

# Erweitertes rollenbasiertes Zugriffskontrollmodell - eRBAC

Das eRBAC ist ein auf dem RBAC basierendes erweitertes Zugriffskontrollmodell. <insert Einleitungsbla>

## Objekttypen

Neben den Entitäten Objekt, Operator und Zugriffsrecht wird die zusätzliche Entität Objekttyp eingeführt. Durch eine Typisierung von Objekten, wird im eRBAC zwischen dem Öffnen einer Anwendungssoftware und dem Aufruf von Objekten innerhalb einer Anwendungssoftware unterschieden. Es werden als Objekttypen:

- Anwendung für Objekte, die den Einstiegspunkt in eine Anwendungssoftware darstellen und
- Klasse für Objekte, die Klassen innerhalb einer Anwendungssoftware repräsentieren

Jeder Rolle sind mindestens ein Objekt des Typs Anwendung und beliebig viele Objekte des Typs Klasse zugeordnet. Durch diese Einteilung zwischen Anwendung und Klasse kann eine Aufrufstruktur durch eine, eine automatische Weiterleitung zwischen Authentifizierung und Zugriffskontrolle, implementiert werden. Dazu besitzt ein Objekt des Typs Anwendung noch zusätzlich die Attribute Aufrufadresse, welche die Adresse der aufzurufenden Anwendung speichert und Aufrufbezeichnung welche den Namen der Anwendung zur Darstellung in bspw. Menüs beinhaltet.

Objekte und Operatoren können in eRBAC unabhängig voneinander definiert werden. Durch explizite Zuordnung von Operatoren zu Objekten werden die Zugriffsrechte festgelegt. So können aus Gründen der Informationssicherheit unerwünschte Kombinationen vermieden werden.

## Rollentypen und Rollen in eRBAC

In eRBAC werden Rollen in Rollentypen mit getrennten Sicherheitsrichtlinie eingeteilt. Die folgenden Rollentypen sind in eRBAC definiert:

- Anwendungsrollen
- Virtuelle Rollen
- Administrationsrollen
- Delegationsrollen

**Anwendungsrollen** bündeln die Zugriffsrechte vom öffnen der Anwendung bis hin zur Überprüfung jedes einzelnen Zugriffs auf von außen zugreifbare Funktionen eines Anwendungssystems. Sie können sowohl einem Subjekt direkt zugeordnet als auch in einer Rollenhierarchie eingebunden werden.

**Virtuelle Rollen** sind Anwendungsrollen zum kapseln von Zugriffsrechten welche von mehreren Rollen benötigt werden. Dieser Rollentyp wird keinem Subjekt zugeordnet, sondern wird nur in der Rollenhierarchie verwendet

**Administratorrollen** bündeln die Zugriffsrechte, die für die Rechteverwaltung notwendig sind. Die Administratorrolle ist aber disjunkt von den Rollen der anderen Rollentypen.

From:  
<https://wiki.ihb-eg.de/> - **FlexWiki**

Permanent link:  
<https://wiki.ihb-eg.de/doku.php/erbac/erbac?rev=1448544260>

Last update: **2017/04/13 10:47**

