

KCEFM » KOMPETENZCENTER  
ELEKTRONISCHES  
FAHRGELDMANAGEMENT NRW



# **VDV-Kernapplikation Kontrollservice (KOSE)**

**Ergebnis der Diskussion  
in der  
VDV-AG „Weitere Standardisierung der KA“**

November 2007

## 0 Inhaltsverzeichnis

Kapitel	Seite
0 Inhaltsverzeichnis.....	2
1 Vorbemerkung.....	3
2 Einleitung .....	4
3 Modelle zur Führung der Sperrlisten .....	4
3.1 Regionaler Ansatz.....	4
3.2 Organisationsspezifischer Ansatz .....	5
3.3 Produktorientierter Ansatz .....	5
3.4 Mandantenfähiger Ansatz .....	6
4 Organisation, Verträge, Haftung .....	6
5 Fazit .....	7
6 Anlagen .....	9

## 1 Vorbemerkung

Seit 2003 setzen Verkehrsunternehmen in Nordrhein-Westfalen eTickets ein. Die mehr als 1,5 Millionen Abonnement-Kunden in den Verkehrsverbänden Rhein-Sieg (VRS) und Rhein-Ruhr (VRR) sowie in der Verkehrsgemeinschaft Niederrhein (VGN) erhalten ihre Fahrscheine auf Chipkarten. Zur Verwaltung der Sperrlisten betreibt jeder Verbundraum ein eigenes sogenanntes Verbundsystem, das die Sperraufträge der Unternehmen einsammelt und als gesamte Sperrliste rückverteilt. Für Sperraufträge, die über Verbundgrenzen hinweg gereicht werden müssen, ist ein darüber liegendes Landessystem errichtet worden. Mit Zunahme der Sperrungen, die mehr als einen Verbundraum betreffen, hat diese Systemarchitektur ihre Schwächen offenbart.

Inzwischen haben die Verkehrsunternehmen ihr eTicket-System verändert. Seit Beginn 2007 werden Chipkarten nach dem Standard der VDV-Kernapplikation eingesetzt. Da sich aber parallel noch für einige Zeit Karten alten Typs in Umlauf befinden werden, konnte die Frage, das Sperrlisten-Management hin zum KOSE der Kernapplikation zu migrieren, nicht gestellt werden. Allerdings wird es nur eine Frage der Zeit sein, bis man auch in Nordrhein-Westfalen konkret über den KOSE nachdenken muss. Neu hinzukommende eTicket-Projekte werden sich wahrscheinlich nicht den Altsystemen von VRS, VRR und VGN anschließen wollen. Und auch die Betreiber der Altsysteme werden sich vielleicht einmal für die Vorteile des KOSE interessieren.

Um nicht unvorbereitet zu sein, wenn in Nordrhein-Westfalen der Wunsch bzw. die konkrete Forderung nach einem KOSE laut wird, hat sich das KCEFM aus technischer, organisatorischer, vertraglicher und haftungsrechtlicher Sicht erste Gedanken zum KOSE gemacht und diese in die in der VDV-AG „Weitere Standardisierung der KA“ geführte Diskussion eingebracht.

Entsprechend ist dieses Dokument als Zusammenfassung des aktuellen Diskussionsstandes sowie als Orientierungshilfe für die weitere fachliche Beratung zu verstehen.

## 2 Einleitung

Mit KOSE ist der **K**ONTROLL**S**ERVICE der VDV-Kernapplikation gemeint, wobei es sich letztendlich um das Sperrlisten-Management handelt.

Es gibt in der VDV-Kernapplikation zwei Arten von Sperrlisten:

- Organisationen und Objekte des Sicherheitssystems befinden sich auf der so genannten nicht Nutzermedium bezogenen Sperrliste. Diese Sperrliste wird von der VDV-Kernapplikations GmbH & Co KG gefüllt. Es ist nicht zu erwarten, dass diese Liste sehr groß wird. Diese Sperrliste ist nicht Gegenstand des vorliegenden Dokumentes.
- Zu sperrende Objekte wie elektronische Tickets, die auf dem in der Hand des Kunden befindlichen Nutzermedium (z. B. Chipkarte) vorhanden sind, befinden sich auf der so genannten Nutzermedium bezogenen Sperrliste. Diese Liste wird von den Verkehrsunternehmen gefüllt. Erfahrungen in anderen ((eTicket-Anwendungen (z. B. VRS, VRR) lassen darauf schließen, dass diese Liste, wenn es eine bundesweit einheitliche ist, sehr groß wird.

Im Rahmen des vom Bundesministerium für Bildung und Forschung geförderten Forschungsprojektes wurde diese Problematik bei der Nutzermedium bezogenen Sperrliste auch erkannt aber letztendlich nicht gelöst. Im „Technischen Konzept Sicherheit“ der VDV-Kernapplikation wird als Modell zur Führung von Nutzermedium bezogenen Sperrlisten eine Lösung mit mehreren regionalen Sperrlisten und damit mehreren KOSE diskutiert.

## 3 Modelle zur Führung der Sperrlisten

Ausgehend von dem regionalen Ansatz bei der Gestaltung des KOSE wurden mehrere Ansätze diskutiert. Die Ergebnisse dieser Diskussionen sind im folgenden näher beschrieben.

### 3.1 Regionaler Ansatz

Als erstes wurde der regionale Ansatz aus dem „Technischen Konzept Sicherheit“ diskutiert. Hier zeigten sich massive Schwächen, die im Detail auch der Grafik auf Seite 10 entnommen werden können.

- Aus der räumlichen Gültigkeit, die von den verschiedensten Faktoren und nicht nur von einer Preisstufe bestimmt wird, leitet sich ab, an welche regionalen KOSE ein Sperrauftrag zu schicken ist. Es wurde als unmöglich angesehen, diese komplexen Regeln den Verkehrsunternehmen zu vermitteln. Auch wenn dies gelingen würde, wäre der Aufwand für die Pflege dieser Daten nicht zu rechtfertigen.<sup>1</sup>
- Verkehrsunternehmen die in mehreren Regionen tätig sind, müssen sich mehrere Sperrlisten abholen. Dabei kommt es dann auch zu unnötigen doppelten Sperraufträgen.

---

<sup>1</sup> Dies ist bereits bei dem existierenden Sperrlisten-Management für das eTicket in den Verbänden VGN, VRS und VRR gescheitert, bei dem es sich letztendlich um eine regionale Lösung handelt.

- Letztendlich stellt sich auch die Frage, wer sich für welchen KOSE in welcher Region verantwortlich fühlt. Der Aufwand für die fachliche und technische Betreuung eines KOSE-Systems ist nicht zu unterschätzen.
- Ein weiteres Indiz dafür, dass der regionale Ansatz falsch ist, bildet schon die Spezifikation der VDV-Kernapplikation: Der Begriff „Region“ oder eine ähnliche Formulierung wird dort nicht verwendet.

Aufgrund dieser massiven Schwächen und der Tatsache, dass überhaupt kein Vorteil ersichtlich war, wurde dieser Ansatz verworfen.

### 3.2 Organisationsspezifischer Ansatz

Um dem Problem der mehreren abzuholenden Sperrlisten zu begegnen, wurde ein Ansatz diskutiert, bei dem jede Organisation (Verkehrsunternehmen) nur eine Sperrliste abholen muss. Dieser Ansatz entspricht auch einer Prämisse der VDV-Kernapplikation. Aber auch hier zeigten sich elementare Schwächen, die im Detail der Grafik auf Seite 11 entnommen werden können.

- Wenn ein Verkehrsunternehmen nur eine Sperrliste abholen muss, bedingt das, dass es genau einem KOSE zugeordnet ist. Die Verkehrsunternehmen müssen also wissen, welche anderen Verkehrsunternehmen ihre elektronischen Tickets akzeptieren und an welchen KOSE sie angeschlossen sind. Auch hier müssen komplexe Regeln gepflegt und den Verkehrsunternehmen vermittelt werden.
- Das eigentliche Problem liegt aber in der Frage, wer sich dafür verantwortlich fühlt, zu klären, welche Verkehrsunternehmen an welchen KOSE anzuschließen sind. Hier fehlt jegliche Motivation, die jemanden dazu bewegen könnte, sich dieser Aufgabe anzunehmen.

Da auch dieser Ansatz nicht überzeugen konnte, wurde er ebenfalls verworfen.

### 3.3 Produktorientierter Ansatz

Da in der VDV-Kernapplikation die Produkte, die die Grundlage für die elektronischen Tickets bilden, das Bindeglied zwischen allen Beteiligten darstellen, wurde auch ein produktorientierter Ansatz diskutiert. Die Grafik auf Seite 12 gibt die entsprechenden Strukturen detaillierter wieder.

- Jeder Organisation, die Produkte definiert (im Allgemeinen die Verbände), ist ein KOSE zugeordnet. Die Verkehrsunternehmen müssen Sperraufträge für Produkte des Verbundes 1 an den KOSE 1 schicken usw. Diese Regel wurde als den Verkehrsunternehmen vermittelbar angesehen.
- Zwar müssen die Verkehrsunternehmen mehrere Sperrlisten abholen, aber es steht eindeutig fest, wo dies zu geschehen hat.
- Ebenso steht auch fest, wer sich um den KOSE kümmern muss. Dies sind die Verbände.

Insgesamt wurde dieser Ansatz als der richtige Weg angesehen.<sup>2</sup>

---

<sup>2</sup> Die Verkehrsunternehmen in den Verbänden VGN, VRS und VRR migrieren zur Zeit zu diesem Ansatz.

### 3.4 Mandantenfähiger Ansatz

Bei diesem Ansatz wurde der produktorientierte Ansatz aus 3.3 insofern weiterentwickelt, als dass die KOSE der verschiedenen Verbände in einem mandantenfähigen bundesweiten KOSE zusammengeführt wurden. Details können der Grafik auf Seite 13 entnommen werden.

- Jedes Verkehrsunternehmen muss den Sperrauftrag, der über eine Produktkennung verfügt, nur an einen KOSE schicken und auch nur eine für sie maßgeschneiderte Sperrliste abholen.
- Erreicht wird dies durch die Konfiguration des bundesweiten KOSE durch die Verbände. Sie teilen dem KOSE mit, welche Verkehrsunternehmen ihre Produkte verkaufen bzw. akzeptieren. Aus diesen Konfigurationsdaten erzeugt der KOSE für jedes Verkehrsunternehmen eine maßgeschneiderte Sperrliste.

Dieser Ansatz wurde von den Mitgliedern der Arbeitsgruppe insbesondere unter dem Gesichtspunkt der bundesweiten Interoperabilität der VDV-Kernapplikation als umsetzbar angesehen.

## 4 Organisation, Verträge, Haftung

Aus technischer Sicht ist es unerheblich, wer diesen bundesweiten mandantenfähigen KOSE betreibt, solange er spezifikationskonform und für jedermann zugänglich ist.

Aus organisatorischen, vertrags- und haftungsrechtlichen Gründen ist es jedoch zwingend erforderlich, dass die VDV-Kernapplikations GmbH & Co KG als Applikationsherausgeberin und Verantwortliche für das Sicherheitssystem auf die Verantwortung für den KOSE übernimmt. Dies beinhaltet auch, dass die VDV-Kernapplikations GmbH & Co KG als Auftraggeberin die Kontrolle über den Auftragnehmer, der den KOSE de facto betreibt (z. B. ein IT-Dienstleister), ausübt:

- Die VDV-Kernapplikations GmbH & Co KG übt die zentrale Rolle im Gesamtsystem der Kernapplikation aus. Sie ist die neutrale Instanz, die die Applikation herausgibt (Applikationsherausgeber) und das Sicherheitssystem zur Verfügung stellt.
- Nur wer bei der VDV-Kernapplikations GmbH & Co KG akkreditiert ist, darf das Sicherheitsmanagement/-system der Kernapplikation nutzen. Konkret: Akkreditierte Organisationen (z. B. Verkehrsunternehmen) werden von der VDV-Kernapplikations GmbH & Co KG auf eine White List gesetzt. Nur wer auf dieser White List steht, wird vom Betreiber des Trust Centres (T-Systems) beliefert. Gleichzeitig besteht ein inhaltlicher Zwang, das Sicherheitsmanagement/-system zu nutzen. Hier nicht angeschlossene Organisationen können allein aus technischen Gründen keine interoperablen ((eTickets ausgeben und/oder akzeptieren.
- Damit eine bundesweite Interoperabilität von ((eTickets überhaupt funktioniert, muss der KOSE gleichermaßen von allen Organisationen genutzt werden wie das Sicherheitsmanagement/-system. Sollte dies nicht der Fall sein, so könnten Organisationsgrenzen überschreitenden Fahrberechtigungen nicht durchgängig gesperrt werden. Interoperable ((eTickets wären damit grundsätzlich missbräuchlich verwendbar. Diese Interoperabilität beginnt bereits an der Verbundgrenze. Beispiel: Auf der vielbefahrenen Strecke zwischen

Köln (VRS) und Düsseldorf (VRR) besteht bereits die Notwendigkeit, grenzüberschreitend ((e)Tickets zu sperren.

- Der KOSE muss genauso diskriminierungsfrei zur Verfügung gestellt werden wie das Sicherheitsmanagement/-system. Ansonsten ist der Anschluss aller Verkehrsunternehmen / Verkehrsverbünde, die ((e)Tickets ausgeben oder akzeptieren, nicht zu erwarten.
- Um den Anschluss an den bundesweiten mandantenfähigen KOSE bei allen EFM-Teilnehmern sicherzustellen, muss dies im Akkreditierungsvertrag geregelt sein. Hier ist eine Verpflichtung einzubauen, am KOSE teilzunehmen. In einem Vertragsverhältnis, das in der Struktur dem zum Sicherheitsmanagement/-system ähnelt, sind die Haftungsrisiken und Haftungspflichten zwischen VDV-Kernapplikations GmbH & Co KG, ((e)Ticket-Anwender und dem KOSE-Betreiber klar zu regeln. In der Folge müssen die die VDV-Kernapplikation anwendenden Verkehrsunternehmen ergänzend zu den drei Verträgen zum Sicherheitsmanagement/-system einen vierten Vertrag zum KOSE abschließen.
- Der eigentliche Betrieb des KOSE kann nicht bei der VDV-Kernapplikations GmbH & Co KG liegen. Dazu wäre sie weder technisch, noch personell, noch finanziell (Haftung!) in der Lage.
- Es ist unabdingbar, dass die VDV-Kernapplikations GmbH & Co KG vertraglich Auftraggeber gegenüber dem Entwickler und Betreiber des KOSE ist. Nur so kann sichergestellt werden, dass sowohl bei Erstentwicklung, Aufbau und Inbetriebnahme also auch bei späteren Erweiterungen und/oder Weiterentwicklungen das Gesamtsystem für Deutschland im Blick steht, keine Partikularinteressen dominieren bzw. ein fairer Interessenausgleich möglich ist.

## 5 Fazit

Die Empfehlung des KCEFM lautet daher, dass die VDV-Kernapplikations GmbH & Co. KG als Applikationsherausgeber entsprechend dem „Technischen Konzept Sicherheit“ der VDV-Kernapplikation die Sperrlistenausgabe für die Nutzermedium bezogene Sperrliste in Form eines bundesweiten mandantenfähigen KOSE organisiert. Diese Empfehlung entspricht auch dem europäischen Modell gemäß EN 24014-1.

Aus Sicht des KCEFM ist der unter 3.4 beschriebene bundesweite KOSE die einzige Lösung, die grundsätzlich sicherstellt, dass auch bundesweit interoperable Produkte problemlos gesperrt werden können. Gegen die Realisierung mehrerer KOSE sprechen folgende Gründe:

- Die KOSE-Funktionalität müsste nicht nur mehrfach realisiert, sondern auch mehrfach finanziert werden.
- Die Umsetzung der KOSE-Funktionalität stellt eine technische, organisatorische und vertragliche Herausforderung dar, die besondere Fähigkeiten in diesen Bereichen erfordert und nicht von jedem bewältigt werden kann. Ein korrekt funktionierender KOSE ist für die Verkehrsunternehmen unabdingbar, um vor finanziellen Verlusten geschützt zu sein.
- Es besteht die Gefahr von proprietären Lösungen.

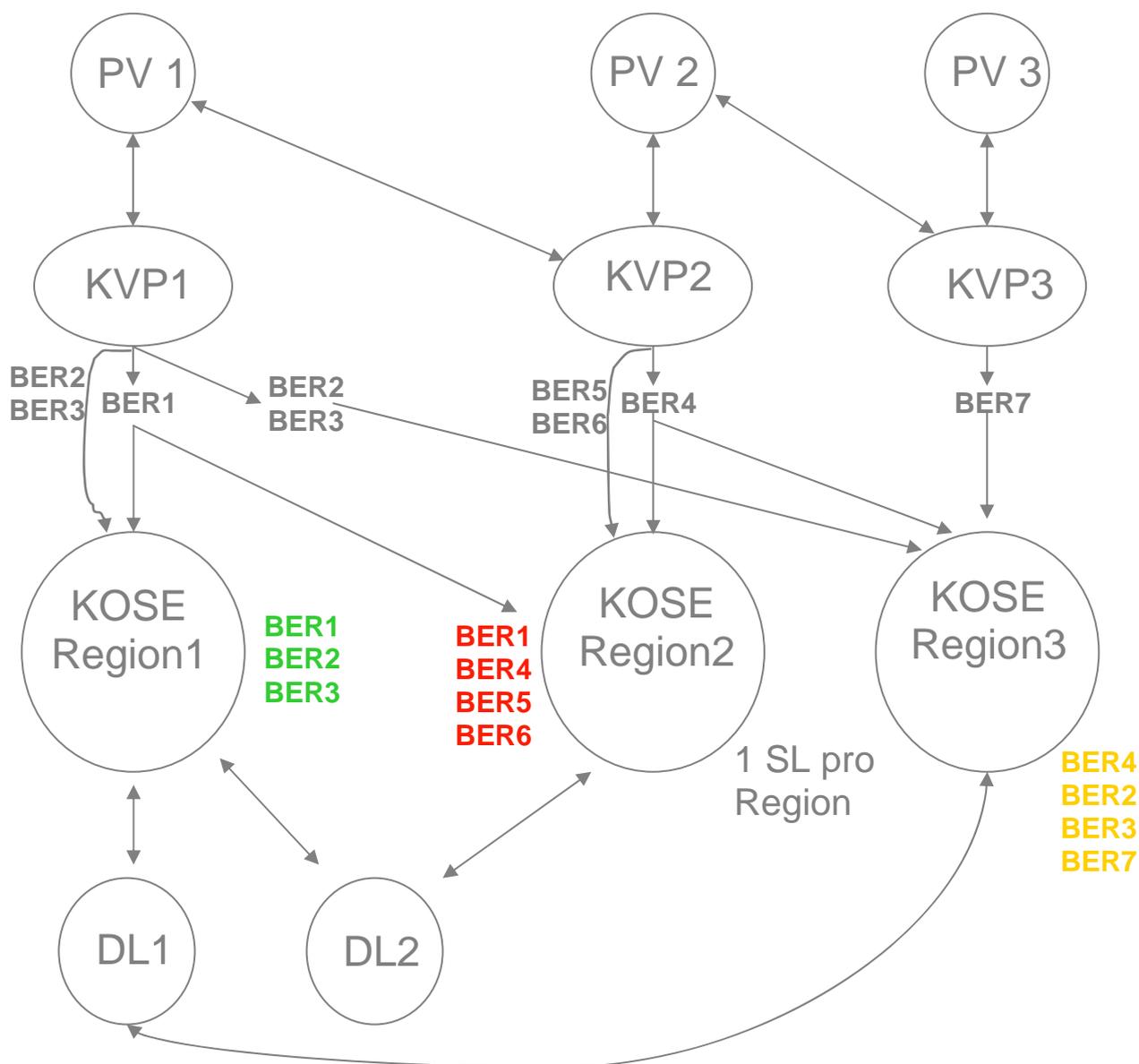
- Die Sperrung von bundesweit interoperablen Produkten wird bei mehreren KOSE unter Berücksichtigung der Haftungsfragen als sehr schwierig angesehen. Das bei der VDV-Kernapplikation bewährte Prinzip der bilateralen Verträge zwischen einem Verkehrsunternehmen und der VDV-Kernapplikations GmbH & Co. KG bzw. dem Dienstleister für das Sicherheitsmanagement könnte nicht mehr eingehalten werden. Stattdessen müssten Verträge mit mehreren KOSE abgeschlossen werden, die wiederum untereinander Verträge schließen müssten. Dies wird wegen der schwierigen bis unmöglichen Vertragsgestaltung nach Auffassung des KCEFM dazu führen, dass bundesweit interoperable Produkte nicht realisierbar sind.

## 6 Anlagen

### Grafische Darstellungen verschiedener Ansätze

Anlage 1 – regionaler Ansatz	Seite 10
Anlage 2 – organisationsspezifischer Ansatz	Seite 11
Anlage 3 – produktorientierter Ansatz	Seite 12
Anlage 4 – mandantenfähiger Ansatz	Seite 13

## – Anlage 1 – regionaler Ansatz



Es gibt nach geografischen Regionen gegliederte KOSEs.

Alle KVPs müssen wissen, in welchen Regionen ihre gesperrten Objekte räumlich gültig sind, und die Sperraufträge entsprechend verteilen.

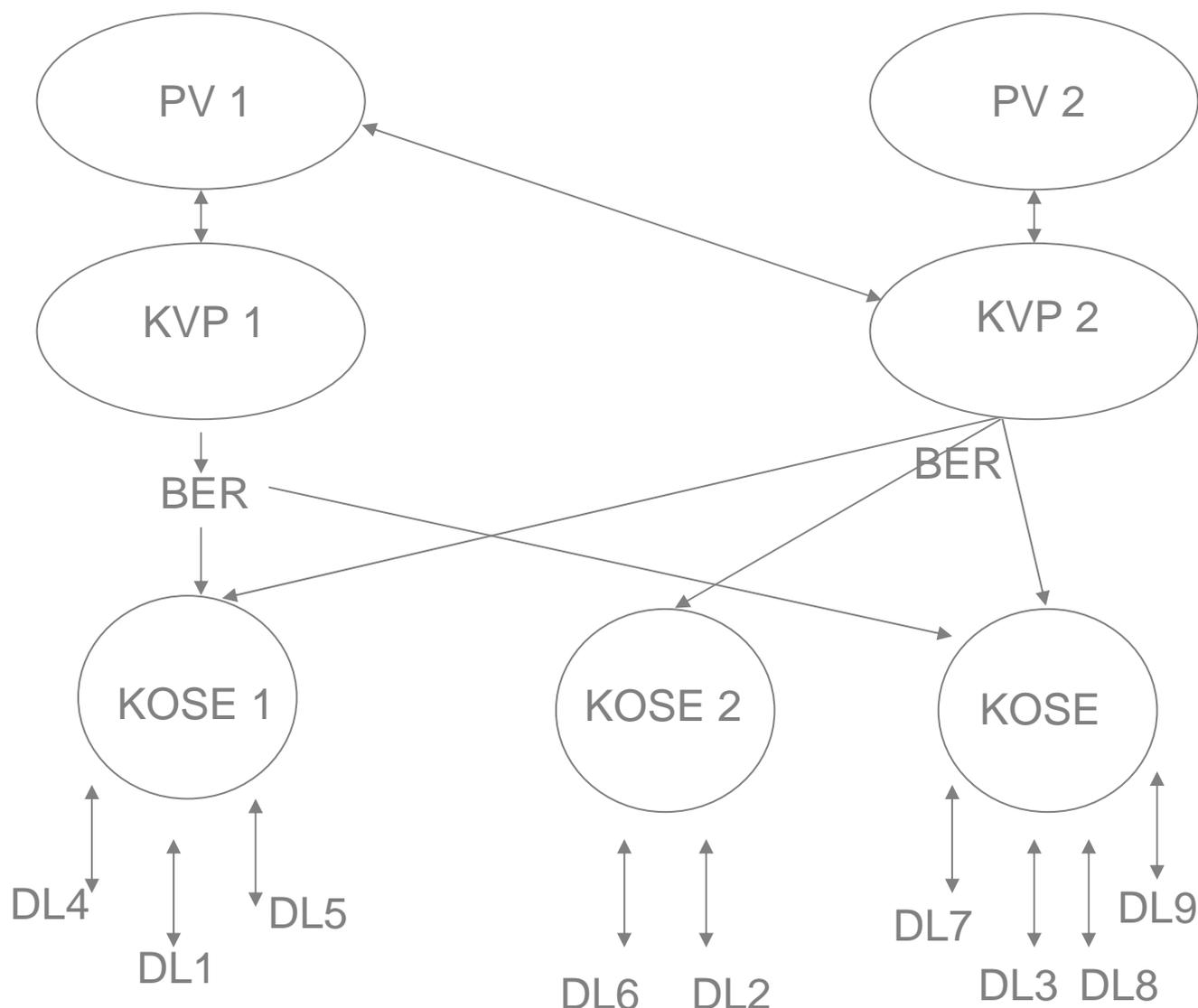
Die KOSEs führen die eingehenden Sperraufträge zu einer SLNM. Dies geschieht KVP/DL/PV-unabhängig.

Problem: Insbesondere DLs bewegen sich durch mehrere Regionen. Welche SLNM brauchen sie?

DL1 muss z.B. SLNM von Region 1 und 3 holen, zusammenführen und ggf. filtern, da BER2/3 in beiden SL vorhanden sind – Sperrlistengröße (Integrität??)

### Kümmererproblem beim KOSE.

## – Anlage 2 – organisationsspezifischer Ansatz



Jeder KVP verteilt Sperraufträge an die KOSE, an die diejenigen DL, KVP und PV angeschlossen sind, die die Produkte (als BER) akzeptieren.

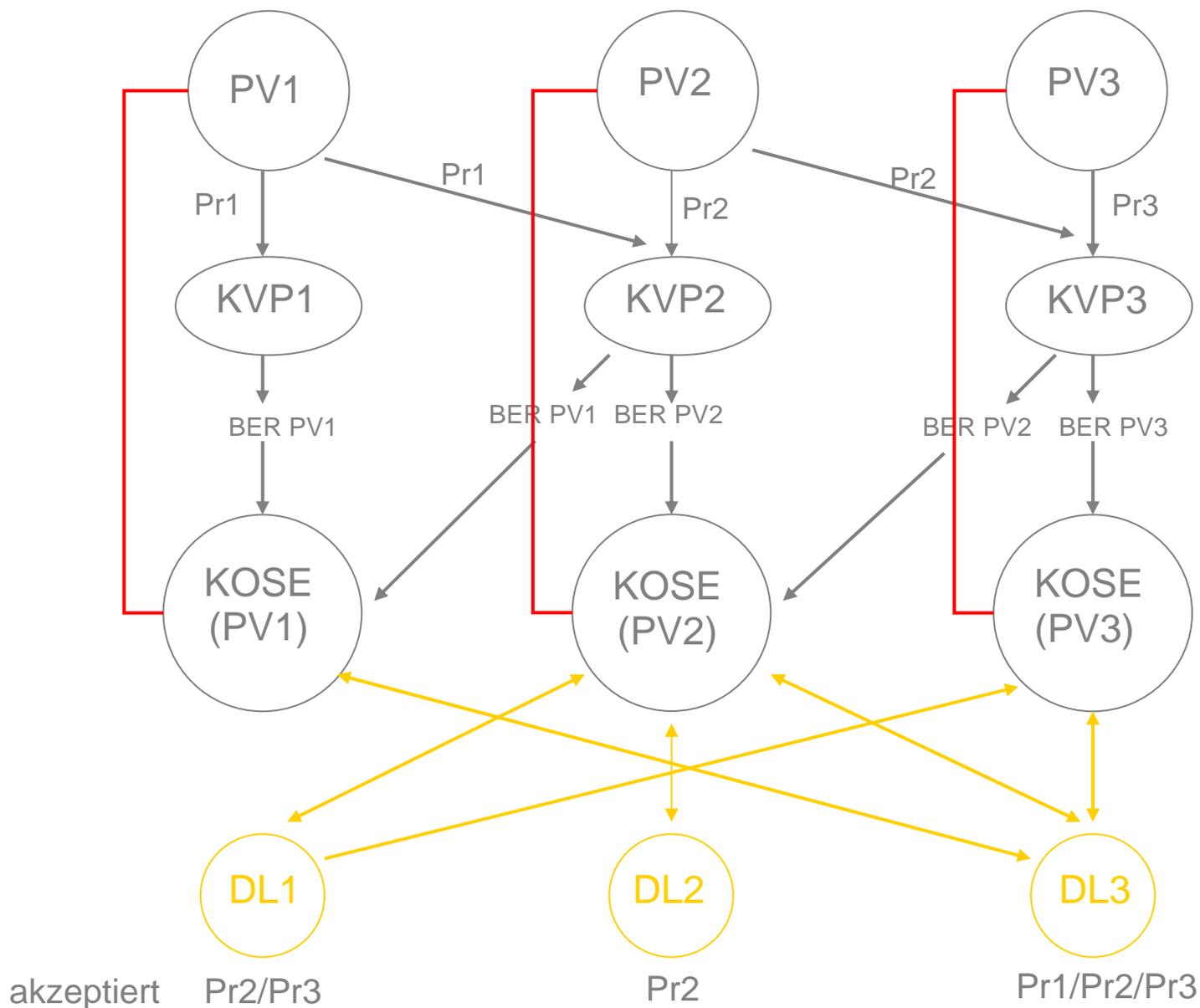
Pflege umfangreicher Zuordnungslisten (bei wem?) erforderlich (inkl. Schnittstellen). Welcher KVP und DL akzeptiert das Produkt und bei welchem KOSE ist er angeschlossen?

Jeder KOSE erstellt je DL, KVP oder PV dessen individuelle Sperrliste bezogen auf die bei ihm akzeptierten Produkte.

Damit existiert für jeden DL, KVP oder PV genau seine SLNM.

### **Kümmererproblem beim KOSE.**

## – Anlage 3 – produktorientierter Ansatz



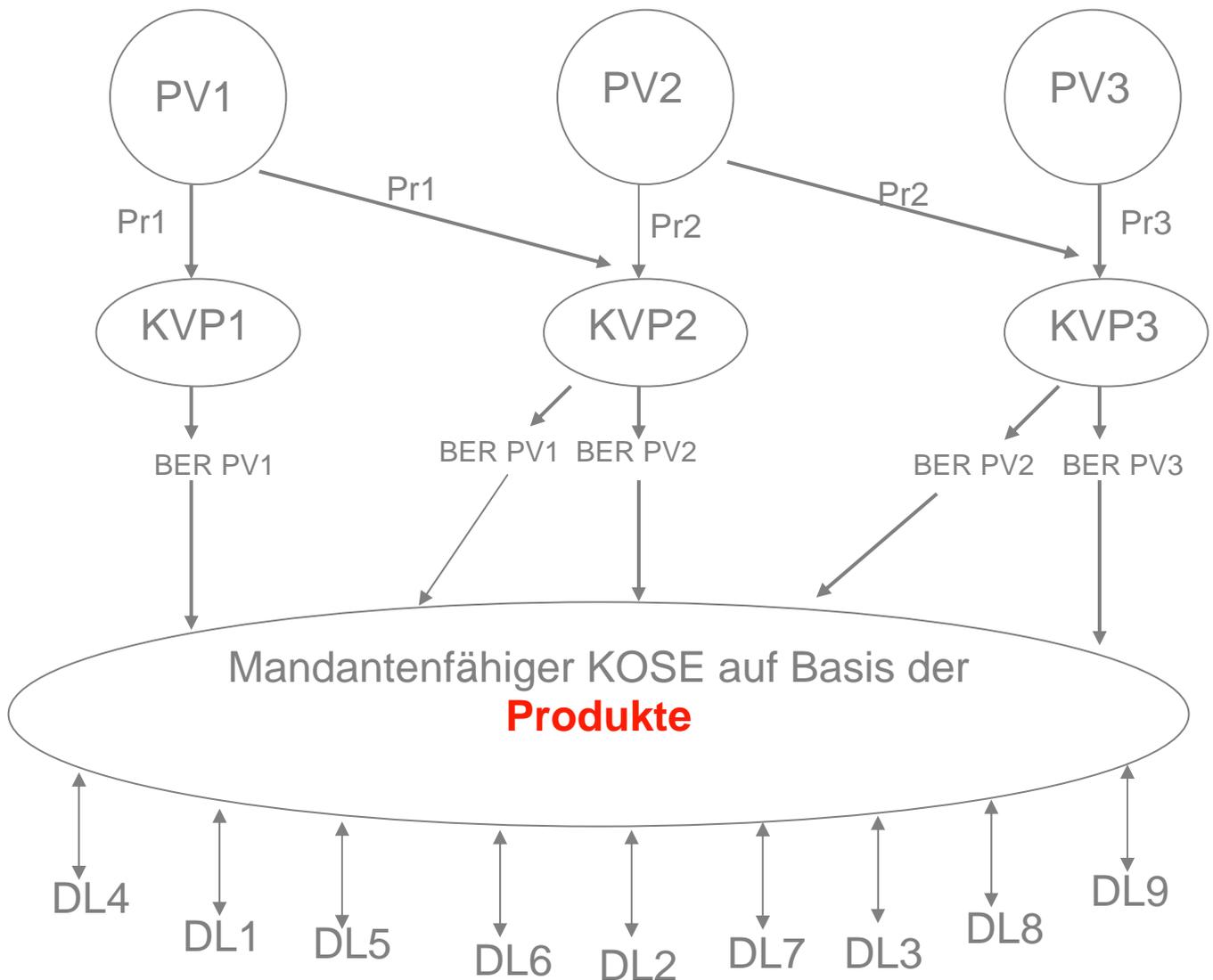
Die KVPs schicken die Sperraufträge an den zum PV gehörenden KOSE.

SL werden je PV getrennt erstellt. Es existiert also genau 1 SLNM zu einem PV bei genau 1 KOSE

DL und KVP benötigen die PV-KOSE-Zuordnung und müssen ihre Sperrlisten zusammenführen (Integrität, Sicherheit??)

**Kümmerner = PV**

## – Anlage 4 – mandantenfähiger Ansatz

**Sperrsteuerung:**

KVPs verteilen Sperraufträge mit Produkt\_ID (CR).

KOSE erhält von PV KVP- und DL-Listen (CR)

KOSE erstellt je DL, KVP und PV dessen individuelle Sperrliste bezogen auf die akzeptierten Produkte.

DL, KVP und PV rufen nur 1x ab

**Prämisse:**

einfache Verteilregel +  
eindeutiger Abruf +  
Sicherheit beim KOSE

herausgegeben von:

**Kompetenzcenter Elektronisches Fahrgeldmanagement NRW (KCEFM)**

Das KCEFM ist eine Einrichtung des Landes Nordrhein-Westfalen  
beim Verkehrsverbund Rhein-Ruhr (VRR).

Verkehrsverbund Rhein-Ruhr AöR  
AugustastraÙe 1  
45879 Gelsenkirchen

**[www.kcefm.de](http://www.kcefm.de)**

**November 2007**