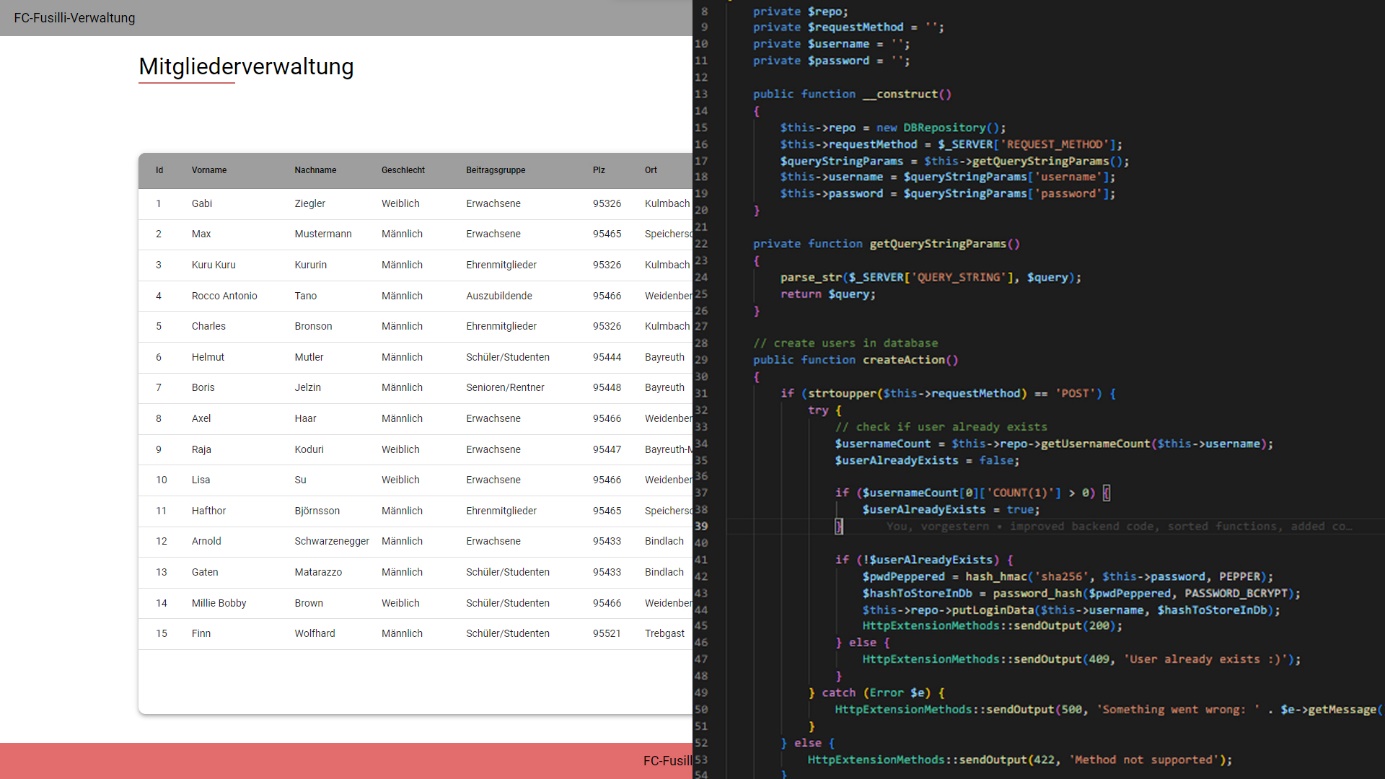
Juli - 2022

WEBBASIERTER-DATENBANKMANAGER



Gruppe 4 – Fusilli

|  |  |
| --- | --- |
| Thomas S. | @Noodle693 |
| Marco H. | @GodlesZ95 |
| Samuel S. | @Gunzli02 |
| Michael W. | @miwied |

Inhaltsverzeichnis

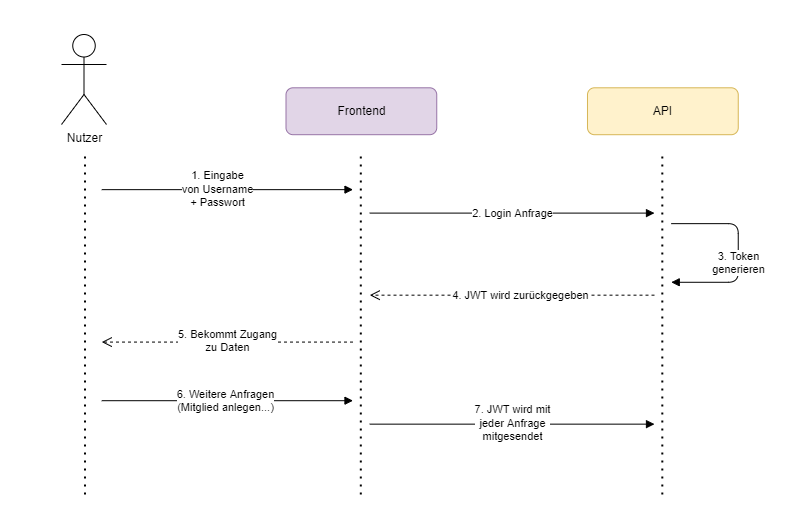
**JSON Web Token (JWT)**

Wir nutzen für die Autorisierung aller HTTP Anfragen, über die wir Daten von der API nach außen geben, einen JSON Web Token, der beim Login generiert wird.

Wir gleichen die Gültigkeit dieses Tokens bei jeder Anfrage ab, damit ein unautorisierter Zugriff auf die personenbezogenen Daten unmöglich ist.

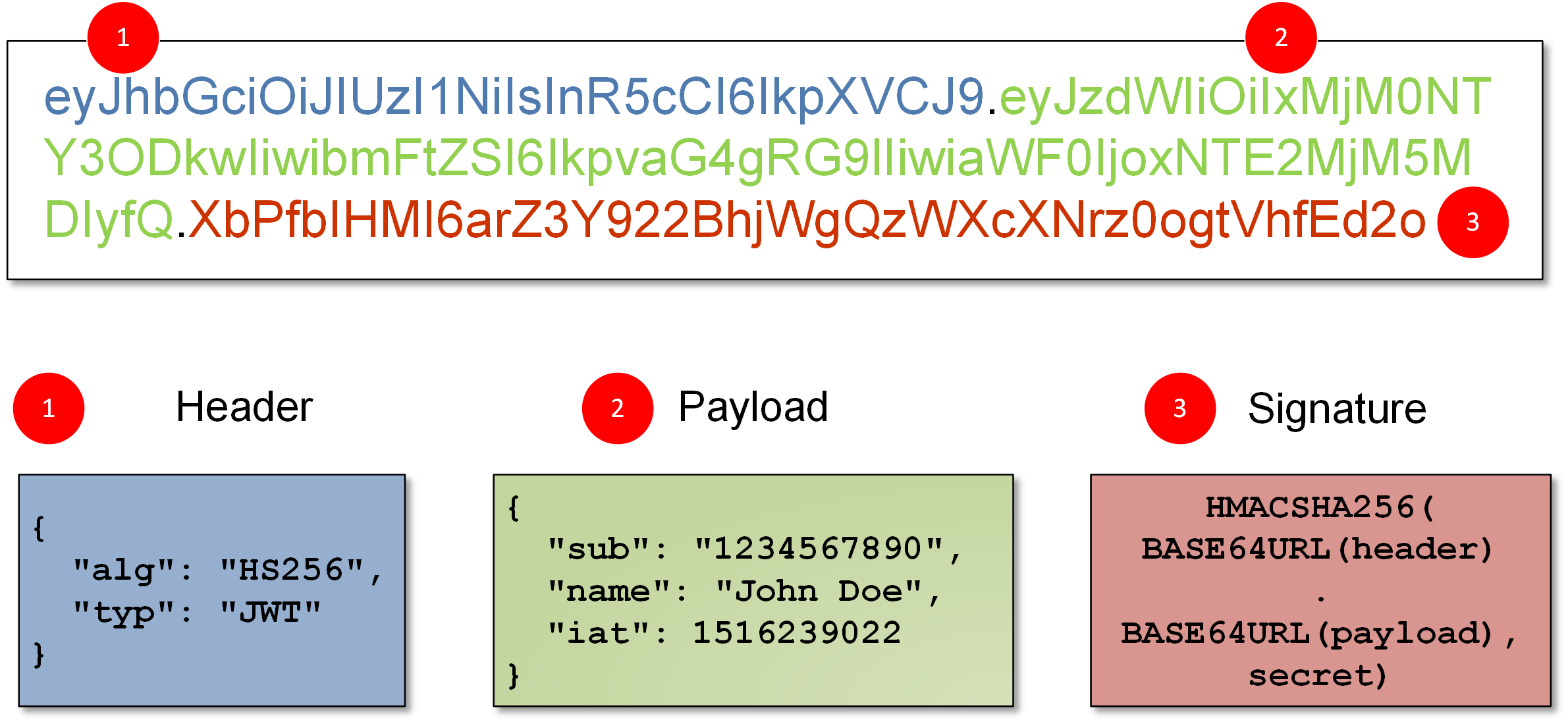
Das Generieren und der Abgleich finden über das Firebase/PHP-JWT Package statt. Wir haben uns für dieses Package entschieden, da wir die Funktionalität ohnehin genauso dupliziert hätten.

Dieses Diagramm soll erstmal den Ablauf visualisieren. Im Anschluss gehen wir genauer auf die Generierung, den Aufbau des Tokens und die technische Abfrage ein.



Zunächst erklären wir den Aufbau des JWT - im Anschluss beleuchten wir den 3. Schritt im Diagramm, die Generierung.

**Aufbau**



Der JWT besteht aus 3 verschlüsselten Teilen, die durch Punkte getrennt sind.

1. Zunächst die Header-Information worin der Typ des Tokens sowie der Verschlüsselungsalgorithmus enthalten sind. Wie Sie später sehen werden, verwenden wir selbst den HS512 Algorithmus – dies steht für HMAC SHA512, also die SHA512 Hashfunktion in Verbindung mit einem Nachrichtenauthentifizierungscode.
2. Die Payload. Hier finden sich selbst festgelegte sowie allgemein empfohlene „Claims“ (key-value-pairs). Alle Zeitpunkte sind von Beginn der Unixzeit an in Sekunden gerechnet angegeben. In kurz: die Anzahl der Sekunden seit dem 01.01.1970 um 00:00 Uhr UTC.

Wir senden also den Zeitpunkt, wann der Token generiert wurde (iat – issued at), den Herausgeber des Tokens (iss – issuer), das Datum ab wann der Token gültig ist (nbf – not before), wann er abgelaufen ist (exp – expiration) und den Nutzernamen im Klartext (userName).

1. Die Signatur der gesamten Message, welche verifiziert, dass die Nachricht während dem Senden nicht verändert wurde. Hier wird das Paket aus Header, Payload und einem eigens festgelegten Secret-Key verschlüsselt (bei uns ebenso mit HS512).

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung**Generierung**

Die Generierung sieht wie folgt aus.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Thema 2 …