druhé DC v oddělené místnosti s plně nezávislou podporou na všech úrovních (napájení, chlazení, síťové připojení) a výhledově přesun do druhé lokality. Využití druhé lokality je možné pro všechny části řešení podle návrhu Dodavatele, nejen pro Dozorovou část.

3.3.2 Bezpečné propojení a připojení do Internetu

SPCSS provozuje síťovou infrastrukturu včetně telekomunikačních linek a aktivních síťových bezpečnostních prvků, zahrnující redundantní připojení do internetu a NIXu s vlastním AS, propojení do CMS a KIVS, propojení do resortních sítí (GOVBONE), ochranu proti DoS a DDoS útokům, ochranu proti síťovým útokům (IPS, IDS), SSL terminátory (SSL akcelerátory, SSL off-loadery), síťové firewally, webový aplikační firewall (WAF), load balancery.

Součástí síťové infrastruktury SPCSS jsou rovněž standardní síťové služby NTP, DNS, e-mail a VPN (vzdálený přístup). Síťová infrastruktura SPCSS je plně integrována do provozního a bezpečnostního monitoringu SPCSS. Část návrhové, implementační a provozní dokumentace síťové infrastruktury SPCSS je chráněna v režimu utajovaných informací stupně Vyhrazené dle Zákona o ochraně utajovaných informací.

Síťová infrastruktura SPCSS při redundantním návrhu komponent výpočetního výkonu a diskového prostoru splňuje požadavky na celkovou dostupnost systému 99,982%.

Bezpečnostní standardy SPCSS obecně nevyžadují šifrování vnitřních komunikací, šifrovaná komunikace na vnitřních sítích se používá ve vybraných případech podle bezpečnostních požadavků příslušného IS (viz kapitolu 5.3 této přílohy Smlouvy)

Primární úroveň antivirové ochrany je předpokládána na aplikační úrovni a je zajišťována Dodavatelem jako součást Plnění.

3.3.3 Poskytování výpočetního výkonu

SPCSS provozuje v rámci svých služeb privátní cloud formou IaaS. Standardem je platforma x86, 64bit. Privátní cloud je rozdělen do dvou datových center (DC1, DC2), v každém datovém centru je dále rozdělen do dvou virtualizačních domén umístěných na oddělených HW platformách. V oblasti virtualizace jsou podporovány technologie KVM, VMware a MS Hyper-V. Licence virtualizačního software jsou součástí služby SPCSS. Součástí služby jsou i aktualizace verzí virtualizačního software.

Stavební bloky výpočetního výkonu umožňují tři plány alokace vCPU a vRAM: Plán A pro standardní aplikace optimálně zohledňující poměr vCPU a vRAM a dále plán B pro procesorově náročnější aplikace a plán C pro paměťově náročné aplikace. Níže uvedená tabulka blíže specifikuje konfiguraci základních výpočetních bloků pro jednotlivé plány:

	Procesor	Počet vCPU (core)	vRAM (GB)
Plán A	E5-2630 v3 (Haswell) 3.2GHz	1	4
Plán B	E5-2698 v3 (Haswell) 3.6GHz	1	2

Plán C	E5-2698 v3 (Haswell) 3.6GHz	1	8

Každý plán je daná kombinace vCPU a vRAM. Zdroje požadované pro virtuální instanci jsou pak násobkem základního výpočetního bloku. V případě, že požadovaný poměr počtu vCPU a GB vRAM nevyhovuje jednomu z uvedených plánů (např. poměr 1:3), je nutno použít nejbližší vhodný plán a jeho násobek pokrývající jak potřeby vCPU, tak vRAM (v uvedeném příkladu to mohou být 2 bloky v plánu B nebo 1 blok v plánu A).

Pro účely nacenění licencí SW produktů s licenční politikou vázanou na počet CPU patic může Dodavatel předpokládat 8 core na CPU a 2CPU na fyzický server.

Všechny plány využívají stejnou síťovou infrastrukturu a mají shodný síťový profil. Virtualizované bloky výpočetního výkonu je možno použít ve všech bezpečnostních zónách včetně DMZ.

Pro potřeby návrhu a zajištění požadované dostupnosti a geografické redundance Dodavatel pro každou virtuální instanci specifikuje hodnotu následujících parametrů (výběrem z hodnot uvedených v tabulce):

Parametr	Hodnoty	Vysvětlení
Lokalita	DC1/DC2	Umístění na virtualizační platformě v datovém centru DC1 (primární lokalita) nebo DC2 (záložní lokalita)
Redundance	Ne/Doména/DC	Typ redundance výpočetního výkonu realizované interně v rámci jednoho stavebního bloku výpočetního výkonu na úrovni virtualizace: **Ne – dostupnost 99,5%** ročně - nemá alokovaný výpočetní výkon pro pasivní zálohu, nebo má alokovaný výkon pro pasivní zálohu v rámci jedné virtualizační domény (není garantováno umístění na jiném HW) **Doména – dostupnost 99,982%** ročně - má alokovaný výpočetní výkon pro pasivní zálohu v jiné virtualizační doméně (garantováno umístění na jiný HW) ve stejném datovém centru **DC – dostupnost 99,99%** ročně - má alokovaný výpočetní výkon pro pasivní zálohu v jiném datovém centru *Poznámka:* alokovaný výpočetní výkon pro pasivní zálohu umožňuje migraci virtuální instance v případě výpadku HW na jiný server virtualizační farmy ve stejné nebo jiné lokalitě prostředky virtualizační platformy

V oblasti operačních systémů jsou podporovány operační systémy MS Windows Datacenter 2012 a novější a Red Hat Enterpise Linux verze 7.0 a novější, SUSE Linux Enterprise Server 12 SP2 a novější. Licence OS jsou součástí služby SPCSS (nebo pořízeny Objednatelem). Části řešení vyvíjené na zakázku (tj. mimo SW produkty) musí být nezávislé na konkrétní verzi operačního systému, resp. podporující nejnovější verze OS.

Pro účely návrhu technické infrastruktury v Příloze č. 8 Smlouvy a pro účely hodnocení nákladů životního cyklu veřejné zakázky jsou definovány Zjednodušené stavební bloky a Cenové jednotky. Jejich mapování na stavební bloky popsané v této kapitole určuje následující tabulka:

Cenová jednotka	Zjednodušený stavební blok	Smluvně závazné parametry
Core Windows neredundantní	Core Windows neredundantní	OS Windows, Redundance Ne
Core Windows redundantní	Core Windows lokálně redundantní	OS Windows, Redundance Doména
	Core Windows DC redundantní	OS Windows, Redundance DC
Core Linux neredundantní	Core Linux neredundantní	OS Linux, Redundance Ne
Core Linux redundantní	Core Linux lokálně redundantní	OS Linux, Redundance Doména
	Core Linux DC redundantní	OS Linux, Redundance DC

V kapitole 3.4 Přílohy č. 8 Smlouvy jsou uvedeny závazné celkové součty jednotlivých Cenových jednotek pro všechna prostředí dohromady. Tyto hodnoty jsou závazné dle odst. 3.8 a 13.2.14 Smlouvy. V ostatních

kapitolách Přílohy č. 8 Smlouvy jsou smluvně závazné pouze údaje o počtu Zjednodušených stavebních bloků pro jednotlivá prostředí a jejich Lokalita (DC1/DC2). Ostatní parametry stavebních bloků výpočetního výkonu uvedené v této kapitole (např. přesný typ a verze OS, plán alokace vRAM) mohou být ve spolupráci se SPCSS upřesněny v rámci Návrhu architektury řešení v Etapě 1A. Pro tento detailní návrh budou Dodavateli k dispozici všechny výše uvedené parametry a případně i možnost odvození dalších optimalizovaných parametrů (např. plánů alokace vRAM), které nemají vliv na Smluvně závazné parametry, pokud to technické podmínky SPCSS dovolí.

3.3.4 Poskytování diskového prostoru

SPCSS poskytuje následující služby diskových polí (stavební bloky diskového prostoru):

Kód jednotky	Název jednotky (nemusí se shodovat se skutečným účelem)	Popis
STOR1	Produktivní pole	Rychlá high-end storage. Pro soubory o velikosti 500 GB pole dosahuje min. **15 000 IOPS pro zápis a 35 000 IOPS** pro čtení a a propustnost **2000 MB/s.** Doba doručení změn je do 10% 5 dní, nad tento limit 40 pracovních dní. STOR1 podporuje využití flash disků, včetně dedikování určité flash-only diskové kapacity.
STOR2	Sekundární pole	Non high-end storage. **Nejsou poskytovány garance propustnosti nebo IOPS**. Průměrné hodnoty jsou až 10 000 IOPS na 250GB pro zápis a propustnost 650 MB/s. Doba doručení změn je do 10% 5 dní, nad tento limit 40 pracovních dní.
BACK	Backup pole	Uložená data s přenosem po Ethernetu, rychlost obnovy 100GB/h a vyšší. Pro soubory o velikosti 250 GB pole dosahuje 10 000 IOPS pro zápis
BACK2	Backup/Restore normal	Uložená data s přenosem výhradně po ethernetu, rychlost 11GB/h
BACK3	Longterm Backup/Restore	Uložená data s retencí 1 rok a delší pro dlouhodobé archivace.

Pro potřeby návrhu a zajištění požadované dostupnosti a geografické redundance Dodavatel pro každý diskový prostor na STOR1 nebo STOR2 specifikuje hodnotu parametrů (výběrem z hodnot uvedených v tabulce):

Parametr	Hodnoty	Vysvětlení
Lokalita	DC1/DC2	Umístění v datovém centru DC1 (primární lokalita) nebo DC2 (záložní lokalita)
Redundance	Ne/Lokální/DC	Typ redundance diskového prostoru realizované interně v rámci jednoho stavebního bloku diskového prostoru na úrovni diskových polí **Ne – dostupnost 99,5%** ročně - nemá alokovanou záložní kopii dat na jiném diskovém poli **Lokální – dostupnost 99,982%** ročně - asynchronně nebo synchronně replikovaná záložní kopie dat na jiném diskovém poli ve stejném DC **DC – dostupnost 99,99%** ročně - asynchronně nebo synchronně replikovaná záložní kopie dat na diskovém poli v jiném datovém centru *Poznámka:* replikovaná záložní kopie dat na jiném diskovém poli umožňuje v případě výpadku HW přepnutí na záložní kopii prostředky diskové nebo virtualizační platformy. V případě propojení stavebních bloků výpočetního

		výkonu a diskového prostoru s parametrem redundance DC jsou v případě výpadku lokality automaticky propojeny i záložní kopie těchto jednotek.

Replikace dat na úrovni diskových úložišť je k dispozici, a to synchronní i asynchronní replikace mezi poli. Propustnost replikační linky je 8 Gbit.

Pro účely návrhu technické infrastruktury v Příloze č. 8 Smlouvy a pro účely hodnocení nákladů životního cyklu veřejné zakázky jsou definovány Zjednodušené stavební bloky a Cenové jednotky. Jejich mapování na stavební bloky popsané v této kapitole určuje následující tabulka:

Cenová jednotka	Zjednodušený stavební blok	Smluvně závazné parametry
GB disky neredundantní	GB disky neredundantní	Redundance Ne
GB disky redundantní	GB disky lokálně redundantní	Redundance Doména
	GB disky DC redundantní	Redundance DC

Zjednodušené stavební bloky diskového prostoru, a tedy i Cenové jednotky, se použijí jak pro datová úložiště pro DMS a všechny DB AISG, tak i pro systémové disky serverů. Systémovými disky jsou rozuměny diskové prostory jednotlivých virtuálních serverů pro uložení souborů operačního systému, instalace a konfigurace aplikací, lokální dočasné soubory a logy apod. Tyto bloky se nepoužijí pro paměť RAM, která se tedy nezahrnuje do těchto Cenových jednotek.

V kapitole 3.4 Přílohy č. 8 jsou uvedeny závazné celkové součty jednotlivých Cenových jednotek pro všechna prostředí dohromady. Tyto hodnoty jsou závazné dle odst. 3.8 a 13.2.14 Smlouvy. V ostatních kapitolách Přílohy č. 8 Smlouvy jsou smluvně závazné pouze údaje o počtu Zjednodušených stavebních bloků pro jednotlivá prostředí a jejich Lokalita (DC1/DC2). Ostatní parametry stavebních bloků diskového prostoru uvedené v této kapitole (např. typ jednotky z pohledu rychlosti a propustnosti, způsob replikace redundantních jednotek) mohou být ve spolupráci se SPCSS upřesněny v rámci Návrhu architektury řešení v Etapě 1A. Pro tento detailní návrh budou Dodavateli k dispozici všechny výše uvedené parametry a případně i možnost odvození dalších optimalizovaných parametrů (např. kombinovaná alokace rychlých a pomalých disků), které nemají vliv na Smluvně závazné parametry, pokud to technické podmínky SPCSS dovolí.

3.3.5 Správa operačních systémů

Instalaci, konfiguraci a správu operačních systémů na úrovni fyzických i virtuálních serverů provádí SPCSS. Administrátorské účty OS jsou v rukách SPCSS. Dodavatel používá pro implementaci a podporu provozu Aplikace (včetně databází) uživatelské účty, využití administrátorských účtů je možné pouze se součinností SPCSS nebo bezpečným mechanismem schváleným SPCSS (např. sudo s nastavením specifických povolených příkazů). Dodavatel musí navrhnout implementaci Aplikace a SW produktů tak, aby eliminoval, respektive snížil na minimální nutnou úroveň, nutnost použití administrátorských účtů při provozní podpoře Aplikací a SW produktů.

Licence OS a virtualizačního software jsou součástí služby SPCSS (nebo pořízeny Objednatelem). Součástí správy operačních systémů je provedení aktualizací verzí OS. Aktualizace OS a virtualizačního software bude plánována ve spolupráci s Dodavatelem a Objednatelem.

Součástí služby SPCSS není dodávka, implementace a správa aplikačních komponent operačních systémů, respektive nadstavbových SW produktů a licencí přibalených k základnímu OS, jako jsou například web servery, aplikační servery, middleware nebo adresářové služby pro účely správy aplikačních uživatelů, ani případné SW licence, maintenance a subskripce s nimi spojené.

3.3.6 Správa databází

Instalaci a prvotní konfiguraci databází (rozuměno databázové SW produkty a jejich konfigurace) provede Dodavatel. Správu databází bude provádět SPCSS. K administrátorským účtům databází a účtům vlastníků

schémat bude mít v době provozu přístup pouze SPCSS. Dodavatel může použít pro implementaci a podporu Aplikace (včetně databází) uživatelské účty, využití administrátorských účtů a účtů vlastníků schémat je možné pouze se součinností SPCSS. Dodavatel musí navrhnout implementaci databází a Aplikace obecně tak, aby eliminoval, resp. snížil na minimální nutnou úroveň nutnost použití administrátorských účtů a účtů vlastníků schémat při provozní podpoře aplikací.

Součástí správy databází je provedení aktualizací verzí databázových SW produktů. Aktualizace databázových SW produktů bude plánována ve spolupráci s Dodavatelem a Objednatelem.

Licence databázových SW produktů nejsou součástí služby SPCSS, licence, maintenance a/nebo subskripce databázových SW produktů potřebných pro implementaci a provoz AISG jsou součástí Plnění Dodavatele a musí být uvedeny v seznamu SW produktů a licencí.

3.3.7 Zálohování a archivace dat

Služba je poskytována SPCSS v rozsahu uvedeném v backup plánech, jejichž návrh je odpovědností Dodavatele. Backup plán musí obsahovat minimálně následující údaje:

a) co se zálohuje (diskové prostory, vybrané adresáře, databázové prostory)
b) co se nemá zálohovat (výjimky)
c) kdy se zálohuje (čas spuštění zálohy a frekvence opakování)
d) typ zálohy (plná, přírůstková, differential a podobně)
e) retence dat (jak dlouho budou data uložena)

Mezi další požadavky, z nichž některé jsou součástí nefunkčních požadavků uvedených v kapitole 5 této přílohy Smlouvy, patří například držení dat ve více kopiích, specifikace RTO (jak rychle musí být data obnovena), specifikace RPO (maximální povolená doba ztráty dat), časové omezení backup okna (záloha musí doběhnout do tří hodin po startu) a podobně.

Služba je poskytována pomocí software Tivoli Storage Manager (dále jen TSM). Licence zálohovacího systému jsou součástí služby. Součástí služby jsou i aktualizace verzí zálohovacího software. Aktualizace zálohovacího software bude plánována ve spolupráci s Dodavatelem a Objednatelem.

Pásky mohou být na vyžádání vyjmuty a uloženy do trezorů, umístněných v samostatných trezorových místnostech v oddělené režimové zóně. TSM servery a jejich disková pole jsou umístněné v oddělených režimových zónách od páskových knihoven. Každá z uvedených zón je současně samostatným požárním úsekem vybaveným SHZ a EPS s odpovídajícím zajištěním fyzické bezpečnosti.

3.3.8 CKB, SOC a bezpečnostní monitoring

Služby centra kybernetické bezpečnosti (CKB) a Security operation centra (SOC) zajišťují provozní služby kybernetické bezpečnosti systémů a sítí v souladu se standardy ČSN ISO/IEC 27000 a Zákonem o kybernetické bezpečnosti (ZKB), včetně detekce, řešení a hlášení bezpečnostních incidentů. Součástí standardních služeb SPCSS v oblasti bezpečnostního monitoringu je i dohledový systém typu SIEM, který odpovídá požadavkům zákona 181/2014 Sb. na úrovni kritické informační infrastruktury (SPCSS jako podnik je prvkem KII).

Dodavatel navrhne a implementuje metriky bezpečnostního monitoringu na aplikační úrovni a společně s SPCSS zajistí jejich integraci do monitoring nástrojů SPCSS. Integrace bezpečnostního monitoringu na aplikační úrovni bude provedena formou logování. Licence systému bezpečnostního monitoringu jsou součástí služby SPCSS. Část návrhové, implementační a provozní dokumentace CKB a bezpečnostního monitoringu je chráněna v režimu utajovaných informací stupně Vyhrazené dle Zákona o ochraně utajovaných informací.

3.3.9 Provozní monitoring infrastruktury a služeb

SPCSS poskytuje dohled infrastruktury v režimu 7x24 v podobě proaktivního monitoringu stavu serverů a datových sítí na různých úrovních, včetně měření Service Level Agreement (dále jen „SLA“). Systém

provozního monitoringu je integrován do ServiceDesku SPCSS (dále jen „SD SPCSS“), který zajistí řešení procesů Incident managementu.

Požadavky na logování a monitoring na aplikační úrovni budou definovány ve fázi Analýzy. Dodavatel navrhne a implementuje systém logování Aplikace a SW produktů v souladu s bezpečnostními a provozními požadavky SPCSS. Dodavatel navrhne a implementuje nástroje provozního a bezpečnostního monitoringu na aplikační úrovni a společně s SPCSS zajistí jejich integraci do nástrojů provozního monitoringu SPCSS.

SPCSS používá nástroje provozního monitoringu od firmy CA. Licence monitoring systému jsou součástí služby SPCSS.

Přímý přístup Dodavatele do nástrojů provozního monitoringu není standardně poskytován, primární nástroj pro komunikaci s Dodavatelem je ServiceDesk SPCSS. V rámci přípravy provozní dokumentace budou ve spolupráci Dodavatele a SPCSS navrženy způsoby předávání informací z monitoringu potřebné pro řešení problémů a analýzy stavu AISG.

4 Licence a subskripce SW produktů

Licence software na úrovni operačních systémů, virtualizace, zálohování a monitoringu jsou součástí Technické infrastruktury a jsou dodávány jako součást provozních služeb SPCSS.

Všechny SW produkty nad úrovní Technické infrastruktury, potřebné pro vybudování a provoz AISG, včetně aplikačních serverů, middleware a databází, jsou považovány za SW produkty na aplikační úrovni a jsou součástí Díla. Pokud budou součástí Díla licence SW produktů Microsoft, musí být kompatibilní s podporovanou verzí OS (Datacenter edition).

5 Nefunkční technické požadavky

5.1 Dozorová část

ID	Kategorie požadavků	Požadavek	Hodnota/popis
RT6	Performance	Response times - doba od přijetí dotazu na úrovni vnitřní sítě po dobu, kdy odpověď systému opouští vnitřní síť (doba zpracování v AISG, tj. doba odpovědi externích systémů se nezapočítává).	1 s Povinnost dodržení hodnoty odezvy do 1s pro 90% požadavků a zároveň nepřekročení průměrné hodnoty odezvy do 1s pro 100% požadavků.
RT8	Performance	Počet konkurentních připojení - omezení na úrovni webových serverů (maxConnections limit). Nepředpokládá se existence trvalého otevření spojení mezi provozovateli a AISG.	1000
RT9	Kapacita	Propustnost - kolik hráčů musí systém zvládnout ověřit a/nebo registrovat	200 000 hráčů za 1 hodinu
RT10	Kapacita	Úložiště – maximální čistá datová kapacita úložného prostoru bez záloh, redundancí dat a overheadu uložení na úložištích	První rok: 1 TB (včetně záznamů o transakcích a změnách), rozdělení mezi DB hráčů a DB vyloučení je předpokládáno v poměru 1:3 *Pozn.: v 1 roce provozu se předpokládá rozsáhlá registrace hráčů, zatímco náběh ověřování hráčů oproti DB vyloučení bude pozvolný*
RT11	Kapacita	Požadavky na meziroční nárůsty	Každý další rok 1TB (včetně záznamů o transakcích a změnách), rozdělení mezi DB hráčů a DB vyloučení je předpokládáno v poměru 1:8 *Pozn.: výpočet celkové čisté datové kapacity úložiště Dozorové části za 5 let provozu je tedy: 1 + 1 + 1 + 1 + 1 = 5TB, z toho:* *DB hráčů: 0,25 + 0,11 + 0,11 + 0,11 + 0,11 = 0,69 TB* *DB vyloučení: 0,75 + 0.89 + 0,89 + 0,89 + 0,89 = 4,31 TB (záznamy o transakcích budou tvořit 90% z velikosti DB vyloučení)*
RT13	Dostupnost (Availability)	V jakých lokalitách musí být systém dostupný	EU/EHP
RT16	Integrita	Zachytávání chyb - postup při výpadku nebo chybě části systému	systém musí být vysoce dostupný
RT17	Integrita	Zachytávání chybných dat - postup při detekci chyb v datech	eliminace vhodným návrhem systému a nastavením integritních omezení, po zachycení chybných dat následuje provedení analytického rozboru na straně dodavatele
RT18	Integrita	Integrita dat - způsob zajištění integrity dat	zajištěna bude kontrolou
RT19	Obnova	RTO - jak rychle musí být data obnovena	1,5 h pro všechna data kromě záznamů o transakcích v DB vyloučení

ID	Kategorie požadavků	Požadavek	Hodnota/popis
	(Recovery)		24 h pro záznamy o transakcích v DB vyloučení
RT20	Obnova (Recovery)	RPO - maximální povolená doba ztráty dat	0,5 h
RT28	Maintainability	Shoda s architekturními standardy	SOA (Service Oriented Architecture)
RT30	Maintainability	Shoda se standardy kódování	UNICODE
RT33	Archivace a skartace	Po jaké době dojde k přesunu do archivu nebo mazání dat ze systému	Data o hráčích budou udržována po dobu 5 let ode dne, kdy byl hráč z databáze vymazán, resp. pominul důvod k udržování těchto údajů v databázi. Data týkající se sebeomezujících opatření, platebních údajů a ostatní navázaná na jednotlivé provozovatele budou udržována po dobu 5 let ode dne jejich jednotlivé změny. Po uplynutí výše uvedených lhůt budou data vymazána bez požadavku archivace.
RT38	Konfigurace	Míra konfigurovatelnosti systému	parametry nesmí být napevno v kódu, ale musí být administrátorsky spravované s možností přenastavit parametry

5.2 Správní část

ID	Kategorie požadavků	Požadavek	Hodnota/popis
RT6	Performance	Response times - načítání aplikace, načítání obrazovky, čas obnovy (refresh times), atd. Doba od přijetí dotazu na úrovni vnitřní sítě po dobu, kdy odpověď systému opouští vnitřní síť (doba zpracování v AISG, tj. doba odpovědi externích systémů se nezapočítává).	max. 4 s Povinnost dodržení hodnoty odezvy do 4s pro 90% požadavků a zároveň nepřekročení průměrné hodnoty odezvy do 4s pro 100% požadavků.
RT8	Performance	Počet současně přihlášených uživatelů, kteří ale nejsou všichni současně aktivní (tj. např. čtou obrazovku).	500
RT9	Capacity	Propustnost - počet přihlášení a odhlášení uživatelů za 1 hodinu	2000
RT10	Capacity	Úložiště – maximální čistá datová kapacita úložného prostoru bez záloh, redundancí dat a overheadu uložení na úložištích	První 1 rok a 5 měsíců (migrace dat z IS SDSL + Etapa 2 + první rok provozu): 500 GB, rozdělení mezi DB správní a DMS je předpokládáno v poměru 1:2
RT11	Capacity	Požadavky na meziroční nárůsty	Každý další rok 150 GB, rozdělení mezi DB správní a DMS je předpokládáno v poměru 1:2 *Pozn.: výpočet celkové čisté datové kapacity úložiště Správní části za 5 let a 5 měsíců provozu je tedy: 500 + 150 + 150 + 150 +150 = 1100 GB, z toho:*

ID	Kategorie požadavků	Požadavek	Hodnota/popis
			DB správní: 167 + 50 + 50 + 50 + 50 = 367 GB *DMS: 333 + 100 + 100 + 100 + 100 = 733 GB*
RT13	Dostupnost (Availability)	V jakých lokalitách musí být systém dostupný	EU/EHP
RT16	Integrita	Zachytávání chyb - postup při výpadku nebo chybě části systému	není alternativa k systému a neexistuje náhradní postup
RT17	Integrita	Zachytávání chybných dat - postup při detekci chyb v datech	validace na GUI/formuláři
RT18	Integrita	Integrita dat - způsob zajištění integrity dat	zajištěna bude kontrolou
RT19	Obnova (Recovery)	RTO - jak rychle musí být data obnovena	24 h
RT20	Obnova (Recovery)	RPO - maximální povolená doba ztráty dat	24 h od poslední zálohy
RT28	Maintainability	Shoda s architekturními standardy	SOA (Service Oriented Architecture)
RT30	Maintainability	Shoda se standardy kódování	UNICODE
RT31	Usability	Standardy uživatelského rozhraní	vyhláška č. 64/2008 Sb.
RT32	Usability	Lokalizace	ČJ a části vystavené mimo MF určené pro provozovatele v ČJ a AJ
RT33	Archivace a skartace	Po jaké době dojde k přesunu do archivu nebo mazání dat ze systému	Data budou udržována po dobu 3 let ode dne účinnosti rozhodnutí nebo skončení platnosti povolení. Po uplynutí výše uvedených lhůt budou data archivována / uložena do interního archivu AISG.
RT38	Konfigurace	Míra konfigurovatelnosti systému	parametry nesmí být napevno v kódu, ale musí být administrátorsky spravované s možností přenastavit parametry

5.3 Řešení bezpečnosti

Řešení bezpečnosti (bezpečnostní návrh a dokumentace - analýza a identifikace aktiv a rizik, bezpečnostní politika, bezpečnostní dokumentace provozu) AISG jako celku je odpovědností Dodavatele. Objednatel poskytne Dodavateli platnou dokumentaci bezpečnostní politiky a relevantní směrnice MF, dále prostřednictvím SPCSS vstupy a informace o standardech provozu, bude spolupracovat na řešení bezpečnosti na úrovni infrastruktury a bude ve spolupráci s Dodavatelem implementovat a provozovat bezpečnostní monitoring.

Bezpečnostní požadavky na AISG jako celek odpovídají požadavkům na Významný informační systém (VIS) ve smyslu ust. §2 písm. d) dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů ve znění pozdějších předpisů (dále jen Zákon o kybernetické bezpečnosti, ZKB) a souvisejících vyhlášek č. 316/2014 Sb. a č. 317/2014 Sb.

Stupeň úrovně ochrany dat dle stupnice pro hodnocení důležitosti aktiv vyhlášky č. 316/2014 Sb. bude stanoven na základě schváleného bezpečnostního návrhu.

Systém řízení bezpečnosti AISG musí být navržen a implementován v souladu s normou ČSN ISO/IEC 27001. Systém řízení provozu a správy AISG musí být navržen a implementován v souladu s normou ČSN ISO/IEC 20000.

AISG a jeho dokumentace musí vyhovovat požadavkům zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů (dále jen ZOOÚ) a požadavkům obecného nařízení o ochraně osobních údajů 2016/679 (GDPR), které bude účinné od 25.5.2018.

AISG musí být odolný proti známým bezpečnostním hrozbám a útokům z vnějších i vnitřních sítí.

5.4 Logování, provozní a bezpečnostní monitoring

Dodavatel navrhne systém logování Aplikací a SW produktů dle bezpečnostních a provozních požadavků Objednatele a SPCSS. Může být požadováno logování vybraných událostí do databázového logu. Dodavatel přizpůsobí formát a identifikaci log záznamů požadavkům MF a SPCSS na následné zpracování logů.

Součástí systému logování Aplikací a SW produktů bude podrobné logování chybových stavů jednotlivých rozhraní, včetně dočasného (řádově dny) uchovávání přijatých i odesílaných zpráv mezi systémem AISG a spolupracujícími systémy.

Integrace AISG do provozního monitoringu SPCSS je požadována v takovém rozsahu, aby monitoring systém umožnil dohled provozních stavů systému a sledování plnění parametrů SLA. Vlastní implementaci monitoringu provede Objednatel prostřednictvím SPCSS. Dodavatel bude spolupracovat na analýze dohledových metrik a návrhu a implementaci metrik na úrovni Aplikace, SW produktů a Dat a společně s SPCSS zajistí jejich integraci do monitoring nástrojů SPCSS. Součástí implementace monitoringu je naplnění konfigurační databáze (CMDB). Detailní požadavky na monitoring budou definovány v rámci Etapy 1A.

Součástí provozního monitoringu bude i měření dostupnosti jednotlivých služeb a částí AISG (end-to-end monitoring), na jehož definici a implementaci bude Dodavatel spolupracovat.

Dále je požadována integrace AISG do systému bezpečnostního monitoringu SPCSS (SIEM, CKB). Vlastní implementaci bezpečnostního monitoringu provede Objednatel prostřednictvím SPCSS. Dodavatel ve spolupráci se SPCSS provede analýzu hrozeb. Dodavatel navrhne a implementuje metriky bezpečnostního monitoringu na úrovni Aplikace, SW produktů a Dat a společně s SPCSS zajistí jejich integraci do monitoring nástrojů SPCSS. Integrace bezpečnostního monitoringu na úrovni Aplikace, SW produktů a Dat bude provedena formou logování.

SPCSS aktuálně připravuje výběr vhodného nástroje pro řízení přístupových oprávnění (PAM), který plnohodnotně uspokojí požadavky zákona 181/2014 Sb. a provozní požadavky SPCSS. Pro účely zpracování nabídky může Dodavatel předpokládat existenci takového nástroje a zajištění jeho licencování jako součást služeb SPCSS.