

Apple Pay

SCMP API

JCN Gateway

Developer Guide



© 2021. 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 Unpublished rights reserved under the copyright laws of the United States.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

Authorize.Net, eCheck.Net, and The Power of Payment are registered trademarks of Cybersource Corporation. Cybersource, Cybersource Payment Manager, Cybersource Risk Manager, Cybersource Decision Manager, and Cybersource Connect are trademarks and/or service marks of Cybersource Corporation. Visa, Visa International, Cybersource, the Visa logo, and the Cybersource logo are the registered trademarks of Visa International in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Version: 21.05

Contents

- Recent Revisions to This Document..... 4**
- About This Guide..... 5**
- Getting Started.....6**
 - Requirements for Using Apple Pay.....6
 - Supported Processors.....7
 - Enrolling in Apple Pay.....7
 - Generating a New CSR.....8
 - Transaction Request Report..... 8
- Apple Pay Integrations..... 10**
 - In-App Transactions Using the Cybersource API.....10
 - Cybersource Decryption (In-App Transactions)..... 11
 - Merchant Decryption (In-App Transactions)..... 12
 - Web Transactions.....13
 - Cybersource Decryption (Web Transactions)..... 14
 - Merchant Decryption (Web Transactions)..... 15
 - Configuring Your Apple Pay Requirements..... 15
 - Setting Up Apple Pay JavaScript..... 17
- Requesting Services..... 19**
 - Requesting the Authorization Service..... 19
 - Using Our Decryption Method..... 19
 - Using the Merchant Decryption Method..... 22
 - Requesting Additional Services..... 24
- API Fields..... 25**

Recent Revisions to This Document

21.05

This revision contains only editorial changes and no technical updates.

21.04

Changed the name of the **merchant_url** field to **merchant_domain_name**. See the [API Field Reference for the SCMP API](#).

21.03

Added the **tms_network_token_option** field. See the [API Field Reference for the SCMP API](#).

21.02

Updated the **card_type** field. See the [API Field Reference for the SCMP API](#).

21.01

Added the **merchant_url** field. See the [API Field Reference for the SCMP API](#).

20.03

Updated information about recurring payments. See [Supported Processors](#).

20.02

This revision contains only editorial changes and no technical updates.

20.01

This revision contains only editorial changes and no technical updates.

About This Guide


This section provides you with information about the structure and content within this guide.


Audience and Purpose

This document is written for merchants who want to use Apple Pay in an iOS application and use information from Apple to process payments through Cybersource. This document provides an overview for integrating Apple and Cybersource services into an order management system.

Conventions

The following special statements are used in this document:

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

 **Warning:** A *Warning* contains information or instructions, which, if not heeded, can result in a security risk, irreversible loss of data, or significant cost in time or revenue or both.

Related Documentation

For further technical documentation, visit the Cybersource Technical Documentation Portal:

<https://docs.cybersource.com/en/index.html>

Customer Support

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

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

Getting Started

Requirements for Using Apple Pay

In order to use the Cybersource platform to process Apple Pay transactions, you must have:

- A Cybersource account.

If you do not already have a Cybersource account, contact your local Cybersource sales representative.

- A merchant account with a supported processor. See [Supported Processors](#).
- An *Admin* or *Team Agent* user of the [Apple Pay Developer](#) account.

Important:

Apple Pay relies on authorizations with payment network tokens. You can sign up for Apple Pay only when both of the following statements are true:

- Your processor supports payment network tokens.
- Cybersource supports payment network tokens with your processor.

If one or both of the preceding statements are not true, you must take one of the following actions before you can sign up for Apple Pay:

- Obtain a new merchant account with a processor that supports payment network tokens.
- Wait until your processor supports payment network tokens.

Related information

[Supported Processors](#)

Supported Processors

Merchant-initiated transactions, multiple partial captures, and subsequent authorizations are described in the *Authorizations with Payment Network Tokens* guide. Recurring payments and split shipments are described in the *Credit Card Services* guide.

Processor	Card Types	Optional Features
JCN Gateway	<ul style="list-style-type: none">• JCB	<ul style="list-style-type: none">• Multiple partial captures• Subsequent authorizations


Related information

[Authorizations with Payment Network Tokens Developer and Credit Card Services guides \(available on the Payment Services > Credit Card Services page\)](#)

Enrolling in Apple Pay

1. Log in to the Business Center:
 - Test: <https://ebctest.cybersource.com/ebc2>
 - Production: <https://ebc.cybersource.com/ebc2>
2. On the left navigation panel, click the **Payment Configuration** icon.
3. Click **Digital Payment Solution**. The Digital Payments page appears.
4. Click **Configure**. The Apple Pay Registration panel opens.
5. Enter your Apple Merchant ID.
6. Click **Generate New CSR**.
7. To download your CSR, click the **Download** icon next to the key.
8. Follow your browser's instructions to save and open the file.
9. Complete the enrollment process by submitting your CSR to Apple.

10. For information about adding certificates to your Apple Merchant ID, refer to the Apple Pay PassKit: <https://developer.apple.com/documentation/passkit>.
11. Test your software by following the steps in [Requesting the Authorization Service](#).

 **Important:** If you are using a Cybersource test account, you must connect to the Apple developer system and not to the Apple production system.

After you complete your testing, you must create a new CSR for the Cybersource production system, and you must use that CSR for the Apple production system. Until you perform these steps, you cannot enable payments in your iOS application.

12. Repeat Steps 1 through 11 with your Cybersource production account and the Apple production account.

Generating a New CSR

1. Log in to the Business Center:
 - Test: <https://ebctest.cybersource.com/ebc2>
 - Production: <https://ebc.cybersource.com/ebc2>
2. On the left navigation panel, click the **Payment Configuration** icon.
3. Click **Digital Payment Solution**. The Digital Payments page appears.
4. Click **Configure**. The Apple Pay Registration panel opens.
5. To download your CSR, click the **Download** icon next to the key.
6. Follow your browser's instructions to save and open the file.
7. To edit your Apple Merchant ID, click the **Edit** icon. The Edit CSR panel opens.
8. Modify your merchant ID as necessary, and click **Update**.

Transaction Request Report

Through the Business Center, you can use the Transaction Request Report to obtain information about your transactions:

- Use the Transaction Search page to identify Apple transactions. You can search for transactions by date, application type, customer name, and other transaction identifiers.

- For information about the Transaction Request Report, see the [Business Center Reporting User Guide](#).

Apple Pay Integrations

In-App Transactions Using the Cybersource API

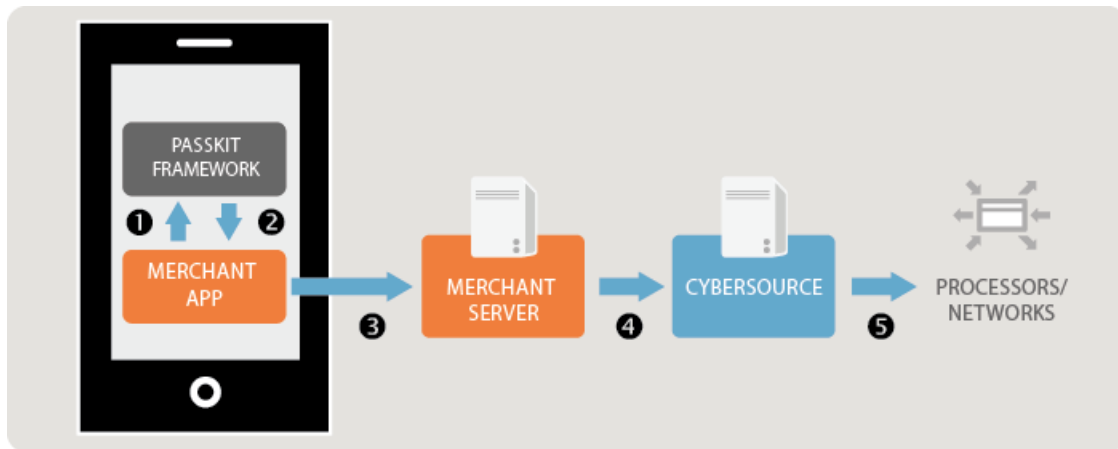
This section describes how in-app transactions are processed using the Cybersource API:

- [Cybersource Decryption \(In-App Transactions\)](#)
- [Merchant Decryption \(In-App Transactions\)](#)

For information about processing web transactions, refer to:

- [Cybersource Decryption \(Web Transactions\)](#)
- [Merchant Decryption \(Web Transactions\)](#)

Cybersource Decryption (In-App Transactions)



1. When the customer chooses to pay with Apple Pay, you use the Apple PassKit Framework to request the encrypted payment data from Apple.
2. Apple uses the Secure Element to create a payment token (the **PKPaymentToken** structure) and encrypt the token's payment data (the **paymentData** field of the **PKPaymentToken** structure) before it sends your application.
3. You forward the encrypted payment data to your order management system.
4. Using the Cybersource API, you submit the authorization request. In the **encrypted_payment_data** field, include the Base64-encoded value obtained from the **paymentData** field of the **PKPaymentToken** structure.
5. Cybersource decrypts the payment data and forwards the information to the payment network, which includes your processor and the relevant payment card company.

! Important: You must use the Business Center or one of the Cybersource API services to capture, credit, or void the authorization. Refer to the *Credit Card Services* guide (see Related information below) for information.

Related information

[Requesting the Authorization Service for JCB Transactions \(Cybersource Decryption\)](#)
[Credit Card Services guide on Payment Services > Credit Card Services page](#)

Merchant Decryption (In-App Transactions)



1. When the customer chooses to pay with Apple Pay, you use the Apple PassKit Framework to request the encrypted payment data from Apple.
2. Apple uses the Secure Element to create a payment token (the **PKPaymentToken** structure) and encrypt the token's payment data (the **paymentData** field of the **PKPaymentToken** structure) before it sends your application.
3. You forward the encrypted payment data to your order management system to decrypt. For information on decryption, see: https://developer.apple.com/library/archive/documentation/PassKit/Reference/PaymentTokenJSON/PaymentTokenJSON.html#//apple_ref/doc/uid/TP40014929-CH8-SW1
4. Using the Cybersource API, you submit the authorization request and include the decrypted payment data.
5. Cybersource forwards the information to the payment network, which includes your processor and the relevant payment card company.

! Important: You must use the Business Center or one of the Cybersource API services to capture, credit, or void the authorization. Refer to the *Credit Card Services* guide (see Related information below) for information.

Related information

[Requesting the Authorization Service for JCB Transactions \(Merchant Decryption\)](#)

[Credit Card Services guide on Payment Services > Credit Card Services page](#)

Web Transactions

This section describes how web transactions are processed using the Cybersource API:


- [Cybersource Decryption \(Web Transactions\)](#)
- [Merchant Decryption \(Web Transactions\)](#)

For information about processing in-app transactions, refer to:

- [Cybersource Decryption \(In-App Transactions\)](#)
- [Merchant Decryption \(In-App Transactions\)](#)

Cybersource Decryption (Web Transactions)

1. When the customer chooses to pay with Apple Pay, you use the Apple Pay JavaScript to request the encrypted payment data from Apple.
2. Apple uses the Secure Element to create a payment token (the **PKPaymentToken** structure) and encrypt the token's payment data (the **paymentData** field of the **PKPaymentToken** structure) before it sends your application using the **onpaymentauthorized** callback function.
3. You forward the encrypted payment data to your order management system.
4. Using the Cybersource API, you submit the authorization request. In the **encrypted_payment_data** field, include the Base64-encoded value obtained from the **paymentData** field of the **PKPaymentToken** structure.
5. Cybersource decrypts the payment data and forwards the information to the payment network, which includes your processor and the relevant payment card company.


 **Important:** You must use the Business Center or one of the Cybersource API services to capture, credit, or void the authorization. Refer to the *Credit Card Services* guide (see Related information below) for information.

Related information

[Credit Card Services guide on the Payment Services > Credit Card Services page](#)

Merchant Decryption (Web Transactions)

1. When the customer chooses to pay with Apple Pay, you use the Apple Pay JavaScript to request the encrypted payment data from Apple.
2. Apple uses the Secure Element to create a payment token (the **PKPaymentToken** structure) and encrypt the token's payment data (the **paymentData** field of the **PKPaymentToken** structure) before it sends your application using the **onpaymentauthorized** callback function.
3. You forward the encrypted payment data to your order management system to decrypt. For information on decryption, see: https://developer.apple.com/library/archive/documentation/PassKit/Reference/PaymentTokenJSON/PaymentTokenJSON.html#//apple_ref/doc/uid/TP40014929-CH8-SW1
4. Using the Cybersource API, you submit the authorization request and include the decrypted payment data.
5. Cybersource forwards the information to the payment network, which includes your processor and the relevant payment card company.

 **Important:** You must use the Business Center or one of the Cybersource API services to capture, credit, or void the authorization. Refer to the *Credit Card Services* guide (see Related information below) for information.

Related information

[Credit Card Services guide on the Payment Services > Credit Card Services page](#)

Configuring Your Apple Pay Requirements

Refer to <https://developer.apple.com/develop> for details about configuring your requirements.

1. Register your merchant ID.

If you are currently processing In-App transactions, you can use the same merchant ID for processing web transactions.

2. Create or upload a Certificate Signing Request (CSR), which is used to encrypt the payment information during the payment process.

If you are using the merchant decryption method, generate a new CSR.

If you are using the Cybersource decryption method, upload the CSR that you created in the Business Center when you enrolled in Apple Pay.

If you are currently processing In-App transactions, you can use the same CSR for processing web transactions.

3. Register your domain. Registration is required in order to use Apple Pay on your website.
4. Create a Merchant Identity Certificate. This certificate is required in order to connect to the Apple servers.

After configuring your Apple Pay requirements, you can set up any optional features (refer to the *Authorizations with Payment Network Tokens* guides).

Related information

[Authorizations with Payment Network Tokens guides \(available on the Payment Services > Credit Card Services page\)](#)

[Enrolling in Apple Pay](#)

[Generating a New CSR](#)

Setting Up Apple Pay JavaScript

Preparing to use Apple Pay JavaScript to accept payments on your website involves several stages of development. This section is an overview of those stages. For detailed instructions, follow the references to the Apple developer site.

- **Enabling the Apple Pay JavaScript API:**

Before you can display an Apple Pay button on your website or create an Apple Pay session, you need to ensure that the Apple Pay JavaScript API is enabled on your device. See [Enabling the Apple Pay JavaScript API](#).

- **Displaying the Apple Pay button:**

Use the CSS templates provided by Apple to display the Apple Pay button on your website. See the Apple developer documentation on [Displaying Apple Pay Buttons Using CSS](#) for more information.

- **Creating the `ApplePaySession` class and object:**

The **`ApplePaySession`** class manages the payment process on your website. The **`ApplePaySession`** object is the entry point for Apple Pay on your website. See Apple's Developer article: For information about creating the **`ApplePaySession`** object, see the Apple developer reference on the [ApplePaySession](#) class.

To create the **`ApplePaySession`** object:

- Use the **Version number** and **Payment request** arguments. The API version is 1. See the Apple developer reference on the [ApplePayPaymentRequest](#) structure for information on how to display the payment form.
- After creating the **`ApplePaySession`**, call its **`begin`** method to display the payment form. You can call this method only when invoked by a user request. See the Apple developer reference on the [begin](#) method for details.

- **Getting merchant validation:**

When the payment form is displayed, the **`onvalidatemerchant`** callback function is called and provides a URL to pass to your server for validating the merchant session. See the Apple developer reference on [onvalidatemerchant](#). Also, refer to the Merchant Validation section of the Apple developer reference on the [ApplePaySession](#) class.

- **Handling payment confirmation:**

When the customer confirms the payment by clicking or tapping the Apple Pay button, the **`onpaymentauthorized`** callback function is invoked and provides the payment token. See the Apple developer reference on the [onpaymentauthorized](#) instance.

- **Handling encrypted payment data:**

The following two methods are available for handling encrypted payment data for Apple Pay transactions:

- **Merchant Decryption:**

This method forwards the encrypted payment data to your order management system to decrypt. For information on decryption, see the Apple [Payment Token Format Reference](#) for details. You use the Cybersource API to submit the authorization request and include the decrypted payment data.

- **Cybersource Decryption:**

This method forwards the encrypted payment data to your order management system. You use the Cybersource API to submit the authorization request and include the Base64-encoded value obtained from the **paymentData** object in the **encrypted_payment_data** field.

For example:

```
session.onpaymentauthorized = function (event) {  
    var paymentDataString =  
    JSON.stringify(event.payment.token.paymentData);  
    var paymentDataBase64 = btoa(paymentDataString);  
}
```

Enabling the Apple Pay JavaScript API

1. Verify that the **window.ApplePaySession** class exists.

2. Calls one of the following methods:

- **canMakePayments**—verifies that the device is enabled for Apple Pay.
- **canMakePaymentsWithActiveCard**—verifies that the device is enabled for Apple Pay and the customer has a card stored on the device. You can call this method only if Apple Pay is the default payment method during your checkout flow, or if you want to add the Apple Pay button to your product detail page.

Requesting Services

Requesting the Authorization Service

You can request the authorization service using the Cybersource decryption method or the merchant decryption method.

Related information

[Requesting the Authorization Service for JCB Transactions \(Cybersource Decryption\)](#)

[Requesting the Authorization Service for JCB Transactions \(Merchant Decryption\)](#)

Using Our Decryption Method

Requesting the Authorization Service for JCB Transactions (Cybersource Decryption)

1. Set the **encrypted_payment_data** field to the Base64-encoded value obtained from the **paymentData** property of the **PKPaymentToken** object.
2. Set the **encrypted_payment_descriptor** field to `Rk1EPUNPTU1PTi5BUFBMR5JTkFQUC5QQV1NRU5U`.
3. Set the **payment_solution** field to `001`.

Related information

[API Field Reference for the SCMP API](#)

[Cybersource Decryption \(In-App Transactions\)](#)

[Cybersource Decryption \(Web Transactions\)](#)

[Relaxed Requirements for Address Data and Expiration Date](#)

Example (Cybersource Decryption)

Request (JCB Transactions)

```
bill_address1=123 Main Street
bill_address2=Suite 12345
bill_city=Small Town
bill_country=US
bill_state=CA
bill_zip=98765
card_type=007
currency=USD
customer_cc_expmo=12
customer_cc_expyr=2031
customer_cc_number=555555555555xxxx
customer_email=js@example.com
customer_firstname=Jane
customer_lastname=Smith
customer_phone=999-999-9999
eci_raw=05
grand_total_amount=100.00
ics_applications=ics_auth
merchant_id=med123
cavv=EHuWW9PiBkWvqE5juRwDzAUFBAk=
payment_solution=001
```

Response (JCB Transactions)


```
request_token=Ahj/7wSR5C/p6oJEylgKIkGLNkwcsmrWHHlU5tGHST/hHgzdACT/hVB3c
currency=USD
request_id=4465838340055000001541
auth_rflag=SOK
ics_rmsg=Request was processed successfully.
auth_auth_amount=100.00
auth_rcode=1
auth_trans_ref_no=13209255CGJSMQCR
auth_auth_code=888888
auth_rmsg=Request was processed successfully.
ics_rflag=SOK
auth_auth_response=100
auth_avs_raw=I1
auth_auth_time=2015-11-03T205035Z
merchant_ref_number=ref123
ics_rcode=1
token_prefix=128945
token_suffix=2398
```

```
token_expirationMonth=08  
token_expirationYear=2021
```

Using the Merchant Decryption Method

Requesting the Authorization Service for JCB Transactions (Merchant Decryption)

1. Set the **customer_cc_number** field to the payment network token value.
2. Set the **customer_cc_expmo** and **customer_cc_expyr** fields to the values from the payment network token expiration date.
3. Set the **cavv** field to the 3D Secure cryptogram of the payment network token.

 **Important:** Include the whole 20-byte cryptogram in the **cavv** field. For a 40-byte cryptogram, split the cryptogram into two 20-byte binary values (block A and block B). Set the **cavv** field to the block A value and set the **xid** field to the block B value.

4. Set the **eci_raw** field to the ECI value contained in the Apple Pay response payload.
5. Set the **payment_network_token_transaction_type** field to [1](#).
6. Set the **payment_solution** field to [001](#).

Related information

[API Field Reference for the SCMP API](#)

[Merchant Decryption \(In-App Transactions\)](#)

[Merchant Decryption \(Web Transactions\)](#)

[Relaxed Requirements for Address Data and Expiration Date](#)

Example (Merchant Decryption)

Authorization Request (JCB Transactions)

```
bill_address1=123 Main Street
bill_address2=Suite 12345
bill_city=Small Town
bill_country=US
bill_state=CA
bill_zip=98765
card_type=007
currency=USD
customer_cc_expmo=12
customer_cc_expyr=2031
customer_cc_number=356611111111xxxx
customer_email=js@example.com
customer_firstname=Jane
customer_lastname=Smith
customer_phone=999-999-9999
eci_raw=05
grand_total_amount=100.00
ics_applications=ics_auth
merchant_id=med123
cavv=EHuWW9PiBkWvqE5juRwDzAUFBAk=
payment_network_token_transaction_type=1
payment_solution=001
```

Authorization Response (JCB Transactions)

```
auth_auth_amount=100.00
auth_auth_avs=X
auth_auth_code=888888
auth_auth_response=100
auth_avs_raw=I1
auth_rcode=1
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_trans_ref_no=15356268CR2XF23X
currency=USD
ics_rcode=1
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
merchant_ref_number=ref123
request_id=4697369268106124601541
request_token=Ahj/7wSR/UoVm1bMmziHSZjMECT/h+KjMHSB04gwGA2dDjQoxQAAA6xdr
```

Requesting Additional Services

To request the following additional services, refer to the *Credit Card Services* guide (see Related information below):

- **Capture:** A follow-on service that uses the request ID returned from the previous authorization. The request ID links the capture to the authorization. This service transfers funds from the customer's account to your bank and usually takes two to four days to complete.
- **Sale:** A sale is a bundled authorization and capture. Request the authorization and capture services at the same time. Cybersource processes the capture immediately.
- **Authorization Reversal:** A follow-on service that uses the request ID returned from the previous authorization. An authorization reversal releases the hold that the authorization placed on the customer's credit card funds. Use this service to reverse an unnecessary or undesired authorization.

Related information

[Credit Card Services guide on the Payment Services > Credit Card Services page](#)

[Authorizations with Payment Network Tokens guide > Digital Payment Solutions page](#)

API Fields

See the [API Field Reference guide](#) for your API type.