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 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 Autorisierungserver. Der Autorisierungserver 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.

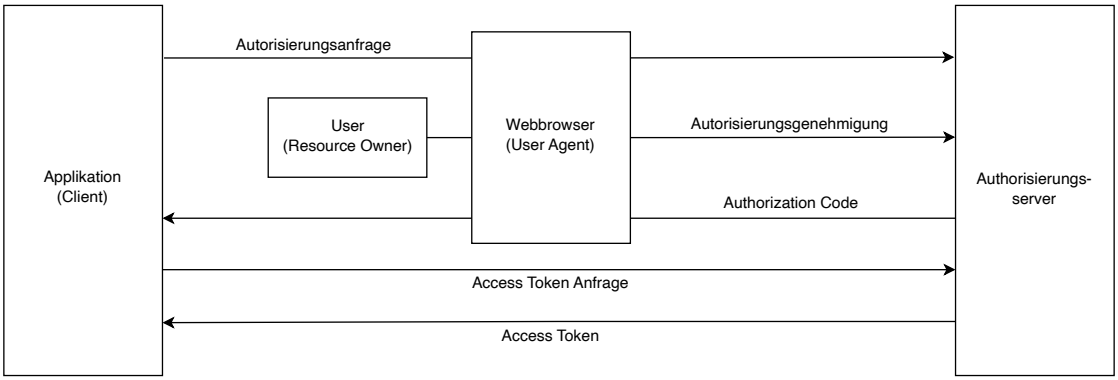

Abbildung 2.1: Ablauf des Authentication Code Grant

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 weiteren *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 angefordern.

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=<Identifier 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 Neuanmeldung 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 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

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.

```
[
{
 id: "<STRING>",
 short_name: "<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 3.3: 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.

3.4 Schnittstellen für Benutzer

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

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

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

Tabelle 3.6: Zugelassene Operationen auf /api/users

3.4.1.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Route gibt für den eingeloggten Benutzer seine persönlichen Daten wieder. 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.

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

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

Feldname	**Datentyp**	**Beschreibung**

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

3.4.2 Endpunkt in der REST-API: /api/users/$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	Ja	POST
DELETE	Nein	

Tabelle 3.9: Zugelassene Operationen auf /api/users/$id

3.4.2.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Route gibt für den per ID ausgewählten Benutzer seine persönlichen Daten wieder. Diese können eingeschränkt werden durch den Kontext, in dem sich der anfragende Benutzer befinden.

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.

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

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

Feldname	Datentyp	Beschreibung

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

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

Tabelle 3.11: Berechtigungen auf dem Endpunkt

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

Tabelle 3.11: Berechtigungen auf dem Endpunkt

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

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

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

Tabelle 3.12: Zugelassene Operationen auf /api/users/$id/assignments

3.4.3.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Sie gibt für den per ID ausgewählten Benutzer seine Zuordnungen im System wieder. Für diese Daten gelten die Einschränkungen die durch den Kontext des anfragenden Benutzers gegeben sind.

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

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

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

Feldname	Datentyp	Beschreibung

Tabelle 3.13: Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

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

Tabelle 3.14: Berechtigungen auf dem Endpunkt

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

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

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

Tabelle 3.15: Zugelassene Operationen auf /api/users/$id/classes

3.4.4.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Route gibt für den per ID ausgewählten Benutzer seine für ihn hinterlegten Klassen im System wieder. Für diese Daten gelten die Einschränkungen die durch den Kontext des anfragenden Benutzers gegeben sind.

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

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

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

Feldname	Datentyp	Beschreibung

Tabelle 3.16: Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

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

Tabelle 3.17: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.18* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

3.4.5.1 READ

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

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

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

eine Liste mit Schulfächern für den ausgewählten Benutzer zurück. Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.6*. Die einzelnen Felder der Antwort werden in *Tabelle 3.19* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.20* entnommen werden.

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

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

Feldname	Datentyp	Beschreibung

Tabelle 3.19: Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

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

Tabelle 3.20: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.21* 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/$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 3.7*. 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 ...
4 ]
```

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

Feldname	Datentyp	Beschreibung

Tabelle 3.22: Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

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

Tabelle 3.23: Berechtigungen auf dem Endpunkt

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

Tabelle 3.23: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.24* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

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

Tabelle 3.24: Zugelassene Operationen auf /api/users/$id/guardians

3.4.7.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Die Route gibt für den per ID ausgewählten Benutzer die Liste mit den IDs seiner Eltern, Erziehungsberechtigen und Vormünder wieder. Dies geschieht im Kontext der Informationen die der anfragende Nutzer sehen darf.

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 ...
4 ]
```

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

Feldname	Datentyp	Beschreibung

Tabelle 3.25: Beschreibung der Felder in einem JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

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

Tabelle 3.26: Berechtigungen auf dem Endpunkt

3.5 Schnittstellen für Schulfächer an Schulen

Ein Schulfach ist eine Unterrichtseinheit, welche in einem Schuljahr oder Halbjahr stattfindet und an eine Schule gebunden ist. In der Regel ist 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 3.27* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

3.5.1.1 READ

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

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

Tabelle 3.27: Zugelassene Operationen auf /api/subjects

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

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

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

Feldname	Datentyp	Beschreibung

Tabelle 3.28: Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

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

Tabelle 3.29: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.30* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

3.5.2.1 READ

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

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

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

Die Antwort erfolgt mit dem JSON-Objekt *Listing 3.10*. Die einzelnen Felder der Antwort werden in *Tabelle 3.31* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.32* entnommen werden.

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

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

Feldname	Datentyp	Beschreibung

Tabelle 3.31: Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

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

Tabelle 3.32: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.33* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

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

Tabelle 3.33: Zugelassene Operationen auf /api/subjects/$id/classes

3.5.3.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Diese Route gibt bei 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 3.11*. Die einzelnen Felder der Antwort werden in *Tabelle 3.34* beschrieben. Die Berechtigungen auf den Endpunkt können *Tabelle 3.35* entnommen werden.

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

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

Feldname	Datentyp	Beschreibung

Tabelle 3.34: Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

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

Tabelle 3.35: Berechtigungen auf dem Endpunkt

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

Tabelle 3.35: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.36* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

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

Tabelle 3.36: Zugelassene Operationen auf /api/subjects/$id/students

3.5.4.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Eine READ-Anfrage auf diese Route gibt eine Liste mit Objekten, welche Schüler von wann bis wann an 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 3.12*. Die einzelnen Felder der Antwort werden in Tabelle *Tabelle 3.37* beschrieben. Die Berechtigungen auf den Endpoint können *Tabelle 3.38* entnommen werden.

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

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

Feldname	Datentyp	Beschreibung

Tabelle 3.37: Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

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

Tabelle 3.38: Berechtigungen auf dem Endpunkt

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

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

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

Tabelle 3.39: Zugelassene Operationen auf /api/subjects/$id/teachers

3.5.5.1 READ

Es sind nur Anfragen mit der HTTP-GET-Methode für ein READ auf die Daten zugelassen. Bei einer READ-Abnfrage auf diese Route wird eine Liste von Objekten mit Metainformationen zu den unterrichtenden Lehrkräften des per ID ausgewählten Unterrichtsfaches zurückgegeben. Für die Daten gilt, dasd diese anhand des Kontextes des anfragenden Users Einschränkungen unterliegen.

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

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

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

Feldname	Datentyp	Beschreibung

Tabelle 3.40: Beschreibung der Felder in eine JSON-Objekt für das Zuordnen eines Benutzer in einer Rolle zu einer Schule

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

Tabelle 3.41: Berechtigungen auf dem Endpunkt

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

Die *Tabelle 3.42* listet auf, welche Operationen zugelassen sind und welche HTTP-Methoden dabei verwendet werden.

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

Tabelle 3.42: Zugelassene Operationen auf /api/subjects/$id/timetable

3.5.6.1 READ

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

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

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

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

Feldname	Datentyp	Beschreibung

Tabelle 3.43: Beschreibung der Felder in einem JSON-Objekt für den Stundenplan eines Schulfachs

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

Tabelle 3.44: Berechtigungen auf dem Endpunkt

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

Tabelle 3.44: Berechtigungen auf dem Endpunkt

3.6 Schnittstellen für Klassen

Muss noch überarbeitet werden!

- Soll für aktiven Benutzer bei 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.

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 ßync-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

Tabellenverzeichnis

Listings