D Í L Č Í O B J E D N Á V K A č. 102

Číslo související rámcové dohody: 01IN-003773 (dále jen „rámcová dohoda“)
Číslo dílčí objednávky: 01IN-005449
Ze dne: 22. 2. 2023

Objednatel:	**Dodavatel:**
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 objednáváme:

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: 917 000,- Kč/ 1 109 570,- Kč

Jméno a příjmení oprávněné osoby objednatele: [redacted]

Přílohy:
Příloha č. 1 - ŘSD_Návrh řešení_integrace registračních formulářů s IDM a následné WFL

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

Příloha č. 1

Návrh řešení – Integrace Registračních formulářů s IDM a vytvoření schvalovacího WFL, Rozšíření portálu pro reset hesla o reset hesla dělníkům

Pro společnost:

Ředitelství silnic a dálnic ČR

Datum: 17. února 2023

IBA CZ, s. r. o.,
Radlická 751/113e,
158 00 Praha 5

IČO: 25783572
DIČ: CZ25783572

www.ibacz.eu
info@ibacz.eu
(+420) 251 050 100

OBSAH

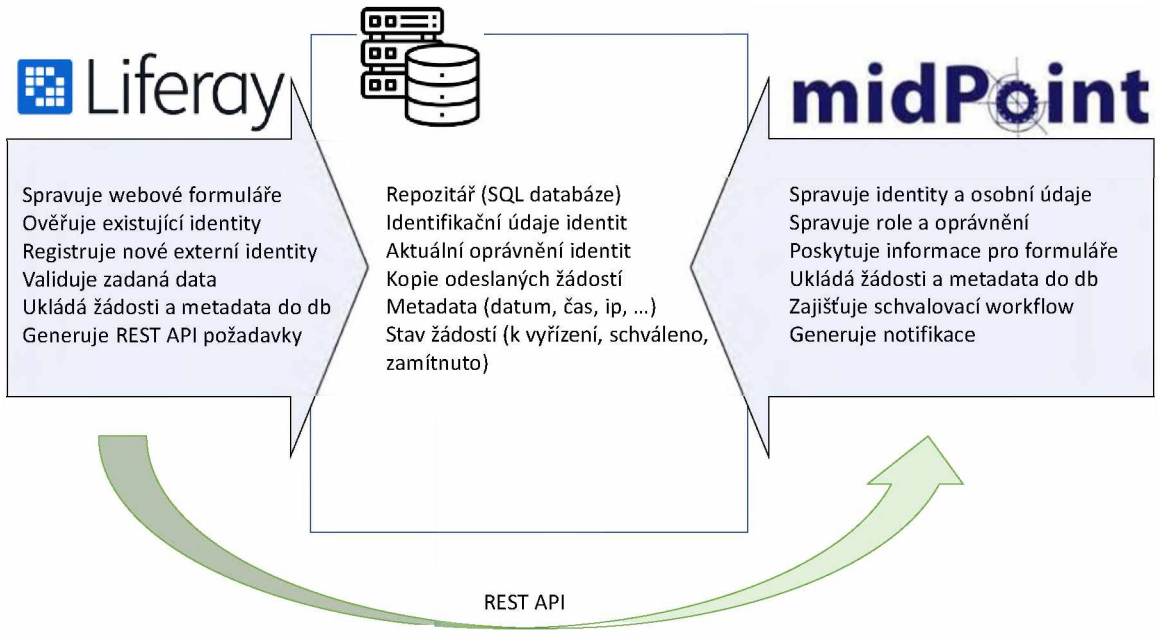
1 INTEGRACE IDM A LIFERAY

IDM a LifeRay (LR) formuláře jsou aktuálně integrovány v rámci aplikace pro reset hesel zaměstnanců a externistů. IDM poskytuje LR data o identitách (interních a externích) v rozsahu údajů potřebných pro ověření uživatele, který žádá o změnu hesla. Po ověření žadatele zasílá LR nové heslo na REST API systému IDM. IDM po změně hesla notifikuje uživatele formou SMS a emailové zprávy.

Stávající integrace využívá SQL tabulku pro ukládání dat, která je ze strany IDM plněna údaji o identitách. Tabulka je pro LR přístupná i pro zápis, je proto možné, v případě potřeby, zapisovat do stejné tabulky data i ze strany LR formulářů. Tato konfigurace se během provozu osvědčila, navrhujeme proto tuto strukturu zachovat a pro další formuláře pouze rozšiřovat schéma dat v SQL tabulce/tabulkách.

1.1 Rozšíření stávávající integrace

Formuláře LR lze v kombinaci s IDM využít i v dalších případech. Podle aktuálního stavu implementace IDM lze například zakládat nové identity (interní i externí), u stávajících identit lze aktualizovat vybrané atributy (které nejsou aktualizovány z HR systému), lze využít mechanizmus schvalovacích workflow, která jsou součástí IDM apod. Ve všech těchto případech se jedná na straně LR o sběr dat a ověření žadatele, samotné změny údajů a další operace již probíhají na straně IDM. Informace o výsledcích registračních/schvalovacích procesů lze poté ukládat zpět do SQL tabulky, a jsou tím pádem přístupné webové aplikaci LR.



Při integraci LR a IDM je nutné průběžně zohledňovat primární funkce IDM, tj. správu identit, jejich životního cyklu a evidenci oprávnění do navazujících koncových systémů. IDM může v omezené míře evidovat a zpracovávat i evidenční údaje mimo standardní rozsah, nicméně toto není jeho hlavním účelem. Volba formulářů by měla korespondovat s hlavními funkcemi IDM a

formuláře by měly být integrovány s IDM pouze v případech, kdy IDM spravuje a řídí dané objekty (oprávnění do koncových systémů, evidenční data identit apod.).

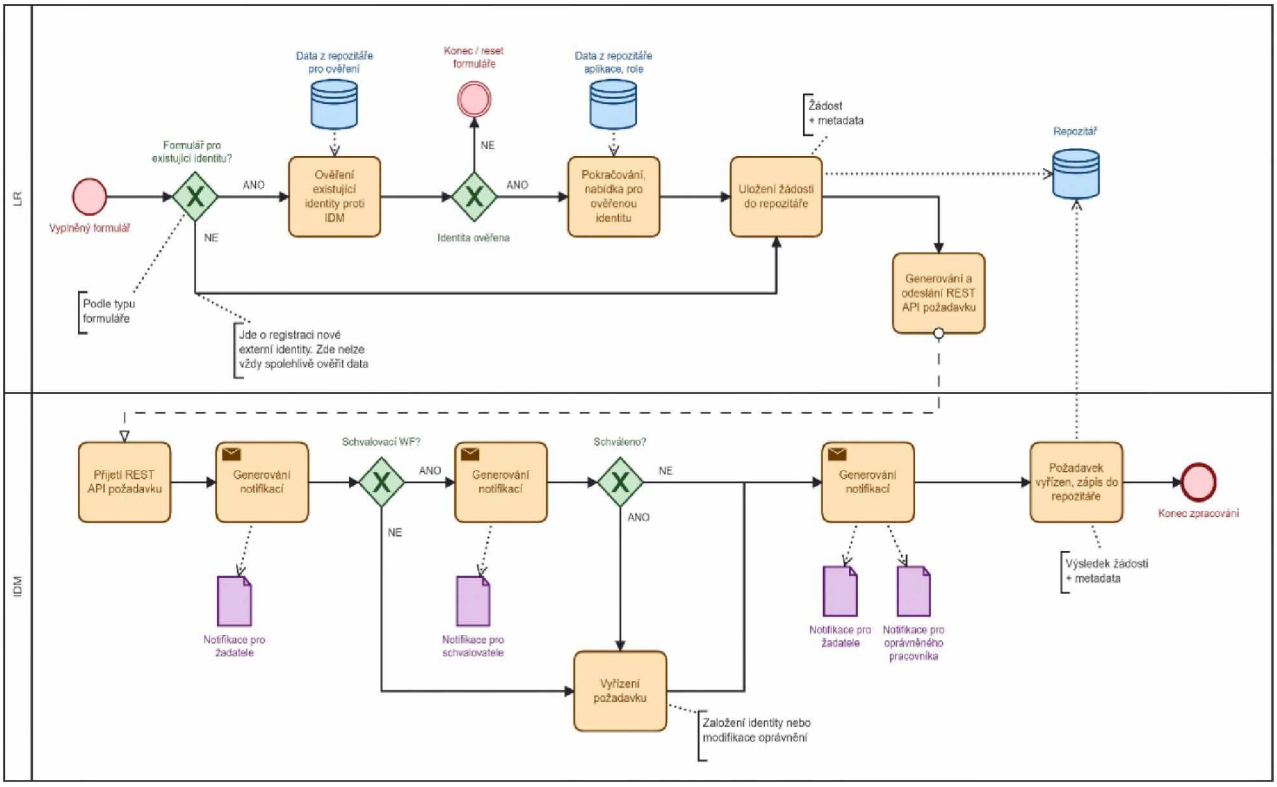
1.2 Technické předpoklady integrace

Oba koncové systémy (LR a IDM) jsou již v prostředí ŘSD plně implementovány. Hlavním požadavkem integrace je proto zřízení společného uložiště (repozitáře), kam budou mít oba systémy přístup ke čtení a zápisu. Podle konkrétního formuláře musí být možné strukturu repozitáře modifikovat. Tyto modifikace vyplynou z analýzy, která je součástí přípravy konkrétního formuláře.

LR je webová aplikace přístupná z internetu, je zde nutné zabezpečit ochranu proti útokům a zároveň zajistit ochranu vytvořeného repozitáře, který obsahuje osobní údaje identit.

LR ve vybraných případech posílá data přímo na API systému IDM. K tomuto účelu bude zřízen v systému IDM zvláštní účet s potřebným oprávněním. Tento účet bude používán pouze k účelům komunikace s LR. Na straně IDM lze vytvořit více takových účtů a jednotlivé formuláře tak mohou pracovat pouze s nezbytným minimem oprávnění k objektům v IDM.

1.3 Návrh procesu



2 REGISTRACE IDENTIT

Na základě diskuzí se zástupci ŘSD a jejich požadavků byl vytvořen tento dokument, který slouží, jako podklad pro nabídku na realizaci napojení a úprav webové aplikace formulare.rsd.cz, kdy část

aplikace sloužící pro registraci nových uživatelů s žádostí o nové přístupy do systémů bude napojena na IDM, ve kterém bude vytvořeno schvalovací workflow pro schválení přístupu žadatelů do daného systému.

2.1 Webový formulář pro registraci identit a žádosti o oprávnění (LR)

Požaduje údaje o **externí** identitě minimálně v rozsahu:

- Jméno, příjmení, název společnosti
- Identifikátor kontraktu (konzistentní s evidencí v IDM)
- Kontaktní údaje (mobilní telefon a emailová adresa)

Pro **existující** identitu navíc přidělené osobní číslo, případně aktuální organizační útvar.

Seznam aplikací, do kterých žádá o přístup, případně seznam rolí (konkrétních oprávnění do aplikací).

Formulář může být předvyplněn daty z repozitáře. Může obsahovat seznam aplikací a rolí, o které je možné žádat. Nezobrazuje osobní údaje.

Formulář určen pro identity již evidované v IDM provede **ověření žadatele** (SMS token na mobilní telefon, odesláním linku na email apod.)

Formulář pro registraci nových externích identit **nebude** obsahovat žádná další data o aplikacích, případně konkrétních oprávněních. Nové externí identity nelze při registraci spolehlivě ověřit.

Formulář je **zabezpečen** proti útokům z internetu a pro autentizaci v IDM API používá výhradně k tomu určené IDM účty.

Další údaje podle potřeby (Cookies, GDPR souhlas, Captcha, ...).

2.2 Repozitář / společné uložiště LR a IDM (SQL databáze)

Obsahuje evidenci všech dat zaslaných konkrétním formulářem, včetně potřebných meta-dat (datum a čas odeslání žádosti, alternativně IP adresy a pod).

Obsahuje data poskytovaná IDM v rozsahu potřebném pro předvyplnění konkrétního formuláře (např. seznam rolí k dané aplikaci).

Obsahuje nezbytné osobní údaje všech identit z IDM, potřebné k ověření žadatele. Tyto údaje nejsou formulářem zobrazovány, jsou použity k validaci zadaných dat.

2.3 IDM (midPoint)

Eviduje všechny identity (interní i externí)

Po přijetí požadavku ze strany LR zajistí spuštění schvalovacího workflow. V případě, že schvalování není vyžadováno, provede danou operaci ihned.

V rámci schvalovacího workflow zajistí notifikace na příslušné schvalovatele, notifikaci o přijetí požadavku na žadatele (pokud se nejedná o registraci nové externí identity) a po ukončení workflow zpracuje výsledek. Po schválení požadavku provede změny, v každém případě (tj. i při

zamítnutí) notifikuje žadatele a pověřeného zaměstnance ŘSD o výsledku a výsledek žádosti uloží do společného repozitáře.

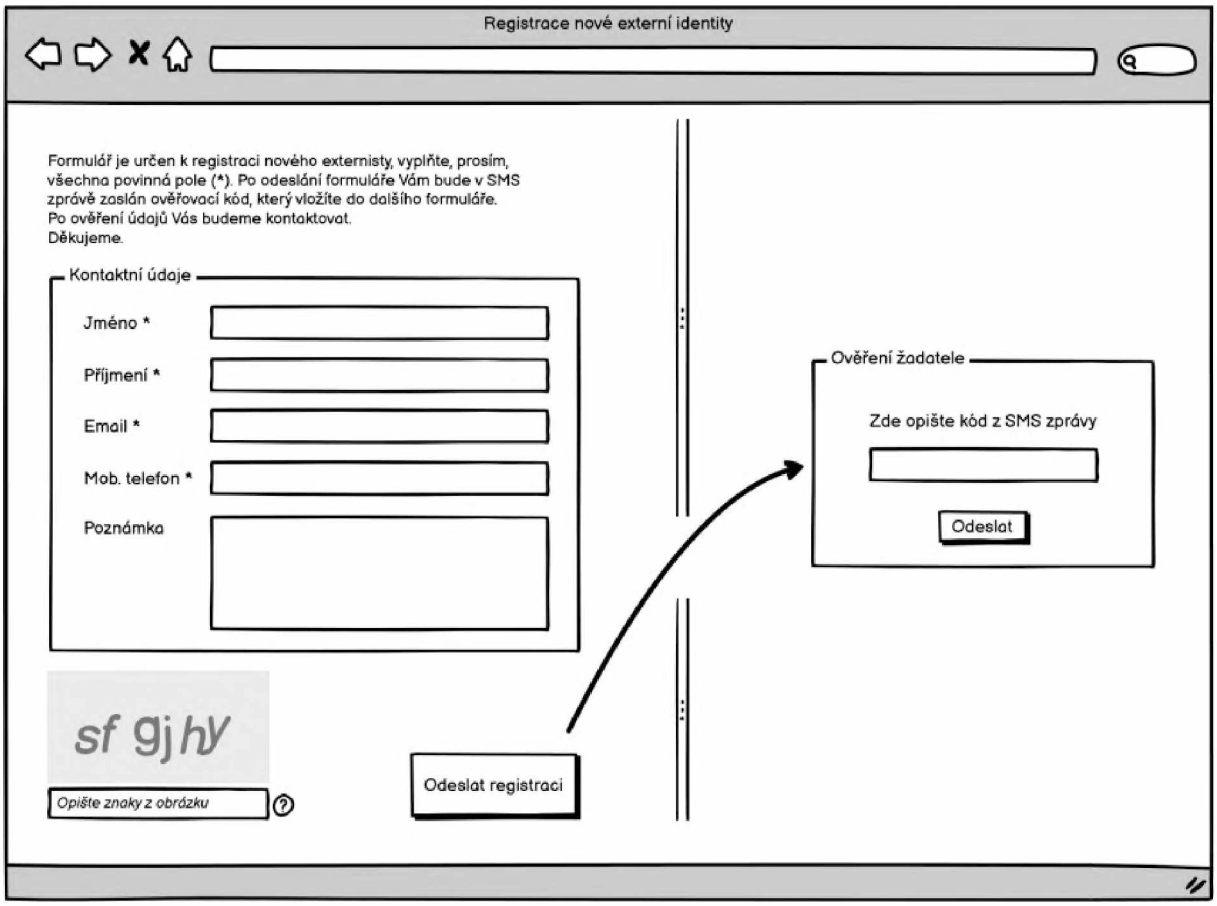
2.4 Alternativní způsob komunikace LR a IDM

Výchozí nastavení předpokládá ukládání žádostí na straně LR do repozitáře a okamžité odesílání požadavku na API IDM. Po vyřízení požadavku IDM aktualizuje záznam v repozitáři (doplní „výsledek" žádosti).

Alternativně lze uvažovat i o konfiguraci, kdy LR pouze ukládá žádosti do repozitáře, opatří je příznakem „k vyřízení" a IDM tyto požadavky vyřizuje dávkově formou naplánovaných úloh v předem určených časech. Toto řešení bude vhodné v případech, kdy lze očekávat vyšší frekvenci žádostí/registrací a je žádoucí regulovat vytížení ŘSD systémů. Zbytek procesu je již stejný, IDM rozesílá notifikace a ukládá výsledky žádostí do repozitáře.

2.5 Návrhy a příklady formulářů

2.5.1 Formulář registrace nové externí identity



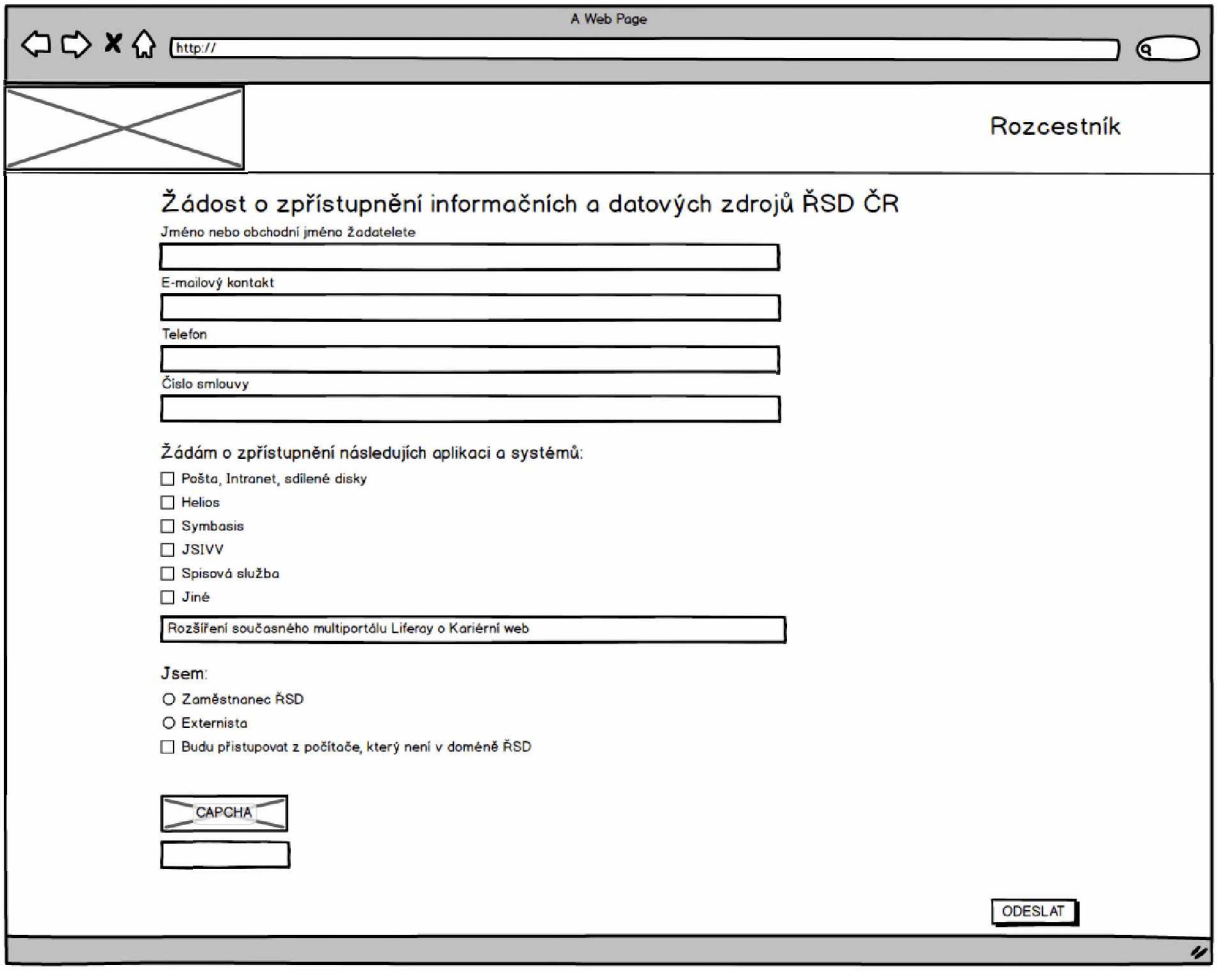
LR
při registraci validuje data ve formuláři (formát emailu a mobilního telefonu), formálně ověří správnost údajů (pokud bude např. povinné DIČ a pod) ukládá data o žádosti do repozitáře odesílá REST API požadavek na IDM.

IDM
přijme REST API požadavek kzaloží požadavek za založení nové identity pověřený pracovník ŘSD obdrží žádost o schválení nové identity žádost **zamítnuta**: IDM notifikuje žadatele, ukládá výsledek žádosti do repozitáře žádost **schválena**: IDM založí identitu, přiřadí výchozí sadu rolí/oprávnění, notifikuje žadatele, odesílá login emailem, heslo SMS zprávou, výsledek žádosti ukládá do repozitáře.

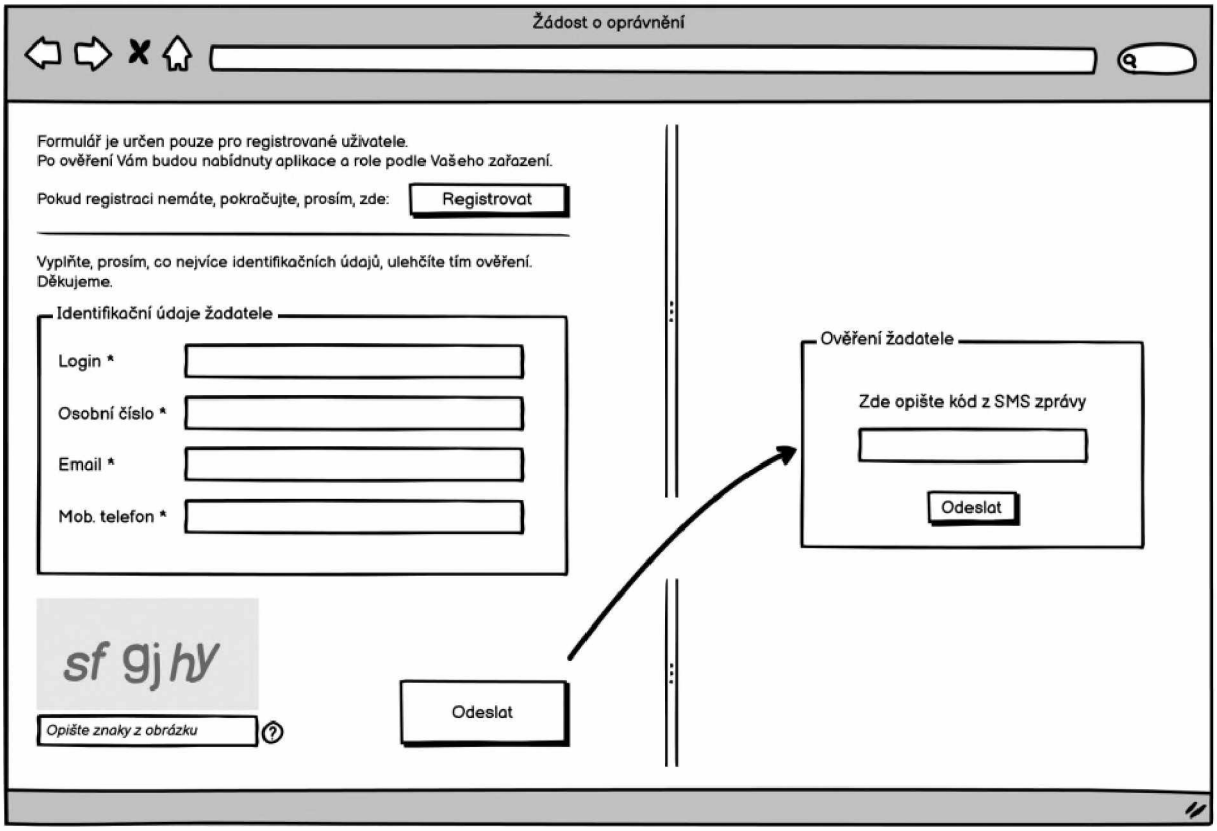
2.5.1.1 Registrace nového uživatele

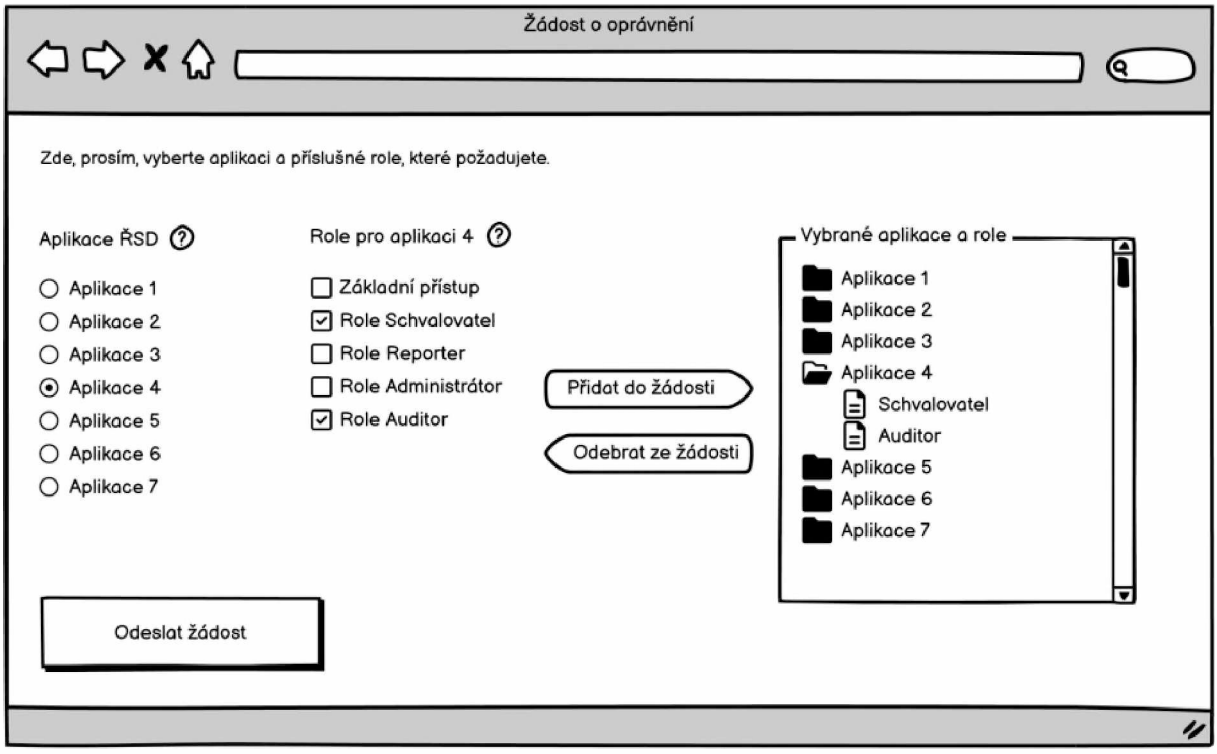
Na základě požadavku ze strany ŘSD, dojde k vytvoření formuláře pro registraci externistů dle výše popsaného principu fungování.

Wireframe formuláře



2.5.2 Formulář žádosti o přístup/oprávnění do aplikace ŘSD (pro existující identity)





Formulář požaduje základní identifikační údaje (osobní číslo, login, email, telefon), na základě kterých ověří identitu odesláním SMS tokenu. Po úspěšném ověření proces pokračuje. Na základě ověření LR zobrazuje potenciální možnosti, seznam aplikací a seznam rolí. Volitelně formulář nemusí zobrazovat aplikace a oprávnění, které již identita má (pro přehlednost). Opakovaná žádost zbytečně vyvolává schvalovací workflow. Ukládá data žádosti do repozitáře. Odesílá REST API požadavek na IDM.

IDM
přijme REST API požadavek založí požadavek na přidělení/změnu oprávnění pověřený pracovník ŘSD obdrží žádost o schválení nových oprávnění žádost **zamítnuta**: IDM notifikuje žadatele, ukládá výsledek žádosti do repozitáře žádost **schválena**: IDM přidělí/upraví oprávnění, notifikuje notifikuje žadatele a výsledek žádosti ukládá do repozitáře.

Ve **výjimečných** případech lze formuláře kombinovat, např. spojit registraci identity s žádostí o přístup do interních systémů. Zde je nutné pamatovat na možnost, že oba tyto procesy (založení identity a žádost o oprávnění) mohou mít nastaveno workflow, kde může dojít k zamítnutí, tj. bude nutné adekvátně upravit systém notifikací směrem k žadateli. Dále je nutné pečlivě zvážit rozsah zobrazovaných údajů, pokud se jedná o registraci nové externí identity, u které nelze spolehlivě validovat vložené údaje.

2.5.2.1 Formulář ISUDAS

Aktuální stav

Aplikační role ISUDaS jsou v systému IDM založeny a oprávnění uživatelů mohou proto být aktivně řízena systémem IDM. Řízení oprávnění ISUDaS bude realizováno v rozsahu přidávání a odebírání uživatelů v definovaných Active Directory skupinách. Ve výchozím nastavení jde o skupiny v „OU=ISUDaS,OU=RSD_Skupiny,DC=rsd,DC=cz“. Členství ve skupinách Active Directory znamená, že uživatel dané oprávnění vlastní.

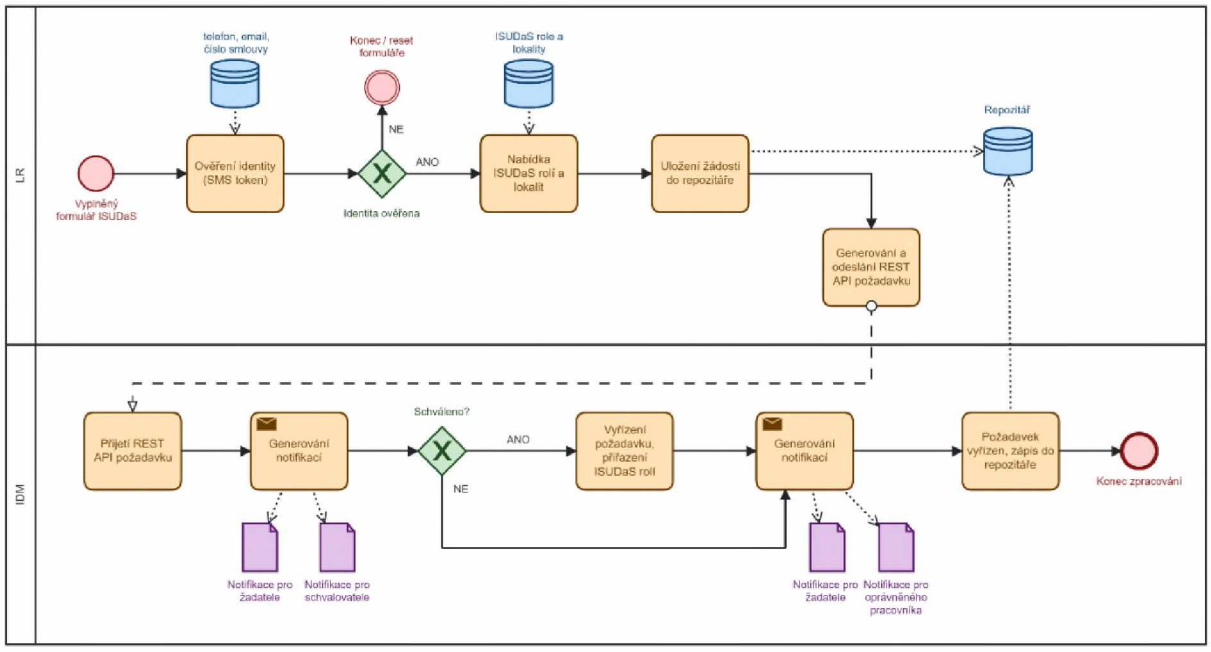
Technické předpoklady

Formulář ISUDaS je určen výhradně pro existující identity. Před samotným zadáním požadavků na jednotlivá oprávnění bude proto daný žadatel ověřen. Aktuální ověřovací mechanizmus je SMS token, který bude žadateli odeslán formou SMS zprávy na mobilní telefon, který je u něj evidován v IDM. V případě, že telefon není evidován nebo je neplatný, nemůže ověření proběhnout a proces se ukončí.

Nabídka rolí pro daného (ověřeného) žadatele může být upřesněna databázovým dotazem na již existující oprávnění a lze proto tuto nabídku dynamicky měnit. Je proto v rámci implementace důležité definovat sadu rolí, kterou bude formulář žadateli nabízet.

Požadavek na přidání rolí bude formulářem odeslán jako REST požadavek na aplikační rozhraní IDM.

Návrh procesu



Repozitář / společné uložiště LR a IDM

Data v repozitáři budou doplněna o aktuální ISUDaS role a jejich aktuální držitele.

Požadavky odeslané ISUDaS formulářem budou v repozitáři evidovány.

Dále bude repozitář doplněn o další data, potřebná k vygenerování REST požadavku na IDM.

IDM (midPoint)

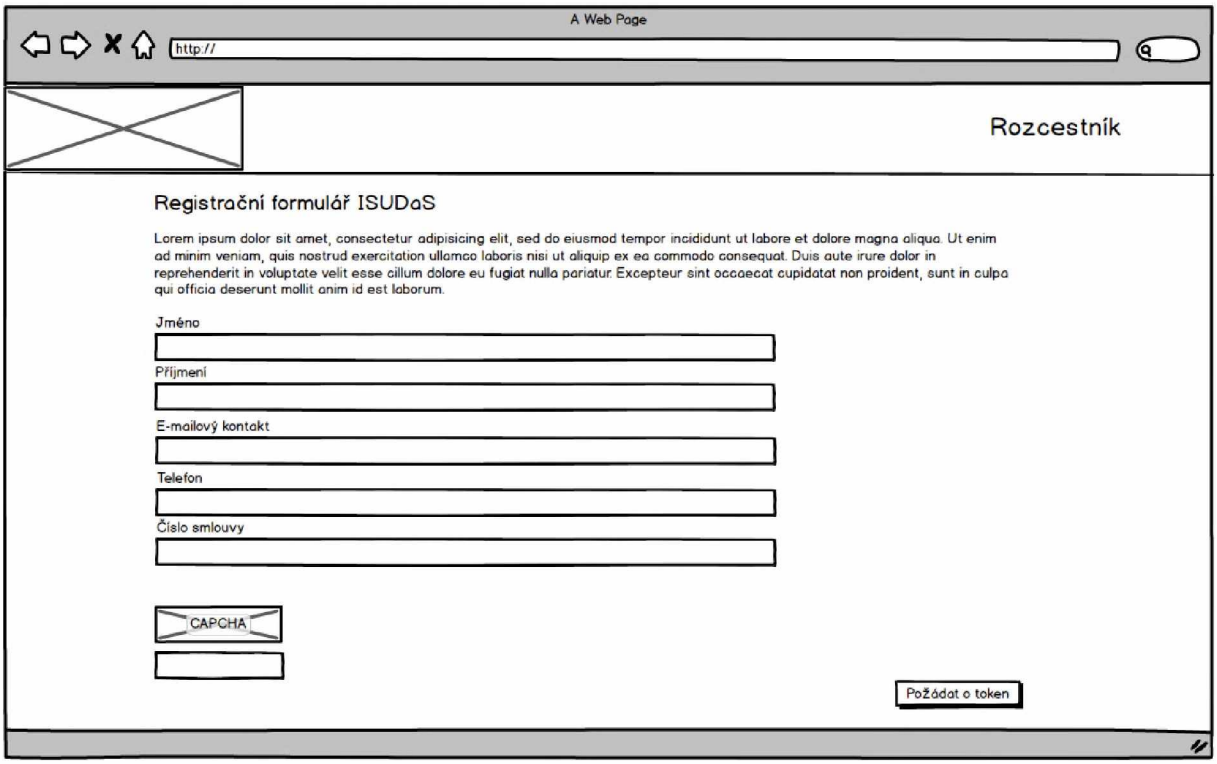
K rolím ISUDaS bude v IDM doplněn schvalovatel/vlastník role, který bude oprávněn schvalovat přidělování rolí.

Bude nastaven obsah notifikací, odesílaných v jednotlivých fázích procesu.

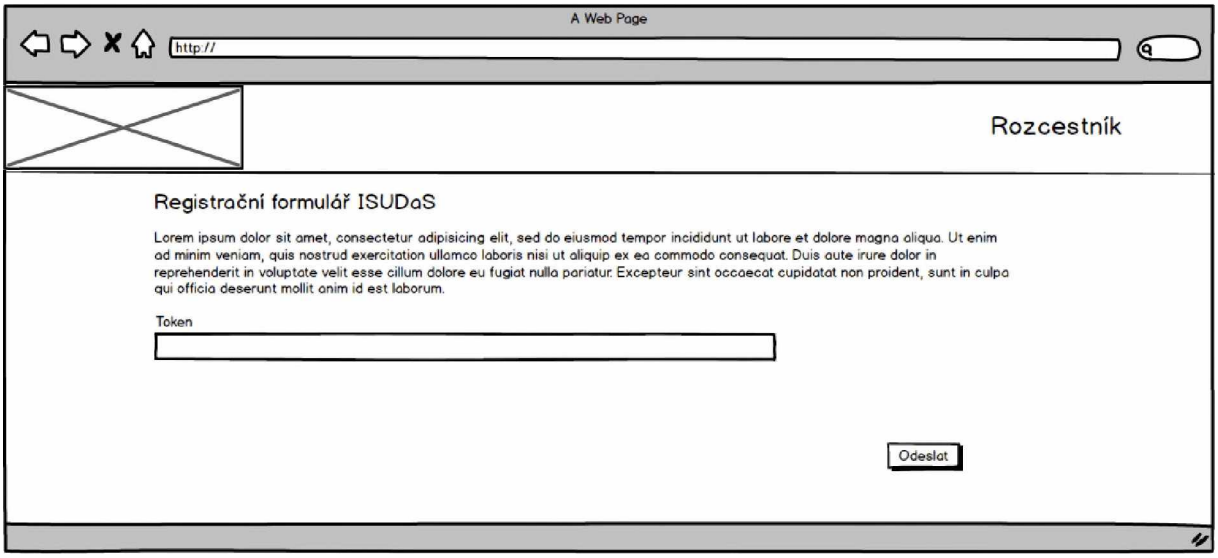
Bude nastaven proces přenosu a aktualizace dat směrem z IDM do společného repozitáře.

Wireframe formuláře

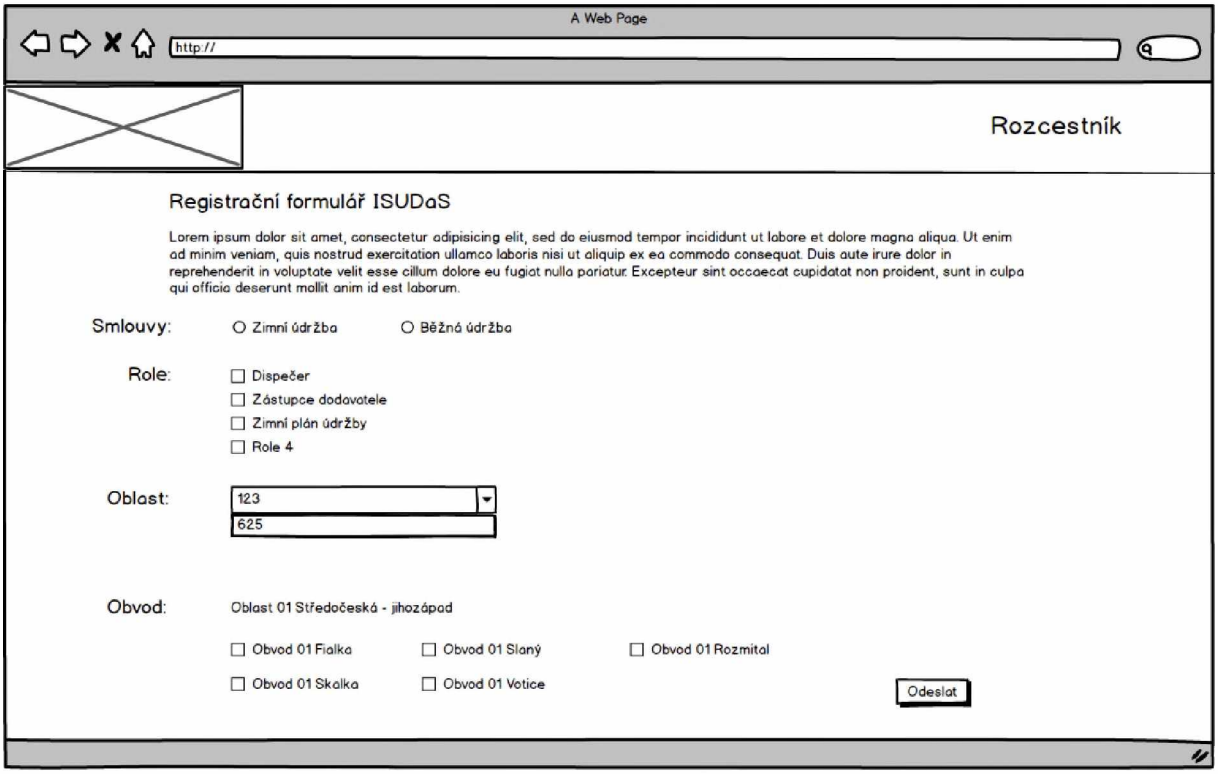
- Úvodní stránka, pro vyplnění údajů žadatele.



Ověření identity žadatele pomocí tokenu.



Samotná žádost o přístup.



3 ROZVOJOVÝ POŽADAVEK PORTÁLU PRO RESET HESLA

3.1 Specifikace požadavku

Dalším požadavkem ze strany ŘSD, bylo rozšíření portálu pro reset hesla o možnost zajištění resetu hesla osobám na pozici dělník. Reset hesla pro takové uživatele je zajištěn tím způsobem, že je o něj možno požádat pouze ve vnitřní síti ŘSD, kdy resetované, nové heslo je zasláno nadřízené osobě dané osoby.

3.2 Podoba formuláře

4 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 zafixování potřeb, integrací a oblastí služeb.

5 HARMONOGRAM

Společnost IBA počítá s dobou trvání projektu do **3 měsíců** od případné akceptace nabídky, avšak tento termín považuje za nejzazší. Za předpokladu využití paralelního zapojení všech účastníků na projektu a aktivní součinnosti zúčastněných stran, může být tento termín i dřívější.

6 CENA

6.1 Nabídková cena

Níže uvedená cena představuje sumu veškerých prací, potřebných k realizaci vytvoření aplikace a zajištění požadovaných rozvojových požadavků.

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	35,00	5 400,00 Kč	189 000 Kč
	programátor/kodér	MD	140,00	5 200,00 Kč	728 000 Kč
	Celkem		175,00	Cena celkem	917 000,00 Kč

Celková maximální cena realizace je **917 000 Kč bez DPH**.

6.2 Fakturační milníky

Na základě akceptovaných předložených akceptačních protokolů ŘSD.

Digitálně podepsal [redacted]
Datum: 2023.02.23 17:34:03 +01'00'

Digitálně podepsal: [redacted]
Datum: 23.02.2023 14:15:43 +01:00