



Spolufinancováno
Evropskou unií



MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Příloha smlouvy č. 8 – Průřezové požadavky na architekturu a řešení systému eMatrika

ID	Oblast	Název požadavku	Popis požadavku
IT1	Administrace	Údržba systému	Údržba Informačního systému (upgrade minor verze, patch) musí probíhat jasně definovaným způsobem bez nutnosti opakování vývoje nestandardů.
IT2	Administrace	Změny systému	Změny nastavení systému lze plánovat v čase, tj. lze nastavit dobu platnosti (start i konec).
IT3	Administrace	Dostupnost systému	Architektura informačního systému musí umožnit souběžný provoz různých verzí komponent a spolupráci různých provozních prostředí. Škálování a provoz musí být umožněn souběžně v různých geograficky oddělených a soběstačných lokalitách. Bude-li nevyhnutelné kompletní vypnutí části funkcionalit nebo celého systému, odstávka smí činit nejvýše 2 hodiny během týdne.
IT4	Administrace	Škálovatelnost řešení	Systém musí reagovat na změny požadavků na výkon systému (změna počtu uživatelů, pracovních příkazů, apod.)
IT5	Administrace	Synchronizace	Informační systém musí monitorovat průběh synchronizace, alerty, chyby.
IT6	Administrace	Logování	Systém umožňuje vedení formy více úrovněového systémového (či aplikačního) logu k dohledání změn provedených v systému (např. změna oprávnění, změna atributu z jednoho na druhý u entit (audit log, aktivace datové pumpy atd.) Z vedení musí být minimálně patrné, jakou atribut obsahoval hodnotu před změnou a jakou hodnotu po změně. Dále kdo změnu provedl a kdy ji provedl.
IT7	Administrace	Logování do SIEM	Napojení logů do centrálního systému logů – SIEM, Syslog – 514/TCP nebo UDP dle aktuální RFC 5424, či Win.
IT8	Administrace	Logování do dalších externích komponent	Napojení logů do další (i externích) komponent veřejné správy.
IT9	Administrace	Datové pumpy/joby	Možnost řídit nastavení datových pump/jobů (vypnout, zapnout atd.).

ID	Oblast	Název požadavku	Popis požadavku
IT10	Administrace	Joby centrálně	Možnost nechat řídit joby z centrální aplikace (jako je Gitlab pipelines, Ansible).
IT11	Administrace	Správa uživatelů	Vynucené odpojení uživatele, aktivce/dektivace účtu. Synchronizaci s CAAIS, logování přihlášení, odhlášení atd.
IT12	Administrace	Diagnostika stavu systému	Monitorování stavu jednotlivých aplikačních modulů s možností restartu apod. Přehled o stavu modulů systému.
IT13	Administrace	Customizace	Nastavení chování systému (globální, lokální parametry).
IT14	Administrace	Číselníky a položky	Systém je schopen vést číselníky (a jejich hodnoty včetně možné subkategorizace a odlišného druhu chování), objekty a atributy objektu (např. křestní jméno objektu Kontakt), které mezi prostředními mají stejné ID (např. pro účely synchronizace). Je umožněno řídit jejich stav (aktivní, neaktivní, podmíněný, viditelný na formuláři, přístup uživatele na zobrazení, zápis apod.).
IT15	Architektura	Požadavky na SLA a sizing	Viz. Příloha smlouvy č. 3a - Podklad pro dodavatele k cenové tabulce
IT16	Back-end	Navrženo pro cloud	Aplikace je navržena a vyvíjena jako cloud native. Na případně pořízeném fyzickém HW je vytvořena vrstva privátního cloudu. Komponenty aplikace umožňují automatické škálování a obnovu provozu po výpadku prostřednictvím obecných orchestračních služeb. Konfigurace komponent aplikace je dodávána z hostitelského prostředí. Komponenty provádějící zpracování informace neukládají, ukládací komponenty informace nezpracovávají. Infrastruktura je komponentami konzumována způsobem infrastructure-as-a-code.
IT17	Back-end	Kontejnerizace	Informační systém umožňuje provoz v kontejnerizačním prostředí.
IT18	Back-end	Zálohování Informačního systému	Informační systém musí umožnit vytvoření konzistentní zálohy všech částí systému, včetně dat, a to na denní bázi, bez odstávky systému a bez omezení funkčnosti systému. Doba retence je řešena dle KII.
IT19	Back-end	Archivace dat v aplikaci	Systém musí umožnit archivaci definovaných/všech datových objektů, které nejsou využívány. Např. logy, deaktivované objekty, atp.
IT20	Back-end	Podpora agregace dat a následné komprese archivovaných hodnot	Systém musí podporovat víceúrovňově konfigurovatelnou agregaci a následnou kompresi pro všechny archivované hodnoty v čase. (Pro příklad: Hodnoty stárí do 1 měsíce – 1 minutovky, starší měsíce – 15 minutovky, starší 3 měsíců – 1 hodinovky, starší roku –1 den, ale zachovat agregovaná data [avg, max, min] z nejkratšího intervalu).

ID	Oblast	Název požadavku	Popis požadavku
IT21	Back-end	Aplikační messaging integrace	a S okolními systémy probíhá šifrovaná komunikace dle pravidel NÚKIB a resortu MV.
IT22	Back-end	Řízení messaging integrací	a Požadavky systémů na užití integrace (volání služeb) je řízeno modulem API (případně další vyhodnocování oprávnění, podmínek). Pro vzájemnou komunikaci modulů aplikace je přípustný pouze protokol TCP/IP.
IT23	Back-end	Mezimodulová komunikace	Je požadovaná třívrstvá a vícevrstvá (3–tier a N–tier) architektura, tj. logické oddělení prezentačních funkcí, aplikační logiky a databáze.
IT24	Back-end	Architektura aplikace	Je požadované (dle DCeGOV standardu, obecně Webhook/SNMP/MIB/UDP) napojení na centrální dohledový systém DCeGOV.
IT25	Back-end	Aplikační monitoring	
IT26	Back-end	Integrační monitoring	Musí existovat monitorovací nástroj integrace s přehledem, kdy a jaká integrace proběhla, s jakým požadavkem (hlavičkou/tělem) volání, kdo ji inicioval, jak byla vyhodnocena a provedena a s jakým výsledkem integrace skončila. Bude sledován tok informací od okamžiku předání ze zdrojového systému do Informačního systému či zpět. Musí být nastavitelná úroveň monitorování zejm. logování samotného datového obsahu zpráv. Musí být nastavitelný způsob zpracování případných chybových stavů, včetně jejich logování a odeslání formou upozornění na uživatele/administrátora.
IT27	Back-end	Bezpečnost – nepřípustná neautorizovaná externí komunikace	Požadujeme dodávku Informačních systémů bez zabudované závislosti na jakékoli externí komunikaci mimo infrastrukturu Zadavatele. Jakákoli externí komunikace musí být odůvodněná a předem autorizovaná Zadavatelem. Jakákoli závislost on–line či off–line na externí komunikaci, která není spojena s business funkcí (např. on–line ověřování licencí či ověřovací token) není přípustná.
IT28	Back-end	Bezpečnost – autentizace a správa identit	Správa identit a rolí a přihlašování uživatelů a správců jsou prováděny pomocí systémů správy identit objednatele – CAAIS, AD, LDAP, TACACS+. S výjimkou účtů s vysokými oprávněními, určených pro výchozí nastavování a diagnostiku nepreferujeme ukládání a správu identit uvnitř komponent poptávaného Informačního systému.

ID	Oblast	Název požadavku	Popis požadavku
IT29	Back-end	Bezpečnost – Single–Sign–On	Pro ověřování identit v backendových a infrastrukturních komponentách informačního systému je požadováno Single–Sign–On řešení, ve kterém musí být v maximální možné míře využíván OpenID Connect, záložně SAML 2.0 protokol.
IT30	Back-end	Bezpečnost – nepřípustné použití speciálních HW prostředků na koncové stanici	Použití čipových karet, USB tokenů, HW klíčů a jiných HW prostředků na koncové stanici je přípustné pouze za účelem vytváření důvěry transakcí a identit. Pro jiné účely není přípustné.
IT31	Back-end	Bezpečnost – autentizace server–server komunikace	Pro autentizaci server–server komunikace je požadováno využití PKI s certifikáty CCITT X.509 v3.
IT32	Back-end	Klient – architektura lehkého klienta	Zadavatel požaduje v klient–server architektuře na straně uživatelských koncových stanic „lehkého“ browser–based klienta, tj. pouze s komponenty základního nastavení (jako například html, JavaScript, CSS).
IT33	Back-end	Klient – nevhodné doplňky a zásuvné moduly	Je zakázána instalace dalších doplňků a zásuvných modulů na koncových stanicích uživatelů (jako například Active–X, Silverlight, Adobe Flash, Adobe Air, Adobe Shockwave, Java/JRE, .Net)
IT34	Back-end	Klient – nepřípustné ukládání a zálohování lokálních dat	Informační systém musí být navržen tak, aby nebylo nutné zálohovat žádná data na straně koncové stanice. Klient Informačního systému nesmí komplikovat automatickou re–instalaci koncové stanice, tj. používání klienta bezprostředně po kompletní re–instalaci koncové stanice nesmí vyžadovat obnovu dat (jak aplikačních tak uživatelských).
IT35	Back-end	Klient – komunikace se serverem	Komunikace se serverovou stranou musí být realizována výhradně prostřednictvím šifrovaného protokolu za dodržení doporučení NÚKIB. Je zakázáno využití šifer, které jsou končící nebo nejsou považovány za kvantově odolné.
IT36	Back-end	Klient – deployment klienta	Jsou preferované minimální zásahy do prostředí koncové stanice uživatele portálu úředníka, tj. v maximální možné míře použít základní aplikační vybavení koncové stanice a deployment na koncovou stanici vůbec neprovádět. V případě deploymentu je preferovaná instalace SW entit do prostředí koncové stanice pomocí automatizovaného instalačního balíčku nástroje MS SCCM.

ID	Oblast	Název požadavku	Popis požadavku
IT37	Back-end	Rozšiřování	Systém musí umožnit postupné rozšiřování o nové funkcionality. Rozšíření nesmí ovlivnit záruku na dílo, pokud závadu prokazatelně nezpůsobilo.
IT38	Back-end	Programovací jazyky	Při tvorbě komponent informačního systému budou použity moderní programovací jazyky a postupy, které umožní ověřování obchodní logiky komponent a aplikace.
IT39	Back-end	Zdrojové kódy – předávání	Zdrojové kódy systému musí být uloženy v GIT (GitLab).
IT40	Back-end	Zdrojové kódy – dokumentace	Kód aplikace musí obsahovat dokumentaci popisující význam jednotlivých částí kódu.
IT41	Back-end	Zdrojové kódy customizace – dokumentace	Kód aplikace vyvinutý pro Zadavatele musí obsahovat dokumentaci popisující význam jednotlivých částí kódu.
IT42	Back-end	Verzování a režim údržby	Systém umožní verzování sebe jako celku a svých podjednotek (modulů). Systém je možno přepnout do režim údržby (maintenance mode), který řízeně neumožní přihlášení běžných uživatelů. Systém musí zobrazovat informace (infopanel, notifikace), že je plánována údržba.
IT43	Back-end	Nepovolené služby třetích stran	Systém s výjimkou webové prezentace pro anonymní návštěvníky pro svoji funkčnost nesmí využívat služby, které nejsou klasifikovány jako ISVS, zejm. pak analytické služby typu Google Analytics a využívat nebo odkazovat na zdroje jako např. styly či písma na internetu.
IT44	Back-end	Publikace služeb	Systém publikuje svoje služby, portály a web v interní doméně cms2.cz a částí pro veřejnost (web, klientský portál eMatriky) v doméně gov.cz.
IT45	Back-end	IPv4 a IPv6	Systém musí podporovat komunikaci protokoly IPv4 a IPv6
IT46	Integrace	Včasná průběžná automatická synchronizace dat s jiným IT systémem	Je požadováno, aby každá změna dat byla včas, průběžně a automaticky propagována do systému Zadavatele.
IT47	Integrace	Udržení konzistentního stavu dat i v případě chyby v rozhraních	V případě chyby v rozhraních (např. při neschopnosti přijímacího systému zpracovat data) musí být udržován konzistentní stav dat mezi back-end systémem a Informačním systémem. Propojené systémy nesmí data "ztrácet", ani je zbytečně a nevhodně "duplikovat".

ID	Oblast	Název požadavku	Popis požadavku
IT48	Integrace	Integrace na e-mail – dynamický obsah	Systém umožní generování e-mailů s dynamickým obsahem (převzetí atributů z některých objektů systému) a jejich následné odeslání.
IT49	Integrace	Integrace na e-mail – příloha	Systém umožní generování e-mailů včetně přiložení výstupu jako přílohy a jejich následné odeslání.
IT50	IT1 – Frontend	Bezpečnost – Single–Sign–On	Pro ověřování identit na portálových částech je vyžadována Single–Sign–On integrace s NIA pro občany a CAAIS pro úředníky a správce.
IT51	Odezvy systému	Latence na straně klienta	Klientská aplikace nebude přidávat latenci více než 100 ms od back-end funkcí. Je požadována garance interaktivní odezvy na úrovni klienta: • maximálně 1 sekunda pro 90 % funkcí, • maximálně 6 sekund pro 19 % funkcí, • maximálně 30 sekund pro 1 % funkcí (zejména reporty).
IT52	Odezvy systému	Odezvy funkcí	Činnosti back-endu, jejichž předpokládaná doba provádění je delší než 3 sekundy, musí být doplněny o vizualizaci, že se činnosti provádí a optimálně i "progressbar". Reporty (nepoužívané denně) náročné na zpracování mohou běžet v jednotkách, max. v desítkách minut.
IT53	Odezvy systému	Odezvy optimalizačních funkcí (nikoli online operace)	U optimalizačních funkcí (systém provádí optimalizaci nad skupinou objektů pro zvýšení jejich efektivity) je požadována garance odezvy na úrovni klienta pro podporu činností uživatele a funkcí na mobilním klientu následovně: maximálně 180 sekund pro 99% optimalizačních funkcí (funkce, které běží na pozadí).
IT54	Odezvy systému	Odezva API	Řešení, které vystavuje/používá API (např. pro integraci), musí být stabilní v odezvě (stejně dotazy mají obdobnou odezvu v odpovědi). Pro úlohy typu endpoint a ID musí být odpověď do cca 200 ms. Pokud je nutné API "vzbudit", tak je povoleno prvotní dotaz API/endpointu mít pomalejší. Otestování pomocí aplikace třetí strany (např. Postman) a setu smluvených dotazů.
IT55	Ostatní	Technická dokumentace	Dokumentace k dodávce a Informačnímu systému je v otevřeném formátu a je odemčena k editaci.

ID	Oblast	Název požadavku	Popis požadavku
IT56	Ostatní	Uživatelská dokumentace	V systému existuje kontextové nápověda, ta umožňuje popsat části, a to jak v obecné rovině toho, kde se uživatel právě nachází (obrazovka), tak musí mít možnost popsat konkrétní prvky, jako například formuláře, validaci položek, závislosti apod. Nápověda odkazuje na podrobnější vysvětlení do uživatelské dokumentace. Nápověda k jednotlivým atributům je řešena v sekci Formuláře. Manuál systému je dynamicky složený z jednotlivých nápověd.
IT57	Ostatní	Uživatelská dokumentace – generování manuálu	Způsob generování manuálu by měl být v základních možnostech konfigurovatelný – řazení dle abecedy, hierarchizace, tvorba kapitol, případné nezařazení do manuálu aj.
IT58	Ostatní	Licence	Zakoupená licence na SW musí být ve vlastnictví Zadavatele na dobu neurčitou. V odůvodněných případech případně i na dobu určitou. Vždy však musí být zachován předpoklad kontinuity řešení pomocí případných budoucí aktualizací verzí licencí.
IT59	Ostatní	Vlastnictví kódu	Zadavatel je "vlastníkem" zdrojových kódů systému. Se zdrojovým kódem může nadále libovolně nakládat.
IT60	Ostatní	Podporované prohlížeče	Prostředí uživatele musí být kompatibilní s těmito prohlížeči: Mozilla Firefox, Google Chrome v aktuálně dostupné verzi v době provádění testů převzetí díla.
IT61	Ostatní	Podporované prohlížeče	Prostředí uživatele musí být kompatibilní s těmito prohlížeči: Microsoft Edge a Safari v aktuálně dostupné verzi v době provádění testů převzetí díla.
IT62	Ostatní	Impersonace	Možnost, aby administrátor zobrazil GUI jakoby byl přihlášený vybraný uživatel.
IT63	Ostatní	Systémový landscape	Návrh informačního systému musí obsahovat alespoň třístupňový systémový landscape – prostředí. Vývojové (vývoj funkcionalit), testovací (testování funkcionalit) a produktivní (ostré) prostředí systému. Systém umožňuje bez účasti dodavatele a vzniku významných nákladů tvorbu a správu těchto a dalších prostředí.
IT64	Ostatní	Přenosy mezi prostředími – strukturální	Systém musí obsahovat mechanismy, kterými je zajištěn snadný, bezpečný a balíčkovací systém přenosu mezi jednotlivými prostředími. Systém umožňuje přenést definice datového modelu (databáze), číselníky, atributy (včetně jejich nastavení), komponenty šablon (e–maily, dokumenty) či další součásti.

ID	Oblast	Název požadavku	Popis požadavku
IT65	Ostatní	Přenosy mezi prostředími – datová	Systém umožně přenášet i samotná data mezi prostředími. Tedy migrace např. dat položky zákazník z DEV do TEST.
IT66	Ostatní	Přenosy mezi prostředími – zachování ID	Systém při přenosu umožní zachování stejného ID (např. atributu číselníku PSČ s hodnotou 12000 má GUID, tento GUID při přenesení zůstane zachován).
IT67	Ostatní	Nahrávání dat – vynucení ID	Systém umožní nahrávání dat v režimu vynucení systémového ID.
IT68	Ostatní	Úplná lokalizace uživatelského prostředí	Je požadováno, aby veškeré interakce Informačního systému s uživateli (včetně obsahu Náповědy a práce s Náповědou) byly plně lokalizovány do českého jazyka a bylo možné do textů lokalizace zákaznický zasahovat. Požadavek lokalizace se netýká interakcí Informačního systému s administrátorem (administrátorského rozhraní).
IT69	Ostatní	Vícejazyčnost uživatelského prostředí	Aplikace musí umožňovat více jazyků. Veškeré texty musí mít svoji variantu v odpovídajícím jazyce. Jako základní jsou Čeština a Angličtina (US).
IT70	Ostatní	Vícejazyčnost uživatelského prostředí – lokalizace	Aplikace musí podporovat různou lokalizaci (čísla, měny, formáty jednotek). U jednoho jazyka může být různá lokalizace.
IT71	Ostatní	Vícejazyčnost uživatelského prostředí – lokalizace	Aplikace musí zohledňovat responsivnost u jiného jazyka. Např. německá slova jsou dlouhá, nesmí dojít k přetékání textu před grafiku, atp.
IT72	Ostatní	Jazyk administrátorského prostředí	Je požadováno, aby veškeré interakce Informačního systému s administrátory (včetně obsahu Náповědy a práce s Náповědou) byly v českém nebo anglickém jazyce a bylo možné do textů zákaznický zasahovat. Požadavek se netýká interakcí Informačního systému s uživatelem (uživatelského rozhraní).

ID	Oblast	Název požadavku	Popis požadavku
IT73	Ostatní	Self–Service reporting	Systém obsahuje funkci self reportingu. Systém musí umožnit – zobrazit data v tabulkovém zobrazení (list, grid), – měnit sloupce a jejich pořadí, – filtrovat data jak z dané entity, tak ze souvisejících entit (z vazby M:N, 1:N i N:1) (např. základní podmíněné funkce pro zobrazení, jako najdi pouze ty záznamy, kde v navázané entitě obsahuje nějaké pole a hodnotu), – uložit filtr, – sdílet uložený filtr, – opětovně vyvolat uložený filtr, – tvorbu základních typů grafů jako je sloupcový, koláčový, trychtýřový, – exportovat přehledy jako csv, xlsx.
IT74	Ostatní	Přístup ke službám	Web a klientský portál musí být funkční na běžných prohlížečích a platformách běžně užívaných operačních systémů, a to bez požadavků instalace jakéhokoliv podpůrného SW či jiných komponent.
IT75	Prostupy	Firewalling a WAF	Aplikace vystavěné v perimetru jsou chráněny Firewallingem a WAF profily.
IT76	UX/UI	Uživatelský prožitek (UX) a uživatelské rozhraní (UI)	Systém splňuje zásady UX, systémy jsou koncipované pro typické rozložení prostoru západní civilizace pro čtení zleva doprava, odshora dolů. V odůvodněných případech i rozložení jiná (arabské státy, Asie včetně uzpůsobení jazykovým a sociokulturním vlivům, např. reklamní stránky pro trh Číny). Splnění požadavku lze ověřit např. provedením kontroly všech obrazovek oproti Nielsonově desetibodové heuristice (Heuristická evaluace). Pro kontrolu webových portálů a stránek se pro zhodnocení a optimalizace používá Lighthouse report (Google). Řešení je v souladu s grafickým a logo manuálem MV a digitálního governmentu. Systém by měl obsahovat krom svého primárního režimu i režim noční/tmavý, nebo naopak denní/světlý.
IT77	UX/UI	Responzivita	Minimálně portálová část systému je koncipována jako mobile first a je responzivní. Standardní obrazovky: Chytrý telefon, Tablety, Notebook, Desktop. Standardizované breakpointy dle doporučení šířka (width) 600 px, 768 px, 992 px, 1200 px.
IT78	UX/UI	Design system – občan	Systém, zejm. samobslužný portál, musí využívat a splňovat podmínky design systému eGovernmentu (designsystem.gov.cz).

ID	Oblast	Název požadavku	Popis požadavku
IT79	UX/UI	Design system – úředník	Systém, zejm. jeho úřednická část (portál) musí zohlednit designsystém eGovernmentu (designsystem.gov.cz). Výsledkem je prostředí, ve kterém úředník po celou dobu pracovní doby efektivně může ergonomicky vykonávat matriční agendu.
IT80	UX/UI	Přístupnost	Systém musí dodržovat zákon č.99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací.

