Gruppe: swp08-6

Gruppenleiter/Verantwortlicher: Johannes Kreidler Erstellungsdatum: 19.05.08

Entwurfsbeschreibung der Rollen- und Rechtemanagements von OLAT

1. Allgemeines

Das Rollen- und Rechtekonzept von OLAT leht sich in vielerlei Hinsicht an das Policy-Konzept von Java an.
Ein angemeldeter OLAT-Benutzer kann gewisse Aktionen ausführen, wie zum Beispiel Zugriff auf oder Lesen von Daten. Je nach seiner Stellung im System unterscheidet sich die Menge seiner Rechte. Einerseits werden dem Benutzer Rechte durch die intern festgelegten Systemrollen zugewiesen, aber auch durch seine Zugehörigkeit zu Benutzergruppen.

2. Produktübersicht

Generell gibt es in OLAT vier verschiedene Systemrollen, diese sind Gast, Benutzer, Autor und Administrator. Dabei sind sämtliche Rechte des Erstgenannten jeweils auch Rechte der darauf folgenden Rollen. Eine der Rollen zugeordnet zu sein, entspricht zu der jeweiligen Gruppe, die gewisse Rechte hat zu gehören. Es folgt ein kurzer Überblick über die angesprochenen Rollen und deren Rechte.

Der Gast

Als Gast kann man nur grundlegende Einsichten in das OLAT-Portal gewinnen. Man erkennt die Struktur und Navigation, kann einige Kurse suchen und sehen und sich mit der Hilfefunktion näher mit OLAT vertraut machen.

Der Benutzer

Als Benutzer hat man bereits die Möglichkeit, die OLAT-Oberfläche seinen eigenen Anforderungen und Erwartungen anzupassen, zum Beispiel die Sprache. Man kann außerdem seine Persönlichen Daten editieren und auf einer Visitenkarte, anderen Benutzern zusammenstellen. Weiter kann sich ein Benutzer in bestehende Kurse ein- sowie austragen und selbst Arbeitsgruppen erstellen.

Der Autor

Als Autor hat man im OLAT-Portal über die Rechte des Benutzers hinaus die Möglichkeit Lernressourcen zu erstellen, das beinhaltet Kurs, Test, Fragebogen, Wiki, Glossar

Ressourcenordner oder Forum. Man kann ebenfalls die Sichtbarkeit, die Anmeldung und die Lern- sowie Rechtegruppen seiner Lernressourcen verwalten.

Der Administrator

Als Aministrator hat man die Rechte aller anderen Systemrollen und die eines Mitglieds aller Systemgruppen. Darüber hinaus kann man alle Systeminformaionen sehen und verwalten, Properties erweitern und eine Reihe weiterer, toller Sachen.

Von den vier Rollen abgesehen, kann man im OLAT-Portal zwei Systemgruppen angehören, nämlich Gruppenverwlter oder Benutzerverwalter. Hier folgt eine kurze Zusammenfassung ihrer Rechte.

Gruppenverwalter

Als Gruppenverwalter kann man Gruppenkontexte sowie krusübergreifende Lern- und Rechtegruppen verwalten. Beispielsweise kann man einem Gruppenkontext mehrere Gruppen zuordnen.

Benutzerverwalter

Als Benutzerverwalter kann man neue Benutzer erstellen oder importieren und ihnen bestimmte Systemrollen zuweisen.

3. Grundsätzliche Struktur- und Entwurfsprinzipien für das Gesamtsystem

Ein wichtiges Prinzip ist die Authentifizierung, das bedeutet, dass sich ein OLAT-Nutzer zuerst als Gast oder mit seinem Namen und seinem Passwort im Portal einloggen muss, bevor er darauf arbeiten darf. Das geschieht über Normal Formbase username/password login, und Shibboleth 1.3 login.
Ein weiteres ist das Prinzip der Authorisierung. Die Basissicherheit ist ein wenig an die Java-Scurity angelehnt.
Die Rechte sind positiv, das heißt, sie beinhalten stets die Erlaubnis, etwas zu tun und niemals ein Verbot.
Außerdem sind sie additiv, was bedeutet, dass die Menge aller Rechte eines OLAT-Nutzers die Vereinigung all jener Rechte sind, die ihm aus allen Gruppen, denen er angehört, zugesprochen werden.
Eine Policy schützt die OLAT-Ressourcen vor unerlaubtem Zugriff, indem sie Rechte nur bestimmten Securitygroups gewährt.
Das funktioniert folgendermaßen. Jeder registrierte OLAT-Nutzer hat eine eindeutige Identity im System. Merhere solcher Identities befinden sich in Gruppen, sogenannten Securitygroups. Es kann aber auch eine Identiy in mehreren Securitygroups sein.

Es gibt im OLAT-Portal auch eine Reihe von Ressourcen, zum Beispiel Lern- oder Kurs ressourcen und verschiedene Rechte, beispielsweise hasrole, access oder read.
Um nun die Rechte und die OLAT-Benutzer zu verbinden, werden die Policies benutzt. Eine Policy besteht nämlich aus genau einer Ressource, genau einer Securitygroup und genau einem Recht. Genauer gesagt hat die Policy einen Fremdschlüssel auf eine Securitygroup, einen Fremdschlüssel auf eine Ressource und einen kurzen Text, in dem das Recht beschrieben wird.
Das bedeutet ein bestimmter OLAT-Nutzer hat ein bestimmtes Recht, auf eine bestimmte Ressource zuzugreifen, wenn seine Identity wenigstens in einer Securitygroup ist, die von einer Policy referenziert wird, welche dieses Recht auf diese Ressource hat.

4. Grundsätzliche Struktur- und Entwurfsprinzipien der einzelnen Pakete

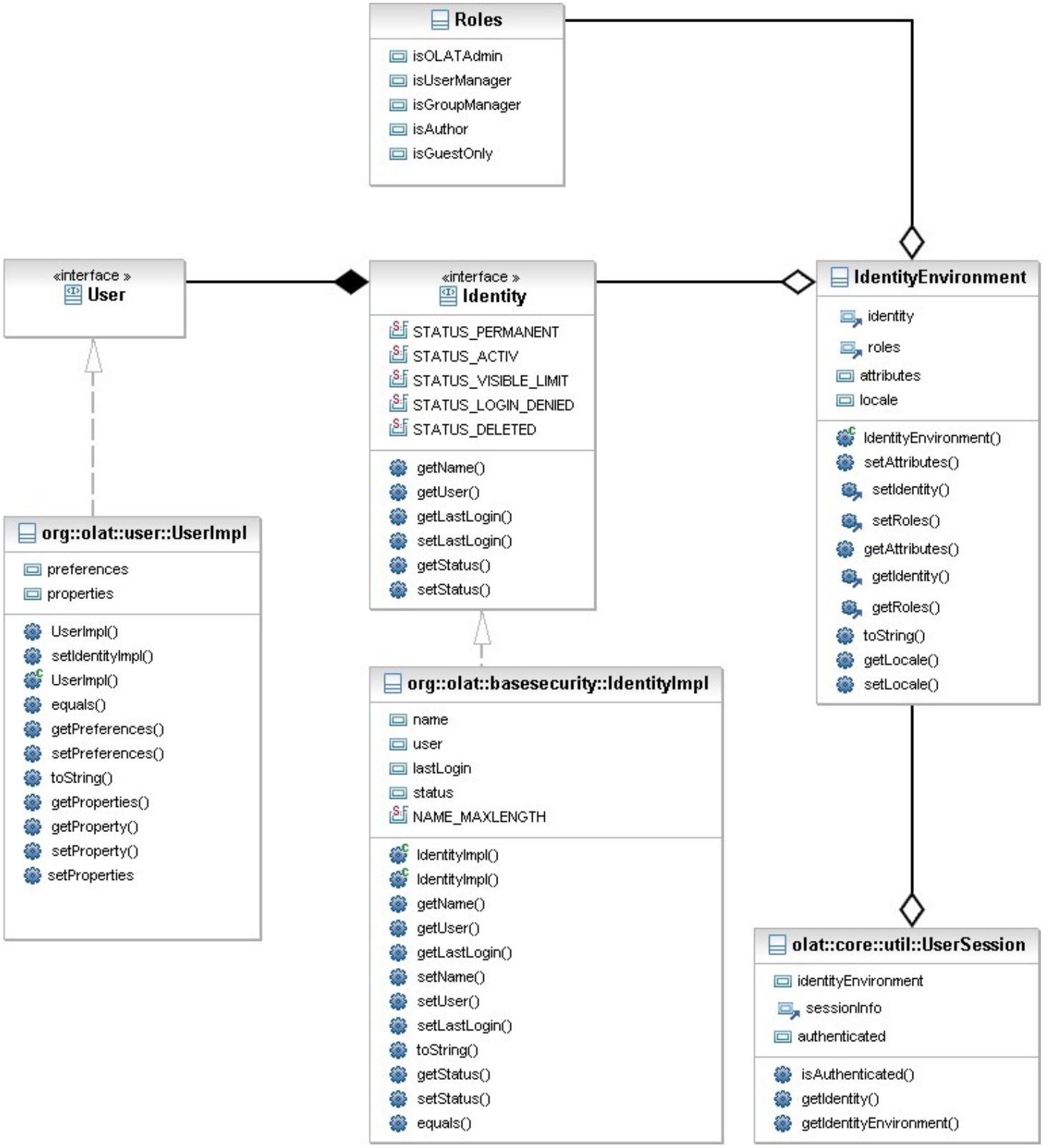
org.olat.core.id

verschiedene Interfaces und Klassen werden im Package „org.olat.core.id“ definiert, die im Kontext des Rechte und Rollenkonzepts besonders für die interne Repräsentation eines registrierten und angemeldeten OLAT-Nutzers von Interesse sind. Denn durch das Interface Identity (und deren konkreter Implementierung org.olat.basesecurity.IdentityImpl) wird ein erster Grundpfeiler des Policy-Konzepts realisiert (siehe nachfolgendes Klassendiagramm)

Insofern man also auf die Instanz der aktuellen UserSession zugreifen kann, lassen sich die Identität und die zugewiesenen Systemrollen eines angemeldeten Nutzers eindeutig bestimmen.

Gruppe: swp08-6

Gruppenleiter/Verantwortlicher: Johannes Kreidler Erstellungsdatum: 19.05.08

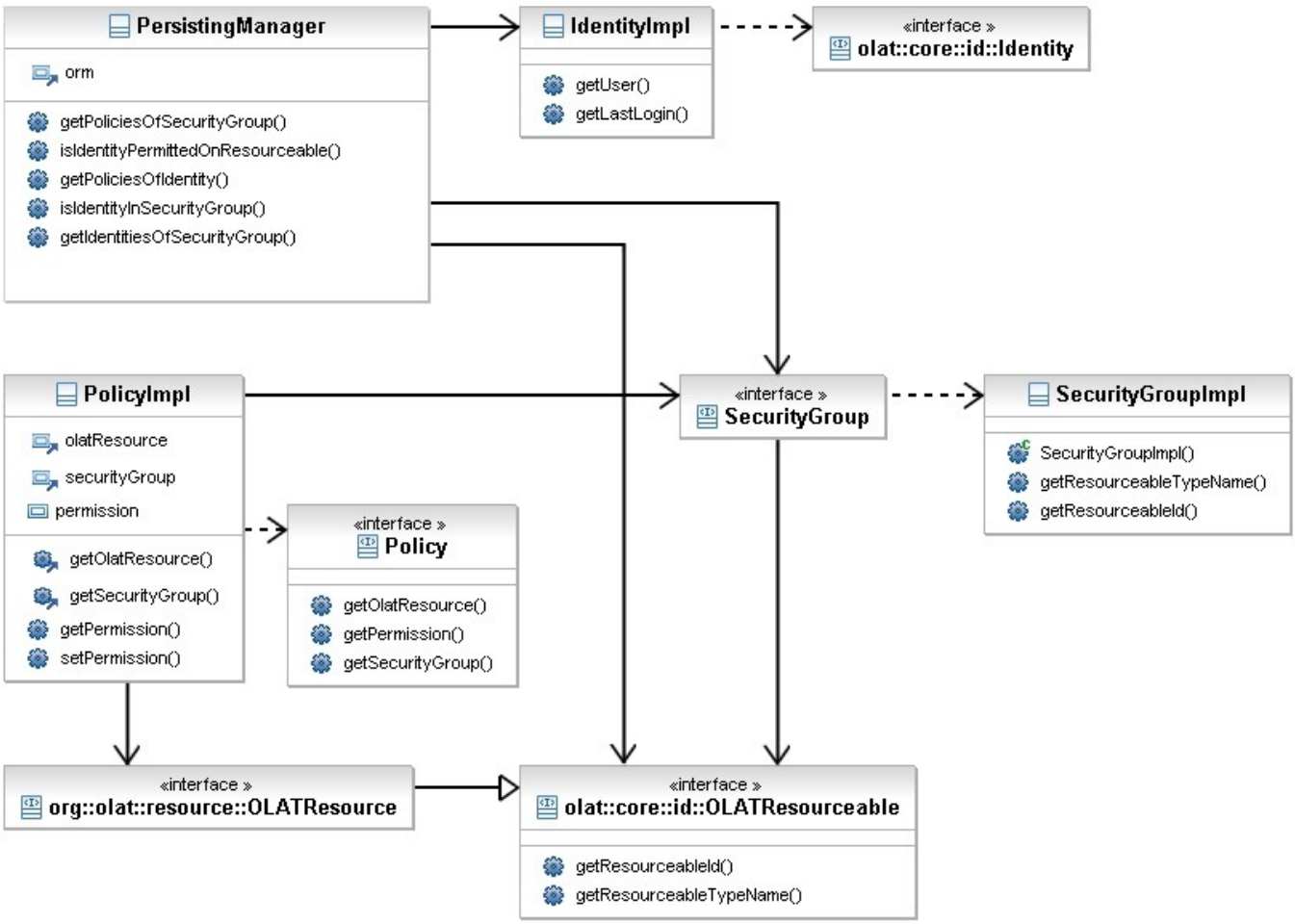


Gruppe: swp08-6

Gruppenleiter/Verantwortlicher: Johannes Kreidler Erstellungsdatum: 19.05.08

org.olat.basesecurity

Dieses Packet erweitert das Policy-Konzept und verwaltet Zugriffe auf Ressourcen im OLAT.
Es wird immer geprüft, welche Identities zu welchen SecurityGroups gehören oder welche Policies zu einer bestimmte SecurityGroup.
Der OLATResourceManagers prüft über einen Datenbank-LookUp ob eine Policy mit angegebenem Zugriffsrecht existiert, mit einer beliebigen SecurityGroup eine bestimmte Identity vergleicht.
Danach wird eindeutig klar, ob diese Identität Zugriff auf fragliche OLAT-Ressource bekommt oder nicht.



Zugriff auf das Rechte- und Rollenmanagement von den Erweiterungspunkten

Der Zugriff auf das Reche und Rollenmanagement erfolgt im Allgemeinen über den UserRequest, so auch an den Erweiterungspunkten. Jedem Controller wird ein UserRequest übergeben, über den sich leicht nachprüfen lässt ob der User die Rechte hat, bestimmte Sachen auszuführen, oder sie sogar nicht mal zu sehen.
Entsprechend dem Rollenkonzept kann so das Rechtemanagement jeder OLAT-Erweiterung organisiert werden. So wird in der Demoextension z.B. mittels

```
UserRequest.getUserSession().getRoles().isGuestOnly()
```

abgefragt ob es sich um einen Gast handelt und - sofern es ein Gast ist - der Tab mit den Demoextensions nicht angezeigt.
Alle Anderen Rollen können nach dem gleichen Schema abgefragt werden, so gestaltet sich das Management der Rechte und Rollen unkompliziert.
Dabei ist jedoch zu beachten, dass außer den vier Rollen: Administrator, Author, Benutzer und Gast, keine Rechtegruppen vorhanden sind (Benutzer können noch zusätzliche Rechte haben, z.B. Gruppenmanager).

Erweiterungpunkt für die elektronische Studentenakte (ESA)

Da das bisherige Rechtesystem statisch ist, ESA aber eine neue Rolle braucht müsste das es ein dynamisches Rechtesystem geben. Die elektronische Studentenakte braucht die Rolle „Prüfungsamt“ welches Änderungen an den Studentenakten vornehmen darf. Dazu muss es für den Bereich in dem die Studentenakte liegt besondere Rechte haben (vergleichbar mit Adminrechten) in anderen Bereichen jedoch nicht.
Der Erweiterungspunkt im Rechtesystem sollte, um höchste Flexibilität gewährleisten zu können, die Möglichkeit geben eigene Rollen mit selbst zusammengestellten Rechten zu erstellen.
Im Falle des Prüfungsamtes bedeutet das, dass außer dem Prüfungsamt höchstens noch der Administrator Schreibzugriff auf die Studentenakten besitzt (den er nicht notwendigerweise braucht, eine Einschränkung der bestehenden Rollen währe also eine Ergänzung des notwendigen Erweiterungspunktes).
Die Studentenakte selbst würde dabei einen eigenen Bereich zwischen persönlichem Bereich und Prüfungsamt bekommen. In diesem Bereich ist dann der Benutzer mit eingeschränkten Rechten ausgestattet (nur lese Rechte), das Prüfungsamt dagegen ist in diesem Bereich mit allen Rechten ausgestattet (lese- und schreib- Rechte so wie der Möglichkeit diverser relevanter Ergänzungen).