KCEFM » KOMPETENZCENTER
ELEKTRONISCHES
FAHRGELDMANAGEMENT NRW

Migration zur VDV-Kernapplikation

Rahmenlastenheft
Kontaktloses
Personalisierungsgerät

KCEFM » KOMPETENZCENTER
ELEKTRONISCHES
FAHRGELDMANAGEMENT NRW

0 Allgemeines

0.1 Inhaltsverzeichnis

Kapitel **Seite**

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 könnten mit einer definierten offenen Software-Schnittstelle kompatibel zur *VDV-Kernapplikation* ausgerüstet werden.

In dem vorliegenden Rahmenlastenheft werden die grundlegenden Eigenschaften und die mindestens zu realisierenden Funktionen eines kontaktlosen Personalisierungsgerätes beschrieben. Da es sich bei diesem Rahmenlastenheft ausschließlich um eine reine Funktionsbeschreibung handelt, kann es nur Teil einer kompletten Ausschreibungsunterlage sein. Dies ist entsprechend zu berücksichtigen.

2 Allgemeines

Das komplette Personalisierungsgerät besteht aus bis zu drei Komponenten:

- Chip-Personalisierungsgerät
- gegebenenfalls Drucker für Chipkartenaufdruck
- gegebenenfalls Stapel/Magazin

Dabei ist zu beachten, dass das hier angesprochene Personalisierungsgerät in der *VDV-Kernapplikation* konkret nicht berücksichtigt wird. Dies ist darin begründet, dass ein Personalisierungsgerät, wie es hier beschrieben ist, zusammen mit der Software des Arbeitsplatzrechners, an den es angeschlossen ist, ein KVP(Kundenvertragspartner)-Terminal bildet. Es handelt sich im Sinne der *VDV-Kernapplikation* also um eine interne Teilkomponente des KVP-Terminals. Die Anforderungen an dieses KVP-Terminal sind in [1] beschrieben. Aus diesem Dokument sind die Anwendungsfälle zum EFS sowie die Kommunikationsschnittstellen und die technischen Anforderungen zu berücksichtigen.

Die Kommunikation mit der ansteuernden Software also mit dem Hintergrundsystem oder dem Konverter, die alle drei Komponenten umfasst, ist zumindest unter Berücksichtigung von [2] zu realisieren.

3 Chip-Personalisierungsgerät

Die Komponente Chip-Personalisierungsgerät übernimmt die Kommunikation mit dem Nutzermedium über eine kontaktlose Schnittstelle gemäß [3] und [4] sowie mit dem SAM gemäß [5] und [6]. Aufgabe dieser Komponente ist es, die Transaktionsklassen oder Kommandos hinsichtlich des EFS in eine entsprechende Kommunikation mit dem Nutzermedium und dem SAM umzusetzen, also letztendlich Elektronische Tickets zu lesen, zu schreiben, zu sperren und zu löschen.

Bei der *VDV-Kernapplikation* muss sich das Terminal also das Personalisierungsgerät gemäß [5] gegenüber dem SAM authentifizieren. Hierzu wird in dem SAM ein öffentlicher Betreiberschlüssel gespeichert. Der für die Authentifizierung 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 [1]). 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 hinaus könne auch mehrere Erfassungsschlüssel ($MK_{ERF\_KM\_MAC}$) vorhanden sein. Der jeweils zu verwendende Erfassungsschlüssel kann ebenfalls den Daten der auszugebenden Berechtigung entnommen werden.

4 Drucker für Chipkartenaufdruck

Die Komponente Drucker für Chipkartenaufdruck sollte die folgenden Mindestanforderungen erfüllen:

- Druck einer monochromen Bitmap über die gesamte Chipkartenrückseite sowie über ESC-Sequenzen gesteuerte Textausgabe gemäß [2]

- Thermotransfer- oder Thermosublimationsdruck

Näheres hierzu ist den übrigen Ausschreibungsunterlagen zu entnehmen.

5 Stapel/Magazin

Gegebenenfalls verfügt das Gerät über einen oder mehrere Stapel bzw. Magazine. Die in diesem Fall erforderlichen Ansteuerungen können [2] entnommen werden.

Näheres hierzu ist den übrigen Ausschreibungsunterlagen zu entnehmen.

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

[2] Migration zur VDV-Kernapplikation, Schnittstelle Personalisierungsgerät - Hintergrundsystem, Version 1_10, KompetenzCenter Elektronisches Fahrgeldmanagement NRW

[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