

KOMORA VETERINÁRNÍCH LÉKAŘŮ ČR

PROJEKT: IDENTITNÍ A AUTENTIZAČNÍ SYSTÉM

ZAKÁZKA: SLUŽBY INTEGRAČNÍHO ROZHRANÍ PRO CEP

TECHNICKÁ SPECIFIKACE PŘEDMĚTU VEŘEJNÉ ZAKÁZKY MALÉHO ROZSAHU

VÝCHOZÍ SITUACE

SYSTÉM KVL ID

Komora veterinárních lékařů ČR (dále jen „Komora“ nebo „KVL“) provozuje jednotný identitní bod a autentizační uzel – KVL ID. Ten umožňuje jednotnou a z jednoho místa přístupnou autentizaci uživatelů z různých aplikací KVL nebo aplikací spolupracujících organizací (např. SVS ČR). Přitom je identitní a autentizační uzel KVL pro tyto aplikace – klienty dostupná bez ohledu na jejich vnitřní architekturu, způsob vývoje či nasazení, nebo dodavatele.

KVL ID je robustní řešení, které umožňuje efektivní správu identit uživatelů, jejich autentizaci a autorizaci v různých aplikacích a službách KVL. Tento systém postupně nahrazuje stávající zastaralé a obtížně spravovatelné řešení autentizačního uzlu na bázi OAuth1.0, které navíc není využíváno zdaleka všemi aplikacemi KVL.

KVL ID zahrnuje komponentu pro vlastní autentizaci a autorizaci protokolem OpenID Connect a funkcionalitu modulu pro Identity Management systém, ve kterém jsou identity a uživatelské účty spravovány zejména v návaznosti na záznamy Matriky KVL.

Autentizační a autorizační uzel umožňující aplikacím KVL autentizovat uživatele protokolem OIDC a poskytnout o něm údaje volající aplikaci (autorizace). Systém za tím účelem zajišťuje správu identit, tzn. uživatelských účtů a souvisejících profilů (údajů o uživatelích) v rámci organizace.

POTŘEBA ROZŠÍŘENÍ PRO INTEGRACI S CEP

Komora v současné době implementuje informační systém Centrální evidence psů (dále jen „CEP“), a to dodavatele vybraným příslušnou veřejnou zakázkou s názvem „Informační systém Centrální evidence psů“, uveřejněnou pod systémovým číslem P24V00000155 – viz profil zadavatele https://ezak.tendera.cz/profile_display_1793.html, resp. přímý odkaz na zakázku https://ezak.tendera.cz/contract_display_1756.html.

Dle příslušné technické specifikace systému CEP je autentizace do něj, protože jde o agendový systém v souladu s požadavky a pravidly eGovernmentu, je realizována prostřednictvím Národní identitní autority (NIA), anebo Centrálního autentizačního a autorizačního informačního systému (CAAIS, dříve JIP/KAAS).

Tyto autentizační a identitní systémy však neobsahují informace o skutečnosti, zdali je autentizovaná osoba veterinárním lékařem (dále také „SVL“ – soukromý veterinární lékař), či nikoliv. Tato informace je však pro CEP stěžejní, neboť podle ní určují, v jaké roli do CEP uživatele vstupuje.

A protože informaci o roli uživatele a jeho referenčních údajích udržuje právě KVL ID, je nutné rozšířit jeho funkcionalitu o služby integračního rozhraní, které systému CEP umožní klást na základě referenčních údajů dotazy, zdali je daná osoba (identifikovaná právě sadou referenčních údajů) veterinářem, či nikoliv. Současně tato služba bude vracet i další vybrané údaje z identity uživatele pro použití v CEP

SPECIFIKACE PLNĚNÍ

Modul integračních služeb pro CEP bude disponovat následující funkcionalitou:

AUTENTIZACE S VYUŽITÍM NIA – SVL A CHOVATEL

Popsaná funkcionalita není součástí předmětu plnění této zakázky a slouží pouze pro poskytnutí kontextu celého uživatelského scénáře.

Jde o scénář přihlášení, resp. autentizace do CEP, kdy osobou přistupující k CEP je fyzická osoba obecně z řad veřejnosti. Až o jejím ztotožnění je na základě záznamů v CEP určeno, jde-li o SVL či chovatele.

SVL a chovatel, tedy fyzické osoby se autentizují pomocí NIA, přičemž zvolí vhodný identifikační prostředek (státní nebo soukromoprávní, tzn. např. mobilní klíč eGovernmentu nebo bankovní identitu – viz ilustrační obrázek).



Po úspěšném přihlášení prostřednictvím NIA získá CEP atributy vydávané poskytovateli služeb v rozsahu povinných atributů a atributů rozšířených na základě uživatelem uděleného souhlasu. V profilu uživatele v NIA je to patrné z evidovaného souhlasu.

SLUŽBA ZTOTOŽNĚNÍ SVL v KVL ID

Tato služba je součástí předmětu plnění této zakázky.

V případě autentizace uživatele, kterým je SVL, CEP tuto skutečnost zjistí pomocí ztotožnění autentizovaného uživatele v KVL ID. Detailní postup je následující:

- 1) SVL se jako osoba (občan) autentizuje do CEP s pomocí NIA.
- 2) NIA poskytne referenční údaje o autentizovaném SVL: jméno, příjmení, dat. nar., bydliště atd. a hlavně AIFO (po překladu z BSI skrz službu ISZR).
- 3) CEP se vyhledá ve své DB, jestli pro dané AIFO eviduje nějaký záznam a v něm i komorové číslo (dále také jako „KID“).
- a) Pokud ano, tzn. KID už v CEP DB existuje, tak se CEP se dotáže KVL ID, jestli je daný KID aktivním SVL.
 - i. Pokud ano, autorizace je úspěšná, uživatel je SVL.
 - ii. Pokud ne, smaže se KID k danému AIFO v CEP DB a jde se dál na bod b.

- b) Pokud ne, tzn. KID v CEP zatím neexistuje, CEP pošle dotaz na KVL ID s referenčními údaji z NIA, jestli Matrika eviduje takového SVL, aby mu vrátila jeho KID.
- i. Pokud KVL ID odpoví, že ano, vrátí KID daného SVL, CEP si uloží KID k AIFO do své DB a je tím ztotožněno, že tahle osoba je SVL, autorizace je úspěšná, uživatel je SVL.
 - ii. Jinak je autorizace neúspěšná, osoba není SVL, CEP si do své DB nic neuloží.

DOPLŇKOVÉ FUNKCIONALITY A SLUŽBY

V rámci plnění jsou požadovány další doplňkové funkcionality, rozšíření a služby KVL ID:

- komponenty uživatele – zapomenuté heslo, změny údajů uživatele v profilu;
- komponenta pro identifikaci a návrhu sloučení identit, zpracování sloučení identit;
- komponenta pro přerušení nebo ukončení činnosti;
- komponenta pro obnovu platnosti dokladů (student, veterinář-nečlen);
- komponenta pro přehled aktivních tokenů a obnovu účtu.

KOMPONENTA PRO SLOUČENÍ IDENTIT

Jde o situaci (scénář), kdy uživatel byl původně studentem Veterinární univerzity Brno, kterou úspěšně ukončil a následně se stal členem Komory. Jde tedy o stejnou osobu, která již v systému identitu má, ale změní se její role.

Přitom však také může dojít ke změně některých údajů, jak doplňkových (např. bydliště), tak referenčních (např. příjmení v případě sňatku). Takže nelze s jistotou říci vždy, podle jakých údajů jde o 100% shodu identit. Algoritmus hledání při snaze o ztotožnění musí s touto okolností počítat.

Sloučení identity tedy obecně tvoří 2 kroky:

- 1) Návrh na sloučení na základě výsledku algoritmu hledání při snaze o ztotožnění, nebo manuální návrh uživatelem.
- 2) Vlastní sloučení provedené administrátorem systému.

Požadavky uživatele z jeho Žádosti o sloučení a návrhy na sloučení identit ze synchronizace má za úkol řešit uživatel s rolí *Referentka KVL*. Ten obdrží o každém návrhu sloučení e-mailovou notifikaci a má k dispozici **přehled účtů navržených ke sloučení**.

Návrh, resp. požadavek na sloučení může *Referentka KVL* vyřešit potvrzením nebo zamítnutím. Pokud sloučení provede, dojde ke změně typu identity na *Veterinář* a údaje ze slučovaného účtu (obvykle nově vzniklý synchronizací z Matriky) jsou zapsány do záznamu původní identity. Např. pokud je původní identitou účet typu *Student*, je jeho typ změněn na *Veterinář* a jsou mu doplněny údaje, které ve slučováném účtu typu *Veterinář* jsou k dispozici. Zejména tak nově vznikne *registrační číslo*, popř. IČO veterináře.

Pokud slučovaný účet již existoval a byl i aktivní, je deaktivován.

Pokud však sloučení identit zamítne, pak bude slučovaný účet ponechán. V případě nově vzniklé identity účtu *Veterinář* systém odešle uživateli notifikaci, aby si vytvořil heslo a tím účet aktivoval. Při zamítnutí musí uživatel s rolí *Referentka KVL* uvést důvod.

Příklad neúspěšného scénáře sloučení identit: Osoba (žena), v systému již vedená jako uživatelka typu *Student*. Dokončila školu a provdala se. Přišla na KVL a registrovala se jako *Veterinářka* v Matrice. Při registraci zadala svůj osobní e-mail, nikoli školní a také své nové příjmení (po svatbě). Při importu systém nenajde shodu s jejím původním studentským účtem, jelikož pouhá shoda v křestním jméně a datu narození nejsou dostačující pro automatické sloučení identit. Uživatelka se následně přihlásí do IS komory, ve kterých neuvidí své údaje ze studijních let. Z tohoto důvodu existuje funkcionality v profilu uživatele pro zadání Žádosti o sloučení identit.

Při sloučení identit nebo zamítnutí jsou zaznamenány údaje o sloučení (datum a čas, slučované účty, popř. důvod zamítnutí) obdobně jako v Transakčním protokolu.

KOMPONENTA PRO PŘERUŠENÍ NEBO UKONČENÍ ČINNOSTI

Systém musí identifikovat záznamy o SVL, kteří přicházejí synchronizací z Matriky a u kterých došlo (a) k přerušení činnosti nebo (b) k ukončení činnosti. V druhém případě to pak vede automaticky na deaktivaci identity, resp. uživatelského účtu a daný SVL už se v systému nemůže autentizovat.

Přerušení výkonu činnosti

Při synchronizaci z Matriky přijde daný záznam identity s informací, že *Veterinář* přerušil výkon svojí veterinární činnosti (např. mateřská dovolená, dlouhodobý pobyt v zahraničí apod.), tzn. má tzv. *uložené osvědčení*.

Systém reaguje změnou atributu vykonává na *NE* a do atributu datum změny запиše datum, kdy k přerušení činnosti došlo (z exportu z Matriky), popř. aktuální datum, pokud tento atribut v exportu není.

Ukončení činnosti – deaktivace

Při synchronizaci z Matriky neprijde daný záznam identity (není v exportu z Matriky, tzn. *Veterinář* ukončil svoje členství v KVL). Systém provede deaktivaci identity, tzn. změni atribut aktivní na *NE*.

Současně systém do atributu zdroj deaktivace запиše hodnotu *Matrika*. Pokud účet deaktivuje *Správce KVLID*, je hodnota *správce*). To ale nemůže nastat při synchronizaci z Matriky, ale jen operací *Správce KVLID* v GUI aplikace.

KOMPONENTA PRO OBNOVU PLATNOSTI DOKLADŮ

Systém pro uživatele typu *Student* ve Správě identit i v Profilu daného uživatele zobrazuje datum expirace potvrzení o studiu (*Platnost do*), případně jej barevně (např. červeně) zvýrazní, pokud platnost vypršela, a méně výraznou barvou (např. oranžově), jestliže vyprší v následujících 30 dnech (lhůta dána v Nastavení systému) od aktuálního dne zobrazení.

Současně uvedené milníky systém každý den na pozadí kontroluje a v případě splnění uvedených podmínek pro každou z nich pošle notifikaci uživateli. V případě (po) vypršení platnosti potvrzení pošle systém znovu uživateli notifikaci o vypršení a deaktivaci jeho účtu, který mu je v ten moment skutečně deaktivován. Současně a souhrnně pro všechny takové studenty odešle systém notifikaci jednou zprávou uživatelům s rolí *Referentka KVL*.

Uživatel z obdržené notifikace přistoupí na formulář pro vložení nového potvrzení o studiu, ve kterém vloží nové PDF se skenem potvrzení. Dále celý proces pokračuje analogicky podle kapitoly Identita uživatele na základě žádosti o uživatelský účet.

Funkcionalita na nahrání nového potvrzení je dostupná pro *Studenta* pouze v případě, že *Studentovi* ještě nevypršelo potvrzení o studiu. Jakmile jednou vyprší a *Student* je deaktivován, tak je možné potvrzení nahrát jen *Referentkou KVL*. Obnovení účtu musí *Student* řešit jinou cestou (email, telefon).

Vložení nového potvrzení o studiu a jeho potvrzení uživatelem s rolí *Referentka KVL* je protokolováno v Transakčním protokolu.

KOMPONENTA PRO PŘEHLED AKTIVNÍCH TOKENŮ A OBNOVU ÚČTU

Ověřeným uživatelům aplikace dovolí **zobrazit přehled všech aktuálně dostupných tokenů**, které může **odvolat**, což zapříčiní **odstranění daného autorizačního tokenu**, který byl použit pro přístup k IS komory. O každém tokenu uživatel uvidí informaci, **pro který IS komory byl token vygenerován a platnost** do kdy je token validní. Neplatné tokeny se automaticky mažou z databáze. Tudiž je uživatel nadále neuvidí v systému.

Odvolání tokenu je protokolováno v Transakčním protokolu.