

Research Documentation

Topic: *JSON Web Token (JWT) - Authentication
Technology Research*

Prepared by: Mohammed Alherz

Assignment: Spring Boot Security Exercise

Date: Aug 25, 2025

What is JWT?

JSON Web Token (JWT) is a secure way to send information between two parties. It's like a digital ID card that contains user data. JWT is compact and safe, making it perfect for web applications and mobile apps.

JWT Structure

JWT has three parts separated by dots (.) as shown in figure1:

Header - Contains the token type and security method

Payload - Holds the actual user information

Signature - Proves the token is real and unchanged

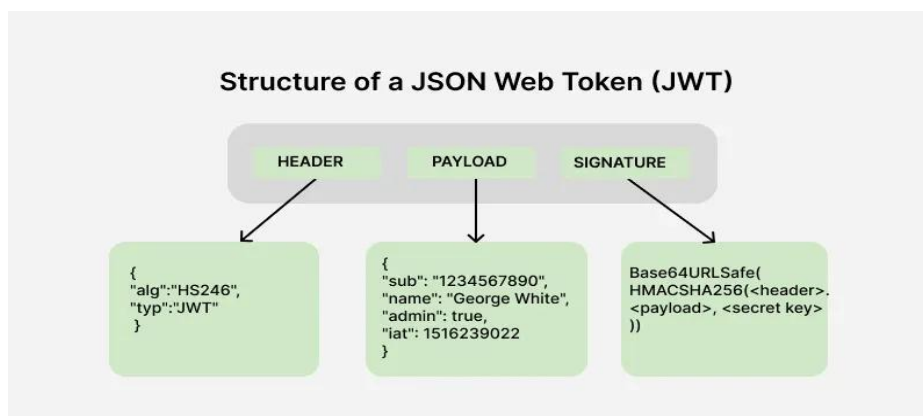


Figure 1 JWT parts

How JWT Works

1. User logs in with username and password
2. Server checks if details are correct
3. Server creates a JWT token with user info
4. Token is sent back to user
5. User sends token with every request
6. Server reads token to know who the user is

Key Benefits

- **No server storage needed** - All info is in the token
- **Works everywhere** - Can use with any programming language
- **Fast** - Small size makes it quick to send
- **Secure** - Digital signature prevents tampering

Security Features

- Digital signatures ensure tokens can't be faked
- Tokens expire automatically for safety
- Information is encoded to prevent easy reading
- Can set different access levels for users

Common Uses

- **Website login** - Keep users logged in
- **Mobile apps** - User authentication
- **API access** - Secure data sharing
- **Single sign-on** - Use one login for multiple sites

Best Practices

- Set short expiration times
- Use strong passwords for signing
- Store tokens safely on client side
- Always check if token is valid
- Don't put sensitive data in tokens

Limitations

- Hard to cancel tokens immediately

- Tokens can become large with too much data
- Not good for storing lots of user information
- Need careful handling to stay secure

Conclusion

JWT is a modern way to handle user login and security in web applications. It's simple, fast, and secure when used correctly. While it has some limits, JWT is widely used because it makes applications easier to build and scale.