



**Hochschule für Technik  
und Wirtschaft Berlin**

University of Applied Sciences

*Design & Implementation of a Fraud Detection System for Autonomous Teams (Total  
pages should be: 50 [without Attachments])*

Abschlussarbeit

zur Erlangung des akademischen Grades:

**Bachelor of Science (B.Sc.)**

an der

Hochschule für Technik und Wirtschaft (HTW) Berlin  
Fachbereich 4: Informatik, Kommunikation und Wirtschaft  
Studiengang *Angewandte Informatik*

1. Gutachterin: Prof. Dr. Christin Schmidt
2. Gutachter: MSc. Tobias Dumke

Eingereicht von Louis Andrew [s0570624]

Datum

Last updated on Mon Jun 13 13:29:26 UTC 2022

## **Abstract**

[Summary of the thesis]

# Contents

<b>1. Introduction</b>	<b>1</b>
1.1. Background and Motivation . . . . .	3
1.2. Goal . . . . .	3
1.3. Scope . . . . .	3
<b>2. Fundamentals</b>	<b>4</b>
2.1. Kontext . . . . .	4
2.1.1. Domain . . . . .	4
2.1.2. Technologien . . . . .	4
2.1.3. Methoden und Konzepte . . . . .	4
2.2. ... . . . .	4
2.2.1. ... . . . .	4
2.2.2. ... . . . .	4
<b>3. Requirement Analysis (!)</b>	<b>5</b>
3.1. Goal? . . . . .	5
3.2. Application Environment . . . . .	5
3.3. Analysis / State of Art . . . . .	5
3.4. Requirements . . . . .	5
<b>4. Conception and Design</b>	<b>6</b>
4.1. System Architecture . . . . .	6
4.2. Software Architecture . . . . .	7
4.3. Technologies . . . . .	8
4.3.1. User Interface . . . . .	9
4.3.2. FDS . . . . .	10
4.3.3. Message Broker / Notification System . . . . .	10
4.3.4. Database and Caching Memory . . . . .	10
4.4. Software Design . . . . .	10
4.4.1. Controller . . . . .	11
4.4.2. Model . . . . .	16
4.4.3. View . . . . .	22
<b>5. Implementation</b>	<b>26</b>
5.1. Model . . . . .	26
5.2. View . . . . .	26
5.3. Controller . . . . .	26
<b>6. Test</b>	<b>27</b>

## *Contents*

<b>7. Demonstration and Evaluation</b>	<b>28</b>
7.1. Ausblick . . . . .	29
<b>Bibliography</b>	<b>30</b>
<b>8. List of Abbreviations</b>	<b>32</b>
<b>9. Glossary</b>	<b>33</b>
<b>A. Appendix</b>	<b>I</b>
A.1. Supplemental Figures . . . . .	I
A.2. Quell-Code . . . . .	I
A.3. Tipps zum Schreiben Ihrer Abschlussarbeit . . . . .	I

# List of Figures

1.1. Example image: Who is Steinlaus?; Bildquelle [9] . . . . .	2
1.2. Beispielgrafik: Fressende Steinlaus; Bildquelle [8] . . . . .	2
4.1. System architecture diagram . . . . .	6
4.2. Software architecture diagram . . . . .	7
4.3. Software architecture diagram with technologies used . . . . .	9
4.4. System sequence diagram for a customer validation when a new customer is registered . . . . .	11
4.5. System sequence diagram for notifications on suspicious cases . . . . .	13
4.6. System sequence diagram for validation rules management . . . . .	14
4.7. System sequence diagram for validation rules management . . . . .	15
4.8. UML diagram of the validation rule model . . . . .	17
4.9. UML diagram of the validation result model . . . . .	20
4.10. Mock up of the rule management form page . . . . .	23
4.11. Mock up of the validation form page . . . . .	24
4.12. Mock up of the validation progress page . . . . .	25
A.1. UML diagram of the customer model . . . . .	I

# List of Tables

1.1. Übersicht: Untersuchte Steinläuse . . . . .	2
--	---

# Listings

4.1. Validation rule example (JSON) . . . . .	18
4.2. Validation rule <b>condition</b> attribute example with ALL condition (JSON)	18
4.3. Validation rule <b>condition</b> attribute example with ANY condition (JSON)	19
4.4. Validation result example (JSON) . . . . .	21
5.1. Ein Beispiel: Hello World (JavaScript) . . . . .	26

# 1. Introduction

Vorliegendes Template enthält exemplarisch (und damit unvollständig) Gliederungspunkte, Bestandteile und Hinweise für ein typisches Softwareentwicklungsprojekt, bei dem ein Prototyp erstellt wird. Es dient als Hilfestellung zu Ihrer weiteren Verwendung. Selbstverständlich müssen Sie selbst weitere Ergänzungen und Anpassungen vornehmen.

**Viel Erfolg sowie gutes Gelingen bei Ihrer Abschlussarbeit!**

Der Textteil beginnt hier und wird arabisch mit dieser Seite beginnend mit »1« arabisch nummeriert. Der Textteil gliedert sich in Kapitel und Unterkapitel. Soll jede Hierarchieebene benannt werden, dann ist folgende Terminologie üblich:

- 1. Hierarchieebene: Chapter
- 2. Hierarchieebene: Section
- 3. Hierarchieebene: Subsection
- 4. Hierarchieebene: Subsubsection

Der inhaltliche Aufbau einer Abschlussarbeit im Studiengang *Angewandte Informatik* hängt selbstverständlich vom Thema und vom Inhalt ab. Abweichungen von der diesem Template zu Grunde liegenden Gliederungsstruktur sind immer möglich, manchmal sogar zwingend notwendig. Stimmen Sie sich diesbezüglich immer mit Ihren Gutachter(inne)n ab.

Vergessen Sie niemals, all Ihre verwendeten Quellen anzugeben und korrekt zu zitieren<sup>1</sup>. Quellen können manuell referenziert und im Quellenverzeichnis eingetragen werden. Ergänzend bieten viele Textverarbeitungssysteme auch ausgelagerte Quellenverwaltungsdateien und -systeme an, über die mittels entsprechender Befehle im Textteil zitiert werden kann<sup>2</sup>.

Visualisieren Sie im Textteil angemessen, z.B. mittels Abbildungen und Tabellen. Vorliegendes Template enthält beispielhaft eingebundene Abbildungen und eine Tabelle (vgl. f.), welche der Steinlausforschung<sup>3</sup> entnommen sind.

---

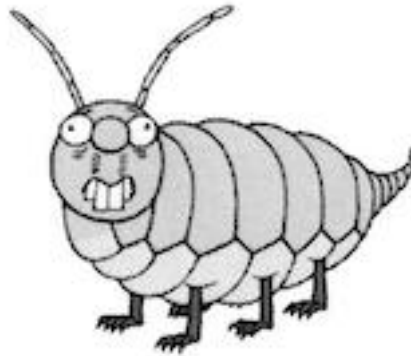
<sup>1</sup>Ergänzende Informationen können Sie auch in eine Fußnote auslagern. Hier wird die Fußnote dazu genutzt, um Ihnen bei Interesse am Thema Zitation vertiefende Quellen (z.B. [1] oder [2]) anzubieten.

<sup>2</sup>Wie Sie hoffentlich feststellen werden, erfolgt die Literaturverwaltung in diesem Template mittels einer \*.bib-Datei (diese enthält die verwendeten Quellen), welche die \*.tex-Datei mittels Verwendung von biblatex und bibtex ergänzt.

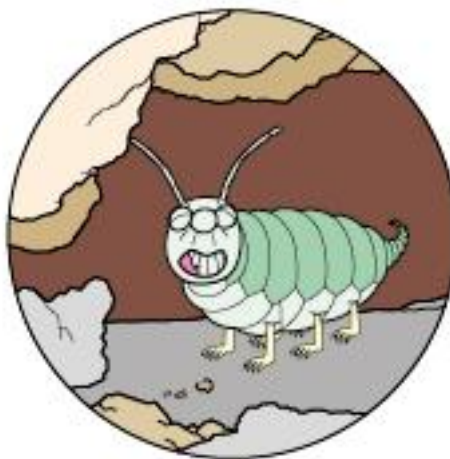
<sup>3</sup>Analog zu Straube (In: [13]) handelt es sich bei der Steinlaus (*petrophaga lorioti*) um das »kleinste einheimische Nagetier«. Als stimmungsaufhellender Endoparasit erreicht es eine Größe von ca. 0,3 bis 3 mm und stammt aus der Familie der Lapivora. Die Steinlaus kommt ubiquitär vor und ist in der Regel apathogen.



## 1. Introduction



**Figure 1.1.:** Example image: Who is Steinlaus?; Bildquelle [9]



**Figure 1.2.:** Beispielgrafik: Fressende Steinlaus; Bildquelle [8]

**Table 1.1.:** Übersicht: Untersuchte Steinläuse

Untersuchte Objekte mit Lokation des Habitats		
ID (nickname)	Ort	Grö"se/Länge (in mm)
1 (Rosalinde)	Berlin, Mauerpark	1.4
2 (Devil in disguise)	Brandenburg, BER-Airport	2.8
3 (Hannes)	Berlin, Olympia-Stadion	2.1
4 (Her Majesty)	Berlin, Humboldt-Forum	2.0

## *1. Introduction*

### **1.1. Background and Motivation**

The background and motivation of the thesis is to get my bachelor degree.

### **1.2. Goal**

Goal of the thesis is to build a cool software

### **1.3. Scope**

Scope of the thesis is to not build a new internet protocol

## 2. Fundamentals

**TODO!** [Beschreibung des Kontextes der Arbeit mit allen durch die Problemstellung tangierten Bereichen, Methoden, Theorien, Erkenntnissen, Technologien, ... ]

### 2.1. Kontext

#### 2.1.1. Domain

#### 2.1.2. Technologien

#### 2.1.3. Methoden und Konzepte

### 2.2. ...

#### 2.2.1. ...

#### 2.2.2. ...

## 3. Requirement Analysis (!)

[Beschreibung der Erhebung, Granularisierung und Priorisierung der zu Grunde liegenden Anforderungen]

### 3.1. Goal?

Hi mom, I'm . trying to cite ISO thingy [6]

### 3.2. Application Environment

### 3.3. Analysis / State of Art

### 3.4. Requirements

Optionals:

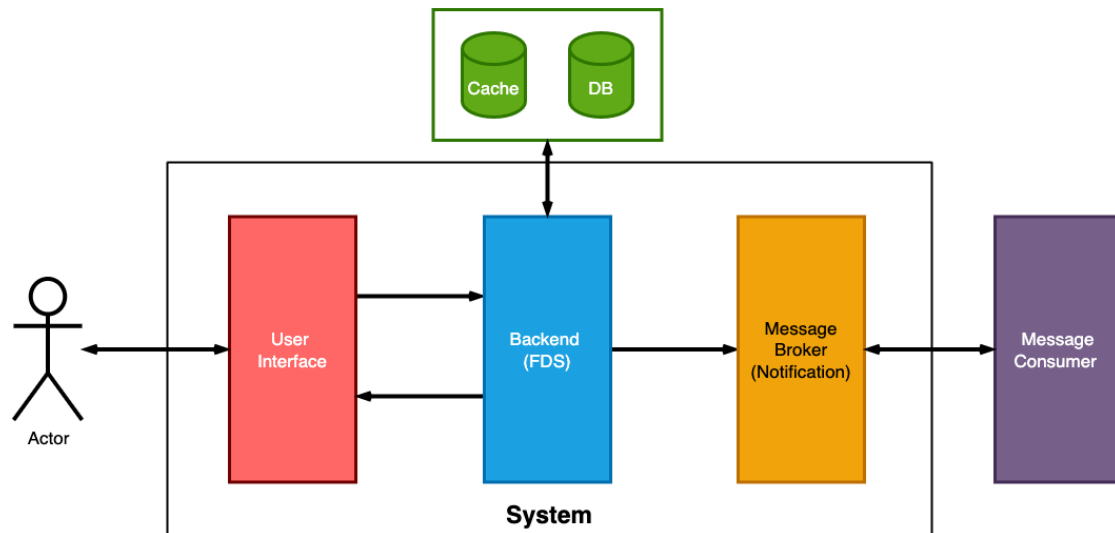
- *Rahmenbedingung*
- Methods

## 4. Conception and Design

As the requirements are analyzed, the concept and design of the system can now be defined. This chapter describes the structure, functionalities, technologies and patterns used by the system to fulfill the requirements listed.

### 4.1. System Architecture

A system architecture diagram is created to help to understand the system as well as its components better.



**Figure 4.1.:** *System architecture diagram*

The system diagram visualizes the components of the system and their interaction with each other. Internally, the system contains 3 independent components; user interface (UI), fraud detection service (FDS) and a message broker (notification system). Externally, the system would interact with a database and optionally a cache memory<sup>1</sup> to persist information needed for the validation process. The diagram also visualizes an external system (*message consumer*) which is indeed out of the system's scope, but plays an important role to determine which action should be taken on certain events. Further information on the function as well as connection between each component will be discussed on the next section.

<sup>1</sup>Cache memories are small, but extremely fast memory used in computer systems to store information that are going to be accessed in a small timeframe [14]

## 4.2. Software Architecture

As the requirement is clear and the components of the system are defined, a software architecture is needed. A software architecture plays a major role in a software development project by providing a structure on how the software should be built and decisions made during this stage would be vital for the development process going forward. As Garlan wrote in one of his work *Software Architecture*, a software architecture “plays a key role as a bridge between requirements and implementation.”[5] A software architecture diagram is therefore created to help visualize the structure, functions and role of each component of the system.

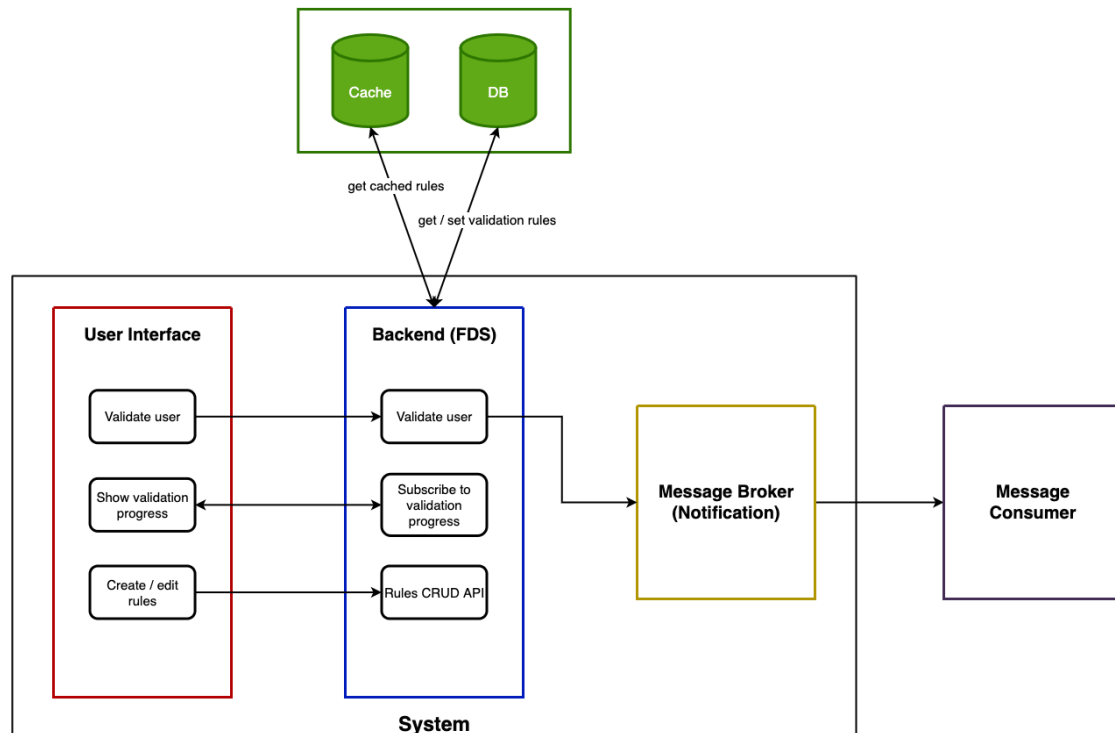


Figure 4.2.: Software architecture diagram

In a real world production environment, the user interface might need to be separated into several independent applications. A dedicated app to manage validation rules should be reachable only for internal employees (such as a developer from the company) while a customer facing UI that contains a registration form could also trigger a validation process directly after a new registration. An additional UI to display the progress of the currently running validation processes could also be built specifically for customer service agents, so that a fast reaction on certain suspicious customers can be done. For this project, all the use cases mentioned above will be implemented and combined into a single web application.

The fraud detection service (*backend, FDS*) is the core engine of the system where validation processes would be run. The FDS is responsible for all CRUD operations regarding the validation rules. User should be able to create, read, update and delete validation rules via an HTTP request. A detailed explanation on validation rules will

#### 4. Conception and Design

be discussed in subsection 4.4.2. A database connection should be established on the FDS to persist the validation rules. An optional connection to a cache memory could also be established to enable a faster access to the data needed.

The core functionality of the FDS is to run validation process of a customer by evaluating a collection of validation rules in relation to a given customer data. The execution of the validation process could be scheduled via a single HTTP request that contains the customer data on its request payload<sup>2</sup>. A validation process is run asynchronously, the FDS will not return the result of the validation directly as a response to the HTTP request. This is intended to prevent a slow response time of the FDS.

Clients could then subscribe to the latest progress of a validation process by accessing an additional endpoint provided by the FDS. A subscription mechanism will be implemented to prevent the need of a request polling on the client side, either by using the WebSocket protocol<sup>3</sup> or something similar.

After a validation process is completed, the FDS should return the result of a validation and further actions should be handled by external services out of the system's scope. This separation of concern is intended to decouple the execution of a validation process and the processing of its result. As there might be several implications on what a validation result might mean, the validation result will be distributed across multiple clients. To achieve this functionality, the Observer [4, pp. 293-303] design pattern will be implemented, and a messaging system is needed to act as a bridge between the message producer and its consumers. In this specific architecture, the FDS will act as a message producer, producing a message containing the validation result to the message broker whenever a validation process is done and the external services will act as message consumers, by consuming a message queue created by the message broker and running actions on certain cases independently.

### 4.3. Technologies

The software architecture determines not only the structure of the software, but it also helps in defining which type of technologies might be needed to build the system as efficiently as possible. Different technologies have their own advantages and disadvantages, and the goal of this phase is not to find the best technology or the best programming language, but rather to find the most suitable set of technologies given the priorities of the project and preferences of the writer. From the software architecture diagram listed on Figure 4.2, the technologies to be used on the following components should be defined:

- User interface (web application)
- FDS (server-side application)
- Message broker / notification system

---

<sup>2</sup>A request payload refers to data sent by a client to the server during an HTTP request, usually attached to the request body[12, section "4.3 Message Body"]

<sup>3</sup>In [11], Fette and Melnikov introduced the WebSocket protocol as a way to establish a two-way communication between a browser-based client and a remote host without relying on opening multiple HTTP connections.

## 4. Conception and Design

- Database and caching memory

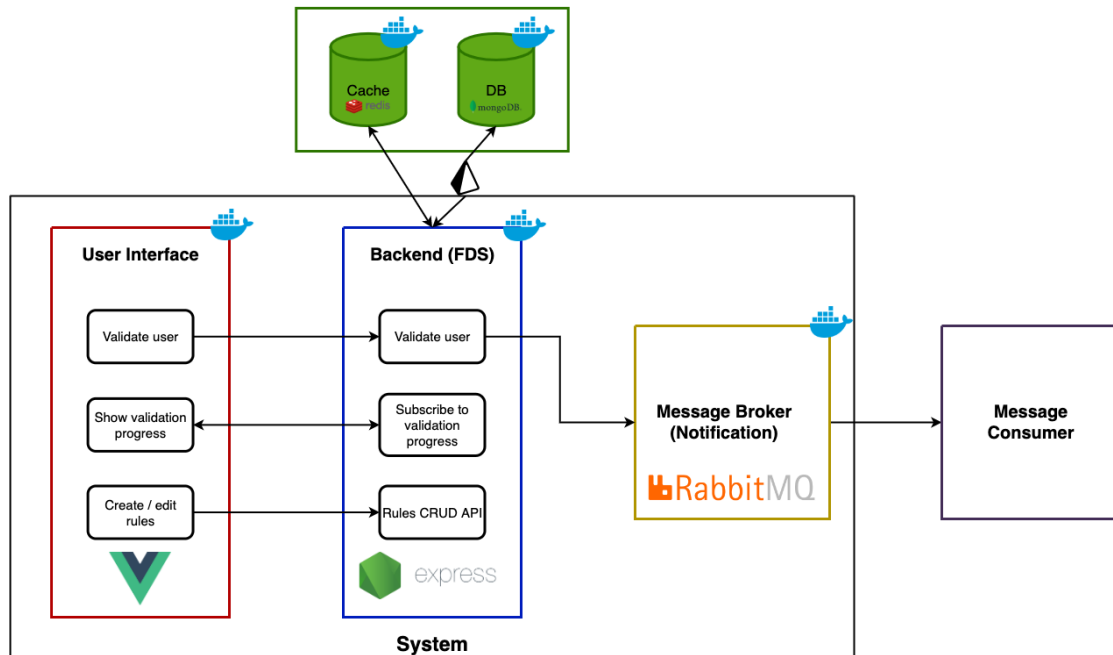


Figure 4.3.: Software architecture diagram with technologies used

The previous software architecture diagram is therefore extended with additional logos of the technology used for each component of the system. All internal components of the system should be run as a Docker<sup>4</sup> container. Running the applications as a Docker container means that each application is started and run in isolation, ensuring portability to other operating systems. The database and caching memory will also be run as a Docker container, to avoid the need of installing the dependencies needed and to enable the possibility to start all the components of the system using a single command with Docker Compose<sup>5</sup>.

### 4.3.1. User Interface

The technology used to build the user interface is VueJS (3. Version, also known as Vue3)<sup>6</sup>, a JavaScript framework built on top of HTML, CSS and JavaScript for building a reactive user interfaces using a component-based programming paradigm. To ensure type safety, the user interface is built with TypeScript<sup>7</sup>, rather than plain JavaScript, which is also supported by Vue3.

<sup>4</sup>Docker is an open source software used to containerize applications in a package with its dependencies and operating system, making it runnable in any environment. Homepage: <https://www.docker.com/>

<sup>5</sup>Docker Compose is an open source tool for running multiple Docker containers. GitHub repository: <https://github.com/docker/compose>

<sup>6</sup>Vue3 is an open source JavaScript framework to build user interfaces. GitHub repository: <https://github.com/vuejs/core>

<sup>7</sup>TypeScript is an open source programming language built by Microsoft on top of JavaScript by adding additional optional static typing. A TypeScript program will be compiled to a plain JavaScript program, before being executed in environment such as browser or NodeJS environment. GitHub repository: <https://github.com/microsoft/TypeScript>



## 4. Conception and Design

### 4.3.2. FDS

The technology chosen to build the FDS is Node.JS<sup>8</sup>. Node.JS is chosen not only because the writer is familiar with it, but also the event loop architecture of Node.JS enables the possibility to perform non-blocking I/O operations asynchronously. Each validation process will be an asynchronous process, which wouldn't block the main thread of the application. To ensure type safety, TypeScript is also used here rather than plain JavaScript. Express.JS<sup>9</sup> is the web framework of choice to build the FDS. Express.JS provides a simple and declarative API to build a web application with ease and speed. An object-relational mapping tool (ORM) is used in this application to provide an easier access to the database, and additionally to keep the database schema in sync between the database server and the FDS application. The ORM of choice for the application is Prisma<sup>10</sup>, as it provides a straightforward integration with TypeScript, generating TypeScript types automatically from the database schema.

### 4.3.3. Message Broker / Notification System

A reliable message broker is needed to make sure that all validation result actually reaches the consumers. The technology chosen for this component is RabbitMQ<sup>11</sup>, as it is not only reliable, but also has an easy guide to set up as well as a big collection of client libraries for multiple programming languages.

### 4.3.4. Database and Caching Memory

A database is needed to store data regarding validation rules. Each database system has their own use cases and weaknesses. For this particular project, MongoDB<sup>12</sup> will be used as the database system of choice. Redis<sup>13</sup> is chosen as the technology of choice for the caching memory because of its simple API and reliability.

## 4.4. Software Design

The system was implemented using the Model-View-Controller (MVC) programming approach. The system does not strictly adhere to the MVC pattern, but uses it as a guideline to categorize the components of the system and its functionalities. Krasner

---

<sup>8</sup>Node.JS is an open source JavaScript runtime environment that runs on Google's V8 engine, enabling JavaScript programs to be run out of the browser environment. GitHub repository: <https://github.com/nodejs/node>

<sup>9</sup>Express JS is an open source web application framework for Node.JS. GitHub repository: <https://github.com/expressjs/expressjs.com>

<sup>10</sup>Prisma is an open source ORM for Node.JS and TypeScript. GitHub repository: <https://github.com/prisma/prisma>

<sup>11</sup>RabbitMQ is a messaging broker, enabling the distribution of messages across multiple clients. RabbitMQ homepage: <https://www.rabbitmq.com/>

<sup>12</sup>MongoDB is a source-available NoSQL database developed by MongoDB Inc. MongoDB homepage: <https://www.mongodb.com/>

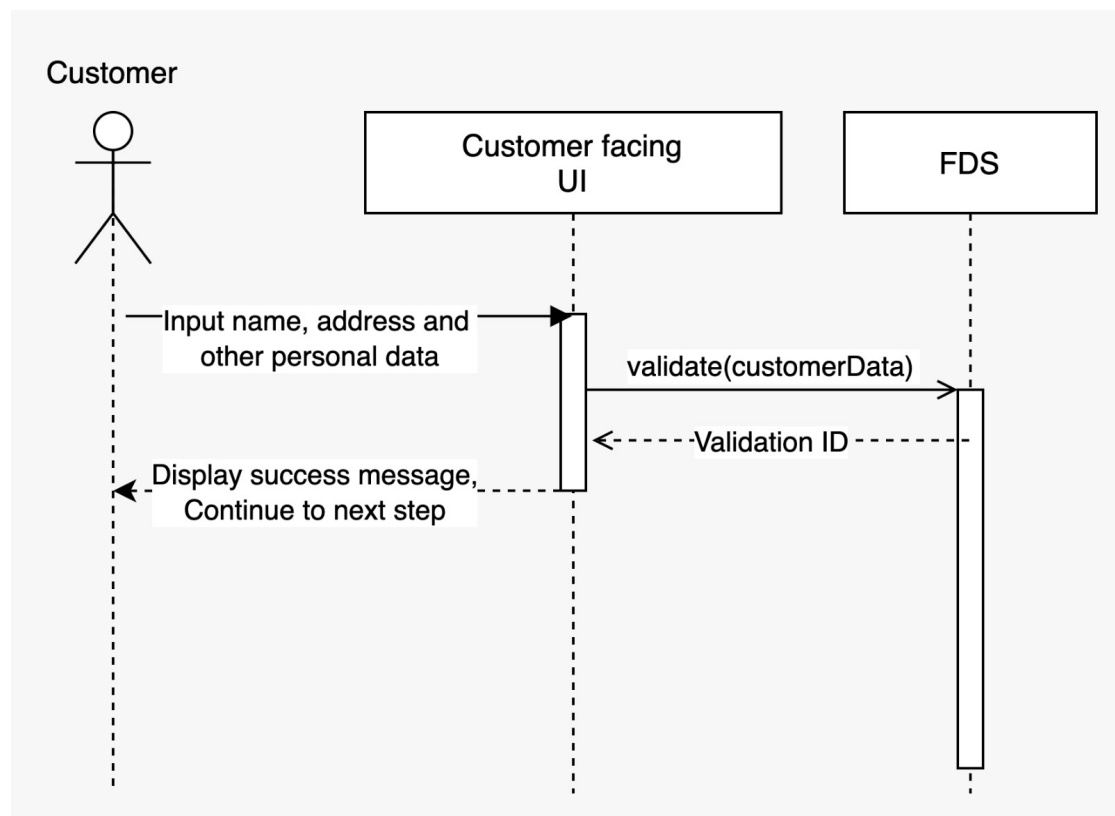
<sup>13</sup>Redis is an open-source in-memory data structure store. GitHub repository: <https://github.com/redis/redis>

and Pope [7] discussed the benefit of using the MVC pattern to provide modularity by isolating functional components of the system, making it easier to design and modify.

### 4.4.1. Controller

Krasner and Pope defined an application's controller in [7] as an interface to associate the components of the system (*model and view*) and incoming events (*such as event coming from input devices*). In other words, the controller component is responsible in defining the flow or sequence of a system based on an incoming event, routing commands to the appropriate model and updating the view in the process. In this subsection, an analysis of the use cases listed on **TODO: ref to use cases** will be done, and consequentially a sequence of operations will be defined for each specific use case. An additional sequence will also be defined as a way complete the system and fulfill the requirements defined.

#### Customer Validation on a Registration Event



**Figure 4.4.:** System sequence diagram for a customer validation when a new customer is registered

A system sequence can be defined by analyzing the following use case:

“As a stakeholder, I want to verify customer, so that the company can have more confidence that the existing user base is trustworthy”

#### 4. Conception and Design

One of the opportunity to do a verification process is during a new customer registration. Verifying a customer after each new registration might help the stakeholder to be more confident, that the user base is trustworthy and necessary actions can be taken as soon as possible to reduce the possible damage made in the future by fraudulent customers. The following sequence will be executed as a way to validate a customer directly after a new registration:

- A new customer inputs his or her personal data to a customer facing UI and clicks the "Register" button
- The customer facing UI makes an HTTP Post request to the FDS, containing the user's personal data on its request payload
- The FDS receives the HTTP request, and schedules a new validation process to be executed asynchronously
- The FDS responds to the HTTP request by returning a validation ID pointing to the scheduled validation process
- Customer facing UI shows a success message and continues registration to the next step while the validation process runs

##### Notification on Suspicious Cases

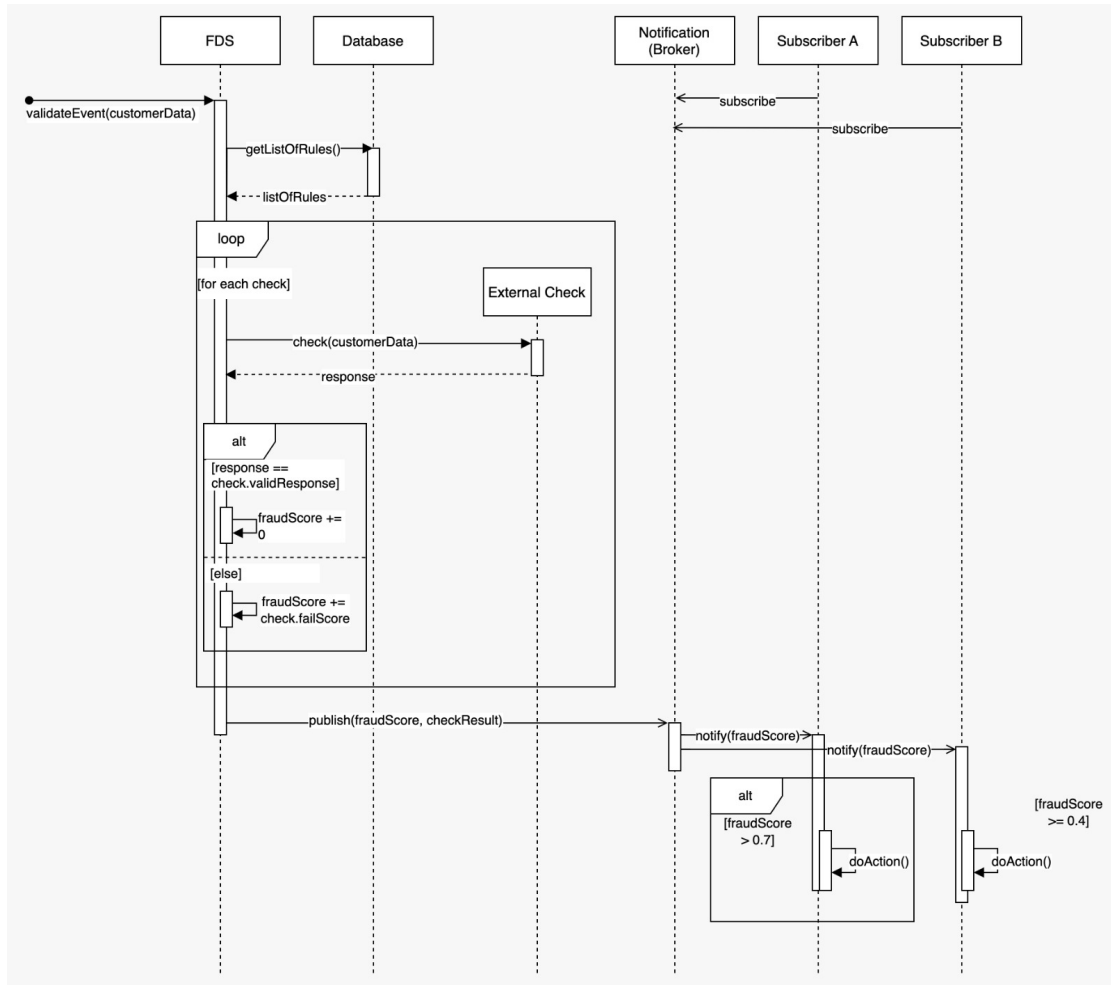
To fulfill the requirements listed on **TODO: Link Analysis**, a further examination of the following use case should be done:

"As an employee, I want to be notified when a user seems suspicious, so that I can do necessary actions accordingly"

The FDS runs a rule evaluation by making an HTTP request to an external URL and comparing the HTTP response to the conditions listed on the validation rule. As working with external systems is unpredictable and there is no guarantee that the external system has a fast response time, a validation process is run asynchronously, meaning that the FDS would not return the validation result with a resulting fraud score directly to the client when a validation process is scheduled. At the end of a validation process, the concerned parties might need some kind of notification on certain cases, to make sure actions required can be made as soon as possible. The following sequence illustrates the sequence of activities done by the system to validate a certain customer and sending a notification on its completion:

- The FDS receives an HTTP request to schedule a validation process and responds by returning the ID of the validation process
- FDS retrieves a list of validation rules from the database
- FDS begins to initiate a validation process by setting the fraud score to 0 and looping through the list of validation rules for evaluation
- A validation rule will be evaluated by making an HTTP request to the external endpoint defined by the validation rule and evaluating its response according to the condition specified
- If the response matches all the conditions specified by the validation rule, the rule evaluation will be considered as a success and the fraud score will be incremented

#### 4. Conception and Design



**Figure 4.5.:** System sequence diagram for notifications on suspicious cases

- with 0. Otherwise, the rule evaluation will be considered as a failure and the fraud score will be incremented by the *fail score* specified by the validation rule
- After the evaluation of all validation rules retrieved from the database is completed, the FDS publishes the validation result to an exchange hosted by the message broker
- The message consumers consume the message from the exchange and react accordingly<sup>14</sup>

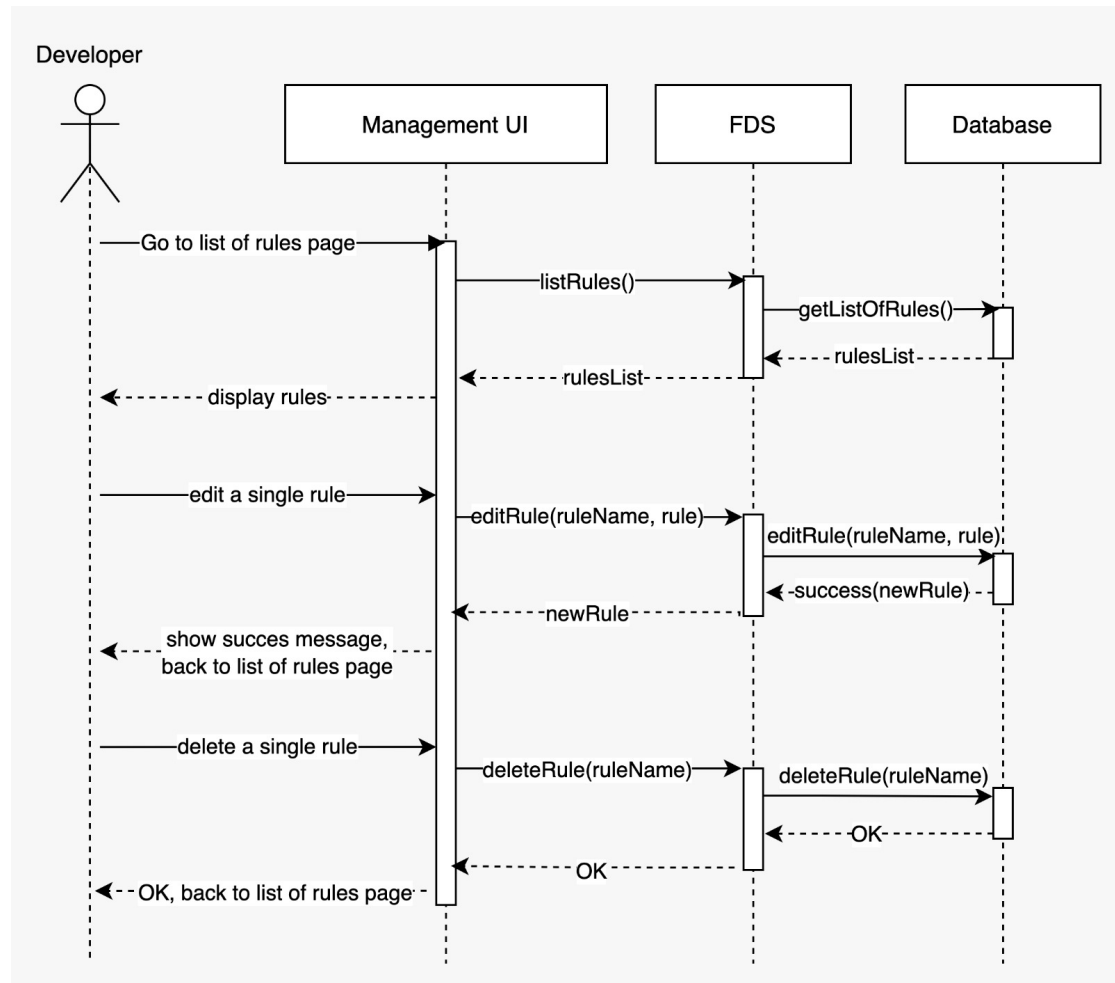
#### Managing Validation Rules

Another sequence can also be defined as a result of an analysis of the following use case:

“As an employee, I want to manage my own rule to validate users, so that I can use my expertise to find suspicious customers as efficiently as possible without the communication overhead with other teams”

<sup>14</sup>For example: sending an email notification if the fraud score exceeds 0.7.

#### 4. Conception and Design



**Figure 4.6.:** System sequence diagram for validation rules management

A possibility for each team to manage their own validation rules without being dependent to other teams is needed. By reducing the impediment in the process (having to consult other teams, communication overhead), every team can focus on generating validation rules that reflect a fraudulent customer as efficiently as possible, according to their own domain knowledge and expertise. The following sequence illustrates the functionality of managing validation rules:

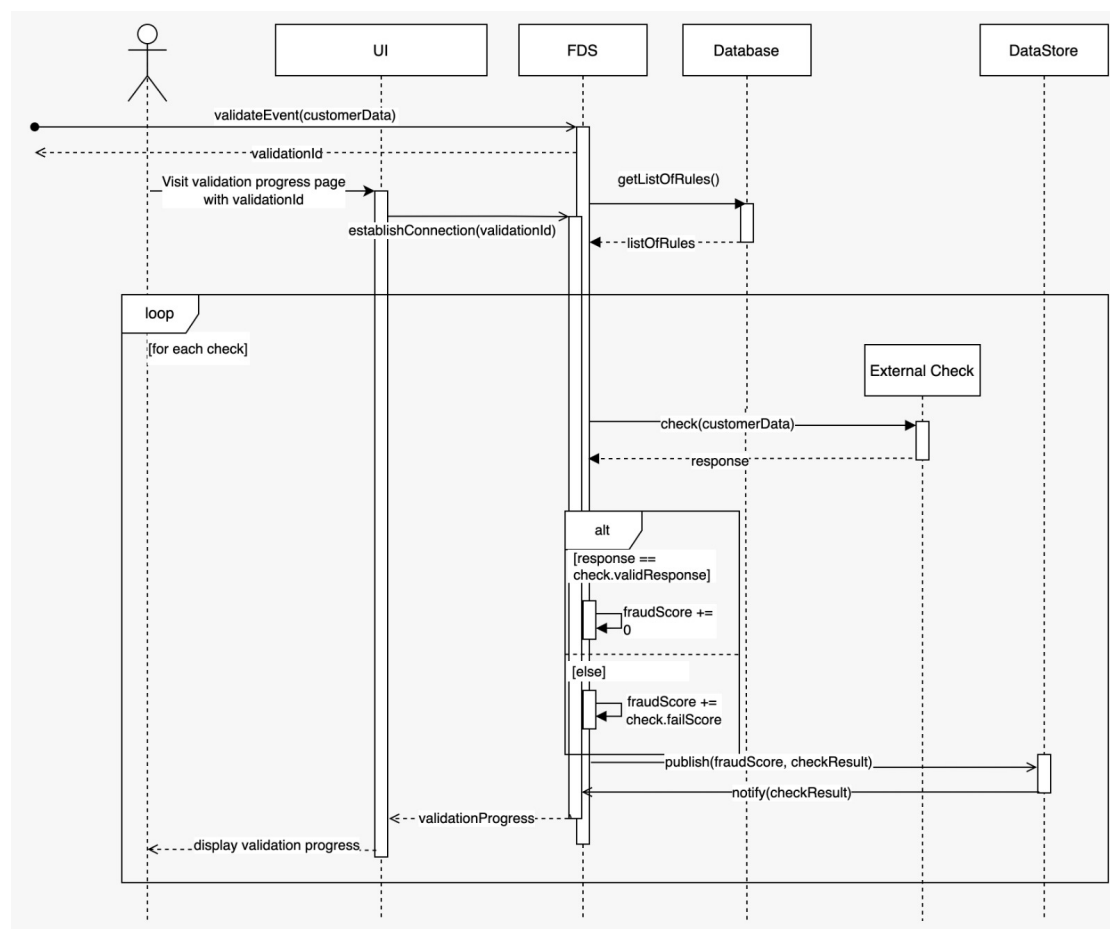
- A user (e.g. Developer) can access the management UI and go to the page that displays a list of available validation rules
- The FDS retrieves a list of validation rules from the database
- User can click on a single rule and edit the rule
- The management UI makes an HTTP PUT<sup>15</sup> request to the database to edit an existing rule
- The FDS receives the HTTP request, modifies the rule on the database and returns the edited rule as a response

<sup>15</sup>In [12, "9.6 PUT"], HTTP PUT method is described as a method to store or modify an entity, defined by the Request-URI

#### 4. Conception and Design

- The management UI displays a success message and redirects user back to the list of rules page
- User can click on a single rule and delete the rule
- The management UI makes an HTTP DELETE<sup>16</sup> request to the database to delete an existing rule
- The FDS receives the HTTP request and delete the rule on the database, returning a 204<sup>17</sup> status code as an identifier of a successful operation
- The management UI displays a success message and redirects user back to the list of rules page

#### Validation Real-Time Progress



**Figure 4.7.:** System sequence diagram for validation rules management

Even though the user should receive a notification on certain cases, there might be times when a user wants to intentionally monitor the progress of a validation process.

<sup>16</sup>In [12, “9.7 DELETE”], HTTP DELETE method is described as a method to delete a resource on the host server, pointed by the Request-URI

<sup>17</sup>In [12, “10.2.5 204 No Content”], the 204 status code should be used if the server fulfilled the request, but no data should be returned by the HTTP response

#### 4. Conception and Design

To achieve such functionality, the user interface should establish a connection to the FDS, and receive notification whenever there is an update on the validation result. The sequence of such functionality will be as follows:

- The FDS receives an HTTP request to schedule a validation process and responds by returning the ID of the validation process
- FDS retrieves a list of validation rules from the database and initiate the validation process
- A user visits the validation progress page with the returned validation ID
- The user interface establishes a connection with the FDS subscription endpoint
- After each rule evaluation, the FDS stores the latest validation result to a data store<sup>18</sup>
- Every time the data store receives a new data, the user interface will get a notification and the latest result from the FDS subscription endpoint
- The user interface updates the view containing the latest validation result

##### 4.4.2. Model

As mentioned by Krasner and Pope [7], an application's model is a domain specific simulation or implementation of a structure. The model component of an MVC application contains business logic and manages the state of an application as well as its storage. The essential models of the system can be defined by revisiting the sequences listed on subsection 4.4.1 and identifying the important structures needed to fulfill the requirements needed.

##### Validation Rule

A validation rule is a structure of information used in a validation process by supplying the FDS the necessary information to make an HTTP request to an external endpoint and evaluating its response, affecting the overall fraud score of a validation process through its evaluation result. Through a detailed analysis of the sequence illustrated on Figure 4.5, it is essential that the *validation rule* model contains the following attributes:

- A URL pointing to an external endpoint
- A list of conditions to evaluate the response returned by the external endpoint
- A unique identifier
- A fail score, which determine the severity of the rule if the evaluation failed

It might also be necessary to have an identifier in the validation rule to skip its evaluation in certain cases. Other than that, as the FDS would make an HTTP request to an external endpoint based on the information listed on a validation rule, the following attributes are needed to provide a more robust configuration:

- HTTP method to be used to make the request

---

<sup>18</sup>A data store in this context can be a caching memory or a simple class to store some temporary information

#### 4. Conception and Design

- Request header<sup>19</sup>
- Request body

As the FDS interacts with external endpoints, there is no guarantee that the external endpoint will always be accessible. An additional attribute to specify and configure a retry strategy in such cases can be useful. However, a retry strategy can be really specific to its implementation and therefore will be discussed in **TODO: Add retry strategy implementation**.

An additional *priority* attribute is also provided to enable the possibility to run rule validations according to its priority order.

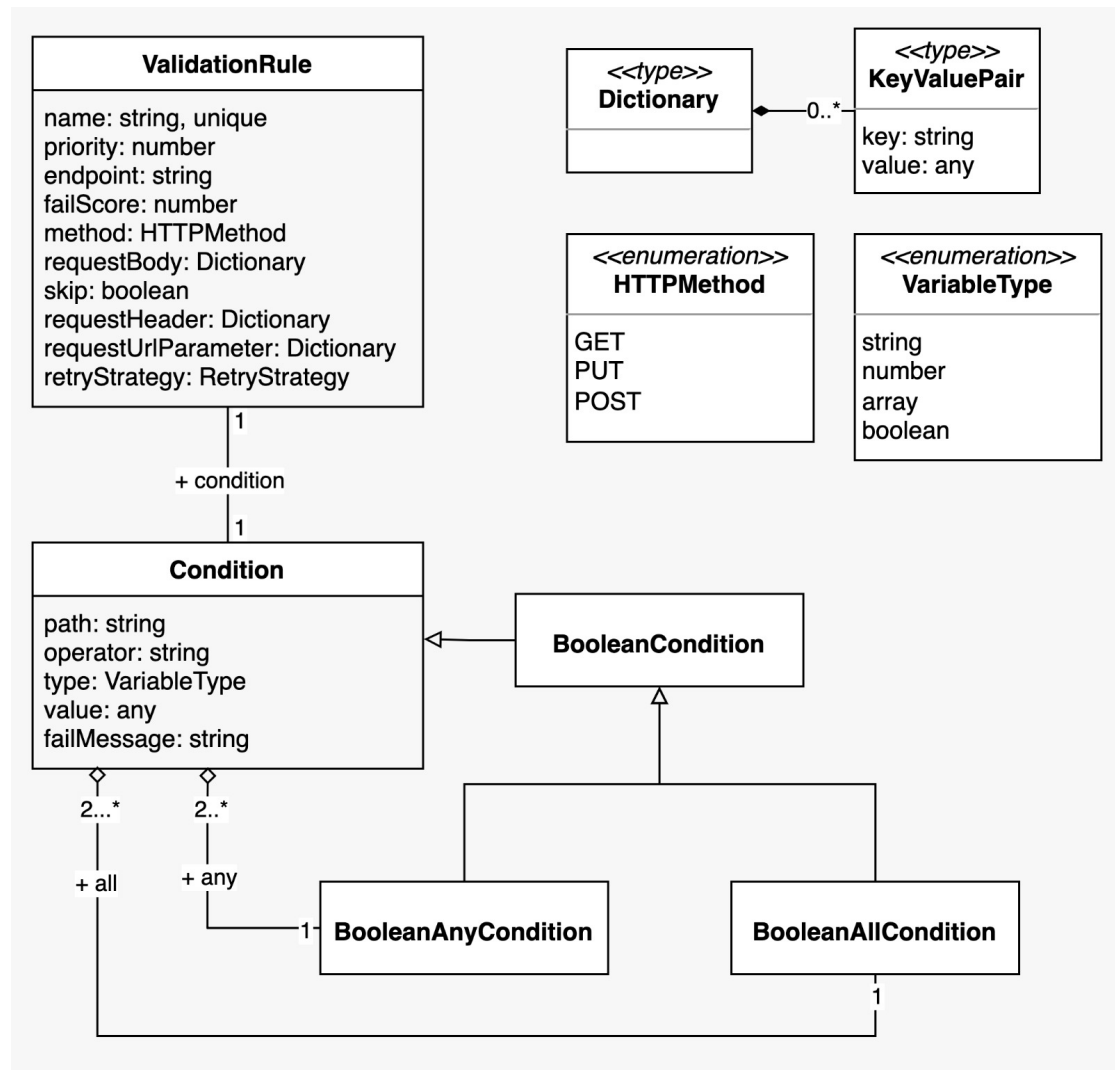


Figure 4.8.: UML diagram of the validation rule model

The *condition* attribute plays an important role for a validation rule, as it defines how the response returned by the external endpoint should be structure to pass a rule

<sup>19</sup>In [12, "5.3 Request Header Fields"]: request header is defined as additional information passed by the client to the host server about the particular request or about the client.



#### 4. Conception and Design

evaluation. It is intended to design the condition attribute to be robust and configurable. The *path* of a condition defines a JSONPath[3] expression to access information available of the current validation scope, such as customer information or response returned by the external endpoint. The *type* attribute of a condition determines the type of the attribute accessed by the *path* attribute. The *type* attribute determines which type of operators are available to use<sup>20</sup>. The *operator* attribute refers to a name of operator to be used to evaluate the condition (for example: "eq", "incl"). The available operator names are predefined and restricted to the condition's type attribute. More information regarding operators will be discussed in **TODO: Add operator implementation**. The *failMessage* attribute of a condition refers to a message that is going to be appended to the validation result's *messages* attribute after a validation is completed.

```
1 {
2   "name": "Example",
3   "skip": false,
4   "priority": 2,
5   "endpoint": "http://localhost:8000/validate",
6   "method": "GET",
7   "failScore": 0.7,
8   "condition": {
9     "path": "$.response.statusCode",
10    "type": "number",
11    "operator": "eq",
12    "value": 200,
13    "failMessage": "Status code doesn't equal to 200"
14  },
15  "requestUrlParameter": {},
16  "requestBody": {},
17  "requestHeader": {}
18 }
```

**Listing 4.1:** Validation rule example (JSON)

A validation rule might contain more than a single condition to pass an evaluation. In such cases, the user need to define whether how to determine whether an evaluation should pass: either pass an evaluation if **ALL** the conditions is true or pass an evaluation if **AT LEAST ONE (ANY)** of the conditions is true. This can be achieved by having the *condition* attribute as an object with a single attribute, either *all* or *any* and an array of conditions as the attribute's value.

```
1 {
2   "condition": {
3     "all": [
4       {
```

<sup>20</sup>For example: a condition with *type* "string" cannot use the "incl" operator, because the "incl" operator is only available for "array" type

#### 4. Conception and Design

```
5      "path": "$.response.statusCode",
6      "type": "number",
7      "operator": "eq",
8      "value": 200,
9      "failMessage": "Status code doesn't equal to 200"
10    },
11    {
12      "path": "$.response.body.valid_address",
13      "type": "boolean",
14      "operator": "eq",
15      "value": false,
16      "failMessage": "Address is invalid"
17    }
18  ]
19 }
20 }
```

**Listing 4.2:** Validation rule *condition* attribute example with ALL condition (JSON)

```
1  {
2    "condition": {
3      "any": [
4        {
5          "path": "$.response.statusCode",
6          "type": "number",
7          "operator": "eq",
8          "value": 200,
9          "failMessage": "Status code doesn't equal to 200"
10        },
11        {
12          "path": "$.response.body.valid_address",
13          "type": "boolean",
14          "operator": "eq",
15          "value": false,
16          "failMessage": "Address is invalid"
17        }
18      ]
19    }
20  }
```

**Listing 4.3:** Validation rule *condition* attribute example with ANY condition (JSON)

#### Validation Result

A validation result is the result of a validation process. A validation result contains a resulting fraud score, which is the probability of a certain customer being a fraud.

#### 4. Conception and Design

The algorithm to calculate the fraud score will be discussed as part of the **TODO: Link implementation**. By evaluating the sequences listed on Figure 4.4 and Figure 4.5, the following attributes are needed:

- A unique validation ID
- A fraud score

Furthermore, information regarding the total checks, runned checks, and additional information that contains the start and end date of the validation process as well as the customer information used for the validation are essential. The customer information is generic, and the system should be able to do a validation process regardless of its structure. The validation result should also return a list of validation rule names, whose evaluations are skipped due to its *skip* attribute being set to *true*.

Even though the resulting fraud score determines the probability of a customer being a fraud, it is also important to further analyze the actual evaluation result of each validation rule. For example, a certain action can be run if the evaluation of a specific rule failed or the information regarding the rule evaluations can also be used to display the current progress of a validation process (implementation of this specific functionality will be discussed more in **TODO: cite to implementation**).

To provide such information on a validation result, the *events* attribute will be introduced, which refers to rule evaluation events within a validation process. A rule evaluation event should contain the following attributes:

- Unique identifier of the event (name of the rule being evaluated)
- Status of the event (not started, failed, passed or running)
- If available, start date of a rule evaluation event
- If available, end date of a rule evaluation event
- A list of messages, containing error messages of an evaluation event

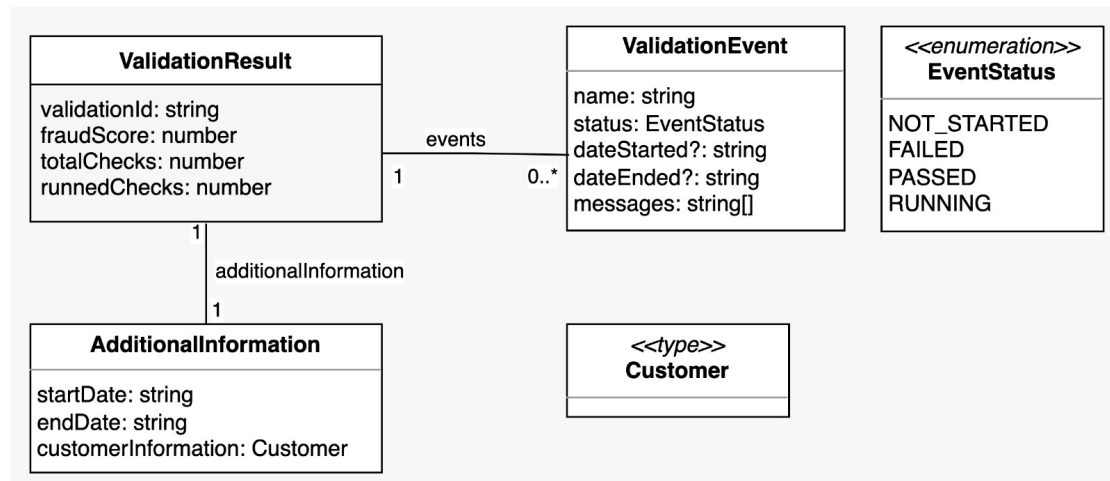


Figure 4.9.: UML diagram of the validation result model

#### 4. Conception and Design

```
1 {
2   "validationId": "3112dc4a-45f5-41b8-883a-715dcbe9a490",
3   "totalChecks": 3,
4   "runnedChecks": 2,
5   "skippedChecks": [
6     "Skip rule",
7   ],
8   "additionalInfo": {
9     "startDate": "2022-06-12T09:16:24.618Z",
10    "customerInformation": {
11      "firstName": "Scooby",
12      "lastName": "Doo",
13      "address": {
14        "streetName": "Suite 5000 185 Berry St",
15        "city": "San Fransisco",
16        "state": "CA",
17        "country": "United States",
18        "postalCode": 94107
19      },
20      "email": "scooby-doo@fraud.co",
21      "phoneNumber": "123131123"
22    }
23  },
24  "events": [
25    {
26      "name": "User's email domain is not blacklisted",
27      "status": "PASSED",
28      "dateStarted": "2022-06-12T09:16:34.694Z",
29      "dateEnded": "2022-06-12T09:16:39.725Z",
30      "messages": []
31    },
32    {
33      "name": "User's email is not blacklisted",
34      "status": "FAILED",
35      "dateStarted": "2022-06-12T09:16:39.725Z",
36      "dateEnded": "2022-06-12T09:16:44.756Z",
37      "messages": [
38        "User's email is blacklisted!"
39      ]
40    }
41  ],
42  "fraudScore": 0.425
43 }
```

**Listing 4.4:** Validation result example (JSON)

### 4.4.3. View

In [7], Krasner and Pope described an application's view as the graphical representation of an application's model. Several mock-ups are made to better visualize how the user interface should be structured using a UI design tool called Figma.

#### Rule Management Form

To facilitate the validation rule management functionality visualized in Figure 4.6, a page containing a form to create, edit, delete and read a validation rule will be created. The rule management form is intended to be used by internal employee, preferably with technical background<sup>21</sup> to manage a validation rule that will be used to validate a customer.

The page should represent every attribute of a validation rule and gives the user the ability to modify the attribute if necessary. The form will be used both for rule creation and rule modification. For a rule creation, the form fields will be left blank. For a rule modification, the form fields will be filled with the rule's current data.

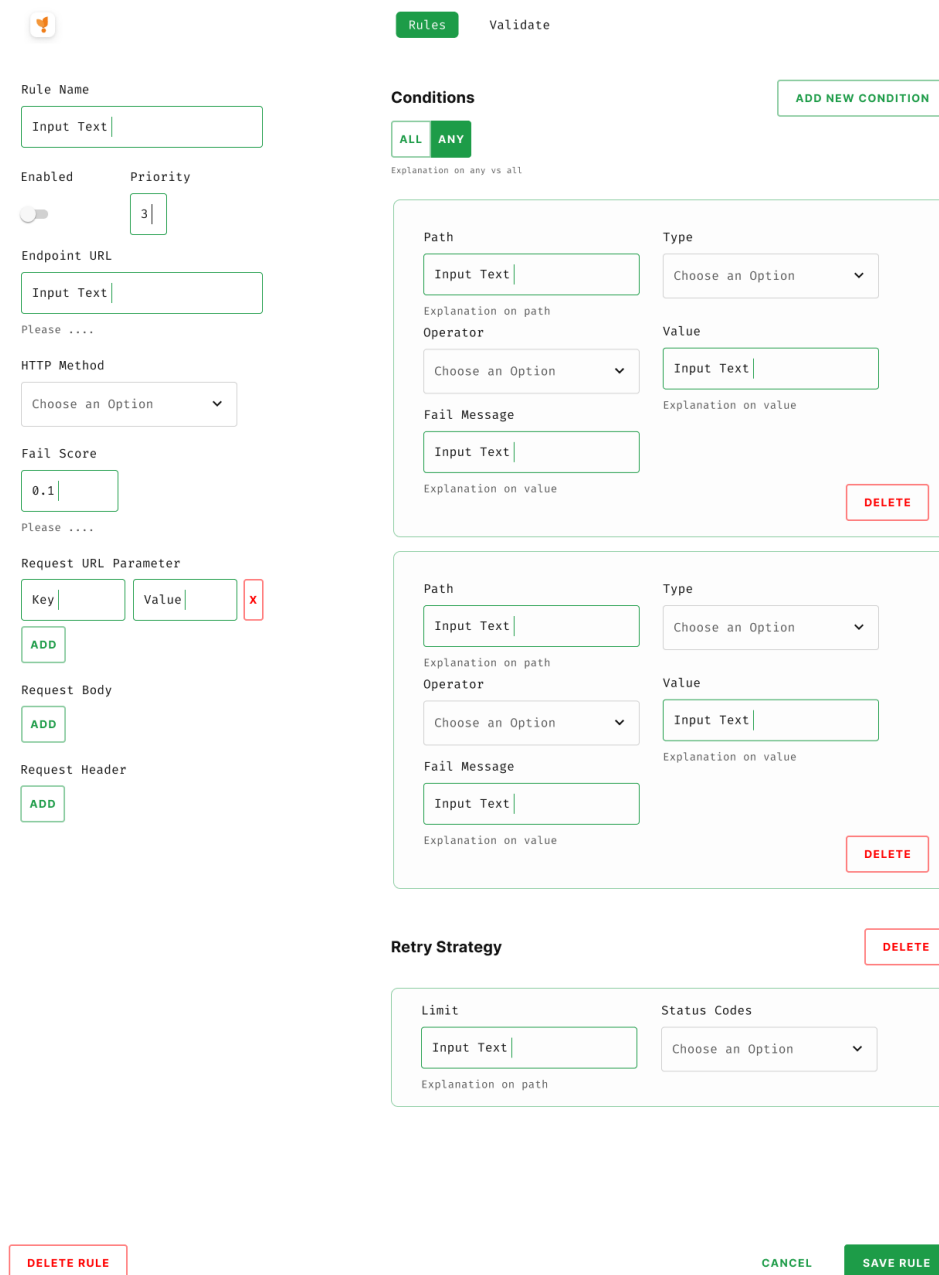
The RULE NAME field is used to display or enter a unique name of the validation rule. If the form is used to modify an existing rule, the field should be disabled, as a validation rule's name cannot be modified.

The CONDITIONS section can be used to add one or more condition to a validation rule. The form fields of each condition includes a dedicated input field for each attribute of a condition, as described in subsubsection 4.4.2. The TYPE and OPERATOR form fields are a selectable field, meaning the user has to select one out of several choices provided. This is intended to restrict input from the user, preventing an invalid condition being submitted to the FDS<sup>22</sup>. User can also delete a condition if necessary by clicking the DELETE button available on each condition segment. If more than one condition is present, a selectable button will be displayed to select whether the "any" or "all" condition will be used.

As the *retryStrategy* attribute of a validation rule is not required, it is possible to delete an existing retry strategy, by clicking on the DELETE button available on the RETRY STRATEGY section of the form. If no retry strategy is present, a button to add a new retry strategy and to display the LIMIT and STATUS CODES fields will be displayed.

According to the model of a validation rule, *requestBody*, *requestHeader* and *requestUrlParameter* should be a dictionary that could contain as many entries as possible. To mimic this functionality as a form field, the REQUEST BODY, REQUEST HEADER and REQUEST URL PARAMETER fields are a dynamic input field. A dynamic input field enables the user to add a new key-value pair to the dictionary by clicking on the ADD button and inputting the values to the corresponding input fields. To delete an entry of a dictionary, a delete button is provided next to each key-value fields.

## 4. Conception and Design



The mockup shows a 'Rules' management interface. On the left, a sidebar contains fields for 'Rule Name' (Input Text), 'Enabled' (toggle), 'Priority' (3), 'Endpoint URL' (Input Text), 'HTTP Method' (Choose an Option), 'Fail Score' (0.1), and 'Request URL Parameter' (Key/Value with an 'X' icon). Below these are 'Request Body' and 'Request Header' sections, each with an 'ADD' button. At the bottom left is a 'DELETE RULE' button. The main area has a 'Validate' tab and an 'ADD NEW CONDITION' button. Under 'Conditions', there are two identical condition blocks. Each block has fields for 'Path' (Input Text), 'Type' (Choose an Option), 'Operator' (Choose an Option), 'Value' (Input Text), and 'Fail Message' (Input Text). Each block also has an 'Explanation on path' and 'Explanation on value' label, and a 'DELETE' button. Below the conditions is a 'Retry Strategy' section with a 'Limit' (Input Text), 'Status Codes' (Choose an Option), and an 'Explanation on path' label, along with a 'DELETE' button. At the bottom right are 'CANCEL' and 'SAVE RULE' buttons.

Figure 4.10.: Mock up of the rule management form page

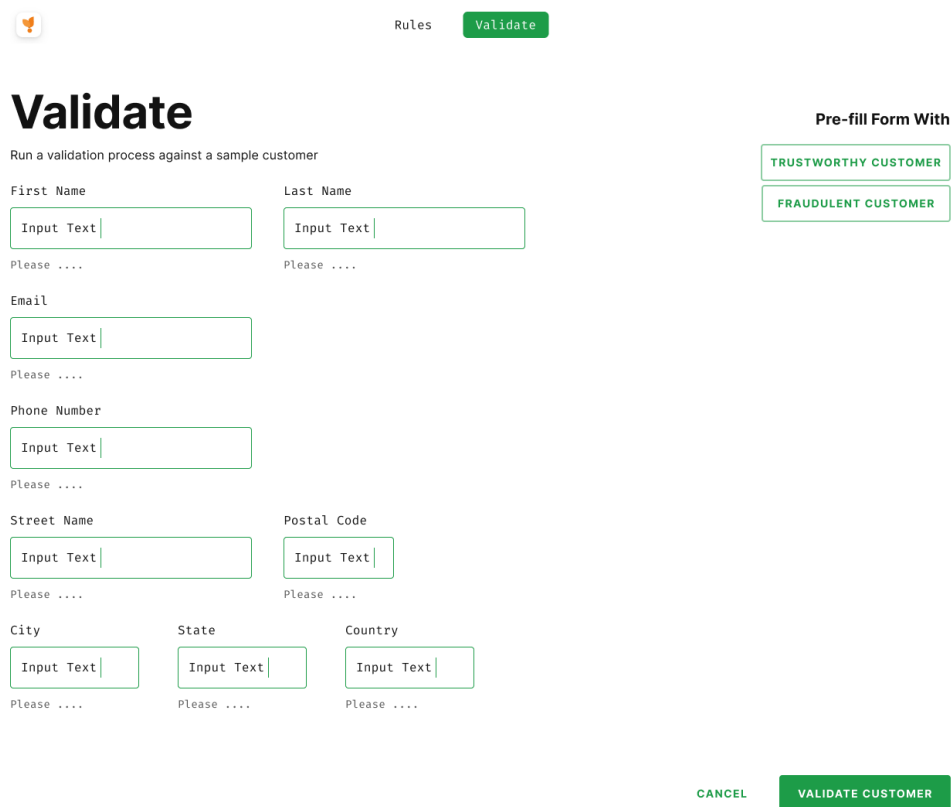
### Validation Form

A sample registration form is also created to give the user a possibility to run a validation process on a certain customer. The validation form is intended to be used by end customer, as a mean to register his-/herself into the system. Internal employees

<sup>21</sup>An understanding on how HTTP works is a prerequisite to use the form

<sup>22</sup>For example, on *type* field, user can only choose on of the following: (number, string, array, boolean)

## 4. Conception and Design



The mockup shows a web interface for a validation process. At the top left is a small orange bird icon. To its right are the labels 'Rules' and a green 'Validate' button. Below this is a large 'Validate' heading, followed by the instruction 'Run a validation process against a sample customer'. The form consists of several input fields: 'First Name' and 'Last Name' (each with an 'Input Text' box and a 'Please ...' label), 'Email' (with an 'Input Text' box and a 'Please ...' label), 'Phone Number' (with an 'Input Text' box and a 'Please ...' label), 'Street Name' and 'Postal Code' (each with an 'Input Text' box and a 'Please ...' label'), 'City', 'State', and 'Country' (each with an 'Input Text' box and a 'Please ...' label'). To the right of the form, under the heading 'Pre-fill Form With', are two buttons: 'TRUSTWORTHY CUSTOMER' and 'FRAUDULENT CUSTOMER'. At the bottom right of the form are two buttons: 'CANCEL' and 'VALIDATE CUSTOMER'.

**Figure 4.11.:** *Mock up of the validation form page*

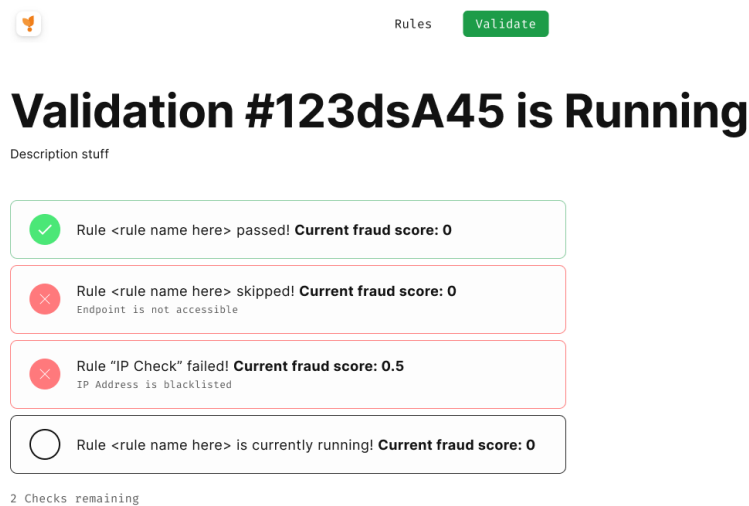
can also use the validation form to test the validation rules.

The page should represent a customer model by displaying every attribute of a customer in a form field (please refer to Figure A.1 for more information on the customer model). For demonstration purposes, it might be beneficial to have a list of sample customers, so that the user can run a validation on a certain set of customers quickly, without having to first fill out the form by him-/herself. To provide this functionality, a list of buttons, containing a description text of the sample customer will be displayed next to the validation form. Upon clicking on one of the buttons, the validation form will be filled with the sample customer's data and the user can directly click on the VALIDATE CUSTOMER button to begin the validation process.

#### 4. Conception and Design

##### Validation Progress

To provide a transparency on an asynchronous validation process, a page that displays the current progress of a validation process in real time might be beneficial. This page is intended for demonstration purposes, but can also be beneficial for security agents to keep track of the validation processes run by the FDS.



**Figure 4.12.:** Mock up of the validation progress page

The page displays the current progress of a certain validation in real time. It represents the *events* attribute of a validation result in a timeline, displaying the events in a list ordered by its *dateEnded* attribute. The page gives the user information regarding the evaluation result of each validation rule (success, failure or in progress), the current fraud score and the names of validation rules that are skipped. If present, the messages of an event should also be displayed.



## 5. Implementation

[Beschreibung der Implementierung<sup>1</sup> auf Basis des Entwurfs und der Methodologie / der geplanten Vorgehensweise zur Problemlösung im Kontext der Anforderungen. Hier ist Raum für Listings, wie z.B. das nun Folgende:

```
1  const helloWorld = "Hello, world!"
2  console.log(helloWorld)
```

**Listing 5.1:** *Ein Beispiel: Hello World (JavaScript)*

Umfangreicher Quell-Code sollte in den Anhang ausgelagert werden.]

### 5.1. Model

### 5.2. View

### 5.3. Controller

Optionals:

- Architecture -> (can be in controller)
- Techs

---

<sup>1</sup>Beachten Sie bei der Implementierung und deren Dokumentation bitte Clean Code Empfehlungen (vgl. hierzu z.B. [10]).

## 6. Test

[Beschreibung, wie Sie auf Basis des geplanten Testvorgehens was mit welchen Kriterien und Technologien getestet haben]

## 7. Demonstration and Evaluation

[Beschreibung der Ergebnisse aus allen voran gegangenen Kapiteln sowie der zuvor generierten Ergebnisartefakte mit Bewertung, wie diese einzuordnen sind]

### **7.1. Ausblick**

[Beschreibung und Begründung potenzieller zukünftiger Folgeaktivitäten im Zusammenhang mit Ihrer Arbeit (z.B. weitere Anforderungen, Theoriebildung, ... )]

# Bibliography

- [1] Helmut Balzert, Marion Schröder, and Christian Schaefer. *Wissenschaftliches Arbeiten. Ethik, Inhalt & Form wiss. Arbeiten, Handwerkszeug, Quellen, Projektmanagement, Präsentation*. 2. Auflage. Herdecke, Witten: W3L, 2011. ISBN: 978-3-86834-034-1.
- [2] Norbert Franck and Joachim Stary. *Die Technik wissenschaftlichen Arbeitens: eine praktische Anleitung*. 17. Auflage. Paderborn: Schöningh, 2013. ISBN: 978-3-50697-027-5.
- [3] Jeff Friesen. "Extracting JSON Values with JsonPath". In: *Java XML and JSON: Document Processing for Java SE*. Berkeley, CA: Apress, 2019, pp. 299–322. ISBN: 978-1-4842-4330-5. DOI: 10.1007/978-1-4842-4330-5\_10. URL: [https://doi.org/10.1007/978-1-4842-4330-5\\_10](https://doi.org/10.1007/978-1-4842-4330-5_10).
- [4] Erich Gamma et al. *Design Patterns*. Addison-Wesley, 1995.
- [5] David Garlan. "Software architecture". In: *Proceedings of the conference on The future of Software engineering - ICSE '00* (2000). DOI: 10.1145/336512.336537.
- [6] ISO. *ISO/IEC 25010:2011*. Mar. 2011. URL: <https://www.iso.org/standard/35733.html>.
- [7] Glenn Krasner and Stephen Pope. "A cookbook for using the model-view controller user interface paradigm in Smalltalk-80". In: *Journal of Object-oriented Programming - JOOP* 1 (Jan. 1988).
- [8] Lorient. *Möpse und Menschen. Eine Art Biographie. Zurich*. In: faz.net. Online: [https://media0.faz.net/ppmedia/aktuell/feuilleton/1461387463/1.721778/format\\_top1\\_breit/die-steinlaus-trotzt-seit.jpg](https://media0.faz.net/ppmedia/aktuell/feuilleton/1461387463/1.721778/format_top1_breit/die-steinlaus-trotzt-seit.jpg); letzter Zugriff: 13 VI 19. 1983.
- [9] Lorient. *Steinlaus, Lorient Katalog, Diogenes Verlag, Zürich*. In: tagblatt.de. Online: <https://www.tagblatt.de/Bilder/Loriots-legendaere-Steinlaus-Lorient-Katalog-1993-2003-125217h.jpg>; letzter Zugriff: 14 VI 19. 1993, 2003.
- [10] Robert Martin. *Clean Code: A Handbook of Agile Software Craftsmanship*. 1st ed. Pearson, 2008.
- [11] Alexey Melnikov and Ian Fette. *The WebSocket Protocol*. RFC 6455. <http://www.rfc-editor.org/rfc/rfc6455.txt>. RFC Editor, 2011. URL: <http://www.rfc-editor.org/rfc/rfc6455.txt>.
- [12] Henrik Nielsen et al. *Hypertext Transfer Protocol – HTTP/1.1*. Tech. rep. 2616. June 1999. 176 pp. DOI: 10.17487/RFC2616. URL: <https://www.rfc-editor.org/info/rfc2616>.
- [13] Pschyrembel online. *Steinlaus*. Online: <https://www.pschyrembel.de/Steinlaus/KOLHT>; letzter Zugriff: 14 VI 19. 2016.

### *Bibliography*

- [14] Alan Jay Smith. “Cache Memories”. In: *ACM Computing Surveys* 14.3 (1982), pp. 473–530. doi: 10.1145/356887.356892.
- [15] Wikipedia. *Academic Use*. Online: [https://en.wikipedia.org/wiki/Wikipedia:Academic\\_use](https://en.wikipedia.org/wiki/Wikipedia:Academic_use); letzter Zugriff: 13 VI 19. 2019.

## 8. List of Abbreviations

## 9. Glossary



# A. Appendix

## A.1. Supplemental Figures

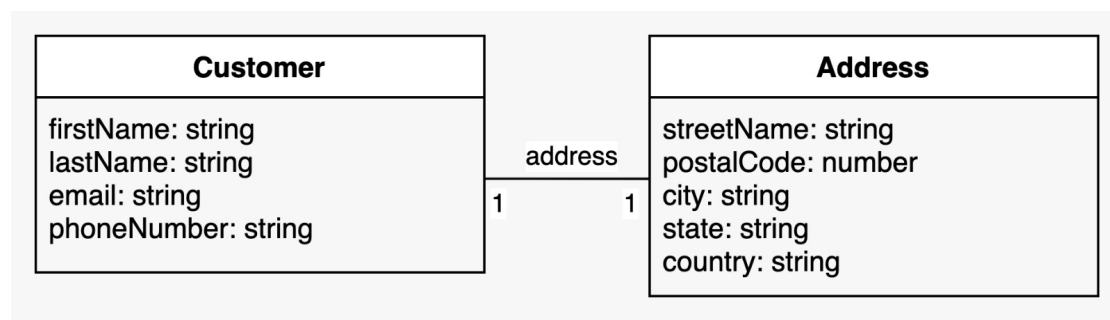


Figure A.1.: UML diagram of the customer model

## A.2. Quell-Code

## A.3. Tipps zum Schreiben Ihrer Abschlussarbeit

- Achten Sie auf eine neutrale, fachliche Sprache. Keine „Ich“-Form.
- Zitieren Sie zitierfähige und -würdige Quellen (z.B. wissenschaftliche Artikel und Fachbücher; nach Möglichkeit keine Blogs und keinesfalls Wikipedia<sup>1</sup>).
- Zitieren Sie korrekt und homogen.
- Verwenden Sie keine Fußnoten für die Literaturangaben.
- Recherchieren Sie ausführlich den Stand der Wissenschaft und Technik.
- Achten Sie auf die Qualität der Ausarbeitung (z.B. auf Rechtschreibung).
- Informieren Sie sich ggf. vorab darüber, wie man wissenschaftlich arbeitet bzw. schreibt:
  - Mittels Fachliteratur<sup>2</sup>, oder
  - Beim Lernzentrum<sup>3</sup>.
- Nutzen Sie  $\text{\LaTeX}$ <sup>4</sup>.

<sup>1</sup>Wikipedia selbst empfiehlt, von der Zitation von Wikipedia-Inhalten im akademischen Umfeld Abstand zu nehmen [15].

<sup>2</sup>Z.B. [1], [2]

<sup>3</sup>Weitere Informationen zum Schreibcoaching finden sich hier: <https://www.htw-berlin.de/studium/lernzentrum/studierende/schreibcoaching/>; letzter Zugriff: 13 VI 19.

<sup>4</sup>Kein Support bei Installation, Nutzung und Anpassung allfälliger  $\text{\LaTeX}$ -Templates!

## Eidesstattliche Versicherung

Hiermit versichere ich an Eides statt durch meine Unterschrift, dass ich die vorstehende Arbeit selbstständig und ohne fremde Hilfe angefertigt und alle Stellen, die ich wörtlich oder annähernd wörtlich aus Veröffentlichungen entnommen habe, als solche kenntlich gemacht habe, mich auch keiner anderen als der angegebenen Literatur oder sonstiger Hilfsmittel bedient habe. Die Arbeit hat in dieser oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegen.

---

Datum, Ort, Unterschrift