



Příloha č. 1 – Specifikace a rozsah předmětu plnění

1 Předmět plnění

Univerzita Karlova provozuje centralizovaně řadu systémů postavených na frameworku Verso. Byly realizovány v různém období během posledních patnácti let a při jejich implementaci byly uplatňovány rozdílné přístupy k práci s daty získávanými ze základních systémů univerzity, jako je personalistika či centrální autentizační služba.

Předmětem plnění je analýza a následná dodávka potřebných řešení pro

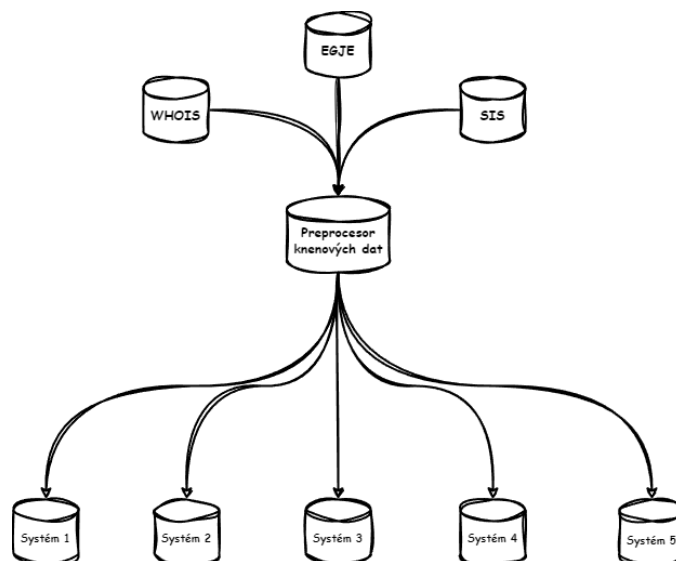
- preprocesor kmenových dat
- přesun stávajících instancí na nové databáze a virtuální servery (v součinnosti s univerzitními administrátory databází a serverů; dodávka samotných databází a serverů přitom není součástí plnění)
- rozšíření počtu provozovaných instancí
- jednotnou rekonfiguraci všech instancí
- doplnění jednotného záhlaví s novým univerzitním logem na uživatelské rozhraní všech instancí
- napojení všech stávajících i nově vzniklých instancí na preprocesor kmenových dat
- a tím vytvoření jednotného „ekosystému Verso“

Pro přehlednost uvádíme, že níže uvedené kapitoly 1.1 se vztahuje k dílčí části plnění veřejné zakázky probíhající v 1. fázi – dodání preprocesoru kmenových dat a souvisejících integračních skriptů, a body 1.2, 1.3 a 1.4 se pak vztahují k dílčí části plnění veřejné zakázky probíhající ve 2. fázi – rozšíření a zvýšení robustnosti architektury systémů Verso a revize integračních skriptů, a to v souladu s čl. 4.2 a 4.2 Výzvy k podání nabídek, jíž je tato specifikace přílohou.

1.1 Preprocesor kmenových dat

Preprocesor kmenových dat bude nový prvek v architektuře centralizovaných systémů Verso na UK. Jeho primárním účelem bude zprostředkovat připojení jednotlivých systémů Verso na ostatní systémy Univerzity Karlovy za účelem jejich integrace a výměny dat. V současné době se jedná především o integraci na centrální personální systém UK Whois, mzdový systém EGJE a studijní informační systém. Dále zprostředkuje integraci na personální systémy spolupracujících fakultních nemocnic.

Postavení preprocesoru v rámci architektury ekosystému Verso je naznačeno obecným schématem níže:



Preprocesor zajistí

- konverzi dat získávaných z těchto externích systémů do datové struktury Verso
- automatizovatelnou správu příznaků příslušnosti dat k jednotlivým součástem „ekosystému Verso“ (např. pro zajištění poskytování osobních údajů pouze do těch systémů, které jsou oprávněny s nimi pracovat)
- centralizovanou správu uživatelských oprávnění k jednotlivým částem „ekosystému Verso“

Preprocesor dále poskytne

- nástroj pro registraci externích uživatelů vstupujících do ekosystému Verso z prostředí mimo UK
- nástroj pro správu části uživatelských oprávnění, které nelze spravovat automatizovaně na základě údajů z personalistiky UK

1.1.1 Centralizovaná správa uživatelských oprávnění

Centralizovaná správa uživatelských oprávnění se opírá o principy kompozice rolí ve frameworku Verso a o princip přidělování uživatelských rolí koncipovaných na základě procesních rolí, které uživatelé zastávají v rámci procesu, jež je podporován příslušných IT řešením. Elementární role (role zajišťující konkrétní funkcionality systému) se skládají do vyšších a vyšší celků tak, aby společně vytvořily role úrovně (úrovně role jsou kompozicí elementárních a dalších funkčních rolí a tvoří "rolový profil" příslušné uživatelské úrovně) a konečně role přímo přiřazené uživatelům.

Role se uživateli vždy přiřazují na konkrétní uzel organizační struktury (vzácně se používá také nákladová struktura - aktuálně pouze v IS Pracovní cesty). V rámci struktury uživatelských rolí se u každé role uvažuje úroveň přidělení z hlediska organizační struktury. Tyto úrovně jsou pro tyto potřeby určeny takto:

- **kořen** (nejvyšší položka struktury; při přiřazení role na kořen vykonává uživatel práva plynoucí z dané role v rozsahu celé organizační struktury)
 - **univerzita** (při přiřazení role na univerzitu vykonává uživatel práva plynoucí z dané role v rozsahu celé univerzity, tj. nemá působnost např. nad fakultními nemocnicemi, které jsou ve stromu organizační struktury v jiné větvi)
 - **úroveň součásti UK** (při přiřazení role na součást UK vykonává uživatel práva plynoucí z dané role v rozsahu dané součásti UK - např. přístup k záznamům dané fakulty apod.)
 - **úroveň sekce** (některé fakulty jsou členěny na sekce příp. instituty; při přiřazení role na součást UK vykonává uživatel práva plynoucí z dané role v rozsahu pracovišť zařazených do dané sekce)
 - **úroveň pracoviště** (organizační struktura termín "pracoviště" nedefinuje, pro potřeby ekosystému Verso jsou budou některé uzly označeny příznakem "pracoviště"; zjednodušeně lze říci, že jde o uzly nižší úrovně než je součást či sekce, s vyloučením uzlů reprezentujících akademické orgány, virtuální uzly apod.)

Role se přiřazují

- automaticky dle údajů z personalistiky, a to na základě
 - vztahů (pracovních, studijních, jiných) – obvykle role základních uživatelů; preprocesor umožní konfiguraci vazby mezi různými typy vztahů osob k UK, resp. jejím součástí a rolí, která má být přidělena
 - funkcí přiřazených osobě – obvykle role pro "agendové správce" či některé role manažerských; systém umožní konfiguraci vazby mezi funkcemi osob evidovanými v personalistice a rolí, která má být přidělena
- na základě
 - ručního přidělení příslušným agendovým správcem – preprocesor poskytne nástroj,
 - ve kterém lze konfigurovat
 - role, které se tímto nástrojem přidělují
 - oprávnění (na základě rolí) přidělovat konkrétní role
 - oprávnění (na základě rolí) zobrazit přidělení konkrétních rolí
 - příznak viditelnosti přidělované role
 - který umožní zobrazení
 - historie přidělovaných rolí
 - přidělení rolí přidělovaných jiným způsobem
 - samoobslužné registrace externích uživatelů vstupujících do ekosystému Verso z prostředí mimo UK

1.2 Rozšíření architektury ekosystému Verso a přesun na nové db a virtuály

Stávající systémy jsou provozovány ve dvou, třech nebo čtyřech instancích – vždy jedné produkční a jedné či několika neprodukčních. Provozují se na postupně zastarávající infrastruktuře. Cílem je vytvoření pěti instancí celého ekosystému Verso:

- **PRODUKCE** – produkční prostředí
- **STAGE** – synchronizované testovací prostředí
 - každou noc se provede kopie obsahu produkce do stage (zajistí UK)
 - slouží k ručnímu přetestování problémů hlášených v produkci
 - slouží k automatizovaným end-to-end testům před nasazením nové verze do produkce
- **TEST** – nesynchronizované testovací prostředí
 - slouží k testování klíčových uživatelů
- **BUILD** – nesynchronizované testovací prostředí
 - slouží k internímu testování dodaných úprav a nových verzí a k jejich akceptaci
- **DEV** – nesynchronizované testovací prostředí
 - slouží především dodavatelům k jejich interním testům před dodáním úprav k akceptaci

Univerzita zřídí pro každé prostředí samostatnou databázi a jeden nebo více (dle potřeby) virtuální servery s nainstalovaným prostředím Docker. (Univerzita si ponechá správu databází a virtuálů na nejvyšší administrátorské úrovni ve své kompetenci.) Předmětem plnění je realizace přesunu a příslušné rekonfigurace jednotlivých instancí. UK přitom zajistí potřebnou součinnost v podobě migrací či kopií dat do nových schémát v nových databázích, získání serverových certifikátů, nastavení URL a zřízení potřebných emailových schránek pro technické emailové účty používané jednotlivými instancemi.

Maximální cílový počet instancí je 65. Jejich postupný převod se bude řídit aktuálními potřebami univerzity a jejich procesů tak, aby co nejméně ohrozil běžnou činnost univerzity. Práce budou plánovány s týdenním předstihem a jejich ukončení se předpokládá nejpozději do 30. 9. 2025.

1.3 Rekonfigurace a nové záhlaví

Součástí přesunu/zřízení každé instance bude uvedení její konfigurace do jednotného stavu, což zahrnuje především

- instalaci aplikačního serveru do prostředí Docker a související konfiguraci
- přesun instančních modulů na nový aplikační server
- nastavení, zprovoznění emailové komunikace systému z emailové adresy dedikované pro danou instanci – technické notifikace
- vestavěný HelpDesk – načítání emailů došlých do nově zřízené emailové schránky, konfiguraci hlaviček From a ReplyTo
- napojení na správnou instanci CULu, vč. zajištění dedikovaných uživatelů v CUL pro každou instanci
- napojení na správnou instanci tiskového serveru Jasper
- napojení na správnou instanci Elektronické podpisové knihy
- napojení na správné instance ekonomických systémů
- napojení na správnou instanci elektronické spisové služby
- rekonfiguraci napojení na centrální autentizační službu
- úpravu API pro centrální monitoring verzí modulů nasazených na jednotlivých instancích nástrojem Spider
- napojení na preprocesor kmenových dat
- úprava databázových objektů potřebných pro získávání kmenových dat ze správného zdroje
- nasazení nového záhlaví, které bude dodáno zadavatelem



1.4 Zvýšení robustnosti

V průběhu rozšiřování architektury je třeba též provést revizi stávajících integračních skriptů s cílem

- skripty sjednotit napříč instancemi tak, aby bylo možné je verzovat – a centrálně sledovat, jaká verze je nasazena na které instanci
 - obsah skriptu v jedné verzi tedy musí být totožný v celém prostředí
 - případná instanční specifika musí být vyčleněna do samostatných skriptů
- skripty rozdělit tak, aby bylo možné zajistit častější čerpání některých částí dat
 - data o uživatelských oprávněních, přiřazených rolích a jejich kompozici – ideálně jednou za 5 minut
 - data o vztazích a funkcích osob – několikrát denně
 - data o organizační struktuře – jednou denně
- snížit chybovost spojenou s vysokou mírou diverzity integračních skriptů
- snížit celkovou zátěž danou neefektivními postupy při čerpání dat