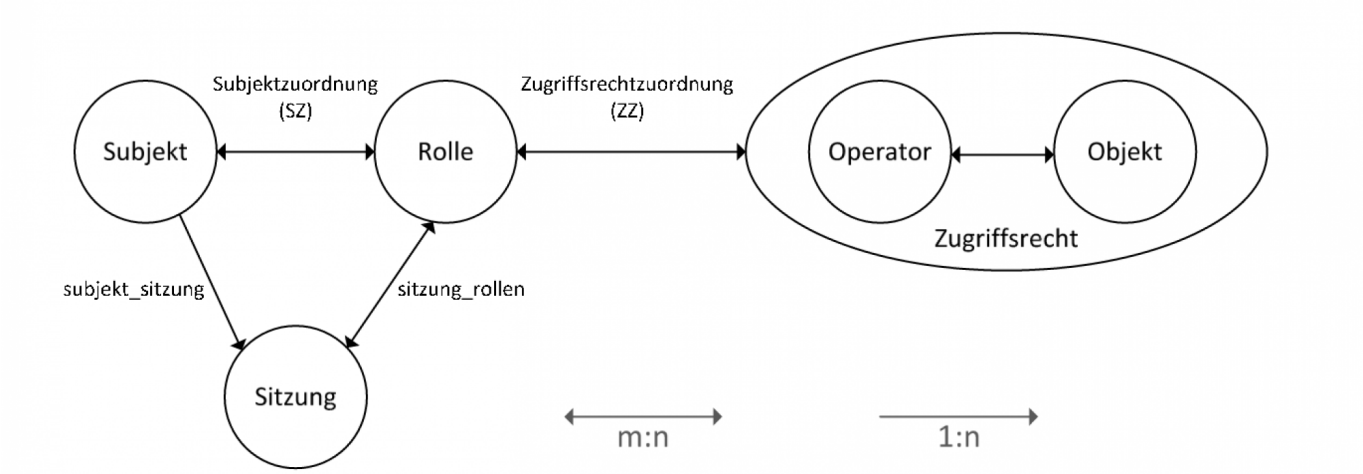
Rollenbasiertes Zugriffskontrollmodell (RBAC)

Das RBAC ist ein Modell zur Beschreibung der Zugriffskontrolle, in dem Subjekten Rollen zugewiesen werden, an welche wiederum Zugriffsrechte gebunden sind. Dadurch erben die Subjekte die für ihre Aufgaben notwendigen Zugriffsrechte. Das Referenzmodell des RBAC umfasst das Kerndmodell, die Rollenhierachie und die Aufgabentrennung. Dabei muss ein Zugriffskontrollsystem mindestens das Kernmodell enthalten (ANSI INCITS 359-2004 2004).

Kernmodell

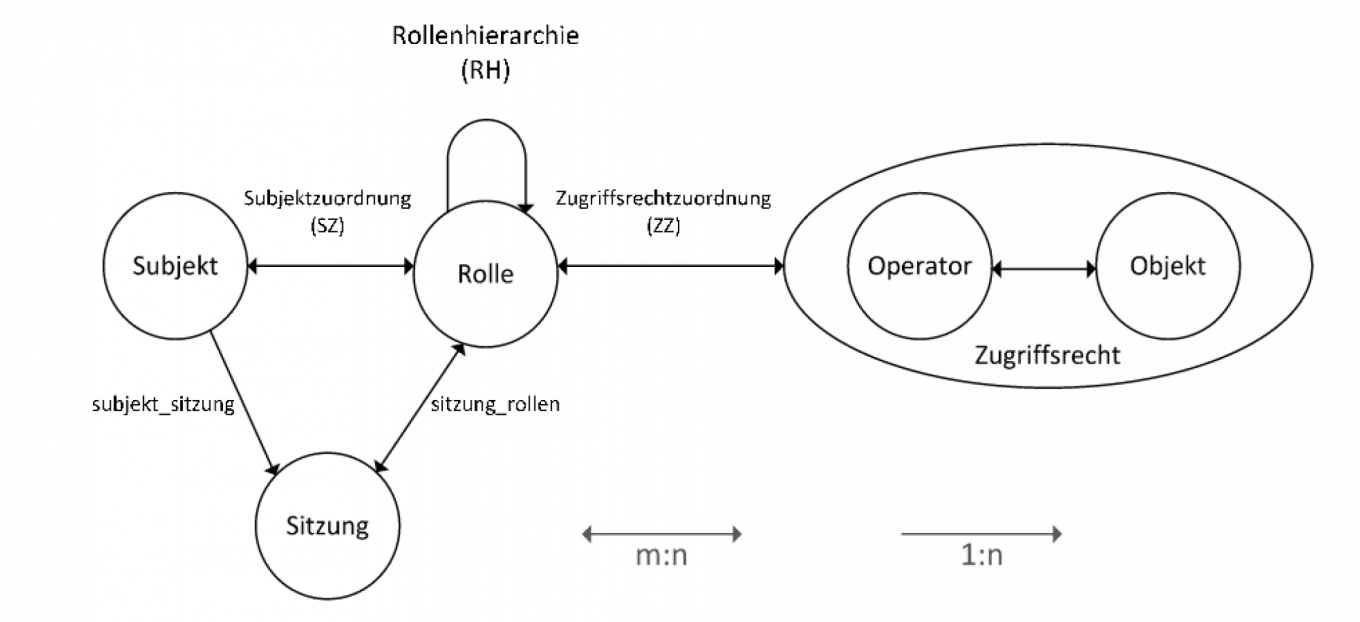
Im Kernmodell wird mit dem Subjekt der personelle Aufgabenträger im betrieblichen Informationssystem verstanden. Disem werden Rollen zugewiesen, welche Funktionen und damit Zugriffsrechte innerhalb einer Organisation entsprechen. Zugriffsrechte sind Genehmigungen einen Operator (z.B. lesen oder schreiben) auf vom RBAC geschütze Objekte(z.B. eine Text-Datei) anzuwenden. Eine Sitzung ist eine Verbindung zwischen dem Subjekt und einer Teilmenge der Rollen die ihm zugeordnet sind. Ein Subjekt kann beliebig viele Sitzungen öffnen. Daraus folgt, das ein Subjekt zu einem bestimmten Zeitpunkt die Wahl hat, welche der ihm über die Rollen zugewisenden Zugriffsrechte er benutzt. Das erweiterte Rollenbasiertes Zugriffskontrollmodell fügt dem RBAC noch die Unterschiedung zwischen verschiedenen Objekt-/ und Rollentypen Objekt-/ und Rollentypen hinzu.



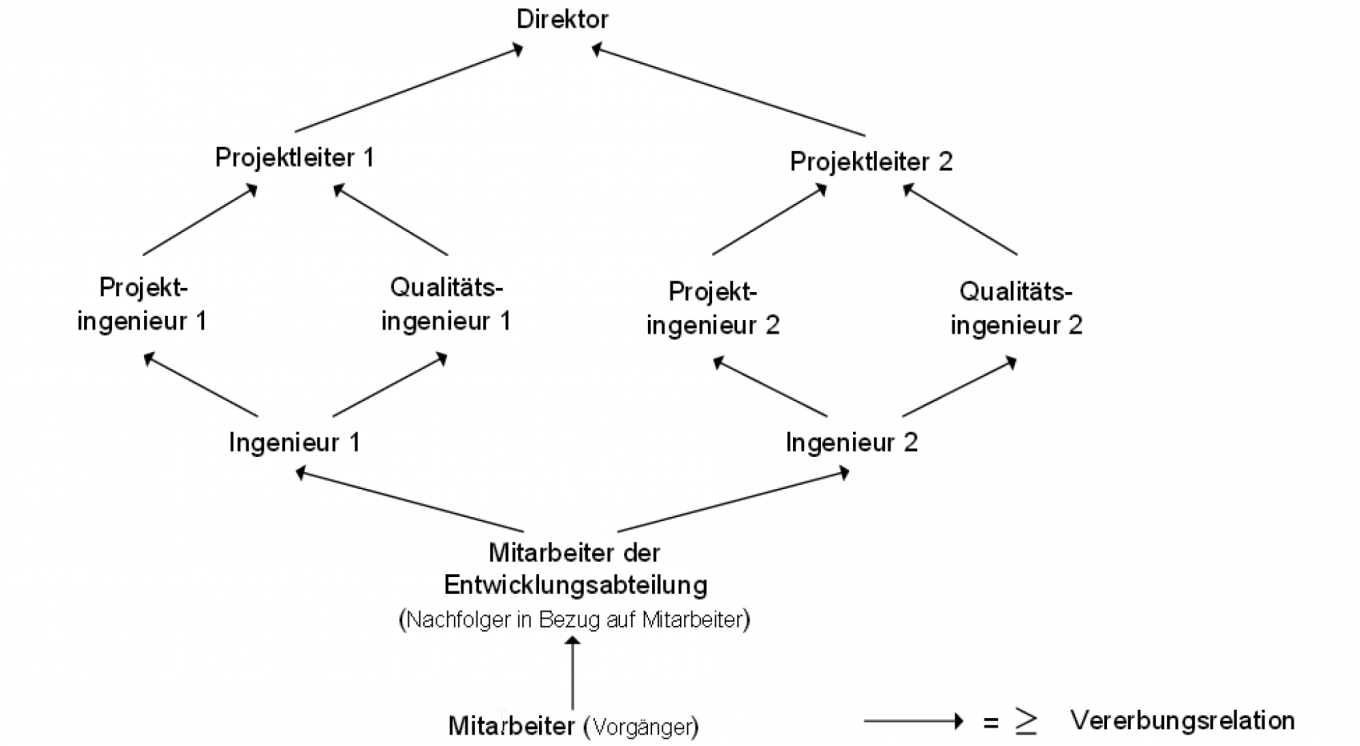
Für eine formale Zusammenfassung des Kernmodells des RBAC klicken Sie hier.

Rollenhierachie

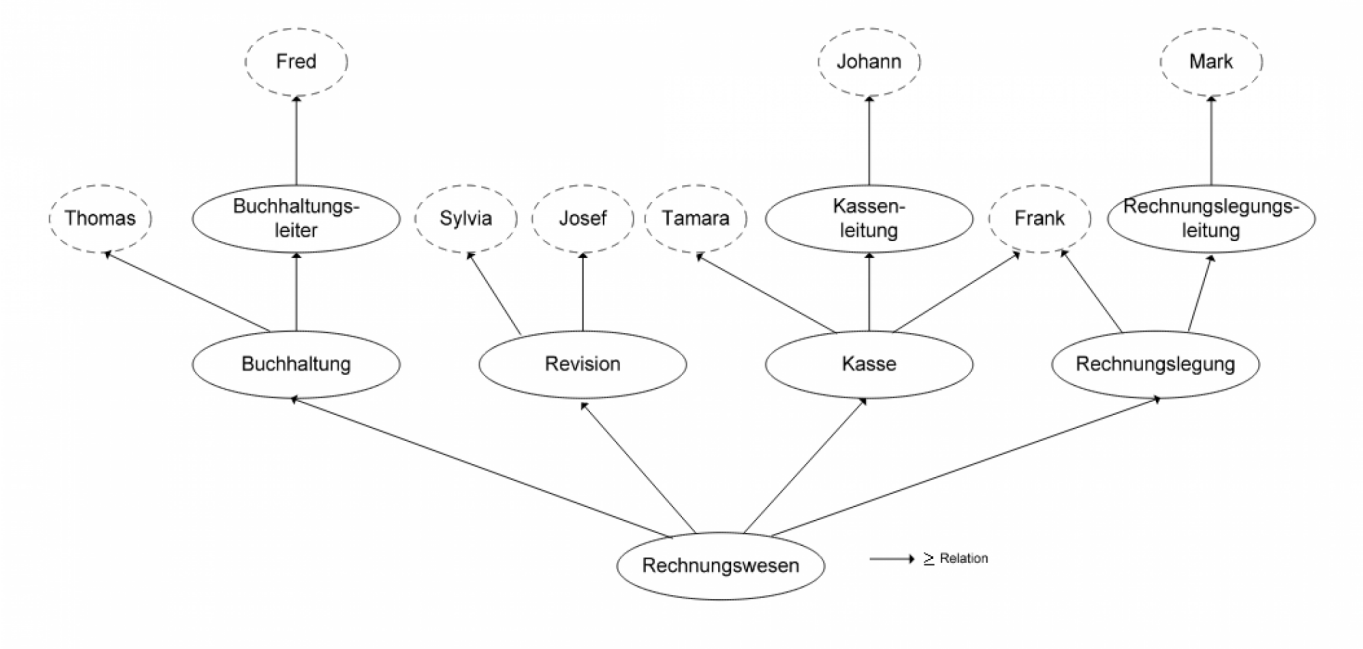
Die Rollenhierachie ist eine Möglichkeit organisatorische Beziehungen zwischen Rollen abzubilden (Ferraiolo et al. 2001, S.234). Sie definiert eine Vererbungsbeziehung zwischen Rollen und wird über eine Zugriffsrechtsvererbung oder eine Subjektmitgliedschaftsvererbung beschrieben.



Rollenhierachien können nochmals in beschränkte und allgemeine Rollenhierachien unterschieden werden. Dabei versteht man unter einer allgmeinen Rollenhierachie eine beliebige partielle Ordnung. Sie unterstütz eine Mehrfachvererbung, um Zugriffsrechte bzw. Subjektmitgliedschaften von zwei oder mehr Quellen zu erben.



Eine Rolle kann bei der beschränkten Rollenhierarchie einen oder mehrere direkteNachfahren haben, aber die Rolle ist beschränkt auf einen einzigen unmittelbaren Vorgänger. Das eRBAC fügt der Rollenhierachie noch die Spezialisierung der Rollen durch Parametrisierung und Personalisierung hinzu.

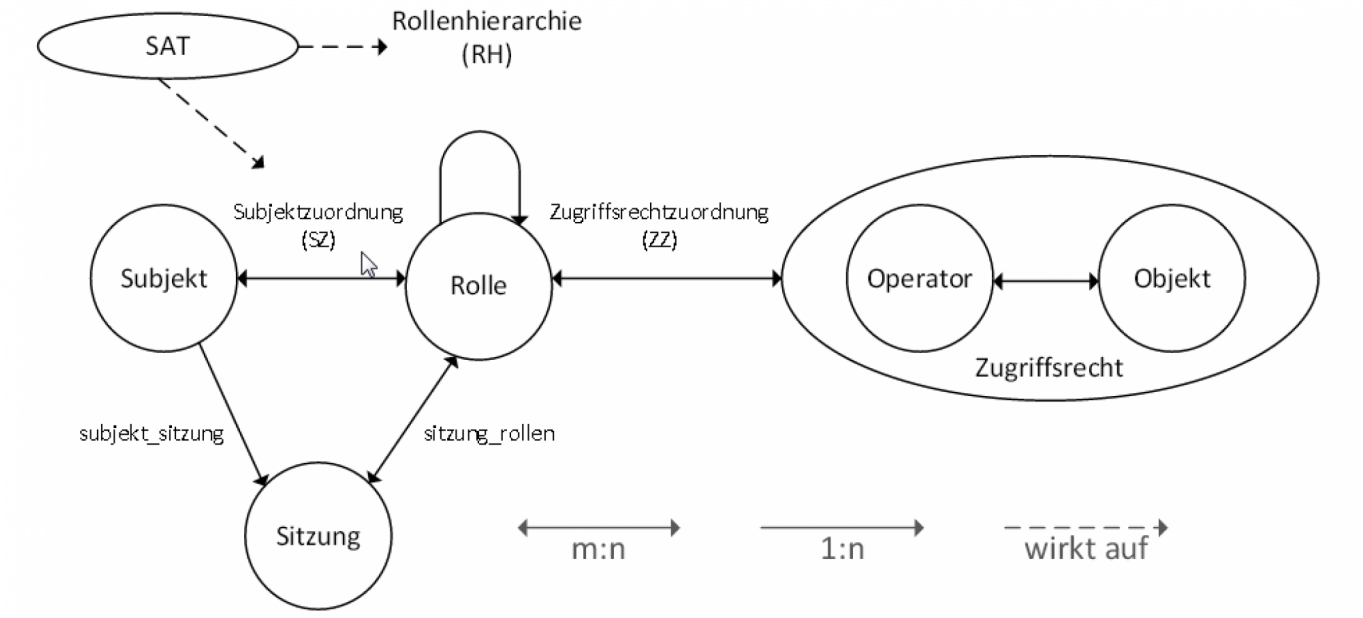


Für eine formale Zusammenfassung der Rollenhierachie des RBAC klicken Sie hier.

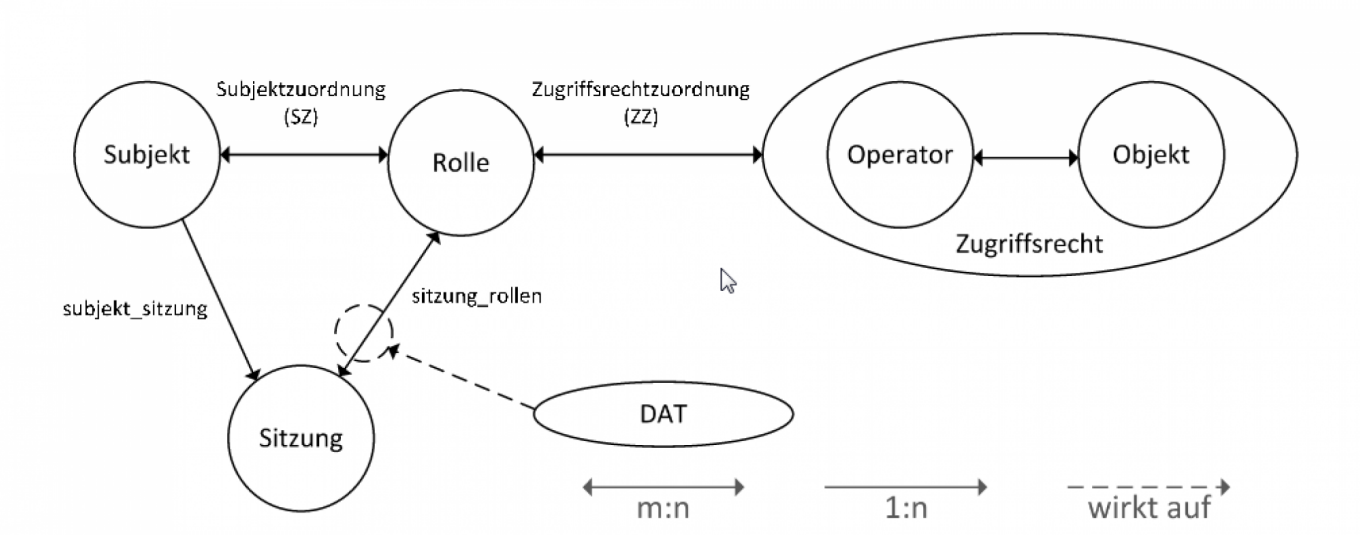
Aufgabentrennung

Die Azfgabentrennung kann dem RBAC-Kernmodell als zusätzliche Komponente orthogonal zur Rollenhierachie hinzugefügt werden man unterscheidet zwischen der statische (SAT) und eine dynamische Aufgabentrennung (DAT).

Das SAT stellt das Konzept der sich ausschließenden Rollen zur Verfügung. Damit wird bereits bei der Subjektzuordnung geprüft, dass keine Konfliktären Rollen vorhanden sind. Damit kann eine Betriebsweite organisatorische Aufgabentrennung bzw. Datenschutz besser durchgesetzt werden. Diese Art der Beschränkung ist auf der administrativen Ebene angesiedelt, da somit verhindert werden soll das bei der Veerbung in der Rollenhierachie die SAT verletzt wird.



Die DAT (dynamische Aufgabentrennung) begrenzt ebenfalls wie SAT die verfügbaren Zugriffsrechte. Sie definiert eine Bedingung auf die Beziehung sitzung_Rolle und verhindert so das bestimmte Rollen in der gleichen Sitzung aktiviert sind. Im Vergleich zur SAT bietet die DAT eine größere administrative Flexibilität.



Für eine formale Zusammenfassung der Aufgabentrennung des RBAC klicken Sie hier.

Neben dem drei Elemente der RBAC werden im Standard auch Funktionen für jede der Komponenten in den Bereichen Administration, Rechteprüfung und Protokollierung definiert. Dabei sind die einzigen zwischenden Funktionen, jene die sich auf das Kernmodul beziehen. Alle Funktionen des Kernmoduls und bei Bedarf der Erweiterungen müssen durch die Implementierung übernommen werden.

Literatur

ANSI INCITS 359-2004 (2004) Role Based Access Control. American National Standard for Information Technology.http://www.cs.purdue.edu/homes/ninghui/readings/AccessControl/ANSI+INCITS+359-2004.pdf. Abruf am 2014-08-17.

Ferraiolo DF, Sandhu RS, Gavrila S, Kuhn DR, Chandramouli R (2001) Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security 4(3):224-274.