Inhaltsverzeichnis

0.1 Datenmodell-Beispiele

0.1.1 Benutzer (Datenmodelle)

```
{
 id: "USER-01",
 name: "Leming",
 surename: "Zobel",
 birtdate: "03-01-2003",
 sex: "male",
 assignments: [
 {
  school_id: "SCHULE-01",
  role: "students",
  start: "01-09-2009",
  end: "31-08-2016",
  school-years: ["SJ-09/10","SJ-10/11","SJ-11/12","SJ-13/14","SJ-14/15","
      SJ-15/16"]
 }, {
  school_id: "SCHULE-04",
  role: "students",
  start: "01-09-2016",
  school-years: ["SJ-16/17","SJ-17/18","SJ-18/19","SJ-19/20","SJ-20/21"]
 },{
  school_id: "SCHULE-02",
  role: "external-students",
  start: "01-09-2019",
  end: "31-08-2020",
  school-years: ["SJ-19/20"]
 },
 ],
 guardians: [
 {
  user_id: "USER-02",
  start: "01-09-2009",
  end: "03-01-2020",
 },  {
  user_id: "USER-04",
  start: "01-09-2009",
  end: "03-01-2020",
 }
 ],
 classes: [
  {
   class_id: "KLASSE-0001",
   school_id: "SCHULE-01",
   school-year: "SJ-09/10",
   start: "01-09-2009",
   end: "31-08-2010",
  }, {
   class_id: "KLASSE-0002",
   school_id: "SCHULE-01",
   school-year: "SJ-10/11",
```

```
    start: "01-09-2010",
    end: "31-08-2011",
   }, {
    class_id: "KLASSE-0003",
    school_id: "SCHULE-01",
    school-year: "SJ-10/11",
    start: "01-09-2010",
    end: "31-08-2011",
   },
  ],
  subjects: [
   {
    subject_id: "SUBJECT-0001",
    subject_ref_id: "DE",
    school_id: "SCHULE-01",
    school-year: "SJ-09/10",
    start: "01-09-2009",
    end: "28-02-2010".
    time_tabel [
     {
      day: "1",
      start: "08:00:00",
      end: "08:45:00",
      repeat: "weekly"
     }, {
      day: "2",
      start: "08:00:00",
      end: "08:45:00",
      repeat: "weekly"
     }, {
      day: "3",
      start: "08:50:00",
      end: "09:35:00",
      repeat: "biweekly",
      start: "week-1"
     }, {
      day: "4",
      start: "08:50:00",
      end: "09:35:00",
      repeat: "biweekly",
      start: "week-2"
     }, {
      day: "3",
      start: "08:50:00",
      end: "09:35:00",
      repeat: "once",
      date: "30-10-2009"
     }
   }, {
    subject_id: "SUBJECT-0002",
    subject_ref_id: "MA",
    school_id: "SCHULE-01",
    school-year: "SJ-09/10",
```

```
    start: "01-09-2009",
    end: "31-08-2010"
  },

 ]
}
```

Listing 1: Beispiel Benutzer mit Rolle 'students'

```
{
 id: "USER-02",
 name: "Altes Leming 1",
 surename: "Zobel",
 birtdate: "03-01-2003",
 sex: "female",
 assignments: [
 {
  school_id: "SCHULE-01",
  role: "guardians",
  start: "01-09-2009",
  end: "31-08-2016",
  school-years: ["SJ-09/10","SJ-10/11","SJ-11/12","SJ-13/14","SJ-14/15","
      SJ-15/16"]
 }, {
  school_id: "SCHULE-04",
  role: "guardians",
  start: "01-09-2016",
  school-years: ["SJ-16/17","SJ-17/18","SJ-18/19","SJ-19/20","SJ-20/21"]
 }, {
  school_id: "SCHULE-02",
  role: "guardians",
  start: "01-09-2019",
  end: "31-08-2020",
  school-years: ["SJ-19/20"]
 }, {
  school_id: "SCHULE-02",
  role: "teacher",
  start: "01-09-2019"
 }
 ],
 childs: [
 {
  user_id: "USER-01",
  start: "01-09-2009",
  end: "03-01-2020",
 },  {
  user_id: "USER-03",
  start: "01-09-2009",
  end: "03-01-2020",
 }
 ],
 classes: [
  {
   class_id: "KLASSE-0031",
```

```
    school_id: "SCHULE-02",
    school-year: "SJ-09/10",
    start: "01-09-2009",
    end: "31-08-2010",
   }, {
    class_id: "KLASSE-0032",
    school_id: "SCHULE-02",
    school-year: "SJ-20/21",
    start: "01-09-2020",
    end: "31-08-2021",
   }, {
    class_id: "KLASSE-0033",
    school_id: "SCHULE-02",
    school-year: "SJ-20/21",
    start: "01-09-2020",
    end: "31-08-2021",
   },
  ]
}
```

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

```
{
 subject: "SUBJECT-0001",
 name: "Deutsch 1-A"
 subject_ref: "DE",
 school: "SCHULE-01",
 school-year: "SJ-09/10",
 start: "01-09-2009",
 end: "28-02-2010",
 classes: [ "KLASSE-01","KLASSE-03","KLASSE-05" ],
 grade: [ "1" ],
 students: [
  {
   user: "USER-01",
   start: "01-09-2009",
   end: "28-02-2010",
  }, {
   user: "USER-06",
   start: "01-09-2009",
   end: "28-02-2010",
  }, {
   user: "USER-07",
   start: "01-09-2009",
   end: "31-12-2009",
  },
 ],
 teachers: [
  {
   user: "USER-08",
   start: "01-09-2009",
   end: "28-02-2010",
  }, {
   user: "USER-09",
```

```
    start: "01-09-2009",
    end: "31-12-2009",
   }, {
    user: "USER-10",
    start: "05-10-2009",
    end: "05-10-2009",
   },
  ],
  timetable [
   {
    day: "1",
    start: "08:00:00",
    end: "08:45:00",
    repeat: "weekly"
   }, {
    day: "2",
    start: "08:00:00",
    end: "08:45:00",
    repeat: "weekly"
   }, {
    day: "3",
    start: "08:50:00",
    end: "09:35:00",
    repeat: "biweekly",
    week: "week-1"
   }, {
    day: "4",
    start: "08:50:00",
    end: "09:35:00",
    repeat: "biweekly",
    week: "week-2"
   }, {
    day: "3",
    start: "08:50:00",
    end: "09:35:00",
    repeat: "onetime",
    date: "30-10-2009"
   }
  ]
}
```

Listing 3: Beispiel eines Schulfachs

1 Einleitung und Vorüberlegungen

Ziel dieses Dokument ist es, eine REST-API und die darauf verwendeten Datenobjekte zu spezifieren 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 Authentifizierung und Autorisierung

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

Der Ablauf der Autorisierung per OAuth2-Protokoll im Authorization-Code-Flow ist in der folgenden Grafik dargestellt [1].

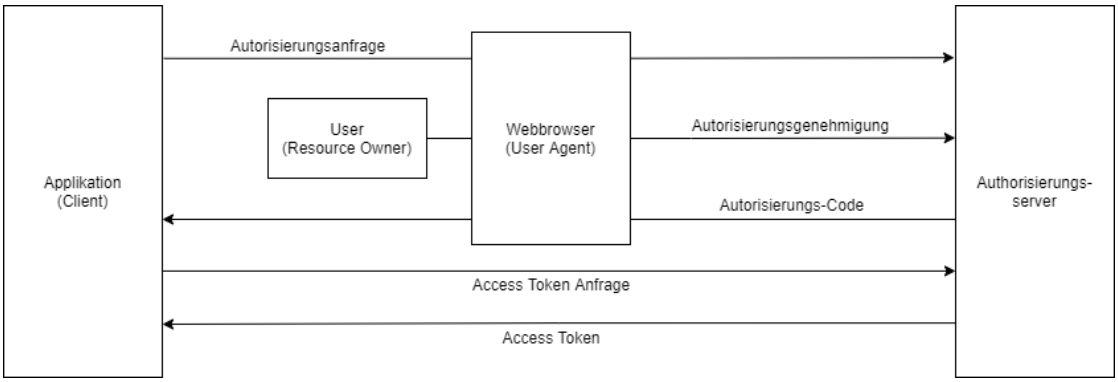

Abbildung 2.1: Access-Token-Erstellung im Authentication-Code-Flow

Über den Access Token erhält der Benutzer schließlich Zugriff auf das Zielsystem bzw. auf die REST-API, über den ID Token auf die ID (uuid) und ggf. weitere personenbezogene Daten des Benutzers. Sofern die personenbezogenen Daten für die Anlage eines Benutzerkontos (z.B. Vor- und Nachname, E-Mail-Adresse) benötigt werden, können diese durch die geeignete Wahl von scopes und claims im Aufruf der Autorisierungs-URL vom Resource Server abgefragt werden und initial zur Benutzerkontoerstellung genutzt werden.

Der IDM-Provider muss dabei den Autorisierungsserver (OpenID Provider) und Resource Server zur Verfügung stellen, zudem müssen folgende Endpunkte definiert sein:

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. Die ID des Benutzers im Access Token allein reicht nicht aus, um die Sichtbarkeit der Daten korrekt zu beschränken, da einem Benutzer im IDM mehrere Institut-Rolle-Kombinationen zugewiesen sein können (z.B. an verschiedenen Institutionen als Lehrkraft tätig oder an derselben Institution sowohl Lehrkraft als auch

Endpunkt	Funktion des Endpunkts
Autorisierung	Initiierung der Autorisierung und Benutzerzustimmung mit definierten Parametern (u.a. scopes/claims und Redirect-URL)
Token	Liefert ID und Access Token zurück
Revocation	Endpunkt, um den Access Token zu widerrufen
UserInfo	Kann definierte Benutzerdaten zur Verfügung stellen (z.B. uuid, Vor- und Nachname, E-Mail-Adresse)

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

Elternteil eines Schülers). Daher muss die Information, mit welcher Kombination von Institution und Rolle innerhalb dieser Institution der Aufruf eines REST-API-Endpunkts durchgeführt wird, an den IDM-Provider übermittelt werden. Dies geschieht durch die Erweiterung der Scopes-Liste (um jeweils den Scope für die Institution und die Rolle) als Parameterübergabe beim Autorisierungsvorgang. Die zusätzlichen Scopes für Institution und Rolle sind somit im Access Token hinterlegt und können bei der Generierung des zurückzuliefernden JSON-Objekts verwendet werden.

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 Institution. Um die Tokengenerierung zu vereinheitlichen, wird für Benutzerkonten mit der Rolle ”sync-system” statt des Institutionsnamens die Bezeichnung der IDM-Domäne verwendet.

Beispiel:

```
1 https://<URl zu Autorisierungsendpunkt>?response_type=code
2 &client_id=<Identifier von Client-App>
3 &redirect_uri=<Redirect-URL>
4 &scope=openid sync-system idm-domain
5 &state=<Undurchschaubarer Wert fuer Sicherheitszwecke>
```

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

Für den Logout bzw. Aktualisierungen aus dem IDM kann der Access Token am Autorisierungsserver widerrufen werfen (Token Revocation.)

3 REST-API-Definition

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

3.1 Schnittstellen für Schulfächer

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

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

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

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

3.1.1.1 READ

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

```
[
{
 id: "<STRING>",
 name: "<STRING>"
},
...
{
 id: "<STRING>",
 name: "<STRING>"
}
```

```
]
```

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

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

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

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

Tabelle 3.3: Berechtigungen auf dem Endpunkt

3.2 Schnittstellen für Schuljahre

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

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

3.3 Schnittstellen für Schulen

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

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

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

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

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

Tabelle 3.5: Zugelassene Operationen auf /api/schools

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

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

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

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

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

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

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

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

3.3.3.1 READ

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

```
[
 {
  school_id: "<STRING>",
  user_id: "<STRING>",
  role: "<STRING>",
  start: "<TIMESTAMP>",
  end: "<TIMESTAMP>",
  school-years: ["<STRING>",...,"<STRING>"]
 },
...
 {
  school_id: "<STRING>",
  user_id: "<STRING>",
  role: "<STRING>",
  start: "<TIMESTAMP>",
  end: "<TIMESTAMP>",
  school-years: ["<STRING>",...,"<STRING>"]
 },
]
```

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

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

Tabelle 3.9: Berechtigungen auf dem Endpunkt

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

Tabelle 3.9: Berechtigungen auf dem Endpunkt

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

Tabelle 3.9: Berechtigungen auf dem Endpunkt

3.3.3.2 CREATE

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

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

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

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

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

```
{
 user_id: "<STRING>",
 role: "<STRING>",
 start: "<TIMESTAMP>"
 school-years: ["<STRING>",...,"<STRING>"]
}
```

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

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

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

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

Tabelle 3.11: Berechtigungen auf dem Endpunkt

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

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

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

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

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

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

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

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

3.3.5.1 READ

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

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

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

Feldname	Datentyp	Beschreibung

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

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

Tabelle 3.15: Berechtigungen auf dem Endpunkt

3.4 Schnittstellen für Benutzer

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

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

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

Tabelle 3.16: Zugelassene Operationen auf /api/users

3.4.1.1 READ

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

```
{
 id: "<STRING>",
 name: "<STRING>",
 surename: "<STRING>",
 dateofbirth: "<CALENDARDATE>",
 sex: "<ENUM>",
}
```

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

Feldname	Datentyp	Beschreibung

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

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

Tabelle 3.18: Berechtigungen auf dem Endpunkt

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

Tabelle 3.18: Berechtigungen auf dem Endpunkt

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

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

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

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

3.4.2.1 READ

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

```
{
 id: "<STRING>",
 name: "<STRING>",
 surename: "<STRING>",
 dateofbirth: "<CALENDARDATE>",
 sex: "<ENUM>",
}
```

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

Feldname	Datentyp	Beschreibung

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

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

Tabelle 3.21: Berechtigungen auf dem Endpunkt

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

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

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

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

3.4.3.1 READ

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

```
{
 school_id: "<STRING>",
 role: "<STRING>",
 start: "<CALENDARDATE>",
 end: "<CALENDARDATE>",
 school-years: ["<STRING>",...]
},
...
```

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

Feldname	Datentyp	Beschreibung

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

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

Tabelle 3.24: Berechtigungen auf dem Endpunkt

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

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

3.4.4.1 READ

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

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

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

```
[
  {
   class_id: "<STRING>",
   school_id: "<STRING>",
   school-year: "<STRING>",
   start: "<CALENDARDATE>",
   end: "<CALENDARDATE>",
  },
  ...
]
```

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

Feldname	Datentyp	Beschreibung

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

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

Tabelle 3.27: Berechtigungen auf dem Endpunkt

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

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

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

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

3.4.5.1 READ

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

```
[
  "<STRING>",
  ...
]
```

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

Feldname	Datentyp	Beschreibung

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

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

Tabelle 3.30: Berechtigungen auf dem Endpunkt

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

Tabelle 3.30: Berechtigungen auf dem Endpunkt

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

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

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

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

3.4.6.1 READ

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

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

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

Feldname	Datentyp	Beschreibung

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

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

Tabelle 3.33: Berechtigungen auf dem Endpunkt

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

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

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

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

3.4.7.1 READ

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

```
[
 id: "<STRING>",
...
]
```

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

Feldname	Datentyp	Beschreibung

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

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

Tabelle 3.36: Berechtigungen auf dem Endpunkt

3.5 Schnittstellen für Schulfächer an Schulen

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

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

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

Tabelle 3.37: Zugelassene Operationen auf /api/subjects

3.5.1.1 READ

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

```
[
 "<STRING>",
 ...
]
```

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

Feldname	Datentyp	Beschreibung

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

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

Tabelle 3.39: Berechtigungen auf dem Endpunkt

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

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

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

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

3.5.2.1 READ

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

```
[
 {
  subject: "<STRING>",
  name: "<STRING>",
  subject_ref: "<STRING>",
  school: "<STRING>",
  school-year: "<STRING>",
  start: "<CALENDARDATE>",
  end: "<CALENDARDATE>",
 },
 ...
]
```

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

Feldname	Datentyp	Beschreibung

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

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

Tabelle 3.42: Berechtigungen auf dem Endpunkt

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

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

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

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

3.5.3.1 READ

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

```
[
 {
  subject: "<STRING>",
  classes: [ "<STRING>", ... ],
 },
 ...
]
```

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

Feldname	Datentyp	Beschreibung

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

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

Tabelle 3.45: Berechtigungen auf dem Endpunkt

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

Tabelle 3.45: Berechtigungen auf dem Endpunkt

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

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

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

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

3.5.4.1 READ

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

```
[
 {
  subject: "<STRING>",
  school: "<STRING>",
 },
 ...
]
```

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

Feldname	Datentyp	Beschreibung

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

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

Tabelle 3.48: Berechtigungen auf dem Endpunkt

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

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

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

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

3.5.5.1 READ

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

```
[
 {
  subject: "<STRING>",
  user: "<STRING>",
  start: "<CALENDARDATE>",
  end: "<CALENDARDATE>",
 },
 ...
]
```

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

Feldname	Datentyp	Beschreibung

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

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

Tabelle 3.51: Berechtigungen auf dem Endpunkt

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

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

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

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

3.5.6.1 READ

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

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

```
[
 {
  subject: "<STRING>",
  user: "<STRING>",
  start: "<CALENDARDATE>",
  end: "<CALENDARDATE>",
 },
 ...
]
```

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

Feldname	Datentyp	Beschreibung

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

Benutzergruppen	Zugelassene Daten
guest	Darf den 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 3.54: Berechtigungen auf dem Endpunkt

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

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

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

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

3.5.7.1 READ

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

```
[
 {
  subject: "<STRING>",
  day: "<ENUM>",
  start: "<TIME>",
  end: "<TIME>",
  repeat: "<ENUM>",
  date: "<CALENDARDATE>",
  week: "<ENUM>",
 },
 ...
]
```

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

Feldname	Datentyp	Beschreibung

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

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

Tabelle 3.57: Berechtigungen auf dem Endpunkt

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

Tabelle 3.57: Berechtigungen auf dem Endpunkt

3.6 Schnittstellen für Klassen

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

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

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

Tabelle 3.58: Zugelassene Operationen auf /api/classes/

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Literaturverzeichnis

[1] D. Hardt, “The OAuth 2.0 Authorization Framework.” RFC 6749, Oct. 2012.

Abbildungsverzeichnis

Tabellenverzeichnis

Listings