

Příloha č. 2

Specifikace řešení a služeb

Tato kapitola obsahuje veškeré specifikace systému z pohledu HW a SW infrastruktury určené pro chod informačního systému řešení dopravních přestupků ADP 2.5 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 jsou všechny služby, licence (včetně potřebných licencí a maintenance databází, operačních systémů, nástrojů pro virtualizaci a podobně) i HW komponenty tvořící řešení. Součástí plnění je také podpora systému jako celku v souladu s dobou trvání smlouvy.

HW a SW komponenty tvořící zabezpečené datové centrum a informační systém SW ADP jsou umístěny v prostorách poskytovatele (zabezpečené datové centrum vyhovující požadavkům na ochranu dat, systémů, správu přístupů a podobně) a poskytovány zákazníkovi v souladu s níže uvedenými parametry.

Pro ověření plnění je garantován přístup oprávněné osoby zákazníka do zabezpečeného datového centra v doprovodu oprávněné osoby poskytovatele a to včetně případného přístupu k serverům a s možností ověřit splnění níže uvedených požadavků.

Architektura systém

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

Prostředí systému

Systém obsahuje oddělené testovací a produkční prostředí. Testovací prostředí běží na jiných HW a SW prostředcích (serverech) než produkční prostředí. Testovací prostředí běží na prostředcích záložního systému.

Produkční prostředí je rozdělené na samostatné aplikační a samostatné databázové servery. Každý z těchto serverů běží na vlastních HW a SW prostředcích (serverech). Produkční prostředí jako celek je replikováno na záložní systém ve stejné lokalitě. Záložní systém není provozován na stejných HW a SW prostředcích (serverech) jako primární.

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

Řešení provádí 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 disponuje minimálně 50% výkonu z pohledu uživatelské odezvy systému oproti primárnímu systému.

V případě výpadku primárního systému lze provoz přesměrovat na záložní systém do 1 pracovního dne od zjištění a nahlášení takového výpadku ze strany zákazníka prostřednictvím modulu Help Desk.

Testovací prostředí je konfiguračně shodné s provozním prostředím. Testovací prostředí nedisponuje stejným výkonem (z pohledu výpočetního výkonu a diskového prostoru jako provozní prostředí).

Výpočetní výkon a diskový prostor je pro testovací prostředí vždy realizován v rozsahu odpovídajícím potřebám provádění testů systému s využitím testovacího prostředí.

Výkon systému

Výkon systému odpovídá a bude odpovídat počtu detekovaných/zpracovávaných přestupků (datových paketů) a je průběžně výkonově škálován v návaznosti na reálný stav měření a celkové počty měření v čase.

Délka doby odezvy systému při produkčním zatížení odpovídá běžným zvyklostem obdobných informačních systémů a je 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 probíhá v průběhu řádného provozu. Řešení garantuje odezvy při založení/úpravě/zrušení jednoho záznamu v jednotkách sekund (na straně poskytnutého systému).

Vícenásobné operace nepřekračujícím běžné časy jiných informačních systémů pracujících s evidenčními záznamy DRMS v závislosti na množství zobrazovaných záznamů a jsou prováděny na pozadí bez omezení ostatních funkcí systému a práce uživatele.

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

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

Spolehlivost a dostupnost systému

Provoz systému se, z pohledu spolehlivosti systému a návazných SLA parametrů, nachází v jednom ze tří následujících stavů:

- **V provozu** – systém je v provozu v případě, že se uživatelé 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 uživatel mohl tyto funkcionality využít.
- **Mimo provoz** – systém je mimo provoz v případě, že se uživatelé nemohou 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 jeden uživatel (nebo případná automatická pravidelná kontrola systému) identifikuje nedostupnost funkcionality systému nebo systému jako celku, tento stav nahlásí Pronajímateli prostřednictvím systému Help Desk a zároveň tento stav není způsoben uživatelem (tj. uživatel splňuje veškeré náležitosti pro přístup a práci se systémem).

Systém je 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 18:00) 98%.
- Dostupnost produkčního prostředí bude mimo obvyklou pracovní dobu 95%.

System je považován za nedostupný v době trvání systémového stavu "mimo provoz" a "omezení funkcionality" od okamžiku oprávněného nahlášení nedostupnosti či nesprávné funkčnosti uživatelem systému poskytovateli prostřednictvím služby Help Desk až do okamžiku obnovení provozu nebo nabídnutí náhradního řešení pro nedostupnou či nesprávně fungující funkcionality systému.

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

V rámci služby Help Desk se eviduje každé uživatelské hlášení nedostupnosti systému s informací, zda se jednalo o oprávněné či neoprávněné hlášení. Poskytovatel je povinen tyto informace zpřístupnit oprávněným osobám zákazníka. Hlášení poruch a závad ze strany oprávněných osob zákazníka, stejně jako dalších požadavků souvisejících se službou podpory a servisu, je možné elektronicky a telefonicky, v souladu s požadavky na modul Help Desk a Help Line

Služba Help Desk je pro potřeby hlášení poruch, závad a požadavků dostupná pro oprávněné osoby zákazníka minimálně v pracovní době od 07:00 do 18:00, přičemž reakční čas poskytovatele na oprávněné požadavky zákazníka jsou definovány v rámci SLA parametrů.

SLA parametry

Priorita	Charakteristika problému	Doba vyřešení požadavku od jeho nahlášení
Havárie	System nelze spustit nebo dochází ke ztrátě dat, nebo system 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 existují zásadní problémy s výkonem klíčových funkcí systému	2 pracovní dny
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 18:00 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.

Pro bezpečnou identifikaci a autorizaci přístupů uživatelů systém podporuje následující metody identifikace a autentizace uživatelů:

- Identifikaci a autorizaci fyzických osob – použití kombinace jméno a heslo spolu s ověřením IP adresy nebo s využitím zabezpečené VPN.
- Definovat přístupová práva daného uživatele k jednotlivým měřením a případům a návazným dokumentům a datům v rámci rolí v systému.
- Víceúrovňovou správu systému (nastavení uživatelů, skupin a jejich rolí).
- Identifikaci a autorizaci okolních informačních systémů – například použití kombinace serverový certifikát a IP adresa.

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

Auditovatelnost provedených úkonů

Systém zaznamenává 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 Pronajímatelem při zajišťování provozu systému – systém nesmí umožnit 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 (Pronajímatel nemá vliv na provádění měření, rozsah měření a počet měření, veškeré zásahy Pronajímatele souvisí výhradně se servisní činností a jsou prováděny na základě pokynů Nájemce).

Systém neumožňuje žádné jiné, než výše uvedené, způsoby pro přístup a manipulaci s daty.

Důvěrnost a integrita dat

Systém je navržen s ohledem na vysokou míru zabezpečení celého řešení. Systém je připojen přímo na Internet. Řešení proto obsahuje firewally pro vytvoření demilitarizované zóny (DMZ). Síťový firewall poskytuje stavovou inspekci protokolu http. Žádný neproověřený provoz nebude vpuštěn na aplikační servery, kde bude prováděn přístup do datové vrstvy. Je zajištěn zabezpečený individuální přístup prostřednictvím Internetového prohlížeče.

Systém garantuje, 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.

Přístup do systému

Přístup k funkcionalitám systému je 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 jsou dostupné funkcionality systému v plné šíři.

Antivirová ochrana

Systém obsahuje řešení antivirové kontroly dokumentů (minimálně těch, které jsou v systému uloženy v nezašifrované podobě). Antivirový nástroj je poskytnut pronajímatelem.

Uživatelská podpora

Poskytovatel vždy řeší požadavky zákazníka, které jsou oprávněné v rámci provádění školení uživatelů 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 vztahuje 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 je 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 „Hot Line“ pro oprávněné osoby zákazníka.

Poskytovatel zajišťuje průběžnou údržbu veškeré dokumentace vztahující se k programovému vybavení

Legislativní maintenance

Součástí plnění je 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 zajistí update veškerého provozovaného hardware i software/firmware vyplývající z dalšího vývoje programových a technických produktů, u hardware pak například ze změn vynucených změnou platné legislativy v rámci certifikace a ověřování měřících zařízení. V případě legislativních změn souvisejících s obecně závaznými právními předpisy je součástí poskytnutí update programového či hardwarového vybavení nejpozději do data nabytí jejich účinnosti. Součástí bude také průběžná údržba veškeré dokumentace vztahující se k programovému i hardwarovému vybavení.

Počet uživatelů systému

Licence poskytnuté k systému a řešení jako celku nejsou omezeny počtem uživatelů a poskytovatel vždy na žádost zákazníka doplní či aktualizuje uživatele a jejich role a oprávnění v systému do 2 kalendářních dnů od přijetí žádosti prostřednictvím modulu Help Desk nebo Help Line.

Licence jsou poskytnuty tak, aby v systému mohli pracovat jak uživatelé z řad zákazníka, tak uživatelé z řad správního orgánu určené pro řešení detekovaných přestupků, je-li tento odlišný od organizace zákazníka.

Licence neomezují počet připojených měřících zařízení, tedy poskytnutý systém je schopen přijmout a zpracovat data o přestupcích (měření rychlosti) i z jiných měřících zařízení, které zákazník či příslušné město se správním orgánem pořídí mimo zařízení dodané poskytovatelem, 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 v rámci specifikace MOR a MUR v této příloze.