|  |  |  |
| --- | --- | --- |
|  | УНИВЕРЗИТЕТ У НОВОМ САДУ  **ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА У НОВОМ САДУ** |  |

Јелена Хрњак

**РАЗВОЈ ВЕБ апликацијА са безбедносном конфигурацијом**

**коришћењем НаменскОГ језикА *SECURI***

Мастер рад

- Мастер академске студије -

Нови Сад, 2023.

|  |  |  |  |
| --- | --- | --- | --- |
| Редни број, **РБР**: | |  | |
| Идентификациони број, **ИБР**: | |  | |
| Тип документације, **ТД**: | | Монографска документација | |
| Тип записа, **ТЗ**: | | Текстуални штампани материјал | |
| Врста рада, **ВР**: | | Мастер рад | |
| Аутор, **АУ**: | | Јелена Хрњак | |
| Ментор, **МН**: | | др Владимир Димитриески, доцент | |
| Наслов рада, **НР**: | | Наменски језик за генерисање... | |
| Језик публикације, **ЈП**: | | Српски / ћирилица | |
| Језик извода, **ЈИ**: | | Српски | |
| Земља публиковања, **ЗП**: | | Република Србија | |
| Уже географско подручје, **УГП**: | | Војводина | |
| Година, **ГО**: | | 2023 | |
| Издавач, **ИЗ**: | | Ауторски репринт / Факултет техничких наука | |
| Место и адреса, **МА**: | | Нови Сад, Трг Доситеја Обрадовића 6 | |
| Физички опис рада, **ФО**: (поглавља/страна/ цитата/табела/слика/графика/прилога) | | 6/45/0/50/36/0/0 | |
| Научна област, **НО**: | | Електротехничко и рачунарско инжењерство | |
| Научна дисциплина, **НД**: | | Примењене рачунарске науке и информатика | |
| Предметна одредница/Кqучне речи, **ПО**: | | Доменски оријентисано моделовање и језици | |
| **УДК** | |  | |
| Чува се, **ЧУ**: | | Библиотека Факултета техничких наука, Нови Сад | |
| Важна напомена, **ВН**: | |  | |
| Извод, **ИЗ**: | | TODO | |
| Датум прихватања теме, **ДП**: | |  | |
| Датум одбране, **ДО**: | |  | |
| Чланови комисије, **КО**: | Председник: |  |
|  | Члан: |  | Потпис ментора |
|  | Члан, ментор: | др Владимир Димитриески, доцент |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Accession number, **ANO**: | |  | |
| Identification number, **INO**: | |  | |
| Document type, **DT**: | | Monographic publication | |
| Type of record, **TR**: | | Textual printed material | |
| Contents code, **CC**: | | Graduate-master Thesis | |
| Author, **AU**: | | Jelena Hrnjak | |
| Mentor, **MN**: | | Vladimir Dimitrieski, PhD, Assistant Professor | |
| Title, **TI**: | | ... | |
| Language of text, **LT**: | | Serbian | |
| Language of abstract, **LA**: | | Serbian | |
| Country of publication, **CP**: | | Republic of Serbia | |
| Locality of publication, **LP**: | | Vojvodina | |
| Publication year, **PY**: | | 2023 | |
| Publisher, **PB**: | | Author’s reprint/Faculty of Technical Sciences | |
| Publication place, **PP**: | | Novi Sad, Faculty of Technical Sciences, Dositeja Obradovica sq. 6 | |
| Physical description, **PD**: (chapters/pages/ref./tables/pictures/graphs/appendixes) | | 6/45/0/50/36/0/0 | |
| Scientific field, **SF**: | | Electrical and computer engineering | |
| Scientific discipline, **SD**: | | Applied computer science and informatics | |
| Subject/Key words, **S**/**KW**: | | Domain-Specific Modeling Languages | |
| **UC** | |  | |
| Holding data, **HD**: | | The Library of Faculty of Technical Sciences, Novi Sad, Serbia | |
| Note, **N**: | |  | |
| Abstract, **AB**: | | TODO | |
| Accepted by the Scientific Board on, **ASB**: | |  | |
| Defended on, **DE**: | |  | |
| Defended Board, **DB**: | President: |  |
|  | Member: |  | Menthor's sign |
|  | Member, Mentor: | Vladimir Dimitrieski, PhD, Assistant Professor |  |

|  |  |  |
| --- | --- | --- |
|  | УНИВЕРЗИТЕТ У НОВОМ САДУ ⚫ **ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА**  21000 НОВИ САД, Трг Доситеја Обрадовића 6 | Датум: |
|  |
| **ЗАДАТАК ЗА ДИПЛОМСКИ РАД** | Лист/Листова: |
|  |

| Студијски програм: | **Рачунарство и аутоматика** |
| --- | --- |
| Руководилац стидијског програма: | др Милан Рапаић, редовни професор |

*(Податке уноси предметни наставник - ментор)*

|  |  |  |  |
| --- | --- | --- | --- |
| Студент: | **Јелена Хрњак** | Број индекса: | **Е2 64/2022** |
| Област: | **Примењене рачунарске науке и информатика** | | |
| Ментор: | **др Владимир Димитриески, доцент** | | |
| НА ОСНОВУ ПОДНЕТЕ ПРИЈАВЕ, ПРИЛОЖЕНЕ ДОКУМЕНТАЦИЈЕ И ОДРЕДБИ СТАТУТА ФАКУЛТЕТА ИЗДАЈЕ СЕ ЗАДАТАК ЗА МАСТЕР РАД, СА СЛЕДЕЋИМ ЕЛЕМЕНТИМА:   * проблем – тема рада; * начин решавања проблема и начин практичне провере резултата рада, ако је таква провера неопходна; * литература | | | |

**НАСЛОВ ДИПЛОМСКОГ РАДА:**

|  |
| --- |
| **Наменски језик за генерисање...** |

**ТЕКСТ ЗАДАТКА:**

|  |
| --- |
| * ... * ... |

|  |  |
| --- | --- |
| Руководилац студијског програма: | Ментор рада: |
|  |  |

|  |
| --- |
| Примерак за: - Студента; - Ментора |

**Садржај**

[1. Увод 1](#_Toc142147110)

[1.1 Структура рада 1](#_Toc142147111)

[2. Преглед постојећег стања у области 2](#_Toc142147112)

[3. Технологије коришћене при развоју наменског језика 3](#_Toc142147113)

[4. Апстрактна синтакса наменског језика 4](#_Toc142147114)

[4.1.1 Концепт *Application* 5](#_Toc142147115)

[4.1.2 Концепт Database 7](#_Toc142147116)

[4.1.3 Концепт *Entity* 8](#_Toc142147117)

[4.1.4 Концепт *Attribute* 8](#_Toc142147118)

[4.1.5 Концепт *User* 9](#_Toc142147119)

[4.1.6 Концепт *Role* 9](#_Toc142147120)

[4.1.7 Концепт *RoleInstance* 9](#_Toc142147121)

[4.1.8 Концепт *Controller* 9](#_Toc142147122)

[4.1.9 Концепт *Authentication* 10](#_Toc142147123)

[4.1.10 Концепт *Endpoint* 10](#_Toc142147124)

[4.1.11 Концепт *Security* 11](#_Toc142147125)

[4.1.12 Концепт *BasicAuthentication* 11](#_Toc142147126)

[4.1.13 Концепт *JWT* 11](#_Toc142147127)

[4.1.14 Концепт *Claim* 11](#_Toc142147128)

[4.1.15 Концепт *RegisteredClaim* 12](#_Toc142147129)

[4.1.16 Концепт *OAuth2* 12](#_Toc142147130)

[4.1.17 Концепт *Provider* 12](#_Toc142147131)

[5. Закључак 14](#_Toc142147132)

[Литература 16](#_Toc142147133)

[Биографија 17](#_Toc142147134)

# Увод

Коришћење веб апликација представља неизоставни део свакодневног живота за велики број корисника, али корисници често нису свесни колико личних података те апликације прикупљају, обрађују и складиште и колико безбедносни пропусти могу да утичу на њих. С обзиром на осетљивост и важност података којима апликације неретко рукују, неовлашћен приступ би могао да доведе до безбедносних ризика, укључујући злоупотребу и нарушавање приватности корисника. Стога, обезбеђивање високог нивоа заштите корисника и њихових података представља кључан циљ приликом развоја сигурних веб апликација.

Имплементација жељеног нивоа аутентификације и ауторизације, представља основу ефикасне заштите података од потенцијалних напада, крађе и злоупотребе. Међутим, обезбеђивање одговарајуће заштите за апликације представља сложен и временски захтеван процес, те је самим тим подложан грешкама. С обзиром да се безбедоносни апекти апликације изнова конфигуришу при почетној имплементацији сваке апликације, поред тога што је сложен и дуготрајан, овакав посао постаје и репетативан.

Са циљем уклањања наведених недостатака, тежи се оптимизацији и аутоматизацији развоја безбедних веб апликација како би се елиминисали безбедносни пропусти и грешке, али и уштедело време потребно при имплементацији. Једно од могућих решења представља аутоматско генерисање почетне веб апликације са конфигурисаним безбедносним механизмима који задовољавају потребе и захтеве корисника. Аутоматизација значајно олакшава рад програмерима због уштеде времена, доприноси квалитету софтвера и минимизира шансе за грешку.

Циљ овог рада је креирање модела сигурних веб апликација и генерисање кода на основу тог модела. Посебна пажња усмерена је ка убрзању конфигурисања безбедносних аспеката, али и развоја осталих целина веб апликације. За постизање овог циља креиран је наменски језик *Security Domain-Specific Language (securityDSL)* за моделовање апликација уз генераторе који модел трансформишу у извршиви код*.*

Како би моделовање веб апликација било могуће, неопходно је да *securityDSL* садржи концепте за моделовање свих елемената апликације. Основни елементи се односе на базу података, слој за репрезентацију података, обраду захтева корисника и безбедносну конфигурацију. Наменски језик *securityDSL* омогућава једноставну спецификацију свих параметара апликације помоћу синтаксе која је програмерима лако читљива и позната. На основу модела и наведених параметара, генератори генеришу извршиви код намисан у програмском језику *Java [1]*, коришћењем развојног оквира *Spring Boot[2]*. Овим имплементација сигурних веб апликација постаје једноставнија и ефикасниј,а уједно се смањује могућносг грешака у процесу развоја.

## Структура рада

Након уводног поглавља следи поглавње ,,Преглед постојећег стања у области” где је направљен осврт на постојећа решења и извршена анализа сличности и разлика у односу на наменски језик *securityDSL* и пратеће генераторе. У овом поглављу дате су теоријске основе моделом вођеног развоја и наменских језика, пружајући увид у постојеће стандарде.

Треће поглавље ,,Наменски језик за моделовање веб апликација“ обухвата детаљан опис делова наменског језика и концепата које овај језик садржи.

У поглављу ,,Генерисање веб апликација са безбедносном конфигурацијом“ описана је имплементација генератора који трансформишу модел у извршиви код. Детаљно су описани кораци генерисања апликације и конфигурације безбедносних аспеката.

Поглавље ,,Закључак“ садржи резултате истраживања и осврт на постигнућа у раду. Дате су препоруке за будућа унапређења и развој, као и могућност примене.

# Преглед постојећег стања у области

## Преглед постојећих начина за моделовање веб апликација

## Теоријске основе моделима вођеног развоја и наменских језика

## Преглед безбедносних механизама у *Spring Boot* апликацијама

### *Java*

### *Spring Boot*

### *Basic Authentication*

### Аутентификација помоћу *JSON Web* токена

### *OAuth2.0*

### *PostgreSQL*

### *MySQl*

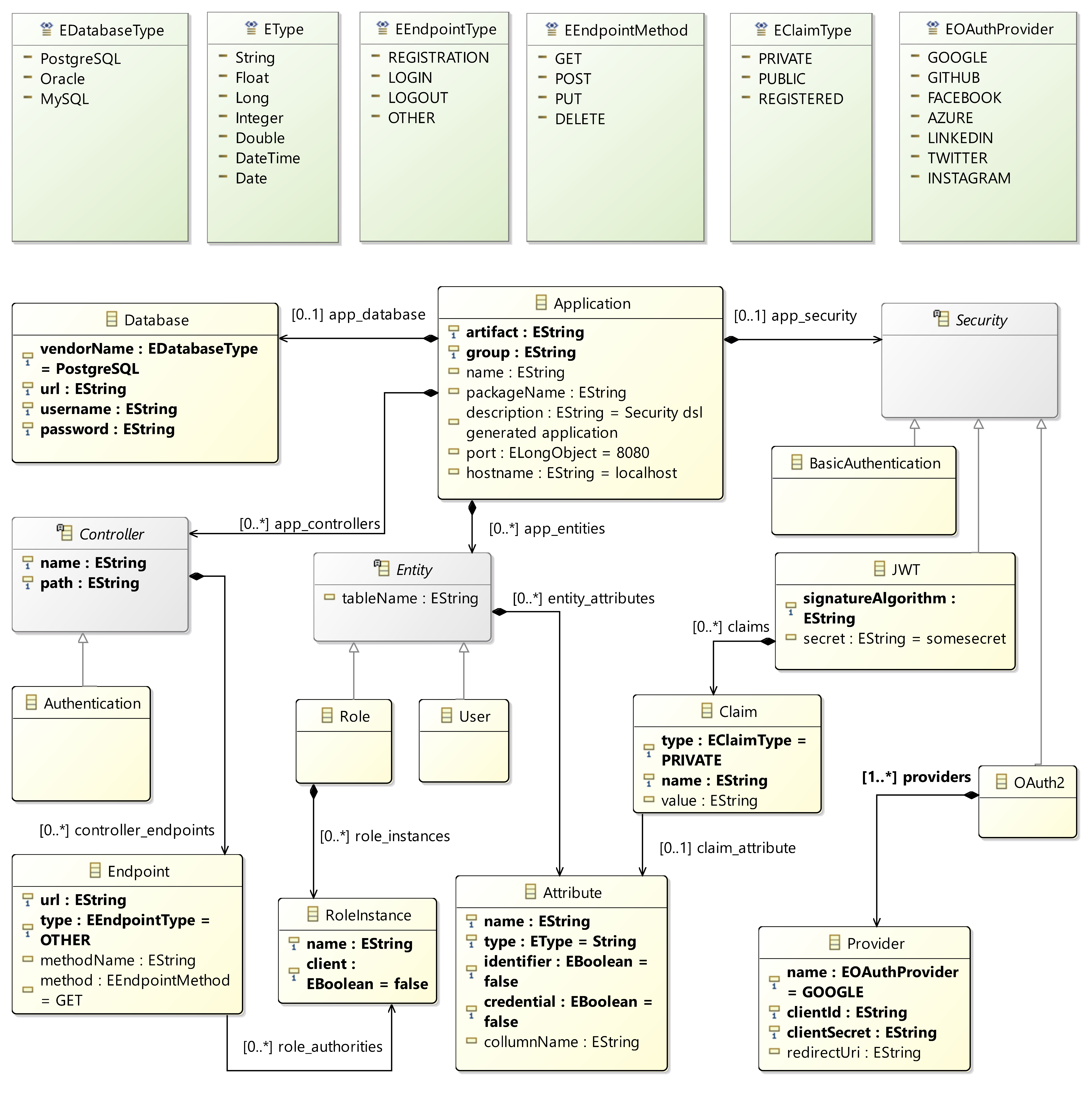
### *Oracle*

# Наменски језик за моделовање вебапликација

## Апстрактна синтакса

Апстрактна синтаска омогућава опис структуре наменског језика *securityDSL* и представљена је помоћу мета-модела (слика 4.1). Апликација која се генерише, а самим тим и апстрактна синтакса наменског језика *securityDSL*, може се поделити у пет целина:

* параметри који се односне на саму апликацију (као што су артефакт, опис итд.),
* параметри базе података,
* слој за репрезентацију података (ентитети),
* слој за обраду захтева корисника (контролери) и
* сигурносни слој који се односи на аутентификацију и контролу приступа корисника.



Слика 4.1 – Апстракнта синтакса наменског језика *securityDSL*

У даљем тексту дат је опис концепата апстрактне синтаксе, где су енглески називи концепата који су приказани на слици наведени курзивом.

Коренски концепт апстрактне синтаксе је апликација (*Application*) и садржи податке о параметрима неоходним за иницијализацију апликације. Кориснику је остављена могућност проширења генерисане апликације додатним концептима уз ограничења која ће бити наведена у наставку поглавља. Могуће је подесити параметре за повезивање са базом података *(Database)*, а поред тога, могу се дефинисати ентитети (*Entity*) који се односе на кориснике (*User*) и роле (*Role*). При дефинисању ентитета, неопходно је навести обележја (*Attribute*) за сваки ентитет. Концепт који се односи на обраду захтева корисника (*Controller*) је повезан са концептом *Endpoint* где је остављена могућност додавања метода које се односе на различите функционалности апликације. Навођењем инстанци рола (*RoleInstance*) које ће се налазити у систему и повезивањем са одређеним *endpoint-*овима омогућена је контрола приступа. Контролер за аутентификацију (*Authentication*) може да садржи методе за регистрацију, пријаву на систем и одјаву са система.

Посебан део апстрактне синтаксе односи се на сигурносни слој (*Security*), где су подржана три безбедносна механизма: основна аутентификација (*BasicAuthentication*), аутентификација заснована на *JWT* токенима (*JWT*) и *OAuth2.0* аутентификација *(OAuth2).* У зависности од жељеног механизма могу се дефинисати додатни параметри описани адекватним концептима.

Сваки од наведених концепата могу се додати или изоставити у зависности од потреба корисника. Оваква апстрактна синтакса омогућава кориснику флексибилност и једноставно проширење генерисане апликације у складу са потребама.

У наставку поглавља описани су сви концепти апстрактне синтаксе наменског језика *securityDSL* уз опис обележја и асоцијација концепата. Поред тога, наведена су и појашњена ограничења имплементирана помоћу декларативног језика *OCL.*

### Концепт *Application*

Коренски концепт апстрактне синтаксе *Application* садржи обележја која се односе на основне параметре неопходне за иницијализацију апликације.

|  |  |  |  |
| --- | --- | --- | --- |
| Назив обележја | Тип податка | Обавезно | Опис |
| *artifact* | *EString* | да | Назив артефакта |
| *group* | *EString* | да | Назив групе који представља организацију, компанију или тим који развија апликацију |
| *name* | *EString* | не | Назив апликације |
| *packageName* | *EString* | не | Назив пакета (*namespace)* у ком се налази изворни код апликације |
| *description* | *EString* | не | Опис апликације |
| *port* | *ELongObject* | не | Порт на ком апликација слуша захтеве |
| *hostname* | *EString* | не | Адреса рачунара или сервера на ком се извршава апликација |

Табела 4.1 – Обележја концепта *Application*

Портови у опсегу од 1024 до 49151 представљају регистроване портове који се могу доделити апликацији. Ограничење *validRegisteredPort* (листинг 4.1) гарантује да апликација користи валидан и регистрован порт.

**invariant** validRegisteredPort('Port must be in the valid range of

1024 to 49151!'):

**self**.*port* >= 1024 **and** **self**.*port* <= 49151;

Листинг 4.1 – Порт апликације мора бити унутар опсега регистрованих портова

|  |  |  |  |
| --- | --- | --- | --- |
| Назив асоцијације | Референцирани концепт | Кардиналитет | Опис |
| *app\_database* | *Database* | 0..1 | База података апликације |
| *app\_entitites* | *Entity* | 0..\* | Eнтитети у апликацији |
| *app\_controllers* | *Controller* | 0..\* | Контролери у апликацији |
| *app\_security* | *Security* | 0..1 | Безбедносна подешавања апликације |

Табела 4.2 – Асоцијације концепта *Application*

Апликација може садржати ентитете, контролере, базу података и аспекте безбедности. Кориснику је остављен простор да наведе или изостави одређене целине. Међутим, навођење неких целина повлачи одређена ограничења. Уколико се наведу ентитет, неопходно је да апликација има дефинисану базу података која складишти податке о тим ентитетима. Ово је омогућено *OCL* ограничењем *hasDatabawseForEntity* (листинг 4.2).

Листинг 4.2 – Уколико апликација има дефинисане ентитете, мора да има дефинисану базу података

**invariant** hasDatabaseForEntity('An application must have a database defined if it has entities!'):

**self**.*app\_entities* -> *isEmpty*() **or** **not** **self**.*app\_database*->*isEmpty*();

### Концепт Database

Апстрактни концепт *Database* представља параметре за повезивање апликације са базом података. Тип података *EDatabaseType* представља енумерацију заназив компаније која је развила жељени систем за управљање базама података. Корисник је дужан да унесе валидне креденцијале и конекциони стринг како би апликација успешно успоставила везу са базом података. Ово омогућава да апликација чита, додаје и ажурира податке сачуване у бази података.

|  |  |  |  |
| --- | --- | --- | --- |
| Назив обележја | Тип податка | Обавезно | Опис |
| *vendorName* | *EDatabaseType* | да | Систем за управљање базама података, при чему су могуће вредности *PostgreSQL, MySQL* и *Oracle* |
| *url* | *EString* | да | Конекциони стринг за повезивање са базом података |
| *username* | *EString* | да | Корисничко име за приступ бази података |
| *password* | *EString* | да | Лозинка за приступ бази података |

Табела 4.3 – Обележја концепта *Database*

### Концепт *Attribute*

Концепт *Attribute* моделује обележја која описују различите карактеристике ентитета. *EType* представља енумерацију за тип податка обележја моделованог концептом *Attribute.* Атрибут представља идентификатор ентитета уколико је вредност обележја *identifier* једнака *true,* док је атрибут креденцијал уколико је вредност обележја *credential* једнака *true.*

|  |  |  |  |
| --- | --- | --- | --- |
| Назив обележја | Тип податка | Обавезно | Опис |
| *name* | *EString* | да | Назив обележја |
| *type* | *EType* | да | Тип обележја, при чему су могуће вредности *String, Float, Long, Integer, Double, DateTime* и *Date* |
| *identifier* | *EBoolean* | да | Да ли је обележје идентификатор |
| *credential* | *EBoolean* | да | Да ли је обележје креденцијал |
| *collumnName* | *EString* | не | Назив колоне у табели базе података који се односи на обележје |

Табела 4.4 – Обележја концепта *Attribute*

### Концепт *Entity*

Ентитети апликације моделовани су помоћу концепта *Entity.* Асоцијација ентитета са концептом *Attribute* омогућава да ентитети садрже сва релевантна обележја за домен апликације*.*

|  |  |  |  |
| --- | --- | --- | --- |
| Назив обележја | Тип податка | Обавезно | Опис |
| *tableName* | *EString* | не | Назив табеле у бази података која се односи на ентитет |

Табела 4.5 – Обележја концепта *Entity*

Ограничење *uniqueTableName* (листинг 4.3) гарантује да сви ентиети имају јединствен назив табеле у бази података што спречава потенцијалне проблеме приликом рада са подацима. За ентитете за које није наведен, назив табеле биће изједначен са називом ентитета у множини (*users* или *roles*).

**invariant** uniqueTableName('Table names must be unique!'):

*Entity*.*allInstances*() ->

*select*(e | *e*.*tableName* <> **null**) -> *isUnique*(e | *e*.*tableName*.*toLower*());

Листинг 4.3 – Сви ентитети имају јединствен назив табеле у бази података

|  |  |  |  |
| --- | --- | --- | --- |
| Назив асоцијације | Референцирани концепт | Кардиналитет | Опис |
| *entity\_attributes* | *Attribute* | 0..\* | Обележја ентитета |

Табела 4.6 – Асоцијације концепта *Entity*

Асоцијација *entity\_attributes* моделује придруживање одређених атрибута ентитету. Јединственост назива атрибута у оквиру ентитета омогућена је ограничењем  *uniqueAttributeName* (листинг 4.4), док јединственост назива колона у табели, гарантује ограничењне *uniqueCollumnName* (листинг 4.5). Неопходно је ентитети да поседују тачно један идентификатор, што је обезбеђено ограничењем onlyOneIdentifier (листинг 4.6).

**invariant** uniqueAttributeName('Attribute names within an entity must be unique!'):

**self**.*entity\_attributes* -> *isUnique*(a | *a*.*name*);

Листинг 4.4 – Сви атрибути у окциру ентитета имају јединствене називе

**invariant** uniqueCollumnName('Column names must be unique if defined!'):

**self**.*entity\_attributes* -> *exists*(a | *a*.*collumnName* <> **null**) **implies**

**self**.*entity\_attributes* -> *isUnique*(a | *a*.*collumnName*);

Листинг 4.5 – Сви атрибути имају јениствене називе колона унутар табеле у бази података

**invariant** onlyOneIdentifier('Entity must have exactly one identifier attribute!'):

**self**.*entity\_attributes* -> *size*() > 0 **implies**

**self**.*entity\_attributes* -> *select*(a | *a*.*identifier*) -> *size*() = 1;

Листинг 4.6 – За ентитет мора да постоји тачно један атрибут који је идентификатор

### Концепт *User*

Приликом генерисања кода, концепт *User* биће искоришћен за генерисање класе које представља ентитет корисника апликације. Наслеђује концепт *Entity,* те садржи обележја која ближе описују корисника. Могуће је постојање највише једне инстанце концепта *User* за исправну конфигурацију апликације (листинг 4.7)

**invariant** uniqueUserEntity('There can be at most one entity of type "User" in the model!'):

*Entity*.*allInstances*() -> *select*(e | *e*.*oclIsTypeOf*(*User*)) -> *size*() <= 1;

Листинг 4.7 – Могуће је постојање највише једне инстанце концепта *User*

Атрибут који представља лозинку је подразумеван и биће генерисан са остатком кода, те не постоји потреба за експлицитним навођењем истог (листинг 4.8). Како би аутентификација била омогућена неопходно је да класа *User*, поред постојеће лозинке, поседује још тачно један атрибут који представља креденцијал (нпр. корисничко име). Ради једноставније провере креденцијала он мора бити типа *String.* Ово је гарантовано ограничењем *oneStringTypeCredentialForUser* (листинг 4.9). Увођењем креденцијала, потребно је онемогућити их у класама које не представљају кориснике система (листинг 4.10).

**invariant** noAttributeNamedPassword('User entity cannot have an attribute

named "password"!'):

**self**.*entity\_attributes* -> *forAll*(a | *a*.*name*.*toLower*() <> 'password');

Листинг 4.8 – За концепт *User* не сме да постоји атрибут који представља лозинку

**invariant** oneStringTypeCredentialForUser('User entity must have exactly one attribute of type String marked as a credential!'):

**self**.*entity\_attributes* -> *select*(a | *a*.*credential*) -> *size*() = 1

**and**

**self**.*entity\_attributes* ->

*select*(a | *a*.*credential*) -> *forAll*(a | *a*.*type* = *EType*::*String*);

Листинг 4.9 – За концепт *User* мора да постоји тачно један атрибут типа *String* који представља креденцијал

Листинг 4.10 – Само концепти *User* могу да поседују атрибут који представља креденцијал

**invariant** otherEntitiesDoesntHaveCredential('Entities other than User

cannot have a credential attribute!'):

**not** **self**.*oclIsTypeOf*(*User*) **implies** **self**.*entity\_attributes* -> *select*(a | *a*.*credential*) -> *isEmpty*();

### Концепт *Role*

Концепт *Role* наслеђује концепт *Entity* и моделује ентитет који се односи на роле апликације. Роле могу бити имплементиране као класе са различитим обележјима или као енумерација, што зависи од изабране безбедносне конфигурације у оквиру апликације. Могуће је постојање највише једне инстанце концепта *Role* (листинг 4.11).

|  |  |  |  |
| --- | --- | --- | --- |
| Назив асоцијације | Референцирани концепт | Кардиналитет | Опис |
| *role\_instances* | *RoleInstance* | 0..\* | Инстанце роли у апликацији |

Табела 4.7 – Асоцијације концепта *Role*

**invariant** uniqueRoleEntity('There can be at most one entity of type "Role" in the model!'):

*Entity*.*allInstances*() -> *select*(e | *e*.*oclIsTypeOf*(*Role*)) -> *size*() <= 1;

Листинг 4.11 – Могуће је постојање највише једне инстанце концепта *Role*

Дефинисано је ограничење *uniqueRoleInstanceName* (листинг 4.12), које осигурава да свака инстанца роле има уникатан назив. Ово ограничење омогућава избегавање конфликата приликом додавања нових рола.

**invariant** uniqueRoleInstanceName('Role instance names must be unique!'):

**self**.*role\_instances* -> *isUnique*(r | *r*.*name*);

Листинг 4.12 – Инстанце рола морају имати јединствен назив

### Концепт *RoleInstance*

Инстанце рола, било да је у питању енумерација или ентитет са обележјима, моделоване су помоћу концепта *RoleInstance*. Представљају роле које је могуће доделити корисницима система како би била омогућена контрола приступа ресурсима апликације.

|  |  |  |  |
| --- | --- | --- | --- |
| Назив обележја | Тип податка | Обавезно | Опис |
| *name* | *EString* | да | Назив конретне роле |
| *client* | *EBoolean* | да | Ознака да ли је рола клијент. Уколико је вредност обележја *false* рола је администраторска |

Табела 4.8 – Обележја концепта *RoleInstance*

### Концепт *Endpoint*

*Endpoint* је концепт који представља тачку комуникације између корисника и апликације, што га чини битним елементом за контролу приступа, односно саму безбедност апликације. Корисници комуницирају са сервером путем *endpointa* шаљући захтеве за извршавање одређених функционалности. Асоцијација *role\_authorities* описује роле којима је дозвољен приступ *endpoint*-у, односно роле које имају овлашћење да приступе одређеној функционалности систмеа.

|  |  |  |  |
| --- | --- | --- | --- |
| Назив обележја | Тип податка | Обавезно | Опис |
| *url* | *EString* | да | Путања, односно *URL* адреса *endpoint-*а, |
| *type* | *EEndpointType* | да | Тип *endpoint*-a, где су могуће вредности регистрација (*REGISTRATION*), пријављивање (*LOGIN*), одјављивање (*LOGOUT*) и друго (*OTHER*) |
| *methodName* | *EString* | да | Назив методе на коју се односи *endpoint* |
| *method* | *EEndpointMethod* | не | *HTTP* метод који означава каква је врста захтева, при чему су могуће вредности *GET, POST, PUT* и *DELETE* |

Табела 4.9 – Обележја концепта *Endpoint*

|  |  |  |  |
| --- | --- | --- | --- |
| Назив асоцијације | Референцирани концепт | Кардиналитет | Опис |
| *role\_authorities* | *RoleInstance* | 0..\* | Роле које имају право приступа *endpoint*-у |

Табела 4.10 – Асоцијације концепта *Endpoint*

Ограничење *urlStartsWithForwardSlash* (листинг 4.13) гарантује да путање *endpoint*-а започињу карактером ‘/’ што доприноси конзистентности апликације. Поред овог ограничења, битно је да роле којима је дозвољен приступ буду јединствене у оквиру *endpoint*-a (листинг 4.14).

**invariant** urlStartsWithForwardSlash('Endpoint URL should start with a forward

slash!'): **self**.*url*.*at*(1) = '/';

Листинг 4.13 – Путање *endpoint*-а започињу карактером ‘/’

Листинг 4.14 – Роле којима је додељен приступ *endpoint*-у не могу да се дуплирају унутар истог

**invariant** uniqueRoleAuthorities('Role authorities must be unique for each endpoint!'):

**self**.*role\_authorities* -> *isUnique*(r | *r*.*name*);

### Концепт *Controller*

Концепт *Controller* описује контролере апликације. Садржи информације о називу и путањи контролера, при чему је неопходно да обе вредности буду јединствене унутар апликације (листинг 4.15 и листинг 4.16). Уобичајено је да се називи контролера разликују од путања како би се избегли конфликти приликом рутирања захтева што је гарантовано ограничењем *uniqueControllerPath*. Путања контролера представља апсолутну путању у оквиру апликације, те је неопходно да почиње карактером '/'. Ово такође омогућава конзистентност генерисаног кода (листинг 4.17). Ентитети који се односе на кориснике (*User*) и роле (*Role*) доводе до постојања класа са истим називима, па самим тим постоји ограничење назива контролера (листинг 4.18).

|  |  |  |  |
| --- | --- | --- | --- |
| Назив обележја | Тип податка | Обавезно | Опис |
| *name* | *EString* | да | Назив контролера |
| *path* | *EString* | да | Путања контролера |

Табела 4.11 – Обележја концепта *Controller*

|  |  |  |  |
| --- | --- | --- | --- |
| Назив асоцијације | Референцирани концепт | Кардиналитет | Опис |
| *controller\_endpoints* | *Endpoint* | 0..\* | *Endpoint-*ови контролера |

Табела 4.12 – Асоцијације концепта *Controller*

**invariant** uniqueControllerName('Controllers should have unique names!'):

*Controller*.*allInstances*() -> *isUnique*(c | *c*.*name*);

Листинг 4.15 – Називи контролера унутар апликацјие морају да будујединствени

**invriant** uniqueControllerPath('Controller paths should be unique and

different from names!'):

*Controller*.*allInstances*() -> *isUnique*(c | *c*.*path*)

**and**

*Controller*.*allInstances*() ->

*forAll*(c | '/' + *c*.*name*.*toLower*() <> *c*.*path*.*toLower*());

Листинг 4.16 - Путање контролера унутар апликације морају да буду јединствени и да се разлику од назива контролера

**invariant** controllerPath('Controller path should start with \'/\'!'):

**self**.*path*.*at*(1) = '/';

Листинг 4.17 – Путања контролера мора да почиње караткером ‘/’

Листинг 4.18 – Ограничење назива за контролере

**invariant** controllerNotNamedUserRole('Controller names cannot be "User" or "Role"!'):

**not** *Controller*.*allInstances*() ->

*exists*(c | *c*.*name*.*toLower*() = 'user' **or** *c*.*name*.*toLower*() = 'role');

За правилно рутирање захтева и рад апликације неопходна је јединственост назива метода на које се односи *endpoint* (листинг 4.19)и путање *endpoint*-а(листинг 4.20) унутар контролера. *Endpoint*-овиза регистрацију, пријаву и одјаву са система имају препоручене, унапред дефинисане *HTTP* методе: *POST, POST* и *GET* редом. За *endpoint-*ове типа *OTHER* неопходно је навести метод (листинг 4.21). Регистрација, пријава и одјава са система су функционалности контролера за аутентификацију, те се ове врсте *endpoint-*ова не могу наћи у друдим конторлерима (листинг 4.22).

**invariant** uniqueEndpointMethodNames('Endpoints within a controller must have unique method names!'):

**self**.*controller\_endpoints* -> *isUnique*(e | *e*.*methodName*);

Листинг 4.19 – *Endpoint-*ови унутар контролера морају имају јединствене називе метода

**invariant** uniqueEndpointURLs('Endpoints within a controller must have unique URLs!'):

**self**.*controller\_endpoints* -> *isUnique*(e | *e*.*url*);

Листинг 4.20 – *Endpoint-*ови унутар контролера морају имају јединствене путање

**invariant** methodRequiredForOtherType('Endpoints of type "OTHER" must have a defined method!'):

**self**.*controller\_endpoints* -> *select*(e | *e*.*type* = *EEndpointType*::*OTHER*) -> *forAll*(e | *e*.*method* <> **null**);

Листинг 4.21 – *Endpoint-*ови типа *OTHER* морају да имају дефинисан *HTTP* метод

**invariant** endpointLimits('Controllers of type other than "Authentication" should not have registration, login, or logout endpoints!'):

**not** **self**.*oclIsTypeOf*(*Authentication*) **implies** (

**self**.*controller\_endpoints* ->

*select*(e | *e*.*type* = *EEndpointType*::*REGISTRATION*) -> *isEmpty*()

**and**

**self**.*controller\_endpoints* ->

*select*(e | *e*.*type* = *EEndpointType*::*LOGIN*) -> *isEmpty*()

**and**

**self**.*controller\_endpoints* ->

*select*(e | *e*.*type* = *EEndpointType*::*LOGOUT*) -> *isEmpty*());

Листинг 4.22 – *Endpoint-*ови за регистрацију, пријаву и одјаву са система могу да се налазе само у котнролеру за аутентификацију

### Концепт *Authentication*

Концепт *Authenticatiion* наслеђује *Controller.* Контролер за аутентификацију обрађује захтеве који се односе на регистрацију корисника, пријаву и одјаву корисника са система, те су информације о корисницима и њиховим ролама неопходни. Самим тим, уколико постоји контролер за аутентификацију, неопходно је да постоје инстанце концепата *User* и *Role* (листинг 4.23). Могуће је постојање највише једног контролера за аутентификацију (листинг 4.24). Уколико контролер за аутентификацију постоји, дозвољено је постојање највише једног *endpoint-*a за регистрацију, пријаву и одјаву са система што спречава вишеструко дефинисање истих функционалности (листинг 4.25).

Листинг 4.23 – За дефинисан контролер за аутентификацију, неопходно је постојање инстанци концепата User и Role

**invariant** hasUserAndRoleForController ('Authentication controller requires at least one User entity and one Role entity!'):

*Entity*.*allInstances*() -> *exists*(e | *e*.*oclIsTypeOf*(*User*))

**and**

*Entity*.*allInstances*() -> *exists*(e | *e*.*oclIsTypeOf*(*Role*));

Листинг 4.24 – Могуће је постојање највише једног контролера за аутентификацију

**invariant** uniqueAuthenticationController('There can be at most one controller of type "Authentication" in the model!'):

*Controller*.*allInstances*() ->

*select*(c |*c*.*oclIsTypeOf*(*Authentication*)) -> *size*() <= 1;

Листинг 4.25 – Могуће је постојање највише једног *endpoint-*а за регистрацију, пријаву и одјаву са система

**invariant** authenticationLimits('Authentication can have at most one registration, login, and logout endpoint!'):

**self**.*controller\_endpoints* ->

*select*(e | *e*.*type* = *EEndpointType*::*REGISTRATION*) -> *size*() <= 1

**and**

**self**.*controller\_endpoints* ->

*select*(e | *e*.*type* = *EEndpointType*::*LOGIN*) -> *size*() <= 1

**and**

**self**.*controller\_endpoints* ->

*select*(e | *e*.*type* = *EEndpointType*::*LOGOUT*) -> *size*() <= 1;

### Концепт *Security*

Концепт *Security* представља важну апстракцију у моделу која је кључна за обезбеђивање сигурне апликације. Овај концепт омогућава имплементацију жељеног нивоа аутентификације и ауторизације, што представља основу ефикасне заштите података од поденцијалних напада и злоупотребе. Кроз наслеђивање, омогућене су три различите безбедносне конфгифурације:

* *Basic Authentication,*
* *JSON Web Token* и
* *OAuth2.0.*

Овим се обезбеђује флексибилност и могућност одабира најбољег безбедносног механизма у зависности од потреба и захтева система.

### Концепт *BasicAuthentication*

Концепт *BasicAuthentication* наслеђује *Security* и моделује основну безбедносну конфигурацију. У случају одабира основне аутентификације (*BasicAuthentication*) роле ће у апликацији бити представљене као енумерација. Самим тим нису дозвољена обележја, већ само инстанце ролa (листинг 4.26)*.*

**Invariant** basicAuthNoRoleAttributes('Basic authentication cannot have role attributes!'):

*Entity*.*allInstances*() -> *select*(e | *e*.*oclIsTypeOf*(*Role*))

> *forAll*(role | *role*.*entity\_attributes* -> *size*() = 0)

Листинг 4.26 – У случају основне аутентификације нису дозвољена придружена обележја конепту *Role*

### Концепт *JWT*

Аутентификацију помоћу *JSON Web* токена моделује концепт *JWT* који наслеђује концепт *Security.*

|  |  |  |  |
| --- | --- | --- | --- |
| Назив обележја | Тип податка | Обавезно | Опис |
| *signatureAlgorithm* | *EString* | да | Алгоритам који се користи за потписивање *JWT* токена |
| *secret* | *EString* | не | Тајни кључ који се користи за потписивање *JWT* токена |

Табела 4.13 – Обележја концепта *JWT*

|  |  |  |  |
| --- | --- | --- | --- |
| Назив асоцијације | Референцирани концепт | Кардиналитет | Опис |
| *claims* | *Claim* | 0..\* | Тврдње у оквиру *JWT* токена |

Табела 4.14 – Асоцијације концепта *JWT*

За аутентификацију помоћу токена *JWT* роле представљају класу са обележјима. Како би инстанце ролa биле омогућене, неопходно је да у случају одабира аутентификације на основу *JWT* токена за класу *Role* постоји тачно једно обележје које је типа *String.* Поред тога, дозвољено је само обележје које представља идентификатор. У случају да је идентификатор типа *String,* нису дозвољена додатна обележја. Ово је гарантовано обележјима *roleHasMaxTwoAttributes* и *roleHasStringAttribute* (листинг 4.27).

**invariant** roleHasMaxTwoAttributes ('Role entities can have at most two attributes!'):

*Entity*.*allInstances*() -> *select*(e | *e*.*oclIsTypeOf*(*Role*)) ->

*forAll*(role | *role*.*entity\_attributes* -> *size*() <= 2);

**invariant** roleHasStringAttribute('Role entities must have either one identifier attribute of type String or both identifier and non-identifier attributes of type String!'):

*Entity*.*allInstances*() -> *select*(e | *e*.*oclIsTypeOf*(*Role*)) ->

*forAll*(role | (*role*.*entity\_attributes* -> *select*(a | *a*.*identifier*

**and** *a*.*type* = *EType*::*\_'String'*) -> *size*() = 1

**and** *role*.*entity\_attributes* ->

*select*(a | *a*.*type* = *EType*::*\_'String'*) -> *size*() = 1)

**or** (*role*.*entity\_attributes* -> *select*(a | *a*.*identifier*

**and** *a*.*type* <> *EType*::*\_'String'*) -> *size*() = 1

**and** *role*.*entity\_attributes* ->

*select*(a | *a*.*type* = *EType*::*\_'String'*) -> *size*() = 1));

Листинг 4.27 – У случају аутентификације помоћу *JWT* токена*,* рола може да има тачно једно обележје типа *String*

### Концепт *Claim*

Концепт *Claim* представља трврдње које садржи *JWT* токен, односно податке о кориснику, стању апликацје или самом токену које се преносе путем токена. Постоје три типа тврдњи: регистроване (предефинисане), приватне и јавне. Поред типа, тврдња има назив који представља идентификаотр пода тка и вредност која се односи на дати назив. Уколико се тврдња односи на податке о кориснику, она је повезана са атрибутом који садржи њену вредност. Све тврдње морају имати јединствен назив (листинг 4.28) и за један атрибут може бити везана највише једна тврдња (листинг 4.29)

|  |  |  |  |
| --- | --- | --- | --- |
| Назив обележја | Тип податка | Обавезно | Опис |
| *type* | *EClaimType* | да | Тип тврдње, при чему су могуће вредности *PRIVATE, PUBLIC* и *REGISTERED* |
| *name* | *EString* | да | Назив трвдње |
| *value* | *EString* | не | Вредност тврдње |

Табела 4.16 – Обележја концепта *Claim*

|  |  |  |  |
| --- | --- | --- | --- |
| Назив асоцијације | Референцирани концепт | Кардиналитет | Опис |
| *claim\_attributes* | *Attribute* | 0..1 | Атрибут на ког се тврдња односи и који садржи додатне информације о њој |

Табела 4.17 – Асоцијације концепта *Claim*

**invariant** uniqueClaimNames('Claims must have unique names'):

*Claim*.*allInstances*() -> *isUnique*(c | *c*.*name*);

Листинг 4.28 – Тврдње морају имати јединствен назив

**invariant** uniqueClaimAttribute('Claim attributes must be unique!'):

*Claim*.*allInstances*() -> *select*(c | *c*.*claim\_attribute* <> **null**) ->

*isUnique*(c | *c*.*claim\_attribute*);

Листинг 4.29 – Атрибут може бити повезан са највише једном тврдњом

Основне регистроване, односно предефинисане трврње су време важења токена након ког он више није валидан (*expirationTime),* корисници или субјекти којима је токен намењен (*audience*)*,* издавач токена (*issuer)* и идентификатор корисника (*subject*) те оне морају бити типа *REGISTERED.* Поред тога, тврдње *expirationTime* и *audience* су обавезне јер су неопходне за аутентификацију путем токена(листинг 4.30)*.* С обзиром да *еxpirationTime, audience* и *issuer* не садрже податке о кориснику, оне не могу бити повезане са атрибутом корисника, већ морају имати дефинисану вредност (листинг 4.31), док остале тврдње морају бити повезане са неким атрибутом (4.32). Тврдња везана за време важења токена мора да има позитивну вредност (листинг 4.33).

**invariant** subjectRegisteredClaim('If claim name is "subject", it must be of type REGISTERED'):

*Claim*.*allInstances*() -> *select*(c | *c*.*name* = 'subject') ->

*forAll*(sc | *sc*.*type* = *EClaimType*::*REGISTERED*);

**invariant** issuerRegisteredClaim('If claim name is "issuer", it must be of type REGISTERED'):

*Claim*.*allInstances*() -> *select*(c | *c*.*name* = 'issuer') ->

*forAll*(sc | *sc*.*type* = *EClaimType*::*REGISTERED*);

**invariant** hasExpirationTimeClaim('The claim "expirationTime" must exist and be of type REGISTERED'):

*Claim*.*allInstances*() ->

*exists*(c | *c*.*name* = 'expirationTime' **and** *c*.*type* = *EClaimType*::*REGISTERED*);

**Invariant** hasAudienceClaim('The claim "audience" must exist and be of type REGISTERED'):

*Claim*.*allInstances*() ->

*exists*(c | *c*.*name* = 'audience' **and** *c*.*type* = *EClaimType*::*REGISTERED*);

Листинг 4.30 – Основне регистроване тврдње морају бити типа *REGISTERED* и тврдње *expirationTime* и *audience* су обавезне

**Invariant** issuerValueNotNull('If the claim name is "issuer", it must have value and must not be linked to an attribute'):

*Claim*.*allInstances*() -> *select*(c | *c*.*name* = 'issuer') ->

*forAll*(sc | *sc*.*value* <> **null** **and** *sc*.*claim\_attribute* = **null**);

**invariant** audienceValueNotNull('If the claim name is "audience", it must have value and must not be linked to an attribute'):

*Claim*.*allInstances*() -> *select*(c | *c*.*name* = 'audience') ->

*forAll*(sc | *sc*.*value* <> **null** **and** *sc*.*claim\_attribute* = **null**);

**invariant** expirationTimeValueNotNull('If the claim name is "expirationTime", it must have value and must not be linked to an attribute'):

*Claim*.*allInstances*() -> *select*(c | *c*.*name* = 'expirationTime') ->

*forAll*(sc | *sc*.*value* <> **null** **and** *sc*.*claim\_attribute* = **null**);

Листинг 4.31 – Тврдње *issuer, audience* и *expirationTime* морају имати дефинисану вредност и не могу бити везане за атрибут ентитета *User*

**Invariant** otherClaimsNoValue('Claim must be linked to an attribute'):

*Claim*.*allInstances*() -> *select*(c | *c*.*name* <> 'issuer' **and** *c*.*name* <>

'audience' **and** *c*.*name* <> 'expirationTime') ->

*forAll*(sc | *sc*.*value* = **null** **and** *sc*.*claim\_attribute* <> **null**);

Листинг 4.32 – Тврдње које нису *issuer, audience* и *expirationTime* не могу имати дефинисану вредност и морају бити везане за атрибут ентитета *User*

**Invariant** expirationTimeValueIsPositiveNumeric('If the claim name is "expirationTime", the value must be a positive number'):

*Claim*.*allInstances*() -> *select*(c | *c*.*name* = 'expirationTime') ->

*forAll*(sc | *sc*.*value* <> **null** **and** *sc*.*value*.*toInteger*() > 0);

Листинг 4.33 – Тврдња везана за време важења токена мора да има позитивну вредност

### Концепт *OAuth2*

|  |  |  |  |
| --- | --- | --- | --- |
| Назив асоцијације | Референцирани концепт | Кардиналитет | Опис |
| *providers* | *Provider* | 1..\* | Конфигурисани провајдери у апликацији |

Табела 4.18 – Асоцијације концепта *OAuth2*

### Концепт *Provider*

|  |  |  |  |
| --- | --- | --- | --- |
| Назив обележја | Тип податка | Обавезно | Опис |
| *name* | *EOAuthProvider* | да | Назив провајдера, при чему су могуће вредности *Google, Github, Facebook, Microsoft azure, Linkedin, Twitter* и *Instagram* |
| *clientId* | *EString* | да | Идентификациони број клијента додељен од стране провајдера |
| *clientSecret* | *EString* | да | Тајни кључ клијента додељен од стране провајдера за сигурносну контролу приликом комуникације са провајдером |
| *redirectUri* | *EString* | не | Адреса за преусмерење након успешне аутентификације |

Табела 4.19 – Обележја концепта *Provider*

# Генерисање веб апликација са безбедносном конфигурацијом

# Закључак

# Скраћенице

* *ecurityDSL – Security Domain-Specific Language*
* *JWT - JSON Web Token*
* *OCL* – *Object Constraint Language*
* URL – *Uniform Resource Locator*
* HTTP – *Hypertext Transfer Protocol*

# Литература

*[1] Java Documentation,* [*https://docs.oracle.com/en/java/*](https://docs.oracle.com/en/java/)

*[2] Spring Boot Documentation,* [*https://spring.io/projects/spring-boot/*](https://spring.io/projects/spring-boot/)

*[3] PostgreSQL,* [*https://www.postgresql.org/about/*](https://www.postgresql.org/about/)

*[x] Basic Authentication,* [*https://docs.spring.io/spring-security/reference/servlet/authentication/passwords/basic.html#page-title*](https://docs.spring.io/spring-security/reference/servlet/authentication/passwords/basic.html%23page-title)

# Биографија

Јелена Хрњак рођена је 21. августа 1999. године у Бачкој Тополи где је стекла основно образовање у основној школи ,,Никола Тесла”. Даље школовање је наставила у Суботици где је завршила Гимназију ,,Светозар Марковић”, природно-математички смер. Школске 2018/2019 године уписује се на Факултет техничких наука Универзитета у Новом Саду, смер Рачунарство и аутоматика. Основне академске студије завршила је 2022. године и исте године уписује се на мастер академске студије на студијском програму Рачунарство и аутиматика Факултета теничких наука. Положила је све испите предвиђене планом и програмом мастер академских студија.