SPRÁVA ŽELEZNIC

Příloha č. 1 Smlouvy

Bližší specifikace předmětu plnění

Jednotná identita uživatele

Obsah

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČO: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Jednotná identita uživatele

Cílem je rozšíření autentizačního modulu a centrálního modulu Portal Core portálu Liferay SŽ o registraci a autentizaci externích uživatelů. Cílem je zajištění jednotné identity uživatele pro různé oblasti/agendy/aplikace portálu.

Pojmy a zkratky

Pojem/zkratka	Popis
AD	Active direktory = adresářové služby LDAP implementované firmou Microsoft pro řadu systémů Windows NT.
LDAP	Definovaný protokol pro ukládání a přístup k datům na adresářovém serveru.
Liferay	Liferay Portal je bezplatný open-source podnikový portál založený na jazyce Java a distribuovaný pod licencí GNU Lesser General
NTLM	Autentizační protokol, používaný zejména protokolem SMB a některými implementacemi síťových protokolů Microsoft Windows za účelem ověření uživatele nebo spojení.
Portlet	Webové komponenty umožňující integraci webových aplikací a portálů.
SAP	Podnikový informační systém se souborem adaptivních řešení k optimalizaci obchodních procesů.
SOAP	Protokol pro výměnu zpráv založených na XML přes síť, hlavně pomocí http.
SSO	Jednotné přihlášení, umožňující uživateli přihlásit se pomocí jediného ID a hesla k libovolnému z několika souvisejících, ale nezávislých softwarových systémů.
URL	Řetězec znaků s definovanou strukturou, který slouží k přesné specifikaci umístění zdrojů informací na Internetu

Externí uživatelé

Modul portal core bude rozšířen o externí uživatele. U externího uživatele budou evidovány údaje:

- jméno,
- příjmení,
- e-mailová adresa,
- aplikace, do kterých má přístup,
- způsob autentizační metody.

Profil uživatele

Bude implementován nový portlet, pomocí kterého si externí uživatel zobrazí vlastní profil. V profilu má uveden seznam dostupných aplikací včetně možnosti prokliknuti na home-page aplikace.

Dále má uživatel k dispozici výběr autentizačních metod a možnost nastavení příslušné autentizační metody. Na výběr bude ze dvou metod:

- autentizace pomocí zadání jména a hesla,
- autentizace pomocí Google.

Přehled uživatelů

Bude implementován nový portlet, pomocí kterého si administrátor portálu zobrazí přehled všech externích uživatelů:

- údaje uživatele,
- seznam jemu přiřazených aplikací.

Registrace aplikace do portal core

Při zavádění nové aplikace, která bude pracovat s externími uživateli, bude tato aplikace zavedena do modulu portal core. Modul portal core bude obsahovat administraci aplikací. Při zadávání nové aplikace se bude zadávat:

- název aplikace,
- popis aplikace,
- URL pro přesměrování na úvodní stránku aplikace,
- URL pro dokončení registrace v aplikaci,
- autentizační údaje aplikace pro volání rozhraní portal core (disponuje generátorem hesel, min podmínky: 13 znaků, 1 velké písmeno, 1 speciální znak),
- URL endpointu aplikace,
- přihlašovací údaje k endpointu aplikace,
- příznak, zda se uživatel může sám odregistrovat.

Přehled registrovaných aplikací

Bude vytvořen portlet s přehledem všech registrovaných aplikací a možností vytvoření nové aplikace a editaci aplikace.

Rozhraní portal core

Nové rozhraní Portal core pro externí uživatele bude obsahovat metody:

- registrujUzivatele – spustí registraci nového uživatele (uživatel už může existovat),
- potvrdRegistraci – aplikace potvrzuje do portal core úspěšné dokončení registrace uživatele do aplikace,
- zamitniRegistraci – aplikace informuje portal core o nedokončené registraci uživatele,

- odstranUzivatele – aplikace chce ukončit uživatele. Pokud je uživatel odstraněn ze všech aplikací, tak dojde k jeho odstranění z Liferay. V opačném případě je nutné účet v Liferay ponechat.

Implementace bude pomocí technologií EJB 3.0 a webové služby protokol SOAP.

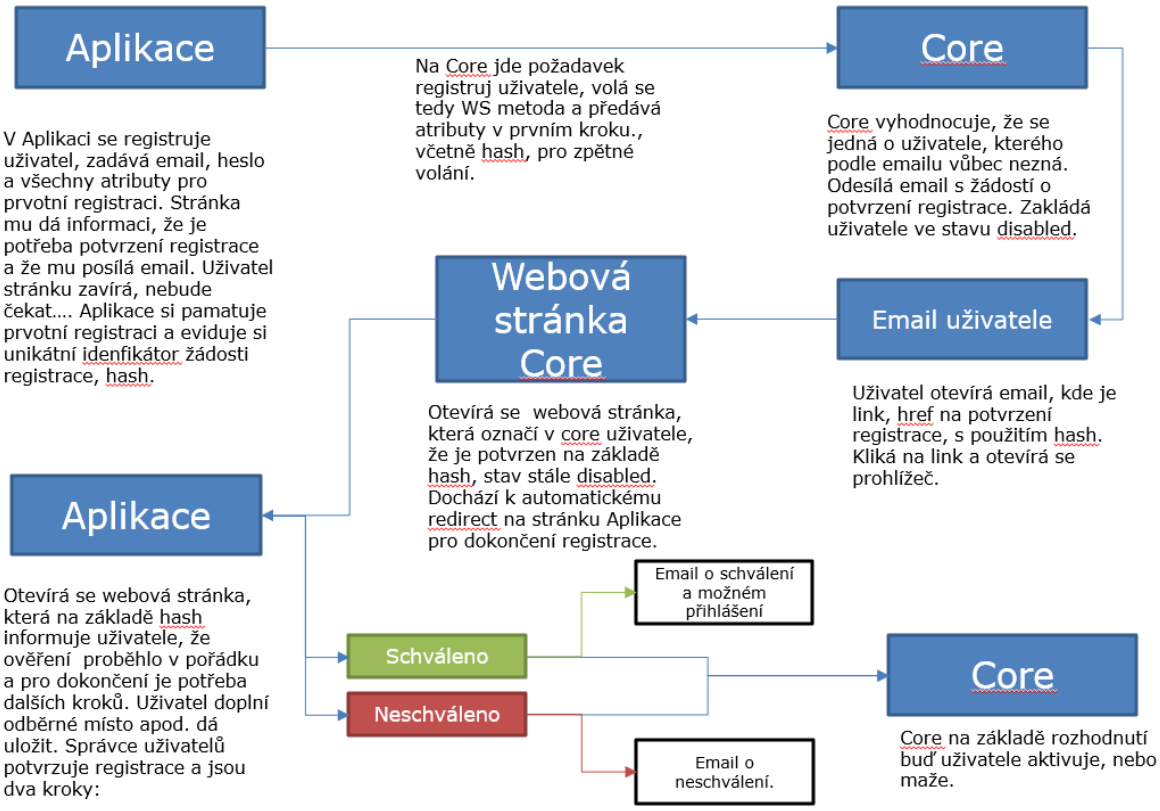
Proces ověření uživatele

Při volání metody overUzivatele mohou nastat situace:

1. Jedná se o nového uživatele.
2. Uživatel je již v portálu registrován, a další aplikace ho chce registrovat.

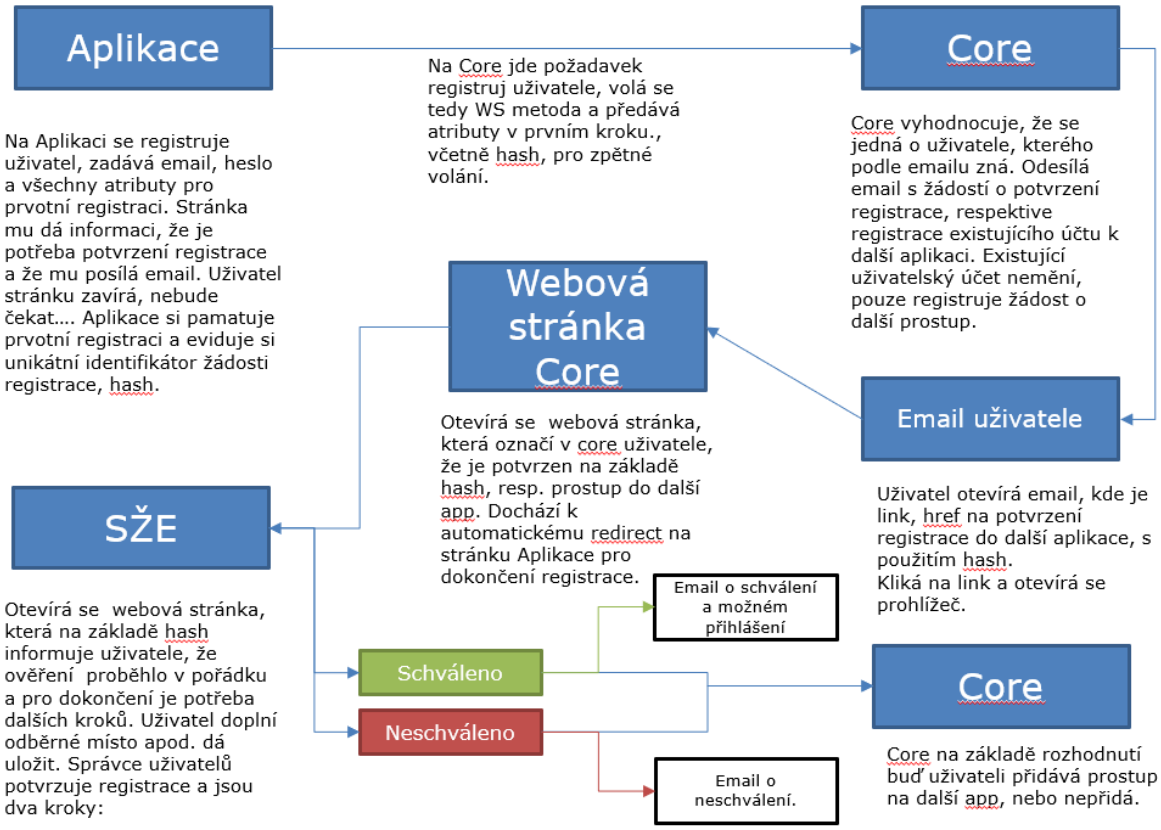
Nový uživatel

Popis procesu: Uživatel zobrazí registrační formulář, který je v aplikaci, do které se chce registrovat. Po zadání údajů odešle aplikace požadavek na registraci uživatele do modulu portal core. Ten dle e-mailové adresy ověří, zda se jedná o nového, nebo existujícího uživatele. Portal core odesílá e-mail, ve kterém je url, pomocí které se ověří e-mailová adresa. Po kliknutí na URL je uživatel přesměrován na stránku modulu portal core, která uživatele přesměruje na obrazovku aplikace, kde dokončí registraci. Aplikace dokončí ověření uživatele dle vlastních potřeb. V případě úspěšného dokončení registrace je tato informace



Obrázek 1 Proces ověření nového uživatele

Existující uživatel



Obrázek 2 Proces ověření existujícího uživatele

Nedokončení registrace

V případě nedokončení registrace bude uživatel po 3 dnech upozorněn na nedokončenou registraci. Po dalších dvou dnech (celkem po 5-ti dnech od vyplnění registrace) bude jeho registrace zrušena.

Stejná kontrola bude probíhat na straně aplikací.

Sloučení účtů

Při registraci uživatele do portálu může dojít k tomu, že uživatel má již existující účet, ale při nové registraci zadá jinou e-mailovou schránku. V takovém případě vznikne nový uživatelský účet v portálu, jelikož není možné identifikovat, že se jedná o stejného uživatele. Z tohoto důvodu je požadována funkcionalita na sloučení více účtů do jednoho. Při slučování účtů musí dojít ověření, že vlastníkem slučovaných účtů je stejný člověk. To může být např. formou odeslání e-mailové zprávy, kde kliknutím na odkaz uživatel potvrdí vlastnictví všech slučovaných e-mailových adres. Uživatel bude moct slučování provést v jeho profilu, tedy po přihlášení na jeden z účtů. Účet, kterým je uživatel přihlášen, je primární, a tento účet zůstane zachován, duplicitní účet bude zrušen.

Nefunkční požadavky

V této kapitole jsou popsány nefunkční požadavky, které musí nový modul splňovat.

Kompatibilita a existujícím autentizačním modulem

Musí být zajištěna kompatibilita s již existujícím autentizačním modulem portálu SŽ, případně nový modul musí převzít veškeré funkcionality existujícího autentizačního modulu, včetně zajištění podpory již napojených aplikací. Aktuální autentizační modul řeší oblasti:

- autentizace uživatele vůči SAPu,
- autentizace uživatele vůči AD (více forestové AD dle doménového jména, podpora pro migraci uživatelů mezi doménami, podpora pro migraci uživatele
- SSO pomocí NTLMv2,
- podpora různých způsobů ověření uživatele pro přístup z externí nebo interní sítě.
- podpora IDM a jeho unikátního identifikátoru uživatele

Logování

Transakční protokol

Veškeré úkony (insert, update, delete) budou logovány (stará hodnota, nová hodnota, datum změny, autor změny) na úrovni transakčního protokolu nad databází.

Auditování událostí

Je požadován audit všech událostí, které jsou volány mezi portal core a aplikacemi.

Zakázané domény

V rámci konfigurace je požadováno mít možnost nastavit zakázané domény, pro které není možné registrovat e-mailovou adresu.

Součinnost při integraci aplikací

Pro potřeby integrace aplikací na centrální modul externích uživatelů je požadováno:

- Součinnost s dodavateli aplikací.
- Implementační manuál.
- Specifikace integračního rozhraní.