

ELDAX Seyfor

eIDAS SMART TRUST eLECTRONIC PLATFORM

ePOXID



GO DIGITAL

ELDAX.CZ

Obsah

1	OBEČNÉ	3
1.1	Využití	3
1.1.1	Popis funkcionalit řešení.....	3
1.2	Typický scénář práce uživatele a využití ELDax/ePOXID	5
2	KLÍČOVÉ VLASTNOSTI	5
2.1	Možnosti administrace	5
2.2	Aktuálně implementované možnosti autentizace uživatele (implementování IdP).....	6
2.3	Systémové požadavky.....	6
2.4	Podporované specifikace.....	6
3	UKÁZKA ROZHRANÍ A MOŽNOSTI KONFIGURACE	7

1 OBECNÉ

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

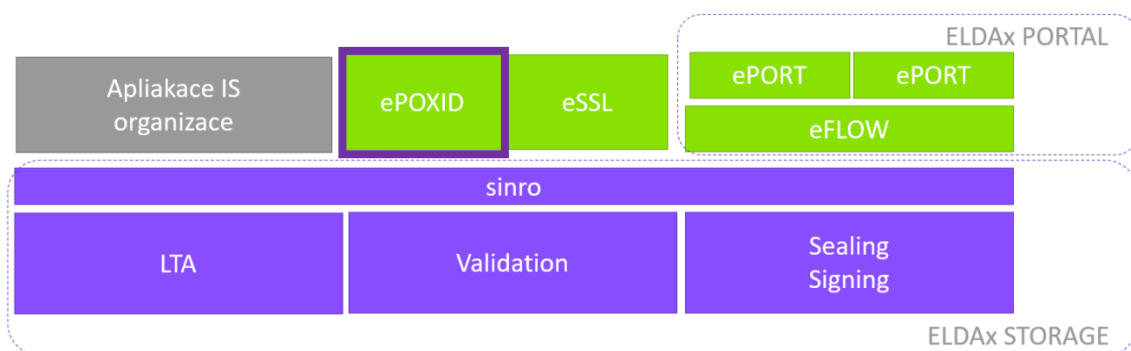
Řešení ELDAX/ePOXID slouží pro autentizaci a autorizaci uživatelů a zajištění SSO (Single sign-on). Řešení je součástí platformy ELDAX eIDAS SMART TRUST eELECTRONIC PLATFORM a je koncipováno jako samostatný prvek (část) celé platformy ELDAX.

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 uloženi 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.



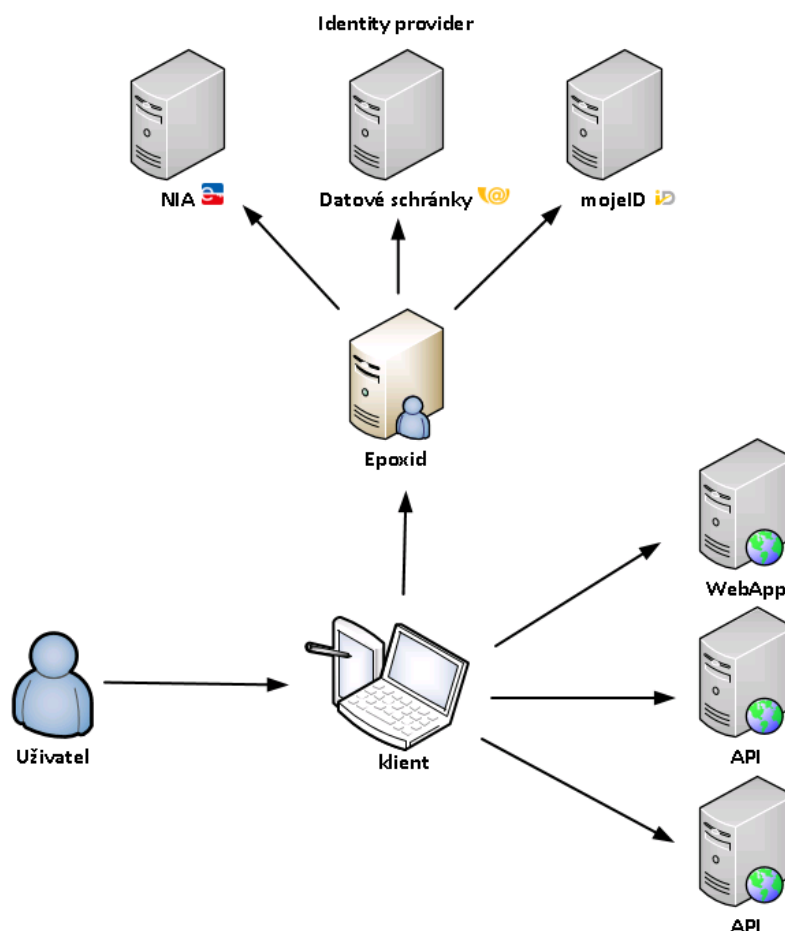
Obrázek 1 Struktura platformy ELDAX v návaznosti na ePOXID

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 (implementování 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...)

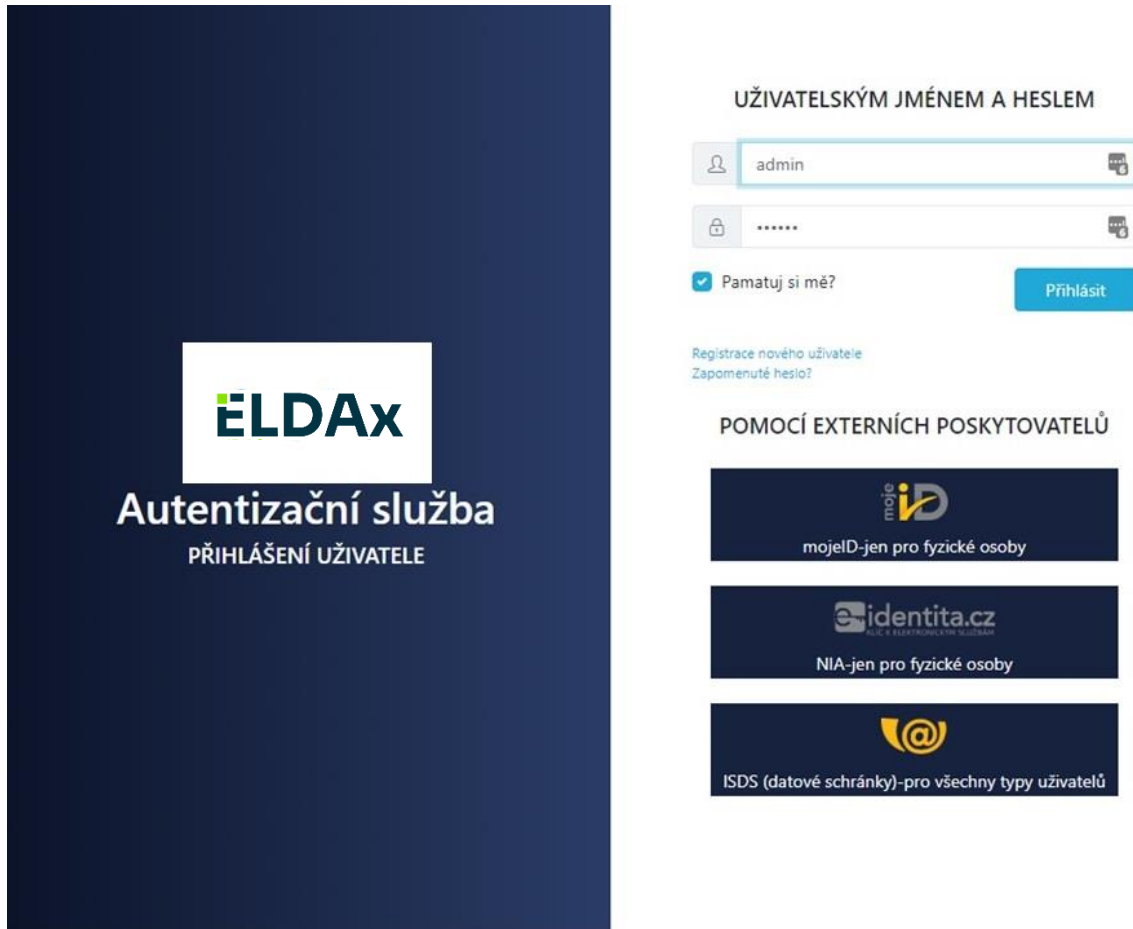
2.3 Systémové požadavky

- 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




The screenshot displays the ELDax login interface. On the left, a dark blue banner features the ELDax logo and the text "Autentizační služba PŘIHLÁŠENÍ UŽIVATELE". On the right, the login form is titled "UŽIVATELSKÝM JMÉNEM A HESLEM". It includes two input fields: one for the username "admin" and one for the password ".....". A checkbox labeled "Pamatuj si mě?" is checked. A blue "Přihlásit" button is positioned to the right of the password field. Below the login form, there are links for "Registrace nového uživatele" and "Zapomenuté heslo?". Under the heading "POMOCÍ EXTERNÍCH POSKYTOVATELŮ", three external provider options are listed: "mojeID" (mojeID-jen pro fyzické osoby), "e-identita.cz" (NIA-jen pro fyzické osoby), and "ISDS (datové schránky)-pro všechny typy uživatelů".

Obrázek 3 Přihlašovací obrazovka s ukázkou tří nakonfigurovaných poskytovatelů externích identit

Autentizační služba

Profil uživatele

Profil uživatele
Přihlašovací údaje
Dvoufaktorová autentizace
Připojené účty

Jméno	<input type="text" value="Přemysl"/>
Příjmení	<input type="text" value="Nezval"/>
Telefon	<input type="text" value="+420 600 300 400"/> 
E-mail	<input type="text" value="@ foo@foo.cz"/> <p style="font-size: 0.8em; margin-top: 5px;">Změnu e-mailu bude nutné potvrdit kódem, který Vám bude zaslán na nový e-mail.</p>
Adresa	
Ulice	<input type="text" value="Traťová 1"/>
Obec	<input type="text" value="Brno"/>
PSČ	<input type="text" value="61900"/>

Uložit změny
Zpět na Portál občana
Odhlásit se

Obrázek 4 Profil uživatele

epoxid Verze 2.0.20085.1

Home page IDP Uložit změny Zrušit změny

Nastavení

Správa IDP

Správa klientů

API zdroje

Správa certifikátů

Systém

Základní data **Nastavení**

Název

Schéma

Popis
Zobrazuje se na přihlašovací obrazovce

URL loga

URL ikony

Povoleno

Obrázek 5 Administrace