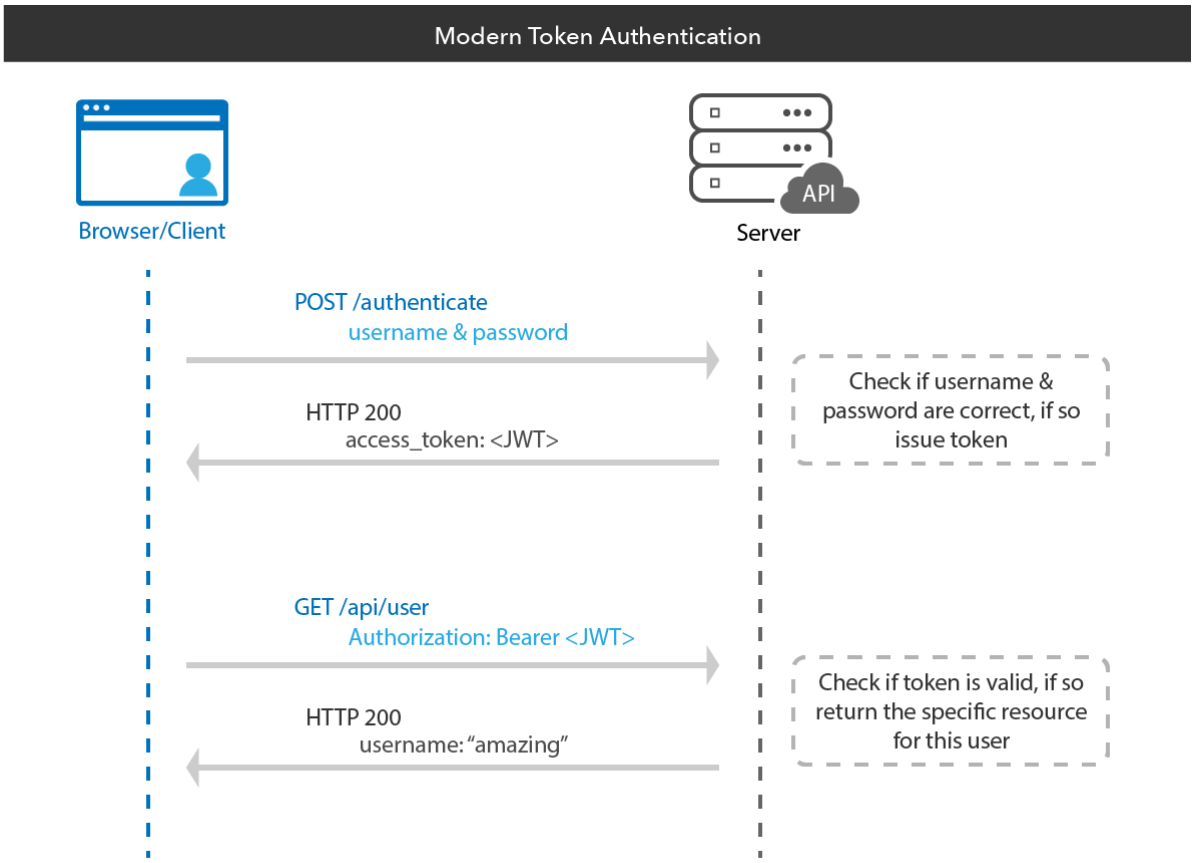
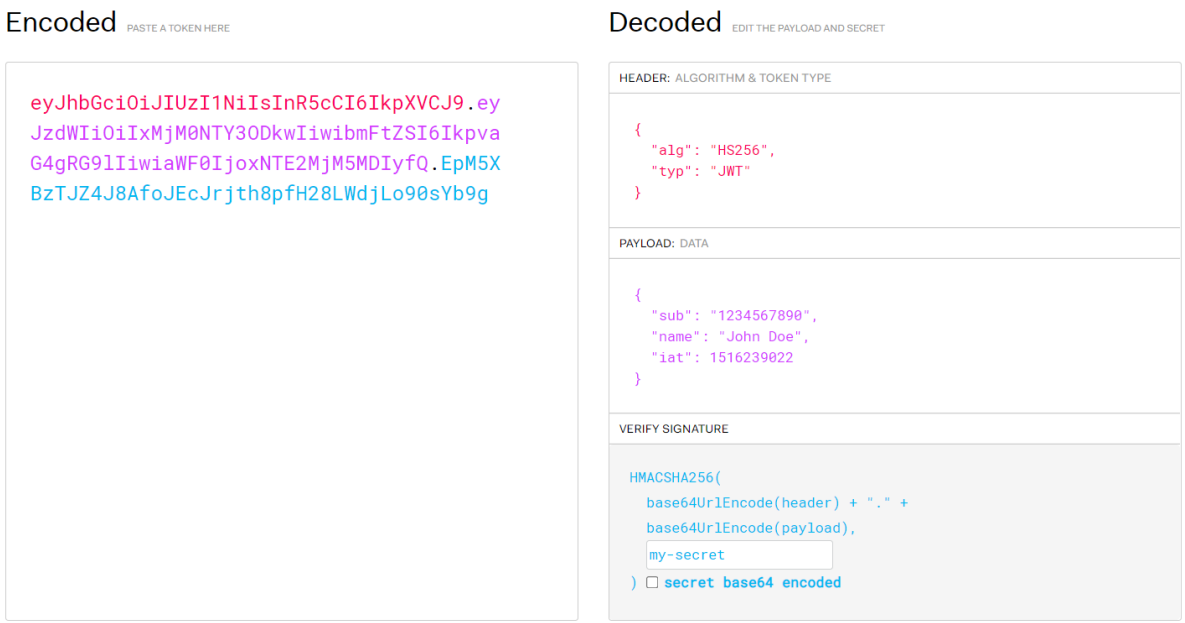
Chứng thực người dùng HTTP API với JSON Web Token (JWT)

Để thực hiện các lời gọi HTTP API, đầu tiên người dùng cần chứng thực với server thông qua username và password. Nếu hợp lệ, server sẽ trả về một JSON Web Token (JWT) có giá trị trong một thời gian nhất định (ví dụ như 24 giờ). Người dùng sẽ đính kèm JWT cho mỗi lời gọi HTTP API sau đó. Thông thường JWT sẽ được đặt trong phần header authorization của mỗi yêu cầu. Tiến trình này có thể được minh họa bằng sơ đồ dưới đây.



Một JWT gồm 3 thành phần: header, payload và signature cách nhau bởi dấu chấm. Các thành phần này đều được biểu diễn dưới dạng (encode) base64, ví dụ (https://jwt.io/):



Giới thiệu về HTTP API chứng thực phía server

Giải nén tập tin *backend.zip* đã cho, thực thi các lệnh sau để chạy backend:

```
cd backend
npm install
npm run start
```

Server chạy tại cổng 3000. Server này cung cấp HTTP API tương tự server các bạn đang dùng trong buổi thực hành, tuy nhiên có hai điểm khác biệt chính sau:

- Để thực hiện gọi HTTP API, client cần có header authorization chứa một JWT token hợp lệ.
- Hỗ trợ 2 route mới là *POST /api/auth/signup*, *POST /api/auth/signin* lần lượt thực hiện chức năng đăng ký và đăng nhập.

Hãy dùng một HTTP API Client (ví dụ Postman) để thực hiện yêu cầu GET /api/contacts (tạm thời không cần quan tâm đến header authorization) và quan sát kết quả.

POST /api/auth/signup: thực hiện đăng ký người dùng mới, client cần gửi dữ liệu JSON có dạng sau về server, ví dụ:

```
{ "username": "baobui", "email": "baobui@example.com", "password": "123456" }
```

Nếu đăng ký thành công, người dùng có thể đăng nhập với tài khoản vừa tạo.

Hãy dùng một HTTP API Client (ví dụ Postman) để thực hiện đăng ký một người dùng mới (lưu ý đặt header Content-Type là application/json cho yêu cầu) và quan sát kết quả.

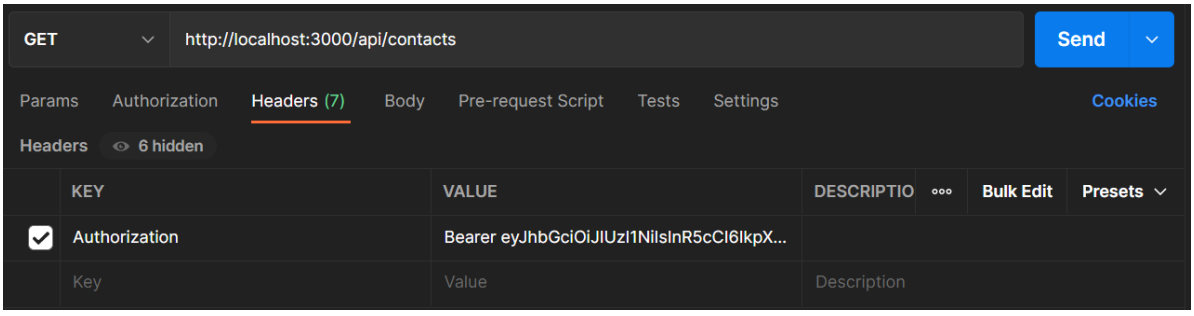
POST /api/auth/signin: thực hiện đăng nhập, client cần gửi dữ liệu JSON có dạng sau về server, ví dụ:

```
{ "username": "baobui", "password": "123456" }
```

Nếu đăng nhập thành công, server sẽ gửi về một JWT có thời hạn trong vòng 24 giờ (bên trong JWT này có chứa id của người dùng).

Hãy dùng một HTTP API Client (ví dụ Postman) để thực hiện đăng nhập với người dùng vừa tạo (lưu ý đặt header Content-Type là application/json cho yêu cầu). Lưu giá trị của JWT trả về từ server. Tiếp theo, thực hiện yêu cầu GET /api/contacts với header authorization dạng như sau:

```
Authorization: Bearer điền-vào-jwt-đã-lưu
```



(Các bạn có thể tham khảo code của backend để hiểu thêm về cách cài đặt phương pháp chứng thực này).

Ứng dụng Vue hỗ trợ đăng ký và đăng nhập

Giải nén tập tin *frontend.zip* đã cho, thực thi các lệnh sau để chạy frontend:

```
cd frontend
npm install
npm run dev
```

Ứng dụng vue được chạy ở cổng 3001 (http://localhost:3000/), thực hiện đăng nhập hoặc đăng ký để vào phần quản lý các liên hệ.