Regelwerk für das deutsche ec-Geldautomatensystem

"Deutsches ec-Geldautomatensystem"
Vereinbarungen, Richtlinien, und Anlagen zu den
Verträgen über das deutsche ec-Geldautomatensystem

Übersicht über die deutsche ec-Geldautomaten-Vereinbarung

Vereinbarung über das deutsche ec-Geldautomatensystem

1 Bedingungen für den ec-Service

2 Richtlinien für das deutsche ec-Geldautomatensystem

- 1 Anforderungen an die Geräteausstattung und die Bedienerführung
- 2 Aufbau und Kurzbeschreibung der Magnetspuren
  - 1. Aufbau der Spur 3
  - 2. Aufbau der Spur 2
- 3 Verschlüsselungsverfahren innerhalb des deutschen ec-Geldautomatensystems
- 4 Datensätze für den nationalen Online-Verbund
  - 1. Beschreibung der Datensätze für die Autorisierungsnachrichten
  - 2. Beschreibung der Datensätze zur Netzwerküberwachung
  - 3. Beschreibung der Datensätze für die Advice-Nachrichten nach Ersatzautorisierungen
- 5 Sperrverarbeitung bei der Evidenzzentrale
  - 1. Datensätze für die Sperrenverarbeitung bei der Evidenzzentrale
  - 2. Verarbeitungsgrundsätze in der Evidenzzentrale
- 6 Lastschriften aus Verfügungen im Rahmen des deutschen ec-Geldautomatensystems
  - 1. Deutsche Karten an deutschen ec-Geldautomaten
  - 2. Ausländische Karten an deutschen ec-Geldautomaten
  - 3. Deutsche Karten an ausländischen ec-Geldautomaten
- 7 Kartenechtheitsprüfung nach dem MM-Verfahren

Anlage 1

Bedingungen für den ec-Service

Die Bedingungen werden derzeit überarbeitet, dieses Klauselwerk wird gesondert gemäß § 102 GWB gemeldet.

5. Für die Ausstattung der Karten und der ec-Geldautomaten sowie für die verfahrenstechnischen Bedingungen und die Sicherheitsanforderungen gelten die "Richtlinien für das deutsche ec-Geldautomaten-System" (Anlage 2) und die dazugehörigen Anhänge.

6. Für alle Fragen, die im Zusammenhang mit dieser Vereinbarung auftreten, ist im Rahmen des Betriebswirtschaftlichen Arbeitskreises der Spitzenverbände des Kreditgewerbes der Arbeitsstab "Geldautomaten" zuständig. Die Beschlüsse des Arbeitsstabes "Geldautomaten" sind für die angeschlossenen Institute bindend.

7. Das automatenbetreibende Institut ist berechtigt, zusammen mit dem Verfügungsbetrag von dem kartenausgebenden Institut ein Entgelt für die Benutzung seines ec-Geldautomaten zu verlangen. Die maximale Höhe des Entgelts für Verfügungen mit deutschen Karten wird von den Vertragspartnern im Arbeitsstab "Geldautomaten" festgesetzt. Das Entgelt für Verfügungen mit ausländischen Karten wird in Abstimmung mit EUROPAY International festgesetzt.

8. Sofern angeschlossene Institute im Zusammenwirken mit Unternehmen ec-Geldautomaten betreiben, darf weder durch Werbung noch durch Kennzeichnung der Eindruck entstehen, das Unternehmen sei der Betreiber des ec-Geldautomaten. Diese Institute haben die Unternehmen zu verpflichten, diese Regelung einzuhalten.

9. Bei Schäden, die durch die Benutzung von ec-Geldautomaten mit gefälschten oder verfälschten Karten entstehen, sowie bei sonstigen Schäden, die im Interesse des Systems abgedeckt werden müssen und deren Übernahme einem einzelnen Institut nicht zugemutet werden kann, erfolgt unter bestimmten Voraussetzungen ein Ausgleich zwischen den Vertragspartnern. Die näheren Einzelheiten sowie insbesondere der Schlüssel zur Umlage derartiger Schäden auf die einzelnen Vertragspartner werden vom Arbeitsstab "Geldautomaten" bestimmt. Bis zu einer Regelung werden diese Schäden von dem im Magnetstreifen der Karte spezifizierten Institut aufgenommen.

10. Änderungen dieser Vereinbarung nebst Anlagen beschließen die Vertragspartner auf Anregung des Arbeitsstabes "Geldautomaten". Sie werden für die angeschlossenen Institute verbindlich, wenn diese den Änderungen nicht binnen einer Frist von einem Monat nach deren Bekanntgabe widersprechen; auf diese Möglichkeit des Widerspruchs werden die angeschlossenen Institute bei Bekanntgabe der Änderungen in jedem Einzelfall hingewiesen. Widerspricht ein angeschlossenes Institut einer Änderung der Vereinbarung, die bei der Bekanntgabe ausdrücklich als wesentlich bezeichnet worden ist, so scheidet es mit dem Zeitpunkt des Inkrafttretens dieser Änderung aus dem deutschen ec-Geldautomatensystem aus.

11. Diese Vereinbarung kann von jedem der Vertragspartner mit einer Frist von 24 Monaten zum Ende eines jeden Monats gekündigt werden. Jedes angeschlossene Institut kann seine Teilnahme ebenfalls mit einer Frist von 24 Monaten aufkündigen; es haftet sodann, unbeschadet der Kündigung, für Schäden, die durch die Benutzung der von ihm ausgegebenen Karten entstanden

Für die Autorisierung institutsübergreifender Verfügungen sind die Nachrichtenbeschreibungen gemäß Anhang 4 maßgebend. Die Transaktionskosten für den online-Verbund bis zur Übergabestelle des kartenausgebenden Instituts werden von der GA-betreibenden Seite getragen.

5. Evidenzzentrale

Die Vertragspartner beauftragen eine Evidenzzentrale mit der Aufnahme und Verteilung von Sperren. Diese Evidenzzentrale ist außerdem für die Annahme und Verteilung von Notteiefonsperren zuständig.

Die Form der Meldungen für Sperren ist im Anhang 5 geregelt.

6. Benutzung der Sperren

Die angeschlossenen Institute verpflichten sich, weder Sperren zu von anderen Kreditinstituten ausgegebenen Karten - unabhängig davon, im Rahmen welcher Anwendung das Institut Kenntnis von der Sperre erlangt hat - an Dritte weiterzugeben noch diesen auf sonstige Weise zur Nutzung zur Verfügung zu stellen oder für diese zu nutzen.

7. Behandlung eingezogener Karten

Eingezogene Karten sind dem kartenausgebenden Institut mit bankülicher Sorgfalt unverzüglich gebührenfrei und nicht entwertet zuzuleiten. Das Versandrisiko trägt das kartenausgebende Institut. Eingezogene Karten ausländischer Emittenten sind an die von den Vertragspartnern jeweils genannte Stelle zu senden.

8. Einziehung der Aufwendungen

Die angeschlossenen Institute ziehen die Beträge, die von einem ec-Geldautomaten ausgezahlt worden sind, zusammen mit dem Entgelt per Lastschrift im Einzugsermächtigungsverfahren ein. Durch die Ausgabe von Karten ermachtigen die angeschlossenen Institute jedes andere Institut zur Einziehung von Beträgen, die durch eine Benutzung dieser Karten ausgezahlt worden sind, samt der hierdurch entstehenden Entgelte. Die Einziehung erfolgt unverzüglich nach der Benutzung der Automaten beleglos. Für die Verrechnung ist die Satzbelegung gemäß Anhang 6 maßgebend. Es gelten die Richtlinien für den belegiosen Datentragerausiausch mit der Maßgabe, daß für die Richtigkeit der Daten auf dem Magnetstreifen der Kartenausgeber einzustehen hat. Die angeschlossenen kartenausgebenden Institute lösen Lastschriften, mit denen die ausgezahlten Beträge und die Entgelte eingezogen werden, unverzüglich ein. Die Einlösungspflicht der kartenausgebenden Institute bezieht sich auf alle durch sie positiv autorisierte Verfügungen, es sei denn, der Geldautomatenbetreiber ist den ihm obliegenden Prüfvorschriften nicht nachgekommen.

Eine Rückgabe der Lastschriften wegen Widerspruchs, wegen fehlender Deckung oder aus anderen Gründen im Sinne des Abkommens über den Lastschriftverkehr ist nicht möglich. Reklamationen werden außerhalb des Lastschriftverfahrens unmittelbar zwischen den beteiligten angeschlossenen Instituten abgewickelt. Sollte es zwischen den beteiligten angeschlossenen Instituten insoweit zu keiner Einigung kommen, so wird der Arbeitsstab "Geldautomaten" eine Entscheidung herbeifuhren

-Verfügungszeit

-Betrag

-PAN (Erste Kontonummer aus Feld 3 der Spur 3)

-Kartenfolgenummer

-Verfalldatum der Karte

-Autorisierungskennzeichen aus der Antwortnachricht

(einschließlich der Rechner-ID)

-Transaktionsnummer

-Antwortcode

-Ergebnis der MM-Prüfung

13. Diese Daten sind 6 Jahre lang aufzubewahren. Bei elektronischer Aufbewahrung des Protokolls gelten die §§ 257 bis 261 HGB.

14. Die Vorderseite des Gerates sollte bei outdoor-Automaten hinlänglichen Schutz gegen Vandalismus bieten.

15. Die vom ec-Geldautomaten verwendeten kryptographischen Schlüssel sind in einer besonders gesicherten Umgebung abzulegen und zu verarbeiten.

16. ec-Geldautomaten sind mit einem MM-Sicherheitssystem auszustatten. Hierfur gilt Anhang 7.

17. Bei ec-Geldautomaten in angeschlossenen Instituten, die lediglich wahrend der Geschaftszeiten zugänglich sind, kann auf einen Tresorschutz für die MM-Box verzichtet werden, wenn die Box entsprechend - z. B. durch die Alarmanlage - gegen unberechtigten Zugriff geschützt ist. Bei allen übrigen Installationen ist die Box im Tresor unterzubringen. Dies gilt nicht für CIM-86.

18. Bei Aufstellung von ec-Geldautomaten im Zusammenwirken mit Unternehmen gelten die §§ 18, 19 UVV Kassen entsprechend. Es ist sicherzustellen, daß das Kreditinstitut oder seine Beauftragten jederzeit das Recht haben, den Aufstellungsort zu betreten, soweit dies zur Gewahrleistung der Betriebsfähigkeit oder der Sicherheit erforderlich ist.

Anhang 2 zu den Richtlinien für das deutsche ec-Geldautomatensystem

Aufbau und Kurzbeschreibung der Magnetspuren

1. Aufbau der Spur 3

Bankkarten - Magnetstreifenkarten - Aufbau und Inhalt der 3. Spur. Nachfolgend ist der Inhalt der DIN/ISO Norm 4909 - Stand Juni 1977 - Abschnitt 8 'Aufbau und Inhalt der Datenfelder auf der 3. Spur' abgedruckt.

Feld 1 Startzeichen (Start Sentinel)

Zweck Das Startzeichen ist das 1. Zeichen auf der Magnetspur und wird von den Leseeinrichtungen benutzt, um den Beginn der Daten zu erkennen.

Feldlänge 1 Stelle

Inhalt Nur 11 gemäß ISO 3554 Abschnitt 6.5.2 ist zulässig

Feld 2 Kennziffer für den Spuraufbau (Format Code)

Zweck Diese Ziffer kennzeichnet den Aufbau der Spur 3

Feldlänge 2 Stellen

Inhalt 00 Ungültig im internationalen Datenaustausch
01 Gültig im internationalen Datenaustausch

Anmerkung: Kartenausgeber, die Kennziffern aus dem Bereich 02-89 benutzen wollen, müssen über ihre nationalen Normenorganisationen einen entsprechenden Antrag an das zuständige ISO-Komitee richten.

Erläuterungen zu Feld 2

Die Kennziffern "90" bis "99" sind einer künftigen Vereinbarung des deutschen Kreditgewerbes vorbehalten.

Feld 3 PAN = Erste Kontonummer (Primary Account Number)

Zweck Eindeutige Kennzeichnung des Kartenausgebers, dem der Geschäftsvorfall zuzuordnen ist, sofern nicht andere Weisungen bestehen.

Feldlänge 22 Stellen

Inhalt		
	3.1 Branchenhauptschlüssel "59"	2 Stellen
	3.2 Bankleitzahl des kontoführenden Instituts	8 Stellen
	3.3 Feldseparator "D" nach ISO 3554 Abschnitt 6.5.2	1 Stelle
	3.4 Kundenkontonummer	10 Stellen
	3.5 Prüfziffer	1 Stelle

Beispiel: Kontonummer ohne Prüfziffer 4 992 739 871

	4	9	9	2	7	3	9	8	7	1
		x 2		x 2		x 2		x 2		x 2
		18		4		6		16		2

Schritt 1

	4+1+8+9+4+7+6+9+1+6+7+2 = 64	Schritt 2
oder	1+8+4+6+1+6+2+4+9+7+9+7 = 64	Schritt 2
oder	4+9+7+9+7+1+8+4+6+1+6+2 = 64	Schritt 2
	70-64 = 6	Schritt 3

Prüfziffer für die Kontonummer 4 992 739 871 = 6
Kontonummer mit Prüfziffer 4 992 739 871 6

Feld 4 FS = Feldseparator (Field Separator)

Zweck Kennzeichnung des Endes der 1. Kontonummer (PAN) unabhängig vom Vorhandensein der Daten.

Feldlänge 1 Stelle

Inhalt Nur 13 gemäß ISO 3554 Abschnitt 6.5.2 ist zulässig

Feld 5 Länderschlüssel (Country Code)

Zweck Bei Verwendung des Branchenhauptschlüssels "59" muß ein dreistelliger Länderschlüssel codiert werden, der das Land kennzeichnet, an das der durch die Karte ausgelöste Geschäftsvorfall zu leiten ist.

Feldlänge 3 Stellen

Inhalt 280

Feld 6 Währungsschlüssel (Currency Code)

Zweck Numerischer Wert des Währungsschlüssels, der die Art der Währung angibt, in der gerechnet werden muß.

Feldlänge 3 Stellen

Inhalt Drei Nullen in diesem Feld geben an, daß die Karte für den internationalen Austausch nicht zugelassen ist. Alle anderen Währungsschlüssel werden gemäß ISO 4217 abgeleitet; für die internationale ec-Karte ist der Währungsschlüssel 954.

Feld 7 Währungsexponent (Currency Exponent)

Zweck Zur Bestimmung des Geldwertes in den Feldern "Limit" (8) und "Restbetrag" (9).

Feldlänge 1 Stelle

Inhalt Null

Erläuterungen zu Feld 10:

Das Feld soll mit dem laufenden Datum beschrieben werden, wenn der Wert des Feldes "Zyklusbeginn" zuzüglich der "Zykluslänge" (Feld 11) weniger als das laufende Datum beträgt, außer die "Zykluslänge" ist mit "80" bis "99" codiert.
Dieses Feld wird im deutschen ec-GA-System nicht benutzt; es ist frei für institutsbezogene Anwendungen.

Feld 11 Zykluslänge (Cycle Length)

Zweck Bezeichnet den Zeitraum, in dem die Summe aller Verfügungen das Limit nicht übersteigen darf.

Feldlänge 2 Stellen

Inhalt

00	-	Eine Karte, auf der der Feldinhalt für den Restbetrag (Feld9) pro Zyklus nicht hochgeschrieben wird.
01-79	-	Anzahl der Tage, die einen Zyklus bilden.
80	-	Der Zyklus soll 7 Tage betragen. Das Feld Zyklusbeginn (10) wird durch Addieren von 7 bzw. einem Vielfachen von 7 auf den neuesten Stand gebracht.
81	-	Der Zyklus soll 14 Tage betragen. Das Feld Zyklusbeginn (10) wird durch Addieren von 14 bzw. einem Vielfachen von 14 auf den neuesten Stand gebracht.
82	-	1/2-Monatszyklus, der immer am 1. oder 15. Tag eines Kalendermonats beginnt.
83	-	Monatszyklus, der am gleichen Datum eines jeden Kalendermonats beginnen soll, abhängig von dem Datum, das im Feld Zyklusbeginn steht (10) und bei der Ausstellung der Karte festgelegt wurde.
84	-	3-Monatszyklus, der am gleichen Datum eines jeden dritten Kalendermonats beginnen soll, abhängig von dem Datum, das im Feld Zyklusbeginn steht (10) und bei der Ausstellung der Karte festgelegt wurde.
85	-	6-Monatszyklus, der am gleichen Datum eines jeden sechsten Kalendermonats beginnen soll, abhängig von dem Datum, das im Feld Zyklusbeginn steht (10) und bei der Ausstellung der Karte festgelegt wurde.
86	-	Einjahreszyklus, der am gleichen Datum eines jeden Kalenderjahres beginnen soll, abhängig von dem Datum, das im Feld Zyklusbeginn steht (10) und bei der Ausstellung der Karte festgelegt wurde.
87-99	-	Reserviert für die zukünftige Belegung durch ISO/TC 68

Erläuterungen zu Feld 11:

Die Kennziffern "87" bis "99" finden vorerst keine Verwendung.
Dieses Feld wird im deutschen ec-GA-System nicht benutzt; es ist frei für institutsbezogene Anwendungen.

Feld 12 Fehlbedienungszähler (Retry Count)

Zweck Registriert die Anzahl der noch möglichen Versuche, die persönliche Geheimzahl (PIN = persönlicher Geheimcode) einzugeben, die dieser Karte zugeordnet sind.

Feldlänge 1 Stelle

Feld 15 **Kontenart und Benutzungseinschränkung der ersten Kontonummer (Type of Account and Service Restriction - PAN)**

Zweck Die erste Stelle kennzeichnet die Art des Kontos in Feld 3. Die zweite Stelle legt die Art der zugelassenen Verfügung fest.

Feldlänge 2 Stellen

Inhalt Kontenart (1. Stelle)
2 Kontokorrentkonto
Benutzungseinschränkung (2. Stelle)
0 Keine Einschränkung
8 Autorisierung durch den Kartenausgeber
9 interner Gebrauch

Feld 16 **Kontenart und Benutzungseinschränkung für die zusätzliche Kontonummer-1 (Type of Account and Service Restriction - SAN-1)**

Zweck Wie bei Feld 15, aber auf die Kontonummer im SAN-1 Feld bezogen, wie in Feld 21 definiert.

Feldlänge 2 Stellen

Inhalt "00"

Erläuterungen zu Feld 16:

Dieses Feld wird im deutschen ec-GA-System nicht benutzt.

Feld 17 **Kontenart und Benutzungseinschränkung für die zusätzliche Kontonummer-2 (Type of Account and Service Restriction - SAN-2)**

Zweck Wie bei Feld 15, aber auf die Kontonummer im SAN-2 Feld bezogen, wie in Feld 23 definiert.

Feldlänge 2 Stellen

Inhalt "00"

Erlauterungen zu Feld 17:

Dieses Feld wird im deutschen ec-GA-System nicht benutzt.

Feld 18 **Verfalldatum (Expiry Date)**

Zweck Zur Angabe des Verfalldatums

Feldlänge 4 Stellen in der Form JJMM
JJ - Verfalljahr
MM - Verfallmonat

Erläuterungen Feld 23:

Karten im Sinne dieser Vereinbarung enthalten keine "zusätzliche Kontonummer-2".

Feld 24 FS = Feldseparator (Field Separator)

Zweck Angabe eines Festpunktes. Kennzeichnet Feldende der zusätzlichen Kontonummer-2 unabhängig davon, ob diese vorhanden ist.

Feldlänge 1 Stelle

Inhalt Nur 13 gemäß ISO 3554 Abschnitt 6.5.2 ist zulässig

Feld 25 Nachrichtenbegrenzungshinweis (Relay Marker)

Zweck Ermöglicht die Verkürzung der auszutauschenden Nachrichten. Gibt an, ob die im Feld 27 vorhandenen zusätzlichen Daten übernommen werden müssen.

Feldlänge 1 Stelle

Inhalt 1

Erläuterungen zu Feld 25:

Dieses Feld wird im deutschen ec-GA-System nicht benutzt.

Feld 26 Gesamtsicherheitsprüfung (Crypto Check Digit)

Zweck Schaffung einer sicherheitsmäßigen Bindung von Daten auf der Spur 3 und dem Magnetstreifen.

Feldlänge 1 Stelle

Inhalt FS - Feldseparator
Nur 13 gemäß ISO 3554 Abschnitt 6.5.2 ist gültig und zeigt an, daß zwischen den Daten auf Spur 3 und dem Magnetstreifen keine Gesamtsicherheitsprüfung vorgenommen wurde.

Feld 27 Zusätzliche Daten (Discretionary Data)

Zweck Zusätzliche Daten.

Feldlänge mindestens 12 Stellen,
maximal 26 Stellen

Inhalt Numerisch

Kurzbeschreibung der Spur 3

Feld-N	Dis	Feldbezeichnung	Codierung ec-int.	ec-nat.	Kundenk	Feldtyp
1	0	Startzeichen		X'B'		K
2	1	Formatcode	X'01'	X'00'	X'00'	K
3	3	PAN				
3.1	3	Branchenhauptschlüssel		X'59'		K
3.2	5	Blz kontoführendes Institut		X'nnnnnnnn		
3.3	1	Feldseparator		X'D'		K
3.4	1	Kundenkontonummer		X 'nnnnnnnnn		V
3.5	2	PZ-Prüfung nach Luhn		X'n'		V
4	2	Feldseparator		X'D'		K
5	2	Länderschlüssel		X'280'		K
6	2	Währungsschlüssel	X'954'	X'000'	X'000'	K
7	3	Währungsexponent		X'0'		K
8	3	Limit pro Zyklus		X 'nnnn'		I
9	3	Restbetrag pro Zyklus		X 'nnnn'		UI
10	4	Zyklusbeginn		X 'nnnn'		UI
11	4	Zykluslänge		X 'nn'		I
12	4	Fehlbedienungszähler		X 'n' n = 0 bis Anfangswert		U
13	4	PIN-PARM				
13.1	4	Algorithmusschlüssel		X '01'		K
13.2	5	Offset 1		X 'nnnn'		V
14	5	Freizügigkeitsschl.	X '0'	X '1'	X '2'	K
15	5	Kontoart und Benutzungseinschränkung				
15.1	5	Kontoart		X '2'		K
15.2	5	Benutzungseinschränk.	X '0'	X '0'	X '8'	K
16	5	Kontoart und Benutzg. SAN - 1 -		X '00'		K
17	5	Kontoart und Benutzg. SAN - 2 -		X '00'		K

2. Aufbau der Spur 2

Aufbau und Feldbelegung der Spur 2 von Magnetstreifen auf eurocheque- oder Kundenkarten zur Benutzung im ec-Geldautomatensystem

Der Aufbau und der Inhalt der Spur 2 entspricht den Definitionen des eurocheque ATM/POS Handbuchs.

Feld 1 Startzeichen (Start Sentinel)

Zweck Das Startzeichen ist das 1. Zeichen auf der Magnetspur und wird von den Leseeinrichtungen benutzt, um den Beginn der Daten zu erkennen.

Feldlänge 1 Stelle

Inhalt Nur 11 gemäß ISO 3554 Abschnitt 6.5.2 ist zulässig

Feld 2 PAN = Erste Kontonummer (Primary Account Number)

Zweck Eindeutige Kennzeichnung des Kartenausgebers und des Karteninhabers, dem der Geschäftsvorfall zuzuordnen ist.

Feldlänge 19 Stellen

Inhalt	2.1	2 Stellen	Branchenhauptschlüssel "67"
	2.2	1 Stelle	Kennzeichnung für Deutschland "2"
	2.3	1 Stelle	Kennzeichnung der Institutsgruppe
	2.4	4 Stellen	Kennzeichnung des Instituts innerhalb der Institutsgruppe
	2.5	10 Stellen	Kunden-Kontonummer (übereinstimmend mit Kontonummer in Spur 3)
	2.6	1 Stelle	Prüfziffer (Ermittlung siehe Beschreibung "Luhn-Check-Digit" der PAN in Spur 3)

Erläuterungen zu Feld 2.3:

Der Inhalt von Feld 2.3 ist wie folgt definiert:

1 = Postbank
2 = Banken
5 = Institute der deutschen Sparkassenorganisation
6 = Genossenschaftsbanken
9 = Genossenschaftsbanken

Feld 3 FS = Feldseparator (Field Separator)

Zweck Kennzeichnung des Endes der 1. Kontonummer (PAN) unabhängig vom Vorhandensein der Daten.

Feldlänge 1 Stelle

Inhalt Nur 13 gemäß ISO 3554 Abschnitt 6.5.2 ist zulässig

Kurzbeschreibung der Spur 2

Feld-Nr.	Displ.	Feldbeschreibung	Codierung ec-int.	Kundenk. i.-nat.	Kundenk. national	Feldtyp
1	0	Startzeichen		X'B'		K
2	1	PAN				
2.1	1	Branchenhauptschlüssel		X'67'		K
2.2	3	'Kurz-BLZ' kontoführendes Institut		X'2nnnnn'		I
2.3	9	Kundenkontonummer		X'nnnnnnnnnn'		I
2.4	19	Prüfziffer nach Luhn		X'n'		I
3	20	Feldseparator		X'D'		K
4	21	Verfallsdatum (JJMM)		X'nnnn'		V
5	25	Servicecode				K
5.1	25	Funktionskennzeichen	X'1'	X'1'	X'5'	K
5.2	26	Autorisierungskennzeichen	X'0'	X'0' oder X'2'	X'2'	K
5.3	27	Servicekennzeichen	X'1'	X'1' oder X'3'	X'1'	K
6	28	Zusätzliche Daten				
6.1	28	Reserviert		X'0'		K
6.2	29	PIN Verification Value		X'nnnn'		V
6.3	33	Kartenfolgenummer		X'n'		V
6.4	34	Reserve		X'nnnn'		V
7	38	Textendekennzeichen		X'F'		K
8	39	LRC-Zeichen		X'h'		V

Legende Abkürzungen :

Abkürzung:	Bedeutung :
X' '	Dateninhalt in hexadezimaler Darstellung
h	Hexadezimal = Zeichen von 0 bis F
n	numerisches Zeichen = Zeichen von 0 bis 9

Legende Feldtyp:

Feldtyp:		Bedeutung :
K	Konstante;	Inhalt für alle Karten, die an dem deutschen ec-GA-System teilnehmen, vorgeschrieben. Ändert sich nicht während Lebensdauer der Karte.
V	Variable:	Inhalt ist abhängig von der erstellten Karte. Ändert sich nicht während der Lebensdauer der Karte.
I	Institut:	Feld wird in der institutsübergreifenden Anwendung nicht genutzt. Es ist frei für eine institutsbezogene Nutzung.

Ermittlung der persönlichen Geheimzahl für den Kunden.

Zur Berechnung der persönlichen Geheimzahl wird das DES-Verfahren mit dem jeweiligen Institutsschlüssel als DES-Key angewandt.

Eingangswerte für diese Berechnung sind folgende Felder des Magnetstreifens:

- 3.2 Bankleitzahl (Stellen 4 bis 8) 5 Stellen
- 3.4 Kundenkontonummer 10 Stellen
- 19 Kartenfolgenummer 1 Stelle

Das Ergebnis des Algorithmus wird mit Hilfe der in DES vorgeschlagenen Umwandlungstabellen in einen 16stelligen Dezimalwert umgesetzt. Hierbei ergeben hexadezimal 0 bis 9, dezimal 0 bis 9 und hexadezimal A bis F dezimal 0 bis 5.

Hieraus bilden die Stellen 3 bis 6 die 4stellige persönliche Geheimzahl des Kunden. Wenn die Stelle 3 eine "0" ergibt, wird sie in eine "1" umgewandelt. (Diese Umwandlung unterbleibt bei der Berechnung der zur Offset-Ermittlung notwendigen Ergebnisse des DES-Algorithmus mit Poolschlüssel.)

Ermittlung der Offsets

Im deutschen ec-Geldautomatensystem werden maximal 2 Schlüssel vorrätig gehalten und wahlweise eingesetzt:

- Der Institutsschlüssel, der zur Ermittlung und Prüfung der persönlichen Geheimzahl der eigenen Kunden des Instituts herangezogen wird, das den ec-GA betreibt
- Der Poolschlüssel, der zur Ermittlung und Prüfung der persönlichen Geheimzahl aller anderen Benutzer dient

Bei institutsinterner Nutzung ist die vom Kunden eingetastete persönliche Geheimzahl mit dem Ergebnis der unter Punkt 2 beschriebenen Algorithmus-Rechnung zu vergleichen.

Bei institutsübergreifender Nutzung ist folgender Rechenvorgang anzuwenden:

Eingetastete persönliche Geheimzahl des Kunden

./. Ergebnis des DES-Algorithmus mit Poolschlüssel

= jeweils gültiger Offset

oder

Ergebnis des DES-Algorithmus mit Poolschlüssel

+ jeweils gültiger Offset

= vom Kunden eingetastete persönliche Geheimzahl

Die empfangende Übergabestelle prüft die zulässige Verwendung der gesendeten Generationsnummer in Relation zu der absendenden Rechner-ID.

Bei einer etwaigen Kompromittierung eines in Produktion befindlichen Keys nutzt die Übergabestelle des Schlüsseleigners nur noch das nicht kompromittierte Key-Set.

Gleichzeitig hat der Schlüsseleigner durch ein schriftliches Avis an die anderen Übergabestellen und die Übertragung eines neuen Key-Sets (unter der Generationsnummer des kompromittierten Key-Sets) an die Verlage den notwendigen Schlüssel-Wechsel einzuleiten.

Die o. a. Prozedur kann auch zu einem vorbeugenden Schlüssel-Wechsel benutzt werden.

Nach schriftlicher Weisung des Schlüsseleigners an die Übergabestellen ist die Nutzung einer Schlüsselgeneration im System nicht mehr zulässig. Nach einer solchen Weisung dürfen Anfragen mit dieser Schlüsselgeneration nicht mehr bearbeitet werden und das Key-Set mit dieser Generationsnummer ist bis zur Verteilung neuer Schlüssel unter dieser Generationsnummer gesperrt.

PIN-Block-Berechnung und -Prüfung (PAC-Verfahren)

Vor der Übertragung ist die PIN wie folgt zu verschlüsseln:

1. Aufbau des PIN-Blocks

Ausgangsgröße der PIN-Verschlüsselung ist ein Klartext PIN-Block (PB), bestehend aus 64 bits. Der PIN-Block ist wie folgt aufzubauen:

PIN-Block

PB-Teil	Anzahl der Stell (Halbbyte)	Bit	Inhalt	Erläuterung
1	1	1 - 4	X '4'	Länge der Geheimzahl
2	4	5 - 20	XL4 'n'	Geheimzahl
3	restliche Stellen	21 - 64	XL 11 '0'	Kontrollzeichen

Der Klartext PIN-Block wird mit dem PIN-Block-Key (oder PAC-Master-Key) unter Verwendung des DES-Algorithmus verschlüsselt.

Ist der PIN-Block-Key verschlüsselt gespeichert, so ist er zunächst zu entschlüsseln (vgl. die nachstehende schematische Darstellung).

MAC(1)	=	EKS (Block 1)
MAC(i)	=	EKS (Block (i) xor MAC (i-1)) (i>1)
MAC	=	MAC (n)

Wobei die Nachricht aus einer Anzahl (n) von 8 Byte-Blocks besteht.

Block i	=	der i-te 8 Byte Block einer Message.
Block n	=	letzter Block einer Message.

Falls dieser kürzer als 8 Bytes ist, wird er rechts mit hex. Null gefüllt.

Berechnung des Session-Keys für den MAC

Die Sicherung der Nachricht erfolgt unter Verwendung eines MAC-Session-Keys, der für jede Nachricht nach folgendem Prinzip neu gebildet wird:

Zunächst wird ein 64 bit-langer Zufallswert erzeugt. Dieser Zufallswert wird unter Verwendung des DES-Algorithmus und des MAC-Master-Keys entschlüsselt. Das Ergebnis dieser Rechnung ist der für die MAC-Berechnung benötigte MAC-Session-Key (vgl. nachstehende Abb. Teil 1).

Der Zufallswert, der für die Berechnung des Session-Keys gebildet wurde, ist zur Prüfung der MAC-Rechnung durch den Nachrichtenempfänger in Bit-Map-Pos. 57 einzustellen. In Bit-Map-Pos. 57 (9. Stelle) ist die Schlüsselgeneration des MAC-Master-Keys anzugeben.

Berechnung des MAC

Unter Verwendung dieser Session-Keys und nach dem oben beschriebenen ANSI-Algorithmus wird der MAC berechnet (vgl. Abb. Teile 2 und 3). Das Ergebnis dieser Rechnung ist der MAC, der in Bit-Map-Pos. 64 eingestellt wird.

Mit diesem Session-Key wird der MAC der empfangenen Nachricht nach dem gleichen Verfahren wie beim Sender errechnet und das Ergebnis der Berechnung mit dem in Bit-Map-Pos. 64 enthaltenen Wert verglichen.

Abkürzungen und Definitionen

-	Key	=	64 bits
-	EXXX	=	encrypted unter dem XXX-Key
-	(XXX)	=	verschlüsselter Key
-	=>EXXX(YYY)	=	der Key YYY wurde mit dem Key XXX verschlüsselt
-	KS	=	Session-Key = Key zur Berechnung/ Prüfung eines MA
-	KSB	=	MAC-Master-Key
-	PB	=	PIN-Block
-	KP	=	PIN-Block-Key
-	KKi	=	der i-te Key (i=1-9)
-	KT	=	Transport-Key oder Terminal-Key

Die obengenannten Keys haben folgende Funktionen:

a) Terminal (Transport)-Key (KT)

Der Terminal- oder Transport-Key dient zur Verschlüsselung von sicherheitsrelevanten Keys auf Transportwegen und bei der Speicherung von verschlüsselten Keys außerhalb von HSM.

Ein Host-Master-Key kann ebenfalls ein KT sein.

b) PIN-Block-Key (KPi)

Der PIN-Block-Key (auch PAC-Master-Key) dient zur Verschlüsselung des PIN-Blocks. Er wird mit einem KT verschlüsselt verteilt.

- kennzeichnet den Schlüssel, der zur Verschlüsselung des PAC verwendet wurde.
- ist gruppenübergreifend in der angefügten Schlüsselnummerntabelle vereinbart.

c) MAC-Master-Key (KSBi)

Der MAC-Master-Key dient zur Entschlüsselung einer Zufallszahl, die in BMP 57 als mit dem MAC-Master-Key verschlüsselter Session-Key für die MAC-Verifizierung eingestellt wird.

- kennzeichnet den Schlüssel, der zur Verschlüsselung des PAC verwendet wurde.
- ist gruppenübergreifend in der angefügten Schlüsselnummerntabelle vereinbart.

Gruppenübergreifend sind sowohl für den PIN-Block-Key wie auch für den MAC-Master-Key mehrere Schlüssel definiert und den Verbandsgruppen zugeordnet.

Der Absender einer Nachricht bestimmt durch seine Zugehörigkeit zu einer der definierten Schlüsselgruppen die 'Generation' des Schlüssels beim Senden.

Durch Steuerparameter ist vorzusehen, daß im laufenden Betrieb von einer Schlüsselgeneration auf eine andere umgeschaltet werden kann.

Es werden bis zu 9 PIN-Block- und MAC-Master-Keys gekennzeichnet als KP1 ... KP9 und KSB1.....KSB9 geliefert.

BMP	max. Stellen	Bytes	Format	Bezeichnung	Inhalt	national 10 12 10 13	10 12 13 10	0 4 0 0	0 4 1 0
11	6	3	pov	Transaktionsnummer des GA (GV.Nr.)		X	U	X	U	A	U
Beispiel für den Dateninhalt: X'123456' (möglichst täglich eindeutig pro GA) Prüfvorschriften BMP 11 - keine											
12	6	3	pov	Uhrzeit	HHMMSS HHMM = Uhrzeit in der Lastschrift	X	U	X	U	A	U
Beispiel für den Dateninhalt: X'120000' Hinweis - gesetzliche Vorschriften über Sommer- und Winterzeit beachten Prüfvorschriften BMP 12 - Die Uhrzeit darf max. 2 Stunden von der Uhrzeit in der AZ abweichen. Sekunden werden nicht in die Prüfung einbezogen. - die Prüfung wird nur bei der Nachzeit 0200 und 0320 durchgeführt Fehlerbehandlung - Antwortcode 98											
13	4	2	pov	Datum	MMTT = Datum in der Lastschrift	X	U	X	U	A	U
Beispiel für den Dateninhalt: X'1231' Hinweis - Schaltjahre und Jahreswechsel beachten Prüfvorschriften BMP 13 - das Datum in den Autorisierungsanfragen muß, mit der Ausnahme gegen Mitternacht, dem laufenden Tagesdatum entsprechen - 120 Min. vor und 120 Min. nach 00.00 darf das Datum für den folgenden bzw. zurückliegenden Tag verwendet werden - die Prüfung wird nur bei der Nachricht 0200 und 0320 durchgeführt Fehlerbehandlung - Antwortcode 98											
14	4	2	pov	Verfallcatum der Karte	JJMM Spur 3 Feld 18	X	U	X	U	A	U
Beispiel für den Dateninhalt: X'9412' Prüfvorschriften BMP 14 - bei ec-Karte - MM = 12 oder 11 - JJ = nicht kleiner lfd. Jahr und nicht großer lfd. Jahr plus 2 bei Kundenk. - MM nicht kleiner 01 und nicht großer 12 - JJ = nicht kleiner lfd. Jahr - wenn Jahr = lfd. Jahr, dann muß der Monat gleich oder großer lfd. Monat sein. Fehlerbehandlung - Antwortcode 33 oder 30											
20	4	2	pov	Landercode der Kart	Feld 5 Spur 3	X	-	X	-	A	-
Beispiel für den Dateninhalt: '0280' Prüfvorschriften BMP 20 - X'0280' Fehlerbehandlung - Antwortcode 30											
23	4	2	pov	Kartenfolge-Nr	Feld 19 aus Spur 3	X	U	X	U	A	U

BMP	max. Stellen	Bytes	Format	Bezeichnung	Inhalt	national 0 2 0 1 0 0	0 2 0 0	0 3 1 0	0 3 2 0	0 4 0 0	0 4 1 0
Beispiel für den Dateninhalt: - BMP 33.1: X'F0F3' fix - BMP 33.2: X'254999' Definition - Unter der anfragenden Stelle ist die Stelle zu verstehen, die für den GA verantwortlich die Nachricht aufbaut und absendet. - Unter der autorisierenden Stelle ist das System zu verstehen, welches z.B. eine Autorisierungsanfrage positiv oder negativ beantwortet. Prüfvorschriften BMP 33 - Die beiden erstenStellen 21,22, 25, 26, und 29 sind zu prüfen. Fehlerbehandlung - Im Fehlerfall wird die Nachricht nicht beantwortet.											
34				PAN	bei MII (Branchenhauptschlüssel) = 59	X	U	X	U	A	U
34.1	2	2	CL2	Längenfeld	X'F1F1'						
34.2	22	11	hex	Datenfeld	aus Feld 3 Spur 3 linksbündig						
Beispiel für den Dateninhalt: - BMP 34.1: X'F1F1' fix - BMP 34.2: X'5940050000D11111111119' Prüfvorschriften BMP 34 1.) X'59' gefolgt von 2.) X'nnnnnnnnn' 8 Stellen BLZ: 1. Stelle der BLZ 1-8 3.) X'D' Feldseparator 4.) X 'nnnnnnnnnn' 10 Stellen Kontonummer 5.) X'n' Prüfziffer der PAN nach Luhn prüfen Fehlerbehandlung - Antwortcode Prüfung 1 bis 4 : AC 30											
38	6	3	pov	Autorisierungs-KZ	Referenz-Nr. der AZ	-	X	-	X	-	X
Beispiel für den Dateninhalt: X'123456' Hinweis - Die Referenz-Nummer muß pro autorisierender Stelle kalendertäglich eindeutig sein. - national - wenn Nachrichtenart = X'0210', BMP 3.1 = X'0100'' BMP 25 = X'60' und BMP 39 = X'00' dann DTA-Lastschrift mit C6a X'1' im ersten Halbbyte von links, dahinter rechtsbündig die Referenznummer gepackt ohne Vorzeichen und in C7a/b '05001' Prüfvorschriften BMP 38 - keine											
39	2	1	pov	Antwort code	00 - Transaktion ok Feld 27.1 bei 0210 immer beschreiben - in Nachricht 0330: zulässige Anzahl PI Fehlversuche nicht überschritten, Feld gem. BMP 63 beschreiben - in Nachricht 0410: Storno ok	-	X	-	X	-	X

BMP	max. Stellen	Bytes	Format	Bezeichnung	Inhalt	national 0 0 0 0 0 0 / 2 2 3 3 4 4 / 0 1 2 3 0 1 / 0 0 0 0 0 0
42	(16)	(8)	pov	Kennzeichnung des GA-Betreibers		X U X U A U
42.1	8	4	pov	interne Daten des GA-Betreibers	Die linken 4 Bytes können durch den Absender der Nachrichten 0200, 0300 und/oder 0400 mit andere Werten als mit X'00000000 belegt werden (z.B. logisc Terminalnummer). Die Werte müssen num. sein.	
42.2	8	4	pov	Bankleitzahl des GA-Betreibers	= BLZ des GA-Betreibers in der Lastschrift	

Beispiel für den Dateninhalt:
- BMP 42.1: X'nnnnnnnn'
- BMP 42.2: X' 50050000

Hinweis
- Die BMP 42 wird in den Nachrichten 0210, 0330 und 0410 unverändert zurückgegeben.

Prüfvorschriften BMP 42.1
- keine

Prüfvorschriften BMP 42.2
- keine

Fehlerbehandlung
- Antwortcode 30

47				Einzelelemente der Karte aus Spur 3		X - X - - -
47.1	3	3	CL3	Längenfeld	X'F0F1F1'	
47.2	22	11	pov			
-1					6 Stellen Feld 13 2 Stellen Algorithmus-schlüssel 4 Stellen Offset 1	
-2					4 Stellen Feld 27.1 Datum der letzten Verfügung	
-3					4 Stellen Feld 27.2 Offset 2/PVV	
-4					4 Stellen Feld 27.3 Offset	
-5					1 Stelle MM-Prüfung Konstant '1' MM korrekt	
-6					1 Stelle Feld 14 Freizügigkeitsschlüssel	
-7					2 Stellen Feld 15 1 Stelle Kontoart 1 Stelle Benutzungseinschränkung	

BMP	nax. Stellen	Bytes	Format	Bezeichnung	Inhalt	national 02 02 03 03 04 04 01 11 21 31 01 11 10 10 00 00 00 01
Beispiel für den Dateninhalt: BMP 52.1 X' AF7E41D698BA36B0' Prüfvorschriften BMP 52 - keine Aufbau des klaren PIN-Blocks: - X ' nppppp00000000000' - n = Anzahl eingegebener Ziffern für die PIN - pppp = Ziffern 1-4 - 0 = restliche Stellen hinter der PIN bis zur 8 Byte-Länge Fehlerbehandlung - Antwortcode 99						
57				Session-Key		X X X X X X
57.1	3	3	CL3	Längenfeld	X'F0F0F9'	
57.2		8	b		für die jeweilige Anfrage gültiger Schlüssel, verschlüsselt mit MAC-Master-Key	
57.3	2	1	b		Schlüsselnummer - 01 bis 09 reserviert für GA-international und für gruppenübergreifenden Verbund zwischen BdB, BVR, DSGV und VO 01/05 BdB 02/06 BVR 03/07 DSGV 04/08 VOB 09 Test	
Beispiel für den Dateninhalt: - BMP 57.1: 'F0F0F9' fix - BMP 57.2: 'hhhhhhhhhhhhhhhh' - BMP 57.3: '01' Hinweis für die Auswahl des Schlüssels: - Die eine Nachricht absendende Übergabestelle verwendet zur Verschlüsselung (Bildung/Umschlüsselung PAC und MAC) unabhängig vom Empfänger einen seiner Keys (01 bis 08, beim Test 09) Prüfvorschriften BMP 57 - siehe gesonderte Beschreibung über Verschlüsselungsverfahren Fehlerbehandlung - siehe gesonderte Beschreibung über Verschlüsselungsverfahren						
58				Ersatzangabe/ Restlimit bzw. Kontostand		- 0 - - - -
58.1	3	3	CL3	Längenfeld		
58.2	12	6	pov	in der Bedeutung 'noch verfügbarer Betrag'	Inhalt X'F0F0F6' DM rechtsbündig mit 2 Dezimalstellen	
Beispiel für den Dateninhalt: - BMP 58.1: X'F0F0F6' - BMp 58.2: X ' 00000000035000' = verfügbarer Betrag DM 350.-- Erläuterung zu BMP 58 - nur bei BMP 3= X'0100' und BMP 39 = X'13' ist in der Nachricht 0210 der noch verfügbare Betrag enthalten (auch Null möglich)						

Verstöße gegen das definierte Datenformat werden mit Antwortcode 30 beantwortet

Regeln für die Prüfungspflicht:

Der Absender einer z. B. Autorisierungsanfrage muß alle vorgegebenen Prüfungen durchführen, die ihm möglich sind.

Der Autorisierende hat a l l e definierten Prüfungen durchzuführen.

Werden Nachrichten 'nur' weitergeleitet, sind die Prüfungen unter der Beschreibung des Nachrichtentypes und der Bit-Map-Positionen 1, 3 und 33 beschrieben.

Die Antwort einer autorisierenden Stelle ist der entsprechenden Anfrage zuzuordnen. Ist diese Zuordnung nicht möglich, so ist die Antwortnachricht nicht weiter zu bearbeiten. Sofern die Transaktion seitens des Geldautomaten noch offen ist, so ist eine Ersatzautorisierung in der den GA unterstützenden AZ nicht zulässig.
Bei unplausiblen Dateninhalten der BMP 33, 39, 57 oder 64 kann so verfahren werden, als wäre der Antwortcode '96' eingegangen. Zusätzlich ist beim Nachrichtentyp 0210 eine Korrekturmeldung - mit BMP 25 = '97' - dann abzusetzen, wenn die MAC-Verifizierung der Antwortnachricht Fehler ergibt.

Stornierung von Autorisierungsanfragen:

Stornierungsnachrichten vom Nachrichtentyp 0400 für eine Autorisierungsanfrage werden max. 2 mal wiederholt.

BMP	max. Stellen	Bytes	Format	Bezeichnung	Inhalt	0 8 0 0	1 8 1 0
13	4	2	pov	Datum	Format MMTT	X	U
Beispiel für den Dateninhalt: X'1231' Hinweis - Schaltjahre und Jahreswechsel beachten Prüfvorschriften BMP 13 - keine Fehlerbehandlung - Antwortcode 98							
33				Rechner-ID	Kennzeichen der anfragenden bzw. antwortende Übergabestelle		
33.1	2	2	CL2	Längenfeld	X'F0F3'	X	X
33.2	6	3	pov	Datenfeld	Durch ZKA sind definiert '21nnnn' = Postbank '22'nnnn' = Banken '25nnnn' = Sparkassen/LB '26nnnn' = GENO '29nnnn' = GENO	X	X
Beispiel für den Dateninhalt: - BMP 33.1: 'X' F0F3' fix - BMP 33.2: X'254999' Prüfvorschriften BMP 33 - Die beiden ersten Stellen 21. 22. 25. 26. und 29 sind zu prüfen Fehlerbehandlung - Im Fehlerfall wird die Nachricht nicht beantwortet							
39	2	1	pov	Antwortcode	00 - Transaktion ok 91 - AS nicht erreicht 96 - Bearbeitung z.Z. nicht möglich; 96 - MAC falsch; 98 - Abweichung Datum/ Uhrzeit	- - - -	X X X X
Beispiel für den Dateninhalt: X'00' Prüfvorschriften BMP 39 - bei ungültigen Antwortcodes Anfrage nach n Minuten wiederholen							
42	(16)	(8)	pov	Kennzeichnung des absendenden Systems		X	U
42.1	8	4	pov	interne Daten des absendenden Systems	Die linken 4 Bytes können durch den Absender der Nachrichten 0800 mit anderen Werten als X'00000000' belegt werde (z.B. logische Terminal-nummer) Die Werte müssen num. sein.		
42.2	8	4	pov	Bankleitzahl des anfragenden Syste	ggf. Pseudo-BLZ		

Regel für die Belegung der Bit-Map-Positionen:

Alle bei der jeweiligen Nachricht in der Tabelle nicht mit '-' oder 'O' gekennzeichneten BMP sind M u ß f e l d e r.

Kennzeichen für Datenformate:

b	=	binär
hex	=	hexadezimal
p	=	dezimal gepackt mit Vorzeichen
pov	=	dezimal gepackt ohne Vorzeichen
CLn	=	Character in der Länge n

Verstöße gegen das definierte Datenformat werden mit Antwortcode 30 beantwortet.

Regeln für die Nutzung der Netzwerknachrichten.

Netzwerknachrichten werden "nur" zwischen den Übergabestellen der Netze ausgetauscht.

Mit ihrer Hilfe wird die "Betriebsbereitschaft" einer "Übergabestelle" überwacht.
Ebenfalls wird mit ihrer Hilfe das alternative Routing und das Umschalten von Primär- auf Sekundär-System (und zurück) durchgeführt.

Entsprechende Regeln für das Umschalten sind von den Übergabestellen vorzugeben.

BMP	nax. Stel-len	By-tes	For-mat	Bezeichnung	Inhalt	0 8 0 0	0 8 1 0
Beispiel für den Dateninhalt: X '120000' Hinweis - gesetzliche Vorschriften über Sommer- und Winterzeit beachten Prüfvorschriften BMP 12 - Die Uhrzeit darf max. 2 Stunden vor der Uhrzeit in der AZ abweichen. Sekunden werden nicht in die Prüfung einbezogen. - die Prüfung wird nur bei der Nachricht 0200 und 0320 durchgeführt Fehlerbehandlung - Antwortcode 98							
13	4	2	pov	Datum	MMTT = Datum der Lastschrift	X	U
Beispiel für den Dateninhalt: X'1231' Hinweis - Schaltjahre und Jahreswechsel beachten Prüfvorschriften BMP 13 - das Datum in den Autorisierungsanfragen muß, mit der Ausnahme Mitternacht, dem laufenden Tagesdatum entsprechen - 120 Min. vor und 120 Min. nach 00.00 darf das Datum für den folgenden bzw. zurückliegenden Tag verwendet werden - die Prüfung wird nur bei der Nachricht 0200 und 0320 durchgeführt Fehlerbehandlung - Antwortcode 98							
14	4	2	pov	Verfalldatum der Karte	JJMM Spur 3 Feld 18	X	U
Beispiel für den Dateninhalt: X' 9412' Prüfvorschriften BMP 14 bei ec-Karte - MM = 12 oder 11 - JJ = nicht kleiner lfd. Jahr und nicht größer lfd. Jahr plus 2 bei Kundenk.- MM nicht kleiner 01 und nicht großer 12 - JJ = nicht kleiner lfd. Jahr - wenn Jahr = lfd. Jahr, dann muß der Monat gleich oder größer lfd. Monat sein Fehlerbehandlung - Antwortcode 33 oder 30							
23	4	2	pov	Kartenfolge-Nr	Feld 19 aus Spur 3	X	U
Beispiel für den Dateninhalt: X'0001' Prüfvorschriften BMP 23 - X'000' bis X'0009' - bei der Prüfung am Konto oder an einer Karten-Datei - Datenbank wird auf exakt gültige Karte geprüft Fehlerbehandlung - bei ungleich 0 - 9 Antwortcode 30							
25	2	1	pov	Konditionscode	'60 Fremder Kunde	X	U
Beispiel für den Dateninhalt: X ' 60' Prüfvorschriften BMP 25 - nur X'60' erlaubt Fehlerbehandlung - Antwortcode 30							

BMP	max. Stellen	Bytes	Format	Bezeichnung	Inhalt	0	0
						8	8
						0	1
						0	0
Beispiel für den Dateninnalt: X'00' Prüfvorschriften BMP 39 - bei ungültigen Antwortcodes Protokoll ins Fehlerlog							
41	8	4	pov	örtliche GA-Num-m (des GA -Betreibers	rechtsbundig, rechten 4 Stellen = Termi- nalnummer (Maschinen- nummer) in der Lastschrif	X	U
Beispiel für den Dateninnalt: X'nnnn1234' Prüfvorschriften BMP 41 - keine							
42	(16)	(8)	pov	Kennzeichnung des GA-Betreibers		X	U
42.1	8	4	pov	interne Daten des G Betreibers	Die linken 4 Bytes können durch den Absender der Nachrichten 0120 mit anderen Werten als mit X'00000000' belegt werde (z.B. logische Terminal- nummer). Die Werte müssen num. sein.	X	U
42.2	8	4	pov	Bankleitzahl des G Betreibers	= BLZ des GA-Betreibers in der Lastschrift		
Beispiel für den Dateninhalt: - BMP 42.1: X'nnnnnnnn' - BMP 42.2: X'50050000' Hinweis - Die BMP 42 wird in der Nachricht 0120 unverändert zurückgegeben Prüfvorschriften 42.1 - keine Prüfvorschriften 42.2 - keine Fehlerbehandlung - Antwortcode 30							
47				Einzelemente der Karte aus Spur 3		X	-
47.1	3	3	CL3	Längenfeld	X'F0F1F1'		
47.2	22	11	pov		6 Stellen Feld 13		
- 1 0					2 Stellen Algorithmus- schlüssel 4 Stellen Offset 1		
- 2					4 Stellen Feld 27.1 Datum der letzten Verfügung		
- 3					4 Stellen Feld 27.2 Offset2/PVV		
- 4					4 Stellen Feld 27.3 Offset 3		
- 5					1 Stelle MM- Prüfung Konstant '1' MM korrekt		

Beispiel für den Dateninhalt: - BMP 57.1: 'F0F0F9' fix - BMP 57.2: 'hhhhhhhhhhhhhhhh' - BMP 57.3: '01' Hinweis für die Auswahl des Schlüssels: - Die eine Nachricht absendende Übergabestelle verwendet zur Verschlüsselung (Bildung/Umschlüsselung MAC) unabhängig vom Empfänger einen seiner Keys (01 bis 08, beim Test 09). Prüfvorschriften BMP 57 - siehe gesonderte Beschreibung über Verschlüsselungsverfahren Fehlerbehandlung - siehe gesonderte Beschreibung über Verschlüsselungsverfahren						
64		8	b	MAC	X	X
Beispiel für den Dateninhalt: X'hhhhhhhhhhhhhhhh' Prüfvorschriften BMP 64 - siehe gesonderte Beschreibung über MAC-Verschlüsselungsverfahren						

Legende und Erläuterungen:

X'h' = Darstellung eines hexadezimalen Wertes
X = Absender einer Nachricht muß den Wert des Feldes (BMP) bestimmen oder einstellen
Ü = Übernahme des Wertes aus der zugehörigen Nachricht 0200, 0320, oder 0400
A = Übernahme des Wertes aus der zugehörigen Anfrage 0200
O = Optional in der Antwort 0210
n = Wert von '0' bis '9'
h = Wert von '0' bis 'F'

Regel für die Belegung der Bit-Map-Positionen:

Alle bei der jeweiligen Nachricht in der Tabelle nicht mit '-' oder 'O' gekennzeichneten BMP sind M u ß f e l d e r.

Anhang 5 zu den Richtlinien für das deutsche ec-Geldautomatensystem
Sperrverarbeitung bei der Evidenzzentrale

1. Datensätze für die Sperrenverarbeitung bei der Evidenzzentrale

Vorsatz (A-Satz)

Feld	Länge Bytes	von - bis Bytes	Format	Inhalt	Erläuterungen
1	4	1-4	b	Satzlänge	Längenangabe des Satzes nach den Konventionen für variable Satzlängen (Satzlängenfeld 4 Bytes, davon 2 Bytes linksbündig binär belegt, restliche Bytes X'40' bzw. X'00)
2	1	5-5	CL1	Satzart	Konstante 'A'
3	8	6-13	CL8	Bankleitzahl	Bankleitzahl des absendenden Rechenzentrums
4	8	14-21	CL8	Bankleitzahl	Bankleitzahl des empfangenden Rechenzentrums (Evidenzzentrale)
5	4	22-25	CL4	Paßwort	Absenderkennwort
6	6	26-31	CL6	Datum	JJMMTT, Datum der Weiterleitung
7	6	32-37	CL6	Uhrzeit	HHMMSS, Uhrzeit der Weiterleitung
8	3	38-40	CL3	Versions-Nr.	fortlaufende Versions-Nr. von der Evidenzzentrale (nur in der Datei von der Evidenzzentrale an Teilnehmer) (sonst C ' ' oder CL3 '0'
9	40	41-80	CL 40	frei	CL 40 ' ' oder CL 40 '0'
	80				

Feld	Länge Bytes	von - bis Bytes	Format	Inhalt	Erläuterungen
					22 - Systemsperre bei Mehrfachverfügungen oder Umsetzung einer von EPI erzeugten Priorität-1 Sperre EINZUG 23 - Systemsperre bei mehr als drei PIN-Fehlversuchen im Inland 24 - Sperre durch Kunden über Notte-lefon (siehe Hinweis 2) EINZUG 25 - Systemsperre bei mehr als drei PIN-Fehlversuchen im Ausland ABWEISUNG 27 - Sperre einer Karte für die Nutzung im Ausland (siehe Hinweis 3) ABWEISUNG 29 - Sperre alle einer BLZ zuzuordnenden Karten (siehe Hinweis 1) ABWEISUNG Anwendungssperren: 31 - Sperre der Scheckfunktion im Inland ABWEISUNG 32 - Sperre der Geldautomatenfunktion. ABWEISUNG 33 - Sperre der elect.-cash-Funktion ABWEISUNG 34 - Sperre der Geldautomaten- und der Scheckfunktion ABWEISUNG 35 - Sperre der electr.-cash- und der Scheckfunktion ABWEISUNG 36 - Sperre der electr. cash- und der Geldautomatenfunktion ABWEISUNG Schlüsselzahlen für Plausibilitätsprüfunge und Fehlermeldungen (siehe Hinweis 4) 50 - Bankleitzahl nicht plausibel 51 - Kontonummer nicht plausibel 52 - Kartenfolge-Nr. nicht plausibel oder zulässig, zulässiger Inhalt : - bei ec-Karten: 0-9 oder A - bei Kreditkarten: X'40' 53 - Datum/Uhrzeit nicht plausibel 54 - Schlüsselzahl falsch oder nicht plausibel 55 - Nachsatz falsch 56 - Satzart falsch 57 - Institut zur Sperraufhebung nicht berechtigt 58 - Feld 11 nicht plausibel 59 - Feld 12 nicht plausibel 60 - Sperre für bereits gesperrte Karte 61 - einer/mehrere Sperre/en oder einer/mehrer Sperraufhebung/en der gleichen Karte

Anmerkung:

Die Verarbeitung des Feldes 1 ist vorerst nicht gegeben, muß jedoch zukünftig möglich sein.

Hinweise:

1. In diesem Fall enthalten die Felder 4 und 5 in Satzart 'C' Nullen. Feld 6 enthält das Verfalldatum oder Nullen.

2. Telefonisch (durch den Kunden) aufgegebene Sperrmeldungen sind durch das kartenausgebende Institut unverzüglich aufzuklären. Die 24er Sperre ist aufzuheben und durch eine Karten- oder Kontosperre mit zutreffendem Verfalldatum (nicht '0000') zu ersetzen. Ist das Feld 'Verfalldatum der Karte' bei dem Sperrenschlüssel 24 mit einem Verfalldatum gefüllt, muß das entsprechende Feld der Sperraufhebung mit dem gleichen Inhalt versehen werden. Enthält das Feld 'Verfalldatum der Karte' bei dem Sperrenschlüssel 24 '0000', muß das entsprechende Feld der Sperraufhebung ebenfalls '0000' enthalten.

3. Die Sperre ist für solche Fälle vorgesehen, bei denen nur die Nutzung der Karte im Ausland ausgeschlossen werden soll. Sie ist nur nach mißbräuchlichen Verwendungen der Karte oder der Kartendaten im Ausland zu verwenden.

4. Bei Fehlermeldungen der Evidenzzentrale werden die Inhalte der Felder 1 - 7 sowie 9 und 10 aus der eingegangenen Meldung unverändert zurückgegeben.

5. Sollen alle für eine Kontonummer ausgegebenen Kartenfolgenummern mit dem entsprechenden Verfalldatum gesperrt werden, so enthält dieses Feld 'A'.

2. Verarbeitungsgrundsätze in der Evidenzentrale

Ordnungsbegriff

Ordnungsbegriffe für die Sperrenverarbeitung in der Evidenzzentrale sind:

- Bankleitzahl
- Kontonummer
- Kartenfolgenummer
- Verfalldatum

Folgende Kombinationen von signifikanten Daten, 'Ersatzwerten' und Sperrenschlüsseln sind erlaubt:

Bankleitzahl	Kontonummer	Karten-folge-nummer	Verfall-datum	erlaubt bei Sperrenschl.	Bedeutung/Wirkung
nnnnnnnn	0	0	0000	nur 29	Sperre aller Karten einer Bankleitzahl al Verfalljahre
nnnnnnnn	0	0	nnnn	nur 29	Sperre aller Karten einer Bankleitzahl eines Verfalljahres
nnnnnnnn	nnnnnnnnnn	n	nnnn	alle außer 29	Sperre einer Karte/Sperre einer oder mehrerer Funktionen einer Ka
nnnnnnnn	nnnnnnnnnn	A	nnnn	20 und 24	Sperre aller Karten eines Kontos mit einem Verfalldatum
nnnnnnnn	nnnnnnnnnn	A	0000	nur 24	Sperre aller Karten eines Kontos mit jedem Verfalldatum

"n" kennzeichnet einen signifikanten Feldinhalt, also eine existente Bankleitzahl, Kontonummer, Kartenfolgenummer oder Verfalldatum.

Andere "Kombinationen" von signifikanten Feldern und Ersatzwerten als in der Tabelle dargestellt sind nicht erlaubt.

Löschungen für in der Evidenzzentrale gespeicherte Sperren müssen in allen Feldern des Ordnungsbegriffes die gleichen Werte enthalten wie der Eintrag in der Evidenzzentrale.

Es muß der dem Sperrschlüssel zugeordnete Schlüssel für die Aufhebung der Sperre verwendet werden.

Sperren, die in einem Teil des Ordnungsbegriffes einen 'Ersatzwert' enthalten, sind "Gruppensperren" weil sie für eine "Gruppe" von Karten gelten.

Weiterleitung von Sperren an EUROPAY Brüssel

Die Sperren im deutschen ec-Geldautomatensystem werden taggleich an EUROPAY Brüssel weitergeleitet.
Dabei werden sie nach folgender Tabelle in Schlüssel umgesetzt. die nach der Definition im ATM-/POS-Handbuch für das europäische ec-Geldautomaten-Netz gültig sind :

Schlüssel national		Schlüssel/Priorität international
10 - 19	-->	0
22 - 23	-->	2
20	-->	3
24	-->	3
27	-->	5
29	-->	5

2. Verarbeitungsgrundsätze in der Evidenzentrale

Ordnungsbegriff

Ordnungsbegriffe für die Sperrenverarbeitung in der Evidenzzentrale sind:

- Bankleitzahl
- Kontonummer
- Kartenfolgenummer
- Verfalldatum

Folgende Kombinationen von signifikanten Daten, 'Ersatzwerten' und Sperrenschlüsseln sind erlaubt:

Bankleitzahl	Kontonummer	Karten-folge-nummer	Verfall-datum	erlaubt bei Sperrenschl.	Bedeutung/Wirkung
nnnnnnnn	0	0	0000	nur 29	Sperre aller Karten einer Bankleitzahl al Verfalljahre
nnnnnnnn	0	0	nnnn	nur 29	Sperre aller Karten einer Bankleitzahl eines Verfalljahres
nnnnnnnn	nnnnnnnnnn	n	nnnn	alle außer 29	Sperre einer Karte/Sperre einer oder mehrerer Funktionen einer Ka
nnnnnnnn	nnnnnnnnnn	A	nnnn	20 und 24	Sperre aller Karten eines Kontos mit einem Verfalldatum
nnnnnnnn	nnnnnnnnnn	A	0000	nur 24	Sperre aller Karten eines Kontos mit jedem Verfalldatum

"n" kennzeichnet einen signifikanten Feldinhalt, also eine existente Bankleitzahl, Kontonummer, Kartenfolgenummer oder Verfalldatum.

Andere "Kombinationen" von signifikanten Feldern und Ersatzwerten als in der Tabelle dargestellt sind nicht erlaubt.

Löschungen für in der Evidenzzentrale gespeicherte Sperren müssen in allen Feldern des Ordnungsbegriffes die gleichen Werte enthalten wie der Eintrag in der Evidenzzentrale.

Es muß der dem Sperrschlüssel zugeordnete Schlüssel für die Aufhebung der Sperre verwendet werden.

Sperren, die in einem Teil des Ordnungsbegriffes einen 'Ersatzwert' enthalten, sind "Gruppensperren" weil sie für eine "Gruppe" von Karten gelten.

Feld	Lange Bytes	von-bis Bytes	Format	Inhalt	Erläuterungen
		75-75		X'40'	1 Stelle
		76-79		Verfalldatum	'JJMM' aus BMP 14 der Nachricht 0200
		80-87		XL8'40'	8 Stellen
		88-91		Gebühr des GA-Betreibers	'DMPF' mit führenden Nullen ohne Komm 2 Stellen DM und 2 Stellen Pfennige
15	27	92-118	CL27	Kundeninfor-matio	linksbündig
		92-99		Bankleitzahl	8 Stellen (BLZ des GA-betreibenden Instituts) aus BMP 42.2 der Nachricht 020
		100-100		X'40'	1 Stelle
		101-104		Maschinen-Nr.	4 Stellen die rechten vier Stellen aus BMP 41 der Nachricht 0200
		105-105		X'40'	1 Stelle
		106-110		Uhrzeit der Verfügung	5 Stellen HH.MM die linken vier Stellen aus BMP 12 der Nachricht 0200 druckaufbereitet
		111-111		X'40'	1 Stelle
		112-116		Konstante 'KARTE'	5 Stellen
		117-117		X'40'	1 Stelle
		118-118		Kartenfolge-numm	1 Stelle aus Feld 19 der Spur 3
16	27	119-145	CL27	Kundeninfor-matio	linksbündig
				Konstante	
		119-128		'EC-AUTOMAT'	10 Stellen
		129-129		X'40'	1 Stelle
		130-134		Datum der Verfügung	5 Stellen TT.MM aus BMP 13 der Nachricht 0200 druckaufbereitet
		135-135		X'40'	1 Stelle
		136-145		Ortsbezeich-nung	10 Stellen Kurzbezeichnung des GA-Standortes (nic belegte Stellen = X'40')
17	3	146-148	b	3X'40'	Reserve
18	2	149-150	p	Erweiterungs-kennzeichen	X'000F'
	150				

CLnn = alpha-numerische Daten (linksbündig, nicht belegte Stellen X'40')
p = numerische Daten gepackt, positives Vorzeichen
pov = numerische Daten gepackt, ohne Vorzeichen
b = binär
num = numerisch, nur Ziffern 0 - 9

Feld	Lange Bytes	von-bis Bytes	Format	Inhalt	Erlauterungen
		80-80		X'40'	1 Stelle
		81-84		Maschinen-numme	4 Stellen die rechten vier Stellen aus BMP 41 der Nachricht 0100 'GA international aktiv'
		85-85		X'40'	1 Stelle
		86-89		Verfalldatum	4 Stellen JJMM aus BMP 14 der Nachricht 0110 'GA international aktiv'
		90-90		X'40'	1 Stelle
		91-91		Kartenfolge-numm	1 Stelle aus BMP 23 der Nachricht 0110 'GA international aktiv'
15	27	92-118	CL27	Internationale Cleanrnginfor- mati PAN	bis 19 Stellen aus Feld 2 der Spur 2, linksbündig aus BMP 2.2 der Nachricht 0110 'GA international aktiv' (in Character) Rest X '40'
16	27	119-145	CL27	Internationale Clearinginfor- mationen	
		119-128		Standort des GA	10 Stellen
		129-129		X'40'	1 Stelle
		130-137		Verfügungsbetrag	8 Stellen DM ohne Gebühren rechtsbündig ohne Punkt und Komma mit 2 Dezimalstellen a BMP 4 der Nachricht 0110 'GA internatio aktiv'
		138-138		X'40'	1 Stelle
		139-144		Referenznummer der AZ	6 Stellen aus der BMP 38 der Nachricht 0110 'GA international aktiv'
		145-145		X'40'	1 Stelle
17	3	146-148	b	3X'40'	Reserve
18	2	149-150	p	Erweiterungs- kennzeichen	X'000F'
	150				

CLnn =alpha-numerische Daten (linksbündig, nicht belegte Stellen X'40')
p =numerische Daten gepackt, positives Vorzeichen
pov =numerische Daten gepackt, ohne Vorzeichen
b =binär
num =numerisch, nur Ziffern 0-9

Feld	Länge Bytes	von - bis Bytes	Format	Inhalt	Erläuterungen
		79-81		3X'40'	3 Stellen
		82-90		Ref Nr der Verrechnungsstelle	9 Stellen
		91-91		X'40'	1 Stelle
15	27	92-118	CL27	Kunden-information	linksbündig
		92-97		Konstante 'EC-GAA'	6 Stellen wenn Zahlungssystem = ec und wenn BMP 3 der Nachr. 0100 'GA international passiv'=Rechner-ID der GZS dann Konstante 'EC-GAA'
		98-98		X'40'	1 Stelle
		99-103		Konstante 'KARTE'	5 Stellen
		104-104		X'40'	1 Stelle
		105-105		Kartenfolge-nummer	1 Stelle aus BMP 23 der Nachricht 0100 'GA international passiv'
		106-106		X'40'	1 Stelle
		107-110		Konstante 'KURS'	4 Stellen
		111-118		Kurs der Fremdwährung XXX.XXXX	8 Stellen
16	27	119-145	CL27	Kundeninfor-matio	
		119-121		Währungsbe-zeichnung	3 Stellen
		122-130		Währungsbetrag XXXXXX.XX	9 Stellen
		131-140		Konstante 'FREMDGBDM'	10 Stellen
		141-145		Fremgebühren XX.XX	5 Stellen
17	3	146-148	b	3X'40'	Reserve
18	2	149-150	p	Erweiterungs-kennzeichen	X '001F'
	150				

Anhang 7 zu den Richtlinien für das deutsche ec-Geldautomatensystem

Kartenechtheitsprüfung nach dem MM-Verfahren.

Grundsätze der MM-Prüfung

Die Auswertung des MM-Prüfergebnisses muß im Transaktionsverlauf so angeordnet sein, daß die vorgeschriebene Reaktion in Abhängigkeit von dem Ergebnis vor einer für den Kunden (auch z. B. durch den Ablauf) erkennbaren Aussage "PIN falsch" oder "PIN richtig" erfolgt.

Transaktionen mit deutschen Karten im deutschen ec-Geldautomatensystem sind nur statthaft, wenn durch den GA-Betreiber das positive Ergebnis der MM-Prüfung festgestellt wurde.

Das Ergebnis ist positiv, wenn von der MM-Box der Geldautomatensoftware die Qualitat "1 bis 5" gemeldet wird.

Wird die Qualität "6" gemeldet, sind die MM-Merkmale zwar vorhanden, aber nicht lesbar. Die Karte ist abzuweisen.

Ist das Ergebnis der MM-Prüfung negativ (stimmt also der Referenzwert in der Spur 3 nicht mit dem von der MM-Einrichtung aktuell ermittelten Wert überein), ist die Karte einzuziehen.

Bei (Funktions-)Fehlern des MM-Systems ist der (Lese- und MM-Prüf-) Vorgang zu wiederholen und die Karte bei Andauern der Störung abzulehnen.

Karten ohne MM-Merkmal wird die Qualität "0" zugeordnet. Hat die eingegebene Karte die Merkmale der zum System gehörenden Karten (Spuraufbau, Ländercode, Freizügigkeitsschlüssel, Benutzungseinschränkung und Kartensicherungscode) und wird die Qualität "0" erkannt, so ist die Karte einzuziehen.