Einsatz einer Gemeinsamen Service-Stelle (GSS) im Rahmen der VDV-Kernapplikation

WHITE PAPER
Version 1 / 2021

Inhaltsverzeichnis

02 Inhaltsverzeichnis & Abbildungsverzeichnis
03 1. Management Summary
04 2. Einführung
05 3. Systemarchitektur
06 4. Gemeinsame Service Stelle (GSS)
08 5. Ende-zu-Ende-Verschlüsselung und Transport Layer Security (TLS)-Verschlüsselung
10 6. Die Zentrale Vermittlungsstelle (ZVM)
11 7. Besonderheiten bei Nutzung einer GSS
11 7.1. Auszug aus den rechtlichen Rahmenbedingungen
12 7.2. Preisgabe persönlicher Schlüssel
12 7.3. Sonderkonfiguration in der ZVM
13 7.4. Mandantenfähigkeit der GSS
13 7.5. Leistungsfähigkeit der GSS
13 7.6. Sicherheit der GSS
14 8. Kostenbetrachtung zu GSS und ZVM
14 Glossar
15 Anlage

Abbildungsverzeichnis

04 Abbildung 1: Rollenmodell der VDV-KA
05 Abbildung 2: Systemarchitektur im eTicket Deutschland
15 Abbildung 3: Drei Grundmodelle zur systemischen Umsetzung
16 Abbildung 4: Modell einer GSS für ein DL-System für drei VU
16 Abbildung 5: Modell einer GSS für das DL- und KVP-System mehrerer VU mit verschiedenen Rollen
17 Abbildung 6: Modell einer GSS für das DL-, KVP- und PV-System für mehrere VU und VV mit verschiedenen Rollen

1. MANAGEMENT SUMMARY

Mit der deutschlandweiten Verbreitung der VDV-Kernapplikation (VDV-KA) sieht es der VDV eTicket Service (VDV-ETS) in der Rolle des Applikationsherausgebers als Verpflichtung an, die Teilnehmer an (((eTicket Deutschland auch über Themen zu informieren, die das Umfeld des Standards betreffen. Mit den stetig zunehmenden Erkenntnissen aus Umsetzungsprojekten will der VDV-ETS so Handreichungen und Unterstützung geben, um von den Umsetzungserfahrungen anderer zu profitieren.

Mit diesem White Paper beginnt der VDV-ETS daher eine Schriftenreihe zu Themen rund um (((eTicket Deutschland. Die Reihe wird je nach Bedarf verschiedene Themen aufgreifen. Das Thema dieses ersten White Papers beleuchtet den Einsatz einer bisher so genannten “Regionalen Vermittlungsstelle”.

In einigen Umsetzungsprojekten von (((eTicket Deutschland werden von Verkehrsunternehmen und Verkehrsverbünden gemeinsame Service-Stellen implementiert und betrieben. In diesen werden Systemfunktionen in einem gemeinsamen System gebündelt, die sonst jeweils im eigenen Hintergrundsystem realisiert werden müssten. Aufgrund der historischen Entwicklung wurden solche Service-Stellen bisher als “Regionale Vermittlungsstellen” bezeichnet. Da solche Service-Stellen weder zwingend einen regionalen Bezug, noch Vermittlungsfunktion zum Interoperabilitätsnetzwerk (ION) haben, ist dieser Begriff unzutreffend und missverständlich. Von ihrer Funktion und Architektur her sind solche Systeme als “Gemeinsame Service-Stellen” (GSS) zu verstehen. Sie werden im Folgenden daher auch als solche bezeichnet.

- **GSS sind aus Sicht des VDV-KA-Standards zulässig, da es sich um Funktionsauslagerungen aus den Hintergrundsystemen von (((eTicket Deutschland Teilnehmern handelt.**
- **GSS sind dort sinnvoll, wo im Rahmen von (((eTicket Deutschland eTicket-Funktionalitäten von mehreren Teilnehmern in einem System genutzt und als Service für alle ausgeführt werden.**
- **Allein als Zugang zum ION sind GSS weder erforderlich noch sinnvoll.**

Im Hinblick auf die Einhaltung des Standards gelten für GSS die gleichen Anforderungen, wie sie für die Hintergrundsysteme aller VU und VV gelten: zum ION hin muss gemäß VDV-Kernapplikation (VDV-KA) kommuniziert werden. Damit wird eine sichere Ende-zu-Ende-Verschlüsselung erreicht, die allen Anforderungen des Bundesdatenschutzgesetzes (BDSG) sowie den Anforderungen an den IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entspricht.

Um die Erfordernisse des BDSG und des IT-Grundschutzes des BSI auf der gesamten Nachrichtenstrecke Ende-zu-Ende zu erfüllen, ist auch für die Kommunikation zwischen Verkehrsunternehmen und GSS die Verschlüsselung der Daten gemäß VDV-Kernapplikation erforderlich.

2. EINFÜHRUNG

Die VDV-KA ist der mit Fördermitteln des Bundes geschaffene, offene Standard für das eTicketing im öffentlichen Personenverkehr in Deutschland. Der Standard spezifiziert die erforderlichen Schnittstellen und stellt eine einheitliche Sicherheitsarchitektur bereit. Weiterhin definiert er die Verfahren und Kommunikationsmuster auf Geschäftsprozessebene.

Der Standard basiert auf dem Rollenmodel gemäß EN/ISO 24014–1. Damit weist er allen Beteiligten ihre Rollen, Aufgaben und Verantwortlichkeiten zu (s. Abbildung 1).

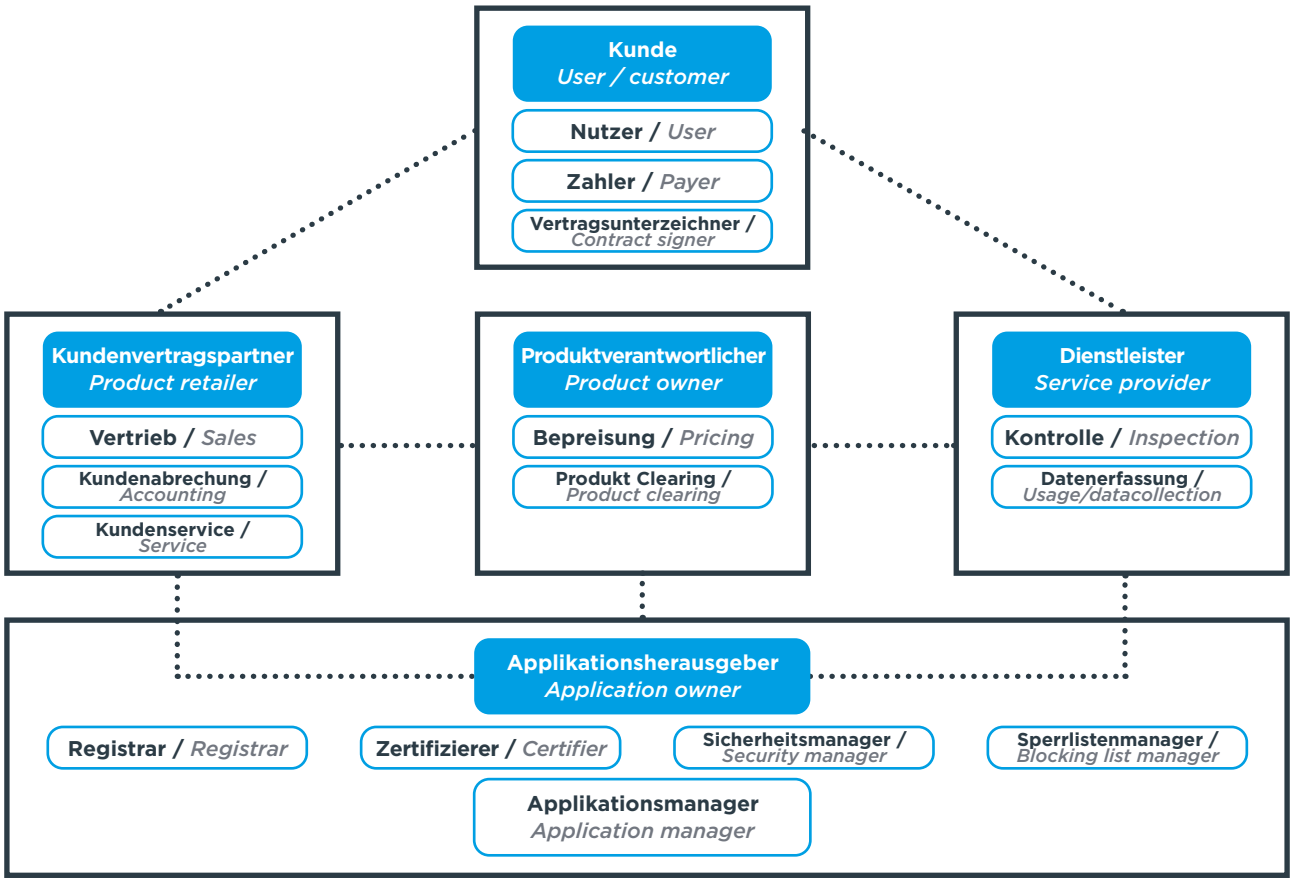

Abbildung 1: Rollenmodell der VDV-KA

Die VDV eTicket Service GmbH & Co. KG (VDV-ETS) nimmt die Rolle des Applikationsherausgebers ein. Gemäß der Definition der EN/ISO 24014–1 ist der VDV-ETS damit auch Hüter und Weiterentwickler des Standards und der Betreiber von zentralen Diensten, die für das reibungslose Funktionieren des Standards in allen Teilnehmersystemen erforderlich sind. Für den Bereich „Elektronisches Fahrgeld-Management“ repräsentiert der VDV-ETS Deutschland bei der International Organization for Standardization (ISO), dem Europäische Komitee für Normung (CEN) und anderen Organisationen. Die Wort- und Bildmarke „(((eTicket Deutschland“ sowie die unterschiedlichen eingetragenen Designs sind markenrechtlich geschützt.

3. SYSTEMARCHITEKTUR

Die Systemarchitektur beschreibt die Struktur des eTicketsystems an Hand von Systemkomponenten (zum Beispiel Chipkarte, Handy, Terminal und HGS) und ihre Schnittstellen untereinander. Hierdurch wird nicht die Funktionalität (das „Was“) sondern eher die Verknüpfung der Komponenten zueinander (das „Wie“) abgebildet. Die Systemarchitektur erfüllt keinen Selbstzweck sondern ist die Voraussetzung um Feinentwurf und Implementierung eines eTicketsystems in der Praxis durchführen zu können.

In der Regel wird die Systemarchitektur eines eTicketsystems in drei bis fünf funktionalen Ebenen abgebildet. Jeweils abhängig von der gewünschten Funktionalität sowie Anzahl und Größe der beteiligten Organisationen (siehe Abbildung 2):

- **Bei kleinen E-Ticketsystemen (ein oder wenige VU, ein Aufgabenträger) besteht die Systemarchitektur meist nur aus den Ebenen 1 bis 3.**
  Typisches Beispiel: Die vielen Inselsysteme, die es in den 90er Jahren in Deutschland gab.
- **Sehr viele ausländische eTicketsysteme basieren auf vier funktionalen Ebenen („4-level-model“).**
  Beispiele sind London, Dänemark, die Niederlande und Hongkong
- **In Deutschland wird heute meist ein 5-Ebenen Modell in der Systemarchitektur angewendet**

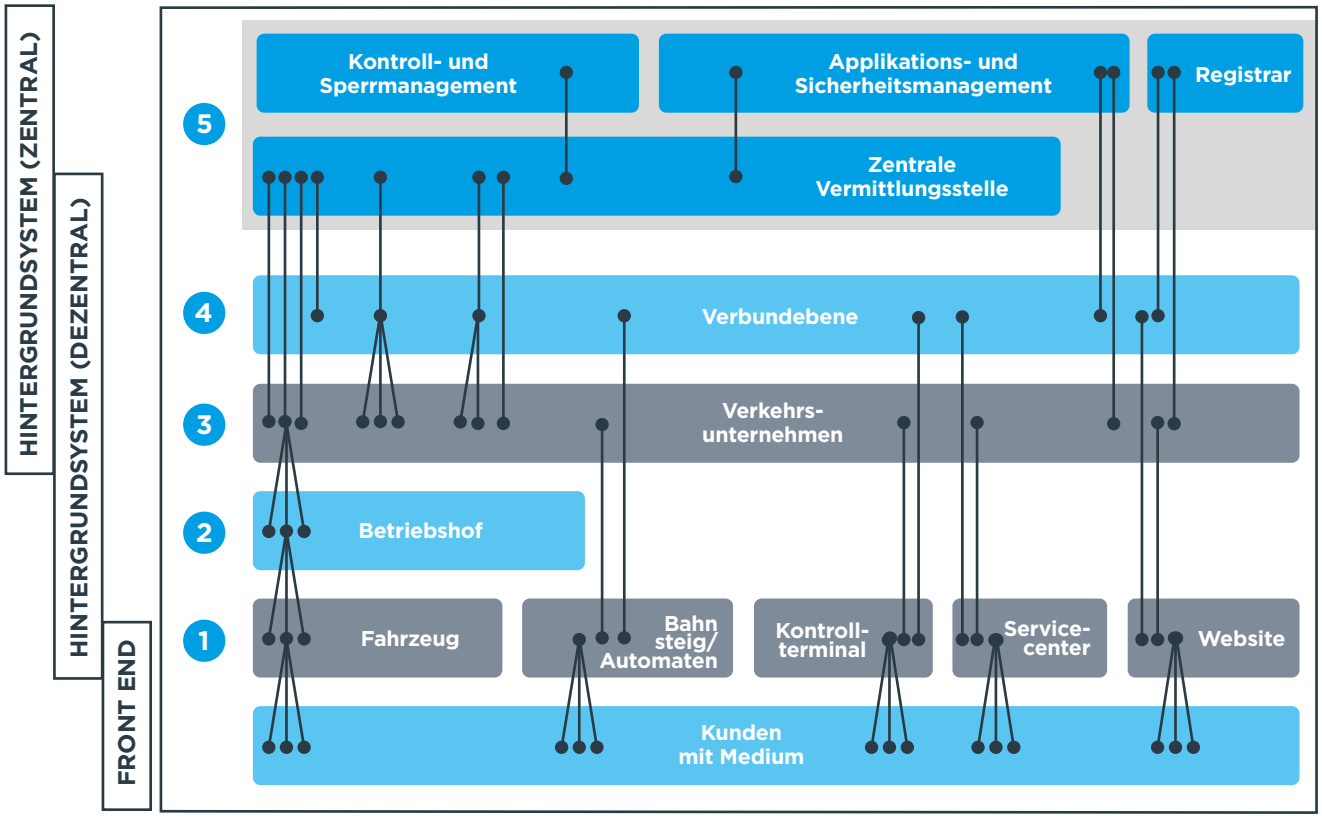

Abbildung 2: Systemarchitektur im eTicket Deutschland

In der Gestaltung der Systemarchitektur bei der Umsetzung der VDV-KA gibt es mehrere Möglichkeiten (vgl. Abbildung 2). Dabei sind die in der Spezifikation genannten drei folgenden Aspekte von zentraler Bedeutung:

- **Integrität; dies ist die Sicherstellung, dass Daten nicht unautorisiert verändert oder zerstört werden.**
- **Verbindlichkeit; dies ist die Sicherstellung, dass die Aktionen einer Instanz eindeutig und ausschließlich dieser Instanz zugeordnet werden und dass die Kommunikationsbeziehung nicht geleugnet werden kann.**
- **Vertraulichkeit; diese ist gegeben, wenn sicher gestellt werden kann, dass Informationen nicht durch unautorisierte Personen, Instanzen oder Prozesse eingesehen werden können.**

Die VDV-KA ist ein Standard, der – trotz der sehr heterogenen organisatorischen Gegebenheiten im ÖP(N)V – einwandfrei und zuverlässig funktionieren muss. Deshalb ist die Systemarchitektur der VDV-KA so ausgelegt worden, dass die unterschiedlichen Organisationsstrukturen und Ausprägungen des ÖP(N)Vs bedient werden können.

4. GEMEINSAME SERVICE STELLE (GSS)

Bereits während der Entwicklung des Standards bestand in der Branche Konsens, dass reale Systeme eines Verkehrsunternehmens (VU) mehrere Rollen in sich vereinen oder auch Funktionen von Rollen in unterschiedlichen Systemen realisiert werden können. Wie zu erwarten, entstanden bereits bei den ersten Umsetzungsprojekten GSS, in denen die Teilnehmer Servicefunktionen bündelten, die sonst im eigenen Hintergrundsystem hätten abgebildet werden müssen.

Ein Beispiel hierfür ist der „Enterprise Service Bus“ des Hamburger Verkehrsverbundes (HVV).
Im Enterprise Service Bus sind die PV-Funktionalitäten des HVV realisiert. Da die Zentrale Vermittlungsstelle (ZVM) des (((eTicket Deutschland zum Zeitpunkt der Inbetriebnahme noch nicht zur Verfügung stand, wurde diese GSS zusätzlich sowohl für den Nachrichtenaustausch untereinander als auch zum ION hin konstruiert. Damit wurde der Enterprise Service Bus wie alle GSS gezielt auf die speziellen Bedürfnisse der Beteiligten, in diesem Fall im Raum Hamburg, zugeschnitten.

Solche Service-Stellen entstanden aus ähnlichen Gründen auch an anderen Orten in Deutschland. Bei der Datendrehscheibe (DDS) der Deutschen Bahn (DB) handelt es sich zum Beispiel ebenfalls um eine GSS. Sie hat jedoch die Aufgabe, unterschiedliche IT-Plattformen im DB-Konzern, auch für die Kommunikation mit den Terminals zu vernetzen und das DB-Gateway zur ZVM zur Verfügung zu stellen. Weitere realisierte GSS sind die Verbundintegrationsplattform Baden-Würtemberg, das vHGS des RMV sowie das PRION des VBB.

Aufgrund der jeweils regionalen und/oder unternehmensspezifischen Bedürfnisse besitzen die bestehenden GSS unterschiedliche Auslegungen und sind nicht miteinander vergleichbar. Diese Systeme befinden sich innerhalb der Systemgrenzen der gemeinsamen Nutzer und fallen damit allein in deren Zuständigkeit und Verantwortung. Diese Nutzer sind in der Regel Verkehrsunternehmen (VU) und Verkehrsverbünde (VV).

Für solche Systeme ist aufgrund der historischen Entwicklung bisher die Bezeichnung „Regionale Vermittlungsstelle“ (RVS) entstanden. Aufgrund der geschilderten Entwicklung ist jedoch ausdrücklich festzuhalten, dass diese Bezeichnung historisch entstanden, nicht im Sinne der regionalen Anbindung an das ION gemeint und damit irreführend ist.

Weiterhin ist festzuhalten, dass GSS von der Systemarchitektur her nicht regional ausgeprägt sein müssen. Wenn z.B. mehrere VU und VV eines Ballungsraumes eine Service-Stelle nutzen, kann sich diese physisch in einem geografisch völlig anderen Bereich Deutschlands befinden.
Ebenfalls denkbar ist, dass sich auch räumlich völlig getrennte Partner eine GSS teilen.

Insofern macht es Sinn, solche Einheiten als gemeinsame Service-Stelle für mehrere Nutzer zu begreifen und sie deshalb als „Gemeinsame Service-Stelle“ (GSS) zu bezeichnen. Die Modelle im Anhang zeigen mögliche Varianten und Anwendungsszenarien für die GSS. Über die gezeigten Beispielmodelle hinaus kann es zahlreiche weitere Varianten geben.

Während der Erstellung des KA-Releases 1.107 wurde der Versuch unternommen, die Vermittlungsfunktion innerhalb einer GSS zu spezifizieren. Mit der anschließend deutlich werdenden Verschiedenartigkeit der GSS wurde jedoch ebenso deutlich, dass eine einheitliche Spezifikation für eine solche Stelle weder machbar noch sinnvoll ist, und als spezielle Architekturausprägung eines Hintergrundsystems nicht zum KA-Standard gehört.
GSS sind aus Sicht des VDV-KA-Standards zulässig, da es sich um Funktionsauslagerungen aus den Hintergrundsystemen von (((eTicket Deutschland-Teilnehmern handelt und der Standard für die Architektur der Teilnehmersysteme keine Vorgaben macht.

Sinnvoll sind GSS dort, wo Systemfunktionalitäten als Dienstleistung von mehreren Teilnehmern genutzt und an gemeinsamer Stelle ausgeführt werden. Daraus ergibt sich natürlich die Notwendigkeit, Daten von der GSS weiter an die dahinter liegenden einzelnen Teilnehmersysteme zu vermitteln bzw. Daten von diesen entgegenzunehmen und in das ION zu übergeben.

Allein als Zugang zum ION sind GSS weder erforderlich noch sinnvoll.

5. ENDE-ZU-ENDE-VERSCHLÜSSELUNG UND TRANSPORT LAYER SECURITY (TLS)-VERSCHLÜSSELUNG

Im Hinblick auf die Einhaltung des KA-Standards gelten für GSS die gleichen Anforderungen, wie sie für die Hintergrundsysteme aller VU gelten: Im Interoperabilitätsnetz (ION) des (((eTicket Deutschland muss gemäß VDV-KA-Spezifikation kommuniziert werden. Dies bedeutet, dass vom sendenden Teilnehmersystem bis zum empfangenden Teilnehmersystem hin die Nachricht mit Web Service Security (WSS) und unter Verwendung der VDV-ETS-Public Key Infrastructure (VDV-ETS-PKI) verschlüsselt werden muss.

Grund für diese Maßnahme ist, dass die Nachricht auf dem Weg vom Sender zum Empfänger aus technischen Gründen über verschiedene Hubs, Switches, Router und Server läuft. Ohne geeignete Verschlüsselung sind Nachrichten stets der Gefahr des Missbrauchs durch unerlaubte Verarbeitung und/oder Verfälschung ausgesetzt. Der Missbrauch kann an jedem durchlaufenen Hub, Switch, Router und Server der Nachrichtenstrecke stattfinden. Die Missbrauchsbandbreite reicht dabei von der Speicherung und Nutzung der persönlichen Daten der Fahrgäste über die Erfassung von Umsatzvolumina des VU bis hin zu finanziellen Schäden.

Ist das empfangende Teilnehmersystem an eine GSS angebunden, die Teile der fachlichen Daten verarbeiten oder prüfen soll, müssen diese von der GSS entschlüsselt werden können. Deshalb muss die GSS in diesem Falle vom VDV-KA-Teilnehmer autorisiert sein, diese Entschlüsselung auszuführen bzw. bei Übergabe von Daten in das ION zu verschlüsseln.

Gemäß Sicherheitskonzept der VDV-KA bedeutet dies, dass dann aber auch die Nachrichten von der GSS an/von dahinterliegenden Teilnehmersystemkomponenten verschlüsselt übertragen werden müssen. Bei Verwendung von TLS muss sichergestellt werden, dass alle Kommunikationspartner ausschließlich geeignete Cipher Suites für TLS verwenden, in der GSS registriert sind und vertrauenswürdigen Zertifikate (z.B. der VDV-ETS-PKI) nutzen. In der VDV-KA ist die Cipher Suite mit der Bezeichnung „TLS_DHE_RSA_WITH_AES_256_CBC_SHA“ vorgeschrieben (siehe RFC 5280 unter http://www.ietf.org/rfc/rfc5280.txt). RSA-Schlüsselpaare mit Modulus-länge 2048 Bit sowie AES- Schlüssel mit Länge 256 Bit werden verwendet. Das Handshake des TLS Standards muss auf Basis dieser Zertifikate verpflichtend zwischen den Endepunkten der Kommunikation ablaufen (und zwar unabhängig davon, dass Hubs, Switches, Router etc. dazwischen liegen).

Dies bedeutet, dass eine als verschlüsselt initiierte Verbindungsaufnahme immer zu einer verschlüsselten Verbindung führt oder abgebrochen wird. Es wird genau ein vorgegebenes Verschlüsselungsverfahren unterstützt oder höchstens zusätzlich ein gleichwertiger Fallback zugelassen.
Das größte Problem bei TLS stellen die Zertifizierungsstellen dar. Die Zertifikate für TLS werden von weltweit über 700 Zertifizierungsstellen ausgestellt. Durch die große Anzahl gibt es keine ausreichende Kontrolle, ob eine Zertifizierungsstelle korrekt arbeitet. Immer wieder werden Fälle bekannt, in denen dies nicht der Fall war. Deswegen sollten in GSS integrierte Teilnehmer im VDV-KA konformen Umfeld bekannt geben, mit welcher PKI gearbeitet wird. Diese muss die VDV-KA-Sicherheitsanforderungen erfüllen. Vorzugsweise sollte dies die

VDV-ETS-PKI sein, bei der sie ohnehin registriert sind und deren TLS-Zertifikate ohne weiteres auch anderweitig verwendet werden können.

Folgende Hinweise soll das TLS-Thema hier nochmals sensibilisieren:
Im Geschäft mit Privatkunden ist die Nachfrage nach verschlüsselter Kommunikation groß. Gleichzeitig sind Privatkunden in der Regel nicht bereit, für diese Verschlüsselung Kosten auf sich zu nehmen oder aufwändige Prozesse zu akzeptieren. Daher werden im Business-to-Customer-Bereich (B2C) trotz des bekannten Risikos regelmäßig TLS-Zertifikate genutzt, deren Zertifizierungsstelle vom Anwender nicht geprüft wurde oder mit vertretbarem Aufwand auch gar nicht geprüft werden kann.

Außerdem kaufen zahlreiche B2C-Anbieter ihre Zertifikate nicht direkt bei einer Zertifizierungsstelle, sondern von Zwischenhändlern oder von Hosting-Providern, die TLS-Verschlüsselung als Zusatzdienstleistung verkaufen. Dadurch haben solche B2C-Anbieter de facto keine Kenntnis über die Zertifizierungsstelle, deren Zertifikate sie verwenden.

Eine weitere Schwachstelle bei TLS ist die Zertifizierung bzw. Zertifikatsausstellung selbst. Grundsätzlich kann jede Zertifizierungsstelle Zertifikate für jeden Rechner im Internet (Host) ausstellen. Deshalb kann es für jeden Host von unterschiedlichen Zertifizierungsstellen mehrere Zertifikate geben. Wenn eine Zertifizierungsstelle bei der Zertifikatsausstellung den erforderlichen Schritten nicht genau folgt, kann sich ein Angreifer ein gültiges Zertifikat für einen fremden Host ausstellen lassen.

Die Erfahrung zeigt, dass es Zertifizierungsstellen gibt, die versehentlich oder bewusst gültige Zertifikate für jeden Antragsteller ausstellen. Gründe hierfür sind Defizite in der internen Organisation der Zertifizierungsstelle, bewusste Gewinnmaximierung zu Lasten der Qualität oder Druck einer staatlichen Stelle. Dadurch befinden sich stets Zertifikate im Umlauf, deren wahrer Inhaber ein anderer als der vorgegebene ist. Damit ist die ganze Bandbreite des Missbrauchs möglich, angefangen vom Mitlesen bis hin zu aktiven Angriffen (Man-in-the-Middle-Angriff).

Bei asymmetrischer Verschlüsselung werden vom Kommunikationspartner ein öffentlicher und ein privater Schlüssel erzeugt. Der öffentliche Schlüssel ist für jeden zugänglich, der private hingegen muss geheim gehalten werden. Beide Schlüssel muss der B2C-Anbieter erzeugen, bevor er ein Zertifikat bei einer Zertifizierungsstelle beantragen kann. Da nicht alle B2C-Anbieter die Schlüsselerzeugung selbst ausführen möchten oder können, gibt es Zertifizierungsstellen, die ihren Kunden anbieten, beide Schlüssel für sie zu erzeugen. Damit ist der private Schlüssel nicht mehr geheim und das auf dieser Basis ausgestellte Zertifikat nicht sicher.

Zusammenfassend gilt: „Wähle deine Zertifizierungsstelle mit Bedacht“. Das hat der VDV-ETS für die VDV-KA-Teilnehmer mit Beauftragung des T-Systems-Trust Centers erledigt. Hier wird auf allen Strecken eine Verschlüsselung gewährleistet, die allen Anforderungen des Bundesdatenschutzgesetzes (BDSG) sowie den Anforderungen an den IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entsprechen.

6. DIE ZENTRALE VERMITTLUNGSSTELLE (ZVM)

Die Aufgabe der ZVM ist die sichere und schnelle Vermittlung aller KA-Nachrichten zwischen allen Teilnehmern an (((eTicket Deutschland. Sie stellt sicher, dass nur in der KA zugelassene Nachrichten von registrierten Teilnehmern ausgetauscht werden und dass die Teilnehmer gemäß ihrer registrierten Rolle(n) auch dazu berechtigt sind. Die ZVM vermittelt daher auch die Nachrichten zu den VDV-ETS-Systemen KOSE (Sperrlistenservice) und ASM (Applikations- und Sicherheitsmanagement).

Die Vermittlung aller Nachrichten zwischen allen Teilnehmern bedeutet beispielsweise nicht nur die Vermittlung zwischen Regionen, sondern auch zwischen VU, die innerhalb einer Stadt oder Region arbeiten. Daher besteht auch innerhalb einer Stadt oder Region kein Bedarf, eine regionale Vermittlungsstelle ohne die zusätzlichen Service-Funktionen einer GSS einzusetzen.

Die ZVM übernimmt im Gegensatz zu einer GSS keine Service-Funktionen anderer Rollen. Die zentralisierte Übernahme von Service-Funktionen von VU bzw. ihren VDV-KA-Teilnehmersystemen ist den GSS vorbehalten. Die ZVM gewährleistet ausschließlich die sichere und schnelle Vermittlung aller KA-Nachrichten zwischen allen Teilnehmern an (((eTicket Deutschland.

Für diese Aufgabe ist die ZVM hochspezialisiert. Sie arbeitet

- **unternehmensneutral**
- **hochsicher**
- **hochperformant**
- **7x24 Stunden**
- **dem „Stand der Technik“ entsprechend**

Die Auslegung der ZVM als zentrales System gewährleistet für die Nutzer minimalen Anmelde- und Konfigurationsaufwand. Dazu werden im ASM die Organisationsidentifikatoren (ORG_ID) mit Rollen und IP-Adressen aller Teilnehmer an (((eTicket Deutschland zentral gepflegt und von diesem aktuell der ZVM zu Verfügung gestellt. Würde jedes Teilnehmersystem diese Pflege selbst erledigen, müsste jedes VU und jeder VV dauerhaft entsprechendes Personal bei sich vorhalten.

Durch die gewählte Lösung müssen alle Teilnehmer

- **nur 1 Adresse kennen (die der ZVM)**
- **nur 1 Adresse pflegen (die der ZVM)**
- **sich nicht mehr um die sichere Zustellung kümmern, sobald die Nachricht bei der ZVM eingereicht wurde**

„Sichere Zustellung“ bedeutet dabei, dass die Nachricht

- **vollständig und unverfälscht angekommen ist**
- **beim richtigen Empfänger**
- **mit der korrekten Adresse**
- **und dass sie von einem echten VDV-KA-Absender versandt wurde**

Dies bedeutet weiter, dass die ZVM auch die Pufferung und zeitversetzte Zustellung von Nachrichten im Fall der Nichtverfügbarkeit eines Teilnehmers (offline z.B. wegen Wartung) sowie die Ausnahmebehandlung in Fehlerfällen (z.B. Fehler in der Nachricht) übernimmt.

Das entbindet den Sender der Nachricht allerdings nicht davon, zu einer versandten Nachricht den Eingang einer Bestätigung („TXB“) zu überwachen oder auf eine Ablehnung wegen fehlerhafter Dateninhalte („TXA“) zu reagieren. Diese Kontrollen können nur durch das sendende VU durchgeführt werden und sind nicht Aufgabe der ZVM.

7. BESONDERHEITEN BEI NUTZUNG EINER GSS

Alle Teilnehmer an (((eTicket Deutschland haben mit VDV-ETS einen (((eTicket-Teilnahmevertrag geschlossen, der die Rechte und Pflichten der Teilnehmer regelt. Damit können sich alle Unternehmen und Verbünde gegenseitig darauf verlassen, dass sich alle an das Regelwerk halten, auch wenn der operative Betrieb mit einer GSS abwickelt. Dadurch wird für alle Teilnehmer eine gemeinsame und sichere Arbeitsgrundlage geschaffen.

7.1. Besonderheiten bei Nutzung einer GSS

§ 5 Abs. 4 (((eTicket-Regelwerk sagt über die Pflichten der Teilnehmer aus:

„Die Teilnehmer haben durch geeignete Maßnahmen sicherzustellen, dass in ihrem Einflussbereich sowie im Einflussbereich der von ihnen eingeschalteten Dritten keine missbräuchliche Verwendung von (((eTicket-Systemkomponenten, der (((eTicket-Produkte und des (((eTicket-Systems möglich ist.“

In § 2 Abs. 3 (((eTicket-Regelwerk sind die Pflichten der Regiegesellschaft, also VDV-ETS, geregelt:

„Der VDV-ETS ist verpflichtet, im Falle von Verstößen von Teilnehmern gegen deren Pflichten aus dem (((eTicket-Teilnahmevertrag, einschließlich des (((eTicket-Regelwerks, nach entsprechender Ankündigung

und angemessener Fristsetzung gegenüber dem verstoßenden Teilnehmer geeignete Maßnahmen zu ergreifen.“

Der VDV-ETS wird bei der Auswahl der Maßnahmen die wirtschaftlichen Interessen des Betroffenen sowie die berechtigten Interessen aller Teilnehmer berücksichtigen.“

Aus dieser gegenseitigen Verpflichtung heraus ergeben sich eine Reihe von Punkten, die bei Nutzung eine GSS zu beachten sind.

7.2. Preisgabe persönlicher Schlüssel

Durch die Ende-zu-Ende-Verschlüsselung kann eine KA-Nachricht nur im System des vorgesehenen Empfängers entschlüsselt und gelesen werden, das über die öffentlichen Schlüssel und Zertifikate verfügt. Jeder VDV-KA-Teilnehmer ist solch ein Empfänger.

Nutzt dieser eine GSS, müssen eingehende Nachrichten schon in der GSS entschlüsselt werden, damit die GSS die Nachrichten prüfen, verarbeiten und weiterleiten kann. Ausgehende Nachrichten müssen in der GSS mittels VDV-ETS-PKI verschlüsselt werden.
Die GSS muss als vertrauenswürdige Instanz arbeiten. Die Entschlüsselung der eingehenden Nachrichten und die Verschlüsselung der ausgehenden Nachrichten setzen voraus, dass das VU dem Betreiber der GSS seine(n) privaten Schlüssel aushändigen muss. Der Betreiber der GSS muss seinerseits sämtliche ihm übergebenen Schlüssel gemäß den aktuellen Sicherheitsstandards verwalten.

Um die Vertrauenswürdigkeit sicherzustellen, könnte eine Umverschlüsselung in der GSS stattfinden. Die Authentizität und Nichtabstreitbarkeit von Nachrichten des Senders (Ende-zu-Ende bis zum Empfänger) erhält man zumindest zum Teil dadurch, dass der Sender die VDV-KA-Nachricht vor dem Verschlüsseln signiert. Diese signierte Nachricht wird von der GSS aufbewahrt und 1:1 an den Empfänger hinter der GSS weitergeleitet – allerdings nun neu verschlüsselt.

7.3. Preisgabe persönlicher Schlüssel

Der Betrieb einer GSS erfordert, dass eine Sonderkonfiguration in der ZVM vorgenommen wird. Die ZVM kann Nachrichten nicht mehr nur anhand der ORG_ID und Rolle eines Teilnehmers routen, sondern muss wissen, welche Teilnehmer welche GSS nutzen. Daher ist es erforderlich, die Zuordnung von Teilnehmern zur GSS als Routinginformation in der ZVM zu hinterlegen.

7.4. Mandantenfähigkeit der GSS

Der Betreiber der GSS muss sicherstellen, dass er seine Teilnehmer als datentechnisch und organisatorisch abgeschlossene Einheiten im System behandelt (Mandantenfähigkeit). Nur so kann eine ungewollte und unzulässige Vermischung oder Zusammenfassung der Nutzungsdaten der Teilnehmer vermieden und die Daten der Teilnehmer untereinander geschützt werden.

7.5. Leistungsfähigkeit der GSS

Da die GSS für ihre Nutzer die Verbindung zum ION darstellt, muss von Seiten der Nutzer sehr genau auf die Leistungsfähigkeit der GSS geachtet werden.

Mindestens folgende Gesichtspunkte müssen hier beachtet werden:

- **Servicezeit 7x24 Stunden**
- **definierte und im Betrieb überwachte Performanz, die auch für Betriebsspitzen ausreichend dimensioniert ist**
- **zuverlässig organisierte Ausfallsicherheit, einschließlich der entsprechenden Recovery-Mechanismen**

7.6. Sicherheit der GSS

Wie alle IT-Systeme, kann die GSS ein Sicherheitsrisiko darstellen. Der VDV-ETS rät daher dringend zu prüfen, ob die jeweilige GSS mindestens die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichten Anforderungen einhält. Darüber hinaus sollten die relevanten Normen und Standards der Internationalen Organisation für Standardisierung (ISO) eingehalten werden.
Die IT-Grundschutz-Kataloge des BSI definieren für bestimmte Anforderungen konkrete Maßnahmenkataloge und für andere Anforderungen ein strukturiertes Vorgehen, um die notwendigen Maßnahmen zur Schaffung und Erhaltung von IT-Sicherheit zu identifizieren.
Die ISO stellt für IT-Sicherheit die ISO/IEC 27000-Schriftenreihe zur Verfügung. ISO/IEC 27001 stellt die Norm für Informationssicherheitsmanagementsysteme (ISMS) dar, ISO/IEC 27002 den Leitfaden für das Informationssicherheitsmanagement (vormals ISO/IEC17799:2005).
Zusätzlich stellt die ISO mit der ISO/IEC 20000 die ISO/IEC-Norm für IT-Servicemanagement zur Verfügung.

Darüber hinaus bietet die IT Infrastructure Library (ITIL) eine Best-Practices-Sammlung für das IT-Servicemanagement an. Der Payment Card Industry Data Security Standard (PCI-DSS) setzt als Regelwerk für die Abwicklung von Kreditkartentransaktionen den Schwerpunkt für Sicherheit bei Finanztransaktionen, wie sie auch im elektronischen Fahrgeldmanagement vorkommen.

8. KOSTENBETRACHTUNG ZU GSS UND ZVM

Die Kosten für die Betriebsführung einer GSS gestalten sich entsprechend den jeweils unterschiedlichen lokalen bzw. regionalen Ausgestaltungen sehr unterschiedlich. Dabei ist zu beachten, dass die Umsetzung der in Kapitel 6 genannten Punkte naturgemäß eine nicht unerhebliche Grundlast an Aufwänden verursacht, die nur bei der Nutzung einer GSS anfällt.

Für die Nutzung von ZVM und KOSE fallen für die Teilnehmer keine zusätzlichen Kosten an. Dies ist für alle Teilnehmer einheitlich im (((eTicket-Teilnahmevertrag festgelegt. Diese Festlegung kann nur durch Beschluss der Teilnehmerversammlung geändert werden.

Der VDV-ETS wird über die Gebühren der NM-Zertifikate finanziert. Die Teilnehmer bezahlen ihre NM-Zertifikate bei T-Systems. T-Systems leitet einen Teil der Gebühren an den VDV-ETS weiter. Aus diesem Gebührenanteil werden sämtliche Kosten des VDV-ETS finanziert, die für alle (((eTicket Deutschland-Teilnehmer anfallen. Nur individuell angeforderte Dienstleistungen wie z.B. Schulungen oder Beratungsaufträge werden den Teilnehmern separat in Rechnung gestellt.

Dies bedeutet, dass die ZVM wie auch alle anderen zentralen Systeme des (((eTicket Deutschland Inklusivleistungen des VDV-ETS sind. Über seine NM-Zertifikate ist für jeden Teilnehmer die ZVM-Nutzung bereits abgegolten. Die Nutzung einer GSS nur zu Vermittlungszwecken ist daher auch aus ökonomischer Sicht nicht sinnvoll.

GLOSSAR

Abkürzungen und Definitionen können dem VDV-KA Glossar entnommen werden.

ANLAGE

Schematische Darstellungen von möglichen Varianten einer GSS.

Drei Grundmodelle zur systemischen Umsetzung verschiedener Rollen

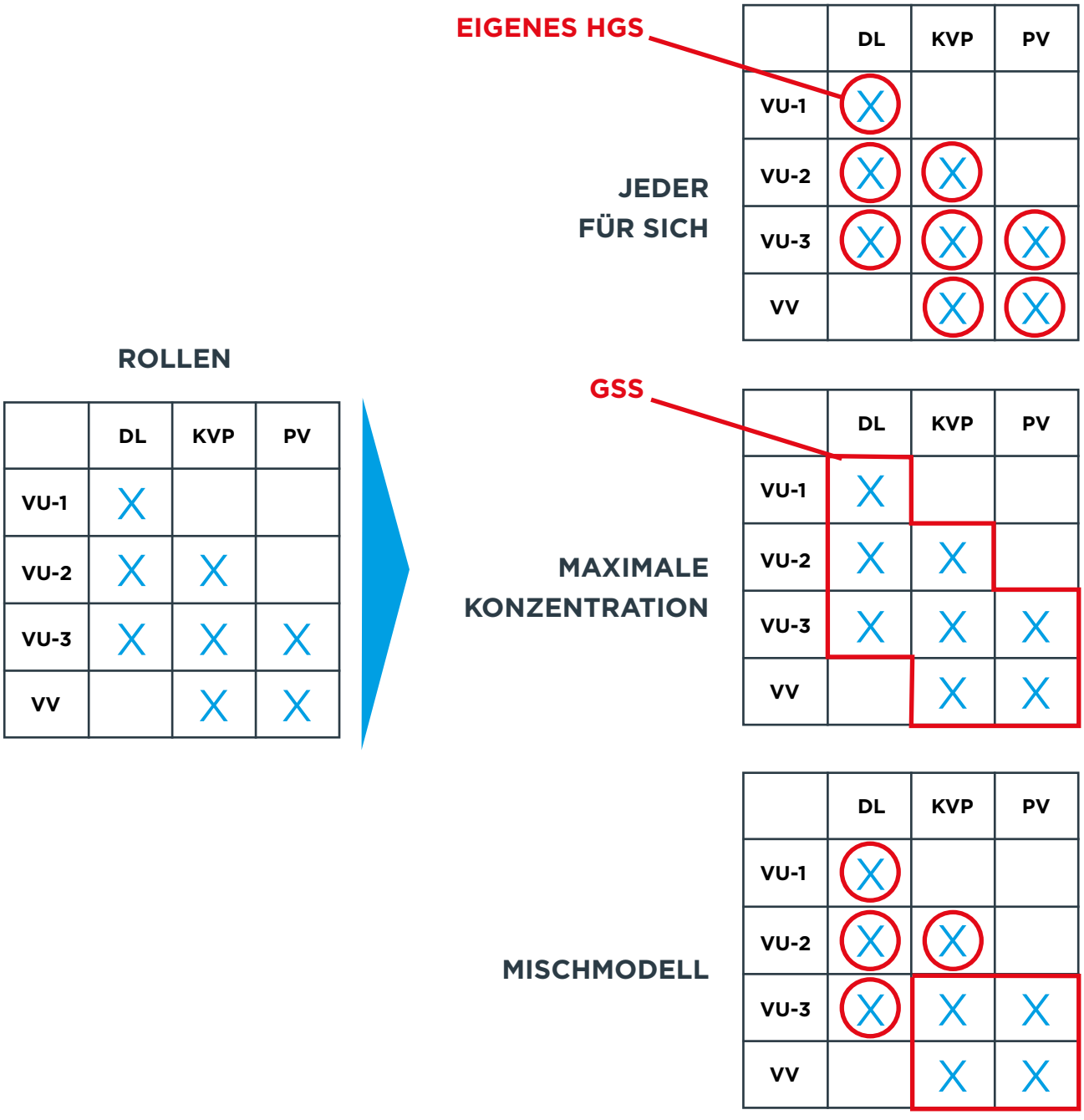

Abbildung 3: Drei Grundmodelle zur systemischen Umsetzung

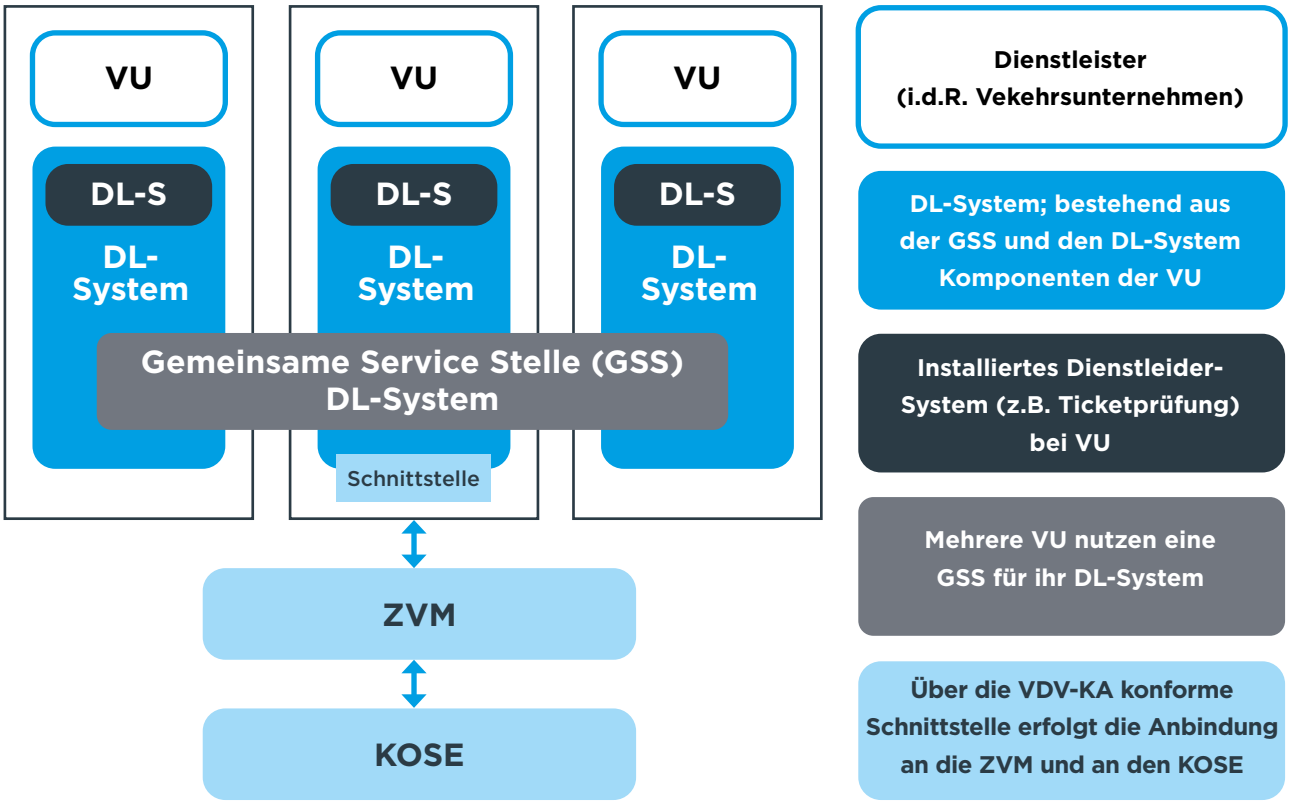

Abbildung 4: Modell einer GSS für ein DL-System für drei VU

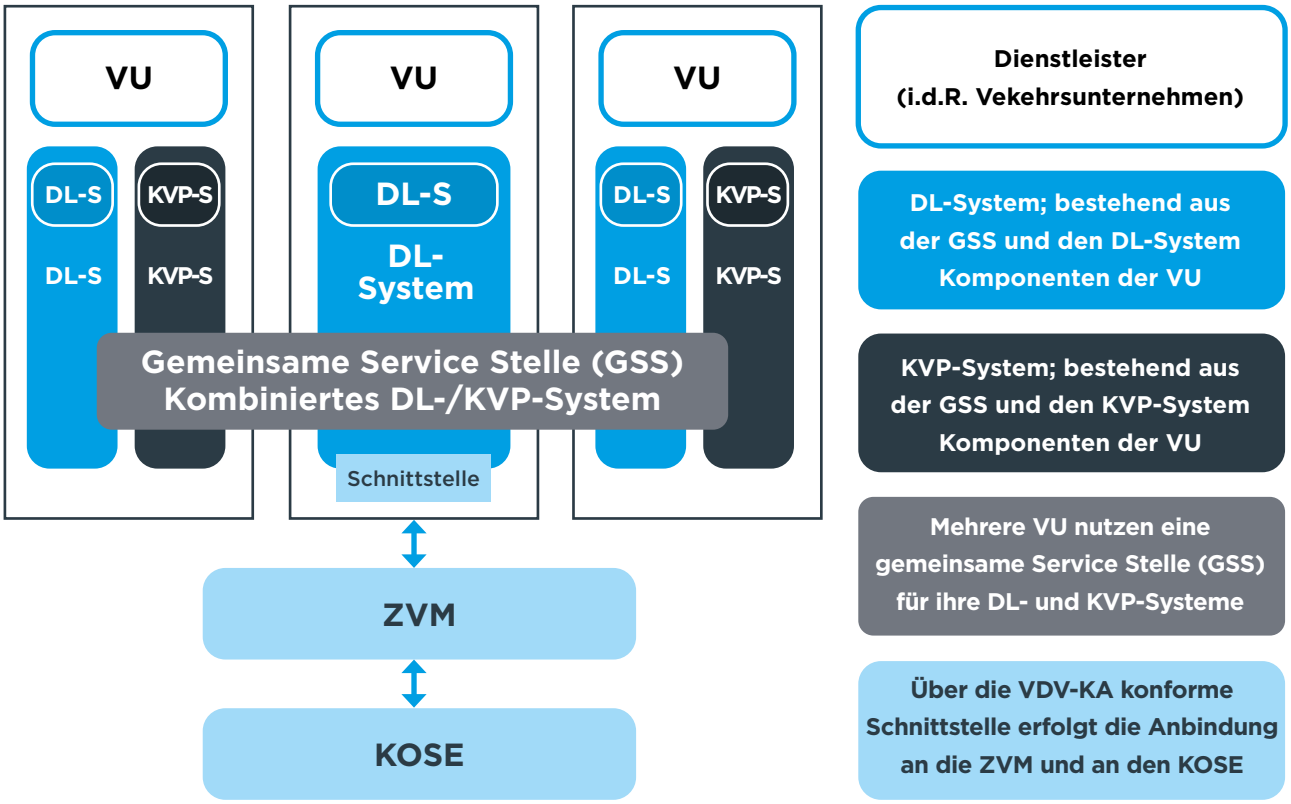

Abbildung 5: Modell einer GSS für das DL- und KVP-System mehrerer VU mit verschiedenen Rollen

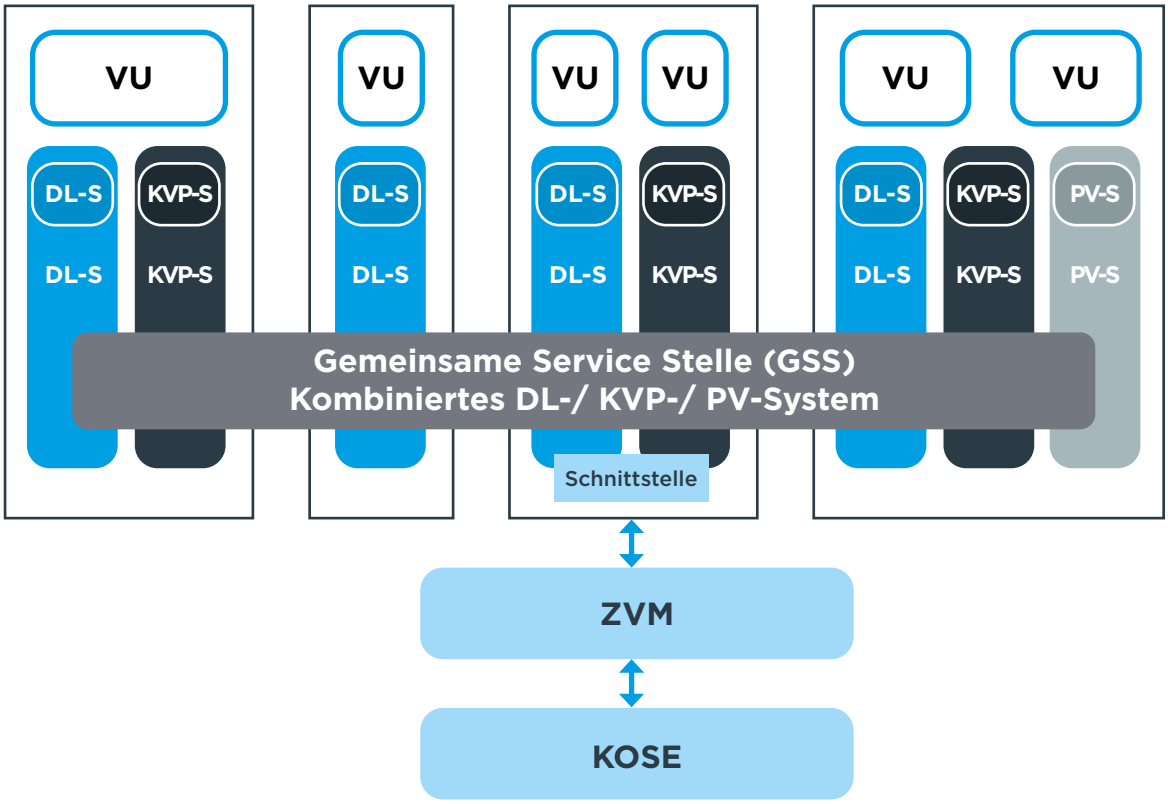

Abbildung 6: Modell einer GSS für das DL-, KVP- und PV-System für mehrere VU und VV mit verschiedenen Rollen

HERAUSGEBER

VDV eTicket Service GmbH & Co. KG
Im Mediapark 8a
50670 Köln

Tel: 0049 221 716174 0
Fax: 0049 221 716174 123
E-Mail: info@eticket-deutschland.de

Veröffentlicht 19. Januar 2015