Technická specifikace požadavků na infrastrukturu DC a poskytované služby

Tato kapitola obsahuje specifikace systému z pohledu HW a SW infrastruktury určené pro chod Agendy a také další specifikace systému jako celku a k systému poskytovaných či garantovaných služeb, především:

- Parametry architektury serverů v zabezpečeném datovém centru.
- Parametry uživatelské podpory a SLA parametry.
- Parametry poskytování maintenance.
- Servisní služby.

Součástí plnění musí být všechny služby, licence (včetně potřebných licencí a maintenance databází, operačních systémů, nástrojů pro virtualizaci a podobně) i HW komponenty tvořící řešení. Součástí plnění musí být také podpora systému jako celku v souladu s dobou trvání Smlouvy.

Poskytnuté HW a SW komponenty musí tvořit zabezpečené datové centrum v režimu minimálně TIER3 a Agenda musí být instalován na těchto komponentách v prostorách Poskytovatele (zabezpečené datové centrum vyhovující požadavkům na ochranu dat, systémů, správu přístupů a podobně). Celek musí být poskytován Uživateli a jeho oprávněným osobám v souladu s dále uvedenými parametry.

Pro ověření plnění musí být po celou dobu trvání smluvního vztahu garantován přístup oprávněných osob Uživatele do zabezpečeného datového centra v doprovodu oprávněné osoby Poskytovatele, a to včetně případného přístupu k serverům, s možností ověřit splnění níže uvedených požadavků a požadavků kladených na datová centra v režimu TIER3.

Poskytovatel předloží při podáním nabídky a vloží do smlouvy jako přílohu dokumenty prokazují:

- Certifikaci datového centra v režimu TIER3, nebo
- popis a příslušné dokumenty týkající se datového centra, ze kterých bude zřejmé, že datové centrum plní TIER3 a umožní na vyžádání oprávněným osobám Uživatele fyzickou kontrolu datového centra.

Architektura systému

Architektura systému musí vycházet ze zásad a principů servisně orientované architektury (SOA) s důrazem na silnou podporu tvorby a řízení oběhu dokumentů. Systém musí zajistit napojení na otevřená API rozhraní navazujících systémů a pro tyto systémy vystavit otevřené API v případech opačné vazby.

Prostředí Systému

Systém musí obsahovat oddělené testovací a produkční prostředí. Testovací prostředí musí běžet na jiných HW a SW prostředcích (serverech) než produkční prostředí. Testovací prostředí může běžet na prostředcích záložního systému. V případě, kdy je záložní systém využíván i pro testovací prostředí a záložní systém je využit po havárii primárního produkčního prostředí na zajištění dočasného produkčního provozu, nesmí být využíváno testovací prostředí na záložním systému vytvořené.

Produkční prostředí musí být rozdělené na samostatné aplikační a samostatné databázové servery. Každý z těchto serverů musí běžet na vlastních HW a SW prostředcích (serverech). Produkční prostředí jako celek musí být replikováno na záložní systém ve stejné lokalitě, případně geograficky oddělené lokalitě při zachování maximální bezpečnosti dat a parametrů datového centra jako v primární lokalitě. Záložní systém nesmí být provozován na stejných HW a SW prostředcích (serverech) jako primární.

Provoz produkčního a záložního systému bude standardně realizován v režimu Active/Passive.

Řešení musí provádět replikaci dat do záložního systému. Data na záložní server jsou přenášena průběžně, přičemž záloha dat z produkčního systému nesmí být starší více jak 60 minut. Záložní systém musí disponovat minimálně 50% výkonu z pohledu uživatelské odezvy systému oproti primárnímu systému.

V případě výpadku primárního systému musí být provoz přesměrován na záložní systém do jednoho pracovního dne od zjištění a nahlášení takového výpadku ze strany oprávněných osob Uživatele Poskytovateli.

Testovací prostředí musí být konfiguračně shodné s provozním prostředím. Testovací prostředí nemusí disponovat stejným výkonem (z pohledu výpočetního výkonu a diskového prostoru) jako provozní prostředí. Výpočetní výkon a diskový prostor musí být pro testovací prostředí vždy realizován v rozsahu odpovídajícím potřebám provádění testů systému s využitím testovacího prostředí.

Výkon systému

Výkon systému musí po celou dobu poskytování systému odpovídat počtu reálně zpracovávaných přestupků (spisů a k nim příslušných dat) a celkovému rozsahu uložených a zpracovávaných dat a musí být průběžně výkonově škálován v návaznosti ne reálný počet a stav řešení přestupků.

Délka doby odezvy systému při produkčním zatížení musí odpovídat běžným zvyklostem obdobných informačních systémů a bude měřena na straně serveru. Do odezvy systému se nezapočítává čas (režie) daná integracemi na navazující systémy třetích stran, přičemž se nezapočítává prokazatelná doba na vyřízení požadavku systému vůči těmto navazujícím systémům od odeslání požadavku do přijetí odpovědi.

Měření odezvy systému bude probíhat v průběhu řádného provozu. Řešení musí garantovat odezvy při založení/úpravě/zrušení jednoho záznamu v jednotkách sekund (na straně poskytnutého systému).

Vícenásobné operace musí být prováděny na pozadí bez omezení ostatních funkcí systému a práce oprávněných osob Uživatele v Agendě.

Systém musí garantovat stabilní provoz. Případné dlouhodobější odstávky (např. servisní zásahy, upgrade apod.) jsou přípustné pouze mimo provozní dobu.

Výkon systému musí garantovat, že v průběhu provozu systému nedochází k prodlužování doby odezev na jednotlivé funkcionality systému.

Spolehlivost a dostupnost systému ADP

Provoz systému se, z pohledu spolehlivosti chodu a dostupnosti Agendy (spolehlivost a dostupnost HW komponent datového centra je samostatně definovaná požadavkem na režim TIER3) a návazných SLA parametrů, může nacházet v jednom ze tří následujících stavů:

- **V provozu** - systém je v provozu v případě, že se oprávněné osoby Uživatele mohou do systému přihlásit a využívat veškeré funkcionality, které jsou předmětem technické specifikace, nebo je pro nedostupné funkcionality (např. z důvodu jejich chyby) nabídnuto náhradní řešení umožňující dosažení shodného výsledku jako v případě, kdy by oprávněné osoby Uživatele mohly tyto funkcionality využít.
- **Mimo provoz** - systém je mimo provoz v případě, že se oprávněné osoby Uživatele nemohou přihlásit do systému

- **Omezení funkcionality** - systém se nachází v stavu „omezení funkcionality“, když nejsou splněny podmínky ani pro jeden z předešlých stavů

Systém nabývá "omezení funkcionality" či stavu "mimo provoz" v případě, kdy alespoň jedna oprávněná osoba Uživatele (nebo případná automatická pravidelná kontrola systému) identifikuje nedostupnost funkcionality systému nebo systému jako celku, tento stav nahlásí Poskytovateli a zároveň tento stav není způsoben oprávněnou osobou Uživatele (tj. oprávněná osoba splňuje veškeré náležitosti pro přístup a práci se systémem).

Systém musí být, včetně HW infrastruktury a provozních postupů, navržen a vytvořen tak, aby umožnil zajištění následujících parametrů dostupnosti:

- Dostupnost produkčního prostředí bude v obvyklé pracovní době (pracovní dny od 07:00 do 16:00) 98%.
- Dostupnost produkčního prostředí bude mimo obvyklou pracovní dobu 95%.

Systém bude považován za nedostupný v době trvání systémového stavu "mimo provoz" a "omezení funkcionality" od okamžiku oprávněného nahlášení nedostupnosti či nesprávné funkčnosti oprávněnou osobou Uživatele Poskytovateli až do okamžiku obnovení provozu nebo nabídnutí náhradního řešení pro nedostupnou či nesprávně fungující funkcionalitu systému.

Celková plánovaná doba dostupnosti je definována jako počet hodin v daném kalendářním měsíci. Servisní okno systému bude stanoveno od 22:00 do 24:00 v pracovní den a od 00:00 do 24:00 v den pracovního klidu.

V rámci hlášení poruch a problémů se musí evidovat každé hlášení nedostupnosti systému s informací, zda se jednalo o oprávněné či neoprávněné hlášení. Poskytovatel je povinen tyto informace zpřístupnit oprávněným osobám Uživatele. Hlášení poruch a závad ze strany oprávněných osob Uživatele, stejně jako dalších požadavků souvisejících se službou podpory a servisu, bude možné elektronicky a telefonicky na definované kontaktní údaje dle Smlouvy, případně s využitím vhodných technických prostředků Poskytovatele na základě dohody s Uživatelem v rámci předimplementační analýzy.

Dostupnost oprávněných osob Poskytovatele, nebo technického prostředku dle shora řečeného, musí být pro potřeby hlášení poruch, závad a požadavků pro oprávněné osoby Uživatele minimálně v pracovní době od 07:00 do 16:00, přičemž reakční čas Poskytovatele na oprávněné požadavky Uživatele definují SLA parametrů.

SLA parametry

Priorita	Charakteristika problému	Doba vyřešení požadavku od jeho nahlášení
Havárie	Systém nelze spustit nebo dochází ke ztrátě dat, nebo systém lze spustit, ale nefunguje některá z klíčových funkcí (přijetí měření, validace měření, přijetí podnětu, zobrazení detailu měření či případu, generování dokumentů, apod.) a neexistuje dočasné náhradní řešení, nebo	2 pracovní dny

	existují zásadní problémy s výkonem klíčových funkcí systému	
Porucha	Nefunguje některá z méně důležitých funkcí systému (úpravy v nastavení, číselnících a organizační struktuře, notifikace, tiskové výstupy, apod.), nebo Existují problémy s výkonem u důležitých funkcí systému (vyhledávání, hromadné úpravy záznamů, hromadné operace apod.)	1 pracovní týden
Chyba	Ostatní problémy	2 pracovní týdny

Poznámka: Požadavky v rámci SLA parametrů je možné hlásit v rozmezí od 07:00 až 16:00 každého pracovního dne. Na požadavek vznesený mimo tuto lhůtu se bude pohlížet jako na požadavek vznesený na začátku nejbližšího pracovního dne.

Za vyřešení se považuje i takový zásah, který způsobí změnu priority problému na menší.

Pokud nastane souběh požadavku s prioritou Havárie s požadavky s prioritou Porucha (resp. Chyba), má řešení požadavku s prioritou Havárie přednost před ostatními požadavky. Doba řešení požadavků s prioritou Porucha a Chyba bude automaticky prodloužena o dobu řešení požadavku s prioritou Havárie.

Požadavky na bezpečnou identifikaci a autorizaci přístupů uživatelů do systému:

- Identifikace a autorizace fyzických osob – použití kombinace jméno a heslo spolu s ověřením IP adresy nebo s využitím zabezpečené VPN.
- Definice přístupových práv daného uživatele k jednotlivým měřením a případům a návazným dokumentům a datům v rámci rolí v systému.
- Víceúrovňová správa systému (nastavení uživatelů, skupin a jejich rolí).
- Identifikace a autorizace navazujících informačních systémů – například použití kombinace serverový certifikát a IP adresa.

Po přihlášení budou uživateli přidělena přístupová práva na základě předem definovaných pravidel. Identifikace (činnost) přihlášeného uživatele bude po celou dobu práce uživatele v systému zaznamenána/logována.

Požadavky na uditovatelnost provedených úkonů

Systém musí zaznamenat veškeré operace:

- Prováděné uživateli prostřednictvím GUI systému – uživatelé mohou k datům přistupovat pouze tímto způsobem
- Související s činností systému - data mohou být v souladu s touto technickou specifikací měněna také automaticky systémem

- Související s komunikací s okolními IS – tato komunikace může být realizována pouze prostřednictvím webových služeb
- Prováděné následně Poskytovatelem při zajišťování provozu systému – systém neumožňuje jakoukoli modifikaci dat, aniž by došlo k zaznamenání o data a času modifikace dat o identifikace osoby, která změnu dat provedla o původní hodnoty dat o nové hodnoty dat (Poskytovatel nemá vliv na provádění měření, rozsah měření a počet měření, veškeré zásahy Poskytovatele souvisí výhradně se servisní činností a jsou prováděny na základě pokynů Uživatele).

Požadavky na důvěrnost a integritu dat

Systém musí být navržen a implementován s ohledem na vysokou míru zabezpečení celého řešení. Bude-li systém připojen přímo na Internet, musí řešení obsahovat firewally pro vytvoření demilitarizované zóny (DMZ). Síťový firewall musí poskytovat stavovou inspekci protokolu http. Žádný neprověřený provoz nesmí být vpuštěn na aplikační servery, kde bude prováděn přístup do datové vrstvy. Musí být zajištěn zabezpečený individuální přístup prostřednictvím Internetového prohlížeče.

Systém musí garantovat, že:

- Systémem uchovávaná data nemohou být zpřístupněna neautorizovaným osobám, přičemž přístup a veškerá manipulace s daty musí je zaznamenávána.
- Data nejsou a nemohou být během komunikace odposlouchávána či pozměněna neautorizovanou stranou, přičemž pro komunikaci mezi uživatelem a systémem je použit zabezpečený komunikační protokol min. SSL verze 3.0 nebo TLS verze 1.1.
- Systémem uchovávaná data nelze změnit nebo poškodit neautorizovanou stranou.

Požadavky na přístup do systému

Přístup k funkcionalitám systému musí být zajištěn pro standardní PC prostřednictvím běžného webového prohlížeče. Za standardní PC se považuje PC s OS Windows XP a vyšším plus odpovídající verzí prohlížeče Internet Explorer a Mozilla Firefox, případně Chrome.

Pro shora pospané PC musí být dostupné funkcionality systému v plné šíři.

Požadavky na uživatelskou podporu

Poskytovatel musí vždy řešit oprávněné požadavky Uživatele v rámci provádění školení oprávněných osob Uživatele a především v rámci garance bezchybného provozu systému, respektive odstraňování všech vad, chyb a poruch, které během provozu systému nastanou a jsou zaviněny poskytnutým systémem či činností Poskytovatele systému. V případě, kdy vada, chyba či problém vznikne mimo poskytnutý systém (typicky například neohlášená změna API rozhraní systému třetí strany), nezapočítává se čas nutný k nalezení a nápravě do času supportu.

Support se musí vztahovat na podporu všech dotčených částí systému v rozsahu specifikovaném v příslušných přílohách s popisem specifikací konkrétních částí systému, nebo v rozsahu níže uvedeném, pokud pro dotčenou část systému není uvedeno samostatně jinak.

Součástí plnění musí být dále poskytování servisních prací zahrnujících řešení problémů s provozem programového vybavení, konzultace k používání programového vybavení, reinstalace programového

vybavení, instalace nových verzí, meziverzí či hotfix, obnova programového vybavení po havárii, na základě zadavatelem předaných záloh, provoz poradenské služby pro oprávněné osoby Uživatele.

Poskytovatel musí zajistit průběžnou údržbu veškeré dokumentace vztahující se k programovému vybavení

Legislativní maintenance

Součástí plnění musí být poskytování legislativní maintenance na všechny dotčené části systému v rozsahu specifikovaném v příslušných přílohách s popisem specifikací konkrétních částí systému, nebo v rozsahu níže uvedeném, pokud pro dotčenou část systému není uvedeno samostatně jinak.

Poskytovatel musí zajistit update veškerého provozovaného hardware i software/firmware vyplývající z dalšího vývoje programových a technických produktů. V případě legislativních změn souvisejících s obecně závaznými právními předpisy bude součástí plnění poskytnutí update programového či hardwarového vybavení nejpozději do data nabytí jejich účinnosti. Součástí plnění musí být také průběžná údržba veškeré dokumentace vztahující se k programovému i hardwarovému vybavení.

Počet oprávněných osob ze strany Uživatele systému

Licence poskytnuté k systému a řešení jako celku nesmí být omezeny počtem oprávněných osob z řad Uživatele a Poskytovatel vždy na žádost Uživatele doplní či aktualizuje oprávněné osoby a jejich role a oprávnění v systému do 2 kalendářních dnů od doručení žádosti Uživatele.

Licence nesmí omezit počet připojených měřících zařízení či původců dat, tedy poskytnutý systém musí být schopen přijmout a zpracovat data o přestupcích (měření rychlosti) i z jiných měřících zařízení, které Uživatel či jiné město/obec se správním orgánem v gesci Uživatele, pořídí. Přičemž ale platí, že každé takové zařízení musí být schopno na určenou webovou službu, nebo alespoň určené úložiště, zaslat datovou větu s daty o přestupku (standardní XML) a k tomu navázaný ZIP balíček obsahující kompletní fotodokumentaci přestupku v rozsahu, v jakém jsou data a fotografie specifikovány platnou legislativou.