



## OBJEDNÁVKA č. 70 084/25

**Vyřizuje/Telefon:** P. Kostrhová / +420 224 969 292

**Termín plnění:** do 31.7.2025

**Záruční doba:**

**Místo plnění:** VFN, U Nemocnice 2, Praha 2

Odbor provozu IT

**Osoba oprávněná k převzetí předmětu plnění**

Bc. Zbyněk Pecka

Tel.: 725 070 471

[zbynek.pecka@vfn.cz](mailto:zbynek.pecka@vfn.cz)

**Dodavatel:** BCV solutions s.r.o.

7. Května 1168/70

149 00 Praha 4

**IČ:** 28360851 **DIČ:** CZ28360851

**Kontakt:**

**Tel./e-mail:** [lucie.cirkvova@idstory.com](mailto:lucie.cirkvova@idstory.com)

| Číslo položky | Předmět plnění                                                                                      | Cena za MJ bez DPH | Sazba DPH | Cena za MJ s DPH | Množství (hod) | Cena za položku včetně DPH |
|---------------|-----------------------------------------------------------------------------------------------------|--------------------|-----------|------------------|----------------|----------------------------|
| 1             | API rozhraní IdM - FONS Enterprise (58,5 MD)                                                        | 2 000,00 Kč        | 21%       | 2 420,00 Kč      | 468            | 1 132 560,00 Kč            |
| 2             | Sleva 3%                                                                                            | 28 080,00 Kč       | 21%       | 33 976,80 Kč     | 1              | 33 976,80 Kč               |
|               | Dle podmínek smlouvy č. PO 835/S/23 - 28/24<br>Na základě nabídky uvedené v příloze této objednávky |                    |           |                  |                |                            |

|                                                                                                                 |                            |                        |
|-----------------------------------------------------------------------------------------------------------------|----------------------------|------------------------|
| <b>Fakturační adresa</b>                                                                                        | <b>Cena celkem bez DPH</b> | <b>907 920,00 Kč</b>   |
| Všeobecná fakultní nemocnice v Praze<br>Ekonomický úsek - Odbor účetnictví<br>U Nemocnice 499/2, 128 08 Praha 2 | <b>Cena celkem s DPH</b>   | <b>1 098 583,20 Kč</b> |

Platba po dodání. Na fakturu a dodací list/akceptační protokol uveďte číslo této objednávky. PP je možno dodat ihned po oboustranném podepsání objednávky. Celková cena uvedená v objednávce je konečná a nejvýše přípustná pro PP dle specifikace v objednávce. Celkovou cenu lze překročit pouze při prokazatelné změně DPH, a to pouze ve výši shodné s tímto navýšením. Celková cena zahrnuje veškeré náklady spojené s realizací PP. Prodávající je povinen, po vzniku práva fakturovat, vystavit a objednateli předat fakturu ve dvojím vyhotovení s rozepsáním položek PP přesně dle objednávky a uvedením jejich jednotkových cen. K faktuře bude přiložena kopie řádně opatřeného dodacího listu/akceptačního protokolu potvrzeného osobou oprávněnou k převzetí/akceptaci PP s uvedením záruční doby PP a v případě relevance s uvedením všech výrobních, sériových a produktových čísel – bez tohoto dokladu nelze fakturu proplatit. Vystavená faktura musí obsahovat všechny náležitosti řádného daňového dokladu dle platné právní úpravy. V případě, že faktura nebude obsahovat všechny požadované náležitosti, je oprávněn ji objednatel do 15 dnů prodávajícímu vrátit k opravě a doplnění. Dnem nového doručení faktury začíná běžet nová lhůta splatnosti faktury. Splatnost faktury se sjednává na 60 dní ode dne jejího doručení objednateli. V případě prodlení objednatele s úhradou řádně fakturované ceny je prodávající oprávněn požadovat zaplacení smluvního úroku z prodlení ve výši 0,01 % z nezaplacené částky za každý i započatý den prodlení. Prodávající je oprávněn požadovat zaplacení úroku z prodlení až po uplynutí 30 dnů od sjednané lhůty splatnosti. Objednatel je oprávněn požadovat zaplacení smluvní pokuty ve výši 0,1% z celkové kupní ceny bez DPH za každý i započatý den prodlení s dodáním zboží. Faktura může být zaslána i elektronicky ve formátu PDF na adresu faktury@vfn.cz. Dodací list/akceptační protokol přiložen v nascanované podobě. Prodávající bere na vědomí, že dodávané technické nebo programové prostředky nesmí být prostředky, které jsou zveřejněny na stránkách Národního centra kybernetické bezpečnosti (provozované NÚKIB, <https://www.govcert.cz/>) a označeny jako hrozba v době uzavření objednávky. Veškeré poskytované služby nesmí být provozovány na výše uvedených technických nebo programových prostředcích označených NÚKIB jako hrozba. Prodávající bere na vědomí, že objednatel je povinen dle zákona č. 340/2015 Sb. o registru smluv, ve znění pozdějších předpisů, uveřejnit tuto objednávku včetně případných dodatků zákonem stanoveným způsobem.

**Počet listů:** -1- **Přílohy:** 1/14 **Poznámka:** NS 15081

**Objednávku přijímám a souhlasím s podmínkami**

|                     |                                                                                                             |
|---------------------|-------------------------------------------------------------------------------------------------------------|
| <b>Datum:</b>       | Datum: 20.3.2025                                                                                            |
| <b>Prodávající:</b> | <b>Objednatel:</b><br><br>Ing. Michal Jelínek<br>Náměstek ředitele pro Informatiku a digitální transformaci |
| <b>Razítko:</b>     |                                                                                                             |



# **NÁVRH ŘEŠENÍ NAPOJENÍ FONS ENTERPRISE**



**VFN PRAHA**

## POPIS ŘEŠENÍ

Tento dokument mapuje potřebu VFN napojit do IdM systém FONS Enterprise (dále jen FE). Cílem je, aby IdM spravovalo základní operace nad uživateli (vytvoření, aktualizace), blokaci v systému po odchodu zaměstnance, nebo po přechodu do mimo evidenčních stavů. Dále se jedná o propagaci certifikátu daného zaměstnance a jeho aktualizaci (především sériové číslo) a oprávnění v tomto systému na základě pracovních smluv z personálního systému OKbase.

Zdrojem pro výše uvedená data bude IdM, které čerpá z personálního systému OKbase (uživatelé, organizační struktura a pracovní smlouvy) a certifikační autority elidentity (certifikáty).

## Relevantní architektura FONS ENTERPRISE (dále FE)

Z pohledu IdM jsou podstatné dvě entity: uživatel a skupina - integrace řeší, jak bude IdM do FE předávat uživatele a skupiny. Definici oprávnění pro jednotlivé skupiny v rámci FE už bude klikat ručně administrátor FE v této aplikaci.

## Uživatel

Uživatelem je fyzická osoba, která má standardní atributy a specifická EAVs (systém FONS Enterprise operuje s atributy workplaceCode a workplaceCodeDefault, ty jsou ale nepovinné). V prostředí VFN se uživatelem s účtem v FE mohou stát následující skupiny:

- zaměstnanci VFN (zdroj: OKbase),
- externí spolupracovníci (zdroj: manuální zadání ze strany dispečinku),
- studenti 1. lékařské fakulty (zdroj: import dat na základě předání studijního oddělení).

Při propisování do FE je nutné brát ohled na to, že každá skupina nemusí mít k dispozici všechny atributy předchozí skupiny. Jmenovitě se jedná například o následující atributy:

- certifikát,
- název pracovní pozice,
- kód kliniky.

Primárním zdrojem uživatelů je OKbase, na základě jejich existence a jejich kontraktů je bude propagovat do FE.

## Skupina

Skupina je nositelem oprávnění v systému FONS Enterprise, uživatel může mít přidělenou jednu a více skupin, jde tedy o mechanismus ekvivalentní rolím v IdM.

IdM bude do FE zakládat skupiny a spravovat jejich přiřazení uživatelům, nebude ale jejich primárním zdrojem. Tím bude v jistém smyslu také OKbase, přičemž logika je:

- každá smlouva (kontrakt) v OKbase znamená právě jednu skupinu
- kód skupiny se odvozuje z atributů kontraktu

IdM tedy bude vytvářet kódy skupin a v případě, že dosud v FE neexistují, je tam zakládat, avšak slouží jako prostředník/překladatel mezi OKbase a FE, IdM si je nevymýšlí ani se v něm ručně neupravují.

V rámci přidělování a odebírání skupin je nutné počítat s typem uživatelů, který nemá k dispozici data o úvazku/PPV (smluvní vztah z VFN je na základě jiné smlouvy než pracovněprávní vztah) - například studenti a externí spolupracovníci.

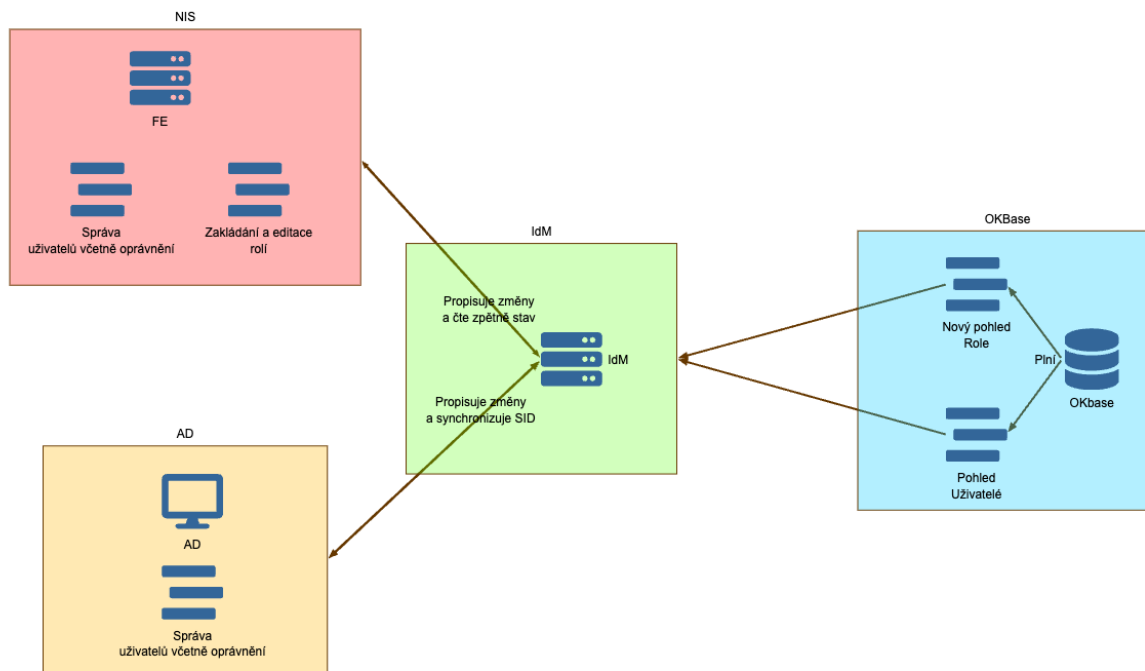
## FE API

Pro komunikaci mezi IdM a FE bude na straně FE implementováno REST API, jehož návrh je v dokumentu <https://redmine.bcvolutions.eu/attachments/11200>.

Autentizace bude probíhat přes Basic Auth či Bearer token a obsahuje endpointy pro kompletní správu uživatelů, skupin a správu přidělení skupin uživatelům, to je dostačující k tomu napsat REST API konektor pro FE poskytující veškerou potřebnou funkčnost.

FE API pro editaci uživatele používá v URL interní identifikátor uživatele `userId`, s čímž nemáme problém, pro takové případy slouží atribut `uid` na `SysSystemEntity` (coby obrazu uživatele v cílovém systému).

# Implementace na straně IdM



Přirozený přístup z hlediska IdM je skupiny reprezentovat jako role, best practice je pak oddělit správu skupin jako takových od zbytku funkčnosti. To pak vede na dvě samostatné komponenty řešení, správu skupin a správu uživatelů a jejich skupin.

## Správa skupin

V rámci implementace konektoru pro FE dojde k oddělení částí pro správu uživatelů a skupin. V rámci connid se jedná o objekty typu `__ACCOUNT__` a `__GROUP__` další podporované objekty nebude nutné v IdM spravovat.

Tato komponenta by při (pravděpodobně noční) synchronizaci přišla na řadu jako první a provedla by následující

1. načtení všech kontraktů z OKbase
  - zde je doporučeno provést transformaci přímo ve výměníku z HR,
  - ve výměníku bude vytvořena nová struktura (pohled), která bude obsahovat všechny aktivní pozice a složení jejich názvů workCode atd.
  - IdM bude pomocí rekonciliace tyto data synchronizovat,
  - v IdM nebude docházet k mazání těchto záznamů - v případě smazání bude pouze tento případ logován,
  - pro mazání je možné použít jednorázovou mazací rekonciliaci, kterou bude pouštět administrátor manuálně.
2. založení příslušných neexistujících rolí v IdM

3. zjištění existujících skupin v FE
4. založení neexistujících skupin v FE

## Správa uživatelů a jejich skupin

Po doběhnutí předchozí fáze synchronizace bude v IdM připraveno vše potřebné pro aktualizaci uživatelů a jejich skupin. Druhá funkční komponenta bude:

1. načetla z OKbase uživatele a jejich kontrakty
2. aktualizovala uživatele v IdM
3. aktualizovala přidělení rolí v IdM odpovídajících FE skupinám
4. poslala do FE aktualizované uživatele a přidělení skupin na základě přidělených rolí v IdM

## Mazání skupin

Předchozí fáze se postarají o to, že v FE budou všichni uživatelé a budou mít přidělené správné skupiny. Neřeší však problém, že se některé skupiny mohou stát obsoleté (třeba když úplně zanikne nějaké oddělení) a FE se o tom nedozví.

Pro tento případ by mohla do budoucna následovat třetí fáze:

1. dotažení skupin z FE
2. zjištění, které skupiny už nejsou podle IdM použité
3. odeslání smazání nepoužívaných skupin do FE

Mazání skupin není v tuto chvíli součástí projektu – bude diskutováno a případně řešeno po nasazení do produkce.

# Základní technický návrh napojení v konektoru

Konektor musí mít konfigurovatelné položky. V základu se bude jednat o tyto:

- host,
- jméno/heslo (GuardedString),
- token (GuardedString),
- definici názvu unikátního atributu (userId).

Jednotlivé endpointy není aktuálně nutné vyjmenovávat (pravděpodobnost změny je nízká - rozdíl oproti host/ip).

Konektor bude implementovat operace pro dva typy entit `__ACCOUNT__` a `__GROUP__` (rozdělení v kódu lze zajistit pomocí `ObjectClass`). Na základě dat z REST API FE je nutné automaticky definovat a vytvářet schéma systému (zde výrazně doporučuji jít touto cestou v případě dalších rozvojů tohoto systému konzultantem).

Pro každý objekt bude podporovat následující operace v konektoru:

- create,
- update,
- delete,
- schema,
- createFilterTranslator,
- executeQuery (rekonciliace a get) - synchronizace deltou není potřeba implementovat.

Pro spojení s RESTem FE je možné využít již zavedenou Unirest kong závislost – více v dokumentaci produktu.

## Počáteční napojení

V současné době už ve FE jsou tisíce uživatelů, kteří mají přidělené nějaké skupiny, součástí řešení tedy musí mít úvodní porovnání tohoto stavu s tím, co by po napojení poslalo IdM, tedy rozdílový report a řešení nesrovnalostí.

Uživatelé jsou nyní do FE (včetně dalších atributů) zakládání manuálně od vícero uživatelů (jmenovitě M. Šnoblůvá - správce certifikační autority, konzultanti Stapro, Dispečink). Výrazně doporučujeme před napojením provést linkovací/párovací synchronizaci a data porovnat.

## Spravované atributy

Pro kompletní seznam všech spravovaných atributů doporučuji pročíst poskytnutý dokument s popisem FE API. Zároveň před samotným napojením bude potřeba revidovat aktuální napojení na systém Medea a projít atributy, zda nějaké nechybí a případně si říct, zda je přenášet.

Kvůli případnému budoucímu rozšiřování a dalšímu vývoji bych byl proto nepsat v konektoru nic způsobem "natvrdo". Mapování atributů IdM - Medea udělat na základě dynamicky vygenerovaného schématu a mapování v IdM.

## Odstavení původního NIS

Po přechodu na FE bude nutné vymyslet plán odstavení původního NIS Medea - v implementaci konektoru se s tímto musí počítat především při implementaci rekonsiliace, kde bude nutné provádět porovnání dat mezi IdM x FE x Medea. K samotnému odstavení bude možné použít funkci readOnly/disabled na systému samotném.

V prostředí VFN se předpokládá, že bude nutné vypínat správu účtů v původním NIS a zapnout ji v novém NIS postupně (pravděpodobně dle klinik?). Pokud se půjde tímto způsobem bude nutné vymyslet, jak deaktivovat propis pouze pro danou část uživatelů (processor na disable provisioningu atd.). Bohužel nepůjde použít skript v account managementu - účty budou již existovat. V případě že se půjde "velkým třeskem" je možné výše uvedenou implementaci vynechat.

# CENOVÁ KALKULACE

| POLOŽKA                                                                                                                                                                     | MD  | CENA v Kč<br>bez DPH |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----------------------|
| <b>Vývoj Konektoru</b>                                                                                                                                                      |     |                      |
| Návrh řešení                                                                                                                                                                | 2   | 32000                |
| <b>Správa skupin:</b>                                                                                                                                                       |     |                      |
| Implementace                                                                                                                                                                | 5   | 80000                |
| Automatické testy                                                                                                                                                           | 3   | 48000                |
| <b>Správa účtů:</b>                                                                                                                                                         |     |                      |
| Implementace                                                                                                                                                                | 5   | 80000                |
| Automatické testy                                                                                                                                                           | 2   | 32000                |
| <b>Řešení výstupů testování</b>                                                                                                                                             |     |                      |
| Vydání nové verze IdStory                                                                                                                                                   | 2   | 32000                |
| Projektové řízení                                                                                                                                                           | 1   | 16000                |
| <b>Celkem za vývoj konektoru</b>                                                                                                                                            |     | 320000               |
| <b>Nasazení konektoru v prostředí zákazníka</b>                                                                                                                             |     |                      |
| Úprava na straně výměníku: vytvoření nového pohledu ve výměníku (všechny aktivní pozice a složení jejich názvů workCode atd.), který bude udržovat role dle pozic uživatele | 5   | 80000                |
| Vytvoření nového systému v IdM                                                                                                                                              | 2   | 32000                |
| Synchronizace rolí z výměníku OKbase                                                                                                                                        | 2   | 32000                |
| Nový systém a mapování pro provisioning na FE pro identity (skripty, konfigurace, atd)                                                                                      | 4   | 64000                |
| Nový systém a mapování pro provisioning na FE pro role (skripty, konfigurace, atd)                                                                                          | 2   | 32000                |
| Automatická synchronizace SID z AD do IdM                                                                                                                                   | 2   | 32000                |
| Prvotní párování existujících účtů mezi IdM a FE a porovnání s Medea                                                                                                        | 4,5 | 72000                |
| Dokumentace nových napojení a změn pro stávající                                                                                                                            | 2   | 32000                |
| Řešení přechodu z Medea                                                                                                                                                     | 2   | 32000                |
| Přechod do produkce                                                                                                                                                         | 6   | 96000                |
| Projektové řízení za obě části                                                                                                                                              | 7   | 112000               |
| <b>Celkem za nasazení v prostředí VFN</b>                                                                                                                                   |     | 616000               |
| <b>Celková cena vývoj konektoru + nasazení</b>                                                                                                                              |     | <b>936 000</b>       |
| <b>Sleva pro VFN 3 %</b>                                                                                                                                                    |     | <b>28 080</b>        |
| <b>Nová cena pro VFN</b>                                                                                                                                                    |     | <b>907 920</b>       |

## **DODACÍ A FAKTURAČNÍ PODMÍNKY**

- Nabídka je platná do 30.03.2025.
- Splatnost faktur je nastavena dle smlouvy.
- Akceptace proběhne po přechodu do produkce. Podepsaný akceptační protokol je podkladem pro fakturaci.
- Všechny ceny jsou uvedeny bez DPH.
- Práce budou prováděny v pracovní době, tedy PO-PA 09-17.
- Nutnou podmínkou realizace prací, dle harmonogramu je dodání API FONS ze strany společnosti Stapro do 07.04.2025.

[illegible]

# PLATFORMA IDSTORY

IdStory je naše vlastní řešení automatizace správy identit na koncových systémech z jednoho místa. IdStory uchovává informace o všech důležitých událostech a změnách týkajících se životního cyklu identit. Platforma zahrnuje kromě IdM množství dalších modulů rozšiřujících jeho funkci v rámci oblasti IAM.



## IdM

Automatizace správy  
uživatelů  
Správa rolí  
Auditing  
Procesní řízení



## Access Manager

SSO  
Řízení přístupu k aplikacím  
Federace identit,  
Autentizace externí identitou



## Moduly

Synchronizace hesel z MS AD  
Recertifikace  
Resetu hesla  
certifikační autorita  
správy VPN  
SMS modul  
reporty  
,Správa technických účtů  
správy licencí  
Rozcestník

## VYBRANÉ REFERENCE



Ministerstvo zahraničních věcí  
České republiky



GENERALI  
INVESTMENTS



Český  
hydrometeorologický  
ústav



dpd



HYUNDAI



VŠEOBECNÁ FAKULTNÍ  
NEMOCNICE V PRAZE

# TĚŠÍME SE NA SPOLUPRÁCI

Web: [www.idstory.com](http://www.idstory.com)  
Telefon: +420 777 785 847  
Adresa: 7. května 1168/70, Praha 4 – Chodov 14900  
Email: [lucie.cirkvova@idstory.com](mailto:lucie.cirkvova@idstory.com)

Název: BCV solutions s. r. o.  
IČO/DIČ: 28360851/CZ28360851  
Sídlo : 7. KVĚTNA 1168/70, CHODOV, 149 00 PRAHA

