Architecture Deep Dive in Spring Security

Spring Security is a framework that provides authentication, authorization, and protection against common attacks.it is the de-facto standard for securing Spring-based applications.

3 Key Areas in Security

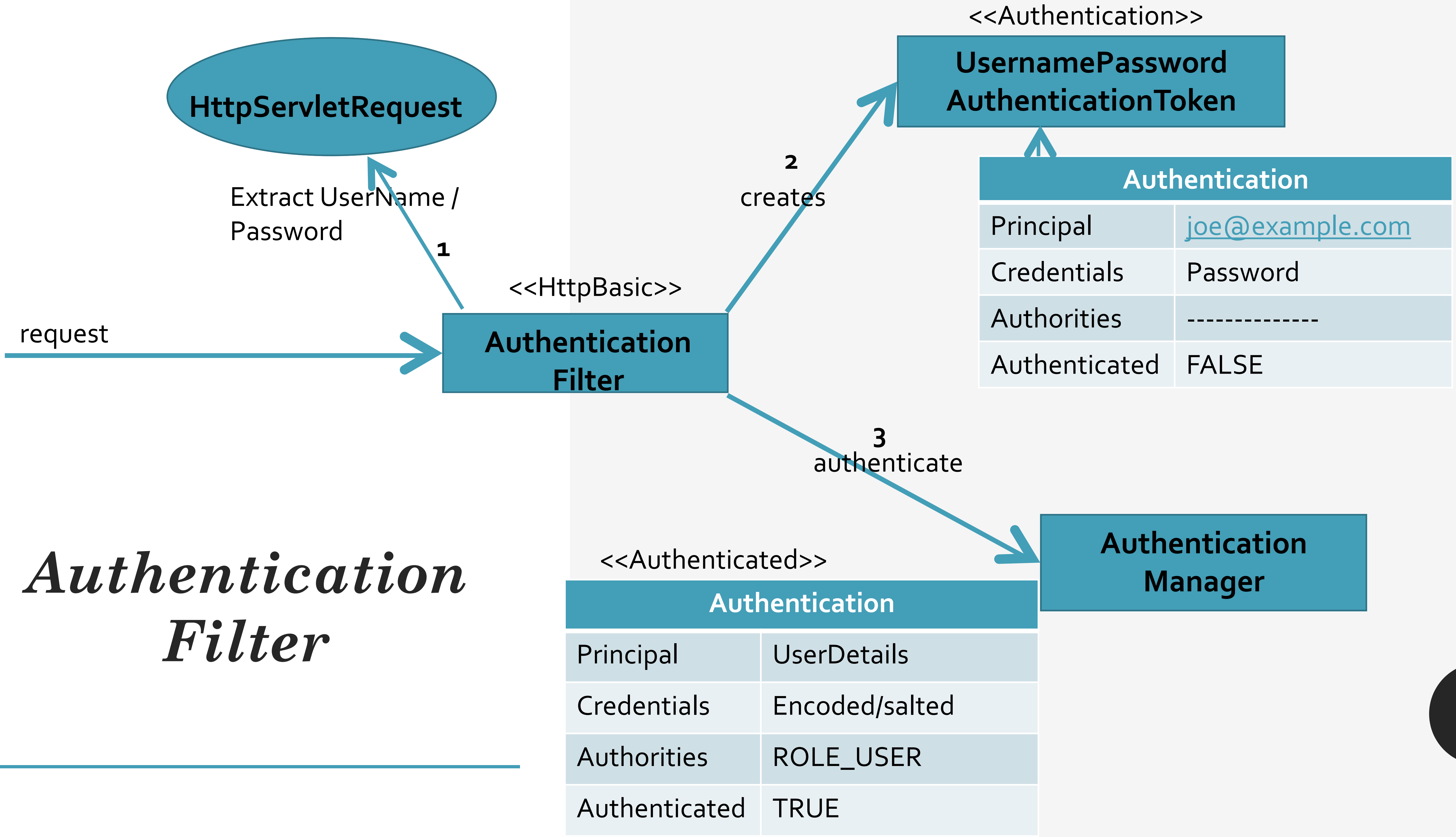
- Authentication
- Authorization
- Exception Handling

Authentication

- **Who am I ?**
- **Authentication Strategies**
  - Authenticating users to your web apps ensures that the wrong people don’t get access to your service.
  - Without strong authentication and proper implementation strategies, your service could be compromised, which means anything from user data could be stolen to even permanent shutdown of the business or organization your web services support.

    - HTTP Basic Auth
    - Custom Form Login
    - OAuth
    - OAuth 2.0
    - JSON Web Tokens (JWT)
    - Single-Sign-On

Authentication Filter

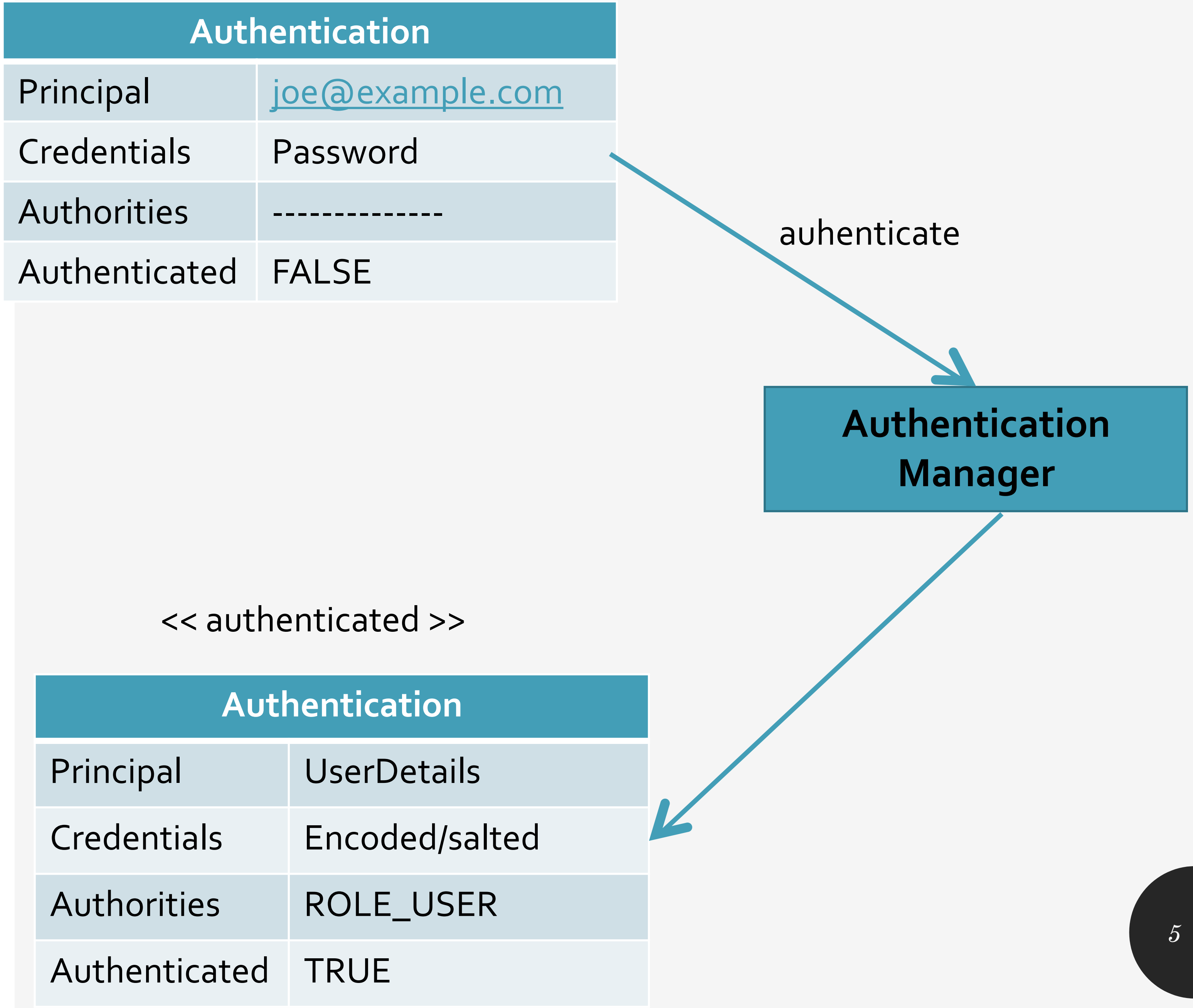


Authentication	
Principal	joe@example.com
Credentials	Password
Authorities	--------------
Authenticated	FALSE

<<Authenticated>>

Authentication	
Principal	UserDetails
Credentials	Encoded/salted
Authorities	ROLE_USER
Authenticated	TRUE

Authentication



Authentication	
Principal	joe@example.com
Credentials	Password
Authorities	--------------
Authenticated	FALSE

auhenticate

Authentication Manager

<< authenticated >>

Authentication	
Principal	UserDetails
Credentials	Encoded/salted
Authorities	ROLE_USER
Authenticated	TRUE

org.springframework.security.authentication

Authentication Manager

- public interface AuthenticationManager

- Processes an Authentication request.

- Authentication authenticate(Authentication auth)

  - Attempts to authenticate the passed Authentication object, returning a fully populated Authentication object (including granted authorities) if successful.

org.springframework.security.authentication

ProviderManager

- public class ProviderManager

  implements AuthenticationManager

  - Iterates an Authentication request through a list of AuthenticationProviders.

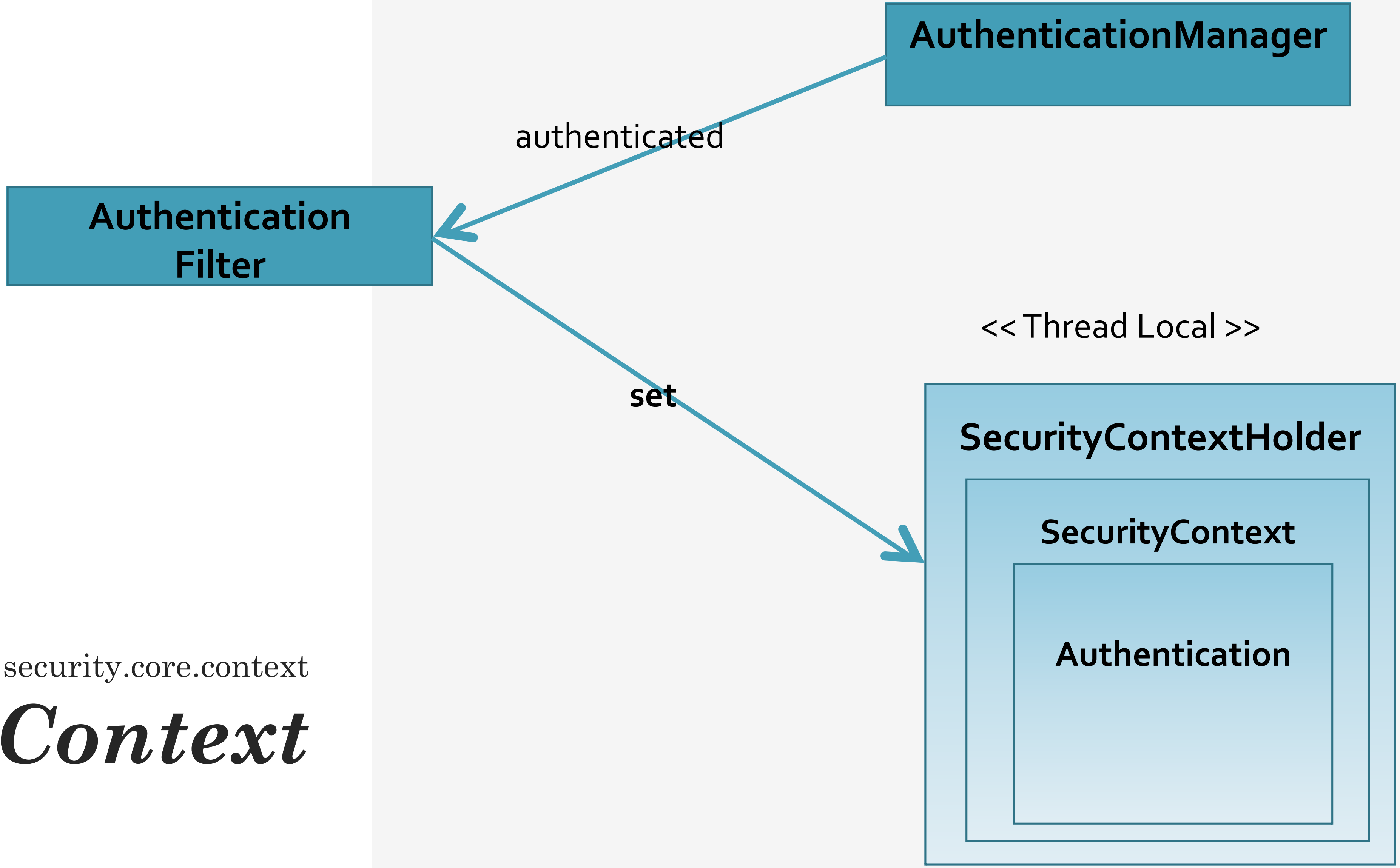
org.springframework.security.authentication

Authentication Provider

- public interface AuthenticationProvider
- Indicates a class can process a specific Authentication implementation.

org.springframework.security.core.context

SecurityContext



Authentication Recap

- Authentication Filter creates an “Authentication Request" and passes it to the Authentication Manager

- Authentication Manager delegates to the Authentication Provider

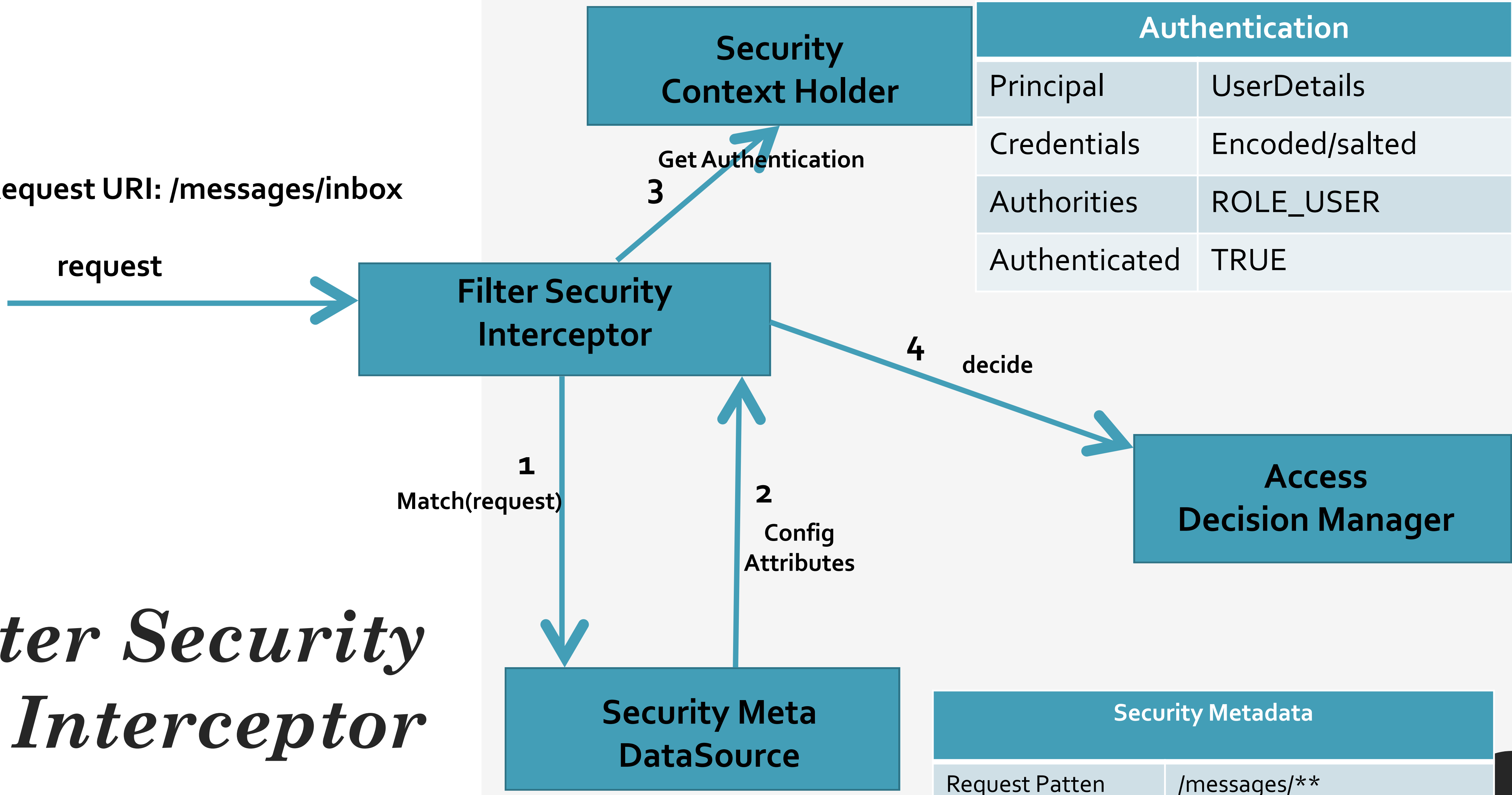
- Authentication Provider uses a UserDetailsService to load the UserDetails and returns an “Authenticated Principal”

- Authentication Filter sets the Authentication in the SecurityContext

Authorization

- **Authorization** is the function of specifying access rights/privileges to resources related to information security and computer security in general and to access control in particular.

Filter Security Interceptor



Authentication	
Principal	UserDetails
Credentials	Encoded/salted
Authorities	ROLE_USER
Authenticated	TRUE

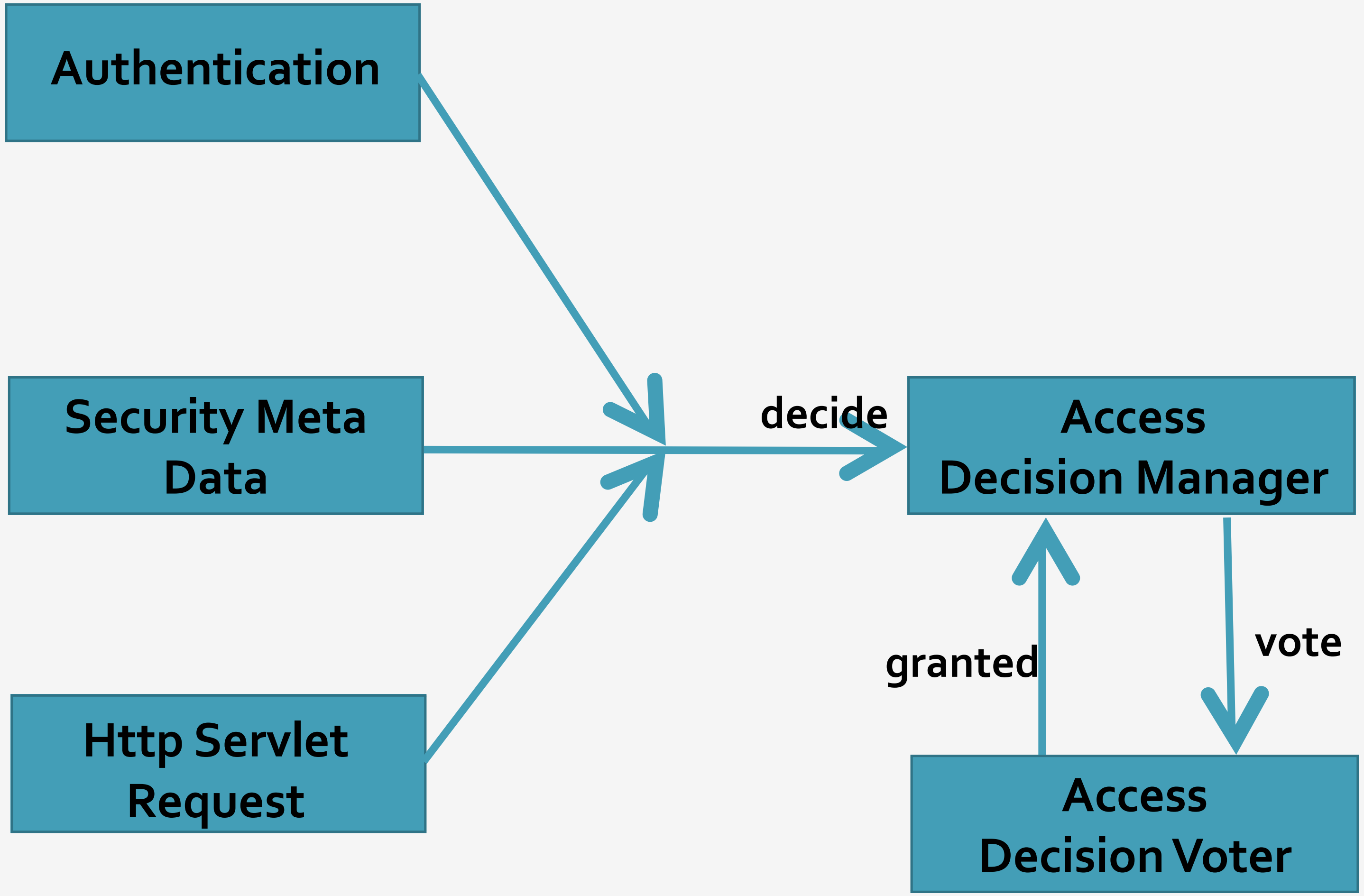
Security Metadata	
Request Patten	/messages/**
Config Attribute	ROLE_USER

Authentication	
Principal	UserDetails
Credentials	Encoded/salted
Authorities	ROLE_USER
Authenticated	TRUE

Security Metadata	
Request Patten	/messages/**
Config Attribute	ROLE_USER

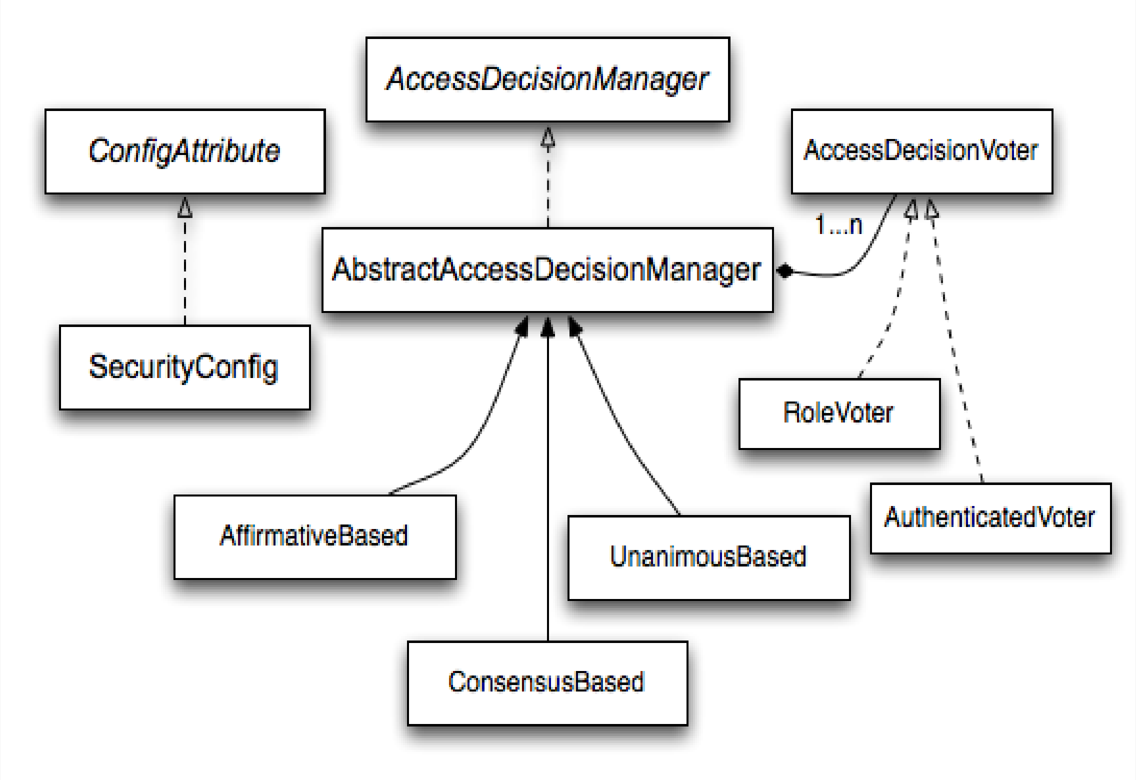
Request URI: /messages/inbox

Filter Security Interceptor



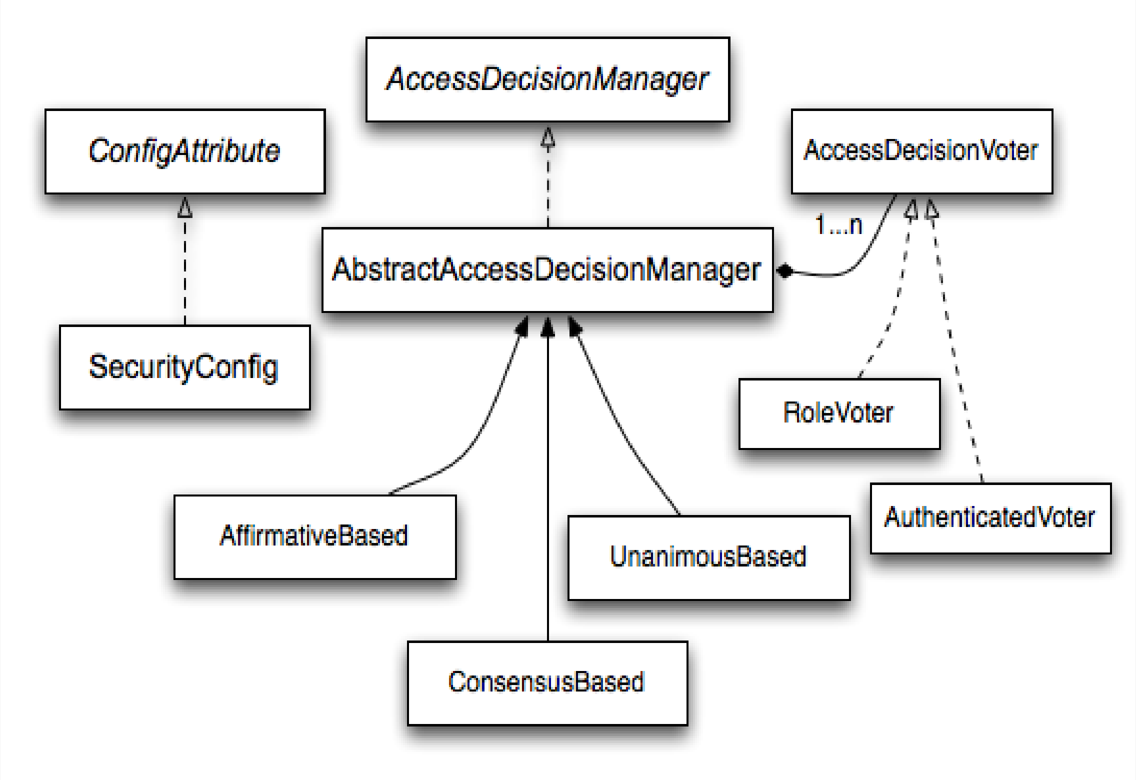
AccessDecision Manager

- public interface AccessDecisionManager
- Makes a final access control (authorization) decision.



AccessDecision Voter

- public interface AccessDecisionVoter<S>
- Indicates a class is responsible for voting on authorization decisions.



Authorization Recap

- FilterSecurityInterceptor obtains the “Security Metadata” by matching on the current request

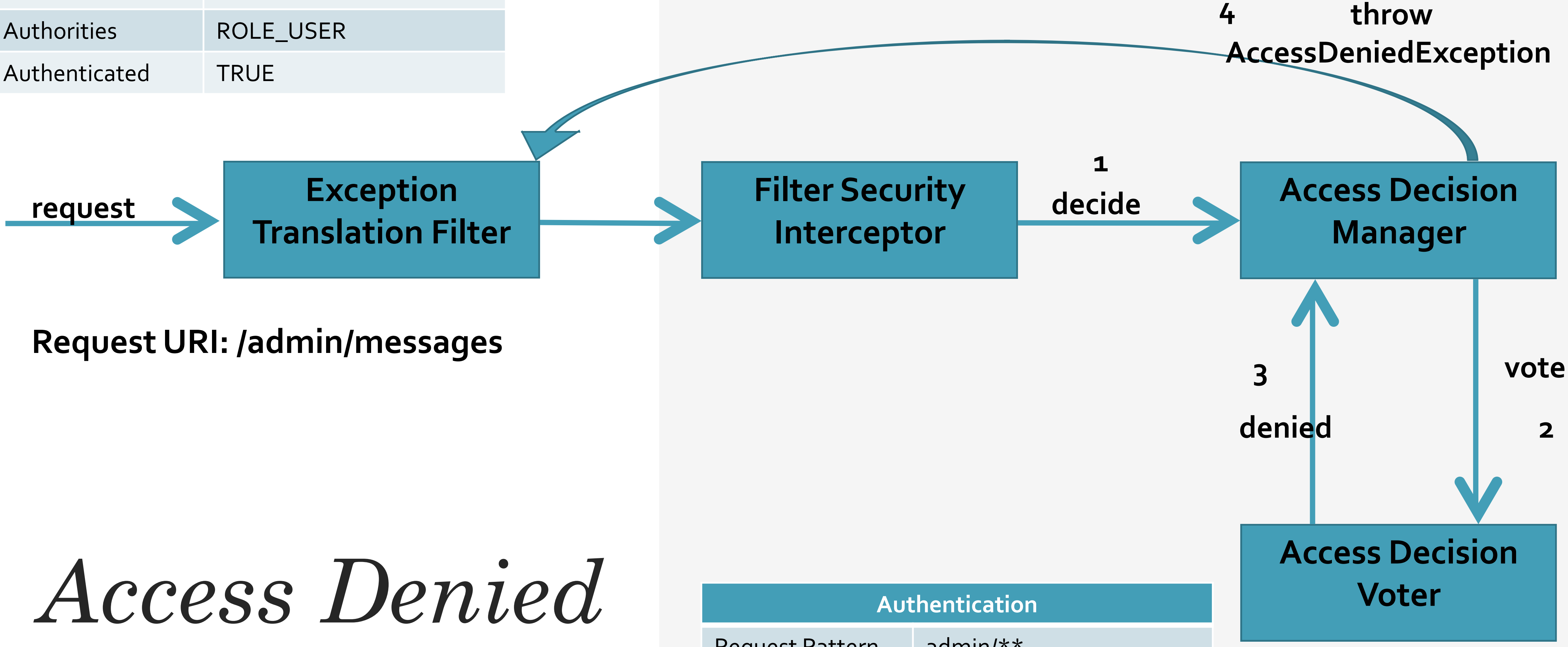
- FilterSecurityInterceptor gets the current Authentication

- The Authentication, Security Metadata and Request is passed to the AccessDecisionManager

- The AccessDecisionManager delegates to it's AccessDecisionVoter(s) for decisioning

Exception Handling

Authentication	
Principal	UserDetails
Credentials	Encoded/salted
Authorities	ROLE_USER
Authenticated	TRUE

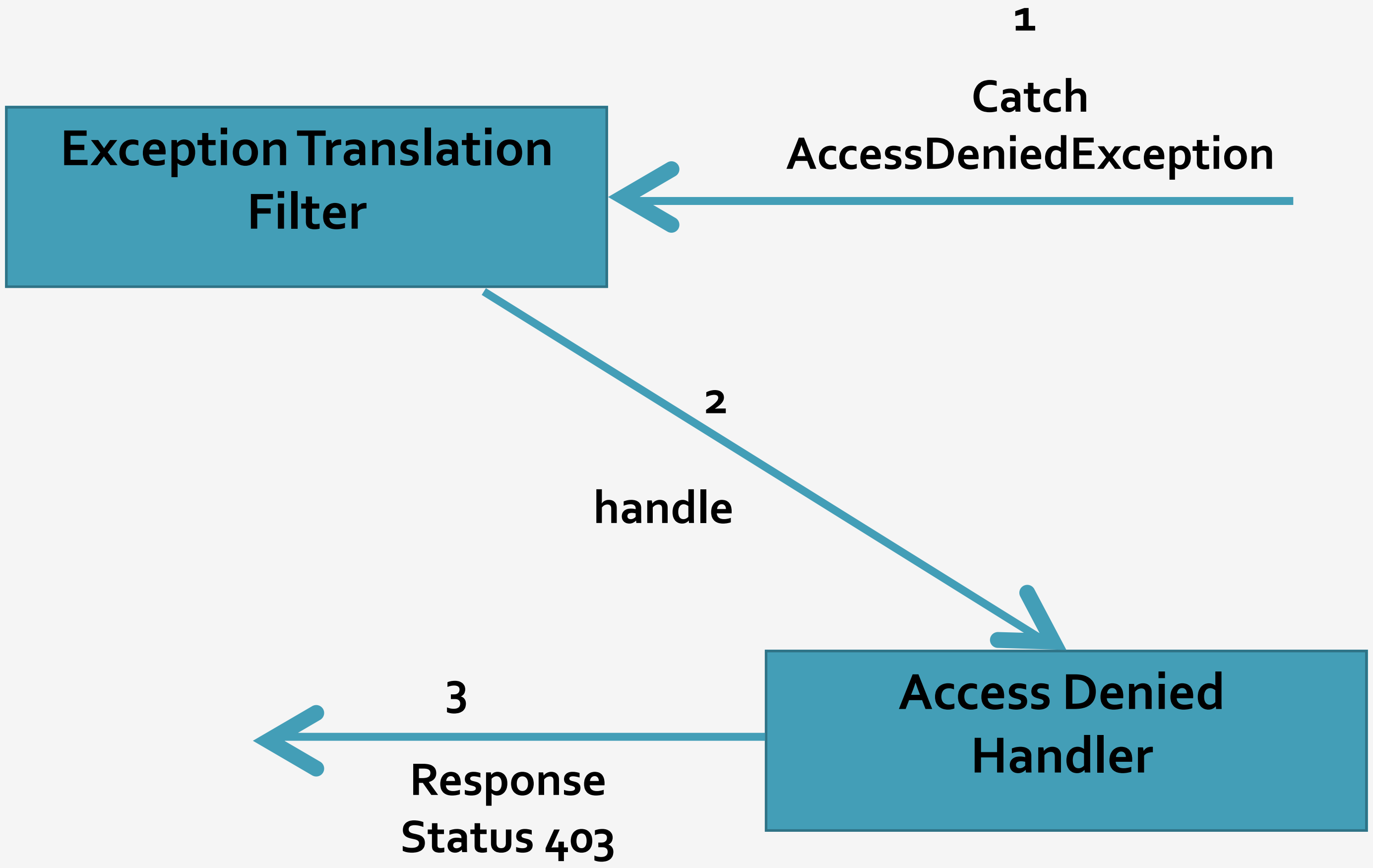

4 throw AccessDeniedException
request
Exception Translation Filter
Filter Security Interceptor
1 decide
Access Decision Manager
3 denied
vote 2
Access Decision Voter

Request URI: /admin/messages

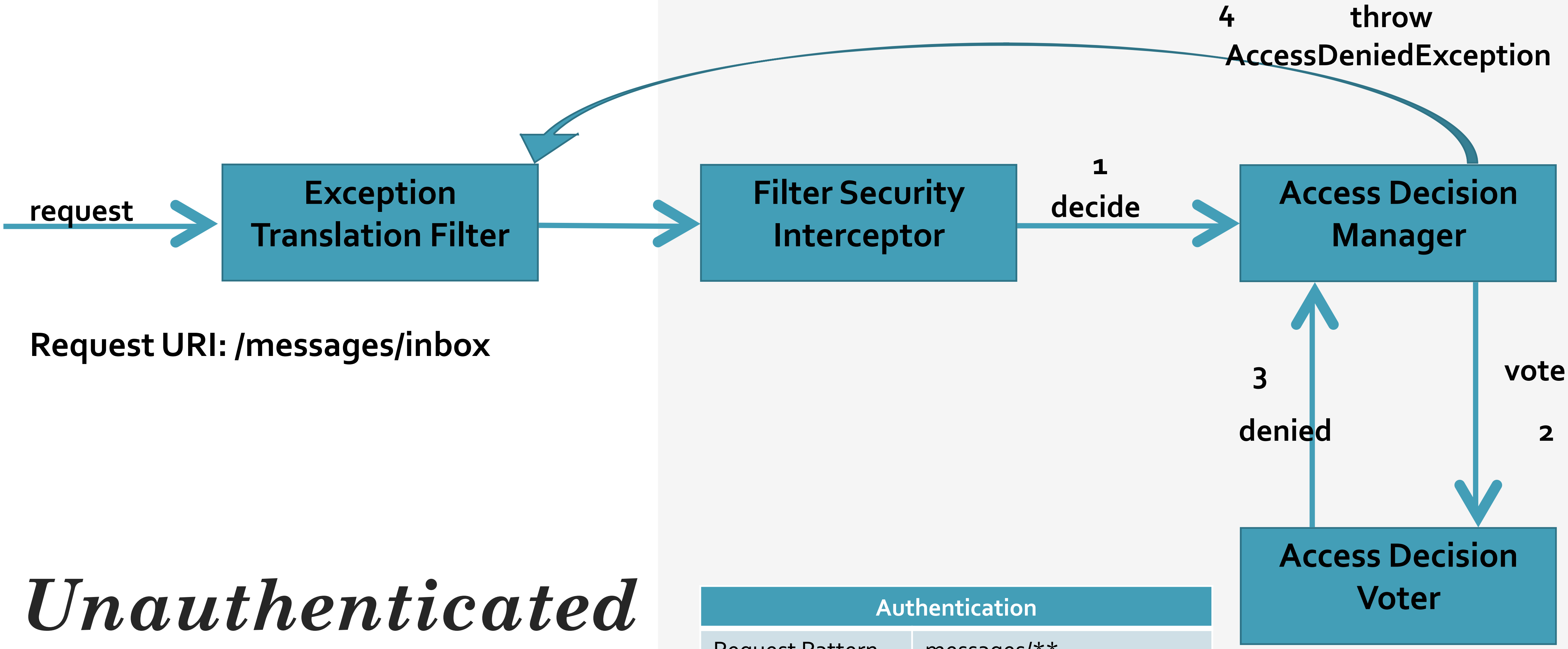
Access Denied

Authentication	
Request Pattern	admin/**
Config Attributes	ROLE_ADMIN

Access Denied Handler



Authentication	
Principal	anonymousUser

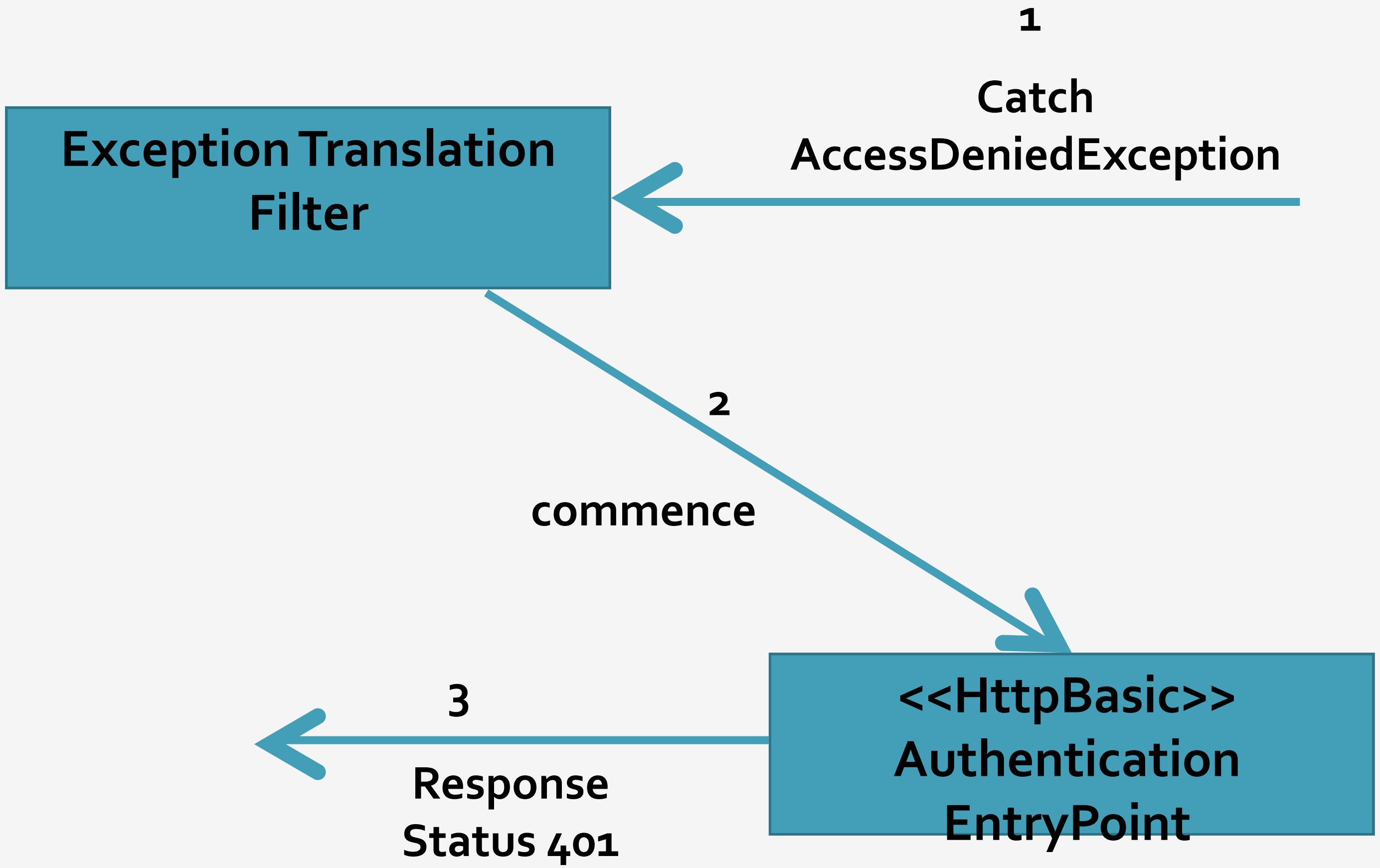

4 throw AccessDeniedException
request
Exception Translation Filter
Filter Security Interceptor
1 decide
Access Decision Manager
3 denied
vote 2
Access Decision Voter

Request URI: /messages/inbox

Unauthenticated

Authentication	
Request Pattern	messages/**
Config Attributes	ROLE_USER

Start Authentication



WWW-Authenticate: Basic realm=spring

Exception Handling Recap

- When "Access Denied" for current Authentication, the ExceptionTranslationFilter delegates to the AccessDeniedHandler, which by default, returns a 403 Status.

- When current Authentication is "Anonymous", the ExceptionTranslationFilter delegates to the AuthenticationEntryPoint to start the Authentication process.