



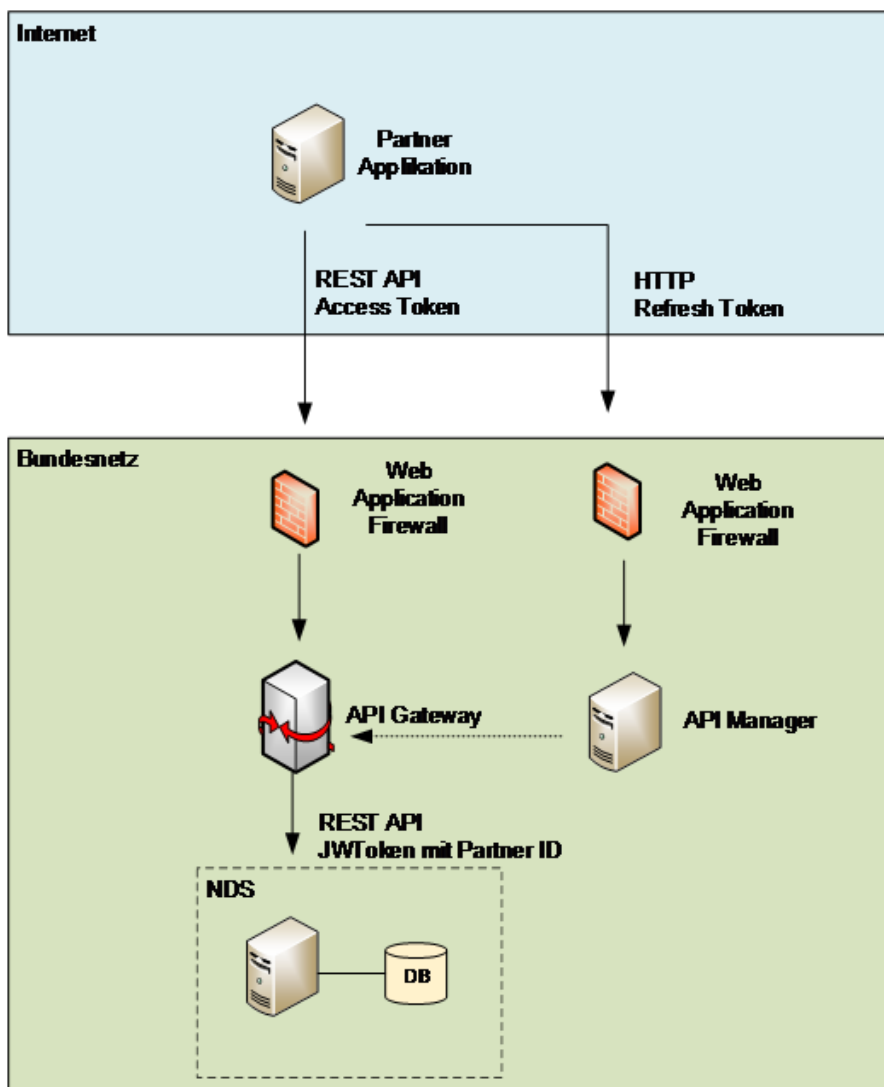
Leitfaden zur Integration von «Standard-API» der NDS für Partner des BASPO

Einleitung

Die neue Nationale Datenbank für Sport (NDS) bietet neben den webbasierten User Interfaces auch eine REST-basierte Maschinenschnittstelle für die Abfrage von Kursdaten an. Dieses Dokument beschreibt die Funktionsweise des Zuganges sowie die nötigen Schritte zur Integration.

Architektur

Folgende Abbildung zeigt schematisch das Zusammenspiel der einzelnen Komponenten für den Zugang zur «Standard-API».



Das blau hinterlegte Rechteck stellt die Partner-Applikation mit ihrer Serverinfrastruktur dar. Aus Sicht des Bundes sind die Partner-Applikationen auf dem Internet. Ein Prozess auf deren Applikationen rufen die von der NDS bereitgestellte Schnittstelle auf.

Das grün hinterlegte Rechteck zeigt die Infrastruktur des Bundes.

- Die NDS-Applikation implementiert sämtliche Geschäftsfunktionen von der NDS und persistiert die Daten in der NDS-Datenbank. Zudem werden verschiedene Umsysteme angebunden (im Bild nicht gezeigt) sowie REST-API implementiert.
- Der API-Gateway ist eine Standardkomponente des Bundes, welche die Teilnehmer einer API authentisiert und autorisiert. Er exponiert APIs in das Internet und leitet die Requests zur Zielapplikation weiter. Die Partner resp. Teilnehmer der Schnittstelle sind im API-Gateway registriert.
- Am API-Manager wird das Access-Token mit dem Refresh-Token erneuert. Refresh- und Access-Token sind jeweils eine Woche lang gültig.
- Die Web-Application Firewall-WAF ist eine Sicherheitskomponente, welche den eingehenden Netzwerkverkehr analysiert.

Die Pfeile zeigen die Richtung des Verbindungsaufbaus an.

Funktionsweise

Die API ist als REST-Schnittstelle implementiert. Die Schnittstelle wird mit einem Access-Token abgesichert, das bei jedem Request als http-header mitgegeben werden muss. Der API-Gateway authentisiert damit den Aufrufer und setzt die zum Access-Token gehörende Partner-ID in das JWT-Token, welches dem NDS-Backend weitergeleitet wird. Das NDS-Backend wiederum autorisiert aufgrund der Partner-ID.

Hier in Beispielaufruf mit curl

```
curl -k -H "Authorization: Bearer <access_token>" -v <url>  
<access_token>: gültiges Access Token  
<url>: URL der API, z.B. https://api.baspo.admin.ch/nds/api/courseList/?courseStatus=APPROVED
```

Das Access-Token hat eine Gültigkeit von einer Woche. Danach muss es mit dem Refresh-Token am API-Manager erneuert werden. Das Refresh-Token kann nur einmal zum Erneuern des Access-Tokens verwendet werden. In der Response sind neue Refresh- und Access-Token

Authorization Request

```
curl -k -u <clientId>:<clientSecret> -d "grant_type=refresh_token&refresh_token=<refresh-token>"  
https://keymanager.api.admin.ch/token/v2
```

Authorization Response

```
{  
  "access_token": "eyJ4NXQiOiJPRFkxT1dVNFlqZGtaV1...DMlzeiF8qW75_Y6G3CoS2O55C35g", "refresh_token": "c8108211-  
a15c-37cc-8f33-f2638a5cd38e",  
  "token_type": "Bearer",  
  "expires_in": 604800  
}
```

Die Partner-Applikation ist verantwortlich, dass das Access-Token fristgerecht erneuert wird.

Die Partner-Applikationen implementieren die Aufrufe in der Programmiersprache ihrer Wahl. http libraries sind für nahezu jede Sprache erhältlich.

Bei Verlust des Refresh-Token muss beim BASPO ein neues erfragt werden.

Registrierung

Will ein Partner die API benutzen, muss er einen Antrag an das BASPO stellen (siehe Kontakt ganz unten).

Nach der Genehmigung registriert das BASPO den Partner in der NDS und erfasst für diesen Partner einen Client im API-Gateway. Bei der Registrierung auf dem API-Gateway werden für jeden Partner ein Client-Key, ein Client-Passwort, sowie ein Access-Token und ein Refresh-Token generiert. Die Informationen werden vom BASPO per verschlüsselter Mail an den Partner übermittelt. Die ID in der Kopfzeile bezeichnet die Partner-ID (hier «17986»)

Anbei ein Beispiel mit anonymisierten Daten

----- 17986 -----

Consumer Key: H01.....G8a

Consumer Secret: vLbE.....u0a

Access Token: eyJ0eXAiO.....rA

Refresh Token: 138.....8dcde

Expires in: 604802

Umgebungen

NDS stellt 2 Umgebungen zu Verfügung:

- Eine produktive Umgebung, welche ausschliesslich für den produktiven Betrieb verwendet werden darf.
- Eine Abnahme-Umgebung für Integrationszwecke

URLs:

Produktion: <https://api.baspo.admin.ch/nds/api>

Abnahme: <https://abn-api.baspo.admin.ch/nds/api>

KeyManager: <https://keymanager.api.admin.ch/token/v2>

Kontakt

info-js@baspo.admin.ch