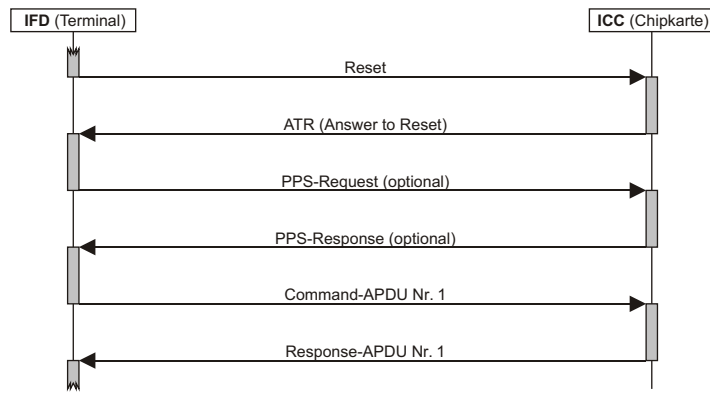
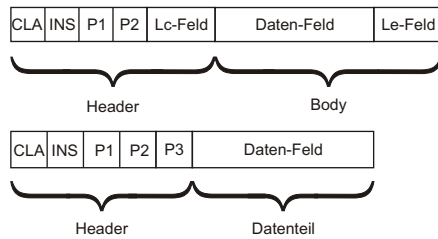


Datenübertragung

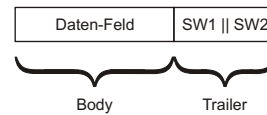


Aufbau von APDUs

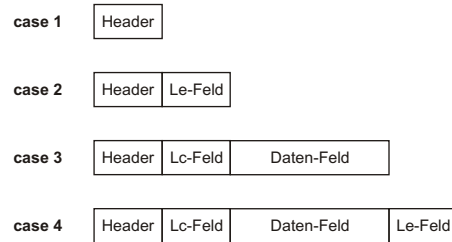
Kommando-APDU



Antwort-APDU



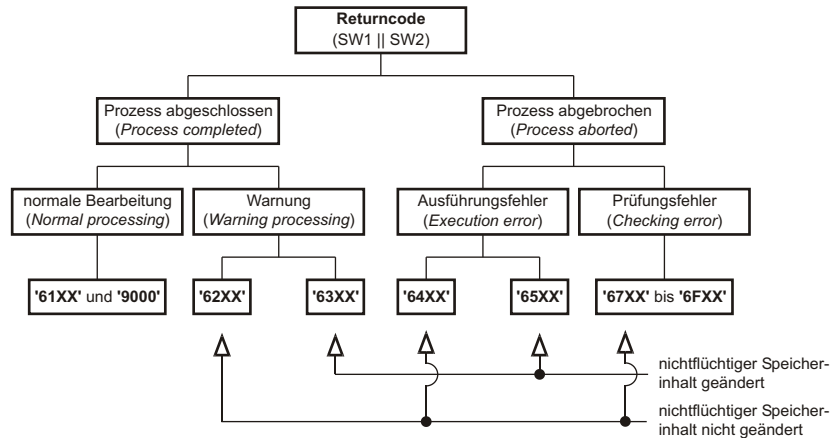
Cases von Kommandos



Wichtige reservierte FIDs

FID	Name und Zweck	Norm
'2F00'	Diese FID ist reserviert für die Datei Datei EF _{DIR} (<i>directory</i>) und wird zur Speicherung von Application Identifiers (AIDs) mit dazugehöriger Pfadangabe zur korrespondierenden Anwendung benutzt.	ISO/IEC 7816-4
'2F01'	Diese FID ist reserviert für die Datei EF _{ATR} mit den Erweiterungen zum ATR.	ISO/IEC 7816-4
'3F00'	Das MF ist das Wurzelverzeichnis für alle Dateien einer Chipkarte.	ISO/IEC 7816-4, GSM 11.11, TS 102.221, EMV
'3FFF'	Diese FID ist reserviert für die Dateiselektion durch Pfadangabe.	ISO/IEC 7816-4
'FFFF'	Diese FID ist reserviert für zukünftige Benutzung durch ISO/IEC.	ISO/IEC 7816-4

Systematik der Returncodes



Wichtige Returncodes

Returncode	Bedeutung	Returncode	Bedeutung
'61xx'	Kommando erfolgreich ausgeführt, xx Byte Daten sind als Antwort vorhanden und können mit GET RESPONSE angefordert werden.	'6A00'	Falsche Parameter P1/P2 (allgemein)
'6281'	Die zurückgegebenen Daten können u.U. fehlerhaft sein	'6A80'	Parameter im Datenteil sind falsch
'6282'	Es konnten weniger als Le Bytes gelesen werden, da das Dateiende vorher erreicht wurde	'6A81'	Funktion wird nicht unterstützt
'6283'	Die selektierte Datei ist reversibel gesperrt (<i>invalidated</i>).	'6A82'	Datei wurde nicht gefunden
'6284'	Die File Control Information (FCI) ist nicht nach ISO/IEC 7816-4 strukturiert.	'6A83'	Record wurde nicht gefunden
'62xx'	Warnung; Zustand des nichtflüchtigen Speichers unverändert.	'6A84'	Ungenügend Speicherplatz in der Datei
'63Cx'	Zähler hat den Wert x erreicht (0 x 15, (die genaue Bedeutung ist vom jeweiligen Kommando abhängig)	'6A85'	Lc inkonsistent mit TLV Struktur
'63xx'	Warnung; Zustand des nichtflüchtigen Speichers verändert	'6A86'	Inkorrekte Parameter P1/P2
'64xx'	Ausführungsfehler; Zustand des nichtflüchtigen Speichers unverändert	'6A87'	Lc inkonsistent mit P1/P2
'6581'	Speicherfehler (z.B. bei Schreiboperation)	'6A88'	referenzierte Daten nicht gefunden
'65xx'	Ausführungsfehler; Zustand des nichtflüchtigen Speichers verändert	'6B00'	Parameter 1 oder 2 falsch
'6700'	Länge falsch	'6Cxx'	falsche Länge Le; xx gibt die korrekte Länge an
'67xx' ... '6Fxx'	Prüfungsfehler	'6D00'	Kommando (Instruction) wird nicht unterstützt
'6800'	Funktionen im Class Byte werden nicht unterstützt (allgemein)	'6E00'	Class wird nicht unterstützt
'6881'	Logische Kanäle werden nicht unterstützt	'6F00'	Kommando abgebrochen – Genauere Diagnose nicht möglich (z.B. Fehler im Betriebssystem)
'6882'	Secure Messaging wird nicht unterstützt	'9000'	Kommando erfolgreich ausgeführt
'6900'	Kommando nicht erlaubt (allgemein)	'920x'	Schreiben ins EEPROM nach x-maligem Versuch erfolgreich
'6981'	Kommando inkompatibel zur Dateistruktur	'9210'	Ungenügend Speicherplatz
'6982'	Sicherheitszustand nicht erfüllt	'9240'	Schreiben ins EEPROM nicht erfolgreich
'6983'	Authentisierungsmethode gesperrt	'9400'	kein EF selektiert
'6984'	referenzierte Daten sind reversibel gesperrt (<i>invalidated</i>)	'9402'	Adressbereich überschritten
'6985'	Benutzungsbedingungen nicht erfüllt	'9404'	FID nicht gefunden, Record nicht gefunden, Vergleichsmuster nicht gefunden
'6986'	Kommando nicht erlaubt (kein EF selektiert)	'9408	Selektierter Dateityp unpassend zum Kommando
'6987'	erwartete Secure Messaging Datenobjekte fehlen	'9802'	Keine PIN definiert
'6988'	Secure Messaging Datenobjekte inkorrekt	'9804'	Zugriffsbedingungen nicht erfüllt, Authentisierung fehlgeschlagen
		'9835'	ASK RANDOM / GIVE RANDOM nicht ausgeführt
		'9840'	PIN-Prüfung nicht erfolgreich
		'9850'	INCREASE / DECREASE kann nicht ausgeführt werden, da Grenzwert erreicht
		'9Fxx'	Kommando erfolgreich ausgeführt, xx Byte Daten sind als Antwort vorhanden und können mit GET RESPONSE angefordert werden.

Kodierung wichtiger Kommandos nach ISO/IEC 7816-4

SELECT FILE (case 4)

Datenelement	Codierung	Bemerkung
CLA	'00'	Das für ISO/IEC 7816 Kommandos reservierte Class-Byte ohne Benutzung von Secure Messaging.
INS	'A4'	Das Instruction-Byte für SELECT FILE, d.h. das Kommando zur Auswahl von Dateien (MF, DFs oder EFs).
P1	...	P1 = '00' Lc = 0 Selektion des MF P1 = '00' Lc = 0 Selektion einer Datei mit FID (FID in DATA enthalten) P1 = '04' Selektion eines DF mit dem DF Name (DF Name in DATA enthalten) P1 = '08' Selektion einer Datei durch die Angabe des FID basierten Pfades (Pfad in DATA enthalten) vom MF aus. P1 = '09' Selektion einer Datei durch die Angabe des FID basierten Pfades (Pfad in DATA enthalten) vom aktuellen DF aus.
P2	...	P2 = '00' Rückgabe von optionalen FCI. P2 = '04' Rückgabe von optionalen FCP. P2 = '08' Rückgabe von optionalen FMD.
Lc
DATA	...	Codierung in der Beschreibung von P1 enthalten.
Le	...	Le = 0' Rückgabe aller zur Selektion gehörenden Daten.

READ BINARY (case 2)

Datenelement	Codierung	Bemerkung
CLA	'00'	Das für ISO/IEC 7816 Kommandos reservierte Class-Byte ohne Benutzung von Secure Messaging.
INS	'B0'	Das Instruction-Byte für READ BINARY, d.h. das Kommando zum Lesen von Daten aus Dateien der Struktur „transparent“.
P1	...	P1.b8 = 0 Lese Daten aus der aktuell selektierten Datei mit Offset; Offset = (P1.b7 ... P1.b1 P2) P1.b8 = 1 Lese Daten nach impliziter Dateiselektion durch Short-FID und mit Offset; Short-FID = (P1.b5 ... P1.b1), Offset = P2
P2	...	Codierung in der Beschreibung von P1 enthalten.
Le	...	Le = 0 Lese alle Daten bis zum Ende der Datei. Le > 0 Le ist die Anzahl der zu lesenden Bytes.

UPDATE BINARY (case 3)

Datenelement	Codierung	Bemerkung
CLA	'00'	Das für ISO/IEC 7816 Kommandos reservierte Class-Byte ohne Benutzung von Secure Messaging.
INS	'D6'	Das Instruction-Byte für UPDATE BINARY, d.h. das Kommando zum Schreiben von Daten in Dateien der Struktur „transparent“.
P1	...	P1.b8 = 0 Schreibe Daten in die aktuell selektierte Datei mit Offset; Offset = (P1.b7 ... P1.b1 P2) P1.b8 = 1 Schreibe Daten nach impliziter Dateiselektion durch Short-FID und mit Offset; Short-FID = (P1.b5 ... P1.b1), Offset = P2
P2	...	Codierung in der Beschreibung von P1 enthalten.
Lc	...	Lc ist die Anzahl der zu schreibenden Bytes.
DATA	...	Die zu schreibenden Bytes mit der Länge Lc.

Kodierung wichtiger Kommandos nach ISO/IEC 7816-4

READ RECORD (case 2)

Datenelement	Codierung	Bemerkung
CLA	'00'	Das für ISO/IEC 7816 Kommandos reservierte Class-Byte ohne Benutzung von Secure Messaging.
INS	'B2'	Das Instruction-Byte für READ RECORD, d.h. das Kommando zum Lesen von Daten aus einer Datei mit Record-orientierter Struktur.
P1	...	P1 = 0 Lese den aktuellen Record P1 0 Lese den Record mit der in P1 angegebenen Recordnummer oder Record Identifier.
P2	...	P2.b8 ... P2.b4 = °00000° Lese Daten aus der aktuell selektierten Datei P2.b8 ... P2.b4 °00000° Lese Daten nach impliziter Dateiselektion durch Short-FID; Short-FID = (P2.b8 ... P2.b4) P2.b3 ... P2.b1 = °000° Lese den ersten (<i>first</i>) Record mit dem Record Identifier, übergeben in P1 P2.b3 ... P2.b1 = °001° Lese den letzten (<i>last</i>) Record mit dem Record Identifier, übergeben in P1 P2.b3 ... P2.b1 = °010° Lese den nächsten (<i>next</i>) Record mit dem Record Identifier, übergeben in P1 P2.b3 ... P2.b1 = °011° Lese den vorherigen (<i>previous</i>) Record mit dem Record Identifier, übergeben in P1 P2.b3 ... P2.b1 = °100° P1 = 0 Lese den aktuellen Record P2.b3 ... P2.b1 = °100° P1 0 Lese den Record mit der Recordnummer, übergeben in P1. P2.b3 ... P2.b1 = °101° Lese alle Records ab der in P1 übergeben Recordnummer bis zum Ende der Datei. P2.b3 ... P2.b1 = °110° Lese alle Records vom Ende der Datei bis zu der in P1 übergeben Recordnummer.
Le	...	Le = 0 Lese alle Bytes bis zum Ende des Records/der Records. Le > 0 Le ist die Länge des Records/der Records.

UPDATE RECORD (case 3)

Datenelement	Codierung	Bemerkung
CLA	'00'	Das für ISO/IEC 7816 Kommandos reservierte Class-Byte ohne Benutzung von Secure Messaging.
INS	'DC'	Das Instruction-Byte für UPDATE RECORD, d.h. das Kommando zum Schreiben von Daten in eine Datei mit Record-orientierter Struktur.
P1	...	P1 = 0 Schreibe den aktuellen Record P1 0 Schreibe den Record mit der in P1 übergebenen Recordnummer.
P2	...	P2.b8 ... P2.b4 = °00000° Schreibe Daten in die aktuell selektierte Datei P2.b8 ... P2.b4 °00000° Schreibe Daten nach impliziter Dateiselektion durch Short-FID; Short-FID = (P1.b8 ... P1.b4) P2.b3 ... P2.b1 = °000° Schreibe den ersten (<i>first</i>) Record P2.b3 ... P2.b1 = °001° Schreibe den letzten (<i>last</i>) Record P2.b3 ... P2.b1 = °010° Schreibe den nächsten (<i>next</i>) Record P2.b3 ... P2.b1 = °011° Schreibe den vorherigen (<i>previous</i>) Record P2.b3 ... P2.b1 = °100° Schreibe den Record mit der in P1 übergebenen Recordnummer
Lc	...	Lc ist die Länge des zu schreibenden Records.
DATA	...	Der zu schreibende Record.

VERIFY (case 3)

Datenelement	Codierung	Bemerkung
CLA	'00'	Das für ISO/IEC 7816 Kommandos reservierte Class-Byte ohne Benutzung von Secure Messaging.
INS	'20'	Das Instruction-Byte für VERIFY, d.h. das Kommando zum Vergleich von übergebenen Daten mit Referenzdaten (typischerweise einer PIN).
P1	'00'	---
P2	...	P2 = '00' Explizite Informationen werden nicht übergeben. P2.b8 = °0° Es werden für die ganze Chipkarte gültige Referenzdaten verwendet (<i>global reference data</i>). P2.b8 = °1° Es werden für eine oder mehrere Anwendungen gültige Referenzdaten verwendet (<i>specific reference data</i>). P2.b7 P2.b6 = °00° RFU Bits P2.b5 ... P2.b1 Nummer der Referenzdaten.
Lc	...	Lc ist die Länge des übergebenen Vergleichswertes.
DATA	...	Der übergebene Vergleichswert (in der Regel eine PIN).