CONSPECT ICT diensten

Oracle Consultancy
Applicatiebeheer
Detachering
Java/J2EE
DBA

Securing Spring Web Flow

Marten Deinum

Marten Deinum

- > 7 jaar Java/J2EE ervaring in diverse projecten
  - Online & Telefonisch bankieren
  - Pechhulp registratie
  - Urenregistratie/raadplegen uitzendbranche
- Spring
  - Actief lid van Spring forum
  - SpringFAQ initiator (alpha status)
  - Spring Contributor (bugfixes, ideeën, weblog)

CONSPECT ICT diensten

Agenda

- Acegi Security System for Spring
- Spring Web Flow
- Het ‘probleem’
- De oplossing (SWF-93)
- Demo
- Vragen?

Acegi Security System for Spring (1/2)

- Authenticatie/Autorisatie
- Declarative security
  - Spring Beans
  - URL
- Spring configuratie
- Flexibel (daarom SWF-93)

Acegi Security System for Spring (2/2)

- Hoe werkt Acegi in een web-based omgeving?
  - Servlet filters zoals:
    - `AuthenticationProcessingFilter`
    - `FilterSecurityInterceptor`
  - Interceptors (AOP) zoals:
    - `MethodSecurityInterceptor`

Spring Web Flow (1/2)

- Eenvoudige configuratie van complexe scherm flows
- Focus op
  - definitie van flows
  - Executie van flow definities
- Spring configuratie

Spring Web Flow (2/2)

- Een flow bestaat uit één of meerdere states, mogelijke states:
  - Action
  - View
  - Subflow
  - Decision
- Gebruiker signaleert middels ‘events’ wat er is gebeurd (b.v. druk op een knop).
- De flow bepaalt op basis van deze ‘events’ **wat er vervolgens moet gebeuren**
- Een flow is een ‘blackbox’

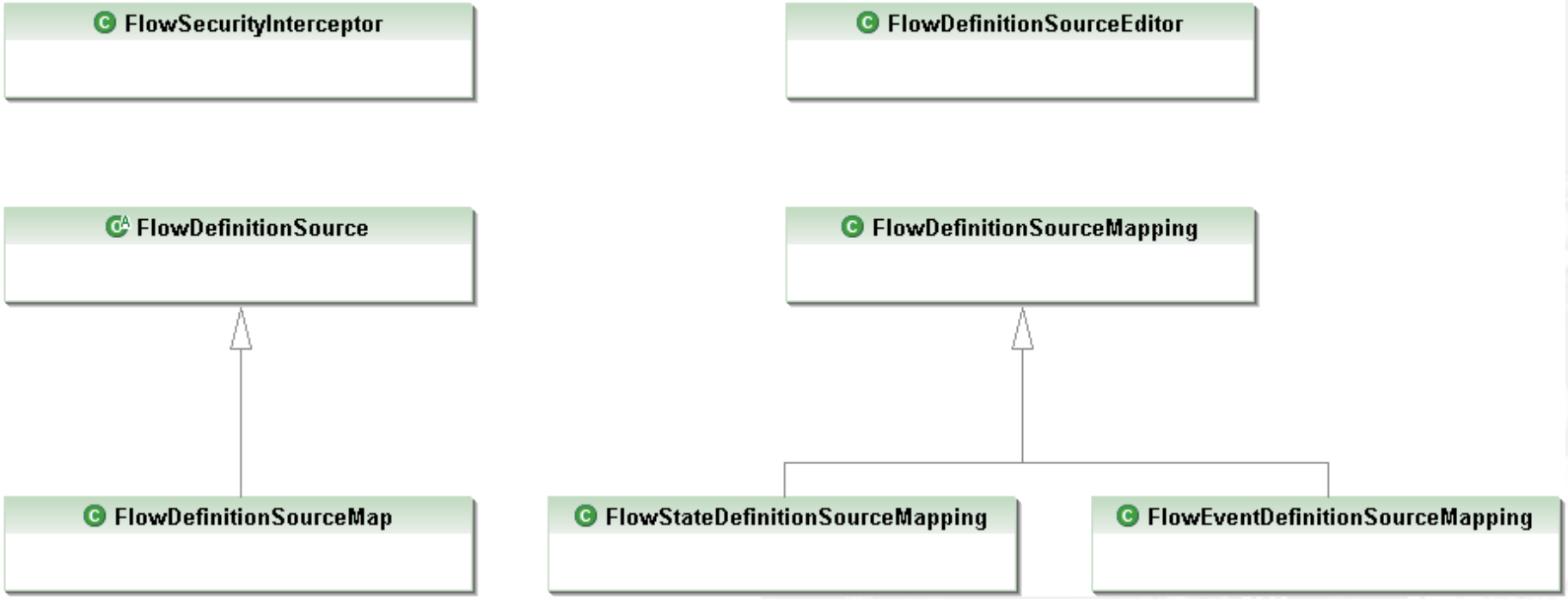
Het ‘probleem’

- Spring web flow werkt met 1 Controller/1 Url
  - /myapp/flowController?_flowId=[flowid]
- 1 flow kan geschikt zijn voor meerdere rechten/rollen
- Bepaalde actie (event) kan b.v alleen voor beheerders zijn
- Een state kan geschikt zijn voor mensen met bepaalde rechten (beheerders e.d.)
- Acegi heeft out of the box method based security en url based security

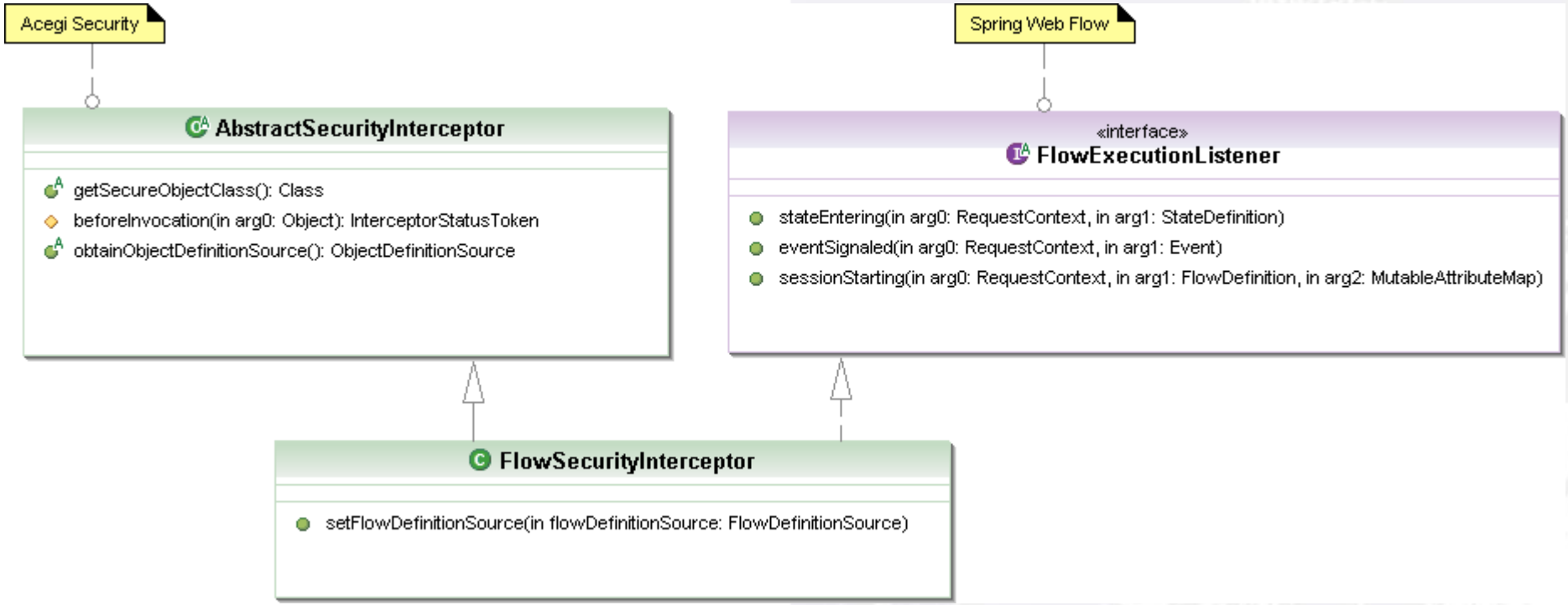
Kortom we willen beveiliging kunnen toepassen op <u>flows</u>, <u>events</u> en op <u>state</u>.

De oplossing (SWF-93) (1/6)

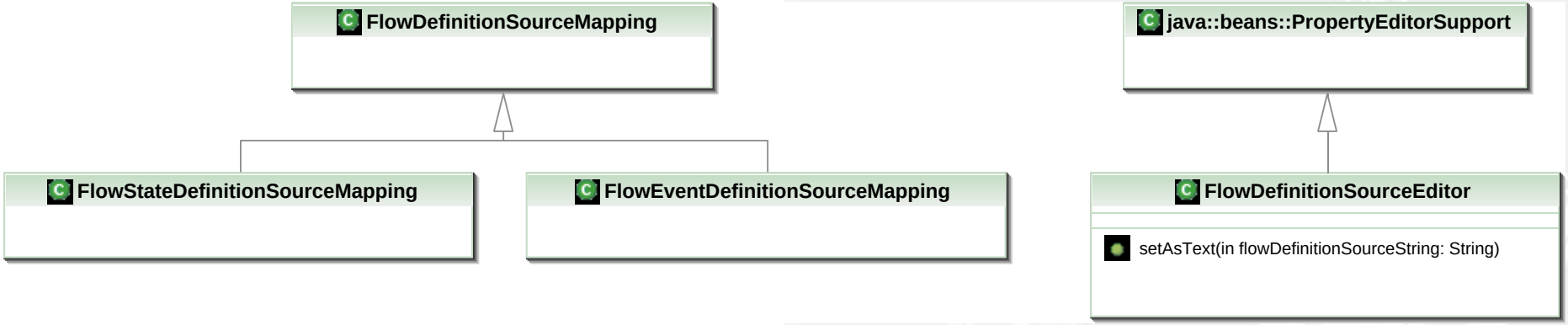
SWF-93 Class Diagram



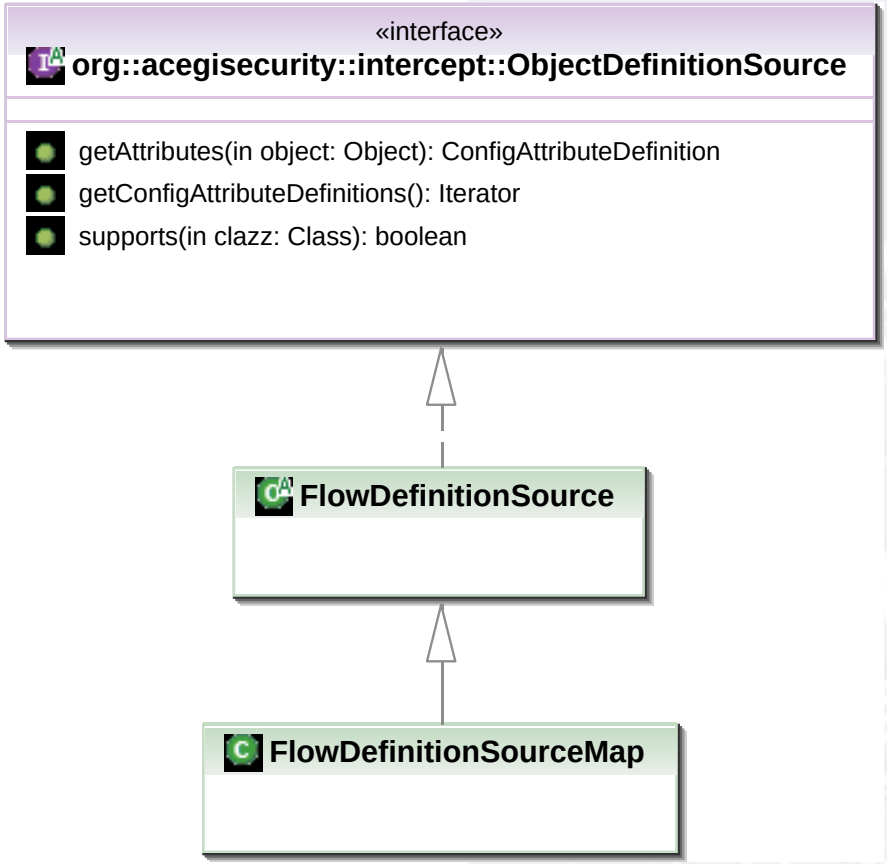
De oplossing (SWF-93) (2/6)



De oplossing (SWF-93) (3/6)



De oplossing (SWF-93) (4/6)



De oplossing (SWF-93) (5/6)

- Beveiliging is een kwestie van configuratie van 2 onderdelen
  - `FlowSecurityListener` configuratie
  - Geconfigureerde `FlowSecurityListener` toevoegen aan FlowExecutor

```
<flow:executor registry-ref="flowRegistry" id="flowExecutor">
    <flow:repository type="continuation"/>
    <flow:execution-listeners>
        <flow:listener ref="flowSecurityListener"/>
    </flow:execution-listeners>
</flow:executor>
```

De oplossing (SWF-93) (6/6)

```
<bean id="flowSecurityListener" class="FlowSecurityInterceptor">
    <property name="rejectPublicInvocations" value="false"/>
    <property name="authenticationManager" ref="authenticationManager"/>
    <property name="accessDecisionManager" ref="accessDecisionManager"/>
    <property name="flowDefinitionSource">
        <value>
            EditUser-flow=ROLE_USER
            SearchBook-flow.event.details=ROLE_USER,ROLE_BOOKADMIN
            SearchBook-flow.event.remove=ROLE_BOOKADMIN
            SearchBook-flow.state.editBook=ROLE_BOOKADMIN
            EditBook-flow=ROLE_BOOKADMIN
            AdminUser-flow=ROLE_USERADMIN
        </value>
    </property>
</bean>
```

DEMO

- Stap 1: Acegi Security url en methode beveiliging (probleem)
- Stap 2: Spring Web Flow beveiliging (oplossing)

CONSPECT ICT diensten

Samenvatting (1/2)

- Probleem
  - URL Beveiliging vanwege opzet web flow moeilijker
  - Flow, state of event kan alleen voor bepaalde rechten toegankelijk zijn.
  - URL based te grof
  - Methodbased te fijn en te laat
- Oplossing (SWF-93)
  - Configureerbare SecurityInterceptor
  - Mogelijkheid tot afschermen flow, event of state

Samenvatting (2/2)

- Links
  - http://www.springframework.org
  - http://opensource.atlassian.com/projects/spring/browse/SWF-93
  - http://www.acegisecurity.org
  - http://www.springframework.org/webflow
- Contact
  - marten.deinum@conspect.nl
  - http://forum.springframework.org
  - http://blog.deinum.biz

Workshop

- Spring Web Flow & Security
- Dinsdag 3 juli en donderdag 16 augustus
- Meer informatie bij stand of via www.conspect.nl