

Inhaltsverzeichnis

0.1	Datenmodell-Beispiele	1
0.1.1	Benutzer (Datenmodelle)	1
1	Einleitung und Vorüberlegungen	6
1.1	Benutzerrollen	6
2	Autorisierung und Authentifizierung	8
2.1	OAuth2	8
2.2	OpenID Connect	9
2.3	Einschränkung der Daten	9
3	REST-API-Definition	11
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	13
3.3	Schnittstellen für Schulen	13
3.3.1	Endpunkt in der REST-API: /api/schools	13
3.3.2	Endpunkt in der REST-API: /api/schools/\$id	13
3.3.3	Endpunkt in der REST-API: /api/schools/\$id/users	14
3.3.3.1	READ	14
3.3.3.2	CREATE	17
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	29
3.5.1.1	READ	29
3.5.2	Endpunkt in der REST-API: /api/subjects/\$id	30
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/students	32
3.5.4.1	READ	32
3.5.5	Endpunkt in der REST-API: /api/subjects/\$id/teachers	34
3.5.5.1	READ	34
3.5.6	Endpunkt in der REST-API: /api/subjects/\$id/timetable	35
3.5.6.1	READ	35
3.6	Schnittstellen für Klassen	36
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	37
3.6.5	Endpunkt in der REST-API: /api/classes/\$id/users	38
Literaturverzeichnis		39
Abbildungsverzeichnis		40
Tabellenverzeichnis		41
Listings		44

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    birthdate: "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.

Rollenname	Beschreibung der Rolle
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.

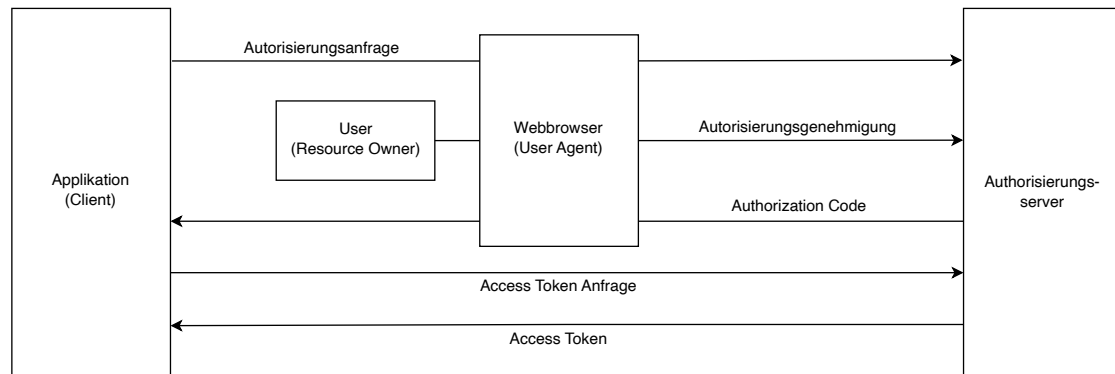


Abbildung 2.1: Ablauf des Authentication Code Grant

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

Die Schnittstelle für Schulfächer listet die Teilmenge der abgestimmten Referenzschulfächer auf welche von dem IDM unterstützt werden. Die gesamte Menge aller abgestimmten Referenzschulfächer kann aus *Tabelle 3.1* entnommen werden.

ID	Abkürzung	Ausgeschriebener Name

Tabelle 3.1: Liste der abgestimmten Referenzschulfächer

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

Die *Tabelle 3.2* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden. In der *Tabelle 3.1* ist eine Liste der vollständigen Fächer enthalten.

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

Tabelle 3.2: 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. Bei einer lesenden Anfrage wird eine Liste der Teilmenge der Referenzschulfächer welche vom IDM unterstützt werden zurückgegeben.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.1*. Die einzelnen Felder der Antwort werden in *Tabelle 3.3* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.4* entnommen werden.

```

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

```

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 3.3: 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 3.4: Berechtigungen auf dem Endpunkt

3.2 Schnittstellen für Schuljahre

Die Schnittstelle für Schuljahre hat die Aufgabe alle im IDM verfügbaren Schuljahre mit ihren allgemeinen Informationen bereitzustellen. ***Muss noch ausgearbeitet werden!***

- Datenmodel einfach muss nur noch beschrieben werden
- Wird nur die im IDM verfügbaren Schuljahre anzeigen

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

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 3.5: Zugelassene Operationen auf /api/school-years

3.3 Schnittstellen für Schulen

Muss noch überarbeitet werden!

- Soll für aktiven Benutzer bei Dreieckern aufrufen nur liste von sein Schulen die er grade sehen kann wieder geben.
- Verhalten für anfrage mit ID muss noch bestimmt werden.
- Datenmodel muss noch gemacht werden.
- Filtermöglichkeiten müssen diskutiert und beschrieben werden.

3.4 Schnittstellen für Benutzer

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

Die *Tabelle 3.17* 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 3.6: 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 3.18* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.19* entnommen werden.

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

Listing 3.2: JSON-Antwort für einen GET-Aufruf der Route /api/users

Feldname	Datentyp	Beschreibung

Tabelle 3.7: Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzers 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 3.8: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.20* 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 3.9: 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. Diese können eingeschränkt werden durch den Kontext in den sich der anfragende User befinden.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.6*. Die einzelnen Felder der Antwort werden in *Tabelle 3.21* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.22* entnommen werden.

```

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

Listing 3.3: JSON-Antwort für einen GET-Aufruf der Route `/api/users/$id`

Feldname	Datentyp	Beschreibung

Tabelle 3.10: 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	

Tabelle 3.11: Berechtigungen auf dem Endpunkt

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

Tabelle 3.11: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.23* 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 3.12: 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. Für diese Daten gelten die Einschränkungen die durch den Kontext des anfragenden Benutzers gegeben sind.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.7*. Die einzelnen Felder der Antwort werden in *Tabelle 3.24* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.25* entnommen werden.

```

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

```

Listing 3.4: JSON-Antwort für einen GET-Aufruf der Route /api/users/\$id/assignments

Feldname	Datentyp	Beschreibung

Tabelle 3.13: 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 3.14: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.26* 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 3.15: Zugelassene Operationen auf `/api/users/$id/classes`

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. Für diese Daten gelten die Einschränkungen die durch den Kontext des anfragenden Benutzers gegeben sind.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.8*. Die einzelnen Felder der Antwort werden in *Tabelle 3.27* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.28* entnommen werden.

```

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

```

Listing 3.5: JSON-Antwort für einen GET-Aufruf der Route `/api/users/$id/classes`

Feldname	Datentyp	Beschreibung

Tabelle 3.16: 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 3.17: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.29* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

3.4.5.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Gibt für den per ID ausgewählten Benutzer im Kontext des Anfragenden Benutzers

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

Tabelle 3.18: Zugelassene Operationen auf `/api/users/$id/subjects`

eine Liste mit Schulfächern für den ausgewählten Benutzer zurück. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.9*. Die einzelnen Felder der Antwort werden in *Tabelle 3.30* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.31* entnommen werden.

```

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

```

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

Feldname	Datentyp	Beschreibung

Tabelle 3.19: 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 3.20: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.32* 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 3.21: 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. Für diese Daten gelten die Einschränkungen die durch den Kontext des anfragenden Benutzers gegeben sind.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.10*. Die einzelnen Felder der Antwort werden in *Tabelle 3.33* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.34* entnommen werden.

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

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

Feldname	Datentyp	Beschreibung

Tabelle 3.22: 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	

Tabelle 3.23: Berechtigungen auf dem Endpunkt

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

Tabelle 3.23: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.35* 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 3.24: 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. Dies geschieht im Kontext der Informationen die der anfragende Nutzer sehen darf.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.11*. Die einzelnen Felder der Antwort werden in *Tabelle 3.36* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.37* entnommen werden.

```

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

```

Listing 3.8: JSON-Antwort für einen GET-Aufruf der Route /api/user/\$id/guardians

Feldname	Datentyp	Beschreibung

Tabelle 3.25: 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 3.26: Berechtigungen auf dem Endpunkt

3.5 Schnittstellen für Schulfächer an Schulen

Ein Schulfach ist eine Unterrichtseinheit, welche in einem Schuljahr oder Halbjahr stattfindet und an eine Schule gebunden ist. In der Regel ist ein einer Jahrgangsstufe zugeordnet, es kann aber auch mehreren Jahrgangsstufe zugeordnet sein wenn es sich um ein Jahrgangsstufenübergreifendes Unterrichtseinheit handelt. Des weiteren hat ein Schulfach immer eine liste an Teilnehmenden Schülern und welche Lehre. Dazu können noch Informationen kommen welche Klassen an diesen Fach teilnehmen. Weiter Optionale Informationen zu einen Schulfach sind angaben über den Stundenplan, wie an welchen Tagen, zu welcher Uhrzeit, wie Lange und in welchen Rhythmus das Fach stattfindet.

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

Die *Tabelle 3.38* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

3.5.1.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Es werden nur die IDs der Daten Präsentiert die für den Anfragen Benutzer in seinen Kontext existieren.

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

Tabelle 3.27: Zugelassene Operationen auf /api/subjects

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.12*. Die einzelnen Felder der Antwort werden in *Tabelle 3.39* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.40* entnommen werden.

```

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

```

Listing 3.9: JSON-Antwort für einen GET-Aufruf der Route /api/subjects

Feldname	Datentyp	Beschreibung

Tabelle 3.28: 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 3.29: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.41* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

3.5.2.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Diese Route gibt bei einer READ Anfrage für das per ID ausgewählt Unterrichtsfach die Allgemeinen Informationen davon wieder. Die Daten welche wieder gegeben werden sind durch den Kontext des anfragenden Benutzers eingeschränkt.

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

Tabelle 3.30: Zugelassene Operationen auf `/api/subjects/$id`

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.13*. Die einzelnen Felder der Antwort werden in *Tabelle 3.42* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.43* entnommen werden.

```

1 {
2   subject: "<STRING>",
3   name: "<STRING>",
4   subject_ref: "<STRING>",
5   school: "<STRING>",
6   school-year: "<STRING>",
7   start: "<CALENDARDATE>",
8   end: "<CALENDARDATE>",
9 }

```

Listing 3.10: JSON-Antwort für einen GET-Aufruf der Route `/api/subjects/$id`

Feldname	Datentyp	Beschreibung

Tabelle 3.31: 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 3.32: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.44* 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 3.33: 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. Diese Route gibt bei einem READ eine List von Klassen IDs wieder welche den per ID ausgewählten Unterrichtsfach zugeordnet sind. Für die Daten gilt das diese anhand des Kontextes des Anfragenden Users Einschränkungen unterliegen.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.14*. Die einzelnen Felder der Antwort werden in *Tabelle 3.45* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.46* entnommen werden.

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

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

Feldname	Datentyp	Beschreibung

Tabelle 3.34: 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 3.35: Berechtigungen auf dem Endpunkt

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

Tabelle 3.35: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.47* 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 3.36: Zugelassene Operationen auf /api/subjects/\$id/students

3.5.4.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Eine READ Anfrage auf diese Route gibt eine Liste mit Objekten welche Schüler von wann bis wann an den per ID ausgewählten Unterrichtsfaches teilgenommen hat wieder. Die Daten werden durch den Kontext des anfragenden Benutzers eingeschränkt.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.15*. Die einzelnen Felder der Antwort werden in *Tabelle 3.48* beschrieben. Die Berechtigungen auf den Endpoint können *Tabelle 3.49* entnommen werden.

```

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

```

Listing 3.12: JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id/students

Feldname	Datentyp	Beschreibung

Tabelle 3.37: 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 3.38: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.50* 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 3.39: Zugelassene Operationen auf /api/subjects/\$id/teachers

3.5.5.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Bei einen READ auf diese Route wird eine Liste von Objekten mit Metainformationen zu den Unterrichtenden Lehren des per ID ausgewählten Unterrichtsfaches zurückgegeben. Für die Daten gilt das diese anhand des Kontextes des Anfragenden Users Einschränkungen unterliegen.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.16*. Die einzelnen Felder der Antwort werden in Tabelle *Tabelle 3.51* beschrieben. Die Berechtigungen auf den Endpoint können *Tabelle 3.52* entnommen werden.

```

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

```

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

Feldname	Datentyp	Beschreibung

Tabelle 3.40: 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 3.41: Berechtigungen auf dem Endpunkt

3.5.6 Endpunkt in der REST-API: `/api/subjects/$id/timetable`

Die *Tabelle 3.53* 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 3.42: Zugelassene Operationen auf `/api/subjects/$id/timetable`

3.5.6.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Es werden für das per ID ausgewählte Unterrichtsfach die Daten zu für den Stundenplan ausgegeben. Die Daten sind durch den Kontext des Anfragenden Users eingeschränkt.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.17*. Die einzelnen Felder der Antwort werden in Tabelle *Tabelle 3.54* beschrieben. Die Berechtigungen auf den Endpoint können *Tabelle 3.55* 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 3.14: JSON-Antwort für einen GET-Aufruf der Route `/api/subjects/$id/timetable`

Feldname	Datentyp	Beschreibung

Tabelle 3.43: 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	

Tabelle 3.44: Berechtigungen auf dem Endpoint

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

Tabelle 3.44: Berechtigungen auf dem Endpunkt

3.6 Schnittstellen für Klassen

Muss noch überarbeitet werden!

- Soll für aktiven Benutzer bei Dreieckern aufrufen nur liste von sein Klassen die er grade sehen kann wieder geben.
- Verhalten für anfrage mit ID muss noch bestimmt werden.
- Datenmodel muss noch gemacht werden.
- Filtermöglichkeiten müssen diskutiert und beschrieben werden.

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	Liste der abgestimmten Referenzschulfächer	11
3.2	Zugelassene Operationen auf /api/school-subjects	11
3.3	Beschreibung der Felder in einem JSON-Objekt für ein Schulfach	12
3.4	Berechtigungen auf dem Endpunkt	12
3.5	Zugelassene Operationen auf /api/school-years	13
3.6	Zugelassene Operationen auf /api/schools	13
3.7	Zugelassene Operationen auf /api/schools/\$id	13
3.8	Zugelassene Operationen auf /api/schools/\$id/users	14
3.9	Beschreibung der Felder in einem JSON-Objekt für einen Benutzer an einer Schule	15
3.10	Berechtigungen auf dem Endpunkt	15
3.10	Berechtigungen auf dem Endpunkt	16
3.11	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	17
3.12	Berechtigungen auf dem Endpunkt	18
3.13	Zugelassene Operationen auf /api/schools/\$id/classes	18
3.14	Zugelassene Operationen auf /api/schools/\$id/subjects	19
3.15	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	19
3.16	Berechtigungen auf dem Endpunkt	19
3.17	Zugelassene Operationen auf /api/users	20
3.18	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	20
3.19	Berechtigungen auf dem Endpunkt	20
3.19	Berechtigungen auf dem Endpunkt	21
3.20	Zugelassene Operationen auf /api/users/\$id	21
3.21	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	22
3.22	Berechtigungen auf dem Endpunkt	22
3.23	Zugelassene Operationen auf /api/users/\$id/assignments	22

3.24	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule	23
3.25	Berechtigungen auf dem Endpunkt	23
3.26	Zugelassene Operationen auf /api/users/\$id/classes	24
3.27	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule	24
3.28	Berechtigungen auf dem Endpunkt	24
3.28	Berechtigungen auf dem Endpunkt	25
3.29	Zugelassene Operationen auf /api/users/\$id/subjects	25
3.30	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule	25
3.31	Berechtigungen auf dem Endpunkt	26
3.32	Zugelassene Operationen auf /api/users/\$id/childs	26
3.33	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule	27
3.34	Berechtigungen auf dem Endpunkt	27
3.35	Zugelassene Operationen auf /api/users/\$id/guardians	27
3.36	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule	28
3.37	Berechtigungen auf dem Endpunkt	28
3.38	Zugelassene Operationen auf /api/subjects	29
3.39	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule	29
3.40	Berechtigungen auf dem Endpunkt	29
3.40	Berechtigungen auf dem Endpunkt	30
3.41	Zugelassene Operationen auf /api/subjects/\$id	30
3.42	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule	31
3.43	Berechtigungen auf dem Endpunkt	31
3.44	Zugelassene Operationen auf /api/subjects/\$id/classes	31
3.45	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule	32
3.46	Berechtigungen auf dem Endpunkt	32
3.47	Zugelassene Operationen auf /api/subjects/\$id/students	33
3.48	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule	33
3.49	Berechtigungen auf dem Endpunkt	33
3.49	Berechtigungen auf dem Endpunkt	34
3.50	Zugelassene Operationen auf /api/subjects/\$id/teachers	34
3.51	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzers in einer Rolle zu einer Schule	35
3.52	Berechtigungen auf dem Endpunkt	35
3.53	Zugelassene Operationen auf /api/subjects/\$id/timetable	35

3.54	Beschreibung der Felder in einem JSON-Objekt für den Stundenplan eines Schulfachs	36
3.55	Berechtigungen auf dem Endpunkt	36
3.56	Zugelassene Operationen auf /api/classes/	37
3.57	Zugelassene Operationen auf /api/classes/\$id	37
3.58	Zugelassene Operationen auf /api/classes/\$id/schools	37
3.59	Zugelassene Operationen auf /api/classes/\$id/subjects	38
3.60	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 . . .	12
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	17
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	28
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	32
3.15	JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id/students	33
3.16	JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id/teachers	34
3.17	JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id/timetable	36