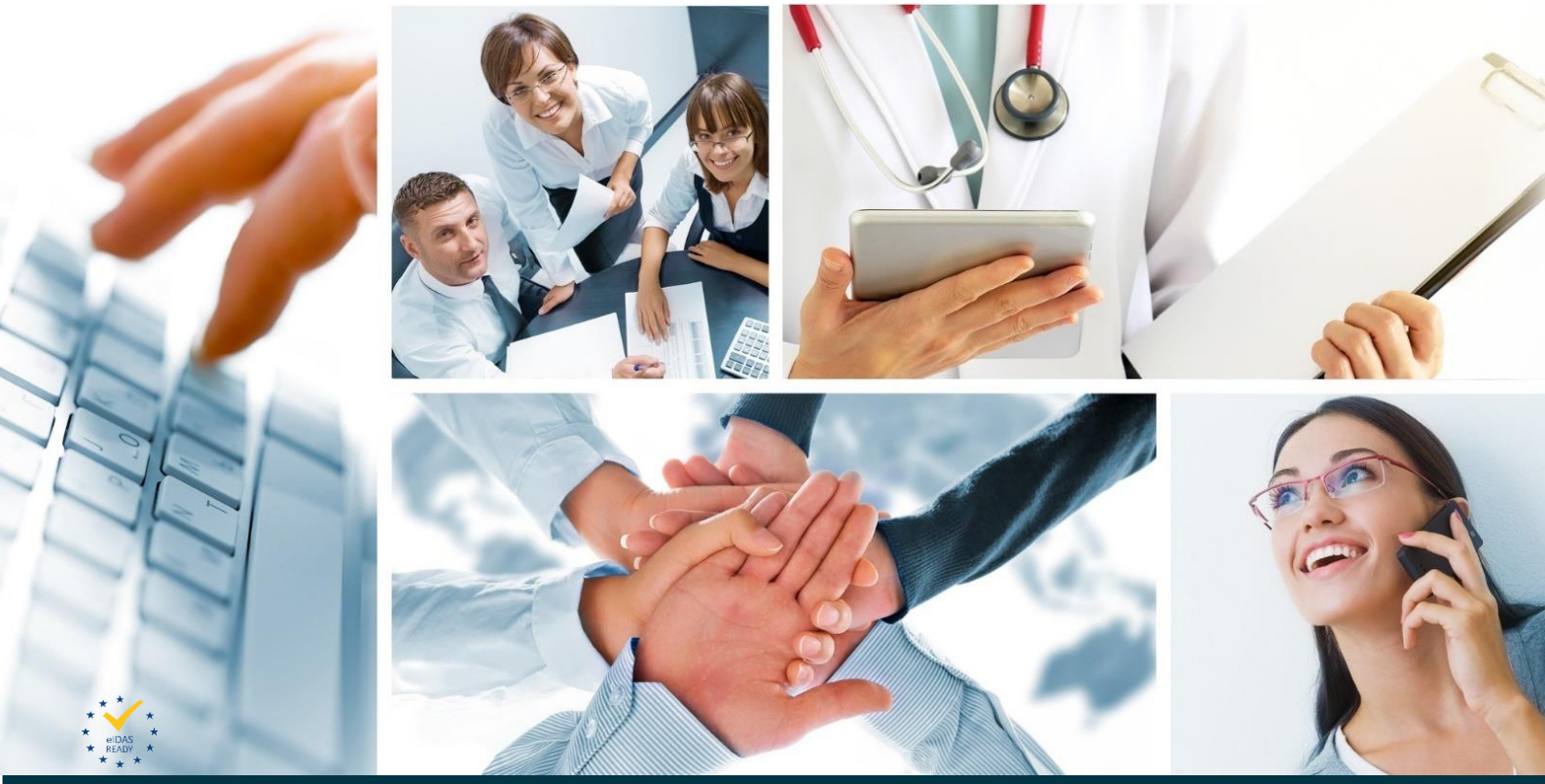
ELDAx Seyfor

eIDAS SMART TRUST eLECTRONIC PLATFORM

ePOXID



GO DIGITAL

ELDAx.cz

ELDAx

Obsah

1 OBECNÉ

Řešení pro autentizaci a autorizaci uživatelů s podporou externích poskytovatelů i interních zdrojů identit

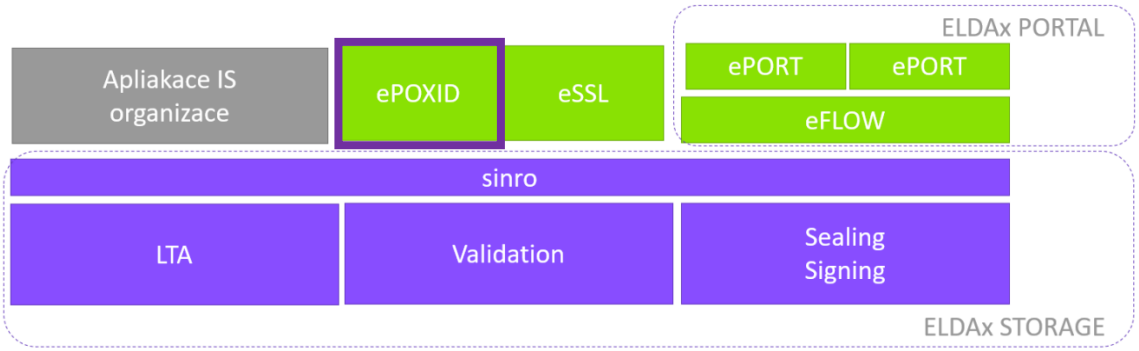
Řešení ELDAx/ePOXID slouží pro autentizaci a autorizaci uživatelů a zajištění SSO (Single sign-on). Řešení je součástí platformy ELDAx eIDAS SMART TRUST eLECTRONIC PLATFORM a je koncipováno jako samostatný prvek (část) celé platformy ELDAx.

1.1 Využití

Jedná se o ideální plně konfigurovatelný doplněk portálových řešení, nebo obdobných řešení, kde je potřeba zajistit funkcionalitu autentizaci a autorizaci pomocí různých externích poskytovatelů identit, jako ne NIA, MOJE ID, JIP/KASS, BankID apod. ELDAx ePOXID je vytvořen způsobem, který umožňuje integraci (zapouzdření) prakticky s jakýmkoliv portálovým řešením nebo informačním systémem.

ELDAx ePOXID umožňuje takovou úroveň integrace a konfigurace, že běžný uživatel při práci v aplikaci nerozpozná, že využívá část systému, která není nativní součástí aplikace, ale jedná se ELDAx ePOXID.

Kromě podpory externích poskytovatelů identit ELDAx ePOXID lze využít například třeba v rámci vlastního informačního systému, kde jsou uživatelé uložení v Active Directory a je potřeba pro systémy provozované v rámci IS (tedy např. i .NET / Java / PhP aplikace) zajistit jednoduše autentizaci/autorizaci a SSO jednotným způsobem.



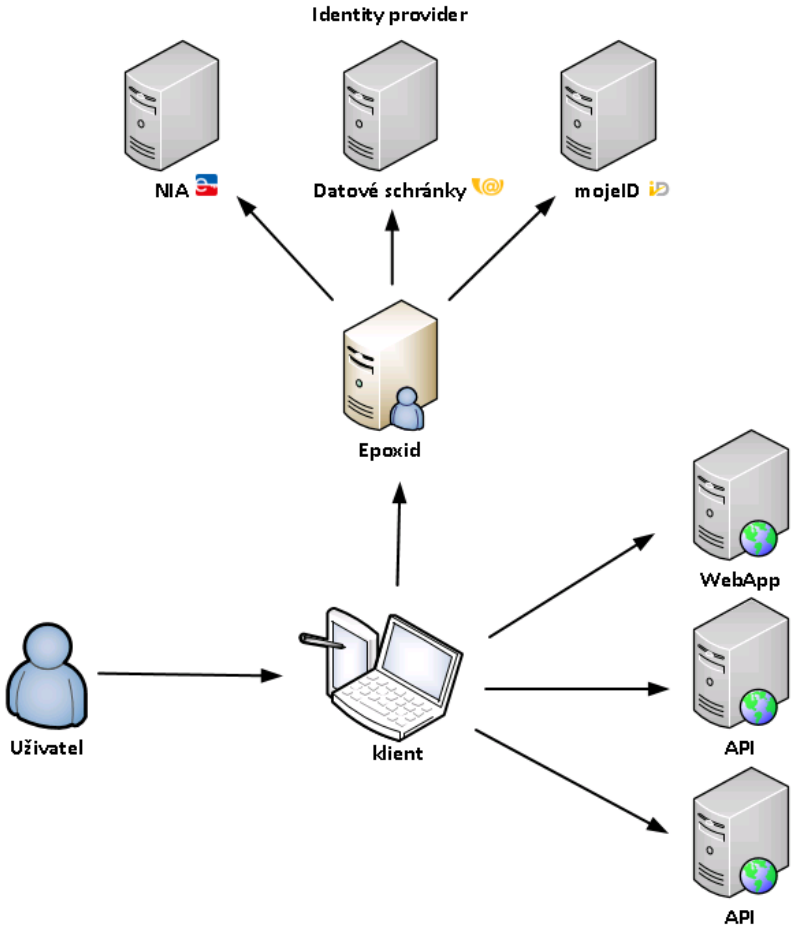
Obrázek 1Struktura platformy ELDAx v návaznosti na ePOXID

1.1.1 Popis funkcionalit řešení

ELDAx/ePOXID slouží k bezpečné autentizaci a autorizaci včetně SSO pro webové aplikace, k zabezpečení API (Bearer token) apod. Jedná se o obecný, plně konfigurovatelný samostatně a nasaditelný prvek platformy ELDAx sloužící k autentizaci uživatele. Je vytvořena na technologii .NET Core a open source

komponentě Identity Server. Jedná se v principu o OpenID Connect a OAuth 2.0 framework pro .NET. IdentityServer je certifikován OpenID Foundation a součást .NET Foundation.

ELDAx/ePOXID zprostředkovává připojenému systému (klient) autentizaci (přihlášení) uživatele, pomocí uživatelem zvoleném správcem identit (IdP), nebo pomocí jména a hesla. Profilové údaje identity uživatele jsou předávány v podobě claimů. ELDAx/ePOXID je možné využít i pro autorizaci uživatele, kdy jsou předávány role uživatele. Role je možné uživateli přiřadit v rámci administračního rozhraní ELDAx/ePOXID, nebo získat od IdP, pokud tuto možnost podporuje, např. Active Directory. Jednotlivé role jsou opět předávány v podobě claimů.



Obrázek 2 Architektura řešení

1.2 Typický scénář práce uživatele a využití ELDAx/ePOXID

Typický scénář přihlášení uživatele je práci v ELDAx/ePOXID takový, že Uživatel v aplikaci klikne na odkaz přihlásit, následně je aplikací přesměrována na ELDAx/ePOXID, kde se přihlásí buď jménem + heslem, nebo zvolí možnost přihlášení pomocí některého s nastavených Identity providera (IdP). Následně je uživatel přesměrován na příslušného IdP, kde se přihlásí a je přesměrován zpět do aplikace, které je předána jeho identita

Jako vnější rozhraní vůči klientu, je použit standardní protokoly SAML2, OpenID Connect (https://openid.net/connect/) a Oauth 2.0. Díky tomu je snadné ELDAx/ePOXID integrovat na webovou aplikaci, které je postavena na nějaké standardní technologii typu .NET, Java, PHP, JavaScript, …, případně již do hotových řešení jako jsou např. WordPress apod.

2 KLÍČOVÉ VLASTNOSTI

- Zprostředkování zabezpečeného přihlášení uživatele pomocí zvoleného IdP
- Volitelně možnost ověřování uživatelů pomocí jména a hesla včetně konfigurovatelné dvou-faktorové autentizace (One time password, email, sms)
- Profilová stránka uživatele
    - Možnost propojení účtů, tzn. jedna identita se může, přihlašovat více způsoby (pomocí různých IdP)
    - Změna hesla
    - Uživatel má možnost zapamatovat si způsob přihlášení, tzn. příště je přesměrován přímo na zvoleného IdP
    - Zobrazení historie přihlášení, změn profilu atd.

- Standardní protokol (OpenId Connect / SAML2) => odpadá složitá integrace
- Multiplatformní, podpora provozu ve vysoké dostupnosti, podpora kontejnerů
- REST API

2.1 Možnosti administrace

- Nastavení a konfigurace systému
- Nastavení profilu uživatele (konfigurace údajů o uživateli)
    - Mapování claimů
- Správu povolených poskytovatelů identit (IDP)
- Správu a konfigurace service providerů
- Správu zabezpečených API zdrojů

- Správu certifikátů (certifikáty se ukládají do systémového úložiště certifikátů uživatele, pod kterým běží služba)
- Správu uživatelů a jejich rolí
- Logy, auditní události

2.2 Aktuálně implementované možnosti autentizace uživatele (implementovaní IdP)

- Jméno + heslo včetně dvou-faktorové autentizace (OTP, email, SMS)
- BankID
- NIA - národní identita
- ISDS
- mojeID
- JIP/KASS
- NTLM / Kerberos
- ADFS (Active directory federation services)
- Social logins (Google, Facebook, atd…)

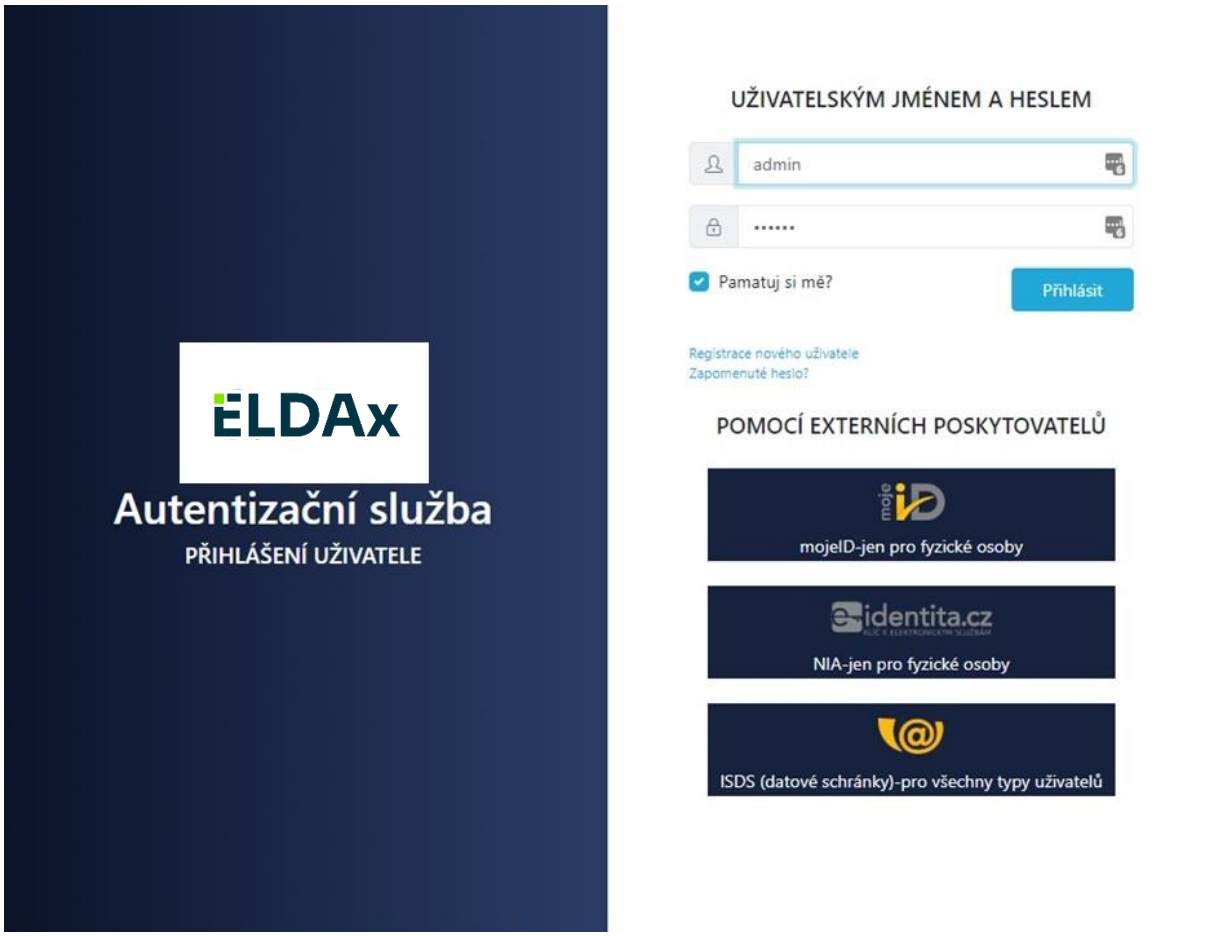
2.3 Systémové požadavky

- Operační systém serveru: Windows Server / Linux.
- Databázové úložiště: MS SQL Server / Postgre SQL.
- Podpora běhu v kontejnerech

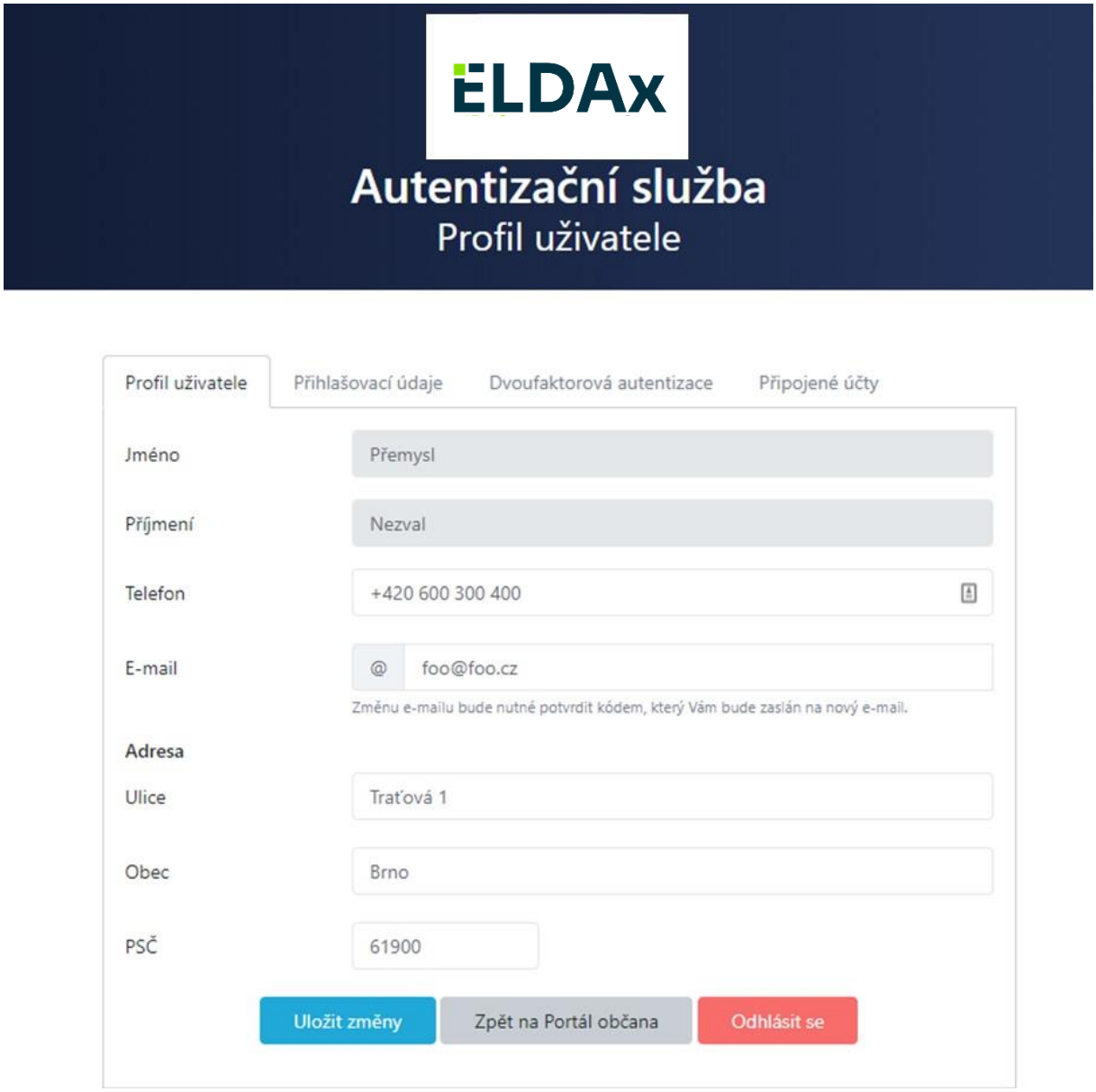
2.4 Podporované specifikace

- OpenID Connect
- OAuth 2.0
- SAML2

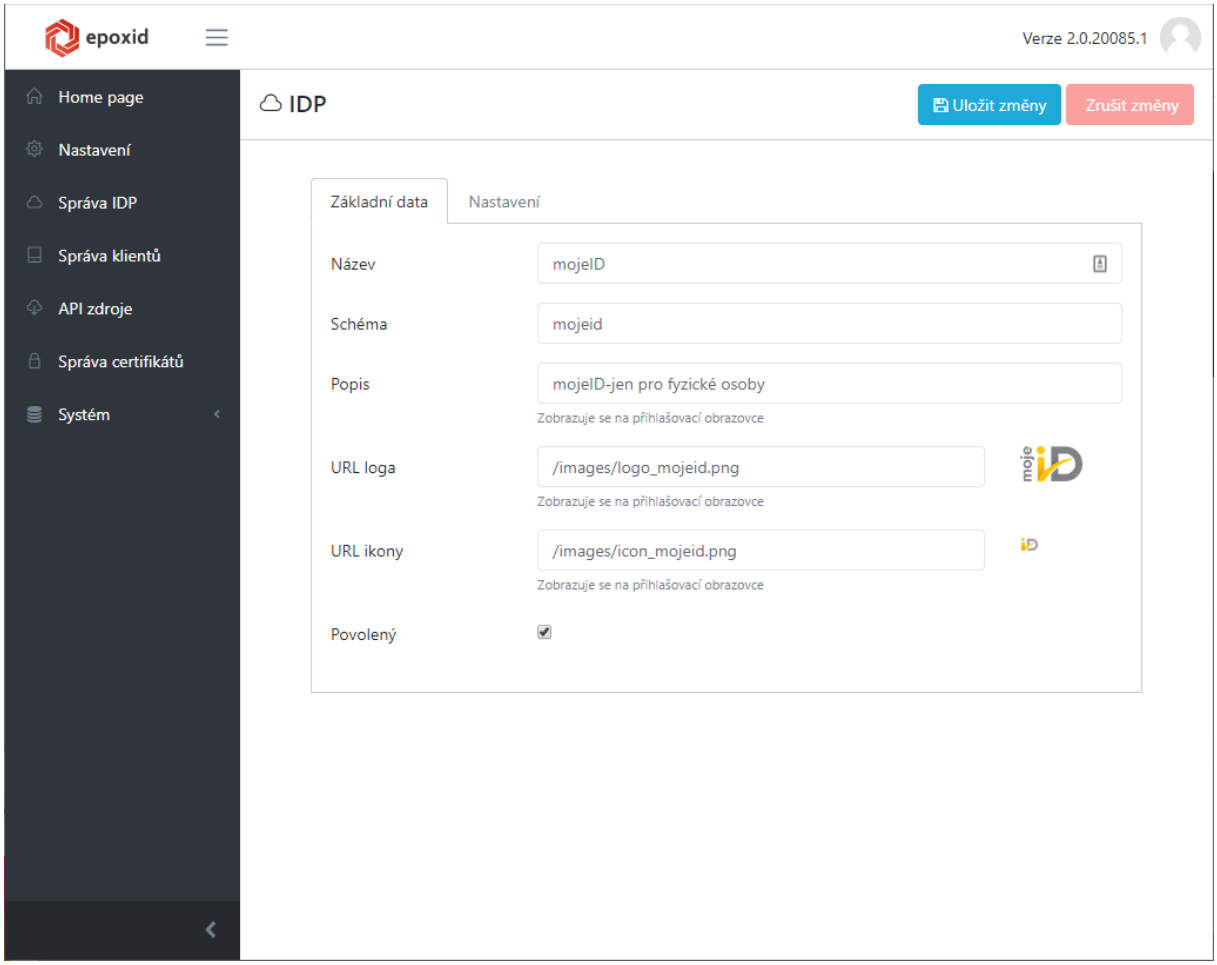
3 UKÁZKA ROZHRANÍ A MOŽNOSTI KONFIGURACE



Obrázek 3 Přihlašovací obrazovka s ukázkou tří nakonfigurovaných poskytovatelů externích identit



Obrázek 4 Profil uživatele



Obrázek 5 Administrace