



FEIG ZVT Befehlsübersicht

Beschreibung der Kassen- / Automatenchnittstelle



Hinweis

© Copyright 2017, 2018 by
FEIG ELECTRONIC GmbH
Lange Strasse 4
D-35781 Weilburg-Waldhausen
Tel.: +49 6471 3109-0
<http://www.feig.de>

Alle früheren Ausgaben verlieren mit dieser Ausgabe ihre Gültigkeit.
Die Angaben in diesem Dokument können ohne vorherige Ankündigung geändert werden.

Weitergabe sowie Vervielfältigung dieses Dokuments, Verwertung und Mitteilung ihres Inhalts sind verboten, soweit nicht ausdrücklich zugestanden. Zuwiderhandlung verpflichtet zu Schadenersatz. Alle Rechte für den Fall der Patenterteilung oder Gebrauchsmuster-Eintragung vorbehalten.

Die Zusammenstellung der Informationen in diesem Dokument erfolgt nach bestem Wissen und Gewissen. FEIG ELECTRONIC GmbH übernimmt keine Gewährleistung für die Richtigkeit und Vollständigkeit der Angaben in diesem Dokument. Insbesondere kann FEIG ELECTRONIC GmbH nicht für Folgeschäden auf Grund fehlerhafter oder unvollständiger Angaben haftbar gemacht werden. Da sich Fehler, trotz aller Bemühungen nie vollständig vermeiden lassen, sind wir für Hinweise jederzeit dankbar.

Die in diesem Dokument gemachten Installationsempfehlungen gehen von günstigsten Rahmenbedingungen aus. FEIG ELECTRONIC GmbH übernimmt weder Gewähr für die einwandfreie Funktion in systemfremden Umgebungen, noch für die Funktion eines Gesamtsystems, welches die in diesem Dokument beschriebenen Geräte enthält.

FEIG ELECTRONIC GmbH übernimmt keine Gewährleistung dafür, dass die in diesem Dokument enthaltenden Informationen frei von fremden Schutzrechten sind. FEIG ELECTRONIC GmbH erteilt mit diesem Dokument keine Lizenzen auf eigene oder fremde Patente oder andere Schutzrechte.

Inhaltsverzeichnis

1. Historie	5
2. Offene Punkte	6
3. Zweck	7
4. Allgemeine Konventionen	8
4.1. Systemvoraussetzungen	8
4.2. Zahlendarstellung.....	8
4.3. Teilstorno oder Endsummenbuchung	8
5. Befehlsübersicht	9
5.1. Befehlstabelle Kasse / Automat => cVEND Terminal.....	9
5.2. Befehlstabelle cVEND Terminal => Kasse / Automat.....	12
5.3. Host-Fehlerbehandlung durch Kasse	13
6. cVEND Funktionen	14
6.1. cVEND gerätespezifische Befehlsübersicht	14
7. Beispiele	16
7.1. Beispiel: Kassenanmeldung.....	16
7.2. Beispiel: Inbetriebnahme	16
7.3. Beispiel: Erweiterte Geräteinformationen.....	18
7.4. Beispiel: Konfiguriere Logausgabe.....	18
7.5. Beispiel: Starte kontinuierliche Logausgabe.....	19
7.6. Beispiel: cVEND Werkseinstellungen	19
7.7. Beispiel: cVEND IP Konfiguration	19
7.8. Beispiel: cVEND Host Konfiguration.....	20

7.9. Beispiel: cVEND Stromsparfunktion	20
7.10. Beispiel: Druckerkonfiguration	21
7.11. Beispiel: Terminal Betriebsmodus	22
7.12. Beispiel: cVEND Datei senden.....	22
Datei-IDs.....	24
8. Erweiterungen des ZVT-Befehls „Ändere PT Konfiguration“ 0813	26
9. Transparenter Kanal	30
9.1. Übersicht.....	30
ISO14443-4 Karten	30
Andere Karten (div. Mifare, FeliCa...)	30
Mifare-Funktionen	30
9.2. Detailbeschreibung der Befehle	31
Karte lesen und identifizieren	31
APDU-Austausch zur Karte.....	33
Transparente Sitzung beenden	33
Mifare Sicherheitsschlüssel laden	34
Mifare Authentifizierung	35
Mifare Datenblock lesen	35
Mifare Datenblock schreiben.....	36
10. Quellennachweise	38
11. Ansprechpartner	39

1. Historie

Version	Status	Author	Date	Notes
2.00	Aktualisierung	Bert Braun	16.01.2018	Zuordnung cVEND TOPP 1.1.3 - Kap.8 : zus. Tags „Ändere PT Konfig“ 08 13
2.1	Aktualisierung	Wenno Ronsdorf	31.01.2018	FEIG Dokumentennummer H80113-Xd-PY-D
2.2	Aktualisierung	Bert Braun Wenno Ronsdorf	23.02.2018	Zuordnung zu cVEND TOPP 1.1.4 - „MDB Enable“ aufgenommen. - H80113-0d-PY-D
2.3	Aktualisierung	Bert Braun	16.05.2018	Zuordnung zu cVEND TOPP 1.1.5 - 06 E0 – Zeige Text - Kap. 9 – transparenter Kanal - Kap.8 : zus. Tags „Ändere PT Konfig“ 08 13 - H80113-1d-PY-D
2.4	Aktualisierung Review	Bert Braun Wenno Ronsdorf	22.06.2018	Zuordnung zu cVEND TOPP 1.1.6 - 08 10 – TMS-Ruf - MDB: Unterstützung CRANE Automat - Konfiguration DFÜ über Kasse - H80113-2d-PY-D
2.5	Aktualisierung	Bert Braun	14.08.2018	Druckerkonfiguration IP-Konfiguration: IPoverUSB
2.6	Aktualisiert	Wenno Ronsdorf	8.10.2018	Aufforderungston via ZVT ändert auch für MDB. (ZVT entfernt)
2.7	Aktualisierung	Bert Braun	24.10.2018	Zuordnung zu cVEND TOPP 1.1.7 - 08 13 Betriebsmodus - H80113-3d-PY-D

2. Offene Punkte

-

CONFIDENTIAL

3. Zweck

Dieses Dokument beschreibt die in der FEIG Deutschen Bezahlapplikation umgesetzten ZVT-Kassenbefehle und ihre korrekte Verwendung.

Das Dokument soll Systemintegratoren der cVEND Bezahlterminals unterstützen, eine Anbindung an die eigenen Kassen- und Automatenysteme zu erstellen.

Eine Kenntnis der übergeordneten ZVT-Spezifikation [\[1\]](#) wird vorausgesetzt.

CONFIDENTIAL

4. Allgemeine Konventionen

4.1. Systemvoraussetzungen

Die in Kap. „5.1. Befehlstabelle Kasse / Automat => cVEND Terminal“ folgende Tabelle führt die im Feig cVEND umgesetzten Befehle der ZVT Kassenschnittstelle auf. Es wird hier der korrekte Umfang und Aufbau der Befehlsbitmaps und TLV Container dargestellt sowie auf die Einschränkungen verwiesen, die sich durch die Ausprägung des cVEND als unbedientes Bezahlterminal ergeben.

Detaillierte Informationen über den grundsätzlichen Aufbau und die Verwendung der ZVT-Kassensbefehle sowie die erforderliche Ablaufsteuerung sind der Spezifikation [\[1\]](#) zu entnehmen.

4.2. Zahlendarstellung

Dieses Dokument verwendet folgende Zahlenformate:

0...9:	Dezimalzahlen
00h...FFh:	Hexadezimalzahlen
b0...1	Binärzahlen

Die in den Beispielen des Kap. „7. Beispiele“ aufgeführten Befehls- und Antwortdaten sind durchweg im Hexadezimalsystem dargestellt, eine besondere Kennzeichnung erfolgt nicht.

4.3. Teilstorno oder Endsummenbuchung

Die ZVT Spezifikation [\[1\]](#) lässt bei unbedienten Bezahlterminals zwei Varianten der Kartenzahlung zu: Zum einen die Vorautorisierung mit folgendem Teilstorno über die nicht genutzte Summe, zum anderen die Vorautorisierung mit Endsummenbuchung. Diese Varianten können grundsätzlich parallel genutzt werden, beispielsweise abhängig von der präsentierten Kundenkarte:

Kreditkarten:	Endsummenbuchung
Girocard / Maestro:	Teilstorno

Letztlich bestimmen jedoch die jeweiligen Netzbetreiber die Verwendung und Zuordnung dieser beiden Zahlungsvarianten, so dass die tatsächliche Konfiguration immer mit dem technischen Ansprechpartner des Netzbetreibers abgestimmt sein muss.

Das cVEND Bezahlapplikation errechnet dabei selbstständig den Stornobetrag für ein Teilstorno, wenn zwar über die Kassenschnittstelle ursprünglich eine Endsummenbuchung veranlasst wurde, die Konfiguration des Netzbetreibers jedoch ein Teilstorno verlangt.

5. Befehlsübersicht

In den Implementierungsdetails werden die ausgewerteten Bits eines Bytes durch folgende Konvention dargestellt:

1xxx 1xx1b : x = Bit nicht ausgewertet, 1 = Bit ausgewertet (MSB.....LSB, b= Binärformat)

Resultat: In o.g. Beispiel werden von der cVEND Applikation nur die Bits 0, 3 und 7 ausgewertet.

Eine Anmeldung der Kasse bzw. des Automaten ist obligatorisch. Die Kasse / der Automat bleibt danach auch nach Neustart des Terminals angemeldet. Siehe Kap. 7.1. Beispiel: Kassenanmeldung.

5.1. Befehlstabelle Kasse / Automat => cVEND Terminal

ZVT-Befehl	ZVT-Beschreibung	cVEND Implementierung
05 01h	Statusabfrage	Passwort wird nicht ausgewertet Ausgewertete BMP: 03 : Servicebyte Siehe PA00P015 13.08 en , S. 103ff.
06 00h	Anmeldung	Passwort wird nicht ausgewertet. Bitauswertung Service-Byte: xxxx xxx1b Bitauswertung Config-Byte: 1xxx 111xb Tagauswertung TLV-Container: 1Ah, 26h, 27h, 0Ah, 1F04h. Siehe PA00P015 13.08 en , S. 26ff.
06 01h	Autorisierung	Passwort wird nicht ausgewertet. Bitauswertung Service-Byte: xxxx xxx1b Bitauswertung Config-Byte: 1xxx 111xb Tagauswertung TLV-Container: 1Ah, 26h, 0Ah, 1F04h. Siehe PA00P015 13.08 en , S. 29ff.
06 02h	Abmeldung	Keine Besonderheiten Siehe PA00P015 13.08 en , S. 57ff.
06 10h	Kassensummen	Keine Besonderheiten Siehe PA00P015 13.08 en , S. 85ff.
06 12h	Belegdruck wiederholen	Keine Besonderheiten Siehe PA00P015 13.08 en , S. 51.
06 18h	Terminal Reset	Ausgewertete BMP: keine Siehe PA00P015 13.08 en , S. 88.
06 1Ah	Systemdatenausdruck	Ausgewertete BMP: keine Siehe PA00P015 13.08 en , S. 89.
06 1Bh	Setze Terminal ID	Ausgewertete BMP: 29 Siehe PA00P015 13.08 en , S. 90.
06 20h	Beleg wiederholen	Keine Besonderheiten Siehe PA00P015 13.08 en , S.52.

06 22h	Vorautorisierung / Reservierung	Ausgewertete BMPs: 01h, 02h, 04h, 0Eh, 19h, 22h, 23h, 24h, 2Dh, 3Bh, 3Ch, 49h. Siehe PA00P015 13.08 en , S. 40.
06 23h	Teilstorno	Ausgewertete BMPs: 04h, 0Bh, 3Bh, 3Ch, 49h, 87h. Siehe PA00P015 13.08 en , S. 41.
06 23 03 87 FFh	Teilstorno, Unterfunkt. Abfrage offener Vorautorisierungen	Siehe PA00P015 13.08 en , S. 42.
06 24h	Endsummenbuchung	Ausgewertete BMPs: 04h, 0Bh, 19h, 3Bh, 3Ch, 49h, 87h. Siehe PA00P015 13.08 en , S. 44.
06 25h	Storno Vorautorisierung	Ausgewertete BMPs: 04h, 19h, 49h, 87h. Siehe PA00P015 13.08 en , S. 45.
06 30h	Storno	Passwort wird nicht ausgewertet. Ausgewertete BMPs: 04h, 0Eh, 19h, 22h, 23h, 24h, 2Dh, 3Bh, 3Ch, 49h, 87h. Siehe PA00P015 13.08 en , S. 40.
06 50h	Kassenschluss	Passwort wird nicht ausgewertet Ausgewertete BMP: 06h. Siehe PA00P015 13.08 en , S. 46.
06 70h	Diagnose	Ausgewertete BMP: 06h. Tagauswertung im TLV-Container: 1Bh. Siehe PA00P015 13.08 en , S. 48ff.
06 91h	Datum und Uhrzeit setzen	Passwort wird nicht ausgewertet. Ausgewertete BMP: 0Ch, AAh. Siehe PA00P015 13.08 en , S. 57.
06 93h	Initialisierung	Passwort wird nicht ausgewertet. Ausgewertete BMPs: keine Siehe PA00P015 13.08 en , S. 50ff.
06 B0h	Abbruch	Ausgewertete BMP: D2h. Siehe PA00P015 13.08 en , S. 56.
06 C0h	Karte lesen	Ausgewertete BMP: 06h, 19h, FCh BMP FCh, Bit 1: 1 = Aufforderungston unterdrücken, Bit 2: 1 = Ergebniston unterdrücken. In Tag 4Ch der Statusmeldung wird ein eindeutiges kryptografisches Token aus der PAN der präsentierten Karte geliefert, mit dessen Hilfe die Karte in der Nachfolgetransaktion selektiert werden kann. Mit gesetztem Bit 0x10 in Tag 1F15 kann ein „schneller“ Low-Level Card-Detect durchgeführt werden. Siehe PA00P015 13.08 en , S. 54.
06 C1h	Mifare Schlüssel laden	Siehe Kap. 9. Transparenter Kanal“
06 C2h	Mifare Authentifizierung	Siehe Kap. 9. Transparenter Kanal“
06 C3h	Mifare Block lesen	Siehe Kap. 9. Transparenter Kanal“
06 C4h	Mifare Block schreiben	Siehe Kap. 9. Transparenter Kanal“

06 C5h	Transp. Sitzung schließen	Siehe Kap. 9. Transparenter Kanal“ Siehe PA00P015 13.08 en , S. 112
06 C6h	APDU senden	Siehe Kap. 9. Transparenter Kanal“ Siehe PA00P015 13.08 en , S. 112
06 E0h	Zeige Displaytext	Ausgewertete BMP: F0h, F1h, F2h, F9h Text wird zentriert auf Display angezeigt. Bei Tag F0h = 00h ersetzt Text den Idletext. Attribute zur Fontskalierung werden nicht unterstützt. Max. Zeilenlänge: 24 Z. Siehe PA00P015 13.08 en , S. 58.
08 10h	TMS Ruf	Ausgewertete BMP: keine Siehe PA00P015 13.08 en , S. 75.
08 13h	Ändere PT Konfiguration	Ausgewertete BMP: 06h Siehe Kap. 7.8. Beispiel: cVEND Host Konfiguration, 7.9. Beispiel: cVEND Stromsparfunktion, 7.10. Beispiel: Druckerkonfiguration sowie 7.11. Beispiel: Terminal Betriebsmodus.
08 14h	Datei senden	Ausgewertete BMP: 06h Siehe Kap. 7.12. Beispiel: cVEND Datei senden
08 30h	Wähle Terminalsprache	Unterstützte Sprachen: Deutsch, Englisch. Im Terminalmodus „unbedient“ wird neben der Kundensprache auch die Terminalsprache eingestellt. Siehe PA00P015 13.08 en , S. 74.
0F A1h	cVEND Funktion	Siehe Kap. 6. cVEND Funktionen

5.2. Befehlstabelle cVEND Terminal => Kasse / Automat

Das cVEND verwendet folgende ZVT-Befehle zur Kommunikation mit dem Kassen- / Automaten-system, wenn das System zuvor im ZVT-Befehl Anmeldung (0600) jeweils die Akzeptanz für diese Befehle signalisiert hat (BMP26h).

ZVT-Befehl	ZVT-Beschreibung	cVEND Implementierung
04 0Fh	Statusinformation	Gesendete BMP: 25h. Siehe PA00P015_13.08_en , S. 115ff.
04 FFh	Zwischenstatus	Kein Timeout, kein TLV-Container. Siehe PA00P015_13.08_en , S. 125.
06 0Fh	Abschlussmeldung	Gesendete BMPs: 27h, 0Ch, AAh, 19h, 29h, 49h. Siehe PA00P015_13.08_en , S. 122.
06 1Eh	Abbruch	Gesendete TLV-Tags: Fehler-ID, Zusatzdaten. Siehe PA00P015_13.08_en , S. 122.
06 D1h	Zeile drucken	<Attribut> wird ausgewertet. Kein TLV-Container. Siehe PA00P015_13.08_en , S. 123.
06 D3h	Textblock drucken	Gesendete BMPs: 25h, 07h, 09h. Siehe PA00P015_13.08_en , S. 124.
06 D8h	DFÜ über Kasse - Anwahl	Einschränkung: siehe [a] Siehe PA00P015_13.08_en , S. 128.
06 DBh	DFÜ - Auflegen	Einschränkung: siehe [a] Siehe PA00P015_13.08_en , S. 129.
06 D9h	DFÜ - Daten senden	Einschränkung: siehe [a] Siehe PA00P015_13.08_en , S. 129.
06 DAh	DFÜ - Daten empfangen	Einschränkung: siehe [a] Siehe PA00P015_13.08_en , S. 130.
06 DDh	DFÜ – Transparenter Modus	Einschränkung: siehe [a] Siehe PA00P015_13.08_en , S. 130.

[a] Die DFÜ Funktionen werden vom cVEND Terminal nur dann verwendet, wenn die Verbindung zum Hostrechner mit E2E Verschlüsselung betrieben wird.

Ist keine E2E Verschlüsselung im cVEND Terminal konfiguriert, lehnt das Terminal die ZVT-Kassenanmeldung mit „Abbruch“ ab, wenn diese eines der DFÜ-Kommandos mittels der Tag 26h Liste zu aktivieren versucht.

5.3. Host-Fehlerbehandlung durch Kasse

Ist eine Kassenanwendung über die ZVT-Schnittstelle beim Terminal angemeldet, so wird die Fehlermeldung AC=A1 des Hostrechners, die einen Kassenschnitt als Folgeaktion anfordert, vom Terminal nicht automatisch verarbeitet, um den Kassenablauf nicht zu stören.

Der Fehlercode wird kassenseitig in den Statuscode 240 = F0h umgesetzt, die Kassenanwendung muss auf diesen Statuscode hin einen Kassenschnitt zum PT veranlassen.

CONFIDENTIAL

6. cVEND Funktionen


Zusätzlich zu den offiziellen ZVT ECR Befehlen unterstützt das cVEND Terminal den Befehl „0F A1 – cVEND Funktion“ und „08 14 – Datei senden“ für zusätzliche, gerätespezifische Funktionen. Das cVEND antwortet mit einer Abschlussmeldung „06 0F“ ergänzt um eventuelle Systemdaten.

Siehe Kap. 7.3. Beispiel: Erweiterte Geräteinformationen und folgende.

6.1. cVEND gerätespezifische Befehlsübersicht

Aktuell verwendete Unterbefehle:

Erweit. Befehl	Inhalt	Details
00 01h	Erweiterte Geräteinformationen	<u>Sendedaten:</u> 2 Bytes : erw. Befehl 00 01h <u>Empfangsdaten:</u> 8 Bytes : Seriennummer, 17 Bytes : SW-Version 8 Bytes : Terminal ID (TID) ASCII Kodierung Details siehe Kap. 7.3. Beispiel: Erweiterte Geräteinformationen
02 53h	Konfiguriere Logausgabe Setzt Detailgrad der Logausgabe und der Fehlerausgabe. (Servicepasswort wird vom FEIG Kundenservice erteilt.)	<u>Sendedaten:</u> 3 Bytes : Servicepasswort BCD 2 Bytes : erw. Befehl: 02 53h 1 Byte : Errorlevel / Loglevel <u>Empfangsdaten:</u> Abschlussmeldung Details siehe Kap. 7.4. Beispiel: Konfiguriere Logausgabe
02 54h	Starte / Stoppe Logausgabe Steuert die Logausgabe über UDP an einen konfigurierbaren Logrechner. Zur temporären Freischaltung der UDP Logausgabe wird ein Zugriffstoken benötigt, das die Gültigkeit der Freischaltung festlegt. Zum Abschalten der Logfunktion muss kein Zugriffstoken übermittelt werden. Durch Abschalten der Logfunktion wird das Zugriffstoken im Terminal gelöscht. Zum erneuten Aktivieren der Logfunktion muss daher das Token erneut übermittelt werden. (Servicepasswort und Zugriffstoken werden	<u>Sendedaten:</u> 3 Bytes : Servicepasswort BCD 2 Bytes : erw. Befehl: 02 53h 1 Bytes : Modus: 00h – 02h 00h : Log aus 01h : Log lesen einmalig 02h : Log lesen kontinuierl. 4 Bytes : IP Adresse Logrechner, Hexformat 2 Bytes : UDP Port Logrechner, Hexformat Var. Länge : Zugriffstoken, Hexformat

	vom FEIG Kundenservice erteilt.)	<u>Empfangsdaten:</u> Abschlussmeldung Details siehe Kap. 7.5. Beispiel: Starke kontinuierliche Logausgabe
02 55h 	<p>Werkseinstellungen aufrufen</p> <p>(Servicepasswort wird vom FEIG Kundenservice erteilt.)</p> <p>Achtung: Dieser Befehl versetzt sofort ohne weitere Rückfrage das Terminal in den Werkzustand!</p> <p>Alle noch im Terminal gespeicherten Umsätze gehen hierdurch unwiederbringlich verloren. Es wird daher dringend empfohlen, zuvor den Kassenschnitt durchzuführen, um gespeicherte Umsätze einzureichen.</p> <p>Nach dem Aufrufen der Werkseinstellungen ist das erneute Setzen der TID erforderlich, sowie eine Inbetriebnahme durchzuführen.</p>	<p>Sendedaten:</p> <p>3 Bytes : Servicepasswort BCD</p> <p>2 Bytes : Befehl: 02 55h</p> <p>Empfangsdaten:</p> <p>Abschlussmeldung</p> <p>Details siehe Kap. 7.6. Beispiel: cVEND Werkseinstellungen</p>

7. Beispiele

7.1. Beispiel: Kassenanmeldung

ZVT-Kassenbefehl:

060039123456DE0978063126140A02040F0A02060F0A02061E0A0204FF0A0206D327021401100220
041201401F0401B01F0501004002C0001A021000

Aufbau:

06 00 : ZVT Kommando: Anmeldung
39 : Länge 57 Bytes
12 34 56 : Passwort
DE : Configbyte 11011110b
09 78 : CC Euro
06 31 : TLV-Container, Länge 49 Bytes
26 14 : Liste vom ECR unterstützter ZVT-Befehle, Länge 20 Bytes:
0A 02 04 0F : Statusinformation
0A 02 06 0F : Abschlussmeldung
0A 02 06 1E : Abbruch
0A 02 04 FF : Zwischenstatusmeldung
0A 02 06 D3 : Drucke Textblock
27 02 : Liste der von Kasse unterstützten Zeichenkodierungen
14 01 : ISO 8859-1
10 02 20 04 : Händlerdisplay: 32x4 Zeichen
12 01 40 : Zeilenlänge Drucker: 40 Zeichen
1F 04 01 B0 : Druckparameter
1F 05 01 00 : Transaktionsparameter: 00h
40 02 C0 00 : EMV-Config Parameter: C000h
1A 02 10 00 : max. APDU-Länge: 4096 Byte

Der Status einer erfolgreich durchgeführten Anmeldung bleibt auch über einen Neustart des cVEND Terminals hinaus, beispielsweise ausgelöst durch den ZVT-Befehl „Reset Terminal“ oder eine Unterbrechung der Spannungsversorgung, bestehen.

Eine explizite Abmeldung der Kasse kann mit dem ZVT-Befehl „Abmeldung“ (06 02) erfolgen.

7.2. Beispiel: Inbetriebnahme

Zur Erstinbetriebnahme bzw. Inbetriebnahme nach Wiederherstellen der Werkseinstellungen ist es zwingend erforderlich, zunächst eine gültige Terminal-ID (TID) zu setzen. Die TID wird üblicherweise vom zuständigen Netzbetreiber erteilt.

Voraussetzung ist weiterhin, dass das Terminal wie in der Installations- und Bedienungsanleitung [2] beschrieben angeschlossen und in Betrieb genommen wurde sowie die Kassenkommunikation über eine der möglichen Schnittstellen eingerichtet wurde.

Wenn die Kommunikation auf der Kassenschnittstelle soweit fehlerfrei möglich ist, kann nun der ZVT-Befehl „Kassenanmeldung“ (siehe 7.1. Beispiel: Kassenanmeldung) abgesetzt werden.

Nach positiver Abschlussmeldung der Kassenanmeldung wird dann der ZVT-Befehl „Setze TID“ mit der zugeteilten TID durchgeführt:

ZVT-Kassenbefehl:

06 1B	: ZVT Kommando: Setze TID
08	: Länge: 8 Bytes
12 34 56	: Passwort, numerisch, BCD kodiert
29	: Tag: TID
12 34 56 78	: TID, numerisch, BCD kodiert

Das cVEND Terminal übernimmt nun die angegebene TID in seine interne Konfiguration. Danach versucht es, mit dem festgelegten Zahlungshost eine Verbindung aufzunehmen und mit der neu gesetzten TID eine automatische Inbetriebnahme durchzuführen. Dabei werden u.a. mittels Erweiterter Diagnose, Parameterdiagnose und EMV Parameterdiagnose TID-spezifische Konfigurationsdaten vom Zahlungshost abgerufen und im Terminal abgelegt.

Wenn die automatische Inbetriebnahme beendet ist, folgt eine Abschlussmeldung:

Aufbau Abschlussmeldung cVEND:

06 0F	: ZVT Abschlussmeldung
00	: Länge: 0 Bytes

Die Abschlussmeldung gibt keinen Aufschluss über den Erfolg der automatischen Inbetriebnahme. Hierzu muss der Status der roten LED an der Gerätefront überprüft werden:

Nach einer erfolgreichen Inbetriebnahme mit dem Zahlungshost erlischt die rote LED, das Terminal und die Kasse sind betriebsbereit, Zahlungen können durchgeführt werden.

Falls nach der Abschlussmeldung die rote LED nicht erloschen ist, so ist die Inbetriebnahme fehlgeschlagen. Fehlerursachen hierfür können z.B. sein:

- Kommunikation mit dem Zahlungshost nicht möglich. Ursachen:
 - o Konfiguration im Terminal falsch (falsche IP-Adresse / Port, Verschlüsselungsprobleme)
 - o Netzwerkverbindung gestört, Host nicht erreichbar, Routingprobleme
- TID falsch oder ungültig gesetzt (nicht vom Netzbetreiber zugewiesen)
- TID korrekt, aber am Zahlungshost gesperrt oder falsch konfiguriert

In jedem Fall ist die TID, die Hostkonfiguration und die Netzwerkverbindung zu überprüfen. Nach Beheben der Fehlerursache muss dann eine erneute Inbetriebnahme manuell durchgeführt werden:

ZVT-Kassenbefehl:

06 93	: ZVT Kommando: Initialisierung
03	: Länge: 3 Bytes
12 34 56	: Passwort, numerisch, BCD kodiert

Die Inbetriebnahme liefert ausführliche Zwischenmeldungen (04 FFh) und Druckdaten (06 Dxh) über den Verlauf, bevor sie im Erfolgsfall mit der Abschlussmeldung endet:

Aufbau Abschlussmeldung cVEND:

06 0F : ZVT Abschlussmeldung
 00 : Länge: 0 Bytes

Auch bei einer manuellen Inbetriebnahme gibt ausschließlich der Status der roten LED Aufschluss über den Erfolg des Vorgangs. Nach einer erfolgreichen Inbetriebnahme erlischt die rote LED.

7.3. Beispiel: Erweiterte Geräteinformationen

ZVT-Kassenbefehl:

0F A1 : cVEND Funktion
 02 : Längenbyte
 00 01 : Befehl: Erweiterte Geräteinformationen

Aufbau Abschlussmeldung cVEND:

06 0F : ZVT Abschlussmeldung
 21 : Länge: 33 Bytes
 31 31 45 34 44 39 39 45 : Seriennummer, 8 Bytes, ASCII
 47 45 52 2D 41 50 50 2D 76 30 2E 31 2E 30 20 20 20 : SW-Version, 17 Bytes, ASCII
 36 35 36 35 36 35 36 35 : Terminal ID, 8 Bytes, ASCII
 33 2E 31 34 : Batteriespannung, 4 Bytes, ASCII
 33 38 2E 38 : Temperatur, 4 Bytes, ASCII

7.4. Beispiel: Konfiguriere Logausgabe

ZVT-Kassenbefehl:

0F A1 : cVEND Funktion
 06 : Längenbyte
 01 02 03 : zugeteiltes Servicepasswort
 02 53 : erweiterter Befehlscode „Konfiguriere Logausgabe“
 C3 : Error- / Loglevel (Fatal & Error, Loglevel = 3)
 Hi-Nibble: Errorlevel, b7 = Fatal, b6 = Error, b5 = Warning, b4 = Debug
 Lo-Nibble: Loglevel, x0h (keine Logs) – xFh (alle Logausgaben)

Aufbau Abschlussmeldung cVEND:

06 0F : Abschlussmeldung
 00 : Länge

7.5. Beispiel: Starte kontinuierliche Logausgabe

ZVT-Kassenbefehl:

0F A1 : cVEND Funktion
xx (yy zz) : Längenbyte, kann abhängig von der Länge des Zugriffstokens auch als 2-Byte Wert durch vorangestelltes FFh dargestellt werden (siehe [1]).
01 02 03 : zugeteiltes Servicepasswort
02 54 : erweiterter Befehlscode „Starte / Stoppe Logausgabe“
02 : Modus, 02h = kontinuierliche Ausgabe solange Zugriffstoken gültig
C0 A8 01 02 : IP-Adresse Logrechner, 4 Byte hex, Beispiel: IP 192.168.1.2
13 88 : UDP-Port Logrechner, 2 Byte hex, Standard: UDP-Port 5000
01 02 03... : Zugriffstoken, hex., bis zu 524 Bytes

Aufbau Abschlussmeldung cVEND:

06 0F : Abschlussmeldung
00 : Länge

7.6. Beispiel: cVEND Werkseinstellungen

ZVT-Kassenbefehl:

0F A1 : cVEND Funktion
05 : Längenbyte
xx xx xx : Service Passwort (wird von FEIG Kundenservice erteilt)
02 55 : Befehl: Werkseinstellungen

Aufbau Abschlussmeldung cVEND:

06 0F : Abschlussmeldung
00 : Länge

7.7. Beispiel: cVEND IP Konfiguration

ZVT-Kassenbefehl:

08 13 : ZVT Kommando: Ändere PT Konfiguration
1B : Längenbyte
06 19 : BMP06, Länge 25 Bytes
E4 17 : Tag E4: Container Geräteinformationen, Länge 23 Bytes
FF 40 03 : Tag FF 40: Servicepasswort, Länge 3 Bytes
12 34 56 : Servicepasswort
FF 42 11 : Tag FF 42: IP-Konfigurationsblock, Länge 17 Bytes fix:
00 : IF-Byte, 00h = Ethernet, 01h = IPoverUSB
C0 A8 01 64 : IP-Adresse Terminal, 4 Bytes hex (z.B. statisch 192.168.1.100).
FF FF FF 00 : Netzwerkmaske, 4 Bytes hex, (z.B. 255.255.255.0)
C0 A8 01 01 : Gateway Adresse, 4 Bytes hex, (z.B. 192.168.1.1)

C0 A8 01 FE : DNS Adresse, 4 Bytes hex, (z.B. 192.168.1.254)

Die IP-Adressangabe 0.0.0.0 aktiviert den DHCP-Client, alle folgenden Felder werden dann nicht ausgewertet, müssen jedoch vorhanden sein.

7.8. Beispiel: cVEND Host Konfiguration

ZVT-Kassenbefehl:

08 13 : ZVT Kommando: Ändere PT Konfiguration
14 : Längenbyte
06 12 : BMP06, Länge 17 Bytes
E4 10 : Tag: Container Geräteinformationen, Länge 16 Bytes
FF 40 03 : Tag FF 40: Servicepasswort, Länge 3 Bytes
12 34 56 : Servicepasswort
FF 41 07 : Tag FF 41 „Host Konfigurationsdaten“, Länge 7 Bytes
C0 A8 80 01 : IP-Adresse Hostrechner, 4 Byte hex, Beispiel: 192.168.128.1
07 D5 : TCP-Port Hostrechner, 2 Byte hex, Beispiel: 2005
00 : Config Byte: b0 = SSL (0=aus / 1=ein), b1 = Message Framing (0=aus / 1=ein), b2 = DFÜ über Kasse (0=aus / 1=ein)

Aufbau Abschlussmeldung cVEND:

06 0F : Abschlussmeldung
00 : Länge

7.9. Beispiel: cVEND Stromsparfunktion

Das cVEND Terminal unterstützt einen Energiesparmodus, um z.B. in batteriebetriebenen Einsatzumgebungen die Batteriestandzeit zu verlängern, wenn das Terminal längere Zeit inaktiv ist. Mit dem Kommando „Konfiguriere Stromsparfunktion“ kann ein Leerlaufintervall in Sekunden definiert werden, nach dem das cVEND in den Schlafmodus fällt. Es kann dann z.B. durch Aktivieren der Weckleitung wieder in Betrieb gesetzt werden, wenn erneut eine Transaktion abzuwickeln ist. Da das cVEND neben der Bezahlapplikation bis zu 7 weitere Applikationen bedienen kann, benötigt die Stromsparfunktion Informationen darüber, wie viele Applikationen sich im Leerlauf befinden müssen, bevor das Terminal in den Schlafmodus fällt. Nur wenn die gesamte Anzahl konfigurierter Applikationen gemeinsam Leerlauf signalisiert, kann das cVEND in den Schlafmodus wechseln. Damit wird verhindert, dass eine noch aktive Applikation irrtümlich durch einen Schlafmodus unterbrochen wird.

ZVT-Kassenbefehl:

08 13 : ZVT Kommando: Ändere PT Konfiguration
 0F : Längenbyte
 06 0D : BMP06, Länge 13 Bytes
 E4 0B : Tag: Container Geräteinformationen, 11 Bytes
 FF 40 03 : Tag FF 40: Servicepasswort, Länge 3 Bytes
 12 34 56 : Servicepasswort
 FF 43 02 : Tag FF 43: Energiesparkonfiguration, Länge 2 Bytes
 14 : Leerlaufzeit, 20 Sek. 1 Byte
 01 : Anzahl Idle Applikationen, 00 = keine Energiesparfunktion, 01 = nur Bezahlapplikation,
 02...07 = Bezahlapplikation und weitere Applikationen, 1 Byte

Aufbau Abschlussmeldung cVEND:

06 0F : Abschlussmeldung
 00 : Länge

Die Leerlaufzeit bestimmt die Nachlaufzeit, die verstreicht, nachdem alle angemeldeten Applikationen Leerlauf gemeldet haben bis zum tatsächlichen Eintritt in den Schlafmodus.

Der Wert „Anzahl Idle Applikationen“ muss dabei der Anzahl der Applikationen im cVEND entsprechen, die tatsächlich ihren Leerlauf signalisieren können. Werden mehr Applikationen angemeldet, als im Gerät vorhanden sind, wird das cVEND niemals in den Schlafmodus fallen, da die konfigurierte Anzahl Leerlaufapplikationen dann nicht erreicht werden kann.

7.10. Beispiel: Druckerkonfiguration

Das cVEND Terminal bietet in bestimmten Konfigurationen die Möglichkeit, einen externen Belegdrucker anzusteuern. Um das Druckbild an unterschiedliche Druckermodelle anpassen zu können, kann der TOPP Applikation die maximal mögliche Anzahl von Druckpunkten (= Dots) pro Druckzeile des Druckers mitgeteilt werden.

Um eine maßstabsgerechte Darstellung der Druckzeichen auf dem Beleg zu erzielen, verwendet die TOPP Applikation ausschließlich den grafischen Druckmodus „8 Dots, single density“ entsprechend ESC/POS Code „0x1B 0x2A 0x00...“

Bei Druckern, die Belegschnitt (= Abschneiden des gedruckten Belegs) unterstützen, kann über ein weiteres Konfigurationsbyte die Art des Belegschnitts, teilweiser oder voller Schnitt, konfiguriert werden.

08 13 : ZVT Kommando: Ändere PT Konfiguration
 10 : Längenbyte
 06 0E : BMP06, Länge 14 Bytes
 E4 0C : Tag: Container Geräteinformationen, 12 Bytes
 FF 40 03 : Tag FF 40: Servicepasswort, Länge 3 Bytes
 12 34 56 : Servicepasswort
 FF 4B 03 : Tag FF 4B : Druckparameter, Länge 3 Bytes
 00 C0 : Druckbreite in Dots (192 Dots = Standardbreite SD bei 57mm Papierbreite), 2 Bytes
 01 : Schneidemodus: 00 = kein Belegschnitt, 01 = teilw. Belegschnitt, 02 = voller Belegschnitt

Aufbau Abschlussmeldung cVEND:

06 0F : Abschlussmeldung
00 : Länge

7.11. Beispiel: Terminal Betriebsmodus

Für bestimmte Umgebungen kann es erforderlich sein, den EMV-Betriebsmodus des cVEND Terminals von „unbedient“ (Standard) nach „bedient“ zu ändern.



Führen Sie diese Änderung ausschließlich nach Rücksprache und Freigabe durch Ihren Netzbetreiber durch! Ein willkürliches Ändern des Betriebsmodus kann ungewollte Auswirkungen auf die Zahlungsfunktionalität des cVEND Terminals haben.

Um die Umstellung erfolgreich vornehmen zu können, muss das cVEND zuvor über den Befehl Werkseinstellungen zurückgesetzt werden, so dass keine EMV-Konfigurationsdaten mehr vorliegen. Nach Ändern des Betriebsmodus muss eine Inbetriebnahme mit der zugewiesenen TID erfolgen.

Der aktuell eingestellte Betriebsmodus ist aus dem Systemdatenausdruck, Abschnitt „Konfiguration“, Feld „TrmType“ zu entnehmen.

08 13 : ZVT Kommando: Ändere PT Konfiguration
0E : Längenbyte
06 0C : BMP06, Länge 14 Bytes
E4 0A : Tag: Container Geräteinformationen, 12 Bytes
FF 40 03 : Tag FF 40: Servicepasswort, Länge 3 Bytes
12 34 56 : Servicepasswort
FF 4D 01 : Tag FF 4D : Terminal-Betriebsmodus (EMV Tag 9F35), Länge 1 Byte
16 : Betriebsmodus. 22 = bedient, 25 = unbedient.

Aufbau Abschlussmeldung cVEND:

06 0F : Abschlussmeldung
00 : Länge

7.12. Beispiel: cVEND Datei senden

Mit dem Befehl „Datei senden“ können Dateien an das cVEND Terminal übertragen werden. Speziell dient dieses Kommando dazu, über die Kassenschnittstelle aktualisierte Anwendungen oder Firmware-Aktualisierungen an das cVEND übertragen zu können und nach erfolgreicher Überprüfung eine Installation dieser zu veranlassen. Die Dateien müssen dazu eine gültige Signatur aufweisen sowie in einer speziellen Struktur vorliegen.

Ein mit dem FEIG cVEND SDK erzeugtes und mit dem Smart-Card-HSM signiertes Applikationsupdate besteht dabei immer aus den beiden Dateien:

- update.spec
- update.tar.gz

Diese Dateien können mit einem einzigen Befehl „Datei senden“ übertragen werden. Für jede zu sendende Datei muss dazu im ZVT-Kassenbefehl ein Tag 0x2D enthalten sein, das die Datei-ID und die Dateilänge spezifiziert.

Nach erfolgreicher Übertragung überprüft das cVEND die empfangenen Dateien auf Anzahl und Größe und legt diese in den zugehörigen Aktualisierungsordnern im cVEND ab. Beim folgenden Neustart werden die Dateien auf Größe, Inhalt und passende Signatur hin überprüft und bei positivem Ausgang installiert.



Damit dieses Kommando vom cVEND akzeptiert wird, dürfen keine Umsatzdateien mehr im cVEND gespeichert sein. Führen Sie daher zuerst die Funktion „Kassenschnitt“ durch und prüfen Sie deren erfolgreichen Verlauf.



Ist die Dateiübertragung erfolgreich, führt das cVEND ohne weitere Warnung einen Neustart durch, in dessen Verlauf die Softwareaktualisierung durchgeführt wird.

ZVT-Kassenbefehl:

08 14 : ZVT-Kommando: Datei senden
1D : Längenbyte
12 34 56 : Servicepasswort
06 18 : BMP06, Länge 24 Bytes
2D 0A : Tag: Dateiinformationen 1. Datei, Länge 10 Bytes
1D 01 20 : Sub-Tag: Datei-ID, Länge 1 Byte, siehe Tabelle 2
1F 00 04 : Sub-Tag: Dateilänge, 4 Bytes
00 00 02 67 : Längenangabe (hier: 615 Bytes)
2D 0A : Tag: Dateiinformationen 2. Datei, Länge 10 Bytes
1D 01 21 : Sub-Tag: Datei-ID, Länge 1 Byte, siehe Tabelle 2
1F 00 04 : Sub-Tag: Dateilänge, 4 Bytes
00 33 ED DC : Längenangabe (hier: 3403228 Bytes)

Bei korrektem Aufbau bestätigt das cVEND Terminal die Nachricht und fordert mit einer Dateianfragenachricht 040C den ersten Datenblock an:

04 0C 0D : Dateianfragemeldung, Länge 13 Bytes
06 0B : BMP06, Länge 11 Bytes
2D 09 : Tag: Anforderung 1. Datei, Länge 9 Bytes
1D 01 20 : Tag: Datei-ID, Länge 1 Byte
1E 04 00 00 00 00 : Offset des nächsten Dateiblocks

Die Kasse bestätigt die Dateianfragemeldung und startet die Dateiübertragung beginnend mit dem angeforderten Dateiblock.



Die Blocklänge bei der Dateiübertragung kann bis zu 64 kB betragen. Sie kann unabhängig von der max. ZVT-APDU-Länge (Tag 0x1A) in der ZVT-Anmeldung gewählt werden.

Wir empfehlen zur Optimierung der Übertragungsgeschwindigkeit bei der Dateiübertragung eine Blockgröße von 32 kB bis 64 kB zu nutzen.

Der letzte Datenblock kann in der Länge von den vorherigen Blöcken abweichen, um die tatsächliche Dateilänge zu erfüllen. Es darf kein „Auffüllen“ auf die vorher genutzte Blockgröße erfolgen.

80 00 FF 00 80 : ACK, 3-Byte Längensfeld: 32768 Bytes Nutzdaten
<Daten> : 32768 Bytes Nutzdaten.

Das cVEND bestätigt den erhaltenen Datenblock jeweils wieder mit einer Dateianfragemeldung wie oben, erhöht jedoch bei jeder Dateianfrage den Offsetwert um die Menge der bereits erfolgreich empfangenen Daten.

Mit weiteren Bestätigungs- und Anfragenachrichten wird somit die gesamte Datei übertragen. Das cVEND Terminal erwartet genau die Menge Datenbytes für jede Datei, die im zugehörigen Tag 0x1F angegeben wurde.

Wurde bei Übertragung über eine serielle Schnittstelle ein Datenblock fehlerhaft empfangen, so wird vom Terminal der fehlerhafte Block durch Wiederholen der entsprechenden Offsetangabe erneut angefordert. Ist auch nach drei Wiederholungen keine fehlerfreie Übertragung dieses Datenblocks gelungen, so wird die Dateiübertragung terminalseitig mit einer ZVT-Abbruchmeldung beendet und die bereits empfangenen Daten werden verworfen.

Die sendende Applikation muss daher bei jeder Dateianfragemeldung den vom Terminal übermittelten Offsetwert auswerten und daraus den nächsten zu sendenden bzw. zu wiederholenden Datenblock ermitteln.

Datei-IDs

Über die Datei-ID wird bestimmt, welches Ziel die zu übertragende Datei im Terminal hat. Dabei wird davon ausgegangen, dass ein mit dem FEIG SDK erzeugtes Applikationsupdate immer aus zwei Dateien besteht, ein cVEND Firmwareupdate aus vier Einzeldateien:

Applikationsupdate	Firmwareupdate
update.spec	kernel.gz
update.tar.gz	rootfs.gz
	u-boot.update.env.img.gz
	update.spec

Tabelle 1

Da das cVEND Terminal bis zu 8 verschiedene Applikationen verwalten kann, bestimmt die App-ID die Zugehörigkeit des Updates zur aktualisierenden Applikation.

Die Datei IDs folgen dabei dem Schema:

ID-Bereich (hex)	Zieldatei	Applikation / Firmware
10h	kernel.gz	cVEND Firmware
11h	rootfs.gz	cVEND Firmware
12h	u-boot.update.env.img.gz	cVEND Firmware
13h	update.spec	cVEND Firmware
20h	update.spec	cVEND TOPP – E2EE – app0

21h	update.tar.gz	cVEND TOPP – E2EE – app0
22h	update.spec	cVEND TOPP – app1
23h	update.tar.gz	cVEND TOPP – app1
24h	update.spec	Kundenapplikation – app2
25h	update.tar.gz	Kundenapplikation – app2
26h	update.spec	Kundenapplikation – app3
27h	update.tar.gz	Kundenapplikation – app3
28h	update.spec	Kundenapplikation – app4
29h	update.tar.gz	Kundenapplikation – app4
30h	update.spec	Kundenapplikation – app5
31h	update.tar.gz	Kundenapplikation – app5
32h	update.spec	Kundenapplikation – app6
33h	update.tar.gz	Kundenapplikation – app6
34h	update.spec	Kundenapplikation – app7
35h	update.tar.gz	Kundenapplikation – app7

Tabelle 2

Jede gültige Signatur einer Updatedatei enthält ebenfalls die Information über die Zielapplikation. Wird versehentlich eine Updatedatei mit falscher Datei-ID geladen, so wird der Fehler vom cVEND Updateprozess erkannt und die entsprechende Datei verworfen. Eine Beeinträchtigung anderer Applikationen durch fehlgeleitete Updatedateien ist dadurch ausgeschlossen.

Wird eine Updatedatei mit der gleichen Datei-ID wie eine vorhergehende Datei geladen, so wird dadurch die vorher geladene Datei überschrieben.

Für weitere Informationen über die cVEND Applikationsverwaltung siehe auch [3].

8. Erweiterungen des ZVT-Befehls „Ändere PT Konfiguration“ 0813

Um am unbedienten cVEND TOPP Einstellungen wie TCP/IP-Konfiguration, Konfiguration des Energiesparmodus oder MDB-Parameter über die ZVT-Schnittstelle vornehmen zu können, wurde der ZVT-Befehl „Ändere PT Konfiguration“ (0813) um zusätzliche Tags erweitert.

Alle Tags können analog Kap. „7.7. Beispiel: cVEND IP Konfiguration“ dem Kommando 0813 für die Konfiguration des jeweiligen Parameters übergeben werden.

Eine Übersicht der zusätzlichen Tags und ihrer Standardwerte liefert die folgende Liste:

Tag	Länge	Kodierung	Feldname	Standardwert	Beschreibung
FF40	6		Passwort		
	6	BCD	Service-Passwort	000000	kann Provider-abhängig variieren
FF41	7		cVEND Host Konfiguration		
	4	hex	Host IP Adresse	0.0.0.0	kann Provider-abhängig variieren
	2	hex	Host IP Port	0	kann Provider-abhängig variieren
	1	bin8	b0 : SSL, b1 : Message Framing, b2 : DFÜ über Kasse	0bxxxxxx00	b0 : 0 = kein SSL, 1 = SSL b1 : 0 = kein Msg Framing, 1 = Msg Framing b2 : 0 = DFÜ direkt, 1 = DFÜ über Kasse
FF42	17		cVEND IP Konfiguration		
	1	hex	Interface Byte	0x00	0x00 : Ethernet, 0x01 : IPoverUSB
	4	hex	IP-Adresse	0.0.0.0	0.0.0.0 : DHCP-Client aktivieren
	4	hex	Netzwerkmaske	0.0.0.0	auch bei DHCP-Betrieb erforderlich (0.0.0.0)
	4	hex	Gateway Adresse	0.0.0.0	auch bei DHCP-Betrieb erforderlich (0.0.0.0)
	4	hex	DNS Adresse	0.0.0.0	auch bei DHCP-Betrieb erforderlich (0.0.0.0)
FF43	2		Power Management		
	1		Idle Loop Intervall (s)	75	Nachlaufzeit vor Ruhezustand
	1	Highnibble	xxx1 : Wecken über Scheduler	1	1: ein, 0: aus
		Lownibble	Anzahl PM Applikationen	0	0 : kein PM, Dauerbetrieb 1 : Ruhezustand, wenn 1. App (TOPP) idle 2 : Ruhezustand, wenn 1. + 2. App idle 3 : ...

Tag	Länge	Kodierung	Feldname	Standardwert	Beschreibung
FF44	14		MDB LowLevel Konfiguration		
	1	hex	MDB Geräteadresse (hex)	10	entsprechend NAMA MDB Spez. 4.2
	4	hex	Master Timeout	200	ms/10
	4	hex	Interbyte Timeout	15	ms/10
	4	hex	Poll Idle Intervall	5000	ms
	1	bin	b0 : Pollantworten während Bootvorgang	0bxxxxxxx1	0 : keine Poll-Antworten vor Appl.-Start 1 : Poll-Antworten ab Power-On
FF45	18		State Machine Konfiguration		
	2	BCD	Währungskenner	1978	entsprechend NAMA MDB Spez. 4.2
	4	bin	Optionale Feature Bytes	0x0000002A	entsprechend NAMA MDB Spez. 4.2
	1	hex	max. Applikation Timeout	70	entsprechend NAMA MDB Spez. 4.2 (Max. non response time) (s)
	1	hex	Misc Options (hex)	01	entsprechend NAMA MDB Spez. 4.2
	1	hex	max. Reader Level (hex)	03	MDB Reader Level: 01 bis 03
	1	hex	min. Reader Level (hex)	01	MDB Reader Level: 01 bis 03
	1	hex	Betragsskalierung	1	entsprechend NAMA MDB Spez. 4.2 (Scale factor)
	1	hex	Dezimalstellen	2	entsprechend NAMA MDB Spez. 4.2 (Decimal places)
	4	hex	max. Aufladebetrag	0	entsprechend NAMA MDB Spez. 4.2 (Revalue limit amount)
	4	bin	Quirk Flags	0x00000002	b0 : Altersverifikation über Callback statt int. Behandlung b1 : Revalue Limit wirksam auch ohne Karte b2 : Vend Request auch aus Always Idle zulässig b3 : Revalue denied senden statt Revalue 0 b4 : Unterdrücke Kartenevent Callback in Always Idle b5 - b31 : reserviert
	1	hex	Methode Altersverifizierung	0	Siehe BDTA Jugendschutz Spez.
FF46	6		Applikationskonfiguration		
	1	hex	Druckmodus	0	0 : Zeilenlänge dyn. , max. FTL Blocklänge + CR 1 : bei Belegbreite <31: dyn. Länge FTL mit CR 2 : bei Belegbreite <31: dyn. Länge ohne CR 3 : Zeilenlänge = Beleglänge mit Padding , o. CR
	1	hex	Belegbreite	40 = 0x28	Druckzeichen
	4	hex	Dummy Credit	0	0 : 0xFFFF (0xFFFFFFFF bei 32-bit Beträgen)

Tag	Länge	Kodierung	Feldname	Standardwert	Beschreibung
FF47	1		Startmodus MDB-Dienst		
	1	hex	Definiert das Verhalten der cVEND TOPP Applikation zur Startkonfiguration des MDB-Dienstes.	0	0 : Vollautomatisch cVEND box / box+ : MDB-Dienst ein, cVEND plug : MDB-Dienst aus 1 : Automatisch: cVEND box / box+ : MDB-Dienst ein, cVEND plug: keine Änderung 2 : MDB-Dienst immer starten 3 : MDB-Dienst immer außer Betrieb 4 : Keine Änderung der Startkonfiguration, MDB-Dienst wird von TOPP Appl. nicht verwendet, MDB-Dienst kann von anderen Applikationen gestartet und verwendet werden.
FF48	2		Displayschoner (nur cVEND box+)		
	1	hex	Leerlaufzeit bis zum Einsetzen des Displayschoners	5	0 – 255 : Minuten (0= kein Bildschirmschoner)
	1	hex	Displayschoner Modus	1	0 : Display schwarz steuern 1 : Grafikanimation
FF49	1		Aufforderungston bei Zahlvorgängen		
	1	hex	Unterdrücken des akustischen Signals bei Zahlvorgängen	1	0 : Kein Aufforderungston 1 : Aufforderungston bei Zahlung aktiv
FF4A	1		MDB Applikations-Schalter		
	1	bin	MDB Kompatibilitätsflags	3	b0 : Aufforderungston bei Zahlung (0 = aus / 1 = ein) b1 : Display-Request zum VMC (0 = aus / 1 = ein) b2 : Ergebniston Zahlung (0 = ein, 1 = aus)
FF4B	3		Druckerkonfiguration		
	2	hex	Druckbreite	192	Druckbreite in Dots / Zeile
	1	hex	Schneidemodus Beleg	0	0 = kein Belegschnitt, 1 = Teilschnitt, 2 = Komplettschnitt
FF4C	1		Ergebniston bei Zahlvorgängen ZVT		
	1	hex	Unterdrücken des akustischen Ergebnissignals bei Zahlvorgängen	1	0 : Kein Ergebniston nach ZVT-Zahlung 1 : Ergebniston nach ZVT-Zahlung

FF4D	1		Terminal Modus		
	1	hex	Einstellen des Terminal-Betriebsmodus (nach EMV-Tag 9F35)	25	22 : Bedientes Terminal 25 : Unbedientes Terminal

CONFIDENTIAL

9. Transparenter Kanal

9.1. Übersicht

Die cVEND TOPP Applikation unterstützt neben dem Einsatz offizieller Bezahlkarten auch die Verwendung proprietärer Kontaktloskarten, die z.B. eine Kundenidentifikation oder eine Techniker-authentifizierung ermöglichen können.

Um vor einer Bezahlaktion bereits vom Anwender das Präsentieren einer Karte zwecks Erkennung des Kartentyps anzufordern, wird das ZVT-Kommando 06C0 „Read Card“ verwendet. Es fordert den Kunden zur Kartenpräsentation auf und identifiziert die erkannte Karte. Danach werden über die Kassenschnittstelle die Details und Parameter der Karte ausgegeben. Die Kassenanwendung kann nun über das weitere Vorgehen entscheiden.

ISO14443-4 Karten

Wurde durch ReadCard eine ISO14443-4-kompatible Karte erkannt, so können mittels 06C6 „Send APDU“ weitere Kommandos an die Karte abgesetzt werden. Diese müssen jedoch im jeweiligen Kartenkontext zulässig sein.

Bei ISO14443-4 Karten wird beim Read-Card zusätzlich ein Select-PPSE durchgeführt. Übermittelt die Karte daraufhin eine AID-Liste, so wird diese in der Rückgabemeldung des ReadCard-Befehls zur Kassenanwendung übermittelt. Die zurückgegebene AID-Liste kann dann von der Kassenanwendung verwendet werden, um gezielt eine der Anwendungen für eine folgende Transaktion zu selektieren.

Darüber hinaus sind SELECT-Kommandos auf andere Kartenapplikationen (AIDs) möglich. Die in SELECT Kommandos angegebenen AIDs werden dabei zusätzlich gegen eine im cVend Terminal hinterlegte Freigabeliste gefiltert, um missbräuchliche Zugriffe auf sicherheitsrelevante Applikationen zu verhindern.

Derzeit sind beispielsweise für die girocard die Applikationen DF_MARKTPLATZ, DF_FAHRSCHEIN oder DF_GELDKARTE selektierbar. Weitere Applikationen können vom FEIG Support der Freigabeliste hinzugefügt werden, wenn die entsprechende Berechtigung an ihrer Verwendung nachgewiesen wird.

Andere Karten (div. Mifare, FeliCa...)

Wenn der Befehl „ReadCard“ anhand des SAK ein anderes Kartenprotokoll als ISO14443-4 erkennt, so werden in der Antwort zur Kassenanwendung weitere Identifikationsmerkmale der Karte mitgeliefert, die der Kassenanwendung eine Identifikation des aktuellen Kartentyps ermöglichen.

Hat die Kassenanwendung die Karte erfolgreich identifiziert, kann sie auch hier mit dem Befehl 06C6 „SendAPDU“ weitere Daten mit der Karte austauschen.

Mifare-Funktionen

Für Mifare-Karten mit Sicherheitsfunktionen werden Befehle unterstützt, die diese Sicherheitsfunktionen bedienen und nach Laden der passenden kryptografischen Schlüssel und Authentifizierung des Terminals Zugriff auf deren gesicherte Bereiche ermöglichen.



Der Programmierer der Kassensoftware ist bei Verwendung dieser Befehle selbst dafür verantwortlich, insbesondere beim Beschreiben von Mifare-Karten die nötige Vorsicht walten zu lassen, damit nicht sicherheitsrelevante Bereiche der Karten versehentlich überschrieben und diese Karten dadurch ggf. unbrauchbar gemacht werden.

Befehlsübersicht „transparenter Kanal“

<i>Befehl</i>	<i>Name</i>	<i>Beschreibung</i>	<i>Karten</i>
06 C0	Read Card	Einlesen einer Karte, Ermitteln des Kartentyps	Alle
06 C1	Mifare Load Keys	Einbringen eines Mifare Schlüssels in das Kartenterminal zur nachfolgenden Authentifizierung	Mifare
06 C2	Mifare Authenticate	Authentifizierung des Terminals gegenüber einer Mifare Karte mittels eines der eingebrachten Schlüssel.	Mifare
06 C3	Mifare Read Block	Lesen eines Datenblocks von einer Mifare Karte	Mifare
06 C4	Mifare Write Block	Schreiben eines Datenblocks einer Mifare Karte	Mifare
06 C5	Close Session	Schließen des transparenten Kanals zur Karte und Ende der Sitzung.	Alle
06 C6	Send APDU	Senden eines Kartenkommandos und Empfangen der Kartenantwort.	Alle

9.2. Detailbeschreibung der Befehle

Karte lesen und identifizieren

Der Befehl „Read Card“ dient zum Erkennen und Identifizieren einer vom Kunden vorgehaltenen Karte. Der grundsätzliche Befehlsaufbau entspricht [PA00P015 13.08 en](#), S. 54.

Zusätzlich wird im BMP06 Container das folgende TLV-Tag ausgewertet:

<i>Tag</i>	<i>Länge</i>	<i>Kodierung</i>	<i>Feldname</i>	<i>Standardwert</i>	<i>Beschreibung</i>
1F15	1		Lesemodus		
	1	bin	Definiert die Leseparameter und Rückgabedaten.	C0h	b0 – b3 : nicht verwendet, RFU b4 : 0 = Lesen über Zahlungsmodul 1 = Nur Kartenidentifikation (keine LED-Fortschrittsanzeige) b5 : wie in ZVT (Betrag GK lesen)

					b6 : 1 = UID auslesen b7 : 1 = eindeutiges Token erzeugen

Nach Absenden des ReadCard Befehls aktiviert das cVEND Terminal das HF-Feld und fordert den Kunden zum Vorhalten einer Karte auf. Bei gesetztem Bit 4 in Tag 1F15h wird der Aufforderungston sowie die LED-Anzeige unterdrückt.

Abhängig von der erkannten Karte können in der Terminalantwort neben den in [PA00P015_13.08_en](#) definierten Tags und Strukturen folgende Tags erscheinen:

Tag	Länge	Kodierung	Feldname	Beschreibung
4C	10		UID	
	10	hex	UID, von vorne aufgefüllt auf 10 Bytes.	UID der Karte, kann für die meisten Karten ermittelt werden und dient der weiteren Identifizierung
1F45	var.		ATS	
	var.	hex	ISO14443-4 ATS	Inhalt des ATS (=Antwort auf RATS) bei ISO14443-4 kompat. Karten, wenn dieser übermittelt wurde.
1F4C	1		Kartentyp	
	1	hex	Ermittelter Kartentyp	00h : ISO14443-4 kompat. 01h : Mifare 02h : FeliCa
1F4D	2 o. 3		Karten Subtyp	
	2 o. 3	hex	Detaillierter Karten Subtyp aus ATQA	0001h : Mifare classic 1k 0002h : Mifare classic 4k 0003h : Mifare Ultralight 0004h : SLE55R 0026h : Mifare mini 0027h : Infineon My-D Move 002Fh : Jewel 0036h : Mifare plus SL1 2k 0037h : Mifare plus SL1 4k 0038h : Mifare plus SL2 2k 0039h : Mifare plus SL2 4k FE03h : Mifare Emulation FE04h : Mifare plus SL3 010344h : Mifare Desfire

1F4F	2		ATQA	
	2	hex	ATQA der gerade gelesenen Karte.	ATQA
1F50	1		SAK	
	1	hex	SAK der gerade gelesenen Karte	SAK Byte

APDU-Austausch zur Karte

Mit dem Befehl „SendAPDU“ (06C6h) können nach erfolgreicher Identifikation einer Karte weitere APDUs zur Karte gesendet werden und deren Antworten darauf empfangen werden.

Die grundsätzliche Verwendung des Befehls erfolgt gemäß [PA00P015 13.08 en](#) S.112

Der Befehl 06C6h „SendAPDU“ wird mit einem BMP06 Container versehen, der ein oder mehrere Tags 1F46h enthält, die jeweils eine APDU zur Karte enthalten.

Es besteht so die Möglichkeit, mit einem Befehlsaufruf mehrere APDUs mit der Karte auszutauschen.

Die Rückantwort des Terminals enthält außer der ZVT-ACK Sequenz wiederum einen BMP06 Container, der nach erfolgreicher APDU-Bearbeitung zu jedem gesendeten Tag 1F46 genau ein Antwort-Tag 1F46 mit der Kartenantwort auf die gesendete APDU enthält.

Bei APDUs, die ein SELECT-Kommando enthalten, wird der übergebene Dateiname gegen eine im cVEND-Terminal abgelegte Whitelist geprüft und nur nach deren pos. Antwort zur Karte gesendet.

Dadurch ist gewährleistet, dass über den transparenten Kanal keine Kartenfunktionen selektiert werden können, die die Sicherheit von Karte und cVEND-Terminal kompromittieren könnten.

Zurzeit werden SELECT-Kommandos auf die AIDs „2PAY.SYS.DDF01“ (PPSE), sowie die Short-IDs „d2 76 00 00 25 4d 01 02 00“, „d2 76 00 00 25 46 53 02 00“, „d2 76 00 00 25 46 53 02 00“ zugelassen.

Zur weiteren Verwendung des Befehls wird auf die Spezifikation [4] verwiesen.

Transparente Sitzung beenden

Der Befehl „Close Card Session“ (06C5h) beendet eine transparente Datensitzung mit einer Karte.

Die grundsätzliche Verwendung des Befehls erfolgt gemäß [PA00P015 13.08 en](#) S.112

Der Befehl 06C5h wird ohne weitere Daten (Länge Datenfeld =0) gesendet. Er beendet die Kommunikation mit der Karte und schaltet das HF-Feld des cVEND Lesers ab. Gleichzeitig wird der vom zugehörigen ReadCard-Befehl erzeugte Kartenkontext gelöscht.

„Close Card Session“ muss am Ende einer transparenten Datensitzung zur Karte aufgerufen werden, damit mit einem neuerlichen ReadCard-Befehl eine andere Karte aktiviert werden kann.

Mifare Sicherheitsschlüssel laden

Mit dem Befehl „Mifare Load Keys“ (06C1h) kann das cVEND Terminal auf eine Kartensitzung zu einer Mifare-Karte vorbereitet werden, wenn diese eine Authentifizierung des Terminals zum Zugriff verlangt. Mit diesem Befehl können ein oder mehrere Schlüsselcontainer im cVEND Terminal abgelegt werden. Ein folgender „Mifare Authenticate“ kann dann auf den benötigten Schlüssel referenzieren, um das cVEND-Terminal gegenüber der Karte zu authentifizieren.

Geladene Schlüssel bleiben bis zum Neustart des cVEND-Terminals erhalten und können somit auch für nachfolgende Mifare-Sitzungen genutzt werden.

Die Referenz auf einen bestimmten Schlüssels erfolgt durch den Schlüsseltyp und den Schlüsselindex.

Der Befehlsaufbau folgt der Form

06 C1 xx [06 <TLV-Container>] (xx=Länge der Befehlssequenz)

Im BMP06 Container ist pro zu übertragendem Schlüssel je ein E5 TLV-Container aufzubauen, der folgende Tags enthalten muss:

Tag	Länge	Kodierung	Feldname	Standardwert	Beschreibung
1F49	1		Schlüsseltyp		
	1	hex	Ordnet den Schlüssel einem Mifare-Kartentyp zu	n.v.	60h : Mifare classic key A 61h : Mifare classic key B 62h : Mifare ultralight key
1F4A	1		Schlüsselindex		
	1	hex	Dient zum Referenzieren auf diesen Schlüsselcontainers bei nachfolgendem Mifare Authenticate Befehlen	n.v.	numerischer Index
1F5C	var		Mifare Schlüssel		
	var	hex	Schlüsseldaten	n.v.	Mifare Schlüsseldaten im Klartext

Das cVEND Terminal antwortet mit einer Bestätigung „80 00“, wenn mindestens ein Schlüssel erfolgreich eingebracht wurde. Bei fehlerhafter Ausführung wird eine NAK-Sequenz „84 1E“ ausgegeben.

Mifare Authentifizierung

Mit dem Befehl „Mifare Authenticate“ (06C2h) kann sich das Terminal mit Hilfe eines der zuvor geladenen Mifare-Sicherheitsschlüssel (siehe Kap. „Mifare Sicherheitsschlüssel laden“) gegenüber einer Mifare-Karte authentifizieren. Eine erfolgreiche Authentifizierung erlaubt danach den Zugriff auf geschützte Datenblöcke der Mifare-Karte. Die Freischaltung eines Datenblocks wirkt jeweils für den gesamten Sektor, in dem er sich befindet. Um einen kompletten Mifare-Sektor freizuschalten genügt es daher, ein „Mifare Authenticate“ auf den ersten Datenblock des Sektors auszulösen.

Der Befehlsaufbau folgt der Form

06 C2 xx [06 <TLV-Container>] (xx=Länge der Befehlssequenz)

Im BMP06 Container sind für den Datenblock, der freigeschaltet werden soll, die Blocknummer sowie die Referenzen auf Schlüsseltyp und –index anzugeben. Dazu werden folgende TLV-Tags verwendet:

Tag	Länge	Kodierung	Feldname	Standardwert	Beschreibung
1F48	1-4		Blocknummer		
	1-4	hex	Eine Blocknummer aus dem Sektor, der freigeschaltet werden soll	n.v.	Blocknummer 0 - max. Blocknummer, abhängig von der Speichergröße der Karte
1F49	1		Schlüsseltyp		
	1	hex	Ordnet den Schlüssel einem Mifare-Kartentyp zu	n.v.	60h : Mifare classic key A 61h : Mifare classic key B 62h : Mifare ultralight key
1F4A	1		Schlüsselindex		
	1	hex	Dient zum Referenzieren auf diesen Schlüsselcontainers bei nachfolgendem Mifare Authenticate Befehlen	n.v.	numerischer Index

Mifare Datenblock lesen

Einzelne Datenblöcke einer Mifare Karte können mit dem Befehl „Mifare Read Block“ ausgelesen werden. Ist der jeweilige Sektor, in dem der Block enthalten ist, durch einen kryptografischen

Schlüssel geschützt, muss zuvor ein Block dieses Sektors über die Mifare Authentifizierung freigeschaltet worden sein.

Der Befehlsaufbau folgt der Form

06 C3 xx [06 <TLV-Container>] (xx=Länge der Befehlssequenz)

Im BMP06 Container sind die Nummer des zu lesenden Datenblocks sowie bei Mifare Ultralight ein zusätzlicher Zugriffskenner anzugeben. Dazu werden folgende TLV-Tags verwendet:

Tag	Länge	Kodierung	Feldname	Standardwert	Beschreibung
1F48	1-4		Blocknummer		
	1-4	hex	Blocknummer des auszulesenden Blocks	n.v.	Blocknummer 0 - max. Blocknummer, abhängig von der Speichergröße der Karte
1F4D	2		Zugriffskenner		
	2	hex	nur bei Mifare Ultralight erforderlich	00 03	zusätzlicher Zugriffskenner für Mifare Ultralight Tags

War der Zugriff auf den Datenblock erfolgreich, liefert das Terminal in der Bestätigung 80 00h einen BMP06 Container mit der Kartenantwort:

Tag	Länge	Kodierung	Feldname	Standardwert	Beschreibung
1F4B	16		Blocknummer		
	16	hex	Blockdaten	n.v.	Ausgelesene Blockdaten des angeforderten Blocks.

Mifare Datenblock schreiben

Um einen Datenblock einer Mifare-Karte zu beschreiben, kann der Befehl „Mifare Write Block“ (06 C3h) verwendet werden. Ist der jeweilige Sektor, in dem der Block enthalten ist, durch einen kryptografischen Schlüssel geschützt, muss zuvor ein Block dieses Sektors über die Mifare Authentifizierung freigeschaltet worden sein.

Der Befehlsaufbau folgt der Form

06 C4 xx [06 <TLV-Container>] (xx=Länge der Befehlssequenz)

Im BMP06 Container sind die Nummer des zu schreibenden Datenblocks sowie bei Mifare Ultralight ein zusätzlicher Zugriffskenner anzugeben. Dazu werden folgende TLV-Tags verwendet:

Tag	Länge	Kodierung	Feldname	Standardwert	Beschreibung
1F48	1-4		Blocknummer		
	1-4	hex	Blocknummer des zu beschreibenden Blocks	n.v.	Blocknummer 0 - max. Blocknummer, abhängig von der Speichergröße der Karte. Wird beim Schreiben mehrerer Blöcke eine Sektorgrenze überschritten, so endet der Befehl in einem Fehler, da u.U. für
1F4B	4 / 16				
	4 / 16	hex	Zu schreibende Blockdaten	n.v.	Blockdaten sollten in Vielfachen der jeweiligen Blockgröße von 16 Bytes (4 Bytes bei Mifare Ultralight) übergeben werden.
1F4D	2		Zugriffskenner		
	2	hex	nur bei Mifare Ultralight erforderlich	00 03	zusätzlicher Zugriffskenner für Mifare Ultralight Tags

Es ist mit „Mifare Write Block“ möglich, mehrere aufeinanderfolgende Blöcke eines Sektors in einem Befehl zu beschreiben. Wenn jedoch dabei eine Sektorengrenze überschritten wird, wird der gesamte Schreibvorgang mit Fehlermeldung abgebrochen.

„Mifare Write Block“ nimmt keine weiteren Plausibilitätsprüfungen gegen die Speicherstruktur der jeweiligen Karte vor. Der Programmierer ist dafür verantwortlich, beim Beschreiben von Mifare Karten die Speicherstruktur der jeweiligen Karte zu beachten. Beispielsweise führt ein versehentliches Beschreiben des letzten Blocks eines Sektors zum Überschreiben des zugehörigen kryptografischen Schlüssels, der Sektor kann dadurch unbrauchbar werden.

10. Quellennachweise

- [1] ZVT ECR Spezifikation, Version 13.08, 25. Mai 2018
- [2] FEIG – cVEND TOPP, Deutsche Poseidon Bezahlapplikation, Installations- und Kurzbedienungsanleitung. Feig H70310-Xd-ID-D
- [3] FEIG cVEND Software Development Kit – Handbuch
- [4] ISO7816-4:2013 : Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange

CONFIDENTIAL

11. Ansprechpartner

Bei Problemen oder Fehlern kontaktieren Sie bitte den FEIG Kundendienst über folgende E-Mail Adresse:

cVEND-support@feig.de

CONFIDENTIAL