Verkehrsverbund Rhein-Ruhr
Elektronisches Fahrgeldmanagement

Administrierung der PayCard-Sicherheitsmodule

Version 1_0
Stand: 23.01.02

Verkehrsverbund Rhein-Ruhr GmbH

0 Allgemeines

0.1 Inhaltsverzeichnis

Kapitel **Seite**

0.2 Abbildungsverzeichnis

Abbildung **Seite**

1 Vorbemerkungen

Auf dem Gebiet des Verkehrsverbundes Rhein-Ruhr (VRR) soll (schrittweise) ein System für elektronisches Fahrgeldmanagement eingeführt werden. In der ersten Stufe soll dabei ein Fahrausweis in der Form eines Elektronischen Tickets in einer Chipkarte gespeichert werden. Als Chipkarte soll dabei unter anderem die PayCard von card.etc eingesetzt werden.

Die PayCard ist bereits für die Speicherung von Elektronischen Tickets vorbereitet. Sie bietet dafür eine Zusatzanwendung „eTicket“ kompatibel zu [1]. Zu dieser Zusatzanwendung gehören Datenstrukturen in der PayCard, die der Speicherung von Elektronischen Tickets dienen, und Sicherheitsmodule, die für den Zugriff auf die PayCard benötigt werden. Diese Sicherheitsmodule lassen sich administrieren. Für diese Administrationsaufgaben muss auf die Sicherheitsmodule kryptographisch abgesichert zugegriffen werden.

In dem vorliegenden Dokument werden Richtlinien festgelegt, die die Funktion des zentralen Sicherheitsmoduls und den Austausch von Daten zwischen Verkehrsunternehmen und dem zentralen Sicherheitsmodul beschreiben und im Rahmen des elektronischen Fahrgeldmanagements des VRR verbindlich eingehalten werden müssen.

2 Allgemeines

Nach [5] muss für die kryptographisch abgesicherte Administration der Sicherheitsmodule in den Initialisierungsgeräten jedes Verkehrsunternehmen sein Back-Office-System mit einem entsprechenden Sicherheitsmodul ausstatten. Da dieses Sicherheitsmodul eine zentrale Rolle im gesamten Sicherheitskonzept besitzt, wäre – je nach Realisierungsform – bei einem Verlust (Hardware-Form) oder einer illegalen Kopie (Software-Form) dieses Sicherheitskonzept empfindlich getroffen. Um diese Risiken entscheidend zu minimieren, stellt der VRR dieses Sicherheitsmodul seinen Verkehrsunternehmen zentral zur Verfügung.

Basierend auf [4] wurden in [2] die konkreten administrierbaren Daten festgelegt. Dies sind im Einzelnen:

- Obergrenzen (Limits) beim Einbringen eines Elektronischen Tickets
    - Maximaler Wert eines neuen Elektronischen Tickets, das ohne gekoppelten Bezahlvorgang eingebracht werden kann
    - Maximale Summe der Werte der Elektronischen Tickets, die ohne gekoppelten Bezahlvorgang eingebracht werden können
    - Aktuelle Summe der Werte der Elektronische Tickets, die ohne gekoppelten Bezahlvorgang bereits eingebracht wurden
    - Maximale Anzahl der Elektronischen Tickets, die ohne gekoppelten Bezahlvorgang eingebracht werden können
    - Aktuelle Anzahl der Elektronischen Tickets, die ohne gekoppelten Bezahlvorgang bereits eingebracht wurden

- Funktionskontrolle
  - Erlaubnis, ein Elektronisches Ticket komplett zu erstellen
  - Erlaubnis, auf das Feld ZD-Info zuzugreifen
  - Erlaubnis, das Verfallsdatum zu ändern
- Kopplung an einen Bezahlvorgang mit der PayCard

Damit der Administrierungsvorgang eingeleitet werden kann, unter dem das Laden neuer Daten verstanden wird, meldet das Initialisierungsgerät nach einer Statusanfrage und nach jedem Einbringen eines Elektronischen Tickets alle aktuellen administrierbaren Daten sowie mindestens noch die SAM-ID und das Datum des Ablaufs der Gültigkeit des Sicherheitsmoduls an das Back-Office-System des Verkehrsunternehmens, das dann entscheidet, ob der Administrierungsvorgang durch das Initialisierungsgerät eingeleitet werden soll, sowie die gemeldeten Daten hinsichtlich Aktivierung und Ablauf der Gültigkeit auswertet. Der Administrierungsvorgang sollte z.B. dann eingeleitet werden,

- wenn die gemeldeten aktuellen Daten bei den Obergrenzen einen im Back-Office-System projektierbaren Prozentsatz der im Back-Office-System hinterlegten maximalen Daten bei den Obergrenzen erreicht haben und/oder
- wenn die gemeldeten maximalen Daten bei den Obergrenzen unterschiedlich zu den im Back-Office-System hinterlegten maximalen Daten sind und/oder
- wenn die gemeldeten Daten zur Funktionskontrolle unterschiedlich zu den im Back-Office-System hinterlegten Daten sind und/oder
- wenn die gemeldeten Daten bezüglich der Kopplung an einen Bezahlvorgang mit der PayCard unterschiedlich zu den im Back-Office-System hinterlegten Daten sind.

Je nach Ergebnis werden nun bis zu drei nacheinander durchzuführende Administrierungsvorgänge notwendig, nämlich bezüglich

- der Obergrenzen (Limits) beim Einbringen eines Elektronischen Tickets und/oder
- der Funktionskontrolle und/oder
- der Kopplung an einen Bezahlvorgang mit der PayCard.

Dabei sind bei der Adminstration der Obergrenzen die aktuellen Daten wie im entsprechenden Rohkommando bereits berücksichtigt auf Null zu setzen.

Die Entscheidung, wann der Administrierungsvorgang genau eingeleitet wird, liegt letztendlich immer beim Back-Office-System des Verkehrsunternehmens, dass außerdem sicherstellen muss, dass auch bei mehreren Initialisierungsgeräten immer nur ein Administrierungsvorgang zeitgleich durchgeführt wird, da es nur einen Zugang zum zentralen Sicherheitsmodul gibt.

3 Datenaustausch und Funktion des zentralen Sicherheitsmoduls

Der Datenaustausch ist – wie in Abbildung 1 dargestellt – ausgehend vom Initialisierungsgerät über das Back-Office-System eines Verkehrsunternehmens bis zum zentralen Sicherheitsmodul transparent. Das Initialisierungsgerät erzeugt als Rohkommando die in 4 definierte Zeichenkette mit Platzhaltern für die in 2 beschriebenen administrierbaren Daten. Diese werden dann vom Back-Office-System in das jeweilige Rohkommando eingetragen und an das zentrale Sicherheitsmodul übertragen. Das zentrale Sicherheitsmodul berechnet nun mit den Daten des übergebenen Rohkommandos das Kryptogramm und stellt das nun fertig gestellte Kommando zum Abholen durch das Back-Office-System bereit, das dieses unverändert an das Initialisierungsgerät und damit zum Sicherheitsmodul weiterleitet. Der Vorgang ist ggf. für verschiedene Parameter zu wiederholen. Näheres zum Sicherheitskonzept der PayCard siehe [3].

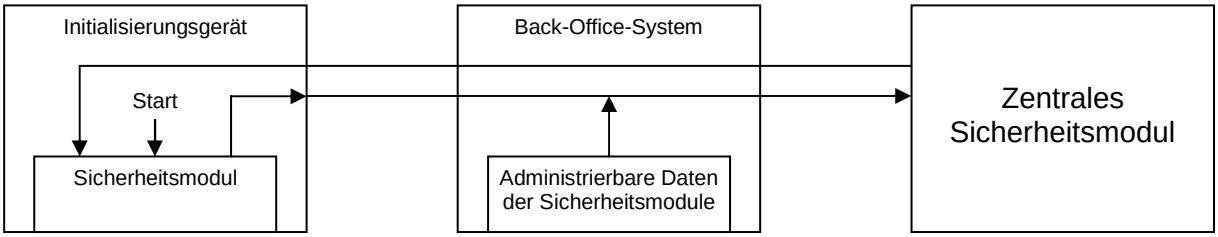

Abbildung 1: Datenaustausch

4 Datenformate

Sowohl das gewünschte Rohkommando als auch das fertig gestellte Kommando werden zwischen dem Back-Office-System und dem zentralen Sicherheitsmodul als Datei ohne weitere zusätzliche Daten übertragen. Näheres dazu ist in 5 beschrieben. Der Datenaustausch zwischen Initialisierungsgerät und Back-Office-System ist in einem separaten Dokument beschrieben.

Das Rohkommando im Input-File zum Ändern der Obergrenzen (Limits) hat die folgende Struktur:

Felder	Inhalt	Codierung	Länge (Byte)
PAN des SAMs aus EF_Application/MF	„927600248XXXXXXXXXF“	BCD	10
Application expiration date des SAMs aus EF_Application/MF	JJMMTT	BCD	3
Application effective date des SAMs aus EF_Application/MF	JJMMTT	BCD	3
Key version aus EF_Info/DF_eTicket des SAMs	„XX“	HEX	1
Zufallszahl (RND) des SAMs	„XXXXXXXXXXXXXXXX“	HEX	8
Kommando-Header für Limit-Änderung (PUT DATA mit SM)	„0CDA00C8“	HEX	4
Länge des Kommandos (18 Byte Daten + 8 Byte Kryptogramm)	„1A“	HEX	1
Maximaler Wert eines neuen Elektronischen Tickets, das ohne gekoppelten Bezahlvorgang eingebracht werden kann	EEEEEECC (E = Euro, C = Cent)	BCD	4
Maximale Summe der Werte der Elektronischen Tickets, die ohne gekoppelten Bezahlvorgang eingebracht werden können	EEEEEECC (E = Euro, C = Cent)	BCD	4
Aktuelle Summe der Werte der Elektronische Tickets, die ohne gekoppelten Bezahlvorgang bereits eingebracht wurden	„00000000“	BCD	4
Maximale Anzahl der Elektronischen Tickets, die ohne gekoppelten Bezahlvorgang eingebracht werden können	„XXXXXX“	HEX	3
Aktuelle Anzahl der Elektronischen Tickets, die ohne gekoppelten Bezahlvorgang bereits eingebracht wurden	“000000“	HEX	3

Das zentrale Sicherheitsmodul errechnet nun nach Prüfung der „Key version“ den kartenspezifischen Limit-Key des SAMs aus „PAN, expiration und effective date“. Dann generiert es ein Kryptogramm über die Kommandodaten mittels des errechneten Keys und der Zufallszahl des SAMs. Das Kryptogramm wird an das Kommando angehängt und bildet das fertige Kommando für das jeweilige SAM. Bei den übrigen Kommandos verhält sich das zentrale Sicherheitsmodul prinzipiell gleich.

Das fertig gestellte Kommando im Output-File hat die folgende Struktur:

Felder	Inhalt	Codierung	Länge (Byte)
Kommando-Header für Limit-Änderung (PUT DATA mit SM)	„0CDA00C8“	HEX	4
Länge des Kommandos (18 Byte Daten + 8 Byte Kryptogramm)	„1A“	HEX	1
Maximaler Wert eines neuen Elektronischen Tickets, das ohne gekoppelten Bezahlvorgang eingebracht werden kann	EEEEEECC (E = Euro, C = Cent)	BCD	4
Maximale Summe der Werte der Elektronischen Tickets, die ohne gekoppelten Bezahlvorgang eingebracht werden können	EEEEEECC (E = Euro, C = Cent)	BCD	4
Aktuelle Summe der Werte der Elektronische Tickets, die ohne gekoppelten Bezahlvorgang bereits eingebracht wurden	„00000000“	BCD	4
Maximale Anzahl der Elektronischen Tickets, die ohne gekoppelten Bezahlvorgang eingebracht werden können	„XXXXXX“	HEX	3
Aktuelle Anzahl der Elektronischen Tickets, die ohne gekoppelten Bezahlvorgang bereits eingebracht wurden	„000000“	HEX	3
Kryptogramm über Header und Daten	„XXXXXXXXXXXXXXXX“	HEX	8

Das Rohkommando im Input-File zum Ändern der Funktionskontrolle hat die folgende Struktur:

Felder	Inhalt	Codierung	Länge (Byte)
PAN des SAMs aus EF_Application/MF	„927600248XXXXXXXXXXF”	BCD	10
Application expiration date des SAMs aus EF_Application/MF	JJMMTT	BCD	3
Application effective date des SAMs aus EF_Application/MF	JJMMTT	BCD	3
Key version aus EF_Info/DF_eTicket des SAMs	„XX“	HEX	1
Zufallszahl (RND) des SAMs	„XXXXXXXXXXXXXXXX“	HEX	8
Kommando-Header für „Function control“-Änderung (PUT DATA mit SM)	„0CDA00C9“	HEX	4
Länge des Kommandos (3 Byte Daten + 8 Byte Kryptogramm)	„0B“	HEX	1
Erlaubnis, ein Elektronisches Ticket komplett zu erstellen	„00“ (nicht erlaubt) oder „01“ (erlaubt)	HEX	1
Erlaubnis, auf das Feld ZD-Info zuzugreifen	„00“ (nicht erlaubt) oder „01“ (erlaubt)	HEX	1
Erlaubnis, das Verfallsdatum zu ändern	„00“ (nicht erlaubt) oder „01“ (erlaubt)	HEX	1

Das fertig gestellte Kommando im Output-File hat die folgende Struktur:

Felder	Inhalt	Codierung	Länge (Byte)
Kommando-Header für Limit-Änderung (PUT DATA mit SM)	„0CDA00C9“	HEX	4
Länge des Kommandos	“0B“	HEX	1
Erlaubnis, ein Elektronisches Ticket komplett zu erstellen	“00“ (nicht erlaubt) oder “01“ (erlaubt)	HEX	1
Erlaubnis, auf das Feld ZD-Info zuzugreifen	“00“ (nicht erlaubt) oder “01“ (erlaubt)	HEX	1
Erlaubnis, das Verfallsdatum zu ändern	“00“ (nicht erlaubt) oder “01“ (erlaubt)	HEX	1
Kryptogramm über Header und Daten	„XXXXXXXXXXXXXXXX“	HEX	8

Das Rohkommando im Input-File zum Ändern der Kopplung an einen Bezahlvorgang mit der PayCard hat die folgende Struktur:

Felder	Inhalt	Codierung	Länge (Byte)
PAN des SAMs aus EF_Application/MF	“927600248XXXXXXXXXXF”	BCD	10
Application expiration date des SAMs aus EF_Application/MF	JJMMTT	BCD	3
Application effective date des SAMs aus EF_Application/MF	JJMMTT	BCD	3
Key version aus EF_Info/DF_eTicket des SAMs	„XX“	HEX	1
Zufallszahl (RND) des SAMs	„XXXXXXXXXXXXXXXX“	HEX	8
Kommando-Header für „Function control“-Änderung (PUT DATA mit SM)	„0CDA00CA“	HEX	4
Länge des Kommandos (1 Byte Daten + 8 Byte Kryptogramm)	“09“	HEX	1
Kopplung an einen Bezahlvorgang mit der PayCard	“00“ (nicht gekoppelt) oder “01“ (gekoppelt)	HEX	1

Das fertig gestellte Kommando im Output-File hat die folgende Struktur:

Felder	Inhalt	Codierung	Länge (Byte)
Kommando-Header für Limit-Änderung (PUT DATA mit SM)	„0CDA00CA“	HEX	4
Länge des Kommandos	“09“	HEX	1
Kopplung an einen Bezahlvorgang mit der Pay-Card	“00“ (nicht gekoppelt) oder “01“ (gekoppelt)	HEX	1
Kryptogramm über Header und Daten	„XXXXXXXXXXXXXXXX“	HEX	8

5 Datenaustauschmechanismus

Nachfolgend ist der Austausch von Daten zwischen dem zentralen Sicherheitsmodul beim VRR und den DV-Systemen der Verkehrsunternehmen skizziert, der auf einfachen Mechanismen beruht und die Integration verschiedenartigster DV-Systeme bei minimalem Aufwand ermöglicht.

Die Übertragung erfolgt analog zur Verbindung zum Verbundsystem über eine ISDN-Wählverbindung. Als Prokoll für die Übertragung der Dateien wird ftp eingesetzt. Hierfür sind von den DV-Systemen bei den Verkehrsunternehmen die folgenden Voraussetzungen zu erfüllen:

- Alle beteiligten Rechner sind über eine IP-Adresse ansprechbar.
- Die DV-Systeme bei den Verkehrsunternehmen bilden die ftp-Clients.

Das zentrale Sicherheitsmodul beim VRR wird hierfür mit der ftp-Server-Funktionalität ausgestattet. Die DV-Systeme bei den Verkehrsunternehmen können so den ftp-Client mit der in der Regel standardmäßig vorhandenen Software realisieren.

Die Namen der zu sendenden Dateien müssen aus dem VU-Kürzel, der Art der Datei und dem aktuellen Datum und der aktuellen Uhrzeit jeweils getrennt durch einen Unterstrich bestehen. Die einzelnen Dateien haben den Typ dat und sind daher wie folgt zu benennen:

- Datei mit Rohkommando:

  VU-Kürzel_SAM_RKM_JJJJMMTT_SSMM.dat

- Datei mit fertig gestelltem Kommando:

  VU-Kürzel_SAM_FKM_JJJJMMTT_SSMM.dat

Das Verfahren geht davon aus, dass die VUs die aktive Rolle spielen. Das hat den Vorteil, dass die VUs den Datenaustausch optimal in ihren Geschäftsablauf einfügen können.

Grundregeln:

1. Es stehen zwei Verzeichnisse für den Datenaustausch zur Verfügung. Das Verzeichnis "IN" dient zum Ablegen von Daten, die das VU an das zentrale Sicherheitsmodul sendet, im Verzeichnis "OUT" stehen die zur Abholung bereitgestellten Daten.

2. Die Pfade zu diesen Verzeichnissen werden automatisch eingestellt.

3. Daten, die ein Unternehmen in das "IN"-Verzeichnis kopiert, werden vom zentralen Sicherheitsmodul im Rahmen des Datenpflegeprozesses automatisch übernommen und archiviert. Die Vorteile dieses Verfahrens sind:

   * Das sendende VU kann aus dem Vorhandensein bzw. dem Nichtvorhandensein einer Datei im Verzeichnis "IN" erkennen, ob seine Daten verarbeitet worden sind.

   * Das (versehentliche) Überschreiben von gelieferten Daten kann verhindert werden, indem das sendende Unternehmen nicht das Recht erhält, eine vorhandene Datei zu löschen.

- Das zentrale Sicherheitsmodul kann auf einfache Weise prüfen, ob ein Unternehmen neue Daten geliefert hat (durch die Existenz einer Datei im entsprechenden IN-Verzeichnis).

- Durch die Archivierung der Daten mit einer eindeutigen Namenskonvention können alle Datenpflegevorgänge und auch alle Datenaustauschvorgänge nachvollzogen werden.

Abbildung 2 zeigt diesen Mechanismus.

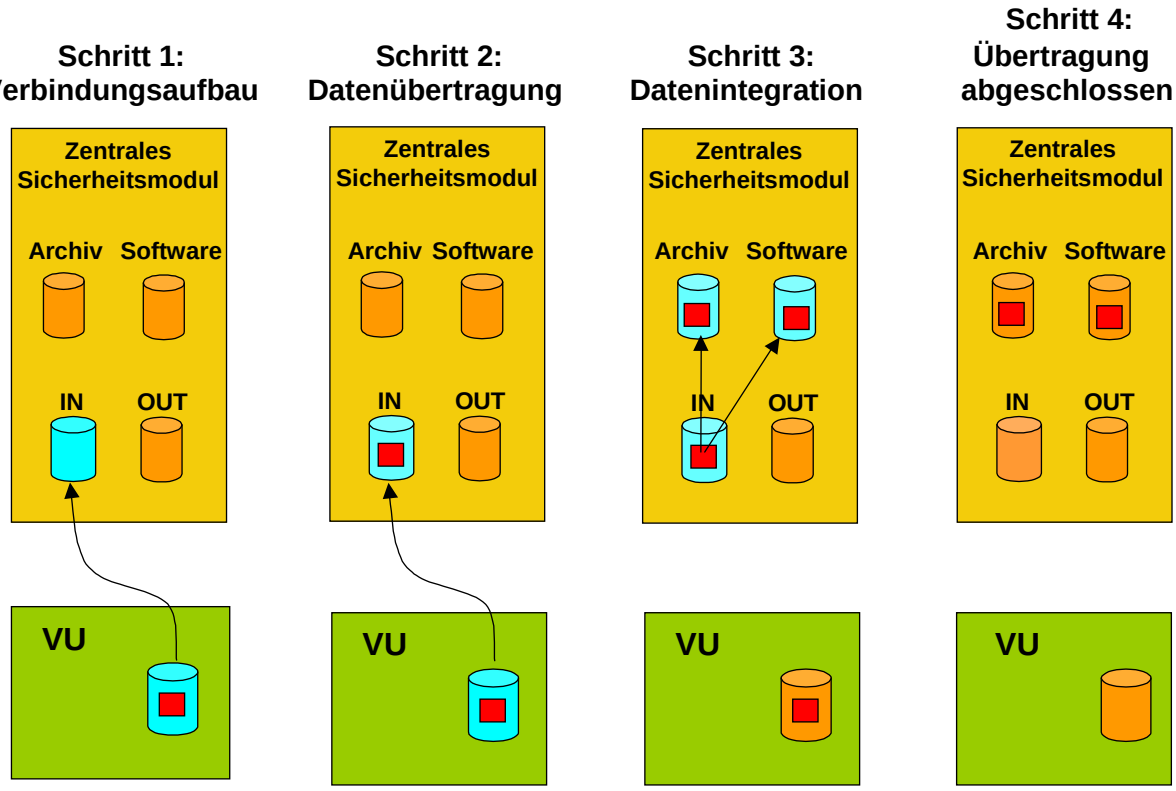

Abbildung 2: Datenübertragung vom VU zum zentralen Sicherheitsmodul

4. Für den Datenaustausch vom zentralen Sicherheitsmodul zu den VUs gilt ein analoger Mechanismus. Hat ein Unternehmen erfolgreich seine Daten aus dem Verzeichnis "OUT" geladen, so wird diese Datei vom zentralen Sicherheitsmodul in ein anderes Verzeichnis verschoben und archiviert. Dazu muss das zentrale Sicherheitsmodul über den Erfolg des Datenaustausches informiert werden. Dieses erfolgt durch Senden einer Datei mit dem Namen „VU-Kürzel_SAM_KOK_JJJJMMTT_SSMM.txt", das den vom zentralen Sicherheitsmodul übernommenen Dateinamen als ASCII-Text jeweils abgeschlossen mit Carriage Return („D“ hex) beinhaltet.

   Auch bei diesem Mechanismus lässt sich der aktuelle Stand der Verarbeitung sowohl für das VU als auch für das zentrale Sicherheitsmodul sofort erkennen. Steht eine Datei in dem OUT-Verzeichnis, so ist ersichtlich:

   - Für das VU, dass aktuelle Daten zur Abholung bereit stehen.

   - Für das zentrale Sicherheitsmodul, dass die aktuellen Daten noch nicht vom VU übernommen worden sind.

Abbildung 3 zeigt diesen Mechanismus.

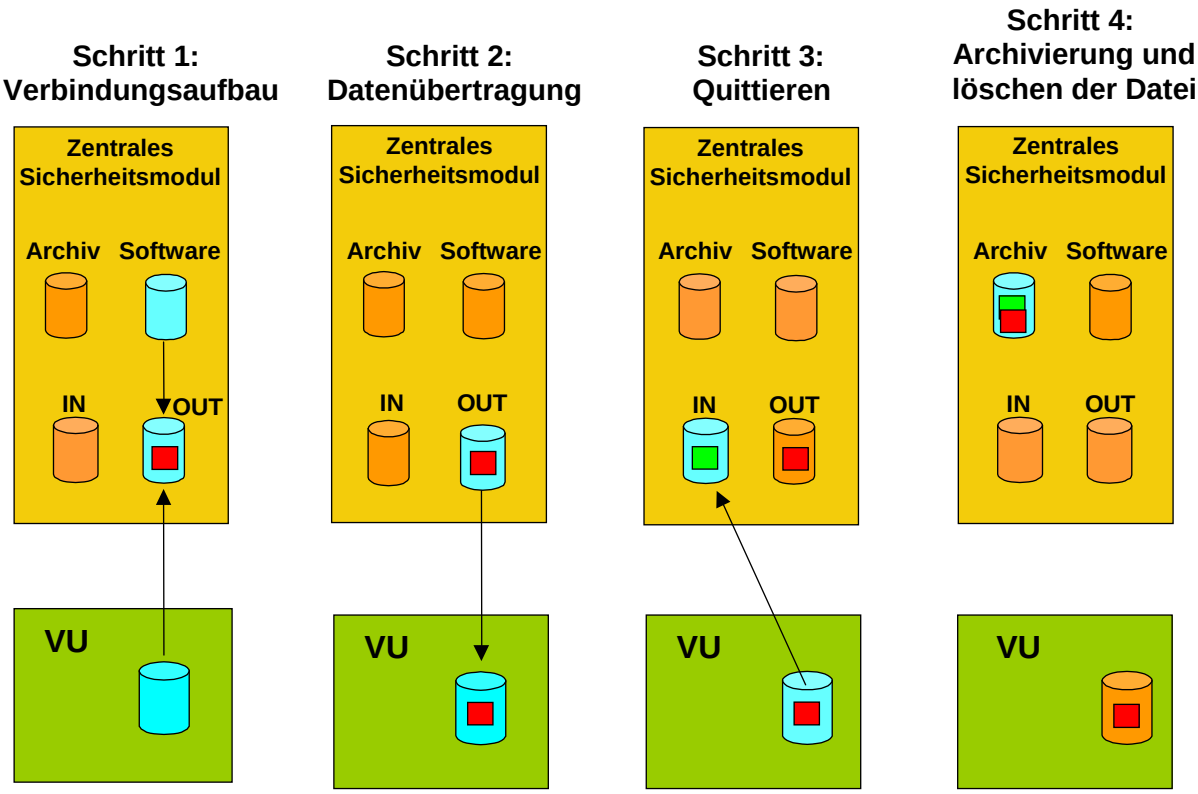

Abbildung 3: Datenübertragung vom zentralen Sicherheitsmodul zum VU

Die oben beschriebenen Datenübertragungen können – je nach Anforderung – jederzeit stattfinden. Die Bearbeitung der von einem VU übergebenen Daten erfolgt unmittelbar nachdem die Datei mit dem Rohkommando in das IN-Verzeichnis gestellt wurde. Das VU kann also sofort, ohne die Verbindung zu unterbrechen, das OUT-Verzeichnis abfragen, ob die Datei mit dem fertig gestellten Kommando schon vorliegt.

6 Referenzen

[1] Elektronische Tickets auf Chipkarten des deutschen Kreditgewerbes, Version 1.1, November 1999, VDV-Mitteilung

[2] PayCard, Security Application Module (SAM), Interface Specification, Version 3.1, 30.11.2001, card.etc AG

[3] Security concept of the PayCard system, Version 3.1, 13.12.2001, card.etc AG

[4] Einsatz von Chipkarten und Sicherheitsmodulen, VRR-Richtlinie, Version 1.4, 23.01.2002, VRR GmbH

[5] Rahmenvorgabe für die Vertriebskomponente, VRR-Richtlinie, Version 1.1, 13.11.2000, VRR GmbH