

Actuaria App

Nabídka realizace členské aplikace

"Actuaria je profesní organizace českých pojištých matematiků a jiných pojiště technických profesionálů, jejímž smyslem je rozvíjení, používání a sdílení znalostí a dovedností nezbytných pro fungování pojišťovnictví, a to k užítku členů, pojišťoven, jejich klientů a další odborné i laické veřejnosti."

Technologie aplikace

Architektonicky je aplikace rozdělena na *serverovou* a *klientskou* část. Obě části jsou na sobě nezávislé a jejich vzájemné propojení je řešeno přes tzv. API (viz. níže).

Serverová část (server/backend)

Serverová část reaguje na požadavky (volání) klienta a klientovi vrací odpovědi. Serverová část je též odpovědná za správu dat a manipulaci s daty.

Serverová část je realizována prostřednictvím relační databáze MySQL a programovacího jazyku PHP (framework Symfony).

Klientská část (client/frontend)

Klientská část představuje rozhraní, se kterým pracuje uživatel aplikace. Jde o část, kterou uživatel vidí a se kterou interaguje. Na pozadí internetového prohlížeče komunikuje klientská část se serverovou částí.

Členská aplikace má 2 klientské části:

- Administrace a správa dat v serverové části,
- prezentační web WordPress (využívající aplikaci pro přístup uživatelů k uzamčeným článkům a komentáře uživatelů).

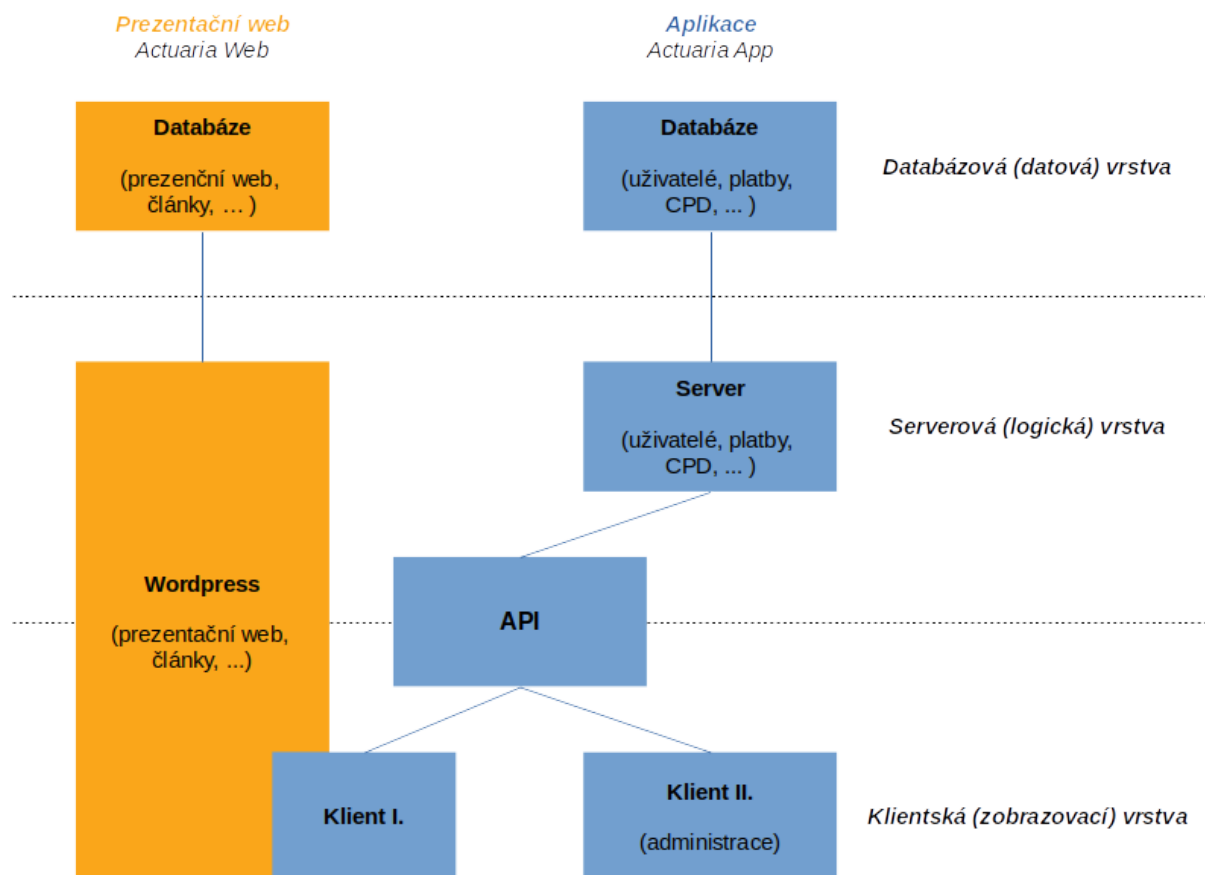
Klientská část je realizována prostřednictvím programovacího jazyka JavaScript (knihovna React) a HTML a CSS.

API

API představuje propojení mezi serverovou částí a klientskou částí. API je zabezpečeno tak, aby požadavky na server mohl volat pouze přihlášený uživatel (administrátor nebo WordPress web).

Model architektury aplikace a propojení s prezentačním webem

Následující obrázek zobrazuje jednotlivé komponenty aplikace, vztahy mezi nimi a propojení s WordPress webem.



Design a UI aplikace

Vizuální identita aplikace vychází z vizuální identity Actuaria a webové prezentace Actuaria (barvy, fonty, logotyp).

V rámci uživatelského rozhraní budou komponenty aplikace respektovat koncept a osnovu dle tzv. [Material Designu](#). Komponenty použité pro aplikaci budou vycházet z knihoven Material Design prototypů.

Cílem je jednoduchá ovladatelnost a přehlednost pro uživatele aplikace.

Jazykové mutace

Aplikace je vyvíjena v CS jazykové mutaci s možností rozšíření o další jazykové mutace (např. EN). Technickým jazykem aplikace je angličtina.

Hlavní funkce členské aplikace

Registrace

Uživatelé se registrují zadáním svého e-mailu pomocí registračního formuláře na webové prezentaci. Po registraci vzniká záznam v databázi uživatelů a následuje proces ověření e-mailu.

Ověření e-mailu

Uživatel ověřuje e-mailovou adresu prostřednictvím odkazu v e-mailu. E-mail může být ověřen i administrátorem aplikace.

Přihlášení

Uživatelé se přihlašují zadáním e-mailu a hesla prostřednictvím přihlašovacího formuláře na webu. Po úspěšném přihlášení získává uživatel autorizační token, který mu umožňuje volat API serverové části.

Zpřístupněné funkce po přihlášení uživatel

Veškeré funkce jsou zpracovávány prostřednictvím volání API serverové části. Jakmile je uživatel přihlášen, provádí v rámci webu následující činnosti.

- Zobrazuje vlastní profil,
- edituje vlastní profil,
- zobrazuje přehled předpisu členských příspěvků,
- zobrazuje přehled uhrazených členských příspěvků,
- zobrazuje veřejný seznam ostatních uživatelů,
- zobrazuje detail profilu jiného uživatele,
- zobrazuje stránky a příspěvky uzamčené pouze pro členy,
- diskutuje pod jednotlivými příspěvky,
- spravuje své publikace,
- spravuje svá data v CPD.

Vlastní profil uživatele a editace vlastního profilu

Přihlášený uživatel vidí svůj vlastní profil. V profilu uživatel edituje některé své atributy a u každého atributu edituje i jeho "viditelnost" pro ostatní skupiny uživatelů.

Následující tabulka zobrazuje evidované atributy uživatele vč. informace, kdo může atribut editovat nebo zobrazit.

Legenda: ADM = administrátor, SU = sám uživatel, PU = přihlášený (jiný) uživatel, SYS = systém / aplikace

Název atributu	Povinný atribut	Kdo edituje	Kdo vidí	Poznámka
Jméno + příjmení	A	SU, ADM	SU, ADM, PU	Vyplní se až po prvním přihlášení.
Obrázek / avatar	N	SU, ADM	SU, ADM, PI	
Rodné příjmení	N	SU, ADM	SU, ADM, PU	
Tituly (před + za)	N	SU, ADM	SU, ADM, PU	
Datum narození	A	SU, ADM	SU, ADM, PU	Vyplní se až po prvním přihlášení.
Kontaktní e-mail	N	SU, ADM	SU, ADM, PU	
Kontaktní telefon	N	SU, ADM	SU, ADM, PU	
Odkaz na LinkedIn	N	SU, ADM	SU, ADM, PU	
Odkaz na FaceBook	N	SU, ADM	SU, ADM, PU	
Webová adresa	N	SU, ADM	SU, ADM, PU	
Bydliště	N	SU, ADM	SU, ADM, PU	
Nejvyšší dosažené vzdělání	N	SU, ADM	SU, ADM, PU	
Koníčky	N	SU, ADM	SU, ADM, PU	
Poznámka / komentář	N	SU, ADM	SU, ADM, PU	
Interní poznámka / interní komentář	N	ADM	ADM	
Osvědčení od	N	SU, ADM	SU, ADM, PU	
Osvědčení do	N	SU, ADM	SU, ADM, PU	
Členství od	N	ADM	SU, ADM, PU	
Členství do	N	ADM	SU, ADM, PU	

Čestné členství	N	ADM	SU, ADM, PU	
Členství v orgánech ČSpA	N	ADM	SU, ADM, PU	
Členství v pracovních skupinách ČSpA	N	ADM	SU, ADM, PU	
Aktuální zaměstnavatel, pracovní pozice a zaměření	N	SU, ADM	SU, ADM, PU	
Role v rámci systému, do které je uživatel zařazen	A	ADM	ADM	
Skupina, do které je uživatel zařazen	N	ADM	SU, ADM, PU	
Přihlašovací kód do ActuView	N	ADM	SU, ADM	
Datum poslední kontroly profilu uživatelem	A	SYS	SYS, ADM	Pokud uživatel naposledy kontroloval aktualitu svého profilu před 365 dny, zobrazí se mu hláška s požadavkem o opětovnou kontrolu.
Uzamčení profilu	A	ADM	ADM	Uživatel se nemůže přihlásit.
Souhlas se zpracováním osobních údajů	A	SU, ADM	SU, ADM	
Souhlas s mailingem	A	SU, ADM	SU, ADM	
Přihlašovací e-mail	A	SU, ADM	SU, ADM	
Přihlašovací heslo	A	SU, ADM	-	
Přehled předpisů plateb	N	ADM	SU, ADM	
Přehled historie plateb	N	ADM	SU, ADM	
Publikace	A	SU, ADM	SU, ADM, PU	

Seznam uživatelů

Přihlášený uživatel zobrazuje seznam všech uživatelů ve formě tabulky. V této tabulce je možné vyhledávat a zobrazit detail jiného uživatele.

Detail jiného uživatele

Přihlášený uživatel vidí v profilu jiného uživatele pouze ty atributy, které jsou uvedené jako "PU" (ve sloupci "Kdo vidí" viz. tabulka výše).

Předpisy plateb a historie plateb

Uživatel vidí ve svém profilu předpisy a historii členských příspěvků. Předpisy a historie plateb jsou editovány administrátorem dávkově prostřednictvím např. sdíleného dokumentu tabulkového editoru (MS Excel, Google Sheets, Airtable).

Předpisy a historie plateb jsou spravovány administrátorem v rámci aplikace. Jsou umožněny dávkové importy.

Uživatelské role

V rámci aplikace existuje pouze role administrátor. Tento administrátor ostatním uživatelům definuje patřičnou "uživatelskou skupinu". Tyto skupiny budou specifikovány v průběhu vývoje aplikace.

Zabezpečení aplikace a vývoje

- Aplikace je hostována na serverech Zhotovitele, které jsou uloženy v datovém centru ServerPark (<https://www.serverpark.cz>), který
 - splňuje technické požadavky TIER IV,
 - zajišťuje výjimečnou fyzickou bezpečnost (<https://www.serverpark.cz/bezpecnost>),
 - monitoruje běh serverů 24 hodin denně,
 - servery byly podrobeny bezpečnostním auditům a penetračním testům od klientů Lagardère TR a Aegon/NN.
- Do databáze mají přístup pouze předem zvolení uživatelé (někteří pouze v režimu read-only).
- Databáze je provozována v odděleném Docker kontejneru.
- Citlivá data v databázi jsou hashovaná v nečitelné podobě.
- Parametry projektů a organizací jsou šifrovány šifrovacími mechanismy databáze a serveru.
- Přenos dat mezi klientem a serverem je šifrován (HTTPS/SSL).
- Registrace a přihlášení probíhá dvoufázově.
- Databáze je pravidelně zálohována 1x denně v nočních hodinách.
- Vstupy do databáze jsou logovány a monitorovány.
- Do administrace databáze jsou povoleny přístupy pouze z konkrétních IP adres.

- API na serveru může volat pouze povolená URL nebo IP adresa.
- Aplikace nepřijímá útoky typu XSS, SQL Injection či jiné podobné techniky.
- Vstupy do aplikace od uživatelů jsou kontrolovány a validovány.
- Architektura aplikace je přizpůsobena tak, aby mohlo existovat více různých nezávislých databází (např. z důvodu potřeby oddělení dat jedné organizace od druhé).
- Kód aplikace je při vývoji verzován prostřednictvím version-control systému Git, který je provozován na NAS zařízení Zhotovitele. Disky NAS jsou šifrovány a denně zálohovány do geograficky oddělené lokality na jiné NAS zařízení, jehož disky jsou také šifrovány.
- Disky všech členů týmu Zhotovitele, kteří mají přístup ke kódu aplikace, jsou šifrované.
- Přístupové údaje ke klíčovému částem aplikace jsou ukládány v šifrovaných databázích password managerů členů týmu Zhotovitele.
- Zhotovitel je pojištěn proti odpovědnosti IT.
- Objednatel na své náklady podrobí aplikaci penetračním testům (např. OWASP) a Zhotovitel na své náklady zajistí vyhovění požadavkům a nápravu nálezů.

Modul CPD

V administraci aplikace administrátor vytváří a publikuje "akci". Pro každou akci vyplňuje předem dané atributy (např. název, datum od-do, kategorie akce, atp.), povinnosti a vytváří předpis pro registrační formulář.

Klientská část akce načítá, zobrazuje je v kalendáři a umožňuje přihlášení uživatelům členské sekce.

Přihlášený uživatel ve svém profilu (a administrátor v rámci profilu uživatele) vidí akce, na které se přihlásil (minulé i budoucí) vč. získaných bodů, statistiky atp.

Administrátorovi je umožněno měnit přihlášení uživatele na akci a rovněž může měnit CPD data uživatele. Veškerá CPD data jsou verzovaná a auditovaná (tzn. jsou evidovány informace o vytvoření, změně atp.).

Během vývoje CPD modulu se předpokládá vyšší součinnost s Objednatelem za účelem zpřesňování zadání a průběžného testování.

Migrace dat

Migrace dat z původního systému do nového systému je oddělená činnost, která není součástí vývoje aplikace. Tato aktivita je naceněna zvlášť s ohledem na možnosti a struktury stávajícího systému.

Hosting a domény

V případě zájmu je možné zajistit hostování webu na serverech Query. Pro více informací viz. github.com/querycz/hosting-domeny a github.com/querycz/vop-hosting-domeny.

V rámci SLA dohody je upřednostňováno hostování na serverech Query kvůli kontrole nad webem a servery a spolehlivým a bezpečným přístupem k serverům.

Pravidelný dohled a aktualizace (SLA)

Pro více informací viz github.com/querycz/service-level-agreement.

Cenový odhad

Položka	Čas	Cena
Základ aplikace	4–5 měsíců	86 000 Kč
Implementace modulu CPD	2 měsíce	35 000 Kč
Migrace dat (dle rozsahu)	1–2 týdny	Dle hodinové sazby
Hosting		2 400 Kč / rok

Ceny jsou uvedeny bez DPH.

Cenová nabídka může být upravena při změně či upřesnění požadavků, o čemž bude Objednatel dopředu informován.

Hodinová sazba

Položka	Počet hod.	Cena
Hodinová sazba	1 hod.	1 200 Kč

Hodinová sazba je uvedena informativně. Použije se u dodatečných prací, které jsou naceněny hodinově (práce nad rámec původního zadání, konzultace, jednorázová aktualizace systému po spuštění atp.).

Obchodní podmínky

github.com/querycz/obchodni-podminky