



라이브 세션-Spring Security 기본-2022.09.21(수)

✓ 인증(Authentication)과 권한 부여(Authorization)

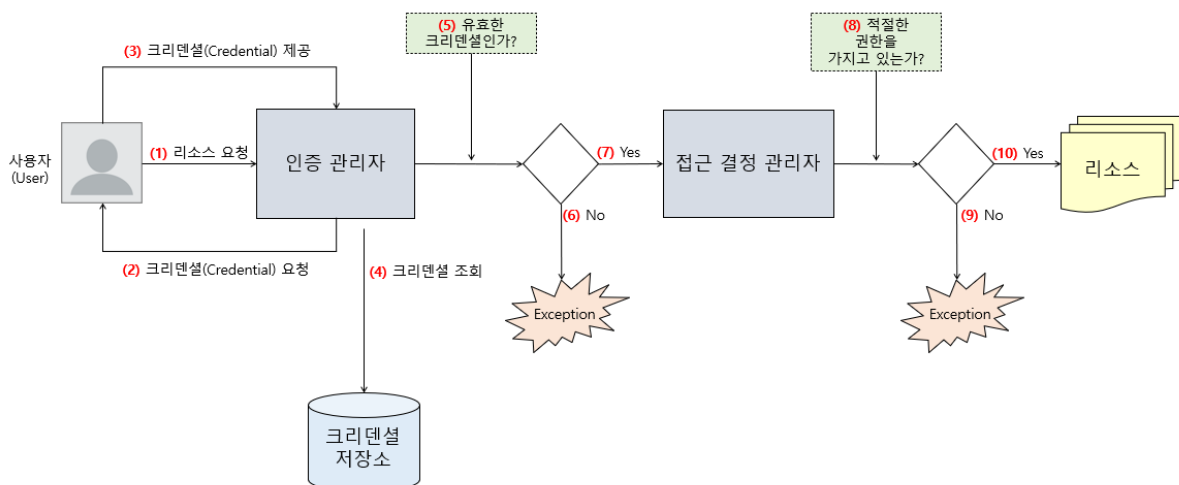
1 인증(Authentication)

- 사용자(클라이언트)가 본인이 맞는지 확인하는 과정
- 일상 생활에서의 인증 예
 - 주민등록증, 운전 면허증, 여권 등을 통한 신원 확인
 - 2 팩터(factor) 인증 예
 - 1차 인증: 신용 카드, 체크 카드 칩안에 포함된 정보
 - 2차 인증: 비밀 번호
- 애플리케이션에서의 인증 예
 - 회원 아이디/패스워드 기반 인증
 - Spring Security에서는 Username/Password 기반 인증과 같음
 - JWT를 통한 자격 검증
 - OAuth2를 이용한 인증
 - 타 서비스에게 인증을 위임하는 방식
 - 2 팩터(factor) 인증 예
 - 온라인 बैं킹
 - 공인 인증서 + 시크릿 카드 또는 OTP 생성기
 - 주식 또는 암호 화폐 거래소
 - 로그인 인증 + 공인 인증서 확인

2 권한 부여(인가, Authorization)

- 인증된 사용자(클라이언트)가 적절한 접근 권한을 가지고 있는지 확인하는 과정
- 일상 생활에서의 권한 부여 예
 - 비행기, 콘서트, 스포츠, 극장에서의 티켓별 등급 좌석
- 애플리케이션에서의 권한 부여
 - 역할(Role) 기반의 권한 부여
 - URL에 접근할 권한이 있는지 확인
 - 메서드에 대한 접근 권한
 - 그룹 기반의 권한 부여
 - 대표적인 예
 - Github의 Repository 접근 그룹 지정

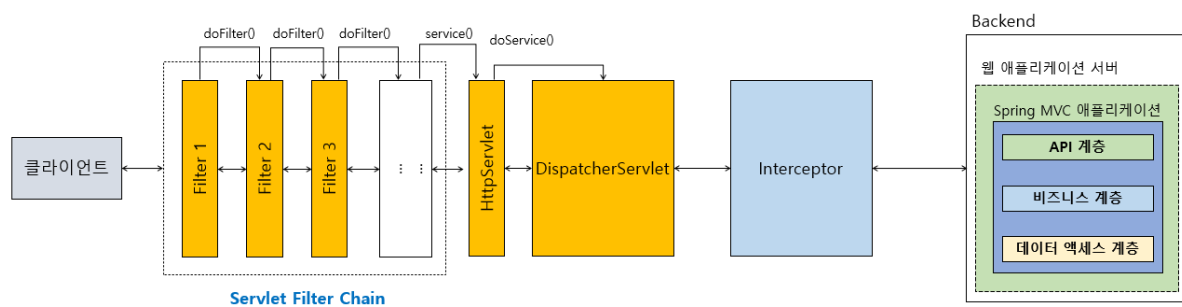
✓ 보호된 웹 애플리케이션의 일반적인 요청 흐름

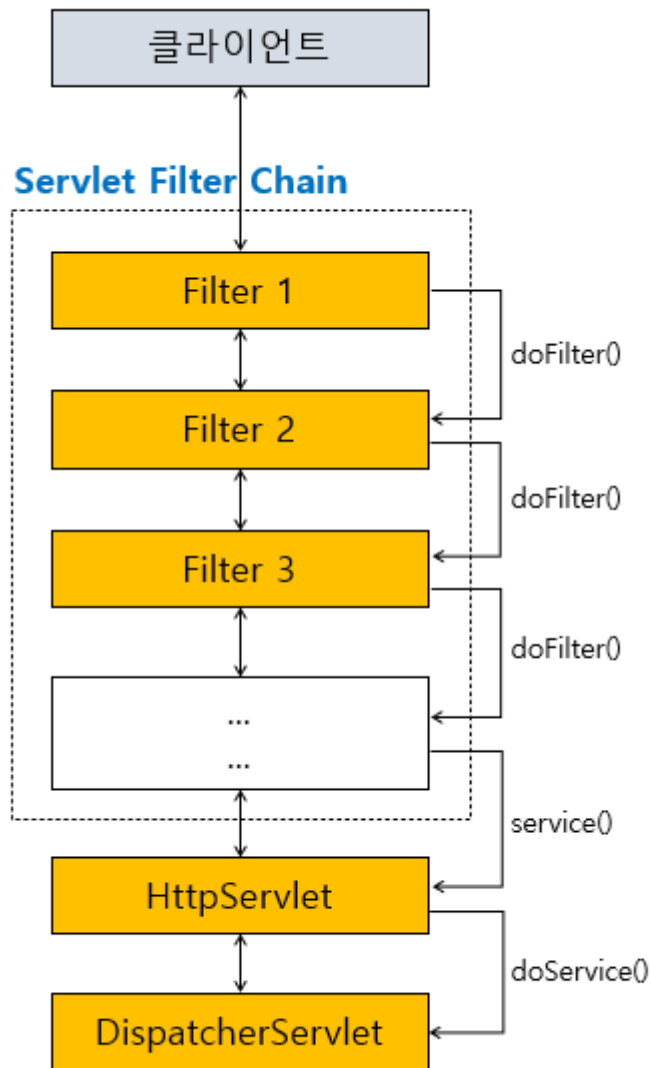


- **크리덴셜(Credentials)**

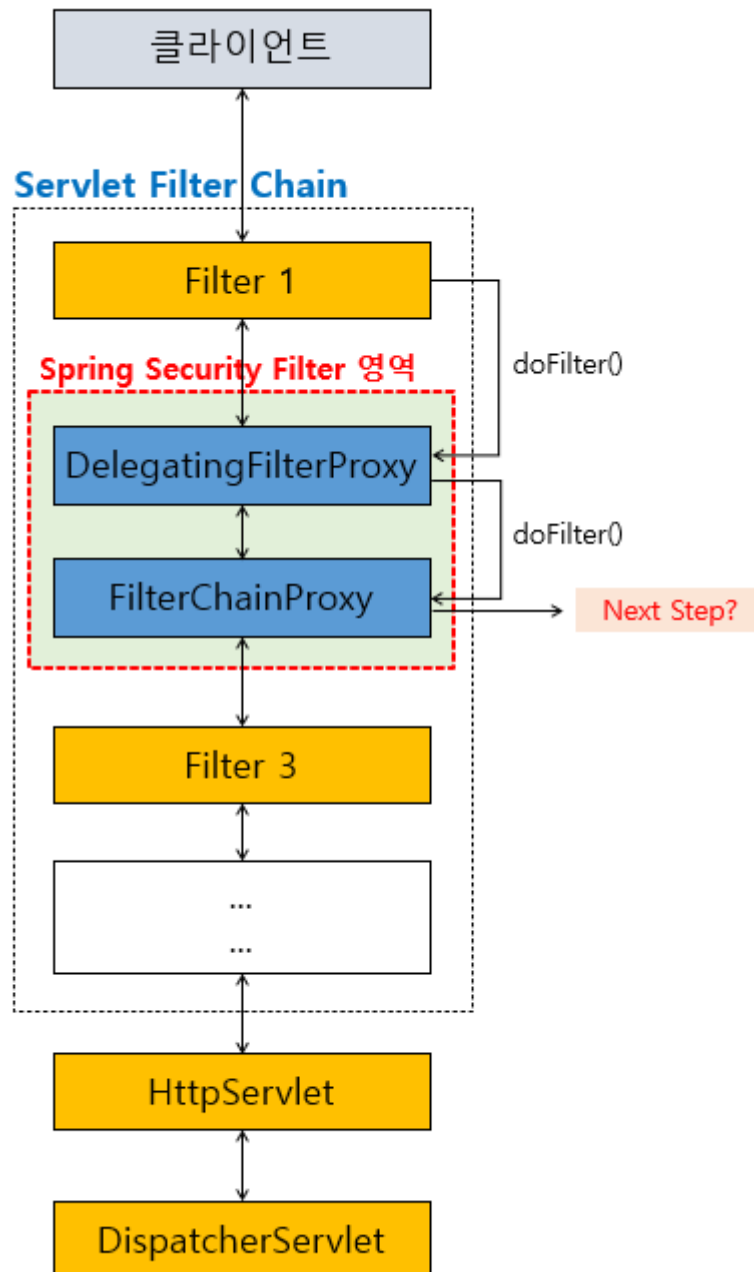
- 사용자가 자신이 맞는지 인증하기 위한 자격 증명 정보
 - 아이디/패스워드

✓ Java 기반의 웹 애플리케이션에서의 서블릿 필터(Servlet Filter)와 필터 체인(Filter Chain)





✅ 서블릿 필터와 Spring Security 필터의 관계



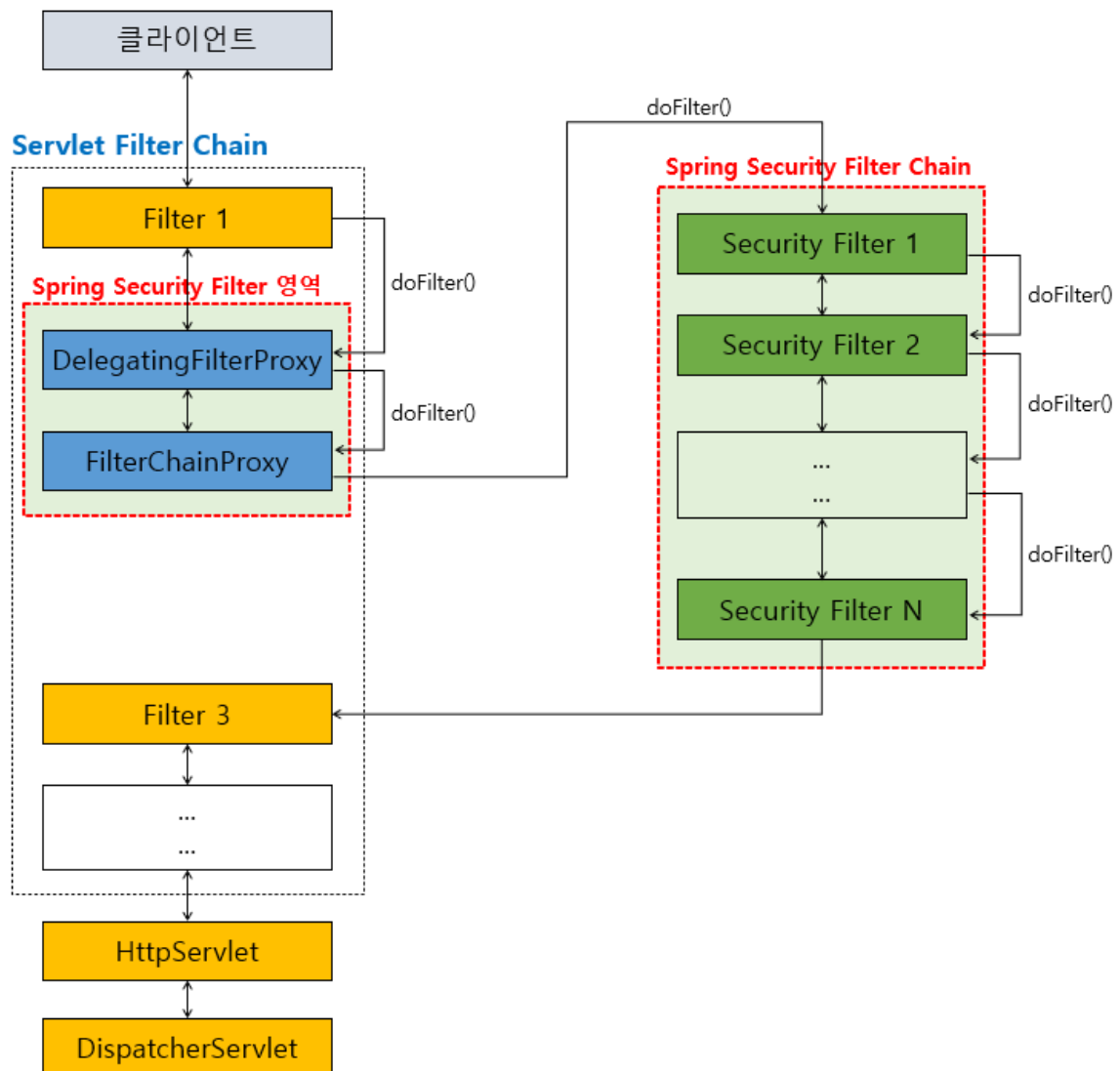
1 DelegatingFilterProxy

- 서블릿 컨테이너 영역의 필터와 ApplicationContext에 Bean으로 등록된 필터들을 연결해주는 브릿지 역할을 한다

2 FilterChainProxy

- Spring Security의 Filter를 사용하기 위한 진입점

- Filter Chain은 URL 별로 여러개 등록 가능
- Filter Chain이 있을 때 어떤 Filter Chain을 사용할지는 FilterChainProxy가 결정하며, 가장 먼저 매칭된 Filter Chain을 실행한다.





Spring Security에서 지원하는 Filter 종류

- 애플리케이션 실행 로그로 확인
-



패스워드 암호화

- 암호화란?
 - 사용자의 민감한 정보를 보호하기 위한 기술
- Cryptography
 - 암호학적 관점에서의 암호화 전체를 아우르는 말
- Crypto Currency
 - 암호 화폐
- Encryption
 - 암호화
- Decryption
 - 복호화
- Encoding / Decoding
 - 데이터의 형식이나 패턴을 목적에 맞게 변환하는 과정
- 암호화 유형
 - 양방향 암호화
 - 암호화도 되고 복호화도 되는 암호화 방식
 - 단방향 암호화
 - 암호화는 되지만 복호화는 되지 않는 암호화 방식
- 키 유형에 따른 암호화 방식
 - 대칭키 암호화 방식

- 하나의 키를 서로 공유해서 해당 키로 암호화/복호화를 수행
 - 비대칭키 암호화 방식
 - 암호화를 수행하는 키와 복호화를 수행하는 키가 다르다.
 - Public Key와 Private Key
 - Public Key로 암호화 하는 것은 민감한 데이터 또는 메시지 보호를 위해서.
 - Private Key로 암호화 하는 것은 디지털 서명을 위해서.
 - 블록체인이 이런 방식임.
-

Hello Spring Security 샘플 애플리케이션 리뷰

- 코드로 확인