

# Inhaltsverzeichnis

0.1	Datenmodell-Beispiele . . . . .	1
0.1.1	Benutzer (Datenmodelle) . . . . .	1
<b>1</b>	<b>Einleitung und Vorüberlegungen</b>	<b>6</b>
1.1	Benutzerrollen . . . . .	6
<b>2</b>	<b>Autorisierung und Authentifizierung</b>	<b>8</b>
2.1	OAuth2 . . . . .	8
2.2	OpenID Connect . . . . .	9
2.3	Einschränkung der Daten . . . . .	9
<b>3</b>	<b>REST-API-Definition</b>	<b>11</b>
3.1	Schnittstellen für Schulfächer . . . . .	11
3.1.1	Endpunkt in der REST-API: /api/school-subjects . . . . .	11
3.1.1.1	READ . . . . .	11
3.2	Schnittstellen für Schuljahre . . . . .	12
3.2.1	Endpunkt in der REST-API: /api/school-years . . . . .	12
3.3	Schnittstellen für Schulen . . . . .	12
3.3.1	Endpunkt in der REST-API: /api/schools . . . . .	12
3.3.2	Endpunkt in der REST-API: /api/schools/\$id . . . . .	13
3.3.3	Endpunkt in der REST-API: /api/schools/\$id/users . . . . .	13
3.3.3.1	READ . . . . .	14
3.3.3.2	CREATE . . . . .	16
3.3.4	Endpunkt in der REST-API: /api/schools/\$id/classes . . . . .	18
3.3.5	Endpunkt in der REST-API: /api/schools/\$id/subjects . . . . .	18
3.3.5.1	READ . . . . .	19
3.4	Schnittstellen für Benutzer . . . . .	20
3.4.1	Endpunkt in der REST-API: /api/users . . . . .	20
3.4.1.1	READ . . . . .	20
3.4.2	Endpunkt in der REST-API: /api/users/\$id . . . . .	21
3.4.2.1	READ . . . . .	21
3.4.3	Endpunkt in der REST-API: /api/users/\$id/assignments . . . . .	22
3.4.3.1	READ . . . . .	22
3.4.4	Endpunkt in der REST-API: /api/users/\$id/classes . . . . .	23
3.4.4.1	READ . . . . .	23
3.4.5	Endpunkt in der REST-API: /api/users/\$id/subjects . . . . .	25
3.4.5.1	READ . . . . .	25

3.4.6	Endpunkt in der REST-API: /api/users/\$id/childs . . . . .	26
3.4.6.1	READ . . . . .	26
3.4.7	Endpunkt in der REST-API: /api/users/\$id/guardians . . . . .	27
3.4.7.1	READ . . . . .	27
3.5	Schnittstellen für Schulfächer an Schulen . . . . .	28
3.5.1	Endpunkt in der REST-API: /api/subjects . . . . .	28
3.5.1.1	READ . . . . .	28
3.5.2	Endpunkt in der REST-API: /api/subjects/\$id . . . . .	29
3.5.2.1	READ . . . . .	30
3.5.3	Endpunkt in der REST-API: /api/subjects/\$id/classes . . . . .	31
3.5.3.1	READ . . . . .	31
3.5.4	Endpunkt in der REST-API: /api/subjects/\$id/schools . . . . .	32
3.5.4.1	READ . . . . .	32
3.5.5	Endpunkt in der REST-API: /api/subjects/\$id/students . . . . .	33
3.5.5.1	READ . . . . .	33
3.5.6	Endpunkt in der REST-API: /api/subjects/\$id/teachers . . . . .	34
3.5.6.1	READ . . . . .	34
3.5.7	Endpunkt in der REST-API: /api/subjects/\$id/timetable . . . . .	35
3.5.7.1	READ . . . . .	36
3.6	Schnittstellen für Klassen . . . . .	37
3.6.1	Endpunkt in der REST-API: /api/classes/ . . . . .	37
3.6.2	Endpunkt in der REST-API: /api/classes/\$id . . . . .	37
3.6.3	Endpunkt in der REST-API: /api/classes/\$id/schools . . . . .	37
3.6.4	Endpunkt in der REST-API: /api/classes/\$id/subjects . . . . .	38
3.6.5	Endpunkt in der REST-API: /api/classes/\$id/users . . . . .	38
<b>Literaturverzeichnis</b>		<b>39</b>
<b>Abbildungsverzeichnis</b>		<b>40</b>
<b>Tabellenverzeichnis</b>		<b>41</b>
<b>Listings</b>		<b>44</b>

## 0.1 Datenmodell-Beispiele

### 0.1.1 Benutzer (Datenmodelle)

```
1 {
2   id: "USER-01",
3   name: "Leming",
4   surname: "Zobel",
5   birtdate: "03-01-2003",
6   sex: "male",
7   assignments: [
8     {
9       school_id: "SCHULE-01",
10      role: "students",
11      start: "01-09-2009",
12      end: "31-08-2016",
13      school-years: ["SJ-09/10", "SJ-10/11", "SJ-11/12", "SJ-13/14", "SJ-14/15", "SJ-15/16"]
14    }, {
15      school_id: "SCHULE-04",
16      role: "students",
17      start: "01-09-2016",
18      school-years: ["SJ-16/17", "SJ-17/18", "SJ-18/19", "SJ-19/20", "SJ-20/21"]
19    }, {
20      school_id: "SCHULE-02",
21      role: "external-students",
22      start: "01-09-2019",
23      end: "31-08-2020",
24      school-years: ["SJ-19/20"]
25    },
26  ],
27  guardians: [
28    {
29      user_id: "USER-02",
30      start: "01-09-2009",
31      end: "03-01-2020",
32    }, {
33      user_id: "USER-04",
34      start: "01-09-2009",
35      end: "03-01-2020",
36    }
37  ],
38  classes: [
39    {
40      class_id: "KLASSE-0001",
41      school_id: "SCHULE-01",
42      school-year: "SJ-09/10",
43      start: "01-09-2009",
44      end: "31-08-2010",
45    }, {
46      class_id: "KLASSE-0002",
47      school_id: "SCHULE-01",
48      school-year: "SJ-10/11",
```

```

49     start: "01-09-2010",
50     end: "31-08-2011",
51 }, {
52     class_id: "KLASSE-0003",
53     school_id: "SCHULE-01",
54     school-year: "SJ-10/11",
55     start: "01-09-2010",
56     end: "31-08-2011",
57 },
58 ],
59 subjects: [
60     {
61         subject_id: "SUBJECT-0001",
62         subject_ref_id: "DE",
63         school_id: "SCHULE-01",
64         school-year: "SJ-09/10",
65         start: "01-09-2009",
66         end: "28-02-2010".
67         time_tabel [
68             {
69                 day: "1",
70                 start: "08:00:00",
71                 end: "08:45:00",
72                 repeat: "weekly"
73             }, {
74                 day: "2",
75                 start: "08:00:00",
76                 end: "08:45:00",
77                 repeat: "weekly"
78             }, {
79                 day: "3",
80                 start: "08:50:00",
81                 end: "09:35:00",
82                 repeat: "biweekly",
83                 start: "week-1"
84             }, {
85                 day: "4",
86                 start: "08:50:00",
87                 end: "09:35:00",
88                 repeat: "biweekly",
89                 start: "week-2"
90             }, {
91                 day: "3",
92                 start: "08:50:00",
93                 end: "09:35:00",
94                 repeat: "once",
95                 date: "30-10-2009"
96             }
97         ], {
98             subject_id: "SUBJECT-0002",
99             subject_ref_id: "MA",
100             school_id: "SCHULE-01",
101             school-year: "SJ-09/10",

```

```

102     start: "01-09-2009",
103     end: "31-08-2010"
104 },
105
106 ]
107 }

```

Listing 1: Beispiel Benutzer mit Rolle 'students'

```

1  {
2    id: "USER-02",
3    name: "Altes Leming 1",
4    surname: "Zobel",
5    birtdate: "03-01-2003",
6    sex: "female",
7    assignments: [
8      {
9        school_id: "SCHULE-01",
10       role: "guardians",
11       start: "01-09-2009",
12       end: "31-08-2016",
13       school-years: ["SJ-09/10", "SJ-10/11", "SJ-11/12", "SJ-13/14", "SJ-14/15", "SJ-15/16"]
14     }, {
15       school_id: "SCHULE-04",
16       role: "guardians",
17       start: "01-09-2016",
18       school-years: ["SJ-16/17", "SJ-17/18", "SJ-18/19", "SJ-19/20", "SJ-20/21"]
19     }, {
20       school_id: "SCHULE-02",
21       role: "guardians",
22       start: "01-09-2019",
23       end: "31-08-2020",
24       school-years: ["SJ-19/20"]
25     }, {
26       school_id: "SCHULE-02",
27       role: "teacher",
28       start: "01-09-2019"
29     }
30   ],
31   childs: [
32     {
33       user_id: "USER-01",
34       start: "01-09-2009",
35       end: "03-01-2020",
36     }, {
37       user_id: "USER-03",
38       start: "01-09-2009",
39       end: "03-01-2020",
40     }
41   ],
42   classes: [
43     {
44       class_id: "KLASSE-0031",

```

```

45     school_id: "SCHULE-02",
46     school-year: "SJ-09/10",
47     start: "01-09-2009",
48     end: "31-08-2010",
49 }, {
50     class_id: "KLASSE-0032",
51     school_id: "SCHULE-02",
52     school-year: "SJ-20/21",
53     start: "01-09-2020",
54     end: "31-08-2021",
55 }, {
56     class_id: "KLASSE-0033",
57     school_id: "SCHULE-02",
58     school-year: "SJ-20/21",
59     start: "01-09-2020",
60     end: "31-08-2021",
61 },
62 ]
63 }

```

Listing 2: Beispiel für Benutzer mit Rollen 'teachers' und 'guardians'

```

1  {
2    subject: "SUBJECT-0001",
3    name: "Deutsch 1-A"
4    subject_ref: "DE",
5    school: "SCHULE-01",
6    school-year: "SJ-09/10",
7    start: "01-09-2009",
8    end: "28-02-2010",
9    classes: [ "KLASSE-01", "KLASSE-03", "KLASSE-05" ],
10   grade: [ "1" ],
11   students: [
12     {
13       user: "USER-01",
14       start: "01-09-2009",
15       end: "28-02-2010",
16     }, {
17       user: "USER-06",
18       start: "01-09-2009",
19       end: "28-02-2010",
20     }, {
21       user: "USER-07",
22       start: "01-09-2009",
23       end: "31-12-2009",
24     },
25   ],
26   teachers: [
27     {
28       user: "USER-08",
29       start: "01-09-2009",
30       end: "28-02-2010",
31     }, {
32       user: "USER-09",

```

```

33     start: "01-09-2009",
34     end: "31-12-2009",
35 }, {
36     user: "USER-10",
37     start: "05-10-2009",
38     end: "05-10-2009",
39 },
40 ],
41 timetable [
42     {
43         day: "1",
44         start: "08:00:00",
45         end: "08:45:00",
46         repeat: "weekly"
47     }, {
48         day: "2",
49         start: "08:00:00",
50         end: "08:45:00",
51         repeat: "weekly"
52     }, {
53         day: "3",
54         start: "08:50:00",
55         end: "09:35:00",
56         repeat: "biweekly",
57         week: "week-1"
58     }, {
59         day: "4",
60         start: "08:50:00",
61         end: "09:35:00",
62         repeat: "biweekly",
63         week: "week-2"
64     }, {
65         day: "3",
66         start: "08:50:00",
67         end: "09:35:00",
68         repeat: "onetime",
69         date: "30-10-2009"
70     }
71 ]
72 }

```

Listing 3: Beispiel eines Schulfachs

# 1 Einleitung und Vorüberlegungen

Ziel dieses Dokument ist es, eine REST-API und die darauf verwendeten Datenobjekte zu spezifizieren bzw. zu modellieren, um Daten aus einem IDM-System beziehen zu können.

Der IDM-Provider ist verpflichtet, mindestens die geforderten Schnittstellen und Protokolle mit der angegebenen Verfügbarkeitsanforderung bereitzustellen. Im Gegenzug erhält der IDM-Provider über viele Objekte die Hoheit der zentralen ID-Vergabe. Eine zentralisierte ID-Vergabe ist notwendig, damit verschiedene nachgelagerte Systeme (z.B. Schulverwaltungssoftwares, Lernplattformen) interoperabel sind.

Es werden die notwendigen Endpunkte definiert, die jeweils zugelassenen Operationen nebst verwendeter HTTP-Methode festgelegt, die Datenobjekte in JSON modelliert sowie der Workflow darauf dargestellt.

## 1.1 Benutzerrollen

Um eine saubere Zugriffssteuerung auf die Daten gewährleisten zu können, definiert dieses Dokument zentral die möglichen Rollen der Akteure. Das korrekte Mapping aus dem jeweiligen IDM-System auf die im Dokument aufgelisteten Rollenbezeichnungen ist dabei vom IDM-Provider sicherzustellen.

Im Nachfolgenden werden die Benutzerrollen des Systems aufgelistet. Die Auflistung der erlaubten und unerlaubten Aktionen erfolgt jeweils in der Definition der Endpunkte.



<b>Rollenname</b>	<b>Beschreibung der Rolle</b>
guest	Gäste und nicht authentifizierte Benutzer
user	authentifizierte Benutzer
students	Schüler
external-students	Schüler von anderen Schulen, die nur einzelne Fächer oder Kurse besuchen
guardians	Eltern, Erziehungsberechtigte, Vormünder von Schülern
teacher	Lehrer
principal	Schulleitung
school-admin	Schul-Administrator
school-board	Schulträger
fed-school-board	Mitarbeiter/-in des Schulministeriums
sync-systems	Systeme, welchen ein Sync mit allen Daten erlaubt ist

Tabelle 1.1: Benutzerrollen, die im zentralen IDM-System vorgesehen sind

## 2 Autorisierung und Authentifizierung

Um den Zugriff auf Client und REST-API gleichermaßen zu steuern und dabei im Client keine Anmeldeinformationen vorhalten zu müssen, wird eine Autorisierung und Authentifizierung per *OAuth2-Protokoll* und *OpenID Connect* vorgeschrieben.

### 2.1 OAuth2

OAuth2 ist ein Standardprotokoll für die Benutzerautorisierung [1].

Der Autorisierungsserver des IDM-Providers muss gemäß RFC 6749 folgende *Endpoints* bereitstellen:

Endpoint	Funktion
Authorization	Initiierung der Autorisierung und Benutzerzustimmung durch parametrisierten Aufruf
Token	Liefert gegen Authorization Code Access Token zurück

Tabelle 2.1: Endpunkte, die durch den IDM-Provider für die Anmeldung per OAuth2 zur Verfügung gestellt werden müssen

OAuth2 definiert sogenannte *Grant Types*, die vom *Client* über das Setzen eines oder mehrerer *response\_type* beim Aufruf des *Authorization Endpoint* gewählt werden können. Diese *Grant Types* beschreiben Möglichkeiten, wie ein Client einen *Access Token* erlangt, über den im Namen des Benutzers anschließend eine API aufgerufen werden kann. Während *response\_type=code* den *Authorization Code Grant* initiiert, liefert *response\_type=token* den Access Token direkt nach Autorisierung zurück. Zudem lassen sich über *Access Token Scopes* vom Client Anwendungsbereiche des vom Autorisierungsserver gelieferten Access Tokens anfordern [1, Abschnitt 3.3].

Die *Internet Engineering Task Force (IETF)* empfiehlt die Verwendung des *Authorization Code Grant* [2, Unterabschnitt 2.1.1]. Je nachdem, ob es sich um einen *Confidential* oder *Public Client* handelt, d.h., ob ein *Client Secret* verwendet werden kann, wird ein *Proof Key for Code Exchange (PKCE)* empfohlen bzw. vorgeschrieben. Der PKCE ist eine Erweiterung des *Authorization Code Grant*, um Cross-Site-Request-Forgery (CSRF) oder Authentication-Code-Injection-Angriffe zu verhindern [3].

Der Ablauf der Autorisierung per OAuth2-Protokoll im *Authorization Code Grant* ist in Abbildung *Abbildung 2.1* dargestellt. Dieser wird durch den *Client* gestartet, gefolgt

von der Autorisierung durch den *Resource Owners* beim Autorisierungsserver. Der Autorisierungsserver sendet einen *Authorization Code* an den *Client*, der diesen wiederum direkt beim Autorisierungsserver gegen den *Access Token* tauscht. Über den Access Token erhält der Benutzer schließlich Zugriff auf die REST-API.

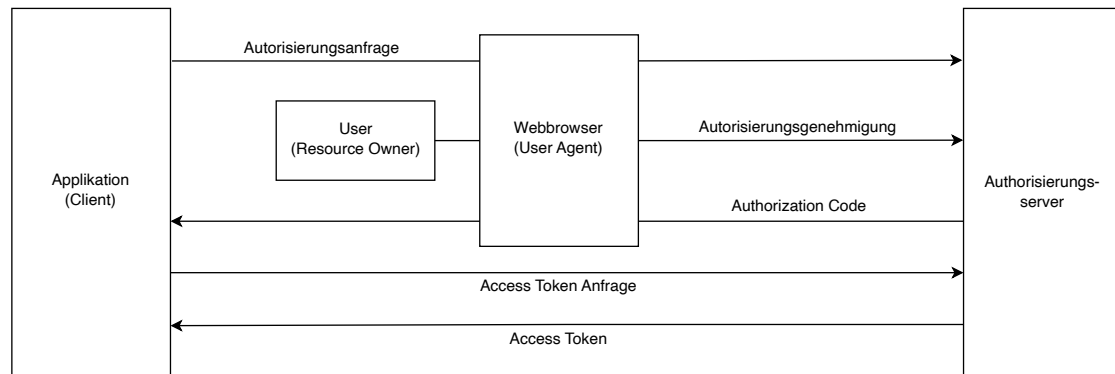


Abbildung 2.1: Ablauf des Authentication Code Grant

## 2.2 OpenID Connect

OpenID Connect ist eine Spezifikation, wie *ID Tokens* mit personenbezogenen Daten ausgegeben werden [4]. Dabei setzt OpenID Connect auf das OAuth2-Protokoll auf. OpenID Connect definiert ein weiteres *response\_type=id\_token*. Dieser ermöglicht es, neben dem Access Token den sogenannten *ID Token* in Form eines JSON Web Tokens [5] vom Autorisierungsserver anzufordern. Um OpenID Connect nutzen zu können, muss im in *Abschnitt 2.1: OAuth2* beschriebenen Autorisierungsprozess der Parameter *Scopes* um *openid* erweitert werden.

Über den ID Token erlangt der Client Zugriff auf personenbezogene Daten des Benutzers. *OpenID Connect* definiert eine Reihe von Standard-*claims* [4, Abschnitt StandardClaims]), die im *Scope*-Parameter beim Aufruf der Autorisierungs-URL aufgelistet werden. Standard-*claims* können um Custom-*claims* erweitert werden, um die gewünschten Benutzerinformationen im ID Token anzufordern.

## 2.3 Einschränkung der Daten

Die Spezifikation der REST-API sieht vor, dass die Sichtbarkeit der Daten an den definierten Endpunkte bereits im JSON-Objekt gemäß der Berechtigung des anfragenden Benutzers berücksichtigt ist. Daher muss der *ID Token* Informationen enthalten, über die der IDM-Provider den Benutzer eindeutig identifizieren kann. Die Informationen aus dem ID Token reichen ggf. jedoch nicht aus, um die Sichtbarkeit der Daten korrekt zu

beschränken, da einem Benutzer im IDM mehrere Schule-Rolle-Kombinationen zugewiesen sein können (z.B. Tätigkeit als Lehrkraft an verschiedenen Schulen oder sowohl Lehrkraft als auch Elternteil eines Schülers an derselben Schule). Daher muss die Information, mit welcher Kombination von Schule und Rolle innerhalb dieser Schule der Aufruf eines REST-API-Endpunkts durchgeführt wird, an den IDM-Provider übermittelt werden. Dies geschieht durch die Erweiterung der *Scopes*-Liste um den Scope für die Schule und die Rolle als Parameterübergabe beim Autorisierungsvorgang. *Listing 2.1* zeigt einen exemplarischen Aufruf des *Authorization Endpoints* mit Übergabe der *Scopes*. Die zusätzlichen *Scopes* für Schule und Rolle sind somit im Access Token hinterlegt und können bei der Generierung des zurückzuliefernden JSON-Objekts verwendet werden.

```
1 https://<URL zum Authorization Endpoint>?response_type=code
2 &client_id=<Identifizier von Client-App>
3 &redirect_uri=<Redirect-URL>
4 &scope=openid teachers id_schule
5 &state=<Undurchschaubarer Wert fuer Sicherheitszwecke>
```

Listing 2.1: Beispielhafter Aufruf des Authorization Endpoints

Ein Sonderfall stellen dabei Benutzerkonten mit der Rolle "sync-system" dar. Diese haben bei Aufruf eines REST-API-Endpunkts grundsätzlich keine Beschränkung auf eine einzelne Schule. Daher muss beim Autorisierungsvorgang auch kein *Scope* für die Schule an den Autorisierungsserver übergeben werden.

Sofern für ein Benutzerkonto im IDM mehrere Schule-Rolle-Kombinationen hinterlegt sein können, müssen Schule und Rolle bei Start des Authentifizierungsprozesses gegebenenfalls durch den Benutzer wählbar sein. Für einen Schule-Rolle-Wechsel ist eine Neuansmeldung bzw. Aktualisierung des Access Tokens bezüglich der *Scopes* für Schule und Rolle notwendig.

## 3 REST-API-Definition

In den folgenden Abschnitten werden die einzelnen Endpunkte der REST-API definiert. Jeder Endpunkt stellt einen Zugriffspunkt auf einen Datentyp dar und es wird definiert, inwiefern die einzelnen Operationen CREATE, READ, UPDATE und DELETE zugelassen sind und welche HTTP-Methode dabei Verwendung findet. Auch erfolgt jeweils die Definition der JSON-Objekte.

### 3.1 Schnittstellen für Schulfächer

#### 3.1.1 Endpunkt in der REST-API: /api/school-subjects

Die *Tabelle 3.1* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden. In der Tabelle <REF> ist eine Liste der vollständigen Fächer enthalten.

Operation	Zugelassen?	HTTP-Methode
CREATE	Nein	
READ	Ja	GET
UPDATE	Nein	
DELETE	Nein	

Tabelle 3.1: Zugelassene Operationen auf /api/school-subjects

##### 3.1.1.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.1*. Die einzelnen Felder der Antwort werden in *Tabelle 3.2* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.3* entnommen werden.

```
1  [  
2  {  
3    id: "<STRING>",  
4    name: "<STRING>"  
5  },  
6  ...  
7  {  
8    id: "<STRING>",  
9    name: "<STRING>"  
10 }
```

Listing 3.1: JSON-Antwort für einen GET-Aufruf der Route `/api/school-subjects`

Feldname	Datentyp	Beschreibung
id	STRING	Eine eindeutige Zeichenkette, die vom IDM-Provider vergeben wird. Sie darf nur aus alphanumerischen Zeichen und Bindestrich bestehen.
name	STRING	Der ausgeschriebene Name eines Schulfaches

Tabelle 3.2: Beschreibung der Felder in einem JSON-Objekt für ein Schulfach

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpunkt nicht aufrufen und keine Daten vom Endpunkt erhalten.
user	Darf den Endpunkt mit GET aufrufen und Endpunkt gibt alle im System vorhandenen Schulfächer in einer Liste zurück.
students	
external-students	
guardians	
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.3: Berechtigungen auf dem Endpunkt

## 3.2 Schnittstellen für Schuljahre

### 3.2.1 Endpunkt in der REST-API: `/api/school-years`

Die *Tabelle 3.4* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

## 3.3 Schnittstellen für Schulen

### 3.3.1 Endpunkt in der REST-API: `/api/schools`

Die *Tabelle 3.5* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Nein	
READ	Ja	
UPDATE	Nein	
DELETE	Nein	

Tabelle 3.4: Zugelassene Operationen auf /api/school-years

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	
UPDATE	Nein	
DELETE	Nein	

Tabelle 3.5: Zugelassene Operationen auf /api/schools

### 3.3.2 Endpunkt in der REST-API: /api/schools/\$id

Die *Tabelle 3.6* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Nein	
READ	Ja	
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.6: Zugelassene Operationen auf /api/schools/\$id

### 3.3.3 Endpunkt in der REST-API: /api/schools/\$id/users

Die *Tabelle 3.7* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden. \$id ist die ID der Schule im IDM, auf welche die nachfolgenden Operationen ausgeführt werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.7: Zugelassene Operationen auf /api/schools/\$id/users

### 3.3.3.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Bei diesem Aufruf wird eine Liste mit von Objekten übermittelt, auf welche der aktuelle Benutzer Zugriff hat, eingeschränkt auf die Schule, welche über die ID ausgewählt wurde. Ein Objekt aus der Liste enthält immer für genau einen Benutzer die Information der Benutzer-ID, der Schul-ID, der Rollen-ID, eines Zeitpunkts, ab wann das Objekt gültig war, und optional eines Zeitpunkts, bis wann das Objekt gültig ist. Gibt es Unterbrechungen in den Zeiträumen, in denen ein Benutzer eine Rolle in einer Schule eingenommen hat, so muss es für jeden Zeitraum ein eigenes Objekt geben. Zum Abrufen von Daten mit IDs müssen die Anwendungen über die entsprechenden Spezialrouten gehen. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.2*. Die einzelnen Felder der Antwort werden in *Tabelle 3.8* beschrieben. Die Berechtigungen auf den Endpunkt können aus *Tabelle 3.9* entnommen werden.

```
1  [
2  {
3    school_id: "<STRING>",
4    user_id: "<STRING>",
5    role: "<STRING>",
6    start: "<TIMESTAMP>",
7    end: "<TIMESTAMP>",
8    school-years: ["<STRING>", ..., "<STRING>"]
9  },
10 ...
11 {
12   school_id: "<STRING>",
13   user_id: "<STRING>",
14   role: "<STRING>",
15   start: "<TIMESTAMP>",
16   end: "<TIMESTAMP>",
17   school-years: ["<STRING>", ..., "<STRING>"]
18 },
19 ]
```

Listing 3.2: JSON-Antwort für einen GET-Aufruf der Route `/api/schools/$id/users`

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpunkt nicht aufrufen und keine Daten vom Endpunkt erhalten.
user	Bekommt eine Liste mit ihren Daten von der ausgewählten Schule wieder.

Tabelle 3.9: Berechtigungen auf dem Endpunkt



Benutzergruppen	Zugelassene Daten
students	Bekommt die Daten aller ihrer Mitschüler von der ausgewählten Schule, mit denen sie gemeinsame Klassen oder Kurse hat, (nur Rollen: <i>students</i> und <i>external-students</i> ), den Daten ihrer Erziehungsberechtigten (nur Rolle <i>guardians</i> ), den Daten ihrer Lehrer von der ausgewählten Schule (nur Rolle <i>teacher</i> ) und den Daten ihrer Schulleiter von der ausgewählten Schule (nur Rolle <i>principal</i> ) wieder.
external-students	Bekommt eine Liste mit den Daten aller ihrer Mitschüler von der ausgewählten Schule, mit denen sie gemeinsame Klassen oder Kurse hat, (nur Rollen: <i>students</i> und <i>external-students</i> ), den Daten ihrer Lehrer von der ausgewählten Schule (nur Rolle <i>teacher</i> ) und den Daten ihres Schulleiters von der ausgewählten Schule (nur Rolle <i>principal</i> ) wieder.
guardians	Bekommt eine Liste mit den Daten ihrer Kinder unter 18 von der ausgewählten Schule (nur Rollen: <i>students</i> und <i>external-students</i> ), den Daten der Personen von der ausgewählten Schule, für die Sie Vormund ist, (nur Rollen: <i>students</i> und <i>external-students</i> ), den Daten der Lehrer ihrer Kinder unter 18 von der ausgewählten Schule (nur Rolle <i>teacher</i> ), den Daten der Lehrer von Personen von der ausgewählten Schule, für die sie Vormund ist, (nur Rolle <i>teacher</i> ), den Daten der Schulleiter ihrer Kinder unter 18 von der ausgewählten Schule, (nur Rolle <i>principal</i> ) und die Daten der Schulleiter von Personen von der ausgewählten Schule, für die sie die Vormundschaft hat, (nur Rolle <i>principal</i> ) wieder.
teacher	Bekommt eine Liste mit den Daten aller Schüler von der ausgewählten Schule, die sie unterrichten, (nur Rollen: <i>students</i> und <i>external-students</i> ), den Daten aller Erziehungsberechtigten von Schülern unter 18 von der ausgewählten Schule, die sie unterrichten, (nur Rolle <i>guardians</i> ), den Daten aller Erziehungsberechtigten von Schülern mit einem Vormund von der ausgewählten Schule, die sie unterrichten, (nur Rolle <i>guardians</i> ) und den Daten aller Kollegen von der ausgewählten Schule (nur mit den Rollen <i>teacher</i> , <i>principal</i> , <i>school-admin</i> ) wieder.

Tabelle 3.9: Berechtigungen auf dem Endpunkt

Benutzergruppen	Zugelassene Daten
principal	Bekommt eine Liste mit ihren Daten, den Daten aller Schüler von der ausgewählten Schule, an der sie Schulleiter ist, (nur Rollen: <i>students</i> und <i>external-students</i> ), den Daten aller Erziehungsberechtigten von Schülern von der ausgewählten Schule, an der sie Schulleiter ist, (nur Rolle <i>guardians</i> ) und den Daten aller Kollegen von der ausgewählten Schule (nur mit den Rollen <i>teacher</i> , <i>principal</i> , <i>school-admin</i> ) wieder.
school-admin	Bekommt eine Liste mit ihren Daten und den Daten aller Personen von der ausgewählten Schule, an der sie die Rolle <i>school-admin</i> hat, mit den Rollen <i>students</i> , <i>external-students</i> , <i>guardians</i> , <i>teacher</i> , <i>principal</i> und <i>school-admin</i> wieder.
school-board	<b>Muss geklärt werden, welche Einschränkungen auf den Daten es hier gibt</b>
fed-school-board	<b>Muss geklärt werden, welche Einschränkungen auf den Daten es hier gibt</b>
sync-systems	Liste mit allen Personen, in den Rollen der Personen an den Schulen, von den es syncen darf.

Tabelle 3.9: Berechtigungen auf dem Endpunkt

### 3.3.3.2 CREATE

Es sind nur Anfragen mit der HTTP-POST-Methode für ein CREATE der Daten zugelassen. Die Aufgabe von CREATE ist es ein Benutzer einer Schule in einer bestimmten Rolle zuzufügen. Die Felder im JSON Object, *Listing 3.3*, im HTTP-Post Body wird für das CREATE wird in *Tabelle 3.10* beschrieben. Im Erfolgsfall wird der Request mit den HTTP-Statuscode 200 - OK Beantwortet. In allen anderen Fällen werden Anfragen mit den HTTP-Statuscode 403 - Forbidden Beantwortet. Es gilt für diesen Endpunkt das der Zugriff explizit Erlaubt sein muss, *Tabelle 3.11*, ansonsten gibt der Endpunkt den HTTP-Statuscode 403 - Forbidden wieder.

Wird ein Datensatz an den Endpunkt für ein Benutzer mit der Rolle *students* gesendet, gilt das wenn der Benutzer schon ein Eintrag mit der Rolle *students* hat der noch Aktiv ist so wird dessen Enddatum auf das Startdatum des neuen Eintrages gestellt. Wenn für Benutzer mit der Rolle *students*, der unter 18 ist, ein Eintrag erstellt wird, muss für seine Eltern, Erziehungsberechtigten oder Vormünder vom System aus entsprechende Einträge für diese Personen mit der Rolle *guardians* Erzeugt werden müssen. Wird für ein Benutzer über 18 mit der Rolle *students* ein Eintrag erstellt und sind vom einen Gericht ein oder mehrere Vormünder bestimmt wurden so muss vom System aus die Entsprechenden Einträge für diese Person mit der Rolle *guardians* Erzeugt werden müssen.

Wird für ein Benutzer mit der Rolle *external-students* ein Datensatz an dem Endpunkt gesendet, muss für seine Eltern, Erziehungsberechtigten oder Vormünder vom System aus entsprechende Einträge für diese Personen mit der Rolle *parents* Erzeugt werden müssen.

Feldname	Datentyp	Beschreibung
school_id	STRING	ID der Schule
user_id	STRING	ID des Benutzers
role	STRING	Rolle des Benutzers an der Schule
start	TIMESTAMP	Zeitpunkt, ab wann der Benutzer diese Rolle innehat
end	TIMESTAMP	Optional; gibt an, bis wann ein Benutzer diese Rolle innehatte
school-years	LIST of STRINGS	Optional; das Feld gibt es nur, wenn die Rolle <i>students</i> oder <i>external-students</i> ist; enthält eine Liste von Schuljahres-IDs

Tabelle 3.8: Beschreibung der Felder in einem JSON-Objekt für einen Benutzer an einer Schule

```

1 {
2   user_id: "<STRING>",
3   role: "<STRING>",
4   start: "<TIMESTAMP>"
5   school-years: ["<STRING>", ..., "<STRING>"]
6 }

```

Listing 3.3: Felder im JSON-Objekt einer CREATE anfrage per HTTP-POST auf der Route `/api/schools/$id/users`

Feldname	Datentyp	Beschreibung
user_id	STRING	ID des Benutzers
role	STRING	Rolle des Benutzers an der Schule.
start	TIMESTAMP	Zeitpunkt ab wann der Benutzer diese Rolle innehat.
school-years	LISTE of STRINGS	Optional, das Feld wird nur benötigt wenn die Rolle <i>students</i> oder <i>external-students</i> ist, Enthält eine Liste von Schuljahres IDs.

Tabelle 3.10: Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Benutzergruppen	Zugelassene Daten
principal	Darf Einträge für Personen mit den Rollen <i>students</i> , <i>teacher</i> , <i>principal</i> und <i>school-admin</i> an der ausgewählten Schule anlegen. Darf für User mit der Rolle <i>students</i> von seiner Schule, an ausgewählten Schule, mit der Rolle <i>external-students</i> anlegen und somit diesen Schüler für ausgewählten Schule freigeben.
school-admin	Darf Einträge für Personen mit den Rollen <i>students</i> , <i>teacher</i> , <i>principal</i> und <i>school-admin</i> an der ausgewählten Schule anlegen. Darf für User mit der Rolle <i>students</i> von seiner Schule, an ausgewählten Schule, mit der Rolle <i>external-students</i> anlegen und somit diesen Schüler für ausgewählten Schule freigeben.
school-board	Darf Einträge für Personen mit den Rollen <i>students</i> , <i>teacher</i> , <i>principal</i> und <i>school-admin</i> an der ausgewählten Schule anlegen, wenn der Schulträger für die Schule Zuständig ist. Darf für User mit der Rolle <i>students</i> für Schulen, von Schulen zu dessen Schulträger er gehört, an der ausgewählten Schule, Einträge mit der Rolle <i>external-students</i> anlegen und somit diesen Schüler für ausgewählten Schule freigeben.
fed-school-board	Darf Einträge für User mit den Rollen <i>students</i> , <i>external-students</i> , <i>teacher</i> , <i>principal</i> und <i>school-admin</i> an der ausgewählten Schule anlegen.

Tabelle 3.11: Berechtigungen auf dem Endpunkt

### 3.3.4 Endpunkt in der REST-API: `/api/schools/$id/classes`

Die *Tabelle 3.12* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.12: Zugelassene Operationen auf `/api/schools/$id/classes`

### 3.3.5 Endpunkt in der REST-API: `/api/schools/$id/subjects`

Die *Tabelle 3.13* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.13: Zugelassene Operationen auf `/api/schools/$id/subjects`

### 3.3.5.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.4*. Die einzelnen Felder der Antwort werden in *Tabelle 3.14* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.15* entnommen werden.

```

1 [
2   "<STRING>",
3   ...
4 ]

```

Listing 3.4: JSON-Antwort für einen GET-Aufruf der Route `/api/schools/$id/subjects`

Feldname	Datentyp	Beschreibung

Tabelle 3.14: Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpunkt nicht aufrufen und keine Daten vom Endpunkt erhalten.
user	
students	
external-students	
guardians	
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.15: Berechtigungen auf dem Endpunkt

## 3.4 Schnittstellen für Benutzer

### 3.4.1 Endpunkt in der REST-API: /api/users

Die *Tabelle 3.16* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	GET
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.16: Zugelassene Operationen auf /api/users

#### 3.4.1.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Route gibt für den eingeloggtten Benutzer seine persönlichen Daten wieder. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.5*. Die einzelnen Felder der Antwort werden in *Tabelle 3.17* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.18* entnommen werden.

```
1 {  
2   id: "<STRING>",  
3   name: "<STRING>",  
4   surname: "<STRING>",  
5   dateofbirth: "<CALENDARDATE>",  
6   sex: "<ENUM>",  
7 }
```

Listing 3.5: JSON-Antwort für einen GET-Aufruf der Route /api/users

Feldname	Datentyp	Beschreibung

Tabelle 3.17: Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpunkt nicht aufrufen und keine Daten vom Endpunkt erhalten.
user	
students	

Tabelle 3.18: Berechtigungen auf dem Endpunkt

Benutzergruppen	Zugelassene Daten
external-students	
guardians	
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.18: Berechtigungen auf dem Endpunkt

### 3.4.2 Endpunkt in der REST-API: /api/users/\$id

Die *Tabelle 3.19* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Nein	
READ	Ja	GET
UPDATE	Ja	POST
DELETE	Nein	

Tabelle 3.19: Zugelassene Operationen auf /api/users/\$id

#### 3.4.2.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Route gibt für den per ID ausgewählten Benutzer seine persönlichen Daten wieder. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.6*. Die einzelnen Felder der Antwort werden in *Tabelle 3.20* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.21* entnommen werden.

```

1 {
2   id: "<STRING>",
3   name: "<STRING>",
4   surname: "<STRING>",
5   dateofbirth: "<CALENDARDATE>",
6   sex: "<ENUM>",
7 }
```

Listing 3.6: JSON-Antwort für einen GET-Aufruf der Route /api/users/\$id

Feldname	Datentyp	Beschreibung

Tabelle 3.20: Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpunkt nicht aufrufen und keine Daten vom Endpunkt erhalten.
user	
students	
external-students	
guardians	
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.21: Berechtigungen auf dem Endpunkt

### 3.4.3 Endpunkt in der REST-API: /api/users/\$id/assignments

Die *Tabelle 3.22* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	GET
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.22: Zugelassene Operationen auf /api/users/\$id/assignments

#### 3.4.3.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Sie gibt für den per ID ausgewählten Benutzer seine Zuordnungen im System wieder. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.7*. Die einzelnen Felder der Antwort werden in *Tabelle 3.23* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.24* entnommen werden.



```

1 {
2   school_id: "<STRING>",
3   role: "<STRING>",
4   start: "<CALENDARDATE>",
5   end: "<CALENDARDATE>",
6   school-years: ["<STRING>", ...]
7 },
8 ...

```

Listing 3.7: JSON-Antwort für einen GET-Aufruf der Route `/api/users/$id/assignments`

Feldname	Datentyp	Beschreibung

Tabelle 3.23: Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpunkt nicht aufrufen und keine Daten vom Endpunkt erhalten.
user	
students	
external-students	
guardians	
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.24: Berechtigungen auf dem Endpunkt

### 3.4.4 Endpunkt in der REST-API: `/api/users/$id/classes`

Die *Tabelle 3.25* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

#### 3.4.4.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Route gibt für den per ID ausgewählten Benutzer seine für ihn hinterlegten Klassen im System wieder. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.8*. Die einzelnen Felder der Antwort werden in *Tabelle 3.26* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.27* entnommen werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	GET
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.25: Zugelassene Operationen auf `/api/users/$id/classes`

```

1 [
2   {
3     class_id: "<STRING>",
4     school_id: "<STRING>",
5     school-year: "<STRING>",
6     start: "<CALENDARDATE>",
7     end: "<CALENDARDATE>",
8   },
9   ...
10 ]

```

Listing 3.8: JSON-Antwort für einen GET-Aufruf der Route `/api/users/$id/classes`

Feldname	Datentyp	Beschreibung

Tabelle 3.26: Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpunkt nicht aufrufen und keine Daten vom Endpunkt erhalten.
user	
students	
external-students	
guardians	
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.27: Berechtigungen auf dem Endpunkt

### 3.4.5 Endpunkt in der REST-API: /api/users/\$id/subjects

Die *Tabelle 3.28* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	GET
UPDATE	Nein	
DELETE	Ja	POST

Tabelle 3.28: Zugelassene Operationen auf /api/users/\$id/subjects

#### 3.4.5.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.9*. Die einzelnen Felder der Antwort werden in *Tabelle 3.29* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.30* entnommen werden.

```
1 [
2   "<STRING>",
3   ...
4 ]
```

Listing 3.9: JSON-Antwort für einen GET-Aufruf der Route /api/users/\$id/subjects

Feldname	Datentyp	Beschreibung

Tabelle 3.29: Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpunkt nicht aufrufen und keine Daten vom Endpunkt erhalten.
user	
students	
external-students	
guardians	
teacher	
principal	
school-admin	

Tabelle 3.30: Berechtigungen auf dem Endpunkt

Benutzergruppen	Zugelassene Daten
school-board	
fed-school-board	
sync-systems	

Tabelle 3.30: Berechtigungen auf dem Endpunkt

### 3.4.6 Endpunkt in der REST-API: /api/users/\$id/childs

Die *Tabelle 3.31* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	GET
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.31: Zugelassene Operationen auf /api/users/\$id/childs

#### 3.4.6.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Route gibt für den per ID ausgewählten Benutzer Benutzer die Liste mit den IDs seiner Kinder wieder. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.10*. Die einzelnen Felder der Antwort werden in *Tabelle 3.32* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.33* entnommen werden.

```

1 [
2   id: "<STRING>",
3   ...
4 ]

```

Listing 3.10: JSON-Antwort für einen GET-Aufruf der Route /api/users/\$id/childs

Feldname	Datentyp	Beschreibung

Tabelle 3.32: Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpunkt nicht aufrufen und keine Daten vom Endpunkt erhalten.
user	
students	
external-students	
guardians	
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.33: Berechtigungen auf dem Endpunkt

### 3.4.7 Endpunkt in der REST-API: /api/users/\$id/guardians

Die *Tabelle 3.34* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	GET
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.34: Zugelassene Operationen auf /api/users/\$id/guardians

#### 3.4.7.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Route gibt für den per ID ausgewählten Benutzer die Liste mit den IDs seiner Eltern, Erziehungsberechtigten und Vormünder wieder. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.11*. Die einzelnen Felder der Antwort werden in *Tabelle 3.35* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.36* entnommen werden.

```

1 [
2   id: "<STRING>",
3   ...
4 ]
```

Listing 3.11: JSON-Antwort für einen GET-Aufruf der Route /api/user/\$id/guardians

Feldname	Datentyp	Beschreibung

Tabelle 3.35: Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpunkt nicht aufrufen und keine Daten vom Endpunkt erhalten.
user	
students	
external-students	
guardians	
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.36: Berechtigungen auf dem Endpunkt

## 3.5 Schnittstellen für Schulfächer an Schulen

### 3.5.1 Endpunkt in der REST-API: /api/subjects

Die *Tabelle 3.37* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	GET
UPDATE	Nein	
DELETE	Nein	

Tabelle 3.37: Zugelassene Operationen auf /api/subjects

#### 3.5.1.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.12*. Die einzelnen Felder der Antwort werden in *Tabelle 3.38* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.39* entnommen werden.

```

1 [
2   "<STRING>",
3   ...
4 ]

```

Listing 3.12: JSON-Antwort für einen GET-Aufruf der Route `/api/subjects`

Feldname	Datentyp	Beschreibung

Tabelle 3.38: Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpunkt nicht aufrufen und keine Daten vom Endpunkt erhalten.
user	
students	
external-students	
guardians	
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.39: Berechtigungen auf dem Endpunkt

### 3.5.2 Endpunkt in der REST-API: `/api/subjects/$id`

Die *Tabelle 3.40* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	GET
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.40: Zugelassene Operationen auf `/api/subjects/$id`

### 3.5.2.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.13*. Die einzelnen Felder der Antwort werden in *Tabelle 3.41* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.42* entnommen werden.

```
1  [  
2  {  
3    subject: "<STRING>",  
4    name: "<STRING>",  
5    subject_ref: "<STRING>",  
6    school: "<STRING>",  
7    school-year: "<STRING>",  
8    start: "<CALENDARDATE>",  
9    end: "<CALENDARDATE>",  
10 },  
11 ...  
12 ]
```

Listing 3.13: JSON-Antwort für einen GET-Aufruf der Route `/api/subjects/$id`

Feldname	Datentyp	Beschreibung

Tabelle 3.41: Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpunkt nicht aufrufen und keine Daten vom Endpunkt erhalten.
user	
students	
external-students	
guardians	
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.42: Berechtigungen auf dem Endpunkt



### 3.5.3 Endpunkt in der REST-API: /api/subjects/\$id/classes

Die *Tabelle 3.43* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	GET
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.43: Zugelassene Operationen auf /api/subjects/\$id/classes

#### 3.5.3.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.14*. Die einzelnen Felder der Antwort werden in *Tabelle 3.44* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.45* entnommen werden.

```
1 [
2   {
3     subject: "<STRING>",
4     classes: [ "<STRING>", ... ],
5   },
6   ...
7 ]
```

Listing 3.14: JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id/classes

Feldname	Datentyp	Beschreibung

Tabelle 3.44: Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpunkt nicht aufrufen und keine Daten vom Endpunkt erhalten.
user	
students	
external-students	
guardians	

Tabelle 3.45: Berechtigungen auf dem Endpunkt

Benutzergruppen	Zugelassene Daten
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.45: Berechtigungen auf dem Endpunkt

### 3.5.4 Endpunkt in der REST-API: /api/subjects/\$id/schools

Die *Tabelle 3.46* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	GET
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.46: Zugelassene Operationen auf /api/subjects/\$id/schools

#### 3.5.4.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.15*. Die einzelnen Felder der Antwort werden in *Tabelle 3.47* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.48* entnommen werden.

```

1 [
2   {
3     subject: "<STRING>",
4     school: "<STRING>",
5   },
6   ...
7 ]

```

Listing 3.15: JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id/schools

Feldname	Datentyp	Beschreibung

Tabelle 3.47: Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpunkt nicht aufrufen und keine Daten vom Endpunkt erhalten.
user	
students	
external-students	
guardians	
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.48: Berechtigungen auf dem Endpunkt

### 3.5.5 Endpunkt in der REST-API: /api/subjects/\$id/students

Die *Tabelle 3.49* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Nein	
READ	Ja	GET
UPDATE	Nein	
DELETE	Nein	

Tabelle 3.49: Zugelassene Operationen auf /api/subjects/\$id/students

#### 3.5.5.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.16*. Die einzelnen Felder der Antwort werden in *Tabelle 3.50* beschrieben. Die Berechtigungen auf den Endpoint können *Tabelle 3.51* entnommen werden.

```

1 [
2   {
3     subject: "<STRING>",
4     user: "<STRING>",
5     start: "<CALENDARDATE>",
6     end: "<CALENDARDATE>",
7   },
8   ...
9 ]

```

Listing 3.16: JSON-Antwort für einen GET-Aufruf der Route  
/api/subjects/\$id/students

Feldname	Datentyp	Beschreibung

Tabelle 3.50: Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpunkt nicht aufrufen und keine Daten vom Endpunkt erhalten.
user	
students	
external-students	
guardians	
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.51: Berechtigungen auf dem Endpunkt

### 3.5.6 Endpunkt in der REST-API: /api/subjects/\$id/teachers

Die *Tabelle 3.52* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Nein	
READ	Ja	GET
UPDATE	Nein	
DELETE	Nein	

Tabelle 3.52: Zugelassene Operationen auf /api/subjects/\$id/teachers

#### 3.5.6.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.17*. Die einzelnen Felder

der Antwort werden in Tabelle *Tabelle 3.53* beschrieben. Die Berechtigungen auf den Endpoint können *Tabelle 3.54* entnommen werden.

```

1 [
2   {
3     subject: "<STRING>",
4     user: "<STRING>",
5     start: "<CALENDARDATE>",
6     end: "<CALENDARDATE>",
7   },
8   ...
9 ]

```

Listing 3.17: JSON-Antwort für einen GET-Aufruf der Route `/api/subjects/$id/teachers`

Feldname	Datentyp	Beschreibung

Tabelle 3.53: Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpoint nicht aufrufen und keine Daten vom Endpoint erhalten.
user	
students	
external-students	
guardians	
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.54: Berechtigungen auf dem Endpoint

### 3.5.7 Endpoint in der REST-API: `/api/subjects/$id/timetable`

Die *Tabelle 3.55* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Nein	
READ	Ja	GET
UPDATE	Nein	
DELETE	Nein	

Tabelle 3.55: Zugelassene Operationen auf `/api/subjects/$id/timetable`

### 3.5.7.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.18*. Die einzelnen Felder der Antwort werden in Tabelle *Tabelle 3.56* beschrieben. Die Berechtigungen auf den Endpoint können *Tabelle 3.57* entnommen werden.

```

1  [
2  {
3      subject: "<STRING>",
4      day: "<ENUM>",
5      start: "<TIME>",
6      end: "<TIME>",
7      repeat: "<ENUM>",
8      date: "<CALENDARDATE>",
9      week: "<ENUM>",
10 },
11 ...
12 ]

```

Listing 3.18: JSON-Antwort für einen GET-Aufruf der Route `/api/subjects/$id/timetable`

Feldname	Datentyp	Beschreibung

Tabelle 3.56: Beschreibung der Felder in einem JSON-Objekt für den Stundenplan eines Schulfachs

Benutzergruppen	Zugelassene Daten
guest	Darf den Endpoint nicht aufrufen und keine Daten vom Endpoint erhalten.
user	
students	
external-students	
guardians	

Tabelle 3.57: Berechtigungen auf dem Endpoint

Benutzergruppen	Zugelassene Daten
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.57: Berechtigungen auf dem Endpunkt

## 3.6 Schnittstellen für Klassen

### 3.6.1 Endpunkt in der REST-API: /api/classes/

Die *Tabelle 3.58* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	GET
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.58: Zugelassene Operationen auf /api/classes/

### 3.6.2 Endpunkt in der REST-API: /api/classes/\$id

Die *Tabelle 3.59* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Nein	
READ	Ja	GET
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.59: Zugelassene Operationen auf /api/classes/\$id

### 3.6.3 Endpunkt in der REST-API: /api/classes/\$id/schools

Die *Tabelle 3.60* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	GET
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.60: Zugelassene Operationen auf `/api/classes/$id/schools`

### 3.6.4 Endpunkt in der REST-API: `/api/classes/$id/subjects`

Die *Tabelle 3.61* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	GET
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.61: Zugelassene Operationen auf `/api/classes/$id/subjects`

### 3.6.5 Endpunkt in der REST-API: `/api/classes/$id/users`

Die *Tabelle 3.62* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

Operation	Zugelassen?	HTTP-Methode
CREATE	Ja	POST
READ	Ja	GET
UPDATE	Ja	POST
DELETE	Ja	POST

Tabelle 3.62: Zugelassene Operationen auf `/api/classes/$id/users`



# Literaturverzeichnis

- [1] D. Hardt, “The OAuth 2.0 Authorization Framework.” RFC 6749, Oct. 2012.
- [2] T. Lodderstedt, J. Bradley, A. Labunets, and D. Fett, “OAuth 2.0 Security Best Current Practice,” Internet-Draft draft-ietf-oauth-security-topics-18, Internet Engineering Task Force, Apr. 2021. Work in Progress.
- [3] N. Sakimura, J. Bradley, and N. Agarwal, “Proof Key for Code Exchange by OAuth Public Clients.” RFC 7636, Sept. 2015.
- [4] N. Sakimura, J. Bradley, M. B. Jones, B. de Medeiros, and C. Mortimore, “OpenID Connect Core 1.0 incorporating errata set 1,” Nov. 2014.
- [5] M. Jones, J. Bradley, and N. Sakimura, “JSON Web Token (JWT).” RFC 7519, May 2015.

# Abbildungsverzeichnis

2.1	Ablauf des Authentication Code Grant . . . . .	9
-----	--	---

# Tabellenverzeichnis

1.1	Benutzerrollen, die im zentralen IDM-System vorgesehen sind . . . . .	7
2.1	Endpunkte, die durch den IDM-Provider für die Anmeldung per OAuth2 zur Verfügung gestellt werden müssen . . . . .	8
3.1	Zugelassene Operationen auf /api/school-subjects . . . . .	11
3.2	Beschreibung der Felder in einem JSON-Objekt für ein Schulfach . . . . .	12
3.3	Berechtigungen auf dem Endpunkt . . . . .	12
3.4	Zugelassene Operationen auf /api/school-years . . . . .	13
3.5	Zugelassene Operationen auf /api/schools . . . . .	13
3.6	Zugelassene Operationen auf /api/schools/\$id . . . . .	13
3.7	Zugelassene Operationen auf /api/schools/\$id/users . . . . .	13
3.9	Berechtigungen auf dem Endpunkt . . . . .	14
3.9	Berechtigungen auf dem Endpunkt . . . . .	15
3.9	Berechtigungen auf dem Endpunkt . . . . .	16
3.8	Beschreibung der Felder in einem JSON-Objekt für einen Benutzer an einer Schule . . . . .	17
3.10	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule . . . . .	17
3.11	Berechtigungen auf dem Endpunkt . . . . .	18
3.12	Zugelassene Operationen auf /api/schools/\$id/classes . . . . .	18
3.13	Zugelassene Operationen auf /api/schools/\$id/subjects . . . . .	19
3.14	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule . . . . .	19
3.15	Berechtigungen auf dem Endpunkt . . . . .	19
3.16	Zugelassene Operationen auf /api/users . . . . .	20
3.17	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule . . . . .	20
3.18	Berechtigungen auf dem Endpunkt . . . . .	20
3.18	Berechtigungen auf dem Endpunkt . . . . .	21
3.19	Zugelassene Operationen auf /api/users/\$id . . . . .	21
3.20	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule . . . . .	22
3.21	Berechtigungen auf dem Endpunkt . . . . .	22
3.22	Zugelassene Operationen auf /api/users/\$id/assignments . . . . .	22

3.23	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule . . . . .	23
3.24	Berechtigungen auf dem Endpunkt . . . . .	23
3.25	Zugelassene Operationen auf /api/users/\$id/classes . . . . .	24
3.26	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule . . . . .	24
3.27	Berechtigungen auf dem Endpunkt . . . . .	24
3.28	Zugelassene Operationen auf /api/users/\$id/subjects . . . . .	25
3.29	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule . . . . .	25
3.30	Berechtigungen auf dem Endpunkt . . . . .	25
3.30	Berechtigungen auf dem Endpunkt . . . . .	26
3.31	Zugelassene Operationen auf /api/users/\$id/childs . . . . .	26
3.32	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule . . . . .	26
3.33	Berechtigungen auf dem Endpunkt . . . . .	27
3.34	Zugelassene Operationen auf /api/users/\$id/guardians . . . . .	27
3.35	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule . . . . .	28
3.36	Berechtigungen auf dem Endpunkt . . . . .	28
3.37	Zugelassene Operationen auf /api/subjects . . . . .	28
3.38	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule . . . . .	29
3.39	Berechtigungen auf dem Endpunkt . . . . .	29
3.40	Zugelassene Operationen auf /api/subjects/\$id . . . . .	29
3.41	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule . . . . .	30
3.42	Berechtigungen auf dem Endpunkt . . . . .	30
3.43	Zugelassene Operationen auf /api/subjects/\$id/classes . . . . .	31
3.44	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule . . . . .	31
3.45	Berechtigungen auf dem Endpunkt . . . . .	31
3.45	Berechtigungen auf dem Endpunkt . . . . .	32
3.46	Zugelassene Operationen auf /api/subjects/\$id/schools . . . . .	32
3.47	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule . . . . .	32
3.48	Berechtigungen auf dem Endpunkt . . . . .	33
3.49	Zugelassene Operationen auf /api/subjects/\$id/students . . . . .	33
3.50	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule . . . . .	34
3.51	Berechtigungen auf dem Endpunkt . . . . .	34
3.52	Zugelassene Operationen auf /api/subjects/\$id/teachers . . . . .	34

3.53	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule . . . . .	35
3.54	Berechtigungen auf dem Endpunkt . . . . .	35
3.55	Zugelassene Operationen auf /api/subjects/\$id/timetable . . . . .	36
3.56	Beschreibung der Felder in einem JSON-Objekt für den Stundenplan eines Schulfachs . . . . .	36
3.57	Berechtigungen auf dem Endpunkt . . . . .	36
3.57	Berechtigungen auf dem Endpunkt . . . . .	37
3.58	Zugelassene Operationen auf /api/classes/ . . . . .	37
3.59	Zugelassene Operationen auf /api/classes/\$id . . . . .	37
3.60	Zugelassene Operationen auf /api/classes/\$id/schools . . . . .	38
3.61	Zugelassene Operationen auf /api/classes/\$id/subjects . . . . .	38
3.62	Zugelassene Operationen auf /api/classes/\$id/users . . . . .	38

# Listings

1	Beispiel Benutzer mit Rolle 'students' . . . . .	1
2	Beispiel f[Pleaseinsertintopreamble]r Benutzer mit Rollen 'teachers' und 'guardians' . . . . .	3
3	Beispiel eines Schulfachs . . . . .	4
2.1	Beispielhafter Aufruf des Authorization Endpoints . . . . .	10
3.1	JSON-Antwort für einen GET-Aufruf der Route /api/school-subjects . . .	11
3.2	JSON-Antwort für einen GET-Aufruf der Route /api/schools/\$id/users .	14
3.3	Felder im JSON-Object einer CREATE anfrage per HTTP-POST auf der Route /api/schools/\$id/users . . . . .	16
3.4	JSON-Antwort für einen GET-Aufruf der Route /api/schools/\$id/subjects	19
3.5	JSON-Antwort für einen GET-Aufruf der Route /api/users . . . . .	20
3.6	JSON-Antwort für einen GET-Aufruf der Route /api/users/\$id . . . . .	21
3.7	JSON-Antwort für einen GET-Aufruf der Route /api/users/\$id/assignments	23
3.8	JSON-Antwort für einen GET-Aufruf der Route /api/users/\$id/classes . .	24
3.9	JSON-Antwort für einen GET-Aufruf der Route /api/users/\$id/subjects .	25
3.10	JSON-Antwort für einen GET-Aufruf der Route /api/users/\$id/childs . .	26
3.11	JSON-Antwort für einen GET-Aufruf der Route /api/user/\$id/guardians	27
3.12	JSON-Antwort für einen GET-Aufruf der Route /api/subjects . . . . .	29
3.13	JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id . . . .	30
3.14	JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id/classes	31
3.15	JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id/schools	32
3.16	JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id/students	33
3.17	JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id/teachers	35
3.18	JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id/timetable	36