

Váš dopis zn.  
Ze dne  
Naše zn. 58334/2023-SŽ-GR-08  
Listů/příloh 11/3

Vyřizuje Miriam Hemzová  
Mobil  
E-mail cnitptk@spravazeleznic.cz

Datum 28. 08. 2023

## **Pozvánka k předběžné tržní konzultaci ve věci eVývěska – informační kiosky pro cestující (náhrada klaprámů)**

Vážená paní, vážený pane,

Správa železnic, státní organizace (dále jen „Zadavatel“ nebo „SŽ“) Vás touto cestou informuje, že připravuje zadávací řízení na veřejnou zakázku s názvem „eVývěska – informační kiosky pro cestující (náhrada klaprámů)“. Vyhlášení této veřejné zakázky bude předcházet předběžná tržní konzultace (dále jen „PTK“), jejímž cílem bude získat relevantní informace pro správné nastavení předmětu plnění, zadávacích podmínek, volby druhu zadávacího řízení či způsobu hodnocení předložených nabídek. Zadavatel usiluje o získání kvalitního plnění, které bude splňovat jeho potřeby, a to za odpovídající cenu.

Cílem výše uvedené veřejné zakázky bude uzavření smlouvy, jejímž předmětem plnění je dosažení nového jednoduchého, moderního a uživatelsky přijatelného nástroje pro zveřejňování povinně zveřejňovaných informací a informací o závadách v provozu na tratích provozovaných SŽ. Informace budou zveřejňovány pomocí elektronických zobrazovacích zařízení (zobrazovací jednotka), které budou v provedení jedna zobrazovací jednotka nebo sestava (soubor) zobrazovacích jednotek. V Pilotním projektu bude instalováno cca 20 ks zobrazovacích jednotek ve vybraných významných uzlech železniční sítě.

Zadavatel v rámci PTK žádá o verifikaci požadovaných parametrů uvedených v Příloze č. 1 – Obecná specifikace poptávaného plnění a o zodpovězení dotazů uvedených v Příloze č. 2 – Otázky k zodpovězení PTK.

Cílem PTK je transparentním způsobem získat přehled o současné situaci na trhu, možnostech dodavatelů, a ujasnění otázek nezbytných pro realizaci veřejné zakázky.

PTK podle evropské zadávací směrnice (2014/24/EU) je možností zadavatele předtím, než vyhlásí veřejnou zakázku, komunikovat s dodavatelem a zjišťovat (případně dalšími relevantními osobami) jejich možnosti a návrhy řešení. V rámci zvoleného modelu bude představen záměr zadavatele, včetně některých navrhovaných detailů jak předmětu veřejné zakázky, tak zadávacího řízení. Dodavatelé se pak budou moci k navrhovaným parametrům zakázky vyjádřit. Dojde tak ke zvýšení transparentnosti zadávacího řízení a získání relevantních a objektivních informací o možnostech trhu, tak aby mohl zadavatel optimálně nastavit zadávací podmínky veřejné zakázky, resp. celkové řešení zadávacího řízení. Vedení PTK je rovněž zcela v souladu s ust. § 33 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „Zákon“).

**Forma PTK:** písemná (s možností pokračování ústní formou, podle potřeb Zadavatele)

### **Způsob konání PTK:**

V prvním kole PTK zašlou dodavatelé či odborné subjekty, jež projeví zájem o účast na této PTK, odpovědi na otázky uvedené v příloze č. 2 - Otázky k zodpovězení PTK na e-mailové adresy: [cnitptk@spravazeleznic.cz](mailto:cnitptk@spravazeleznic.cz)

Zadavatel si v případě potřeby vyhrazuje možnost uskutečnit druhé kolo PTK, přičemž v rámci tohoto druhého kola dojde za účelem konzultace zamýšleného řešení k osobnímu setkání s jednotlivými dodavateli či odbornými subjekty. Zadavatel si vyhrazuje právo pozvat do druhého kola libovolný počet účastníků z kola předchozího, přičemž vždy bude postupovat tak, aby nedošlo ke zvýhodnění žádného z účastníků, zejména neposkytne účastníkům druhého kola žádné přídatné informace.

Předpokládaný počátek plnění předmětu veřejné zakázky je 1. kvartál roku 2024, přičemž může být na základě PTK upraven.

**V případě Vašeho zájmu o účast na této PTK, prosím, zašlete odpovědi na otázky uvedené v příloze č. 2 - Otázky k zodpovězení PTK na e-mailovou adresu: [cnitptk@spravazeleznic.cz](mailto:cnitptk@spravazeleznic.cz)**

**Svoji odpověď prosím doručte nejpozději do 08. 09. 2023.**

Dodavatel či odborný subjekt by ve své odpovědi měl uvést minimálně:

- název dodavatele a sídlo dodavatele;
- IČO dodavatele;
- jméno a funkce kontaktních osob, včetně kontaktních údajů (minimálně e-mail);
- odpovědi na přiložené otázky.

Předběžná tržní konzultace nesmí vést k porušení základních zásad Zákona. Průběh i výsledek předběžné tržní konzultace bude zaznamenán ve zprávě vytvořené zadavatelem. Informace z předběžných tržních konzultací užití v zadávacích podmínkách zadané veřejné zakázky budou v souladu s § 36 odst. 4 Zákona v zadávací dokumentaci výslovně označeny, a to včetně osob, které se na výsledku podílely.

Děkuji za spolupráci.

S pozdravem

**Ing. David Miklas**

ředitel Správy železniční telematiky

### **Přílohy:**

- Příloha č. 1 – Obecná specifikace žádaného plnění
- Příloha č. 2 – Otázky pro písemnou část PTK
- Příloha č. 3 – Platforma 2.0

# Předběžná tržní konzultace k eVývěska – informační kiosky pro cestující (náhrada klaprámů) - Příloha č. 1

## Specifikace předmětu plnění

Zadavatel plánuje veřejnou zakázku s názvem „eVývěska – informační kiosky pro cestující (náhrada klaprámů)“ (dále jen „eVývěska“). Dokument obsahuje definici požadavků na řešení tak, jak si je Správa železnic, státní organizace (dále SŽ) v rámci svého záměru představuje. Předmětem této plánované veřejné zakázky bude dodání software a hardware.

## Cíl projektu

### Pilotní projekt – eVývěska – informační kiosky pro cestující (náhrada klaprámů)

| Poř.č. | Název stanice        | Kategorie dle UIC 180 | TEN-T | Oblastní ředitelství | Kraj            | Počet cestujících | Počet ks zobrazovacích jednotek |
|--------|----------------------|-----------------------|-------|----------------------|-----------------|-------------------|---------------------------------|
| 1      | Olomouc hl.n.        | B                     | ANO   | Ostrava              | Olomoucký       | 20000-199999      | 2                               |
| 2      | Brno hl.n.           | B                     | ANO   | Brno                 | Jihomoravský    | 20000-199999      | 2                               |
| 3      | Pardubice hl.n.      | B                     | ANO   | Hradec Králové       | Pardubický      | 20000-199999      | 2                               |
| 4      | Hradec Králové hl.n. | B                     | NE    | Hradec Králové       | Královéhradecký | 7500-199999       | 2                               |
| 5      | Ústí nad Labem       | B                     | ANO   | Ústí nad Labem       | Ústecký         | 7500-199999       | 2                               |
| 6      | České Budějovice     | B                     | ANO   | Plzeň                | Jihočeský       | 7500-199999       | 2                               |
| 7      | Plzeň hl.n.          | B                     | ANO   | Plzeň                | Plzeňský        | 7500-199999       | 2                               |
| 8      | Kolín                | B                     | ANO   | Praha                | Středočeský     | 7500-199999       | 2                               |
| 9      | Ostrava hl.n.        | B                     | ANO   | Ostrava              | Moravskoslezský | 7500-199999       | 2                               |
| 10     | Karlovy Vary         | C                     | ANO   | Ústí nad Labem       | Karlovarský     | 600 - 3999        | 2                               |

## Obecně

Správa železnic, státní organizace (dále SŽ) zahájila projekt E-Vývěska – informační kiosky pro cestující (náhrada klaprámů). Cílem tohoto projektu je **dosažení nového jednoduchého, moderního a uživatelsky přijatelného nástroje pro zveřejňování povinně zveřejňovaných informací a informací o závadách v provozu na tratích provozovaných SŽ elektronickou formou.** Informace budou zveřejňovány pomocí elektronických zobrazovacích zařízení (zobrazovací jednotka), které budou v provedení jedna zobrazovací jednotka nebo sestava (soubor) zobrazovacích jednotek.

**Současný stav** je pro Správu železnic **nevyhovující**. Informace povinně zveřejňované jsou tisknuty a „vylepovány“ na výlepkových plochách nebo ve vývěsních skříňkách. Jednou z variant je i umístění informací v klaprámech. To s sebou přináší nutnost tisku pro každou stanici a zastávku zvlášť a s tím spojené náklady na tisk, rozvoz a vlastní „výlep“. Při poškození výlepkové plochy nebo samotné informace není vždy okamžitá informace o poškození a nutnosti náhrady. Dále není možnost poskytnutí informace o aktuálním stavu v oblasti závad v provozu infrastruktury. U informací týkajících se plánované výlukové činnosti nelze operativně měnit informace v závislosti na vývoji výlukové činnosti a je nutno změny provádět opětovným „výlepem“.

Z výše uvedených důvodů je nutné realizovat nasazení nového způsobu zveřejnění informací nejen povinně zveřejňovaných, ale i informací o aktuálním stavu v oblasti závad na dopravní cestě majících přímý dopad na cestování po železnici.

Dalším argumentem pro realizaci je i skutečnost, že je realizován projekt SMART zastávek, jejichž prvkem je i informační kiosk sestávající ze 3–4 informačních zobrazovacích jednotek v jednom informačním panelu. **Pro umožnění zobrazení povinně zveřejňovaných informací však není na SŽ doposud žádná standardní technologie přenosu konkrétních dat do informačních panelů (kiosků).**

#### **Cílem je:**

1. Zobrazení povinně zveřejňovaných informací ve formátu .pdf, .doc, .mp4, .jpg v uživatelsky nastavitelném módu (stanovená sekvence zobrazení, časová poloha atd.).
2. Interaktivní ovládání pro umožnění vyhledávání dalších informací na veřejném internetu (vyhledávač spojení, jízdní řády IDS, informace objednavatele veřejné dopravy atd.), s tím, že rozsah vyhledávání může být omezeno jen na předem určené stránky internetu.
3. Dotykové ovládání zobrazovací jednotky pro běžného uživatele a dále pro uživatele s tělesným hendikepem (vozíčkáři, poškozený zrak atd.).
4. Hlasová syntéza pro poskytnutí zveřejňovaných informací pro nevidomé.
5. Základní diagnostické nástroje pro dálkovou diagnostiku.
6. Možnost dálkové obsluhy přes veřejný internet.
7. Obslužný software pro dálkovou obsluhu a diagnostiku odpovídající standardům kybernetické bezpečnosti, a to i pro jiné typy zobrazovacích jednotek, než které mají být dodány v rámci plánované VZ (možnost rozšíření o další zařízení).
8. Otevřené prostředí, kde zobrazovací zařízení není závislé na dodaném SW, tzn. lze využít veřejně prodejnou smart TV.

#### **Současný stav**

U SŽ neexistuje softwarový nástroj umožňující dálkovou obsluhu konkrétních zobrazovacích zařízení a zajišťující zveřejňování informací na těchto zařízeních. Z toho důvodu je prováděno zveřejňování informací pro cestující veřejnost a uživatele veřejně přístupných prostor formou tištěných zpráv umístěných v klaprámech. Tato technologie sdělování informací je dlouhodobě neudržitelná, z toho důvodu je na SŽ řešen projekt eVývěska – informační kiosky pro cestující (náhrada klapráků).

#### **Budoucí stav**

Předpokládáme postupnou náhradu pracovních činností spojených s vyvěšováním, kontrolou čitelnosti a odstraňováním informací v tištěné verzi. Dále požadujeme umožnění rychlého zaslání informací o omezení provozu na dráze, popř. dalších okamžitých důležitých informací na zobrazovací jednotky.

#### **Předběžné požadavky na řešení**

##### **Předpokládaná funkcionální eVývěska pro naplnění cílů projektu:**

1. Zobrazení povinně zveřejňovaných informací ve formátu .pdf, .doc, .mp4, .jpg, .xls v uživatelsky nastavitelném módu (stanovená sekvence zobrazení, časová poloha atd.).
2. Interaktivní ovládání pro umožnění vyhledávání dalších informací na veřejném internetu (vyhledávač spojení, jízdní řády IDS, informace objednavatele veřejné dopravy atd.), s tím, že rozsah vyhledávání může být omezeno jen na předem určené stránky internetu.
3. Dotykové ovládání zobrazovací jednotky pro běžného uživatele a dále pro uživatele s tělesným hendikepem (vozíčkáři, poškozený zrak atd.).
4. Hlasová syntéza pro poskytnutí zveřejňovaných informací pro nevidomé.
5. Základní diagnostické nástroje pro dálkovou diagnostiku.
6. Možnost dálkové obsluhy přes veřejný internet.
7. Obslužný software pro dálkovou obsluhu a diagnostiku odpovídající standardům kybernetické bezpečnosti, a to i pro jiné typy zobrazovacích jednotek než které mají být dodány v rámci plnění zamýšlené VZ (možnost rozšíření o další zařízení).
8. Šifrovaná komunikace e-Vývěska se serverem prostřednictvím certifikátu.

9. Schopnost zobrazování alertních zpráv s minimálním zpožděním proti reálnému času
10. Anti-vandal provedení zařízení s robustně zabezpečeným bodem fyzického připojení k síti i zdroji energie
11. Otevřené API, které komunikuje na zobrazovací jednotku. Zdrojové kódy budou v majetku Správy železnic.
12. Kybernetická bezpečnost, zejména v oblastech:
  - a. řízení přístupu uživatelů a administrátorů;
  - b. zajištění důvěrnosti a integrity přenášených dat a informací;
  - c. zaznamenávání bezpečnostních a provozních událostí;
  - d. řízení kontinuity a zajištění dostupnosti;
  - e. uchovávání auditních záznamů
  - f. ochrana před škodlivým kódem
13. Veškerá komunikace mezi panelem a řídicím prvkem/administrací chráněna pomocí šifrování
14. Pravidelné softwarové aktualizace panelů/řídicích jednotek

### **Automatické zasílání informací ze systémů SŽ a ruční vstup redaktorů nebo šéfredaktorů**

Struktura systému je zamýšlena tak, že většina povinně zveřejňovaných informací bude pomocí SW aplikace zadávat redaktor nebo šéfredaktor. Informace o aktuálním omezení provozu na dráze (plánované a nepředpokládané) budou zasílány do SW aplikace automaticky z konkrétního IS SŽ. U plánovaných omezení bude aktivace a deaktivace zveřejňované informace prováděna IS DOMIN. U neplánovaných (nepředpokládaných) akcí bude aktivace a deaktivace informace provedena přes IS DOMIN nebo ručním vstupem (IS DOMIN nebude provádět kontrolu úprav časů). Další informace, včetně reklamních akcí a jiných sdělení bude zajišťovat redaktor nebo šéfredaktor přes SW aplikaci.

Autorizace a autentizace uživatelů musí probíhat podle standardů SŽ, tzn. ověření uživatele a nastavení oprávnění pomocí platformy MS Active Directory. Diagnostika bude prováděna redaktorem nebo šéfredaktorem v SW aplikace. SW aplikace bude na základě zadání e-mailových adres konkrétních uživatelů zasílat na e-mail informace v případě ohrožení kyberútokem nebo mechanickým útokem (hlášení otřesových čidel) a v případě výpadků, popř. převodu zobrazovací jednotky do bezpečnostní polohy – pohotovostní režim nebo spořič (černá obrazovka při detekci napadení).

### **Předpokládané omezení provozu na dráze (např. plánované výluky, plánované omezení rychlosti jízdy vlaků s vlivem na jízdní doby a přestupní vazby, ad.)**

- ✓ vygenerování vymezení místa plánovaného omezení z IS CSV pro cestující veřejnost (SR70 – pro IS VITAMIN) – výlukové rozkazy doplněné o **informace pro cestující veřejnost** (opatření SŽ, popř. + opatření dopravce);
- ✓ aktivace informace pro veřejnost zveřejněním omezení v IS CSV týdenní plány výluk – odchází do IS DOMIN, kde se vytvoří sestava aktuálního omezení provozu v konkrétním úseku (stanici);
- ✓ odeslání do SW aplikace (uživatel SŽ – redaktor, šéfredaktor) – SW aplikace zajišťuje zveřejnění informace na informačním panelu (zobrazovací jednotce).

### **Nepředpokládané omezení provozu na dráze (např. nepředpokládané výluky, nepředpokládané omezení rychlosti jízdy vlaků s vlivem na jízdní doby a přestupní vazby, ad.)**

- ✓ pořízená informace v IS SŽ (provozní systémy) je předaná do IS DOMIN se „základními informacemi“ použitelnými pro cestující;
- ✓ zaměstnanec řízení provozu bude potvrzovat odeslání informace (tzn. pouze zveřejnění, popř. časový rozsah pro zveřejnění, ukončení zobrazení);

- ✓ šéfredaktor, redaktor (označení pro kontrolní a editační pozici) může provést změny v informaci pro cestující odeslané do SW aplikace IS DOMIN – IS DOMIN neaudituje, jestli je informace totožná s prvotní generovanou a zveřejněnou informací (tzn. po zveřejnění informace bude v IS DOMIN pouze prvek na omezení časového rozsahu nebo ukončení zobrazení). Provádění změn redaktorem a šéfredaktorem probíhá v SW aplikaci (IS DOMIN se tyto úpravy netýkají). Pokud bude redaktorem nebo šéfredaktorem provedena změna v časovém rozsahu zveřejnění nebo přímo ukončení zveřejnění informace, tak tato skutečnost bude zaznamenána v IS DOMIN (aby obsluhující zaměstnanec řízení provozu měl informaci o nemožnosti ovlivnění časového rámce zveřejnění a případného ukončení zveřejnění informace);
- ✓ možnost editace informací šéfredaktorem a redaktorem je z důvodu možné spolupráce s dopravcem na upřesnění nebo zrušení informace pro cestující na žádost dopravce (např. opatření dopravce eliminují dopady na cestující atd.);
- ✓ odeslání do SW aplikace (uživatel SŽ) – SW aplikace zajišťuje zveřejnění informace na informačním panelu (zobrazovacím zařízení).

### **Zveřejnění informací od dopravce (např. konkrétní opatření při výlukách, řešení různých událostí atd.)**

Doprovce nemá uzavřenu smlouvu na pronájem konkrétní zobrazovací jednotky pouze pro svoje účely. Nebo má uzavřenu smlouvu na zveřejňování pouze doplněných informací dopravce k omezení.

- ✓ dopravce zasílá text pro zveřejnění v upravitelné verzi na stanovené pracoviště SŽ redaktorovi;
- ✓ redaktor provede zběžnou kontrolu formátu textu a tento přenesení do připraveného souboru (dokumentu) k odeslání na konkrétní zobrazovací jednotku přes SW aplikaci;
- ✓ po odeslání informace na konkrétní zobrazovací jednotku provede redaktor kontrolu zobrazení pomocí SW aplikace.

### **Zveřejnění dalších informací nesouvisejících s provozem na dráze**

- ✓ Na zobrazovací jednotce bude umožněno zveřejnění reklamních spotů nebo inzertních informací (pracovní příležitosti, nabídka nemovitostí k odkupu atd.);
- ✓ informace „reklamního“ charakteru budou shromažďovány spolu s konkrétními požadavky na způsob a časový rozsah zveřejnění na pracovišti redaktora nebo šéfredaktora;
- ✓ redaktor nebo šéfredaktor provede zveřejnění pomocí SW aplikace na vybrané zobrazovací jednotce v sekvencích, které nesmí narušit převažující časový úsek pro zobrazení povinně zveřejňovaných informací a dalších informací o omezení provozu na dráze. Lze zvažovat i možnost aktivace funkce zajišťující zobrazení reklamních informací po dobu, kdy nebude cestujícím požadována povinně zveřejňovaná informace nebo informace o stavu provozu na dráze.;
- ✓ po zveřejnění provede redaktor nebo šéfredaktor kontrolu zobrazovaných informací na zobrazovací jednotce pomocí SW aplikace;
- ✓ za ukončení zobrazování nebo změnu sekvencí odpovídá redaktor nebo šéfredaktor (pracoviště) zveřejňující konkrétní informace.

### **Bezpečnostní požadavky**

SW aplikace musí být zabezpečena proti neoprávněnému přístupu pomocí ověření uživatele.

S ohledem na požadavek přístupu redaktorů a šéfredaktorů ke všem zveřejněným informacím musí být provedena oprávnění v SW aplikace nebo u vzdáleného přístupu v SW mini PC v roli administrátora.

U uživatelů se předpokládá vícestupňové ověření.

### **Diagnostika**

Zobrazovací jednotky musí být zajištěny tak, aby bylo možné zobrazit jejich aktuální zobrazení v diagnostice, tzn. budou umožňovat zobrazení stavu zobrazovací jednotky (vypnuto, zapnuto, pohotovostní režim, aktivní bez komunikace, aktivní, další definované stavy).

Diagnostický nástroj musí být schopen zablokovat (převést zobrazovací jednotku do bezpečného stavu) v případě kybernetického útoku nebo reakce otřesových čidel na mechanický útok. Zároveň musí zajistit odblokování (znovu zprovoznění) zobrazovací jednotky.

Diagnostický nástroj musí zajistit vzdálený restart zobrazovací jednotky v případě přerušené komunikace o stavu zobrazovací jednotky.

Diagnostický nástroj bude muset umožnit i nastavení časové polohy pro automatické zapínání a vypínání např. v nočních hodinách v době uzavření veřejných prostor stanic a zastávek. Dále bude umožněno nastavení režimu intenzity zobrazení (svítivost).

Diagnostický nástroj bude zajišťovat zasílání hlášení o nestandardním provozu mini PC a zobrazovací jednotky na definované e-mailové adresy SŽ (např. Service Desk, ad.).

### **Využití zařízení pro pronájem dopravcům a třetím osobám**

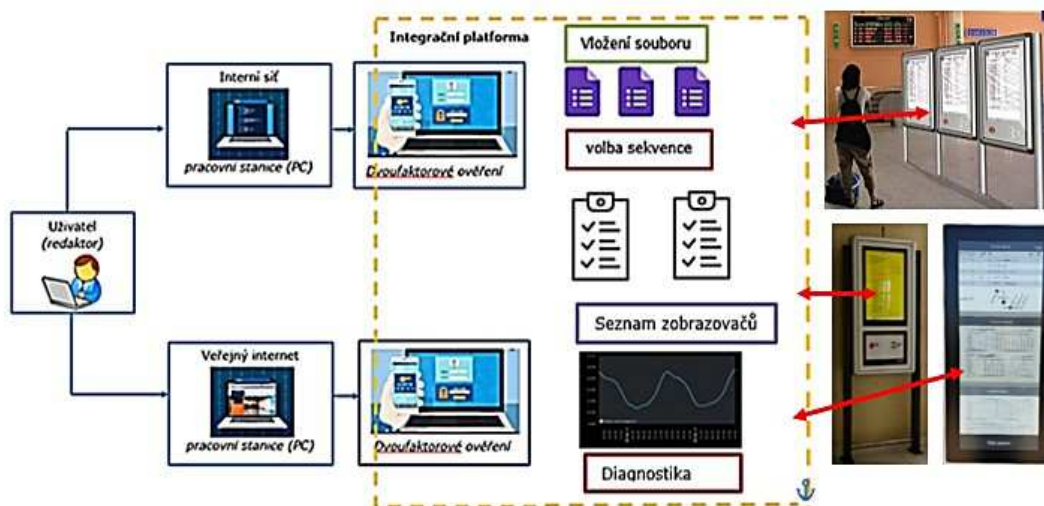
Požadavek na pronájem zobrazovací jednotky dopravcům a popř. reklamních ploch je nutno umožnit pro určitý počet zobrazovacích jednotek v konkrétní stanici nebo zastávce.

V případě využití SW aplikace bude vyřešeno přidělení konkrétního uživatelského práva pro ostatní organizace (třetí osoby). Diagnostika a další nástroje pro dálkovou obsluhu bude pouze pro potřeby SŽ. Pokud bude dopravce nebo jiná osoba požadovat dálkovou obsluhu zařízení, tak požádá konkrétní osobu na SŽ o provedení požadované dálkové obsluhy.

Diagnostické sestavy pro přehled o funkčnosti zobrazovacích jednotek v pronájmu budou na základě ustanovení smluvního vztahu generovány redaktorem nebo šéfredaktorem a zasílány elektronickou cestou smluvní straně.

Záhlaví v zobrazovací ploše bude upraveno tak, aby bylo zcela zřejmé, že se jedná o panel zobrazující obsah, který má svého původce mimo SŽ a SŽ nenese za obsahovou stránku odpovědnost.





*Hrubý přehled řešení zveřejňování informací*

### **Problematika nevidomých uživatelů:**

S ohledem na legislativu a Nařízení EU je nutné zobrazovací jednotky uzpůsobit i pro informování nevidomých osob.

**Nevidomé osoby jsou vybaveny dálkovými ovladači pro ovládání navigačních hlásek. Jednotlivé povely dálkového ovladače jsou řešeny příl. č.1 Vyhlášky č. 398/2009 Sb.: Dálkové ovládání akustických prvků.**

Dálkové ovládání musí být zabezpečeno prostřednictvím přijímače elektronických kódovaných povelů vysílaných **ze vzdálenosti nejméně 40 m na kmitočtu 86,790 MHz**. Odezva vybraných majáčků může být zpožděna o 1 až 3 sekundy.

Pro jednotlivé povely platí tato pravidla:

- a) Povel č. 1 aktivuje informaci o názvu stavby. Vzor je například trylek „Krajský úřad Středočeského kraje“ nebo trylek „Železniční stanice Praha hlavní nádraží“ nebo trylek „třetí nástupiště Praha Hlavní nádraží“.
- b) Povel č. 2 aktivuje příslušný trylek a informaci o stručném popisu interiéru nebo trasy, popřípadě trylek „cink“ a informaci o aktuálním režimu pohyblivých schodů nebo chodníků.
- c) Povel č. 3 aktivuje trylek dopravce a informaci o čísle a směru jízdy vozidla.
- d) Povel č. 4 aktivuje samoobslužné otevírání dveří nebo informuje řidiče o nástupu či výstupu nevidomého do či z vozidla.
- e) Povelem č. 5 se aktivuje akustická signalizace pro chodce.
- f) Povelem č. 6 se aktivuje hlasový výstup elektronických **informačních systémů a obdobných zařízení**.

V praxi by to mělo znamenat, po aktivaci povelu č. 6 nebo kombinaci stisků ovladače na slepecké holi vyvolávající povel č. 6 by se měl aktivovat hlasový výstup v zobrazovací jednotce a měl by nevidomého upozornit na svoje umístění. Dále by měla být zahájena komunikace mezi zobrazovací jednotkou a nevidomým pomocí povelů na ovladači. Nevidomému se přečte text s aktuálními informacemi o provozu na dráze (plánované a neplánované omezení provozu). Dále nebude jakkoliv přečtena grafická informace (obrázky, videa, prezentace, reklamy, ad.).

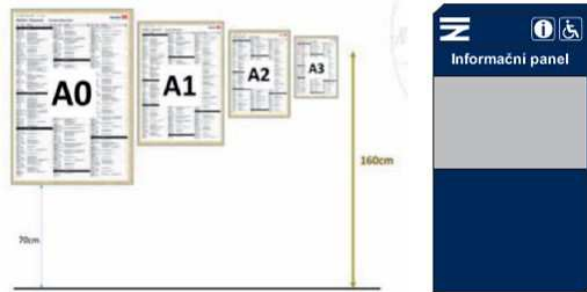
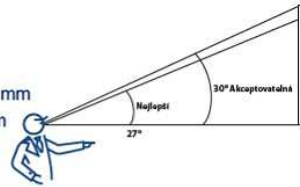
### **Problematika tělesně postižených uživatelů:**

Z důvodu nutnosti zajištění čitelnosti a vlastní čtivosti textu uživateli na invalidním vozíku je stanovena vzdálenost od podlahy ke spodní hraně zobrazovací jednotky na 70 cm.



#### Výška umístění textů

- návrh AG TSI PRM
- 20-30% plochy panelu výše, než 1600 mm
- dolní okraj panelu ne níže, než 700 mm



#### Instalace zobrazovací jednotky

Ve výšce spodní hrany zobrazovací jednotky je vhodné umístění mechanických ovládacích prvků (tlačítek), které po kombinaci stisku přiblíží text umístění v horní úrovni zobrazovací jednotky zhruba do spodní poloviny, aby byla zajištěna čitelnost textu z vozíku. V případě umístění SW ovládacích prvků dotykové obrazovky v horní části zobrazovací jednotky budou tyto přesunuty taktéž do úrovně umožňující ovládání z vozíku.

#### Datové zdroje:

IS DOMIN – informační systém Dopravní omezení manažera infrastruktury (obsahuje předpokládaná a nepředpokládaná omezení provozu)

IS VITAMIN – informační systém Virtuální tabule manažera infrastruktury (obsahuje informace o příjezdech a odjezdech vlaků vztahujících se ke konkrétnímu dopravnímu bodu sítě).

IS GRAPP – informační systém Grafická prezentace polohy (obsahuje data ke grafickému zobrazení polohy konkrétního vlaku a data k omezení provozu na konkrétní části infrastruktury).

[www.spravazeleznic.cz](http://www.spravazeleznic.cz) – webové stránky manažera infrastruktury s informacemi pro širokou veřejnost o stavbách, poloze vlaků, aktuálních omezení nepředpokládaných omezení, vyhledávač spojení atd.

# Předběžná tržní konzultace k eVývěska – informační kiosky pro cestující (náhrada klaprámů) – Příloha č. 2

Tato příloha obsahuje seznam otázek za účelem ověření dostupnosti a kvality všech požadovaných vlastností cílového řešení.

## Dotazy k technickému řešení

### Předmět plnění

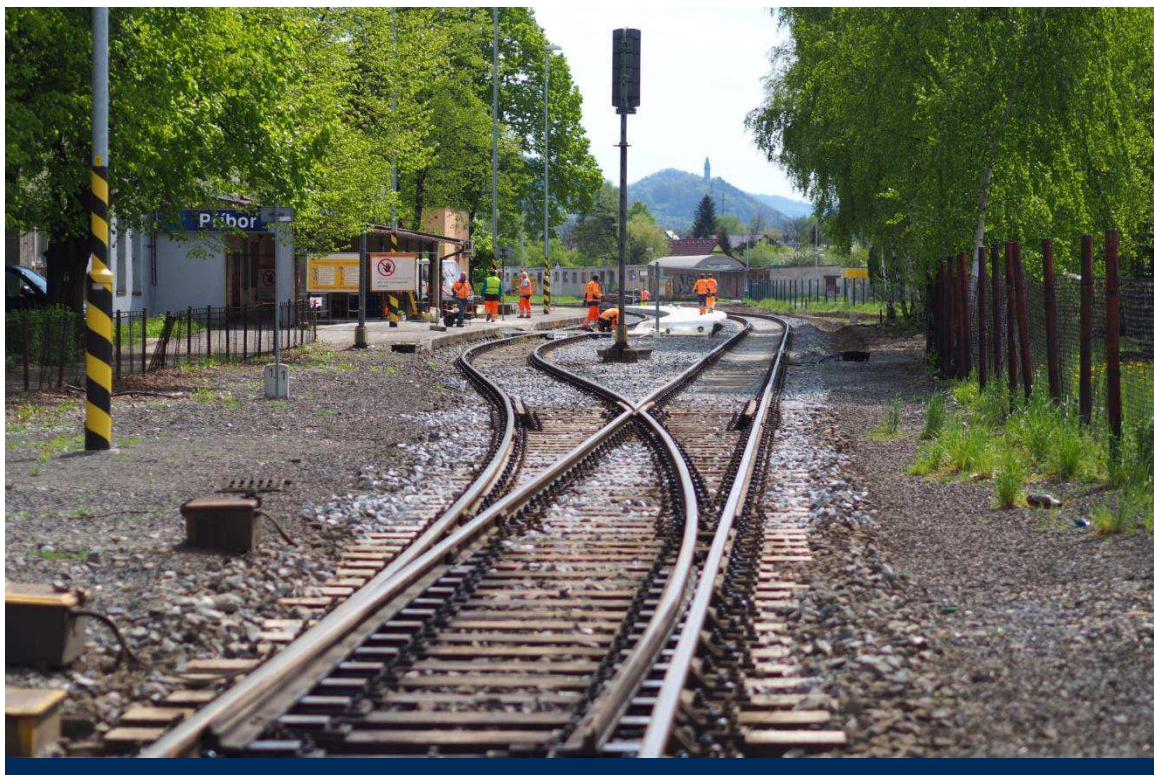
1. Jste schopni dodat plnění specifikované v cílech projektu?
2. Realizovali jste zakázku, jejímž předmětem bylo plnění ve smyslu otázky č. 1 výše?
3. Realizovala vaše společnost, ať již samostatně nebo jako součást konsorcia firem, zakázku obdobného druhu z hlediska předmětu plnění – tj. dodávka, instalace elektronického zobrazovacího interaktivního systému vč. ovládacích prvků pro stanice železniční sítě? Bylo plnění realizováno v ČR, v Evropě nebo mimo Evropu?
4. V případě kladné odpovědi na výše uvedené otázky: Může vaše společnost sdělit, jak dlouho probíhala u zadavatele implementace, zda a jak dlouho je tento systém u zadavatele provozován?
5. Prosím uveďte možnosti anti-vandal provedení a jejich cenové indikace.
6. V jakém časovém období lze podle vašeho názoru realizovat pilotní projekt „eVývěska – informační kiosky pro cestující (náhrada klaprámů)“, včetně dodávky a spuštění softwarového vybavení? Prosíme o uvedení varianty harmonogramu pro plnění celkové a pro plnění rozdělené na dvě etapy (E1 = SW, E2= HW).
7. Kde budou ukládány informace ke zveřejnění na zobrazovacích jednotkách a jak bude řešeno uživatelské nastavení přístupnosti na konkrétní webové stránky?
8. Jak je stavěn váš licenční model k dodávanému softwaru a jaká je struktura položek kalkulace? Jedná se nám o váš způsob cenotvorby v licenční politice, nikoli pouze konečnou výši ceny v případě podání nabídky.
9. Jakým způsobem jsou řešena autorská práva k vámi dodávanému software, a to i s vazbou na zákaznické úpravy?
10. Může dodavatel sdělit základní technické požadavky a prerekvizity poptávaného řešení pro obě části plnění specifikovaného v cílech projektu, tj. hardwarové a software?
11. Může dodavatel nastínit scénář a rizika možného rozdělení projektu/dodávky na dvě etapy, a to na pořízení licencí s konfigurací SW nástroje, zvláště na dodávku HW se zobrazovači (vč. napojení a zprovoznění)?
12. Jaké jsou standardní průměrné doby dodávek HW a zobrazovačů? Např. při jejich poškození a náhradě.
13. Umožňuje software dodavatele diagnostické a reportovací funkce?
14. Jaké protokoly pro přenos dat jsou využívány?
15. Jaký operační systém je používán v zobrazovacích panelech/řídících jednotkách?

### **Obecně**

1. Jaké další informace a úroveň detailu dokumentace jsou potřeba pro nacenění řešení?
2. Jakou požadujete či předpokládáte součinnost od zákazníka pro plnění předmětu veřejné zakázky?
3. Jsou Zadavatelem předložené podklady dostatečné k tomu, abyste mohli stanovit orientační nabídkovou cenu a dobu plnění zakázky?
4. Uvedte kvalifikovaný odhad nákladů na údržbu systému a případné poimplementační úpravy (požadované legislativou nebo Zadavatelem) na 4 roky (tabulka č.1 níže).
5. Uvedte stručný přehled referencí a realizací zakázek obdobného charakteru.

Tabulka č. 1 Odhad nákladů na realizaci pilotního projektu

| <b>Položka</b>                 | <b>Cena (Kč bez DPH)</b> | <b>Poznámka</b> |
|--------------------------------|--------------------------|-----------------|
| <b>Hardware</b>                |                          |                 |
| <b>Ovládací SW</b>             |                          |                 |
| <b>Vývoj, implementace</b>     |                          |                 |
| <b>Servisní podpora 4 roky</b> |                          |                 |
| <b>Celkem</b>                  |                          |                 |



# Platforma SŽ 2.0: Vymezení služeb

Únor 2023

---

## Historie verzí

| Verze | Popis   | Platnost od | Předchozí verze |
|-------|---|-------------|-----------------|
| 1.0   | Úvodní verze Platformy SŽ   | 27.01.2020  |                 |
| 2.0   | Aktualizace Platformy SŽ s názvem „Platforma SŽ 2.0: Vymezení služeb“ | 01.04.2022  |                 |
|       |   |             |                 |
|       |   |             |                 |
|       |   |             |                 |

# Obsah

|   |    |
|---|----|
| Seznam zkratk                                     | 4  |
| 1 Úvod  | 5  |
| 2 Platforma Správy železnic                       | 6  |
| 3 Motivace Platformy SŽ                           | 7  |
| 4 Architektonické principy                        | 8  |
| 5 Služby Platformy SŽ                             | 10 |
| 5.1 Infrastrukturní služby                        | 10 |
| 5.1.1 Služba virtuálních strojů                   | 10 |
| 5.1.2 Služba datového uložení                     | 10 |
| 5.2 Platformní služby                             | 11 |
| 5.2.1 Služba zabezpečeného portálového řešení     | 11 |
| 5.2.2 Služby zabezpečených webových serverů       | 11 |
| 5.2.3 Služby zabezpečených aplikačních serverů    | 11 |
| 5.2.4 Služby zabezpečených databázových prostředí | 11 |
| 5.3 Podpůrné služby                               | 12 |
| 5.3.1 Bezpečnost                                  | 12 |
| 5.3.2 Monitoring, alerting                        | 12 |
| 5.3.3 Aktualizace systémů, Distribuce aplikací    | 12 |
| 5.3.4 Zálohování                                  | 12 |
| 5.3.5 Komunikační infrastruktura                  | 13 |
| 6 Technologie Platformy SŽ                        | 14 |
| 7 Přílohy   | 16 |

## Seznam zkratk

|      |  |
|------|--|
| APP  | Aplikační vrstva   |
| AS   | Aplikační server   |
| AU   | Archivní úložiště  |
| DB   | Databáze   |
| DR   | Disaster Recovery  |
| HW   | Hardware označuje veškeré fyzicky existující technické vybavení počítače                             |
| MFA  | Multi-faktorová autentizace  |
| OS   | Operační systém  |
| SW   | Software je sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost |
| SŽ   | Správa železnic, státní organizace   |
| SŽT  | Správa železničních informačních technologií   |
| VM   | z <i>angl.</i> „ <i>Virtual Machine</i> “. Virtuální stroj   |
| WLS  | WebLogic Server  |
| WS   | Webový server  |
| ZZVZ | Zákon o zadávání veřejných zakázek   |



# 1 Úvod

Cílem tohoto dokumentu je definovat Platformu SŽ, jakožto souhrn podporovaných infrastrukturních služeb, technologií, a architektonických principů, která definuje základní rámec pro návrh řešení ICT. Platforma SŽ naplňuje strategické cíle IS/ICT SŽ, zejména v oblasti efektivního provozu a rozvoje ICT prostředí Správy železnic.

## 2 Platforma Správy železnic

Platforma Správy železnic definuje prostředí, které standardizuje a podporuje návrh, implementaci a provozování veškerého ICT řešení pro Správu železnic. Popisuje infrastrukturní a platformní služby, podporované technologie a upravuje pravidla jejich použití. Primárním cílem Platformy SŽ je poskytnout potenciálním dodavatelům přehled o prostředí SŽ a současně umožnit organizaci SŽ zajištění efektivního vytváření a provozování ICT řešení při dodržení vysoké kvality a bezpečnosti služeb.

Dokument je udržován a pravidelně aktualizován jednotkou SŽT.

Platforma SŽ obsahuje:

- Architektonické principy SŽ
- Katalog služeb Platformy SŽ
- Katalog technologií Platformy SŽ

Při plánování a rozšiřování ICT řešení je nutné respektovat všechny části Platformy SŽ.

Navíc v případech zakázkového vývoje software pro SŽ musí dodavatel splnit požadavky definované v dokumentu Standardy vývoje informačních systémů SŽ, který je přílohou tohoto dokumentu.

## 3 Motivace Platformy SŽ

Cílem Správy železnic je zajistit, že:

- Uchazeči výběrových řízení na ICT řešení mohou být hodnoceni na základě jejich celkové ekonomické efektivity, a nikoliv pouze na základě nabídkové ceny. Podrobná pravidla stanoví Zadávací dokumentace,
- Externí dodávky ICT řešení budou koncepčně a technologicky zapadat do celopodnikového prostředí Správy železnic,
- Dodávané řešení bude možné bezpečně a ekonomicky efektivně provozovat v krátko-, středně-, i dlouhodobém časovém horizontu,
- Provozované technologie SŽ budou perspektivní, moderní a bezpečné,
- Technologická různorodost prostředí SŽ bude:
  - na jednu stranu dostatečně široká, aby neúměrně neomezovala soutěž potenciálních dodavatelů, a
  - na druhou stranu dostatečně ohraničená, aby umožnila efektivní správu systémů zaměstnanci a dodavateli SŽ.

Platforma SŽ je motivovaná schválenou strategií IS/ICT SŽ, a to konkrétně cílem *zajištění dlouhodobého koncepčního rozvoje IS/ICT a jeho souladu se strategickými cíli SŽ, a to zavedením řízení celopodnikové IS/ICT architektury*<sup>1</sup>.

Očekává se, že tento dokument pomůže s nastavením jasných povinných parametrů pro nové uchazeče v oblasti technologických standardů SŽ.

Mezi přínosy dokumentu Platformy SŽ 2.0 patří:

- Nastavení společných (minimálních/maximálních) úrovní vyspělosti jednotlivých technologií napříč IS/ICT SŽ a postupné omezení velkých rozdílů v úrovních používaných technologií.
- Stanovení architektonických a technologických standardů pro tvůrce systémů a pro uchazeče o dodávku IS/ICT pro SŽ.
- Zajištění standardizace technických prostředků.
- Zajištění ochrany předchozích investic.
- Zajištění možnosti bezpečného převzetí systémů do provozu a zajištění provozu interními silami SŽ.

---

<sup>1</sup> Strategie IT a ICT Správy železnic (157463/2021-SŽ-GR-SŽT)

## 4 Architektonické principy

Kapitola stanovuje základní rámec pravidel a principů, které je nutné respektovat při návrhu a realizaci ICT řešení podle Platformy SŽ.

### **P01: Bezpečnost a soulad s vnitropodnikovými předpisy**

- Navrhované řešení a procesy jím podporované musí být v souladu s legislativními a regulatorními nároky a vnitropodnikovými předpisy Správy železnic.
- Řešení musí umožnit monitorování akcí uživatelů, zejména jejich práce s daty a dokumenty.
- Musí být zajištěna administrovatelnost a auditovatelnost integračních vazeb.
- Vývoj a test není realizován na produkčním prostředí.
- Topologie a architektura produkčního a testovacího prostředí musí být identická, odlišovat se může ve výkonu a použitých zdrojích.
- Před nasazením do produkčního prostředí je řešení prokazatelně otestováno.
- Nejsou realizovány integrace mezi produkčními a neprodukčními prostředími.
- Dohled je zajištěn na všech vrstvách řešení (HW, OS, DB, AS, aplikace, koncový uživatel).
- Musí být zajištěno napojení na centrální dohledovou konzoli.
- Služby poskytované do prostředí internetu budou procházet penetračním testem.

Zdůvodnění: Bezpečnost umožňuje chránit hodnoty Správy železnic. Ve SŽ je nutné udržovat vysokou míru bezpečnosti, a to především v oblastech, které mohou mít dopady na lidské životy. Navrhovaná řešení také musí být nezbytně v souladu s Vyhláškou č. 82/2018 Sb.o Kybernetické bezpečnosti.

### **P02: Provozovatelnost řešení**

- Řešení je provozovatelné na službách a technologiích Správy železnic.
- Řešení musí umožňovat převzetí do provozního prostředí Správy železnic
- Řešení umožňuje škálování.

Zdůvodnění: Z důvodu snahy o udržitelnost provozu je stanoven udržitelný počet technologií, které jsou spolehlivé a mají perspektivu svého rozvoje. Aplikace provozovaná na takto definované skupině technologií tak může být v případě potřeby převzata do provozu a spravována týmem IT specialistů SŽ, jež disponuje patřičnými znalostmi, případně vlastní příslušné certifikace, aby mohli tyto technologie či systémy spravovat. Tím dochází nejen ke zvýšení produktivity, ale také k časové a finanční úspoře, především z pohledu lidských zdrojů.

### **P03: Znovupoužitelnost řešení**

- Řešení musí umožňovat logické oddělení dat pro současné využívání funkcionality různými subjekty (tzv. multitenant).
- V rámci Správy železnic se realizuje minimalizace počtu a rozsahu používaných technologií a aplikací.
- Snižováním počtu a rozsahu používaných technologií a aplikací snižujeme komplexitu správy technologického a aplikačního portfolia.
- Řešení je navrhované s opakováním ověřených jednoduchých návrhových vzorů a designových principů.
- Nasazování změn a nových řešení je seskupováno dle funkcionalit a cílových systémů do jednotlivých „release“. Termíny releasů jsou stanoveny jednotkou SŽT.
- Nasazované řešení nesmí ke svému provozu vyžadovat pravidelný nutný zásah administrátora (např. restarty, čištění logů, ...)

Zdůvodnění: V rámci Správy železnic usilujeme o minimalizaci počtu prostředí pro stejnou funkcionalitu. Znovupoužitelná řešení vedou k úspoře lidských, finančních, časových i materiálních zdrojů v životním cyklu celého řešení.

### **P04: Nezávislost na dodavatelích**

- Řešení je navrhované s ohledem na omezení či eliminaci rizika vendor-lock.

- U řešení převzatých do provozu je cíl převzetí schopnosti vytvořit build aplikace bez závislosti na dodavateli.
- Usilujeme o právo zásahu do zdrojových kódů a rozvoje řešení interními kapacitami Správy železnic nebo dalšími dodavateli. Výjimku mohou tvořit jen případy, kdy by takové požadavky byly ekonomicky výrazně nevýhodné nebo je důvod se domnívat, že tato práva budou nadbytečná.

Zdůvodnění: Nebýt závislí na malém počtu dodavatelů umožňuje SŽ být transparentní a flexibilní. Vyšší míra flexibility je také výhodná pro vyjednávání s jednotlivými dodavateli o ekonomických a technických podmínkách.

#### **P05: Nákup a vývoj**

- U nákupu standardizovaných komerčních produktů je požadována schopnost nastavení balíkového řešení interními kapacitami či nezávislými externími dodavateli.
- U standardizovaných agend je preferován nákup a úprava před zakázkovým vývojem nového zákaznického řešení.
- Vzájemné integrace musí být realizované přes aplikační middleware. Integrovaní scénáře zajišťují, aby implementace nových funkcí v řídicí aplikaci minimalizovala vyvolané změny na straně návazných aplikací.
- Preferujeme přírůstkovou integraci před přenosem kompletních informací.
- Preferujeme řešení v min. třívrstvě či vícevrstvé architektuře s min. oddělením databázové, aplikační a prezentační vrstvy.
- Minimalizujeme dodávku řešení s takovými úpravami, které by omezovaly nebo eliminovaly přechod na budoucí vyšší verze produktu.
- V transakčních systémech preferujeme pouze základní operativní reporting. Plný reporting je implementovaný v analytických nástrojích.
- Řešení je řádně dokumentované po stránce vývojové, provozní a uživatelské.
- Případné zdrojové kódy jsou verzovány a ověřeny, že z nich je možno vytvořit interními týmy Správy železnic build aplikace. Zdrojové kódy a dokumentace jsou ukládány na standardizované úložiště Správy železnic.
- Návrh prostředí reflektuje trendy technologií a zároveň business potřeby.

Zdůvodnění: Regulace nákupu a do-vývoje integrací a aplikací slouží k co nejsrozumitelnějšímu a transparentnímu užívání daných technologií. Díky danému postupu v nákupu a vývoji je možné se efektivně vyrovnat s novinkami, které nově nakoupené produkty představují.

#### **P06: Business kontinuita jako zásadní činnost**

- Navržené řešení musí odpovídat kritičnosti aplikace a požadovaným parametrům SLA.
- Servisní model a parametry aplikace odpovídají bezpečnostní klasifikaci a byznysové kritičnosti aplikace.
- Dle servisního modelu jsou definované plány obnovy a „disaster recovery“ postupy.

Zdůvodnění: Správa železnic jakožto správce železniční dopravní cesty, kritické infrastruktury státu, musí být připraven na případné narušení provozu, a proto musí požadovat taková řešení, která umožní zajistit kontinuitu a obnovu klíčových procesů, činností a systémů organizace.

## 5 Služby Platformy SŽ

Tato kapitola popisuje seznam komoditních ICT služeb a jednotlivých HW/SW komponent, které tvoří standard v rámci Správy železnic. Cílem je zajistit ve fázích přípravy poptávky, návrhu ICT řešení a realizace dodávky kompatibilitu se stávajícím ICT prostředím a v maximální míře využít již provozované komponenty a technologie. Seznam služeb a komponent je průběžně aktualizován.

ICT služby Platformy jsou rozděleny do následujících skupin (kategorií):

- **Infrastrukturní**  
Infrastrukturní službou je míněno poskytování IT infrastruktury na úrovni HW, virtualizace, operačních systémů a diskových úložišť.
- **Platformní**  
Platformní služba poskytuje databázovou platformu či portálové řešení, které integruje webové aplikace a služby do jednoho spolupracujícího celku. Podporuje standardizované komunikační protokoly a formáty dat.
- **Podpůrné**  
Podpůrné služby zajišťují komplexní správu a provoz IT infrastruktury. Například monitorovací systémy, zálohování, reporting. Podpůrné služby jsou povinné k využití dodavatelem, pokud není jinak určeno SŽ.

### 5.1 Infrastrukturní služby

#### 5.1.1 Služba virtuálních strojů

Služba virtuálních strojů (dále jen „VM“) je provozována na vysoce dostupné virtualizační technologii VMware a hardware s procesory Intel Xeon E5-26XX, Intel Silver 4215. Všechna VM s operačním systémem Windows Server mají nainstalován balík VMware Open Tool.

Parametry služby jako sizing virtuálních strojů, výběr OS podporovaných Platformou SŽ 2.0, počet a konfigurace síťových karet jsou konfigurovány individuálně na základě požadavků projektu, resp. dodávaného řešení.

SŽ zajišťuje vysokou dostupnost služby virtuálních strojů na úrovni vi, a to v rámci jednoho datového centra. Pokud služby dodávaného řešení vyžadují zajištění vysoké dostupnosti, tato musí být zajištěna dodavatelem v rámci dodávky včetně služby loadbalancingu.

| Služba             | Popis   |
|--------------------|---|
| Win.VMware.x86_64  | Služby virtuálního serveru s operačním systémem Windows Server na virtualizaci VMware a architektuře x86_64   |
| RHEL.VMware.x86_64 | Služby virtuálního serveru s operačním systémem RHEL (RedHat Enterprise Linux) na virtualizaci VMware a architektuře x86_64   |
| SLES.VMware.x86_64 | Služby virtuálního serveru s operačním systémem SLES (SUSE Linux Enterprise Server) na virtualizaci VMware a architektuře x86_64<br>Omezení: Využití pro výhradně pro SAP |

#### 5.1.2 Služba datového úložiště

Služba datového úložiště je provozována na datových úložištích typu SAN, která jsou osazena 10K SAS disky v RAID5 (+hotspare disk) případně RAID 6, nebo disky SSD v RAID5 (+hotspare disk) pro aplikace vyžadující vyšší výkon, typicky databáze. V rámci služby datového úložiště není poskytována služba replikace mezi SAN úložišti, ani služba tieringu. V primárním datovém centru CDP je dále provozováno škálovatelné, výkonné, softwarově-definované datové úložiště postavené na technologii VMware vSAN, využívající prostředků fyzických serverů x86 a jejich komponent (cpu, ram, nic a disk). VMware vSAN je nativně integrované s hypervisorem VMware ESXi.

| Služba                  | Popis   |
|-------------------------|---|
| Lokální datový disk 10K | Služba datového úložiště, provozovaného na SAN storage a 10K discích v RAID 5 (+hotspare) případně RAID 6 poli, pro systémové a datové disky. |
| Lokální datový disk SSD | Služba datového úložiště, provozovaného na SAN storage osazeného SSD disky v poli RAID5 (+hotspare).  |

## 5.2 Platformní služby

Platformní služba (PaaS – Platform as a Service) poskytuje databázovou či integrační platformu (middleware). Tato integruje aplikace a služby do jednoho spolupracujícího celku. Podporuje standardizované komunikační protokoly a formáty dat.

V rámci platformy Správy železnic jsou poskytovány tyto platformní služby:

### 5.2.1 Služba zabezpečeného portálového řešení

| Služba                          | Popis   |
|---------------------------------|---|
| Liferay<br>na Win.VMware.x86_64 | Liferay je přední open-source podnikové portálové řešení založené na jazyce Java, které umožňuje správu dat, aplikací, procesů a integrace současných i nových aplikací z jednoho centrálního uživatelského rozhraní. |

### 5.2.2 Služby zabezpečených webových serverů

| Služba                                      | Popis  |
|---|--|
| Microsoft IIS<br>na Win.VMware.x86_64       | Služba webového serveru postavená na technologiích Microsoft Internet Information Services (IIS) provozovaná na serverech s operačním systémem Windows Server s virtualizací VMware. |
| Apache HTTP Server<br>na Win.VMware.x86_64  | Služba webového serveru postavená na open-source technologii Apache provozovaná na serverech s operačním systémem Windows Server s virtualizací VMware.                              |
| Apache HTTP Server<br>na RHEL.VMware.x86_64 | Služba webového serveru postavená na open-source technologii Apache provozovaná na serverech s operačním systémem RHEL s virtualizací VMware.  |

### 5.2.3 Služby zabezpečených aplikačních serverů

| Služba                                   | Popis  |
|--|--|
| .NET<br>na Win.VMware.x86_64             | Aplikační server Microsoft .NET prostředí pro vývoj a provoz aplikací založených na .NET frameworku  |
| JBOSS<br>na Win.VMware.x86_64            | Služba virtuálního aplikačního serveru JBOSS provozovaná na serverech s operačním systémem Windows Server s virtualizací VMware.   |
| Oracle WebLogic<br>na RHEL.VMware.x86_64 | Služba virtuálního aplikačního Oracle WebLogic Serveru (WLS), pro provoz aplikací postavených na standardu JAVA EE na serverech s operačním systémem RHEL s virtualizací VMware.           |
| Oracle WebLogic<br>na SLES.VMware.x86_64 | Služba virtuálního aplikačního Oracle WebLogic Serveru (WLS), pro provoz aplikací postavených na standardu JAVA EE na serverech s operačním systémem SLES s virtualizací VMware.           |
| Oracle WebLogic<br>na Win.VMware.x86_64  | Služba virtuálního aplikačního Oracle WebLogic Serveru (WLS), pro provoz aplikací postavených na standardu JAVA EE na serverech s operačním systémem Windows Server s virtualizací VMware. |

### 5.2.4 Služby zabezpečených databázových prostředí

| Služba                         | Popis  |
|--------------------------------|--|
| Oracle DB<br>na Oracle Exadata | Databázová služba Oracle DB provozovaná na optimalizovaném hardware Oracle Exadata Database Machine – kombinovaná hardwarová a softwarová platforma. |
| MS SQL<br>na Win.VMware.x86_64 | Služba virtuálních databázových serverů MS SQL Server provozovaná na serverech s operačním systémem Windows Server a virtualizační platformě VMware. |



## 5.3 Podpůrné služby

Podpůrné služby standardně poskytované k využití pro dodávaná ICT řešení.

### 5.3.1 Bezpečnost

Služby zabezpečení infrastruktury.

| Služba                               | Popis   |
|--------------------------------------|---|
| Antivirus                            | Antivirové řešení fSecure, provozované jako virtuální appliance, zajišťuje ochranu koncových stanic a serverové infrastruktury před škodlivým obsahem, zejména malwarem, exploity, síťovými útoky a jinými bezpečnostními hrozbami. Každé datové centrum Správy železnic disponuje vlastní virtuální appliance fSecure. Nasazením antivirového řešení fSecure jako virtuální appliance, jsou minimalizovány konzumované výpočetní zdroje a dopad na výkon virtualizační infrastruktury. |
| PAM                                  | Privileged Access Management (PAM) je řešení které pomáhá kontrolovat, monitorovat, zabezpečit a auditovat privilegované identity před jejich zneužitím.<br><br>Omezení: Aktuálně v pilotním provozu  |
| IDM                                  | Identity Management (IDM) je řešení umožňující řízení uživatelských účtů a jejich oprávnění napříč systémy. IDM umožňuje lepší přehlednost, bezpečnost a automatizaci. V prostředí Správy železnic bylo implementováno open-source řešení MidPoint společnosti Evolveum, jenž nevyžaduje nákup licencí. Toto řešení má otevřenou a rozšiřitelnou architekturu založenou na standardech Java, XML a REST.  |
| Active Directory and Domain Services | Adresářová služba společnosti Microsoft pro správu zařízení a identit a jejich autentizaci a autorizaci v podnikových sítích. Dodávaná řešení musí podporovat integraci na službu Active Directory Správy železnic. Správa železnic provozuje multi-forest prostředí, proto musí aplikace umožňovat využití více AD konektorů, za účelem ověření uživatelů.   |

### 5.3.2 Monitoring, alerting

| Služba     | Popis  |
|------------|--|
| Monitoring |  |
| Zabbix     | Služba dohledu infrastruktury je zajištěna pomocí dohledových agentů instalovaných na provozovaném prostředí nebo bez-agentově se vzdáleným dohledem, sledování standardními protokoly SNMP, HTTP, HTTPS apod. Dodavatelé ve spolupráci s jednotkou SŽT zajistí napojení dodávaných řešení na monitoring Zadavatele. Tím není dotčena případná povinnost dodavatele řešení monitorovat kvalitu a dostupnost dodávaného řešení v rámci vlastního monitoringu. |

### 5.3.3 Aktualizace systémů, Distribuce aplikací

| Služba                                       | Popis   |
|--|---|
| Aktualizace                                  |   |
| Distribuce SW a aktualizace koncových stanic | Technologií System Center Configuration Manager (SCCM) je zajištěna distribuce softwarových balíčků a aktualizace koncových stanic. Patchování klientských stanic probíhá 1 x měsíčně a je plně v gesci Správy železnic.  |
| Aktualizace serverových operačních systémů   | Aktualizace serverových operačních systému Windows Server je řešena skriptovacím jazykem Powershell. Patchování serverových operačních systémů probíhá 1 x měsíčně a je zajištěno Správou železnic, pokud není s dodavatelem řešení dohodnuto jinak.<br>Aktualizace serverových operačních systémů založených na linuxové distribuci je prováděna manuálně, na vyžádání správce aplikace, nebo v reakci na kybernetické hrozby. |

### 5.3.4 Zálohování

| Služba              | Popis  |
|---------------------|--|
| Zálohování a obnova | Služba zálohování prostředí je zajištěna technologií IBM Spectrum Protect (TSM – Tivoli Storage Manager) komplexním řešením pro fyzické fileservery, virtualizované prostředí a širokou škálu aplikací.<br>IBM Spectrum Protect zálohuje data s využitím technologie VMware snapshot.<br><br>Služba zálohování umožňuje 3 základní typy zálohování:<br>Snapshot disku pro dosažení rychlé obnovy celého OS v Crash Consistent stavu včetně aplikační konfigurace. Zpravidla je takto zálohován pouze systémový oddíl |

| Služba | Popis  |
|--------|--|
|        | <p>virtualizovaného serveru. Záloha probíhá jednou denně a retence je nastavena na 30 posledních verzí.</p> <p>Záloha datových svazků připojených k jednotlivým serverům, pro dosažení max. možné odolnosti proti náhodnému smazání či poškození apod. Záloha probíhá jednou denně, kdy se uchovává 90 posledních verzí souborů a poslední smazaná verze souboru je uchovávána 365 dní.</p> <p>Zálohy Oracle nebo SQL databází pomocí agentů. Záloha probíhá dvakrát denně. Přes den jsou zálohovány transakční logy databází, v noci pak vlastní databáze. Retence je nastavena na 60 posledních verzí.</p> |

### 5.3.5 Komunikační infrastruktura

| Služba         | Popis  |
|----------------|--|
| DNS            | Domain Name System (DNS) je kritickou službou, která má zásadní vliv na bezpečnost, odezvu a dostupnost služeb SŽ. Je nezbytná pro správný chod podnikové sítě a služeb na bázi Active directory. Správa železnic provozuje interní i externí službu DNS.  |
| Firewall       | Firewall soustava je velmi důležitým uzlem veškeré komunikace v síti SŽ, jenž pomocí pravidel filtruje síťový provoz a chrání prostředky v síti Správy železnic.   |
| Proxy          | Proxy soustava zajišťuje přístup uživatelů a serverů k internetu. Naprostá většina komunikace uživatelů do internetu prochází přes ni, jiný přístup není povolen. Proxy servery fungují jako prostředník mezi klienty a cílovými servery, mimo perimetr sítě SŽ, překládá klientské požadavky a vůči cílovému serveru vystupuje sám jako klient. |
| Reverzní proxy | Všechna připojení z internetu směřující na některý ze serverů jsou směrována přes reverzní proxy server, který buďto požadavek zpracuje sám nebo ho předá dál serverům. Umožňuje SSL terminaci a kompresi.   |
| VPN            | Služba virtuální privátní sítě, umožňující dodavateli zabezpečený přístup k prostředkům datových center Správy železnic.   |
| VPN S2S        | Služba virtuální privátní sítě Site-to-Site.   |

## 6 Technologie Platformy SŽ

Tato kapitola popisuje technologie, jež tvoří základ k výše uvedeným infrastrukturním a platformním službám.

**Tyto softwarové a hardwarové prostředky nesmějí být přímo použity v návrhu řešení. Jejich použití je možné pouze prostřednictvím výše uvedených infrastrukturních nebo platformních služeb.**

Pro některé případy výběrových řízení pro aplikační software je přípustné použití tzv. zapouzdřených technologií, jež nejsou součástí Platformy SŽ, ale nabízené řešení vyžaduje jejich nasazení.

Zapouzdřená technologie je zpravidla součástí jiné primární technologie jako tzv. podpůrný program. Takový program nevyžaduje samostatnou instalaci, jelikož je instalován jako součást dané komponenty.

Použití takových zapouzdřených technologií je možné jen v následujících případech:

1. Jejich použití nebude klást žádné dodatečné provozní, finanční ani implementační nároky po celou dobu životnosti primární technologie.
2. Nebudou vyžadovat žádné dodatečné licence nad rámec licencí hlavního dodávaného řešení.
3. Aktualizace zapouzdřených technologií bude probíhat pouze současně s aktualizací hlavního dodávaného řešení.
4. Jejich podpora bude poskytována současně a ve stejném rozsahu jako podpora hlavního dodávaného řešení.
5. Zapouzdřené technologie nebudou vyžadovat žádné speciální provozní či bezpečnostní zajištění.

Při použití zapouzdřených technologií je nutné danou technologii identifikovat nejméně v následujícím rozsahu:

- Název
- Verze
- Výrobce
- Licence
- Termín a úroveň podpory

| Technologie                                   | Popis   |
|---|---|
| Integrace                                     |   |
| LifeRay                                       | Bezplatný open-source podnikový portál založený na jazyce Java, umožňující správu dat, aplikací a procesů.  |
| Aplikační servery                             |   |
| Microsoft Internet Information Services (IIS) | Framework pro běh třívrstevných podnikových aplikací s kolekcí rozšiřujících modulů provozovaný nad operačními systémy Windows, vytvořený společností Microsoft.  |
| Oracle WebLogic Server                        | Aplikační server Oracle WebLogic Server (WLS) pro provoz aplikací na platformě J2EE   |
| JBoss   | Aplikační server JBoss pro provoz platformy J2EE pro řešení s potřebou autonomního prostředí, nebo pro aplikace nepožadující vysokou dostupnost   |
| Webové servery                                |   |
| Apache HTTP Server                            | Webový server postavený na open-source technologii Apache.  |
| MS IIS  | Webový server s kolekcí rozšiřujících modulů provozovaný nad operačními systémy Windows, vytvořený společností Microsoft.   |
| Databázové systémy                            |   |
| Oracle Database                               | Relační databázový systém společnosti Oracle určený pro mission critical aplikace.  |
| Microsoft SQL                                 | Relační a analytický databázový systém Microsoft SQL Server.  |
| Serverové operační systémy                    |   |
| Windows Server                                | Operační systém, na němž jsou provozovány aplikační či webové služby a databázové stroje založené zejména na technologiích společnosti Microsoft.   |
| RHEL  | Operační systém RedHat Enterprise Linux (RHEL) je linuxová distribuce společnosti RedHat určená pro komerční sféru. Použití pro aplikační servery.  |
| SLES  | Operační systém SUSE Linux Enterprise Server (SLES) je linuxová distribuce společnosti SUSE určená pro komerční sféru. Použití pro aplikační servery.   |
| Virtualizační platformy                       |   |
| VMware  | Primární virtualizační platforma pro virtualizaci hardwarové platformy x86_64. Tato zajišťuje business kontinuitu, škálovatelnost a flexibilitu provozu pro operační systémy. Platforma je primárně určena pro virtualizaci operačních systémů Windows, případně Linux. |
| Oracle VM                                     | Virtualizační platforma Oracle, pro virtualizaci hardwarové platformy x86_64 založena na technologii Citrix Xen Hypervisor. Omezené využití: Primárně určena pro provoz Oracle DB.  |
| Hardware                                      |   |
| x86_64  | Servery postavené na architektuře x86_64 – 64bitové procesory, provozovány na platformě Intel 2-socketových serverech typu rack a blade.  |
| SAN datová uložení                            | Uložení dat s podporou vysoké dostupnosti, škálování a vysokou úrovní zabezpečení. Podporuje vytváření snapshotů, replikací dat a automatický tiering datových uložení.   |
| Network and Security                          |   |
| VPN   | Zabezpečený vzdálený přístup do sítě SŽ je řešen pomocí technologie Cisco ASA.  |
| Firewall                                      | Zabezpečení pomocí firewall pravidel je zabezpečeno technologií Cisco.  |

## 7 Přílohy

Příloha 1 – Standardy vývoje informačních systémů Správy železnic



**Správa železnic, státní organizace**  
**Název organizační jednotky**  
**Dlážděná 1003/7**  
**110 00 Praha 1**

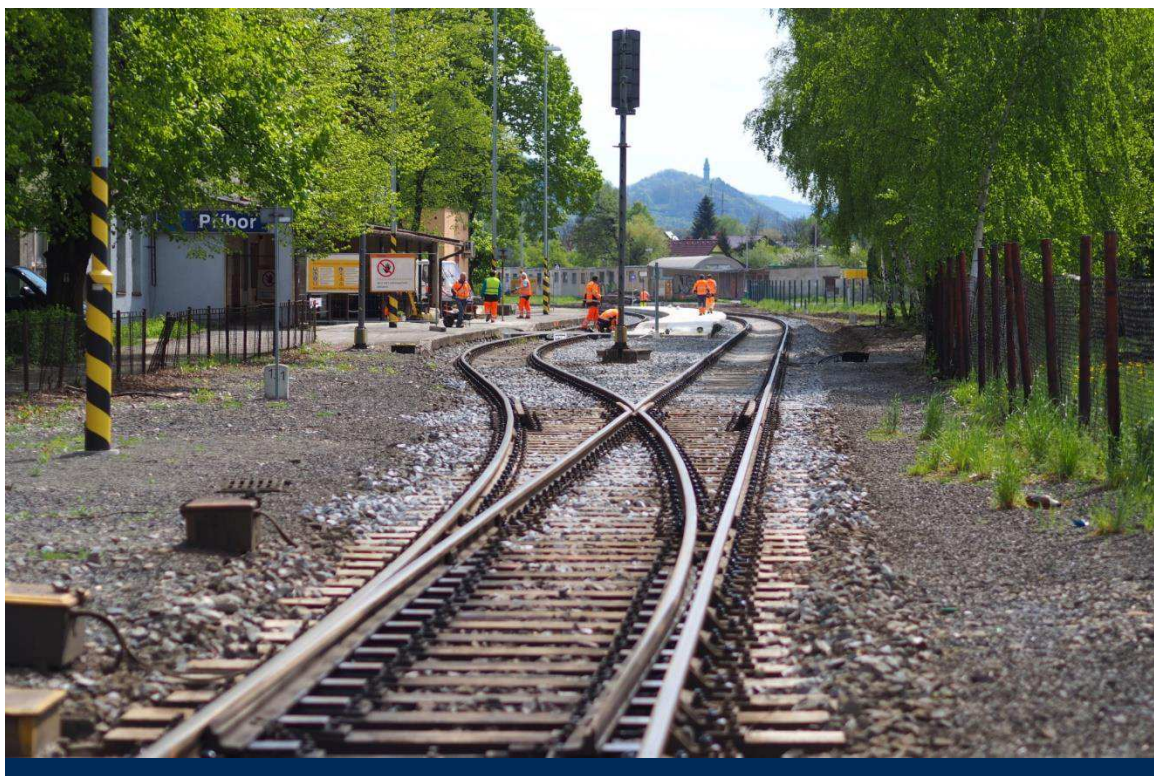
© 2022

Datum tisku  
2023-02-2131

---

**[spravazeleznic.cz](https://spravazeleznic.cz)**





# **Standardy vývoje informačních systémů Správy železnic**

**Březen 2022**

# Historie verzí

| Verze | Popis                 | Platnost od | Předchozí verze |
|-------|-----------------------|-------------|-----------------|
| 0.1   | Draft                 | 22. 3. 2022 |                 |
| 1.0   | První verze dokumentu | 31. 3. 2022 |                 |
|       |                       |             |                 |
|       |                       |             |                 |

# Obsah

|   |   |
|---|---|
| Seznam zkratk a pojmů.....  | 3 |
| 1 Standardy vývoje informačních systémů Správy železnic .....             | 4 |
| 1.1 Dvouvrstvá architektura .....   | 4 |
| 1.1.1 Datová vrstva.....  | 4 |
| 1.1.2 Aplikační vrstva .....  | 4 |
| 1.2 Třívrstvá a vícevrstvá architektura .....                             | 4 |
| 1.2.1 Datová vrstva.....  | 5 |
| 1.2.2 Aplikační vrstva .....  | 5 |
| 1.2.3 Prezentační vrstva .....  | 5 |
| 1.2.4 Integrovaná vrstva .....  | 5 |
| 1.3 Požadavky na prezentační vrstvu .....                                 | 6 |
| 1.3.1 Uživatelské rozhraní (User Interface, UI) .....                     | 6 |
| 1.3.2 Uživatelský prožitek (User Experience, UX) .....                    | 6 |
| 1.4 Bezpečnost .....  | 7 |
| 1.4.1 Zabezpečení aplikací .....  | 7 |
| 1.4.2 Autentizace a autorizace.....                                       | 7 |
| 1.4.3 GDPR .....  | 8 |
| 1.5 Dokumentace .....   | 8 |
| 1.5.1 Technická dokumentace jádra systému.....                            | 8 |
| 1.5.2 E-R modely databáze .....   | 8 |
| 1.5.3 Objektový model pro aplikace .....                                  | 8 |
| 1.5.4 Procesní diagramy, schémata toků dat .....                          | 8 |
| 1.5.5 Komunikační rozhraní.....   | 8 |
| 1.5.6 Drátové modely všech obrazovek uživatelského rozhraní aplikací..... | 8 |
| 1.5.7 Popis konfigurace provozního prostředí.....                         | 9 |
| 1.5.8 Uživatelská příručka .....  | 9 |
| 1.5.9 Příručka administrátora .....                                       | 9 |
| 1.6 Předávání vývoje do provozu.....                                      | 9 |

# Seznam zkratk a pojmů

|             |  |
|-------------|--|
| <b>3NF</b>  | Třetí normální forma   |
| <b>API</b>  | <i>z angl. Application Programming Interface</i> , rozhraní pro programování aplikací                |
| <b>APP</b>  | Aplikační vrstva   |
| <b>AS</b>   | Aplikační server   |
| <b>DB</b>   | Databáze   |
| <b>DBMS</b> | <i>z angl. Database Management System</i> , Systém řízení databáze                                   |
| <b>DC</b>   | Datové centrum   |
| <b>DDL</b>  | <i>z angl. Data Definition Language</i>  |
| <b>DR</b>   | <i>z angl. Disaster Recovery</i> , Obnova po havárii   |
| <b>HA</b>   | <i>z angl. High Availability</i> , Vysoká dostupnost   |
| <b>HW</b>   | Hardware označuje veškeré fyzicky existující technické vybavení počítače                             |
| <b>JSON</b> | <i>z angl. JavaScript Object Notation</i> , JavaScriptový objektový zápis                            |
| <b>OS</b>   | Operační systém  |
| <b>SQL</b>  | Structured Query Language, standardizovaný dotazovací jazyk pro práci v relačních databázích         |
| <b>SW</b>   | Software je sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost |
| <b>SŽ</b>   | Správa železnic, státní organizace   |
| <b>WS</b>   | Webový server  |
| <b>XML</b>  | <i>z angl. Extensible Markup Language</i> , obecný značkovací jazyk                                  |

# 1 Standardy vývoje informačních systémů

## Správy železnic

Při vývoji software ve Správě železnic je požadováno, aby byly plně respektovány obvyklé metodiky a best-practice pro návrh a vývoj software pomocí vícevrstvé architektury. Konkrétní užití jednotlivých vzorů se řídí vhodností, plánovanou zátěží a požadavky na dostupnost vyvíjeného software.

### 1.1 Dvouvrstvá architektura

Dvouvrstvou architekturu při vývoji software lze využít v případě, kdy se jedná o menší, samostatný software, který nebude integrován na další informační systémy, nebo datové zdroje Správy železnic. Užití takového software je plánováno pro menší desítky uživatelů, bez požadavku na vysokou dostupnost a možnosti škálování výkonu a rozložení zátěže prostřednictvím clusterování. U tohoto typu software nejsou definovány požadavky na vysokou odolnost proti chybám, rychlou reakci systému, nebo správu dat pro velké sítě.

Využití dvouvrstvé architektury musí být předem diskutováno s Oddělením IT architektury, které v odůvodněných případech vydá příslušnou výjimku.

#### 1.1.1 Datová vrstva

Realizace datové vrstvy je požadována prostřednictvím preferované relační databáze (dle služeb Platformy) a respektováním metodiky 3NF. Je požadován jednoznačný datový model s minimální redundancí dat a datové struktury budou modelovány a popsány jazykovými konstrukcemi DDL, které jsou kompatibilní s určeným databázovým systémem.

Celá struktura dat bude popsána formálně prostředky E-R modelování. K datovému modelu je požadováno dodat korespondující SQL DDL skripty, který budou plně odpovídat dodané databázi. Je požadováno, aby správnost, úplnost a optimalizace datového modelu byla řešena již v rámci návrhu řešení.

V rámci dvouvrstvé architektury je umožněno, aby logika byla rozprostřena částečně v databázi a částečně v aplikační, resp. prezentační vrstvě.

#### 1.1.2 Aplikační vrstva

Aplikační vrstva a prezentační vrstva je ve dvouvrstvé architektuře realizována jako jedna, společná a nedělitelná vrstva. Je požadováno, aby tato vrstva byla realizována v souladu s principy objektově orientovaného programování a komunikace mezi vrstvami byla realizována standardními zabezpečenými a šifrovanými protokoly. Je požadováno, aby uživatelské identity nebyly z aplikační vrstvy prezentovány do datové vrstvy, přičemž tyto vrstvy musí mezi sebou komunikovat technickým účtem, k tomu účelu v databázi vytvořeném.

Je požadováno, aby aplikační vrstva podporovala Multitasking, tedy umožňovala provádění několika procesů současně a systém byl již v rámci návrhu a vývoje optimalizován plánovaný výkon.

V rámci vývoje musí být ošetřena všechna bezpečnostní rizika popsaná v kapitole 1.4.

### 1.2 Třívrstvá a vícevrstvá architektura

Třívrstvá a vícevrstvá architektura je požadována při vývoji software ve všech případech mimo výjimky definované v kap. 1.1. Specifikace řešení vyžadující třívrstvou architekturu tak může disponovat následujícími vlastnostmi:

- Má být integrován na jiný software Správy železnic, nebo software třetích stran, a to z důvodu jednotného přístupu k datům a procesům vyvíjeného software
- Je plánováno využití pro větší počty uživatelů
- Je požadována vysoká dostupnost (HA)

- Je požadován Clustering pro rozložení zátěže a škálování výkonu
- Je požadována vysoká odolnost proti chybám, rychlá reakce systému, nebo správa dat pro velké sítě

### 1.2.1 Datová vrstva

Realizace datové vrstvy je požadována prostřednictvím preferované relační databáze (dle služeb Platformy) a respektováním metodiky 3NF. Je požadován jednoznačný datový model s minimální redundancí dat, datové struktury budou modelovány a popsány jazykovými konstrukcemi DDL, které jsou kompatibilní s určeným databázovým systémem.

Celá struktura dat bude popsána formálně prostředky E-R modelování. K datovému modelu je požadováno dodat korespondující SQL DDL skripty, který budou plně odpovídat dodané databázi. Je požadováno, aby správnost, úplnost a optimalizace datového modelu byla řešena již v rámci návrhu řešení.

V rámci třívrstvé a vícevrstvé architektury není umožněno, aby logika byla rozprostřena částečně v databázi a částečně v aplikační vrstvě. Aplikační logika je tak striktně pouze v aplikační vrstvě.

### 1.2.2 Aplikační vrstva

Je požadováno, aby tato vrstva byla realizována v souladu s principy objektově orientovaného programování a komunikace mezi vrstvami byla realizována standardními zabezpečenými a šifrovanými protokoly. Je požadováno, aby uživatelské identity nebyly z aplikační vrstvy prezentovány do datové vrstvy, přičemž tyto dvě vrstvy musí mezi sebou komunikovat technickým účtem, k tomu účelu v databázi vytvořeném.

Je požadováno, aby aplikační vrstva podporovala Multitasking, tedy umožňovala provádění několika procesů současně a v již rámci návrhu a vývoje optimalizovat plánovaný výkon.

V rámci vývoje musí být ošetřena všechna bezpečnostní rizika popsaná v kapitole 1.4.

### 1.2.3 Prezentační vrstva

Pro interakci s uživatelem je požadováno, aby prezentační vrstva byla realizována desktopovým klientem (tlustým), nebo webovým klientem (tenkým), a to v závislosti na vhodnosti použití a požadavcích na software kladených. Komunikace mezi prezentační a aplikační vrstvou musí být realizována standardními zabezpečenými a šifrovanými protokoly.

V rámci prezentační vrstvy a desktopového klienta je možné přenesením části aplikační logiky na klienta, tedy využití prostředků klientské stanice ke zvýšení výkonu systému, ale pouze za předpokladu, že tento systém bude zabezpečovat konzistenci aplikační logiky, napříč všemi desktopovými klienty.

Bez aktualizčních mechanismů, které zajistí stejné verze software, na všech klientských stanicích v reálném čase není tato možnost povolena.

### 1.2.4 Integrační vrstva

V případě, kdy vyvíjený software má být integrován na jiný software Správy železnic, nebo software třetích stran, je požadováno, aby tato integrační vrstva byla realizována jako samostatná vrstva, umožňující škálování výkonu a rozložení zátěže.

Realizace integrací mezi aplikačními komponentami musí splňovat principy SOA. Veškerá komunikace tedy musí probíhat prostřednictvím definovaných služeb rozhraní, a není tedy povolena výměna dat prostřednictvím přímých vazeb, jako je sdílení paměti, souborů, nebo databází. Pokud je k dispozici, komunikace probíhá prostřednictvím k tomu určené sběrnice (ESB) nebo integrační platformy.

V případě, že má být vyvíjena komponenta integrována se **spisovou službou SŽ**, musí splňovat požadavky na integraci prostřednictvím Národního standardu pro elektronické systémy spisové služby<sup>1</sup> a integrace musí být rozhraními definovanými v tomto standardu také realizována.

V případě, že má být vyvíjena aplikace integrována s programovým prostředím komponent **systému SAP**, musí být realizována prostřednictvím určené integrační platformy (SAP Cloud Platform, příp. produktu, která jej nahradí). Detailní parametry požadavku na integraci budou definovány v příslušných případech.

## 1.3 Požadavky na prezentační vrstvu

### 1.3.1 Uživatelské rozhraní (User Interface, UI)

Pomocí uživatelského rozhraní může uživatel komunikovat se zařízením, počítačem a programy. Při navrhování vysoce kvalitního uživatelského rozhraní je požadováno zohlednit nejen vzhled rozhraní, ale také jeho logickou strukturu, aby s ním uživatel mohl snadno a rychle komunikovat a dosáhnout požadovaného výsledku bez zbytečného úsilí. Cílem je vytvořit rozhraní, které poskytuje jednoduchou, srozumitelnou a pohodlnou interakci uživatele s informačním systémem.

Pro návrh UI informačních systémů SŽ platí následující zásady:

- standardní ovládací prvky
- uživatelské rozhraní jednoduché a přehledné
- konzistentní prostředí
- účelné rozvržení obrazovek
- barvy a písma dle grafického manuálu
- hierarchie daná typograficky
- informování uživatele, co systém právě dělá
- odpovídající tvar a velikost ovládacích prvků
- kódování znaků UNICODE
- datumové položky dle českého standardu „DD.MM.RRRR“
- jednotný vizuální styl (pro některé projekty dle korporátní identity)
- responzivní design webových aplikací

### 1.3.2 Uživatelský prožitek (User Experience, UX)

UX je to, co uživatel pocítí a pamatuje si v důsledku použití aplikace, systému nebo webu. UX musí být bráno v úvahu při vývoji uživatelského rozhraní, vytváření informační architektury a testování použitelnosti informačních systémů SŽ. Po určení cílového publika a charakteristiky uživatelů je požadováno vytvořit seznam UX požadavků na projekt.

UX informačních systémů SŽ musí mít následující vlastnosti:

- cílem je efektivní uživatel
- návodné ovládání
- ergonomie
- jednoduché, intuitivní
- pravidla přístupnosti, tam kde je požadováno
- zobrazování relativních a požadovaných dat
- rychlost odezvy (doba zpracování požadavku od uživatele by na serveru neměla přesáhnout 0,5s, tak aby celková doba odezvy uživatelský ovládacích prvků byla kratší než 0,8s. V případě, že je předpokládán čas odezvy delší než 0,8s, ale kratší než 2s

<sup>1</sup> NSESSS, <https://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx>



- bude uživateli zobrazen wait cursor a pokud bude předpokládáný čas odezvy delší než 2s bude pro informaci uživatele použit progress bar zobrazující průběh operace.)
- použití lazy loading v odůvodněných případech
  - jednotná terminologie v celém systému
  - ne všechno na jedné obrazovce
  - ne všechno v rozbalovacím menu (příliš mnoho položek)
  - navigace, kde se uživatel v aplikaci nachází
  - minimalizace použití dlouhých textů
  - vhodné využití grafických a obrazových prvků
  - nepoužívat drobný text
  - pečlivé plánování dialogů (logické skupiny)
  - ne překrývající se dialogy
  - jednotné, stejné ovládací prvky v dialozích na stejných místech s popisky s jednotnou terminologií

## 1.4 Bezpečnost

Všechny vyvíjené aplikace musejí splňovat požadavky kladené platnou legislativou.

Z pohledu požadavků na vyvíjený software je nutné zajistit oblasti:

- Zálohování a obnova
- Bezpečnost komunikací
- Řízení přístupu
- Ochrana před škodlivým kódem
- Logování a monitoring
- Bezpečné předávání a výměna informací
- Akvizice, vývoj a údržba

### 1.4.1 Zabezpečení aplikací

Je požadováno, aby jednotlivé vrstvy splňovaly minimálně tyto požadavky:

- Ke komunikaci mezi jednotlivými vrstvami je používán systémový účet, který lze v případě ohrožení kybernetické bezpečnosti deaktivovat, nebo změnit.
- Systémový účet, který je využíván ke komunikaci mezi vrstvami není privilegovaným účtem.
- Všechny vrstvy jsou ošetřeny proti nejzávažnějším bezpečnostním rizikům jako jsou<sup>2</sup>:
  - Injection
  - Broken Authentication
  - Sensitive Data Exposure
  - XML External Entities (XXE)
  - Broken Access Control
  - Security Misconfiguration
  - Cross-Site Scripting (XSS)
  - Insecure Deserialization
  - Using Components with Known Vulnerabilities
  - Insufficient Logging&Monitoring
- Jednotlivé vrstvy uchovávají své konfigurační parametry v šifrované podobě.

### 1.4.2 Autentizace a autorizace

#### 1.4.2.1 Autentizace

Autentizace je proces ověření proklamované identity subjektu. Je požadováno, aby aplikace umožňovala následující typy autentizace:

---

<sup>2</sup> Dle aktuálního seznamu nejzávažnějších bezpečnostních rizik definovaných OWASP (<https://owasp.org/>).



- SSO (Single Sign-On), autentizaci pomocí protokolu Kerberos, nebo OpenID proti Active Directory
- Manuální přihlášení, autentizaci pomocí vyvíjeného software, tzn. Uživatelská jména a hesla jsou uložena v databázi v šifrované podobě.
- Autentizaci pomocí protokolu LDAP, proti Active Directory
- 2FA

#### **1.4.2.2 Autorizace**

Je požadováno, aby vyvíjený software obsahoval vlastní autorizační modul, který bude minimálně umožňovat:

- Vytváření uživatelských účtů
- Vytváření rolí
- Přidělování jednotlivých uživatelských účtů k rolím
- Přidělování konkrétních oprávnění na role

V rámci naplnění povinností vyplývajících ze zákona č. 181/2014 Sb. a vyhlášky č. 82/2018 Sb. je požadováno, aby vyvíjený software umožňoval správu uživatelů a rolí pomocí externího nástroje na řízení identit, tj. Identity management implementovaným ve Správě železnic. Integrace mezi vyvíjeným softwarem a Identity management bude realizována prostřednictvím integrační vrstvy vyvíjeného software.

#### **1.4.3 GDPR**

Je požadováno kompletní splnění všech požadavků na zpracování osobních údajů dle zákona č. 110/2019 Sb. Analýza a návrh opatření musí být řešen již v rámci návrhu řešení.

### **1.5 Dokumentace**

Je požadováno, aby součástí dodávky vyvíjeného software byla dokumentace, a to minimálně v rozsahu:

#### **1.5.1 Technická dokumentace jádra systému**

Dokumentace jádra systému, jeho funkcí, služeb a rozhraní. Dokumentace bude obsahovat kompletní popis architektury jádra systému, výčet a podrobný popis všech jeho funkcí, přehled a popis služeb, které jádro poskytuje dalším komponentám systému, modulům a knihovnám.

#### **1.5.2 E-R modely databáze**

Kompletní dokumentace ve formě E-R schémat pro všechny implementované databáze včetně korespondujících DDL SQL skriptů.

#### **1.5.3 Objektový model pro aplikace**

Dokumentace obsahující objektové modely všech funkcí, jejich komponent, modulů, vztahů.

#### **1.5.4 Procesní diagramy, schémata toků dat**

Dokumentace obsahující procesní diagramy a mapu všech toků dat celého řešení.

#### **1.5.5 Komunikační rozhraní**

Dokumentace všech typů komunikačních rozhraní, všech jejich registrovaných služeb a všech funkcí, struktur dat a vlastností těchto služeb.

#### **1.5.6 Drátové modely všech obrazovek uživatelského rozhraní aplikací**

Dokumentace všech částí software musí obsahovat drátové modely všech obrazovek uživatelského rozhraní včetně popisu funkcí prvků každé obrazovky.

### 1.5.7 Popis konfigurace provozního prostředí

Dokumentace musí obsahovat soupis všech požadavků na nastavení hardwarových a softwarových komponent běhového prostředí jako jsou:

- mapování souborových systémů
- požadavky na operační paměť a počty jader
- konfigurační parametry jednotlivých podpůrných SW prostředků (např. specifika pro nastavení databáze, aplikačního serveru, webového serveru, apod.)

### 1.5.8 Uživatelská příručka

Příručka bude distribuována uživatelům. Musí obsahovat kompletní popis všech uživatelských funkcí pro práci se software. Příručka bude využívána jako základní materiál pro školení nových uživatelů. Příručka musí obsahovat kvalitně a jednoznačně zpracovaný popis kroků pro jednotlivé implementované funkce s vhodným doprovodným obrazovým materiálem ve formě výřezů obrazovek. Musí být napsána v českém jazyce a před finálním odevzdáním zpracovaná jazykovým korektorem.

### 1.5.9 Příručka administrátora

Příručka bude distribuována úzké skupině uživatelů, administrátorům systému. Musí obsahovat kompletní popis všech funkcí pro práci s administrací software. Příručka bude využívána jako materiál pro školení nových administrátorů. Příručka musí obsahovat kvalitně a jednoznačně zpracovaný popis kroků pro jednotlivé implementované funkce s vhodným doprovodným obrazovým materiálem ve formě výřezů obrazovek. Musí být napsána v českém jazyce a před finálním odevzdáním zpracovaná jazykovým korektorem.

## 1.6 Předávání vývoje do provozu

Pokud nebude určeno jinak, veškeré výstupy (zdrojové kódy, konfigurační soubory, testovací data, dokumentace atp.) musejí být předávány prostřednictvím určeného repositáře.