

## SPECIFIKACE TECHNICKÉHO ŘEŠENÍ

### A. OBECNÉ INFORMACE

- Součástí plnění jsou všechny licence (včetně potřebných licencí, databází, operačních systémů, nástrojů pro virtualizaci a podobně), služby i HW komponenty tvořící řešení.
- Součástí plnění je smlouva na dodávku informačního systému jako celku (smlouva o dílo) a také smlouva na technickou podporu systému po dobu 12 měsíců (min. 2MD měsíčně).
- Součástí nabídky bude technický popis nabízeného řešení.

### B. POŽADAVKY NA INFORMAČNÍ SYSTÉM (IS)

- IS bude umožňovat zpracování přestupků importovaných v digitální podobě z automatizovaných technických prostředků bez obsluhy (přestupky zachycené bez zjištění totožnosti přestupce bezprostředně po spáchání přestupku). V současné době provozuje zadavatel měřiče okamžité rychlosti RAMER10P.
- Systém musí umožnit automaticky zpracovávat přestupky generované měřičem úsekové rychlosti a také přestupky z parkování generované dohledovým kamerovým vozem.
- Informační systém musí být dimenzovaný na min. 15.000 přestupků měsíčně v plynulém chodu s maximem hromadných operací (přestupky budou pravděpodobně růst - škálovatelnost). Současný realita 2.000 přestupků měsíčně.
- Požadován je přístup pro 5 systemizovaných míst referentů a vedoucího odboru.
- V rámci implementace bude dodáno produkční a testovací prostředí, na oddělené infrastruktuře (různé servery, atd.)

### INTEGRACE NA OKOLNÍ IS

Informační systém musí být integrován na následující interní systémy zadavatele. Detailní popis webových služeb IS bude řešen s vítězných uchazečem.

- **IS Ginis Standard** (Ekonomický systém)
  - online komunikace v celém procesu správy dopravních přestupků (např. generování šablon dokumentů a následné předávání podkladů pro platbu, atd.)
- **IS eSPIS** (Spisová služba)
  - vazba na organizační strukturu zadavatele
  - komunikace a přenos dokumentů do spisové služby

- **DopisOnline** (služba hybridní pošty)
  - automatizované vypravení dokumentů vzniklých v IS
  - zpětné přenášení informací z odpovědí služby DopisOnline ČP do IS
- **Centrální registry** (ISZR, Eucaris, CRV, atd.)
  - automatizovaná kontrola v dostupných registrech jak jednotlivě tak hromadně nad několika přestupky zároveň
- **SMTP server** (zasílání notifikací)
  - dle způsobu dodání možnost komunikovat s interním Exchange Serverem, nebo možnost využít SMTP server dodavatele

**INFORMAČNÍ SYSTÉM BUDE OBSAHOVAT MIN. NÁSLEDUJÍCÍ LOGICKÉ CELKY:**

**MODUL/FUNKČNÍ ČÁST: VALIDAČNÍ ČÁST**

Modul/funkční část je určen pro načítání přestupků ze samotných měřících zařízení, zapojení dat do části přestupkového a správního řízení a validace vůči registrům. Pro tuto část platí, že z pohledu chování systému a práce uživatelů se jedná o jeden jednotný SW

**MODUL/FUNKČNÍ ČÁST: PŘESTUPKOVÉ A SPRÁVNÍ ŘÍZENÍ**

Modul/funkční část je určen pro práci referentů správního orgánu a garantuje všechny legislativně nezbytné činnosti spojené s prací referentů správního orgánu ve smyslu vedení komplexního přestupkového a správního řízení.

Pro tuto část platí, že z pohledu chování systému a práce uživatelů se jedná o jeden jednotný SW (tzn. jeho administrace oprávnění a přístupů, správa a zacházení s daty a podobně jsou z pohledu uživatele jednotné, není přípustné, aby uživatel pracoval ve více rozhraních zcela odlišného charakteru, chování a byly pro daný SW vedeny samostatné skupiny uživatelů, oprávnění a podobně). Systém garantuje, že od doby předání dat ze zařízení do doby ukončení přestupkového řízení jsou všechna data, logy, operace a další informace prokazující validitu měření a validitu přestupkového řízení kontinuální, jednoznačná a nezpochybnitelná.

**MODUL/FUNKČNÍ ČÁST: STATISTIKA A MANAŽERSKÉ PŘEHLEDY**

Modul/funkční část je určen pro práci oprávněných osob a garantuje možnost tvorby statistických přehledů a zobrazování agregovaných dat souvisejících prováděním měření rychlosti a řešení detekovaných přestupků.

- ✓ Shora uvedené moduly/funkční části nepředstavují konkrétní členění požadovaného SW na určité programové celky, ale definují požadavky na činnosti, procesy, možnosti a technické řešení pro logické okruhy činností uživatelů z řad městské policie a správního orgánu v rámci komplexního procesu řešení přestupků zachycených v režimu odpovědnosti provozovatele vozidla pomocí automatických měřících zařízení pro měření úsekové a okamžité rychlosti.
- ✓ Všechny shora uvedené moduly tvoří jeden komplexní software pokrývající činnost uživatelů pro všechny činnosti nezbytné a vyžadované primárně platnou legislativou pro činnosti vyplývající z platné legislativy pro provádění přestupkového a správního řízení nad detekovanými prostředky a to v souladu se zákonem (příslušná ustanovení daných zákonů týkajících se procesu řešení přestupků v dopravě při měření rychlosti):
  - *13/1997 Sb. Zákon o pozemních komunikacích*
  - *56/2001 Sb. Zákon o podmínkách provozu na pozemních komunikacích*
  - *361/2000 Sb. Zákon o provozu na pozemních komunikacích*
  - *500/2004 Sb. Zákon správní řád*
  - *250/2016 Sb. Zákon o odpovědnosti za přestupky a řízení o nich*
  - *101/2000 Sb. Zákon o ochraně osobních údajů (+ GDPR)*
- ✓ Poskytnutý SW je dodán tak, aby součástí plnění a ceny byly jak všechny programové části vytvořené přímo dodavatelem, tak všechny případné programové části vytvořené třetí osobou, případně komerční či open source části SW (OS, DB, knihovny, algoritmy pro zpracování obrazu a podobně).

## C. POŽADAVKY NA TECHNICKOU INFRASTRUKTURU A POSKYTOVANÍ SLUŽEB

Tato kapitola obsahuje veškeré specifikace systému z pohledu HW a SW infrastruktury určené pro chod informačního systému automatizované správy dopravních přestupků a také další specifikace systému jako celku a k systému poskytovaných či garantovaných služeb, především parametry nezbytné pro určení potřebného výpočetního výkonu, diskového prostoru a především vhodné architektury serverů v zabezpečeném datovém centru.

### 1. Architektura systém

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

## 2. Přístup do systému

Přístup k funkcionalitám systému je zajištěn prostřednictvím běžného webového prohlížeče (webová aplikace).

## 3. Důvěrnost a integrita dat

Systém bude navržen s ohledem na vysokou míru zabezpečení celého řešení.

Systém garantuje, že:

- ✓ Systémem uchovávaná data nemohou být zpřístupněna neautorizovaným osobám, přičemž přístup a veškerá manipulace s daty musí být 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.

## 4. Pro bezpečnou identifikaci a autorizaci přístupů uživatelů bude systém podporovat 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 uživatelům přidělena přístupová práva na základě předem definovaných pravidel. Identifikace (činnost) přihlášeného uživatele bude po celou dobu práce uživatele v systému zaznamenána/logována.

## 5. Monitorování a audit provedených úkonů

Systém zaznamenává veškeré operace, jako například:

- ✓ 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 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.

#### **VARIANTA A) HOSTOVÁNÍ V DATOVÉM CENTRU DODAVATELE:**

##### Datovým centrem se rozumí:

- ✓ Fyzický objekt se zabezpečeným přístupem, kontrolou osob na vstupu, jejich oprávnění a evidencí přístupů do prostor datového centra.
- ✓ HW a SW komponenty v rozsahu a členění dle níže uvedeného zaručující bezproblémový a z pohledu uživatelské odezvy rychlý chod systému.
- ✓ Primární i záložní napájení zaručující chod datového centra i při výpadku primárního napájení bez omezení provozu datového centra.
- ✓ Veškeré prvky nezbytné pro plnou konektivitu systému směrem do i z datového centra
- ✓ Správu vzdálených přístupů a nástroje pro vzdálený přístup a správu systému.

Po ověření plnění je možnost přístupu oprávněné osoby zadavatele do zabezpečeného datového centra v doprovodu oprávněné osoby poskytovatele a to včetně případného přístupu k serverům.

##### **Požadavky na prostředí systému**

V případě hostování v datovém centru dodavatele bude systém obsahovat oddělené testovací a produkční prostředí na různých HW a SW prostředcích.

V případě výpadku primárního systému lze provoz přesměrovat na záložní systém do 2 pracovních dnů od zjištění a nahlášení takového výpadku poskytovateli.

Řešení bude replikováno 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.

##### **Výkon systému**

Výkon systému musí odpovídat počtu detekovaných přestupků. Může být výkonově škálován v návaznosti na reálný stav měření a celkové počty měření v čase.

**VARIANTA B) IMPLEMENTACE DO DATOVÉHO CENTRA ZADAVATELE:**

Možnosti datového centra zadavatele:

- ✓ Virtualizace na platformě Hyper-V
- ✓ Možnost vytvořit jakékoliv verze OS dle požadavku
- ✓ Existující DB cluster s SQL Serverem 2k16
- ✓ Interní 10Gbps páteř a komunikační 1Gbps konektivita
- ✓ Možnost přístupu přes SSL VPN či IPSec (po akceptaci bezpečnostní politiky zadavatele)
- ✓ Zabezpečená infrastruktura