Straßen.NRW.
Landesbetrieb Straßenbau Nordrhein-Westfalen

Kernsystem

Verkehrsrechnerzentralen

Technische Dokumentation

Zugriffsrechte Datenverteiler

Ersteller: Kappich Systemberatung
integrativ und unabhängig
Kompetenz in System- und Verkehrstechnik

Autor: Dipl.-Ing. C. Westermann

Version:	2.0
Stand	03.06.2019
Status:	akzeptiert
PID:	LBNW14.019-2.0
Submodell:	----
Dokument:	LBNW14.019 Zugriffsrechte-2.0.doc
VS-Einstufung:	----
Projekt ID AG:	----
Projekt ID AN:	LBNW14.019 Zugriffsrechte

Kappich Systemberatung

Im Auftrag des Landesbetriebs Straßenbau NRW

1 Allgemeines

Verteilerliste

Entfällt. Dokumentverteilung entsprechend aktuellem Projektverteiler.

Versionsübersicht

Nr.	Datum	Version	Änderungsgrund	Bearbeiter
1	18.03.11	0.1	Ersterstellung	Westermann
2	28.06.11	1.0	Überführung in den Zustand akzeptiert	Westermann
3	05.09.16	1.1	Berücksichtigung der aktuellen Datenmodelle	Westermann
4	03.06.19	2.0	Berücksichtigung der aktuellen Kernsoftware 3.13	Westermann

Tabelle 1-1: Versionsübersicht

Änderungsübersicht

Nr.	Version	geändertes Kapitel	Beschreibung der Änderung
1	0.1	alle	Ersterstellung
2	1.0	alle	Korrekturen interne QS (Kappich)
3	1.1	3.3	Datenmodell Zugriffsrechte (neu) angepasst
4	2.0	3.3, 3.4	Berücksichtigung der aktuellen Kernsoftware 3.13

Tabelle 1-2: Änderungsübersicht

Kurzbeschreibung

In diesem Dokument wird der Mechanismus der Zugriffsrechte beschrieben.

Inhalt

Abkürzungen

siehe Dokument "Abkürzungen".

Definitionen

siehe Dokument "Glossar".

Verzeichnis der Tabellen

Verzeichnis der Abbildungen

2 Erweiterung Vergabe Zugriffsrechte Datenverteiler

2.1 Ausgangslage (alte Zugriffsrechte)

Die Vergabe der Zugriffsrechte ist gemäß der Spezifikation BLAK im Kernsystem implementiert worden. Es hatte sich in der Praxis herausgestellt, dass diese Lösung bei der Vergabe der Zugriffsrechte sehr aufwendig ist und der Mechanismus zur Vergabe und Prüfung der Zugriffsrechte anwenderfreundlich erweitert werden kann.

2.1.1 Aktuelle Spezifikation

Zur Festlegung der Zugriffsrechte werden aktuell in der Konfiguration Rollen/Regionen-Paare spezifiziert, in denen definiert wird, welche Aktivitäten (Rolle) für welche Objekte (Region) zulässig sind. Über die Parametrierung wird festgelegt, welche Rollen/Regionen-Paare einer Berechtigungsklasse und welche Benutzer der Berechtigungsklasse zugeordnet sind.

Abbildung 1 skizziert die aktuelle Struktur zur Festlegung der Zugriffsrechte eines Benutzers.

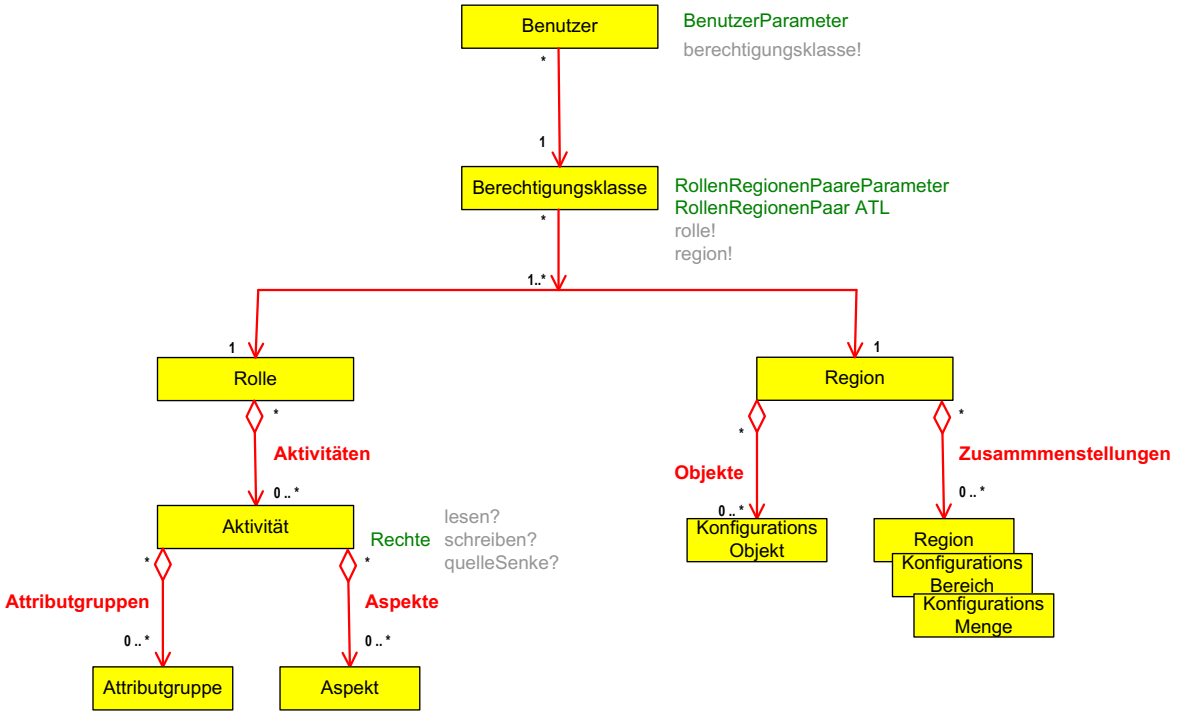

Abbildung 1: Berechtigungsklassen

Wenn die Rechteprüfung aktiviert wird (Aufrufparameter beim Datenverteiler) gilt alles, was nicht explizit als erlaubt spezifiziert wurde, als verboten. Dabei ist die Angabe von Wildcards möglich.

Somit sind bei aktivierter Rechteprüfung vor der Konfiguration und Parametrierung der Zugriffsrechte keine Aktivitäten zu den Konfigurationsobjekten möglich.

Bei den Spezifikationen der Aktivitäten bedeutet die Angabe einer leeren Menge von Attributgruppen oder Aspekten, dass alle Attributgruppen oder Aspekte betrachtet werden. Damit kann die Generalaktivität (alle Aktivitäten erlaubt) durch die Vorgabe der beiden leeren Mengen Attri-

butgruppen und Aspekte mit konfigurierendem Zugriffsdatensatz, der "lesen", "schreiben" und als "Quelle/Senke anmelden" erlaubt. Analog ist die Generalregion spezifizierbar (für alle Konfigurationsobjekte).

Die aktuelle Spezifikation/Realisierung hat als Prioritätenregelung, dass grundsätzlich

- keine Rechte vorliegen (Aktion "lesen" Nein, Aktion "schreiben" Nein, Aktion "Als Quelle/Senke anmelden" Nein)
- die Region keine Konfigurationsobjekte enthält

Bei der Überlagerung von verschiedenen Vorgaben hat ein explizites "Ja" die höchste Priorität und führt dazu, dass einmal erteilte Rechte nicht wieder durch einen weiteren Eintrag entzogen werden können.

Analog ist bei der Spezifikation von Regionen grundsätzlich kein Konfigurationsobjekt enthalten und ein einmal eingetragenes Konfigurationsobjekt ist nicht mehr durch z.B. eine Negativliste aus einer spezifizierten Region entfernbar.

2.1.2 Schwachstellen der aktuellen Lösung

Bei der aktuellen Lösung gibt es Anwendungsfälle, die nur sehr umständlich umsetzbar sind und in Punkto Anwenderfreundlichkeit deutlich verbessert werden könnten:

- Damit sich eine Applikation überhaupt beim Datenverteiler anmelden kann, müssen bestimmte Basisrechte vorhanden sein. Diese Basisrechte müssen z.Z. über denselben Mechanismus konfiguriert und parametriert werden. Hier ist es anwenderfreundlicher, wenn diese Basisrechte implementiert werden (d.h. bei der Anmeldung stehen diese Rechte implizit zur Verfügung), so dass hier keine explizite Versorgung erfolgen muss.
- Bei der Versorgung von Rollen und Regionen sind jeweils nur Wildcard und Positivaussagen möglich. Hiermit fehlt die Möglichkeit, Angaben der Form "alles außer …" einfach zu spezifizieren. Zurzeit müssen für Fälle dieser Art alle Möglichkeiten (bis auf die Ausnahme) in entsprechenden Listen aufgeführt werden.

Weiter gibt es zusätzliche Anwendungsfälle, die damals nicht spezifiziert wurden und dementsprechend nicht implementiert sind. Der gerichtete Datenaustausch zwischen zwei Applikationen wird beim Datenverteiler genau wie bei allen anderen Datenverteilungen über Attributgruppen und Aspekte abgewickelt. Dieser Mechanismus wird insbesondere bei dienstleistenden Applikationen eingesetzt. Z.B. werden beim Archivsystem auf Datenverteilerebene Anfragen und Antworten über die Attributgruppe `ArchivAnfrageSchnittstelle` abgewickelt. Die Funktionalität wird über entsprechende Datenverteilerapplikationsfunktion gekapselt, so dass der Austausch über die entsprechenden Attributgruppen/Aspekt-Kombinationen für den Anwender transparent ist. Allerdings prüft der Datenverteiler an dieser Stelle auch nur, ob die Applikation (respektive der Benutzer, unter dem die Applikation gestartet wurde) die notwendigen Rechte hat, Archivanfragen zu stellen bzw. Archivantworten zu erhalten. Eine inhaltliche Prüfung findet nicht statt. Damit kann zu Zeit nicht vorgegeben werden, dass ein bestimmter Benutzer nur bestimmte Daten beim Archiv anfragen kann.

Ähnliches gilt bei der Kommunikation mit der Konfiguration. Auch hier kann nicht vorgegeben werden, zu welchen Konfigurationsobjekten ein Benutzer Informationen erhalten kann. Weiter ist es nicht möglich, die Erzeugung von neuen dynamischen Objekten z.B. auf bestimmte Objekttypen einzuschränken (z.B. nur neue Benutzer).

Ein weiteres Problem im aktuellen Datenmodell zur Vergabe der Zugriffsrechte ist der hohe Konfigurationsaufwand.

- Es gibt 5 Typen, die für die Vergabe der Zugriffsrechte zuständig sind.

- Insbesondere ist die weitere Ebene zwischen Rolle und Aktivität nicht unbedingt erforderlich.
- Verbesserungsvorschlag:
  An Konfigurationsobjekten vom Typ Rolle direkt einen Parameterdatensatz "hängen", der die alle Möglichkeiten der Konfiguration enthält.
    - Insbesondere entfällt bei dieser Vorgehensweise der Aufwand, für neu definierte Attributgruppen/Aspekt-Kombinationen die Konfiguration zu den Zugriffsrechten zu überarbeiten. Die Parametrierung ist für solche Fälle einfacher.
- Analog kann die Festlegung der Regionen ebenfalls über einen Parameter festgelegt werden. In diesem Fall erfordert z.B. die Übernahme eines weiteren Versorgungsbereichs (z.B. einer UZ) im Regelfall keine Anpassung der Konfiguration sondern nur die Erweiterung des entsprechenden Parameters.

2.2 Zielvorgabe (neue Zugriffsrechte)

Die Vergabe der Zugriffsrechte durch den Datenverteiler soll erweitert werden. Dabei sollen insbesondere die Schwachstellen der aktuellen Implementierung behoben werden.

In diesem Dokument ist die Erweiterung zur Vergabe der Zugriffsrechte beschrieben.

3 Anwenderforderungen / Techn. Anforderungen (neue Zugriffsrechte)

3.1 Implizite Rechtezuteilung

Die während der Initialisierungsphase einer Applikation notwendigen Rechte werden implizit zugeteilt. Das bedeutet, wenn der Benutzer, unter dem die Applikation gestartet wurde, dem Datenverteilersystem bekannt ist, ist die Anmeldung der Applikation ohne weitere explizite Versorgung der Zugriffsrechte möglich.

3.2 Vereinfachte Vergabe von Zugriffsrechten

Die Konfiguration und Parametrierung der Zugriffsrechte wird so erweitert/geändert, dass folgende Vorgaben möglich sind:

Rollenspezifikation

- Alle Attributgruppen/Aspektkombinationen dürfen gelesen werden
- Nur Bestimmte Attributgruppen/Aspektkombinationen dürfen geschrieben bzw. als Quelle/Senke angemeldet werden.
- Bestimmte Attributgruppen/Aspektkombinationen dürfen nicht geschrieben bzw. als Quelle/Senke angemeldet werden.
- Eine Rolle kann durch andere Rollen erweitert werden (Aufbau einer Rollen Hierarchie)

Regionspezifikation

- Alle Konfigurationsobjekte eines Konfigurationsbereichs
- Alle Messquerschnitte eines Konfigurationsbereichs
- Alle Konfigurationsobjekte unterhalb eines Konfigurationsbereichs bis auf die Objekte x,y,z und die vom Typ Messquerschnitt
- Bestimmte Konfigurationsobjekte können ausgeschlossen werden
- Als Filter können Objekttypen und Mengen vorgegeben werden
- Eine Region kann durch andere Regionen erweitert werden

Hierzu ist das Datenmodell zur Spezifikation der Zugriffsrechte und die Software entsprechend anzupassen.

3.3 Datenmodell

Abbildung 3-2 skizziert das Datenmodell zur Beschreibung der (neuen) Zugriffsrechte für einen Benutzer, der sich beim Datenverteilersystem angemeldet:

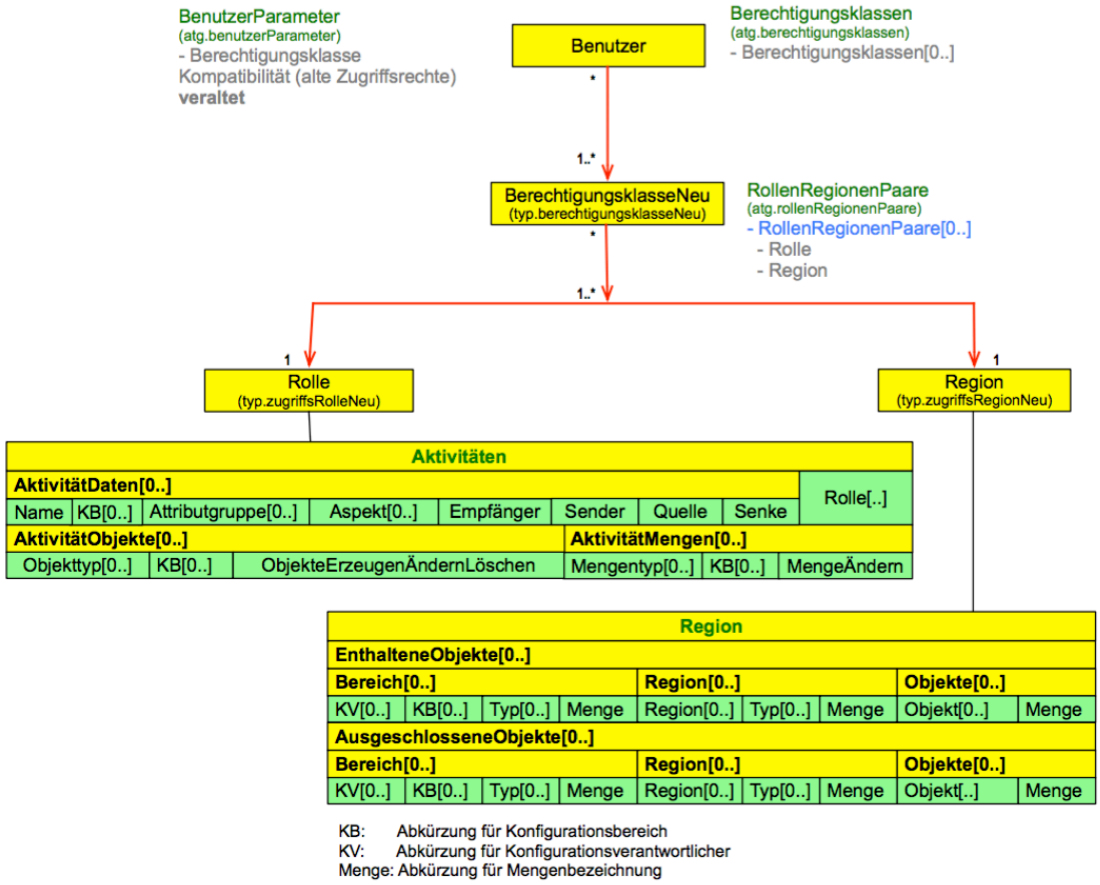

Abbildung 3-2: Datenmodell Zugriffsrechte (neu)

Aus Kompatibilitätsgründen bleibt die Möglichkeit bestehen, die Zugriffsrechte nach der alten Methode zu versorgen (über die Attributgruppe atg.benutzerParameter). Welche Zugriffsrechteprüfung beim Datenverteiler verwendet wird, kann über das Aufrufargument `-rechtePruefung` festgelegt werden[1].

[1] Ab Version 3.13 der Kernsoftware wird unter dem Aufrufparameter **`-rechtePruefung=ja`** die neue Rechteprüfung aktiviert. Der Wert „neu“ wird weiter unterstützt. Wenn die alte Rechteprüfung verwendet werden soll ist **`-rechtePruefung=alt`** zu setzen.

3.3.1 Benutzer

Ein Benutzer ist ein dynamisches Objekt, unter dem sich eine Applikation gegenüber dem Datenverteiler authentifiziert. Bei der Applikation kann es sich um einen Prozess handeln, der auf dem Verkehrsrechner läuft (z.B. die Datenaufbereitung) oder es kann sich z.B. um die Bedienung und Visualisierung handeln. In allen Fällen prüft der Datenverteiler (bei eingeschalteter Rechteprüfung) ob der Benutzer, unter dem die Applikation gestartet wurde, berechtigt ist, die über die Datenverteilerschnittstelle eingeleitete Aktion durchzuführen. Dies kann z.B. das Anmelden von Onlinedaten zu bestimmten Konfigurationsobjekten sein, oder die Erzeugung eines neuen dynamischen Objektes z.B. eines neuen Benutzers.

Welche Berechtigungen ein Benutzer hat, wird durch die Zuordnung von Berechtigungsklassen festgelegt.

Die Berechtigungsklassen werden bei den (neuen) Zugriffsrechten durch Parametrierung der Attributgruppe Berechtigungsklassen festgelegt.

3.3.2 Berechtigungsklassen

Über Berechtigungsklassen können die Rechte verschiedener Benutzer bzw. Benutzertypen zusammengefasst werden.

Berechtigungsklassen sind als Konfigurationsobjekte[2] versorgt. Sie fassen ihrerseits Rollen und Regionen paarweise zusammen.

3.3.3 Rolle

Über eine Rolle[3] wird festgelegt, welche Aktivitäten ein Benutzer, dem diese Rolle zugewiesen wurde, durchführen darf.

Welche Aktivitäten mit den entsprechenden Rollen durchgeführt werden dürfen, ist parametrierbar. Dazu steht die Parameterattributgruppe Aktivitäten zur Verfügung:

Aktivitäten								
AktivitätDaten[0..]								Rolle[..]
Name	KB[0..]	Attributgruppe[0..]	Aspekt[0..]	Empfänger	Sender	Quelle	Senke	
AktivitätObjekte[0..]					**AktivitätMengen[0..]**			
Objekttyp[0..]	KB[0..]	ObjekteErzeugenÄndernLöschen			Mengentyp[0..]	KB[0..]	MengeÄndern	

Abbildung 3-3: Attributgruppe Aktivitäten

Der Datenverteiler prüft ab Version 3.13 bei aktivierter neuer Zugriffsrechteprüfung zusätzlich zu den Onlineberechtigungen die Berechtigung des Benutzers welche Archivanfragen durchgeführt werden können. Dabei werden nur Archivanfragen erlaubt, wenn der Benutzer die entsprechende Berechtigung hat diese Daten auch online als Empfänger anzumelden.

---

[2] Bei den neuen Zugriffsrechten werden hier entsprechende Konfigurationsobjekte vom Typ typ.berechtigungsklasseNeu versorgt.

[3] Bei den neuen Zugriffsrechten werden hier entsprechende Konfigurationsobjekte vom Typ typ.zugriffsRolleNeu versorgt.

Die Aktivitäten werden über drei Attributlisten beschrieben:

- **AktivitätDaten[0..]**
  Hier wird spezifiziert, wie die Zugriffrechte beim Datenaustausch für die entsprechende Rolle gesetzt sind. Es können verschiedenen Aktivitäten definiert und der Rolle zugeordnet werden.
  - **Name**
    Beschreibender Name dieser Aktivität
  - **KB[0..]**
    Array von Konfigurationsbereichen (Referenzen auf Konfigurationsbereiche), die die Auswahl der Attributgruppen filtern.
    Wenn dieses Array leer ist, sind alle Attributgruppen ausgewählt
  - **Attributgruppe[0..]**
    Array von Attributgruppen (Referenzen auf Attributgruppen).
    Wenn dieses Array leer ist, sind alle Attributgruppen ausgewählt
  - **Aspekte[0..]**
    Array von Aspekten (Referenzen auf Aspekte).
    Wenn dieses Array leer ist, sind alle Aspekte ausgewählt

    Die Möglichkeiten einer Aktivität beziehen sich auf alle laut Konfiguration vorgesehenen Attributgruppen/Aspekt-Kombinationen, die sich aus dem Kreuzprodukt der beiden Arrays ergeben. Laut Konfiguration seien die Attributgruppe A1 mit den Aspekten S1, S2 und S3, die Attributgruppe A2 mit den Aspekten S1, S4 und S5 und die Attributgruppe A3 mit den Aspekten S1 und S6 möglich. Damit ergibt sich durch die Spezifikation Attributgruppe[] und Aspekt[S1] die Auswahl A1/S1, A2/S1 und A3/S1.
  - **Datenbefugnisse**
    Über die folgenden Vorgaben wird bestimmt, welche Aktionen ein Benutzer mit den resultierenden Attributgruppen/Aspekt-Kombinationen durchführen kann:
    - **Empfänger**
      Gibt an, ob die Daten mit diesen Rechten empfangen (gelesen) werden dürfen.
    - **Sender**
      Gibt an, ob die Daten mit diesen Rechten gesendet (geschrieben) werden dürfen.
    - **Quelle**
      Gibt an, ob die Daten mit diesen Rechten als Quelle angemeldet werden dürfen.
    - **Senke**
      Gibt an, ob die Daten mit diesen Rechten als Senke angemeldet werden dürfen.

    Bei den oben genannten Attributen sind als Werte jeweils "ja", "nein" und "keine Aussage" möglich.
    Durch den Aufbau der Attributgruppe und dadurch, dass bei einer Berechtigungsklasse mehrere Rollen/Regionen-Paare vorgegeben werden können, ist eine Überlagerung widersprüchlicher Vorgaben möglich, die durch eine Prioritätenvorgabe geregelt werden muss.

    Die Prioritätenreihung ist, wie folgt:

    - Wenn zu einer Attributgruppen/Aspekt-Kombination nach Auswertung der Parameter keine Aussage zu den Rechten vorliegt (d.h. diese Kombination wurde nicht parametriert) bedeutet dies keine Rechte (implizites Nein):
      "**Empfänger**": "nein"; "**Sender**": "nein"; "**Quelle**": nein; "**Senke**": nein

  - Bei der Überlagerung gilt folgende aufsteigende Priorität:
    implizites Nein
    keine Aussage
    Ja
    Nein
    Ein Explizites Nein hat die höchste Priorität und kann nicht mehr aufgehoben werden.

- **AktivitätObjekte[0..]**
  Hier wird spezifiziert, welche Objekte neu angelegt, geändert oder gelöscht werden dürfen[4].
  - **Objekttyp[0..]**
    Objekttypen, die hier betrachtet werden sollen. Wenn das Array leer ist, sind alle Objekttypen gemeint[5].
  - **Konfigurationsbereich[0..]**
    Konfigurationsbereiche, in denen Objekte neu erzeugt, geändert oder gelöscht werden dürfen. Wenn das Array leer ist, dürfen in allen möglichen Konfigurationsbereichen (grundsätzlich dürfen nur KB geändert werden, für die die entsprechende Konfiguration auch der Konfigurationsverantworliche ist) Objekt erzeugt werden.
  - **ObjekteErzeugenÄndernLöschen**
    Gibt an, ob zu den spezifizierten Objekttypen, Objekte erzeugt, geändert oder gelöscht werden dürfen.
    Bei diesem Attribut kann "Ja" oder "Nein" als Wert angegeben werden. Bei widersprüchlichen Angaben hat "Nein" die höhere Priorität.
- **AktivitätMengen[0..]**
  Hier wird spezifiziert, welche Menge geändert werden dürfen.
  - **Mengentyp[0..]**
    Mengen, die hier betrachtet werden sollen. Wenn das Array leer ist, sind alle Mengentypen gemeint.
  - **Konfigurationsbereich[0..]**
    Konfigurationsbereiche, in denen Mengen der angegebenen Mengentypen geändert werden dürfen. Wenn das Array leer ist, dürfen in allen möglichen Konfigurationsbereichen (grundsätzlich dürfen nur KB geändert werden, für die die entsprechende Konfiguration auch der Konfigurationsverantworliche ist) Mengen der angegebenen Mengentypen geändert werden.
  - **MengeÄndern[0..]**
    Gibt an, ob zu den spezifizierten Mengentypen Mengen geändert werden dürfen.
    Bei diesem Attribut kann "Ja" oder "Nein" als Wert angegeben werden. Bei widersprüchlichen Angaben hat "Nein" die höhere Priorität.
- **Rolle[0..]**
  Über die optionale Angabe von ein oder mehreren Rolle können Rollen andere Rollen enthalten. Damit ist es möglich, die Rollen hierarchisch zu gestalten.

---

[4] Diese Zugriffsrechteprüfung wird seit der Version 3.13 der Kernsoftware bei aktivierter neuer Rechteprüfung durchgeführt. Sie ist ab Version 3.13 fest im Datenverteiler integriert (war vorher teilweise als Prototyp durch ein Rechteprüfungs-PlugIn implementiert).

[5] In Version 3.13 müssen hier noch `typ.dynamischesObjekt` und ggf. `typ.konfigurationsObjekt` angegeben werden, um alle Objekte auszuwählen. In folgenden Versionen der Kernsoftware bewirkt ein leeres Array die Wildcard-Auswahl aller Typen.

Bei der Überlagerung von mehreren Rollen werden die Rechte positiv vereinigt. Das bedeutet, wenn eine Rolle eine Aktivität erlaubt und eine andere Rolle diese Aktivität verbietet, ergibt sich als Resultat, dass die entsprechende Aktivität erlaubt ist. Diese Vorgehensweise ergibt sich aus der Anforderung, Rollen hierarchisch aufeinander aufzubauen. Die Rollen A, B, und C beschreiben verschiedene Aktivitäten, wobei die Rolle C mehr Befugnisse ermöglicht als die Rolle B und diese wiederum mehr Befugnisse ermöglicht als die Rolle A. Wenn eine Rolle D die drei Rollen vereinigen soll, dürfen eventuell spezifizierte Verbote der Rolle A nicht Befugnisse der Rolle B oder C überschreiben.

3.3.4 Region

Durch die Region wird spezifiziert, für welche Objekte die Aktivitäten der entsprechenden Rolle aus dem Rolle/Regionen-Paar durchgeführt werden können (z.B. für bestimmte Querschnitte).

Der Parameter enthält zwei Attributlisten, über die spezifiziert werden kann, welche Objekte zu der Region gehören und welche gegebenenfalls ausgeschlossen sind. Die Listen sind gleich aufgebaut und durch weitere Attributlisten strukturiert:

Region								
EnthalteneObjekte[0..]								
Bereich[0..]				**Region[0..]**			**Objekte[0..]**	
KV[0..]	KB[0..]	Typ[0..]	Menge	Region[0..]	Typ[0..]	Menge	Objekt[0..]	Menge
AusgeschlosseneObjekte[0..]								
Bereich[0..]				**Region[0..]**			**Objekte[0..]**	
KV[0..]	KB[0..]	Typ[0..]	Menge	Region[0..]	Typ[0..]	Menge	Objekt[..]	Menge

Abbildung 3-4: Attributgruppe Region

- **EnthalteneObjekte[0..]**
  Über diese Vorgaben werden die in der Region enthaltenen Objekte spezifiziert. Die Vorgabe kann über Bereiche, Regionen und einzelne Objekte parametriert werden.
  - **Bereich[0..]**
    Auswahl von Objekten über Bereiche.
    Attributliste als Array der Größe 0 bis unbegrenzt. Wenn dieses Array leer ist, erfolgt (hierüber) keine Auswahl von Konfigurationsobjekten.
    - **Konfigurationsverantwortlicher[0..]**
      Über dieses Array können Konfigurationsverantwortliche angegeben werden. Die Auswahl eines Konfigurationsverantwortlichen bedeutet, dass alle Konfigurationsbereiche dieses Konfigurationsverantwortlichen betrachtet werden. Wenn das Array Konfigurationsverantwortliche leer ist, ist kein Konfigurationsverantwortlicher und damit kein Konfigurationsbereich ausgewählt.
    - **Typ[0..]**
      Über dieses Array werden die bisher ausgewählten Objekte auf die angegebenen Typobjekte beschränkt. Wenn die beiden Arrays Konfigurationsverantwortliche und Konfigurationsbereich beide zu keiner (Vor)Auswahl von Konfigurationsbereichen geführt haben, wird an dieser Stelle die gesamte Konfiguration betrachtet. D.h., wenn hier z.B. als Typ MessQuerschnitt angegeben wird, werden nur noch Konfigurationsobjekte betrachtet, die von diesem Typ stammen. Wenn das Array Typen leer ist, erfolgt keine Filterung nach Objekttypen. Damit sind alle bisher ausgewählten Konfigurationsobjekte ausgewählt (Also entweder alle Konfigurationsobjekte der (vor)ausgewählten Bereiche oder alle Konfigurationsobjekte der Konfiguration).

- **Mengenbezeichnung**
  Über die Vorgabe eines Mengennamens können die Objekte ausgewählt werden, die in Mengen dieses Namens bei den ausgewählten Objekten enthalten sind. Ist hier z.B. als Menge "FahrStreifen" angegeben, wird für alle bisher ausgewählten Objekte geprüft, ob an dem Konfigurationsobjekt eine Menge dieses Namens vorhanden ist und für diesen Fall werden die enthaltenen Konfigurationsobjekte betrachtet. Wenn hier keine Angabe erfolgt, bleibt die Auswahl bestehen.

- **Region[0..]**
  Auswahl von Objekten über Regionen.
  Attributliste als Array der Größe 0 bis unbegrenzt. Wenn dieses Array leer ist, erfolgt (hierüber) keine Auswahl von Konfigurationsobjekten.

  - **Region[0..]**
    Über dieses Array können bereits definierte Regionen angegeben werden. Die Auswahl einer Region bedeutet, dass alle Konfigurationsobjekte dieser Region betrachtet werden. Wenn das Array Region leer ist, sind alle Konfigurationsobjekte ausgewählt.

  - **Typ[0..]**
    Über dieses Array werden die bisher ausgewählten Objekte auf die angegebenen Typobjekte beschränkt. D.h., wenn hier z.B. als Typ MessQuerschnitt angegeben wird, werden nur noch Konfigurationsobjekte betrachtet, die von diesem Typ stammen. Wenn hier keine Angabe erfolgt, bleibt die Auswahl bestehen.

  - **Mengenbezeichnung**
    Über die Vorgabe eines Mengennamens können die Objekte ausgewählt werden, die in Mengen dieses Namens bei den ausgewählten Objekten enthalten sind. Ist hier z.B. als Menge "FahrStreifen" angegeben, wird für alle bisher ausgewählten Objekte geprüft, ob an dem Konfigurationsobjekt eine Menge dieses Namens vorhanden ist und für diesen Fall werden die enthaltenen Konfigurationsobjekte betrachtet. Wenn hier keine Angabe erfolgt, bleibt die Auswahl bestehen.

- **Objekte[0..]**
  Auswahl von Objekten über die explizite Angabe von einzelnen Objekten.
  Attributliste als Array der Größe 0 bis unbegrenzt. Wenn dieses Array leer ist, erfolgt (hierüber) keine Auswahl von Konfigurationsobjekten.

  - **Objekt[0..]**
    Über dieses Array können beliebige Konfigurationsobjekte angegeben werden. Bei einem leeren Array sind alle Konfigurationsobjekte ausgewählt.

  - **Mengenbezeichnung**
    Über die Vorgabe eines Mengennamens können die Objekte ausgewählt werden, die in Mengen dieses Namens bei den ausgewählten Objekten enthalten sind. Ist hier z.B. als Menge "FahrStreifen" angegeben, wird für alle bisher ausgewählten Objekte geprüft, ob an dem Konfigurationsobjekt eine Menge dieses Namens vorhanden ist und für diesen Fall werden die enthaltenen Konfigurationsobjekte betrachtet. Wenn hier keine Angabe erfolgt, bleibt die Auswahl bestehen.

- **AusgeschlosseneObjekte[0..]**
  Über diese Vorgaben werden die in der Region explizit ausgeschlossenenObjekte spezifiziert.
  Der Aufbau ist analog zur Attributliste **EnthalteneObjekte[0..]**.

Über die beiden Attributlisten EnthalteneObjekte und AusgeschlosseneObjekte kann detailliert definiert werden, welche Konfigurationsobjekte zu einer Region gehören. Hierbei gilt folgende Prioritätenfolge:

- Keine Aussage zu einem Konfigurationsobjekt bedeutet, dass es nicht zu der Region gehört.
- Konfigurationsobjekte, die in der Attributliste EnthalteneObjekte aufgeführt sind, gehören zu dieser Region.
- Ein Eintrag in der Attributliste AusgeschlosseneObjekte hat die höchste Priorität. Hiermit können bereits eingetragene Konfigurationsobjekte wieder eliminiert werden.

3.4 Plug-In Schnittstelle

Bei der Erweiterung der Zugriffsrechteprüfung wird zusätzlich eine Plug-In-Schnittstelle implementiert, über die die Zugriffsrechte von bestimmten Attributgruppen/Aspekt-Kombinationen inhaltlich geprüft werden können. Über diese Schnittstelle wurde z.B. ein Plug-In eingebunden (seit Kernsoftware 3.13 fest im Datenverteiler integriert), das dafür sorgt, dass ein Benutzer nur Archivanfragen zu Daten stellen darf, die er auch online erhalten kann.

3.4.1 Beschreibung der Plug-In-Schnittstelle zur Rechteprüfung

Die Plug-In-Schnittstelle zur Rechteprüfung dient dazu, Rechteprüfungen für externe Applikationen zu ermöglichen, wie zum Beispiel für die Konfiguration bei Konfigurations-Änderungs-Anfragen oder für das Archivsystem bei Archivanfragen.

Dazu teilen die Plug-Ins dem Datenverteiler über das Plug-In-Interface die Attributgruppenverwendungen mit, für die das Plug-In eine Rechteprüfung vornehmen soll. Dies kann beispielsweise die `atg.konfigurationsAnfrageSchnittstelleSchreibend` mit dem Aspekt `asp.anfrage` sein, wenn Konfigurationsänderungen geprüft werden sollen.

Wenn der Datenverteiler ein Datenpaket mit einer gefilterten Attributgruppenverwendung empfängt, wird dieser, bevor er dieses an andere Datenverteiler oder Applikationen weiterleitet, dem Plug-In übergeben. Das Plug-In hat daraufhin die Möglichkeit, das Datenpaket unverändert weiterschicken zu lassen, stattdessen ein modifiziertes Datenpaket zu verschicken, oder das Datenpaket ganz zu verwerfen.

3.4.2 Aufbau des Plug-In-Interface

Zugriffsrechte-Plug-Ins müssen das Interface `AccessControlPlugin` implementieren. Dieses bietet drei grundlegende Funktionen:

- `void initialize(accessControlManager, clientDavInterface)`

  Wird aufgerufen, nachdem das Plug-In instantiiert wurde. Hiermit wird dem Plug-In eine Verbindung zum Datenverteiler und zur Rechteverwaltungsklasse übergeben.

- `Collection<AttributeGroupUsage> getAttributeGroupUsagesToFilter()`

  Fragt das Plug-In nach den Attributgruppenverwendungen, die überprüft werden sollen.

- `Data handleData(userID, baseSubscriptionInfo, data)`

  Übergibt dem Plug-In ein Datenobjekt mit den zugehörigen Kontext-Informationen, damit dieses entscheiden kann, ob es weiter versendet, modifiziert und weiter versendet oder nicht weiter versendet werden soll.

Ausführlichere Beschreibungen sind im Javadoc zu den entsprechenden Funktionen gegeben.

3.4.3 Benutzung von Plug-ins

Plug-Ins werden nur bei aktivierter Rechteprüfung im Datenverteiler benutzt. Die zu verwendenden Plug-Ins müssen über einen Kommandozeilenparameter beim Start des Datenverteilers angegeben werden.

Beispiel:

```
$java \
 de.bsvrz.dav.dav.main.Transmitter \
 -rechtePruefung=ja \
 -zugriffsRechtePlugins=de.bsvrz.dav.dav.util.accessControl.XXX \
...
```

Mehrere Plug-Ins können durch Kommas getrennt werden.

3.4.4 Weitere Informationen

Falls ein Datenpaket durch mehrere Datenverteiler geschickt wird und alle Rechteprüfungs-Plug-Ins verwenden, wird das Datenpaket von allen Datenverteilern geprüft. Dabei erhält das Plug-In zur Rechteprüfung als Benutzer unter Umständen nicht den Benutzer, der die Anfrage gestartet hat sondern den Benutzer unter dem der vorherige Datenverteiler gestartet wurde. Falls die Datenverteiler mit unterschiedlichen Konfigurationen laufen, ist daher normalerweise nur sicherzustellen, dass der Benutzer des vorangehenden Datenverteilers bekannt ist und Rechte für diese Aktion zugewiesen bekommen hat.

Haben sich mehrere Plug-Ins auf eine Attributgruppenverwendung angemeldet, bekommen diese das Datenpaket nacheinander in nicht festgelegter Reihenfolge. Modifiziert ein Plug-In das Datenpaket erhalten nachfolgende Plug-Ins das modifizierte Datenpaket. Wird ein Datenpaket verworfen, wird es nicht an weitere Plug-Ins übergeben.

3.4.5 Verhalten des Plug-Ins falls eine Aktion nicht erlaubt werden soll

Falls eine Aktion nicht erlaubt werden soll, hat das Plug-In im Allgemeinen drei Möglichkeiten, das Durchführen der Aktion zu verhindern.

- Das Datenpaket entsprechend verändern, dass es keinen Schaden anrichtet, beispielsweise bei einer Konfigurationsanfrage den Anfragetyp so ändern, dass nur eine Fehlerantwort von der Konfiguration zurückgeschickt wird
- Ist das nicht möglich oder nicht erwünscht, kann das Plug-In auch den Weiterversand des Datenpakets an z.B. die Konfiguration verhindern und stattdessen selbst an die versendende Anwendung eine Antwort schicken. Dazu muss sich das Plug-In für Antworten auf diese Datenidentifikation anmelden und manuell eine entsprechende Antwort verschicken.
- Die einfachste Möglichkeit ist, das Datenpaket zu verwerfen, ohne das Versenden irgendeiner Antwort zu bewirken. Da dabei in vielen Fällen Timeouts entstehen, die die Applikationen blockieren könnten und weil dabei keine sinnvolle Fehlermeldung entsteht ist diese Möglichkeit im Allgemeinen aber weniger sinnvoll.