



V.I.P. System Overview

V.I.P. System

Effective: 1 June 2017



Visa Supplemental Requirements

Important Note on Confidentiality and Copyright

The Visa Confidential label signifies that the information in this document is confidential and proprietary to Visa and is intended for use only by Visa Clients subject to the confidentiality restrictions in the Visa Rules, non-Client Third-Party Processors that have an executed and valid Exhibit K on file with Visa, and other third parties that have a current nondisclosure agreement (NDA) with Visa that covers disclosure of the information contained herein.

This document is protected by copyright restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Visa.

Visa and other trademarks are trademarks or registered trademarks of Visa.

All other product names mentioned herein are the trademarks of their respective owners.

About Visa Supplemental Documents

This document is a supplement of the *Visa Core Rules and Visa Product and Service Rules*. In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the *Visa Core Rules and Visa Product and Service Rules*, the *Visa Core Rules and Visa Product and Service Rules* shall govern and control.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN: THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. VISA MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.

If you have technical questions or questions regarding a Visa service or capability, contact your Visa representative. If you have technical questions or questions regarding a Visa service or questions about this document, please contact your Visa representative.

Contents

About This Manual.....1

 Audience.....1

 Organization.....1

 Document Conventions.....2

 Documentation Descriptions.....2

 Information Sources.....5

 Report Samples.....5

 More Information.....5

Chapter 1 • System Basics

 1.1 VisaNet Overview.....1-1

 1.1.1 Basic Services Defined.....1-2

 1.2 Visa Products.....1-2

 1.2.1 Comparison of Visa Products.....1-4

 1.3 VisaNet Components.....1-4

 1.4 VisaNet Systems.....1-6

 1.4.1 VisaNet Integrated Payment (V.I.P.) System.....1-7

 1.4.2 BASE I System.....1-7

 1.4.3 Single Message System (SMS).....1-8

 1.4.4 BASE II System.....1-9

 1.4.5 VisaNet Settlement Service (VSS).....1-10

 1.5 Common Member Interface (CMI) and Interface Methods.....1-11

 1.6 Processing Parameters.....1-12

1.7	System Messages.....	1-13
Chapter 2 • System Transaction Processing		
2.1	Transaction Flow.....	2-1
2.2	Message Processing.....	2-2
2.3	Message Validation and Preparation.....	2-2
2.3.1	Message Format.....	2-2
2.3.2	Message Structure.....	2-2
2.3.3	Message Matching.....	2-3
2.3.4	Validation and Preparation Requirements.....	2-3
2.4	Message Routing Basics.....	2-3
2.4.1	Routing Messages.....	2-4
2.4.1.1	Routing Tables.....	2-4
2.4.1.2	Internal Routing Services.....	2-5
2.4.1.3	Gateways to Non-VisaNet Destinations.....	2-5
2.5	Stand-In Processing (STIP).....	2-5
2.5.1	BASE I STIP.....	2-6
2.5.2	SMS STIP.....	2-6
2.6	Response Processing.....	2-7
2.7	Logging.....	2-7
2.8	Additional System Functions.....	2-7
2.8.1	Managing the Network.....	2-7
2.8.2	Managing System Tables.....	2-8
2.8.3	Managing System Databases.....	2-8
2.8.3.1	Cardholder Database Files.....	2-8
2.8.3.2	Merchant Central File (MCF).....	2-9
2.8.4	Reporting.....	2-9
2.8.4.1	BASE I Reports.....	2-10
2.8.4.2	SMS Reports and Raw Data.....	2-10
2.8.4.3	Settlement Reports.....	2-10
2.8.5	Billing.....	2-10

Chapter 3 • System Services

3.1	Service Functional Groups.....	3-1
3.2	Routing Service Definitions.....	3-2
3.2.1	ATM/POS Split Routing Service.....	3-2
3.2.2	Check Acceptance Service.....	3-3
3.2.3	Gateway Services.....	3-3
3.2.4	PIN Debit Gateway Service (PDGS).....	3-3
3.2.5	PIN/No-PIN Split Routing Service.....	3-4
3.2.6	Priority Routing Service.....	3-4
3.2.7	Visa Shortest Online Path (VSOP) Service.....	3-4
3.3	Routing Service Availability.....	3-4
3.4	Risk Management Service Definitions.....	3-5
3.4.1	Card Recovery Bulletin (CRB) Service.....	3-5
3.4.2	Fraud Reporting System (FRS).....	3-5
3.5	Risk Management Service Availability.....	3-5
3.6	Visa Secure Electronic Commerce (VSEC) Service Definition.....	3-5
3.6.1	Visa Secure Electronic Commerce (VSEC) With Verified by Visa (3-D Secure).....	3-5
3.7	VSEC Service Availability.....	3-6
3.8	Chip Card Service Definitions.....	3-6
3.8.1	Visa Contactless Payment Service (VCPS).....	3-6
3.8.2	Visa Smart Debit/Smart Credit (VSDC) Service.....	3-6
3.9	Chip Card Service Availability.....	3-7
3.10	Authorization Database Service Definitions.....	3-7
3.10.1	Automatic Cardholder Database Update (Auto-CDB) Service.....	3-7
3.10.2	Merchant Central File Service (MCFS).....	3-7
3.11	Authorization Database Service Availability.....	3-7
3.12	Authorization Service Definitions.....	3-7
3.12.1	Account Verification Service.....	3-8
3.12.2	Address Verification Service (AVS).....	3-8
3.12.3	Advice Retrieval Service—BASE I.....	3-8
3.12.4	Advice Retrieval Service—SMS.....	3-8

3.12.5	ATM Format Conversion Service.....	3-8
3.12.6	Card Verification Value (CVV) Service.....	3-9
3.12.7	Card Verification Value 2 (CVV2) Service.....	3-9
3.12.8	Cardholder Authentication Verification Value (CAVV) Verification Service.....	3-9
3.12.9	Custom Payment Service (CPS)/ATM.....	3-9
3.12.10	Custom Payment Service (CPS)/POS.....	3-9
3.12.11	Deferred Clearing Advice File (DCAF) Service.....	3-10
3.12.12	Dynamic Card Verification Value (dCVV) Service.....	3-10
3.12.13	Dynamic Key Exchange (DKE) Service.....	3-10
3.12.14	Multicurrency Service.....	3-10
3.12.15	PIN Verification Service (PVS).....	3-11
3.12.16	POS Check Service.....	3-11
3.12.17	Positive Authorization Capacity Management (PACM) Service.....	3-11
3.12.18	Positive Cardholder Authorization Service (PCAS).....	3-11
3.12.19	Preauthorized Payment Cancellation Service (PPCS).....	3-11
3.12.20	Status Check Service.....	3-12
3.12.21	VisaNet Cashback Service.....	3-12
3.13	Authorization Service Availability.....	3-12
3.14	Additional Service Definitions.....	3-13
3.14.1	Chargeback Reduction Service (CRS).....	3-13
3.14.2	ATM Processing Integration.....	3-13
3.15	Additional Service Availability.....	3-13

Chapter 4 • Acquirer and Issuer Responsibilities

4.1	Establishing Processing Centers.....	4-1
4.1.1	Network Stations.....	4-1
4.1.2	Message Support.....	4-1
4.1.3	Testing.....	4-2
4.1.4	Network Management.....	4-2
4.1.5	SMS Reconciliation and Settlement.....	4-2
4.2	Acquirer Processing Center Requirements.....	4-3

4.2.1	POS Connections and Procedures.....	4-3
4.2.2	PIN Security.....	4-4
4.2.3	Response Procedures.....	4-4
4.2.4	Merchant Central File Management.....	4-4
4.2.5	Follow-Up Procedures and Processing.....	4-4
4.2.6	Other Responsibilities.....	4-5
4.3	Issuer Processing Center Requirements.....	4-5
4.3.1	Transaction Authorization.....	4-5
4.3.2	Cardholder Database Management.....	4-6
4.3.3	PIN Security.....	4-6
4.3.4	Coordination With Visa.....	4-6
4.3.5	Response Procedures.....	4-6
4.3.6	Follow-Up Procedures and Processing.....	4-6
4.3.7	Other Responsibilities.....	4-7

Appendix A • Transaction Types

A.1	Cardholder Transactions.....	A-2
A.2	Merchant-Authorized Transactions.....	A-4
A.3	System-Generated Transactions.....	A-4
A.4	Exception Transactions.....	A-4
A.5	Fee-Related Transactions.....	A-5
A.6	Reconciliation Transactions.....	A-5
A.7	File Maintenance Transactions.....	A-5
A.8	Administrative Transactions.....	A-5
A.9	Network Management Transactions.....	A-5

Index	IX-1
--------------	-------	------

THIS PAGE INTENTIONALLY LEFT BLANK.

Figures

- 1-1** VisaNet Communications Network.....1-4
- 1-2** VisaNet Communications Network Flows.....1-6
- 1-3** VisaNet Systems and Transaction Processing.....1-7
- 1-4** VisaNet Software System Components.....1-9
- 1-5** VSS Process.....1-10
- 1-6** V.I.P. System Software at VIC and Processing Center.....1-12
- 2-1** VisaNet Basic Process Flow.....2-1

THIS PAGE INTENTIONALLY LEFT BLANK.

Tables

1	Document Conventions.....	2
2	V.I.P. System Manual Descriptions.....	2
1-1	Comparison of Visa Products.....	1-4
2-1	Message Structure.....	2-2
3-1	Services by Functional Group.....	3-1
3-2	Routing Service Availability.....	3-4
3-3	Risk Management Service Availability.....	3-5
3-4	VSEC Service Availability.....	3-6
3-5	Chip Card Service Availability.....	3-7
3-6	Authorization Database Service Availability.....	3-7
3-7	Authorization Service Availability.....	3-12
3-8	Additional Service Availability.....	3-13
A-1	V.I.P. Transaction Types.....	A-1

THIS PAGE INTENTIONALLY LEFT BLANK.

About This Manual

The *V.I.P. System Overview* presents general information about the *VisaNet Integrated Payment (V.I.P.) System*, the main Visa transaction processing system. The manual describes *VisaNet* (the global Visa transaction processing network), defines its system components, and explains where the V.I.P. System resides within the network.

It also:

- Provides basics about Visa messages, transactions, and V.I.P. transaction processing, and explains Visa services.
- Describes client responsibilities and VisaNet connection considerations.

Audience

The *V.I.P. System Overview* is for readers with little, or no, knowledge of VisaNet, the V.I.P. System, and Visa transaction processing.

Organization

Chapter 1, System Basics—Provides an overview V.I.P. and VisaNet, the V.I.P. authorization process flow, and VisaNet components. Describes V.I.P. *online* and *offline* functions.

Chapter 2, Transaction Processing—Describes V.I.P. messages and transactions and transaction processing.

Chapter 3, System Services—Lists and defines available services.

Chapter 4, Acquirer and Issuer Responsibilities—Identifies client participation requirements and options.

Appendix A, Transaction Types—Lists V.I.P. transaction types and indicates whether the BASE I System and Single Message System (SMS) can process them.

Document Conventions

Table 1 Document Conventions

Convention	Purpose
boldface	Extra emphasis (stronger than italics); field values and codes.
EXAMPLE	Identifies what accompanying text describes or explains.
IMPORTANT	Highlights information in text.
<i>italics</i>	Document titles; emphasis; variables; terms or acronyms being defined.
text in quote marks	Section names; first instance of word used in unconventional or technical context.
text in Courier New font	URLs and email addresses.
NOTE	Provides details about preceding topic.
n/a	Not applicable.
shaded illustrations	Systems or procedures not directly involved in process being illustrated.
white boxes in flow diagrams	Represent request messages.
shaded boxes in flow diagrams	Represent response messages.
dotted line boxes in flow diagrams	Illustrate advice messages.

Documentation Descriptions

V.I.P. System Overview, *V.I.P. System Services*, and *V.I.P. System Reports*, apply to BASE I System and Single Message System (SMS) processing.

V.I.P. System BASE I Processing Specifications and *V.I.P. System BASE I Technical Specifications, Volume 1 and Volume 2*, are specific to BASE I.

For SMS, the Visa U.S.A. (U.S.) region processing specifications for ATM, Interlink, and POS are consolidated in *V.I.P. System SMS Processing Specifications (U.S.)*. For international clients, ATM and POS have separate manuals.

Table 2 V.I.P. System Manual Descriptions

General Information
<i>V.I.P. System Overview</i>
Describes VisaNet and components, connection methods, processing concepts, requirements, and options. Defines V.I.P., BASE I, and SMS, Direct Exchange and Visa Extended Access Servers, issuer and acquirer responsibilities, and Visa Interchange Center operations. Introduces V.I.P. services.
Doc ID 0851-30
<i>V.I.P. System Reports</i>
Provides samples.
Doc ID 0852-30

Table 2 V.I.P. System Manual Descriptions (continued)

<i>V.I.P. System Services, Volume 1</i>	
Describes available services. Descriptions include processing requirements, options, features, key message fields, and message flows.	
Part 1: V.I.P. Basics Part 2: Routing Services Part 3: Risk Management Services Part 4: Visa Secure Electronic Commerce (VSEC) Services Part 5: Chip Card Services	
Doc ID 0853A-30	I
<i>V.I.P. System Services, Volume 2</i>	
Describes available services. Descriptions include processing requirements, options, features, key message fields, and message flows.	
Part 6: Authorization Database Files and Services Part 7: Authorization Services	
Doc ID 0853B-30	I
BASE I	
<i>V.I.P. System BASE I Processing Specifications</i>	
Describes BASE I processing, including message types, processing considerations, related services, and VisaNet connection methods.	
Doc ID 0847-30	I
<i>V.I.P. System BASE I Technical Specifications, Volume 1</i>	
Defines technical specifications of BASE I processing and fields.	
Doc ID 0844A-31	I
<i>V.I.P. System BASE I Technical Specifications, Volume 2</i>	
Defines technical specifications of BASE I processing, message formats, and file specifications.	
Doc ID 0844B-31	I
Interlink	
<i>V.I.P. System SMS Processing Specifications (U.S.)</i>	
Contains SMS information, including message types, processing considerations, connection methods, and services for Interlink, Visa and Plus ATM, Visa POS, and Visa Electron.	
Doc ID 0857-30	I
<i>V.I.P. System SMS Interlink Technical Specifications</i>	
Describes message formats, field descriptions, and file specifications for Interlink.	
Doc ID 0866-29	I

Table 2 V.I.P. System Manual Descriptions (continued)**SMS ATM***V.I.P. System SMS Processing Specifications (U.S.)*

Contains SMS information, including message types, processing considerations, connection methods, and services for Visa and Plus ATM, Interlink, Visa POS, and Visa Electron for clients in the U.S. region.

Doc ID 0857-30

V.I.P. System International SMS ATM Processing Specifications

Contains SMS ATM information, including message types, processing considerations, connection methods, and services for clients outside the U.S. region.

Doc ID 0839-30

V.I.P. System SMS ATM Technical Specifications, Volume 1

Contains field descriptions for ATM.

Doc ID 0868A-29

V.I.P. System SMS ATM Technical Specifications, Volume 2

Contains message formats and file specifications for ATM.

Doc ID 0868B-29

SMS POS*V.I.P. System SMS Processing Specifications (U.S.)*

Contains SMS information, including message types, processing considerations, connection methods, and services for Visa POS, Visa Electron, Visa and Plus ATM, and Interlink for clients in the U.S. region.

Doc ID 0857-30

V.I.P. System International SMS POS (Visa & Visa Electron) Processing Specifications

Contains SMS POS information, including message types, processing considerations, connection methods, and services for clients outside the U.S. region.

Doc ID 0835-30

V.I.P. System SMS POS (Visa & Visa Electron) Technical Specifications, Volume 1

Describes fields for Visa POS and Visa Electron.

Doc ID 0869A-30

V.I.P. System SMS POS (Visa & Visa Electron) Technical Specifications, Volume 2

Describes message formats and file specifications for Visa POS and Visa Electron.

Doc ID 0869B-29

Information Sources

Information is analyzed, rewritten, and reorganized. Technical staff and subject matter experts review and verify updates. Approved comments and change requests received from clients and Visa staff are incorporated.

V.I.P. System Manuals

See [Table 2](#).

VisaNet Business Enhancements Global Technical Letters and Implementation Guides

V.I.P. System Overview includes information from the April 2017 and July 2017 *VisaNet Business Enhancements Global Technical Letter and Implementation Guide*, Version 3.0, effective 9 March 2017.

Other Documents

Visa Core Rules and Visa Product and Service Rules, RTN publications, general and detailed design documents, and service advisories.

Report Samples

- *V.I.P. System Reports*
- *VisaNet Settlement Service (VSS) User's Guide, Volume 2, Reports*

More Information

Visa provides product and service documentation. Clients get guides from Visa representatives. If you have comments or questions about this document or technical questions about Visa services or capabilities, contact your Visa representative.

Related Publications

Visa Rules

Visa Core Rules and Visa Product and Service Rules contain the Visa Rules.

Qualifying merchants and third-party agents can request the *Interchange Qualification Guide*.

Deferred Clearing Advice File (DCAF) Service

V.I.P. System Services, Volume 2.

PIN Management Requirements

Payment Card Industry PIN Security Requirements Manual: Contains requirements for managing, processing, and transmitting PIN data.

PIN-Entry Device Security Requirements and Management Procedures:

- *Payment Card Industry Encrypting PIN PAD (EPP) Security Requirements Manual*
- *Payment Card Industry POS PIN-Entry Device Security Requirements Manual*

POS Check Service

Visa Core Rules and Visa Product and Service Rules

V.I.P. System Services, Volume 2

V.I.P. System SMS POS (Visa & Visa Electron) Technical Specifications

VisaNet Settlement Service (VSS) User's Guide, Volume 2, Reports

Risk Management Services

Card Recovery Bulletin Service User's Guide

Fraud Reporting System (FRS) User's Guide

Issuer's Clearinghouse Service User's Guide

Risk Management Process Guide

V.I.P. System Services, Volume 1

Visa Fraud Monitoring Program Guide

Visa Risk Manager

Security

Payment Technology Standards Manual—Contains standards for PINs and encoding data on Visa payment form factors.

Visa Extended Access Servers (EA Servers)

Extended Access Administration and Installation Guide

Extended Access Management Installation Guide

Extended Access Management Operators Guide

Extended Access Security Administration Guide

Extended Access Server Endpoint Guide

Visa Extended Access Server Endpoint Guide

Visa Incentive Network (VIN)

Credit Rewards Key Implementation Tasks and Best Practices

Credit Rewards: Visa Incentive Network and Credit Interchange Frequently Asked Questions

Visa Incentive Network Member Implementation Guide

Visa Incentive Network Service Description

Visa Signature Registration Toolkit

Visa Traditional Rewards Registration Toolkit

Visa Resolve Online (VROL)

Visa Resolve Online Administrator's Guide

Visa Resolve Online Bulk Systems Interface Development Guide

Visa Resolve Online Member Implementation Guide

Visa Resolve Online Real-Time Systems Interface Development Guide

Visa Resolve Online Reference Manual

Visa Resolve Online User's Guide

Visa Smart Debit/Smart Credit (VSDC) Service

V.I.P. System Services, Volume 1—Contains service description.

JCB, MasterCard, Visa (EMV) Specifications, EMV '96 Version 3.1.1 and EMV 2000 Version 4.0—Contain industry standards for chip card and terminal interaction:
www.emvco.com.

Visa Integrated Circuit Card Specifications (VIS)—Contains technical specifications for VSDC card application, describing VSDC transaction functionality and flow.

Visa Smart Debit and Credit Member Implementation Guide for Acquirers—Provides guidelines for acquirers implementing VSDC programs.

Visa Smart Debit and Credit Member Implementation Guide for Issuers—Provides guidelines for issuers implementing VSDC programs.

Visa Smart Debit and Credit Planning Guide—Helps clients plan VSDC programs and migration strategies.

Visa Smart Debit and Visa Smart Credit Service Description—Describes VSDC program features and benefits.

Visa Smart Debit/Visa Smart Credit System Technical Manual—Provides information for clients and Visa staff who implement and operate VSDC programs.

Miscellaneous Systems and Services

Authorization Gateway Service Cross-Reference Guide—Includes field-by-field data transfer descriptions between V.I.P.-format dual-message transactions, and American Express- and MasterCard-format transactions.

V.I.P. System Services, Volume 1 and Volume 2

Visa Global ATM Planning Guide—Includes program overview, business requirements, optional services, risk management, processing options, testing procedures, and back-office management for Visa and Plus International ATM Program.

Visa Information System User's Guide

Visa Test System—V.I.P. User's Guide

VisaNet Settlement Service (VSS) User's Guide, Volume 1, Specifications

VisaNet Settlement Service (VSS) User's Guide, Volume 2, Reports

System Basics

1

1.1 VisaNet Overview

VisaNet is the Visa financial transaction processing network, supporting transactions routed among acquirers and issuers in all Visa regions. *VisaNet* comprises the network's hardware, software, and communications components, and client regional systems and networks.

Visa has six regions:

- Asia-Pacific (AP)
- Central and Eastern Europe, Middle East, and Africa (CEMEA)
- Latin America and Caribbean (LAC)
- Visa Canada (CAN)
- Visa Europe (VE)
- Visa U.S.A. (U.S.)

Visa Canada and Visa U.S.A. are incorporated entities, and abide by Visa Charter Documents and individual regional by-laws. The AP, CEMEA, LAC, and VE regions are not incorporated separately from Visa Inc., but abide by Visa Charter Documents and regional by-laws.

Depending on the region, VisaNet supports:

- Purchase, cash, and bill and healthcare payment transactions made with Visa cards, including contactless cards.
- Recurring payment and prepaid fully or partially approved transactions.
- Purchases made with major travel and entertainment (T&E) cards.
- Visa and Plus ATM transactions, which, where available, support purchasing products such as stamps, lift tickets, and coupons.
- Transactions supporting regional cardholder incentive rewards programs.
- Purchase and cash transactions made with private-label and proprietary cards.

(VisaNet's basic authorization, clearing, and settlement services process [above] transactions.)

1.1.1 Basic Services Defined

Visa defines basic services as:

- *Authorization* is approving or declining a sales transaction before a purchase is finalized or cash is disbursed. Issuers (or third-party processors acting on their behalf), or VisaNet, when standing in for issuers, perform authorization.
- *Clearing* is collecting transactions from acquirers and delivering them to issuers for posting to cardholders' accounts.
- *Settlement* is calculating and determining each client's net financial position for all transactions cleared by VisaNet, and exchanging funds.

VisaNet authorizes, clears, and settles transactions as dual- or single-message transactions.

- Acquirers send *dual-message transactions* twice, first with only information needed for an authorization decision, and later with additional information for clearing and settlement. Typically, VisaNet performs authorization online and clearing and settlement offline.
- Acquirers send *single-message transactions* once for authorization, but they contain authorization *and* clearing and settlement information. Also called *full-financial* transactions. they typically occur online, while settlement occurs offline.

VisaNet can also process single-message transactions using online *deferred clearing*: VisaNet authorizes transactions online, and clears and settles them later offline.

Merchants and acquirers can use deferred clearing when the final purchase amount is *not* known at authorization time, for instance, for transactions submitted by hotels and car rental agencies.

1.2 Visa Products

This section describes the products this book references. (Visa offers other products this manual does not describe and product platforms such as those for ATM or chip cards.)

NOTE

Not all products are available in all regions.

Platforms are system components, including hardware and software programs, system tables, and hardware infrastructure, providing support for a *product*, such as Visa Classic, or a *product program*, such as the Visa and Plus international ATM program.

Visa offers products that access a cardholder's line of credit and checking or savings account:

Consumer Credit Products—Visa offers ways to pay for goods and services. Products service electronic commerce (e-commerce) and card usage at the point of sale (POS) or at automated teller machines (ATMs). Visa consumer credit products are:

- Visa Classic
- Visa Gold
- Visa Platinum
- Visa Signature
- Visa Signature Preferred
- Visa Infinite
- Smart Visa

- Co-Branded and Affinity Cards
- Visa Secured

Consumer Debit Products—Visa consumer debit products let consumers pay for goods and services without having to carry cash, checks, or credit cards. Visa debit cards are:

- Visa Classic
- Visa Electron
- Visa Flag
- Visa Gold
- Visa Platinum
- V PAY
- Interlink
- Plus

Commercial Solutions—Visa commercial solutions enable businesses to purchase goods and services and track expenses. Visa business cards serve small businesses with up to USD\$25 million in annual revenues and with fewer than 100 employees. Visa's commercial payment cards are:

- Visa Commercial
- Visa Corporate
- Visa Purchasing
- Visa Fleet

Business Suite Products—Visa has payment products that help entrepreneurs run businesses. Visa business cards are:

- Visa Business Credit Card
- Visa Business Check Card
- Smart Visa Business Card
- Visa Business Line of Credit Card

Debit and Prepaid Cards—Visa consumer debit and prepaid products enable consumers to purchase goods and services without having to carry cash, checks, or credit cards. Visa debit and prepaid cards are:

- Visa Payroll Card
- Visa Healthcare Reimbursement Card
- Visa Gift Card
- Visa Buxx

Cash Disbursement Cards—In addition to VisaNet, Visa operates an ATM platform for Visa ATM and Plus, giving Visa cardholders access to cash and account information nationwide. Visa also operates the Visa PIN-based POS network, *Interlink*, which enables customers to use ATM cards at merchants for purchases and cash.

1.2.1 Comparison of Visa Products

Table 1-1 Comparison of Visa Products

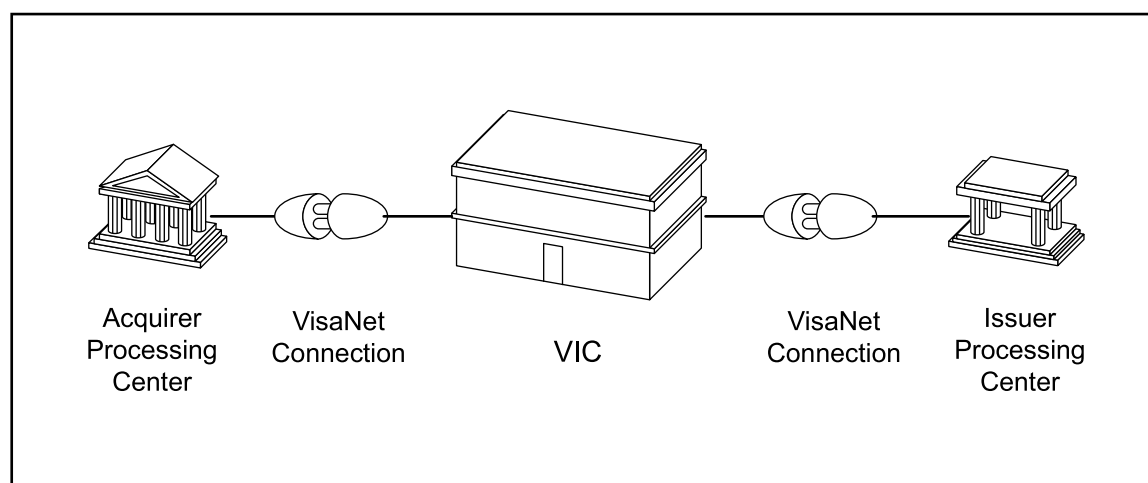
Visa Product	Type of Processing	Cardholder Identification	Acceptance Environment
Visa Debit	Dual- or single-message	<ul style="list-style-type: none"> Usually signature for POS transactions, but PIN can be accepted PIN for ATM transactions 	<ul style="list-style-type: none"> ATM POS
Visa Electron	Dual- or single-message	<ul style="list-style-type: none"> Usually signature for POS transactions, but PIN can be accepted PIN for ATM transactions 	<ul style="list-style-type: none"> ATM POS
Visa Interlink	Single-message	PIN	POS
Plus	Dual- or single-message	PIN	ATM

1.3 VisaNet Components

VisaNet's chief components are:

- VisaNet Interchange Centers (VICs).
- VisaNet connection methods: the Direct Exchange (DEX)[®] Network and Visa Extended Access Servers (EA Servers).
- Acquirers and issuers, including processing centers.

Figure 1-1 VisaNet Communications Network



VisaNet Interchange Centers (VICs)—VICs are Visa data processing centers. Each VIC houses systems performing VisaNet transaction processing. VICs serve as control points for telecommunications facilities of VisaNet.

VisaNet Connection Methods—Visa provides methods for connecting to VisaNet. Connection methods provide interfaces between systems at the VIC and processing centers' host computers. Connection methods connect clients to the BASE I and BASE II dual-message systems, SMS, or all three. Connection methods are:

- Visa Extended Access Servers (EA Servers)

EA Servers sit at participating endpoint sites. The servers perform authorization routing, file staging, delivery services, and secure connectivity to VisaNet.

EA Servers' modular interface adapts to front-end systems and integrates standard, off-the-shelf components clients and processors can scale to meet service needs.

- The Direct Exchange (DEX) Network

Visa Direct Exchange (DEX) provides clients one, secure, and extensible connection into VisaNet for message processing and file delivery services.

DEX has three components:

- The DEX Network uses two circuits and two carriers to ensure availability; both are configured to handle 100% of the endpoints' projected transaction volume. If one circuit experiences problems, the network switches all traffic to the other circuit or carrier without degrading service or interrupting processing.
- The *Visa Message Gateway (VMG)* accepts and routes authorizations for all card and transaction types. VisaNet routes all non-Visa transactions to the card association or gateway for processing. Endpoints must support only one message format; VisaNet provides message translation where necessary.
- The *Open File Delivery (OFD) Service* handles report and file delivery, including the delivery of Automated Clearing House (ACH) data, BASE II data, and various SMS reports and raw data. The OFD Service sends batch files to Visa applications and other DEX endpoints. Endpoints can transfer proprietary payment-related data to another DEX endpoint and to Visa core and non-core applications, such as BASE II, SMS, Visa Resolve Online (VROL), and Visa Account Updater (VAU).

NOTE

Clients in the U.S. region connect through DEX. Clients in all other Visa regions connect through DEX or EA Servers.

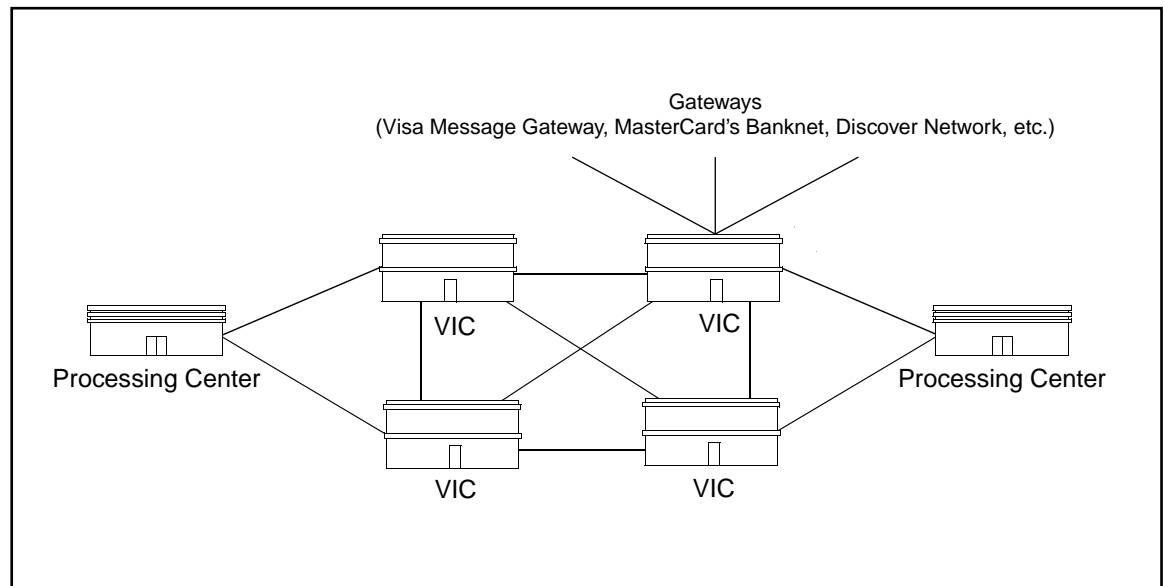
Clients choose options for receiving reports and raw data and routing files. Options vary regionally.

Processing Center—A *processing center*, or *processor*, is a data processing facility operated or designated by an issuer or acquirer. Processing centers house card processing systems supporting merchant and business locations and maintaining cardholder data and billing systems.

Each processing center communicating with VisaNet is linked to two VICs. Centers connect to the closest, or primary, VIC. If one VIC experiences system interruptions, VisaNet automatically routes clients' transactions to a secondary VIC, ensuring continuity of service.

Each VIC is also linked to all other VICs. These links enable processing centers to communicate with each other through multiple VICs. (Processing centers can also access networks of other card programs through VICs.)

Figure 1-2 VisaNet Communications Network Flows



VisaNet operates 24 hours a day throughout the year.

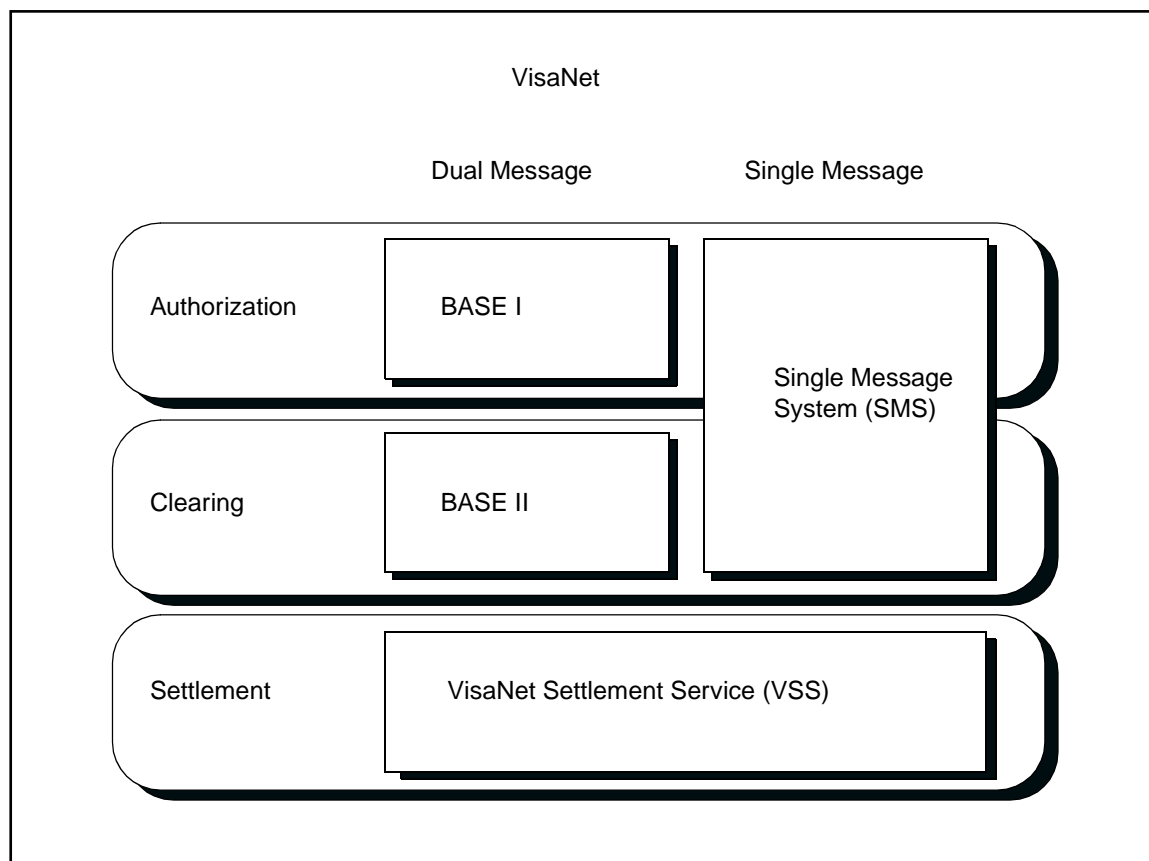
- VisaNet backs up VisaNet connection methods.
- VisaNet backs up the V.I.P. lines from the connection methods to the VICs.
- VICs back up each other.

VisaNet ensures its links have multiple back-ups. The connection from one point in the network to another is not usually a fixed link; instead, VisaNet chooses the best possible path at time of transmission. Rerouting around failed lines occurs automatically.

1.4 VisaNet Systems

VICs house systems performing authorization, clearing, and settlement:

- The VisaNet Integrated Payment (V.I.P.) System, which includes the BASE I System and the Single Message System (SMS)
- The BASE II System
- The VisaNet Settlement Service (VSS)

Figure 1-3 VisaNet Systems and Transaction Processing

1.4.1 VisaNet Integrated Payment (V.I.P.) System

V.I.P. is the primary transaction routing (switching) and processing system for online authorization and financial requests entering VisaNet.

V.I.P. has one system supporting *dual-message processing* (clients request transaction authorization in a first message, and financial clearing information in a second message), and another system supporting *single-message processing* (processing interchange card transactions containing authorization and clearing information in one message). Settlement occurs separately.

1.4.2 BASE I System

BASE I is the system processing authorization-only requests online. *Authorization request messages* are the first sent in dual-message processing; *BASE II clearing messages* are the second.

BASE I supports online and offline functions and BASE I files, including internal system tables and the Merchant Central File (MCF).

BASE I Online Functions—Support dual-message authorization processing and include routing, cardholder and card verification, stand-in processing (STIP), Card Verification Value (CVV) validation, PIN verification, and file maintenance.

A bridge from BASE I to SMS enables BASE I clients to communicate with SMS clients and access SMS gateways to outside networks.

BASE I Offline Functions—Include reporting and generating Visa Card Recovery Bulletins. BASE I reporting includes authorization, Exception File, Advice File, and POS reports.

1.4.3 Single Message System (SMS)

SMS processes *full-financial transactions* containing authorization *and* clearing information. Because one message contains both, this is called *single-message processing*. SMS also supports *dual-message processing* (participants submit authorization requests first, then clearing and settlement in financial request messages), communicating with BASE I and accessing outside networks to complete processing. **Only** SMS performs single-message processing.

A bridge from SMS to BASE I lets SMS users communicate with BASE I users and access BASE I gateways to outside networks.

SMS supports online and offline functions and SMS internal system tables controlling access and processing. SMS supports the Merchant Central File for U.S.-region clients.

SMS Online Functions—Perform real-time cardholder transaction and exception processing, supporting authorization *and* full-financial transactions and transaction delivery to BASE II for clients using dual-message processing.

SMS accumulates reconciliation totals, performs activity reporting, and passes activity data to VisaNet, which supports settlement and funds transfer processing for SMS. VisaNet handles settlement and funds transfer as follow-up to SMS transaction processing. The *VisaNet Settlement Service (VSS)* performs settlement and delivers results through advices and reports.

BASE I and SMS use client-supplied cardholder data and parameters to perform online processing. They interact with offline systems, including BASE II and exception processing systems.

SMS processes Visa, Plus, Interlink, and other card transactions.

Issuers can have SMS, or BASE I, BASE II, and SMS, process transactions. Issuers can use different processing methods for different Visa products.

SMS Offline Functions—Process settlement and funds transfer requests and provide settlement and activity reporting. (SMS clients can also receive BASE I reports.) Offline systems support a bridge to and from BASE II for Visa and Plus clearing transactions VisaNet sends between SMS clients and BASE II clients.

NOTE

SMS access methods use V.I.P. International Organization for Standardization (ISO) message format and observe all rules for its use.

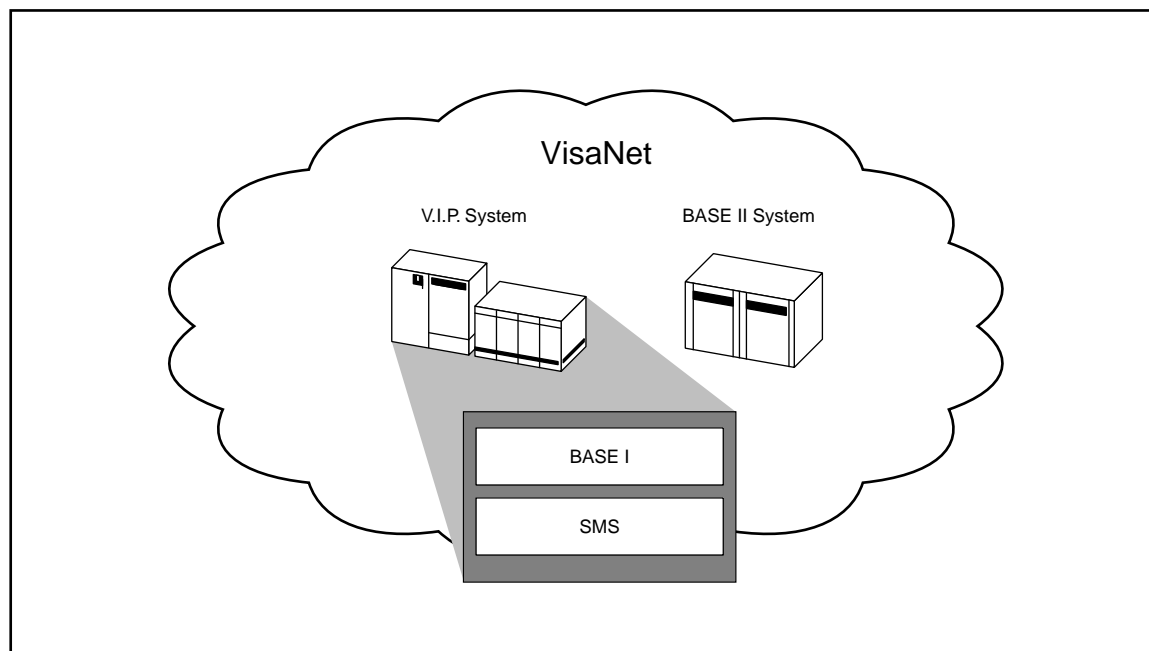
1.4.4 BASE II System

BASE II is an international electronic batch transaction clearing system facilitating interchange data exchange between acquirers and issuers and calculating interchange fees.

BASE II performs the second part of dual-message processing. Through BASE I or SMS connections, clients submit authorization messages, which V.I.P. clears through VisaNet connections to BASE II. A bridge to V.I.P. permits interchange between BASE II centers and SMS centers.

BASE II passes message data to VSS, which settles with issuers and acquirers.

Figure 1-4 VisaNet Software System Components



Clients and processors using BASE I and BASE II can use SMS to process transactions or use different processing methods for transaction types.

EXAMPLE

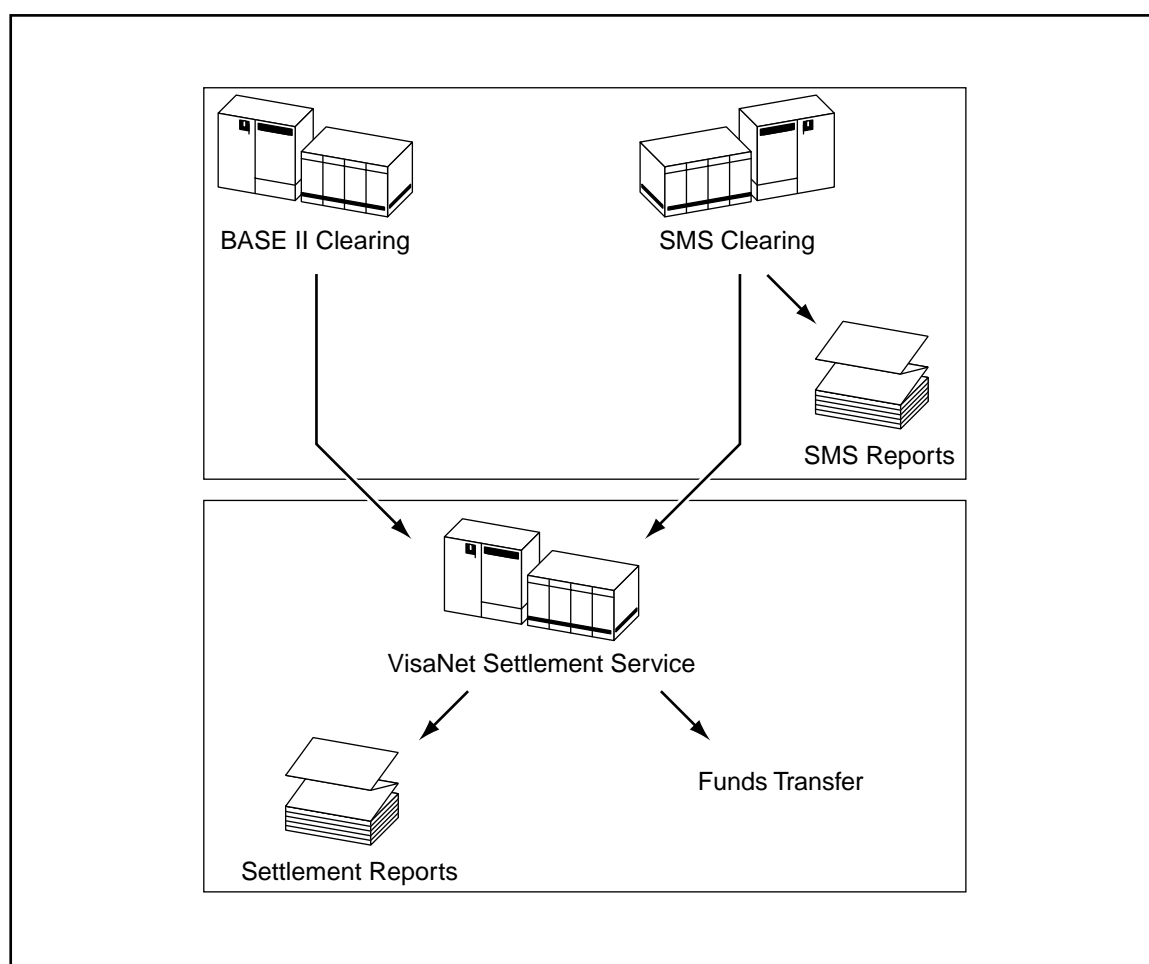
Issuers can use BASE I and BASE II for POS and use SMS for ATM.

1.4.5 VisaNet Settlement Service (VSS)

VisaNet processes interchange transactions for SMS and BASE II through separate systems. SMS and BASE II perform their own clearing functions. *Clearing* is collecting transactions from clients or processors and delivering them to other clients or processors. Clearing includes *valuation*, calculating fees and charges. Once systems clear transactions, they are ready for settlement. *Settlement* is calculating and determining clients' net financial positions for transactions cleared by VisaNet, and funds exchange.

VSS consolidates SMS and BASE II settlement functions into one service. VisaNet sends settlement information to clients and processors from SMS and BASE II in standardized reports. VSS provides flexibility in defining financial relationships, selecting reports and report destinations, and establishing funds transfer points.

Figure 1-5 VSS Process



1.5 Common Member Interface (CMI) and Interface Methods

The CMI allows clients and centers to use one communications line to send and receive BASE I and SMS messages. Lines from VisaNet connections, or *stations*, to V.I.P. connect at the CMI at VICs.

The CMI processes BASE I *and* SMS messages and routes them to BASE I or SMS destinations and to networks when messages specify networks other than VisaNet (for instance, MasterCard's Banknet).

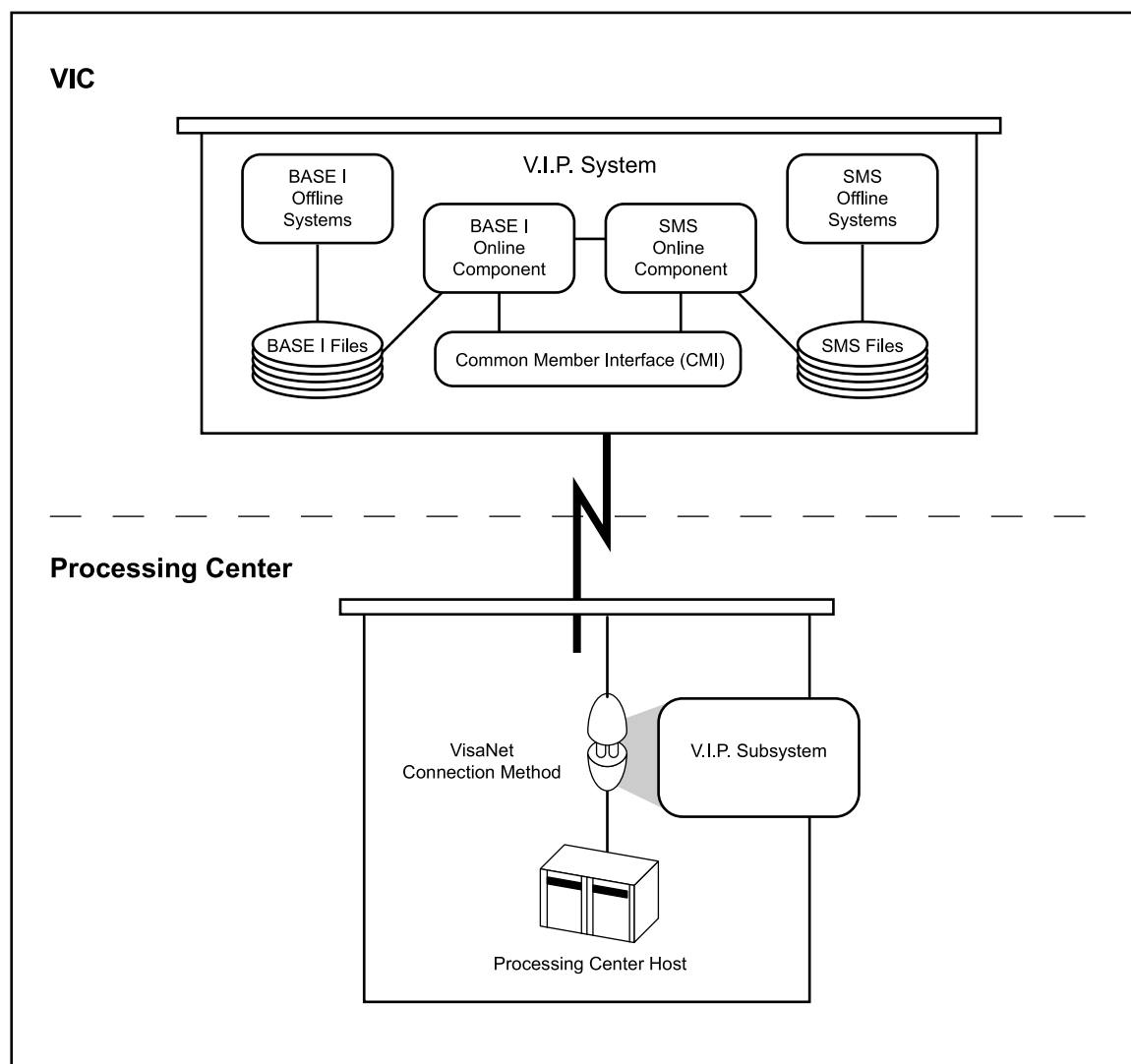
NOTE

Clients establish processing and routing parameters for their stations in system tables through the Customer Online Repository (CORE). Clients contact Visa representatives to establish or change CORE settings.

The CMI accepts messages in all message formats. CMI functions include basic editing and routing.

With the CMI, BASE I centers, including those using BASE I and SMS, can send BASE I messages. SMS centers, including those using SMS and BASE I, can send SMS messages. The CMI chooses system based on request sources, processing requested, and processing networks when messages specify networks.

Besides the CMI, other interface methods are available to clients and processors. These allow users to communicate with *only one* V.I.P. component—BASE I or SMS.

Figure 1-6 V.I.P. System Software at VIC and Processing Center

1.6 Processing Parameters

Users control processing primarily by selecting options and establishing limits and parameters. V.I.P. executes most functions according to parameters users select. Most V.I.P. services offer options for implementation and operation.

Some services allow users to choose options by *BIN* (a card number range for a card program). Other options apply to messages processed by a processing center. Additional options enable individual stations at centers to handle certain transaction types. V.I.P. also enables issuers in Visa Canada and the U.S. region to link incentive and rewards programs with consumer card products at the card-account level.

V.I.P. maintains records of routing and processing rules applying to BINs, processing centers, and stations. V.I.P. stores parameters in *system tables* (or *system globals* or *system files*). Typically, multiple BINs point to one center.

V.I.P. keeps records of:

- Issuers to account numbers
- Issuers and acquirers to centers
- Centers to VICs
- Centers to network stations

Users report changes in account number ranges or center designations to Visa.

1.7 System Messages

Information passes between clients and V.I.P. as BASE I and SMS messages. These are Visa variations of the International Organization for Standardization (ISO) 8583 message, the international financial message format standard. Messages include:

- Bitmaps specifying data fields in messages.
- Message type identifier.
- Fields VisaNet needs for intended functions.

NOTE

*V.I.P. assigns a transaction identifier (TID) to **all** POS and ATM dual- and single-message transactions, including preauthorizations, Plus transactions, and fee collection and funds disbursement messages.*

V.I.P. checks messages for validity and edits them. The CMI performs message format conversion.

Maintaining message *integrity*—correctness and completeness—is critical to V.I.P. processing. Message integrity assures participants follow Visa processing rules and act on messages or transactions as defined in *Visa Core Rules and Visa Product and Service Rules*. For instance, V.I.P. preserves message integrity by evaluating message:

- Duplicates
- Sequence
- Consistency

V.I.P. identifies key data tracing elements to maintain message integrity:

- Acquiring institution ID
- Card acceptor identification code
- Card acceptor terminal identification
- Network identification code
- Original data elements (including original message type identifier)
- Retrieval reference number
- System audit trace number
- Transaction identifier (TID)

All participants keep track of incoming and outgoing messages.

THIS PAGE INTENTIONALLY LEFT BLANK.

System Transaction Processing

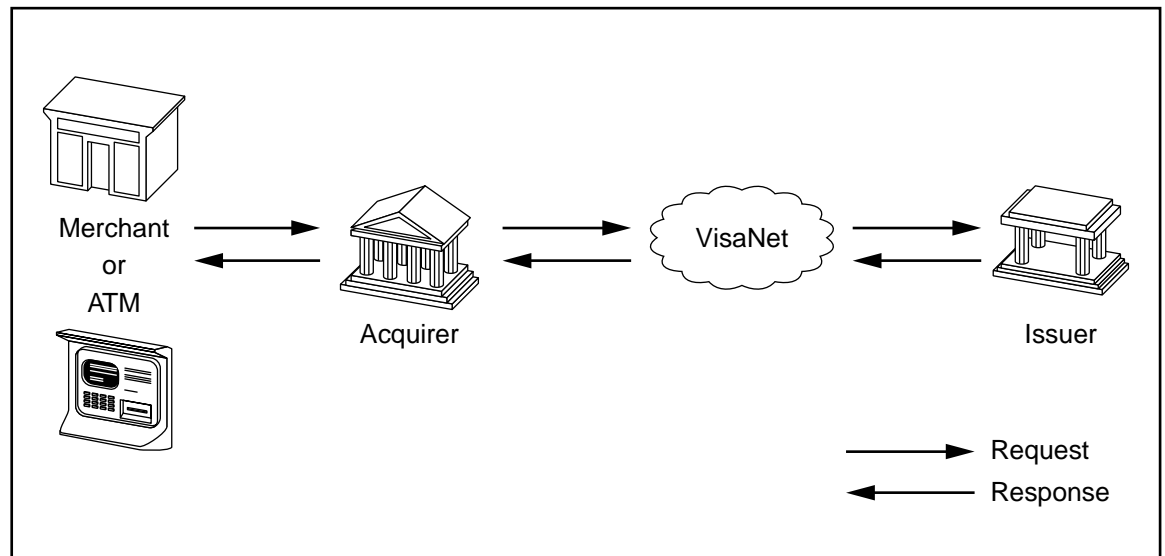
2

This chapter describes transaction flows, V.I.P. message format and structure, and V.I.P. message processing, including stand-in processing (STIP) and routing. It also describes managing system tables and databases, and reporting.

2.1 Transaction Flow

The transaction flow between an acquirer and issuer for a purchase at a merchant location varies depending on the complexity of the transaction and the processing services used.

Figure 2-1 VisaNet Basic Process Flow



1. A cardholder, merchant, or clerk inserts a card into an ATM, or swipes it (or keys it in) at a POS terminal. Cardholders can also initiate POS transactions using *contactless* technology (the card transfers cardholder data to the terminal without physical contact). The terminal prompts the cardholder for a PIN, if applicable.
2. The merchant creates a financial request message and forwards it to the acquirer. The request includes the transaction type, merchant name, encrypted PIN, and transaction amount.
3. The acquirer logs the request, excluding the PIN information, and forwards the message to VisaNet.
4. V.I.P. prepares and logs the transaction, performs currency conversion if requested, and routes the message to the issuer. V.I.P. bases the routing decision on the card number

and other transaction field values, and on routing options selected by the acquirer and issuer. V.I.P. may route the transaction to its stand-in processor (STIP) instead of to the issuer for processing, depending on issuer and Visa options for processing in issuer-available and issuer-unavailable conditions.

5. The issuer or STIP verifies the PIN, checks the transaction amount against the account's available balance or open-to-buy balance, and checks daily activity limits and other controls. The issuer logs the transaction and, for approved transactions, places a hold on the funds or reduces the cardholder's available balance by the amount of the transaction. The issuer creates an authorization or financial response message based on the results of these edits and sends it to VisaNet.
6. V.I.P. processes the message response, logs it, and forwards the response to the acquirer.
7. The acquirer logs the financial response and forwards it to the merchant to complete the transaction. The acquirer ensures it delivers the response successfully. If the cardholder did not enter a PIN earlier, the transaction requires the cardholder's signature.

2.2 Message Processing

When V.I.P. receives a message, it performs:

- Message validation and preparation.
- Message routing.
- Stand-in processing (STIP), as required.
- Response processing and logging.

2.3 Message Validation and Preparation

V.I.P. checks the format and content of messages it receives and matches messages within a transaction.

2.3.1 Message Format

Issuers and acquirers format messages according to Visa standards. Visa bases the V.I.P. message format and content on International Organization for Standardization (ISO) 8583 requirements.

BASE I and SMS clients support the V.I.P. message format. The V.I.P. format enables clients to use both processing systems for their transactions and provides enhanced processing capabilities.

2.3.2 Message Structure

V.I.P. messages contain bitmaps so they transmit *only* required data.

Table 2-1 Message Structure

Message Header	Message Type Identifier	Bitmaps	Data Fields
----------------	-------------------------	---------	-------------

Message Header—Contains message identifiers, routing information, and processing control codes and flags.

Message Type Identifier—Specifies the message class and category of function. For instance, *0100* indicates an authorization request. All messages contain a message type identifier.

Bitmaps (one or more)—Specify which data fields are in a message. In addition to a primary bitmap, messages can include second and third bitmaps. Each map contains 64-bit fields, corresponding to the number of possible fields in a message bitmap.

Data Fields—Contain information needed to process a message.

2.3.3 Message Matching

V.I.P. transactions generally consist of *pairs* of messages: a request message followed by a response message. V.I.P. compares information in key data fields to match messages within a transaction. Messages comprising a transaction are called a *message set*.

V.I.P. message matching enables the acquirer, issuer, and V.I.P. to link messages and control real-time account posting and settlement accumulator updating. For a cardholder transaction, processors must use only the messages allowed in the associated transaction set. V.I.P. uses message matching to prevent invalid messages within a transaction and ensure transaction integrity.

2.3.4 Validation and Preparation Requirements

Messages must comply with V.I.P. requirements for the message type. Also, processing stations must use V.I.P. format specifications.

Messages must comply with V.I.P. message format specifications. If they do not, V.I.P. returns them to the sender with a reject code indicating why it rejected it.

V.I.P. performs edits and adds processing elements. V.I.P. also performs client- or Visa-designated functions such as:

- Message enhancement
- Chip authentication
- PIN verification
- PIN translation
- Card Verification Value (CVV), Card Verification Value 2 (CVV2), Integrated Circuit Card CVV (iCVV), and Dynamic CVV (dCVV) verification
- Cardholder Authentication Verification Value (CAVV) verification
- Currency conversion
- Reimbursement program screening

Once V.I.P. validates a message, it is ready for routing.

2.4 Message Routing Basics

Routing is sending messages between VisaNet and acquirer and issuer centers *and* switching messages to V.I.P. stand-in processing (STIP) for authorization on issuers' behalf.

2.4.1 Routing Messages

To route messages, V.I.P. uses client-supplied information in system tables and message headers, message type identifiers, and data fields. V.I.P. compares message information to *BINs* (card number ranges for card products, such as Visa Classic) and center information in system tables, including:

- Account number.
- Card type.
- Source address.
- Destination address.

Visa assumes responsibility for routing requests to destinations. Acquirers do not have to determine destinations because V.I.P. routes requests based on account numbers.

NOTE

In some cases, V.I.P. uses data other than account numbers to determine routing. For instance, for SMS transactions, V.I.P. also uses values in the network ID field.

Issuers designate which issuer center should receive requests through:

- Associating issuer BINs with issuer centers, **or**
- Designating multiple centers and specifying transaction types VisaNet routes to them.

2.4.1.1 Routing Tables

V.I.P. provides routing table services for acquirers. *Routing tables*, or *BIN tables* or *account range tables*, are batch data files listing card prefixes, prefix lengths, and account number lengths. They contain records of relationships of issuers to account numbers, issuers and acquirers to centers, centers to VICs, and centers to stations. They help V.I.P. and acquirers make authorization routing decisions.

Routing files are:

- ATM Routing
- Consolidated Routing
- Interlink and Visa Routing
- PIN at Point-of-Sale Routing
- Visa Routing
- POS Debit Device Routing

Entries in Visa BIN routing tables contain digits (up to 12) necessary to identify card ranges or portfolios. Table entries can be BINs (for instance, **412345**), or longer numbers for Plus proprietary programs (for instance, **504667214**).

Clients control routing by establishing relationships among account number ranges, transaction types, and center stations. BASE I and SMS route transactions based on:

- Routing and transit numbers.
- Network IDs.
- Card types.
- Account numbers.
- Account ranges.
- Centers.
- Stations.
- User preferences for priority routing and PIN processing.

Visa requires all Visa and Plus acquirers to use routing tables. Visa requires all Visa POS acquirers in the U.S. region to use the POS Debit Device routing table. See *Visa Core Rules and Visa Product and Service Rules*. Clients contact their Visa representatives for tables.

2.4.1.2 Internal Routing Services

In addition to basic routing, Visa provides services enabling clients to specify alternate routing for transactions with specified characteristics. Most are optional.

EXAMPLE

Issuers can designate an alternate path for routing certain transactions. They can route ATM transactions differently from POS transactions; route transactions containing PINs differently from non-PIN transactions; exception transactions differently from authorization and financial transactions.

Additionally, V.I.P. can route transactions according to client specifications using services that route low-risk transactions to STIP:

- The Positive Cardholder Authorization Service (PCAS) uses PCAS-established issuer, advice, and activity limits to determine whether to route transactions to issuers or STIP.
- The Positive Authorization Capacity Management (PACM) Service routes transactions to issuers or STIP by using issuer limits and a dynamic limit called the *diversion threshold*. STIP determines this by comparing transaction volume to issuer capacity.

2.4.1.3 Gateways to Non-VisaNet Destinations

If destinations are systems or networks outside VisaNet, V.I.P. uses Gateway Services to reformat and deliver messages. BASE I and SMS have connections, or *gateways*, to outside systems and networks. Gateway Services route transactions through gateways and return messages to clients using the same connections.

See Part 2 of *V.I.P. System Services, Volume 1*.

2.5 Stand-In Processing (STIP)

V.I.P. acts as a back-up processor when issuers request it or are unavailable. During this back-up processing, V.I.P. authorizes, declines, or refers transactions on issuers' behalf. This is called *stand-in processing (STIP)*.

Issuers specify the STIP parameters V.I.P. uses. Visa card issuers can maintain cardholder data at VICs and select limits controlling which transactions STIP can approve. Other card programs processed according to the Visa Rules are eligible for STIP at issuers' discretion.

Whether V.I.P. routes transactions to issuers or STIP for approval depends on:

- Issuer availability when the transactions are processed.
- Issuer-specified processing parameters.
- Visa-mandated conditions for transaction types.

If account and transaction conditions require issuers, rather than STIP, to make final authorization decisions, STIP forwards requests to issuers if they are available; if they are not, STIP processes transactions according to issuer-unavailable parameters.

V.I.P. usually creates advices for issuers of STIP actions. Issuers have options for recovering advices.

NOTE

V.I.P. stores SMS advices for 30 days; SMS issuers must retrieve them within this 30-day timeframe.

Visa offers issuers optional, issuer-or-STIP routing services:

- Positive Authorization Capacity Management (PACM) Service—Routes authorization requests to issuers or STIP based on dollar amount thresholds and message traffic volumes.
- Positive Cardholder Authorization Service (PCAS)—Routes authorization requests to issuers or STIP according to risk control parameters that include dollar amount thresholds.

Issuers can include Visa Advanced Authorization (VAA) risk score thresholds in their STIP parameters.

2.5.1 BASE I STIP

BASE I STIP:

- Protects issuers from transaction volumes exceeding their processing capacity.
- Allows issuers to control authorization processing expenses by having STIP approve low-risk, small-ticket transactions.
- Enables issuers to provide a high level of cardholder service during issuer-unavailable conditions while still controlling risk.

The first two functions pertain largely to *issuer-available* STIP; the third applies largely to *issuer-unavailable* STIP. The circumstances and implications between issuer-available and issuer-unavailable processing drive rules for how V.I.P. processes transactions.

When transactions fail issuer-available STIP processing, V.I.P. typically (at the issuers' option) "forward-refers" them to issuers for authorization decisions. STIP forward-refers transactions having elevated risk to issuers and approves transactions within issuer-unavailable risk parameters. This minimizes false declines (declining a "good" cardholder because of transaction characteristics or cardholder spending indicating heightened risk).

When issuers are unavailable, STIP *cannot* forward-refer transactions; instead, it generates responses for acquirers. This elevates customer service risk. Thus, for issuer-unavailable processing, issuers can choose to relax cardholder spending-related risk controls for increased customer service levels.

To identify elevated risk, BASE I STIP:

- Checks CVV or iCVV, CAVV, dCVV, PIN, expiration date, and Exception File.
- Validates account number with Luhn modulus-10 algorithm.
- Checks cardholder spending and activity and transaction amount.

BASE I STIP gives issuers options to determine functions V.I.P. is to perform and how V.I.P. should use them.

2.5.2 SMS STIP

SMS STIP protects issuer processing capacities and allows issuers to maintain high levels of cardholder service during issuer-unavailable conditions. Risk control options include:

- Establishing transaction activity limits for card ranges and individual cardholders.
- Checking Exception File for positive account limits (for instance, generous limits for **VIP** [Very Important Person] accounts) or negative account controls (for instance, card pick-up).

- Checking CVVs on cards' magnetic stripes, CVVs or iCVVs on cards' chip images, CAVVs, or dCVVs.
- Checking PINs and monitoring PIN-entry attempts.
- Validating account numbers with Luhn modulus-10 algorithm.
- Checking card expiration dates.

SMS STIP also handles issuer-generated messages including chargebacks, fee collections and funds disbursements, and text messages for unavailable acquirers.

2.6 Response Processing

V.I.P. processes responses it receives from issuer centers before it forwards them to acquirer processing centers. V.I.P.:

- Checks the format and content of responses.
- Adds a code to indicate the response came from the issuer rather than STIP.
- Drops the CVV- or iCVV-check result code from messages if it is present.

All responses STIP processes also contain the code specifying the source of the response. The code indicates why STIP processed the request.

When V.I.P. sends a request to an issuer center, it keeps a copy of the message and waits the allowable period of time governed by the *Visa Core Rules and Visa Product and Service Rules* for a response. If there is no response from the issuer by that time, V.I.P. discards the message and does not send a response to the acquirer.

The *Assured Transaction Response (ATR)* ensures that issuers or STIP return timely responses to all requests for authorization and reversals of Visa card transactions, and for other card transactions. This function is optional for issuers.

With ATR, when V.I.P. sends a request to an issuer center, it keeps a copy of the message and sets a timer. If the issuer processing center does not respond within a specified number of seconds, V.I.P. reroutes the request to STIP.

2.7 Logging

After V.I.P. validates the message source, it logs the request. V.I.P. logs each request and response message, along with certain system-processing information, in a system log it uses to prepare reports, research problems, and perform billing functions.

2.8 Additional System Functions

In addition to message processing, V.I.P. performs additional functions to support clients, V.I.P., and VisaNet.

2.8.1 Managing the Network

V.I.P. supports network management messages controlling centers' access to the system. They enable centers to:

- Sign on to and off from the system.
- Respond to test messages.
- Monitor response time and connectivity.
- Request advices, and optionally, accelerate advice delivery.

V.I.P. also creates administrative messages to alert center stations to abnormal system conditions. Administrative messages require the attention of center staff, who should route them to a console or terminal for immediate review.

2.8.2 Managing System Tables

V.I.P. maintains records of client- and Visa-established routing and processing rules applying to BINs, processing centers, and stations. V.I.P. stores these parameters in the system tables.

Visa maintains system tables. BASE I and SMS use them for processing. Tables contain:

- System parameters
- Lists of BINs
- Card number ranges
- Center-selected processing parameters
- Client-selected processing parameters such as those issuers specify for STIP
- Station-specific parameters such as types of messages processed (BASE I, SMS, or both)

2.8.3 Managing System Databases

Clients supply cardholder and merchant information to V.I.P. for it to use. Clients add, change, and delete it to reflect business changes.

Clients report changes in account number ranges or processing center designations to Visa. This is vital to the correct routing of messages. Clients can update the files they maintain and request data from records in those files. Depending on services clients select, V.I.P. can also update information in database files automatically at the time of the transaction.

System databases include:

- The Cardholder Database (CDB)
- The Merchant Central File (MCF)

Issuer centers can update the Cardholder Database files with online messages, the Visa Open File Delivery (OFD) Option (available for clients connected to VisaNet with Direct Exchange [DEX]), Visa Resolve Online (VROL), or batch updates.

Issuers can also call the Global Customer Assistance Service (GCAS) with requests for urgent updates.

Issuer and acquirer centers can update the MCF using online file update messages for individual updates or submitting batch files.

NOTE

Issuers coordinate batch updates with their account managers.

2.8.3.1 Cardholder Database Files

The *Cardholder Database (CDB)* resides at each VIC and contains files maintained by Visa, issuers, or both. The CDB contains cardholder information STIP uses to authorize transactions and verify accounts, addresses, and PINs.

The database also contains Positive Cardholder Authorization Service (PCAS) limits for individual cardholders.

While card issuers are responsible for creating and maintaining several of the CDB files, Visa is responsible for the integrity of these, and all V.I.P. system, files.

The CDB contains:

Activity File—This Visa-generated file contains accumulated counts and amounts of VisaNet-approved transactions and can include accumulated totals of issuer-approved transactions and the count of consecutive invalid PIN-entry attempts STIP accumulates.

Address Verification File—This issuer-created and -maintained file contains cardholder billing address data.

Exception File—This issuer-created and -maintained file contains positive and negative action codes and special instructions for the listed cardholder's account; for instance, it might note STIP must decline all transactions for an account. VisaNet uses the file to create Cardholder Recovery Bulletins (CRBs). See *V.I.P. System Services, Volume 1*.

Certain Visa services, such as the Automatic Cardholder Database Update (Auto-CDB) Service, add and update records in the Exception File to ensure they include accounts in CRB listings.

PIN Verification File—The optional PIN Verification Service (PVS) uses this issuer-created and -maintained file. It contains Visa PIN Verification Values (PVVs) and PIN Verification Key Indexes (PVKIs) for issuers using the Visa PVV method of PIN verification. See *V.I.P. System Services, Volume 2*.

Portfolio File—The optional Preauthorized Payment Cancellation Service (PPCS) uses this issuer-created and -maintained file. It contains issuer-supplied stop payment commands for recurring payment transactions. See *V.I.P. System Services, Volume 2*.

Risk-Level File—Issuers use this issuer-created and -maintained file to assign cardholder's risk levels and merchant group daily activity limits. See *V.I.P. System Services, Volume 1*.

Cardholder Maintenance File—Contains Merchant Marketing Program (MMP) records the offline Visa Incentive Network (VIN) sends to the CDB. The MMP enables issuers in Visa Canada and the U.S. region to link incentive and rewards programs with consumer card products at the card level. Each record includes the card number, product type, and program ID.

2.8.3.2 Merchant Central File (MCF)

The MCF is created and maintained by acquirers. The optional Merchant Central File Service (MCFS) uses data in the MCF when acquirers want V.I.P. to insert more information in their authorization requests (for instance, when they cannot supply merchant category codes). MCF information overrides whatever information is in the request when V.I.P. receives it. The MCF includes:

- Merchant names, cities, country codes, and category codes for Visa and MasterCard transactions.
- ZIP and postal codes for MasterCard transactions.
- Terminal identifiers for American Express and Discover transactions.

2.8.4 Reporting

V.I.P. reporting components generate various reports available by subscription. They document V.I.P. processing activity and include information about listings in the

Exception and Advice files. V.I.P. also produces POS and downgraded transaction reports, which provide individual transaction and summary information for acquirers.

Issuers and acquirers can subscribe to certain reports in raw data format. Clients can format them to customize and analyze their data.

2.8.4.1 BASE I Reports

The authorization component of V.I.P. produces reports.

- Authorization Profile Reports (APRs).
- Cardholder Database.
- Custom Payment Service (CPS).
- Visa Point-of-Sale (POS) (international only).

They are available to SMS users by subscription. APRs and POS reports are available in raw data format.

2.8.4.2 SMS Reports and Raw Data

SMS produces reports.

- Transaction Detail.
- Exception Detail.
- Maintenance.
- Reconciliation.
- Error.

SMS participants can receive raw data records detailing client transaction activity for the processing day.

2.8.4.3 Settlement Reports

Clients can receive settlement reports.

- VisaNet Settlement Service (VSS).
- International Settlement Service.
- National Net Settlement Service (NNSS).

2.8.5 Billing

Visa assesses the fees and charges for V.I.P. processing on a monthly basis. V.I.P. produces printed invoices providing the line-item detail of costs for accessing the system, routing and processing messages, maintaining files, and creating reports. At the client's request, V.I.P. prepares invoices for individual BINs or processing centers.

System Services

3

V.I.P. offers services beyond its basic functionality. Some services are mandatory for all clients or those in specific Visa regions, but most are optional. Clients can subscribe to optional V.I.P. services anytime.

Service enrollment differs for each region. Before service implementation, each client must test its systems and, in many cases, test with Visa to implement the service. Visa representatives can explain the regional requirements and enrollment specifics.

3.1 Service Functional Groups

Table 3-1 Services by Functional Group

Functional Group	Services
Routing	ATM/POS Split Routing Service Check Acceptance Service Gateway Services PIN Debit Gateway Service (PDGS) PIN/No-PIN Split Routing Service Priority Routing Service Visa Shortest Online Path (VSOP) Service
Risk Management	Card Recovery Bulletin (CRB) Service Fraud Reporting System (FRS) Merchant Fraud Performance Program Visa Intelligent Scoring of Risk (VISOR)
Visa Secure Electronic Commerce (VSEC)	Visa Secure Electronic Commerce (VSEC) With Verified by Visa (3-D Secure)
Chip Card	Visa Contactless Payment Service (VCPS) Visa Smart Debit/Smart Credit (VSDC) Service
Authorization Database	Automatic Cardholder Database Update (Auto-CDB) Service Merchant Central File Service (MCFS)

Table 3-1 Services by Functional Group (continued)

Functional Group	Services
Authorization	Account Verification Service Address Verification Service (AVS) Advice Retrieval Service—BASE I Advice Retrieval Service—SMS ATM Format Conversion Service Card Verification Value (CVV) Service Card Verification Value 2 (CVV2) Service Cardholder Authentication Verification Value (CAVV) Verification Service Custom Payment Service (CPS)/ATM Custom Payment Service (CPS)/POS Deferred Clearing Advice File (DCAF) Service Dynamic Card Verification Value (dCVV) Service Dynamic Key Exchange (DKE) Service Multicurrency Service PIN Verification Service (PVS) POS Check Service Positive Authorization Capacity Management (PACM) Service Positive Cardholder Authorization Service (PCAS) Preauthorized Payment Cancellation Service (PPCS) Status Check Service VisaNet Cashback Service
Additional	Chargeback Reduction Service (CRS) ATM Processing Integration

3.2 Routing Service Definitions

See *V.I.P. System Services, Volume 1* for full descriptions.

3.2.1 ATM/POS Split Routing Service

The *ATM/POS Split Routing Service* enables issuers processing Visa, Visa Electron, and Plus transactions to separate transaction types and accept or route them to or from multiple connections.

ATM/POS Account-Type Split Routing—The ATM/POS Account-Type Split Routing option is available for issuers processing ATM transactions. The POS option supports

POS and multipurpose card transactions for issuers in the AP region *only*. Issuers can specify that VisaNet route ATM transactions based on the account the cardholder selects when using a multipurpose card at ATMs, or POS transactions based on the account the cardholder selects when using a multipurpose card at a POS. Issuers can specify up to three connections: one for deposit accounts, one for credit accounts, and one for universal and non-specified accounts.

Alternate Routing—With the Alternate Routing option, acquirers and issuers can designate one or two alternate processors to handle exception and other back-office transactions. Alternate routing is for SMS users only. The alternate processing center can be connected to SMS or an exception processing system.

Issuers can use these options separately or in combination.

3.2.2 Check Acceptance Service

The *Check Acceptance Service* enables merchants in the U.S. region to route check approval requests through VisaNet to selected check acceptance vendors. Equifax Card Services (TeleCredit Los Angeles and TeleCredit Tampa), ETC Scan (Deluxe Data Systems), JBS/NPC, State Street Bank, or TeleCheck, can approve a check used at a merchant through the Check Acceptance Service. The vendor guarantees acceptance of the check by the drawee bank and assumes responsibility for collection if it is returned.

3.2.3 Gateway Services

Both BASE I and SMS have connections, or *gateways*, to other systems and networks. *Gateway Services* enable acquirers to get authorizations on non-Visa-brand transactions through the same VisaNet access methods for Visa transactions. With Gateway Services, acquirers and merchants can route terminal traffic to VisaNet, which routes non-Visa-brand transactions to networks for responses. The service also enables issuers to use their VisaNet connections to receive requests from other networks or services.

3.2.4 PIN Debit Gateway Service (PDGS)

The *PIN Debit Gateway Service (PDGS)* enables merchants in the U.S. region to accept customer payments made with debit and ATM cards bearing a national or regional debit POS mark. Merchants send transactions initiated with these cards (and accessed with PINs) to VisaNet. SMS routes these transactions through the VisaNet Debit Gateway to the direct-debit POS network for delivery to issuers.

Routing options provide merchants flexibility in accessing the debit POS networks, which route transactions to issuers.

PDGS also supports Electronic Benefits Transfer (EBT). *EBT* is a nationwide program of card-accessed, electronically delivered, government-funded benefits issued through a federal-state partnership. The primary function of EBT is the electronic delivery of food stamps and cash benefits.

3.2.5 PIN/No-PIN Split Routing Service

The *PIN/No-PIN Split Routing Service* allows issuers to separate transactions requiring PIN verification from those that don't and route these transactions to multiple issuer processing centers. It offers:

- The *PIN Routing option* for routing POS financial transactions with PINs to SMS and other transactions to BASE I.
- The *Alternate Routing option* for separating original transactions and exception transactions.

Issuers can use these options individually or in combination.

3.2.6 Priority Routing Service

The *Priority Routing Service* determines destinations of authorization, financial, and reversal requests based on the acquirer's processing order preference. It is available for SMS acquirers.

Acquirers assign processing priorities to each card program. By setting up a preferred processing path, acquirers choose how VisaNet should process a transaction qualifying for multiple programs.

3.2.7 Visa Shortest Online Path (VSOP) Service

The *Visa Shortest Online Path (VSOP) Service* allows non-U.S. issuers issuing Visa and MasterCard card products to get MasterCard authorization requests for purchase and cash transactions acquired through VisaNet. This foregoes the need to route MasterCard requests to *Banknet* (MasterCard's processing network) before they go to issuers.

VSOP operates only when the issuer is available to authorize MasterCard transactions; otherwise, V.I.P. routes the transactions to MasterCard through Gateway Services.

3.3 Routing Service Availability

Table 3-2 Routing Service Availability

Routing Service	AVAILABLE FOR...				
	Acquirer	Issuer	BASE I	SMS	Products
ATM/POS Split Routing Service	✓	✓	✓	✓	Visa Electron, Interlink, Plus, Visa
Check Acceptance Service	✓		✓	✓	Available for checks
Gateway Services	✓		✓	✓	Available for all product types
PIN Debit Gateway Service (PDGS)	✓	✓		✓	Available for all product types
PIN/No-PIN Split Routing Service	✓	✓	✓	✓	Visa Electron, Interlink, Plus, Visa
Priority Routing Service	✓			✓	Visa Electron, Interlink, Plus ATM, Visa
Visa Shortest Online Path (VSOP) Service		✓	✓		MasterCard

3.4 Risk Management Service Definitions

This section describes V.I.P.'s fraud risk reduction services.

3.4.1 Card Recovery Bulletin (CRB) Service

The *CRB Service* is an international risk control service that creates card recovery files containing account numbers of cards reported as lost, stolen, or misused. It also helps control fraud on below-floor-limit transactions outside of the U.S. region.

The CRB Service protects cardholders from fraudulent use of their lost or stolen cards. It supports chargeback rights of issuers, acquirers, merchants, and cardholders.

Issuers can list Visa account numbers in the Exception File, coded to appear in specified pick-up files. Issuers can choose to list an account in multiple individual CRB regions, or in individual regions plus multiple groups of regions. Visa acquirers specify which regional pick-up files go to which merchant locations and which pick-up files they want sent to themselves or their processing centers.

3.4.2 Fraud Reporting System (FRS)

FRS is a V.I.P. service helping clients report, track, and analyze fraudulent transactions. FRS consolidates fraud information, helping clients detect fraud patterns and reduce losses.

3.5 Risk Management Service Availability

Table 3-3 Risk Management Service Availability

Risk Management Service	AVAILABLE FOR...			
	Acquirer	Issuer	BASE I	SMS
Card Recovery Bulletin (CRB) Service	✓	✓	✓	✓
Fraud Reporting System (FRS) ¹	✓	✓		✓

1. FRS is available to BASE I participants through TC 40 BASE II records.

3.6 Visa Secure Electronic Commerce (VSEC) Service Definition

This section describes the VSEC Service provided through V.I.P.

3.6.1 Visa Secure Electronic Commerce (VSEC) With Verified by Visa (3-D Secure)

The *VSEC* initiative provides security for transactions sent over the internet and other open networks. VisaNet authenticates cardholders during online purchases. *3-D Secure* is the *authentication technology*; *Verified by Visa (VbV)* is the *authentication service* available to cardholders.

VbV gives cardholders control over card use for online purchases and provides payment security adding extra protection for consumers and merchants.

VbV enables all parties in an electronic commerce payment transaction to transmit confidential payment data and provides authentication the buyer is an authorized user

of an account. VbV is a global program supporting magnetic stripe Visa cards and Visa Smart Debit/Smart Credit (VSDC) cards.

V.I.P. validates results of authentication during authorization using the Cardholder Authentication Verification Value (CAVV) Verification Service.

3.7 VSEC Service Availability

Table 3-4 VSEC Service Availability

VSEC Service	AVAILABLE FOR...			
	Acquirer	Issuer	BASE I	SMS
Visa Secure Electronic Commerce (VSEC) With Verified by Visa (3-D Secure)	✓	✓	✓	✓

3.8 Chip Card Service Definitions

This section describes chip card services provided through V.I.P.

3.8.1 Visa Contactless Payment Service (VCPS)

VCPS enables cardholders to initiate transactions by holding their cards near a contactless-enabled POS terminal reader. The contactless chip and contactless-compliant POS terminal use radio frequency (RF) technology to communicate. Because cards don't touch terminals, merchants serve customers faster in rapid-transaction business environments such as tollbooths and transit stations.

The RF card and terminal interface technology is part of the *Visa Proximity Payment Initiative*, which comprises card-present interface technologies not requiring physical contact between cards and terminals.

VCPS is available to all Visa clients.

3.8.2 Visa Smart Debit/Smart Credit (VSDC) Service

VSDC incorporates debit and credit functionality into chip cards, using the power of the microchip on one card. VSDC supports Visa, Visa Electron, and Plus card products.

The VSDC baseline product, the *chip card*, provides all debit and credit functions currently available through a magnetic stripe product; it also has features allowing issuers to customize products to accommodate market strategy and customers' needs. Issuers can equip VSDC cards for contactless chip transactions through VCPS.

Whenever cardholders use VSDC cards at chip-capable terminals, the interaction between cards and terminals provides enhanced transaction security and functionality. Based on issuer-selected features, the card and terminal interaction results in a payment transaction similar to that performed with magnetic stripe cards. However, with VSDC, card and terminal interaction offers optional risk control features. Issuers can activate features during card personalization when they put account information on the chip.

3.9 Chip Card Service Availability

Table 3-5 Chip Card Service Availability

Chip Card Service	AVAILABLE FOR...			
	Acquirer	Issuer	BASE I	SMS
Visa Contactless Payment Service (VCPS)	✓	✓	✓	✓
VSDC Service	✓	✓	✓	✓

3.10 Authorization Database Service Definitions

This section describes V.I.P. services clients can use to update information in the two main V.I.P. databases.

3.10.1 Automatic Cardholder Database Update (Auto-CDB) Service

Auto-CDB allows V.I.P. to update the Exception File, contained in the Cardholder Database, when issuers return a pick-up response in authorization response messages.

Auto-CDB helps issuers prevent losses from problem accounts by improving the accuracy of cardholder information available to V.I.P. for stand-in processing.

3.10.2 Merchant Central File Service (MCFS)

MCFS supplies information from the Merchant Central File, a database created and maintained by acquirers.

The *Merchant Central File (MCF)* is a VIC-resident file acquirers use to store authorization and reversal request information not supplied by terminals at the POS because of device limitations.

MCFS adds information from the MCF (if data is available) before V.I.P. forwards the request to issuers or STIP.

3.11 Authorization Database Service Availability

Table 3-6 Authorization Database Service Availability

Authorization Database Service	AVAILABLE FOR...			
	Acquirer	Issuer	BASE I	SMS
Automatic Cardholder Database Update (Auto-CDB) Service		✓	✓	✓
Merchant Central File Service (MCFS)	✓		✓	✓

3.12 Authorization Service Definitions

This section describes V.I.P. authorization services.

3.12.1 Account Verification Service

The *Account Verification Service* enables merchants to request account number verification as an initial check for the estimated purchase amount.

Using an authorization request message, merchants can request:

- Account verification only, to perform an initial check for an estimated purchase amount.
- Account verification and authorization, to request authorization when the transaction takes place at the POS.

The service replaces the process of checking Card Recovery Bulletins (CRBs). Instead of using CRB pick-up files, merchants contact their acquirers to initiate account verification requests.

3.12.2 Address Verification Service (AVS)

AVS is an online Visa service enabling merchants to reduce fraud losses by verifying cardholders' billing addresses for card-not-present (CNP) transactions.

Merchants can use AVS for Visa, MasterCard, American Express, and Discover transactions.

3.12.3 Advice Retrieval Service—BASE I

The *BASE I Advice Retrieval Service* keeps issuers informed of stand-in authorizations, reversals, and Cardholder Database file updates by allowing them to retrieve advice data from the advice file at their VIC.

Each VIC maintains an advice file in which it stores STIP response records. Records contain information from authorization or reversal requests, STIP responses, and reasons why STIP processed the requests.

3.12.4 Advice Retrieval Service—SMS

The *SMS Advice Retrieval Service* keeps issuers informed of stand-in authorizations, reversals, deferred clearing advices, and Exception File updates by allowing them to retrieve advice data from the advice file.

NOTE

V.I.P. stores SMS advices online for 30 days. SMS issuers must retrieve them within this 30-day timeframe.

3.12.5 ATM Format Conversion Service

The *ATM Format Conversion Service* gives Visa and Visa Electron SMS issuers, including those co-branded with Plus, the option to receive eligible ATM transactions from dual-message acquirers as full-financial messages.

NOTE

V.I.P. delivers ATM transactions for proprietary cards with the Plus mark to SMS issuers as full-financial messages regardless of the method VisaNet acquires them.

3.12.6 Card Verification Value (CVV) Service

The *CVV Service* is a POS and ATM risk control service protecting clients from fraud losses from counterfeit Visa cards. The CVV Service allows issuers to detect invalid cards by validating the CVV on the cards' magnetic stripe, and the CVV or Integrated Chip Card card verification value (iCVV) on the chips' magnetic stripe image.

The CVV or iCVV is a unique value calculated from magnetic stripe data using a Data Encryption Standard (DES) algorithm established by Visa. V.I.P. or the issuer can perform CVV or iCVV calculations when issuers *and* acquirers participate in the service and magnetic stripe data is transmitted.

3.12.7 Card Verification Value 2 (CVV2) Service

The *CVV2 Service* is a card verification tool that reduces fraud losses on card-not-present transactions, and in the LAC region, in certain situations when cards are present.

Issuers imprint a 3-digit security number (the CVV2) on the back of Visa cards, in accordance with *Visa Core Rules and Visa Product and Service Rules*. Clients use the CVV2 to validate that a genuine Visa card is present during a transaction. The CVV2 is calculated using a secure cryptographic process and a key known only to the issuer and Visa.

3.12.8 Cardholder Authentication Verification Value (CAVV) Verification Service

The *CAVV Verification Service* verifies that CAVVs submitted by acquirers in Verified by Visa (VbV) authorization messages match CAVVs generated by the Visa or an issuer's Access Control Server (ACS) during authentication.

The CAVV is a cryptographic value issuers generate and send to merchants during the authentication process in VbV transactions.

The CAVV Verification Service is available through VbV to enhance the security and integrity of online purchases made using Visa cards. It allows issuers to register cardholders for the service and authenticate the cardholder as the owner of the card account when an online purchase occurs at a participating merchant location. See "[Visa Secure Electronic Commerce \(VSEC\) With Verified by Visa \(3-D Secure\)](#)."

3.12.9 Custom Payment Service (CPS)/ATM

CPS/ATM is an incentive program giving accurate settlement information, ensuring timely delivery of clearing records by acquirers, and reducing exception item processing by improving transaction integrity and life-cycle control.

CPS/ATM is a set of transaction processing requirements helping clients reduce fraud and exception item processing costs. It supports international ATM transactions with custom rate incentive programs for markets.

3.12.10 Custom Payment Service (CPS)/POS

CPS/POS is a series of payment services customized to serve needs of merchant segments for POS transactions. CPS/POS accommodates merchant procedures and decreases

fraud losses and operating expenses. CPS/POS increases client profitability by reducing operating costs, improving risk management techniques, and increasing revenues through increased card usage.

Participants can process CPS/POS transactions as dual messages through BASE I and BASE II.

3.12.11 Deferred Clearing Advice File (DCAF) Service

The *DCAF Service* allows single-message clients to receive original BASE II deferred clearing advices in bulk file deliveries.

BASE II deferred clearing advices originate from dual-message acquirers *not* generating online clearing messages. Without the DCAF Service, SMS clients receive deferred clearing advices online, one advice per station at a time. Capacity problems can occur due to the volume of deferred clearing advices.

To alleviate capacity and resource contention problems, DCAF allows issuers to get deferred clearing advices in bulk files using network lines separate from online station lines. This reduces issuers' online host and network capacity requirements and helps clients manage large volumes of advices.

3.12.12 Dynamic Card Verification Value (dCVV) Service

The *dCVV* is the card verification scheme for *contactless transactions*. dCVV data resides on Track 1, Track 2, or both, of the magnetic stripe or, in chip cards, in the Track 1 Equivalent Data field, the Track 2 Equivalent Data field, or both, in the chip. A dCVV is generated each time a contactless transaction is initiated; the initiator inserts the value in the magnetic stripe data forwarded to the acquirer, replacing other card verification value data and overriding any CVV2 that might be present.

The dCVV Service is optional; Visa considers it an add-on to the CVV Service; thus, clients must participate in the CVV Service before they can participate in the dCVV Service. dCVV processing options are similar to those for the CVV Service. Although the dCVV Service employs an algorithm different from the one used in CVV and iCVV processing, participation requires no new encryption keys.

3.12.13 Dynamic Key Exchange (DKE) Service

The *DKE Service* is an optional service allowing SMS clients to change Data Encryption Standard (DES) cryptographic keys with VisaNet using online messages.

3.12.14 Multicurrency Service

The *Multicurrency Service* supports authorization, clearing, and settlement processing in selected international currencies. SMS Multicurrency Service participants can participate in the Currency Precision Service (CPS) letting clients define the number of decimal positions in message amount fields rather than relying on the Currency Rate Table minor unit values.

3.12.15 PIN Verification Service (PVS)

PVS provides full-time or stand-in verification of PINs used for Visa and Plus ATM transactions, Visa POS, Visa Electron POS, Interlink POS transactions, and Visa Smart Debit/Smart Credit (VSDC) transactions.

At the issuer's option, V.I.P. can verify PINs for issuers, at all times or when the center is unavailable. When V.I.P. verifies PINs, it intercepts all authorization requests containing PINs, verifies the PINs, and passes the requests to the issuers or to V.I.P. STIP for authorization.

3.12.16 POS Check Service

The *POS Check Service* permits merchants to accept consumer and business checks as source documents and convert them to electronic transactions at the POS, and from mail, telephone, or electronic commerce merchants. Participating drawee financial institutions, serving as online authorizing agents for their customers' checks, can clear and settle electronic debits quickly.

3.12.17 Positive Authorization Capacity Management (PACM) Service

PACM helps issuers maximize their authorization and full financial message processing capacity. It monitors issuers' transaction volume every 60 seconds. When the volume of authorization and financial request messages exceeds issuers' processing capacity, *PACM* routes low-risk transactions to STIP for the next minute. It continues to balance volume with capacity until issuers are able to process all transactions.

3.12.18 Positive Cardholder Authorization Service (PCAS)

PCAS is a set of risk control parameters available to issuers to determine whether V.I.P. routes authorization requests to issuers or to STIP.

If VisaNet routes transactions to issuers, they provide responses. If V.I.P. sends transaction to STIP, V.I.P. provides responses based on STIP authorization options and *PCAS* processing limits. Issuers choose from options increasing authorization risk control or customer service levels, or controlling authorization expenses. Issuers can customize parameters by merchant type, cardholder risk level, and cardholder spending.

3.12.19 Preauthorized Payment Cancellation Service (PPCS)

PPCS enables issuers to stop payments on preauthorized payment transactions, such as those for recurring or installment payments.

Participating issuers place stop payment orders in the Portfolio File in the Cardholder Database (CDB). When acquirers submit preauthorized payment transactions, V.I.P. checks the database and if there is a stop payment order for that account, it declines the request.

PPCS enables clients to meet Federal Reserve Regulation E requirements, which govern electronic funds transfers and provide U.S. cardholders with dispute rights for check card transactions. Clients issuing check cards must comply with Regulation E terms.

3.12.20 Status Check Service

Status check requests are authorization requests for one unit of currency (such as one U.S. dollar). Merchants use these requests to verify customers' account status when final transaction amounts aren't known, such as when customers check into hotels. V.I.P. forwards status check requests directly to issuers when they are available, bypassing STIP.

The *Status Check Service* allows merchants such as hotels, auto rental companies, and automated fuel dispenser (AFD) merchants to get authorizations without issuers reducing cardholders' open-to-buy amounts.

3.12.21 VisaNet Cashback Service

The *VisaNet Cashback Service* is a domestic service available as an option to participating regions for issuers, acquirers, and merchants on Visa Flag and Visa Electron products. *Cashback* is cash given to cardholders at the POS when they make purchases.

Clients must complete testing before they can participate in the service. Regions and countries within those regions establish maximum cashback amounts.

3.13 Authorization Service Availability

Table 3-7 Authorization Service Availability

Authorization Service	AVAILABLE FOR...			
	Acquirer	Issuer	BASE I	SMS
Account Verification Service	✓		✓	✓
Address Verification Service (AVS)	✓	✓	✓	✓
Advice Retrieval Service—BASE I		✓	✓	
Advice Retrieval Service—SMS	✓	✓		✓
ATM Format Conversion Service		✓		✓
Card Verification Value (CVV) Service	✓	✓	✓	✓
Card Verification Value 2 (CVV2) Service	✓	✓	✓	✓
Cardholder Authentication Verification Value (CAVV) Verification Service	✓	✓	✓	✓
Custom Payment Service (CPS)/ATM	✓	✓	✓	
Custom Payment Service (CPS)/POS	✓	✓	✓	
Deferred Clearing Advice File (DCAF) Service		✓		✓
Dynamic Key Exchange (DKE) Service	✓	✓		✓
Dynamic Card Verification Value (dCVV) Service	✓	✓	✓	✓
Multicurrency Service	✓	✓	✓	✓
PIN Verification Service (PVS)		✓	✓	✓
POS Check Service	✓	✓		✓
Positive Authorization Capacity Management (PACM) Service		✓	✓	✓
Positive Cardholder Authorization Service (PCAS)		✓	✓	✓

Table 3-7 Authorization Service Availability (continued)

Authorization Service	AVAILABLE FOR...			
	Acquirer	Issuer	BASE I	SMS
Preauthorized Payment Cancellation Service (PPCS)	✓	✓	✓	✓
Status Check Service	✓	✓	✓	✓
VisaNet Cashback Service	✓	✓	✓	✓

3.14 Additional Service Definitions

This section describes additional services available through V.I.P.

3.14.1 Chargeback Reduction Service (CRS)

CRS:

- Reduces client costs by eliminating unnecessary exception items (chargebacks, copy requests, and representments).
- Improves accuracy and timeliness of exception transactions.

CRS applies to Visa and Visa Electron POS transactions *only*; not to ATM or Interlink transactions.

3.14.2 ATM Processing Integration

SMS participants wanting to format and process *all* ATM transactions without distinguishing between Visa and Plus ATM transactions can do so by changing field coding.

3.15 Additional Service Availability

Table 3-8 Additional Service Availability

Additional Service	AVAILABLE FOR...			
	Acquirer	Issuer	BASE I	SMS
Chargeback Reduction Service (CRS)	✓	✓		✓
ATM Processing Integration	✓	✓		✓

THIS PAGE INTENTIONALLY LEFT BLANK.

Acquirer and Issuer Responsibilities

4

This chapter describes the responsibilities and options for clients connecting to V.I.P. Clients must first establish processing centers. Each center must fulfill the responsibilities of acquirers and issuers.

4.1 Establishing Processing Centers

Acquirers and issuers must establish an in-house processing center, or designate another center or third-party processor, to perform processing functions. The center must have systems to supply merchant support services, or cardholder support services, or both. Support services include communicating with merchant sites and cardholders and with V.I.P. at the VIC.

4.1.1 Network Stations

One processing center can have multiple physical network stations in VisaNet, based on volume and business needs, to:

- Handle a high volume of traffic.
- Process BASE I and SMS traffic separately.
- Accommodate multiple acquirer business locations.

EXAMPLE

A client could operate multiple in-house stations at one processing center.

EXAMPLE

An issuer could operate an in-house center with multiple stations to process purchase transactions and contract with another center to handle ATM transactions with PINs.

EXAMPLE

An acquirer could sponsor a merchant center with multiple stations, and operate an in-house center with multiple stations to serve other merchants and its own business locations.

EXAMPLE

A client could operate multiple in-house stations at different centers.

4.1.2 Message Support

The processing center must be capable of generating and receiving all types of V.I.P. messages for the card processing it performs. It must establish access to V.I.P., update system files at the VIC, and provide full message support.

Message support includes:

- Generating the type of message for the function desired.
- Receiving all applicable incoming messages.
- Supplying data required in the V.I.P. request when it is not available from the POS. Acquirer processing centers optionally can use the Merchant Central File Service (MCFS) to supply it.
- Managing messages related to transactions. This is critical to V.I.P. processing. Acquirers and issuers must avoid duplicate postings and must accurately calculate settlement totals.
- Supporting optional services or features used.
- Providing downtime procedures and recovery measures.

The V.I.P. message format provides enhanced processing capabilities to clients and processors. Visa requires that all centers connecting to V.I.P. use the V.I.P. format.

4.1.3 Testing

Visa tests centers' processing capabilities before they use V.I.P. During testing, centers send and receive test messages. Visa monitors transactions to ensure that centers are able to process all messages correctly.

4.1.4 Network Management

Processing centers must be able to control and support:

- Center system status. When the center's authorization system is down, it must sign off from VisaNet. If the center has a front-end processor and it is down, it must sign off from VisaNet.
- Test messages.
- Advice Recovery mode.
- Other network-related functions.

4.1.5 SMS Reconciliation and Settlement

V.I.P. automatically generates reconciliation advices for SMS clients. Visa POS, Visa Electron, Interlink, and ATM acquirers, and Visa POS and Interlink issuers must be able to receive them.

Centers should accumulate *settlement totals*, gross values of transactions processed. If centers process for several institutions, they should be able to allocate settlement totals to those institutions.

Centers should find and resolve settlement discrepancies. Visa assumes that V.I.P. totals are valid unless disproved by centers. Centers can use the activity reports to trace transactions and resolve discrepancies.

If clients want SMS processing:

- Acquirers participating in multiple networks must decide whether to use the Priority Routing Service. To use this service, they must establish a network processing priority list for V.I.P.
- They must decide whether to act as a settlement entity or to designate one. A *settlement entity* is the clearing agent establishing an account for funds transfer. Settlement

entities can establish this account at the transfer agent used by SMS for settlement or at institutions accessible through the Federal Reserve wire transfer system.

When acting as a settlement entity and sponsoring another institution or major merchant, acquirers are responsible for allocating funds transfer totals. VisaNet provides settlement reports at various levels for control and financial accounting but only transfers funds at the settlement-entity level.

- They must determine the level of VisaNet settlement reporting.

4.2 Acquirer Processing Center Requirements

The following requirements apply to acquirer processing centers implementing V.I.P. processing:

- POS connections and procedures
- PIN security
- Response procedures
- Merchant Central File management
- Follow-up procedures and processing
- Other responsibilities

4.2.1 POS Connections and Procedures

Processing centers must establish communication between themselves and their acquirers' points of sale and points of service. Centers install electronic terminals at the POS or provide phone authorization service to merchant sites only requiring authorization processing.

Setting up communications facilities involves:

- Establishing and maintaining a merchant network, an ATM network, or both. Visa requires this step for most BASE I and all SMS acquirer centers.

Acquirer centers are responsible for providing and maintaining:

- POS devices.
- Network communications facilities.
- Merchant operating procedures.
- Capability to support request and response messages to and from the POS.
- Arranging phone service and authorization support for merchant sites and branch offices. Visa requires this step for BASE I acquirer centers serving merchant sites without electronic terminals or providing this service as backup to their network service. Acquirers can choose to contract this service from outside entities.

When acquirers provide phone authorization service, they are responsible for authorization staff that can:

- Take calls requesting transaction approvals.
- Make provisions for entering requests into their processing systems.
- Establishing a system accepting and responding to requests from the POS network, ATM network, or both, or establishing an in-house authorization center.

In addition, acquirers must establish POS procedures using merchant agreements that determine:

- Rules and parameters for card acceptance, such as merchant floor limits (amount limits set by the acquirer [subject to Visa Rules maximums] determining if V.I.P. authorization is needed to complete a transaction.)
- Processing charges and merchant discounts.
- Authorization procedures for normal processing and for when the center cannot make connection with V.I.P. or is down.
- Chargeback, returned item, and representment procedures.
- Procedures for merchant settlement.

Acquirers must provide merchant training for handling transactions established in merchant agreements.

4.2.2 PIN Security

Acquirer centers processing transactions with PINs must provide network security between POS and ATM locations and their own systems. Centers must comply with the Visa Rules for PIN security in requests they send to the VIC.

See the *Payment Technology Standards Manual* for definitive regulations governing PINs.

4.2.3 Response Procedures

Acquirer centers must convert V.I.P. responses into response messages or terminal displays at the POS or ATM. When centers convert responses, they must not change the meaning of the issuers' responses.

Acquirer centers must establish procedures to handle non-routine responses from issuers, for instance, BASE I referrals or partial approvals.

4.2.4 Merchant Central File Management

Acquirer centers using the Merchant Central File Service (MCFS) must establish the policies and procedures to maintain its entries in the Merchant Central File at the VIC. This file management involves establishing controls necessary to ensure data accuracy and procedures for conveying updates to the VIC.

4.2.5 Follow-Up Procedures and Processing

Acquirer centers must establish policies on time-out values. They must allow adequate time for issuer centers to respond but also must be responsive to time-out demands of their own terminals and ATMs. If the response to a request times out:

- BASE I acquirer centers must send a repeat of the request.
- SMS acquirer centers must reverse it and send another request with new key data.

Acquirer centers must support reversal messages.

- BASE I centers use reversals to cancel previously approved transactions.
- SMS centers use reversals to cancel customer transactions and handle timed-out requests. They must also receive reversal advices from SMS. When SMS cannot deliver an approval response to an acquirer, SMS generates a reversal advice. In this case, SMS generates a reversal request for the issuer and generates a reversal advice for the acquirer.

Acquirer centers must establish policies and procedures for processing chargebacks and representments, and for adjustments for merchandise returns, failures at ATMs, and other back-office corrections. Acquirer centers must also comply with requests for originals and copies of sales drafts.

In addition, BASE I acquirer centers must support Visa and Plus transactions with BASE II batch transaction records if they support these products.

SMS acquirer centers must also support chargebacks, representments, adjustments, and copy requests using SMS online messages.

4.2.6 Other Responsibilities

Acquirer centers are generally responsible for other tasks external to V.I.P. processing, including:

- Processing merchant deposits after BASE I processing.
- Maintaining merchant accounts.
- Managing acquirer-to-merchant settlement.

4.3 Issuer Processing Center Requirements

The following requirements apply to issuer processing centers implementing V.I.P. processing:

- Transaction authorization
- Cardholder Database management
- PIN security
- Coordination with Visa
- Response procedures
- Follow-up procedures and processing
- Other responsibilities

4.3.1 Transaction Authorization

Issuers must make authorization decisions for normal and downtime processing, specify parameters for using STIP, and keep cardholder records.

Authorization processing typically involves a computer authorization system with files providing open-to-buy and account balance totals for cardholder accounts.

Issuer centers must maintain records of:

- Cardholders' credit limits.
- Account balances.
- Card restrictions.
- Card statuses, such as:
 - Lost
 - Stolen
 - Fraudulent
 - Pick-up

Issuer centers must also maintain cardholder records in files at the VIC that STIP uses for processing.

4.3.2 Cardholder Database Management

If issuer centers use STIP, they must maintain their Cardholder Database files at the VIC. Procedures include establishing controls to ensure accuracy of cardholder statuses and data plus methods for conveying updates to the VIC. (See *V.I.P. System Services, Volume 2*, for a description of the Automatic Cardholder Database Update [Auto-CDB] Service, which allows V.I.P. to update the Exception File, contained in the CDB, when issuers return a pick-up response code in authorization response messages.)

4.3.3 PIN Security

The issuer processing center is responsible for PIN generation and verification and rules for PIN usage. Visa issuers optionally can use the PIN Verification Service (PVS) to satisfy this requirement.

See the *Payment Technology Standards Manual* for definitive regulations governing PINs.

4.3.4 Coordination With Visa

Issuer centers, or issuers themselves, must provide Visa with the processing parameters V.I.P. is to use for their cardholders, including those determining:

- Routing of requests.
- Verification of PINs and Card Verification Values (CVVs, iCVVs, and dCVVs) at the VIC.
- STIP authorization decisions.

Issuer centers must establish procedures for notifying Visa whenever requirements or parameters change.

4.3.5 Response Procedures

Issuer centers must respond to requests within a reasonable timeframe. Regions establish Automated Response Time (ATR) time limits. Limits vary by region and card program.

If issuers don't respond to a request or reversal within the ATR limit, V.I.P. routes it to STIP. Upon receiving it, STIP provides the authorization decision. If an SMS issuer doesn't respond to an SMS acquirer-generated advice within the ATR limit, STIP responds for the issuer and stores the advice for recovery.

4.3.6 Follow-Up Procedures and Processing

Issuer centers must receive and process repeats, second submissions, or both, of a customer transaction, and receive and process reversals.

SMS issuer centers must also provide, depending on card products they process:

- Support for transaction and reversal advices. STIP, SMS, and BASE II can generate advices.
- Support for adjustments and merchandise returns.
- Chargeback procedures and support for chargeback messages.
- Support for representments.
- Other program-unique functions.

BASE I issuer centers handle such functions through BASE II or outside systems.

SMS issuer centers must ensure they properly track and process messages related to customer transactions. While SMS checks transaction consistency, issuer centers are responsible for validating incoming messages. For instance, if a merchandise return occurs days after the original purchase, SMS cannot check the adjustment message against the original request. Issuer centers must implement this checking.

Issuer centers must respond to cardholder requests for copies or originals of disputed sales drafts.

- BASE I centers must handle these requests through BASE II or outside systems.
- SMS centers must support SMS copy request messages.

4.3.7 Other Responsibilities

Issuer processing centers are also responsible for:

- Rules, charges, and fees for card usage.
- Methods of CVV or iCVV verification, if any, for Visa transactions. Visa issuers optionally can use the Card Verification Value (CVV) Service.
- Method of dCVV verification, if any, for Visa transactions. Visa issuers optionally can use the dCVV Service to perform this process.
- Method of CAVV verification, if any, for Visa transactions. Visa issuers optionally can use the CAVV Service to perform this process.
- Posting to cardholder accounts and preparing cardholder invoices.
- Reporting lost or stolen cards and other fraud control methods.
- Verifying addresses for mail and telephone order and airline transactions. Issuers optionally can use the Address Verification Service (AVS) to satisfy this requirement. (See *V.I.P. System Services, Volume 2* about these optional services.)

Issuer centers may be responsible for tasks at the issuer's request, such as issuing cards (with PIN Verification Values [PVVs] and CVVs or iCVVs, as applicable), issuing PINs, or posting transactions settled through BASE II.

THIS PAGE INTENTIONALLY LEFT BLANK.

Transaction Types

A

Cardholders initiate most transactions at an ATM or POS; merchants, acquirers, and issuers initiate other transactions. *Systems* generate transactions; issuer and acquirer back-office processing initiates others.

Table A-1 V.I.P. Transaction Types

Transaction Type	BASE I	SMS
Cardholder Transactions		
Preauthorization	✓	✓
Preauthorization Completion	✓	✓
Authorization or Verification Request	✓	✓
Prepaid Activation Request	✓	✓
Prepaid Load Request	✓	✓
Prepaid Activation and Load Request	✓	✓
ATM Cash Disbursement	✓	✓
Manual Cash Disbursement	✓	✓
Purchase	✓	✓
• Purchase With Cashback	✓	✓
• Quasi-Cash	✓	✓
• Key-Entered Purchase	✓	✓
• Purchase With Address Verification	✓	✓
• Recurring Payment	✓	✓
• Incremental Authorization	✓	✓
• Partial Amount Authorization	✓	✓
• U.S. Bill Payment	✓	✓
• Contactless	✓	✓
• Electronic Commerce	✓	✓
• Auto-Substantiation	✓	✓
Deferred Clearing Purchase	✓	✓
Below-Floor-Limit Purchase		✓

Table A-1 V.I.P. Transaction Types (continued)

Transaction Type	BASE I	SMS
Merchandise Return		✓
Original Credit	✓	✓
Balance Inquiry	✓	✓
Address Verification Only	✓	✓
Merchant-Authorized Transactions		
Healthcare Eligibility Inquiry	✓	✓
System-Generated Transactions		
Reversal	✓	✓
Cash Disbursement Adjustment		✓
Exception Transactions		
Adjustment		✓
Good-Faith Collection		✓
Chargeback		✓
Chargeback Reversal		✓
Representment		✓
Fee-Related Transactions		
Acquirer-Initiated Fee Collection/Funds Disbursement		✓
Issuer-Initiated Fee Collection/Funds Disbursement		✓
Reconciliation Transactions		
Reconciliation Request and Response		✓
File Maintenance Transactions		
File Update or Inquiry Request	✓	✓
Administrative Transactions		
Free-Text Message	✓	✓
Copy Request		✓
Online Fraud Reporting		✓
Network Management Transactions		
Network Management Request/Response	✓	✓

A.1 Cardholder Transactions

Preauthorization—Merchant locations such as gas stations use this when the merchant doesn't know the purchase amount at the time of transaction. *Preauthorizations* consist of an initial request message followed by a completion message. Merchants must complete the transaction within two (2) hours.

NOTE

If merchants do not submit completion messages within two hours, V.I.P. generates preauthorization reversals and delivers them to issuers. V.I.P. generates 0420 reversal advices for acquirers.

Merchants are guaranteed payment if:

- VisaNet receives preauthorization completion message within two (2) hours of corresponding approved preauthorization request message.
- Amount in completion message does not exceed amount approved by issuer.

IMPORTANT

For MasterCard automated fuel dispenser (AFD) transactions in Visa Canada and the U.S. region, issuers must receive completion messages within one (1) hour of preauthorization messages.

Authorization or Verification Request—Acquirers use this to request authorization or verify account or address information.

Prepaid Activation Request—Merchants and issuers submit this to activate prepaid cards.

Prepaid Load Request—Merchants and issuers submit this to load spending amounts onto activated prepaid cards.

Prepaid Activation and Load Request—Merchants and issuers submit this to activate and load value to cards in one message.

ATM Cash Disbursement—Cardholders use this for cash disbursements from ATMs.

Manual Cash Disbursement—Cardholders get cash in face-to-face environments with this (also called *manual cash*) . It is available for Visa POS and Visa Electron.

Purchase—Includes basic purchase transactions and:

- Purchase With Cashback—Variation permitting cardholders to get cash in addition to goods or services.
- Quasi-Cash—Cardholders use this to purchase items they can directly convert into cash, such as gaming chips and money orders. Available for Visa POS and Visa Electron.
- Key-Entered Purchase—Cardholders and merchants use this for Visa POS transactions as allowed by Visa Rules when terminals cannot read magnetic stripes.
- Purchase With Address Verification—Visa merchants such as direct marketing firms and airlines use this to verify cardholders' addresses as part of purchase requests.
- Recurring Payment—Occurs periodically per agreement between cardholder and merchant for payments of goods and services such as utility bills. Initial transaction can occur in card-present or card-not-present (mail order, telephone order, and electronic commerce) environments. Merchant automatically initiates subsequent, or *recurring*, transactions without cardholders being notified beforehand or necessarily being present.
- Incremental Authorization—Certain merchants, such as hotels and car rental companies, initiate this, which includes an estimated amount that can vary significantly from final transaction amount. May require supplemental, or *incremental*, authorizations or one authorization reversal.
- Partial Amount Authorization—VisaNet supports partial amount authorizations involving multicurrency processing for prepaid cards processed as BASE I dual-message and SMS single-message transactions.
- U.S. Bill Payment—Supports one-time payments, recurring payments, and installment payments, enabling consumer and commercial cardholders in the U.S. region to pay bills.

- **Contactless**—Involves a smart card that passes cardholder data to a terminal using wireless technology such as radio frequency (RF) or infrared.
- **Auto-Substantiation**—Available in the U.S. region only, healthcare auto-substantiation transactions are for purchases eligible for Flexible Spending Accounts (FSAs) or Healthcare Reimbursement Arrangements (HRAs) as defined by Internal Revenue Service (IRS) regulations.

Deferred Clearing Purchase—Merchants such as hotels and car rental agencies use this when purchase amount is not known at time of authorization. It may be preceded by authorization request. Message used to convey deferred clearing information is *deferred clearing advice*.

Below-Floor-Limit Purchase—Visa merchants use this when transaction amount is below floor limit. *Merchant floor limit* is amount limit set by acquirer (subject to Visa Rules maximums) determining if transaction requires V.I.P. authorization for completion. Because issuers do not need to authorize below-floor-limit transactions, V.I.P. or issuers cannot decline them if they meet all requirements. Available only for Visa POS, not for Visa Electron.

Merchandise Return—Permits merchants to credit accounts for cardholders who return merchandise for entire or partial amount.

Balance Inquiry—Allows cardholders to check account balances at ATMs, stand-alone merchant terminals away from POS, and at POS.

Address Verification Only—Visa merchants such as direct marketing firms and airlines use this to verify cardholder's address before submitting purchase transaction.

A.2 Merchant-Authorized Transactions

Healthcare Eligibility—Allows healthcare providers to determine whether cardholder's health insurance coverage is current. These U.S. region-only 0100 authorization requests and 0110 responses are non-financial, information-only transactions and are valid for BASE I, SMS POS, and Interlink.

A.3 System-Generated Transactions

Full and Partial Reversals—ATMs, acquirers' host systems, or V.I.P. can initiate these to reverse approved authorizations, preauthorizations, or financial transactions not completed due to system malfunctions or because they timed out. Financial transactions are cash disbursements, purchases (all variations), and merchandise credits. (Systems cannot reverse deferred clearing purchases and below-floor-limit purchases.)

Cash Disbursement Adjustment—ATM acquirers use this system-generated transaction (debit or credit) to adjust value of cash disbursements because of ATM misdispenses or late completions.

A.4 Exception Transactions

Clients use transactions to correct errors occurring at the point of transaction or during participants' processing.

Adjustment—Acquirers create *adjustments* to original transactions to correct errors such as out-of-balance conditions at the POS. Adjustments can be debits or credits.

Good-Faith Collection (Interlink only)—Interlink acquirers use this variation of adjustment if issuer agrees to accept financial transaction it cannot process under Interlink rules, typically because timeframes for exception processing have expired.

Chargeback—Issuers create *chargebacks* when cardholders dispute transactions, when cardholders assert merchandise was returned but merchandise credits have not been received by issuers, when issuers themselves dispute transactions, or when issuers receive unpostable debit adjustments from acquirers.

Chargeback Reversal—Issuers create *chargeback reversals* to cancel chargebacks sent in error.

Representment—Acquirers create *representments* when they can disprove validity of chargebacks.

A.5 Fee-Related Transactions

Fee-related transactions do not require authorization and cannot be declined.

Fee Collection—Clients use this to collect miscellaneous fees.

Funds Disbursement—Clients use this to remit miscellaneous fees.

A.6 Reconciliation Transactions

Clients can use optional *reconciliation transactions* to receive gross interchange totals at end of processing days. SMS participants use these interchange totals to verify processing totals.

A.7 File Maintenance Transactions

Issuers use *file maintenance transactions* to update or query Cardholder Database files such as Exception File, Address Verification File, or PIN Verification File.

Acquirers use file maintenance transactions to update or query system files such as Merchant Central File (MCF).

A.8 Administrative Transactions

Operations staff use *administrative messages* to request or convey information between issuers and acquirers.

Free-Text Message—Provides or requests general information.

Copy Request Message—Processes requests for documentation. ATM and Interlink transactions do not use these.

Online Fraud Reporting—Reports, tracks, and analyzes fraudulent transactions.

A.9 Network Management Transactions

Clients use *network management transactions* to:

Sign-On—Notifies VisaNet clients are available to send and receive messages.

Sign-Off—Notifies VisaNet clients are not available.

Recovery Sign-On—Requests delivery of advice messages by signing on to Advice Recovery mode.

Recovery Sign-Off—Indicates clients do not want to receive further advice messages and are signing off from Advice Recovery mode.

Reconciliation Request—Requests gross interchange totals.

Echo Test—Clients and V.I.P. use these to confirm availability of communications links between client host systems and VisaNet.

Dynamic Key Exchange—Clients and V.I.P. optionally use this to update working keys online.

Index

A

- Account Verification Service 3-2, 3-8
- acquirer responsibilities
 - establishing follow-up procedures 4-4
 - establishing Merchant Central File policies 4-4
 - establishing POS connections 4-3
 - establishing response procedures 4-4
 - processing options
 - Card Recovery Bulletins 3-5
 - providing PIN security 4-4
- Activity File
 - description 2-9
- Address Verification File
 - description 2-9
- Address Verification Service (AVS) 3-2, 3-8
- adjustment
 - cash disbursement transaction A-4
- administrative
 - messages 2-8
 - transactions A-5
- advice file 3-8
- advice recovery 2-5, 2-7, 4-2
- Advice Retrieval Service—BASE I 3-2
- Advice Retrieval Service—SMS 3-2
- Assured Transaction Response (ATR) 2-7
- ATM cash disbursement A-3
- ATM Format Conversion Service 3-2, 3-8
- ATM Processing Integration 3-2, 3-13
- ATM/POS Split Routing Service 3-1 to 3-2
- ATR, *See* Assured Transaction Response (ATR)
- authorization
 - definition 1-2
 - issuer responsibilities 4-5
 - request A-3
 - services
 - availability 3-12
 - Deferred Clearing Advice File (DCAF) Service 3-10
 - Dynamic Card Verification Value (dCVV) Service 3-10
 - Dynamic Key Exchange (DKE) Service 3-10
 - Multicurrency Service 3-10
 - PIN Verification Service (PVS) 3-11
 - POS Check Service 3-11
 - Positive Authorization Capacity Management (PACM) Service 2-5, 3-11
 - Positive Cardholder Authorization Service (PCAS) 2-5, 3-11
 - Preauthorized Payment Cancellation Service (PPCS) 3-11
 - Status Check Service 3-12
 - VisaNet Cashback Service 3-12
- authorization database services
 - Automatic Cardholder Database Update (Auto-CDB) Service 3-7
 - availability 3-7
 - Merchant Central File Service (MCFS) 3-7
- authorization services
 - Account Verification Service 3-8
 - Address Verification Service (AVS) 3-8
 - ATM Format Conversion Service 3-8
 - BASE I Advice Retrieval Service 3-8
 - Card Verification Value (CVV) Service 3-9
 - Card Verification Value 2 (CVV2) Service 3-9
 - Cardholder Authentication Verification Value (CAVV) Verification Service 3-9
 - Custom Payment Service (CPS)/ATM 3-9
 - Custom Payment Service (CPS)/POS 3-9
 - SMS Advice Retrieval Service 3-8
- Auto-CDB, *See* Automatic Cardholder Database Update (Auto-CDB) Service
- Automatic Cardholder Database Update (Auto-CDB) Service 3-1, 3-7
- AVS, *See* Address Verification Service (AVS)

B

- balance inquiry A-4
- BASE I Advice Retrieval Service 3-8
- BASE I System
 - description 1-7
 - overview 1-7
 - raw data 2-10
 - reports 2-10
 - stand-in processing (STIP) 2-5 to 2-6
- BASE II System 1-9
- billing
 - VisaNet Integrated Payment (V.I.P.) System 2-10
- business suite products 1-3

C

- Card Recovery Bulletin (CRB) Service 3-1, 3-5
- Card Verification Value (CVV)
 - in STIP 2-6 to 2-7
- Card Verification Value (CVV) Service 3-2, 3-9
 - result code processing 2-7
- Card Verification Value 2 (CVV2) Service 3-2, 3-9
- Card-Level Program ID File
 - description 2-9
- Cardholder Authentication Verification Value (CAVV) Verification
 - Service 3-2, 3-9
- Cardholder Database
 - advice file 3-8
 - issuer responsibilities 4-6
- Cardholder Database (CDB)
 - description 2-8
- cardholder transactions A-2
- cash disbursement cards 1-3
- CAVV Service, *See* Cardholder Authentication Verification Value (CAVV) Verification Service
- CDB, *See* Cardholder Database (CDB)
- Chargeback Reduction Service (CRS) 3-2, 3-13
- Check Acceptance Service 3-1, 3-3
- chip card services
 - availability 3-7
 - Visa Contactless Payment Service (VCPS) 3-6
 - Visa Smart Debit/Smart Credit (VSDC) Service 3-6
- clearing
 - definition 1-2, 1-10
- CMI, *See* Common Member Interface (CMI)
- commercial solutions 1-3
- Common Member Interface (CMI)
 - overview 1-11

- processes 1-11
- connection methods
 - VisaNet 1-5
- consumer credit products 1-2
- consumer debit products 1-3
- copy request A-5
- CPS, *See* Custom Payment Service (CPS)
- (CPS)/ATM, *See* Custom Payment Service (CPS)/ATM
- (CPS)/POS, *See* Custom Payment Service (CPS)/POS
- CRB, *See* Card Recovery Bulletin (CRB) Service
- CRB Service, *See* Card Recovery Bulletin (CRB) Service
- CRS, *See* Chargeback Reduction Service (CRS)
- Custom Payment Service (CPS)/ATM 3-2, 3-9
- Custom Payment Service (CPS)/POS 3-2, 3-9
- CVV, *See* Card Verification Value (CVV)
- CVV Service, *See* Card Verification Value (CVV) Service
- CVV2 Service, *See* Card Verification Value 2 (CVV2) Service

D

- DCAF Service, *See* Deferred Clearing Advice File (DCAF) Service
- dCVV Service, *See* Dynamic Card Verification Value (dCVV) Service
- debit cards 1-3
- deferred clearing
 - definition 1-2
 - purchase A-4
- Deferred Clearing Advice File (DCAF) Service 3-2, 3-10
- DEX, *See* Direct Exchange (DEX)
- Direct Exchange (DEX) 1-5
- diversion threshold 2-5
- DKE Service, *See* Dynamic Key Exchange (DKE) Service
- dual-message transaction
 - definition 1-2
- Dynamic Card Verification Value (dCVV) Service 3-2, 3-10
- dynamic key exchange A-6
- Dynamic Key Exchange (DKE) Service 3-2, 3-10

E

- echo test A-6
- establishing POS connection 4-3
- Exception File
 - description 2-9
 - updating 2-9
- exception transactions A-4

F

- fee-related transactions A-5

- file
 - maintenance transactions A-5
- files
 - advice file 3-8
- financial transactions, types A-1
- Fraud Reporting System (FRS) 3-1, 3-5
- free text message A-5
- FRS, *See* Fraud Reporting System (FRS)

G

- Gateway Services 3-1, 3-3
- good-faith collection A-5

H

- healthcare eligibility transaction A-4

I

- issuer processing options
 - Card Recovery Bulletins 3-5
- issuer responsibilities
 - establishing authorization policies 4-5
 - establishing Cardholder Database file policies 4-6
 - establishing follow-up procedures 4-6
 - establishing response procedures 4-6
 - managing processing parameters 4-6
 - providing PIN security 4-6

L

- linking related messages 2-3
- logging
 - VisaNet Integrated Payment (V.I.P.) System 2-7

M

- manual cash disbursement A-3
- matching messages 2-3
- MCF, *See* Merchant Central File (MCF)
- MCFS, *See* Merchant Central File Service (MCFS)
- Merchant Central File
 - acquirer responsibilities 4-4
- Merchant Central File (MCF)
 - description 2-9
- Merchant Central File Service (MCFS) 3-1, 3-7
- Merchant Fraud Performance Program 3-1
- merchant-authorized transactions
 - healthcare eligibility A-4

- message
 - bitmap 2-3
 - data fields 2-3
 - editing 2-2
 - formats 1-13, 2-2
 - header 2-2
 - response processing 2-7, 4-4, 4-6
 - sets 2-3
 - structure 2-2
 - support 4-1
 - type identifier 2-3
- message flows
 - normal processing
 - administrative transactions A-5
 - file maintenance transactions A-5
 - merchant-authorized transactions A-4
 - network management transactions A-5
 - reconciliation transactions A-5
 - system-generated transactions A-4
- messages
 - administrative 2-8
- Multicurrency Service 3-2, 3-10

N

- network management 2-7, 4-2
- network management transactions A-5
- network stations 4-1
- normal processing
 - administrative transactions
 - A-5
 - file maintenance transactions A-5
 - merchant-authorized transactions A-4
 - network management transactions
 - A-5
 - system-generated transactions A-4

O

- online deferred clearing
 - definition 1-2
- online fraud reporting transaction A-5

P

- PACM, *See* Positive Authorization Capacity Management (PACM) Service
- PACM Service, *See* Positive Authorization Capacity Management (PACM) Service

parameters

- issuer managing 4-6
- stand-in processing (STIP) 2-5
- V.I.P. 1-12

PCAS, *See* Positive Cardholder Authorization Service (PCAS)

PIN Debit Gateway Service (PDGS) 3-1, 3-3

PIN security 4-4, 4-6

PIN Verification File

- description 2-9

PIN Verification Service (PVS) 2-9, 3-2, 3-11

PIN/No-PIN Split Routing Service 3-1, 3-4

Portfolio File

- description 2-9

POS Check Service 3-2, 3-11

POS connection, setting up 4-3

Positive Authorization Capacity Management (PACM) Service 3-2, 3-11

Positive Cardholder Authorization Service (PCAS) 3-11

PPCS, *See* Preauthorized Payment Cancellation Service (PPCS)

Preauthorization A-2

Preauthorized Payment Cancellation Service (PPCS) 2-9, 3-2, 3-11

prepaid activation

- request A-3

prepaid activation and load

- request A-3

prepaid cards 1-3

prepaid load

- request A-3

Priority Routing Service 3-1, 3-4

processing

BASE I 1-7

BASE II 1-9

Common Member Interface (CMI) 1-11

networks 1-1

parameters

- issuer responsibilities 4-6
- stand-in processing (STIP) 2-5
- V.I.P. 1-12

Single Message System (SMS) 1-8

VisaNet Settlement Service (VSS) 1-10

processing center

description 1-5

establishing 4-1

network management 4-2

requirements

- acquirer 4-3
- issuer 4-5, 4-7

testing 4-2

processing flow

- transaction 2-1

products

business suite 1-3

cash disbursement cards 1-3

commercial solutions 1-3

consumer credit 1-2

debit cards 1-3

debit products 1-3

prepaid cards 1-3

purchase

auto-substantiation A-4

below-floor-limit A-4

bill payment A-3

contactless A-4

incremental authorization A-3

key-entered A-3

partial amount authorization A-3

recurring payment A-3

with address verification A-3

with cashback A-3

PVS, *See* PIN Verification Service (PVS)

Q

quasi-cash A-3

R

raw data

BASE I System 2-10

Single Message System (SMS) 2-10

reconciliation transactions A-5

reports

BASE I System 2-10

settlement 2-10

Single Message System (SMS) 2-10

VisaNet Integrated Payment (V.I.P.) System 2-9

representment A-5

reversal

transaction

- system-generated A-4

risk management services

availability 3-5

Card Recovery Bulletin (CRB) Service 3-5

Fraud Reporting System (FRS) 3-5

risk-level file

description 2-9

- routing
 - alternatives 2-5
 - definition 2-3
 - information
 - stand-in processing (STIP) 2-5
 - system tables 2-4
 - internal services 2-5
 - services
 - ATM/POS Split Routing Service 3-2
 - availability 3-4
 - Check Acceptance Service 3-3
 - Gateway Services 3-3
 - PIN Debit Gateway Service (PDGS) 3-3
 - PIN/No-PIN Split Routing Service 3-4
 - Priority Routing Service 3-4
 - Visa Shortest Online Path (VSOP) Service 3-4
 - tables 2-4
- S**
 - services
 - Account Verification Service 3-2, 3-8
 - Address Verification Service (AVS) 3-2, 3-8
 - Advice Retrieval Service—BASE I 3-2
 - Advice Retrieval Service—SMS 3-2
 - ATM Format Conversion Service 3-2, 3-8
 - ATM Processing Integration 3-2, 3-13
 - ATM/POS Split Routing Service 3-1 to 3-2
 - Automatic Cardholder Database Update (Auto-CDB)
 - Service 3-1, 3-7
 - BASE I Advice Retrieval Service 3-8
 - Card Recovery Bulletin (CRB) Service 3-1, 3-5
 - Card Verification Value (CVV) Service 3-2, 3-9
 - Card Verification Value 2 (CVV2) Service 3-2, 3-9
 - Cardholder Authentication Verification Value (CAVV)
 - Verification Service 3-2, 3-9
 - Chargeback Reduction Service (CRS) 3-2, 3-13
 - Check Acceptance Service 3-1, 3-3
 - Custom Payment Service (CPS)/ATM 3-2, 3-9
 - Custom Payment Service (CPS)/POS 3-2, 3-9
 - Deferred Clearing Advice File (DCAF) Service 3-2, 3-10
 - Dynamic Card Verification Value (dCVV) Service 3-2, 3-10
 - Dynamic Key Exchange (DKE) Service 3-2, 3-10
 - Fraud Reporting System (FRS) 3-1, 3-5
 - Gateway Services 3-1, 3-3
 - Merchant Central File Service (MCFS) 3-1, 3-7
 - Merchant Fraud Performance Program 3-1
 - Multicurrency Service 3-2, 3-10
 - PIN Debit Gateway Service (PDGS) 3-1, 3-3
 - PIN Verification Service (PVS) 3-2, 3-11
 - PIN/No-PIN Split Routing Service 3-1, 3-4
 - POS Check Service 3-2, 3-11
 - Positive Authorization Capacity Management (PACM)
 - Service 3-2, 3-11
 - Positive Cardholder Authorization Service (PCAS) 3-2, 3-11
 - Preauthorized Payment Cancellation Service (PPCS) 3-2, 3-11
 - Priority Routing Service 3-1, 3-4
 - SMS Advice Retrieval Service 3-8
 - Status Check Service 3-2, 3-12
 - Visa Contactless Payment Service (VCPS) 3-1, 3-6
 - Visa Secure Electronic Commerce (VSEC) With Verified by
 - Visa (3-D Secure) 3-1, 3-5
 - Visa Shortest Online Path (VSOP) Service 3-1, 3-4
 - Visa Smart Debit/Smart Credit (VSDC) Service 3-1, 3-6
 - VisaNet Cashback Service 3-2, 3-12
 - VisaNet Integrated Payment (V.I.P.) System
 - listed by functional group 3-1
 - settlement
 - definition 1-2, 1-10
 - reports 2-10
 - settlement entity
 - definition of 4-2
 - sign on and sign off 2-7
 - sign on/sign off 4-2
 - Single Message System (SMS)
 - description 1-8
 - overview 1-8
 - raw data 2-10
 - reconciliation requirements 4-2
 - stand-in processing (STIP) 2-6
 - Single Message System (SMS) System
 - reports 2-10
 - single-message transaction
 - definition 1-2
 - SMS, *See* Single Message System (SMS)
 - SMS Advice Retrieval Service 3-8
 - stand-in processing (STIP)
 - through V.I.P.
 - BASE I 2-5 to 2-6
 - parameters 2-5
 - Single Message System (SMS) 2-6
 - Status Check Service 3-2, 3-12
 - STIP, *See* stand-in processing (STIP)
 - system databases
 - Cardholder Database files 2-8
 - managing 2-8
 - Merchant Central File (MCF) 2-8

system globals, *See* system tables
 system parameters, *See* processing, parameters
 system tables 2-8
 routing 2-4
 system-generated transaction
 reversal A-4

T

test messages 2-7, 4-2
 testing 4-2
 transaction flow 2-1
 transaction processing
 authorization 1-2
 clearing 1-2
 dual message 1-2
 illustration of flow 2-1
 online deferred clearing 1-2
 settlement 1-2
 single message 1-2
 systems illustration 1-6
 transaction tracing 2-3
 transaction types
 administrative A-5
 cardholder A-2
 exception A-4
 fee-related A-5
 file maintenance A-5
 healthcare eligibility A-4
 list A-1
 merchant-authorized A-4
 network management A-5
 reconciliation A-5
 reversal
 system-generated A-4

V

V.I.P., *See* VisaNet Integrated Payment (V.I.P.) System
 Visa Contactless Payment Service (VCPS) 3-1, 3-6
 Visa Message Gateway 1-5
 Visa Secure Electronic Commerce (VSEC) services
 availability 3-6
 Visa Secure Electronic Commerce (VSEC) With Verified by Visa
 (3-D Secure) 3-1, 3-5
 Visa Shortest Online Path (VSOP) Service 3-1, 3-4
 Visa Smart Debit/Smart Credit (VSDC) Service 3-1, 3-6
 VisaNet
 BASE II System 1-9
 components 1-4
 connection methods 1-5
 definition 1-1
 systems 1-6
 transaction processing 1-6
 V.I.P. processing parameters 1-12
 VisaNet Cashback Service 3-2, 3-12
 VisaNet connection
 network stations 4-1
 VisaNet Integrated Payment (V.I.P.) System
 back-up 1-6
 billing 2-10
 Common Member Interface (CMI)
 illustration 1-11
 components
 BASE I System 1-7
 Common Member Interface (CMI) 1-11
 Single Message System (SMS) 1-8
 logging 2-7
 processing
 parameters 1-12
 reports 2-9
 services, listed by functional group 3-1
 VisaNet Settlement Service (VSS) 1-10
 VisaNet Settlement Service (VSS)
 definition 1-10
 illustration 1-10
 VSDC, *See* Visa Smart Debit/Smart Credit (VSDC) Service
 VSEC, *See* Visa Secure Electronic Commerce (VSEC) With Verified
 by Visa (3-D Secure)
 VSOP, *See* Visa Shortest Online Path (VSOP) Service
 VSOP Service, *See* Visa Shortest Online Path (VSOP) Service
 VSS, *See* VisaNet Settlement Service (VSS)