EMV ’96
Chip Electronic Commerce Specification

Version 1.0
December 1999.

Table of Contents

Table of Tables

Table of Figures

Preface

Introduction

The *EMV '96 Chip Electronic Commerce Specification* defines the use of an integrated chip card (IC Card) application to conduct a credit or debit transaction in an electronic commerce environment using SET 1.0 compliant software.

It leverages two existing specifications to provide the foundation for secure, portable, cost–effective, IC Card based transactions over the Internet. They are:

Specification	Description
Europay, MasterCard, and Visa ICC Specification (EMV)	Provides a specification to ensure credit and debit IC Cards will operate with all chip–reading terminals, regardless of location, financial institution, or manufacturer.
Secure Electronic Transaction™ (SET) Specification	Provides a secure protocol for which credit and debit products may be used to conduct electronic commerce.

In addition, the *EMV '96 Chip Electronic Commerce Specification* takes advantage of two enhancements to the SET protocol, they are:

SET Extension	Description
SET Common Chip Extension	Extends the SET protocol to support the transport of IC Card related data.
Online PIN extension	Extends the SET protocol to support the online transport of a cardholders' PIN.

Features

SET provides an electronic commerce infrastructure that delivers:

- Confidentiality of information
- Integrity of data
- Interoperability
- Certificate based authentication

The Chip Electronic Commerce Specification extends the SET Specification by supporting two key features native to EMV IC Card applications:

- Online card authentication, through the use of a cryptogram
- Cardholder verification, through the use of an optional Cardholder PIN

Continued on next page

Preface, continued

Chip Electronic Commerce System

The Chip Electronic Commerce payment system consists of eight components:

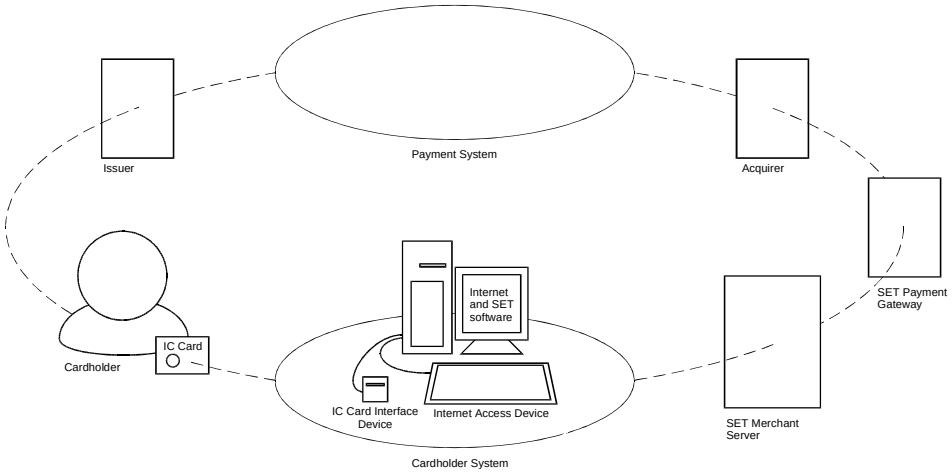

Figure 1— Chip Electronic Commerce System

Component	Description
Issuer	A financial institution that issues payment card products to individuals;
Cardholder	An authorized holder of a payment card issued by an issuer.
EMV IC Card	Stores the cardholder's payment data and is capable of generating a cryptogram to authenticate the card and optionally verify a cardholder's PIN.
Cardholder System	Serves as the interface between the EMV IC Card and the SET merchant server. It is responsible for authenticating the merchant to the cardholder.
Merchant Server	A system that interacts with the Cardholder System for electronic payments. The Merchant Server also interacts with the acquirer using the payment protocol to receive authorization and capture services for electronic payment transactions
Payment Gateway	A system that interacts with the Merchant Server and an acquirer's legacy system to support the authorization and capture of SET transactions.
Acquirer	A financial institution that supports merchants by providing a service for processing payment card transactions;
Payment System	A franchiser of payment system networks and branded instruments.

Continued on next page

Preface, continued

Scope

This specification defines a transaction flow that begins with the Cardholder System checking for the presence of an IC Card while conducting a purchase, continues with the transmission of the purchase and authorization requests, and ends with the transmission of the capture message from the Merchant Server or Payment Gateway.

The Payment Gateway is responsible for reformatting the SET message (along with additional IC Card related data) and transmitting an authorization request to the issuer. The manner in which the Payment Gateway reformats, transmits and receives messages to and from the issuer is dependent on a Payment System's requirements. These requirements are is outside the scope of this document.

Intended audience

This specification is written to address developers of the various software components of the Chip Electronic Commerce system. It assumes the reader is familiar with *EMV '96* and *SET 1.0*.

Organization

The Chip Electronic Commerce Specification contains the following parts:

Part	Title	Contents
1	System Architecture	Defines the additional requirements placed upon the components of the Chip Electronic Commerce system by this specification
2	Transaction Processing	Defines the manner in which a purchase is processed in the Chip Electronic Commerce system
3	Appendices	Provides supplementary information.

Abbreviations and Notations

The following abbreviations and notations are used in this specification.

AAC	Application Authentication Cryptogram
AC	Application Cryptogram
AID	Application Identifier
APDU	Application Protocol Data Unit
ARQC	Authorization Request Cryptogram
ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
BIN	Bank Identification Number
CA	Certificate Authority
CDOL1	Card Data Object List One
CVM	Cardholder Verification Method
CVR	Cardholder Verification Rule
DER	Distinguished Encoding Rules
EMV	Europay, MasterCard, and Visa IC Card Specifications for Payment Systems
IC Card	Integrated Circuit Card
ICC	Integrated Circuit Card
ISO	International Organization of Standards
MIME	Multipurpose Internet Mail Extensions
PAN	Primary Account Number
PC	Personal Computer
PIN	Personal Identification Number
POS	Point of Sale
RFU	Reserved for Future Use
SET	SET Secure Electronic Transaction™ Specification
TC	Transaction Certificate
TDOL	Transaction Certificate Data Object List
TLV	Tag Length Value
URL	Uniform Resource Locator
XID	Transaction ID

Normative References

The following standards and specifications contain provisions that are referenced in this specification:

EMV ‘96	*Integrated Circuit Card Application Specification for Payment Systems*, version 3.1.1, 31 May 1998. *Integrated Circuit Card Specification for Payment Systems*, version 3.1.1, 31 May 1998. *Integrated Circuit Card Terminal Specification for Payment Systems*, version 3.1.1, 31 May 1998.
FIPS Pub 190–1:1995	Secure Hash Standard.
IETF RFC 1738	Uniform Resource Locators.
ISO 3166:1993	Codes for the representation of names of countries.
ISO 4217:1990	Codes for the representation of currencies and funds.
ISO 8825–1:1995(E)	Information technology—ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER), and Distinguished Encoding Rules (DER).
ISO 8859:1987	Information processing—8–bit single–byte coded graphic character sets.
ISO/IEC 7813:1990	Identification cards—Financial transaction cards.
ISO/IEC 7816–5:1994	Identification cards—Integrated circuit(s) cards with contacts—Part 5: Numbering system and registration procedure for application identifiers.
SET Consortium	*SET Secure Electronic Transaction™ (SET) Specification*, Version 1.0,—*Book 1: Business Description*, May 31, 1997. June 1996. *SET Secure Electronic Transaction™ (SET) Specification*, Version 1.0,—*Book 2: Programmer’s Guide*, May 31, 1997. June 1996.
SET Consortium	External Interface Guide to SET Secure Electronic Commerce, September 24, 1997.
SET Consortium	SET Common Chip Extension, September, 1999.
SET Consortium	SET Online PIN Extension, May, 1999.

Definitions

Acquirer	A financial institution that supports merchants by providing services for processing payment card transactions.
Cardholder	An authorized holder of a payment card issued by an issuer.
Cardholder System	The combination of hardware and software required to interact with the cardholder, their IC Card, and a SET Merchant Server in order to participate in EMV chip electronic commerce.
Certificate Authority	Institutions responsible for the creation and distribution of electronic certificates for Cardholders, Merchants, and Payment Gateways.
Issuer	An institution that issues payment card products to individuals.
Merchant	A merchant of goods, services, and/or information who accepts payment for them electronically, and may provide electronic delivery of items for sale (e.g., information).
Merchant Server	A system that interacts with the Cardholder System for electronic payments. The Merchant Server also interacts with the acquirer using the payment protocol to receive authorization and capture services for electronic payment transactions.
Payment Gateway	A system that interacts with the Merchant Server and an acquirer's legacy system to support the authorization and capture of SET transactions.
Payment System	Financial institutions have founded payment card brands that protect and advertise the brand, establish and enforce rules for use and acceptance of their payment cards, and provide networks that connect the financial institutions.

Part I
System Architecture

Overview

Introduction

Part I defines the transaction processing capabilities of each component in the Chip Electronic Commerce system.

Organization

Part I includes the following chapters:

Chapter	Title	Contents	Page
1	EMV Debit/Credit Applications	Describes the attributes of EMV debit or credit card applications that participate in EMV Chip Electronic Commerce transactions.	8
2	Cardholder System	Describes the pre–conditions the Cardholder System shall meet prior to transaction processing.	8
3	Merchant Server	Describes the pre–conditions that Merchant Servers shall meet prior to transaction processing.	17
4	Payment Gateway	Describes the pre–conditions that Payment Gateways shall meet prior to transaction processing.	17

Approach to reading

Manufacturers and developers of IC Cards and card applications and Cardholder Systems should read the requirements for their component as well as the coding of commands described in Part 2.

Developers of Merchant Servers and acquirer Payment Gateways need only read the requirements defined in their self–titled chapters.

Chapter 1
EMV Debit/Credit Applications

Overview

Introduction

The EMV Debit/Credit applications are IC Card applications that are capable of generating for each transaction an application cryptogram that can decline or approve off–line, or else, request the on–line referral or authorization of a transaction.

Requirements

The *EMV '96 Chip Electronic Commerce Specification* does not require any modification to EMV–compliant IC Cards.

Brand Marketing Opportunity

The union of EMV compliant IC Cards and SET compliant Cardholder Systems creates a new brand marketing opportunity for issuers. During application selection, an issuer may supplement the EMV defined branding mechanisms, i.e. the display of an Application Label or Preferred Name, by showing its cardholder a visual image of its brand. More information is provided in Appendix 1, Issuer URL.

To do this, an issuer should store an additional data element, the Issuer URL, in the File Control Information of its Application Definition File. If used, the format, template, tag, and length to be applied to this data element are as follows:

Name	Format	Template	Tag	Length
Issuer URL	ans	'A5'	'9F19'	var.

Table 1—Issuer URL in FCI description

Value	Tag	Presence
FCI Template	'6F'	M
DF Name	'84'	M
FCI Proprietary Template	'A5'	M
Application Label	'50'	O
Application Priority Indicator	'87'	O
PDOL	'9F38'	O
Language Preference	'5F2D'	O
Issuer Code Table Index	'9F11'	O
Application Preferred Name	'9F12'	O
FCI Issuer Discretionary Data	'BF0C'	O
Issuer URL	'9F19'	O

Table 2— Location of Issuer URL in FCI Template

Chapter 2
Cardholder System

Introduction

The Cardholder System is the combination of hardware and software required to interact with the cardholder, the cardholder's IC Card, and a SET Merchant Server in order to participate in *EMV '96 Chip Electronic Commerce.*

This chapter describes the additional requirements imposed upon the Cardholder System by this specification. Since there are many possible ways in which a Cardholder System can be configured, this description treats the component as if it were a black box.

Appendix 3 offers a high level model describing the Cardholder System.

EMV Interface device requirements

The physical requirements that the EMV capable Interface Device (IFD) must meet are prescribed by Part I of the *EMV '96 ICC Specification.*

PIN entry device requirements

The physical characteristics that the Cardholder System and the PIN entry device must possess to process a cardholder's PIN are defined by individual Payment System rules.

The Cardholder System must be aware of its PIN processing and interface device capabilities.

Organization

Chapter 2 includes the following sections:

Section	Title	Description
1	Cardholder System Functions	Describes the functions through which Cardholder Systems interact with IC Cards
2	Commands	Lists the commands that Cardholder Systems shall support.
3	Data Elements	Defines the coding and/or values to be ascribed to data elements that Cardholder Systems shall store or create.
4	SET message extensions	Lists the SET message extensions that Cardholder Systems shall support.

Section 1
Cardholder System Functions

Definition

Section 1 describes the functions performed by the Cardholder System on behalf of the IC Card.

Requirements

The Cardholder System shall perform the following functions, which are detailed in Part II, Transaction Processing:

IC Card to Cardholder System Functions	Page
Card Selection	25
Application Selection	26
Application Initiation	29
Read Application Data	30
Cardholder Verification	31
Terminal Action Analysis	31
Issuer Script Processing & Completion	35

Table 3—IC Card to Cardholder System Functions

EMV design note

Due to the special nature of the electronic commerce environment, the following EMV defined functions are not executed:

EMV Functions not executed
Offline Data Authentication
Processing Restrictions
Terminal Risk Management

Section 2
Commands

Introduction

The Cardholder System communicates with the IC Card application by issuing commands and interpreting the card's response.

Coding conventions and message structure

The coding conventions and structuring of command and response APDUs is prescribed by Part II of the *EMV '96 IC Card Specification for Payment Systems*.

Commands

The creation of these commands is described by Part II of the *EMV '96 ICC Specification for Payment Systems*.

The Cardholder System shall support the following commands:

Command	Description
SELECT	Selects an application definition file, directory definition file or Payment System Environment.
GET PROCESSING OPTIONS	Initiates the transaction within the IC Card.
READ RECORD	Retrieves the data in the records of linear files.
GET DATA	Retrieves a data object not encapsulated in a record within the current application.
VERIFY	Initiates in the IC Card the comparison of the Transaction PIN Data sent in the data field of the command with the reference PIN data associated with the application.
GENERATE AC	Initiates the generation of an application cryptogram by the IC Card.
EXTERNAL AUTHENTICATE	Initiates the verification of the Issuer Authentication Data generated by the issuer.

Table 4—Cardholder System Commands

Processing responses

The Cardholder System shall be able to decode all responses generated by cards, which respond to commands as prescribed by Section 2 of Part II of the *EMV '96 ICC Specification for Payment Systems*.

Section 3
Data Elements

Introduction

Section 3 defines the Data Elements resident at the Cardholder System and their values.

For more information regarding other EMV related Data Elements and their sources, see Table 14—commonChip extension data and its sources on page 45.

Resident Data Elements

The Cardholder System shall store values for the following Resident Data Elements:

Data Element
Amount Other
BrandID—AID Mappings
ISO 8859 Code Table
Terminal Type
Transaction Type
Terminal Verification Results

Table 5—Cardholder System's resident Data Elements

Amount Other

Amount Other encodes a cashback amount. Since there is no cashback in the purchase transaction, the Data Element shall be defined as:

Data Element	EMV tag	Format	Length	Value
Amount Other	'9F04'–or–	b–or–	4	0000
	'9F03'	n12	6	000000000000

Continued on next page

Data Elements, continued

BrandID—AID Table

The BrandID—AID Table contains a mapping from each SET brandID to its corresponding Application Identifiers (AIDs).

The Cardholder System should have a mechanism to update its BrandID-AID Table.

The Cardholder System's BrandID—AID table shall include the following initial mappings:

Brand	AID	Application
Electron	A0000000032010	Visa Electron
Interlink	A0000000033010	Visa Interlink
Maestro	A0000000043060	Maestro
MasterCard	A0000000041010	MasterCard
Visa	A0000000031010	Visa Smart Debit/Credit

Table 6—BrandID—AID table

ISO 8859 code table

The ISO 8859 Code Table enables the Cardholder System to decode card resident data objects such as Application Label and Application Preferred Name. For more information about coding this table, see ISO 8859.

Terminal Type

The Terminal Type specifies the terminal's environment, its communications capabilities and its operational control. To indicate that it is an "unattended, online, controlled by cardholder" device, the Data Element shall be defined as:

Data Element	EMV tag	Format	Length	Value
Terminal Type	'9F35'	n 2	1	34

Transaction Type

The Transaction Type specifies the type of financial transactions the Cardholder System performs. To indicate that the transaction is a purchase of goods or service, the Data Element shall be defined as:

Data Element	EMV tag	Format	Length	Value
Transaction Type	'9C'	n 2	1	00

Continued on next page

Data Elements, continued

Terminal Verification Results

The Terminal Verification Results is a record of the outcome of the various application functions performed by the Cardholder System. It shall be defined as:

Data Element	EMV tag	Format	Length	Value
Terminal Verification Results	'95'	b	5	static and dynamic

The values to be ascribed to bits that are static are indicated below. Bits whose values are to be dynamically set, will be set by the Cardholder System during the course of the transaction, as prescribed later in this specification. The coding of this Data Element is as follows:

Byte	Bit	Meaning	Value
1	8	Offline data authentication was not performed	1
	7	Offline static data authentication failed	0
	6	IC Card Data missing	Dynamic
	5	Card appears on terminal exception file	0
	4	Offline dynamic data authentication failed	0
	3	RFU	0
	2	RFU	0
	1	RFU	0

Byte	Bit	Meaning	Value
2	8	IC Card and terminal have different application versions	0
	7	Expired application	0
	6	Application not yet effective	0
	5	Requested service not allowed for card product	0
	4	New Card	0
	3	RFU	0
	2	RFU	0
	1	RFU	0

Continued on next page

Data Elements, continued

Byte	Bit	Meaning	Value
3	8	Cardholder verification was not successful	Dynamic
	7	Unrecognized CVM	Dynamic
	6	PIN Try Limit exceeded	Dynamic
	5	PIN entry required and PIN pad not present or not working	Dynamic
	4	PIN entry required, PIN pad present but PIN was not entered	Dynamic
	3	Online PIN entered	Dynamic
	2	RFU	0
	1	RFU	0

Byte	Bit	Meaning	Value
4	8	Transaction exceeds floor limit	1
	7	Lower consecutive offline limit exceeded	0
	6	Upper consecutive offline limit exceeded	0
	5	Transaction selected randomly for online processing	0
	4	Merchant forced transaction online	0
	3	RFU	0
	2	RFU	0
	1	RFU	0

Byte	Bit	Meaning	Value
5	8	Default TDOL used	0
	7	Issuer authentication was unsuccessful	Dynamic
	6	Script processing failed before final GENERATE AC	Dynamic
	5	Script processing failed after final GENERATE AC	Dynamic
	4	RFU	0
	3	RFU	0
	2	RFU	0
	1	RFU	0

Section 4
SET Message Extensions

Introduction

Section 4 describes the SET Message Extensions that the Cardholder System shall support in order to conduct an EMV transaction.

Required message extensions

The Cardholder System must be able to support the following message extensions as prescribed by the *SET Common Chip Extension* and *SET Online PIN Extension.*

Message extension	Description
commonChip	Created by the Cardholder System and placed in the PReq message; this extension carries the cryptogram and related data required by the acquirer to format a Payment System's authorization request.
acqCardExtensions	Created by the Payment Gateway and placed within the AcqCardMsgData field of the PRes message; this extension carries Issuer Authentication and Issuer Script data.
onlinePIN	Created by the Cardholder System and placed in the PReq message; this extension identifies the presence in the RSA/OAEP block of PIN data entered by the cardholder.

Chapter 3
Merchant Server

Introduction

The Merchant Server is the component that interacts with the Cardholder System in support of electronic payments. The Merchant Server also interacts with the acquirer's Payment Gateway.

Requirements

The *EMV '96 Chip Electronic Commerce Specification* does not require any modification to Merchant Servers.

Chapter 4
Payment Gateway

Introduction

The Payment Gateway is the system that interacts with the Merchant Server and an acquirer's legacy system to support the authorization and capture of SET transactions. This chapter defines the additional requirements imposed upon the Payment Gateway by this specification.

Required message extension

The Payment Gateway must be able to process the following message extensions as prescribed by the *SET Common Chip Extension*.

Message extension	Description
commonChip	Created by the Cardholder System and placed in the PReq message; this extension carries the cryptogram and related data required by the acquirer to format a Payment System's authorization request.
acqCardExtensions	Created by the Payment Gateway and placed within the AcqCardMsgData field of the PRes message; this extension carries Issuer Authentication and Issuer Script data back to the Cardholder System.

Optional message extension

The Payment Gateway shall be able to process the following message extensions as prescribed by the *SET Online PIN Extension*.

Message extension	Description
onlinePIN	Created by the Cardholder System and placed in the PReq message; this extension identifies the presence in the RSA/OAEP block of PIN data entered by the cardholder.

Changes to Payment Gateway certificate

The SETExtension component of the Payment Gateway's certificate shall indicate that the Payment Gateway supports the commonChip extension.

The SETExtension component of the Payment Gateway's certificate shall indicate that the Payment Gateway supports the onlinePIN extension.

Part II
Transaction Processing

Overview

Introduction

Part II defines the manner in which purchase transactions are processed in the EMV Chip Electronic Commerce system. It describes all EMV functions and SET messages related to the authorization and capture of a payment.

Organization

Part II includes the following chapters:

Chapter	Title	Contents	Page
1	Transaction Flows	Provides an overview of the interactions required to complete a purchase.	19
2	IC Card to Cardholder System Interface	Describes the functions between the IC Card application and the Cardholder System.	23
3	Cardholder System to Merchant Server Interface	Describes the interactions between the Cardholder System and the Merchant Server.	36
4	Merchant Server to Payment Gateway Interface	Describes the interaction between the Merchant Server and the Payment Gateway.	45

Approach to reading

Chapter 1 provides a high–level overview of the transaction processing phases. The remaining chapters describe the processing of each phase in detail.

Therefore, the reader should read Chapter 1 first, to learn the basic order in which transactions are processed. They should then examine the details of each phase of the transaction process by reading the remaining chapters, using the flows in Chapter 1 as a guide.

Familiarity with the transaction processing capabilities of the Chip Electronic Commerce System described in Part I of this document is assumed.

Chapter 1
Purchase Transaction Flow

Overview

Introduction

This chapter provides a high–level overview of the purchase transaction. It provides an illustration of the transaction flow as well as a summary description of each phase.

Organization

This chapter consists of the following sections:

Section	Title	Description
1	Diagram of Transaction Flow	Illustrates the transaction flow.
2	Explanation of Transaction Flow	Provides a brief description of the transaction flow.

Section 1
Diagram of Transaction Flow

Introduction

This section illustrates the EMV functions and SET messages processed to conduct a purchase transaction.

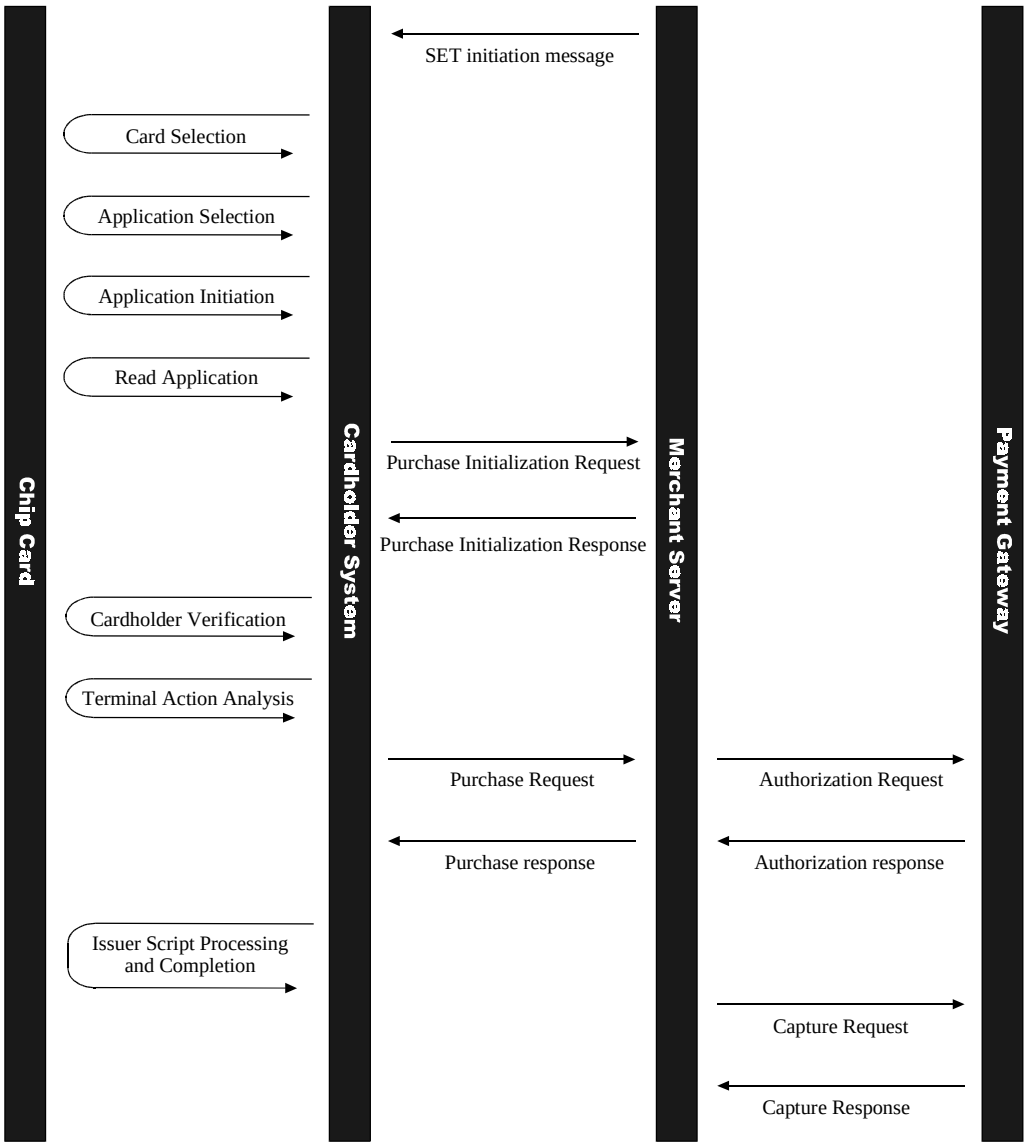

Figure 2—Diagram of transaction flow

Continued on next page

Section 2
Explanation of Transaction Flow

Introduction	This section describes the phases of the purchase transaction in the order in which they occur.
SET Payment Initiation	The Merchant Server invokes the Cardholder System and informs it of the payment brands it accepts.
Card Selection	The cardholder presents to the Cardholder System the payment card to be used for the purchase.
Application Selection	The Cardholder System selects an application from the card, with input from the cardholder if necessary.
Application Initiation	The Cardholder System initiates the card application to determine whether it and the card agree about how the transaction should be processed.
Read Application	The Cardholder System reads the application data.
Purchase Initialization Request	The Cardholder System initializes the purchase by informing the Merchant Server how the cardholder intends to pay.
Purchase Initialization Response	The Merchant Server returns the information necessary to complete the purchase.
Cardholder Verification	The Cardholder System retrieves information from the cardholder that may verify their identity and either presents it to the card or transmits to the issuer for verification
Terminal Action Analysis	The Cardholder System requests an online authorization of the transaction. The card determines whether to decline the transaction off–line or to request an online authorization or referral.

Continued on next page

Explanation of Flow, continued

Purchase Request	The Cardholder System requests a purchase and provides the Merchant Server with the data that it, the Payment Gateway and the issuer need to respond to the request.
Authorization Request	The Merchant Server sends the Payment Gateway the information that it needs to verify the authenticity of the cardholder and to create a Payment System's authorization request message. *Note: SET allows a merchant to return a PRes message to the Cardholder System before authorization processing.*
Authorization Response	The Payment Gateway sends the Merchant Server a message that indicates whether the transaction has been authorized or declined by the issuer.
Purchase Response	The Merchant Server informs the Cardholder System of the status of the transaction sometime after it has received the Cardholder System's Purchase Request.
Issuer Script Processing and Completion	The Cardholder System ends the involvement of the cardholder and IC Card.
Capture Request	The Merchant Server may request that the Payment Gateway capture the transaction after it has received the Payment Gateway's Authorization Response.
Capture Response	The Payment Gateway notifies that Merchant Server of the status of its request for capture.

Chapter 2
IC Card—Cardholder System Functions

Overview

Introduction

Chapter 2 defines the transaction processing phases that involve interaction between the IC Card application and the Cardholder System. Phases that do not involve interaction between the card and the Cardholder System are detailed in following chapters.

Organization

Chapter 2 defines the following phases of transaction processing:

Section	Title	Contents
1	Card Selection	Describes how the Cardholder indicates which payment card to use for the purchase.
2	Application Selection	Describes how the Cardholder System, with input from the cardholder, selects a card application to participate in the transaction.
3	Application Initiation	Describes how the Cardholder System initiates the card application.
4	Read Application Data	Describes how the Cardholder System reads the card application's records.
5	Cardholder Verification	Describes how the Cardholder System verifies the identity of the cardholder.
6	Terminal Action Analysis	Describes how the IC Card application generates an Application Cryptogram.
7	Issuer Script Processing and Completion	Describes how the Cardholder System ends its involvement with the processing of the transaction.

Section 1
Card Selection

Purpose

Card selection is the phase of transaction processing in which the cardholder indicates which payment card should be used for the purchase. This phase supplements the SET defined account selection process.

Conditions of execution

The Cardholder System shall always perform Card Selection.

Process description

The Cardholder System shall integrate the execution of Card Selection with the execution of account selection. In doing so, the following requirements shall be met:

Requirements
All brands accepted by the Merchant Server shall be displayed.
The Cardholder shall be offered all available payment options.
Once a chip card has been selected, the Cardholder System shall request that the Cardholder not remove the card until prompted to do so.

Section 2
Application Selection

Introduction

Application Selection is the transaction processing phase in which the Cardholder System selects the application from the IC Card.

Conditions of execution

This phase is mandatory.

Continued on next page

Application Selection, continued

Process description

The Cardholder System shall perform Application Selection as prescribed by Part III of the *EMV '96 IC Card Specification for Payment Systems.* The *EMV '96* protocol may be briefly described as follows: The terminal compares the list of applications that it supports with those that the card supports, and the Cardholder selects an application from those mutually supported.

The Cardholder System shall assume the role of the "terminal" described in *EMV '96* and behave just like that terminal with the following exceptions:

Exception	Action
Determining supported AID list	The list of applications the Cardholder System supports is a function of the brands the merchant participating in the transaction accepts. To create the list of supported applications, the Cardholder System shall: 1. Examine the SET Initiation Message to determine the brands supported by the merchant 2. Use the BrandID—AID table to build the list of supported AIDs.
No mutually supported applications	If no mutually supported applications are found, the Cardholder System shall either 1. Automatically update the Brand—AID table. 2. Prompt the Cardholder to confirm the correct card has been inserted, and if so, update the Brand—AID table. Otherwise request the Cardholder to remove the card and return to the Card Selection phase. If after an update, a mutually supported application cannot be found, the Cardholder System shall request that the Cardholder remove the card and return to the Card Selection phase.
Selecting the application to be executed	The Cardholder System shall select an application from amongst those that are mutually supported as prescribed by section 3.4 of the *EMV'96 ICC Specification* with the following exception: • If one mutually supported application is found, the Cardholder System shall display the selected application and prompt the Cardholder to confirm the selection. This confirmation may be combined with other confirmations, such as an overall confirmation of the payment details. • If more than one mutually supported applications are found, the Cardholder System shall display the application choices and prompt the Cardholder to select the desired application.

Continued on next page

Application Selection, continued

Application display

The Cardholder System shall display the application(s) as follows:

Step	Action
1	If an Application Preferred Name (tag ‘9F12’) was provided by the card application in its response to the SELECT command, the Cardholder System shall display it to the Cardholder. Otherwise: The Cardholder System shall display the Application Label (tag ‘50’) that was provided by the card application in its response to the SELECT command.
2	If an Issuer URL (tag ‘9F19’) was provided by the card application in its response to the SELECT command, the Cardholder System may use the Issuer URL to request an application logo and display that logo to the Cardholder in addition to the Application Preferred Name or Application Label. The Cardholder System shall decode the Issuer URL as prescribed by Appendix 2.

Section 3
Application Initiation

Introduction

Application Initiation is the transaction processing phase during which the IC Card and the Cardholder System learn the details of the transaction and make an informed decision as to whether they wish to participate.

Conditions of execution

This phase is mandatory.

Process description

The Cardholder System shall initiate the application as prescribed by Section 7.1 of *EMV '96 ICC Application Specification for Payment Systems*. It shall assume the role of the "terminal" described therein.

Section 4
Read Application Data

Introduction

Read Application Data is the transaction processing phase in which the Cardholder System reads the files and records of the card application.

Conditions of execution

This phase is mandatory.

Process description

The Cardholder System shall read the application data as prescribed by the *EMV '96 ICC Application Specification for Payment Systems*. It shall assume the role of the "terminal" described therein.

Section 5
Cardholder Verification

Introduction

Cardholder Verification is the transaction-processing phase in which the Cardholder System retrieves information from the Cardholder that may verify their identity and either presents it to the card or transmits it to the issuer for verification. Appendix 2 provides a flow diagram to assist the reading of this section.

Conditions of execution

The Cardholder System shall perform Cardholder Verification if bit 5 of byte 1 of the Application Interchange Profile is set to one.

Process Description

The Cardholder System shall perform the Cardholder Verification process as prescribed by section 7.5 of the *EMV IC Card Application Specification for Payment Systems*, assuming the role of the "terminal" described therein, with the following exceptions:

Exception	Action
Determining Whether to Prompt for Off–line PIN Entry	When the method of Cardholder Verification requested by the card (as indicated by it's CVRs) requires that the Cardholder provide his/her PIN for off–line verification by the card, the Cardholder System shall determine whether there is a mechanism for transport of the cryptogram to the issuer for authentication. If transport of the cryptogram is not available, the Cardholder System shall not prompt for off–line PIN entry, but shall attempt to process the next CVR. Cardholder applications shall support the following method and may support others. The Cardholder System shall search for the presence of the commonChip OID in the extension to Payment Gateway Certificate. If this OID is present, transport of the cryptogram is available.
Determining Whether to Prompt for Online PIN Entry	When the method of Cardholder Verification requested by the card (as indicated by it's CVRs) requires that the Cardholder provide his/her PIN for online verification by the issuer, the Cardholder System shall determine whether the Payment Gateway supports issuer verification of an online PIN. To do this, the Cardholder System shall search for the presence of the id–set–PIN–Any–Source OID in the extension to Payment Gateway Certificate. If this OID is available, the Cardholder System shall prompt for PIN entry. If this OID is not available, the Cardholder System shall not prompt for PIN entry, but shall attempt to process the next CVR.

Transmitting PIN Online

The Cardholder System shall encipher and transmit the Cardholder's PIN online as prescribed by the *SET Online PIN Extension*.

Section 6
Terminal Action Analysis

Introduction

Terminal Action Analysis is the phase of transaction processing in which the Cardholder System requests an online authorization of the transaction. In response, the card determines whether to decline the transaction off–line or to request an online authorization or referral.

Conditions of execution

This phase is mandatory if the Payment Gateway supports the commonChip extension.

Process description

The Cardholder System shall perform Terminal Action Analysis as prescribed by *EMV '96 ICC Application Specification for Payment Systems.* The Cardholder System shall assume the role of the "terminal" described therein and behave just like that terminal with the following exceptions:

Exception	Description
Changes to Issuer and Terminal Action Code Processing	The Cardholder System shall not compare the Terminal Verification Results to the card's Issuer Action Codes or to Terminal Action Codes.
GENERATE AC Command	The Cardholder System shall tailor the GENERATE AC command by limiting the values of its reference control parameters to ARQC.
Source of data requested in CDOL1	The Data Elements the Cardholder System transmits to the card in the data field of the GENERATE AC command shall be obtained from the sources indicated in Table 8.
Converting Cryptogram Data	Some of the Data Elements the Cardholder System obtains for transmission to the card in the data field of the GENERATE AC command must be converted to formats the card understands as prescribed in Table 9.

Table 7—Terminal Action Analysis exceptions

Continued on next page

Terminal Action Analysis, continued

Source of data requested in CDOL1

The Cardholder System shall obtain the data elements requested by the EMV IC Card in the CDOL1 from the following sources and transaction processing phases indicated below:

Data Element	Transaction Processing Phase	Source
Amount, Authorized	SET Initiation	PurchAmt
Amount, Other	———————————	Cardholder System
Terminal Country Code	Purchase Initialization	Merchant certificate [merchcert.merchantdata.mercountry]
Terminal Verification Results	———————————	Cardholder System
Transaction Currency Code	SET Initiation	PurchAmt
Transaction Date	Purchase Initialization	PreqDate
Transaction Type	———————————	Cardholder System
Unpredictable Number	Terminal Action Analysis	The Cardholder System shall generate the Unpredictable Number as follows: 1. Obtain the SET defined Data Element, XID (Transaction ID). 2. Divide the XID (from left to right) into five 4-byte blocks. 3. Exclusive-or the first block (leftmost) with the second block. 4. Exclusive-or the result from Step 3 with the third block. 5. Exclusive-or the result from Step 4 with the fourth block. 6. Exclusive-or the result from Step 5 with the fifth block. The 4–byte result of this operation is the Unpredictable Number.

Table 8—Source of data requested in CDOL1

Continued on next page

Terminal Action Analysis, continued

Converting CDOL1 data

Before transmitting it to the card in the data field of the GENERATE AC command, the Cardholder System shall convert some of the source data referenced above as follows:

Source Data	Conversion Procedure	Output
PurchAmt	Extract Currency	Transaction Currency Code
PurchAmt	Extract Amount	Amount, Authorised
PreqDate	Extract YYYYMMDD from the PInitRes message and strip the first two digits to derive YYMMDD.	Transaction Date

Table 9—Converting CDOL1 Data for Terminal Action Analysis

Section 7
Issuer Script Processing and Completion

Introduction

Issuer Script Processing and Completion is the transaction processing phase in which the Cardholder System terminates the involvement of the Cardholder and the IC Card with the transaction.

Conditions of executions

This phase is mandatory.

Process description

The Cardholder System shall perform Issuer Script Processing and Completion according to the following conditions:

Condition	Process
The card application declines the transaction.	The Cardholder System shall terminate the transaction, inform the Cardholder that the purchase has been declined and that it is now permissible to remove the card from the Interface Device (IFD).
The PInitRes indicates the Payment Gateway does not support the Common Chip Extension, or The PRes message has been processed and the AuthCode indicates orderReceived, noReply, piAuthMismatch or systemError, or The Cardholder System does not receive a PRes message in a timely manner.	The Cardholder System shall: a) Perform the processing prescribed by Section 7.11 of the *EMV IC Card Application Specification for Payment Systems*, with the following exception. The Cardholder System shall request an AAC and will assign the value ‘Z3’ to the Authorization Response Code (tag ‘8A’). b) Inform the Cardholder that it is now permissible to remove the card from the IFD.

Continued on next page

Issuer Script Processing and Completion, continued

Process description (continued)

The PRes message has been processed and the AuthCode does not indicate orderReceived, noReply, piAuthMismatch or systemError.	The Cardholder System shall: a) Examine the contents of the acqCardExtensions of the PRes to determine whether Issuer Scripts (tag '71' or '72') are present. If scripts are present they are to be processed as per *EMV '96 IC Card Application Specification for Payment Systems* Section 7.10. a) Perform the processing prescribed by Section 7.11 of the *EMV Application Specification for Payment Systems* (using any other EMV data from the acqCardExtensions), with the following exceptions. The Cardholder System shall examine the AuthCode of PRes to determine which type of cryptogram it should request. If the AuthCode indicates declined, callIssuer, amountError, expiredCard, invalidTransaction, the Cardholder System shall request an AAC and will assign the value '05' to the Authorization Response Code (tag '8A'). If the AuthCode indicates approved, the Cardholder System shall request a TC and will assign the value '00' to the Authorization Response Code (tag '8A'). b) After receiving the card's response to the second GENERATE AC command and after the execution of all Issuer Scripts present, inform the Cardholder that it is permissible to remove the card. The results of the second GENERATE AC are ignored.

Chapter 3
Cardholder System—Merchant Server Interface

Overview

Introduction

Chapter 3 describes the transaction processing phases that involve interaction between the Cardholder System and the Merchant Server.

Phases of transaction processing that do not involve interaction between the Cardholder System and the Merchant Server are detailed in chapters 2 and 4.

Organization

Chapter 3 describes the following transaction processing phases:

Section	Title	Contents
1	SET Initiation	Describes the SET Initiation Message used to invoke the Cardholder System.
2	Purchase Initialization Request & Response	Describes the PInitReq and PInitRes messages, which support initialization of the SET protocol.
3	Purchase Request & Response	Describes the PReq and PRes messages, which constitute the purchase transaction between the Cardholder System and Merchant.

Section 1
SET Initiation

Introduction

SET Initiation is the phase of a purchase transaction during which the Merchant Server invokes the Cardholder System and informs it of the transaction details and accepted payment brands.

Conditions of use

The Merchant Server shall initiate every SET purchase transaction.

Creation of SET Payment Initiation message

Merchant Servers shall create SET Payment Initiation messages as prescribed by *External Interface Guide to SET Secure Electronic Commerce*.

Processing of SET Initiation Message

The Cardholder System shall process SET initiation messages as prescribed by *External Interface Guide to SET Secure Electronic Commerce.*

Section 2
Purchase Initialization

Introduction

Purchase Initialization is the phase of a purchase transaction during which:

1. The Merchant Server obtains the information that it needs to understand the context of the transaction.
2. The Cardholder System obtains the information that it needs to create a purchase request, as well as authenticate the Merchant Server and Payment Gateway.

Conditions of use

The Cardholder System shall initialize every purchase transaction.

Rules

The mechanism that SET provides for purchase initialization is the PInitReq and PInitRes messages.

The Cardholder System shall create the PInitReq message as prescribed below.

The Merchant Server shall process PInitReq and create PInitRes as prescribed by SET.

The Cardholder System shall process PInitRes as prescribed by SET.

Continued on next page

Cardholder System Creates PInitReq

Completing PInitReq

The Cardholder System shall create PInitReq as prescribed by SET, with the following exceptions:

Step	Action
1	Obtain the IC Card specific data inputs to PInitReq from the card application.
2	Convert the data objects obtained from the card to SET formats.

Obtaining Data Objects from IC Card

The Cardholder System shall obtain the following data objects from the card application. The sources of these data objects and elements, i.e. the phase of transaction processing during which they are retrieved, are indicated below. Once converted, these data objects shall serve as inputs to the PInitReq message.

SET Data Input	Corresponding Card Data Object	Source	Tag
Language	Language Preference	Application Selection phase	‘5F2D’
BrandID	AID (of selected application)	Application Selection phase	‘4F’
BIN	PAN	Read Application data phase	‘5A’

Table 10—IC Card Data inputs to PInitReq

Note: Cardholder Systems designed for use in a private environment (a home PC for example) may provide an option to use a Cardholder–selected language rather than the IC Card’s language.

Converting Data Objects to Data Inputs

The Cardholder System shall convert the data objects obtained from the card as follows:

Data Element	Conversion Procedure
PAN	Let the first six digits of the PAN constitute the BIN.
AID	Obtain the brand corresponding to this AID from the Brand—AID mapping table.

Table 11—Converting IC Card Data inputs to PInitReq

Cardholder System Processes PInitRes

Processing PInitRes

The Cardholder System shall process the PInitRes as prescribed by SET with the following addition.

The Cardholder System shall examine the Payment Gateway's certificate to ascertain whether it supports the commonChip and onlinePIN extensions.

Section 3
Purchase Request & Response

Introduction

Purchase Request is the transaction processing phase in which the Cardholder System requests the actual purchase from the merchant. Purchase Response is the transaction processing phase in which the Merchant Server informs the Cardholder System of the status of the Purchase Request.

Conditions of use

The Cardholder System shall transmit the Purchase Request (PReq) message after initializing each purchase transaction. The Merchant Server may transmit the Purchase Response (PRes) message anytime after it receives the Purchase Request Message, even before it sends an Authorization Request to the Payment Gateway.

Rules

The mechanism that SET provides for purchase request is the PReq and PRes messages.

The Cardholder System shall create the PReq message as follows:

1. If a SET Cardholder certificate associated with the selected account is available during the transaction, the Cardholder System shall create a PReqDualSigned message, otherwise it shall create a PReqUnsigned message as prescribed by this section.
2. If the Cardholder Verification Method selected was Online PIN, the Cardholder System shall create and append the onlinePIN extension to the PReq message as prescribed in the *SET Online PIN Extension.*
3. If the Terminal Action Analysis phase resulted in an ARQC or an AAR, the Cardholder System shall create and append the commonChip extension to the PReq message as prescribed below.

The Merchant Server shall process the PReq and create a PRes as prescribed by SET.

The Cardholder System shall process the PRes as prescribed by SET.

Continued on next page

Cardholder System's Creation of PReq

Completing PReq

The Cardholder System shall create the PReq as prescribed by SET, making the following changes to the manner in which the Payment Instructions are created:

Step	Action
1	Obtain the IC Card specific data inputs to the Payment Instructions (PI).
2	Convert the data objects obtained from card to SET required formats.

Obtaining Data Elements from IC Card

The Cardholder System shall obtain the following data elements from the card application to serve as inputs to the PI. The sources of these data elements, i.e. the phase of transaction processing during which they are accessed, are indicated below.

PI Input	Corresponding Card Data Element	Source	Tag
Language	Language Preference	Application Selection phase	'5F2D'
BrandID	AID (of selected application)	Application Selection phase	'4F'
PAN	PAN	Read Application data phase	'5A'
BIN	PAN	Read Application data phase	'5A'
CardExpiry	Application Expiration Date	Read Application data phase	'5F24'

Table 12—IC Card Data inputs to Payment Instructions

Continued on next page

Cardholder System's Creation of PReq, continued

Converting Data Elements to PI Inputs

The Cardholder System shall convert the Data Elements obtained from the card as follows:

Data Object	Conversion Procedure
PAN	The first six digits of the PAN identify the BIN.
AID	Obtain the brand corresponding to this AID from the Brand—AID mapping table.
Application Expiration Date	Annex B of the *EMV '96 IC Card Specification for Payment Systems* defines the format for Application Expiration Date to be YYMMDD. However, the SET Specification defines the format for CardExpiry to be YYYYMM. Therefore, the Cardholder System shall reformat Application expiration Date as prescribed below: 1. Drop DD. 2. Use same MM. 3. Convert the YY value to a four–digit year as prescribed by EMV.

Table 13—Converting IC Card Data to PI Inputs

Continued on next page

Cardholder System's Creation of Common Chip Extension

Creating the commonChip extension

When required, the Cardholder System shall append the commonChip extension to the PIHead portion of the PReq message. It shall code this extension as prescribed by *SET Common Chip Extension*. The EMVData field of the extension must include the Data Elements listed in the table below, when available for the transaction.

The data that appears in the EMV data field can be in any order but must be TLV encoded and bit–wise identical to the fields presented to the IC Card. The Cardholder System shall obtain these Data Elements from the source identified in the last column of the table.

Name	Tag	Format	Length	Sources
Amount, Authorized	'9F02'	n	6	SET Initiation Phase
Amount, Other	'9F03'	n12	6	Cardholder System
Application Cryptogram	'9F26'	b	8	Terminal Action Analysis
Application Interchange Profile	'82'	b	2	Application Initiation Phase
Application PAN Sequence Number	'5F34'	n2	1	Read Application Data
Application Transaction Counter	'9F36'	b	2	Read Application Data
Cryptogram Information Data	'9F27'	b	1	Terminal Action Analysis
Issuer Application Data	'9F10'	b	Var. up 32	Terminal Action Analysis
Terminal Country Code	'9F1A'	n	2	Purchase Initialization
Terminal Verification Results	'95'	b	5	Terminal Action Analysis
Track–2 Equivalent Data	'57'	b	Var. up 19	Read Application Data Phase (the Cardholder System shall set the PAN and Expiration Date in this data object to zero before transmitting it in the extension)
Transaction Currency Code	'5F2A'	n	2	SET Initiation Phase
Transaction Date	'9A'	n	3	Purchase Initialization Phase
Transaction Type	'9C'	n	1	Cardholder System
Unpredictable Number	'9F37'	b	4	Terminal Action Analysis

Table 14—commonChip extension data and its sources

Chapter 4
Merchant Server—Payment Gateway Interface

Overview

Introduction

Chapter 4 describes the transaction processing phases that involve interaction between the Merchant Server and the Payment Gateway. It defines the messages through which Merchant Servers and Payment Gateways communicate to complete a phase of transaction processing. Phases of transaction processing that do not involve interaction between the Merchant Server and the Payment Gateway are detailed in chapters 2 and 3.

Organization

Chapter 4 describes the following phases of transaction processing:

Section	Title	Contents
1	Authorization Request & Response	Describes the AuthReq and AuthRes messages, which support the authorization stage of the payment transaction.
2	Capture Request & Response	Describes the CapReq and CapRes messages, which support the capture stage of the purchase transaction.

Section 1
Authorization Request & Response

Overview

Introduction

Authorization Request is the phase in which the Merchant Server requests an authorization for the Cardholder's intended purchase.

Authorization Response is the phase in which the Payment Gateway informs the Merchant Server whether the purchase has been approved or declined by the issuer. It also provides the merchant with the data necessary to request the capture of the transaction.

Conditions of execution

The Merchant Server shall transmit the Authorization Request (AuthReq) message after it receives a valid purchase request from the Cardholder System. The Payment Gateway shall transmit the Authorization Response (AuthRes) message after it has received an authorization response.

Rules

The Merchant Server shall create the AuthReq as prescribed by SET.

The Payment Gateway shall process AuthReq and may create AuthRes as prescribed below.

The Merchant Server shall process AuthRes as prescribed by SET.

Payment Gateway Processing of AuthReq

Payment Gateway processes AuthReq

The Payment Gateway shall process the AuthReq as follows:

Step	Action
1	Process AuthReq as prescribed by SET
2	If the PIHead contains the commonChip extension then: Re–calculate the Unpredictable Number and compare the fresh results with the Unpredictable Number contained in the commonChip extension. If the recalculated and transmitted Unpredictable Numbers do not match then proceed to AuthRes, otherwise continue.
3	Request issuer authorization.

Re–calculating Unpredictable Number

To ensure the cryptogram is fresh, the Payment Gateway shall recalculate the Unpredictable Number transmitted in the extension as prescribed below. The 4–byte result of this operation is the Unpredictable Number.

Step	Action
1	Divide the XID (from left to right) into five 4–byte blocks.
2	Exclusive–or the first block (leftmost) with the second block.
3	Exclusive–or the result from Step 2 with the third block.
4	Exclusive–or the result from Step 3 with the fourth block.
5	Exclusive–or the result from Step 4 with the fifth block.

Table 15—Re–calculating the Unpredictable Number

Payment Gateway Creation of AuthRes

Completing AuthRes

The Payment Gateway shall create AuthRes as prescribed by SET with the following exception.

Exception	Action
1	If the recalculated and transmitted Unpredictable Numbers do not match, the Payment Gateway shall return an Authorisation Response with AuthCode set to piAuthMismatch.
2	If the issuer transmitted Issuer Authentication Data or Issuer Script(s) in its response to the Payment Gateway's earlier authorization request, the Payment Gateway shall transmit this information to the Cardholder System through the acqCardExtensions in the SET AcqCardMsg.
3	If the Merchant Server is to supply the Payment Gateway or the acquirer with the data that is required to capture approved transactions, the Payment Gateway must transmit to the merchant the additional data required to capture transactions in which the cryptogram is used to verify the authenticity of the card.

Modifications to SET Acquirer Card Message

The Payment Gateway must be able to transmit Issuer Authentication Data (tag '91') and Issuer Script(s) (tag '71' or '72') to the Cardholder System by including the acqCardExtensions as defined in the *SET Common Chip Extension*.

Continued on next page

Payment Gateway Creation of AuthRes, continued

Transmitting capture data to the Merchant Server

Merchants who supply the Payment Gateway or the acquirer with the data required to capture approved transactions must provide the EMV data used to verify the authenticity of the card. This additional data is the emvData field of the commonChip extension.

To be able to provide this additional data, the Merchant Server must have received it from the Payment Gateway in one of two fields of the AuthRes message. If the Payment Gateway wishes to enable the Merchant Server to decrypt the emvData, to capture outside of SET for example, the Payment Gateway must transmit it as an extension to the AuthResPayload field of AuthRes. If not, the Payment Gateway may transmit it via the TokenOpaque field of the Capture Token.

Since TokenOpaque is an open type (containing DER-encoded data) meaningful only to the Payment Gateway, to transport EMVData, ChipTokenOpaque may be used as an alternative definition for TokenOpaque, where:

```
ChipTokenOpaque ::=       SEQUENCE {
  emvData           EMVData,
  tokenOpaque       TokenOpaque
}.
```

Section 2
Capture Request & Response

Introduction

Capture Request is the phase of transaction processing in which the merchant requests clearing, i.e., financial payment, for one or more previously authorized transactions. Capture response is the phase of transaction processing in which the Payment Gateway notifies the Merchant Server of the status of its capture request.

Conditions of execution

The means by which the Merchant Server captures transactions and the times at which it does so may vary. For example, a merchant may delay the clearing of a transaction and when clearing the transaction, the merchant may clear it out–of–band to SET.

Rules

The contents of the EMVData field of the commonChip extension should be included in Payment System messages related to the original authorization request (e.g., subsequent authorization requests/reversals needed to process split and recurring payments, and clearing messages in general.) Exactly how this data ultimately reaches the clearing and settlement system depends upon the processing relationships and capabilities of the Merchant Server, Payment Gateway, merchant back office, and the acquirer's system.

Appendices

Organization

The appendices are as follows:

Appendices	Title	Contents
1	Issuer URL	Describes how the Cardholder System may retrieve a graphic for display to the Cardholder.
2	Cardholder System Flow Diagram	An informational appendix providing a flow diagram of the Cardholder System's processing steps.
3	Cardholder System Implementations	An informational appendix providing a high level model of the EMV Cardholder System and recommend guidelines which members and vendors can use as part of their design process.

Appendix 1
Issuer URL

Introduction

The issuer Uniform Resource Locator (URL), located in the ADF, points to the location of (a) brand or financial institution logo(s) that the Cardholder System may retrieve for display to the Cardholder during the transaction.

Structure of Issuer URL

The structure of the Issuer URL is illustrated below. It consists of two parts, the Issuer's server, which is identified by its Scheme and Authority, and an ApplicationID:

URL	**<Scheme>://<Authority><ApplicationID>**
Scheme	Example: http://
Authority	Example: www.bankname.com/
ApplicationID	Examples: Brand–xCreditClassic, or a reference number.

Table 16—Issuer URL data

Example of processing an Issuer URL

In order to retrieve the logo to be displayed, the Cardholder System shall generate the Issuer URL as follows:

Step	Action
1	Read the URL: e.g. http://www.bankname.com/Brand—xCreditClassic.
2	Append the filename for the desired logo prior to sending the request to create: http://www.bankname.com/Brand—xCreditClassic/small.gif

For more information

The graphic formats for the logo are defined in Appendix F of the SET 1.0 Specification.

For more information regarding URL, see IETF RFC 1738 "Uniform Resource Locator (URL)."

Appendix 2
Cardholder System Flow Diagram

(This appendix is informative and does not form an integral part of this Specification)

Introduction

This appendix illustrates the flow of the Cardholder System's processing steps.

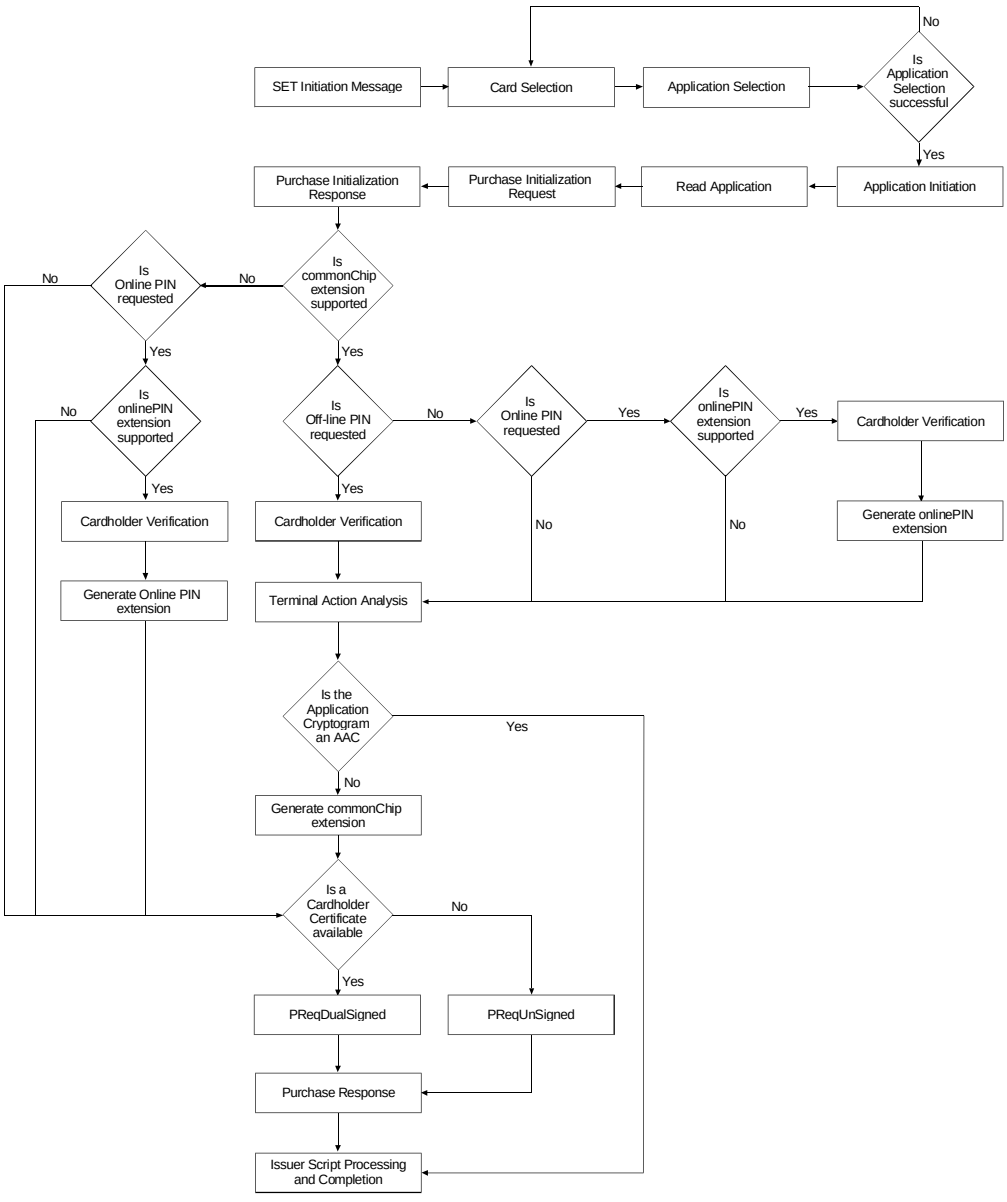

Figure 3—Cardholder System Flow Diagram

Appendix 3
Cardholder System Implementations

(This appendix is informative and does not form an integral part of this Specification)

Overview

Introduction

This specification defines the integration of EMV card technology and SET electronic commerce technology. In it, the communication between the card and the merchant is managed by a system called the Cardholder System. Prior to the development of Chip Electronic Commerce, a SET Cardholder System was usually a software application stored on a PC that acted as a helper to a Web browser. This application is commonly referred to as a SET "wallet".

The design of a Cardholder System however, is not limited to a single device or implementation. A growing number of implementations experiment with client-server architectures, thereby gaining advantages such as simplified distribution and upgrades. Similarly, certain Chip Electronic Commerce implementations have also been designed to provide an authentication migration path, whereby a SET cardholder certificate is used should the merchant and their acquirer not support the IC Card's cryptogram.

This specification does not specify or recommend any particular implementation or describe the merits of any implimentation; rather, it aims to define a high level model of the EMV Cardholder System which members and vendors can use as part of their design process. The aim of this informational appendix is to encourage members and vendors to experiment with different technical configurations based upon this specification. This appendix also explores two sample implementations that address the issue of authenticating an chip card initiated transactions to a merchant and acquirer who are not chip capable.

It is offered by the EMV Chip Electronic Commerce working group as an aid to the ongoing SET Technical Advisory Group efforts to define the technical requirements for server based wallets.

Definition of Cardholder System

The EMV Cardholder System is any combination of hardware and software that allows a cardholder to conduct an EMV compliant SET payment with a merchant's system. It is an abstract term covering any number of logical components that reside on a single physical device, or are distributed across any number of connected devices.

Continued on next page

Cardholder System Implementations, continued

Cardholder System components

The EMV Cardholder System can be divided into seven functional components and a internal communication protocol defining the interaction of each component. The components are:

- Cardholder interface
- Cardholder database
- SET message manager
- SET private key manager
- EMV message manager
- IC Card Interface device
- PIN entry device (optional)
- Internal communication protocol

Components

The relationship between components of the EMV Cardholder System is depicted below:

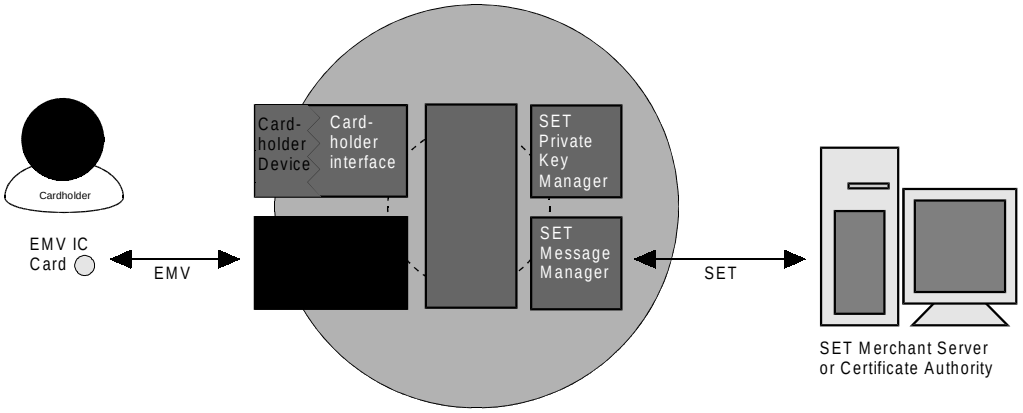

Figure 4—Cardholder System components

Overall guideline

The Cardholder System, being the sum of the components, must minimize the risk of limited or systemic compromise. The specific security requirements must be appropriate for the implementation of the system as a whole. For example, the risks and therefore the security requirements for a classic SET application on a personal computer will be less than those for a server based Cardholder System designed to serve hundreds of cardholders.

Cardholder interface and device

The Cardholder interface and device is responsible for the system's input/output (such as keyboard, screen, and graphic user interface) allowing the Cardholder to interact with the system.

The Cardholder interface and device must protect the Cardholder's input, as well as the display or output of system information in accordance with industry best practice.

Continued on next page

Cardholder System Implementations, continued

Cardholder database	The Cardholder database is responsible for the management of all Cardholder data, both payment data and non–payment data, such as a telephone number. Some configurations may store this data; others might hold it only for the duration of a transaction Cardholder data must be processed and stored in a manner that secures the confidentiality and integrity of sensitive data (both personal and payment related, such as PAN, PANSecret and Expiry) from external and internal attacks.
SET message manager	The SET message manager is responsible for the SET message interaction between a Merchant Server and Cardholder Certificate Authority. The SET Message Manager shall be capable of interfacing with a SET Merchant Server or Certificate Authority as defined by the SET Specification.
SET private key manager	The SET private key manager is responsible for the use and security of the SET Cardholder private key. The SET Private Key Manager, in conjunction with the SET Message Manager, must process certificate request and purchase request signing operations in a manner that assures the security of the private key.
EMV manager	The EMV manager is responsible for the EMV message interaction between an EMV Device and Card. The EMV Manager must, at a minimum, support the EMV Commands, and ChipEC protocols defined in the Chip Electronic Commerce Specification.
IC Card interface device (IFD)	The IC Card Interface device (IFD) is a physical card–reading device that is responsible for allowing the EMV manager to communicate with an EMV card. The IC Card Interface device must, at a minimum, be an EMV level 1 compliant card reader capable of interfacing with the EMV manager.
PIN entry device (optional)	The PIN entry device, which is optional, is a physical Cardholder input device capable of accepting the entry of a PIN. The PIN entry device must comply with applicable Payment System requirements and industry best practices.

Continued on next page

Cardholder System Implementations, continued

Internal communication protocol

The Internal Communication Protocol is responsible for the communication between the Cardholder System components. A Cardholder System may posses one or both types of the communication protocols described below.

Internal communications between interconnected devices.
Components that reside in different devices must communicate in a manner that ensures that the information is passed in a timely, reliable and secure manner. It must also ensure the integrity of the individual components and their host device. At a minimum, sensitive payment data, such as PAN, Expiry and Track 2 equivalent data, should be protected to the same degree as they are in a SET message.

Internal communications within a device.
Components within a device must communicate in a manner that ensures the security of both the information passed, and the integrity of the components themselves. The implementation should follow established best practices for financial applications running on that device/Operating System.

Continued on next page

Cardholder System Implementations, continued

Organization

Appendix 3 includes the following sample implementations:

Section	Title	Description
1	Hosted Cardholder System	A sample implementation of a client–server based Cardholder System where the majority of the Cardholder System components reside on the server. It is designed to provide Cardholder authentication either through the use of a cryptogram, or for those acquirers who have yet to migrate to EMV, a SET Cardholder certificate.
2	Thick client Cardholder System	A sample implementation of a client–server based Cardholder System where the majority of the Cardholder System components reside on the client. It is designed to provide Cardholder authentication through the use of a cryptogram, and/or a SET Cardholder certificate.

Section 1
Hosted Cardholder System

Client–server based Cardholder System

This implementation explores hosting the majority of the SET Cardholder System components on a centralized server. This can facilitate the update and management of a large number of Cardholder Systems as most of their functionality has been concentrated on the server. Furthermore, as the installation of a "thin" Cardholder Client application is less complex, it is expected that the deployment and Cardholder usage will increase.

Component allocation

This implementation allocates the Cardholder System components as follows:

Component	Location
Cardholder interface	Client
Cardholder database	Server
SET message manager	Server
SET private key manager	Server
EMV manager	Client
EMV device	Client
PIN entry device (optional)	Client
Internal communication protocol	Shared

Continued on next page

Hosted Cardholder System, continued

Description of Hosted Cardholder System example

The components interact as follows:

Step	Description
1	The SET Merchant Server sends a standard SET Initiation message.
2	The Chip enabled Cardholder Client forwards the wake–up message to the Cardholder Server requesting that it complete a standard SET transaction. The Cardholder uses a cryptogram as a key to access the server.
3 & 4	The Cardholder Server having received the Client request message, validates the cryptogram by contacting the issuer through an out of band mechanism, and if successful, uses the information in the wakeup message to conduct a SET transaction on the Cardholder's behalf. Depending on the server's capabilities, a certificate and/or a cryptogram may be used in the Purchase Request.
5	Upon the completion of the transaction the Cardholder Server sends a purchase response message to the Cardholder Client informing it of the transaction results.

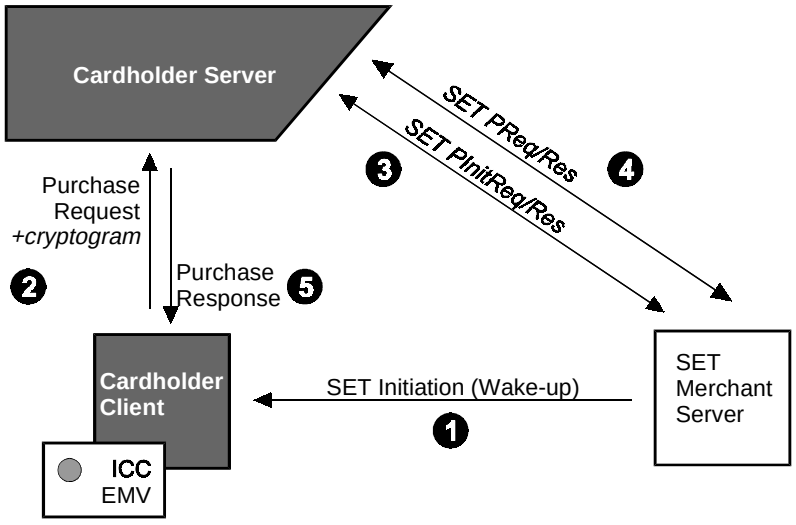

Figure 5—Hosted Cardholder System example

Section 2
Thick Client Cardholder System

Client–server based Cardholder System (thick client)

This example implementation explores hosting the majority of the SET Cardholder System functions on the Cardholder Client, while the server provides a specialized service to the client. The example below describes a server that manages the certificate request and signing processes for a PReqDualsigned transaction. Note, in this example the certificate and private key are not stored on the Cardholder Client.

This implementation might suit markets where some SET merchant/acquirers do not support EMV transactions and where a hosted wallet is not considered appropriate. This configuration may also allow the server to be phased out once EMV is universally accepted.

Component allocation

This implementation allocates the Cardholder System components as follows:

Component	Location
Cardholder interface	Client
Cardholder database	Client
SET message manager	Client
SET private key manager	Server
EMV manager	Client
EMV device	Client
PIN entry device (optional)	Client
Internal communication protocol	Shared

Continued on next page

Thick client Cardholder System, continued

Description of Thick Client example

The components interact as follows:

Step	Description
1	The SET Merchant Server sends a standard SET Initiation message.
2	The Cardholder Client sends a standard SET Purchase Initialization Request message indicating which payment brand is being used and receives a standard response from the merchant.
3	The Chip enabled Cardholder System determines from the Initialization Response if the merchant/acquirer supports EMV. If they do, the transaction will continue as a ChipEC transaction and the server is not required. If they do not, the Cardholder Client generates the Payment Information (Payment information to be signed Data Element, PITBS) for the SET Purchase Request and the sends it to the server as part of a signing request to the server using a cryptogram as the authentication data.
4	The server receives the request for authentication, and once the cryptogram has been verified by the issuer using an out of band mechanism, signs the PITBS data and returns it along with a Cardholder certificate (containing the Cardholder's public key.)
5	The Cardholder System continues the transaction as a standard SET transaction signed with a Cardholder certificate.

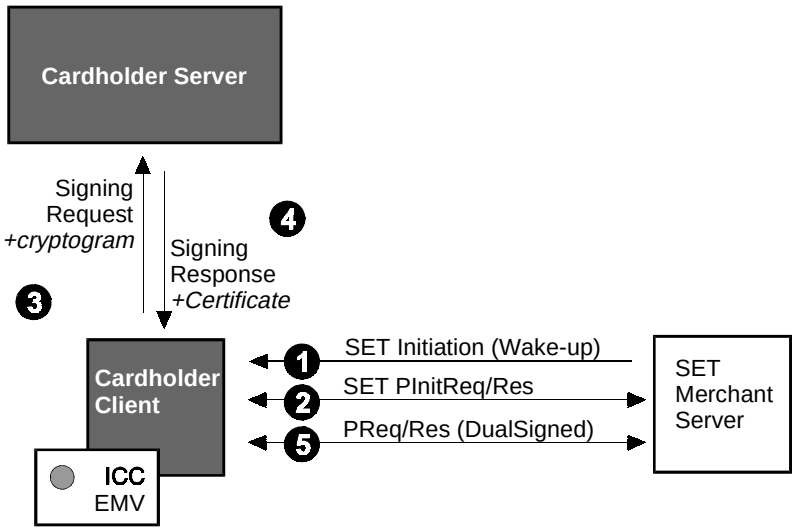

Figure 6—Thick Client example