

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: Bc. Martin Gabriel

Oponent: doc. Ing. Oldřich Trenz, Ph.D.

Studijní program: Informační technologie

Specializace: Softwarové inženýrství

Akademický rok: 2024/2025

Téma diplomové práce: Authentication and Authorization Service for Developers: Implementation of Authentication-as-a-Service on the .NET platform

Hodnocení práce:

Diplomant v rámci práce realizuje řešerši v oblasti autentizačních a autorizačních služeb, navrhuje design a implementaci služby typu Authentication-as-a-Service postavené na platformě .NET. Popisuje autentizační a autorizační standardy typu OAuth a OpenID Connect, provádí jejich srovnání, a to včetně poskytovatelů těchto služeb. Následně navrhuje vlastní službu nabízející přihlášení klientských aplikací, místní a federová přihlášení spolu s řízením přístupu a ochraně před běžnými kybernetickými útoky. Z povahy a obsahu řešení se jedná o aktuální téma a s ohledem na bezpečnost poměrně důležité a vhodné k řešení. Byť ověřování klientů napříč platformami je téma poměrně časté, ale stále řešené. A to nejen s ohledem na preferovanou službu.

Pojetí řešeného úkolu je systematické – práce obsahuje kvalitní řešerši, detailní analýzu dostupných komerčních i open-source řešení (Auth0, Azure AD B2C, Keycloak, atd.), a přesvědčivé zdůvodnění vlastního návrhu. Velmi oceňuji důkladné rozpracování uživatelských scénářů (user stories), funkčních a nefunkčních požadavků včetně bezpečnostních a výkonnostních atributů.

Úroveň zpracování tématu po odborné stránce je velmi dobrá. Implementace respektuje moderní bezpečnostní standardy (např. PKCE, Argon2id, rate-limiting, aj.), využívá nástroje jako OpenIddict, ASP.NET Core, Docker a YARP. Autor zvládl jak návrh architektury, tak vývoj REST API a webového rozhraní a správu rolí uživatelů. Výstupem práce je využitelný open-source produkt.

Po formální stránce je práce na velmi dobré úrovni. Struktura textu je logicky členěna, kapitoly na sebe vhodně navazují, autor používá vhodně odborné pojmy, odkazy na literaturu i obrázky jsou správně využívány. V textu lze najít drobné gramatické chyby či překlepy v úrovni anglickém textu, ale tyto prohřešky nejsou zásadního charakteru.

Práce splňuje všechny nároky kladené na diplomovou práci, je přínosná, technicky vyspělá a přináší taktéž prakticky využitelný výsledek. Student prokázal velmi dobré pochopení jednotlivých technologií, schopnost analytického myšlení a velmi dobrou schopnost spojenou s návrhem a implementací vybraného softwarového řešení.

Otázky k diskusi (výběr otázek):

1. Jaké jsou limity použití OpenIddict oproti robustnějším frameworkům jako IdentityServer?
2. Jak by bylo možné upravit navržené řešení, aby podporovalo více externích poskytovatelů identity (např. Google, Microsoft, Facebook)?



3. Jakým způsobem by bylo možné integrovat auditování událostí (např. přihlášení, změna role, registrace klienta) pro bezpečnostní a provozní účely?
4. Jak by bylo možné rozšířit službu o správu více tenantů (multitenancy), např. v SaaS scénáři?
5. Jakým způsobem by bylo možné automatizovat rotaci kryptografických klíčů (např. RSA) pro podepisování JWT tokenů? Zejména s ohledem na přechodné období, kdy platí oba klíče.

Celkové hodnocení práce:

Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:

A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně, F – nedostatečně.

Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

B - velmi dobře.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum

8. 6. 2025

Podpis oponenta diplomové práce