

PINless Debit Card Services

Using the SCMP API

September 2015



CyberSource Contact Information

For general information about our company, products, and services, go to <http://www.cybersource.com>.

For sales questions about any CyberSource Service, email sales@cybersource.com or call 650-432-7350 or 888-330-2300 (toll free in the United States).

For support information about any CyberSource Service, visit the Support Center at <http://www.cybersource.com/support>.

Copyright

© 2015 CyberSource Corporation. All rights reserved. CyberSource Corporation ("CyberSource") furnishes this document and the software described in this document under the applicable agreement between the reader of this document ("You") and CyberSource ("Agreement"). You may use this document and/or software only in accordance with the terms of the Agreement. Except as expressly set forth in the Agreement, the information contained in this document is subject to change without notice and therefore should not be interpreted in any way as a guarantee or warranty by CyberSource. CyberSource assumes no responsibility or liability for any errors that may appear in this document. The copyrighted software that accompanies this document is licensed to You for use only in strict accordance with the Agreement. You should read the Agreement carefully before using the software. Except as permitted by the Agreement, You may not reproduce any part of this document, store this document in a retrieval system, or transmit this document, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written consent of CyberSource.

Restricted Rights Legends

For Government or defense agencies. Use, duplication, or disclosure by the Government or defense agencies is subject to restrictions as set forth the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and in similar clauses in the FAR and NASA FAR Supplement.

For civilian agencies. Use, reproduction, or disclosure is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer Software Restricted Rights clause at 52.227-19 and the limitations set forth in CyberSource Corporation's standard commercial agreement for this software. Unpublished rights reserved under the copyright laws of the United States.

Trademarks

CyberSource, The Power of Payment, CyberSource Payment Manager, CyberSource Risk Manager, CyberSource Decision Manager, CyberSource Connect, Authorize.Net, and eCheck.net are trademarks and/or service marks of CyberSource Corporation. All other brands and product names are trademarks or registered trademarks of their respective owners.

Contents

Recent Revisions to This Document 5

About This Guide 6

Audience and Purpose 6

Conventions 6

 Note and Important Statements 6

 Text and Command Conventions 7

Related Documents 7

Customer Support 7

Chapter 1 Introduction 8

About Debit Cards 8

Requirements for Processing PINless Debit Cards 8

Overview of a PINless Debit Card Transaction 10

PINless Debit Cards versus Credit Cards 11

Getting Started 12

 Order Tracking 12

 Transaction Reference Number 12

 Request IDs 12

Working with CyberSource Reports for PINless Debits 12

Handling Timeouts and Reversals 13

Chapter 2 Processing PINless Debits with the SCMP API 14

PINless Debit Validate Service 14

 Request Fields 15

 Reply Fields 15

 Reply Flags 16

PINless Debit Service 17

 Request-Level Fields 18

 Offer-Level Fields 21

 Reply Fields 22

 Reply Flags 24

Payment Tokenization	25
Recurring Billing	26
Request and Reply Examples	27
PINless Debit	27

Chapter 3 Testing 28

Sending Requests to the Test System	28
Testing the PINless Debit Validate Service	28
Testing the PINless Debit Service	29

Appendix A Product Codes 30

Index	31
-------	----

Recent Revisions to This Document

Release	Changes
September 2015	Updated the URL for accessing the CyberSource test server. See "Sending Requests to the Test System," page 28 .
June 2015	This revision contains only editorial changes and no technical updates.
December 2013	Separated <i>PINless Debit Card Services Implementation Guide</i> into two documents: <ul style="list-style-type: none">▪ PINless Debit Card Services Using the Simple Order API▪ PINless Debit Card Services Using the SCMP API
June 2013	This revision contains only editorial changes and no technical updates.
March 2013	Removed references to FDC Compass because PINless Debit services are not supported for this processor.
September 2012	This revision contains only editorial changes and no technical updates.

About This Guide

Audience and Purpose

This guide is written for application developers who want to use the CyberSource SCMP API to integrate PINless debit processing into an order management system.

Implementing the CyberSource PINless debit services requires software development skills. You must write code that uses the API request and reply fields to integrate the PINless debit services into an existing order management system.

Conventions

Note and Important Statements



Note

A *Note* contains helpful suggestions or references to material not contained in the document.



Important

An *Important* statement contains information essential to successfully completing a task or learning a concept.

Text and Command Conventions

Convention	Usage
bold	<ul style="list-style-type: none"> Field and service names in text; for example: Include the ics_applications field. Items that you are instructed to act upon; for example: Click Save.
<i>italic</i>	<ul style="list-style-type: none"> Filenames and pathnames. For example: Add the filter definition and mapping to your <i>web.xml</i> file. Placeholder variables for which you supply particular values.
monospace	<ul style="list-style-type: none"> XML elements. Code examples and samples. Text that you enter in an API environment; for example: Set the davService_run field to <code>true</code>.

Related Documents

- *Credit Card Services Using the SCMP API* ([PDF](#) | [HTML](#)) describes the tasks you must complete to integrate the credit card services into your existing order management system.
- *Getting Started with CyberSource Advanced for the SCMP API* ([PDF](#) | [HTML](#)) describes how to get started using the SCMP API.
- *Payment Tokenization Using the SCMP API* ([PDF](#) | [HTML](#)) describes the tasks you must complete in order to create, update, retrieve, and delete customer profiles.
- *Recurring Billing Using the SCMP API* ([PDF](#) | [HTML](#)) describes the tasks you must complete to create, update, retrieve, and delete recurring customer subscriptions.
- *Reporting Developer Guide* ([PDF](#) | [HTML](#)) describes how to download reports.

Refer to the Support Center for complete CyberSource technical documentation:

http://www.cybersource.com/support_center/support_documentation

Customer Support

For support information about any CyberSource service, visit the Support Center:

<http://www.cybersource.com/support>

Introduction

About Debit Cards

Customers commonly use debit cards, which are also called ATM cards or check cards, in card-present situations, such as at the grocery store. In these cases, the customer must provide a personal identification number (PIN) to use the card. Because debit cards usually require a PIN, the use of these cards for card-not-present transactions has been limited.

The debit networks have realized, however, that certain card-not-present situations are low risk because of the nature of some businesses and the relationship between you and your customer. For these situations, the networks created PINless debit card transactions. You might be eligible to process PINless debit payments if your business is in one of the approved industry categories, including educational institutions, insurers, and utilities, among others. Your processor and the debit networks will determine if you are eligible to process PINless debit cards.

Debit cards are branded with the debit network logos, such as STAR, NYCE, Accel, and Pulse, and often with Visa and MasterCard logos as well. The logos indicate that the card can be accepted wherever Visa and MasterCard are accepted and can be processed through either a debit or credit card network. The customer chooses whether to process the card as a debit card or a credit card. In either case, the money is taken out of the customer's bank account and the transaction is included on the customer's bank account statement. The customer does not receive a credit card bill as with a regular credit card.

Requirements for Processing PINless Debit Cards

CyberSource supports PINless debit card transactions with these processors:

- Chase Paymentech Solutions
- FDMS South
- GPN

All PINless debit transactions must be in U.S. dollars. For Chase Paymentech Solutions, the transactions must originate from your web store or your telephone voice response unit/ interactive voice response (VRU/IVR) system. For FDMS South and GPN, the transactions must originate from your web store, VRU/IVR, or call center.

FDMS South and GPN must “close” each day’s transactions for reporting purposes. CyberSource does not send a request to the processor to close your transactions for the day. Instead, the processor automatically closes your transactions for the day at a time agreed to by the processor and you.

Before beginning your integration with CyberSource:

- Contact your processor to determine if you are eligible to process PINless debit transactions. As part of this process, the debit networks might require you to fill out applications.
- Determine whether your processor requires any additional banking information. For example, some processors use a separate terminal ID for debit card transactions.
- Determine whether you must comply with any special debit network requirements when processing PINless debit transactions. For example, some networks require that you verify the customer’s identity before processing the payment.
- Contact CyberSource Customer Support so that your CyberSource account can be configured for PINless debit transactions.

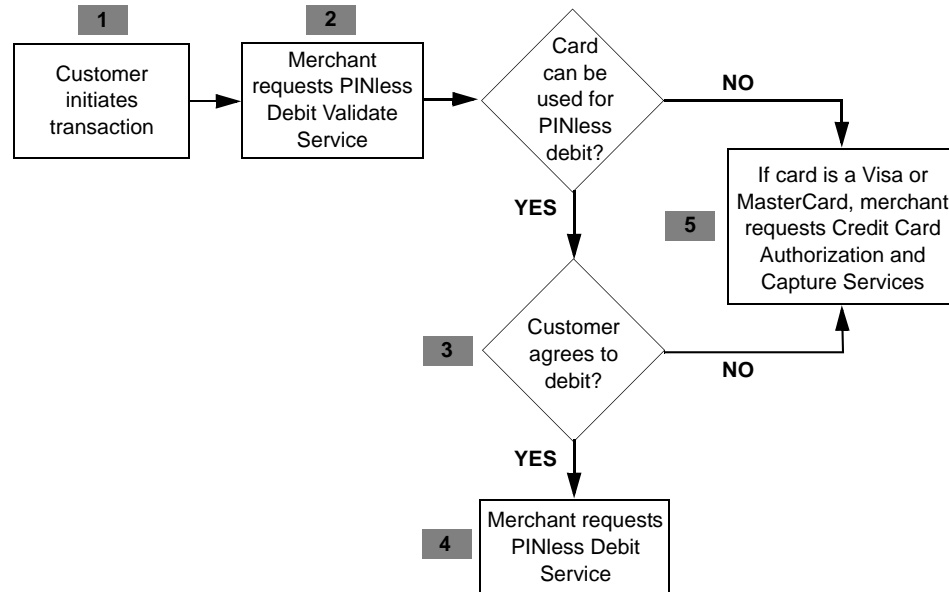
If your processor is GPN and you have determined you can process PINless debit transactions, you can also determine whether the customer’s card is PINless-capable. You can download the BIN (Bank Identification Number) table to perform a BIN lookup on the card. The BIN represents the digits on a payment card that identify the issuer of the card. BINs contained within the file represent cards that may be eligible for PINless processing that can be routed to a participating EFT network for authorization.

To Send an API Request to CyberSource:

- Step 1** In the following URL, replace `sample` with your merchant ID:
<https://ebc.cybersource.com/ebc/PINlessDebitBINInfoQuery.do?merchantId=sample>
 - Step 2** Enter your username and password.
 - Step 3** Click **OK**.
-

Overview of a PINless Debit Card Transaction

A PINless debit card transaction follows this flow:



- 1 You take the customer's order and card number through your web store or through a telephone voice response unit (VRU).
- 2 You request the PINless debit validate service to determine whether the card can be processed as a PINless debit card.
- 3 If the card can be processed as a PINless debit card, you give customer the choice to process the card as a debit/ATM card or a credit card.



Issuer regulations require that you must present the customer with this choice.

- 4 If the customer chooses debit/ATM, you request the PINless debit service. The transaction is routed through the debit card networks. You do not need to request a capture as you would with a credit card.

If the PINless debit service fails, but the card is a Visa or MasterCard, you can choose to process the card as a credit card.

- 5 If the debit card is branded with Visa or MasterCard, and if the customer chooses the credit card option or if the card cannot be used for PINless debit, process the transaction as a credit card transaction, requesting the credit card authorization and capture services together. The transaction is routed through the credit card networks. For information about processing credit cards, see [Credit Card Services Using the SCMP API](#).

Later, if you need to refund a PINless debit payment, you provide a store credit, cash, or check refund. Do not credit the customer's card as you would if it were a credit card.

PINless Debit Cards versus Credit Cards

You can process Visa- or MasterCard-branded debit cards through the credit card network the same way that you process credit cards by using the credit card authorization and capture services, which are described in [Credit Card Services Using the SCMP API](#). The transactions are considered credit card transactions. The only difference is that the bank takes the money from the customer's account instead of compiling all of the transactions for the month and sending the customer a bill.

PINless debit transactions and credit card transactions are processed differently:

- For a PINless debit transaction, you need to request only the PINless debit service. You do not need to request a capture because the PINless debit service authorizes the transaction and moves the money.
- For a credit card transaction, you can typically request an authorization reversal.
- For a credit card transaction, you receive an authorization code indicating an approval. For a PINless debit transaction, you do not necessarily receive an authorization code. Some processors provide an authorization code, but the code is not required for you to receive your money. For a PINless debit transaction, you cannot verbally obtain an authorization code from the processor or bank.
- For a credit card transaction, you can call the credit service the card to provide a refund. For a PINless debit transaction, there is no credit service. To provide a refund for a PINless debit payment, you must provide a store credit, issue a check, or give the customer cash.

Getting Started

See [Getting Started with CyberSource Advanced for the SCMP API](#) for basic information about the CyberSource SCMP API, including general information about the API versions and about order tracking.

Order Tracking

Transaction Reference Number

The field name for the transaction reference number for PINless debit transactions is **pinless_debit_trans_ref_no**.

For Chase Paymentech Solutions and FDMS South, you can use this value to reconcile the transactions in your CyberSource reports with the transactions in your processor reports.

Request IDs

For all PINless debit card services, the request ID is returned in the reply message in **request_id**.

Working with CyberSource Reports for PINless Debits

PINless debit transactions are included in the following CyberSource reports:

- Payment Batch Detail Report
- Payment Batch Summary Report
- Payment Submission Detail Report
- Transaction Detail Report

For information about downloading reports, see the [Reporting Developer Guide](#).

Handling Timeouts and Reversals

Supported processors:

- FDMS South—PINless debits

If a timeout error occurs when you request the PINless debit service, you will not know whether the transaction went through to the debit network or not. CyberSource automatically tries to reverse the transaction on your behalf according to the processor's specifications.

When CyberSource returns a timeout error reply to you, you should request the PINless debit transaction again.

**Note**

It is important that you wait for the response from CyberSource when requesting a PINless debit. Do not configure your CyberSource client to use a timeout value.

You will not receive notification from CyberSource as to whether the attempted automatic reversal succeeded or failed. However, you can search for the transaction in the [Business Center](#) and view the status of the automatic reversal in the top right corner of the Transaction Search Details page. Possible values for the status:

- Reversing—CyberSource is attempting the automatic reversal.
- Reversed—the automatic reversal succeeded.
- Reversal Failed—the automatic reversal failed.

You can also contact the processor to determine whether they successfully processed the automatic transaction reversal. When talking with the processor, you will probably need to reference the receipt number that CyberSource returned in the transaction reply.

It is possible, but very unlikely, that the automatic reversal attempt will fail and yet your original transaction request will have actually gone through to the processor. When this happens for a PINless debit transaction, you bill the customer twice. The customer should contact you when they realize that they have been billed twice, and you can provide a refund.

Processing PINless Debits with the SCMP API

PINless Debit Validate Service

Supported processors:

- Chase Paymentech Solutions
- FDMS South
- GPN

The PINless debit validate service determines whether a card can be used for a PINless debit transaction. To request the service, set the **ics_applications** field to `ics_pinless_debit_validate`. When requesting the service, do not include any other CyberSource services. To determine how to process the card, look at the **pinless_debit_validate_status** field in the reply:

- If the status is `Y`, the card can be used for a PINless debit transaction. You must provide the customer with the choice of processing the card as a debit/ATM card or a credit card.
- If the status is `N`, the card cannot be used for a PINless debit transaction. If you know the card is a credit card, you should process the card as a credit card.
- If the status is `U`, the card was not validated. If you know the card is a credit card, you should process the card as a credit card.

Request Fields

The following table describes the request fields for the `ics_pinless_debit_validate` service. The service has no offer-level fields.

Table 1 Request-Level Fields for `ics_pinless_debit_validate`

Request Field	Description	Required / Optional	Data Type & Length
customer_cc_number	Card number to validate.	Required	For GPN: String with numbers only (19) For all other processors: String with numbers only (20)
ics_applications	CyberSource services to process for the request.	Required	String (255)
merchant_id	Your CyberSource merchant ID. Use the same merchantID service for evaluation, testing, and production.	Required	String (30)
merchant_ref_number	Merchant-generated order reference or tracking number. See the order tracking information in Getting Started with CyberSource Advanced for the SCMP API .	Required	String (50)

Reply Fields

The following table describes the reply fields for the `ics_pinless_debit_validate` service.

Table 2 Reply Fields for `ics_pinless_debit_validate`

Reply Field	Description	Data Type & Length
client_lib_version	Information about the client library used to request the transaction.	String (50)
ics_rcode	One-digit code that indicates whether the entire request was successful. Possible values: <ul style="list-style-type: none"> ■ -1: An error occurred ■ 0: The request was declined ■ 1: The request was successful 	Integer (1)
ics_rflag	One-word description of the result of the entire request. See " Reply Flags ," page 24 , for a list of possible values.	String (50)
ics_rmsg	Message that explains the reply flag ics_rflag .	String (255)
merchant_ref_number	Order reference or tracking number that you provided in the request. If you included multi-byte characters in this field in the request, the returned value might contain corrupted characters.	String (50)

Table 2 Reply Fields for ics_pinless_debit_validate (Continued)

Reply Field	Description	Data Type & Length
pinless_debit_validate_rcode	One-digit code that indicates whether the ics_pinless_debit_validate request was successful. Possible values: <ul style="list-style-type: none"> ■ -1: An error occurred ■ 0: The request was declined ■ 1: The request was successful 	Integer (1)
pinless_debit_validate_rflag	One-word description of the result of the ics_pinless_debit_validate request. See "Reply Flags," page 24 , for a list of possible values.	String (50)
pinless_debit_validate_rmsg	Message that explains the reply flag pinless_debit_validate_rflag .	String (255)
pinless_debit_validate_time	Time of the PINless debit validate service request. The format is YYYY-MM-DDThhmmssZ. For example, 2013-08-11T224757Z is equal to August 11, 2013, at 10:47:57 P.M. The T separates the date and the time. The Z indicates GMT.	String (20)
pinless_debit_validate_status	Whether the card can be used for a PINless debit transaction. Possible values: <ul style="list-style-type: none"> ■ N: No, the card cannot be used for a PINless debit transaction. If it is a credit card, process the card as a credit card. ■ U: The card number was not validated. Process the card as a credit card. ■ Y: Yes, the card can be used for a PINless debit transaction. Present the customer with the choice of processing as a debit/ATM or credit card. 	String (1)
request_id	Identifier for the request generated by the client.	String (26)

Reply Flags

The following table describes the rflags for the **ics_pinless_debit_validate** service.

Table 3 Reply Flags for ics_pinless_debit_validate

Reply Flag	Description
DINVALIDDATA	The request contains invalid data.
DMISSINGFIELD	The request is missing a required field.
ESYSTEM	System error. See the documentation for your CyberSource client for important information about how to handle system errors and retries.
ETIMEOUT	The request timed out.
SOK	The transaction was successful.

PINless Debit Service

Supported processors:

- Chase Paymentech Solutions
- FDMS South
- GPN—Maximum amount is 99,999.00

To request the service, set the **ics_applications** field to `ics_pinless_debit`. For request and reply examples, see ["Request and Reply Examples," page 27](#).

Request the service only after you have:

- Step 1** Determined that the card can be used for a PINless debit, which you do in a separate request for **ics_pinless_debit_validate** as described in ["PINless Debit Validate Service," page 14](#).
- Step 2** Offered the customer a choice of how to process the card and received the customer's permission to process the card as a debit/ATM card.

When requesting the **ics_pinless_debit** service, do not include any of these other types of CyberSource services in your request:

- Any service involving any other method of payment
- Payment Tokenization services
- Recurring Billing services
- Payer Authentication services

Request-Level Fields

The following table describes the request-level fields for the **ics_pinless_debit** service.

Table 4 Request-Level Fields for ics_pinless_debit

Request-Level Field	Description	Required / Optional	Data Type & Length
bill_address1	First line of the billing street address.	Chase Paymentech Solutions: Required All other processors: Optional	String (60)
bill_address2	Second line of the billing street address. Used for additional address information, for example: Attention: Accounts Payable	Optional	String (60)
bill_city	City of the billing address.	Chase Paymentech Solutions: Required All other processors: Optional	String (50)
bill_country	Country of the billing address. Use the two-character <i>ISO Standard Country Codes</i> .	Required	String (2)
bill_state	State of the billing address.	Required if bill_country = US or CA	String (2)
bill_zip	Postal code for the billing address. The postal code must consist of 5 to 9 digits. If the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits] Example: 12345-6789 If the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric] Example: A1B 2C3	Required if bill_country = US or CA	String (10)
currency	Currency used for the order. For PINless debit cards, this value must be USD.	Required	String (5)
customer_cc_expmo	Card expiration month. Format: MM. If you do not have the value, use 12.	Optional	String (2)
customer_cc_expyr	Card expiration year. Format: YYYY. If you do not have the value, use 2021.	Optional	Non-negative integer (4)

Table 4 Request-Level Fields for ics_pinless_debit (Continued)

Request-Level Field	Description	Required / Optional	Data Type & Length
customer_cc_number	PINless debit card number.	Required	For GPN: String with numbers only (19) For all other processors: String with numbers only (20)
customer_email	Customer's email address, including the full domain name. For example, <code>jdoe@example.com</code> .	Optional	String (255)
customer_firstname	Customer's first name.	Chase Paymentech Solutions: Required All other processors: Optional	String (60)
customer_hostname	DNS resolved hostname from customer_ipaddress .	Optional	String (60)
customer_ipaddress	IP address of the customer. For example, <code>10.1.27.63</code> .	Optional	String (15)
customer_lastname	Customer's last name.	Chase Paymentech Solutions: Required All other processors: Optional	String (60)
customer_phone	Customer's telephone number.	Optional	String (15)
e_commerce_indicator	Type of transaction. Certain payment card companies use this information when determining discount rates. Possible values: <ul style="list-style-type: none"> ■ <code>internet</code> (default): eCommerce order placed using a Web site. ■ <code>moto</code>: VRU/IVR order. ■ <code>moto-call center</code>: Call center order. This value is not valid for Chase Paymentech Solutions. ■ <code>moto-ivr</code>: IVR order. This value is not valid for Chase Paymentech Solutions. 	Optional	String (13)

Table 4 Request-Level Fields for ics_pinless_debit (Continued)

Request-Level Field	Description	Required / Optional	Data Type & Length
grand_total_amount	Grand total for the order. You must include either this field or offer0 and the offer-level field amount . See the information about offers and grand totals in Getting Started with CyberSource Advanced for the SCMP API . The maximum PINless debit amount for GPN is 99,999.00.	See description	Decimal (15)
ics_applications	CyberSource services to process for the request.	Required	String (255)
link_to_request	Value that links the current request to a previous authorization request for a debit card or prepaid card. This value is useful when using multiple payment methods to complete an order. For details, see the information about partial authorizations in Credit Card Services Using the SCMP API .	Optional	String (26)
merchant_id	Your CyberSource merchant ID. Use the same merchant ID value for evaluation, testing, and production.	Required	String (30)
merchant_ref_number	Merchant-generated order reference or tracking number. See the order tracking information in Getting Started with CyberSource Advanced for the SCMP API .	Required	String (50)
offer0...N	Offers (line items of the order) for the request. You must include either offer0 and the offer-level field amount , or you must include grand_total_amount . See the information about offers and grand totals in Getting Started with CyberSource Advanced for the SCMP API .	See description	String (50)
ship_to_address1	First line of the shipping address.	Optional	String (60)
ship_to_address2	Second line of the shipping address.	Optional	String (60)
ship_to_city	City of shipping address.	Optional	String (50)
ship_to_country	Country of shipping address.	Optional	String (2)
ship_to_firstname	First name of person receiving the product.	Optional	String (60)
ship_to_lastname	Last name of the person receiving the product.	Optional	String (60)
ship_to_state	State or province of shipping address. Use the State, Province, and Territory Codes for the United States and Canada .	Required if ship_to_country = US or CA.	String (2)

Table 4 Request-Level Fields for ics_pinless_debit (Continued)

Request-Level Field	Description	Required / Optional	Data Type & Length
ship_to_zip	<p>Postal code for the shipping address. The postal code must consist of 5 to 9 digits.</p> <p>If the shipping country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits] Example: 12345-6789</p> <p>If the shipping country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric] Example: A1B 2C3</p>	Optional	String (10)
shipping_method	Shipping method for the product. For example, FEDEX.	Optional	String (10)
timeout	Number of seconds the system waits before the transaction times out. See "Handling Timeouts and Reversals," page 13 , for important information.	Optional	Positive integer (3)

Offer-Level Fields

The following table describes the offer-level fields for the **ics_pinless_debit** service.

Table 5 Offer-Level Fields for ics_pinless_debit

Offer-Level Field	Description	Required / Optional	Data Type & Length
amount	<p>Per-item price of the product. You must include either offer0 and this field, or the request-level field grand_total_amount in your request. This value cannot be negative.</p> <p>You can include a decimal point (.) in this field, but you cannot include any other special characters. The amount will be truncated at the request level to the correct number of decimal places.</p> <p>The maximum PINless debit amount for GPN is 99,999.00.</p>	See description	Decimal (15)
merchant_product_sku	Product identifier code. Required if product_code is not default, stored_value, or one of the values related to shipping and/or handling.	See description	String (30)

Table 5 Offer-Level Fields for ics_pinless_debit (Continued)

Offer-Level Field	Description	Required / Optional	Data Type & Length
product_code	Type of product that the offer contains. The default value is default. See "Product Codes," page 30, for a list of valid values. If you set this to a value other than default, stored_value, or any of the values related to shipping and/or handling, the quantity , product_name , and merchant_product_sku fields are required.	Optional	String (30)
product_name	Name of the product. Required if product_code is not default, stored_value, or one of the values related to shipping and/or handling.	See description	String (30)
quantity	Quantity of the product being purchased. The default value is 1. Required if product_code is not default, stored_value, or one of the values related to shipping and/or handling.	See description	Non-negative integer (10)
tax_amount	Total tax to apply to the product. The tax_amount field is additive. For example, if you send the following offer lines: <code>offer0=amount:10.00^quantity:1^tax_amount:0.80</code> <code>offer1=amount:20.00^quantity:1^tax_amount:1.60</code> the total amount authorized will be for 32.40, not 30.00 with 2.40 of tax included. The tax_amount and the amount values must be the same currency.	Optional	Decimal (15)

Reply Fields

The following table describes the reply fields for the **ics_pinless_debit** service.

Table 6 Reply Fields for ics_pinless_debit

Reply Field	Description	Data Type & Length
client_lib_version	Information about the client library used to request the transaction.	String (50)
currency	Currency used for the order.	String (5)
ics_rcode	One-digit code that indicates whether the entire request was successful. Possible values: <ul style="list-style-type: none"> ■ -1: An error occurred ■ 0: The request was declined ■ 1: The request was successful 	Integer (1)

Table 6 Reply Fields for ics_pinless_debit (Continued)

Reply Field	Description	Data Type & Length
ics_rflag	One-word description of the result of the entire request. See "Reply Flags," page 24 , for a list of possible values.	String (50)
ics_rmsg	Message that explains the reply flag ics_rflag .	String (255)
merchant_ref_number	Order reference or tracking number that you provided in the request. If you included multi-byte characters in this field in the request, the returned value might contain corrupted characters.	String (50)
pinless_debit_amount	Total amount of the payment.	Decimal (15)
pinless_debit_auth_code	Processor's authorization code for the PINless debit payment. Some processors do not return an authorization code. You do not need the code to receive your money.	String (6)
pinless_debit_owner_merchant_id	Merchant ID that was used to create the subscription or customer profile for which the service was requested. If you are enabled for Recurring Billing, this field is returned only if you are using subscription sharing and if your merchant ID is in the same merchant ID pool as the owner merchant ID. See the subscription sharing information in the Recurring Billing Using the SCMP API . If you are enabled for Payment Tokenization, this field is returned only if you are using profile sharing and if your merchant ID is in the same merchant ID pool as the owner merchant ID. See the profile sharing information in Payment Tokenization Using the SCMP API .	String (30)
pinless_debit_processor_response	Processor's response code for the transaction. Note Do not use this field to interpret the result of the request.	String (10)
pinless_debit_rcode	One-digit code that indicates whether the ics_pinless_debit request was successful. Possible values: <ul style="list-style-type: none"> ■ -1: An error occurred ■ 0: The request was declined ■ 1: The request was successful 	Integer (1)
pinless_debit_receipt_number	For Chase Paymentech Solutions, this is the processor-generated debit trace number. For FDMS South and GPN, this is the CyberSource-generated receipt number for the debit. You might need to reference the receipt number if you talk to your processor about the debit or any reversal that might occur. See "Handling Timeouts and Reversals," page 13 .	String (6)
pinless_debit_rflag	One-word description of the result of the ics_pinless_debit request. See "Reply Flags," page 24 , for a list of possible values.	String (50)
pinless_debit_rmsg	Message that explains the reply flag pinless_debit_rflag .	String (255)

Table 6 Reply Fields for ics_pinless_debit (Continued)

Reply Field	Description	Data Type & Length
pinless_debit_time	Time of the PINless debit service request. The format is YYYY-MM-DDThhmmssZ. For example, 2013-08-11T224757Z is equal to August 11, 2013, at 10:47:57 P.M. The T separates the date and the time. The Z indicates UTC.	String (20)
pinless_debit_trans_ref_no	Reference number for the transaction. For Chase Paymentech Solutions and FDMS South, you can use this value to reconcile your CyberSource reports with your processor reports.	String (60)
request_id	Identifier for the request generated by the client.	String (26)

Reply Flags

The following table describes the rflags for the **ics_pinless_debit** service.

Table 7 Reply Flags for ics_pinless_debit

Reply Flag	Description
DCALL	The issuing bank wants to speak with the cardholder. Returned only for Chase Paymentech Solutions.
DCARDEXPIRED	The card has expired.
DCARDREFUSED	The bank declined the transaction.
DINVALIDCARD	The card did not pass CyberSource basic checks, or the card cannot be used as a debit card.
DINVALIDDATA	Data provided is not consistent with the request. For example, the request includes a product with a negative cost.
DMISSINGFIELD	The request is missing a required field.
ESYSTEM	System error. See the documentation for your CyberSource client for important information about how to handle system errors and retries.
ETIMEOUT	The request timed out.
SOK	The transaction was successful.

Payment Tokenization

Applicable services:

- Debit
- Credit

Supported processors:

- GPN

If you are using Payment Tokenization, you can process a debit or credit by using information that is stored in a customer profile. CyberSource uses the subscription ID to reference the customer profile information in the CyberSource database. Instead of providing all the information that is normally required for a transaction, you need to provide only the following values:

- Merchant ID
- Merchant reference number
- Amount of the payment or credit
- Subscription ID

You can override most of the information stored in the customer profile by including the relevant API fields in the debit or credit request. For example, you could provide a different billing or shipping address in the request. You cannot override the account number.

For complete information about Payment Tokenization, see [Payment Tokenization Using the SCMP API](#).

Recurring Billing

Applicable services:

- Debit
- Credit

Supported processors:

- GPN

If you are using Recurring Billing, you can process a debit or credit by using information that is stored in a subscription. CyberSource uses the subscription ID to reference the subscription information in the CyberSource database. Instead of providing all the information that is normally required for a transaction, you only need to provide the following values:

- Merchant ID
- Merchant reference number
- Amount of the payment or credit
- Subscription ID

You can override most of the information stored in the subscription by including the relevant API fields in the debit or credit request. For example, you could provide a different billing or shipping address in the request. You cannot override the account number.

For complete information about Recurring Billing, see [Recurring Billing Using the SCMP API](#).

Request and Reply Examples

PINless Debit

Example 1 Request

```
ics_applications=ics_pinless_debit
merchant_id=infodev
merchant_ref_number=482046C3A7E94F5BD1FE3C66C
customer_firstname=Joe
customer_lastname=Smith
bill_address1=1040 Elm St.
bill_city=San Jose
bill_state=CA
bill_zip=95127
bill_country=US
customer_cc_number=4002269999999999
customer_cc_expmo=12
customer_cc_expyr=2021
customer_phone=650-965-6000
customer_email=jsmith@example.com
offer0=amount:56.01
currency=USD
```

Example 2 Reply

```
request_id=0305782650000167905080
merchant_ref_number=482046C3A7E94F5BD1FE3C66C
ics_rcode=1
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
pinless_debit_amount=56.01
currency=USD
pinless_debit_rcode=1
pinless_debit_rflag=SOK
pinless_debit_rmsg=Request was processed successfully.
pinless_debit_time=2005-01-27T184955Z
pinless_debit_trans_ref_no=RYXWMQX04MC9
pinless_debit_processor_response=XYZ
pinless_debit_receipt_number=987654
pinless_debit_auth_code=123456
client_lib_version=Perl3.2/MSWin324.0/NT4.0/WIN32/C/3.4.5
```

Sending Requests to the Test System

When testing, send your requests to the CyberSource test system:

- Use the CyberSource test server <http://ics2testa.ic3.com>
Your CyberSource SCMP API client has a configuration setting that allows you to specify whether to send requests to the production or test server.

Testing the PINless Debit Validate Service

You can request the PINless debit validate service on the CyberSource test system and receive the appropriate response for that card number.



The BIN tables that CyberSource uses to identify PINless debit cards are not updated as frequently on the test system as they are on the production system, so do not use the CyberSource test system to validate real cards after you are in production.

Testing the PINless Debit Service

Do not use real card numbers to test the PINless debit services. For Chase Paymentech Solutions and FDMS South, use card number 4002269999999999.

You can use specific amounts to trigger certain responses when sending PINless debit transactions to the CyberSource test system. These triggers work only on the test server, not on the production server. To see the list of trigger amounts and responses for each processor, see [SCMP API Testing Information page](#) on the Support Center.

Product Codes

The following table lists the values that you can use for the product code in the **product_code** offer-level field.

Table 8 Product Codes

Product Code	Definition
adult_content	Adult content.
coupon	Coupon applied to the entire order.
default	Default value for the product code. CyberSource uses <code>default</code> when a request message does not include a value for the product code.
electronic_good	Electronic product other than software.
electronic_software	Software distributed electronically rather than on disks or other media.
gift_certificate	Gift certificate.
handling_only	Fee that you charge your customer to cover your administrative selling costs.
service	Service that you perform for your customer.
shipping_and_handling	The shipping portion is the charge for shipping the product to your customer. The handling portion is the fee you charge your customer to cover your administrative selling costs.
shipping_only	Charge for transporting tangible personal property from your location to your customer. You must maintain documentation that clearly establishes the location where the title to the property passed from you to your customer.
subscription	Subscription to a web site or other content.

Index

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

C

Chase Paymentech Solutions
 PINless debit validations [14](#)
 PINless debits [17](#)
 requirements [8](#)
 credit cards [11](#)
 customer profiles [25](#)

E

examples [27](#)

F

FDMS South
 automatic reversals [13](#)
 PINless debit validations [14](#)
 PINless debits [17](#)
 requirements [8](#)

G

GPN
 payment tokenization [25](#)
 PINless debit validations [14](#)
 PINless debits [17](#)
 recurring billing [26](#)
 requirements [8](#)

I

ics_pinless_debit [17](#)
 ics_pinless_debit_validate [14](#)

P

payment tokenization [25](#)
 product codes [30](#)
 profiles [25](#)

R

reconciliation [12](#)
 recurring billing [26](#)
 request IDs [12](#)
 reversals, automatic [13](#)

S

samples [27](#)
 secure data [25](#)
 secure storage [25](#)
 subscriptions [26](#)

T

test servers [28](#)
 timeouts [13](#)
 transaction reference numbers [12](#)

V

validations [14](#)