

# Security Provider

## Vedoucí

Mgr. Pavel Ježek (MFF UK)

## Řešitelé

Michal Foltýn

Martin Baroš

Jozef Ružinský

Jan Bureš

Projekt jako celek má za úkol poskytnout jednotný přístup k bezpečnostní politice pro tenké a tlusté aplikace.

Řešení bude naimplementováno na prostředí Celní správy České republiky.

Projekt se bude skládat z následujících částí:

1. Komponenta pro poskytování bezpečnostních metod pro webové aplikace
2. Komponenta pro poskytování bezpečnostních metod pro tlusté aplikace
3. Komponenta pro monitorování dostupnosti webových služeb na lokálních řadičích
4. Membership provider (SPMembershipProvider)

Výše popsané části projektu jsou nedílnou součástí tohoto celku a každá část plní svou roli, aby byly pokryty potřeby vývojářů (kteří budou produkt používat) i administrátorů systému. Výsledné řešení bude komplexním nástrojem pro poskytování jednotného přístupu k bezpečnostní politice.

Pro implementaci bude použita technologie .NET a adresářová služba Active Directory a databáze MSSQL.

## Hlavní cíle projektu

Kromě implementace samotného zadání se zaměříme na naplnění následujících cílů:

- 1. Rozšiřitelná architektura** - ačkoliv požadavek na tento projekt vzešel od zákazníka, chtěli bychom projekt navrhnout tak, aby jej bylo možné snadno rozšířit i pro jiné projekty. Dále bude kladen důraz na definici jasného a snadno použitelného rozhraní, které je nutnou podmínkou k tomu, aby výsledný produkt byl použitelný i pro třetí strany.
- 2. Vysoká míra automatického testování** - pro zajištění stability a dalšího rozšiřování projektu chceme navrhnout a implementovat automatické testy, které budou důkladně prověřovat požadovanou funkčnost. Již při návrhu architektury budeme zohledňovat požadavek na efektivní tvorbu testů a co nejvyšší pokrytí kódu. V rámci testování chceme navrhnout řešení, které umožní i testování proti databázi a Active Directory, které zpravidla firmy opomíjí a testují pouze proti rozhraní.
- 3. Optimální běh v omezujících podmínkách** - pro zajištění rychlosti odezvy systému chceme optimálně využít dostupné postupy pro přístup do Active Directory (dle dosavadních testů na rozsáhlých uživatelských datech se ukazuje, že některé

běžně používané metody pro přístup do AD jsou pro tuto implementaci nevhodné)

- 4. Podpora alternativních úložišť** – pro efektivní vývoj je nutné zajistit plnou funkčnost produktu i bez dostupnosti Active Directory a DB. Toto bude zajištěno podporou alternativních úložišť. Je vyžadována snadná konfigurace a jednoduché přepínání mezi úložišti bez nutnosti změn v aplikaci.
- 5. Technická dokumentace včetně ukázkových aplikací** - kvůli důrazu na snadné použití produktu pro třetí strany, vytvoříme kromě potřebné technické dokumentace i ukázkové aplikace, které budou prezentovat způsob použití produktu.

## Popis prostředí

### Uživatelské účty

Uživatelské účty jsou uloženy v samostatné doméně v Active Directory. Autentizace probíhá pouze vůči AD, žádný jiný externí systém do tohoto procesu nezasahuje. Základní informace o uživateli jsou uloženy rovněž v AD. Security Provider bude pracovat pouze s informacemi uloženými v AD.

### Databáze

V databázi MSSQL jsou uloženy záznamy o všech aplikacích. Pro každou aplikaci je definován seznam skupin (např. Users, Admins). Pro každou aplikaci je definován seznam Usecase (stránek), které daná aplikace v sobě obsahuje. Následně existuje samostatná převodní tabulka, která určuje, které skupiny mají přístup ke kterým Usecase.

Skupiny definované v každé aplikaci přesně odpovídají skupinám v Active Directory.