Technická specifikace požadavků na Infrastrukturu

Tato kapitola obsahuje veškeré požadavky zadavatele na systém z pohledu HW a SW infrastruktury a také další požadavky kladené na systém jako celek. Tedy níže uvedené požadavky se vztahují i na IS-WIM. Požadavky kladené na IS-WIM dle přílohy č. 1 této ZD jsou považovány primárně za požadavky na funkcionality systému z pohledu uživatele pro práci v rámci přestupkového a správního řízení a validaci dat o měření.

Zadavatel požaduje, aby součástí nabídkové ceny a specifikace nabízené HW a SW infrastruktury byly všechny služby, licence (včetně potřebných licencí a údržby databází, operačních systémů, nástrojů pro virtualizaci a podobně) i HW komponenty tvořící řešení. Součástí nabídky musí být i podpora systému jako celku po období dvou let.

Zadavatel pro potřeby této VZ poskytne výhradně místo pro umístění HW a SW komponent, konektivitu a zdroje napájení.

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 se musí umět napojit na otevřená API navazujících systémů (definice systémů v Příloze č. 5 této ZD) a pro tyto systémy vystavit otevřené API v případech opačné vazby.

Prostředí systému
Dodávka systému musí obsahovat oddělené testovací a produkční prostředí. Testovací prostředí musí běžet na jiných HW a SW prostředcích (serverech) než produkční prostředí. Je povoleno, aby testovací prostředí běželo v záložním systému.

Produkční prostředí
Produkční prostředí musí být oddělené na dvě samostatné části:

Část 1 - Modul zpracování dat z měřících zařízení vysokorychlostního vážení spolu s modulem přestupkového a správního řízení dle přílohy č. 1 této ZD.

Část 2 - Statistický modul systému vysokorychlostního vážení dle přílohy č. 1 této ZD.

Část 1 a Část 2 nesmí být provozována na stejných HW a SW prostředcích (serverech).

Oddělení produkčního prostředí na dvě části (Část 1 a Část 2) vychází z logiky práce s daty v jednotlivých částech systému a požadavcích zadavatele na zajištění dostupnosti dat. V Části 1 se zpracovávají výhradně data z měření ve smyslu přestupkového a správního řízení (ze zařízení jsou předávána data označená jako potencionální přestupek), zatímco v Části 2 se pracuje s on-line daty v kompletním telematickém rozsahu a data z této části jsou propagována do jiných systémů zadavatele, než data z části určené pro práci s přestupky.

Pro produkční prostředí pro Část 1 se požaduje:
Rozdělení produkčního prostředí na samostatné aplikační a samostatné databázové servery. Každý z těchto serverů musí běžet na HW a SW prostředcích (serverech). Produkční prostředí jako celek musí být replikováno na záložní systém ve stejné lokalitě.

Záložní systém nesmí být provozován na stejných HW a SW prostředcích (serverech) jako primární.

Provoz produkčního a záložního systému musí být minimálně v režimu Active / Passive.

V případě výpadku primárního systému musí být provoz přesměrován na záložní systém do 4 pracovních hodin od zjištění a nahlášení takového výpadku dodavateli. Pro hlášení výpadků (poruch a závad) zajistí dodavatel standardní HelpDesk.

Řešení musí provádět replikaci dat do záložního systému. Data na záložní server MUSÍ být přenášena průběžně, přičemž záloha dat z produkčního systému nesmí být starší více jak 30 minut. Záložní systém musí z výkonového pohledu mít minimálně 50% výkon z pohledu uživatelské odezvy systému oproti primárnímu systému.

Pro produkční prostředí pro Část 2 se požaduje:
Produkční prostředí jako celek musí být replikováno na záložní systém ve stejné lokalitě. Záložní systém nesmí být provozován na stejných HW a SW prostředcích (serverech) jako primární.

V případě výpadku primárního systému musí být možné přesměrovat provoz na záložní systém do 4 pracovních hodin od zjištění a nahlášení takového výpadku dodavateli. Pro hlášení výpadků (poruch a závad) zajistí dodavatel standardní HelpDesk.

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

Provoz produkčního a záložního systému musí být minimálně v režimu Active/Passive.

Doplnění:
Shora uvedené požadavky na Část 1 a Část 2 jsou chápány jako minimální a zájemce neomezuje dodavatele v nabídce kvalitnějšího systému, například s vyšší dostupností či provozu v režimu Active/Active.

Testovací prostředí
Testovací prostředí musí být konfiguračně shodné s provozním prostředím. Testovací prostředí nemusí splňovat výkonnostní požadavky kladené na provozní prostředí.

Požadavky na výkon
Systém musí být navržen tak, aby respektoval následující očekávané provozní parametry:

- Počet registrovaných uživatelů
  - 5 pro modul zpracování dat z měřících systémů
  - 50 pro modul přestupkového a správního řízení
  - 5 pro statistický modul
- Datový objem
  - přírůstek 0,3TB/rok v rámci modulu pro zpracování dat z měřících zařízení s plánovanou dobou udržitelnosti dat minimálně 5 let
  - přírůstek 0,5 TB/rok v rámci modulu přestupkového a správního řízení s plánovanou dobou udržitelnosti dat minimálně 5 let

  - přírůstek 1 TB/rok v rámci statistického modulu s plánovanou dobou udržitelnosti dat minimálně 5 let
- Počet detekcí/přestupků
  - 75.000 přestupků ročně v rámci detekce přetížených vozidel (překročení celkové hmotnosti, hmotnosti na nápravu a skupinu náprav)
  - 10.000 přestupků průjezdu vozidel s vyšší než povolenou hmotností, případně vozidel vyhýbajících se vysokorychlostnímu vážení
  - 20.000.000 detekcí průjezdu vozidel nad 3,5t ročně pro účely uchovávání informací o měření dle Přílohy č. 1 této ZD - Statistický modul systému vysokorychlostního vážení

Délka doby odezvy systému musí při uvedeném zatížení odpovídat běžným zvyklostem obdobných informačních systémů a je měřena na straně serveru. Měření odezev systému bude probíhat v průběhu řádného provozu. Řešení musí mít garantované odezvy při založení/úpravě/zrušení jednoho záznamu v jednotkách sekund. Vícenásobné operace v případě zobrazování přehledů záznamů musí být realizováno v časovém horizontu nepřekračujícím běžné časy jiných informačních systémů pracujících s evidenčními záznamy DRMS v závislosti na množství zobrazovaných záznamů.

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

Výkon systému nesmí klesat v průběhu provozu systému, tj. nesmí se prodlužovat doby odezev na jednotlivé funkcionality systému.

Škálovatelnost systému
Systém a jeho HW infrastruktura musí být navržen a vytvořen tak, že zvýšení výkonu a kapacity systému může být realizováno výhradně přidáním kompatibilních komponent, nikoli prostou výměnou stávajících.

Požadavky na spolehlivost a dostupnost systému
Provoz systému se z pohledu spolehlivosti systému a návazných SLA parametrů může nacházet 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 přihlásit
- 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 dodavateli prostřednictvím systému HelpDesk a zároveň tento stav není způsoben uživatelem (tj. uživatel 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 musí být v obvyklé pracovní době (pracovní dny od 07:00 do 17:00) 99%
- Dostupnost produkčního prostředí musí být mimo obvyklou pracovní dobu 97%

Systém bude považován za nedostupný v době trvání systémového stavu "mimo provoz" a "omezení funkcionality" od okamžiku oprávněného nahlášení nedostupnosti či nesprávné funkčnosti uživatelem systému dodavateli prostřednictvím služby HelpDesk 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 je stanoveno od 22:00 do 24:00 v pracovní den.

V rámci služby HelpDesk je dodavatel povinen evidovat každé uživatelské hlášení nedostupnosti systému s informací, zda se jednalo o oprávněné či neoprávněné hlášení. Dodavatel je povinen tyto informace zpřístupnit zadavateli. Hlášení poruch a závad ze strany zadavatele, stejně jako dalších požadavků souvisejících se službou podpory a servisu, musí být možné elektronicky a telefonicky, s využitím nástroje, který každý požadavek zadavatele zaznamená, k požadavku doplní datum a čas nahlášení požadavku a následně bude pomocí tohoto nástroje možné sledovat způsob řešení takového požadavku ze strany dodavatele, případně prostřednictvím tohoto nástroje vést mezi zadavatelem a dodavatelem další komunikaci ve smyslu doplnění či upřesnění požadavku.

Služba HelpDesk musí být pro potřeby hlášení poruch, závad a požadavků ze strany zadavatele dostupná minimálně v pracovní době od 14:00 do 15:00, přičemž reakční čas dodavatele na oprávněné požadavky zadavatele je definován v rámci SLA parametrů.

SLA parametry
Níže uvedené SLA parametry jsou ze strany Zadavatele vnímány jako minimální a zadavatel nebrání dodavateli nabídnout lepší SLA parametry, především v oblasti rychlosti odezvy dodavatele na požadavky zadavatele a rychlosti řešení hlášených závad a poruch systému.

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 existují zásadní problémy s výkonem klíčových funkcí systému	4 pracovní hodiny

Priorita	Charakteristika problému	Doba vyřešení požadavku od jeho nahlášení
Porucha	• nefunguje některá z méně důležitých funkcí systému (úpravy v nastavení, číselnících a organizační struktuře, notifikace, tiskové výstupy, apod.) • problémy s výkonem u důležitých funkcí systému (vyhledávání, hromadné úpravy záznamů, hromadné operace apod.)	1 pracovní den
Chyba	• Ostatní problémy	5 pracovních dní

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.

Požadavky na bezpečnost

Pro identifikaci a autorizaci přístupů uživatelů musí systém podporovat následující metody identifikace a autentizace uživatelů:

- Identifikaci a autorizaci fyzických osob – použití kombinace jméno a heslo
- Definovat přístupová práva daného uživatele k jednotlivým měřením a případům a návazným dokumentům a datům
- Umožnit 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 uživateli přidělena přístupová práva na základě předem definovaných pravidel. Identifikace přihlášeného uživatele bude po celou dobu práce uživatele v systému zaznamenána/logována.

Auditovatelnost provedených úkonůF

Systém musí zaznamenávat 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 dodavatelem při zajišťování provozu systému – systém nesmí umožnit jakoukoli modifikaci dat, aniž by došlo k zaznamenání
    - data a času modifikace dat
    - identifikace osoby, která změnu dat provedla

- původní hodnoty dat
- nové hodnoty dat.

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

Důvěrnost a integrita dat
Systém musí být navržen s ohledem na vysokou míru zabezpečení celého řešení. Systém bude připojen přímo na Internet. Řešení proto musí obsahovat minimálně 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. Bude zajištěn zabezpečený individuální přístup prostřednictvím Internetového prohlížeče.

Systém musí zajistit, že:

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

Přístup do systému
Přístup k funkcionalitám systému musí být zajištěn minimálně pro standardní PC prostřednictvím běžného webového prohlížeče. Zadavatel vyžaduje minimálně přístupnost systému prostřednictvím PC s OS Windows XP a vyšším plus odpovídající verzí prohlížeče Internet Explorer a Mozilla Firefox, případně Chrome.

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

Antivirová ochrana
Systém musí obsahovat řešení antivirové kontroly dokumentů (minimálně těch, které jsou v systému uloženy v nezašifrované podobě). Antivirový nástroj bude poskytnut Dodavatelem.