# **SRS (software requirements specifications)**

Obsah

[**SRS (software requirements specifications)** 1](#_Toc165379934)

[Úvod 1](#_Toc165379935)

[Funkční požadavky 1](#_Toc165379936)

[Nedílné požadavky 2](#_Toc165379937)

[Architektura systému 2](#_Toc165379938)

[Závěr 2](#_Toc165379939)

## Úvod

Tento dokument popisuje požadavky na software pro vývoj autentizační aplikace využívající Node.js, Express.js, MongoDB a přidružené knihovny. Aplikace umožňuje registraci uživatelů, přihlašování, ověřování e-mailu, obnovu hesla a další funkce související s autentizací.

## Funkční požadavky

**Přihlášení uživatele**

* Systém poskytne formulář pro přihlášení registrovaných uživatelů.
* Uživatelé zadají svůj e-mail a heslo pro přihlášení.
* Systém ověří uživatelské přihlašovací údaje proti uloženým datům v databázi MongoDB s použitím bcrypt pro hašování hesel.
* Po úspěšném přihlášení systém přesměruje uživatele na domovskou stránku.
* Neúspěšné pokusy o přihlášení zobrazí odpovídající chybové zprávy.

**Ověření e-mailu**

* Po registraci systém vygeneruje jedinečný ověřovací token pro každého uživatele.
* Systém odešle e-mail obsahující odkaz k ověření na zadanou e-mailovou adresu uživatele.
* Kliknutí na odkaz pro ověření e-mailu ověří e-mailovou adresu uživatele.
* Ověření uživatelé budou mít ve databázi nastavený příznak "isVerified" na true.

**Obnova hesla**

* Uživatelé budou mít možnost obnovit svá hesla v případě zapomenutí.
* Systém poskytne formulář pro obnovu hesla, kde uživatelé mohou zadat svou e-mailovou adresu.
* Po odeslání žádosti o obnovu hesla systém odešle e-mail s instrukcemi a odkazem pro obnovu hesla.
* Kliknutí na odkaz pro obnovu hesla přesměruje uživatele na stránku, kde mohou zadat nové heslo.
* Po obnovení hesla systém uživatele oznámí e-mailem.

## Nedílné požadavky

Bezpečnost

- Hesla uživatelů budou bezpečně hašována pomocí bcrypt před uložením do databáze.

- Ověřovací tokeny a tokeny pro obnovu hesla budou bezpečně generovány a ukládány.

- Veškeré přenosy citlivých dat, jako jsou hesla a tokeny, budou šifrovány pomocí HTTPS.

- Přístup k uživatelským datům v databázi bude omezen pouze na autorizovaný personál.

Výkon

- Aplikace bude schopna efektivně zpracovávat současnou registraci uživatelů, přihlašování a další operace.

- Doba odezvy pro uživatelské interakce, jako je registrace a přihlášení, bude v rámci přijatelných limitů.

Spolehlivost

- Systém bude odolný proti možným selháním, jako jsou chyby v síti, výpadky databáze nebo pády serveru.

- Budou implementovány mechanismy pro zpracování chyb, které elegantně zvládnou neočekávané chyby a poskytnou uživatelům smysluplnou zpětnou vazbu.

Uživatelská přívětivost

- Uživatelské rozhraní bude intuitivní a uživatelsky přívětivé, s jasnými pokyny k provedení každé akce.

- Chybové zprávy budou popisné a povedou uživatele, jak napravit problémy během registrace, přihlášení a dalších interakcí

## Architektura systému

Aplikace bude postavena s využitím následujících technologií:

- Node.js pro běh serverového prostředí JavaScriptu.

- Express.js pro tvorbu webových aplikací a API.

- MongoDB pro ukládání uživatelských dat.

- bcrypt pro hašování hesel.

- nodemailer pro odesílání e-mailů.

- uuid pro generování jedinečných identifikátorů.

## Závěr

Tento dokument Specifikace požadavků softwaru (SRS) poskytuje komplexní přehled funkčních a nedílných požadavků pro autentizační aplikaci. Dodržení těchto požadavků zajistí vývoj bezpečného, spolehlivého a uživatelsky přívětivého autentizačního systému.