NOVATEC

Authentication & Authorization made easy with Spring Security

What‘s new in
Spring Security 6.3, 6.4, 7.0 and
Spring Authorization Server 1.3

Slides & Demo Code

https://github.com/andifalk/whats-new-in-spring-security

Agenda

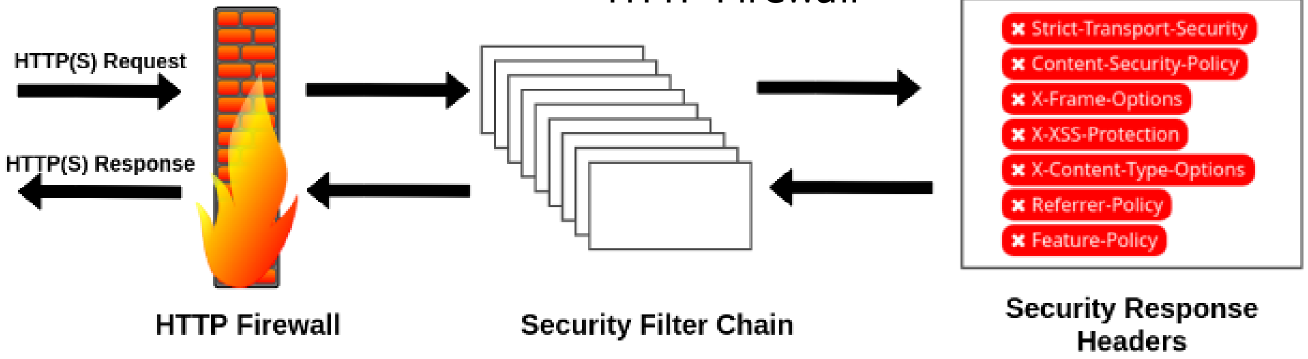
1. Spring Security Introduction
2. What‘s new in Spring Security
   – 6.3
   – 6.4
   – 7.0 (Passkeys)
3. What‘s new in
   Spring Authorization Server 1.3

Spring Security Introduction

- Authentication
  - Basic Auth & Session Cookies
  - SAML 2.0
  - OAuth 2.1 & OpenID Connect
  - …

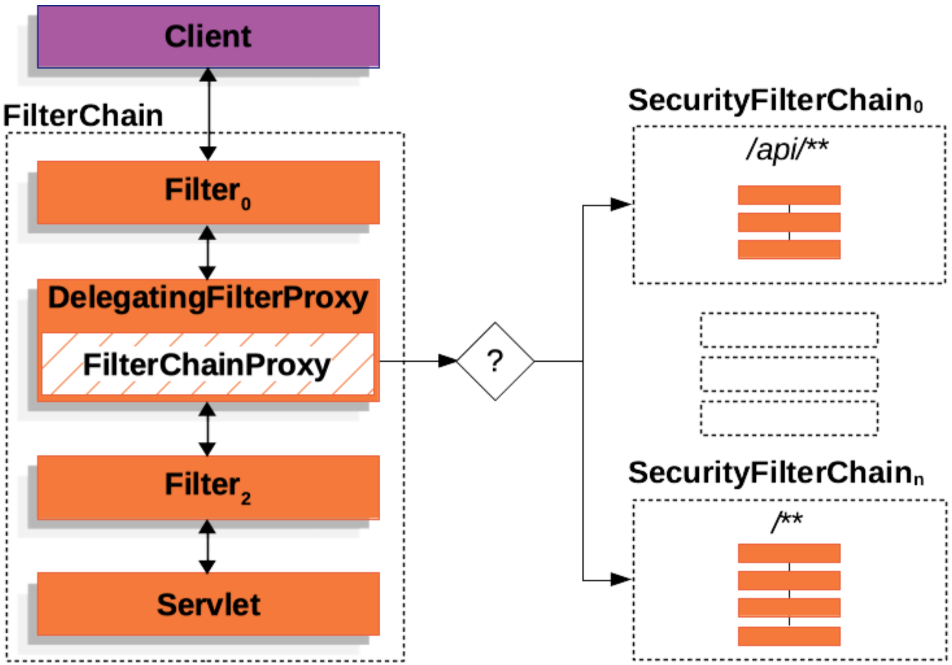
- Authorization
  - Request Based
  - Method Based
- Protection Against Exploits
  - CSRF
  - Security Response Headers
  - HTTP Firewall

- Supports Servlet & WebFlux Stacks



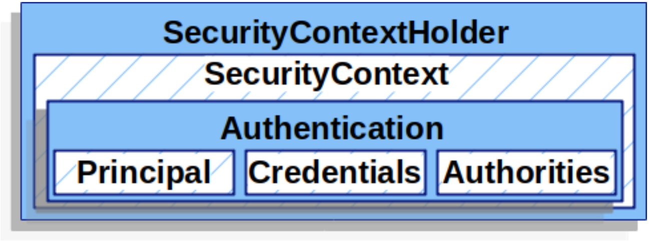
Authentication Architecture & Mechanisms

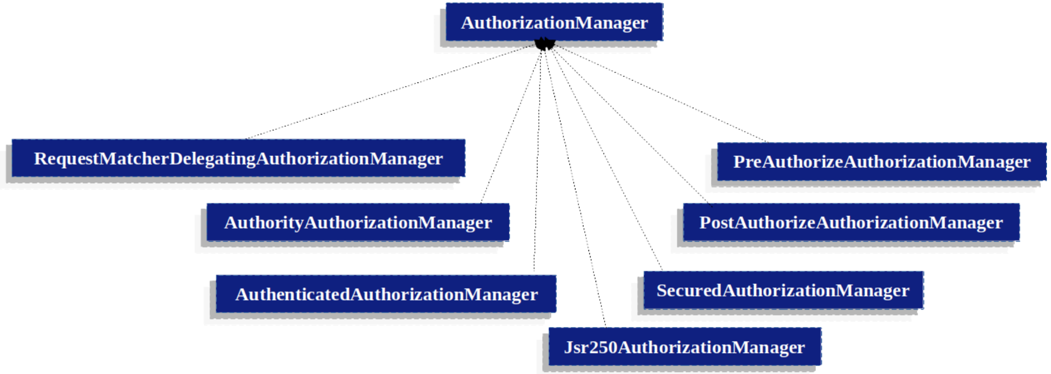
- Username and Password
  (BCrypt, SCrypt, Argon2, Pbkdf2)
- Remember Me (Cookie)
- Central Authentication Server (CAS)
- Java Authentication and Authorization Service (JAAS)
- Pre-Authentication (i.e. using SiteMinder)
  (Only use Spring Security for Authorization)
- X.509 Authentication (Mutual TLS)
- SAML 2.0
- OAuth 2.1 & OpenID Connect
  (JWT & Opaque Tokens)



Authorization Architecture & Mechanisms

- HTTP Request Authorization
- Method Security
  - @Pre-/@PostAuthorize
  - @Pre-/@PostFilter
- Domain Object Security
  with Access Control Lists (ACLs)
- Authorization Events
- Spring Data Integration

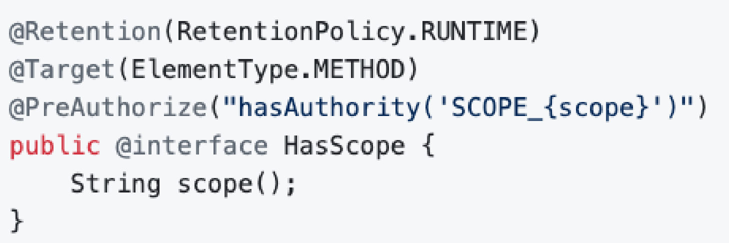



AuthorizationManager
RequestMatcherDelegatingAuthorizationManager
PreAuthorizeAuthorizationManager
AuthorityAuthorizationManager
PostAuthorizeAuthorizationManager
AuthenticatedAuthorizationManager
SecuredAuthorizationManager
Jsr250AuthorizationManager

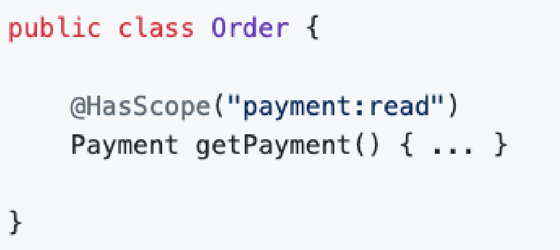
https://docs.spring.io/spring-security/reference/servlet/authorization/index.html
https://docs.spring.io/spring-security/reference/servlet/integrations/data.html

What’s new in Spring Security 6.3

- Authentication
  - Compromised Password Checking (Have I Been Pwned API)
  - OAuth 2.0 Token Exchange Grant
- Authorization
  - Annotation Parameters
  - Secure Return Values
  - Error Handling



```
@Retention(RetentionPolicy.RUNTIME)
@Target(ElementType.METHOD)
@PreAuthorize("hasAuthority('SCOPE_{scope}')")
public @interface HasScope {
    String scope();
}
```

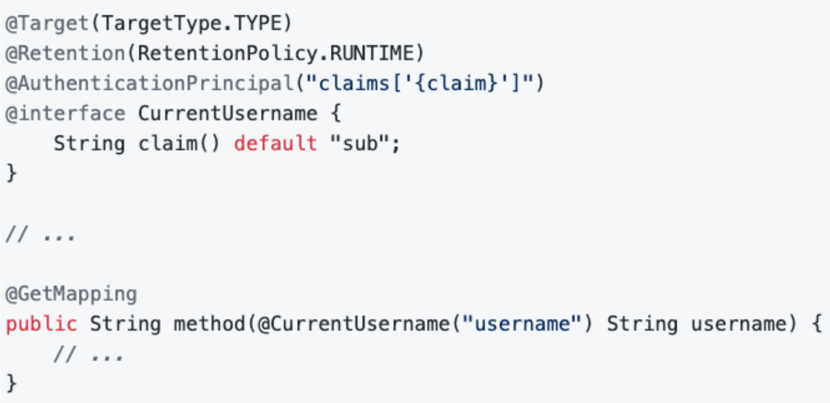


```
public class Order {

    @HasScope("payment:read")
    Payment getPayment() { ... }

}
```

https://docs.spring.io/spring-security/reference/6.3/whats-new.html

What’s new in Spring Security 6.4

- Authentication
  - One-Time Token Login
  - OAuth 2.0 Support for RestClient (OAuth2ClientHttpRequestInterceptor)
  - OpenSAML 5 Support
- Authorization
  - Annotation templates support for @AuthenticationPrincipal and @CurrentSecurityContext
- *Any Requests* Security Filter Chain Validation
- Improved Kotlin Support (i.e. @Pre-/@PostFilter

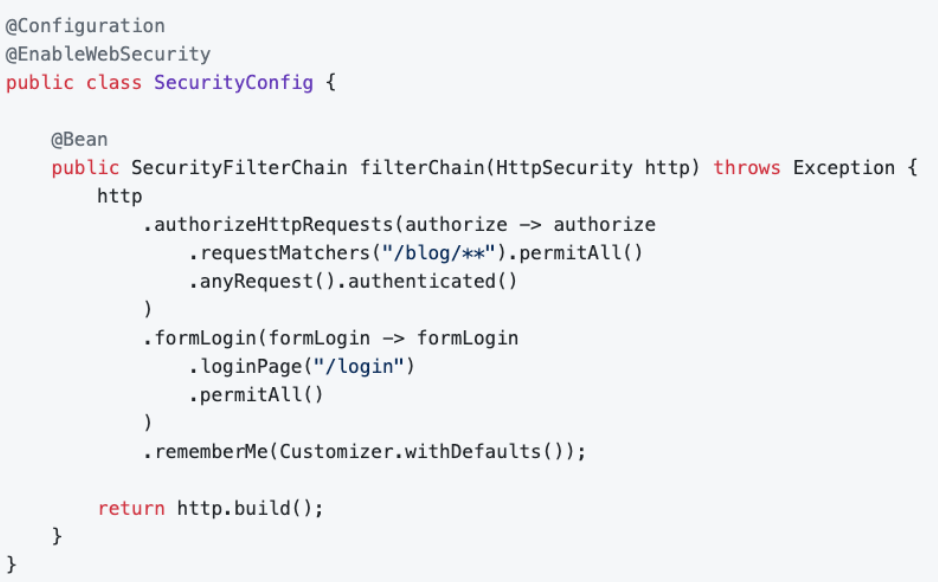


```
@Target(TargetType.TYPE)
@Retention(RetentionPolicy.RUNTIME)
@AuthenticationPrincipal("claims['{claim}']")
@interface CurrentUsername {
    String claim() default "sub";
}

// ...

@GetMapping
public String method(@CurrentUsername("username") String username) {
    // ...
}
```

https://docs.spring.io/spring-security/reference/6.4-SNAPSHOT/whats-new.html

What’s new in Spring Security 7.0

- Authentication
  - WebAuthn / Passkeys Support (?)
- Configuration
  - Usage of Lambda DSL mandatory



```
@Configuration
@EnableWebSecurity
public class SecurityConfig {

    @Bean
    public SecurityFilterChain filterChain(HttpSecurity http) throws Exception {
        http
            .authorizeHttpRequests(authorize -> authorize
                .requestMatchers("/blog/**").permitAll()
                .anyRequest().authenticated()
            )
            .formLogin(formLogin -> formLogin
                .loginPage("/login")
                .permitAll()
            )
            .rememberMe(Customizer.withDefaults());

        return http.build();
    }
}
```

https://github.com/rwinch/spring-security-webauthn

https://github.com/joshlong-attic/springone-2024-goodbye-passwords

https://docs.spring.io/spring-security/reference/6.4-SNAPSHOT/migration-7/index.html

Passkeys (FIDO2) 1x1

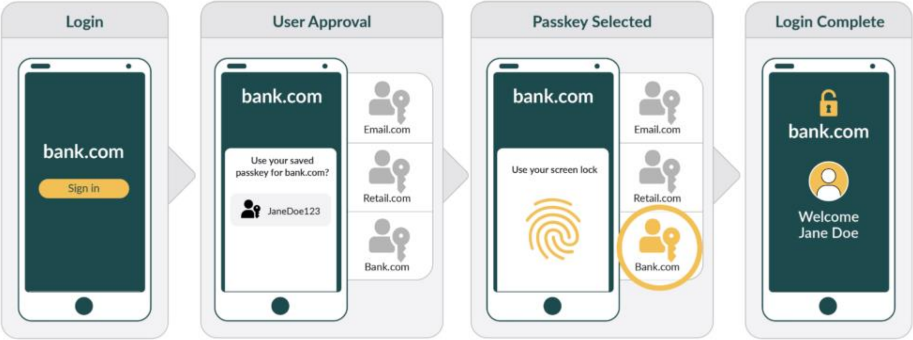
- Replacement for passwords
- Unique cryptographic public/private key pairs (passkeys) to every online service
- Provides faster, easier, and more secure sign-ins to websites and apps
- Works across user's devices.
- Strong and phishing-resistant.

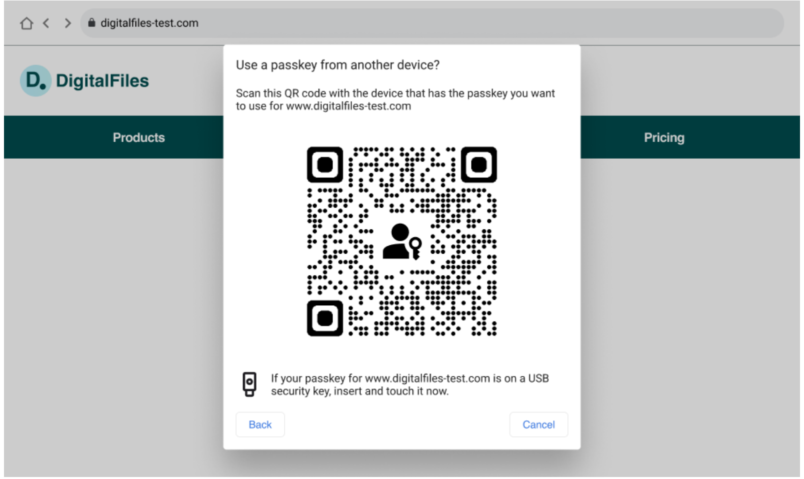
https://fidoalliance.org/passkeys

https://passkeys.dev

https://www.w3.org/TR/webauthn

https://passkeys.directory





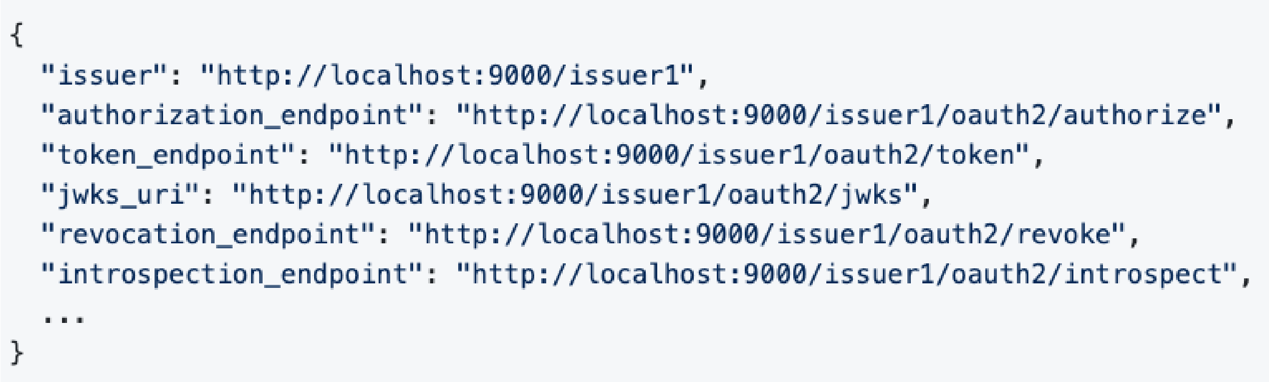
Use a passkey from another device?

Scan this QR code with the device that has the passkey you want to use for www.digitalfiles-test.com

If your passkey for www.digitalfiles-test.com is on a USB security key, insert and touch it now.

What’s new in
Spring Authorization Server 1.3

- RFC 8705 OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens
- RFC 8693 OAuth 2.0 Token Exchange
- Multitenancy support



```
{
  "issuer": "http://localhost:9000/issuer1",
  "authorization_endpoint": "http://localhost:9000/issuer1/oauth2/authorize",
  "token_endpoint": "http://localhost:9000/issuer1/oauth2/token",
  "jwks_uri": "http://localhost:9000/issuer1/oauth2/jwks",
  "revocation_endpoint": "http://localhost:9000/issuer1/oauth2/revoke",
  "introspection_endpoint": "http://localhost:9000/issuer1/oauth2/introspect",
  ...
}
```

https://spring.io/blog/2024/05/22/spring-authorization-server-1-3-goes-ga

NOVATEC

Thank You! Questions?

https://github.com/andifalk/whats-new-in-spring-security

NOVATEC

Novatec Consulting GmbH
Bertha-Benz-Platz 1
D-70771 Leinfelden-Echterdingen

T. +49 711 22040-700
info@novatec-gmbh.de
www.novatec-gmbh.de