Benutzer- und Zugriffsrechteverwaltung

Table of contents

1 Benutzer und Rollen

MyCoRe besitzt eine interne Benutzer- und Rollenverwaltung. Bei der Arbeit mit einer MyCoRe Anwendung arbeitet man zunächst in der **Gastrolle**. Nach Login kann ein Benutzer für zusätzliche Aktionen berechtigt sein und z. B. Zugriff auf lesegeschützte Inhalte erhalten, oder die Möglichkeit, selbständig Inhalte einzustellen und zu bearbeiten haben. Ein vordefinierter Standardnutzer mit **Administratorrechten** hat Zugang zu allen Inhalten und Funktionen.

Benutzer können über die Weboberfläche eingerichtet und verwaltet werden. Für jeden Benutzer werden neben E-Mail Adresse und Datum des letzten Logins optional auch zusätzliche Attribute im System verwaltet, z. B. die Zugehörigkeit zu einer bestimmten Abteilung. Benutzer können mit einem **Gültigkeitsdatum** versehen werden, so dass ein Login nur bis zu diesem Datum möglich ist.

Benutzer können andere Benutzer „besitzen“. Autoren von Inhalten können so z. B. eigene **„Lesenutzer“** einrichten, d.h. Logins, über die sie Zugriff auf lesegeschützte Inhalte gewähren.

Benutzer werden **Rollen** zugewiesen, z. B. die Autoren- oder Administratorenrolle. Rollen sind frei definierbar und als MyCoRe-Klassifikationen implementiert. Dadurch können Sie eine hierarchische Struktur haben (Rollen mit Unterrollen) und über die Weboberfläche verwaltet werden.

2 Authentifizierungsbereiche und Single Sign-on

Jeder MyCoRe-Benutzer ist einem Authentifizierungsbereich („Realm“) zugeordnet. In jedem MyCoRe-System ist zumindest der lokale Bereich konfiguriert, bei dem das Login über ein Passwort direkt in der MyCoRe-Anwendung erfolgt und das Passwort auch über die Weboberfläche verwaltet werden kann.

Zusätzlich können weitere Authentifizierungsbereiche implementiert und konfiguriert werden, über die ein Login bei einem externen Dienst oder über eine externe Methode (etwa LDAP) erfolgt. Bereits implementiert ist eine Authentifizierung über **CAS** (Central Authentication Service) (http://www.jasig.org/cas) , ein Single-Sign-On-Dienst, der an vielen Hochschulen im Einsatz ist. Benutzer können sich über CAS anmelden, so dass die MyCoRe Anwendung nicht mehr das Passwort des Benutzers speichert. Über CAS authentifizierte Benutzer werden nach Login dynamisch in MyCoRe angelegt. Die Attribute wie Rollen und E-Mail des Benutzers werden dabei aus einem LDAP-Verzeichnis ausgelesen.

3 Privilegien und Access Control Lists

Privilegien steuern in MyCoRe-Anwendung die Berechtigung, bestimmte Aktionen auszuführen, z. B. neue Inhalte anzulegen. Sie werden in der Regel einer Benutzerrolle zugeordnet.

Access Control Lists (ACLs) steuern den Zugriff auf bestimmte Ressourcen, z. B. eine bestimmte Seite, ein Formular oder ein Metadaten-Objekt mit seinen Inhalten. ACLs sind Regeln aus booleschen Ausdrücken, die frei definierbar und über die Webanwendung verwaltbar sind. Eine Berechtigung kann z. B. über eine Rollenzugehörigkeit des Benutzers und/oder über einen IP-Check des anfragenden Rechners erteilt werden. Auch komplexere Regeln sind möglich, etwa die Einrichtung eines Embargodatums, ab dem der Zugriff auf eine Ressource frühestens gewährt wird. Eigene ACL-Strategien können über eine Java API implementiert werden.

Wenn MyCoRe-Objekte hierarchisch angelegt sind, können ACLs so eingerichtet werden, dass sie sich entlang der Hierarchie vererben. Die Zugriffsrechte für eine Online-Zeitschrift müssen dann z. B. nur auf dieser Ebene definiert werden und vererben sich an die untergeordneten Hefte und Artikel.