Architecture

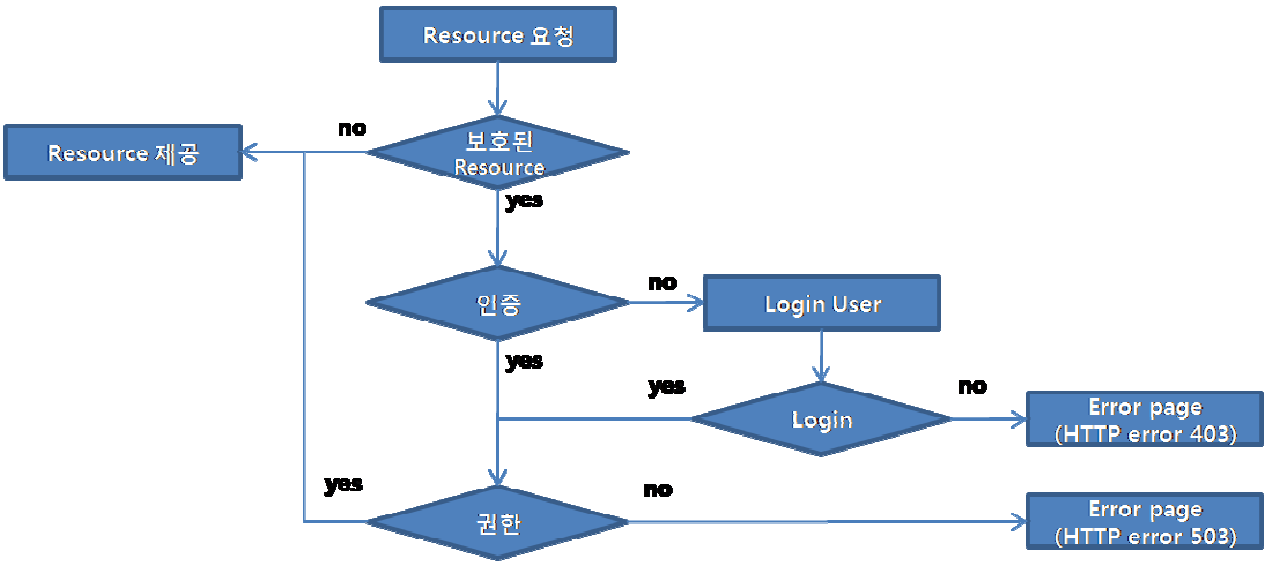
Summary

This explains the basic structure and configuration of Spring Security of eGov development framework. The Server Security of eGov development framework uses the real-time DB based JDBC applied in container rather than XML.

Description

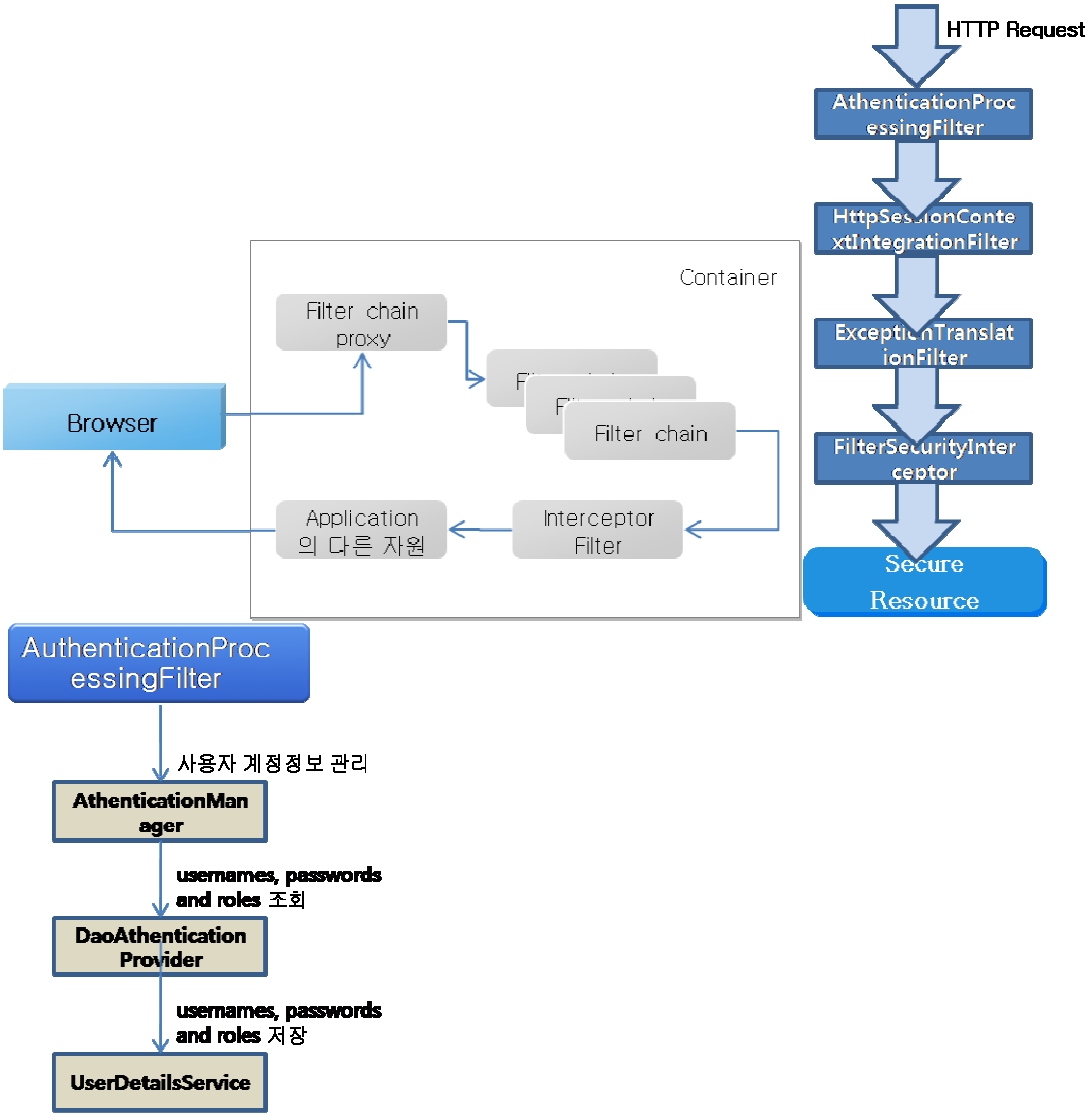
Spring Security Architecture

Web Application Certification Process



1. Request Resource
2. Determine whether the resource is protected against the request
3. Since it is not authenticated yet, redirect to the specific page or HTTP response code(error)
4. Web page login or X509 certificate according to authentication mechanism
5. Request the contents of input form or the HTTP header including authentication details to the server
6. Determine whether credential is effective
    - Proceed to next stage if effective
    - Request credential again if it is not effective(return)
7. Request successful if there is authority to access the protection resource / forbidden 403 HTTP error if there is no access authority

Spring Security Filter Chain



- Information crated at Spring Security – Get SecurityContext using SecurityContextHoler
- To use in various environment including the case when application is distributed, save SecurityContext in SecurityContextHolder using ThreadLocal object.
- ThreadLocal object can contain required status information only in current thread.
- Whenever there is a request from web environment, it is not correct to create SecurityContext that plays the same role again → perform the task of getting and recording SecurityContext information in ThreadLocal using httpSessionContextIntegrationFilter. (save in Session)

Security Configuration

Essential Library

- spring-security-core-2.0.4.jar
- spring-security-taglibs-2.0.4.jar

web.xml Registration

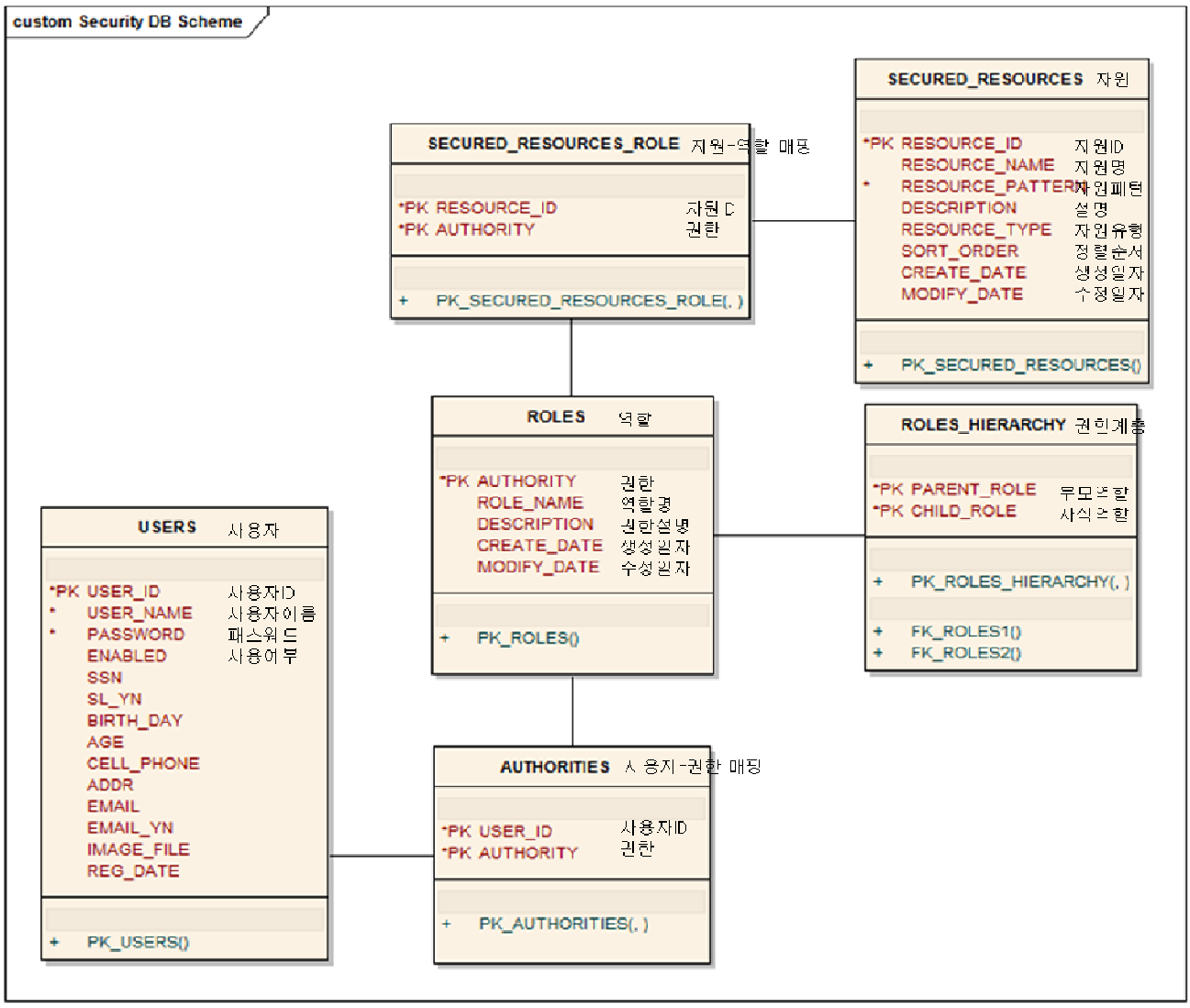
- Register org.springframework.web.filter.DelegatingFilterProxy: Spring Framework class representing the filter implements registered in Spring bean in Application Context.
- Make all web requests delivered to DelegatingFilterProxy of Spring Security.
- DelegatingFilterProxy is the class that can be generally used to deliver web request to other URL based on different URL pattern.
- These entrusted filters are managed in application context and may enjoy the benefit of dependency injection.

example

```
<filter>
        <filter-name>springSecurityFilterChain</filter-name>
        <filter-class>org.springframework.web.filter.DelegatingFilterProxy</filter-class>
</filter>
<filter-mapping>
        <filter-name>springSecurityFilterChain</filter-name>
        <url-pattern>/*</url-pattern>
</filter-mapping>
```

Main Table

Tables related to user certification are the user table and user authority table. The user authority tables are role, resource and role level tables.



DaoAuthenticationProvidor

User Table

```
CREATE TABLE USERS (
        USERNAME VARCHAR(50) NOT NULL,
        PASSWORD VARCHAR(50) NOT NULL,
        ENABLED BIT NOT NULL,
        CONSTRAINT PK_USERS PRIMARY KEY(USERNAME)
);
```

- Required field: USERNAME(user ID), PASSWORD(user password), ENABLED(whether to use account)

- Other fields: use other information of user table for session processing(ex. Resident ID, address, date of birth..)

Authority Table

```
CREATE TABLE AUTHORITIES (
        USERNAME VARCHAR(50) NOT NULL,
        AUTHORITY VARCHAR(50) NOT NULL,
        CONSTRAINT PK_AUTHORITIES PRIMARY KEY(USER_ID,AUTHORITY),
        CONSTRAINT FK_USERS FOREIGN KEY(USER_ID) REFERENCES USERS(USER_ID),
        CONSTRAINT FK_ROLES3 FOREIGN KEY(AUTHORITY) REFERENCES ROLES(AUTHORITY)
);
```

- Required field: USER_ID(user ID), AUTHORITY(authority)

Role Table

```
CREATE TABLE ROLES (
        AUTHORITY VARCHAR(50) NOT NULL,
        ROLE_NAME VARCHAR(50),
        DESCRIPTION VARCHAR(100),
        CREATE_DATE DATE,
        MODIFY_DATE DATE,
        CONSTRAINT PK_ROLES PRIMARY KEY(AUTHORITY)
);
```

AUTHORITY	DESCRIPTION
IS_AUTHENTICATED_ANONYMOUSLY	Anonymous user
IS_AUTHENTICATED_REMEMBERED	REMEMBERED user
IS_AUTHENTICATED_FULLY	Authenticated user
ROLE_RESTRICTED	Restricted user
ROLE_USER	General user
ROLE_ADMIN	Administrator
ROLE_A	A task
ROLE_B	B task

Role Level Table

Table that sores level structure of the role.

```
CREATE TABLE ROLES_HIERARCHY (
        PARENT_ROLE VARCHAR(50) NOT NULL,
        CHILD_ROLE VARCHAR(50) NOT NULL,
        CONSTRAINT PK_ROLES_HIERARCHY PRIMARY KEY(PARENT_ROLE,CHILD_ROLE),
        CONSTRAINT FK_ROLES1 FOREIGN KEY(PARENT_ROLE) REFERENCES ROLES(AUTHORITY),
        CONSTRAINT FK_ROLES2 FOREIGN KEY(CHILD_ROLE) REFERENCES ROLES (AUTHORITY)
);
```

CHILD_ROLE	PARENT_ROLE
ROLE_ADMIN	ROLE_USER
ROLE_USER	ROLE_RESTRICTED
ROLE_RESTRICTED	IS_AUTHENTICATED_FULLY
IS_AUTHENTICATED_FULLY	IS_AUTHENTICATED_REMEMBERED
IS_AUTHENTICATED_REMEMBERED	IS_AUTHENTICATED_ANONYMOUSLY
ROLE_ADMIN	ROLE_A
ROLE_ADMIN	ROLE_B
ROLE_A	ROLE_RESTRICTED

ROLE_B	ROLE_RESTRICTED

Protected resource table

```
CREATE TABLE SECURED_RESOURCES (
        RESOURCE_ID VARCHAR(10) NOT NULL,
        RESOURCE_NAME VARCHAR(50),
        RESOURCE_PATTERN VARCHAR(300) NOT NULL,
        DESCRIPTION VARCHAR(100),
        RESOURCE_TYPE VARCHAR(10),
        SORT_ORDER INTEGER,
        CREATE_DATE DATE,
        MODIFY_DATE DATE,
        CONSTRAINT PK_RECURED_RESOURCES PRIMARY KEY(RESOURCE_ID)
);
```

Protect resources with url, method, pointcut.

RESOURCE_ID	RESOURCE_PATTERN
web-000001	\A/test\.do\Z
web-000002	\A/sale/.*\.do\Z
web-000003	\A/cvpl/((?!EgovCvplLogin\.do).)*\Z
mtd-000001	egovframework.rte.sample.service.EgovSampleService.updateSample
mtd-000002	egovframework.rte.sample.service.EgovSampleService.deleteSample
mtd-000003	execution(* egovframework.rte.sample..service.*Service.insert*(..))

Protected resource role table

Mapping table between protected resources and roles

```
CREATE TABLE SECURED_RESOURCES_ROLE (
        RESOURCE_ID VARCHAR(10) NOT NULL,
        AUTHORITY VARCHAR(50) NOT NULL,
        CONSTRAINT PK_SECURED_RESOURCES_ROLE PRIMARY KEY(RESOURCE_ID,AUTHORITY),
        CONSTRAINT FK_SECURED_RESOURCES FOREIGN KEY(RESOURCE_ID) REFERENCES
SECURED_RESOURCES(RESOURCE_ID),
        CONSTRAINT FK_ROLES4 FOREIGN KEY (AUTHORITY) REFERENCES ROLES(AUTHORITY)
);
```

N. Reference