KCEFM » KOMPETENZCENTER
ELEKTRONISCHES
FAHRGELDMANAGEMENT NRW

VRR

Migration zur VDV-Kernapplikation

Rahmenlastenheft
Anpassung
Personalisierungsgeräte

KCEFM » KOMPETENZCENTER
ELEKTRONISCHES
FAHRGELDMANAGEMENT NRW

VRR

0 Allgemeines

0.1 Inhaltsverzeichnis

Kapitel **Seite**

0 Allgemeines 2
0.1 Inhaltsverzeichnis 2
0.2 Änderungsverzeichnis 2
1 Einleitung 3
2 Struktur der Anpassung der Personalisierungsgeräte 3
3 Anpassung der Prozesse der Personalisierungsgeräte 4
4 Bedienung Schnittstellen 5
5 Wichtige Hinweise 5
6 Referenzen 6

0.2 Änderungsverzeichnis

Die Version 1_5 unterscheidet sich von der Version 1_4 durch die folgenden Änderungen:

Kapitel 3, zweiter Absatz, Mitte:	Es wurde ein wichtiger Hinweis bezüglich der Authentisierung zwischen Terminal und SAM ergänzt.
Kapitel 6:	Die Referenzen wurden aktualisiert.

1 Einleitung

Ab Anfang 2003 haben die Verkehrsunternehmen im VGN/VRR/VRS ihre Abonnement-Tickets auf elektronische Fahrscheine umgestellt. Als Trägermedium für den Kunden dient eine Prozessor-Chipkarte mit dem Datenmodell *EFS-Manager ÖPV* des VDV. Zum Start des elektronischen Fahrgeldmanagements im VGN/VRR/VRS und in der Folgezeit wurden insgesamt circa drei Millionen Chipkarten beschafft.

Die Verkehrsunternehmen haben nun die Weiterentwicklung des bestehenden Systems gefordert. Um dieser Forderung gerecht zu werden, hat das KC EFM für die jetzt anstehende Chipkartenausschreibung die verschiedenen Möglichkeiten untersucht. Als zu erfüllender technischer Standard für die Ausschreibung wurde die *VDV-Kernapplikation* des VDV gewählt, weil nur die Anwendung eines allgemeinen offenen (und damit für alle Hersteller zugänglichen) Standards als Rahmenbedingung für eine Ausschreibung vergaberechtlich zulässig ist und zugleich langfristig das technische Zusammenspiel (Kompatibilität) mit dem Gesamtsystem sichert. Der einzige derzeit verfügbare Standard dieser Art ist die *VDV-Kernapplikation* des VDV.

Als Konsequenz aus dieser Entscheidung müssen die im Einsatz befindlichen Terminals nicht nur für die neue Chipkarte erweitert werden sondern sie müssen auch die unterschiedlichen Datenformate konvertieren. Bei den Kontrollgeräten und weiterhin verwendeten Personalisierungsgeräten kann dies durch entsprechende Maßnahmen durchgeführt werden. In einigen Regionen müssen die Personalisierungsgeräte für die Ticketausgabe jedoch neu beschafft werden, da in Zukunft dort eine rein kontaktlose Chipkarte eingesetzt wird. Diese Personalisierungsgeräte können mit einer definierten offenen Software-Schnittstelle kompatibel zur *VDV-Kernapplikation* ausgerüstet werden.

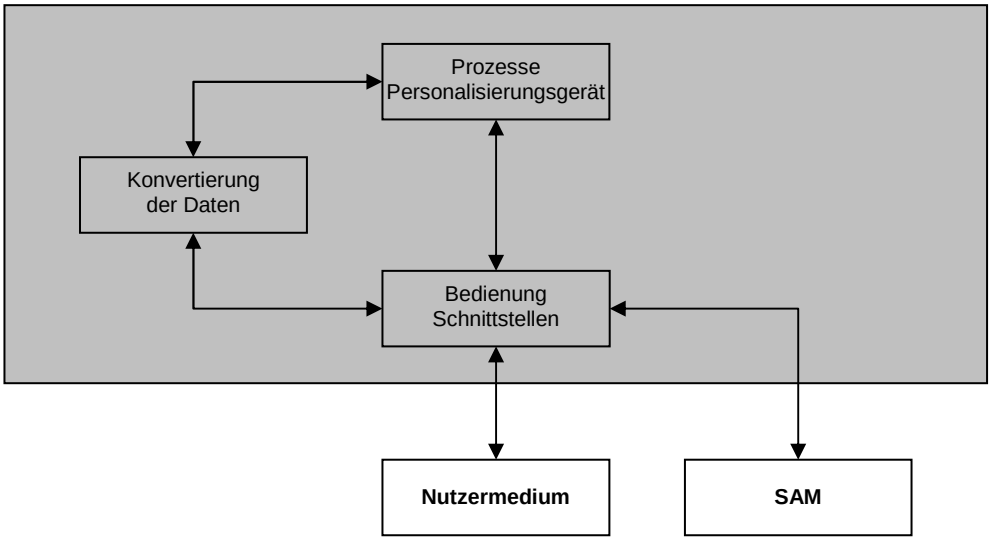
In dem vorliegenden Rahmenlastenheft werden die zu realisierenden Funktionen im Rahmen der Anpassung der weiterhin verwendeten Personalisierungsgeräte beschrieben. Da es sich bei diesem Rahmenlastenheft ausschließlich um eine reine Funktions- und Schnittstellenbeschreibung handelt, kann es nur Teil einer kompletten Ausschreibungsunterlage sein. Dies ist entsprechend zu berücksichtigen.

2 Struktur der Anpassung der Personalisierungsgeräte

Die Anpassung besteht, wie die unten stehende Abbildung zeigt, im Prinzip aus drei Teilen:

- Anpassung der Prozesse der Personalisierungsgeräte an die Gegebenheiten der VDV-Kernapplikation
- Konvertierung der Daten zwischen dem KA-Datenmodell (NRW-KA-EFS) und dem Datenmodell *EFS-Manager ÖPV* (NRW-EFS)
- Bedienung der Schnittstellen zum Nutzermedium und zum SAM

Dabei werden nicht immer Daten konvertiert. Zum Beispiel werden allgemeine Kommandoprozeduren angepasst direkt weitergeleitet.



3 Anpassung der Prozesse der Personalisierungsgeräte

Da eine genaue Beschreibung der Anpassung dieser Geräte in diesem Fall detaillierte Kenntnisse der zur Zeit eingesetzten Software erfordert, kann in diesem Rahmenlastenheft nur auf die grundsätzlich umzusetzenden Maßnahmen eingegangen werden.

Bei der *VDV-Kernapplikation* muss sich das Terminal also das Personalisierungsgerät gemäß [5] gegenüber dem SAM authentisieren. Hierzu wird in dem SAM ein öffentlicher Betreiberschlüssel gespeichert. Der für die Authentisierung erforderliche private Betreiberschlüssel muss an einem Ort abgelegt werden, der vom Terminal erreichbar ist. Dieser Ort sollte der Bedeutung des Schlüssels entsprechend sicher sein. Nähere Hinweise hierzu können [7] entnommen werden. Im Rahmen dieser Authentisierung muss das Terminal die Echtheit des SAM's überprüfen. Hierzu ist im Terminal der zertifizierte öffentliche Schlüssel der Root zu speichern. Eine entsprechende Lösung ist mit den Betreibern der Personalisierungsgeräte abzustimmen. Durch einen RESET des SAM's nach jeder Ausgabe einer Berechtigung kann diese Authentisierung immer wieder erzwungen werden, um so die Sicherheit weiter zu erhöhen. Ob diese Möglichkeit implementiert werden soll, ist mit den Betreibern der Personalisierungsgeräte abzustimmen.

Im Rahmen der Ausgabe einer Berechtigung ist bei den symmetrischen Schlüsseln mit Ausname des Schlüssels des Produktverantwortlichen die jeweils aktuellste nicht gesperrte Generation also die höchste vorhandene Generationsnummer zu verwenden. Die zu verwendende Generation des Schlüssels des Produktverantwortlichen ist dem jeweiligen Produkt-Modul zu entnehmen. Die Umschaltung auf die Notfallversion muss für jeden betroffenen symmetrischen Schlüssel einzeln und für alle zusammmen im Rahmen einer Serviceoperation an den Terminals also den Personalisierungsgeräten möglich sein.

Im Rahmen von Serviceoperationen an den Terminals also den Personalisierungsgeräten müssen offline neue Schlüssel mit dem Kommando *LoadKey* in das SAM geladen werden können (siehe auch [5] und [8]). Hierzu werden vom Sicherheitsmanagemant der *VDV-Kernapplikation* entsprechende Kryptogramme zur Verfügung gestellt. Eine entsprechende Lösung ist dann mit den Betreibern des Kontrollgerätes unter Einbeziehung des Sicherheitsmanagementes der *VDV-Kernapplikation* und des KC EFM abzustimmen.

Ein SAM der VDV-Kernapplikationkann grundsätzlich mehrere Produktverantwortliche (PV) und Kundenvertragspartner (KVP) unterstützen (siehe auch [5]). Die jeweils zu verwendenden Schlüssel ergeben sich aus den Daten der auszugebenden Berechtigung. Darüber hin-

aus könne auch mehrere Erfassungsschlüssel ($MK_{ERF\_KM\_MAC}$) vorhanden sein. Der jeweils zu verwendende Erfassungsschlüssel kann ebenfalls den Daten der auszugebenden Berechtigung entnommen werden.

Die Personalisierungsgeräte bekommen vom ansteuernden Hintergrundsystem zur Zeit die folgenden Aufträge:

- Schreiben (gesichert)
- Lesen (gesichert/ungesichert)
- Markieren
- Löschen
- Rückdatieren (Änderung der zeitlichen Gültigkeit)

Die Umsetzung dieser Aufträge muss nun an das Nutzermedium und das SAM der *VDV-Kernapplikation* angepasst werden. Bei der Konvertierung der Daten sind die Konvertierungsregeln in [1] zu beachten. Die Variante *Rückdatieren* des Auftrages *6.11 Löschen* gemäß [2] ist durch das Löschen des alten und Schreiben eines neuen Tickets unter Berücksichtigung des Verhältnisses zwischen Verfallsdatum und Ende der zeitliche Gültigkeit gemäß [1] umzusetzen. Die Administrierung der SAM's gemäß [2] ist in der *VDV-Kernapplikation* nicht ausführbar.

Letztendlich muss es das Ziel sein, sobald wie möglich wieder mit den vorhandenen Datenstrukturen arbeiten zu können.

4 Bedienung Schnittstellen

Die Schnittstelle zum Nutzermedium ist in [4] und die zum SAM in [5] und [6] beschrieben. Wenn das Personalisierungsgerät um eine kontaktlose Schnittstelle gemäß ISO/IEC 14443 erweitert wird, ist auch [3] zu beachten.

5 Wichtige Hinweise

Bei der Anpassung der Personalisierungsgeräte ist in den Hintergrundsystemen gegebenenfalls sicherzustellen, dass die folgenden durch die VDV-Kernapplikation bedingten Sachverhalte berücksichtigt werden:

- Die Aufträge, die nicht ausführbar sind, dürfen entweder durch das Hintergrundsystem nicht abgesetzt werden oder es müssen die Rückmeldungen entsprechend verarbeitet werden, so dass es nicht zu Fehlfunktionen im Hintergrundsystem kommt.
- Wenn Chipkarten nicht im Thermo-ReWrite-Verfahren bedruckt werden können, muß diese Problematik entsprechend berücksichtigt werden.
- Die Variante *Rückdatieren* des Auftrages *6.11 Löschen* der S&B-Schnittstelle ist bei der VDV-Kernapplikation direkt nicht umsetzbar, da es dort im Gegensatz zum zur Zeit verwendeten Datenmodell das betroffene Feld *Verfallszeitpunkt* nicht gibt. Diese Variante macht alleine eigentlich keinen Sinn, wird aber zur Zeit zum einfachen Begrenzen der zeitlichen Gültigkeit eines Tickets verwendet und wird in das Löschen des alten und Schreiben eines neuen Tickets umgesetzt.

- Das Feld bEFMActTicketCounter der S&B-Schnittstelle wird zur Zeit nur beim Schreiben eines Tickets bzw. beim Überschreiben eines Records mit dem Initialrecord erhöht. Bei der VDV-Kernapplikation wird der vergleichbare Wert EF_Transaktionszähler / SamSequenznummer bei jeder Transaktion (Schreiben, Markieren, Löschen) um 1 erhöht. Das Hintergrundsystem muss, wenn es diesen Wert weiterhin zu Kontrollzwecken auswerten soll, diese Veränderung entsprechend berücksichtigen.

6 Referenzen

Bei den Referenzen sind die zum Zeitpunkt der Erstellung dieses Dokumentes aktuellen Versionen angegeben. Letztendlich sind aber die zum Zeitpunkt der Realisierung aktuellen Versionen verbindlich.

[1] Migration zur VDV-Kernapplikation, Aufbau des NRW-KA-EFS und Konvertierungsregeln, Version 1_6, KompetenzCenter Elektronisches Fahrgeldmanagement NRW

[2] Schnittstellenspezifikation Hintergrundsystem – Initialisierungsgerät zum Projekt EFM-VRR-VRS, Version 1.41, Scheidt&Bachmann GmbH

[3] VDV-Kernapplikation, Systemlastenheft, Anforderungen an das Nutzermedium, Version 1.11

[4] VDV-Kernapplikation, Spezifikation Nutzermedium, Version 1.103

[5] VDV-Kernapplikation, Spezifikation des SAM, Version 1.103

[6] VDV-Kernapplikation, Ergänzung zur Spezifikation des SAM, Version 1.5

[7] VDV-Kernapplikation, Technisches Konzept Sicherheit, Version 1.001

[8] VDV-Kernapplikation, Systemlastenheft, Stationäre personalbediente KVP-Terminals, Version 1.11