SHIFT4

API Specifications

Payment Page Services - Code

Version 2.6 rev 1 | May 2024

Contents

Introduction

The Code Hosted Payment Page (HPP) solution is part of Shift4's payment page services. It enables eCommerce merchants to securely accept payments, as well as fully control their payment page design and cu stomer experience.

The purpose of this document is to provide an in-depth description of the Code payment page solution.

Useful Documents / References

The following documents may be useful in understanding the Code HPP:

- *Source Payment Gateway API* – The Source Payment API specification provides detailed information on processing card-not-present transactions.
- *Source / Credorax Data Transfer Interface* – In-depth description of the Data Transfer Interface and format specifications of the reports provided by Credorax.

These documents can be found on the Shift4's Developers Portal.

Intended Audience

This document is intended for eCommerce merchants wishing to implement the Code HPP solution on their websites to accept payments.

Certification

All new implementations must undergo appropriate certification to ensure the quality of integrations and integrity of merchant data. Please note that only test-card data should be used for testing.

Additional certification will be required if new services or features are to be used.

Publication Identification

Overview

The Code Hosted Payment Page (HPP) solution enables merchants to design their own payment page without storing sensitive PCI data on their servers, using a simple Javascript code. The payment data is encrypted on Shift4 systems and never goes through the merchant's servers, which significantly reduces the merchant's PCI compliance requirements.

How it works

The solution requires implementation of client Javascript and server-to-server RESTful API calls. Transaction requests are sent online and in real-time. The card data is transferred to Shift4 servers, where it is encrypted using a temporary key. The key is then transmitted back to the merchant's server to complete the checkout process.

The Code HPP solution supports requests for Authorisation, Sale and Token transactions, with or without 3D Secure functionality.

Note: Referral transactions, such as refund, void and capture, can be performed through Shift4's Source Payment Gateway API or through the 'Insights' customer portal.

Additional Supported services

Each additional supported service require registration with Shift4.

Contact your account manager for more details.

3D Secure

3D Secure (3-Domain Secure) is an advanced method for performing Strong Customer Authentication (SCA) in card-not-present transactions. Using 3D-secure successfully may protect you from fraud chargeback disputes raised by cardholders and issuers. Refer to Appendix F: 3D Secure for more details.

SmartGuard

SmartGuard is an anti-fraud protection service that protects your revenue by assessing fraud activity in real time. Powered by Machine Learning technology and fraud rule engine capabilities, the SmartGuard service accurately identifies fraudulent payments, so that you can accept more legitimate payments and reduce your false-positive rate. The SmartGuard service offers two plans:

1. **SmartGuard**: An automatic solution using Machine Learning technology
2. **SmartGuard Plus**: A customised solution where you can control and manage your anti-fraud protection settings based on data-driven decisions

For more information, please refer to the SmartGuard Fraud Protection API on Shift4's Developer Portal.

Addresses

Integration addresses:

API call name	Address
Javascript	https://ppskey-int.credorax.com/keypayment/v2/keycreation.js
Store (any)	https://ppskey-int.credorax.com/keypayment/rest/v2/store
Payment	https://pps-int.credorax.com/keypayment/rest/v2/payment?

Production addresses:

API call	Address
Javascript	https://ppskey.credorax.net/keypayment/v2/keycreation.js
Store (any)	https://ppskey.credorax.net/keypayment/rest/v2/store
Payment	https://pps.credorax.net/keypayment/rest/v2/payment?

HTTP Specification

- Protocol: HTTPS
- Method: POST
- Content-Type: [application/www-form-urlencoded] or [application/x-www-form-urlencoded]

Example HTTP Request

```
POST /intenv/service/gateway HTTP/1.1

Host: intconsole.credorax.com

Content-Type: application/x-www-form-urlencoded Content-Length: 176

M=8632876&Pkey=jhdyr56j784jf574gf6598s346dff63jg&K=9823ou1pwieufdp91873p98723rp9872

38r97p198r&O=1&a1=7894654&a4=1099&b1=45454545454054545&b2=1&b3=08&b4=11&b5=003&c1=John+Smith&c3=johnsmith@yahoo.com&d1=111.222.0.101
```

Security/Authentication

A secured channel should be used for server-to-server HTTP requests sent over TLS. The Shift4 Payment Gateway does not authenticate the TLS session using a certificate from the client, thus a non-authenticated TLS session is used. Instead, the client is first authenticated using its source IP and then a secondary authentication check is performed using a SHA256 message cipher which is sent in the request payload and used for verification before processing is approved.

See Appendix A: Message Cipher for further details.

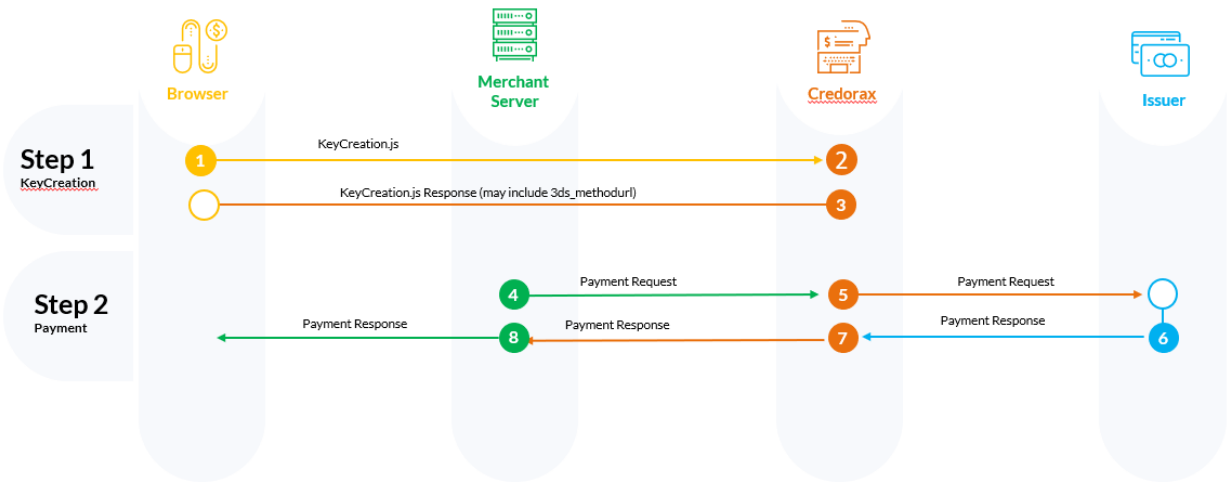
Code HPP Specifications

Step by Step Payment

The Code HPP solution includes two main steps:

1. **Payment key creation** – Merchant sends a request for a Payment key (Pkey) in order to encrypt PCI data (payment card data)
2. **Payment initiation** – Payment is initiated using the encrypted payment data

Transaction Flow Diagram



3D Secure Flow

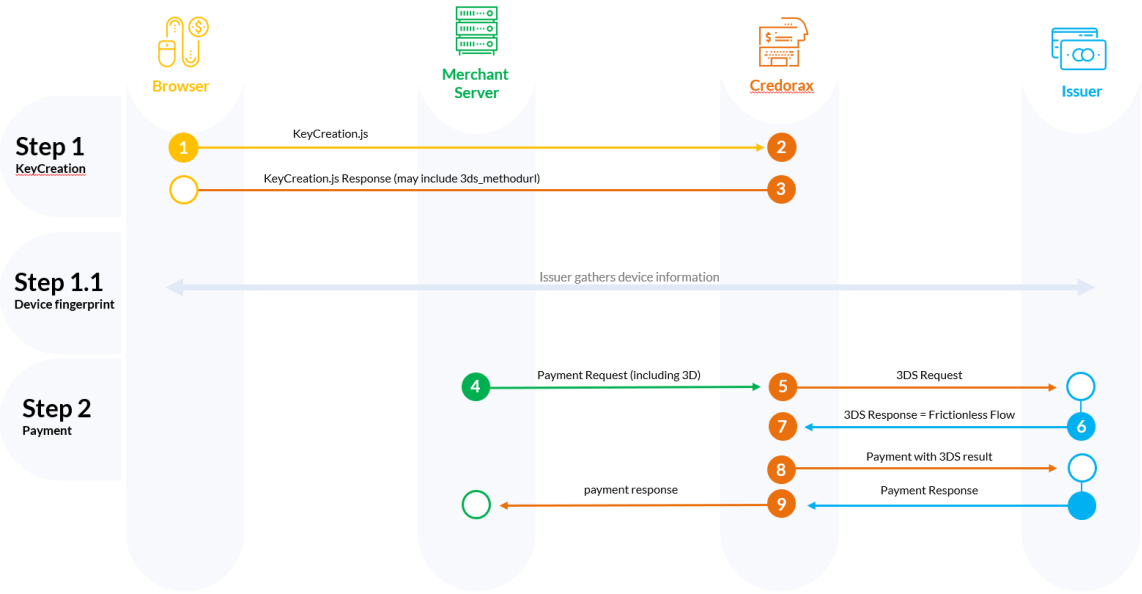
To add a 3D secure layer, you can enforce 3D secure authentication. The 3D Secure authentication is fully controlled and managed by Shift4 as part of the transaction flow, however additional steps may be required on your side. Using 3D Secure requires more parameters at the request level, and additional parameters are returned in the response.

Using Code HPP with 3D secure functionality contains up to four steps:

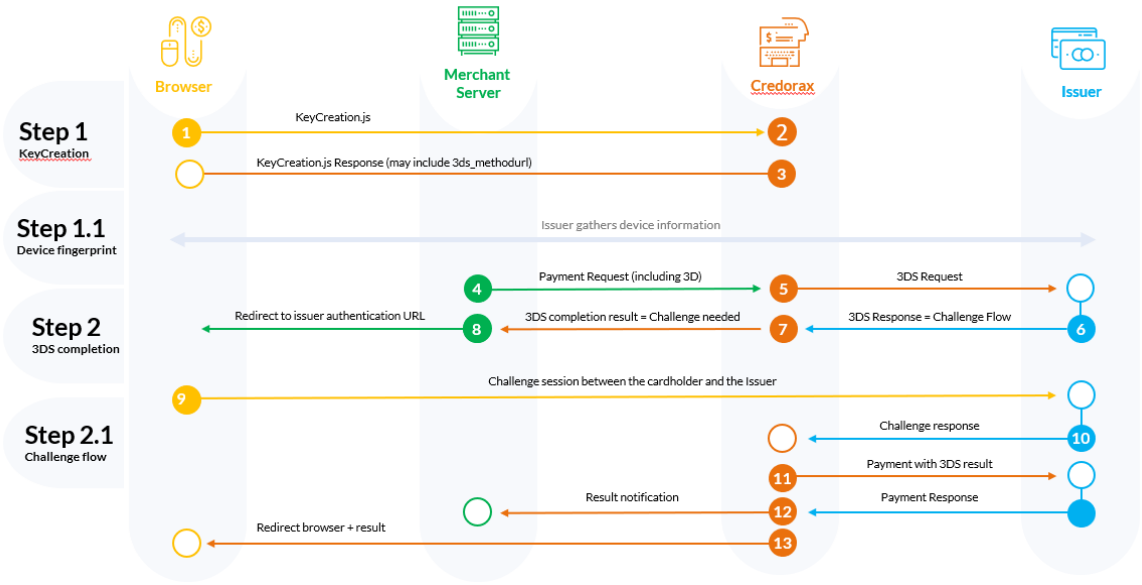
1. **Payment key creation** – Merchant sends a request for a Payment key (Pkey) in order to encrypt PCI data (payment card data)
   a. The issuer may want to collect a device fingerprint as part of the 3D secure process. In this case you need to access the URL provided as part of the response to step 1. See Device fingerprint information retrieval flow for more information.
2. **Payment initiation with 3D secure** – Payment is initiated using the encrypted payment data. If you request to enforce 3D secure, 3D secure is initiated before the payment.

a. The issuer may decide that further cardholder authentication is needed. See Initiating 3D Secure Cardholder challenge for instructions how to implement this step.

Frictionless Flow Diagram



Challenge Flow Diagram



Code HPP API

Step 1 - Payment Key Creation

The Payment key creation API call creates a Payment key (PKey) encrypting the PCI data (payment card data) by using JavaScript on the client side. Embed the following JavaScript in your web page before the end of the `<body>` element:

```
<script src="https://ppskey-
int.credorax.com/keypayment/v2/keycreation.js"></script>keyCreation("M
", "RequestId", "staticKey", "b1", "b3", "b4", "b5", "c1");
```

pass the input parameters to the KeyCreation function.

Note: Make sure you never pass or store PCI data on your server.

PCI data includes the card number, expiry date and CVV.

Request Parameters

Field	Type	Min	Max	m/o/c	Description
M	[A-Z0-9_]	3	8	m	Shift4 assigned gateway merchant ID.
RequestID	[a-zA-Z0-9\-]	36	36	o	Merchant request ID used for your reference. If sent, the value will be returned in the response's ResponseID field, and can be used for tracking and error handling.
Statickey	[0-9A-Za-z]	1	32	m	A key provided to you during onboarding.
b1	[0-9]	8	19	c	PAN – Primary Account Number.
b3	[0-9]	2	2	c	Card expiry month. Two-digit number (format mm).
b4	[0-9]	2	2	c	Card expiry year. Two-digit number (format yy).
b5	[0-9]	3	4	c	Card security code (CVV / CVC) as printed on the card

Field	Type	Min	Max	m/o/c	Description
c1	[\ a-zA-Z]	5	50	c (recommended – when initiating 3D secure transaction, m for Visa 3DS transactions)	Cardholder's full name. The minimum length of this field is five characters. If the cardholder provides a name with less than five characters (e.g., Mr. Lu), you must either add additional non-space characters or not send the field.

Response Parameters

Field	Type	Min	Max	m/o/c	Comment
M	[A-Z0-9_]	3	8	m	Shift4 assigned gateway merchant ID.
ResponseID	[a-zA-Z0-9\-]	36	36	o	If RequestID was sent in the request, this field contains the value sent in it.
PKey	[a-zA-Z0-9\-]	32	32	o	Unique key replacing the PCI data.
z2	[0-9]	1	4	m	Response code. For possible values refer to Appendix B - Response code table.
z3	Text	1	256	m	Response code description. For possible values refer to Appendix B Response code table.
3ds_method	Text	1	2048	o	The issuer's URL that should be used to trigger the collection of the device fingerprint by the issuer
3ds_version	[0-9. /]	3	3	o	Indicates whether the 3D secure version is 1.0 or 2.0
3ds_trxid	[a-zA-Z0-9, -]	36	36	o	Universally unique transaction identifier to identify a single 3D Secure transaction.

store API call

For mobile applications where JavaScript cannot be used, we recommend using the 'store' API call, as shown in the following example:

Method: POST

Path: …/keypayment/rest/v2/store

Headers: Content-Type: application/x-www-form-urlencoded

Parameters location: BODY

Request

```
{
“M” =”XTETEST”,
“RequestID” =”586168338”,
“Statickey” =”12345”,
“b1” =”5223450000000007”,
“b3” =”12”,
“b4” =”25”,
“b5” =”090”,
“c1” =” John Snow”
}
```

Response

```
{
PKey: 34de8833f85540cd8124e084dd703061
z2: 0
z3: Transaction has been executed successfully.
ResponseID: 586168338
}
```

Step 2 – Initiate Payment

In this step, the merchant initiates the payment using the payment key (PKey) generated in step 1. The payment can either include the 3D Secure functionality or a regular TLS message.

Note: The parameters need to be sent as part of the URL

Service name: payment

Request Parameters

Field	Type	Min	Max	m/o/c	Description
PKey	[a-zA-Z0-9\-]	32	32	m	PCI data unique identifier
M	[A-Z0-9_]	3	8	m	Shift4 assigned gateway merchant ID
K	[0-9A-Za-z]	1	32	m	Unique cipher used to authenticate requests Refer to Appendix A: Message Cipher for further details on generating the cipher.
3ds_initiate	[0-3]	2	2	o	Indicates whether to initiate the Source 3D Secure Authentication process. Possible values are: 01: Initiate 3D Secure before completing the payment 02: Process payment without initiating 3D Secure 03: Initiate 3D Secure according to the 3DS Adviser result 04: Only initiate the 3DS Adviser service. Relevant only for op code 98. For additional information about the 3D Secure process, see Appendix F: 3D secure
3ds_compind	[Y,N]	1	1	o	The response received from the issuer after accessing the URL specified in 3ds_method. Indicates whether device fingerprint collection completed successfully.

Field	Type	Min	Max	m/o/c	Description
O	[0-9]	2	2	m	Operation Code: 1: Sale 2: Authorisation 10: Create Token 11: Use Token Sale 12: Use Token Authorisation 23: Create Token with Sale 28: Create Token with Authorisation
a1	[0-9A-Za-z]	1	32	m	Request ID. A unique transaction reference number. This should be unique per transaction per MID.
a4	[0-9]	1	12	m	Requested billing amount. Two exponents are used, without a decimal, except for currencies with zero exponents. Refer to Appendix F: Transaction currencies in the Source Gateway Payment API document. For example, when paying 10.00 GBP, the value should be sent as 1000. When paying 10 JPY, the value should be sent as 10.
a5	[A-Z]	3	3	m	The ISO 4217 numeric currency code for the transaction. Refer to ISO 4217-alpha-3. For the supported Shift4 currency list, refer to Appendix F: Transaction currencies in the Source Gateway Payment API document.
a6	yyMMdd	6	6	m	Transaction date (Local date when transaction was generated).
a7	HHmmss	6	6	m	Transaction time (Local time when transaction was generated).

Field	Type	Min	Max	m/o/c	Description
a9	[0-9]	1	2	o	Transaction type. Valid values are: Value — Description 1 — First recurring 2 — Subsequent recurring 5 — Card-Only Validation 6 — Straight Operation 8 — Unscheduled Card-on-File transactions initiated by the merchant 9 — Unscheduled Card-on-File transactions initiated by the cardholder 10 — Card validations for an unscheduled Card-on-File Note: By default, the transaction type is considered a straight operation unless specified otherwise.
b2	[0-9]	1	2	o	Valid options are: 0: Unknown 1: Visa 2: MasterCard 9: Maestro

Field	Type	Min	Max	m/o/c	Description
c1	[\ a-zA-Z]	5	50	c (recommended – when initiating 3D secure transaction, m for Visa 3DS transactions)	Cardholder's full name. The minimum length of this field is five characters. If the cardholder provides a name with less than five characters (e.g., Mr Lu), you must either add additional non-space characters or not send the field.
c2	[0-9\-]	5	32	c, m for Visa 3ds transactions, o if c3 is sent.	Cardholder's contact phone number (e.g., 999-999-9999). For Visa 3ds transactions cardholder's phone number or email are mandatory.
c3	email	7	64	c, m for Visa 3ds transactions, o if c2 is sent.	Cardholder's email address. The format of the email should be sent as a valid email address, for example: joe@bloggs.com. For Visa 3ds transactions cardholder's phone number or email are mandatory.

Field	Type	Min	Max	m/o/c	Description
c4	[0-9]	1	16	o	Cardholder's billing address street number. If sent, this value will be sent to the issuer and forms part of their AVS checks. If this parameter value is sent, the street number should be omitted from the c5 parameter.
c5	[a-zA-Z0-9\ \-]	4	50	o	Cardholder's billing address street name. Street number should not be included here if the c4 parameter is sent.
c7	[a-zA-Z\ \-]	3	30	o	Cardholder's billing address city name.
c8	[a-zA-Z0-9]	1	3	o	Cardholder's billing address territory code, level 2 country subdivision code according to ISO-3166-2. A reference list can be found at ISO 3166-1-alpha-2.
c9	[A-Z]	2	2	o	Cardholder's billing address country code. Refer to ISO 3166-1-alpha-2.
c10	[a-zA-Z0-9\ \-]	1	9	o	Cardholder's billing address postal/zip code. Any "-"or other special character must be removed prior to sending. If sent, this value will be sent to the issuer and forms part of their AVS checks.
d2	text	3	128	o	Echo parameter. Any value up to 128 bytes long that is sent with a request will be returned within the response.
f21	[0-1]	1	1	o	Boolean field specifying whether to bypass the fraud protection service check. True= Do not send for a fraud check. False or N/A= Send for a fraud check. This is the default value. Available only for merchants using the 'SmartGuard Plus' anti-fraud service.
f22	[0-9]	0	4	o	Sets an ad-hoc threshold for the specific transaction. The threshold must be a value between 0 and 1000. Available only for merchants using the 'SmartGuard Plus' anti-fraud service.

Field	Type	Min	Max	m/o/c	Description
g1	[a-zA-Z0-9]	1	32	o	Token. Token, generated by Shift4, that references a stored card profile.
g6	[0-9A-Za-z]	13	15	o	Initial transaction ID The z50 parameter that was received in the original transaction response. Must be sent to ensure the transaction is considered an MIT transaction. If the transaction is an MIT and the original transaction was prior to 14.9 send the following value: 999999999999999
h3	[0-9]	1	15	o	Sub-Merchant ID. The merchant ID of a sub-merchant that belongs to a Payment Facilitator Refer to Source Payment Gateway: Processors Specification to learn which Payment Processors support Payment Facilitators.
h9	text	1	32	o	Merchant reference number. This optional field is a secondary transaction reference number which can be sent in addition to a1.
i1	text	5	64	o	Free text description of the transaction.

Field	Type	Min	Max	m/o/c	Description
i2	text	1	39	c	Only relevant for merchants with a dynamic descriptor. A Billing Descriptor is a descriptor that appears on the cardholder's statement in the following format: "Merchant DBA Name" + "*" + "City/Customer support number", where: 1) "Merchant DBA Name" is up to 22 characters; 2) "*" is an asterisk; 3) "City/Customer support number" is up to 13 characters and is a description of the product, service or other descriptive information. We recommend listing the support phone number. Note: 1) and 3) should not include an asterisk. All three parts are mandatory. If the billing descriptor does not comply with the requirements listed above, the transaction will be rejected by the gateway. For a Dynamic descriptor: The merchant should be configured for Dynamic descriptor use Only the 'city' part (part 3) can be overridden with dynamic content If a merchant is not configured for Dynamic descriptor use, and if the value provided in the 'city' part does not match the static descriptor, the transaction is rejected Note: the 'Merchant DBA Name' that is sent to the card schemes is based on the name configured in Shift4's systems.
j1	YYYYMMDD	8	8	o	Date of birth of primary account recipient. Required for UK merchants with MCC 6012.
j2	[a-zA-Z0-9*]	1	10	o	Masked PAN or account number from merchant systems. Should contain either the first 6 or last 4 digits of the primary account recipient's PAN or other account identifier utilised by the merchant. May contain an asterisk. Required for UK merchants with MCC 6012.

Field	Type	Min	Max	m/o/c	Description
j3	[a-zA-Z0-9\-\ \]	2	6	o	Postal code of the primary account recipient. Required for UK merchants with MCC 6012.
j4	[a-zA-Z*]	2	6	o	Partial surname of the primary account recipient. May contain an asterisk. Required for UK merchants with MCC 6012.

Response Parameters

Field	Type	Min	Max	Description
T	timestamp	1	32	Transaction processing timestamp in the format MM/dd/yyyy HH:mm:ss
K	[0-9A-Za-z]	1	32	Unique cipher used to authenticate requests Refer to Appendix A: Message Cipher for details on generating the cipher.
M	[A-Z0-9_]	3	8	Shift4 assigned gateway merchant ID
O	[0-9]	2	2	Operation Code: 1: Sale 2: Authorisation 10: Create Token 11: Use Token Sale 12: Use Token Authorisation 23: Create Token with Sale 28: Create Token with Authorisation
d2	text	3	128	Echo parameter. Returned within the response if it was sent with the request.
g1	[a-zA-Z0-9]	1	32	Token. Token, generated by Shift4, that references a stored card profile.
z1	[a-zA-Z0-9]	1	32	Response ID.

Field	Type	Min	Max	Description
z2	[0-9]	1	3	Operation response code 0 indicates the request was successful. For any other value, see Appendix B - Response code table For the full transaction response codes, refer to Appendix B: Operation Result Codes in the Source Gateway Payment API document.
z3	text	5	256	Operation response description. Please refer to Appendix B - Response Code table For the full transaction response codes, refer to Appendix B: Operation Result Codes in the Source Gateway Payment API document.
z4	[a-zA-Z0-9]	1	10	Authorisation code.
z5	[ABC0-9]	1	6	Risk score.
z6	[A-Z0-9]	1	3	Processing response reason code. Refer to Appendix D: Processing Response Reason Codes in the Source Gateway Payment API document.
z9	[A-Z0-9]	1	2	AVS response The Address Verification Service (AVS) Authorisation response provided by the acquirer at the time of Authorisation.
z13	[a-zA-Z0-9]	1	32	Transaction ID. This identifier should be stored because it is used as a transaction reference within Shift4 reports and systems. Also referred to as the Retrieval Reference Number (RRN).
z14	[A-Z]	1	1	CVV2 response code. Valid values are: 'M' - CVV2/CVC2 Match 'N' – CVV2/CVC2 No Match 'P' – Not processed 'S' – The CVV2 should be on the card, but the merchant indicates it is not 'U' – CVV2/CVC2 Unavailable – issuer does not support this parameter 'Y' – CVC1 Incorrect '-' – Not processed

Field	Type	Min	Max	Description
z15	[0-9]	1	10	Approved billing amount, in case of a partial approval by the issuer bank. The amount is provided in the same exponent and currency as the requested amount.
z16	[0-9]	1	10	Balance response. For card-present transactions performed with debit or prepaid cards, the issuer may elect to return the current balance of the associated account. If such a value is provided by the issuer, it will be returned in this field.
z17	[A-Z]	3	3	Balance response currency. If a balance response is provided (see the description of field z16), its currency will be returned in this field.
z21	[0-9,-]	1	3	Indicates the result of sending the transaction to the Fraud Protection service. See Appendix E: z21 optional values for the list of all possible z21 result codes.
z50	[a-zA-Z0-9]	13	15	Initial transaction ID. Received as part of the initial transaction response parameters. Must be sent for every subsequent 'merchant initiated transaction' in parameter g6 (see above).
z55	[a-zA-Z0-9]	32	32	Payment ID. A unique transaction identifier that accompanies all transactions related to the same purchase.
3ds_eci	[0-9]	1	2	The ECI assigned to the authentication
3ds_cavv	[a-zA-Z0-9]	28	40	The authentication value received from the issuer
3ds_trxid	[a-zA-Z0-9]	36	36	The assigned 3D transaction ID

Field	Type	Min	Max	Description
3ds_status	[A-Z]	1	1	The result of the authentication process. Possible values: A – Attempts Processing Performed; Not Authenticated/Verified, but a proof of attempted authentication/verification is provided Y – Authentication/ Account Verification Successful N – Not Authenticated /Account Not Verified; Transaction denied R- Authentication/ Account Verification Rejected; Issuer is rejecting authentication/verification and request that authorisation not be attempted. U - Authentication/ Account Verification Could Not Be Performed, Technical or other problem I - Informational Only; Merchant challenge preference acknowledged. D - Challenge Required; Decoupled Authentication confirmed
3ds_valid_payment	Boolean	1	1	Shift4 recommendation whether to initiate payment following the authentication results
3ds_version	[0-9. /]	3	3	Indicates whether the 3D version is 1.0 or 2.0
3ds_acsurl	[a-zA-Z0-9]	0	2048	The received issuer URL for the authentication process
3ds_pareq	[a-zA-Z0-9]	0	2048	Relevant only for 3D secure 1.0 flows. Used when accessing the 3ds_acsurl

SmartGuard Fraud Protection API

The SmartGuard service enables the merchant to send a transaction to the Shift4 Fraud Protection Service to obtain a risk score. It is available for merchants integrated with the Shift4 fraud protection service **SmartGuard Plus**.

This API call must be sent before the payment API call.

Service name: getFraudScore

Request parameters: identical to the Request Parameters of a payment call.

Response parameters: identical to the Response Parameters of a payment call.

Token Transactions API

To use the Code HPP solution for processing token (Card on File) transactions, you must first obtain a PKey linked to g1 (a token generated by Shift4 that references a stored card profile received in the initial transaction, to be used with operation codes [11], [12]). This can be done either by the keyCreation.js or by a store API call. Once you have the g1, you can use the *TokenkeyCreation.js*, described below, or the *'store" API.* That is, if you want to use a token, keyCreation.js or store is used instead of `keycreation.js`; however the Initiate Payment call is the same as described in Step 2 – Initiate Payment.

TokenkeyCreation Javascript syntax

```
<script src="https://ppskey-int.credorax.com/keypayment/v2/
TokenkeyCreation.js"></script>

TokenkeyCreation("M", "RequestId", "staticKey", "g1", "b5");

pass the input parameters to the TokenkeyCreation function
```

Request Parameters

Field	Type	Min	Max	m/o/c	Comment
M	[A-Z0-9_]	3	8	m	Shift4 assigned gateway merchant ID.
RequestID	[a-zA-Z0-9\-]	36	36	o	If sent, the value will be returned in the response's ResponseID field, and can be used for tracking and error handling.
Statickey	[0-9A-Za-z]	1	32	m	A key provided to you during onboarding.
b5	[0-9]	3	3	c	Card security code (CVV / CVC) as printed on the card
g1	[a-Z0-9]	32	32	m	Token. Token, generated by Shift4, that references a stored card profile. Must be followed by op code [11] or [12] in the payment call.
3ds_getinfo	Boolean	1	1	o	Indicates whether to return the supported version of 3D secure and additional information.

Response Parameters:

Field	Type	Min	Max	m/o/c	Comment
M	[A-Z0-9_]	3	8	m	Shift4 assigned gateway merchant ID.
ResponseID	[a-zA-Z0-9\-]	36	36	o	If RequestID was sent in the request, then ResponseID=RequestID
PKey	[a-zA-Z0-9\-]	32	32	o	PCI data unique identifier provided by Shift4.
z2 [0-9]		1	4	m	Operation response code Response code: 0 indicates the request was successful. For all other values, see Appendix B - Response code table.
z3	Text	1	256	m	Response code description. Refer to Appendix B Response code table.
3ds_method	Text	1	2048	o	The issuer's URL that will be used by the 3DS Method, retrieved from the card range data repository.
3ds_version	[0-9. /]	3	3	o	Indicates whether the 3D secure version is 1.0 or 2.0
3ds_trxid	[a-zA-Z0-9, -]	36	36	o	Universally unique transaction identifier to identify a single 3D Secure transaction.

Appendix A: Message Cipher

In order to ensure data transfer authenticity, every request contains a package signature sent as parameter K. This signature contains the SHA256 hash of all the request values and the merchant's unique signature key.

Calculating the Signature

The signature is calculated as follows:

1. Sort the parameters in the following order M,O,...,c1,c11,c2, h8, h9, i10, i4,... :
   a. Numbers
   b. Capital letters
   c. Small letters

   Note: For fields with multi-digit numbers, each digit is treated as a single character. For example, '10' is not treated as 'ten', it is treated as '1' and '0' separately.

   Example: 3ds_initiate,3ds_version,M,O,...,c1,c11,c2, h8, h9, i10, i4,...
2. Replace the special characters < > " ' ( ) \ with spaces in each parameter value.
3. Remove any leading and trailing spaces in each parameter value.
4. Line up all parameter values in the same order.
5. Append the merchant's unique signature key (provided in the connectivity details) to the value list.
6. Calculate the SHA256 hash of the sorted value set.
7. Include the resulting 64-character string as the request's K parameter.

Signature Calculation Example

The following is an example of signature calculation that employs the following original request parameters:

```
M=8632876&O=1&a1=7894654&a4=1099&b1=4545454545454545&b2=1&
b3=08&b4=11&b5=003&c1=John
Smith&c3=johnsmith@yahoo.com&c10=AB12DE&d1=111.222.0.101
```

1. Sort the parameters:

   M,O,a1,a4,b1,b2,b3,b4,b5,c1,c10,c3,d1

1. Replace any special characters < > " ' ( ) \ with spaces in each parameter value.
2. Remove any leading and trailing spaces in each parameter value.
3. Line up the values:

   86328761789465410994545454545454545410811003John SmithAB1
   2DEjohnsmith@yahoo.com111.222.0.101

4. Append the signature key exactly as it appears in your connectivity details:

8632876178946541099454545454545454510811003John SmithAB1 2DEjohnsmith@yahoo.com111.222.0.101SIGNKEY1

5. Calculate the SHA256 hash of the sorted value set:

   8f03b86acd09da945e367e9f73151252cfc59a3c27ad8402bdd6e543c948232f

6. Include the signature into the request query string:

   K=8f03b86acd09da945e367e9f73151252cfc59a3c27ad8402bdd6e543c948232f&M=8632876&O=1&a1=7894654&a4=1099&b1=4545454545454545&b2=1&b3=08&b4=11&b5=003&c1=John Smith&c10=AB1 2DE&c3=johnsmith@yahoo.com&d1=111.222.0.101

   Note - all API request strings should be URL Encoded before being sent to the Gateway as part of the HTTPS POST method.

Response Signature

If a request results in a successful transaction, the Source Gateway will generate a response signature that can be validated in order to ensure the response's authenticity. In order to do so, apply the steps listed above to the response data and append your signature key (but remove the returned signature). We recommend that you check that both the generated signature and the response signature match.

Appendix B: Response Code

For the full response code list and description for 'initiate payment request' please refer to *Appendix B: Operation Result Codes* in the *Source Payment Gateway API* document.

Z2 (Response code)	Z3 (Description)
-63	The requested gateway mid is not enrolled to 3D-secure service.
-50	An error occurred during the 3D secure process
-38	The transaction has been denied by the Gateway because 3D secure Authentication failed.
-30	Transaction Failed due to error in 3D secure process
-13	The requested gateway mid is not enrolled in the 3D Secure Adviser service
-10	Internal server error. Please contact Source support.
-9	Parameter is malformed: [Field]
-7	Incorrect Gateway Response. Connection is broken
0	Request has been executed successfully
21	Merchant is not found or K is not valid
22	PKey has expired or cannot be found
23	Parameter is missing: [Field]
24	The authentication process failed
25	Transaction has been denied, please try again.
26	Transaction declined. There was a problem in the 3D-secure process.

Appendix D: Definitions & Additional Information

Term	Description
AVS	Address Verification System is a system used to verify the address of a person claiming to own a credit card. The system compares the billing address of the credit card as provided by the user with the address on file recorded by the credit card issuer. The AVS is a proven tool that helps reduce fraud and chargebacks in card-not-present transactions. AVS data is verified by issuers only, supported in the United States, Canada and the UK.
Card-on-file transactions	Transactions that involve storing credit card data for reuse in subsequent orders.
ZIP+4	An expanded ZIP code system used by the U.S. Postal Service that uses the basic five-digit code plus four additional digits.
Billing Descriptor	A billing descriptor is the mechanism that enables a cardholder to associate a record of a transaction as displayed on their statement with a specific purchase. The billing descriptor contains the name of the business (frequently referred to as “Doing Business As” or DBA) and relevant transaction information, such as the merchant location, product or transaction information. Two types of billing descriptors are supported: Static billing descriptor: Defined once and used for all transactions of a merchant. Dynamic billing descriptor: Enables some flexibility per transaction Note: Providing clear and easy to identify billing descriptors helps reduce chargebacks.

Term	Description
Dynamic billing	The Shift4 Source Payment Platform enables the use of a Dynamic Billing Descriptor to reflect a specific service that was provided to the cardholder. The billing descriptor typically contains the phone number as provided in the production connectivity details email. The following limitations apply to the Dynamic Billing Descriptor: The Billing Descriptor must always contain the Merchant DBA name value. The payment page must clearly describe the billing descriptor that will appear on the cardholder statement. The dynamic part of the descriptor (called 'City') has a maximum length of 13 characters. Prior approval from Shift4 is required to use the feature. To use a dynamic billing descriptor, the i2 field of the Source Payment API should be populated. The i2 field must contain: 'the Merchant DBA value', an asterisk, and the dynamic part (called 'city'). If a merchant is not configured for a dynamic descriptor, and if the value provided in the 'City' part does not match the static descriptor, the transaction is rejected. Note: The 'Merchant DBA Name' that is sent to the card schemes is based on the name configured in Shift4's system.

Appendix E: z21 optional values

A list of possible result codes returned in the z21 code:

Code	Description
2	Approved and within the low risk score range.
3	Approved and within the high-risk score range. Please review manually (recommended).
-97	Rejected. Risk score is above limit.
4	Approved according to the pre-defined threshold applied when the Fraud Protection service is unavailable.
-98	Rejected according to the pre-defined threshold applied when the Fraud Protection service is unavailable.
-95	The transaction was not sent to the fraud protection service due to parameter f21.
5	Approved within the low risk score range based on the f22 value.
6	Approved within the high-risk score range based on the f22 value. Please review manually (recommended).
-93	Rejected. Risk score is above the limit based on the f22 value.
7	Fraud protection service was activated for operation code 103.
-92	Fraud protection service is unavailable for operation code 103.

Appendix F: 3D Secure

3D Secure (3-Domain Secure) is an advanced method of performing Strong Customer Authentication (SCA) in card-not-present transactions. Using 3D-Secure successfully may protect you from fraud chargebacks disputes raised by cardholders and issuers.

The Source Payment Gateway offers two modules of 3D Secure:

1. Standard 3D Secure
2. Smart 3D Secure – a decision engine incorporated in the 3D Secure flow that determines whether to initiate the 3D Secure authentication process, based on risk, regulations, and impact on approval rate.

Note:

- Source's 3D Secure service supports both versions of the 3D Secure protocol: 3D Secure 1.0 and 3D Secure 2.0
- To use Source's 3D Secure service, you must be registered to the service and have it activated on your account.

Contact your account manager for more information

3D Secure and Customer Experience: Frictionless Experience vs. Cardholder Challenge

With the introduction of the 3D Secure 2.0 protocol, issuers can better asses the authenticity of a transaction based on information included in the transaction itself. This ensures cardholders enjoy a frictionless shopping and payment experience. Cardholders are not exposed to the risk checks done by the issuer in the background and are not required to provide any password or other information as they used to in the past.

In some cases, the issuer may still want to perform more extensive checks and require the cardholder to respond to a 'challenge'. The challenge can be one or more of the following: entering a one-time-password or other credentials, answering a secret question and/or identifying oneself using a biometric based device (fingerprints, face recognition, etc.). Issuers that are still using the old 3D Secure 1.0 protocol require the cardholder to respond to a challenge for every 3D Secure transaction. Source Payment Gateway 3D Secure service automatically selects the correct 3D Secure flow based on the 3D Secure protocol supported by the issuer.

3D Secure Transaction Flow

The Source Payment Gateway 3D Secure service is fully incorporated into the transaction flow of the payment request, and supports both frictionless workflows as well as challenge flows.

Note:

- The 3D Secure transaction flow may require additional steps to complete the transaction.
- For the challenge flow, consider implementing a notification mechanism to automatically retrieve updates on the transaction processing progress without having to initiate another call to do so. Contact your account manager for more details on how to enrol in this service.

The 3D Secure flow can have up to 4 steps:

1. Initiate the payment key creation (using the `keycreation.js` or the store API call). In the response you will receive the 3D secure version supported by the issuer. If the issuer supports 3D Secure 2.0, in some cases you will receive in the response an additional parameter, 3ds_method, which contains the issuer's URL for triggering device fingerprint data collection.
2. If you wish to perform a 3D Secure transaction, and in order to increase the odds for a frictionless experience, follow the instructions in Device fingerprint information retrieval flow (applicable only when the issuer URL is received).
3. To initiate the 3D Secure process, send the 3ds_initiate parameter as part of the payment request (applicable for Sale and Authorisation operations of all types)
4. In some cases, the challenge flow is required by the issuer. Refer to Initiating 3D Secure Cardholder challenge.

Initiating the 3D Secure process

The 3ds_initiate parameter can have one of the following values:

01	Initiate the standard 3D Secure process
02	Do not initiate 3D Secure for this specific transaction
03	Initiate 3D Secure with the “SMART-3D Secure” program (for more details see 3DS Adviser)
04	Only initiate the 3DS Adviser service. Relevant only for op code 98

Note:

- The transaction will only be processed if the 3D Secure process is completed successfully, whether in a frictionless flow or a challenge flow.
- When initiating Smart3DSecure, if the decision engine determines the transaction should go through the 3D Secure process, it can go through any of the standard 3D Secure flows.

Device fingerprint information retrieval flow

When device fingerprint assessment is required by the issuer, Source responds with the 3ds_method and 3ds_trxid parameters in the Payment Key Creation call.

Name	Type	Description
3ds_method	URL	The issuer's URL that should be used to trigger the collection of the device fingerprint by the issuer
3ds_trxid	[a-zA-Z0-9, -]	Universally unique transaction identifier to identify a single 3D Secure transaction.

Perform the following:

1. Upon receiving the 3ds_method and 3ds_trxid parameters, create a JSON object with the 3DS Method Data elements, as follows:

```
threeDSMethodNotificationURL = <the URL to which the issuer
will send his approval>
threeDSServerTransID = <3ds_trxid>
```

2. Encode the JSON object in Base64.
3. Render a hidden HTML iframe in the cardholder's browser and send a form with a field named `threeDSMethodData`, containing the Base64url JSON Object, via HTTP POST to the 3ds_method URL you received from Source.
4. At this stage you should get a response about the completion of the fingerprint collection process. The information should arrive at the notification URL you provided in the JSON in the `threeDSMethodNotificationURL` parameter.
5. Use the information from the response and send it in the Payment call. This is done by adding the following parameters to the payment call.

Name	Description	Type	Length	Completion Operation [92]
3ds_trxId	Universally unique transaction identifier to identify a single 3D Secure transaction.	[a-zA[Z0-9, -]	36,36	M
3ds_compind	Received from the issuer. Indicates whether device fingerprint collection completed successfully.	[Y, N]	1,1	M

Initiating 3D Secure Cardholder challenge

If you send in 3ds_initiate the values 01 or 03, the Shift4 Payment Gateway initiates the 3D Secure process as needed. The issuer decides whether to challenge the cardholder or not. You receive the challenge information as a response to the payment request (before the payment is complete). If cardholder authentication is needed, you should redirect the cardholder to the issuer's URL (issuer domain) for authentication. The redirection is an HTTP-GET request to the address given in the 3ds_acsurl parameter which is returned as part of the payment response (you can either create an iframe or do a full redirect). Note that at this stage the transaction is pending. Once the cardholder completes the authentication successfully, Shift4 automatically continues to process the transaction, and the browser is redirected back to your website. In parallel a notification is sent to your server (refer to Payment Notification).

3DS Adviser

The 3DS Adviser module offers a smart recommendation engine which routes the transaction through the 3DSecure process only when it is necessary based on regulatory, business-impact and risk aspects. You can control the 3DS Adviser functionality with the following parameters:

Name	Type	Min	Max	Description
f23	[0-9]	1	3	Assigns an ad-hoc threshold which extends the regular fraud threshold, for authorised 3D secure transactions only.

Strong Customer Authentication (SCA)

As a rule, SCA is mandatory for any electronic payment when both acquirer and issuer are in the EU.

However, some business cases do not require SCA, and in some cases you can request to exempt a specific transaction depending on the business model and the transaction's characteristics.

SCA is not required in the following business cases:

- MOTO (mail order/ telephone order) transactions

- Card is an anonymous prepaid cards
- Some cases of merchant-initiated transactions (MIT)
- Transactions where either the issuer or the acquirer is based outside the EU

Exemption management

In some cases you can request a specific transaction to be exempt from the SCA process, based on the transaction characteristics.

Name	Type	o/m	Min, Max	Description
exemption_action	[0-9]	o	2,2	Indicates the merchant preference regarding SCA exemption. Possible values are: 01: Do not request exemption. This is the default behavior for the Shift4 Gateway. If the field is absent from the transaction request, no exemption will be applied. 02: Request an exemption as part of the payment request. 03: Request an exemption as part of the 3D Secure request 04: Request exemption by default. Shift4 will apply for exemption as part of the 3D Secure request if possible. Note: If no value is provided, and you are using the 3DS Adviser module, the Shift4 Payment Gateway requests an exemption (if applicable) as part of the 3D secure process.

Name	Type	o/m	Min, Max	Description
exemption_reason	[0-9]	o	2,2	This field is required when exemption_action = 02 or 03. Possible values: 01: Low value transaction (below 30 EUR or equivalent) 02: Low risk transaction (TRA)[1] 03:Request Trusted Beneficiary Indicator (*Whitelisting*)[2] 04: Secure Corporate Cards [3] 05: Delegated Authentication [4] 06: MIT – Recurring same amount 07: MIT – other [5] 08: Trusted Beneficiary Indicator (*Whitelisting*) – Done[6] [1] Requires real-time fraud monitoring solutions [2] Use this value to indicate to the ACS to obtain confirmation from the cardholder to whitelist the merchant for future purchases [3] This is not a standard exemption you can request. If you know the card used for the transaction is a secure corporate card, use this value to indicate so to Shift4. This will help the 3DS Adviser determine the optimal 3D Secure employment. [4] This exemption option can be used if you implemented an alternative SCA solution as part of your checkout process. This requires your solution be pre-approved and registered with the card schemes. [5] Any MIT transaction must be sent with this flag to make sure the transaction will not require SCA. [6] This is not a standard exemption you can request. If you receive an indication you were whitelisted by a cardholder, use this value on any subsequent transaction by that cardholder to indicate back to the Shift4 gateway that this is a potential whitelisting card. This will help the 3DS Adviser determine the optimal 3D Secure employment.
tra_score	[0-9,A-Za-z]	c	1,8	Indicates the transaction risk analysis result calculated by a third party provider as a basis for exemption_reason=01

Managing SCA for Merchant initiated transaction

Merchant initiated transactions can occur in two business cases:

1. Recurring transaction, where the first original transaction was initiated by the cardholder (for example, initiating a subscription to a product or service). In this case the initial transaction is subject to SCA, but any subsequent transaction can be exempted from SCA.
2. Periodic charges, always initiated by the merchant, based on card details provided by the cardholder not as part of a specific transaction (for example, the cardholder provided their card details to pay utility bills). In this case all subsequent payments will be out of scope except for the initial transaction which is subjected to SCA. In order to properly identify merchant-initiated transactions we added two new parameters you should be prepared to send and receive.

Note: for recurring transactions where the first transaction occurred before 14 September 2019, use the static value = 9999999999999999. This ensures the transaction will be processed without an additional request for SCA.

Exemption – Response Parameters

Name	Type	m/o	Min,Max	Description
whitelist_status	[A-Z]	o	1,1	Y: Merchant is whitelisted by cardholder N: Merchant is not whitelisted by cardholder E: Not eligible as determined by issuer P: Pending confirmation by cardholder R: Cardholder rejected U: Whitelist status unknown, unavailable, or does not apply

Additional Response parameters for the Smart 3D Secure Module

When using the Smart 3D Secure module, additional response parameters are included in the transaction response format:

Name	Type	Min	Max	Description
smart_3ds_result	[0-2]	2	2	Describes the SMART 3D module recommendation Do 3D secure Skip 3D secure
smart_3ds_result_reason	[a-zA-Z0-9]	0	128	An array constructed of 3 sub-elements: psd2_result. Indicates whether transaction is SCA mandatory due to 3D secure. Indicates whether it is worth sending the transaction to 3D secure based on the implication of 3D on the conversion rate. 3ds_risk. Indicates whether to perform 3D secure following the risk score on the transaction.

Payment Notification (Recommended)

The notification service is recommended to better control the transaction flow through the Code HPP; it is applicable to transactions processed with 3D Secure that go through the challenge step. The notification service sends you the result of the processed transaction on a secure channel, before the shopper is redirected to the Success/Fail page.

Security of the Payment Notification

In the payment notification, Shift4 initiates an HTTP request to the merchant's server. The server address is preconfigured during setup.

The payment notification is signed with a digital signature (K) to ensure notification values' completeness.

To ensure that the notifications are sent smoothly from our servers, make sure to whitelist our notification server IPs:

Integration address	52.49.236.75 52.209.227.163
Production address	199.233.202.0/24 199.233.203.0/24

The notification is sent in the standard format of a response message. The z2 and z3 values report the payment result (see Appendix B - Response code table), and the 3ds_status value reports the 3D Secure authentication result.

Additional Parameters for Improved 3D Secure Assessment

The 3D Secure process is based on data transferred to the issuer as part of the transaction details. The more information provided at an early stage, the higher the probability for a frictionless experience for the cardholder.

Recommended Parameters

To increase the probability for a frictionless flow, the card schemes **recommend** that each request contain the maximum accurate data from the following list of parameters:

Requested Data	Shift4 Parameters	Description
Brower IP address	d1	IP address of the browser as returned by the HTTP headers. In either ipv4 or ipv6 format
Buyer email address	c3	Cardholder's email address in valid email address format, such as *joe@bloggs.com*
Billing Information	c4	Cardholder Billing Address street number
	c5	Cardholder Billing Address street name
	c7	Cardholder Billing Address city name
	c8	Cardholder Billing Address Territory Code, a level 2 country subdivision code according to ISO-3166-2. A reference list can be found at ISO 3166-1-alpha-2.
	c9	Cardholder Billing Address Country Code. Please refer to ISO 3166-1-alpha-2 for a list

Requested Data	Shift4 Parameters	Description
	c10	Cardholder Billing Address Postal/ZIP Code
Shipping information	3ds_shipaddrcity	City of the shipping address requested by the Cardholder
	3ds_shipaddrcountry	Country of the shipping address requested by the Cardholder. Please refer to ISO 3166-1-alpha-2 for a list
	3ds_shipaddrline1	First line of the street address or equivalent local portion of the shipping address associated with the card used for this purchase
	3ds_shipaddrline2	Second line of the street address or equivalent local portion of the shipping address associated with the card used for this purchase
	3ds_shipaddrpostcode	ZIP or other postal code of the shipping address associated with the card used for this purchase
	3ds_shipaddrstate	The state or province of the shipping address associated with the card used for this purchase. The value should be the country subdivision code defined in ISO 3166-2.
Do Shipping and Billing addresses match?	3ds_addrmatch	Indicates whether the Cardholder Shipping Address and Cardholder Billing Address are identical.

Request parameters

We recommend you add the following parameters to your payment request when you use the 3D Secure functionality (3ds_initiate = 01 or 03):

Name	Description	Type	min	max	m/o/c
3ds_channel	Indicates the type of channel interface being used to initiate the transaction. The accepted values are: 01 - App-based (APP) 02 - Browser (BRW) 03 - 3DS Requestor Initiated (3RI)	[0-3]	2	2	o
3ds_redirect_url	Contains the merchant URL to which the browser should be redirected after the challenge session	[a-zA-Z0-9]	0	2048	m
3ds_category	Identifies the category of the message for a specific use case. The accepted values are: 01 - PA (Payment authentication) 02 - NPA (NON-payment authentication) 80 – Data only (Mastercard only, valid only for 3ds_channel = 01 or 02)	[0-3]	2	2	o
3ds_compind	Relevant only if 3ds_channel = 02. Received as part of the op code 92 flow.	[Y,N,U]	1	1	c m when 3ds_channel = 02)
3ds_sdkinterface	Specifies the SDK Interface types that the device supports for displaying specific challenge user interfaces within the SDK. Accepted values are: 01 - Native 02 - HTML 03 - Both	[0-3]	2	2	c m only when 3ds_channel=01 (APP).

Name	Description	Type	min	max	m/o/c
3ds_sdkuitype	Contains a list of all UI types that the device supports for displaying specific challenge user interfaces within the SDK. Accepted values for each UI type are: 01 - Text 02 - Single select 03 - Multi select 04 - OOB 05 - Html Other (valid only for HTML UI) For Native UI SDK Interface accepted values are 01-04 and for HTML UI accepted values are 01-05.	Comma separated list	2	14	c m only when 3ds_channel=01 (APP).
3ds_msgextensionid	A unique identifier for the extension. Payment System Registered Application Provider Identifier (RID) is required as prefix of the ID. The maximum length is 64 characters.	[a-zA-Z0-9]	0	64	o
3ds_msgextensinoname	The name of the extension data set as defined by the extension owner. The maximum length is 64 characters.	[a-zA-Z0-9]	0	64	o
3ds_msgextensiondata	The data carried in the extension. The maximum length is 8059 characters.	[a-zA-Z0-9]	0	8059	o

Name	Description	Type	min	max	m/o/c
3ds_reqauthmethod	Information about how the cardholder was authenticated before or during the transaction. The mechanism used by the Cardholder to authenticate to the merchant. Accepted values are: 01 - No authentication occurred (i.e., cardholder "logged in" as guest) 02 - Login to the cardholder account at the merchant system using merchant's own credentials 03 - Login to the cardholder account at the merchant system using federated ID 04 - Login to the cardholder account at the merchant system using issuer credentials 05 - Login to the cardholder account at the merchant system using third-party authentication 06 - Login to the cardholder account at the merchant system using FIDO Authenticator 07 - Login to the cardholder account at the merchant system using FIDO Authenticator (applicable for 3DS version 2.2 and above) 08 - SRC Assurance Data. (applicable for 3DS version 2.2 and above)	[0-6]	2	2	o
3ds_reqauthtimestamp	Date and time in UTC of the cardholder authentication. Field is limited to 12 characters and the accepted format is YYYYMMDDHHMM	[0-9]	12	12	o
3ds_reqauthdata	Data that documents and supports a specific authentication process. The intention is that for each merchant Authentication Method, this field contains data that the issuer can use to verify the authentication process.	[a-zA-Z0-9]	0	255	o

Name	Description	Type	min	max	m/o/c
3ds_reqchallengeind	Indicates whether a challenge is requested for this transaction. For example: For 3ds_category 01-PA, a merchant may have concerns about the transaction, and request a challenge. For 3ds_category 02-NPA, a challenge may be necessary when adding a new card to a wallet. 01 - No preference 02 - No challenge requested 03 - Challenge requested by merchant 04 - Challenge requested: Mandate 05 - No Challenge Requested, transactional risk analysis is already performed 06 - No Challenge Requested, Data share only 07 - No Challenge Requested, SCA is already performed 08 - No challenge requested (utilise whitelist exemption if no challenge required) 09 - Challenge requested (whitelist prompt requested if challenge required)	[0-4]	2	2	o
3ds_reqpriorref	This data element provides additional information to the issuer to determine the best approach for handling a request. The element contains the issuer's Transaction ID for a prior authenticated transaction (for example, the first recurring transaction that was authenticated with the cardholder).	[a-zA-Z0-9]	36	36	o
3ds_reqpriorauthmethod	Mechanism used by the Cardholder to previously authenticate to the merchant. Accepted values for this field are: 01- Frictionless authentication occurred by issuer 02 - Cardholder challenge occurred by issuer 03 - AVS verified 04 - Other issuer methods	[0-4]	2	2	o

Name	Description	Type	min	max	m/o/c
3ds_reqpriorauthtimestamp	Date and time in UTC of the prior authentication. Accepted date format is YYYYMMDDHHMM.	[0-9]	12	12	0
3ds_reqpriorauthdata	Data that documents and supports a specific authentication process. In the current version of the specification this data element is not defined in detail, however the intention is that for each merchant Authentication Method, this field carry data that the issuer can use to verify the authentication process. In future versions of the application, these details are expected to be included. Field is limited to a maximum of 2048 characters.	[a-zA-Z0-9]	0	255	o
3ds_reqdecreqind	Indicates whether the merchant requests the ACS to utilise Decoupled Authentication and agrees to utilise Decoupled Authentication if the ACS confirms its use. Accepted values are: Y - Decoupled Authentication is supported and preferred if challenge is necessary N - Do not use Decoupled Authentication.	[Y,N]	1	1	o
3ds_reqdecmaxtime	Indicates the maximum amount of time (in minutes) that the merchant will wait for an ACS to provide the results of a Decoupled Authentication transaction. Valid values are between 1 and 10080.	[0-9]	1	5	o
3ds_chaccdate	Date that the cardholder opened the account with the merchant. Date format = YYYYMMDD.	[0-9]	8	8	o
3ds_chaccchangeind	Length of time since the cardholder's account information with the merchant was last changed. Includes Billing or Shipping address, new payment account, or new user(s) added. Accepted values are: 01 - Changed during this transaction 02 - Less than 30 days 03 - 30 - 60 days 04 - More than 60 days	[0-4]	2	2	o

Name	Description	Type	min	max	m/o/c
3ds_chaccchange	Date that the cardholder's account with the merchant was last changed. Includes Billing or Shipping address, new payment account, or new user(s) added. Date format = YYYYMMDD.	[0-9]	8	8	o
3ds_chaccpwchangeind	Length of time since the cardholder's account with the merchant had a password change or account reset. The accepted values are: 01 - No change 02 - Changed during this transaction 03 - Less than 30 days 04 - 30 - 60 days 05 - More than 60 days	[0-5]	2	2	o
3ds_chaccpwchange	Date that cardholder's account with the merchant had a password change or account reset. Date format must be YYYYMMDD.	[0-9]	8	8	o
3ds_shipaddressusageind	Indicates when the shipping address used for this transaction was first used with the merchant. Accepted values are: 01 - This transaction 02 - Less than 30 days 03 - 30 - 60 days 04 - More than 60 days.	[0-4]	2	2	o
3ds_shipaddressusage	Date when the shipping address used for this transaction was first used. Date format must be YYYYMMDD.	[0-9]	8	8	o
3ds_txnactivityday	Number of transactions (successful and abandoned) for this cardholder account with the merchant across all payment accounts in the previous 24 hours.	[0-9]	0	10	o
3ds_txnactivityyear	Number of transactions (successful and abandoned) for this cardholder account with the merchant across all payment accounts in the previous year.	[0-9]	0	10	o
3ds_provisionattemptsday	Number of Add Card attempts in the last 24 hours.	[0-9]	0	10	o

Name	Description	Type	min	max	m/o/c
3ds_nbpurchaseaccount	Number of purchases with this cardholder account during the previous six months.	[0-9]	0	10	o
3ds_suspiciousaccactivity	Indicates whether the merchant has experienced suspicious activity (including previous fraud) on the cardholder account. Accepted values are: 01 - No suspicious activity has been observed 02 - Suspicious activity has been observed	[0-2]	2	2	o
3ds_shipnameindicator	Indicates whether the Cardholder Name on the account is identical to the shipping Name used for this transaction. Accepted values are: 01 - Account Name identical to shipping Name 02 - Account Name different from shipping Name	[0-2]	2	2	o
3ds_paymentaccind	Indicates the length of time that the payment account was enrolled in the cardholder's account with the merchant. Accepted values are: 01 - No account (guest check-out) 02 - During this transaction 03 - Less than 30 days 04 - 30 - 60 days 05 - More than 60 days	[0-5]	2	2	o
3ds_paymentaccage	Date that the payment account was enrolled in the cardholder's account with the merchant. Date format must be YYYYMMDD.	[0-9]	8	8	o
3ds_accid	Additional information about the account optionally provided by the merchant.	[a-zA-Z0-9]	0	64	o
3ds_whiteliststatus	Sets the whitelisting status of the merchant. Accepted values are: Y - Merchant is whitelisted by cardholder N - Merchant is not whitelisted by cardholder	[Y, N]	1	1	o
3ds_paytokenind	This field has a value of "true" if the transaction was de-tokenised prior to being received by Shift4.	[a-z]	4	5	o

Name	Description	Type	min	max	m/o/c
3ds_addrmatch	Indicates whether the Cardholder Shipping Address and Cardholder Billing Address are identical. Accepted values: true- Shipping Address matches Billing Address false - Shipping Address does not match Billing Address Note: the default value of this field is 'false'	[a-z]	4	5	o
3ds_homephonecountry	Country Code of the home phone.	[0-9]	1	3	o
3ds_chmobilephone	The mobile phone provided by the Cardholder, without the country code	[0-9]	0	18	o
3ds_mobilephonecountry	Country Code of the mobile phone.	[0-9]	1	3	o (m if 3ds_chmobilephone exists)
3ds_chworkphone	The work phone provided by the Cardholder, without the country code	[0-9]	0	18	o
3ds_workphonecountry	Country Code of the work phone.	[0-9]	1	3	o (m if 3ds_chworkphone exists)
3ds_shipaddrcity	City of the shipping address requested by the Cardholder.	[a-zA-Z]	3	32	o
3ds_shipaddrcountry	Country of the shipping address requested by the Cardholder. Please refer to ISO 3166-1-alpha-2 for a list.	[A-Z]	2	2	c m – if 3ds_shipaddrstate exists or if shipping information is not the same as billing information

Name	Description	Type	min	max	m/o/c
3ds_shipaddrline1	First line of the street address or equivalent local portion of the shipping address associated with the card used for this purchase.	[a-zA-Z]	0	50	o m – when 3ds_addrmatch = false
3ds_shipaddrline2	Second line of the street address or equivalent local portion of the shipping address associated with the card used for this purchase.	[a-zA-Z]	0	50	o m – when 3ds_addrmatch = false
3ds_shipaddrpostcode	ZIP or other postal code of the shipping address associated with the card used for this purchase.	[a-z0-9]	0	16	o m – when 3ds_addrmatch = false
3ds_shipaddrstate	The state or province of the shipping address associated with the card used for this purchase. The value should be the country subdivision code defined in ISO 3166-2.	[0-9]	3	3	o m – when 3ds_addrmatch = false

Name	Description	Type	min	max	m/o/c
3ds_shipindicator	Indicates shipping method chosen for the transaction. Merchants must choose the Shipping Indicator code that most accurately describes the cardholder's specific transaction. If one or more items are included in the sale, use the Shipping Indicator code for the physical goods, or if all digital goods, use the code that describes the most expensive item. Accepted values are: 01 - Ship to cardholder's billing address 02 - Ship to another verified address on file with merchant. In this case, shipping information is required even though 3ds_addrmatch = true. 03 - Ship to address that is different from the cardholder's billing address. In this case, shipping information is required even though 3ds_addrmatch = true. 04 - "Ship to Store" / Pick-up at local store (store address is populated in the shipping address fields). In this case, shipping information is required even though 3ds_addrmatch = true. 05 - Digital goods (includes online services, electronic gift cards and redemption codes) 06 - Travel and Event tickets, not shipped 07 - Other (for example, Gaming, digital services not shipped, emedia subscriptions, etc.)	[0-7]	2	2	o
3ds_deliverytimeframe	Indicates the merchandise delivery timeframe. Accepted values are: 01 - Electronic Delivery 02 - Same day shipping 03 - Overnight shipping 04 - Two-day or more shipping	[0-4]	2	2	o
3ds_deliveryemailaddress	For electronic delivery, the email address to which the merchandise was delivered.	email	7	64	o

Name	Description	Type	min	max	m/o/c
3ds_reorderitemsind	Indicates whether the cardholder is reordering previously purchased merchandise. Accepted values are: 01 - First time ordered 02 - Reordered	[0-2]	2	2	o
3ds_preorderpurchseind	Indicates whether the cardholder is placing an order for merchandise with a future availability or release date. Accepted values are: 01 - Merchandise available 02 - Future availability	[0-2]	2	2	o
3ds_preorderdate	For a pre-ordered purchase, the expected date that the merchandise will be available. Date format must be YYYYMMDD.	[0-9]	8	8	o
3ds_giftcardamount	For a prepaid or gift card purchase, the purchase amount total of the prepaid or gift card(s) in major units (for example, USD 123.45 is 123).	[0-9]	1	12	o
3ds_giftcardcurr	For a prepaid or gift card purchase, the currency code of the card as defined in ISO 4217-alpha-3 except for 955 - 964 and 999.	[0-9]	3	3	o
3ds_giftcardcount	For a prepaid or gift card purchase, the total count of the individual prepaid or gift cards/codes purchased. Field is limited to 2 characters.	[0-9]	0	2	o
3ds_purchasedate	Date and time of the purchase expressed in UTC. The field is limited to 14 characters, formatted as YYYYMMDDHHMMSS.	[0-9]	14	14	m
3ds_recurringexpiry	Date after which no further authorisations shall be performed. This field is limited to 8 characters, and the accepted format is YYYYMMDD. This field is required if 3ds_reqchallengeind = 02 or 03.	[0-9]	8	8	c

Name	Description	Type	min	max	m/o/c
3ds_recurringfrequency	Indicates the minimum number of days between authorisations. The field is limited to 4 characters. This field is required if 3ds_reqchallengeind = 02 or 03.	[0-4]	0	4	c
3ds_transtype	Identifies the type of transaction being authenticated. The values are derived from ISO 8583. Accepted values are: 01 - Goods / Service purchase 03 - Check Acceptance 10 - Account Funding 11 - Quasi-Cash Transaction 28 - Prepaid activation and Loan	[0-9]	2	2	o
3ds_merchantname	Assigned merchant name	[a-zA-Z0-9]	0	32	o
3ds_browseracceptheader	Exact content of the HTTP accept headers.	[a-zA-Z0-9]	0	2048	o m if 3ds_channel=02
d1	IP address of the browser as retuned by the HTTP headers. Supports both ipv4 & ipv6 formats.	ip	7	48	c m for Visa 3DS transactions m if 3ds_channel=02
3ds_browserjavaenabled	Boolean (true/false) that represents the ability of the cardholder browser to execute Java. This field is required for requests where 3ds_channel = 02 (Browser).	[a-z]	4	5	o m if 3ds_channel=02
3ds_browserjavascriptenabled	Boolean that represents the ability of the cardholder browser to execute JavaScript. Accepted values are true / false	[a-z]	4	5	o m if 3ds_channel=02

Name	Description	Type	min	max	m/o/c
d6	Value representing the browser language as defined in IETF BCP47.	[A-Za-z]	2	16	o m if 3ds_channel =02
3ds_browsercolordepth	Value representing the bit depth of the colour palette for displaying images, in bits per pixel. Accepted values are: 1 - 1 bit 4 - 4 bits 8 - 8 bits 15 - 15 bits 16 - 16 bits 24 - 24 bits 32 - 32 bits 48 - 48 bits	[0-9]	1	2	o m if 3ds_channel =02
3ds_browserscreenheight	Total height of the Cardholder's screen in pixels.	[0-9]	1	6	c m for Visa 3DS transactions m if 3ds_channel =02
3ds_browserscreenwidth	Total width of the Cardholder's screen in pixels.	[0-9]	1	6	c m for Visa 3DS transactions m if 3ds_channel =02
3ds_browsertz	Time difference between UTC time and the Cardholder browser local time, in minutes.	[0-9,-]	1	5	o m if 3ds_channel =02

Name	Description	Type	min	max	m/o/c
d5	Exact content of the HTTP user-agent header.	[a-zA-Z0-9]	5	255	o m if 3ds_channel =02
3ds_challengewindowsize	Dimensions of the challenge window that will be displayed to the cardholder. The issuer replies with content that is formatted to appropriately render in this window to provide the best possible user experience. Preconfigured window sizes are given in “width x height” in pixels. Accepted values are: 01 - 250 x 400 02 - 390 x 400 03 - 500 x 600 04 - 600 x 400 05 - Full screen	[0-5]	2	2	o m if 3ds_channel =02
3ds_sdkappid	Universally unique ID created upon all installations and updates of the merchant App on a customer device. This is newly generated and stored by the 3DS SDK for each installation or update. The field must have a canonical form as defined in IETF RFC 4122.	[0-9a-zA-Z]	0	36	o m if 3ds_channel =01
3ds_sdkencdata	JWE object, as a string containing data encrypted by the SDK for the DS to decrypt. The field is sent from the SDK. The data will be present when sending to DS, but not present from DS to ACS.	[0-9a-zA-Z]	0	64k	o m if 3ds_channel =01
3ds_sdkephempubkey	Public key component of the ephemeral key pair generated by the 3DS SDK and used to establish session keys between the 3DS SDK and ACS.	[0-9a-zA-Z]	0	255	o m if 3ds_channel =01
3ds_sdkmaxtimeout	The maximum amount of time (in minutes) for all exchanges. The value must be greater than or equal to 05.	[0-9]	2	2	o m if 3ds_channel =01

Name	Description	Type	min	max	m/o/c
3ds_sdkreferencenumber	Identifies the vendor and version of the 3DS SDK that is integrated in a merchant app, assigned by EMVCo when the 3DS SDK is approved.	[0-9a-z]	0	32	o m if 3ds_channel =01
3ds_sdktransid	Universally unique transaction identifier assigned by the 3DS SDK to identify a single transaction. The field must have a canonical form as defined in IETF RFC 4122.	[0-9]	0	36	o m if 3ds_channel =01

Response parameters

Name	Description	Type	min	max	m/o/c
3ds_whiteliststatussource	Is populated by the Whitelist Status system setting. Possible values: 01 = 3DS Server 02 = DS 03 = ACS 04-79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) 80-99 = Reserved for DS use Note: This is a response parameter only	[0-9]	2	2	o

Change History

Version	Subject/Date	Description
2.6 rev 1	May 2024	Changed the requirement of the following parameters from o to c - m for Visa 3ds transactions: • c1 • c2 • c3 • d1 • 3ds_browserscreenheight • 3ds_browserscreenwidth
2.6	November 2023	Rebrand to Shift4
2.5	February 2022	Added b20 to the Response Parameters list Corrected the TokenkeyCreation Javascript syntax and production address Updated “Appendix A: Message Cipher” Changed c1 from optional to recommended Removed 3dssmart_plan parameter Removed M, K, O, g5 from “Device fingerprint information retrieval flow”
2.4	September 2021	Changed code examples that contained v1 in their paths to v2
2.3	December 2020	Addition of 3DS v2.2-related Decoupled Authentication, Whitelisting and Authentication fields and settings as well as several other small changes and additions.
2.2 rev 1	July 2020	Changed IP addresses for any communication to or from your system
2.2	May 2020	Removed 3ds_smarttype & 3ds_smartplan parameters Added z55 response parameter
2.1 rev 2	January 2020	Updated the Frictionless flow diagram and minor text changes
2.1 rev 1	November 2019	Added IP address for integration environment to be whitelisted on merchant side
2.1	September 2019	Added information about g6 & z50 parameters Added Strong Customer Authentication (SCA) requirements Changes in exemption chapter Minor changes in API formats
2.0	March 2019	Support of 3D Secure 2.0 and Smart 3D Secure

Version	Subject/Date	Description
1.7 rev 2	October 2018	Updated the result in step 6 in the example of the Cypher calculation
1.7 rev 1	June 2018	Updated Integration addresses and Production addresses Added examples for several API calls Added information about the Token Transactions call
1.6 rev 2	April 2017	Changed the payment response field 3DSecureStatus to ThreeDSecureStatusBehavior Changed the ECI return values format
1.6	April 2017	Added information about f21 & f22 parameters Added information about new response code z21 Added information about getFraudScore call Fixed the integration environment address
1.5	Jan. 2017	Added information on how to use token in the code solution and minor corrections to the documentation
1.4	Sep. 2017	Changed the Address of production environment Clarification about transaction type when enrolment response is N.
1.3	18/6/2017	Added information about operation codes 10, 23, 28.
1.2	24/4/2017	URL updated. New error code -10. SSL changed to TLS.
1.1	5/4/2017	Change 3DSecureStatusBehavior to ThreeDSecureStatusBehavior.
1.0	29/3/2017	Created.

Support Information

US: +1.617.715.1977

UK: +44.20.3608.1288

EU: +356.2778.0876

Email: support.europe@shift4.com