

Inhaltsverzeichnis

0.1	Datenmodell-Beispiele	1
0.1.1	Benutzer (Datenmodelle)	1
1	Einleitung und Vorüberlegungen	11
1.1	Benutzerrollen	11
2	Autorisierung und Authentifizierung	13
2.1	OAuth2	13
2.2	OpenID Connect	14
2.3	Einschränkung der Daten	14
3	REST-API-Definition	16
3.1	Schnittstellen für Schulfächer	16
3.1.1	Endpunkt in der REST-API: /api/school-subjects	16
3.1.1.1	READ	16
3.2	Schnittstellen für Schuljahre	17
3.2.1	Endpunkt in der REST-API: /api/school-years	18
3.3	Schnittstellen für Schulen	18
3.3.1	Endpunkt in der REST-API: /api/schools	18
3.3.1.1	READ	19
3.3.2	Endpunkt in der REST-API: /api/schools/\$id	19
3.3.2.1	READ	20
3.3.3	Endpunkt in der REST-API: /api/schools/\$id/users	21
3.3.3.1	READ	21
3.3.4	Endpunkt in der REST-API: /api/schools/\$id/classes	22
3.3.4.1	READ	22
3.3.5	Endpunkt in der REST-API: /api/schools/\$id/subjects	24
3.3.5.1	READ	24
3.4	Schnittstellen für Benutzer	25
3.4.1	Endpunkt in der REST-API: /api/users	25
3.4.1.1	READ	25
3.4.2	Endpunkt in der REST-API: /api/users/\$id	26
3.4.2.1	READ	26
3.4.3	Endpunkt in der REST-API: /api/users/\$id/assignments	27
3.4.3.1	READ	27
3.4.4	Endpunkt in der REST-API: /api/users/\$id/classes	29
3.4.4.1	READ	29

3.4.5	Endpunkt in der REST-API: /api/users/\$id/subjects	30
3.4.5.1	READ	30
3.4.6	Endpunkt in der REST-API: /api/users/\$id/childs	31
3.4.6.1	READ	31
3.4.7	Endpunkt in der REST-API: /api/users/\$id/guardians	32
3.4.7.1	READ	32
3.5	Schnittstellen für Schulfächer an Schulen	34
3.5.1	Endpunkt in der REST-API: /api/subjects	34
3.5.1.1	READ	34
3.5.2	Endpunkt in der REST-API: /api/subjects/\$id	35
3.5.2.1	READ	35
3.5.3	Endpunkt in der REST-API: /api/subjects/\$id/classes	36
3.5.3.1	READ	37
3.5.4	Endpunkt in der REST-API: /api/subjects/\$id/students	37
3.5.4.1	READ	38
3.5.5	Endpunkt in der REST-API: /api/subjects/\$id/teachers	39
3.5.5.1	READ	39
3.5.6	Endpunkt in der REST-API: /api/subjects/\$id/timetable	40
3.5.6.1	READ	40
3.6	Schnittstellen für Klassen	41
3.6.1	Endpunkt in der REST-API: /api/classes/\$id	42
3.6.1.1	READ	42
3.6.2	Endpunkt in der REST-API: /api/classes/\$id/subjects	43
3.6.2.1	READ	43
3.6.3	Endpunkt in der REST-API: /api/classes/\$id/students	44
3.6.3.1	READ	44
3.6.4	Endpunkt in der REST-API: /api/classes/\$id/teachers	46
3.6.4.1	READ	46
3.6.5	Endpunkt in der REST-API: /api/classes/\$id/representatives	48
3.6.5.1	READ	48
4	Weiterführende Konzepte	50
4.1	Löschkonzept	50
	Literaturverzeichnis	51
	Abbildungsverzeichnis	52
	Tabellenverzeichnis	53
	Listings	56

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 {
2     class: "KLASSE-01",
3     name: "Klasse 1-A",
4     school: "SCHULE-01",
5     school-year: "SJ-09/10",
6     start: "01-09-2009",
7     end: "31-08-2010",
8     grade: [ "1", ],
9     subjects: [ "SUBJECT-0001", "SUBJECT-0003", "SUBJECT-0004", ],
10    students: [
11    {

```

```

12     user: "USER-01",
13 }, {
14     user: "USER-06",
15 }, {
16     user: "USER-07",
17     end: "31-12-2009",
18 }, {
19     user: "USER-10",
20 }, {
21     user: "USER-11",
22 },
23 ],
24 teachers: [
25     {
26         user: "USER-208",
27         order: [
28             {
29                 order: "1",
30             },
31         ],
32     }, {
33         user: "USER-209",
34         order: [
35             {
36                 order: "2",
37             },
38         ],
39     },
40 ],
41 representatives: [
42     {
43         user: "USER-10",
44         role: "student",
45         order: "1",
46     }, {
47         user: "USER-07",
48         end: "31-12-2009",
49         role: "student",
50         order: "2",
51     }, {
52         user: "USER-01",
53         start: "04-01-2010",
54         role: "student",
55         order: "2",
56     }, {
57         user: "USER-114",
58         role: "guardian",
59         order: "1",
60     }, {
61         user: "USER-115",
62         role: "guardian",
63         order: "2",
64     },

```



```
65 ]  
66 }
```

Listing 4: Klassen-Datenmodell Beispiel 2: Grundschulklasse

```
1 {  
2   class: "KLASSE-11",  
3   name: "Jarganstuffe 11",  
4   school: "SCHULE-04",  
5   school-year: "SJ-20/21",  
6   start: "01-09-2020",  
7   end: "31-08-2021",  
8   grade: [ "11", ],  
9   subjects: [ ],  
10  students: [  
11    {  
12      user: "USER-01",  
13    }, {  
14      user: "USER-30",  
15    }, {  
16      user: "USER-31",  
17    }, {  
18      user: "USER-32",  
19    }, {  
20      user: "USER-33",  
21    },  
22  ],  
23  teachers: [  
24    {  
25      user: "USER-228",  
26      end: "14-01-2021",  
27      order: [  
28        {  
29          order: "1",  
30          end: "14-01-2021",  
31        },  
32      ],  
33    }, {  
34      user: "USER-229",  
35      order: [  
36        {  
37          order: "2",  
38          end: "14-01-2021",  
39        }, {  
40          order: "1",  
41          start: "15-01-2021",  
42        },  
43      ], {  
44        user: "USER-230",  
45        start: "15-01-2021",  
46        order: [  
47          {  
48            order: "2",  
49            start: "15-01-2021",
```

```

50     },
51   ],
52 },
53 ],
54 representatives: [
55   {
56     user: "USER-01",
57     role: "student",
58     order: "1",
59   }, {
60     user: "USER-31",
61     role: "student",
62     order: "2",
63   }, {
64     user: "USER-141",
65     start: "10-09-2020",
66     role: "guardian",
67     order: "1",
68   }, {
69     user: "USER-142",
70     start: "10-09-2020",
71     role: "guardian",
72     order: "2",
73   },
74 ]
75 }

```

Listing 5: Klassen-Datenmodell Beispiel 2: Jahrgangstufe 11, Sekundarstufe 2

```

1 {
2   class: "KLASSE-21",
3   name: "Klasse 3,4 A",
4   school: "SCHULE-07",
5   school-year: "SJ-15/16",
6   start: "01-09-2015",
7   end: "31-08-2016",
8   grade: [ "3", "4", ],
9   subjects: [ "SUBJECT-0101", "SUBJECT-0102", "SUBJECT-0103", ],
10  students: [
11    {
12      user: "USER-51",
13    }, {
14      user: "USER-52",
15    }, {
16      user: "USER-53",
17    }, {
18      user: "USER-55",
19    }, {
20      user: "USER-54",
21      start: "01-03-2016",
22    },
23  ],
24  teachers: [
25    {

```

```

26     user: "USER-256",
27     order: [
28       {
29         order: "1",
30       },
31     ],
32   }, {
33     user: "USER-257",
34     order: [
35       {
36         order: "1",
37       },
38     ],
39   }, {
40     user: "USER-258",
41     order: [
42       {
43         order: "2",
44       },
45     ],
46   },
47 ],
48 representatives: [
49   {
50     user: "USER-55",
51     role: "student",
52     order: "1",
53   }, {
54     user: "USER-52",
55     role: "student",
56     order: "2",
57   }, {
58     user: "USER-158",
59     start: "10-09-2015",
60     role: "guardian",
61     order: "1",
62   }, {
63     user: "USER-159",
64     start: "10-09-2015",
65     role: "guardian",
66     order: "2",
67   },
68 ]
69 }

```

Listing 6: Klassen-Datenmodell Beispiel 3: Jahrgangsübergreifende Klasse

```

1 {
2   school: "SCHULE-01",
3   name: "Zobel Grundschule",
4   classes: [
5     {
6       class: "KLASSE-0001",
7       start: "01-09-2020",

```

```

8     end: "31-08-2021",
9 }, {
10    class: "KLASSE-0002",
11    start: "01-09-2010",
12    end: "31-08-2011",
13 }, {
14    class: "KLASSE-0003",
15    start: "01-09-2010",
16    end: "31-08-2011",
17 },
18 ],
19 users: [
20   {
21     user: "USER-02",
22     role: "guardians",
23     start: "01-09-2009",
24     end: "31-08-2016",
25     school-years: ["SJ-09/10", "SJ-10/11", "SJ-11/12", "SJ-13/14", "SJ-14/15",
26                   "SJ-15/16"],
27   }, {
28     user: "USER-01",
29     role: "students",
30     start: "01-09-2009",
31     end: "31-08-2016",
32     school-years: ["SJ-09/10", "SJ-10/11", "SJ-11/12", "SJ-13/14", "SJ-14/15",
33                   "SJ-15/16"],
34   }, {
35     user: "USER-208",
36     role: "teacher",
37     start: "01-09-2001",
38   }, {
39     user: "USER-209",
40     role: "teacher",
41     start: "01-09-2007",
42   },
43 ],
44 subjects: [
45   {
46     subject: "SUBJECT-0001",
47     start: "01-09-2009",
48     end: "28-02-2010",
49   }, {
50     subject: "SUBJECT-0101",
51     start: "01-09-2009",
52     end: "28-02-2010",
53   },
54 ],
55 ]

```

Listing 7: Schulen-Datenmodell Beispiel 1

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.

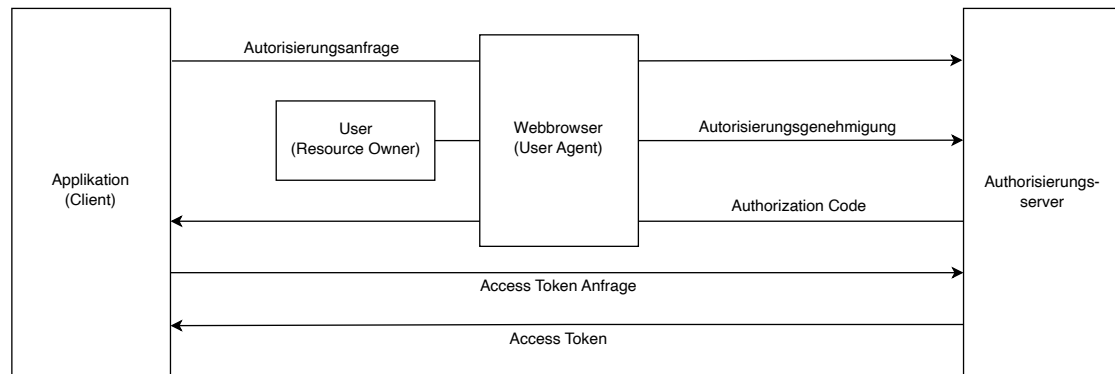


Abbildung 2.1: Ablauf des Authentication Code Grant

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 Autosierungsvorgang 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 Gesamtmenge aller abgestimmten Referenzschulfächer kann *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!***

- Datenmodell muss 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 direktem Aufruf nur die Liste von sein Schulen, die er gerade sehen kann, wiedergeben.
- Verhalten für Anfrage mit ID muss noch bestimmt werden.
- Datenmodell muss noch gemacht werden.
- Filtermöglichkeiten müssen diskutiert und beschrieben werden.

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

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	GET
UPDATE	Nein	
DELETE	Nein	

Tabelle 3.6: Zugelassene Operationen auf /api/schools

3.3.1.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Der Endpunkt gibt eine Liste mit allen Schul-IDs aus die es im System gibt und für die Daten unter `/api/schools/$id` abgerufen werden können

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.2*. Die einzelnen Felder der Antwort werden in *Tabelle 3.7* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.8* entnommen werden.

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

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

Feldname	Datentyp	Beschreibung
	STRING	Eindeutiger Identifikations String der Schule im IDM, womit unter <code>/api/schools/\$id</code> die Schule abgerufen werden kann.

Tabelle 3.7: Beschreibung des Felder in eine JSON-Objekt was die Schul-IDs wieder gibt

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

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

Die *Tabelle 3.9* 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 3.9: Zugelassene Operationen auf /api/schools/\$id

3.3.2.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Diese Route gib für die per ID ausgewählte Schule die Stammdaten zurück.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.3*. Die einzelnen Felder der Antwort werden in *Tabelle 3.10* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.11* entnommen werden.

```

1 {
2   school: "<STRING>",
3   name: "<STRING>",
4 }
```

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

Feldname	Datentyp	Beschreibung
school	STRING	Eindeutiger Identifikations String der Schule im IDM
name	STRING	Name der Schule

Tabelle 3.10: 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	

Tabelle 3.11: Berechtigungen auf dem Endpunkt

Benutzergruppen	Zugelassene Daten
sync-systems	

Tabelle 3.11: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.12* 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 3.12: 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. Dieser Endpunkt listet die Informationen über Benutzer und Ihre Rollen an der Schule auf. Für jede Kombination aus Benutzer, Rolle und ab wann gibt es eine extra Eintrag in der Liste die Zurückgegeben wird. Bei manchen Kombinationen gibt es zudem noch ein Datum biss wann der Benutzer die Rolle innen hatte. Zudem kann es bei einigen Rollen noch die Zusatzinformation geben in welche Schuljahren der User die Rolle innen hatte.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.4*. Die einzelnen Felder der Antwort werden in *Tabelle 3.13* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.14* entnommen werden.

```

1  [
2  {
3    user: "<STRING>",
4    role: "<STRING>",
5    start: "<CALENDARDATE>",
6    end: "<CALENDARDATE>",
7    school-years: ["<STRING>"', ...],
8  },
9  ...
10 ]

```

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

Feldname	Datentyp	Beschreibung
user	STRING	Zeichenkette welche eine ID von einen Benutzer ist, was unter /api/subjects/\$id abgerufen werden kann.
role	STRING	Rolle die der Benutzer innen hat.
start	CALENDARDATE	Ab welchem Tag der Benutzer die Rolle innen hat
end	CALENDARDATE	Optional; Gibt an bis zu welchen Tag der Benutzer die Rolle innen hatte.
school-years	Liste	Optional; Liste mit von Zeichenketten, welche Referenzen auf Schuljahre sind die unter /api/school-years/\$id abgerufen werden können.

Tabelle 3.13: 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 3.14: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.15* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

3.3.4.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Der Endpunkt gibt eine Liste von Referenz-IDs für Klassen an der Schule zurück welche unter /api/classes/\$id abgerufen werden können.

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

Tabelle 3.15: Zugelassene Operationen auf `/api/schools/$id/classes`

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.5*. Die einzelnen Felder der Antwort werden in *Tabelle 3.16* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.17* entnommen werden.

```

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

```

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

Feldname	Datentyp	Beschreibung
	STRING	Zeichenkette welche eine ID von einer Klasse ist, was unter <code>/api/classes/\$id</code> abgerufen werden kann.

Tabelle 3.16: Beschreibung der Felder in einem JSON-Objekt, welches die Klassen an einer Schule repräsentiert.

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

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

Die *Tabelle 3.18* 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 3.18: 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. Der Endpunkt gibt eine Liste von Referenz-IDs für Unterrichtsfächern zurück, welche unter /api/subjects/\$id abgerufen werden können.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.6*. Die einzelnen Felder der Antwort werden in *Tabelle 3.19* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.20* entnommen werden.

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

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

Feldname	Datentyp	Beschreibung
	STRING	Zeichenkette, welche eine ID von einem Unterrichtsfach ist, was unter /api/subjects/\$id abgerufen werden kann.

Tabelle 3.19: Beschreibung der Felder in einem JSON-Objekt, welches die Unterrichtsfächer an einer Schule repräsentieren

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

Tabelle 3.20: Berechtigungen auf dem Endpunkt

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

Tabelle 3.20: Berechtigungen auf dem Endpunkt

3.4 Schnittstellen für Benutzer

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

Die *Tabelle 3.21* 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

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 3.7*. Die einzelnen Felder der Antwort werden in *Tabelle 3.22* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.23* entnommen werden.

```

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

Listing 3.7: JSON-Antwort für einen GET-Aufruf der Route /api/users

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	
teacher	
principal	
school-admin	
school-board	
fed-school-board	
sync-systems	

Tabelle 3.23: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.24* 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 3.24: 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 dem sich der anfragende Benutzer befinden.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.8*. Die einzelnen Felder der Antwort werden in *Tabelle 3.25* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.26* entnommen werden.

```

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

```

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

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

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

Die *Tabelle 3.27* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

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

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

Tabelle 3.27: Zugelassene Operationen auf /api/users/\$id/assignments

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

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.9*. Die einzelnen Felder der Antwort werden in *Tabelle 3.28* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.29* entnommen werden.

```

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

```

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

Feldname	Datentyp	Beschreibung

Tabelle 3.28: 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	

Tabelle 3.29: Berechtigungen auf dem Endpunkt

Benutzergruppen	Zugelassene Daten
sync-systems	

Tabelle 3.29: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.30* 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 3.30: 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 3.10*. Die einzelnen Felder der Antwort werden in *Tabelle 3.31* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.32* 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 3.10: JSON-Antwort für einen GET-Aufruf der Route /api/users/\$id/classes

Feldname	Datentyp	Beschreibung

Tabelle 3.31: 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 3.32: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.33* 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 3.33: 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. Gibt für den per ID ausgewählten Benutzer im Kontext des anfragenden Benutzers eine Liste mit Schulfächern für den ausgewählten Benutzer zurück. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.11*. Die einzelnen Felder der Antwort werden in *Tabelle 3.34* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.35* entnommen werden.

```

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

```

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

Feldname	Datentyp	Beschreibung

Tabelle 3.34: 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 3.35: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.36* 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 3.36: 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 3.12*. Die einzelnen Felder der Antwort werden in *Tabelle 3.37* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.38* entnommen werden.

```

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

```

Listing 3.12: JSON-Antwort für einen GET-Aufruf der Route `/api/users/$id/childs`

Feldname	Datentyp	Beschreibung

Tabelle 3.37: 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 3.38: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.39* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

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.

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

Tabelle 3.39: Zugelassene Operationen auf `/api/users/$id/guardians`

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.13*. Die einzelnen Felder der Antwort werden in *Tabelle 3.40* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.41* entnommen werden.

```

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

```

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

Feldname	Datentyp	Beschreibung

Tabelle 3.40: 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 3.41: 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 es einer Jahrgangsstufe zugeordnet, es kann aber auch mehreren Jahrgangsstufen zugeordnet sein, wenn es sich um eine jahrgangsstufenübergreifende Unterrichtseinheit handelt. Des Weiteren hat ein Schulfach immer eine Liste an teilnehmenden Schülern und Lehrkräften. Dazu können noch Informationen kommen, welche Klassen an diesen Fach teilnehmen. Weitere optionale Informationen zu einem Schulfach sind Angaben über den Stundenplan, an welchen Tagen, zu welcher Uhrzeit, wie lange und in welchem Rhythmus das Fach stattfindet.

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

Die *Tabelle 3.42* 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 3.42: 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. Es werden nur die IDs der Daten präsentiert, die für den anfragenden Benutzer in seinem Kontext existieren.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.14*. Die einzelnen Felder der Antwort werden in *Tabelle 3.43* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.44* entnommen werden.

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

Listing 3.14: JSON-Antwort für einen GET-Aufruf der Route /api/subjects

Feldname	Datentyp	Beschreibung

Tabelle 3.43: Beschreibung der Felder in eine 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 3.44: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.45* 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 3.45: 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. Diese Route gibt bei einer READ-Anfrage für das per ID ausgewählte Unterrichtsfach die allgemeinen Informationen davon wieder. Die Daten, welche wiedergegeben werden, sind 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 3.46* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.47* 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 3.15: JSON-Antwort für einen GET-Aufruf der Route `/api/subjects/$id`

Feldname	Datentyp	Beschreibung

Tabelle 3.46: 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 3.47: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.48* 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 3.48: 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 einer READ-Anfrage eine Liste von Klassen-IDs wieder, welche dem per ID ausgewählten Unterrichtsfach zugeordnet sind. Für die Daten gilt, dass 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 3.49* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.50* entnommen werden.

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

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

Feldname	Datentyp	Beschreibung

Tabelle 3.49: 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 3.50: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.51* 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 3.51: 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 dem per ID ausgewählten Unterrichtsfach teilgenommen haben, wieder. Die Daten werden durch den Kontext des anfragenden Benutzers eingeschränkt.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.17*. Die einzelnen Felder der Antwort werden in Tabelle *Tabelle 3.52* beschrieben. Die Berechtigungen auf den Endpoint können *Tabelle 3.53* 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/students`

Feldname	Datentyp	Beschreibung

Tabelle 3.52: 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	

Tabelle 3.53: Berechtigungen auf dem Endpoint

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

Tabelle 3.53: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.54* 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 3.54: 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 einer READ-Abfrage auf diese Route wird eine Liste von Objekten mit Metainformationen zu den unterrichtenden Lehrkräften des per ID ausgewählten Unterrichtsfaches zurückgegeben. Für die Daten gilt, dass diese anhand des Kontextes des anfragenden Users Einschränkungen unterliegen.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.18*. Die einzelnen Felder der Antwort werden in *Tabelle 3.55* beschrieben. Die Berechtigungen auf den Endpoint können *Tabelle 3.56* entnommen werden.

```

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

```

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

Feldname	Datentyp	Beschreibung

Tabelle 3.55: 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 3.56: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.57* 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 3.57: 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 3.19*. Die einzelnen Felder der Antwort werden in Tabelle *Tabelle 3.58* beschrieben. Die Berechtigungen auf den Endpoint können *Tabelle 3.59* 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 3.19: JSON-Antwort für einen GET-Aufruf der Route
/api/subjects/\$id/timetable

Feldname	Datentyp	Beschreibung

Tabelle 3.58: Beschreibung der Felder in einem JSON-Objekt für den Stundenplan eines Schulfachs

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 3.59: Berechtigungen auf dem Endpunkt

3.6 Schnittstellen für Klassen

Muss noch überarbeitet werden!

- Soll für aktiven Benutzer bei direktem Aufruf nur die Liste von seinen Klassen, die er gerade sehen kann, wiedergeben.
- Verhalten für Anfrage mit ID muss noch bestimmt werden.
- Datenmodel muss noch gemacht werden.
- Filtermöglichkeiten müssen diskutiert und beschrieben werden.

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

Die *Tabelle 3.60* 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 3.60: Zugelassene Operationen auf /api/classes/\$id

3.6.1.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Bei Anfragen an diesen Endpunkt werden die allgemeinen Daten einer Klasse ausgegeben.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.20*. Die einzelnen Felder der Antwort werden in *Tabelle 3.61* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.62* entnommen werden.

```

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

```

Listing 3.20: JSON-Antwort für einen GET-Aufruf der Route /api/classes/\$id

Feldname	Datentyp	Beschreibung
class	STRING	ID der Klasse im System.

Tabelle 3.61: Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

Feldname	Datentyp	Beschreibung
name	STRING	Name der Klasse, welche zum Anzeigen verwendet wird.
school	STRING	ID, zu welcher Schule die Klasse gehört.
school-year	STRING	Schuljahr, in welchem die Klasse existiert.
start	CALENDARDATE	Zeitpunkt, ab wann das Klassenobjekt existiert, falls dies abweichend zum Startzeitpunkt des Schuljahres ist.
end	CALENDARDATE	Zeitpunkt, bis wann das Klassenobjekt existiert, falls dies abweichend zum Endzeitpunkt des Schuljahres ist.
grade	List of STRINGs	Enthält eine Liste von Klassenstufen von Schülern in dieser Klasse.

Tabelle 3.61: 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 3.62: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.63* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

3.6.2.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Bei Anfragen an diesen Endpunkt wird eine Liste von Fächern, welcher dieser Klasse zugeordnet ist, aufgelistet.

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

Tabelle 3.63: Zugelassene Operationen auf `/api/classes/$id/subjects`

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.21*. Die einzelnen Felder der Antwort werden in *Tabelle 3.64* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.65* entnommen werden.

```

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

```

Listing 3.21: JSON-Antwort für einen GET-Aufruf der Route `/api/classes/$id/subjects`

Feldname	Datentyp	Beschreibung

Tabelle 3.64: 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 3.65: Berechtigungen auf dem Endpunkt

3.6.3 Endpunkt in der REST-API: `/api/classes/$id/students`

Die *Tabelle 3.66* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

3.6.3.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Bei Anfragen an diesen Endpunkt wird eine Liste von IDs von Schülern, die in der Klasse sind, zurückgegeben. Optional ist der Eintritts- sowie der Austrittszeitpunkt. Diese Felder werden gesetzt, falls ein Schüler nicht über den kompletten Zeitraum Teil der Klasse war.

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

Tabelle 3.66: Zugelassene Operationen auf `/api/classes/$id/students`

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.22*. Die einzelnen Felder der Antwort werden in *Tabelle 3.67* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.68* entnommen werden.

```

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

```

Listing 3.22: JSON-Antwort für einen GET-Aufruf der Route `/api/classes/$id/students`

Feldname	Datentyp	Beschreibung
user	STRING	Die User-ID des Schülers
start	CALENDARDATE	Optional; wird gesetzt, falls ein Schüler später zu eine Klasse hinzugefügt wird.
end	CALENDARDATE	Optional; wird gesetzt, falls ein Schüler früher aus einer Klasse genommen wird.

Tabelle 3.67: 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 3.68: Berechtigungen auf dem Endpunkt

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

Tabelle 3.68: Berechtigungen auf dem Endpunkt

3.6.4 Endpunkt in der REST-API: /api/classes/\$id/teachers

Die *Tabelle 3.69* 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 3.69: Zugelassene Operationen auf /api/classes/\$id/teachers

3.6.4.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Bei Anfragen an diesen Endpunkt wird eine Liste von IDs von Klassenlehrern zurückgegeben, die der Klasse als Klassenlehrer zugeordnet sind. Optional ist der Eintritts- sowie Austrittszeitpunkt. Diese Felder werden gesetzt, falls der Klassenlehrer dies nicht über den kompletten Zeitraum der Klasse war.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.23*. Die einzelnen Felder der Antwort werden in *Tabelle 3.70* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.71* entnommen werden.

```

1  [
2  {
3    user: "<STRING>",
4    start: "<CALENDARDATE>",
5    end: "<CALENDARDATE>",
6    order: [
7      {
8        order: "<NUMBER>",
9        start: "<CALENDARDATE>",
10       end: "<CALENDARDATE>",
11      },
12      ...
13    ],
14  },
15  ...
16 ]

```


Listing 3.23: JSON-Antwort für einen GET-Aufruf der Route `/api/classes/$id/teachers`

Feldname	Datentyp	Beschreibung
user	STRING	Die User-ID des Lehrers
start	CALENDARDATE	Optional; wird gesetzt, falls der Lehrer erst während des Zeitraums einer Klasse als Klassenlehrer zugewiesen wird.
end	CALENDARDATE	Optional; wird gesetzt, falls der Lehrer vor Ende des Zeitraums der Klasse nicht mehr der Klasse als Klassenlehrer zugewiesen ist.
order	Object List	Eine Liste mit Objekten, die angibt, welche Position der Lehrer von wann bis wann in der Klasse innehatte. Niedrigere Nummer heißt höhere Position.
order.order	NUMBER	Die Ordnungsnummer, welche angibt welche Position der Lehrer in einer Klasse inne hat. Beginnt immer bei 1. Es können auch mehrere Lehrer dieselbe Nummer haben, falls die Klasse zum Beispiel mehrere gleichberechtigte Klassenlehrer hat.
order.start	CALENDARDATE	Optional; Zeitpunkt, ab dem der Lehrer die Position innehatte.
order.end	CALENDARDATE	Optional; Zeitpunkt, bis zu dem der Lehrer die Position innehatte.

Tabelle 3.70: Beschreibung der Felder in einem JSON-Objekt aus der Liste der Lehrer

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

Tabelle 3.71: Berechtigungen auf dem Endpunkt

3.6.5 Endpunkt in der REST-API: /api/classes/\$id/representatives

Die *Tabelle 3.72* 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 3.72: Zugelassene Operationen auf /api/classes/\$id/representatives

3.6.5.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Bei Anfragen an diesen Endpunkt wird eine Liste von Schülern oder Vormündern, welche in einer Klasse oder Jahrgangsstufe die Statusgruppe repräsentieren, zurückgegeben. Die Position wird durch eine Ordnungsnummer widerspiegelt. Je kleiner die Nummer, desto wichtiger der Repräsentant der Statusgruppe. Es können auch mehrere Repräsentanten einer Statusgruppe die gleiche Ordnungsnummer haben. Zusätzlich kann Eintrittszeitpunkt sowie der Austrittszeitpunkt vermerkt werden, falls dieser abweichend zum Zeitraum der Klasse ist.

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.24*. Die einzelnen Felder der Antwort werden in *Tabelle 3.73* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.74* entnommen werden.

```
1  [  
2  {  
3    user: "<STRING>",  
4    role: "<STRING>",  
5    order: "<NUMBER>",  
6    start: "<CALENDARDATE>",  
7    end: "<CALENDARDATE>",  
8  },  
9  ...  
10 ]
```

Listing 3.24: JSON-Antwort für einen GET-Aufruf der Route /api/classes/\$id/representatives

Feldname	Datentyp	Beschreibung
user	STRING	Die User-ID des Repräsentanten der Statusgruppe

Tabelle 3.73: Beschreibung der Felder in einem JSON-Objekt aus der Liste der Lehrer

Feldname	Datentyp	Beschreibung
role	STRING	Die Rolle, welcher der Repräsentant der Statusgruppe im System hat (zugelassen sind student oder guardian).
order	NUMBER	Die Ordnungsnummer, die angibt, welche Position der Repräsentant der Statusgruppe in einer Klasse innehat.
start	CALENDARDATE	Optional; wird benötigt, wenn der Repräsentant der Statusgruppe zu einem abweichenden Zeitpunkt das Amt bekommt.
end	CALENDARDATE	Optional; wird benötigt, wenn der Repräsentant der Statusgruppe vorzeitig vor Ende des Zeitraums der Klasse nicht mehr als Repräsentant der Statusgruppe fungiert.

Tabelle 3.73: Beschreibung der Felder in einem JSON-Objekt aus der Liste der Lehrer

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

Tabelle 3.74: Berechtigungen auf dem Endpunkt

4 Weiterführende Konzepte

4.1 Löschkonzept

Bei Verwendung der in diesem Dokument definierten REST-API muss der Client ein Löschkonzept auf die über die REST-API bezogenen Daten definieren bzw. diesem mit dem IDM-Provider abstimmen.

Der Client hat die Möglichkeit, über ein Benutzerkonto mit der Rolle "sync-system" die im Client vorhandenen Datenobjekte und Referenzen darauf über die REST-API beim IDM-Provider zu revalidieren. Existiert diese Möglichkeit der Rücksynchronisation im Client nicht, so müssen Überlegungen getroffen werden, wann Daten als veraltet gelten und nach welchen Aufbewahrungsfristen diese auf Client-Seite gelöscht werden. Für Benutzerkonten kann ein Kriterium sein, wie lange sich eine Person nicht mehr im Client eingeloggt hat, bevor Maßnahmen getroffen werden, den Datenstand aktuell zu halten (Ankündigung der Deaktivierung/Löschung des Benutzerkontos, Löschung des Benutzerkontos).

Bei Löschung eines Benutzerkontos im Client ist zu prüfen, inwiefern Daten vorliegen, die dem geistigen Eigentum der Inhaberin bzw. des Inhabers des Benutzerkontos unterliegen, und diese für einen definierten Zeitraum nach Löschung des Benutzerkontos durch die Inhaberin bzw. den Inhaber zur Sicherung abrufbar sind.

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	14
-----	--	----

Tabellenverzeichnis

1.1	Benutzerrollen, die im zentralen IDM-System vorgesehen sind	12
2.1	Endpunkte, die durch den IDM-Provider für die Anmeldung per OAuth2 zur Verfügung gestellt werden müssen	13
3.1	Liste der abgestimmten Referenzschulfächer	16
3.2	Zugelassene Operationen auf /api/school-subjects	16
3.3	Beschreibung der Felder in einem JSON-Objekt für ein Schulfach	17
3.4	Berechtigungen auf dem Endpunkt	17
3.5	Zugelassene Operationen auf /api/school-years	18
3.6	Zugelassene Operationen auf /api/schools	18
3.7	Beschreibung der Felder in eine JSON-Objekt was die Schul-IDs wieder gibt	19
3.8	Berechtigungen auf dem Endpunkt	19
3.9	Zugelassene Operationen auf /api/schools/\$id	20
3.10	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	20
3.11	Berechtigungen auf dem Endpunkt	20
3.11	Berechtigungen auf dem Endpunkt	21
3.12	Zugelassene Operationen auf /api/schools/\$id/users	21
3.13	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	22
3.14	Berechtigungen auf dem Endpunkt	22
3.15	Zugelassene Operationen auf /api/schools/\$id/classes	23
3.16	Beschreibung der Felder in eine JSON-Objekt, welches die Klassen an einer Schule repräsentiert.	23
3.17	Berechtigungen auf dem Endpunkt	23
3.18	Zugelassene Operationen auf /api/schools/\$id/subjects	24
3.19	Beschreibung der Felder in eine JSON-Objekt welches die Unterrichtsfächer an einer Schule repräsentieren	24
3.20	Berechtigungen auf dem Endpunkt	24
3.20	Berechtigungen auf dem Endpunkt	25
3.21	Zugelassene Operationen auf /api/users	25
3.22	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	26
3.23	Berechtigungen auf dem Endpunkt	26
3.24	Zugelassene Operationen auf /api/users/\$id	26

3.25	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	27
3.26	Berechtigungen auf dem Endpunkt	27
3.27	Zugelassene Operationen auf /api/users/\$id/assignments	28
3.28	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	28
3.29	Berechtigungen auf dem Endpunkt	28
3.29	Berechtigungen auf dem Endpunkt	29
3.30	Zugelassene Operationen auf /api/users/\$id/classes	29
3.31	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	29
3.32	Berechtigungen auf dem Endpunkt	30
3.33	Zugelassene Operationen auf /api/users/\$id/subjects	30
3.34	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	31
3.35	Berechtigungen auf dem Endpunkt	31
3.36	Zugelassene Operationen auf /api/users/\$id/childs	31
3.37	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	32
3.38	Berechtigungen auf dem Endpunkt	32
3.39	Zugelassene Operationen auf /api/users/\$id/guardians	33
3.40	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	33
3.41	Berechtigungen auf dem Endpunkt	33
3.42	Zugelassene Operationen auf /api/subjects	34
3.43	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	34
3.44	Berechtigungen auf dem Endpunkt	35
3.45	Zugelassene Operationen auf /api/subjects/\$id	35
3.46	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	36
3.47	Berechtigungen auf dem Endpunkt	36
3.48	Zugelassene Operationen auf /api/subjects/\$id/classes	36
3.49	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	37
3.50	Berechtigungen auf dem Endpunkt	37
3.51	Zugelassene Operationen auf /api/subjects/\$id/students	38
3.52	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	38
3.53	Berechtigungen auf dem Endpunkt	38
3.53	Berechtigungen auf dem Endpunkt	39
3.54	Zugelassene Operationen auf /api/subjects/\$id/teachers	39

3.55	Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	40
3.56	Berechtigungen auf dem Endpunkt	40
3.57	Zugelassene Operationen auf /api/subjects/\$id/timetable	40
3.58	Beschreibung der Felder in einem JSON-Objekt für den Stundenplan eines Schulfachs	41
3.59	Berechtigungen auf dem Endpunkt	41
3.60	Zugelassene Operationen auf /api/classes/\$id	42
3.61	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	42
3.61	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	43
3.62	Berechtigungen auf dem Endpunkt	43
3.63	Zugelassene Operationen auf /api/classes/\$id/subjects	44
3.64	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	44
3.65	Berechtigungen auf dem Endpunkt	44
3.66	Zugelassene Operationen auf /api/classes/\$id/students	45
3.67	Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule	45
3.68	Berechtigungen auf dem Endpunkt	45
3.68	Berechtigungen auf dem Endpunkt	46
3.69	Zugelassene Operationen auf /api/classes/\$id/teachers	46
3.70	Beschreibung der Felder in einem JSON-Objekt aus der Liste der Lehrer .	47
3.71	Berechtigungen auf dem Endpunkt	47
3.72	Zugelassene Operationen auf /api/classes/\$id/representatives	48
3.73	Beschreibung der Felder in einem JSON-Objekt aus der Liste der Lehrer .	48
3.73	Beschreibung der Felder in einem JSON-Objekt aus der Liste der Lehrer .	49
3.74	Berechtigungen auf dem Endpunkt	49

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
4	Klassen-Datenmodell Beispiel 2: Grundschulklasse	5
5	Klassen-Datenmodell Beispiel 2: Jahrgangstufe 11, Sekundarstufe 2	7
6	Klassen-Datenmodell Beispiel 3: Jahrgangsübergreifende Klasse	8
7	Schulen-Datenmodell Beispiel 1	9
2.1	Beispielhafter Aufruf des Authorization Endpoints	15
3.1	JSON-Antwort für einen GET-Aufruf der Route /api/school-subjects . . .	17
3.2	JSON-Antwort für einen GET-Aufruf der Route /api/schools	19
3.3	JSON-Antwort für einen GET-Aufruf der Route /api/school/\$id	20
3.4	JSON-Antwort für einen GET-Aufruf der Route /api/schools/\$id/users .	21
3.5	JSON-Antwort für einen GET-Aufruf der Route /api/schools/\$id/classes	23
3.6	JSON-Antwort für einen GET-Aufruf der Route /api/schools/\$id/subjects	24
3.7	JSON-Antwort für einen GET-Aufruf der Route /api/users	25
3.8	JSON-Antwort für einen GET-Aufruf der Route /api/users/\$id	27
3.9	JSON-Antwort für einen GET-Aufruf der Route /api/users/\$id/assignments	28
3.10	JSON-Antwort für einen GET-Aufruf der Route /api/users/\$id/classes . .	29
3.11	JSON-Antwort für einen GET-Aufruf der Route /api/users/\$id/subjects .	30
3.12	JSON-Antwort für einen GET-Aufruf der Route /api/users/\$id/childs . .	32
3.13	JSON-Antwort für einen GET-Aufruf der Route /api/user/\$id/guardians	33
3.14	JSON-Antwort für einen GET-Aufruf der Route /api/subjects	34
3.15	JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id	35
3.16	JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id/classes	37
3.17	JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id/students	38
3.18	JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id/teachers	39
3.19	JSON-Antwort für einen GET-Aufruf der Route /api/subjects/\$id/timetable	41
3.20	JSON-Antwort für einen GET-Aufruf der Route /api/classes/\$id	42
3.21	JSON-Antwort für einen GET-Aufruf der Route /api/classes/\$id/subjects	44
3.22	JSON-Antwort für einen GET-Aufruf der Route /api/classes/\$id/students	45
3.23	JSON-Antwort für einen GET-Aufruf der Route /api/classes/\$id/teachers	46
3.24	JSON-Antwort für einen GET-Aufruf der Route /api/classes/\$id/representatives	48