Rechtemodellierung für Portalverbundanwendungen		**Konvention** **PVRechte 1.0.0** **Empfehlung**
Kurzbeschreibung	Definition der Modellierung von Zugriffsrechten für die einfache Integration der Rechte in den Stamm- und Anwendungsportalen und deren einfache Verwaltung	
Autor(en):	Peter Pichler Harald Stradal	Projektteam / Arbeitsgruppe: **AG Integration und Zugänge (AG-IZ)**
Beiträge von:	Hildegard Freidl, Ignaz Gritschenberger, Peter Reif	

Version 1.0.0 : **27.4.2012** Fristablauf: **18.7.2013**

Bezeichnung des Vorschlags

Inhaltsverzeichnis

Dieses Dokument beschreibt als KONVENTION Vorgaben und Empfehlungen für die Modellierung von Rechtesystemen für den Portalverbund der österreichischen Behörden.

1 Ausgangssituation

Bei vielen PV Anwendungen kommt es bei der Einführung zu Problemen, da die vorgegebenen Rechtemodelle mit den vorhandenen Werkzeugen und Prozessen nicht – bzw. nur mit großem Aufwand bewältigt werden können.

Oft haben die für die Anwendungsentwicklung Verantwortlichen wenig Erfahrung mit dem Portalverbund. Darum werden manchmal Rechtesysteme entworfen, die für eine an viele verschiedene Stammportale delegierte Rechteverwaltung nicht ideal sind.

Die Dokumentation der Berechtigungssysteme ist für die von der Rechteverwaltung zu treffende Entscheidung über die Zulässigkeit einer Rollenzuordnung oftmals unzureichend. Die Entwicklung von allgemein gut verwendbaren Rechtesystemen wird durch den Umstand erschwert, dass im Portalverbund verschiedenste Softwareprodukte im Einsatz sind, um Endbenutzern an Stammportalen Rechte zuzuordnen. Diese verwalten Rechte auf unterschiedliche Weise.

Zudem werden von unterschiedlichen Anwendungen verschiedenste Formen für Rechteparameter vorgeschrieben, um denselben Sachverhalt darzustellen.

Beispiel:

Aufgabenstellung: Ein Recht soll mit Hilfe eines PVP Rechteparameters regional auf die Landesgrenzen eines Bundeslandes beschränkt werden.

Verwendete bzw. geplante Lösungsvarianten:

- Parametername GKZ, als Wert ist der von der Statistik Austria für die Bildung von Gemeindekennziffern verwendete nummerische BL-Code (1-9) gefolgt von „0000“ zu verwenden. (z.B. GKZ=10000 für das Burgenland)
- Parametername GKZ, als Wert ist der von der Statistik Austria verwendete BL-Code zu verwenden. (z.B. GKZ=1 für das Burgenland)
- Parametername BL; als Wert ist die Abkürzung zu verwenden, wie sie früher für Kfz-Kennzeichen verwendet wurden.
- Parametername ORG, als Wert ist das VKZ der für die das Gebiet zuständigen Landesregierung zu verwenden
- Parametername OKZ, als Wert ist das OKZ der nicht behördlichen Organisation zu verwenden, um deren Wirkungsbereich zu beschreiben

2 Ziele

Dieses Dokument soll Vorgaben für das Design von PVP-Rechten geben. Die Einhaltung dieser Vorgaben soll gewährleisten, dass PVP-Rollen und deren allfällige Parameter unabhängig von der verwendeten Rechteverwaltung auf einfache und für den jeweiligen dezentralen Rechteverwalter verständliche und nachvollziehbare Art zugeordnet und entzogen werden können. Hierfür ist eine Simplifizierung zu erreichen, die der derzeitigen Komplexität von teilweise verschachtelten Berechtigungssystemen vorzuziehen ist.

Zudem soll definiert werden, welche Problemstellungen der Zugriffskontrolle mithilfe von PVP Rollen gelöst werden können und für welche andere Systeme verwendet werden sollen. Einige Berechtigungsfragen können nicht via PVP gelöst werden und wären in der jeweiligen Anwendung selbst zu lösen (Beispiel: PVP-Recht CMS-Redakteur, wobei der Inhaber des Rechtes oftmals die Redaktionsgruppen wechselt)

Es sollen Standards für Parameter definiert werden (z.B.: Ausdruck eines regionalen Wirkungs-/Einzugsbereiches).

3 Begriffsbestimmung

Akteur

Ein Akteur kann eine natürliche Person, oder ein technisches System (Systemprincipal, Applikationsuser) sein, welche erlaubterweise mit dem jeweiligen Zielsystem interagieren.

PVP-Rolle

Unter dem Begriff PVP-Rolle wird eine Textinformation verstanden, mit der einem Akteur Zugriffsrechte („Authorization“) innerhalb einer bestimmten PVP Anwendung eingeräumt werden.

Eine PVP-Rolle kann mehrere UseCases bzw. Subfunktionen einer Anwendung abdecken. So könnte die PVP-Rolle „Sachbearbeiter“ das Erfassen, Speichern, Ändern, Anfragen, Lesen und Drucken von bestimmten Daten in einer Anwendung umfassen.

Im PVP Protokoll werden alle PVP-Rollen des Akteurs für die jeweilige Anwendung übertragen.

Eine PVP-Rolle besteht aus dem Namen eines Rechtes und optional aus einer beliebig langen Liste von Parametern

Recht1([Parameter1=Wert1, Parameter1=Wert2,...]);Recht2(...)

PVP-Recht

Die möglichen PVP-Rollen einer Anwendung werden über die ldap.gv.at Datenstruktur gvApplicationRight (=PVP-Recht) beschrieben.

Dabei werden ein (zumindest) innerhalb der Anwendung eindeutiger Name, die für die Ausübung des Rechtes notwendige Sicherheitsklasse, sowie die zulässigen PVP-Parameter definiert.

PVP-Parameter

Der Begriff PVP-Parameter steht für ein Key-Value-Pair, das für die Bildung von PVP-Rollen verwendet wird. Mithilfe von PVP-Parametern kann die Bedeutung einer Rolle bzw. eines Rechtes konkretisiert werden.

Beispiel:

MAW_UPDATE(GKZ=60301)

Der Parameter „GKZ=60301“ erlaubt die Ausübung des Rechtes MAW_UPDATE für das Gebiet der steirischen Gemeinde Aibl.

4 Anwendungsbereich von PVP Rechten

Prozesse und Akteure im Rahmen der Zuordnung bzw. des Entzugs von PVP Rollen

Das Zu- bzw. Aberkennen von PVP Rollen ist eine Entscheidung, die auf Basis der gegebenen rechtlichen Grundlagen zu fällen ist. Zum Beispiel ist beim Zuordnen von Rollen, die Zugriff auf datenschutzrechtlich relevante Inhalte ermöglichen, zu prüfen, ob die im Datenschutzgesetz genannten Voraussetzungen gegeben sind. (z.B. ob die Verwendung der Daten aufgrund einer gesetzlichen Vorschrift bzw. Ermächtigung erfolgt). Der Betreiber einer Anwendung kann zusätzliche Vorgaben veröffentlichen, die ebenfalls einzuhalten sind. Beispielsweise kann die erfolgreiche Absolvierung von bestimmten Schulungsmaßnahmen notwendig sein.

In den Stammportalen wird das Vorliegen der notwendigen Voraussetzungen geprüft und organisatorische Maßnahmen gesetzt die sicherstellen, dass Rollen wieder entzogen werden, sollten die Voraussetzungen wegfallen. Die für die Rechteverwaltung zuständigen Personen sind nur im Ausnahmefall selbst Akteure in der jeweiligen Anwendung. Es kann NICHT davon ausgegangen werden, dass Rechteverwalter Experten für das Fachgebiet der jeweiligen Anwendung sind.

Die Zugriffssteuerung über PVP Rechte gehört zur Klasse der „Mandatory Access Control“ (MAC) Systeme.

Anwendungsgebiet

Das Prinzip der dezentralen Rechtevergabe mittels PVP-Rollen wurde geschaffen, da das Wissen darüber, welche Personengruppen für welche Tätigkeiten zu berechtigen sind, bei der Zugriffsberechtigten Stelle und nicht beim Anwendungsverantwortlichen vorhanden ist.

Mithilfe von PVP Rollen werden jene Zugriffsrechte verwaltet, die von der Rechteverwaltung der Stammportale auf Basis der Zuständigkeit der Mitarbeiter unter Prüfung der für die Erteilung notwendigen Voraussetzungen in der jeweiligen Organisation verwaltet werden sollen.

Zugriffskontrollsysteme, die nicht mithilfe von PVP Rollen umgesetzt werden können

PVP Rollen entstehen niemals durch Aktionen in der Anwendung, sondern werden immer mithilfe von anwendungsunabhängigen Rechteverwaltungssystemen zugeteilt.

Die Einräumung von Zugriffsrechten nach dem Prinzip der „Discretionary Access Control“(DAC,) erfolgt niemals über PVP Rechte, sondern immer in der Anwendung selbst. In DAC ist zu jedem einzelnen Objekt festgelegt, welche Benutzer welche Rechte haben. DAC-Rechte entstehen typischerweise im Rahmen der Neuanlage von Objekten (z.B. erhält jene Person alle Rechte an einem Objekt, die es angelegt hat) bzw. durch das Weitergeben der eigenen Rechte an eine andere Person.

Beispiel für DAC

In einem System für die elektronische Abbildung des Aktenlaufes ist vorgesehen, dass ein Akt nach seiner Anlage nur von jener Person bearbeitet werden darf, die ihn angelegt hat. Diese Person kann das Recht zur Bearbeitung weitergeben.

Beispiel für MAC

Für ein System für die Abbildung elektronischer Aktenläufe soll für jeden Akteur festgelegt werden, welche Typen von Akten angelegt werden können.

Anmerkungen

Wie die beiden Beispiele schon andeuten, kann DAC und MAC kombiniert werden.

Sollen DAC Konzepte umgesetzt werden, so muss die Anwendung einen eigenen Benutzerdatenbestand führen. (z.B. um beim Weitergeben eines Rechtes entsprechende Suchfunktionen zur Verfügung stellen zu können). In Portalverbundanwendungen sollen solche anwendungseigenen Benutzerdatenbestände automatisch aus den übermittelten PVP Headern aufgebaut und gewartet werden.

5 Vorgaben und Vorschläge für die Modellierung von PVP Rechtesystemen

Schreibweise und Namensgebung

(1) Namen von PVP-Rechten

Regel:

PVP-Rechte SOLLEN eindeutige und sprechende Namen haben, die einem bestimmten Benutzerkreis bzw. UseCase zuordenbar sind. Sie SOLLEN NICHT case-sensitiv interpretiert werden. Umlaute und Sonderzeichen ausgenommen „-“ und „_“ sind zu vermeiden. Die empfohlene Maximallänge beträgt 40 Zeichen.

Beispiel:

Best Practice

Für die Musteranwendung (kurz MAW) werden folgende Rechte mit folgenden Namen definiert:

- ANFRAGE bzw. MAW_ANFRAGE
- UPDATE bzw. MAW_UPDATE
- ADMIN bzw. MAW_ADMIN
- SACHBAERBEITER bzw. MAW_SACHBEARBEITER

Bad Practice

Für die Musteranwendung werden folgende Rechte mit folgenden Namen definiert:

- 01
- 02
- 03

(2) Namen von Parametern

Regel:

Parameter SOLLEN NICHT case-sensitiv interpretiert werden. In der von den Anwendungsverantwortlichen veröffentlichten Schreibweise MÜSSEN sie jedenfalls die gewünschte Wirkung erzielen.

Der Parametername soll aus wenigen Zeichen bestehen (z.B. GKZ, OKZ, VKZ,...). Die Bedeutung der verwendeten Abkürzung (GKZ...Gemeindekennzahl) soll in Dokumentation beschrieben sein. Die empfohlene Maximallänge beträgt 40 Zeichen.

Be**gründung:**

Fehler in der Groß- und Kleinschreibung sind in der Praxis häufig. Diese sind besonders schwer zu finden, wenn die von Anwendung erwartete Schreibweise von der der Dokumentation abweicht. Insbesondere aufgrund von automatischen „Korrekturen“ verschiedener Textverarbeitungsprogramme ist es schon öfters zu Fehlern in der Dokumentation der Anwendungsbetreiber gekommen. Darum ist es ideal, wenn Anwendungen und Anwendungsportale Parameternamen unabhängig von Groß- und Kleinschreibung behandeln.

Kurze Parameternamen führen zu leichter lesbaren Rollen.

(3) Anzahl der Parameter, mit der eine Rolle ausgestattet wird

Regel:

Die für die Bildung von Rollen notwendigen Parameterlisten, SOLLEN so kurz wie möglich gehalten werden.

Optionale PVP-Parameter SOLLEN vermieden werden. Wenn für ein PVP-Recht Parameter vorgesehen sind, SOLLEN für dieses PVP-Recht keine PVP-Rollen ohne Parameter gebildet werden.

Begründung:

Die Angabe langer Listen ist wartungsaufwändig. Erfassungsfehler sind häufig und in langen Zeichenketten auch schwerer zu finden. Zudem ist zu bedenken, dass http-Header (mittels derer PVP Rechte zumeist übertragen werden) eine reale Maximallänge haben.

(4) OKZ als Parameter für die Einschränkung auf Organisationen

Regel:

Wenn eine PVP-Rolle auf bestimmte Organisation beschränkt werden muss, SOLL dafür ein PVP-Parameter mit dem Namen „OKZ“ verwendet werden. Als Parameterwert für OKZ MÜSSEN Organisationskennzeichen gem. der Spezifikation Verwaltungs- und Organisationskennzeichen (VKZ) verwendet werden.

Beispiel:

OKZ=BMI,OKZ=BKA,OKZ=XFN-262918w

(um auszudrücken, dass ein Recht für das Innenministerium, das Bundeskanzleramt und die Land, forst- und wasserwirtschaftliche Rechenzentrum GmbH ausgeübt werden kann)

Anmerkung:

Mithilfe von OKZ können auch Firmen, Vereine, Kammern beschrieben werden.

Wird das OKZ als Parameter verwendet, so ist eine Mischung OKZ-VKZ zu vermeiden und NUR das OKZ zu verwenden.

Begründung:

Durch die Einhaltung dieser Regel, wird es für die Benutzer- und Rechteverwaltungen vereinfacht, bessere Oberflächen für die Definition von Parameterwerten zu schaffen.

(5) GKZ als Parameter für die Beschreibung geografischer Regionen Gemeindegebiet, politischer Bezirk, Bundesland

Regel:

Um die Wirkung eines Rechtes auf ein Gemeindegebiet, einen politischen Bezirk oder ein Bundesland einzuschränken SOLL der PVP-Parameter GKZ verwendet werden. Als Parameterwert sollen 5 stellige Zahlen verwendet werden.

<u>Für das gesamte Bundesgebiet</u>

Wenn der Parameter GKZ verwendet wird, so soll es möglich sein mit dem Parameter GKZ=00000 das Recht für das gesamte Bundesgebiet der Republik Österreich zu gewähren.

<u>Gebiet eines Bundesland</u>

Für Bundesländer soll die Statistik-Österreich Bundesland-Kennziffer (erste Stelle der Gemeindekennziffer) gefolgt von „0000“ als Wert für den Parameter GKZ verwendet werden.

<u>Politischer Bezirk</u>

Um ein Recht für das Gebiet eines politischen Bezirkes zuzuordnen, soll die von der Statistik Austria verwaltete Kennziffer für politische Bezirke (ersten drei Stellen der

Gemeindekennziffer) gefolgt von „00“ verwendet werden. Wenn es möglich ist mit einer GKZ Bezirke anzugeben, dann soll es auch möglich sein durch Angabe einer GKZ eines Bundeslandes das Recht für alle Bezirke des angegebenen Bundeslandes zu erteilen.

Gemeindegebiet

Für die Bezeichnung von Gemeindegebieten SOLL die von der Statistik Austria verwalteten und publizierten Gemeindekennziffern verwendet werden. Ist es möglich ein Gemeindegebiet anzugeben, so soll es auch möglich sein einen Bezirk (für alle Gemeindegebiete des Bezirkes) bzw. ein Bundesland anzugeben.

Beispiele:

Best Practice

MAW_UPDATE(GKZ=61117,GKZ=61511)

Das Recht MAW_UPDATE darf für das Gemeindegebiet der Gemeinden Trofaiach und Mureck wahrgenommen werden

MAW_UPDATE(GKZ=61100, GKZ=61500)

Das Recht MAW_UPDATE darf für das Gebiet der Bezirke Leoben und Radkersburg ausgeübt werden.

MAW_UPDATE(GKZ=60000)

Das Recht darf für das Gebiet des Bundeslandes Steiermark ausgeübt werden

Bad Practice

Das Recht MAW_UPDATE soll mit einer GKZ eingeschränkt werden. Es dürfen aber nur Gemeindekennziffern verwendet werden. (Die oben genannten Formen mit „00“ bzw. „0000“ werden nicht unterstützt)

Beispielrolle der BH Leoben:

MAW_UPDATE(GKZ=61101, GKZ=61102, GKZ=61103, GKZ=61104, GKZ=61105, GKZ=61106, GKZ=61107, GKZ=61108, GKZ=61109, GKZ=61110, GKZ=61111, GKZ=61112, GKZ=61113, GKZ=61114, GKZ=61115, GKZ=61116, GKZ=61117, GKZ=61118, GKZ=61119)

Begründung:

Durch die Wiederverwendung von Konzepten sinkt der Schulungsaufwand für RechteverwalterInnen. In Rechteverwaltungssoftware kann die Eingabe von Gemeindekennzahlen durch spezielle Editoren unterstützt werden.

Organisatorische Vorgaben

(6) Beliebige Kombinierbarkeit von Rollen

Regel:

Sofern es nicht verboten ist, dass mehrere PVP-Rollen von derselben Person ausgeführt werden, MÜSSEN Rollen einer Anwendung beliebig kombinierbar sein.

Beispiel:

In der Musteranwendung werden die Rechte MAW_Chef und MAW_Mitarbeiter eingeführt. Beide Rechte ermöglichen verschiedene Aktionen in der Musteranwendung zu setzen. Es muss möglich sein einem Akteur sowohl die Rolle MAW_Chef als auch die Rolle MAW_Mitarbeiter zuzuordnen.

Begründung:

An Stammportalen werden Personen aufgrund Ihrer Zuständigkeiten PVP-Rollen - zugeordnet. Prinzipiell steht es den Organisationen frei zu bestimmen, ob verschiedene Aufgaben in einer PV Anwendung von einer – oder von verschiedenen Personen ausgeführt werden sollen.

(7) Parameter dürfen nur berechtigend und nie einschränkend interpretiert werden

Regel:

Ein Parameter bzw. eine Rolle dürfen die Rechte eines Benutzers nur erweitern, aber nie einschränken; Whitelisting statt Blacklisting.

Bespiel:

Für die Musteranwendung soll die Möglichkeit Daten zu erfassen auf bestimmte Bundesländer eingeschränkt werden.

Best Practice:

Für die Musteranwendung wird für die o.g. Anwendungsfälle ein PVP-Recht definiert – MAW-UPDATE. Bei Verwendung des Rechtes MAW-UPDATE müssen mit dem Parameter GKZ, die Bundesländer angeben werden, für die Daten erfasst werden können.

Beispiele:

MAW-UPDATE(GKZ=10000,GKZ=30000,GKZ=60000,GKZ=90000)

Für Benutzer die Daten für die Bundesländer Burgenland, Niederösterreich, Steiermark und Wien erfassen dürfen.

Bad Practice:

Für die Musteranwendung wird für die o.g. Anwendungsfälle ein PVP-Recht definiert – MAW-UPDATE. Bei Verwendung des Rechtes MAW-UPDATE müssen mit dem Parameter GKZ, die Bundesländer angeben werden, für die Daten NICHT erfasst werden können.

Gleiche Berechtigung wie in Best Practice:

MAW-UPDATE(GKZ=20000,GKZ=40000,GKZ=50000,GKZ=70000,GKZ=80000)

Begründung:

Die Administration der Berechtigungen kann bei Verwendung einschränkender Parameter für den Rechteverwalter sehr komplex und undurchschaubar werden.

Beispiel fortgesetzt:

Aufgrund besserer Lesbarkeit wird

MAW-UPDATE(GKZ=10000)

als

UPD(1)

geschrieben

Best Practice: Gruppe A hat die Berechtigung

UPD(1,3,5,8,9)

Gruppe B hat

UPD(6,7,8)

ist jemand in beiden Gruppen, sendet das Stammportal

UPD(1,3,5,8,9);UPD(6,7,8)

oder die kumulierte Variante

UPD(1,3,5,6,7,8,9)

Bad Practice: Gruppe A hat die BLACKLIST-Berechtigung

UPD(2,4,6,7)

Gruppe B hat

UPD(1,2,3,4,5,9)

ist jemand in beiden Gruppen, sendet das Stammportal

UPD(1,2,3,4,5,6,7,9)

was dem Benutzer zu wenig Rechte einräumt. Der Rechteverwalter muss ihm daher expliziert das Recht

UPD(2,4)

zuweisen. Das bedeutet bei den meisten Rechteverwaltungssystemen das Anlegen einer weiteren Gruppe.

Semantische Bedeutung von Rechten und Parametern

(8) Kumulierbarkeit und Separierbarkeit von Parametern

Regel:

Für Rechte, die im Portalverbund der österreichischen Behörden angeboten werden MÜSSEN die Möglichkeiten in einer Anwendung identisch sein, wenn sie mit einer Rolle mit mehreren Parametern ausgedrückt werden oder mit mehreren Rollen des selben Rechtes, sofern insgesamt dieselben Parameter bekanntgegeben werden. Derselbe Parameter kann auch mehrmals angegeben werden, ohne dass sich dadurch die Bedeutung ändert

Es MUSS gelten:

Recht_A(Parameter1); Recht_A(Parameter2); Recht_A(Parameter3)
==
Recht_A(Parameter1, Parameter2, Parameter3)
==
Recht_A(Parameter1, Parameter3);Recht_A(Parameter2)

==

Recht_A(Parameter1, Parameter2);Recht_A(Parameter1, Parameter3)

Begründung:

Durch Kumulierung werden PVP-Rollen kürzer.

Das Rechtesystem ist leicht verständlich. Mit allen im Portalverbund im Einsatz befindlichen Rechteverwaltungen können so konstruierte Rechtesysteme verwaltet werden. Einem Benutzer kann in einer Rechteverwaltung – das gleiche Recht mehrfach mit verschiedenen Parametern zugewiesen werden. (z.B. über Gruppen)

Anmerkung:

Diese Regel hat zur Folge, dass Abhängigkeiten zwischen Parametern nicht dargestellt werden können.

Beispiel:

MAW_Einkauf(OKZ=(...);BGR=(...))

OKZ... Organisationseinheit für die beschafft werden darf

BGR...Beschaffungsgruppe

Beispielrollen:

MAW_EINKAUF(OKZ=BMI:II1a, BGR=WAFFEN)

MAW_EINKAUF(OKZ=BMI:I2a, BGR=AUTOS)

ergeben kumuliert

MAW_EINKAUF(OKZ=BMI:II1a, BMI:I2a, BGR=WAFFEN,BGR=AUTOS)

Aufgrund der Vorschrift zur Möglichkeit der Kombinierbarkeit müsste es möglich sein, einer Person beide Rollen zuzuordnen. Aufgrund des Kumulierbarkeitsgebotes ist es mit einem solchen Rechteaufbau nicht möglich, die Kombination zwischen Organisationseinheit und Beschaffungsgruppe über Parameter darzustellen. Die Möglichkeit einzukaufen kann auf Organisationen und auf Beschaffungsgruppen eingeschränkt werden. Es ist aber nicht möglich darzustellen, dass für die eine Organisationseinheit nur Waffen und für die andere nur Autos beschafft werden dürfen.

Optimierung:

Rechteverwaltungen können prinzipiell kumulieren, um die Anzeige übersichtlicher zu gestalten. Stammportale können kumulieren um die Länge der Header zu verkürzen. Anwendungsportale können diese Aufgabe ebenfalls übernehmen. Am Anwendungsportal implementiert vereinfacht sich die Interpretation der PVP Rollen für die Anwendung.

(9) Reihenfolge von Rechten und Parametern

Regel:

Die Reihenfolge der Angabe von Rechten und Parametern MUSS frei von semantischer Bedeutung sein. Sie darf keine Auswirkung auf die Möglichkeiten bei der Benutzung der Anwendung haben.

Recht_A(Parameter1,Parameter2); Recht_B(Parameter3)
==
Recht_B(Parameter3);Recht_A(Parameter2,Parameter1)

Begründung:

Zumeist werden Akteuren PVP-Rollen durch Gruppen („Funktionsprofile“) zugeordnet. Die Zugriffsrechte eines Akteurs für eine Anwendung sind dann die Vereinigungsmenge der seinen verschiedenen Gruppenzugehörigkeiten zugeordneten Rollen, wobei die Reihenfolge der Rechte und Parameter nicht festgelegt werden kann.

(10) Atomare Rechteparameter

Regel:

Parameter SOLLEN atomare Wertebereiche haben. Für den Begriff „atomarer Wertebereich“ ist hier sinngemäß jene Definition anzuwenden, die zur Beschreibung der Ersten Normalform der Datenbankmodellierung verwendet wird.

Beispiel:

Das Recht MAW_UPDATE soll zusätzlich zum Bundesland auf einen der Verwaltungsbereiche „PV“ (Personalverwaltung), „BW“ (Bauen und Wohnen) und „SA“ (Steuern und Abgaben) beschränkt werden können.

Best Practice

Für jeden Verwaltungsbereich wird ein eigenes Recht definiert MAW_UPDATE_PV, MAW_UPDATE_SA und MAW_UPDATE_BW. Die Landesregierung wird mit dem Parameter OKZ definiert

Beispielrollen Best Practice:

MAW_UPDATE_PV(OKZ=L1,OKZ=L2);MAW_UPDATE_SA(OKZ=L1)

Bad Practice

Abweichend von der obigen Regel wird festgelegt, dass mehrere Verwaltungsbereiche nicht in einem Parameter angegeben werden dürfen.

Beispielrollen Bad Practice:

MAW_UPDATE(MAW_WOFUER=L1$PV, MAW_WOFUER=L1$SA, MAW_WOFUER=L2$PV)

Die Kombination von Bundesland und Verwaltungsbereich widerspricht der Regel atomarer Parameterwerte. Bei dieser Variante wurde die Regel aber nur einmal (weniger) verletzt.

Very Bad Practice1:

Es wird festgelegt, dass das Recht MAW_Update mit dem Parameter MAW_WOFUER zu konkretisieren ist. Der Wert des Parameters MAW_WOFUER ist aus dem VKZ des

Bundeslandes gefolgt vom Zeichen „$“ und gefolgt von der Liste der Verwaltungsbereiche zu bilden. Mehrere Verwaltungsbereiche sind wieder durch „$“ zu trennen.

Beispielrollen Very-Bad-Practice:

MAW_UPDATE(MAW_WOFUER=L1PVSA, MAW_WOFUER=L2$PV)

Sowohl die Kombination aus Bundesland und Verwaltungsbereich als auch die Angabe mehrerer Verwaltungsbereiche in einem Parameter ist ein Verstoß gegen die Regel atomarer Parameterwerte.

Begründung:

In vielen Benutzer- und Rechteverwaltungen ist es möglich für Rechteparameter Wertelisten zu hinterlegen. Wenn mehrere Sachverhalte in einen Parameter kodiert werden, so werden die Wertelisten sehr groß und unübersichtlich.

Very Bad Practice2:

Damit der Parameter so atomar wie möglich bleibt, werden für die Eingrenzung mehrere unterschiedliche Parameter festgelegt (BL und PARAM)

Beispielrollen für Very Bad Practice2:

MAW-UPDATE(PARAM=1, PARAM=2, BL=6)

Hat ein Anwender nun aus einem anderen Grund erneut das Recht MAW-UPDATE mit anderen Parametern zugewiesen wird die Regel der Kumulierbarkeit verletzt.

Beispiel der Verletzung:

MAW-UPDATE(PARAM=1, PARAM=2, BL=6) UND

MAW-UPDATE(PARAM=4, BL=8) kumulierte zu dem unerwünschten Ergebnis

MAW-UPDATE (PARAM=1, PARAM=2, PARAM=4, BL=6, BL=8) also einer mehr Rechten in beiden Bundesländern (BL).

Bei derartigen Fällen, wo die Rollenmodellierung die zweite Dimension (atomarer Parameter) verlassen MUSS, um praktikabel administriert werden zu können, muss anwendungsseitig entschieden werden, ob mehrere Rollen eine sinnvolle Alternative zu nichtatomaren Parametern darstellen, oder ob aus Verwaltungsgründen die SOLL-Regel gemäß dem Beispiel „Bad Practice“ verletzt werden kann.