Search

Tempo
INTALIO Security Service

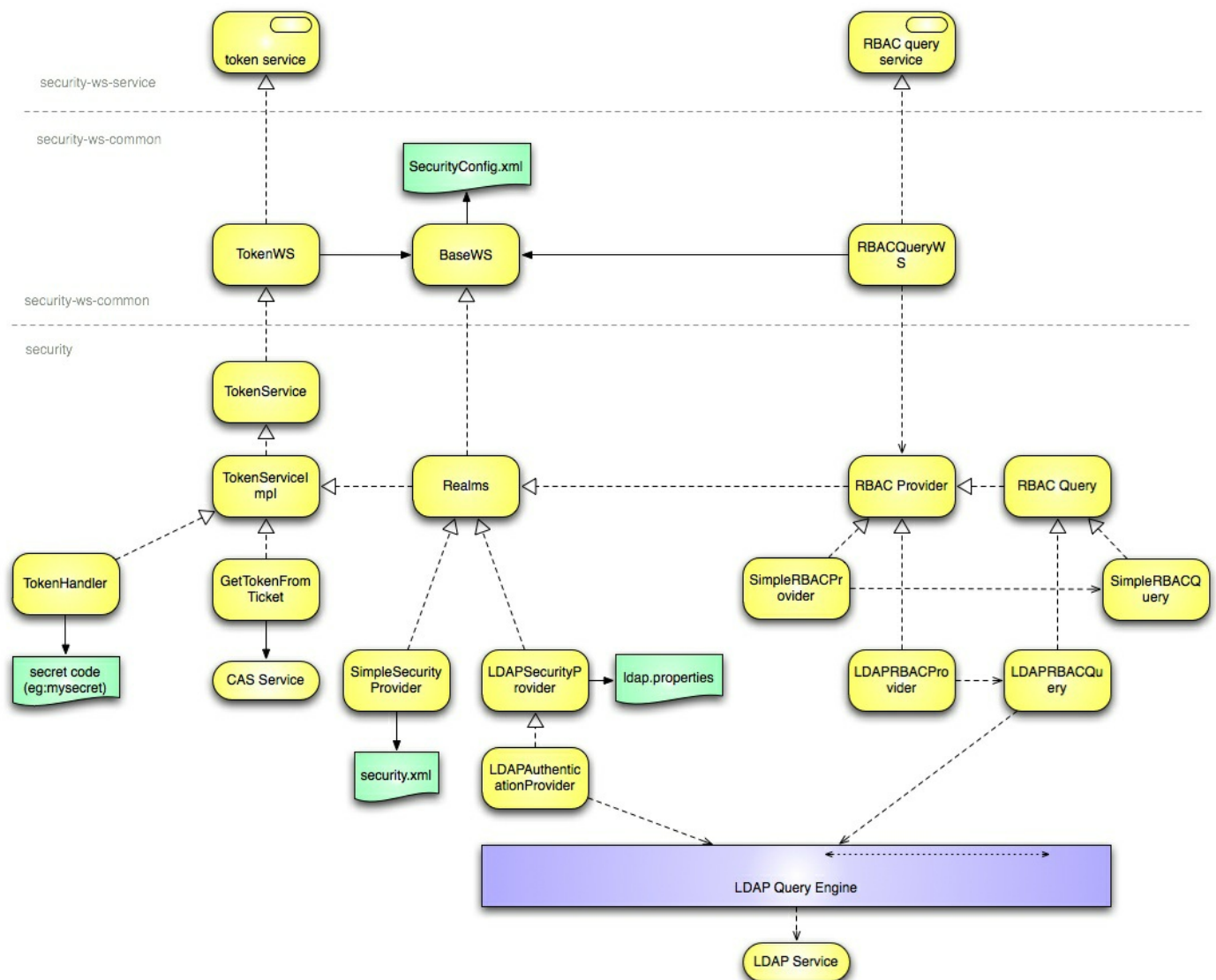Log In

View **Attachments (2)** **Info**

Browse Space

Added by Jackie Ju, last edited by Ark Xu on Dec 08, 2008

Security Architecture of current tempo

B4P user assignment/management

Using Logical People Groups

During deployment each logical people group is bound to a people query.

```
<htd:potentialOwners>
  <htd:from logicalPeopleGroup="regionalClerks">
   <htd:argument name="region">
    htd:getInput("part1")/region
   </htd:argument>
  </htd:from>
</htd:potentialOwners>
```

Using Literals

directly specifying the user identifier(s) or the name(s) of groups
eg: user identifiers:

```
<htd:potentialOwners>
   <htd:from>
     <htd:literal>
        <htd:organizationalEntity>
          <htd:users>
             <htd:user>Alan</htd:user>
             <htd:user>Dieter</htd:user>
             <htd:user>Frank</htd:user>
             <htd:user>Gerhard</htd:user>
             <htd:user>Ivana</htd:user>
             <htd:user>Karsten</htd:user>
             <htd:user>Matthias</htd:user>
             <htd:user>Patrick</htd:user>
          </htd:users>
        </htd:organizationalEntity>
     </htd:literal>
```
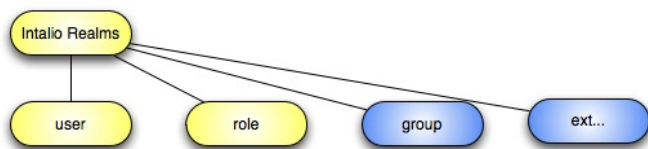
```
      </htd:from>
  </htd:potentialOwners>
```

eg: group names:

```
  <htd:potentialOwners>
    <htd:from>
      <htd:literal>
        <htd:organizationalEntity>
          <htd:groups>
            <htd:group>bpel4people_authors</htd:group>
          </htd:groups>
        </htd:organizationalEntity>
      </htd:literal>
    </htd:from>
  </htd:potentialOwners>
```

Using Expressions

be assigned using expressions returning either an instance of the **htd:tOrganizationalEntity** data type or the **htd:tUser**

```
  <htd:potentialOwners>
    <htd:from>
      htd:getInput("part1")/approvers
    </htd:from>
  </htd:potentialOwners>

  <htd:businessAdministrators>
    <htd:from>
      htd:except(htd:getInput("part1")/admins,
      htd:getInput("part1")/globaladmins[0])
    </htd:from>
  </htd:businessAdministrators>
```

Security Extension proposal

The yellow part is the current tempo and the blue part is the extension that support the logical group or any other expressions used for query. There is no limitation how the query should be implemented in B4P spec. For the expressions used for B4P, we need to provide a generic RBACQuery that could convert the xPath to the real query.

B4P Implementation Notes

- Authentication is reused.
- People assignment on generic human role is defined in User Process at design time.
- According to b4p spec, the underlying people assignment will be retrieved from HT request or coordinate protocal. But since the coordinating protocal won't be implemented in this phase, so people assignment will deployed into Tempo.
- The logic group will be directly mapped to actual group in LDAP or Simple realm, which is also Open Issue and have to be confirmed.

Comments