

# DÍLČÍ OBJEDNÁVKA č. 81

Číslo související rámcové dohody: 01IN-003773 (dále jen „rámcová dohoda“)

Číslo dílčí objednávky: 01IN-005182

Ze dne: 14.7.2022

<b>Objednatel:</b>	<b>Dodavatel:</b>
Ředitelství silnic a dálnic ČR - Úsek informatiky	IBA CZ, s.r.o.
Adresa: Čerčanská 2023/12, Praha 4, 140 00	Praha 5, Jinonice, Radlická 751/113e
IČO: 65993390	IČO: 25783572
DIČ: CZ65993390	DIČ: CZ25783572

Tato dílčí objednávka je návrhem na uzavření dílčí smlouvy ve smyslu čl. III uzavřené Rámcové dohody. Způsob akceptace dílčí objednávky Dodavatelem (uzavření dílčí smlouvy), obchodní a platební podmínky a další práva a povinnosti Smluvních stran touto dílčí dohodou výslovně neupravená stanovuje rámcová dohoda.

## Na základě uzavřené rámcové dohody u Vás objednáваме:

Služby dle nabídky, která je přílohou č. 1 této dílčí objednávky

**Místo dodání: ŘSD ČR, Čerčanská 2023/12, 140 00 Praha 4**

**Termín dodání:** do 3 měsíců od nabytí účinnosti objednávky, nebude-li dohodnuto jinak.

**Kontaktní osoba objednatele:** [REDACTED]

**Celková hodnota objednávky v Kč bez DPH / s DPH:** 596.800,-/ 722.128,-

**Jméno a příjmení oprávněné osoby objednatele:** [REDACTED]

## Přílohy:

Příloha č. 1 - ŘSD\_Návrh řešení\_obnova IDM\_V1

PODEPSÁNO PROSTŘEDNICTVÍM UZNÁVANÉHO ELEKTRONICKÉHO PODPISU DLE ZÁKONA Č. 297/2016 SB., O SLUŽBÁCH VYTVÁŘEJÍCÍCH DŮVĚRU PRO ELEKTRONICKÉ TRANSAKCE, VE ZNĚNÍ POZDĚJŠÍCH PŘEDPISŮ

# Návrh řešení – Obnova řešení IDM Midpoint

Pro společnost:  
Ředitelství silnic a dálnic ČR

Datum: 14. července 2022

# OBSAH

<b>1</b>	<b>POPIS POŽADAVKU</b> .....	<b>4</b>
<b>2</b>	<b>NÁVRH ŘEŠENÍ</b> .....	<b>4</b>
2.1	Architektura a HW/SW požadavky.....	4
2.1.1	HW požadavky.....	4
2.1.2	SW požadavky – aplikační server.....	4
2.1.3	SW požadavky – databázový server.....	5
2.1.4	Jednotky deployment-u.....	5
2.1.5	Návrh architektury řešení.....	5
2.2	Dostupné zálohy a návrh řešení.....	6
2.2.1	Users.....	6
2.2.2	Organizations.....	6
2.2.3	Role.....	7
2.2.4	Report.....	7
2.3	Postup řešení.....	7
<b>3</b>	<b>SOUČINNOST</b> .....	<b>7</b>
<b>4</b>	<b>HARMONOGRAM</b> .....	<b>8</b>
<b>5</b>	<b>CENA</b> .....	<b>8</b>
5.1	Nabídková cena.....	8
5.2	Fakturační milníky.....	8

# 1 POPIS POŽADAVKU

Dokument popisuje fyzickou a logickou architekturu obnovy systému IDM (Open Source platformy midPoint) v ŘSD po incidentu zapříčiňujícím kompletní ztrátu dat.

Dokument zahrnuje požadovanou konfiguraci serverů doporučených pro prostředí midPoint.

## 2 NÁVRH ŘEŠENÍ

### 2.1 Architektura a HW/SW požadavky

#### 2.1.1 HW požadavky

idm.rsd.cz

idmt.rsd.cz

Tabulka 1 - RSD\_IDM\_PROD

Název:	RSD_IDM_PROD
IP adresy:	Public IP adresy (doplnit)
Operační systém:	Rocky Linux 8 (latest)
CPU:	16 core
RAM:	32 GB
Disk:	140 GB
Primární aplikace:	PostgreSQL, midPoint

Tabulka 2 - RSD\_IDM\_TEST

Název:	RSD_IDM_TEST
IP adresy:	Public IP adresy (doplnit)
Operační systém:	Rocky Linux 8 (latest)
CPU:	16 core
RAM:	32 GB
Disk:	140 GB
Primární aplikace:	PostgreSQL, midPoint

#### 2.1.2 SW požadavky – aplikační server

##### 2.1.2.1 OS

Doporučený OS:

- **Rocky Linux 8 (latest)**

##### 2.1.2.2 Java

Podporované platformy a verze:

- **OpenJDK 17**

V rámci řešení bude implementováno OpenJDK 17.

### 2.1.2.3 Web container

Podporovaná platforma a verze:

- **MidPoint verze 4.4.2 má již v sobě zabudovaný container**

V rámci řešení tedy již není potřeba instalovat samostatný Apache Tomcat jak tomu bylo v předešlých verzích.

### 2.1.3 SW požadavky – databázový server

Podporované platformy a verze DB repositářů

- **PostgreSQL 14**

### 2.1.4 Jednotky deployment-u

Jednotky deploymentu představují logické balíčky komponent, které budou nasazeny na jeden samostatný server.

Tabulka 3 - Jednotky deployment-u

Jednotka deploymentu	Instalované komponenty
midPoint server +	Aplikace midPoint Nginx web server OpenJDK
midPoint DB úložiště	DB úložiště (db objekty a data) PostgreSQL (databázový server)

### 2.1.5 Návrh architektury řešení

Kapitola specifikuje fyzickou architekturu řešení midPoint IDM.

Tabulka 4 - IP a DNS adresy

Typ prostředí (VLAN)	IP rozsah LAN segmentu	MidPoint komponent	IP adresa serveru	DNS
Produkční prostředí		Apache Tomcat (midPoint)	10.102.0.221	idm.rsd.cz
		DB repositář	10.102.0.221	idm.rsd.cz
Testovací prostředí		Apache Tomcat (midPoint)	10.102.0.220	idmt.rsd.cz
		DB repositář	10.102.0.220	idmt.rsd.cz

Tabulka 5 - IP / DNS a port integrovaných komponentů řešení

	IP / DNS a port integrovaných komponentů řešení	
	TEST	PROD
SMTP Server	owa.rsd.cz	owa.rsd.cz

NTP	time1.rsd.cz, time2.rsd.cz	time1.rsd.cz, time2.rsd.cz
DNS	10.128.1.16/10.128.1.18	10.128.1.16/10.128.1.18

## 2.2 Dostupné zálohy a návrh řešení

Jelikož došlo ke ztrátě celého virtuálního stroje, na kterém midPoint fungoval, bude potřeba nainstalovat a nastavit úplně nové prostředí na virtuálním stroji. Tuto situaci bychom využili k instalaci nejnovější LTS **midPoint verze 4.4.2** s novou repository databáze **Native PostgreSQL Repository**.

Samotné obnovování konfigurací poté bude vycházet z **dochovaných konfiguračních XML souborů uložených v ŘSD GIT repository** a jejich importem do čerstvě nainstalovaného midPointu.

Seznam důležitých dochovaných XML objektů, které bude možno obnovit:

- archetypes
- connectors
- lookupTables
- objectCollections
- objectTemplates
- resources
- securityPolicies
- sequences
- systemConfigurations
- tasks
- valuePolicies

Seznam důležitých nedochovaných XML objektů, kde se bude muset využít alternativní postup:

- users
- roles
- organizations
- reports

### 2.2.1 Users

#### Zdroje dat pro Users typu FTE (Zaměstnanci)

Dle posledních informací máme potvrzeno, že databáze systému Okbase byly zachovány a bude tedy možné provést import FTE Zaměstnanců z DB pohledu stejným způsobem, jaký fungoval doposud.

#### Zdroje dat pro Users typu EXT (Externisté)

IDM midPoint byl autoritativním zdrojem dat pro externí zaměstnance a jejich XML soubory se nedochovaly. Podle našich informací se ovšem dochovaly záznamy externistů v Active Directory. Navrhujeme tedy udělat CSV export všech externistů z AD včetně jejich údajů a nainportovat je zpět do midPointu pomocí CSV resource.

### 2.2.2 Organizations

#### Zdroje dat pro Organizations typu Liniová organizační struktura

Dle posledních informací máme potvrzeno, že databáze systému Okbase byly zachovány a bude tedy možné provést import Liniové organizační struktury z DB pohledu stejným způsobem, jaký fungoval doposud.

#### Zdroje dat pro Organizations typu Stavby dle krajů

Nadřazená struktura se vytvoří manuálně, jednotlivé stavby se pak doplní automaticky při importu staveb.

#### Zdroje dat pro Organizations typu Externí společnosti

Dokážeme extrahovat z číselníku.

#### Zdroje dat pro Organizations typu Kontrakty

Dokážeme extrahovat z číselníku.

#### Zdroje dat pro Organizations typu Katalog rolí

Nadřazená struktura se vytvoří manuálně, celá struktura se pak naplní rolmi při jejich importu.

### Zdroje dat pro Organizations typu Evidenční stav

Nadřazená struktura se vytvoří manuálně, celá struktura se pak naplní uživateli při jejich importu.

#### 2.2.3 Role

##### Zdroje dat pro Role typu Aplikační

IDM midPoint byl autoritativním zdrojem dat pro Aplikační role a jejich XML soubory se nedochovaly. Podle našich informací se ovšem dochovaly záznamy rolí v Active Directory. Navrhujeme tedy udělat CSV export všech Aplikačních rolí z AD včetně jejich údajů a naimportovat je zpět do midPointu pomocí CSV resource. Alternativní postup by byl naimportovat starý RBAC CSV soubor, data v tomto souboru však budou velmi stará a nebudou obsahovat novější role.

##### Zdroje dat pro Role typu Stavby

K tomuto typu rolí nemáme dostatek informací. Jejich zdrojem byl API Endpoint, který nevíme, zda zůstal zachován. Pokud ano, nemělo by nic bránit tomu z něj znovu naimportovat Stavby původním způsobem.

##### Zdroje dat pro Role typu Organizační

Pokusíme se obnovit ze záloh udělaných na našich lokální strojích.

#### 2.2.4 Report

Reporty nebyly zachovány, navíc staré Jasper reporty nejsou kompatibilní s novou verzí midPointu 4.4.2. Jediným řešením tedy zbývá je vytvořit manuálně znovu v novém formátu.

### 2.3 Postup řešení

- Instalace a konfigurace OS
- Instalace a konfigurace databáze
- Instalace midPointu
- Kontrola SystemConfiguration (hooky a notifikace, SMS gateway a SMTP server)
- Doplnění dokumentace, pokud bude např. ponecháno nové GUI
  - **První fáze**
- Import zachovaných XML souborů z ŘSD GIT
  - **Druhá fáze**
- Vytvoření organizačních struktur
- Napojení Okbase a AD, import FTE uživatelů z Okbase a propagace do AD
- Import externistů z CSV souboru a propagace do AD
- Import Aplikačních rolí (popřípadě staveb) a propagace do AD
  - **Třetí fáze**
- Vytvoření organizačních rolí
  - **Čtvrtá fáze**
- Napojení CES (REST konektor IBA) / pouze zakládání nových účtů
- Reporty a exporty pro ESSS / org útvary / uživatelé + role / z ESSS se data neimportují (Spisovka zatím není)
- ESSS role založení ručně (10 ks)
  - **Poté co budou připraveny externí aplikace připraveny**

Projekt napojení ESD byl v přípravné fázi, na straně ESD nebylo připraveno API.

Napojení externích aplikací lze finalizovat pouze v případě, že tyto budou obnoveny v původním nastavení.

V opačném případě bude nutná součinnost s autory (ext. společnostmi). Zde jde zejména o aplikaci ESD, CES a jejich API.

## 3 SOUČINNOST

V rámci analytické fáze požadujeme součinnost zaměstnanců RSD (případně dodavatelů systému) v roli:

**Projektový manažér**

Zastřešuje koordinaci činností, realizaci integračních požadavků analýzy anebo implementace na straně zákazníka.

**Garant systému (byznys vlastník):**

V rámci analýzy poskytuje konzultace v rozsahu dotčených systém, u kterých se požaduje ukládání a verzování zdrojových kódů.

**Garant (-i) (Integrační architekt, vlastník služby, vlastník oblasti, apod.):**

Zaměstnanec je garantem projektu v oblasti architektury řešení. V průběhu projektu je obeznámen s možnými variantami použité technologie, kdy zabezpečí a odsouhlasí, že navržené řešení lze implementovat do existujícího prostředí.

**Součinnost při analýze**

Pro úspěšné dokončení analytické fáze je nutná součinnost zákazníka v rozsahu potřebném pro zařizování potřeb, integrací a oblastí služeb.

## 4 HARMONOGRAM

Společnost IBA počítá s dobou trvání projektu **do 3 měsíců** od případné akceptace nabídky, za předpokladu využití paralelního zapojení všech účastníků na projektu a aktivní součinnosti zúčastněných stran.

## 5 CENA

### 5.1 Nabídková cena

Předpokládaná, maximální cena realizace je **596 800 Kč** bez DPH.

ŘSD	Položka (role, příp. skupina rolí)	M.J.	Počet M.J.	Cena za 1 M.J. v Kč bez DPH	Cena za počet M.J. v Kč bez DPH
	projektových manažer	MD	20,00	██████████	██████████
	programátor/kodér	MD	94,00	██████████	██████████
				<b>Cena celkem</b>	<b>596 800,00 Kč</b>

Práce osob zastoupených v rolích typu konzultant/analytik, architekt/návrhář jsou zahrnuty čerpány z objednávky 01IN-004792.

### 5.2 Fakturační milníky

Na základě protokolů

Digitálně podepsal: ██████████  
Datum: 14.07.2022 18:07:41 +02:00

Digitálně podepsal ██████████  
Datum: 2022.07.27 09:29:35 +02'00'