KB금융그룹 | 국민의 평생 금융파트너

2025년 상반기 K-디지털 트레이닝

Security Filter Chain

[KB] IT's Your Life

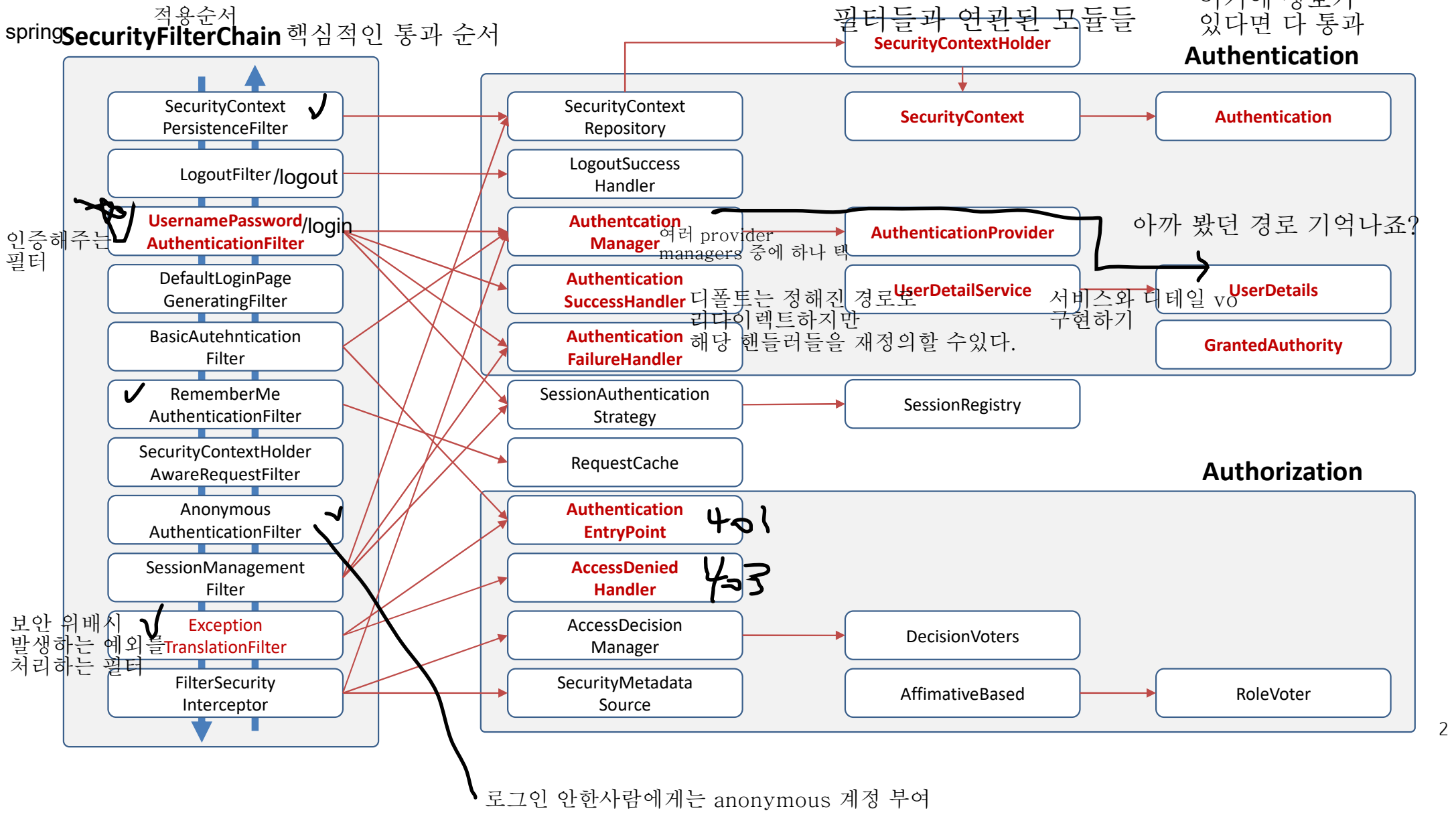
KB 국민은행

클라가 jwt를 갖고 있다가 로그아웃하면 버려버리면 돼

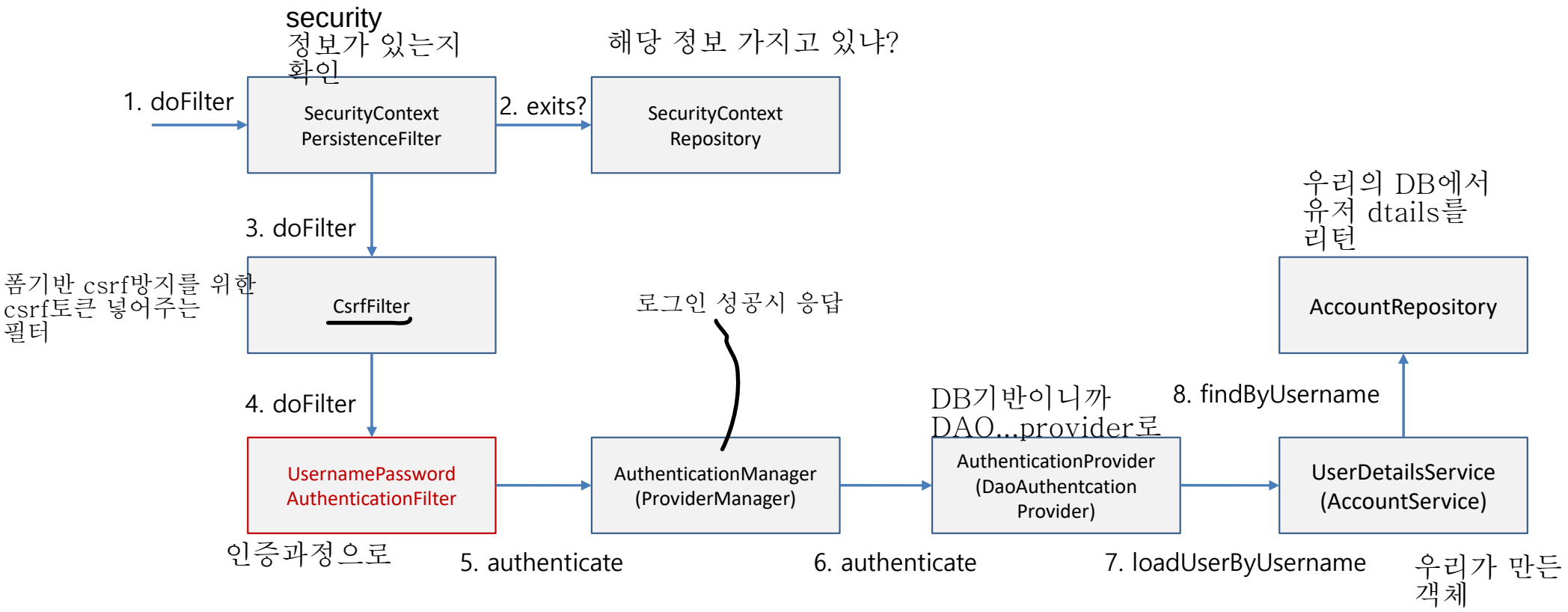
쿼리스트링이나 multipart 형식으로 아이디와 비번이 넘어가는 요청이면 (폼기바)이면 그냥 usernamepasswordauthenticationfilter을 사용하면 되지만

JSON형식으로 담아서 오면 JWT용 usernamepasswordauthenticationfilter를 커스텀해서 사용해야한다,

Security Filter Chain



Security Filter Chain



받은 user details로

실제 password하고
입력한거하고 같은 확인

각 필터의 대한 설명 나중에 참고

Security Filter Chain

SecurityContextPersistenceFilter

- request가 발생하면 SecurityContext 객체의 생성, 저장, 조회를 담당하는 필터
- 새로운 SecurityContext를 생성하여 SecurityContextHolder에 저장 — 로그인(인증)완료후엔
- 익명의 사용자의 경우
  - AnonymousAuthenticationFilter에서 AnonymousAuthenticationToken객체를 SecurityContext에 저장
- 인증 시
  - UsernamePasswordAuthenticationFilter에서 인증 성공 후 SecurityContext에 UsernamePasswordAuthentication객체를 Authentication객체와 함께 저장
  - 인증이 완료되면 Session에 SecurityContext를 저장하고 응답함
- 인증 후
  - Session에서 SecurityContext를 꺼내 SecurityContextHolder에 저장 √
  - SecurityContext내 Authentication객체가 있으면 인증을 유지 √

LogoutFilter

- 유저의 로그아웃을 진행
- 설정된 로그아웃 URL로 오는 요청을 감시하여 , 해당 유저를 로그아웃 처리

Security Filter Chain

- **UsernamePasswordAuthenticationFilter**
  - 설정된 로그인 URL로 오는 요청을 감시하며, 유저 인증을 처리
  - 인증 실패시, AuthenticationFailureHandler를 실행
- **DefaultLoginPageGenerationgFilter**
  - 사용자가 별도의 로그인 페이지를 구현하지 않은 경우, 기본적으로 설정한 로그인 페이지를 처리
- **BasicAuthenticationFilter**
  - HTTP요청의 (BASIC)인증 헤더를 처리하여 결과를 SecurityContextHolder에 저장
- **RememberMeAuthenticationFilter**
  - SecurityContext에 인증(Authentication) 객체가 있는지 확인
  - RememberMeServices를 구현한 객체의 요청이 있을 경우, Remember-Me인증 토큰으로 컨텍스트에 주입

Security Filter Chain

- **AnonymousAuthenticationFilter**
  - SecurityContextHolder에 인증(Authentication)객체가 있는지 확인
  - 필요한 경우 Authentication 객체를 주입

- **SessionManagementFilter**
  - 요청이 시작된 이후 인증된 사용자인지 확인하고, 인증된 사용자일 경우, SessionAuthenticaitonStrategy를 호출하여 세션 고정 보호 메커니즘을 활성화하거나 여러 동시 로그인을 확인하는 것과 같은 세션 관련 활동을 수행

- **ExceptionTranslationFilter**
  - 필터체인 내에서 발생하는 모든 예외(AccessDeniedException, AuthenticationException)를 처리

- **FilterSecurityInterceptor**
  - HTTP 리소스의 보안처리를 수행

Security Filter Chain

보안 에러

- 401 에러: 로그인 없이 접근한 경우
- 403 에러: 권한 부족