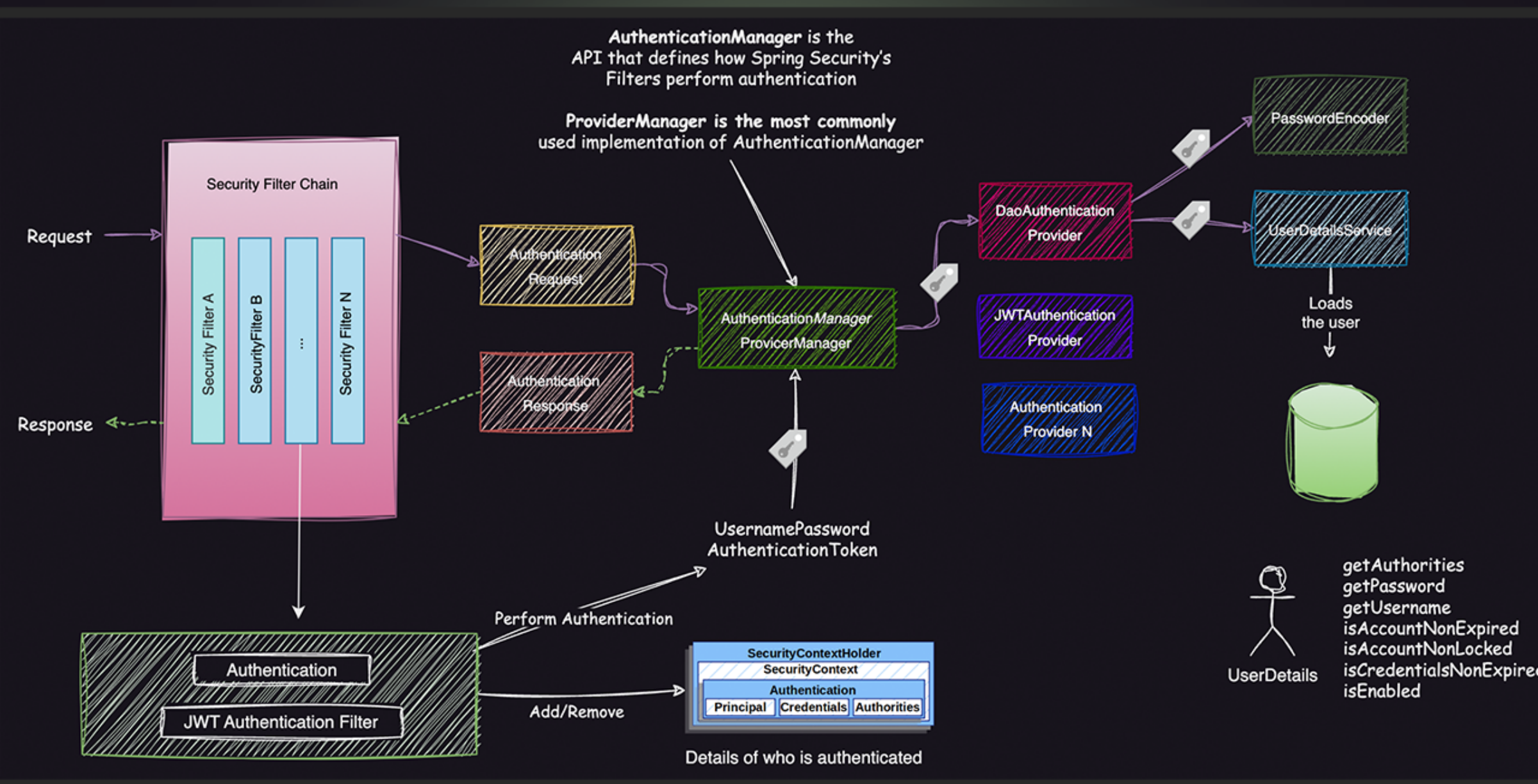
# Spring Security Architecture Explained




amigoscode.com

# Authentication

When a user attempts to access a protected resource, Spring Security will check the authenticity of the user's credentials. If the credentials are valid, the user will be granted access to the resource.

amigoscode.com

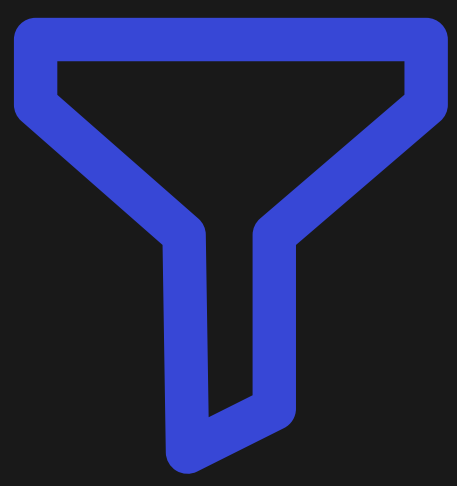
# Authorization

Once the user is authenticated, Spring Security will check to see what actions the user is allowed to perform based on their role and other security-related information. This is called authorization, and it determines what resources a user can access and what actions they can perform.

amigoscode.com

# Filters

Spring Security uses a chain of filters to process incoming requests and enforce security rules. Each filter performs a specific task, such as checking the authenticity of requests or performing authorization.



amigoscode.com

# Configuration

The security rules for a Spring Security-protected application are defined in a configuration file. This configuration file determines which resources are protected, what actions are allowed for each resource, and what authentication and authorization mechanisms are used.

amigoscode.com

# Security Context

The Spring Security framework maintains a security context for each user session, which holds information about the user's authentication status and what actions they are allowed to perform. This information is used to make authorization decisions for each request.

amigoscode.com

# Access Desisions

When a request is received, the security filters in the filter chain will use the information in the security context to make access decisions for that request. If the request is granted, the request will continue to be processed by the application. If the request is denied, the user will be redirected to an error page or a login page, depending on the nature of the request and the security configuration.


amigoscode.com


PREMIUM PROGRAMMING
COURSES

amigoscode.com