Autorisierung

Authentifizierung

Die API der Deutschen Digitalen Bibliothek ist durch eine Authentifizierung (Wer ruft auf?) über das OAuth 1.0a Protokoll geschützt. Es ist eine vollständige Implementierung von OAuth integriert. Die jetzige Version wurde lediglich vereinfacht und der Ablauf entschlackt, wodurch der Unterschied zu einer Basic Authentication nicht direkt ersichtlich sein kann.

Das OAuth Protokoll verwendet verschiedene Parameter und Verschlüsselungstechniken, um den Benutzer zweifelsfrei zu identifizieren. In dem momentan implementierten Mechanismus wird die Verwendung der Parameter und Verschlüsselungen auf ein Minimum reduziert, um einen einfachen Zugriff auf die API Methoden zu ermöglichen.

Alle Methoden, die geschützt sind, erwarten eine vordefinierte Menge an Parametern die auf zwei Wegen mitgegeben werden können:

1. Entweder via **HTTP Request Header** oder
2. über **Query Parameter**.

Erlaubte Parameter

Parametername	Verwendung
`oauth_consumer_key`	Eindeutiger API-Schlüssel des Benutzers

HTTP Request Header

Wird die Authentifizierung über den HTTP Request Header durchgeführt, schreibt das OAuth Protokoll einen Header der folgenden Form vor:

```
GET /items/OAXO2AGT7YH35YYHN3YKBXJMEI77W3FF/view HTTP/1.1
Host: api.deutsche-digitale-bibliothek.de
Authorization: OAuth oauth_consumer_key="abcdefgh12345678"
```

Die geschützte Methode wird dabei wie folgt aufgerufen, z. B. https://api.deutsche-digitale-bibliothek.de/items/OAXO2AGT7YH35YYHN3YKBXJMEI77W3FF/view

Query Parameter

Wird die Authentifizierung dagegen mit Query-Parametern ausgeführt, bleibt der Header unberührt und alle Parameter werden im Methodenaufruf mitgegeben. Dazu muss der oben genannte Parameter an die URL angehängt werden. Dabei ist zu beachten, dass die URL nach dem Anhängen des API Keys und der Parameter entsprechend kodiert werden muss (URL-Encoding).

https://api.deutsche-digitale-bibliothek.de/items/OAXO2AGT7YH35YYHN3YKBXJMEI77W3FF/view?oauth_consumer_key=abcdefgh123456789

Verschlüsselung

Derzeit ist eine Verschlüsselung nur über das HTTP Secure Protokoll verfügbar. Die OAuth-Verschlüsselung ist nicht aktiviert. Informationen hierzu können in der Spezifikation nachgelesen werden.

Autorisierung

Benutzergruppen

Momentan sind drei Benutzergruppen/Rollen definiert: VOLL, LESEND und EINGESCHRÄNKT. Benutzer werden je nach ihrer Benutzergruppe für den Aufruf der Methoden autorisiert. Bei jedem Zugriff auf die geschützten Methoden wird dem Benutzer eine Gruppe gemäß dem nachfolgenden Schema zugeordnet:

	VOLL	LESEND	EINGESCHRÄNKT
Kein API Key			x

Unbekannter API Key			x
Korrekter API Key		x	
Administrator API Key	x		

- **VOLL** hat dabei Zugriff auf alle Methoden und bekommt alle Informationen über sämtliche Objekte der DDB ausgeliefert.
- **LESEND** darf alle Methoden verwenden, die dieser Sicherheitsstufe entsprechen.
- **EINGESCHRÄNKT** darf nur Methoden der geringsten Sicherheitsstufe verwenden.