eTicket Service

Kontrolle

# Kontrollnachweise bei Elektronischen Fahrscheinen

Version: 1.0

Datum: 22.11.2017

Autor [redacted]

# Inhaltsverzeichnis

# 1 Einleitung

Bei der Kontrolle von Elektronischen Fahrscheinen (EFS) als (((eTicket oder VDV-Barcode sollen gemäß der Spezifikation der VDV-Kernapplikation von den Kontrollgeräten (DL-Terminals) Kontrollnachweise (TXEBER/TXEMBER) erzeugt werden. Diese werden bei einem (((eTicket als Fahrttransaktion auf der Chipkarte in der Berechtigung und im Applikationslogbuch gespeichert und über das DL-System als TXEBER/TXEMBER an das PV-System und von dort an das KVP-System zur weiteren Überprüfung weitergeleitet. Bei einem VDV-Barcode wird nur ein TXESTBER erzeugt und an das PV-System und von dort an das KVP-System zur weiteren Überprüfung weitergeleitet. Kontrollnachweise werden immer dann erzeugt, wenn ein EFS als (((eTicket oder VDV-Barcode für die tarifliche Kontrolle ausgelesen wird und im Ergebnis authentisch, nicht gesperrt und zeitlich gültig und im Falle einer (teil)automatisierten tariflichen Prüfung tariflich gültig ist. Die Ergebnisse nachfolgender manueller tariflicher Prüfungen wie z. B. die Prüfung auf persönliche Gültigkeit aber auch die komplette manuelle tarifliche Prüfung verhindern nicht mehr die Erzeugung eines Kontrollnachweises.

Die Kontrollnachweise stellen ein – beim (((eTicket mit einem MAC (Message Authentication Code / Prüfzahl) abgesichertes – authentisches „Lebenszeichen“ eines EFS dar. Sie dienen der Überprüfung der Funktionalität und der Sicherheit eines gesamten EFM-Systems, das der VDV-Kernapplikation entspricht.

Das Sicherheitssystem der VDV-Kernapplikation besteht aus zwei Teilen. Der erste Teil umfasst Sicherheitsfunktionen wie z. B. die oben erwähnte MAC-Bildung. Im Rahmen des zweiten Teils dem Monitoring in den Hintergrundsystemen (KVPS und PVS) werden diese Sicherheitsfunktionen ausgewertet.

Die Kontrollnachweise werden dazu im Rahmen des Monitorings verschiedenen Prüfungen unterzogen (siehe Kapitel 2). Dies ist der Geschäftszweck aufgrund dessen Kontrollnachweise erzeugt werden.

Die Erzeugung von Bewegungsprofilen gehört nicht zu diesem Geschäftszweck. Die PV- und KVP-Systeme sind auch nicht darauf ausgelegt. Die Kontrollnachweise sind auch für die tarifliche Kontrolle ohne Bedeutung, sie werden nur in diesem Zusammenhang erzeugt.

Für die Kontrollnachweise wird die Datenstruktur „Fahrttransaktion“ verwendet. Diese Datenstruktur wird für die Weiterleitung an das PV- und KVP-System um einen Adressteil

für den Versand (TXBASE in TXEBER, TXEMBER und TXESTBER) sowie bei TXEBER/TXEMBER um den PV- und KVP-MAC und bei TXESTBER um die Signatur des VDV-Barcodes ergänzt.

# 2 Transaktionsprüfungen

Das Sicherheitssystem der VDV-Kernapplikation ist aufwendig gestaltet, um den Schutz der Interessen der Teilnehmer zu gewährleisten. Das Sicherheitssystem besteht zum einen aus kryptografischen Funktionen sowie diversen abgesicherten und nicht abgesicherten Zählern und zum anderen aus Prüfungen, denen die verschiedenen Datensätze unterzogen werden. Ohne diese Prüfungen kann nicht festgestellt werden, ob Funktionalität und Sicherheit des EFM-Systems gegeben und die Komponenten des Sicherheitssystems ausreichend sicher sind. Die Prüfungen werden mit einem zeitlichen Nachlauf durchgeführt.

Die Kontrollnachweise werden gemäß dem Dokument KA TXx_Prüfungs-ANW (Dateiname ANW_Transaktionsprüfung_Vyxz.pdf) den folgenden Prüfungen unterzogen. Kapitel, die mit einer 3 beginnen, beschreiben Prüfungen des PV. Kapitel, die mit einer 4 beginnen, beschreiben Prüfungen des KVP. Kapitel, die mit einer 5 beginnen, beschreiben Prüfungen des DL.

## 2.1 Prüfung 1: Ausgabetransaktion vorhanden?

- KA TXx_Prüfungs-ANW Kapitel 3.2.1 Prüfung: Ausgabetransaktion TXABER/TXAMBER/TXASTBER liegt vor
- KA TXx_Prüfungs-ANW Kapitel 4.2.17 Prüfung Ausgabetransaktion vorhanden

Ist eine Ausgabetransaktion zu diesem EFS vorhanden? Wenn nein, ist dieser EFS illegal erzeugt worden oder es liegt ein Fehler im Gesamtsystem vor. Diese Prüfung ist insbesondere bei der Anwendung des Aktionsmanagements (ALISE) von Bedeutung, da hierfür der KVP-Schlüssel auch an andere Unternehmen verteilt werden muss.

## 2.2 Prüfung 2: Zeitliche Gültigkeit

- KA TXx_Prüfungs-ANW Kapitel 3.2.10 Prüfung: Zeitpunkt der Transaktionsausführung liegt innerhalb der im TXABER/TXAMBER/TXASTBER übermittelten zeitlichen Gültigkeit

Ist die Kontrolltransaktion innerhalb der zeitlichen Gültigkeit der Berechtigung durchgeführt worden und ist dabei eine eventuelle vorzeitige Rücknahme der Berechtigung berücksichtigt worden? Wenn nein, ist dieser EFS illegal erzeugt worden oder es liegt ein Fehler im Gesamtsystem vor.

## 2.3 Prüfung 3: Lückenlosigkeit der Transaktionen

- KA TXx_Prüfungs-ANW Kapitel 3.2.4 Prüfung: berLogSeqNummer
- KA TXx_Prüfungs-ANW Kapitel 4.2.10 Prüfung: berLogSeqNummer

Ist die berLogSeqNummer lückenlos und liegen somit alle Transaktionen zu diesem EFS vor? Wenn nein, liegt ein Fehler im Gesamtsystem vor. Beim VDV-Barcode gibt es eine Ausnahme. Hier ist dieser Wert auf 1 eingefroren, was entsprechend überprüft werden muss.

## 2.4 Prüfung 4: Signaturprüfung

- KA TXx_Prüfungs-ANW Kapitel 3.2.6 Signaturprüfung aller eingehenden Transaktionen TXx
- KA TXx_Prüfungs-ANW Kapitel 4.2.1 Signaturprüfung aller eingehenden Transaktionen TXx

Sind der PV- und der KVP-MAC korrekt? Wenn nein, ist dieser EFS illegal erzeugt worden oder es liegt ein Fehler im Gesamtsystem vor. Diese Prüfung wird im PVS und KVPS mit den ergänzten Daten ($MAC_{PV}$ und $MAC_{KVP}$, siehe Kapitel 1) durchgeführt. Daran können PV und KVP jeweils an ihrem MAC erkennen, dass diese Transaktion zwischen einem authentischen NM und einem authentischen SAM durchgeführt wurde. Insbesondere im Zusammenspiel mit der Prüfung, ob eine Ausgabetransaktion vorhanden ist und dies nicht der Fall ist, kann hier bei korrekten MACs auf ein illegal genutztes SAM geschlossen werden.

## 2.5 Prüfung 5: Prüfung gegen Sperrliste

- KA TXx_Prüfungs-ANW Kapitel 3.2.7 Prüfung von Datenelementen in eingehenden Transaktionen TXx gegen Sperrlisten
- KA TXx_Prüfungs-ANW Kapitel 3.2.11 Prüfung: Transaktion für gesperrte Berechtigung wird eingereicht
- KA TXx_Prüfungs-ANW Kapitel 4.2.14 Prüfung von Datenelementen in eingehenden Transaktionen TXx gegen Sperrlisten

Sind Datenelemente der Kontrolltransaktion auf einer Sperrliste? Wenn ja, liegt ein Fehler oder interner Betrugsversuch im Gesamtsystem vor. Es wurde eine Kontrolltransaktion eingereicht, die auf Grund von Sperreinträgen in einer Sperrliste oder auf Grund des im PVS vermerkten Status am Terminal nicht hätte ausgeführt werden dürfen. Man kann hier auch einzelne Terminals identifizieren, welche aus irgendwelchen Gründen nicht die richtige Sperrliste verarbeiten.

## 2.6 Prüfung 6: Prüfung der Transaktionsorte und Transaktionszeitpunkte

- KA TXx_Prüfungs-ANW Kapitel 3.2.3 Prüfung: Transaktionszeit/Transaktionsort für alle TXx

Sind Transaktionszeit und Transaktionsort plausibel? Wenn nein, ist bei einer Chipkarte eine Fälschung des EFS oder ein fehlerhaft ausgegebener EFS im Umlauf. Beim VDV-Barcode bedeutet dies, dass eine Kopie des EFS oder ein fehlerhaft ausgegebener EFS im Umlauf ist. Diese Prüfung ist wegen der Kopierfähigkeit des VDV-Barcodes von entscheidender Bedeutung für die Systemsicherheit. Bei einem VDV-Barcode kann auch eine ungewöhnlich häufige Kontrolle ein Hinweis auf die illegale mehrfache Nutzung eines regulären nicht kopierten Fahrscheins darstellen.

Transaktionszeit und Transaktionsort sind dann plausibel, wenn vorhergehende oder nachfolgende Transaktionen zu gleichen oder geringfügig differierenden Zeitpunkten an unterschiedlichen Terminals nicht an weit auseinanderliegenden Orten stattgefunden haben. Hierzu ist eine Ortsangabe erforderlich, die für ein Bewegungsprofil zu ungenau und für die Plausibilitätsprüfung genau genug ist. Daher wird hier das Datenelement logTransaktionsOrt_ID in den Allgemeinen Transaktionsdaten benutzt. Es wird einheitlich

die jeweilige Tarifhaltestelle eingetragen. Die genauen Vorgaben dazu muss der PV machen.

Als Ergebnis steht zusammen mit dem Inhalt des logTransaktionsZeitpunkt in den Allgemeinen Transaktionsdaten und der berBerechtigung_ID für eine Auswertung die Information zur Verfügung, dass der EFS x am Ort y zum Zeitpunkt z angetroffen wurde. Nun kann das System automatisiert überprüfen, ob zu einer Berechtigung in einem vorgegebenen Zeit-fenster (z. B. 1 Tag) mehr als n (z. B. 5) TXEBER, TXEMBER bzw. TXESTBER eingegangen sind und dies auch noch zeitlich eng (z. B. bis zu 1 Stunde) beieinander liegen. Sollte dies der Fall sein, können z. B. mit Hilfe der Technischen Adresse manuell weitere Analysen erfolgen.

# 3 Datenstruktur „Fahrttransaktion“

Die Datenstruktur „Fahrttransaktion“ besteht aus den „Allgemeinen Transaktionsdaten“, dem „Transaktion Produktspezifischen Teil“ und den „Allgemeinen Fahrttransaktionsdaten“. Im Folgenden werden die Ausprägung als Kontrollnachweis bei EFS und die auszuführenden Prüfungen beschrieben.

## 3.1 Allgemeine Transaktionsdaten

Die allgemeinen Transaktionsdaten, die eine technische Adresse darstellen, beschreiben

- wer (logTransaktionsOperator_ID),
- wann (logTransaktionsZeitpunkt),
- welche Transaktion (logTransaktionsTyp.code) durchgeführt hat und
- die wievielte Transaktion das mit dieser Applikation/Chipkarte war (logApplikationSeqNummer).

Außerdem werden folgende Elemente genutzt:

- der Ort (logTransaktionsOrt_ID), an dem die Transaktion durchgeführt wurde (siehe auch Kapitel 2.6),
- das Terminal (logTerminal_ID), das die Transaktion durchgeführt hat und
- das SAM (logNmTransaktion_ID), das die Transaktion durchgeführt hat.

## 3.2 Transaktion Produktspezifischer Teil

Der Transaktion Produktspezifische Teil enthält bei den derzeit genutzten Strukturen für die Abbildung von Tarifprodukten als EFS (TLV EFS) keine Daten. Letztendlich wird aber die verwendete Struktur und damit der Inhalt des Transaktion Produktspezifische Teils vom PV spezifiziert.

## 3.3 Allgemeine Fahrttransaktionsdaten

Die allgemeinen Fahrttransaktionsdaten beschreiben

- mit welchem EFS (berBerechtigung_ID), der ein bestimmtes Tarifprodukt (prodProdukt_ID) abbildet, die Kontrolltransaktion durchgeführt wurde und
- die wievielte Transaktion das mit diesem EFS war (berLogSeqNummer).
- Die Datenelemente berLogLinieVariante_ID, berLogFahrt_ID, Fahrtabschnitttransaktion–Fahrtbeginn und Fahrtabschnitttransaktion–Vorgaenger werden bei Kontrollnachweisen nicht benutzt und daher mit 0x00 gefüllt.
- Die Datenelemente $MAC_{Kontrolle}$ und Version $K_{Kontrolle}$ sichern die Kontrolltransaktion ab und werden im Rahmen der nächsten Transaktion überprüft.

## 3.4 Detailübersicht und Prüfungen

Die folgende Tabelle gibt eine Übersicht über die verwendete Datenstruktur mit ihren einzelnen Datenelementen und den mit ihnen durchgeführten Prüfungen im PV- und KVP-System. Der Inhalt der Datenelemente ist in den Kapiteln 3.1, 3.2 und 3.3 und die Prüfungen sind im Kapitel 2 beschrieben.

Mit Negativfall ist in der folgenden Tabelle das negative Ergebnis bei einer der beschriebenen Prüfungen gemeint.

| Datenelemente | | | Prüfung |
|---|---|---|---|
| Allgemeine Transaktionsdaten | | logApplikationSeqNummer | Fehleranalyse bei Chipkarten |
| | logNmTransaktion_ID | SamSequenznummer | Kapitel 2.5 |
| | | SAM_ID.samNummer | Kapitel 2.5 |
| | | logTransaktionsOperator_ID | Kapitel 2.5 |

| Datenelemente | | | Prüfung |
|---|---|---|---|
| | logTerminal_ID | terminalTyp.code | Generell im Negativfall |
| | | terminalNummer | Generell im Negativfall |
| | | Organisation_ID.organisationsNummer | Generell im Negativfall |
| | | logTransaktionsZeitpunkt | Kapitel 2.2 und 2.6 |
| | logTransaktionsOrtID | ortTyp.code | Kapitel 2.6 |
| | | OrtNummer | Kapitel 2.6 |
| | | Organisation_ID.organisationsNummer | Kapitel 2.6 |
| | | logTransaktionsTyp.code | Prüfung, ob Code für Kontroll-nachweis |
| Transaktion Produkt-spezifischer Teil | | wird vom PV-spezifiziert | wird vom PV spezifiziert |

| Datenelemente | | | Prüfung |
|---|---|---|---|
| Allgemeine Fahrttransaktionsdaten | | berLogSeqNummer | Kapitel 2.3 |
| | berBerechtigung_ID | berechtigungNummer | Kapitel 2.1 und 2.5 |
| | | Organisation_ID.organisationsNummer | Kapitel 2.1 und 2.5 |
| | prodProdukt_ID | produktNummer | Kapitel 2.1 |
| | | Organisation_ID.organisationsNummer | Kapitel 2.1 und 2.5 |
| | berLogLinieVariante_ID | Linie_ID.linienNummer | Kein Inhalt |
| | | VariantenNummer | Kein Inhalt |
| | berLogFahrt_ID | fahrtNummer | Kein Inhalt |
| | | Organisation_ID.organisationsNummer | Kein Inhalt |
| | Fahrtabschnitttransaktion-Fahrtbeginn | logTransaktionsZeitpunkt | Kein Inhalt |
| | | berLogHaltestelle_ID (Struktur „Ort_ID“) | Kein Inhalt |
| | | berLogSeqNummerFahrtbeginn | Kein Inhalt |
| | Fahrtabschnitttransaktion-Vorgaenger | logTransaktionsZeitpunkt | Kein Inhalt |
| | | berLogHaltestelle_ID (Struktur „Ort_ID“) | Kein Inhalt |
| | | $MAC_{Kontrolle}$ | Prüfung im Terminal |
| | | Version $K_{Kontrolle}$ | Kapitel 2.5 |

# 4 Datenschutzrechtliche Aspekte

Mit der Orts- und Zeitangabe in den Allgemeinen Transaktionsdaten kann prinzipiell ein Bewegungsprofil erstellt werden. Dies ist aber gesetzlich nicht zugelassen und auch nicht der Geschäftszweck. Darüber hinaus sollten die Daten der Kontrollnachweise im KVPS insbesondere von den Kundendaten separiert und der Zugriff restriktiv geregelt werden.

Es ist zu beachten, dass der Geschäftszweck für die Kontrollnachweise entfällt, wenn die oben beschriebenen Prüfungen aus welchen Gründen auch immer nicht umgesetzt werden. Darüber hinaus bedeutet das auch, dass das Sicherheitssystem nicht korrekt weil nicht komplett umgesetzt worden ist. Dies kann Einnahmenausfälle aufgrund von Betrug nach sich ziehen, da dieser nicht mehr erkannt wird. Des Weiteren sind Sonderlösungen bezüglich der Erzeugung oder der Weiterleitung der Kontrollnachweise erforderlich.

# 5 Löschfristen

Die Daten eines Kontrollnachweises können dann gelöscht werden, wenn alle Prüfungen durchgeführt wurden und das Ergebnis positiv ist. Einzig die berBerechtigung_ID, die prodProdukt_ID, die berLogSeqNummer und der logTransaktionsTyp.code bleiben gespeichert, um die Prüfung der berLogSeqNummer (siehe Kapitel 2.3) bei der nächsten Transaktion durchführen zu können und einen sauberen Datenbestand zur Berechtigung zu erhalten.

Wenn das Ergebnis negativ ist (Betrugsversuch, Systemfehler) muss eine im Regelfall manuelle Nachbehandlung erfolgen, die die Löschfrist verlängert.

Die Fristen müssen unter Berücksichtigung von Beschwerdefristen, der spätesten Lieferfristen der Kontrollnachweise und der Kapazitäten für die Nachbearbeitung insbesondere der Prüfung im Kapitel 2.6 für jedes EFM-System individuell festgelegt werden.